Dynamic Attributes Connector

The following topics discuss how to configure and use the Dynamic Attributes Connector.

About the Dynamic Attributes Connector

The dynamic attributes connector enables your access control 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:

Table 1: List of supported connectors by dynamic attributes connector version and platform

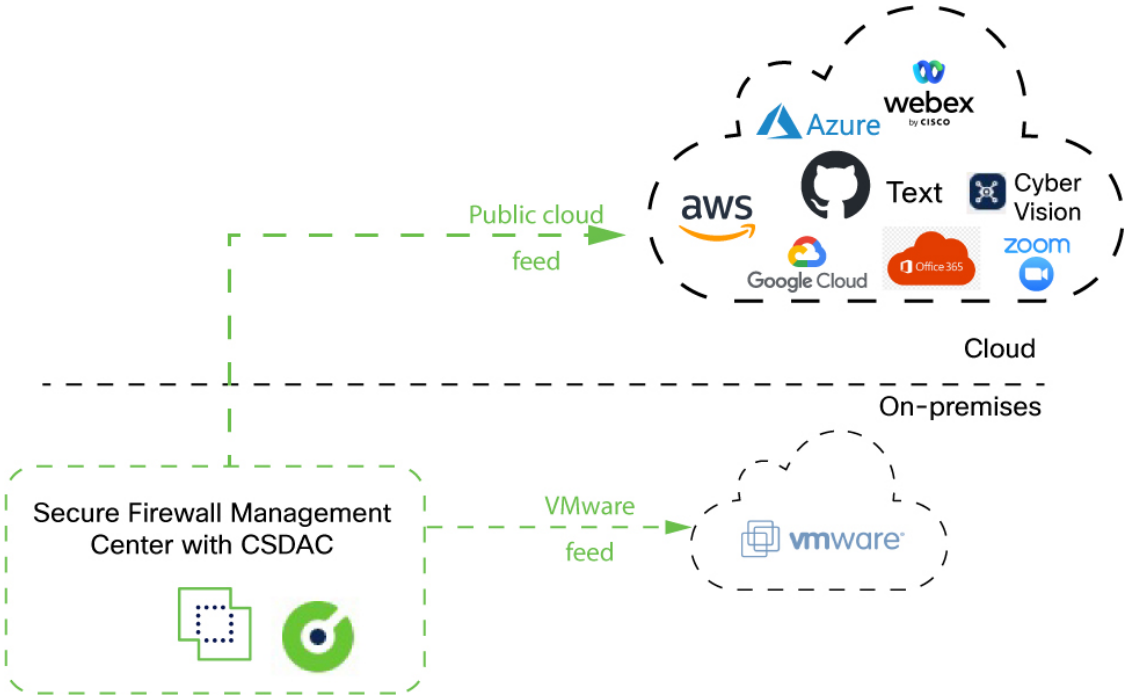
CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

How it works

This topic discusses the architecture of the Dynamic Attributes Connector.

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



- The system supports certain public cloud providers.

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

- The dynamic attributes connector is provided with Secure Firewall Management Center.

Related topics

- Enable the dynamic attributes connector
- About the dashboard, on page 7

History for the dynamic attributes connector

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New connectors	7.6	20241127	AWS security groups, AWS service tags, and Cisco Cyber Vision These connectors can send an on-premises Secure Firewall Management Center dynamic objects as can Security Cloud Control. To receive dynamic objects from an on-premises dynamic attributes connector, version 3.0 of the on-premises dynamic attributes connector is required.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dynamic Attributes Connector	7.4.0	7.4.0	This feature is introduced. The Dynamic Attributes Connector is now included in the Secure Firewall Management Center. You can use the dynamic attributes connector to get IP addresses from cloud-based platforms such as Microsoft Azure in access control rules without having to deploy to managed devices. More information: • The dynamic attributes connector included with this product: About the Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: *Cisco Secure Dynamic Attributes Connector Configuration Guide* New/modified screen: **Integration** > **Dynamic Attributes Connector**

System requirements for the Dynamic Attributes Connector

The Dynamic Attributes Connector has the following memory requirements:

FMCv: Amount of RAM	Secure Firewall Management Center hardware model	Maximum number of (connectors + Azure AD realms)
At least 32 GB	Firepower 1000, Firepower 1600, vFMC	10
At least 64 GB	Firepower 2500, Firepower 2600,vFMC 300	20
At least 128 GB	Firepower 4500, Firepower 4600	30

The preceding limits apply to both virtual machines and physical machines.

The system prevents you from exceeding these limits to avoid deployment issues.

Enable the dynamic attributes connector

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access control rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

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

Step 3 Slide to **Enabled**.

Step 4 Messages are displayed while the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

Configure networks and subnets for Docker containers

The Dynamic Attributes Connector uses Docker containers to retrieve connector data in the Secure Firewall Management Center. To avoid conflicts with the Secure Firewall Management Center management interface and other IP addresses used in your network, you can optionally use the command discussed in this section to change Docker IP addresses and ranges.

About Docker networks

The Docker daemon is used by the dynamic attributes connector requires the following networks:

- `docker0` which is used internally by the Docker daemon.
- A series of IPv6 networks named `veth`*`number`*.

  These are internal bridge networks used by the dynamic attributes connector.
- Docker bridge networks used by dynamic attributes connector connectors named `br-`*`number`*.

Before you enable the dynamic attributes connector, there is only one Docker interface, named `docker0`, set to 172.18.0.1/16 (for a Secure Firewall Management Center Virtual; on-premises managers use different IP address ranges). The table in the Examples section provides details.

Change Docker networks and subnets

First enable the dynamic attributes connector as discussed in Enable the dynamic attributes connector.

To change Docker networks and subnets, run `/usr/local/sf/bin/change_docker_subnet.sh -b` *`CIDR-network`* `-s` *`address-pool-size`* as a user with `root` privileges where:

- `-b` *`CIDR-network`* sets a network base address pool in CIDR notation.
- `-s` *`address-pool-size`* sets a netmask for the network base address. You can use this option to limit the number of addresses in a base address range in the event the network range overlaps existing network ranges; in particular, we recommend certain `-s` values for Secure Firewall Management Center models to make sure you don't exceed the available RAM in the machine. (Docker containers are used by dynamic attributes connector connectors and those limits are shown in System requirements for the Dynamic Attributes Connector, on page 4.)

Important The networks you assign to Docker must be in an internal network range and must *not* conflict with networks used by the Secure Firewall Management Center or by other devices in your internal network.

Examples

The following table shows examples.

Secure Firewall Management Center model	Recommended -s value	Sample -b value	Dynamic Attributes Connector container addresses used
Firepower 1000, Firepower 1600, vFMC	27 (netmask 255.255.255.224)	172.19.0.0/16	30 IP addresses `docker0`: 172.19.0.1 Bridge networks `br-number` gateway `172.19.0.33` with subnet `172.19.0.32/27` Connectors created in networks like `172.19.0.38/27`, `172.19.0.39/27`, and so on
Firepower 2500, Firepower 2600, vFMC 300	26 (netmask 255.255.255.192)	192.168.0.0/16	62 IP addresses `docker0`: 192.168.1.1 Bridge networks `br-number` gateway `192.168.1.65`with subnet `192.168.1.64/26` Connectors created in networks like `192.168.1.71/26`, `192.168.1.72/26`, and so on
Firepower 4500, Firepower 4600	25 (netmask 255.255.255.128)	192.168.0.0/16	126 IP addresses `docker0`: 192.168.1.1 Bridge networks `br-number` gateway `192.168.1.129`with subnet `192.168.1.128/25` Connectors created in networks like `192.168.1.136/25`, `192.168.1.135/25`, and so on

For reference, the complete commands follow:

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

Verify the networks

To verify your network settings, enter `sudo docker network inspect muster-net`. The command results are displayed in JSON format.

Troubleshoot

Following are some solutions to common errors you might encounter using this command.

Error: `Pull subnet value can not be greater than size`

Solution: Change the value of `-s` so it is less than the CIDR network value.

For example,

INCORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

CORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

Error: After running the command, the Docker networks are wrong.

Solution: Restart the Docker daemon: `sudo pmtool restartbyid docker`

Error: **`Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?`**

Solution: Restart Docker: `pmtool restartbyid docker`

Error: Input can't be empty

The `-s` parameter is required.

Error: **`Pull size - 32 - can not be greater than 32 or less than 0`**

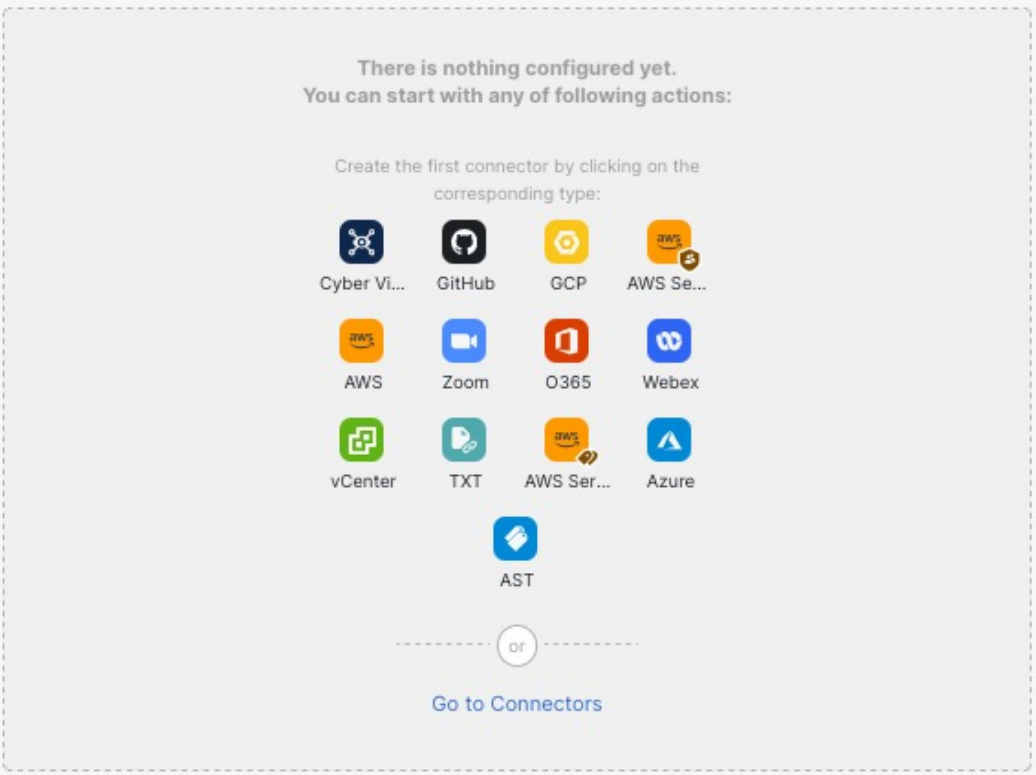
Solution: Change the value of `-s` so it is greater than 0 and less than 32.

About the dashboard

To access the dynamic attributes connector dashboard, log in to the Secure Firewall Manager and click **Integration** > **Dynamic Attributes Connector** at the top of the page.

If the dynamic attributes connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

The dynamic attributes connector Dashboard page displays the status of your connectors, adapters, and filters at a glance. Following is an example of the Dashboard of an unconfigured system:



Among the things you can do with the Dashboard are:

- Add, edit, and delete connectors and dynamic attributes filters.

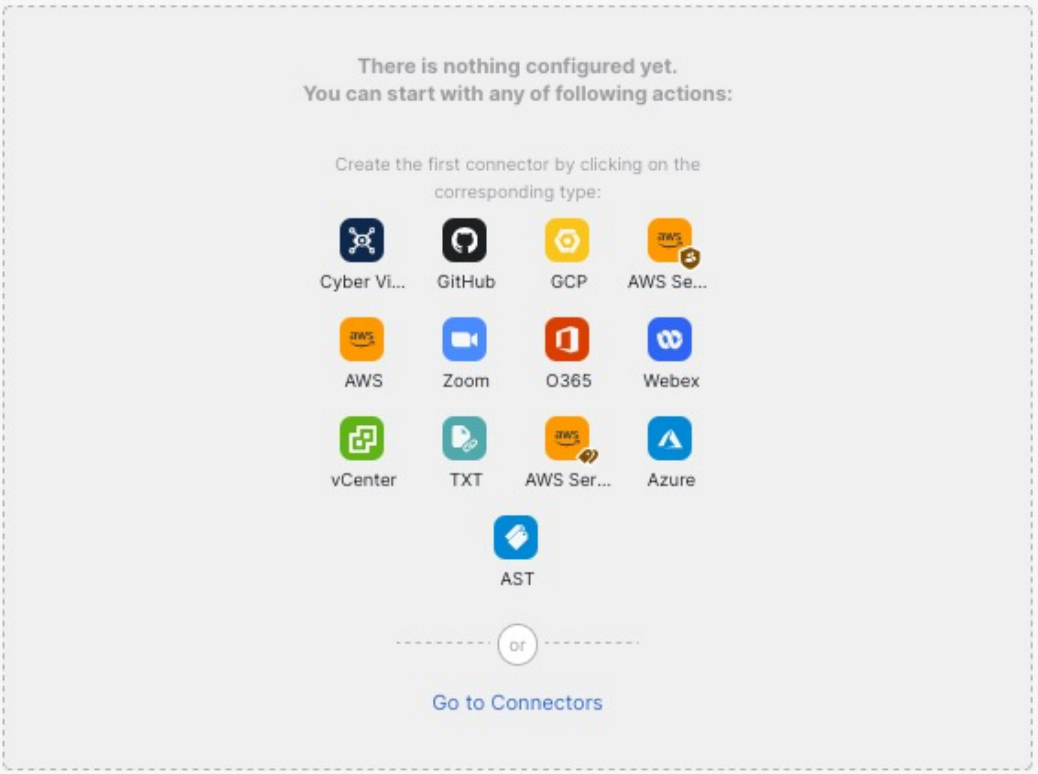
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

Related Topics

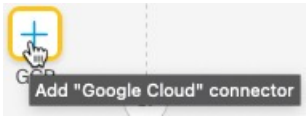
- Dashboard of an unconfigured system, on page 8
- Dashboard of a configured system, on page 9
- Add, edit, or delete connectors, on page 10
- Add, edit, or delete dynamic attributes filters, on page 12

Dashboard of an unconfigured system

Sample dynamic attributes connector Dashboard page of an unconfigured system:



The Dashboard initially displays all the types of connectors you can configure for your system. You can do any of the following:

- Hover the mouse pointer over a connector and click 

to create a new one.
- Click **Go to Connectors** to add, edit, or delete connectors (good for creating, editing, or deleting multiple connectors at the same time).

For more information, see Create a connector, on page 13.

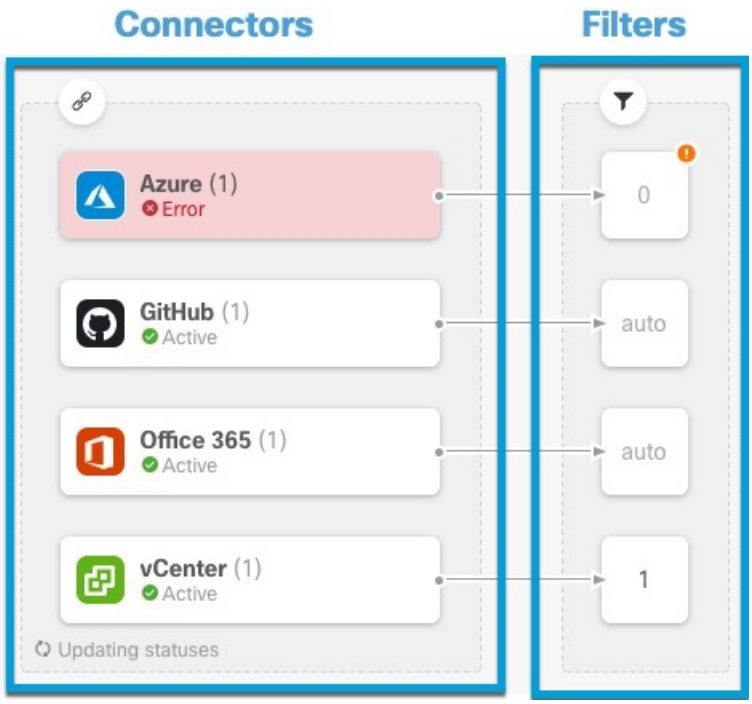
Related Topics:

- Dashboard of a configured system, on page 9
- Add, edit, or delete connectors, on page 10
- Add, edit, or delete dynamic attributes filters, on page 12

Dashboard of a configured system

Sample dynamic attributes connector Dashboard page of a configured system:

Click an area in the figure to learn more about it or click one of the links following the figure.



1 Create a connector, on page 13
2 Create dynamic attributes filters, on page 36

The Dashboard shows the following (from left to right):

Connectors column	Filters column
List of connectors with a number indicating how many of each type are configured. Connectors collect dynamic attributes that could be sent to the Secure Firewall Manager. Dynamic attributes filters specify what data is sent. Click to view more information about all configured connectors. You can also click the name of a connector to add, edit, or delete connectors; or to view detailed information about them. For more information, see Add, edit, or delete connectors, on page 10.	List of dynamic attributes filters associated with each connector with a number indicating how many of each filter are associated with a connector. Click to view more information about all configured filters. You can also click the name of a filter to add, edit, or delete filters; or to view detailed information about them. For more information, see Add, edit, or delete dynamic attributes filters, on page 12.

Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

The Dashboard indicates whether or not an object is available. The Dashboard page is refreshed every 15 seconds but you can click **Refresh** ( ) at the top of the page at any time to refresh immediately. If issues persist, check your network connection.

Related Topics:

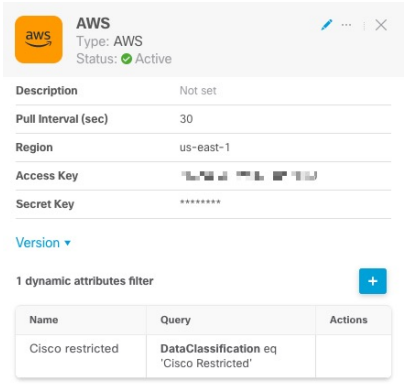
- Add, edit, or delete connectors, on page 10
- Add, edit, or delete dynamic attributes filters, on page 12

Add, edit, or delete connectors

The Dashboard enables you to view or edit connectors. You can click the name of a connector to view all instances of that connector or you can click for the following additional options:

- **Go to Connectors** to view all connectors at the same time; you can add, edit, and delete connectors from there.
- **Add Connector** > ***type*** to add a connector of the indicated type.

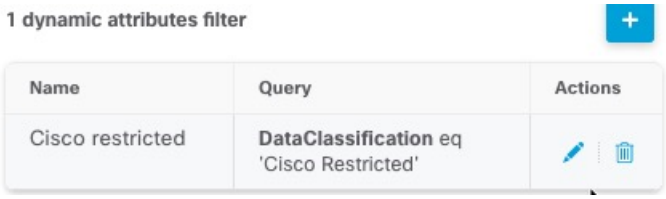
Click any connector in the connectors column ( ) to display more information about it; an example follows:



You have the following options:

- Click the Edit icon ( ) to edit this connector.
- Click the More icon ( ) for additional options.
- Click to close the panel.
- Click **Version** to display the version of the . You can optionally copy the version to the clipboard if necessary for Cisco TAC.

The table at the bottom of the panel enables you to add dynamic attributes filters; or to edit or dynamic attributes connector delete connectors. A sample follows:



Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters, on page 36.

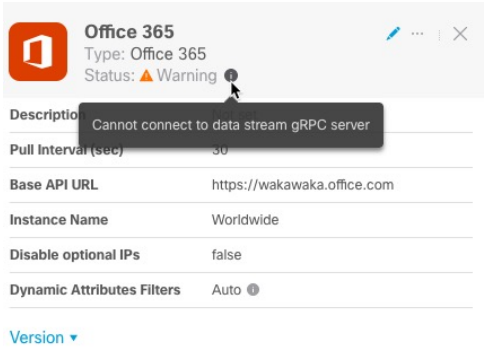
Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

View error information

To view error information for a connector:

1. On the Dashboard, click the name of the connector that is displaying the error.
2. In the right pane, click **Information** ( ).

   An example follows.



3. To resolve this issue, edit the connector settings as discussed in Create an Office 365 connector, on page 30.
4. If you cannot resolve the issue, click **Version** and copy the version to a text file.
5. Provide all of this information to Cisco TAC.

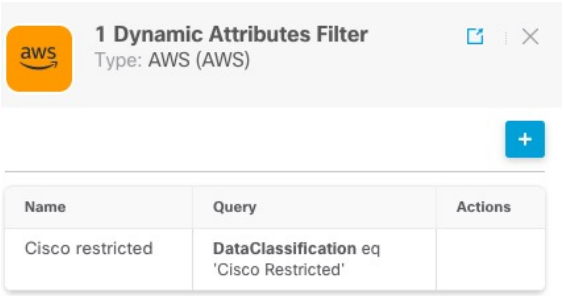
Add, edit, or delete dynamic attributes filters

The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click  for the following additional options:

- **Go to Dynamic Attributes Filters** to view all configured dynamic attributes filters. You can add, edit, or delete dynamic attributes filters from there.
- **Add Dynamic Attributes Filters** to add a filter.

For more information about adding dynamic attributes filters, see Create dynamic attributes filters, on page 36.

An example follows:



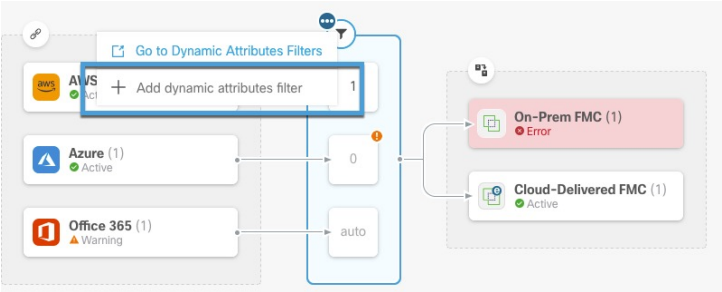
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have the following options:

- Click a filter instance to view summary information about dynamic attributes filters associated with a connector.
- Click the Add icon ( ) to add a new dynamic attributes filter.

  For more information, see Create dynamic attributes filters, on page 36.
- Click in the filters column ( ) indicates the indicated connector has no associated dynamic attributes filters. Without associated filters, the connector can send nothing to Firewall Management Center.

  One way to resolve the issue is to click in the filters column and click **Add Dynamic Attributes Filter**. A sample follows.



- Click to add, edit, or delete filters.
- Click to close the panel.

Create a connector

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

We support the following:

Table 2: List of supported connectors by dynamic attributes connector version and platform

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

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Amazon Web Services connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from AWS to Secure Firewall Management Center 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 Secure Firewall Management Center . For a list of these attributes, see Amazon Web Services connector—About user permissions and imported data, on page 14.

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.

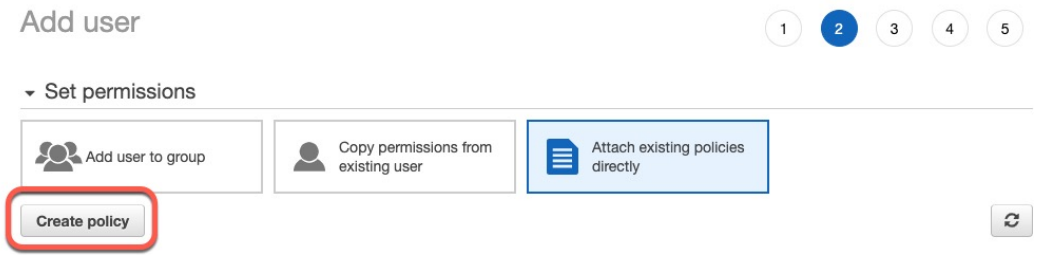
Note
This is the only opportunity you have to retrieve the user's key.

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 16.

Create an AWS connector

This task discusses how to configure a connector that sends data from AWS to the Secure Firewall Management Center 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 14.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center . For a list of these attributes, see Amazon Web Services connector—About user permissions and imported data, on page 14.

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.

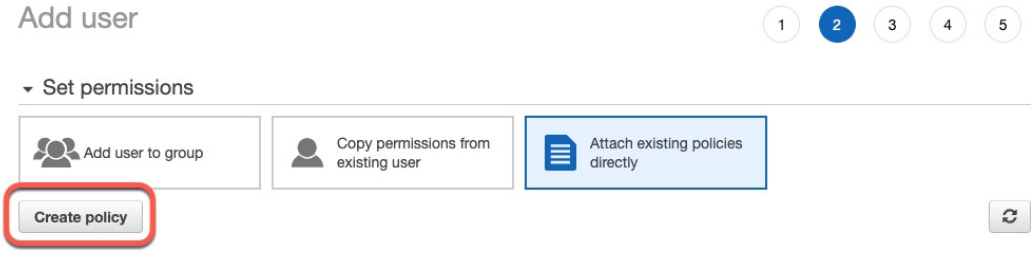
Note
This is the only opportunity you have to retrieve the user's key.

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 16.

Create an AWS Security Groups connector

This task discusses how to configure a connector that sends AWS security groups data to the Secure Firewall Management Center 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 14.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
URL	(Required.) Do not change the URL unless advised to do so.

Step 5 Click **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center . For a list of these attributes, see Azure connector—About user permissions and imported data, on page 20.

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**.

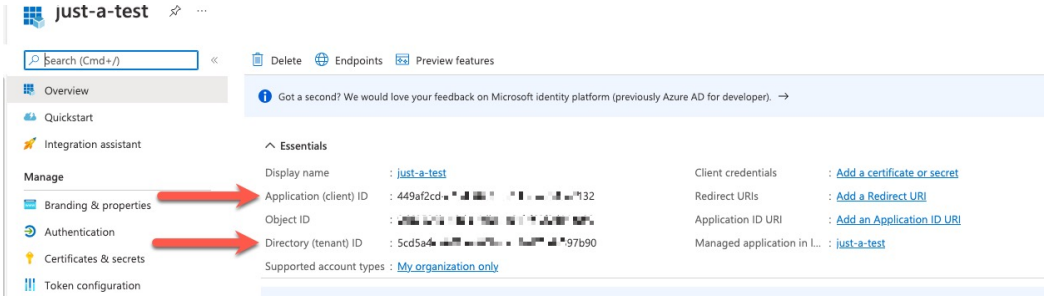
Step 5 In the **Name** field, enter a name to identify this application.

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.

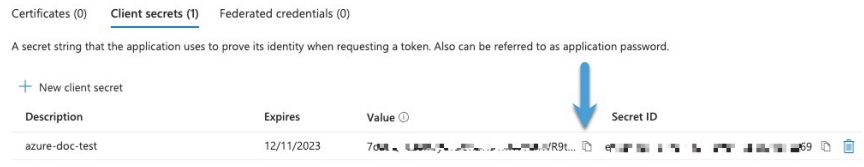


Step 9 Next to Client Credentials, click **Add a certificate or secret**.

Step 10 Click **New Client Secret**.

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

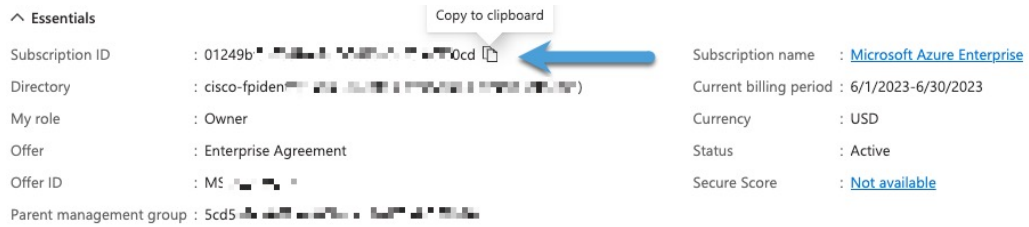
Step 12 Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



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.



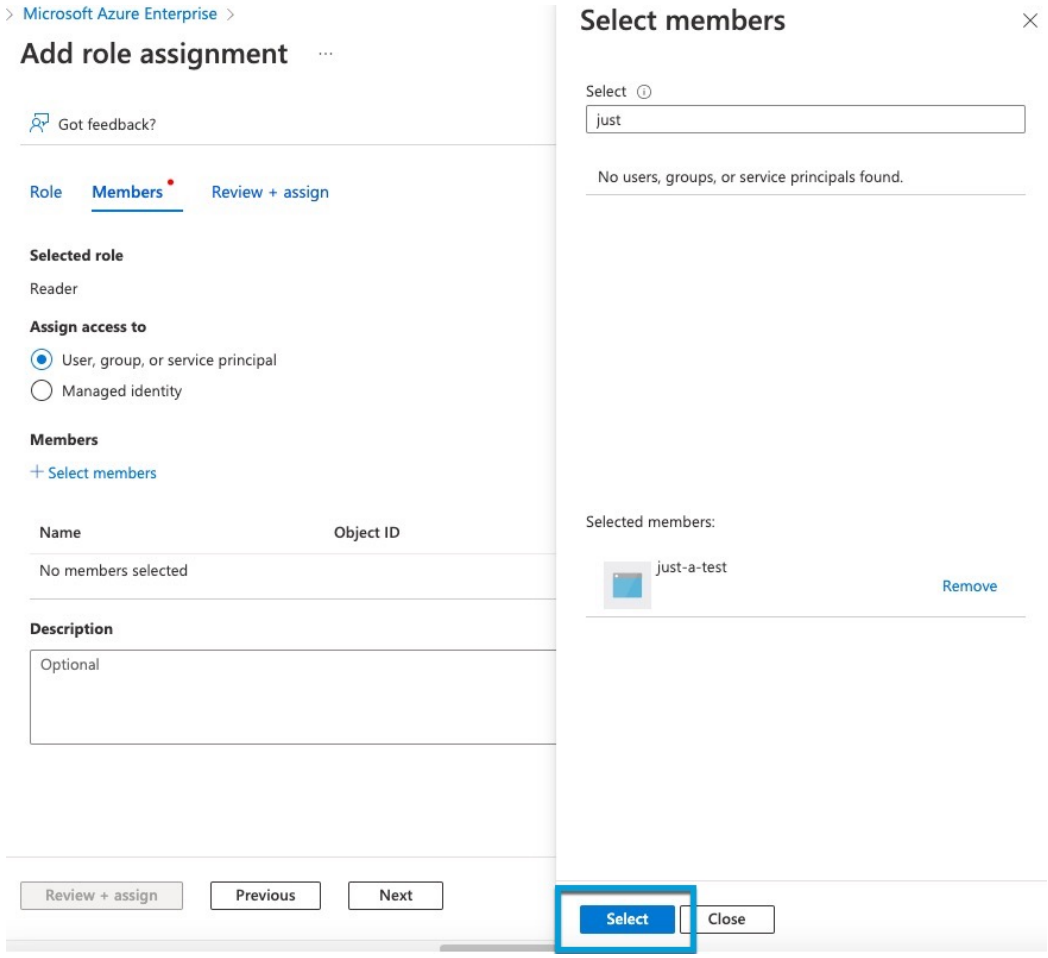
Step 16 Click **Access Control (IAM)**.

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 23.

Create an Azure connector

This task discusses how to create a connector to send data from Azure to Secure Firewall Management Center 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 21.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 **Save**.

Step 6 Make sure **Ok** is displayed in the Status column.

Create a Cisco Cyber Vision connector

This task discusses how to send data from Cisco Cyber Vision to the Secure Firewall Management Center .

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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Cyber Vision Prefix	Enter an alphanumeric string to identify dynamic objects from this Cyber Vision's IP address when objects are sent to Secure Firewall Management Center . 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 Secure Firewall Management Center . 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information:

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
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 39. • 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 Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter 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 **Save**.

Step 7 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 Secure Firewall Management Center 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 Secure Firewall Management Center . For a list of these attributes, see Google Cloud connector—About user permissions and imported data, on page 28.

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.

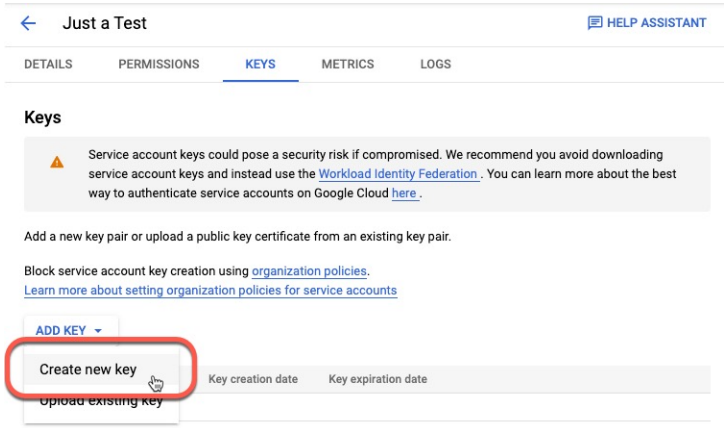
Step 7 Click **Done**.

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 29.

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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

- Add a new connector: click Add icon (+), then click the name of the connector.

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.

Value	Description
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 **Save**.

Step 6 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 Secure Firewall Management Center 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 Secure Firewall Management Center . For a list of these attributes, see vCenter connector—About user permissions and imported data, on page 31.

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**.

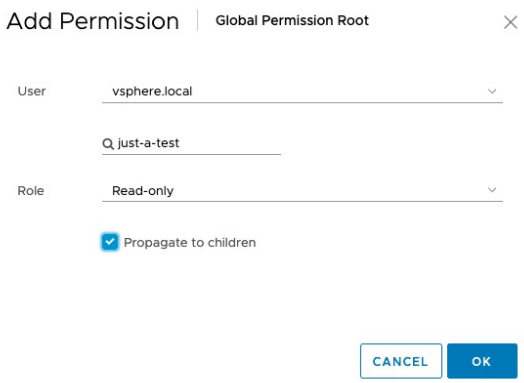
Step 8 Click **Add**(+).

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 32.

Create a vCenter connector

This task discusses how to create a connector for VMware vCenter to send data to the Secure Firewall Management Center 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 39.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

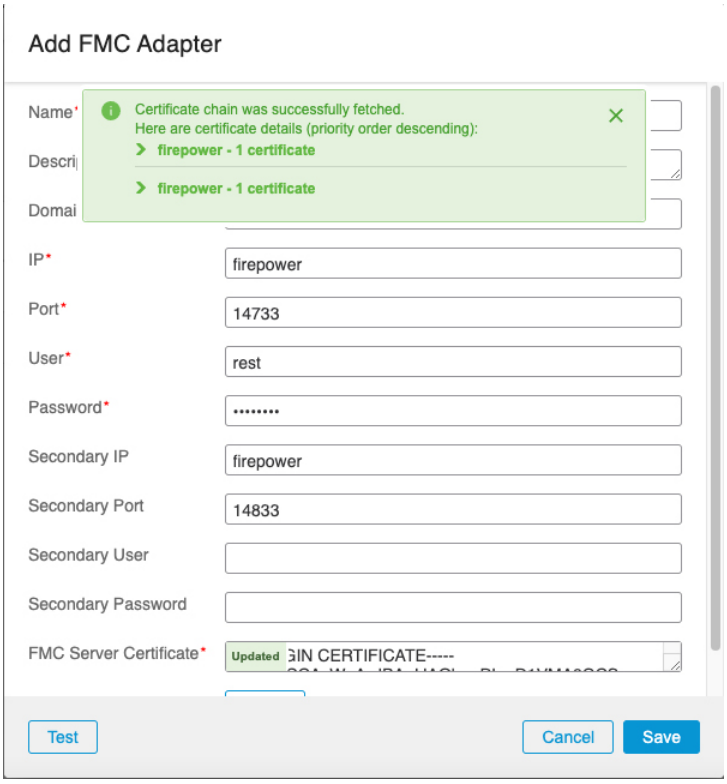
- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	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.
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.

Value	Description
vCenter Certificate	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 39. • Click **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 39. • 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 39. • 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 39.

Step 5 Click **Save**.

Create a Webex connector

This section discusses how to create a Webex connector that sends data to the Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 Secure Firewall Management Center 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 Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 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 dynamic attributes filters

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

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 45.

Before you begin

Create a connector, on page 13

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **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 Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

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

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.

Item	Description
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

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

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

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

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

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

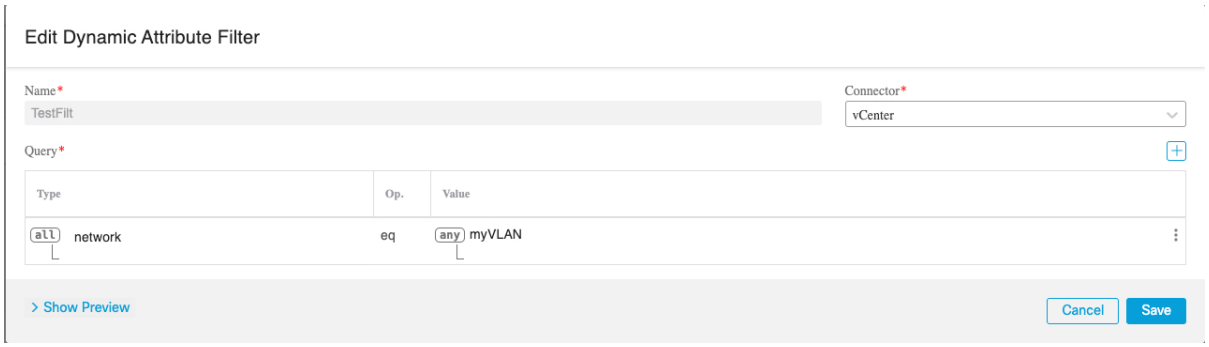
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

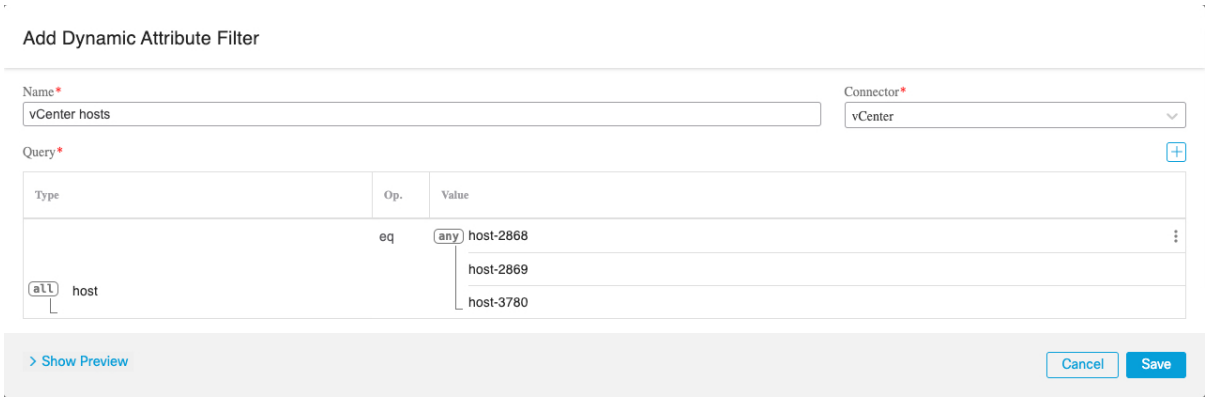
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

The following example shows one criterion: a VLAN.

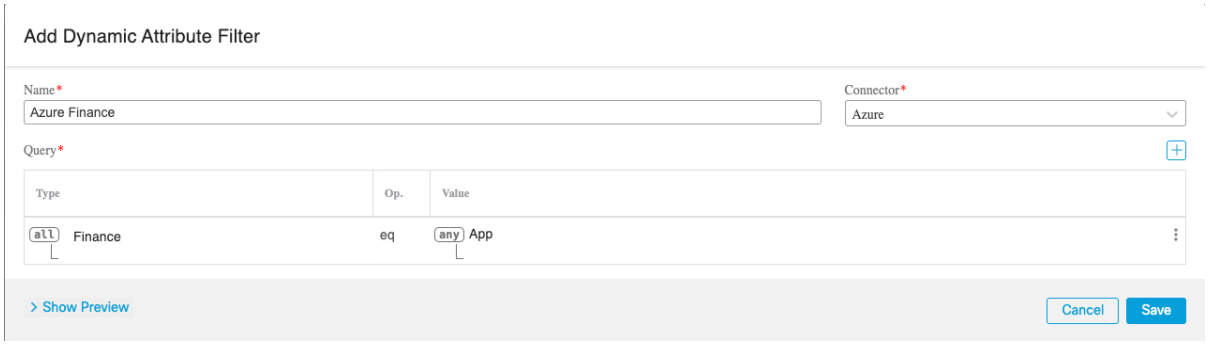


The following example shows three criteria that are joined with OR: the query matches any of three hosts.



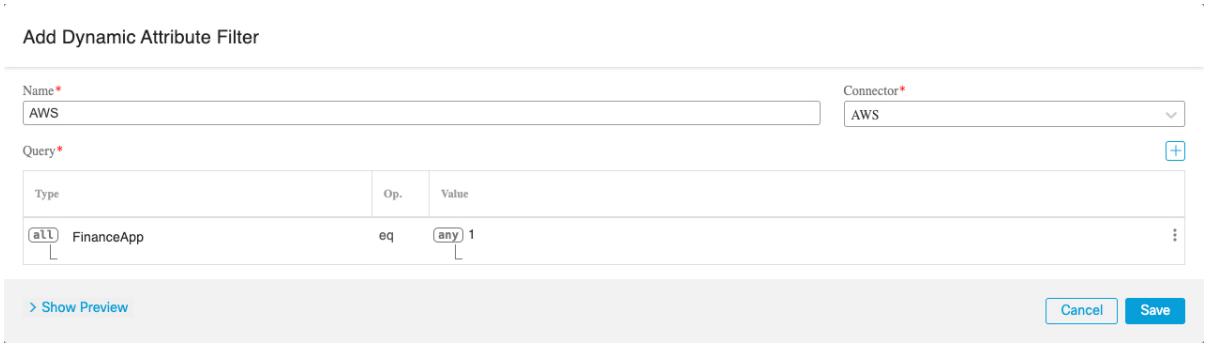
Example: Azure

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.



Manually get a certificate authority (CA) chain

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

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

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

- vCenter or NSX
- Firewall Management Center

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 Firewall Management Center. For example:

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

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

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

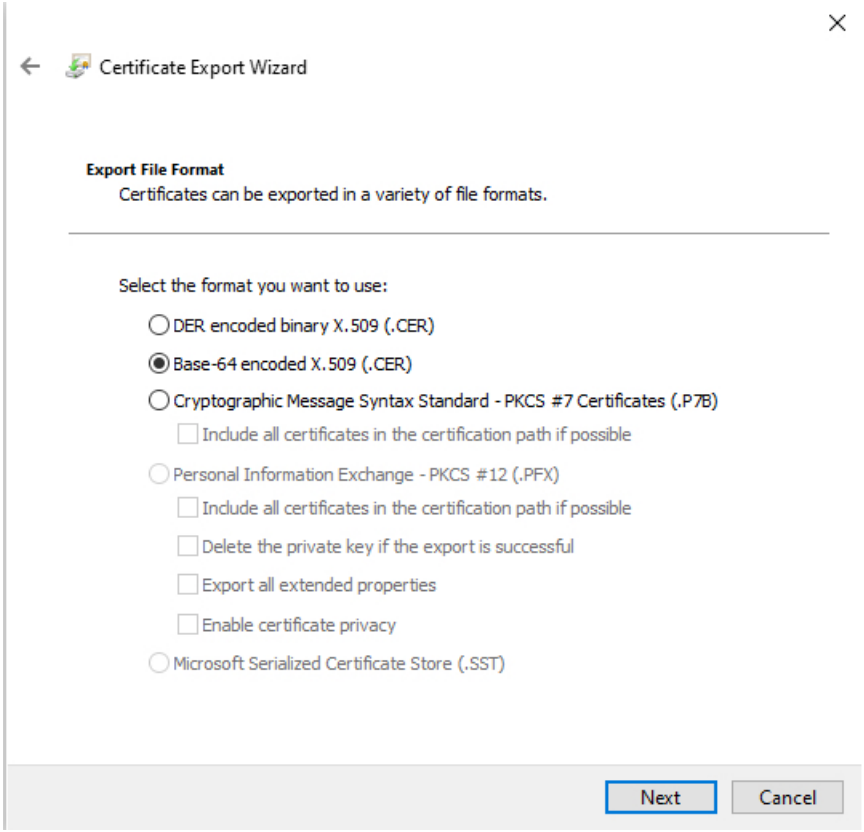
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

Get a Certificate Chain—Windows Chrome

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

1. Log in to vCenter or Firewall Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.
8. Click **Copy to File**.
9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

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



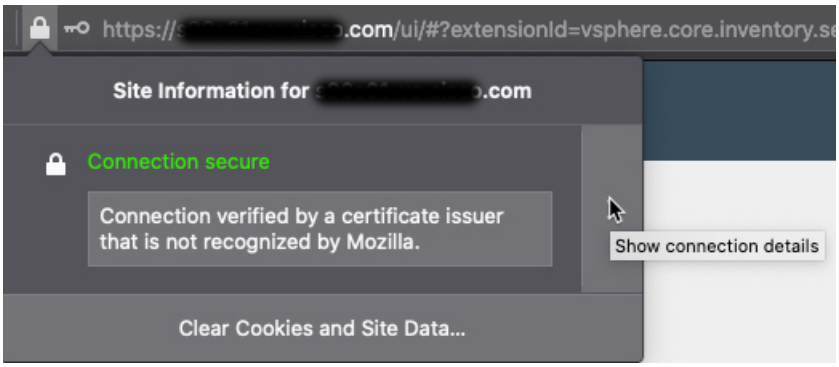
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

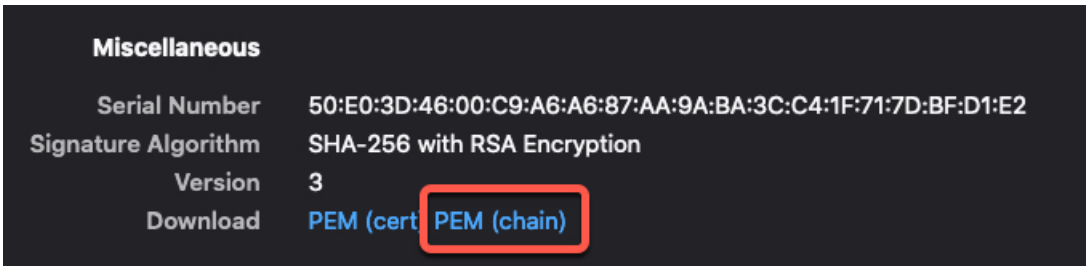
Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter or Firewall Management Center. using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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 or Firewall Management Center.

Use Dynamic Objects in Access Control Policies

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

About dynamic objects in access control 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 **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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

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

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 45.

Before you begin

Create a connector, on page 13

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **Dynamic Attributes Connector** > **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 Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	Click Add .

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

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

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

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

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

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

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

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

Dynamic attributes rule conditions

Dynamic attributes include the following:

- (Source or destination.) Dynamic objects (such as from the dynamic attributes connector)

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

  For more information about the dynamic attributes connector, see About the Dynamic Attributes Connector, on page 1.

- (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.

Create access control 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 Create dynamic attributes filters, on page 36.

Note You cannot create dynamic attributes filters for Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Procedure

Step 1 Log in to the Secure Firewall Management Center

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

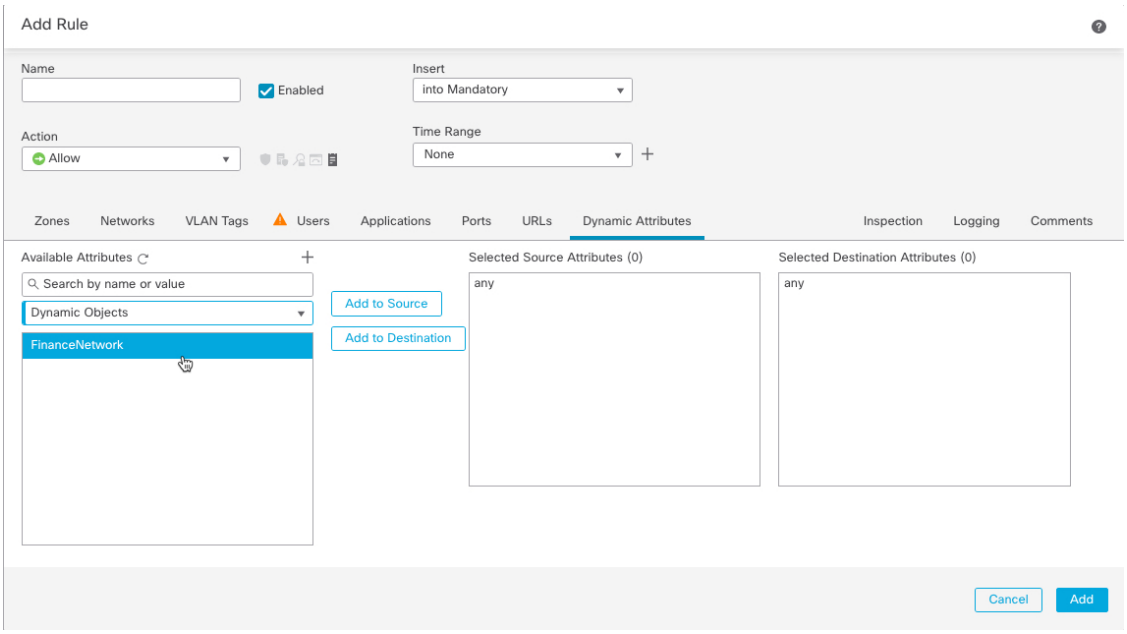
Step 3 Click **Edit** ( ) next to an access control policy.

Step 4 Click **Add Rule**.

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

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

The following figure shows an example.



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.

What to do next

See Dynamic attributes rule conditions, on page 44.

Disable the dynamic attributes connector

If you no longer wish to collect dynamic objects from cloud sources, you can disable the Dynamic Attributes Connector in the Secure Firewall Management Center as discussed in the following task.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

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

Step 3 Slide to **Disabled**.

Troubleshoot using the Secure Firewall Management Center

This task discusses how to generate troubleshoot files for the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **System** (⚙) > **Health** > **Monitor**.

Step 3 In the left pane, click **Firewall Management Center**.

Step 4 At the top, click **System & Troubleshooting Details**.

Step 5 Click **Generate Troubleshooting Files**.

Step 6 Provide the files to Cisco TAC or to your Beta coordinator.

Manually get a certificate authority (CA) chain

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

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

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

- vCenter or NSX
- Firewall Management Center

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 Firewall Management Center. For example:

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

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

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

3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.

- *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.

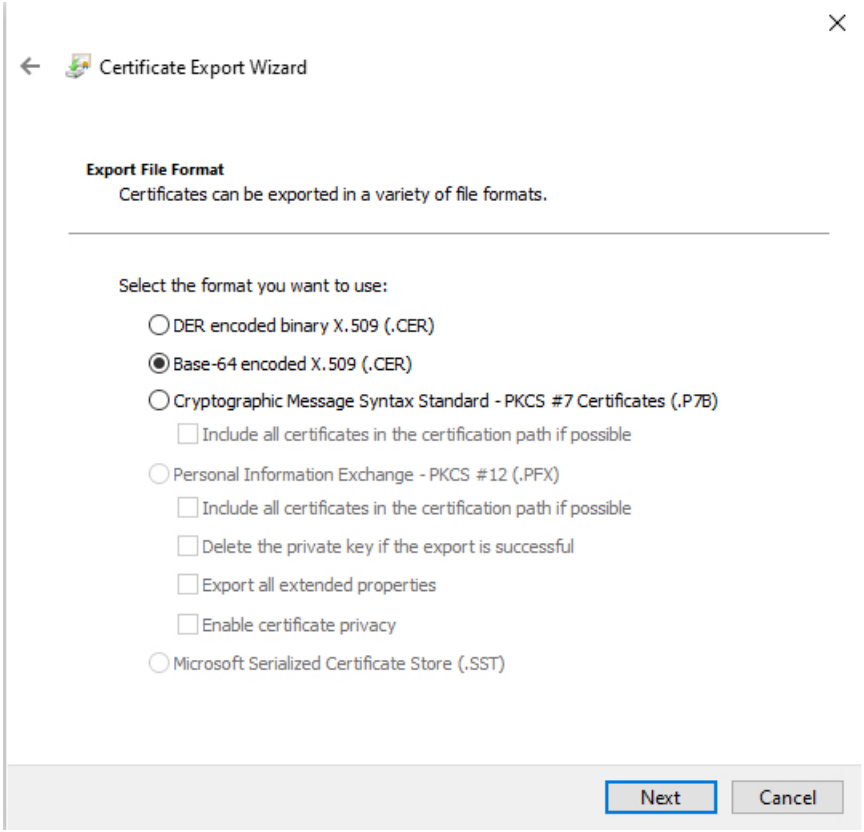
4. Repeat these tasks for vCenter Firewall Management Center.

Get a Certificate Chain—Windows Chrome

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

1. Log in to vCenter or Firewall Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.
8. Click **Copy to File**.
9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

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



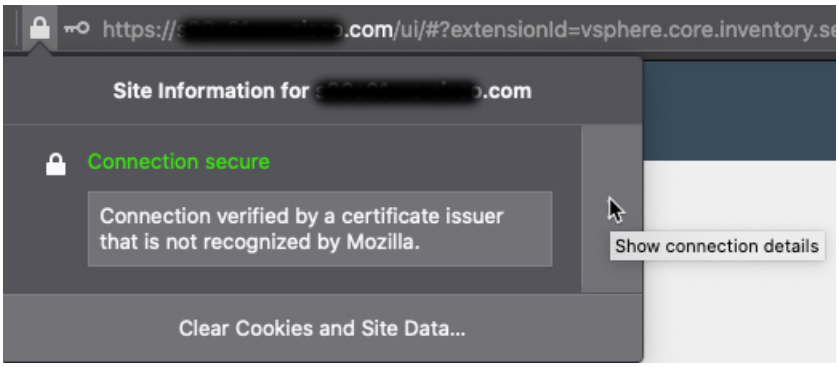
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

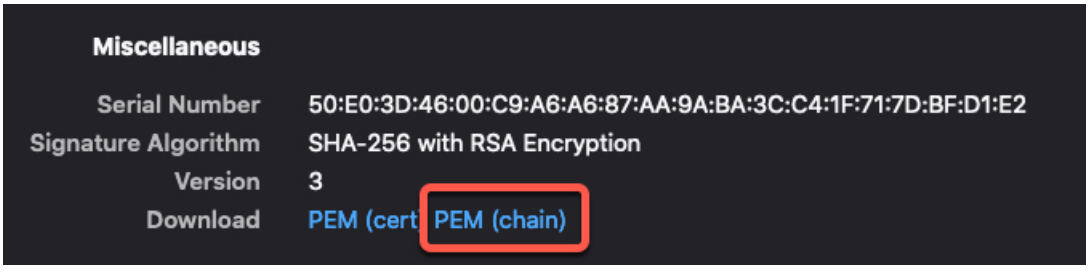
Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter or Firewall Management Center. using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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 or Firewall Management Center.

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 Secure Firewall Management Center reside on the same network, you can connect the Secure Firewall Management Center 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 man-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 Secure Firewall Management Center and with external servers.

Table 3: 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
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 4: 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).

History for the dynamic attributes connector

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New connectors	7.6	20241127	AWS security groups, AWS service tags, and Cisco Cyber Vision These connectors can send an on-premises Secure Firewall Management Center dynamic objects as can Security Cloud Control. To receive dynamic objects from an on-premises dynamic attributes connector, version 3.0 of the on-premises dynamic attributes connector is required.
Dynamic Attributes Connector	7.4.0	7.4.0	This feature is introduced. The Dynamic Attributes Connector is now included in the Secure Firewall Management Center. You can use the dynamic attributes connector to get IP addresses from cloud-based platforms such as Microsoft Azure in access control rules without having to deploy to managed devices. More information: • The dynamic attributes connector included with this product: About the Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: *Cisco Secure Dynamic Attributes Connector Configuration Guide* New/modified screen: **Integration** > **Dynamic Attributes Connector**