

Dynamic Attributes Connector

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

- About the dynamic attributes connector , on page 1
- Dynamic Attributes Connector operation, on page 1
- System requirements for the dynamic attributes connector, on page 8
- Enable the dynamic attributes connector, on page 8
- Dashboard, on page 10
- Connectors, on page 17
- Create dynamic attributes filters, on page 57
- Manually get a certificate authority (CA) chain, on page 60
- Disable the dynamic attributes connector, on page 63
- Troubleshoot the Dynamic Attributes Connector, on page 64
- Recommendation: security requirements for network deployment, on page 64
- Internet access requirements, on page 65
- History for the dynamic attributes connector, on page 66

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.

Dynamic Attributes Connector operation

The dynamic attributes connector queries cloud services and provides attribute information to the secure management center.

Operation modes

You can run the dynamic attributes connector in either network download or air gap mode. These topics provide more details:

- Network download mode, on page 2

• Air gap mode, on page 3

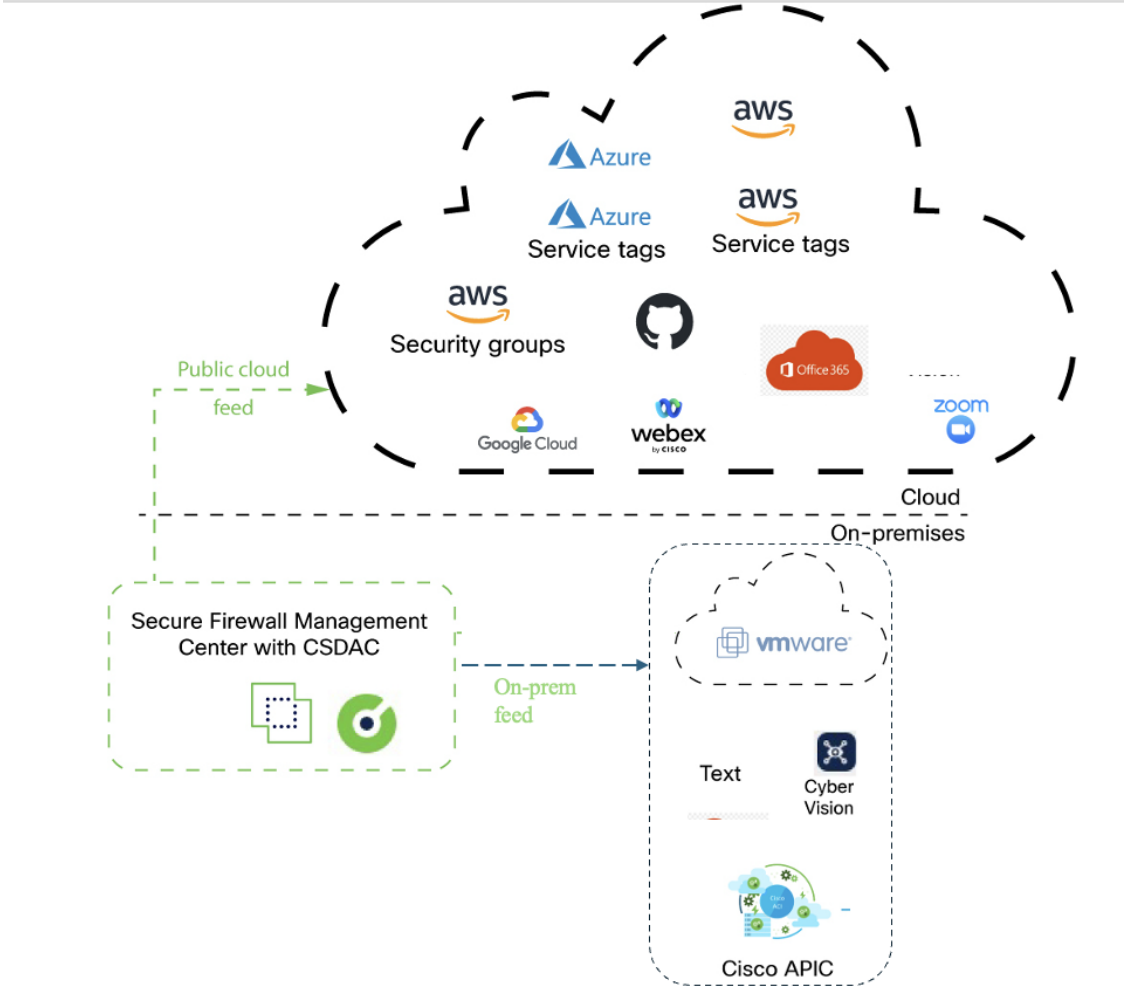
These stages describe how the Cisco Secure Dynamic Attributes Connector processes cloud service information:

1. Connector data ingestion: The connector continuously queries cloud and on-premises sources to retrieve tags, metadata, and network attributes. These tags typically define dynamically allocated network and IP addresses that cannot be used to create access control rules.
2. Dynamic attribute filter creation: Define match conditions to isolate relevant data from the ingested connector data. For example, if an AWS cloud environment contains tags for multiple departments, you can define a filter to isolate only the attributes associated with the "Finance App" tag. Note that you can create dynamic attribute filters for workloads such as AWS, Azure, vCenter, GCP, and so on. Other connectors, such as Generic Text, Office 365, Azure Service Tags, Webex, or Zoom, retrieve data and pass the entire set as dynamic objects.
3. Dynamic objects: After configuring dynamic attribute filters, the filters are stored as dynamic objects in the Firewall Management Center. Use these dynamic objects in access control policies to keep security rules accurate and effective as cloud resources scale or migrate, without manual updates.

Network download mode

The dynamic attributes connector always operates in network download mode. In this mode, the images required to make it work are downloaded from the internet. If your security requirements are strict, you can use *air gapped* mode.

Architectural overview:



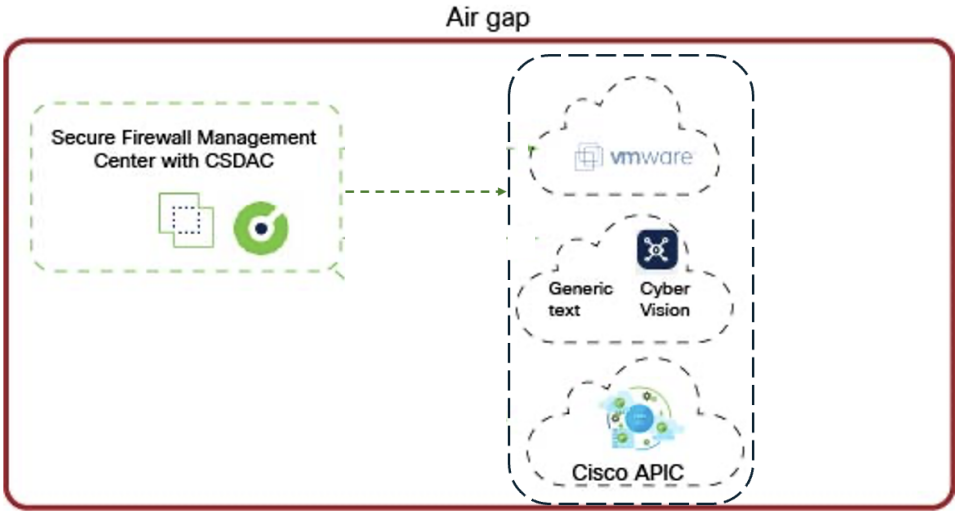
Air gap mode

Air gap mode completely isolates your system from unsecured networks, such as the public internet to prevent unauthorized access or data leakage.

Air gap mode operation

If your Secure Firewall Management Center is not connected to the internet, you can use it and the dynamic attributes connector in *air-gapped* mode. This offline approach safeguards your sensitive data and prevents external exposure.

This figure shows how air gap works:



Air gap supports these connectors:

- Cisco APIC
- Cisco CyberVision
- Generic text
- vCenter

Air gap the dynamic attributes connector

Configure the dynamic attributes connector to operate in air gap mode for offline integration with the Secure Firewall Management Center.

Implement the dynamic attributes connector in your air-gapped Secure Firewall Management Center to maintain strict security control while leveraging independent passive identity services for robust, identity-based policy enforcement.

Before you begin

Make sure you need to use the dynamic attributes connector in air gap mode. Requirements:

- Secure Firewall Management Center and Secure Firewall Threat Defense not connected to the internet
- Secure Firewall Management Center and Secure Firewall Threat Defense all run version 10.1.0 or later
- Using these connectors:
  - Cisco APIC
  - Cisco CyberVision
  - Generic text
  - vCenter

You can also use the passive identity agent in air gap mode, provided all Microsoft AD servers and domain controllers are also air-gapped and available to the Secure Firewall Management Center.

You do *not* need to enable the dynamic attributes connector to use the passive identity agent. For more information, see The passive identity agent identity source.

Follow these steps to air gap the dynamic attributes connector:

Procedure

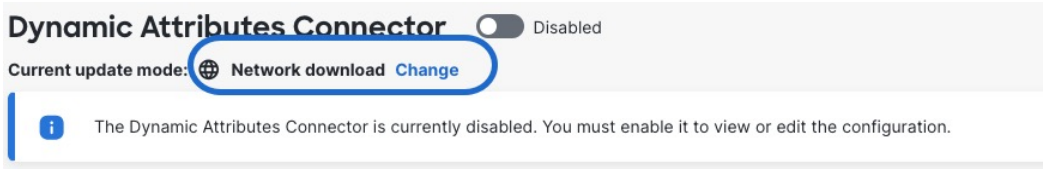
Step 1 Download the connector tar archive file from Cisco software site.

Step 2 Log in to the Secure Firewall Management Center if you have not done so already.

Step 3 Click **Integrations** > **Dynamic Attributes Connector**.

Step 4 If Current update mode is Network download, click **Change**.

Example:



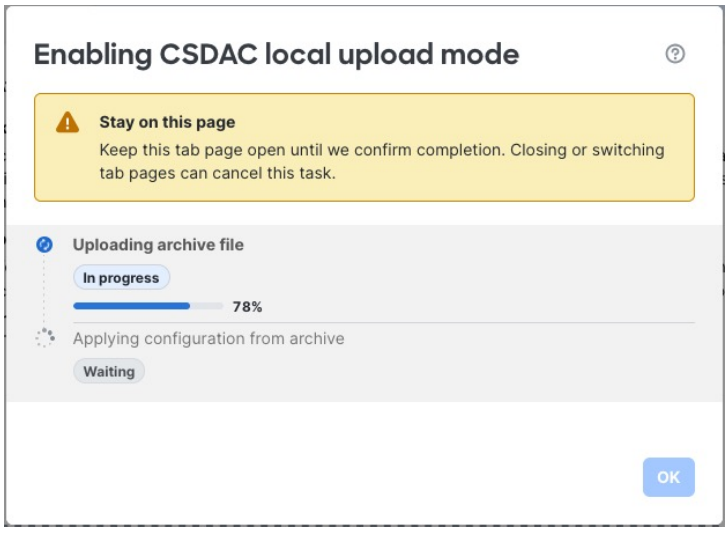
Step 5 On the next page, click **Local Upload**.

Step 6 Either drag and drop the **.tar** file you extracted earlier or click the area on the screen and browse to locate it.

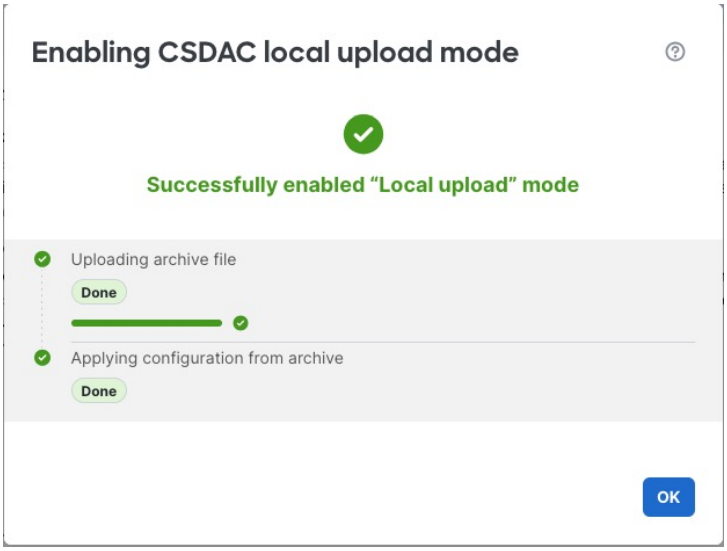
Step 7 Click **Save**; you are required to confirm your choice.

Note Do not close your browser window or tab page until the process is complete.

Example:



Example of a successful installation:



Step 8 Depending on whether or not the upload was successful, you can:

- Successful upload: Enable the dynamic attributes connector, on page 8.
- Failed upload: Troubleshoot the air gap upload, on page 6.

Troubleshoot the air gap upload

When the air gap image upload fails, this reference provides troubleshooting suggestions to help resolve common upload issues.

If the air gap image upload fails, a page similar to this is displayed:

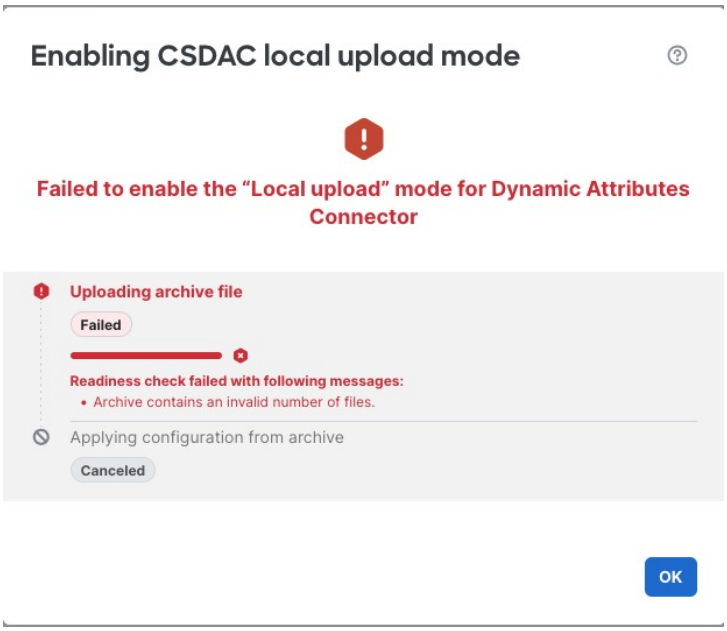


Table 1: Troubleshooting suggestions

Message	Troubleshooting suggestion
Archive contains an invalid number of files Archive is not found or not loaded successfully. Archive is too large. Maximum allowed size is 2GB. Failed to list files in the archive. Archive does not contain the required files. Failed to extract from the archive. The archive might be corrupt.	The archive you tried to upload is probably not for air-gapped dynamic attributes connector. Verify where you obtained the archive and try again.
File is not a valid gzip compressed tar archive. An unexpected error occurred: the public signature key file is missing. Archive signature validation failed. Failed to read or parse the extracted files from the archive. The archive might be corrupt. An unexpected error occurred: failed to read or parse internal docker compose files.	The archive you tried to upload is corrupt. Do not email the archive. Try downloading it again.
The archive contains an unexpected image that is not compatible with the current version. The archive might be corrupt.	The archive version doesn't match the dynamic attributes connector version. Verify your upload and try again.

System requirements for the dynamic attributes connector

The Dynamic Attributes Connector has specific memory requirements that must be met to ensure proper deployment and operation. These limits apply to both virtual machines and physical machines to avoid deployment issues.

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

Enable the dynamic attributes connector to allow objects from cloud networking products to be used in Secure Firewall Management Center access control and DNS rules.

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 and DNS rules.

This task is optional if you use the passive identity agent.

Procedure

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

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

Step 3 Slide to **Enabled**.

Step 4 The system displays messages when the dynamic attributes connector is enabled.

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

See Connectors, on page 17.

Configure networks and subnets for Docker containers

The Dynamic Attributes Connector uses Docker containers to retrieve connector data in the Secure Firewall Management Center . You can change Docker IP addresses and ranges to avoid conflicts with the Secure Firewall Management Center management interface and other network IP addresses.

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

- `docker0` : Used internally by the Docker daemon.
- IPv6 networks (`vethnumber`): Internal bridge networks used by the dynamic attributes connector .
- Docker bridge networks (`br-number`): Used by dynamic attributes connector connectors.

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

- `-b CIDR-network` : Sets a network base address pool in CIDR notation.
- `-s address-pool-size` : Sets a netmask for the network base address to limit the number of addresses and ensure compatibility with available system RAM.



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.

Table 2: Recommended Docker Network Settings

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
Firepower 2500, Firepower 2600, vFMC 300	26 (netmask 255.255.255.192)	192.168.0.0/16	62 IP addresses
Firepower 4500, Firepower 4600	25 (netmask 255.255.255.128)	192.168.0.0/16	126 IP addresses

```
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
```

Troubleshooting

Table 3: Common Docker Network Errors

Error	Solution
Pull subnet value can not be greater than size	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	Solution
Docker networks are wrong	Restart the Docker daemon: `sudo pmtool restartbyid docker`
Cannot connect to the Docker daemon `Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?`	Restart Docker: `pmtool restartbyid docker`
Input can't be empty	The `-s` parameter is required.

Dashboard

Dashboard capabilities include:

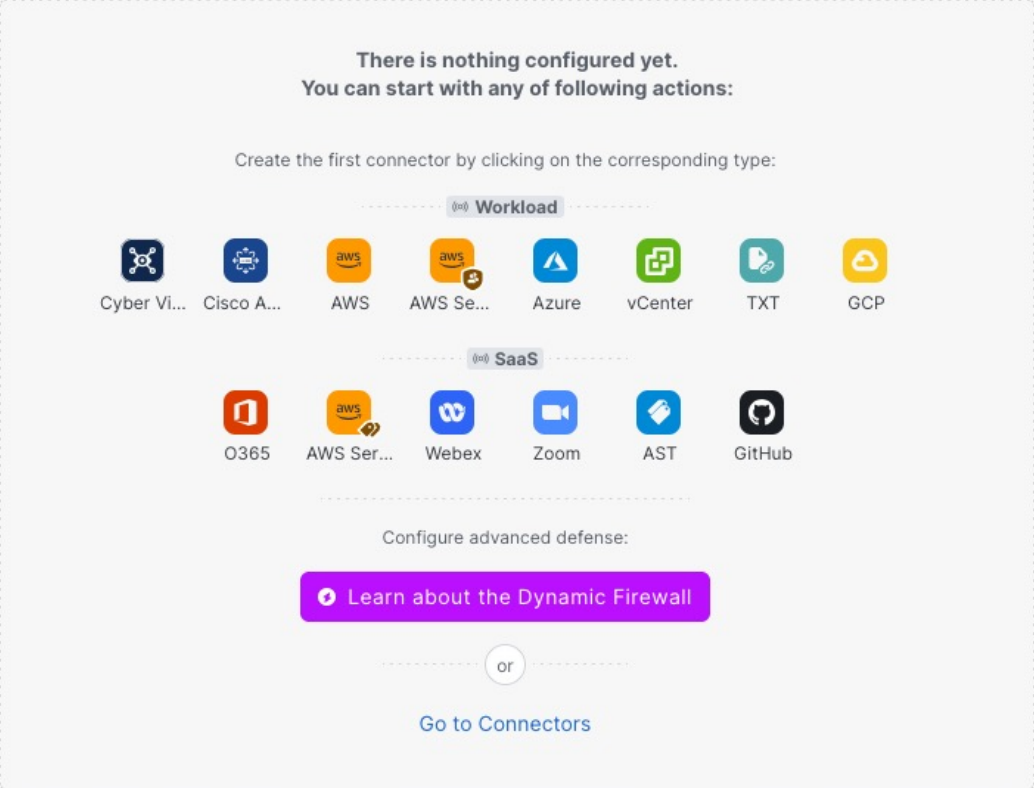
- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

Dashboard access and functionality

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

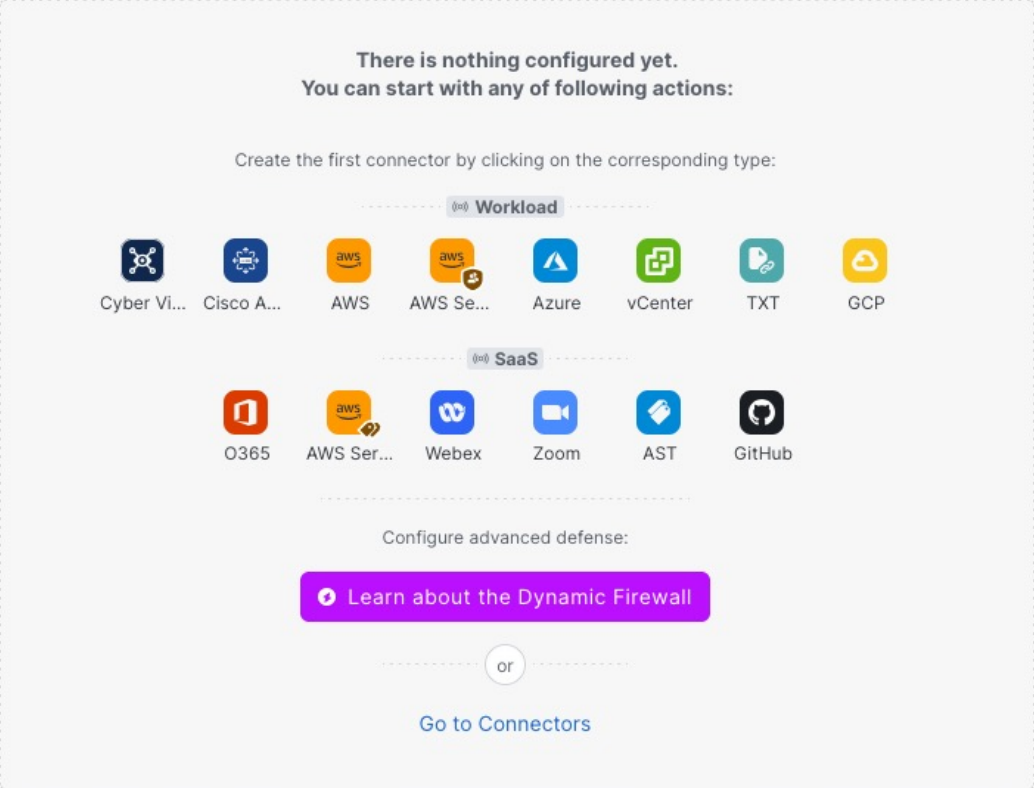
If the dynamic attributes connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

The dynamic attributes connector Dashboard page displays an example of an unconfigured system:

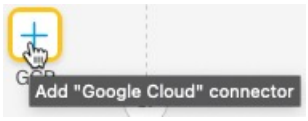


Dashboard of an unconfigured system

This sample dynamic attributes connector Dashboard page shows how an unconfigured system appears initially.



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

- 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 Connectors, on page 17.

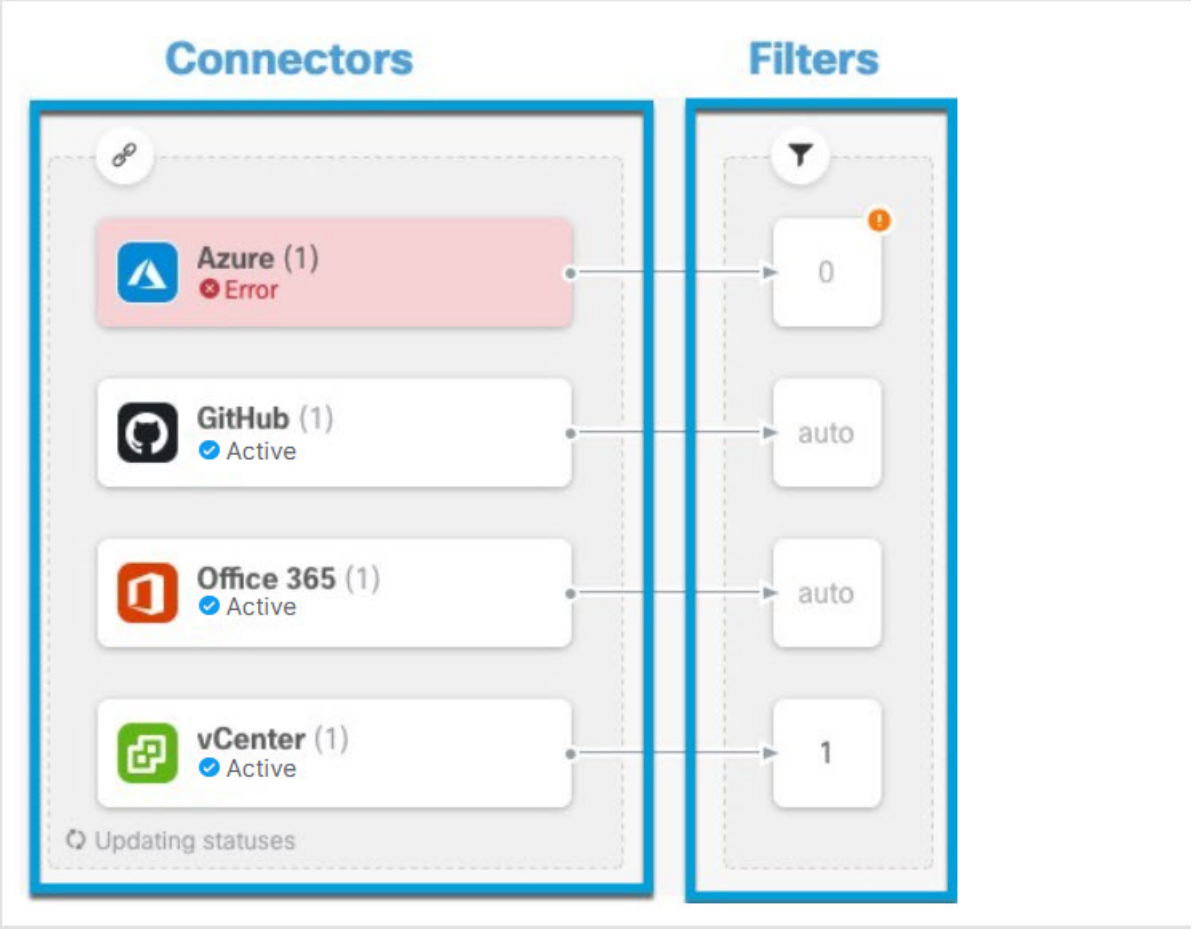
Related Topics:

- Dashboard of a configured system, on page 12
- Add, edit, or delete connectors, on page 14
- Add, edit, or delete dynamic attributes filters, on page 16

Dashboard of a configured system

Sample dynamic attributes connector Dashboard page of a configured system displays at-a-glance information about configured connectors, filters, and adapters.

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



1 Connectors, on page 17
2 Create dynamic attributes filters

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 14.	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 16.

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.

Add, edit, or delete connectors

The Dashboard enables you to manage connectors by viewing, adding, editing, or deleting them. You can also view error information for connectors and troubleshoot issues.

Use the dynamic attributes connector dashboard when you need to manage connectors for your network security infrastructure. The dashboard provides comprehensive options for connector management and troubleshooting.

Procedure

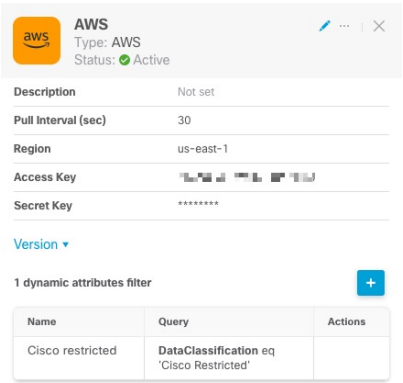
Step 1 Access the connector dashboard and select your desired action.

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.

Step 2 Click any connector in the connectors column ( ) to display more information about it.

An example follows:

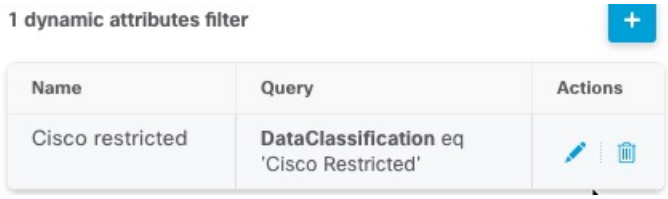


Step 3 Choose from the following management options.

- 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.

Step 4 Use the table at the bottom of the panel to add dynamic attributes filters or to edit or delete connectors.

A sample follows:



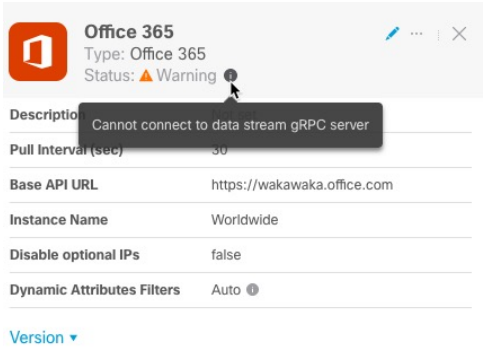
Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters.

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

Step 5 To view error information for a connector, click the name of the connector that is displaying the error.

Step 6 In the right pane, click **Information** ( ).

An example follows.



Step 7 To resolve this issue, edit the connector settings as discussed in Create an office 365 connector, on page 47.

Step 8 If you cannot resolve the issue, click **Version** and copy the version to a text file.

Add, edit, or delete dynamic attributes filters

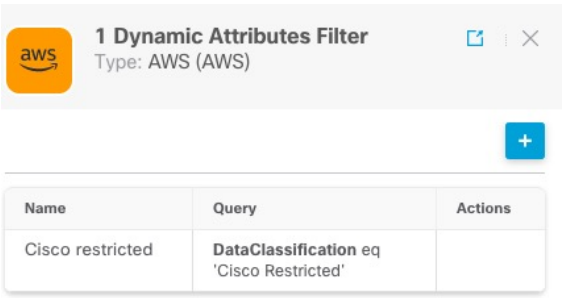
The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click  for additional options.

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.

An example follows:



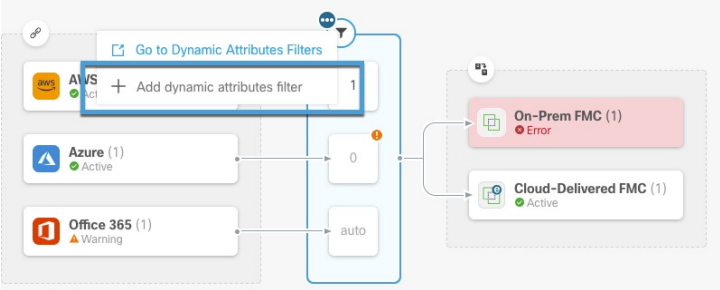
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have these 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.
- 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.

Connectors

A connector is an interface with a cloud service. It retrieves network information from the cloud service to enable the network information to be used in policies on the Secure Firewall Management Center. It supports both air gap mode and network download mode configurations.

Supported connectors

If you are using the dynamic attributes connector in air gap mode, these connectors are available:

- Cisco APIC
- Cisco CyberVision
- Generic text
- vCenter

We support these connectors in network download mode:

Table 4: List of supported connectors by dynamic attributes connector version and platform

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

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 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
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
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.1.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Amazon Web Services connector user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Amazon Web Services (AWS) to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

The dynamic attributes connector usually operates in network download mode, where the necessary images are downloaded from the internet. If you have strict security requirements, consider using air gapped mode.

The connector imports these 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 creates a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

For a list of the dynamic attributes that can be sent, refer to Amazon Web Services connector user permissions and imported data, on page 18.

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.

Follow these steps to create an AWS user with minimal permissions for the dynamic attributes connector:

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**.

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

b) Click **Access Key - Programmatic Access**.

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

d) Add tags to the user if desired.

e) Click **Create User**.

f) Click **Download .csv** to download the user's key to your computer.

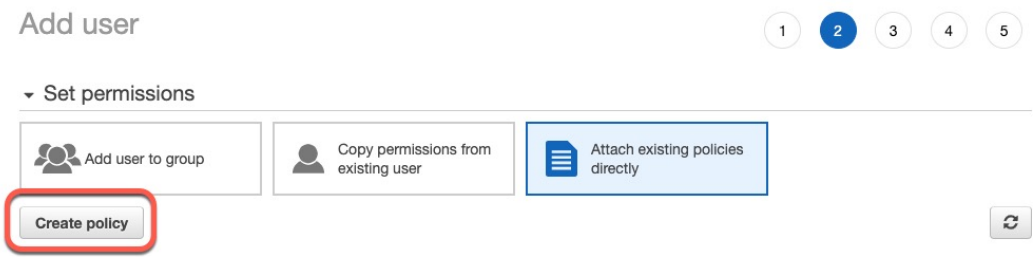
Note This is the only opportunity you have to retrieve the user's key.

g) Click **Close**.

Step 5 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 6 Click **Create Policy**.

a) On the Create Policy page, click **JSON**.



b) Enter the following policy in the field:

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

c) Click **Next**.

Step 7 Click **Review**.

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

Step 8 Attach your policy

a) On the Policies page, enter all or part of the policy name in the search field and press Enter.
b) Click the policy you just created.
c) Click **Actions** > **Attach**.
d) If necessary, enter all or part of the user name in the search field and press Enter.
e) Click **Attach Policy**.

What to do next:

Create an AWS connector, on page 20.

Create an AWS connector

Create a connector to send dynamic objects from AWS to the firewall for use in security policies.

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 19.

Follow these steps to create an AWS connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of these actions:

- 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 required 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.

a) Click **Save**.

The Status column displays **Ok**.

What to do next:

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.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

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 creates a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

For a list of the dynamic attributes that can be sent, refer to Amazon Web Services connector user permissions and imported data, on page 18.

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.

Follow these steps to create an AWS user with minimal permissions for the dynamic attributes connector:

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**.

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

b) Click **Access Key - Programmatic Access**.

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

d) Add tags to the user if desired.

e) Click **Create User**.

f) Click **Download .csv** to download the user's key to your computer.

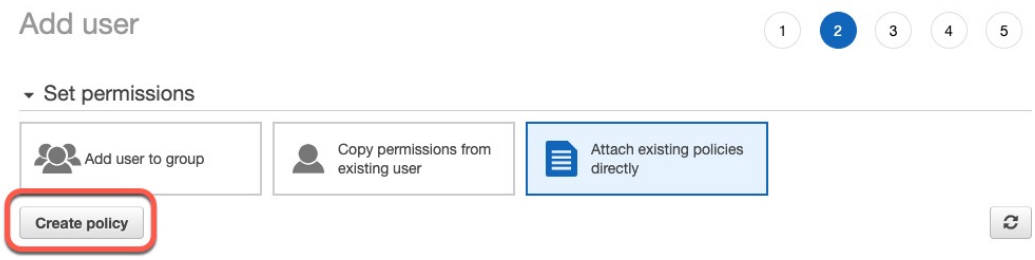
Note This is the only opportunity you have to retrieve the user's key.

g) Click **Close**.

Step 5 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 6 Click **Create Policy**.

a) On the Create Policy page, click **JSON**.



b) Enter the following policy in the field:

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

c) Click **Next**.

Step 7 Click **Review**.

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

Step 8 Attach your policy

a) On the Policies page, enter all or part of the policy name in the search field and press Enter.
b) Click the policy you just created.
c) Click **Actions** > **Attach**.
d) If necessary, enter all or part of the user name in the search field and press Enter.
e) Click **Attach Policy**.

What to do next:

Create an AWS connector, on page 20.

Create an AWS security groups connector

This task creates a connector that sends AWS security groups data to the Secure Firewall Management Center for use in policies.

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

Complete these steps:

- 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 19.

Follow these steps to create an AWS Security Groups connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

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.

a) Click **Save**.

The Status column displays **Ok**.

Create an AWS service tags connector

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

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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 necessary 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.

a) Click **Save**.

The Status column displays **Ok**.

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 these 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

Create an Azure service account with minimal permissions to send dynamic attributes to Secure Firewall Management Center.

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 25.

Before you begin

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

Follow these steps to create an Azure user with minimal permissions for the dynamic attributes connector:

Procedure

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

Step 2 Click **Azure Active Directory**.

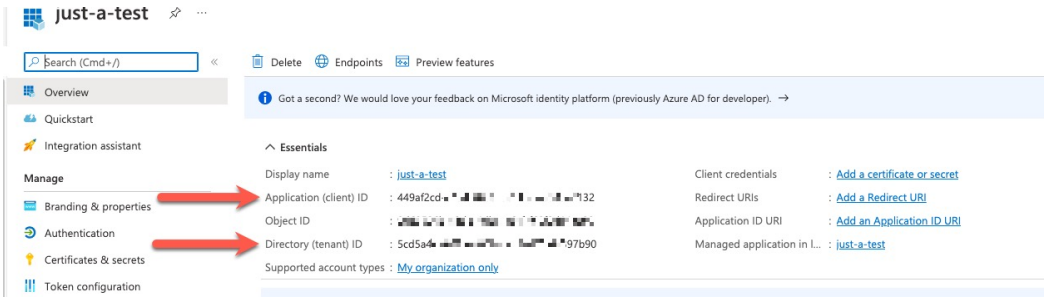
Find the instance of Azure Active Directory for the application you want to set up.

Step 3 Click **Add** > **App registration**.

a) In the **Name** field, enter a name to identify this application.
b) Enter other information on this page as required by your organization.
c) Click **Register**.

Step 4 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*).

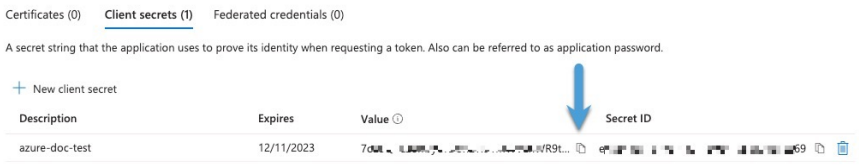
Here is a sample:



Step 5 Next to Client Credentials, click **Add a certificate or secret**.

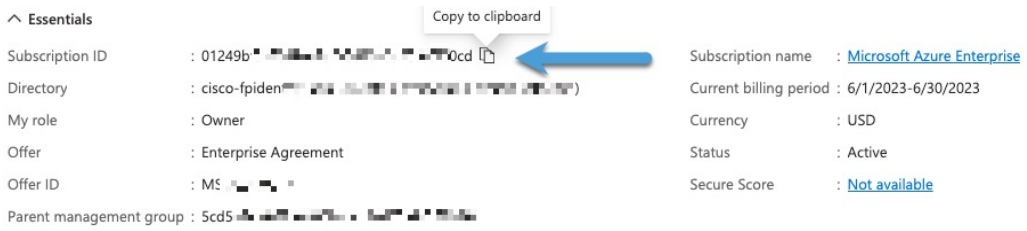
Step 6 Click **New Client Secret**.

a) Enter the requested information and click **Add**.
b) Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



Step 7 Go back to the main Azure Portal page and click **Subscriptions**.

a) Click the name of your subscription.
b) Copy the subscription ID to the clipboard.



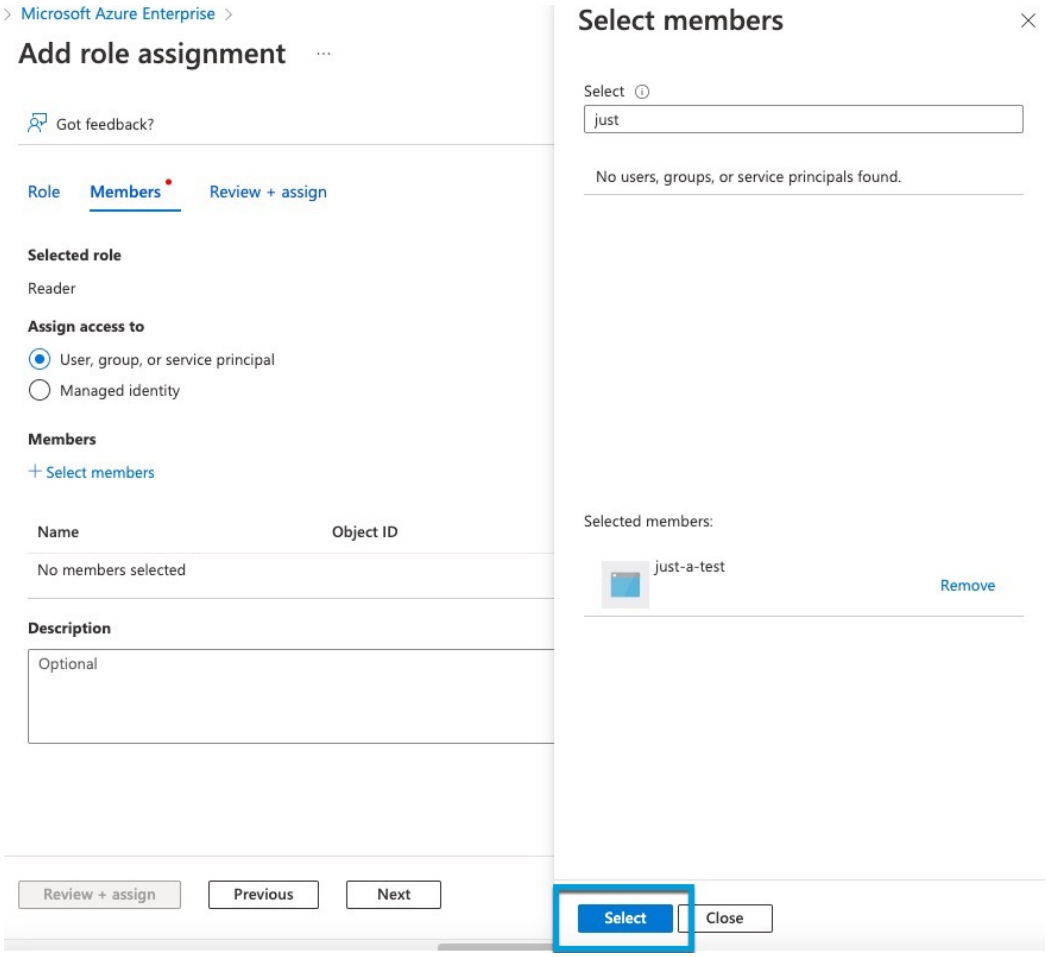
Step 8 Click **Access Control (IAM)**.

a) Click **Add** > **Add role assignment**.

b) Click **Reader** and click **Next**.

c) Click **Select Members**.

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



e) Click **Review + Assign** and follow the prompts to complete the action.

Also see Create an Azure connector, on page 27.

Create an Azure connector

Create a connector to send data from Azure to Secure Firewall Management Center for use in policies.

This connector enables integration between Azure and your security management platform to retrieve dynamic object information for policy implementation.

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 25.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

a) Click **Save**.

The Status column displays **Ok**.

Create an Azure service tags connector

Create a connector for Azure service tags to enable use in policies with automatically updated IP addresses from Microsoft.

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.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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 required 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.

a) Click **Save**.

The Status column displays **Ok**.

Cisco APIC connector

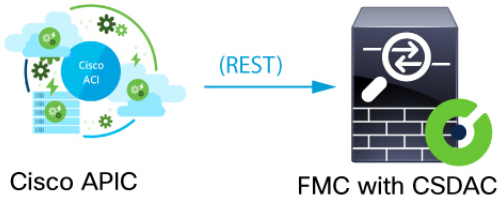
The topics discuss how to configure the Cisco APIC Integration with the Secure Firewall Management Center.

About the Cisco APIC integration with the Secure Firewall Management Center

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

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

The following figure shows how the integration works.



Sample configuration

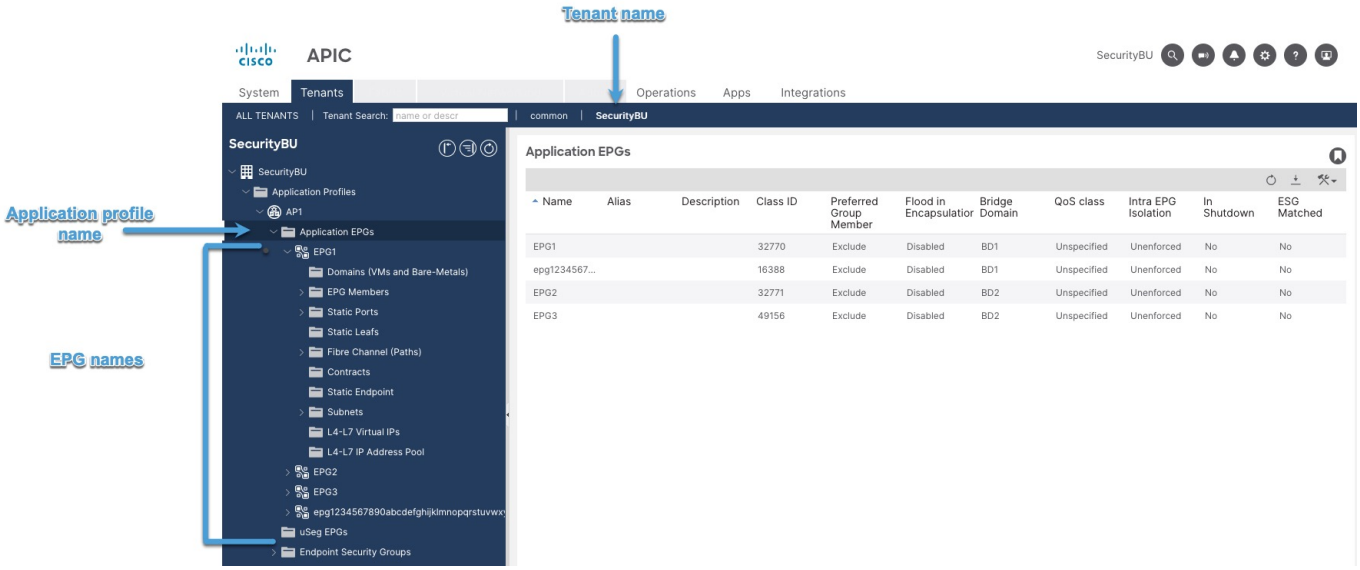
The following sample configuration shows how network object groups are named in the Secure Firewall Management Center based on names in APIC and the APIC connector (not shown).

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

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

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

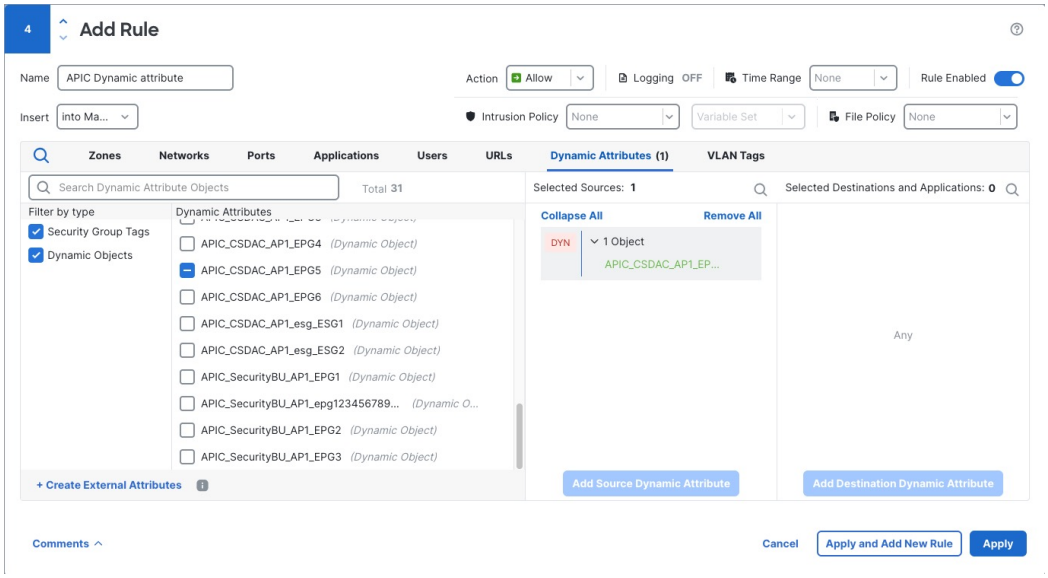
- Cisco APIC application profile name (in this example, `AP1`)
- Cisco APIC EPG name (in this example, `EPG1` through `EPG4`)



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

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

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



More information

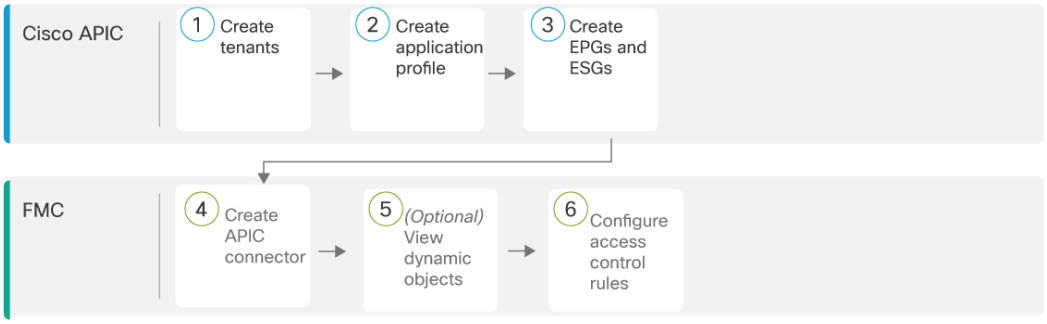
- For more information about the dynamic attributes connector in the Secure Firewall Management Center, see Secure Firewall Management Center Device Configuration Guide.
- APIC Roles and Privileges Matrix
- Endpoint Security Groups
- Basic User Tenant Configuration

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

This reference outlines the workflow for configuring the integration between Cisco APIC and Secure Firewall Management Center to utilize dynamic objects in security policies.

The key components involved in using dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules are:

- Cisco APIC: Provides tenant configuration, application profiles, and endpoint groups (EPGs) or endpoint security groups (ESGs) that serve as network objects.
- Secure Firewall Management Center: Creates a connector to retrieve dynamic objects and incorporates them into access control policies or DNS policies.
- Dynamic attributes connector: Enables the integration between the two systems by fetching EPGs and ESGs from Cisco APIC.



1 Basic User Tenant Configuration
2 Basic User Tenant Configuration
3 EPGs
4 Create a Cisco APIC connector, on page 36
5 View dynamic objects in the Secure Firewall Management Center
6 Create access control rules or DNS rules using dynamic attributes filters

Table 5: Configure Secure Firewall Management Center access control rules or DNS rules using network object groups

Icon	Component	Description
1	Cisco APIC	A tenant allows a Cisco APIC administrator to set up domain-based access control. See Basic User Tenant Configuration
2	Cisco APIC	An application profile is a container for other objects, such as an endpoint group (EPG). See Basic User Tenant Configuration
3	Cisco APIC	An EPG is a container for network objects that serves as the way that devices connect to the network. An ESG is a logical entity that contains a collection of physical or virtual network endpoints. See EPGs and ESGs
	Secure Firewall Management Center	If you haven't done so already, Enable the dynamic attributes connector, on page 8 .
4	Secure Firewall Management Center	Create the Cisco APIC connector which retrieves EPGs and ESGs from Cisco APIC and enables them to be used in Secure Firewall Management Center access control policies or DNS policies . See Create a Cisco APIC connector, on page 36 .
5	Secure Firewall Management Center	(Optional.) View the dynamic objects fetched from Cisco APIC . See View dynamic objects in the Secure Firewall Management Center .
6	Secure Firewall Management Center	To use dynamic objects in access control policies or DNS policies , you must add them as dynamic objects to those rules. See Create access control rules or DNS rules using dynamic attributes filters .

System requirements for the integration with Cisco APIC

Your system must meet these requirements to successfully integrate Cisco APIC with the Secure Firewall Management Center.

- Secure Firewall Management Center version: 10.0.0 and later.

  Essentials license or better required; high availability is supported.

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

Get required information for the integration

Gather the required information to integrate the dynamic attributes connector with Cisco APIC.

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

This task provides the steps to collect all necessary information from Cisco APIC that will be used to configure the integration and name dynamic objects. You need access to the APIC management console and appropriate privileges to complete these steps.

Procedure

Step 1 Get the Cisco ACI Endpoint Update App site prefix and update interval if you're currently using it.

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

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

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

b. Click **Apps**.

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

d. Click **Edit** ().

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

Step 2 Find a user with appropriate access to configure the integration.

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:

a. Log in to Cisco APIC.

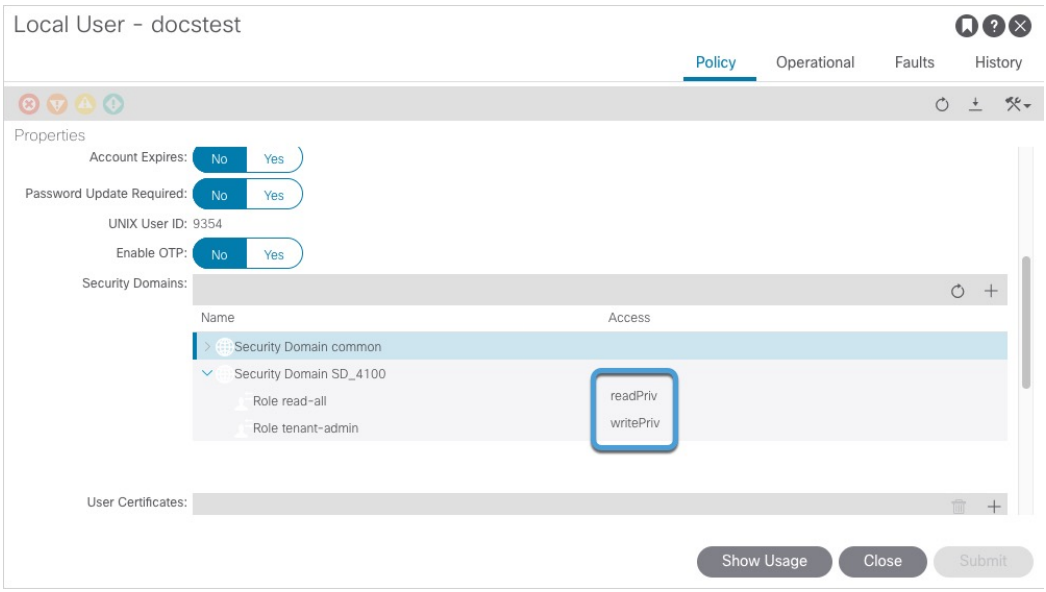
b. Click **Admin**.

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

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

e. Scroll to Security Domains.

f. 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.



Step 3 Get the Cisco APIC tenant name.

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

a. Log in to Cisco APIC.

b. Click **Tenants**.

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

Step 4 Get the 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:

a. Log in to Cisco APIC.

b. Click **Tenants**.

c. Double-click the name of your tenant.

d. Expand your tenant.

e. Expand **Application Profiles**.

f. Write down the name of the application profile that contains EPGs and ESGs to integrate with the Secure Firewall Management Center.

Step 5 Get the EPG name.

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

a. Log in to Cisco APIC.

b. Click **Tenants**.

c. Double-click the name of your tenant.

d. Expand your tenant.

e. Expand **Application Profiles**.

f. Expand the name of the application profile.

g. Expand **Application EPGs**.

h. Write down the name of the EPG or ESG that has network object groups to send to the Secure Firewall Management Center.

This figure shows an example.

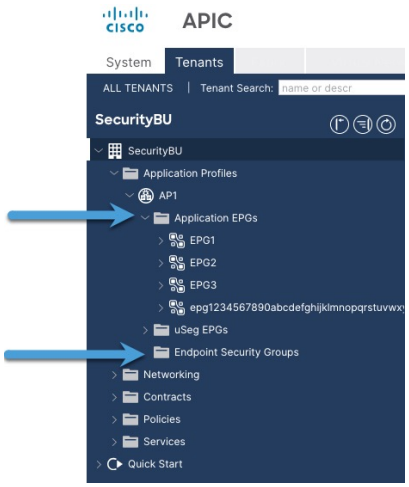
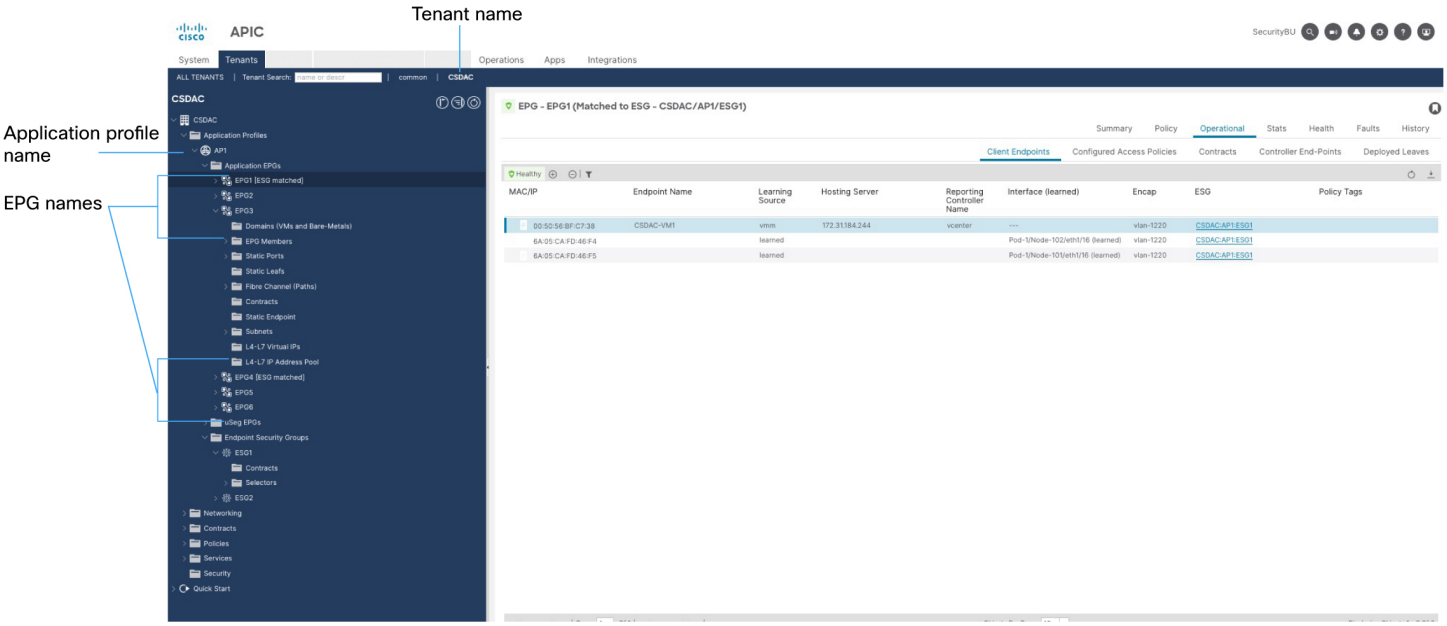


Figure 1: Example values in Cisco APIC



Create a Cisco APIC connector

Create a Cisco APIC connector to establish connectivity between Cisco APIC and the firewall, enabling the retrieval of network object groups from configured endpoint groups (EPGs).

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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

Value	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.
Server Certificate	(Recommended if using fully-qualified domain name.) You have these options: • Paste the certificate authority (CA) chain you got as discussed in Manually get a certificate authority (CA) chain, on page 37. • 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 37. • 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.

Click **Save**.

Status column displays **Ok**.

Manually get a certificate authority (CA) chain

If the certificate authority chain is not fetched automatically, use one of these browser-specific procedures to get a certificate chain to securely connect to vCenter or Firewall Management Center .

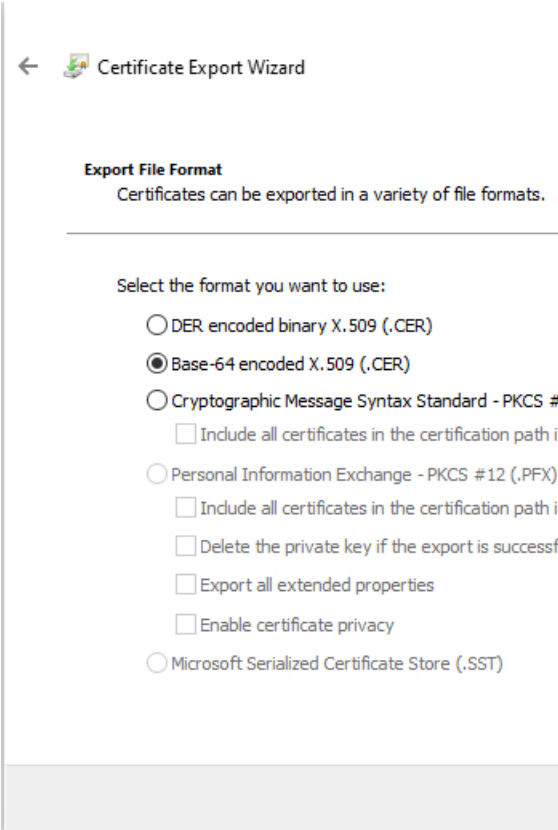
The *certificate chain* is the root certificate and all subordinate certificates.

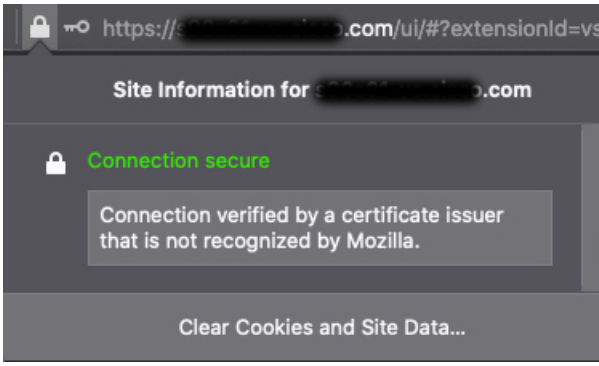
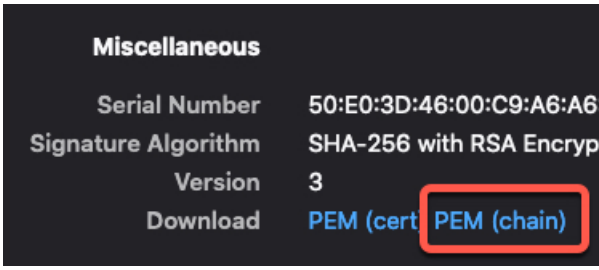
Procedure

	Command or Action	Purpose

Step 1	Get a Certificate Chain—Mac (Chrome and Firefox)	**a.** Open a Terminal window.
		b. Enter this 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`
		c. 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.
		d. Repeat these tasks for vCenter Firewall Management Center .

Step 2	Get a Certificate Chain—Windows Chrome	**a.** Log in to vCenter or Firewall Management Center using Chrome. **b.** In the browser address bar, click the lock to the left of the host name. **c.** Click **Certificate**. **d.** Click the **Certification Path** tab. **e.** Click the top (that is, first) certificate in the chain. **f.** Click **View Certificate**. **g.** Click the **Details** tab.

	Command or Action	Purpose
		h. Click **Copy to File**. **i.** 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)**.  Follow the prompts to complete the export. Open the certificate in a text editor. Repeat the process for all certificates in the chain. You must paste each certificate in the text editor in order, first to last. Repeat these tasks for vCenter or Firewall Management Center .
Step 3	Get a Certificate Chain—Windows Firefox	**a.** Log in to vCenter or Firewall Management Center using Firefox.

	Command or Action	Purpose
		b. Click the lock to the left of the host name. **c.** Click the right arrow (**Show connection details**).  **d.** Click **More Information**. **e.** Click **View Certificate**. **f.** If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA. **g.** Scroll to the Miscellaneous section. **h.** Click **PEM (chain)** in the Download row.  **i.** Save the file. Repeat these tasks for vCenter or Firewall Management Center .

Create a Cisco cyber vision connector

This task creates a connector to send data from Cisco Cyber Vision to the firewall, enabling dynamic attribute integration between these systems.

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.

Follow these steps to create a Cisco Cyber Vision connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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 required 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.
Version 4	(Required) Toggle this button to enable or disable Version 4. When you enable Version 4, the connector fetches hosts and vulnerabilities from the Cyber Vision platform. The Network Map API on the Secure Firewall Management Center uses this data. When you disable Version 4, the connector fetches groups from the Cyber Vision platform and adds them as dynamic objects.
Token	(Required) Enter the API token.

Value	Description
Score Type	Choices are CVSS and CSRS. **CVSS**: Common vulnerability scoring system (CVSS) is an industry-standard system that retrieves values from the national vulnerability database to describe risk associated with vulnerabilities. CVSS scores power a vulnerability's severity and risk value. **CSRS**: The Cisco Security Risk Score (CSRS) CSRS evaluates vulnerabilities beyond technical severity, focusing on how attackers might exploit them. Scores range from 0 to 100 and are based on factors such as existing vulnerabilities, threat intelligence, and the effectiveness of security controls. This score helps prioritize critical vulnerabilities and allocate resources effectively.
Severity	Click the minimum vulnerability severity level for the dynamic attributes connector to send IP addresses to the Secure Firewall Management Center. (For example, if you click high, IP addresses of hosts with either high or severe vulnerabilities are sent.) Choices: • Critical • High • Medium • Low
Dynamic Object Name	Enter a name to identify the dynamic object created by this connector.
Certificate	You have these options: • Paste the certificate authority (CA) chain as discussed in Manually get a certificate authority (CA) chain, on page 37. • Click **Get Certificate** > **Fetch** to automatically fetch the certificate. Ensure that you have specified a valid host and IP address that exactly matches the server certificate. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously. The configured hostname or IP address must be valid for the server certificate. Upload the CA certificate chain used to validate that certificate

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.

Status column displays **Ok**.

Create a generic text connector

Use this task to create a connector that retrieves IP addresses from text files and sends them to the firewall for use in access control rules.

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.

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.

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.

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

Follow these steps to create a generic text connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.
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.

Item	Description
Certificate	(Optional.) If a certificate chain is required for a secure connection to the web server, you have these 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 37. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.
c) Status column displays **Ok**

Create a GitHub connector

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.

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.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Before you begin

You do not have to create a dynamic attributes filters.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

a) (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).

b) Click **Save**.

The Status column displays **Ok**.

Google cloud connector user permissions and imported data

A Google Cloud connector imports dynamic attributes from Google Cloud to Secure Firewall Management Center for use in policies.

Dynamic attributes imported

The connector imports these dynamic attributes from Google Cloud:

- *Labels*: Key-value pairs assigned to virtual machine instances. Use the labels to organize your Google Cloud resources. For more information, see Creating and Managing Labels in the Google Cloud documentation.
- *Network tags*: Text values assigned to virtual machine instances that help identify groups of instances. For more information, see Creating and Managing Tags in the Google Cloud documentation.
- *IP addresses*: IP addresses associated with virtual machine instances in your Google Cloud project and region.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

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

Create a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

This task sets up a service account that provides the minimum permissions necessary for the dynamic attributes connector. For a list of these attributes, see Google cloud connector user permissions and imported data, on page 45.

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.

Click **Create and Continue**.

Step 4 Follow the prompts on your screen until the Grant users access to this service account section is displayed.

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

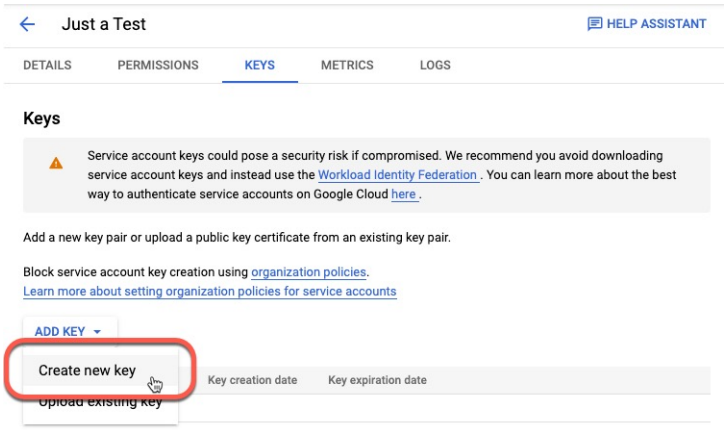
Click **Done**.

A list of service accounts is displayed.

Step 5 Click **More** (⋮) at the end of the row of the service account you created.

Step 6 Click **Manage Keys**.

Step 7 Click **Add Key** > **Create New Key**.



Step 8 Click **JSON**.

Step 9 Click **Create**.

The JSON key is downloaded to your computer.

Keep the key handy when you configure the GCP connector.

See Create a google cloud connector, on page 46.

Create a google cloud connector

Create a Google Cloud connector to enable data transmission from your Google Cloud environment to the firewall for dynamic security attribute monitoring and management.

The Google Cloud connector allows the firewall to receive real-time data from your Google Cloud infrastructure, enabling dynamic security policies based on cloud resource attributes.

Before you begin

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

Follow these steps to create a Google Cloud connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

a) Click **Save**.

The Status column displays **Ok**.

Create an office 365 connector

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, refer to Office 365 URLs and IP address ranges on docs.microsoft.com.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.
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**.

The Status column displays **Ok**.

Tenable connector

These topics provide information about creating and using the Tenable connector for vulnerability management.

About the Tenable connector

Tenable Vulnerability Management is a platform that helps organizations understand, report, and manage known vulnerabilities. When used with the Cloud-Delivered Firewall Management Center, the Tenable connector:

- Creates a dynamic object with a list of IP addresses known to have Common Vulnerability Exposures (CVEs).
- Populates those IP addresses and associated vulnerabilities to the Cloud-Delivered Firewall Management Center network map as host entries.

  Network map entries provide the basis for intrusion policy recommendations.

The dynamic object created by this connector can be used in access control rules, or anywhere dynamic objects are supported. For example, you can use the dynamic object to block vulnerable devices from accessing highly sensitive resources.

Supported products

We support Tenable Vulnerability Management only. We *do not* support Tenable Security Center.

Get the Tenable API key and secret

To configure the Tenable connector, you must create an API key and secret as described in this topic.

Note API keys inherit the permissions of the user account that generates them. Create the API key and secret using an account with full visibility to all hosts and vulnerabilities. For more information, see Permissions.

Procedure

Step 1 Log in to Tenable as an administrator.

Step 2 Click your profile image in the top right of the page.

Step 3 Click **My Profile** > **API Keys**.

Step 4 Click **Generate**.
You are required to confirm the action.

Step 5 Under Custom API keys, click (Copy to clipboard) to copy both the access key and secret key to the clipboard.

Step 6 Save these values for later use.

What to do next

See Create a Tenable connector, on page 50.

Create a Tenable connector

This task explains how to configure the Tenable connector in Security Cloud Control.

Before you begin

- Configure Tenable Vulnerability Management : Consult Tenable documentation.
- Get required information: Get the Tenable API key and secret, on page 49.

We support Tenable Vulnerability Management only. We *do not* support Tenable Security Center.

Required User Role:

- Super Admin

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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 21600 seconds or six hours.) Interval at which IP mappings are retrieved from Tenable. We recommend a minimum value of 3600 seconds (one hour) to avoid issues with Tenable rate limiting.
Integration Key	Enter the API key you got in Get the Tenable API key and secret, on page 49.
Secret Key	Enter the secret key obtained in Get the Tenable API key and secret, on page 49.
Dynamic Object Name	Enter a name to identify the dynamic object created by this connector.

Value	Description
Severity Score	Click the minimum vulnerability severity level for the dynamic attributes connector to send IP addresses to the Secure Firewall Management Center. (For example, if you click **high**, IP addresses of hosts with either high or severe vulnerabilities are sent.) Choices: • **Critical** • **High** • **Medium** • **Low**
Severity System	Choices: • **VPR**: (Vulnerability priority rating.) Proprietary Tenable vulnerability rating that dynamically scores threats. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit: • VPR **critical** is 9.0 and greater • VPR **high** is 7.0 and greater • VPR **medium** is 4.0 and greater • VPR **low** is 0.1 and greater • **CVSSv3**: (Common vulnerability scoring system version 3.) Industry-standard system that retrieves values from the national vulnerability database to describe risk associated with vulnerabilities. CVSS scores power a vulnerability's severity and risk value. For more information, see CVSS vs. VPR.

Step 5 Click **Test**. Save the connector only after the test succeeds.

Step 6 Click **Save**.

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

About Tenable dynamic objects in IDS, IPS, and access control policies

You can use IPS, IDS, and access control policies and rules to monitor or block traffic to and from servers with vulnerabilities identified by the Tenable connector:

1. To monitor traffic and inform you about vulnerabilities *without* blocking the traffic, create an intrusion detection system (IDS) policy with recommendations.
2. To monitor traffic, inform you about vulnerabilities, and block matching traffic, create an intrusion prevention system (IPS) policy with recommendations.

3. Create a new access control policy or add rules to an existing policy. Associate your IDS or IPS policy with an access control rule.

For information about intrusion policies for access control, refer to the Snort 3 configuration guide.

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 these 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

Create a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center .

This task provides the steps to set up a service account with minimum permissions required for the dynamic attributes connector. For a list of these attributes, see vCenter connector—About user permissions and imported data, on page 52.

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.

Follow these steps to create a vCenter user with minimal permissions for the dynamic attributes connector:

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.

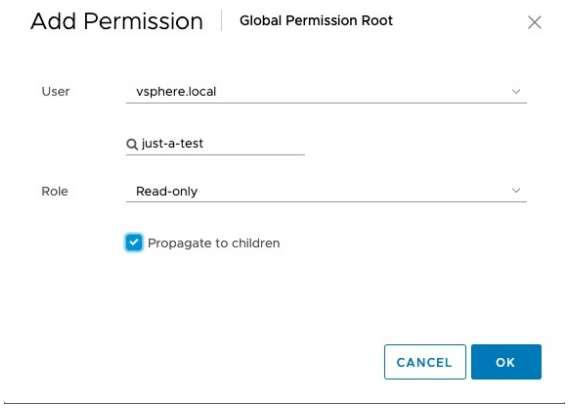
Step 5 Click **Add User**.

a) Enter the requested information and click **Add**.

Step 6 In the left pane, click **Access Control** > **Global Permissions**.

Step 7 Click **Add**( ).

a) From the **User** field, click the name of the vCenter domain in which you created the user.
b) In the search field, enter part of the user's name.
c) From the **Role** list, click **Read-only**.
d) Select the **Propagate to children** check box.



Step 8 Click **OK**.

What to do next

See Create a vCenter connector, on page 53.

Create a vCenter connector

Create a connector for VMware vCenter to send data to the Secure Firewall Management Center for use in policies.

This connector enables the management center to receive dynamic attribute information from vCenter Server for use in security policies and monitoring.

Before you begin

If you use non-trusted certificates to communicate with vCenter, see Manually get a certificate authority (CA) chain, on page 37.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

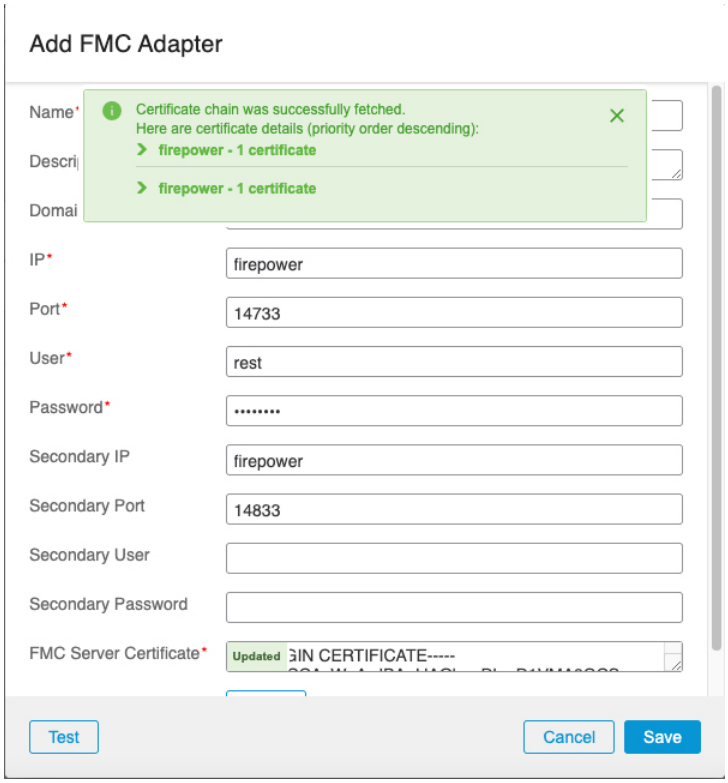
- Add a new connector: click Add icon ( ), then click the name of the connector.

- 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.
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 37. • 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 37. • 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 37. • 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 37.

Step 5 Click **Save**.

Create a Webex connector

This task creates a Webex connector that sends IP addresses to the management system for use in policies. The IP addresses associated with these tags are maintained by Webex.

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.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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.

a) Click **Test** and make sure the test succeeds before you save the connector.
b) Click **Save**.
c) The Status column displays **Ok**.

Create a Zoom connector

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.

The dynamic attributes connector has always operated in network download mode, where we download the images required to make it work from the internet. If you have tighter security requirements, you can consider air gapped mode.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **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 this 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.

a) Click **Test** and make sure the test succeeds before you save the connector.

b) Click **Save**.

The Status column displays **Ok**.

Create dynamic attributes filters

Create dynamic attributes filters to expose them as dynamic objects in Secure Firewall Management Center for use in access control policies.

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 or DNS rules, see Create access control rules or DNS rules using dynamic attributes filters.

Before you begin

Connectors, on page 17

Procedure

Step 1 Log in to the Secure Firewall Management Center.

a. Click **Integrations** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 2 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 3 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 4 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 5 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 6 When you're finished, click **Save**.

Step 7 (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** > **External Attributes** > **Dynamic Object**.

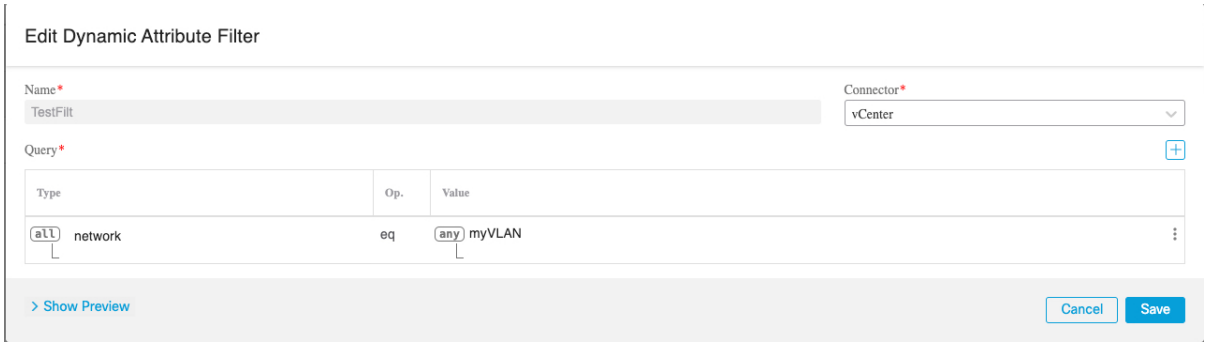
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

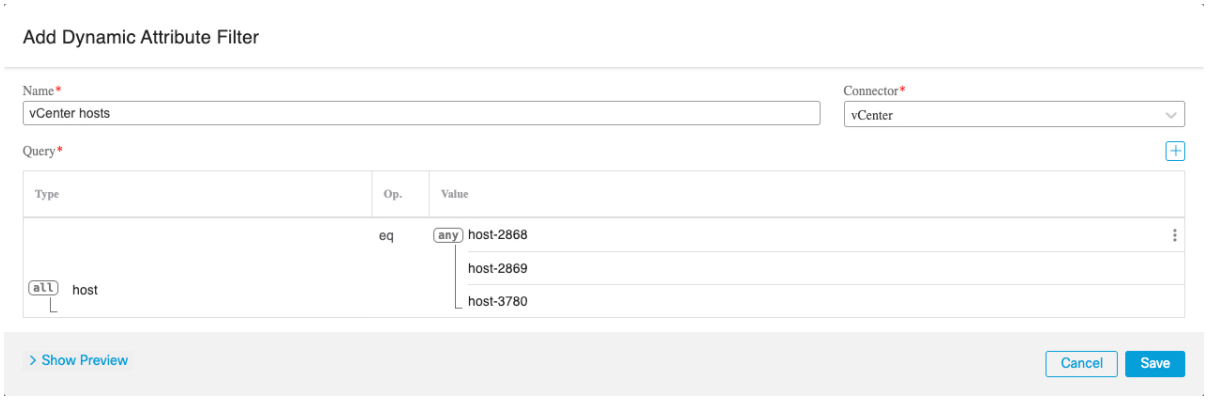
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

This example shows one criterion: a VLAN.

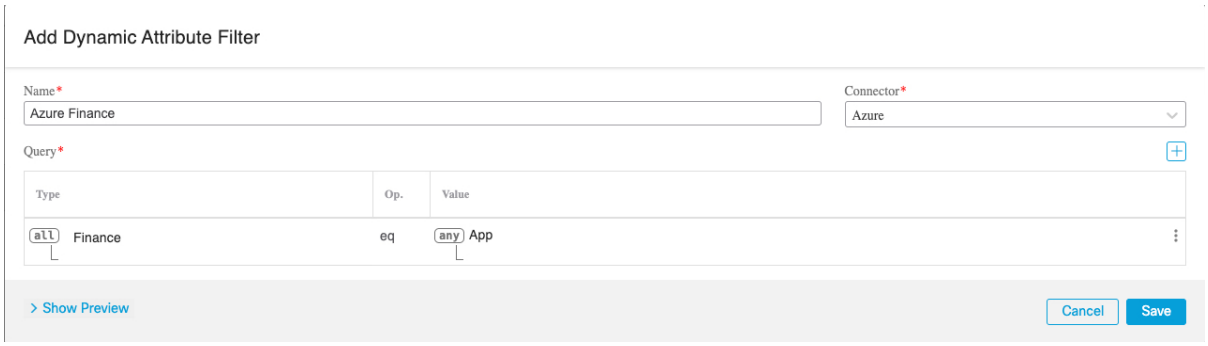


This example shows three criteria that are joined with OR: the query matches any of three hosts.



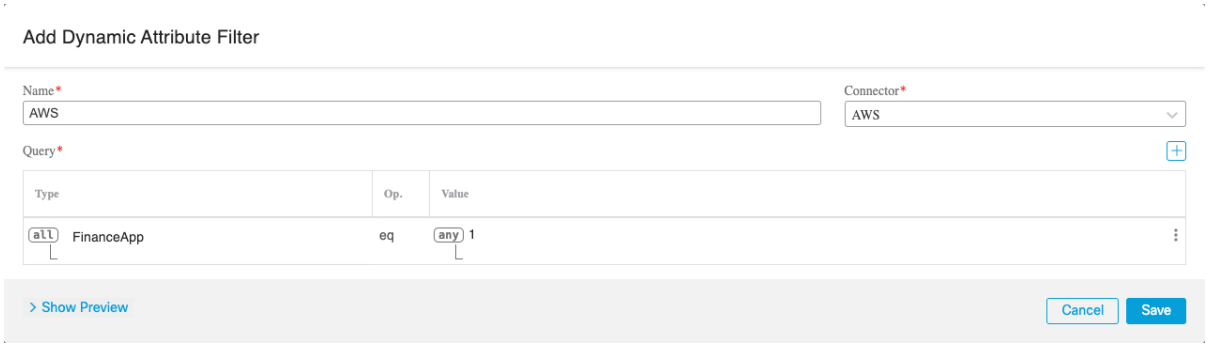
Example: azure

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



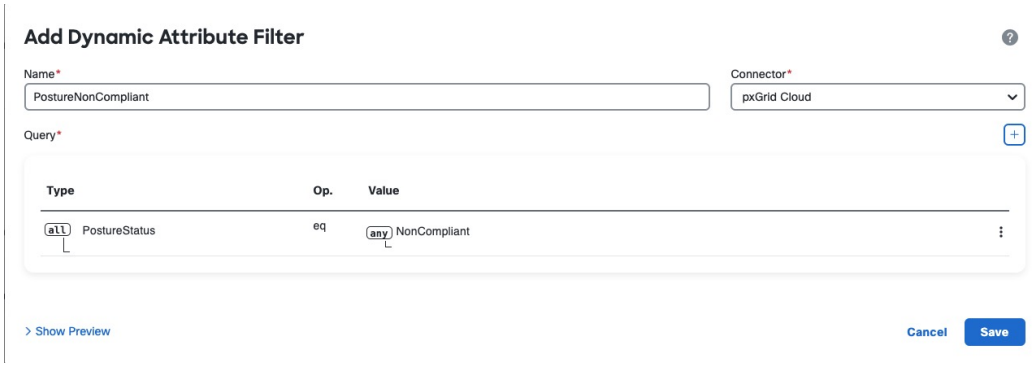
Example: AWS

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



Example: pxGrid cloud

This example shows one criterion: PostureStatus is NonCompliant.



Manually get a certificate authority (CA) chain

If the certificate authority chain is not fetched automatically, use one of these browser-specific procedures to get a certificate chain to securely connect to vCenter or Firewall Management Center .

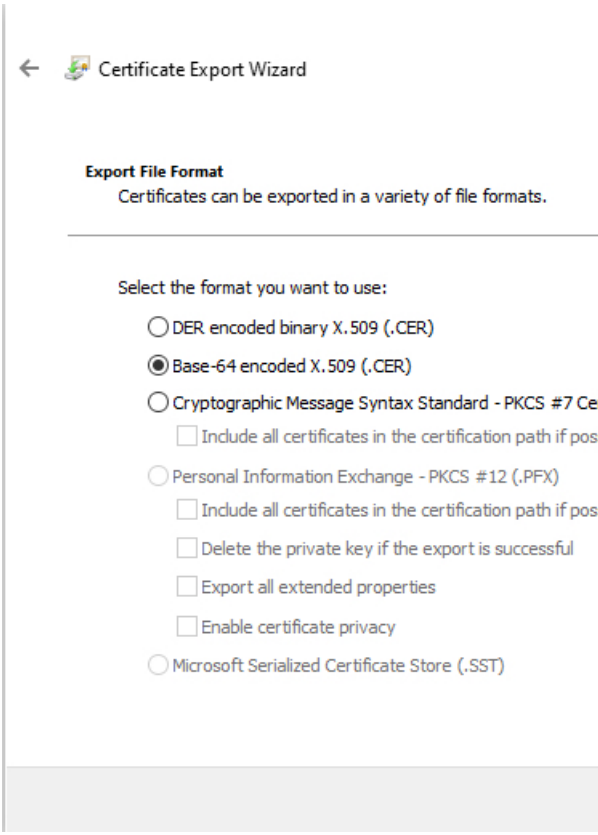
The *certificate chain* is the root certificate and all subordinate certificates.

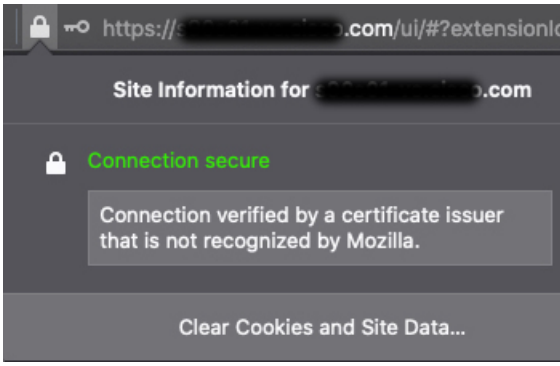
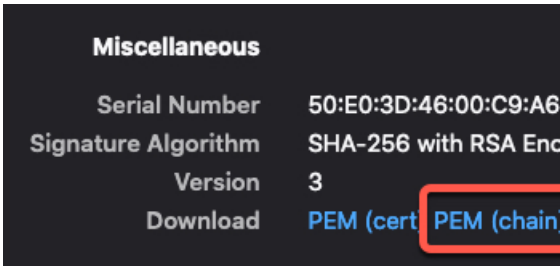
Procedure

	Command or Action	Purpose

Step 1	Get a Certificate Chain—Mac (Chrome and Firefox)	**a.** Open a Terminal window.
		b. Enter this 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`
		c. 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.
		d. Repeat these tasks for vCenter Firewall Management Center .

Step 2	Get a Certificate Chain—Windows Chrome	**a.** Log in to vCenter or Firewall Management Center using Chrome. **b.** In the browser address bar, click the lock to the left of the host name. **c.** Click **Certificate**. **d.** Click the **Certification Path** tab. **e.** Click the top (that is, first) certificate in the chain. **f.** Click **View Certificate**. **g.** Click the **Details** tab.

	Command or Action	Purpose
		h. Click **Copy to File**. **i.** 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)**.  Follow the prompts to complete the export. Open the certificate in a text editor. Repeat the process for all certificates in the chain. You must paste each certificate in the text editor in order, first to last. Repeat these tasks for vCenter or Firewall Management Center .
Step 3	Get a Certificate Chain—Windows Firefox	**a.** Log in to vCenter or Firewall Management Center using Firefox.

	Command or Action	Purpose
		b. Click the lock to the left of the host name. **c.** Click the right arrow (**Show connection details**).  **d.** Click **More Information**. **e.** Click **View Certificate**. **f.** If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA. **g.** Scroll to the Miscellaneous section. **h.** Click **PEM (chain)** in the Download row.  **i.** Save the file. Repeat these tasks for vCenter or Firewall Management Center .

Disable the dynamic attributes connector

Disable the Dynamic Attributes Connector when you no longer wish to collect dynamic objects from cloud sources.

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.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.
Step 2 Click **Integrations** > **Dynamic Attributes Connector**.
Step 3 Slide to **Disabled**.

Troubleshoot the Dynamic Attributes Connector

Troubleshoot using the Secure Firewall Management Center

Generate troubleshoot files to diagnose and resolve issues with 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 **Troubleshooting** > **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.

Recommendation: security requirements for network deployment

Install the dynamic attributes connector 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.

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

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.

This information details the URLs the dynamic attributes connector use to communicate with the Secure Firewall Management Center and with external servers.

Table 6: 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 7: 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

This document provides the history of features for the dynamic attributes connector, including feature introductions and modifications across different product versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Air gap	10.1.0		You have the option of installing and updating dynamic attributes connector connectors, adapters, and internal mode in air gap mode; that is, without an internet connection. **New/modified screens**: **Integrations** > **Dynamic Attributes Connector**, **Current update mode**.
DNS rule support for dynamic objects and security group tags.	10.0.0	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the Dynamic Attributes tab to the add/edit DNS rule dialog box.
Dynamic firewall	10.0.0	10.0.0	Previously, the Secure Firewall Management CenterSecure Firewall Management Center collected information about users exclusively from the configured identity source, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address. The dynamic firewall enables you to add user risk scores from Cisco Identity Intelligence to identity source-provided information so you can set policies based on always-current user posture and risk. We enable you to pair user identity with intelligence and use that information in reporting and access control policies. **New/modified screens**: • Click **Integrations** > **Dynamic Attributes Connector**. Then click next to the name of the identity source and click **Create Dynamic Firewall**.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Cisco APIC connector	10.0.0	10.0.0	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 . **New/updated screens:** • **Integrations** > **Dynamic Attributes Connector** > **Connectors** > **New Connector**
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: **Integrations** > **Dynamic Attributes Connector**