Cisco Secure Dynamic Attributes Connector

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

- About the Cisco Secure Dynamic Attributes Connector, on page 1
- About the Dashboard, on page 5
- Create a Connector, on page 11
- Create an Adapter, on page 25
- Create Dynamic Attributes Filters, on page 26
- Use Dynamic Objects in Access Control Policies, on page 29
- Troubleshoot the Dynamic Attributes Connector, on page 30

About the Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in Secure Firewall Management Center (CDO) access control rules.

Supported connectors

We currently support:

Table 1: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS	Generic text	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Cloud-delivered (Cisco Defense Orchestrator)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

CSDAC version/platform	AWS	Generic text	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	vCenter	Webex	Zoom
Secure Firewall Management Center 7.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

More information about connectors:

- Amazon Web Services (AWS)

  For more information, see a resource like Tagging AWS resources on the Amazon documentation site.

  See Amazon Web Services Connector—About User Permissions and Imported Data, on page 12.

- GitHub

  For more information, see Create a GitHub Connector, on page 19.

- Google Cloud

  For more information, see Setting Up Your Environment in the Google Cloud documentation.

- Microsoft Azure

  For more information, see this page on the Azure documentation site.

  See Azure Connector—About User Permissions and Imported Data, on page 14.

- Microsoft Azure service tags

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

- Office 365 IP addresses

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

- Webex IP addresses

  For more information, see Create a Webex Connector, on page 23.

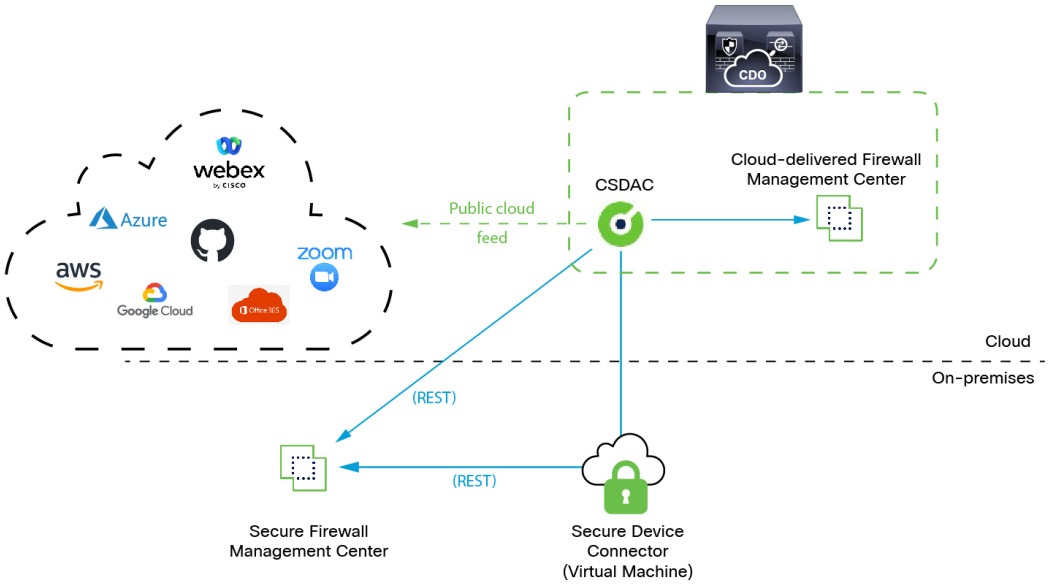
- Zoom IP addresses

  For more information, see Create a Zoom Connector, on page 24.

How It Works

Network constructs such as IP address are not reliable in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. 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.

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



- The system supports certain public cloud providers.

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

- The dynamic attributes connector is provided with CDO; it includes a Cloud-delivered Firewall Management Center and you can connect to an On-Prem Firewall Management Center using either the Secure Device Connector or SecureX.

  For more information about the Secure Device Connector, see Secure Device Connector (SDC).

  For more information about SecureX, see Onboard an On-Prem Firewall Management Center with SecureX.

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

  You can create the following types of adapters:

  - *On-Prem Firewall Management Center* for an on-premises device.

    This type of device might be managed by Cisco Defense Orchestrator (CDO) or it might be a standalone.

  - *Cloud-delivered Firewall Management Center* for devices managed by CDO.

History for the Cisco Secure Dynamic Attributes Connector

Feature	Minimum Management Center	Minimum Threat Defense	Details

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Secure Dynamic Attributes Connector	January 18, 2023	7.4.0	This feature is introduced. The Cisco Secure 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 Cisco Secure Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: Cisco Secure Dynamic Attributes Connector Configuration Guide New/modified screen: **Integration** > **Cisco Dynamic Attributes Connector**

History for the Cisco Secure Dynamic Attributes Connector

Feature	Min. Mgmt Center	Min. Secure Firewall Management Center	Details
Cisco Secure Dynamic Attributes Connector		7.4.0	Additional connectors are supported. For more information, see How It Works, on page 2.
	Any	7.3.0	This feature is introduced. The Cisco Secure 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 Cisco Secure Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: Cisco Secure Dynamic Attributes Connector Configuration Guide New/modified screen: **Integration** > **Cisco Dynamic Attributes Connector**

About the Dashboard

To access the Cisco Secure Dynamic Attributes Connector Dashboard, log in to the Secure Firewall Manager and click **Integration** > **Cisco Dynamic Attributes Connector** at the top of the page.

If the Cisco Secure Dynamic Attributes Connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

The Cisco Secure Dynamic Attributes Connector Dashboard page displays the status of your connectors, adapters, and filters at a glance. Following is an example of the Dashboard of an unconfigured system:

Among the things you can do with the Dashboard are:

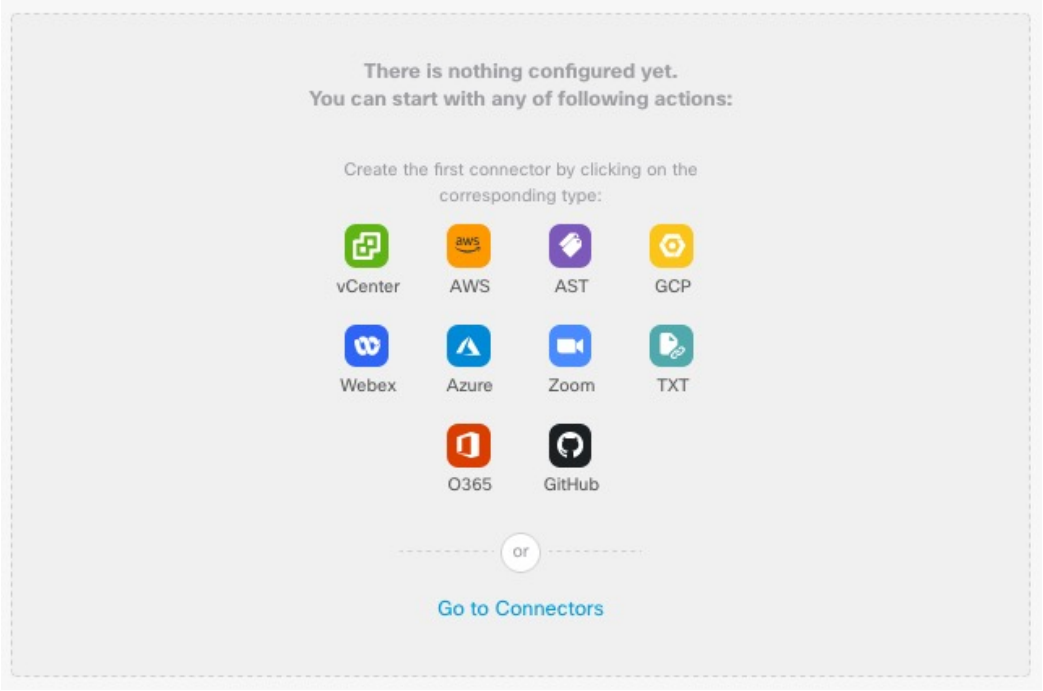
- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

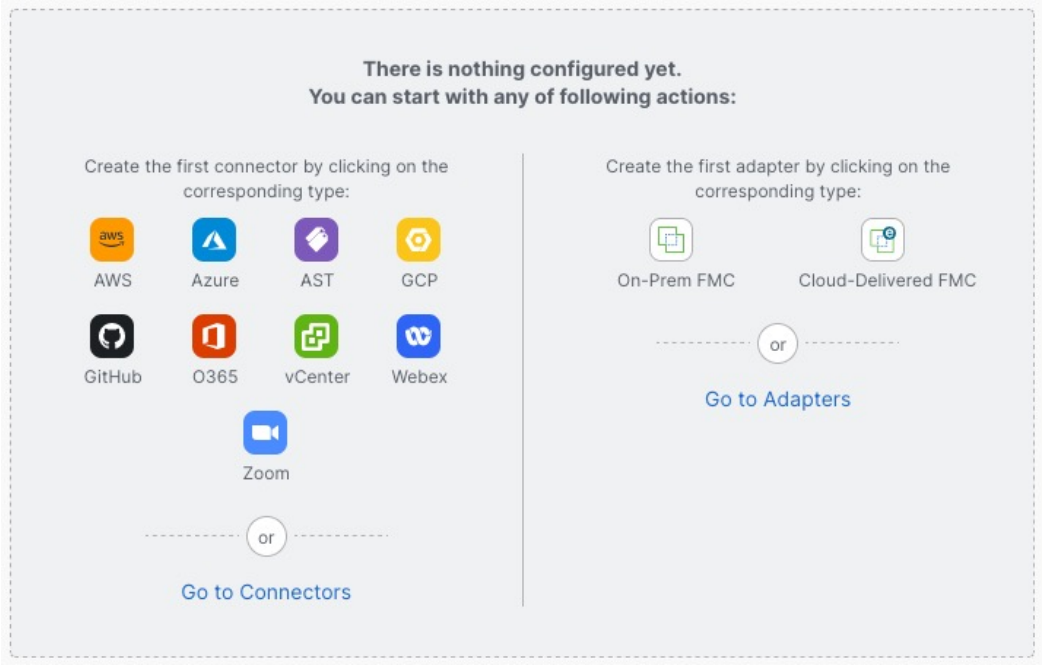
Related Topics

- Dashboard of an Unconfigured System, on page 5
- Dashboard of a Configured System, on page 7
- Add, Edit, or Delete Connectors, on page 8
- Add, Edit, or Delete Dynamic Attributes Filters, on page 10

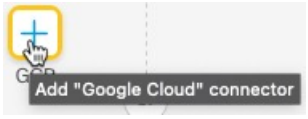
Dashboard of an Unconfigured System

Sample Cisco Secure Dynamic Attributes Connector Dashboard page of an unconfigured system:





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

- Hover the mouse pointer over a connector and click 

to create a new one.

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

  For more information, see Create a Connector, on page 11.

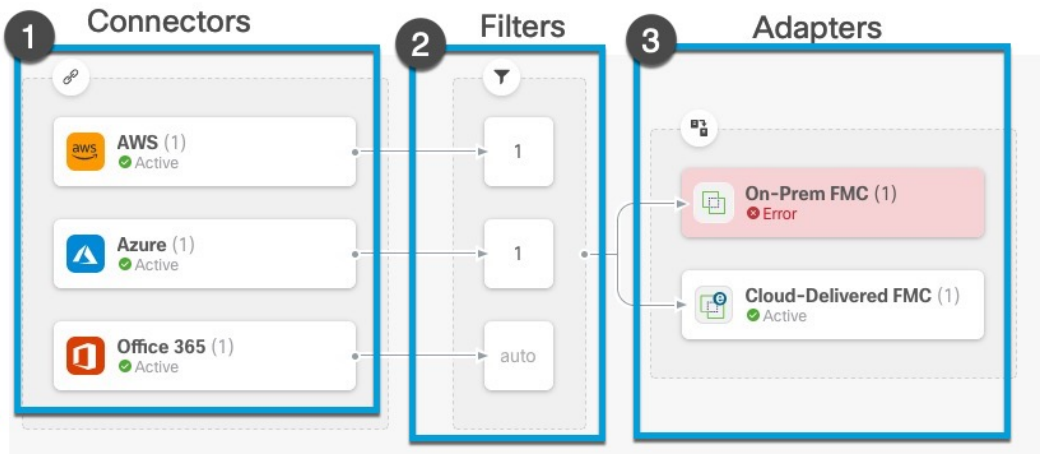
Related Topics:

- Dashboard of a Configured System, on page 7
- Add, Edit, or Delete Connectors, on page 8
- Add, Edit, or Delete Dynamic Attributes Filters, on page 10

Dashboard of a Configured System

Sample Cisco Secure Dynamic Attributes Connector Dashboard page of a configured system:

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



1 Create a Connector, on page 11
2 Create Dynamic Attributes Filters, on page 26
3 Create an Adapter, on page 25

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 8.	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.

Related Topics:

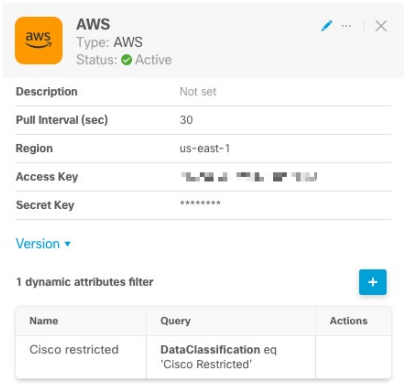
- Add, Edit, or Delete Connectors, on page 8
- Add, Edit, or Delete Dynamic Attributes Filters, on page 10

Add, Edit, or Delete Connectors

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

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

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

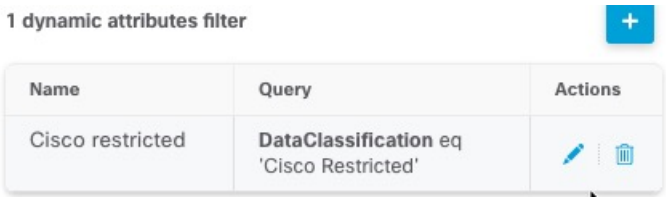


You have the following options:

- Click the Edit icon ( ) to edit this connector.
- Click the More icon ( ) for additional options.
- Click to close the panel.

- Click **Version** to display the version of the . You can optionally copy the version to the clipboard if necessary for Cisco TAC.

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



Click the Add icon ( ) to add a dynamic attributes filter for this connector. For more information, see Create Dynamic Attributes Filters, on page 26.

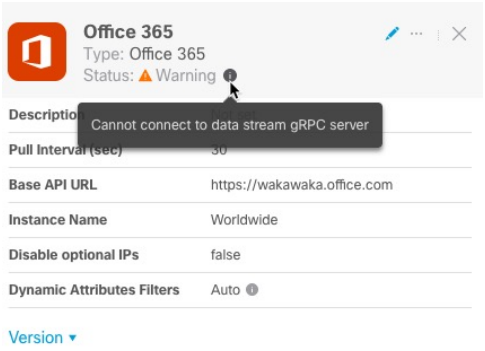
Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

View error information

To view error information for a connector:

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

   An example follows.



3. To resolve this issue, edit the connector settings as discussed in Create an Office 365 Connector, on page 22.
4. If you cannot resolve the issue, click **Version** and copy the version to a text file.
5. Get your CDO tenant ID as discussed in Get Your Tenant ID, on page 31
6. Provide all of this information to Cisco TAC.

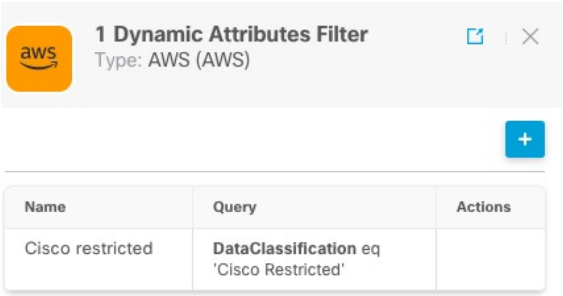
Add, Edit, or Delete Dynamic Attributes Filters

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

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

For more information about adding dynamic attributes filters, see Create Dynamic Attributes Filters, on page 26.

An example follows:



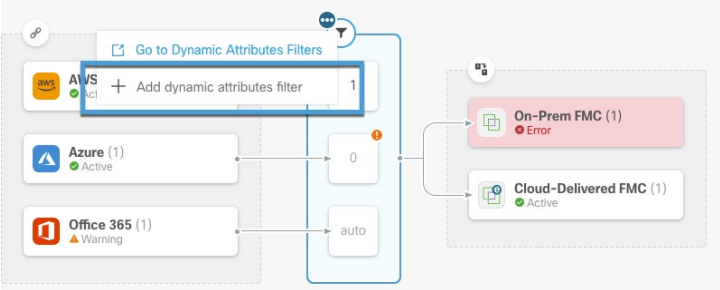
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have the following options:

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

  For more information, see Create Dynamic Attributes Filters, on page 26.
- Click in the filters column ( ) indicates the indicated connector has no associated dynamic attributes filters. Without associated filters, the connector can send nothing to management center.

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



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

Create a Connector

A *connector* is an interface with a cloud service. The connector retrieves network information from the cloud service so the network information can be used in access control policies on the CDO.

We support the following:

Table 2: List of supported connectors by Cisco Secure Dynamic Attributes Connector version and platform

CSDAC version/platform	AWS	Generic text	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	Cisco Multicloud Defense	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
Cloud-delivered (Cisco Defense Orchestrator)	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Secure Firewall Management Center 7.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

See one of the following sections for more information.

Amazon Web Services Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from AWS to CDO for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from AWS:

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

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

- *IP addresses* of virtual machines in AWS.

Minimum permissions required

The Cisco Secure 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 Cisco Secure Dynamic Attributes Connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to CDO. For a list of these attributes, see Amazon Web Services Connector—About 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.

Procedure

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

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

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

Step 4 Click **Add Users**.

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

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

Step 7 At the Set permissions page, click **Next** without granting the user access to anything; you'll do this later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

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

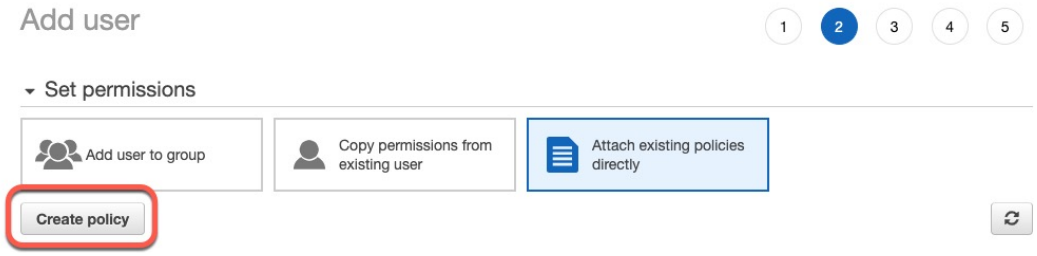
Note This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

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

Step 13 Click **Create Policy**.

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



Step 15 Enter the following policy in the field:

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

Step 16 Click **Next**.

Step 17 Click **Review**.

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

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

Step 20 Click the policy you just created.

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

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

Step 23 Click **Attach Policy**.

What to do next

Create an AWS Connector, on page 13.

Create an AWS Connector

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

Before you begin

Create a user with at least the privileges discussed in Create an AWS User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector, on page 12.

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS.
Region	(Required.) Enter your AWS region code.
Access Key	(Required.) Enter your access key.
Secret Key	(Required.) Enter your secret key.

Step 4 Click **Test** and make sure the test succeeds before you save the connector.

Step 5 Click **Save**.

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

Azure Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from Azure to CDO for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from Azure:

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

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

- *IP addresses* of virtual machines in Azure.

Minimum permissions required

The Cisco Secure 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 Cisco Secure Dynamic Attributes Connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to CDO. For a list of these attributes, see Azure Connector—About User Permissions and Imported Data, on page 14.

Before you begin

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

Procedure

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

Step 2 Click **Azure Active Directory**.

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

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

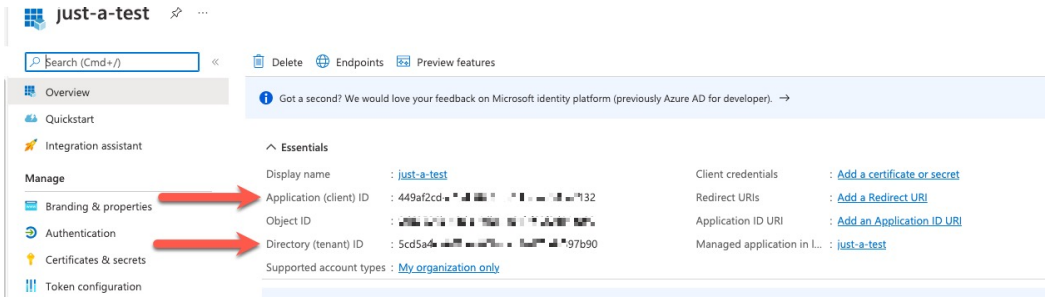
Step 5 In the **Name** field, enter a name to identify this application.

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

Step 7 Click **Register**.

Step 8 On the next page, make note of the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

A sample follows.

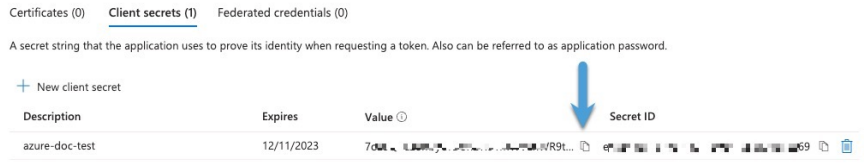


Step 9 Next to Client Credentials, click **Add a certificate or secret**.

Step 10 Click **New Client Secret**.

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

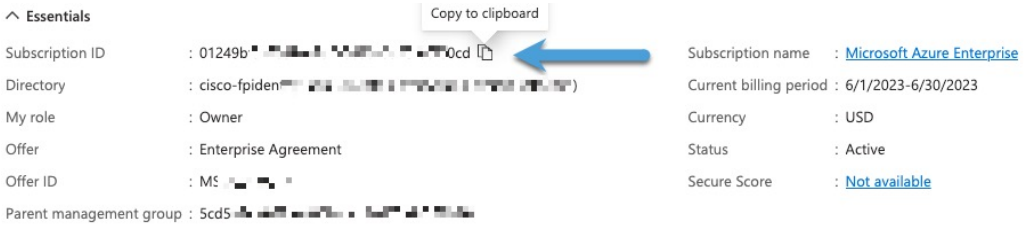
Step 12 Copy the value of the **Value** field to the clipboard. This value, *and not the* ***Secret ID***, is the client secret.



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

Step 14 Click the name of your subscription.

Step 15 Copy the subscription ID to the clipboard.



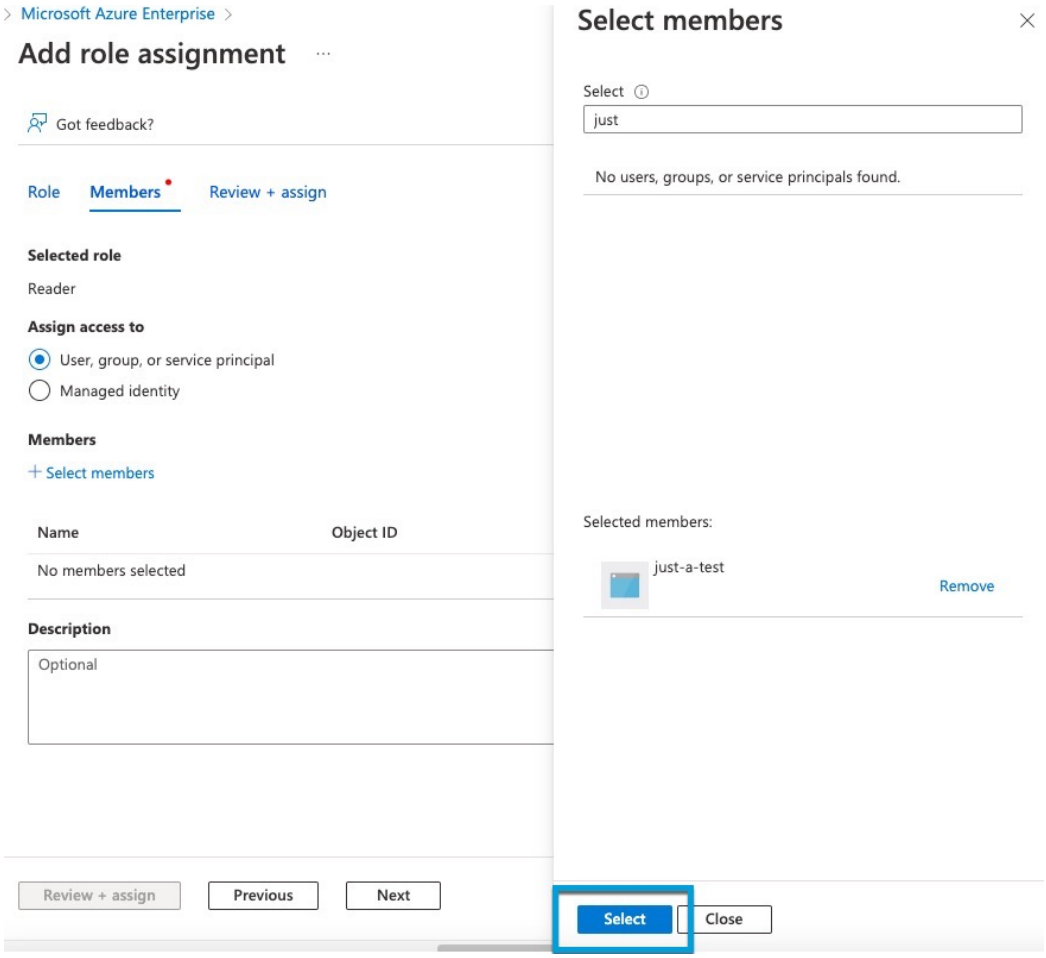
Step 16 Click **Access Control (IAM)**.

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

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

Step 19 Click **Select Members**.

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



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

What to do next

See Create an Azure Connector, on page 17.

Create an Azure Connector

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

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector, on page 15.

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 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.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

Step 4 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 5 Click **Save**.

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

Create an Azure Service Tags Connector

This topic discusses how to create a connector for Azure service tags to the CDO for use in access control 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 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

- Edit a connector: click Edit icon (Edit).
- Delete a connector: click Delete icon (Delete).

Step 3 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.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

Step 4 Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

Step 5 Click **Save**.

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

Create a GitHub Connector

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

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

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

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 Enter a **Name** and an optional description.

Step 4 (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).

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

Step 6 Click **Save**.

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

Google Cloud Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from Google Cloud to CDO for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from Google Cloud:

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

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

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

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

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

Minimum permissions required

The Cisco Secure 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 Cisco Secure Dynamic Attributes Connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to CDO. For a list of these attributes, see Google Cloud Connector—About User Permissions and Imported Data, on page 20.

Before you begin

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

Procedure

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

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

Step 3 Enter the following information:

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

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

Step 4 Click **Create and Continue**.

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

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

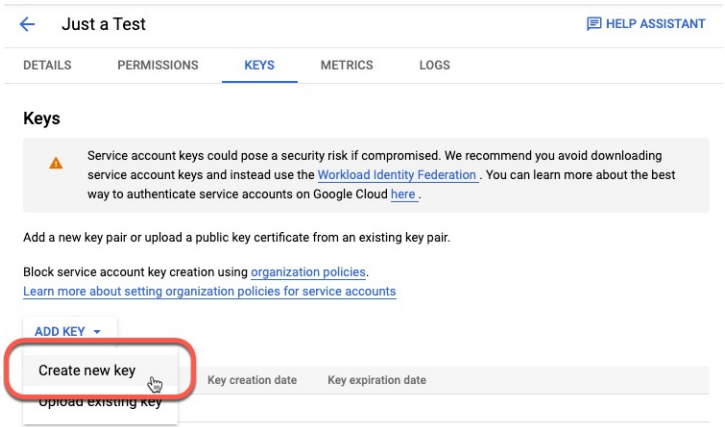
Step 7 Click **Done**.

A list of service accounts is displayed.

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

Step 9 Click **Manage Keys**.

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



Step 11 Click **JSON**.

Step 12 Click **Create**.

The JSON key is downloaded to your computer.

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

What to do next

See Create a Google Cloud Connector, on page 21.

Create a Google Cloud Connector

Before you begin

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

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 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.
GCP region	(Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation.
Service account	Paste the JSON code for your Google Cloud service account.

Step 4 Click **Test** and make sure the test succeeds before you save the connector.

Step 5 Click **Save**.

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

Create an Office 365 Connector

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

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

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

- Delete a connector: click Delete icon (Delete).

Step 3 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.
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 4 Click **Test** and make sure the test succeeds before you save the connector.

Step 5 Click **Save**.

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

Create a Webex Connector

This section discusses how to create a Webex connector that sends data to the CDOfor use in access control 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 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 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.
Provider Reserved IPs	(Required.) (Required.) Slide to enabled to retrieve any reserved IP addresses.

Step 4 Click **Test** and make sure the test succeeds before you save the connector.

Step 5 Click **Save**.

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

Create a Zoom Connector

This section discusses how to create a Zoom connector that sends data to the CDOfor use in access control 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 Click **Tools & Services** > **Dynamic Attributes Connector** > **Connectors**.

Step 2 Do any of the following:

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

Step 3 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Zoom.
Provider Reserved IPs	(Required.) Slide to enabled to retrieve any reserved IP addresses.

Step 4 Click **Test** and make sure the test succeeds before you save the connector.

Step 5 Click **Save**.

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

Create an Adapter

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

You can create the following adapters:

- *On-Prem Firewall Management Center* for an on-premises Management Center device.
- *Cloud-delivered Firewall Management Center* for devices managed by CDO.

Note You must have a **Super Admin** user role to create the first Cloud-delivered Firewall Management Center adapter. To view or modify existing adapters, you must have an Admin or Super Admin user role.

How to Create an On-Prem Firewall Management Center Adapter

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

Before you begin

Onboard the firewall manager to Cisco Defense Orchestrator as discussed in *Onboard a Management Center* in the *Managing Security and Network Devices with Cisco Defense Orchestrator* online help.

Required User Role:

- Super Admin

Procedure

Step 1 Log in to CDO.

Step 2 Click **Tools & Services** > **Dynamic Attributes Connector** > **Adapters**.

Step 3 To add an adapter, click Add icon ( ) > On-Prem Firewall Management Center.

Step 4 To edit or delete an adapter, click Edit icon (Edit), or Delete icon (Delete).

Step 5 Add or edit the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Primary Device	From the list, click the IP address of a management center associated with your tenant.

Value	Description
Secondary Device	(Optional.) If you have a secondary On-Prem Firewall Management Center, click its name from the list.

Step 6 Click **OK**.

How to Create a Cloud-delivered Firewall Management Center Adapter

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

Before you begin

Required User Role:

- Super Admin

Procedure

Step 1 Log in to CDO as a user with the Super Admin role.

Step 2 Click **Tools & Services** > **Dynamic Attributes Connector** > **Adapters**.

Step 3 To add an adapter, click Add icon ( ) > Cloud-delivered Firewall Management Center.

Step 4 To edit or delete an adapter, click Edit icon (Edit), or Delete icon (Delete).

Step 5 Edit the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Cloud FMC URL	From the list, click the URL for your Cloud-delivered Firewall Management Center.

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

Step 7 Click **Save**.

Create Dynamic Attributes Filters

Dynamic attributes filters that you define using the Cisco Secure Dynamic Attributes Connector are exposed in the CDO 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.

Note You cannot create dynamic attributes filters for GitHub, Office 365, Azure Service Tags. 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 29.

Before you begin

Create a Connector, on page 11

Procedure

Step 1 Click **Tools & Services** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 2 Click **Dynamic Attributes Filters**.

Step 3 Do any of the following:

- Add a new filter: click Add icon ( )
- Edit a filter: click Edit icon (Edit)
- Delete a filter: click Delete icon (Delete)

Step 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the CDO Object Manager (**External Attributes** > **Dynamic Object**).
Connector	From the list, click the name of a connector to use.
Query	• Add a new filter: click Add icon ( ) • Edit a filter: click Edit icon (Edit) • Delete a filter: click Delete icon (Delete)

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

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

Item	Description
	• **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

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

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

Step 8 (Optional.) Verify the dynamic object in the CDO.

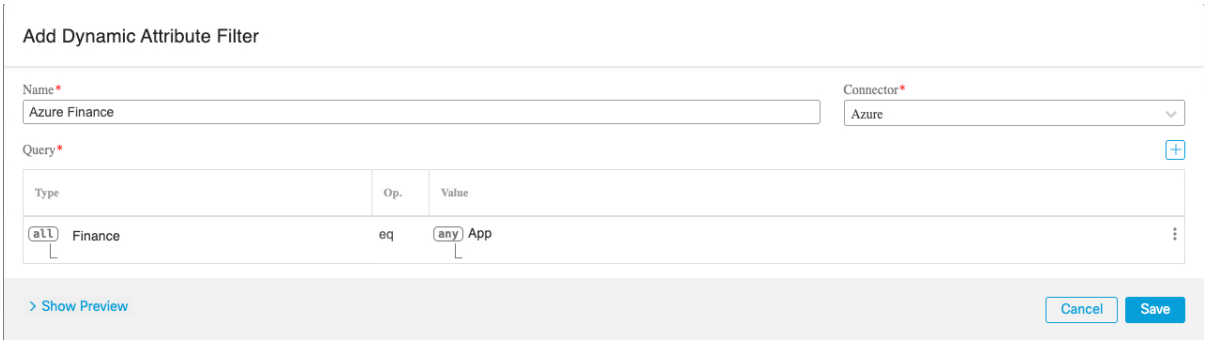
a) Log in to the CDO.
b) Click **Policies** > **FTD Policies**.
c) Click **Objects** > **Object Management**.
d) In the left pane, click **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

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

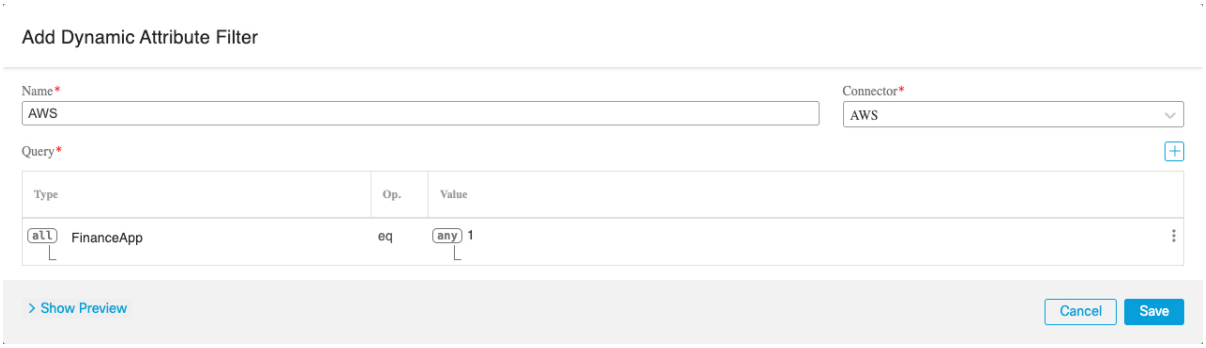
Example: Azure

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



Example: AWS

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



Use Dynamic Objects in Access Control Policies

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

About Dynamic Objects in Access Control Rules

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

You can use these dynamic objects on the access control rule's Dynamic Attributes tab page, similarly to the way you used Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes; for example, in an access control block rule, you can add a Finance dynamic object as a destination attribute to block access to Finance servers by whatever objects match the other criteria in the rule.

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

Create Access Control Rules Using Dynamic Attributes Filters

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

Before you begin

Create dynamic attributes filters as discussed in Create Dynamic Attributes Filters, on page 26.

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

Procedure

Step 1 Log in to CDO.

Step 2 Click **Policies** > **FTD Policies**.

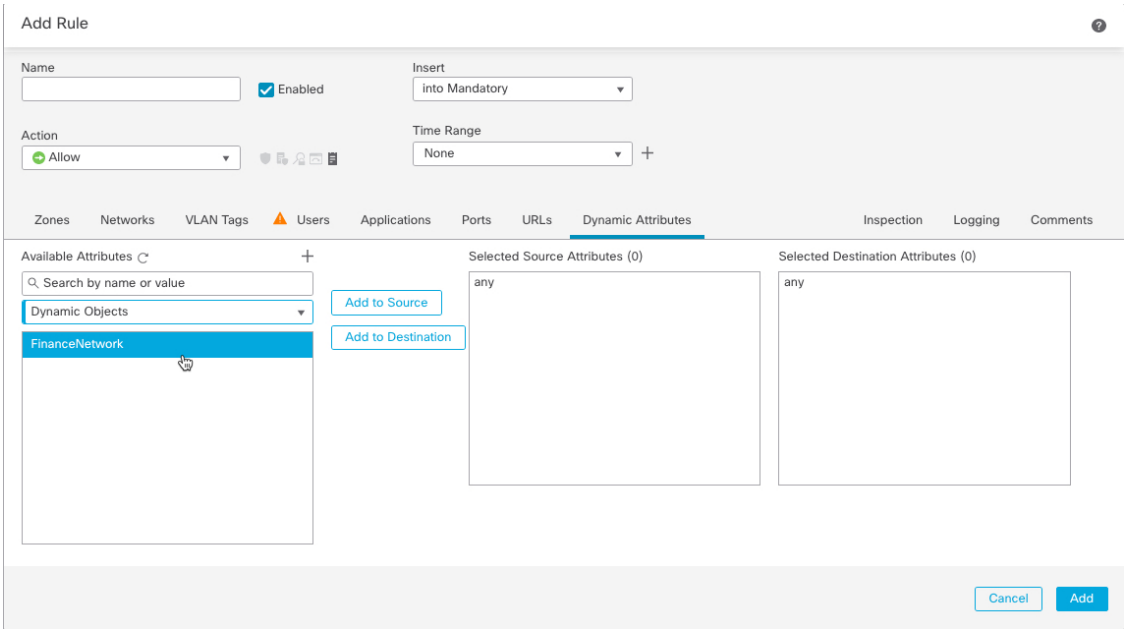
Step 3 Click **Edit** (✎) next to an access control policy.

Step 4 Click **Add Rule**.

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

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

The following figure shows an example.



The preceding example shows a dynamic object named `FinanceNetwork` that corresponds to the dynamic attribute filter created in the Cisco Secure Dynamic Attributes Connector.

Step 7 Add the desired object to source or destination attributes.

Step 8 Add other conditions to the rule if desired.

What to do next

Access Control chapter in the *Cisco Secure Firewall Management Center Device Configuration Guide* (link to chapter)

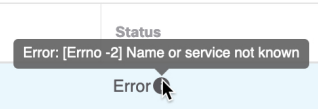
Troubleshoot the Dynamic Attributes Connector

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

Troubleshoot Error Messages

Problem: Name or service not known error

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

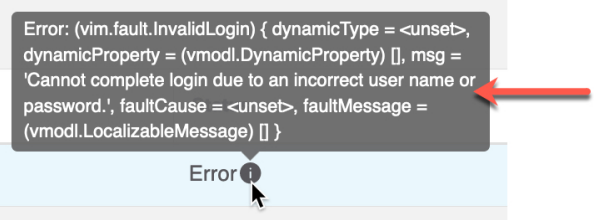


Solution: Edit the connector and check for:

- A trailing slash on a host name
- Verify the password is correct

Problem: Incorrect username or password

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



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

Get Your Tenant ID

If you require assistance with the Cisco Secure Dynamic Attributes Connector, you must provide your tenant ID to Cisco TAC so we can look at your logs.

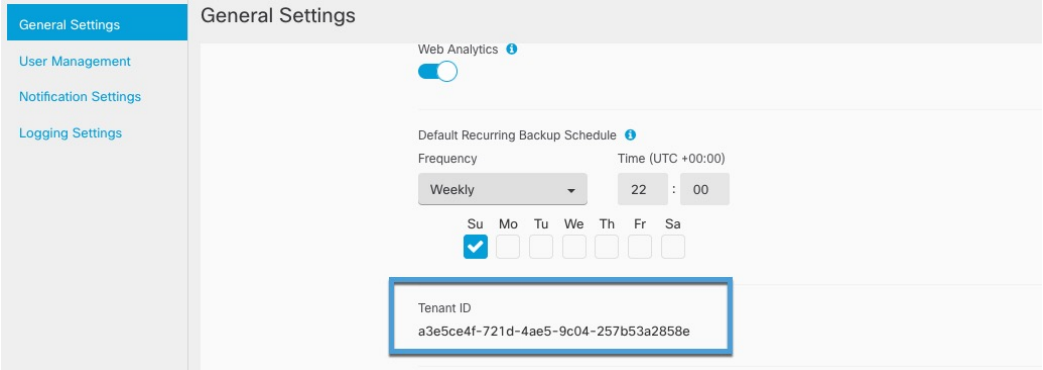
Procedure

Step 1 Log in to CDO.

Step 2 Click **Settings** > **General Settings**.

Step 3 Copy your tenant ID to the clipboard to provide to Cisco TAC.

A sample follows.


General Settings
User Management
Notification Settings
Logging Settings
General Settings
Web Analytics
Default Recurring Backup Schedule
Frequency
Time (UTC +00:00)
Weekly
22
:
00
Su Mo Tu We Th Fr Sa
Tenant ID
a3e5ce4f-721d-4ae5-9c04-257b53a2858e