



Configure the Cisco Secure Dynamic Attributes Connector

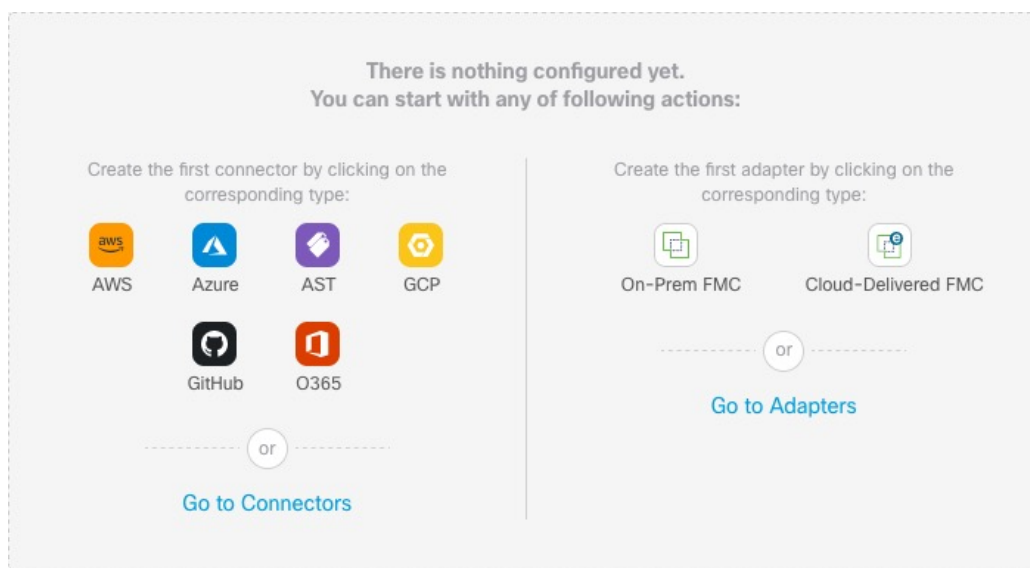
See the following topics for more information:

- [About the Dashboard, on page 1](#)
- [Create a Connector, on page 9](#)
- [Create an Adapter, on page 20](#)
- [Create Dynamic Attributes Filters, on page 22](#)

About the Dashboard

To access the Cisco Secure Dynamic Attributes Connector Dashboard, log in to CDO and click **Tools & Services > Dynamic Attributes Connector > Dashboard** at the top of the page.

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:

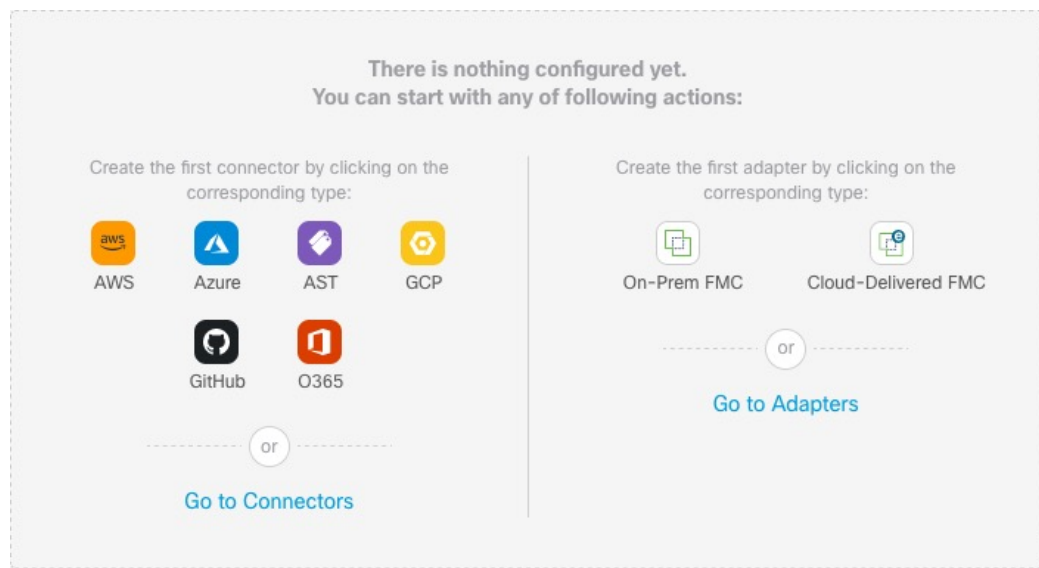
- Add, edit, and delete connectors, dynamic attributes filters, and adapters.
- See how connectors, dynamic attributes filters, and adapters are related to each other.
- View warnings and errors.

Related Topics


- [Dashboard of an Unconfigured System, on page 2](#)
- [Dashboard of a Configured System, on page 3](#)
- [Add, Edit, or Delete Connectors, on page 4](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 6](#)
- [Add, Edit, or Delete Adapters, on page 7](#)

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 and adapters you can configure for your system. You can do any of the following:

- Hover the mouse pointer over a connector or adapter 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 9](#).

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

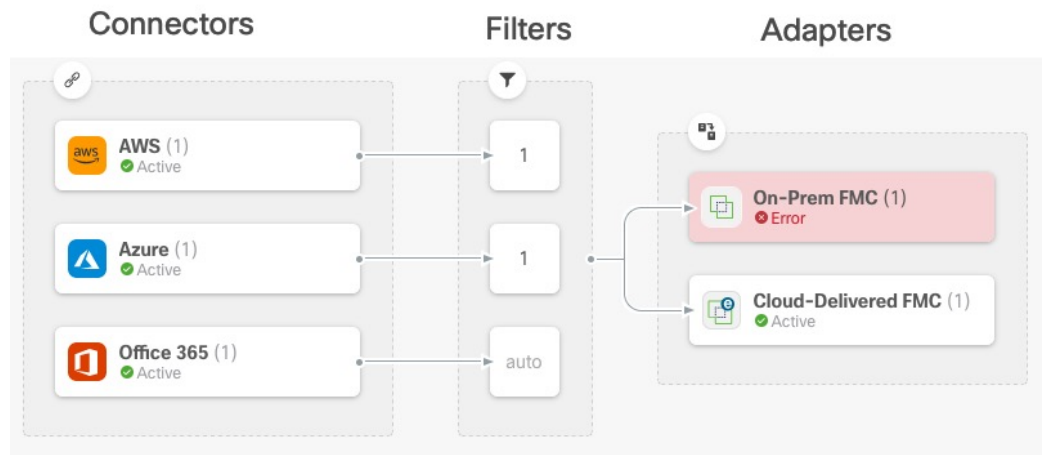
For more information, see [Create an Adapter, on page 20](#).

Related Topics:




- [Dashboard of a Configured System, on page 3](#)
- [Add, Edit, or Delete Connectors, on page 4](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 6](#)
- [Add, Edit, or Delete Adapters, on page 7](#)

Dashboard of a Configured System


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




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

Connectors column	Filters column	Adapters column
<p>List of connectors with a number indicating how many of each type are configured. Connectors collect dynamic attributes that could be sent to the configured adapter. Dynamic attributes filters specify what data is sent.</p> <p>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 4.</p>	<p>List of dynamic attributes filters associated with each connector with a number indicating how many of each filter are associated with a connector.</p> <p>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 6.</p>	<p>List of adapters. Adapters receive dynamic objects from configured connectors using configured dynamic attributes filters; these dynamic objects can be used in access control policies without the need to deploy them.</p> <p>Click  to view more information about all configured adapters. You can also click the name of an adapter to add, edit, or delete adapters; or to view detailed information about them. For more information, see Add, Edit, or Delete Adapters, on page 7.</p>



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 4](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 6](#)
- [Add, Edit, or Delete Adapters, on page 7](#)


Add, Edit, or Delete Connectors

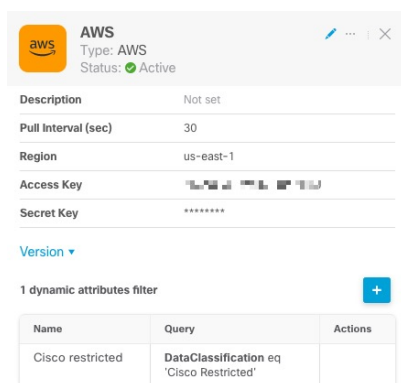
The Dashboard enables you to view or edit connectors. You can click the name of a connector to view all



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:



AWS
Type: AWS
Status: Active

Description: Not set

Pull Interval (sec): 30

Region: us-east-1

Access Key: [Redacted]

Secret Key: [Redacted]

Version ▾

+ 1 dynamic attributes filter

Name	Query	Actions
Cisco restricted	DataClassification eq 'Cisco Restricted'	

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 dynamic attributes connector. 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 delete connectors. A sample follows:

+ 1 dynamic attributes filter

Name	Query	Actions
Cisco restricted	DataClassification eq 'Cisco Restricted'	✎ 🗑

Click the Add icon (+) to add a dynamic attributes filter for this connector. For more information, see [Create Dynamic Attributes Filters, on page 22](#).

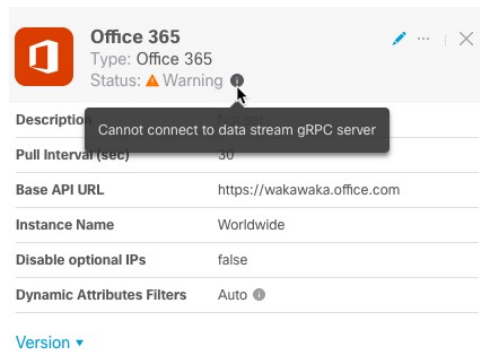
Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

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** (i).


An example follows.



3. To resolve this issue, edit the connector settings as discussed in [Create an Office 365 Connector, on page 19](#).
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](#)
6. Provide all of this information to [Cisco TAC](#).

Add, Edit, or Delete Dynamic Attributes Filters

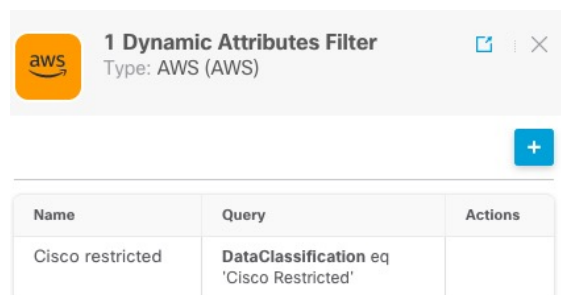
The Dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter

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 22](#).


Click any adapter in the filters column () to display more information about it; 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.

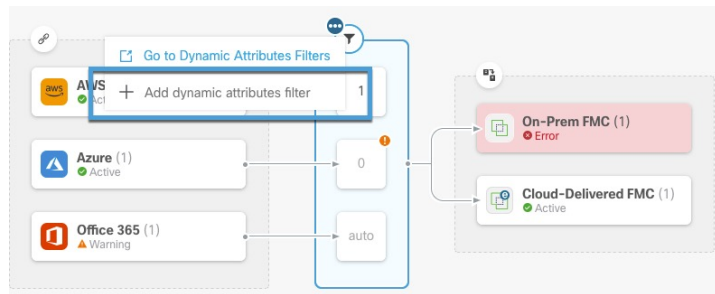
You have the following options:



- 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 22](#).

- 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.

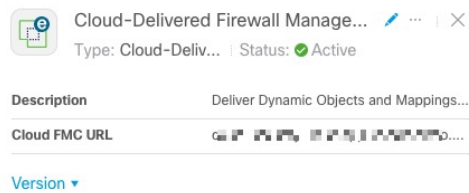
Add, Edit, or Delete Adapters

The Dashboard enables you to view or edit adapters. You can click the name of an adapter to view all instances


of that adapter or you can click  for the following additional options:

- **Go to Adapters** to view all adapters at the same time; you can add, edit, and delete adapters from there.
- **Add Adapter > type** to add an adapter of the indicated type.

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



You have the following options:

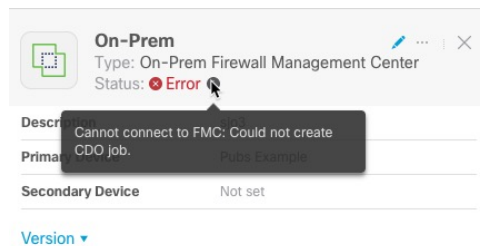
- Click the Edit icon (✎) to edit this connector.
- Click the More icon (⋮) for additional options.
- Click **Version** to display the version of the dynamic attributes connector. You can optionally copy the version to the clipboard if necessary for [Cisco TAC](#).
- Click  to add, edit, or delete adapters. You can also view error details on the resulting page.
- Click ✕ to close the panel.

View error information

To view error information for an adapter:

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

An example follows.



3. To resolve this error, make sure the On-Prem Firewall Management Center is onboarded correctly. For more information, see Onboard an FMC in *Managing FMC with Cisco Defense Orchestrator* ([link to topic](#)).
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](#)
6. Provide all of this information to [Cisco TAC](#).

Related Topics

- [Create an Adapter, on page 20](#)

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

CSDAC version/platform	AWS	Decorator	GitHub	Google Cloud	Azure	Azure Service Tags	ISE	LDAP	Microsoft Office 365	VMware vCenter
Version 1.1 (on-premises)	Yes	No	No	No	Yes	Yes	No	No	Yes	Yes
Version 2.0 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Cloud-delivered (Cisco Defense Orchestrator)	Yes	No	Yes	Yes	Yes	Yes	No	No	Yes	No

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` 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 9](#).

Before you begin

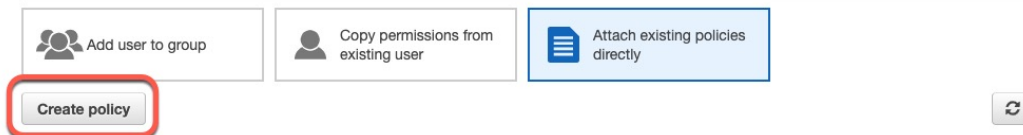
You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see [this article](#) in the AWS documentation.

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**.

Add user

▼ Set permissions



- Step 15** Enter the following policy in the field:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeTags",
        "ec2:DescribeInstances"
      ],
      "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 11.](#)




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 9.](#)

Procedure

- Step 1** Log in to CDO.
- Step 2** Click **Tools & Services > 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 a connector: click Edit icon ( Edit).
 - Delete a connector: click Delete icon ( Delete).
- Step 4** Enter the following information.

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

Value	Description
Secret Key	(Required.) Enter your secret key.

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

Step 6 Click **Save**.

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

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 12](#).

Before you begin

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

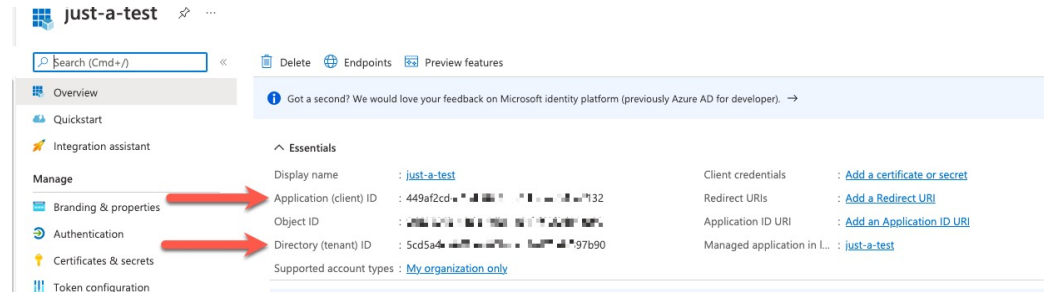
Procedure

-
- 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 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 client **Value** to the clipboard because you'll need it to set up the Azure connector.

Description	Expires	Value	Secret ID	Copy to clipboard
Sample only	10/15/2022	r_Wk...S9wMK...	8fa75b1	

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

Step 14 Copy the subscription ID to the clipboard.

Step 15 On the subscriptions page, click the name of the subscription.

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**.

> Microsoft Azure Enterprise >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role
Reader

Assign access to
☒ User, group, or service principal
☐ Managed identity

Members
+ Select members

Name	Object ID
No members selected	

Description
Optional

Review + assign Previous Next

Select members

Select ①
just

No users, groups, or service principals found.

Selected members:

just-a-test	Remove
-------------	--------

Select Close

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

What to do next

See [Create an Azure Connector, on page 14](#).

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 12](#).

Procedure

Step 1 Log in to CDO.

Step 2 Click **Tools & Services > 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 a connector: click Edit icon (✎ Edit).
- Delete a connector: click Delete icon (🗑 Delete).

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

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

Step 6 Click **Save**.

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

Create an Azure Service Tags Connector

This topic discusses how to create a connector for Azure service tags to the CDO for use in access control policies. The IP addresses association 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 CDO.

Step 2 Click **Tools & Services > 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 a connector: click Edit icon (✎ Edit).

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

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

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

Step 6 Click **Save**.

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

Create 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 Log in to CDO.

Step 2 Click **Tools & Services > 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 a connector: click Edit icon ( Edit).
- Delete a connector: click Delete icon ( Delete).

- Step 4** Enter a **Name** and an optional description.
- Step 5** (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).
- Step 6** Click **Test** and make sure the test succeeds before you save the connector.
- Step 7** Click **Save**.
- Step 8** Make sure **Ok** is displayed in the Status column.
-

Google Cloud Connector—About User Permissions and Imported Data

The 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 17](#).

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.

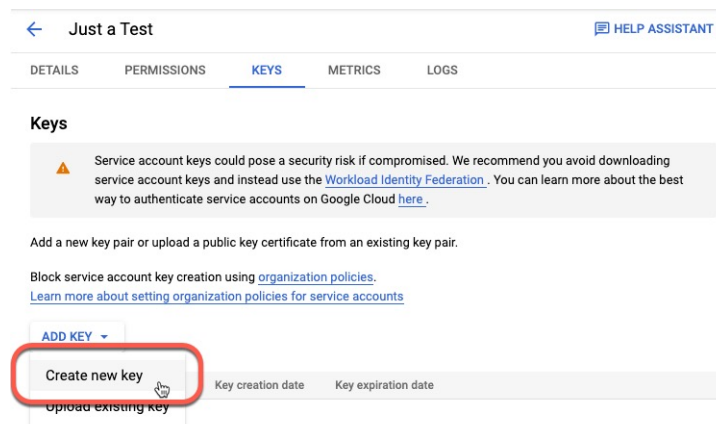
Step 7 Click **Done**.

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 18](#).

Create a Google Cloud Connector

Before you begin

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

Procedure


- Step 1** Log in to CDO.
- Step 2** Click **Tools & Services > 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 a connector: click Edit icon ( Edit).
 - Delete a connector: click Delete icon ( Delete).
- 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. |
| GCP region | (Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation. |
| Service account | Paste the JSON code for your Google Cloud service account. |
- Step 5** Click **Test** and make sure the test succeeds before you save the connector.
- Step 6** Click **Save**.
- Step 7** Make sure **Ok** is displayed in the Status column.



Create an Office 365 Connector

This task discusses how to create a connector for Office 365 tags to send data to the 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** Log in to CDO.
- Step 2** Click **Tools & Services > 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 a connector: click Edit icon ( Edit).
- Delete a connector: click Delete icon ( Delete).

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.
Base API URL	(Required.) Enter the URL from which to retrieve Office 365 information, if it's different from the default. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Instance name	(Required.) From the list, click an instance name. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Disable optional IPs	(Required.) Enter true or false .

Step 5 Click **Save**.

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

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 (), or Delete icon ().
- 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.
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, or 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](#).

Before you begin

Complete all of the following tasks:




- [Create a Connector, on page 9](#)

Procedure




Step 1 Log in to CDO.

Step 2 Click **Tools & Services > Dynamic Attributes Connector > 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Equals to exactly match the key to the value. • Contains to match the key to the value if any part of the value matches.
Values	Click either Any or All and click one or more values from the list. Click Add another value to add values to your query.

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

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

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

- Log in to the CDO.
- Click **Policies > FTD Policies**.
- Click **Objects > Object Manager**.
- 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.

Add Dynamic Attribute Filter

Name* Connector*

Query* +

Type	Op.	Value
all Finance	eq	any App

[> Show Preview](#) Cancel Save

Example: AWS

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

Add Dynamic Attribute Filter

Name* Connector*

Query* +

Type	Op.	Value
all FinanceApp	eq	any 1

[> Show Preview](#) Cancel Save