

Dynamic Attributes Connector

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

- About the dynamic attributes connector , on page 1
- How Cisco secure dynamic attributes connector works, on page 1
- System requirements for the Dynamic Attributes Connector, on page 3
- Enable the dynamic attributes connector, on page 3
- Dashboard, on page 5
- Connectors, on page 12
- Create dynamic attributes filters, on page 32
- Manually get a certificate authority (CA) chain, on page 34
- Dynamic objects in access control rules, on page 37
- Create dynamic attributes filters, on page 38
- Dynamic attributes rule conditions, on page 39
- Create access control rules using dynamic attributes filters, on page 40
- Dynamic firewall, on page 41
- Disable the dynamic attributes connector, on page 56
- Troubleshoot the Dynamic Attributes Connector, on page 57
- Recommendation: security requirements for network deployment, on page 57
- Internet access requirements, on page 57
- History for the dynamic attributes connector, on page 59

About the dynamic attributes connector

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

How Cisco secure dynamic attributes connector works

This topic discusses the architecture of the dynamic attributes connector.

The system functions by querying cloud services and providing attribute information to the secure management center.

Summary

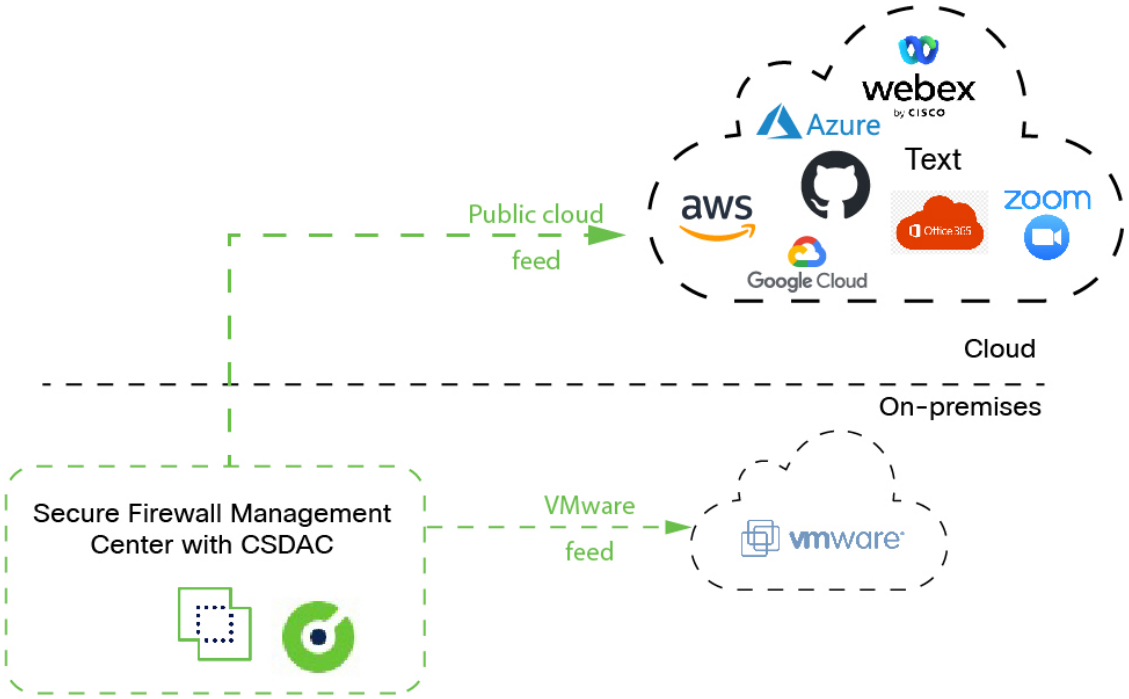
The key components involved in this process are:

- The system supports certain public cloud providers.

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

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

Workflow



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

1. *Connectors* contain the tags and containers to query.

   For example, typically these tags define dynamically allocated network and IP addresses for which you cannot create access control rules. Persisted feeds from the connectors are stored on the dynamic attributes connector for fast access.

2. Tag information is persisted on the dynamic attributes connector where you create *dynamic attributes filters* that define which information is important to use in access control rules.

   For example, if AWS defines networks for the Accounting and Finance Departments virtual machines, you can create a dynamic attributes filter that specifies only the Finance network.

3. The Secure Firewall Management Center receives those dynamic attributes filters as *dynamic objects* and enables you to use them in access control rules.

What's next

Related topics

- Enable the dynamic attributes connector, on page 3
- Dashboard, on page 5

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 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 rules.

Procedure

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

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

Step 3 Slide to **Enabled**.

Step 4 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 12.

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 1: 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 2: 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`
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:

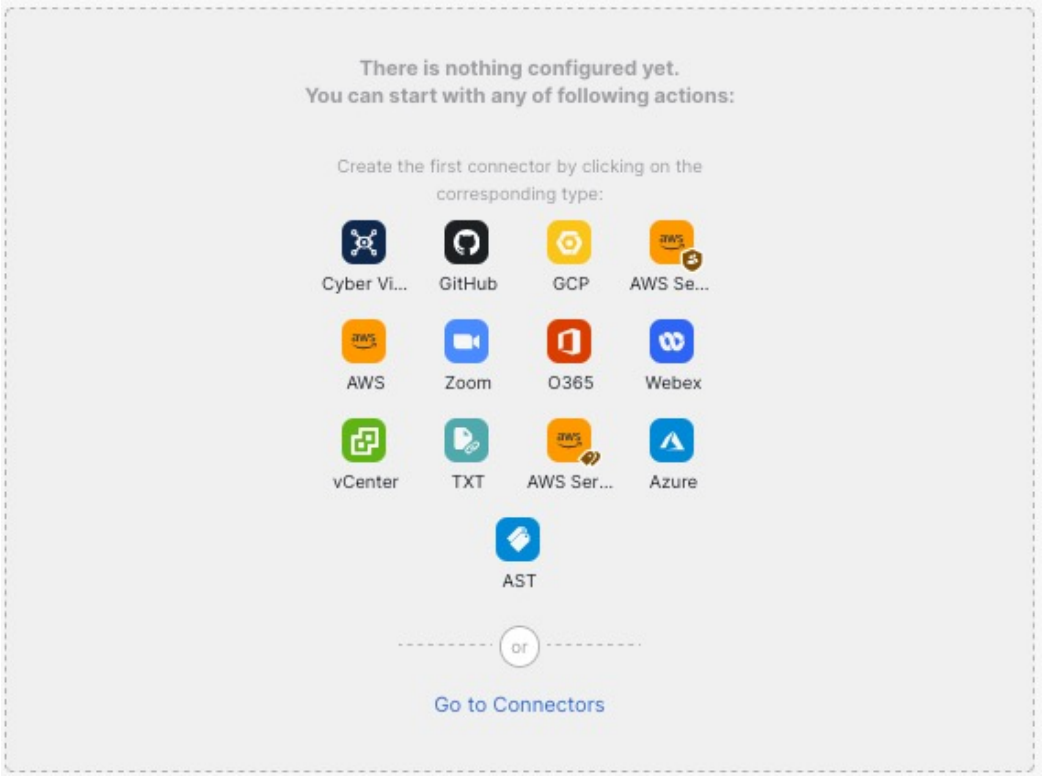
- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

Dashboard access and functionality

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

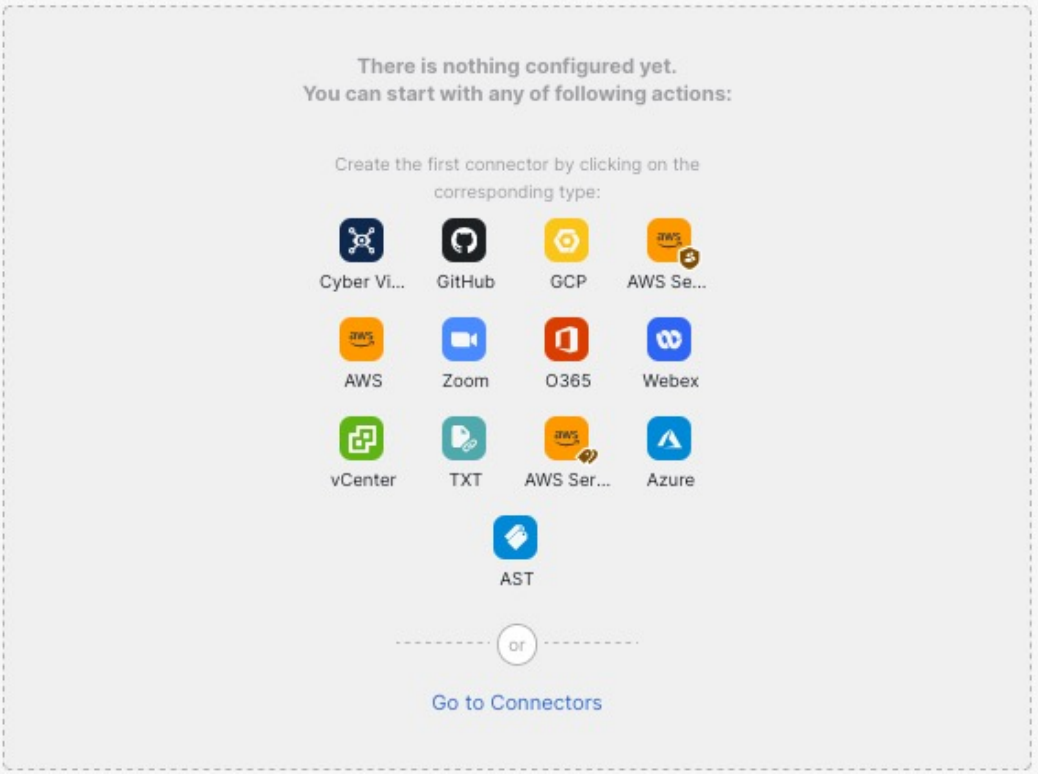
If the dynamic attributes connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

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

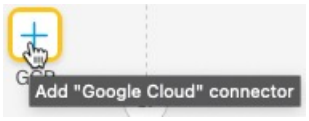


Dashboard of an unconfigured system

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 12.

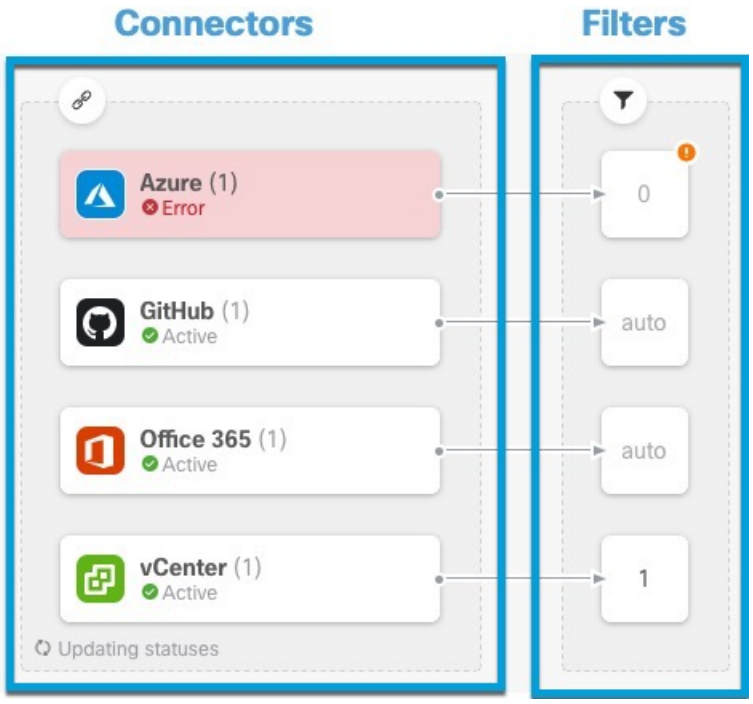
Related Topics:

- Dashboard of a configured system, on page 7
- Add, edit, or delete connectors, on page 9
- Add, edit, or delete dynamic attributes filters, on page 10

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 12

2 Create dynamic attributes filters, on page 32

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 9.	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 10.

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

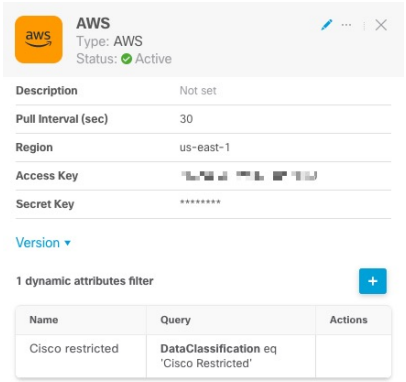
Step 1 Access the connector dashboard and select your desired action.

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:

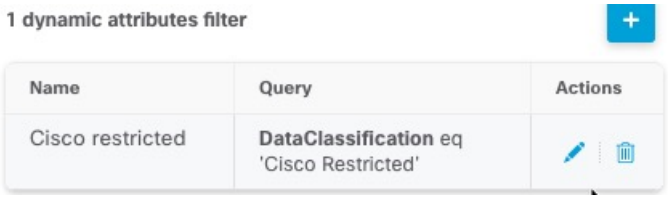


Step 3 Choose from the following management options.

- 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:



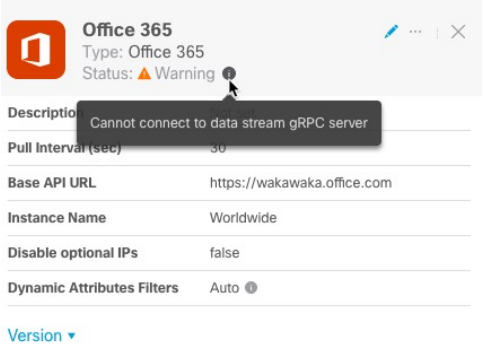
Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters, on page 32.

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 25.

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

What to do next

Provide all of this information to Cisco TAC.

Add, edit, or delete dynamic attributes filters

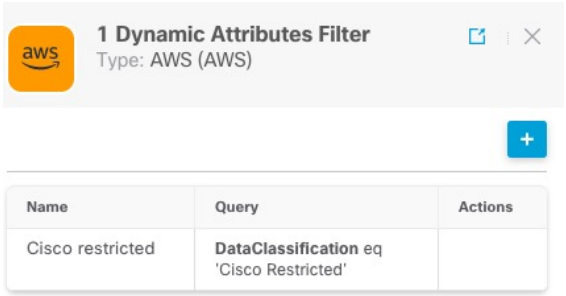
The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click for additional options.

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, on page 32.

An example follows:



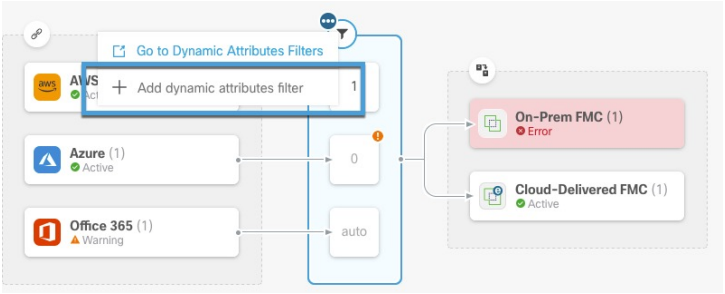
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

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, on page 32.
- 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

We support these connectors:

Table 3: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	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
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

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 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 12.

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.

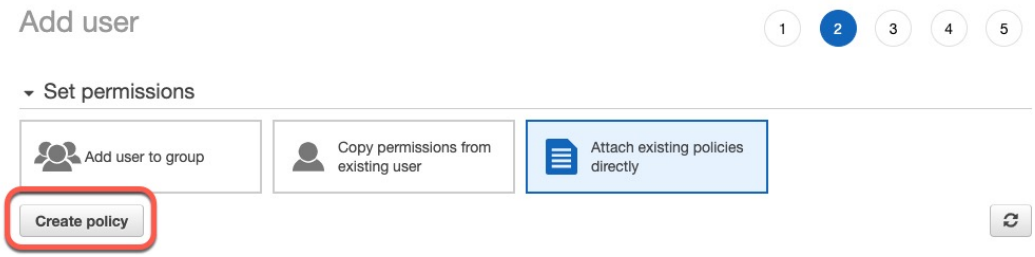
Note
This is the only opportunity you have to retrieve the user's key.

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 14.

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 13.

Follow these steps to create an AWS connector:

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of 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**.

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 15.

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**.

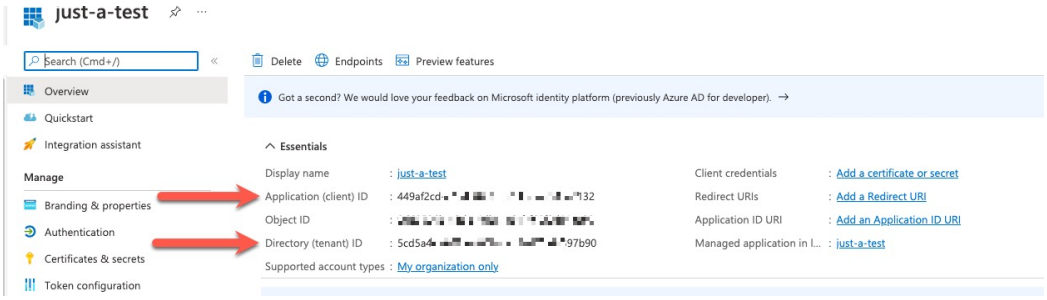
Find the instance of Azure Active Directory for the application you want to set up.

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*).

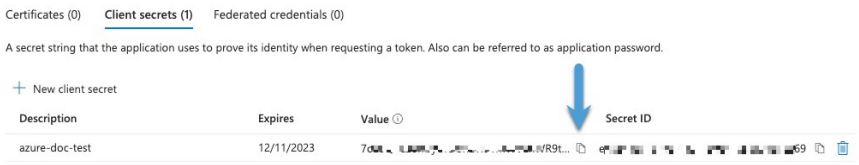
Here is a sample:



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

Step 6 Click **New Client Secret**.

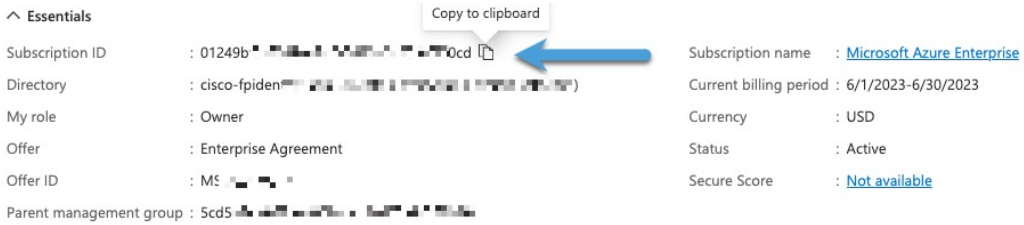
a) Enter the requested information and click **Add**.
b) Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



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.



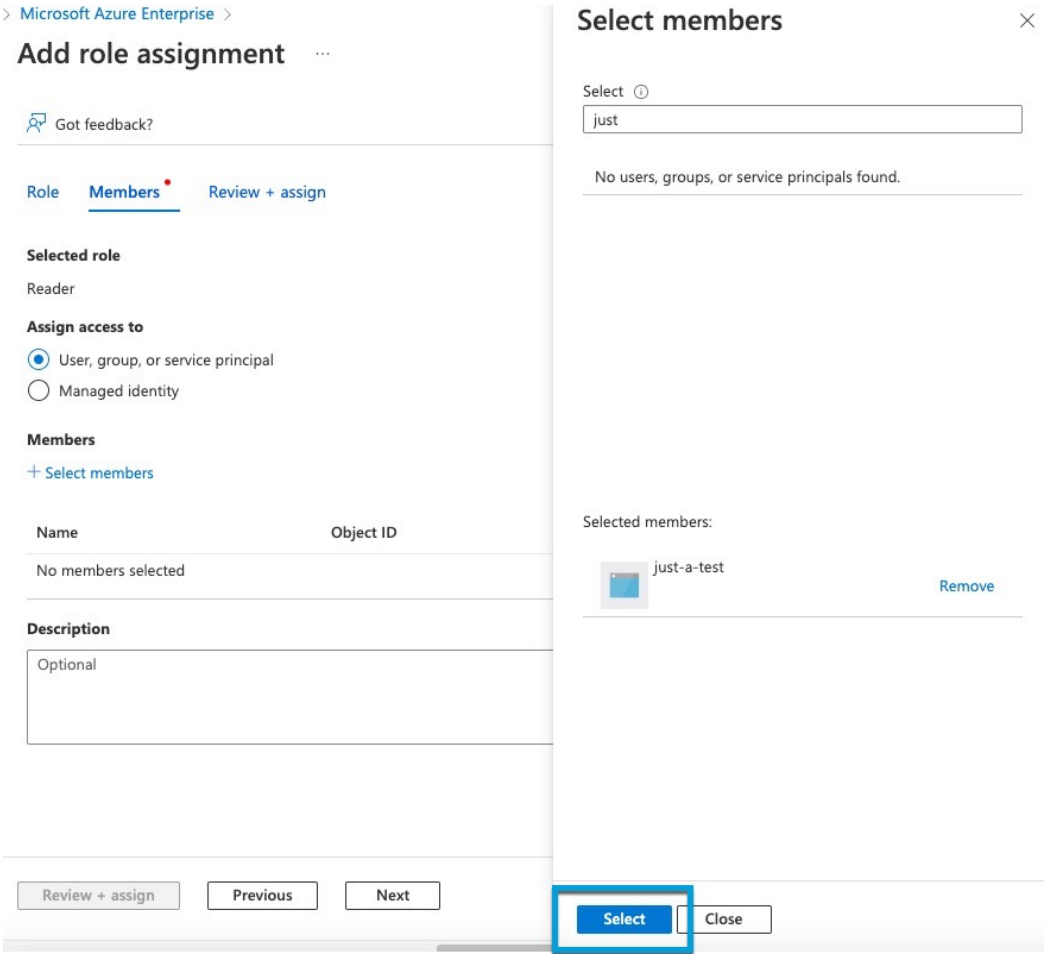
Step 8 Click **Access Control (IAM)**.

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 18.

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 16.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

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.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the 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**.

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 **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information:

Item	Description
Name	Enter a name to identify the connector.
Description	(Optional.) Enter a description
Pull Interval	Change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from the text file. The default is 30 seconds. The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
URLs	Enter a URL from which to retrieve IP addresses.
Add another URL	(Optional.) Click the link to add more URLs to an existing list.
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 34. • 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.

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 **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter a **Name** and an optional description.

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 you can use to organize your Google Cloud resources. For more information, see Creating and Managing Labels in the Google Cloud documentation.
- *Network tags*: Key-value pairs associated with an organization, folder, or project. For more information, see Creating and Managing Tags in the Google Cloud documentation.
- *IP addresses*: Virtual machine addresses in Google Cloud.

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 22.

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.

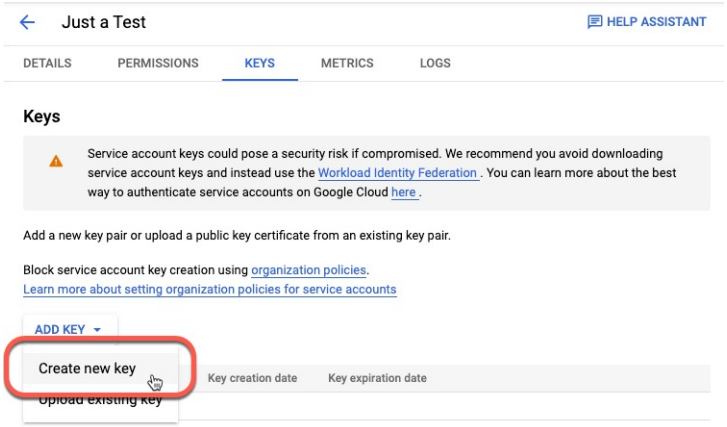
Click **Done**.

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 24.

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 **Integration** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

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.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

Value	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**.

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 26.

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.

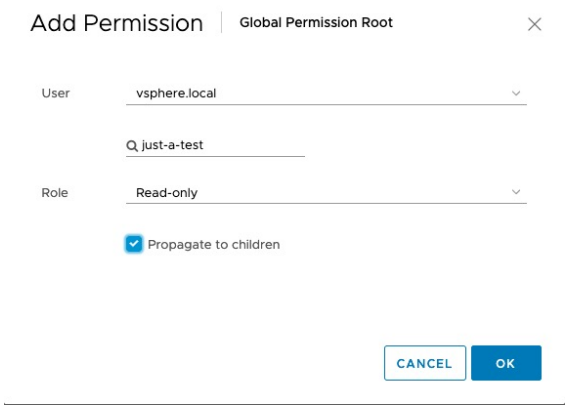
Step 5 Click **Add User**.

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 28.

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 34.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

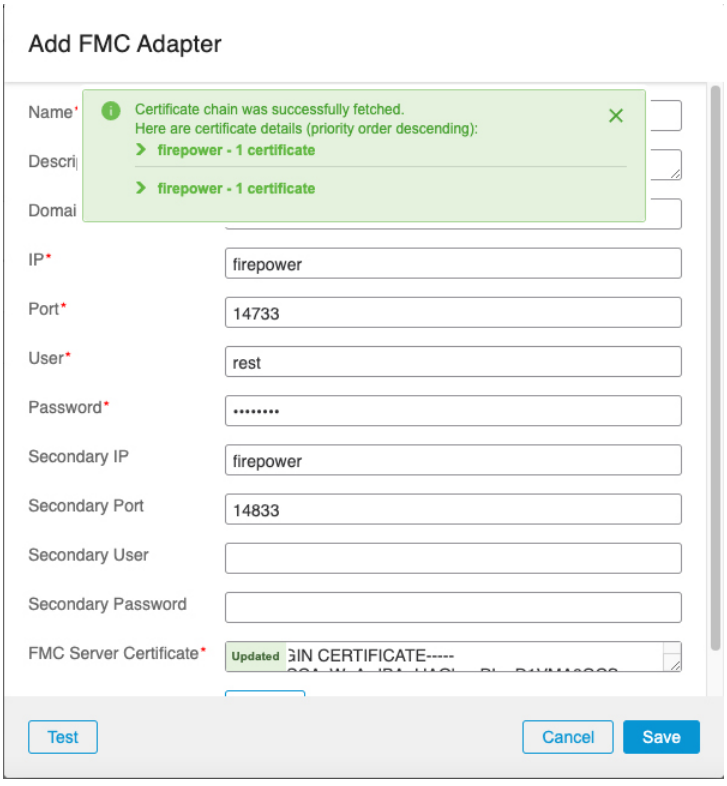
- Add a new connector: click Add icon (), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

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

Value	Description
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.
NSX Password	Enter the NSX user's password.
vCenter Certificate	You have the following options: • Paste the certificate authority (CA) chain you got as discussed in Manually get a certificate authority (CA) chain, on page 34. • 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 34. • 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 34. • 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 34.

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.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

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.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

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

Step 4 Enter 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 rules, see Create access control rules using dynamic attributes filters, on page 40.

Before you begin

Connectors, on page 12

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Click **Integration** > **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** > **Object Management** > **External Attributes** > **Dynamic Object**.

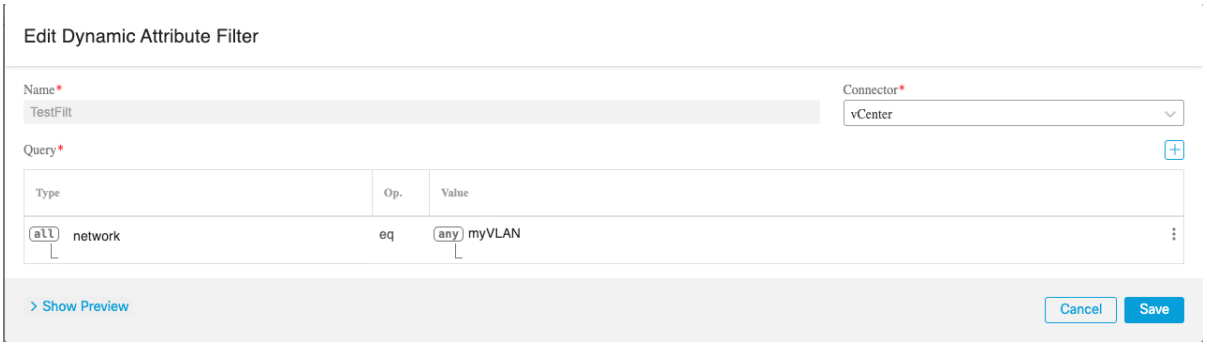
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

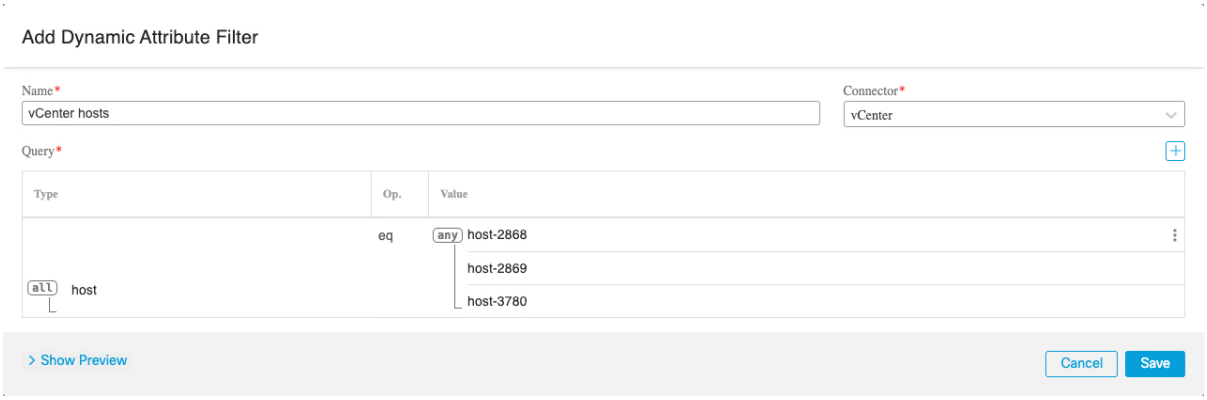
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

This example shows one criterion: a VLAN.

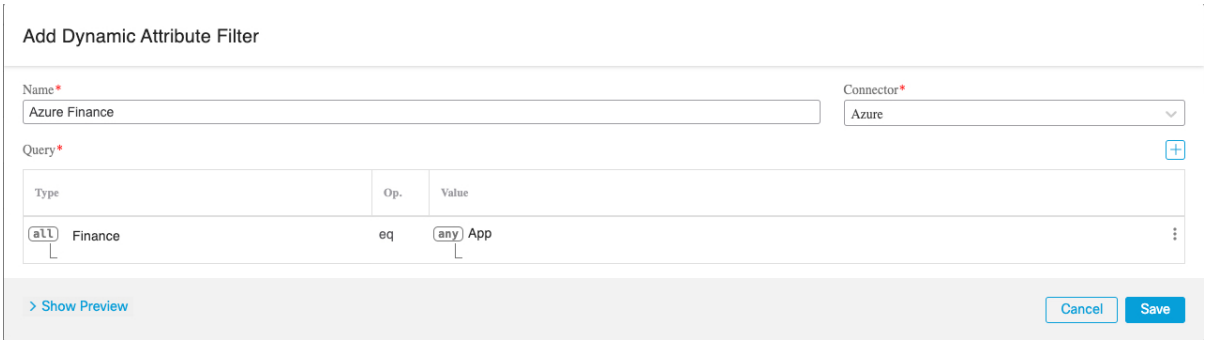


This example shows three criteria that are joined with OR: the query matches any of three hosts.



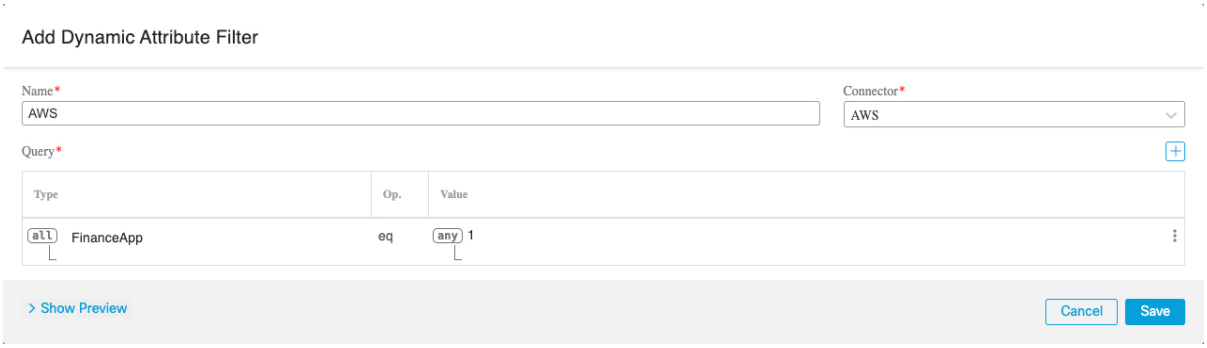
Example: azure

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.



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 .

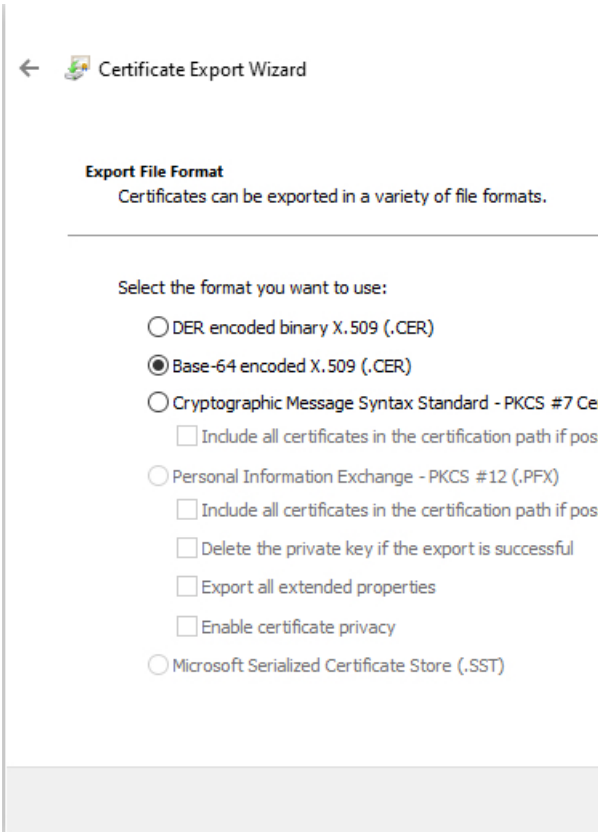
The *certificate chain* is the root certificate and all subordinate certificates.

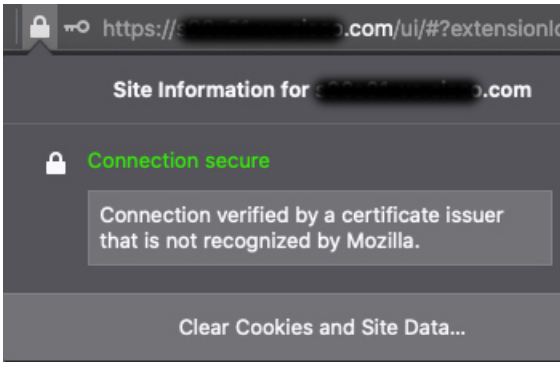
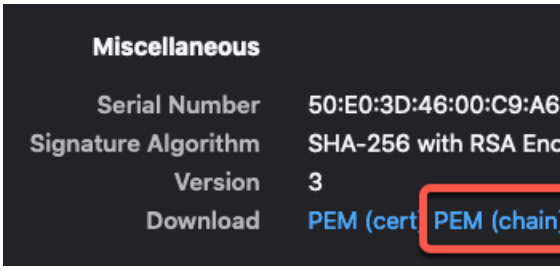
Procedure

	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 .

Dynamic objects in access control rules

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

You can use these dynamic objects on the access control rule's **Dynamic Attributes** tab page. You can add dynamic objects as source or destination attributes.

Dynamic object usage examples

In an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

Dynamic attributes filter limitations

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

Create dynamic attributes filters

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 rules, see Create access control rules using dynamic attributes filters, on page 40.

Before you begin

Connectors, on page 12

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Click **Integration** > **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** > **Object Management** > **External Attributes** > **Dynamic Object**.

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

Dynamic attributes rule conditions

Dynamic attributes rule conditions allow you to specify access control rules based on real-time properties such as network objects, device types, locations, and security tags. These conditions determine how access control rules match traffic based on various attributes, optimizing policy flexibility and accuracy.

Types of dynamic attributes

Dynamic attributes include:

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

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

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

- (source only) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and destination security group tag (SGT) matching and Security group tags.
- (source only) Location IP objects, defined by Cisco ISE
- (source only) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Combining objects in rules

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use these guidelines:

- Objects of different types are ANDd together
- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1, the rule matches if device type 1 is detected on either SGT 1 or SGT 2.

If you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originating from, or destined to, one of those IP addresses.

Create access control rules using dynamic attributes filters

Create access control rules using dynamic objects that are based on dynamic attributes filters you have previously configured.

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

To add dynamic attributes filters to DNS policies, see Create basic DNS policies.

Before you begin

Create dynamic attributes filters as discussed in Create dynamic attributes filters, on page 32.

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.

Follow these steps to create access control rules using dynamic attributes filters:

Procedure

Step 1 Log in to the Secure Firewall Management Center

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

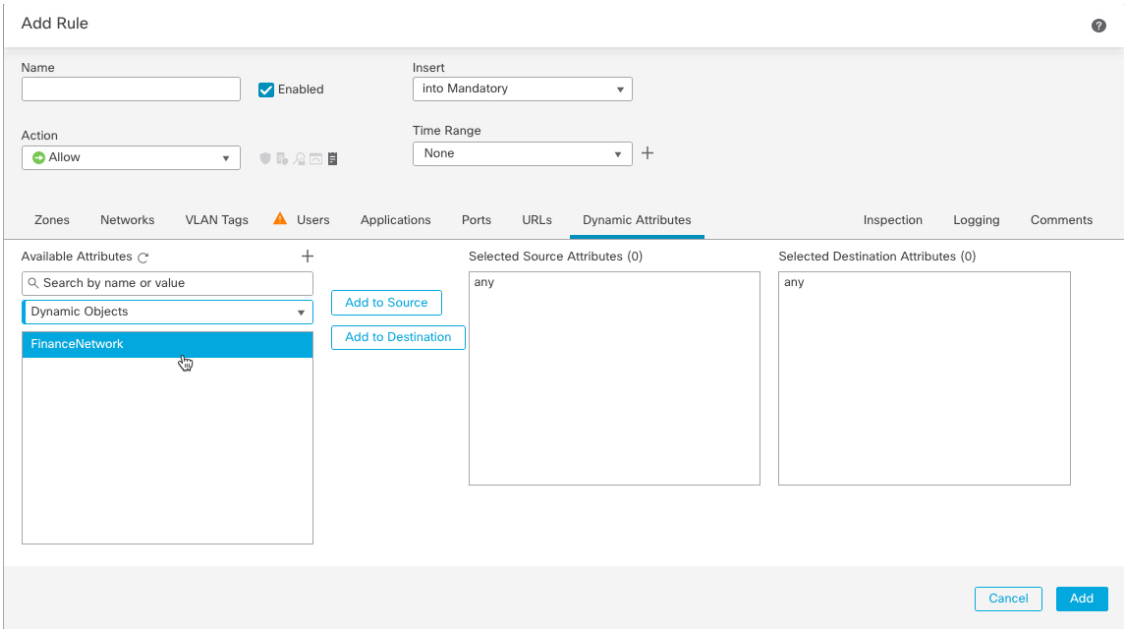
Step 2 Click **Edit** ( ) next to an access control policy.

Step 3 Click **Add Rule**.

Step 4 Click the **Dynamic Attributes** tab.

Step 5 In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.



This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.

Step 6 Add the desired object to source or destination attributes.

Step 7 Add other conditions to the rule if desired.

See Dynamic attributes rule conditions, on page 39.

Dynamic firewall

A dynamic firewall integrates user identity data with user trust data provided by Identity Intelligence to enhance your ability to detect identity-based exploits in your network.

Identity data integration

The dynamic firewall integrates user identity data from Microsoft AD and ISE with user trust data.

Dynamic Firewall

A dynamic firewall integrates identity sources with Identity Intelligence to provide user and device trust information.

Enhanced identity information

Previously, the collected information about users exclusively from the configured identity sources, 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 pair user identity with intelligence and use that information in reporting and access control policies.

To use the dynamic firewall, you must:

- Have an Identity Intelligence tenant

  See Duo Identity Security with Cisco Identity Intelligence.

- Enable the Dynamic Attributes Connector
- Set up an identity source:
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid Cloud

    pxGrid Cloud combines identity and posture in the same feed

    More information: What is pxGrid?

  In addition to providing authentication information, Cisco ISE and pxGrid Cloud can provide the following:

  - SGT Exchange Protocol (SXP) over TCP binding and directory session information if desired. For more information, see the *Cisco Identity Services Engine Administrator Guide*
  - Posture and mobile device management compliance. For more information, see Compliance.

- Set up an identity realm:
  - Create an LDAP realm or an Active Directory realm and realm directory

The *identity source* provides authentication information (login, logout) as well as posture. The identity source can also provide SXP binding and session directory information if desired.

The *identity realm* provides user, group, and IP address information.

How to configure the dynamic firewall

This topic helps you understand the concepts and options to configure the dynamic firewall discussed in Dynamic Firewall, on page 42.

Summary

The dynamic firewall integrates an identity source (such as Cisco ISE) with Cisco Identity Intelligence, which provides user trust information to the Secure Firewall Management Center.

1. Configure Cisco Identity Intelligence to collect user trust information.
2. Configure a supported Secure Firewall Management Center identity source.
3. Configure a supported identity realm.
4. Enable the dynamic attributes connector.
5. Configure the dynamic firewall.

Workflow

The following procedure provides a high-level overview of how to configure the dynamic firewall.

1. As a Duo user with the Owner role, provision a Cisco Identity Intelligence tenant.

   You can provision a tenant from Duo Advantage as discussed in *Provision Your Cisco Identity Intelligence Tenant*.

2. In Cisco Identity Intelligence, create an API integration and use the information to set up the dynamic firewall.

   We use Cisco Identity Intelligence to find user and device risk information in your network.

   For more information about Cisco Identity Intelligence, see How-to Guides.

   For more information about this task, see Get required information for Identity Intelligence, on page 45.

3. (Microsoft Azure AD realm only.) In Identity Intelligence, create a Microsoft Entra ID integration.

   For more information, see Microsoft Entra ID (Azure AD) Data Integration.

4. Create an identity source. (If you already have an identity source, continue with the next step.)

   You can do this in any of the following ways:

   - The Configure Dynamic Firewall dialog box displays **Configure** links to start setting up your identity source.
   - Click **Integration** > **Other Integrations** > **Identity Sources**.

   For more information about creating identity sources, see:

   - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
   - Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
   - Configuring a pxGrid Cloud identity source

5. Create an identity realm.

   We support the following realms:

   - Create an LDAP realm or an Active Directory realm and realm directory

     Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

6. Enable the dynamic attributes connector.

   The dynamic attributes connector is required to use the dynamic firewall. It enables your identity source to integrate with Identity Intelligence to provide enhanced insights into user activity.

   See Enable the dynamic attributes connector, on page 3.

7. Create the dynamic firewall instance. (If you already have a dynamic firewall instance, continue with the next step.)

   Click **Integration** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

   See Create a dynamic firewall instance, on page 47.

8. Associate your identity source with Cisco Identity Intelligence.

   See Associate an identity source with Identity Intelligence, on page 48.

9. View system-defined filters.

   We create dynamic attributes filters for the following:

   - Untrusted device
   - Trusted device
   - Untrusted user
   - Questionable user

   You can edit or replace these dynamic attributes filters as discussed in Create dynamic attributes filters, on page 55.

10. View system-defined access control rules.

    We create an access control policy named Dynamic Firewall Policy (or similar) with the following rules:

    - Block an untrusted user from any source network to any destination network.
    - Monitor a questionable user from any source network to any destination network.
    - Block an untrusted device from any source network to any destination network.

    You can edit or delete the access control policy and rules as discussed in View and edit the system-created access control policy, on page 54.

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 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 rules.

Procedure

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

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

Step 3 Slide to **Enabled**.

Step 4 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 12.

Get required information for Identity Intelligence

Get the necessary credentials and configuration values from Identity Intelligence to enable integration with the dynamic firewall.

This task discusses how to create an API client, which provides all the get required information to set up Identity Intelligence in the dynamic firewall.

If you already have an API client and you know the values of all these parameters, you can skip this procedure and continue with Create a dynamic firewall instance, on page 47:

- **Client ID**
- **API URL**
- **Token URL**
- **Client Secret**

Before you begin

Integrating with the dynamic firewall requires you to create an *API client integration* in Identity Intelligence.

Among the values you must know about your API client integration is the client secret, which is displayed when you create the API client only. For that reason you might need to create the API integration first.

For more information about creating an API cilent integration, see Public API.

Follow these steps to get required information for Identity Intelligence:

Procedure

Step 1 Log in to your Identity Intelligence tenant.

Step 2 Click  (**Integrations**).

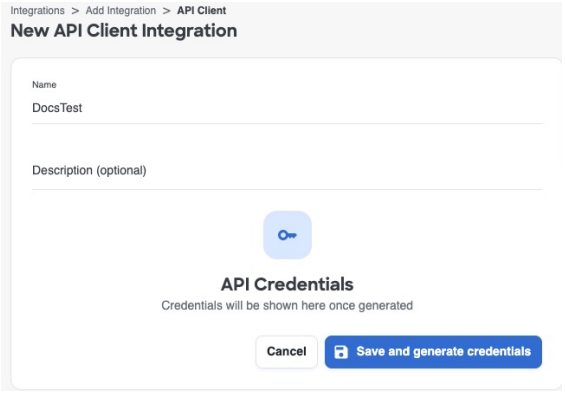
Step 3 Click **Add Integration**.

Step 4 On the next page, under API Clients, click **Add API Client**.

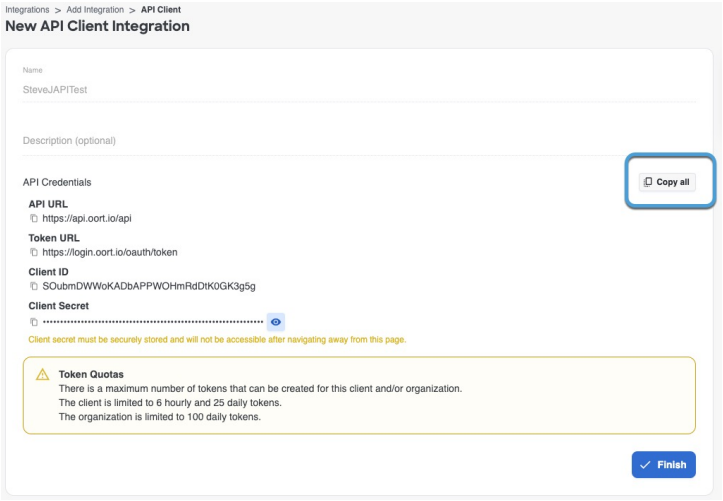
Step 5 Enter a **Name** and an optional **Description**.

Step 6 Click **Save and Generate Credentials**.

This figure shows an example.



Step 7 On the next page, click **Copy all** as this figure shows.



Step 8 Save the credentials for later use.

Step 9 Click **Finish**.

What to do next

See Create a dynamic firewall instance, on page 47.

Create an identity source and realm for the dynamic firewall

Before you configure the dynamic firewall, you must configure a supported identity realm and identity source.

Configure an identity realm

These identity realms are supported:

- Create an LDAP realm or an Active Directory realm and realm directory

Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

Configure an identity source

These identity sources are supported:

- On-premises Cisco ISE: Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Single or multiple Cisco ISE clusters:
  - Configuring a pxGrid Cloud identity source
  - Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)

Create a dynamic firewall instance

Create a new instance of the dynamic firewall to establish an association between an identity source and Identity Intelligence.

This task discusses how to create a new instance of the dynamic firewall, which is an association between an identity source and Identity Intelligence.

Before you begin

Complete all these steps:

- Enable the dynamic attributes connector as discussed in Enable the dynamic attributes connector, on page 3.
- Create an identity source:
  - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
  - Create a pxGrid Cloud identity source.

Follow these steps to create a dynamic firewall instance:

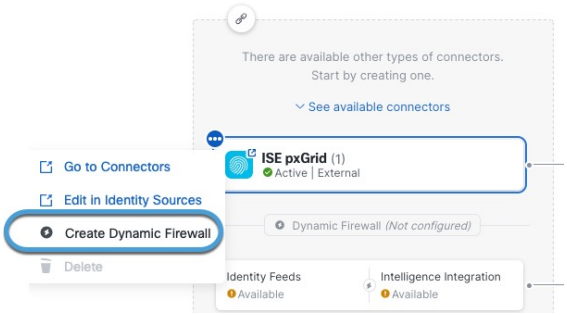
Procedure

Step 1 If you have not already done so, log in to the Secure Firewall Management Center.

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

Step 3 Click  next to the name of the identity source with which to add the dynamic firewall.

The following figure shows an example.



Note
If you do not see an identity source, create one before continuing:

- Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Configuring a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
- Configuring a pxGrid Cloud identity source

Step 4 Click **Create Dynamic Firewall**.

Step 5 Continue with Associate an identity source with Identity Intelligence, on page 48.

Associate an identity source with Identity Intelligence

Associate a supported identity source with Identity Intelligence to enable user and device trust ratings for dynamic firewall configuration.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device trust ratings to the .

For more information, see User Trust Level.

Before you begin

Before you begin, make sure you:

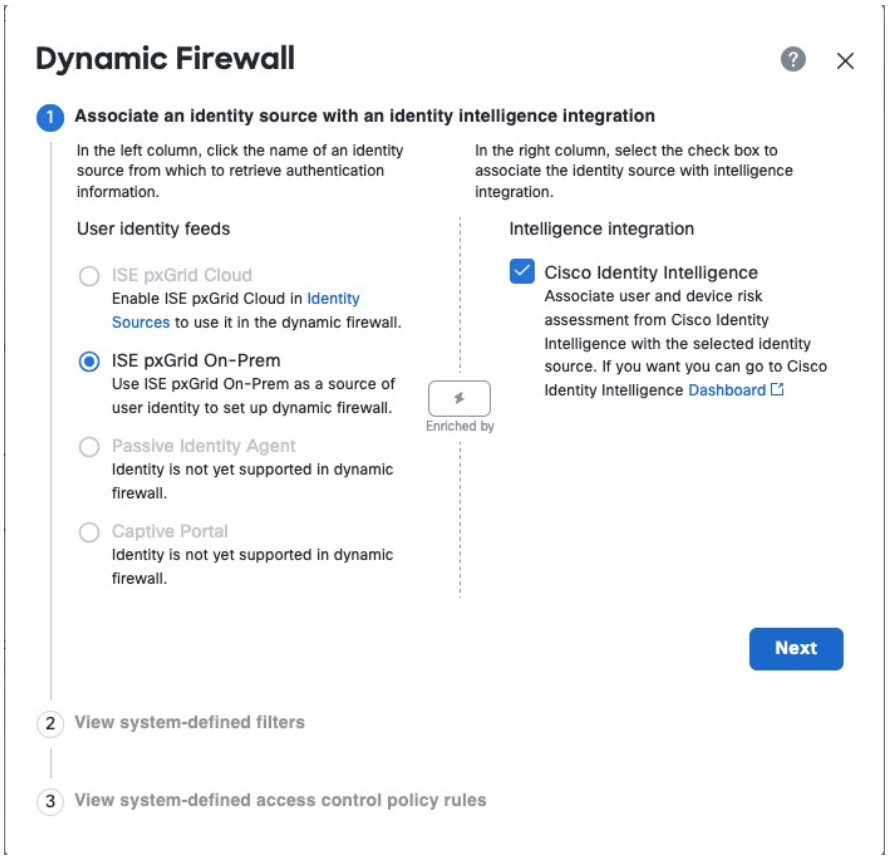
- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in Dynamic Firewall, on page 42.
- Completed the tasks discussed in Create a dynamic firewall instance, on page 47.

Procedure

Step 1 Start with Create a dynamic firewall instance, on page 47.

Step 2 On the next page, from the left column, click your identity source. Then, in the right column, select the **Cisco Identity Intelligence** check box to add user intelligence, including user and device risk.

The following figure shows an example.



Step 3 Click **Next**.

Step 4 Continue with Configure Identity Intelligence, on page 49.

Configure Identity Intelligence

This task enables integration between the dynamic firewall and Identity Intelligence.

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

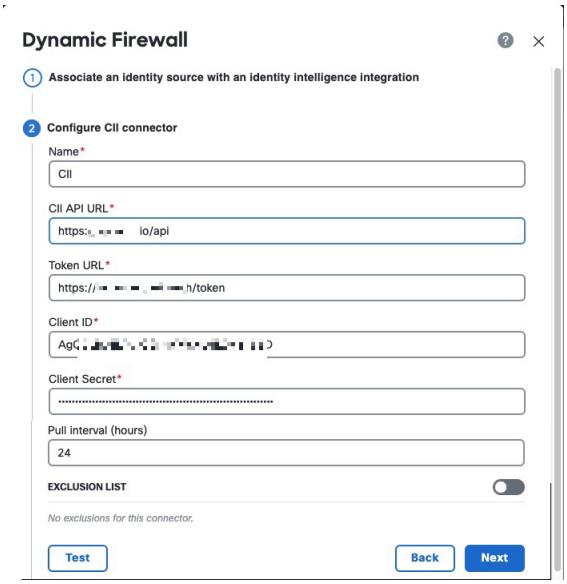
Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 48.

Procedure

Step 1 Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 48.

Step 2 If you selected the **Cisco Identity Intelligence** check box, enter the information you found for Identity Intelligence as described in Get required information for Identity Intelligence, on page 45.

The following figure shows an example.



Step 3 (Optional.) For Identity Intelligence to consider a specific set of users as trusted, slide **Exclusion List** to **Slider enabled** ( ).

Enter one user name per line in **username@domain.com** format. Users in this list are considered trusted by Identity Intelligence.

Step 4 Click **Test**.

Only if the test succeeds, continue with the next step.

If any errors are displayed, check all of your Identity Intelligence values and try again.

Step 5 Click **Next**.

Step 6 Continue with View system-defined filters, on page 50.

View system-defined filters

This task allows you to examine and understand the system-defined dynamic attributes filters that are automatically created during the configuration process.

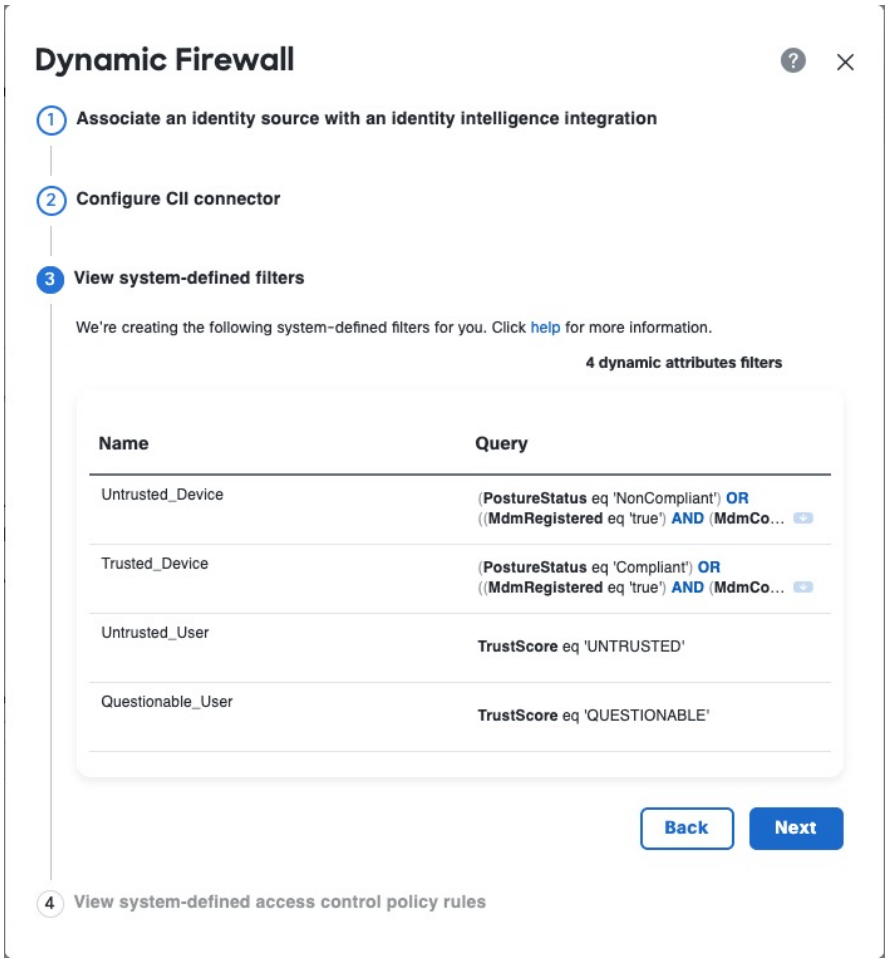
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the .

Before you begin

See Configure Identity Intelligence, on page 49.

Procedure

Step 1 The system displays a set of system-defined dynamic attributes filters, as shown in the following figure.



Step 2 View the system-created filters. Click on any row to expand the filter so you can view the filter and see its details.

Step 3 Click **Next**.

Step 4 Continue with View system-defined access control rules, on page 51.

View system-defined access control rules

This task allows you to review and decide whether to create system-defined access control rules for your dynamic firewall instance.

This task discusses access control rules created by the dynamic firewall.

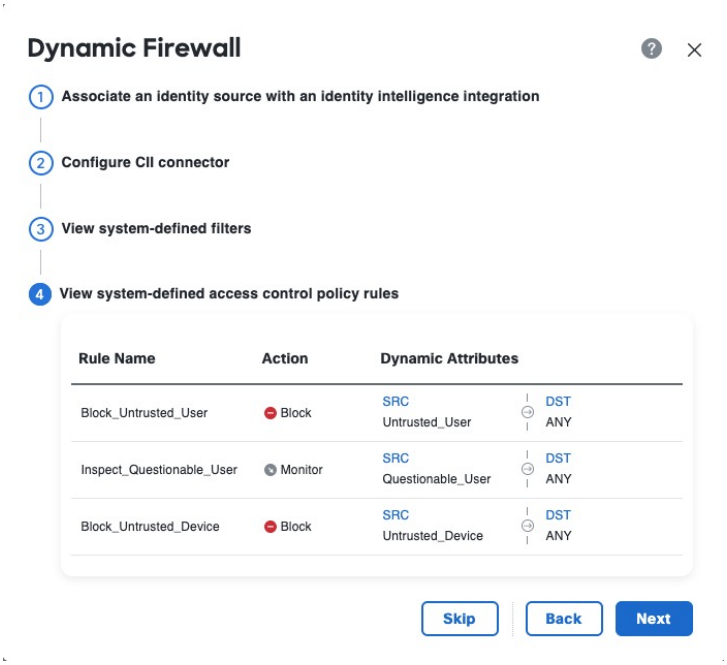
Before you begin

See View system-defined filters, on page 50.

Procedure

Step 1 View the system-created access control rules.

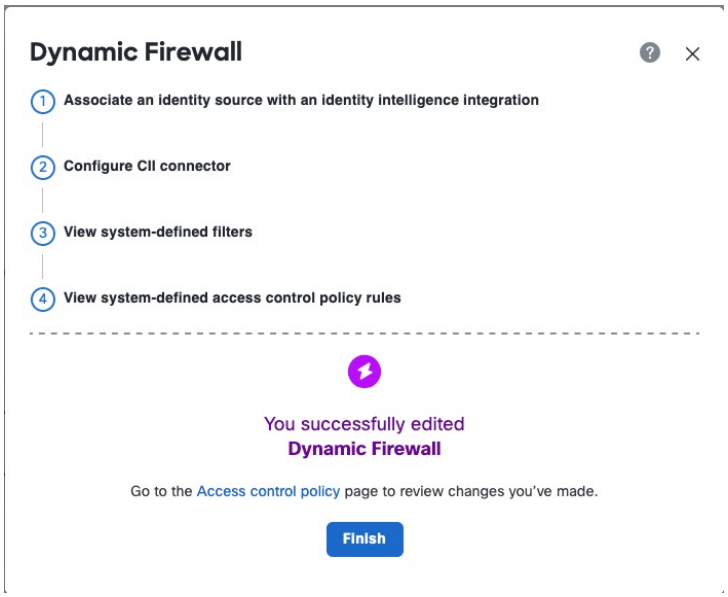
The following figure shows an example.



Step 2 Choose one of these options:

- Click **Skip** to skip creating these access control rules. You can create your own anytime.
- Click **Next** to create an access control policy named Dynamic Firewall Policy with the rules shown in the preceding figure.
- Click **Back** to return to system-created filters.

Step 3 After you click **Next**, if you created access control rules successfully, the following page is displayed:



Edit the user exclusion list

Specify users provided by Identity Intelligence as always being trusted.

You can instruct Identity Intelligence to treat specific users as trusted.

Before you begin

Configure the dynamic firewall as discussed in Create a dynamic firewall instance, on page 47.

Procedure

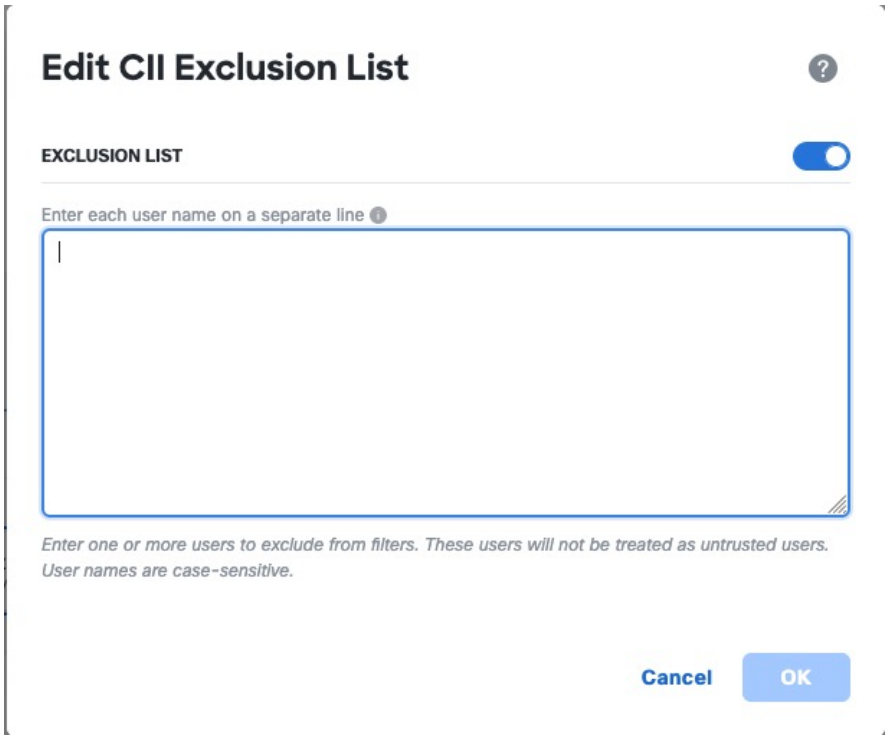
Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

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

Step 3 Click next to the name of the identity source.

Step 4 Click **Edit CII Exclusion List**.

The following dialog box is displayed.



Step 5 In the provided field, enter one user name in `username@domain.com` format on a line, press Enter, and enter another user name.

Each user name is considered as trusted by Identity Intelligence.

View and edit the system-created access control policy

Customize the system-created access control policy by adding devices, changing rules, reordering rules, or deleting rules to meet your specific network security requirements.

This topic discusses how you can edit the system-created access control rules and policy. Initially, the policy isn't associated with any devices but if you want to use it you can add devices, change rules, reorder rules, or delete rules.

Before you begin

Complete the tasks described in View system-defined access control rules, on page 51.

Follow these steps to view and edit the system-created access control policy:

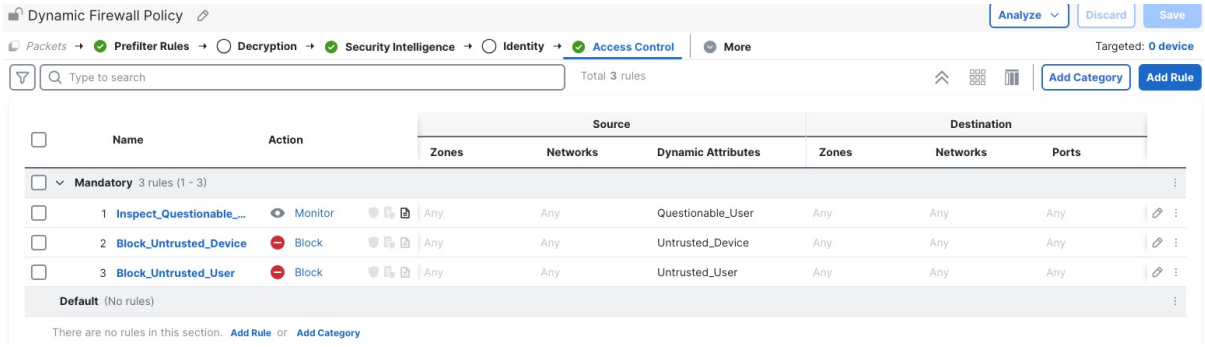
Procedure

Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

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

Step 3 Click **Edit** ( ) next to the policy named Dynamic Firewall Policy (or similar).

The following figure shows a sample access control policy.



Note that in this access control policy, only the rule set to monitor questionable users logs anything. To adjust the logging settings, see Logging settings for access control policies.

Step 4 Do any of the following:

- Target the access control policy at devices: Assign access control policy to devices.
- Edit the policy, including adding logging: Manage access control policies.
- Edit access control rules: Access control rule management.
- Set advanced policy options: Configure advanced settings for the access control policy.
- Associate other policies with this access control policy: Associate prefilter, decryption, and identity policies with an access control.

Create dynamic attributes filters

Create dynamic attributes filters that can be used as dynamic objects in access control policies to restrict access based on specific criteria such as group membership.

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, you could restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.

For more information about access control rules, see Create access control rules using dynamic attributes filters, on page 40.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

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

Step 3 Do any of the following:

- Add a new filter: click **Add** ( ).

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

Step 4 Enter the following information.

- **Name**: Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the Secure Firewall Management Center Object Manager (**External Attributes** > **Dynamic Object**).
- **Connector**: From the list, click the name of a connector to use.
- **Query**: Click Add .

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

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

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

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

What to do next

Verify the dynamic object in the Secure Firewall Management Center .

1. Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.
2. Click **Objects** > **Object Management** > **External Attributes** > **Dynamic Object**.

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

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 **Integration** > **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 **System** (⚙) > **Health** > **Monitor**.

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

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

Step 5 Click **Generate Troubleshooting Files**.

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

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 4: Dynamic Attributes Connector access requirements

URL	Reason
https://*fmc-ip***/api/fmc_platform/v1/auth/generatetoken**	Authentication
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id***/object/dynamicobjects**	GET and POST dynamic objects
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects/***object-id***/mappings?action=add**	Add mappings
https://*fmc-ip***/api/fmc_config/v1/domain/***domain-id*** /object/dynamicobjects/***object-id***/mappings?action=remove**	Remove mappings

Table 5: Dynamic Attributes Connector vCenter access requirements

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

Migration from DockerHub to Amazon ECR

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

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

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

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

Dynamic Attributes Connector Azure access requirements

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

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