Configure the Cisco Secure Dynamic Attributes Connector

Install the dynamic attributes connector and configure connectors, dynamic attributes filters, and adapters to provide management center with dynamic network data that can be used in access control rules.

The dynamic attributes connector enables you to configure connectors to provide the management center with dynamic network data that can be used in access control rules.

See the following topics for more information:

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 management center.

We support the following:

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

CSDAC version/platform	AWS	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	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 the management center 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 the management center. For a list of these attributes, see Amazon Web Services Connector—About User Permissions and Imported Data, on page 2.

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.

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.

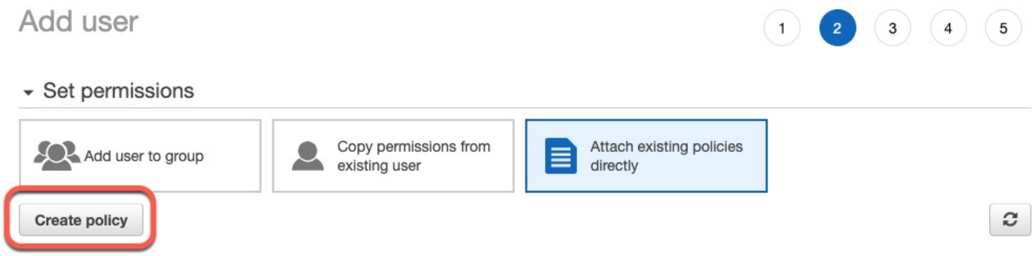
Note This is the only opportunity you have to retrieve the user's key.

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
1
2
3
4
5
Set permissions
Add user to group
Copy permissions from existing user
Attach existing policies directly
Create policy

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 3.

Create an AWS Connector

This task discusses how to configure a connector that sends data from AWS to the management center 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 2.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

Step 5 Click **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 the management center 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 the management center. For a list of these attributes, see Azure Connector—About User Permissions and Imported Data, on page 4.

Before you begin

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

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**.

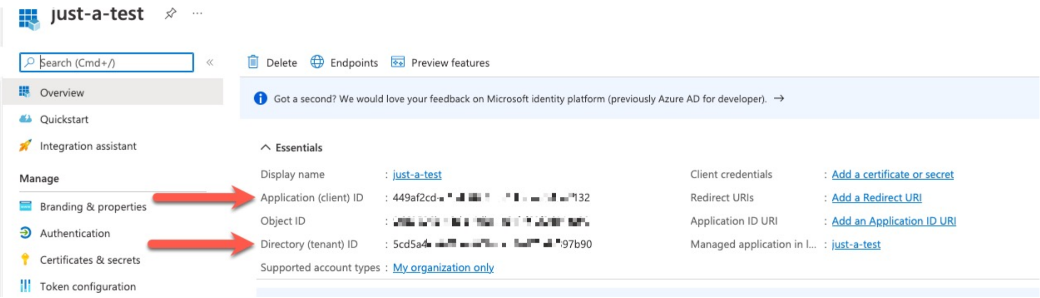
Step 5 In the **Name** field, enter a name to identify this application.

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.



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

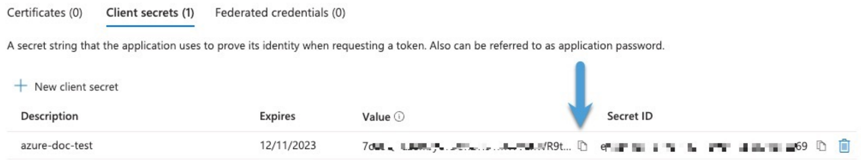
Display name : just-a-test
Application (client) ID : 449af2cd-[redacted]132
Object ID : [redacted]
Directory (tenant) ID : 5cd5a4[redacted]97b90
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : just-a-test

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.



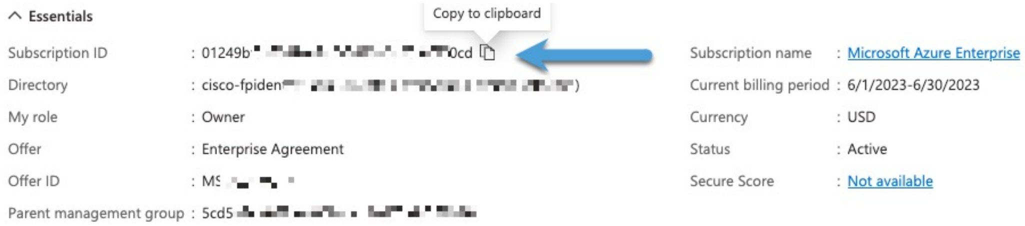
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
azure-doc-test	12/11/2023	7d[redacted]/R9t...	e[redacted]69

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.



Subscription ID	: 01249b[redacted]0cd	Subscription name	: Microsoft Azure Enterprise
Directory	: cisco-fpiden[redacted])	Current billing period	: 6/1/2023-6/30/2023
My role	: Owner	Currency	: USD
Offer	: Enterprise Agreement	Status	: Active
Offer ID	: MS[redacted]	Secure Score	: Not available
Parent management group	: 5cd5[redacted]		

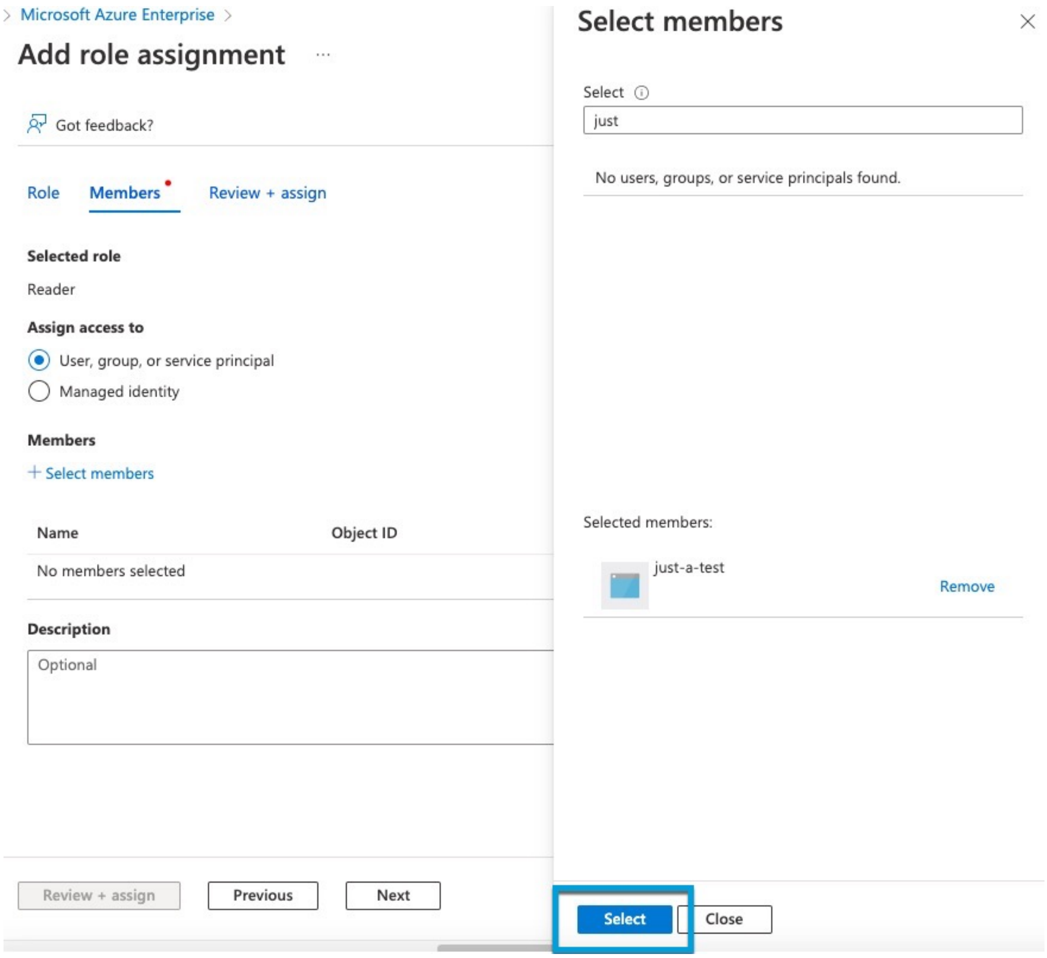
Step 16 Click **Access Control (IAM)**.

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**.



Selected role
Reader

Assign access to
● User, group, or service principal
○ Managed identity

Members
+ Select members

Name	Object ID
No members selected	

Description
Optional

Select members

Select
just

No users, groups, or service principals found.

Selected members:
just-a-test Remove

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

What to do next

See Create an Azure Connector, on page 7.

Create an Azure Connector

This task discusses how to create a connector to send data from Azure to management center 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 5.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **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.
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 management center 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.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **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.
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 management center 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.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

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

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

Step 5 (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).

Step 6 Click **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 the management center 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 the management center. For a list of these attributes, see Google Cloud Connector—About User Permissions and Imported Data, on page 9.

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.

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.

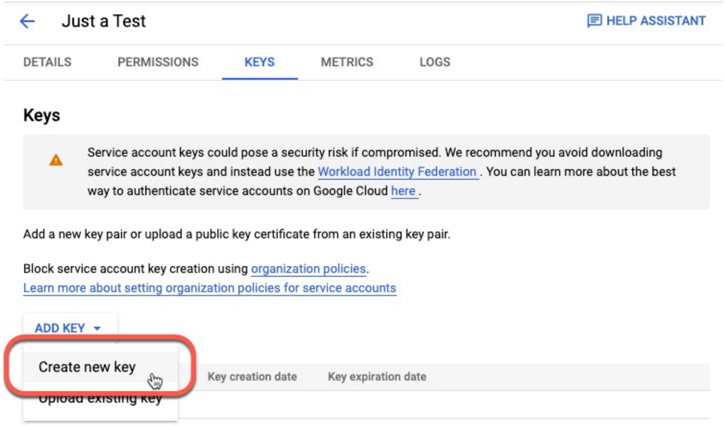
Step 7 Click **Done**.

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**.



Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation . You can learn more about the best way to authenticate service accounts on Google Cloud here .

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

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 10.

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.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **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.
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 management center 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.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **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.
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 **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.

vCenter Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from vCenter to the management center for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from vCenter:

- *Operating system*
- *MAC address*
- *IP addresses*
- *NSX tags*

Minimum permissions required

The Cisco Secure Dynamic Attributes Connector requires a user at minimum with the **Read Only** permission to be able to import dynamic attributes.

Create a vCenter Connector

This task discusses how to create a connector for VMware vCenter to send data to the management center for use in access control policies.

Before you begin

If you use non-trusted certificates to communicate with vCenter, see Manually Get a Certificate Authority (CA) Chain, on page 20.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

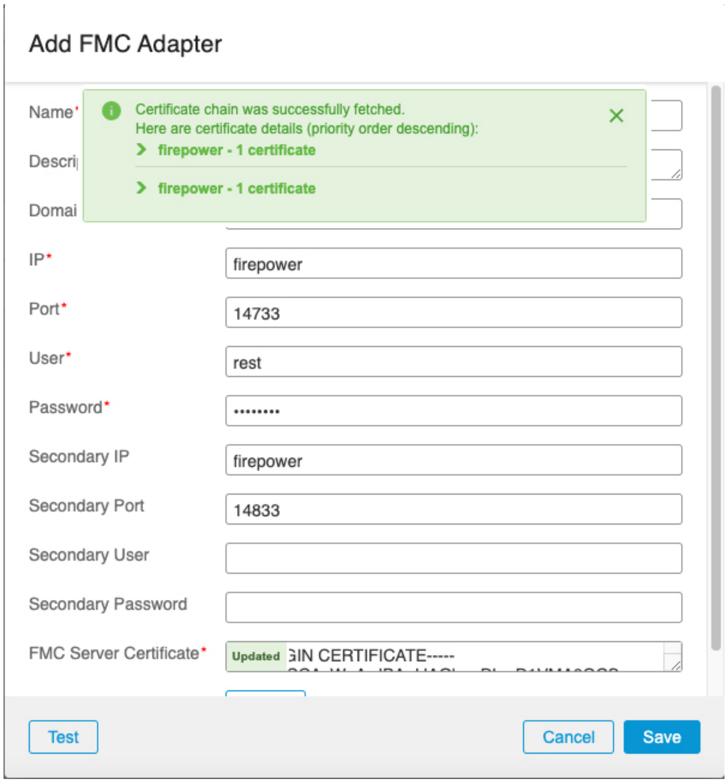
Step 3 Do any of the following:

- 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.
Host	(Required.) Enter any of the following: • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port *Do not* enter a scheme (such as **`https://`**) or trailing slash. For example, **`myvcenter.example.com`** or **`192.0.2.100:9090`**
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.
NSX Password	Enter the NSX user's password.
vCenter Certificate	You have the following options: • 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 20. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:

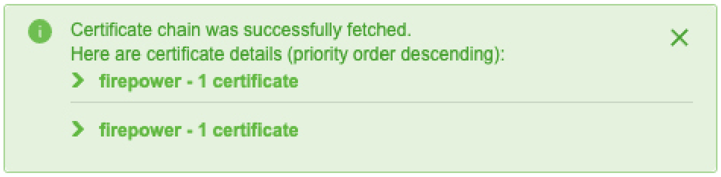


Add FMC Adapter

Certificate chain was successfully fetched.
Here are certificate details (priority order descending):
> firepower - 1 certificate
> firepower - 1 certificate

Name*	
Descri	
Domai	
IP*	firepower
Port*	14733
User*	rest
Password*	••••••••
Secondary IP	firepower
Secondary Port	14833
Secondary User	
Secondary Password	
FMC Server Certificate*	Updated GIN CERTIFICATE-----

Expanding the certificate CA chain at the top of the dialog box displays the certificates similar to the following.



Certificate chain was successfully fetched.
Here are certificate details (priority order descending):
> firepower - 1 certificate
> firepower - 1 certificate

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 20.

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

Step 6 Click **Save**.

What to do next

Create an Adapter, on page 14

Create an Adapter

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

First you can optionally fetch the certificate authority chain, which is required to securely connect to the management center.

Fetching the certificate authority chain requires only the management center host name; creating the adapter requires a user name, password, and other information.

Create a Secure Firewall Management Center User for the Dynamic Attributes Connector

We recommend you create a dedicated management center user for the dynamic attributes connector adapter. Creating a dedicated management center user avoids issues like unexpected logouts from the management center because the dynamic attributes connector periodically logs in using a REST API to update the management center with new and updated dynamic objects.

The management center user must have Access Admin privileges at least.

Step 1 Log in to the management center if you haven't already done so.

Step 2 Click **System** (⚙) > **Users**.

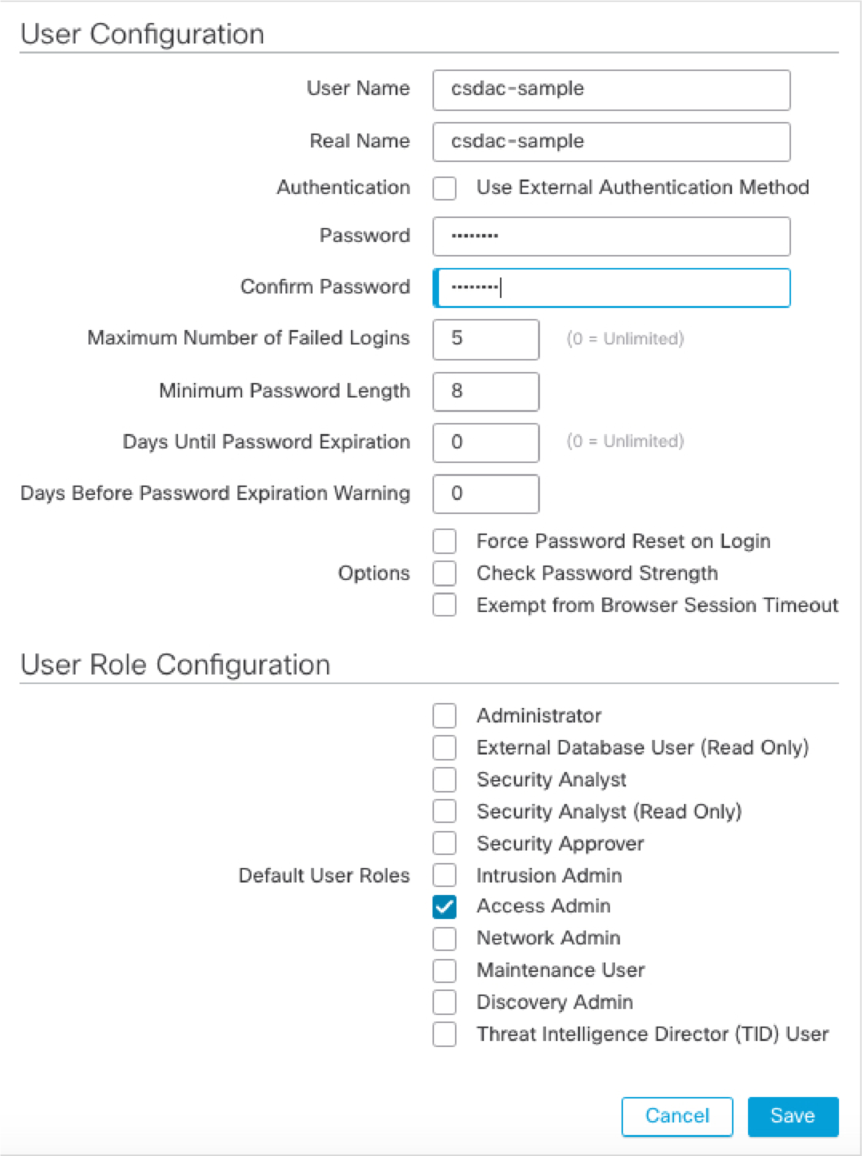
Step 3 Click **Create User**.

Step 4 Enter the information required to create the user.

Step 5 Under User Role Configuration, check any of the following default roles or a custom role with the same privilege level:

- **Administrator**
- **Access Admin**
- **Network Admin**

The following figure shows an example.



User Configuration

User Name: csdac-sample

Real Name: csdac-sample

Authentication: □ Use External Authentication Method

Password: ••••••••

Confirm Password: ••••••••

Maximum Number of Failed Logins: 5 (0 = Unlimited)

Minimum Password Length: 8

Days Until Password Expiration: 0 (0 = Unlimited)

Days Before Password Expiration Warning: 0

Options:
- □ Force Password Reset on Login
- □ Check Password Strength
- □ Exempt from Browser Session Timeout

User Role Configuration

Default User Roles:
- □ Administrator
- □ External Database User (Read Only)
- □ Security Analyst
- □ Security Analyst (Read Only)
- □ Security Approver
- □ Intrusion Admin
- ☑ Access Admin
- □ Network Admin
- □ Maintenance User
- □ Discovery Admin
- □ Threat Intelligence Director (TID) User

You can also choose a custom role with sufficient privileges to allow REST actions or a different default role with sufficient privileges. For more information about default roles, see the User Roles section in the chapter on user accounts.

What to do next

Create an Adapter, on page 14

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 the management center.

Before you begin

See Create a Secure Firewall Management Center User for the Dynamic Attributes Connector, on page 15.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Adapters**.

Step 3 Do any of the following:

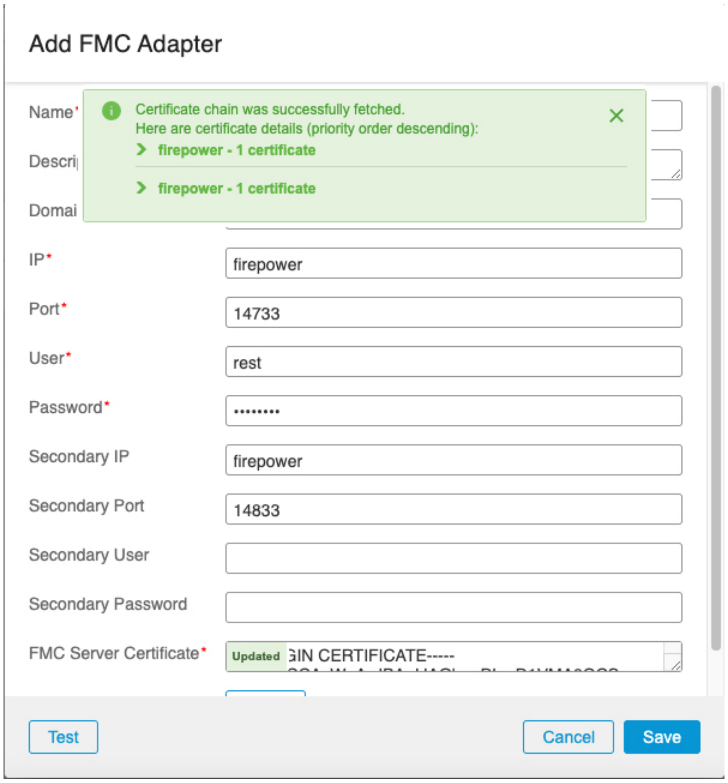
- Add a new connector: click Add icon (+), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Domain	Enter the Secure Firewall Management Center Virtual domain in which to create dynamic objects. Leave the field blank to create dynamic objects in the Global domain. For example, **`Global/MySubdomain`**
IP	(Required.) Enter your Secure Firewall Management Center Virtual's host name or IP address. The host name or IP you enter must exactly match the Common Name of the CA certificate used to securely connect to it.
Port	(Required.) Enter the TLS port used by your Secure Firewall Management Center Virtual.
User	(Required.) Enter the name of an Secure Firewall Management Center Virtual user with the Network Admin role at minimum.
Password	(Required.) Enter the user's password.
Secondary IP	(High availability only.) Enter the secondary Secure Firewall Management Center Virtuals host name or IP address. The host name or IP you enter must exactly match the Common Name of the CA certificate used to securely connect to it.
Secondary Port	(High availability only.) Enter the TLS port used by your secondary Secure Firewall Management Center Virtual.
Secondary User	(High availability only.) Enter the name of a secondary Secure Firewall Management Center Virtual user with the Network Admin role at minimum.
Secondary Password	(High availability only.) Enter the user's password.

Value	Description
Server Certificate	You have the following options: • Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 20. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:



Add FMC Adapter

Certificate chain was successfully fetched.
Here are certificate details (priority order descending):
> firepower - 1 certificate
> firepower - 1 certificate

Name*

Descri

Domai

IP* firepower

Port* 14733

User* rest

Password* ••••••••

Secondary IP firepower

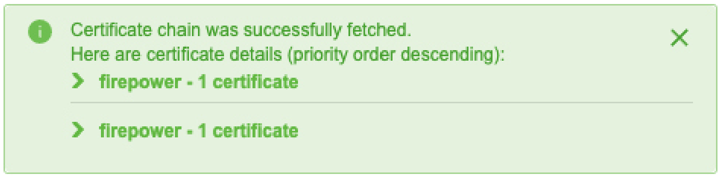
Secondary Port 14833

Secondary User

Secondary Password

FMC Server Certificate* Updated GIN CERTIFICATE-----

Expanding the certificate CA chain at the top of the dialog box displays the certificates similar to the following.



Certificate chain was successfully fetched.
Here are certificate details (priority order descending):
> firepower - 1 certificate
> firepower - 1 certificate

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 20.

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

Step 6 Click **Save**.

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 a managed management center on the Cisco Defense Orchestrator.

Before you can create a Cloud-delivered Firewall Management Center, get the following information first: Get Your Base URL and API Token, on page 19.

Get Your Base URL and API Token

This task dicusses how to get the URL and API token from CDO that are required to create a Cloud-delivered Firewall Management Center adapter.

Before you begin

You must be a CDO Super Admin to complete the tasks discussed in this section.

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

Step 2 In the upper right corner of the page, click **Settings**.

Step 3 Click **General Settings**.

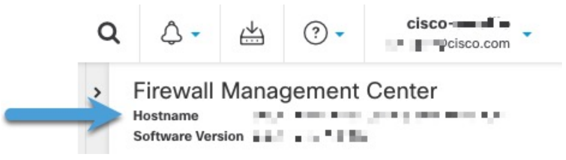
Step 4 Next to API Token, click **Refresh**.

Step 5 Copy the API token to a text file for later use.

Step 6 Click **Tools & Services** > **Firewall Management Center**.

Step 7 Click the name of the management center to which to send dynamic attributes connector data.

Step 8 The value of **Hostname**, preceded by **https://**, is the base URL.
An example follows:



Firewall Management Center
Hostname [redacted]
Software Version [redacted]

What to do next

How to Create a Cloud-delivered Firewall Management Center Adapter, on page 19.

How to Create a Cloud-delivered Firewall Management Center Adapter

This task discusses how to create a Cloud-delivered Firewall Management Center adpater that sends data from the dynamic attributes connector to a device managed by CDO.

Before you begin

You must get the management center base URL and API token from CDO before you can complete this task. For more information, see Get Your Base URL and API Token, on page 19.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Adapters**.

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 unique name to identify this adapter.
Description	Optional description of the adapter.
Base Url	(Required.) Use the Base URL you found in Get Your Base URL and API Token, on page 19.
API Token	(Required.) Use the API token you found in Get Your Base URL and API Token, on page 19.

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

Step 6 Click **Save**.

What to do next

Create Dynamic Attributes Filters, on page 23.

Manually Get a Certificate Authority (CA) Chain

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

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

You must use one of these procedures to connect to the following:

- vCenter or NSX

  It is not necessary to get a certificate chain for connecting to Azure or AWS.
- Management Center

Before you use this procedure, see the section on automatically fetching the certificate authority chain in:

- Create a vCenter Connector, on page 12

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.

2. Enter the following command.

   ```
   security verify-cert -P url[:port]
   ```

   where url is the URL (including scheme) to vCenter or Management Center. For example:

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

   If you access vCenter or the management center using NAT or PAT, you can add a port as follows:

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

3. Save the entire certificate chain to a plaintext file.

   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.

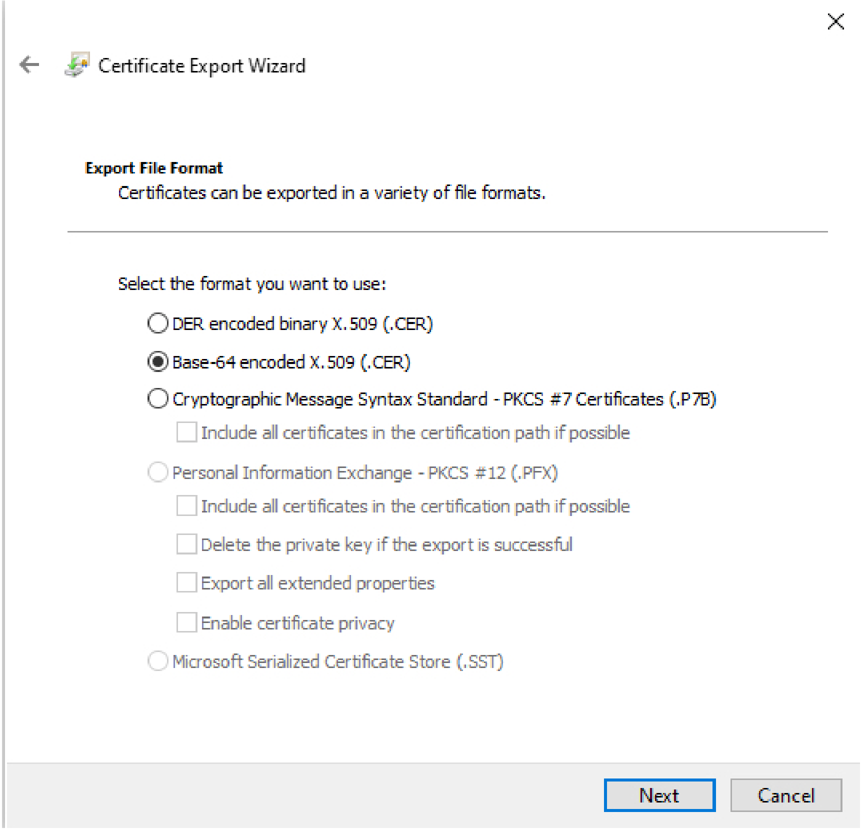
4. Repeat these tasks for both vCenter and the Management Center.

Get a Certificate Chain—Windows Chrome

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

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

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



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

10. Follow the prompts to complete the export.

11. Open the certificate in a text editor.

12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for both vCenter and the FMC.

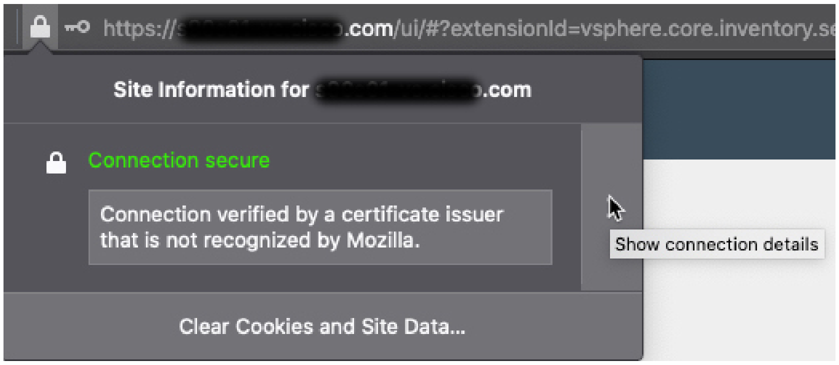
Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter or the Management Center using Firefox.

2. Click the lock to the left of the host name.

3. Click the right arrow (**Show connection details**). The following figure shows an example.



https://[redacted].com/ui/#?extensionId=vsphere.core.inventory.se

Site Information for [redacted].com

Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

Show connection details

Clear Cookies and Site Data...

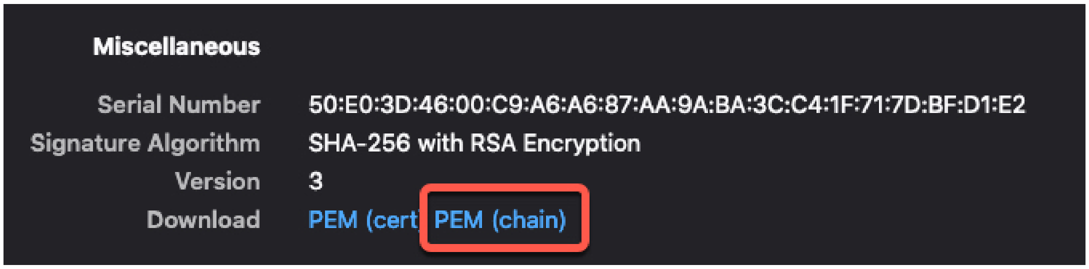
4. Click **More Information**.

5. Click **View Certificate**.

6. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.

7. Scroll to the Miscellaneous section.

8. Click **PEM (chain)** in the Download row. The following figure shows an example.



Miscellaneous

Serial Number	50:E0:3D:46:00:C9:A6:A6:87:AA:9A:BA:3C:C4:1F:71:7D:BF:D1:E2
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

9. Save the file.

10. Repeat these tasks for both vCenter and the Management Center.

Create Dynamic Attributes Filters

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

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.

Before you begin

Create a Connector, on page 1

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Dynamic Attributes Filters**.

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

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 management center.

a) Log in to the management center as a user with the Network Admin role at minimum.

b) Click **Objects** > **Object Management**.

c) In the left pane, click **External Attributes** > **Dynamic Object**.

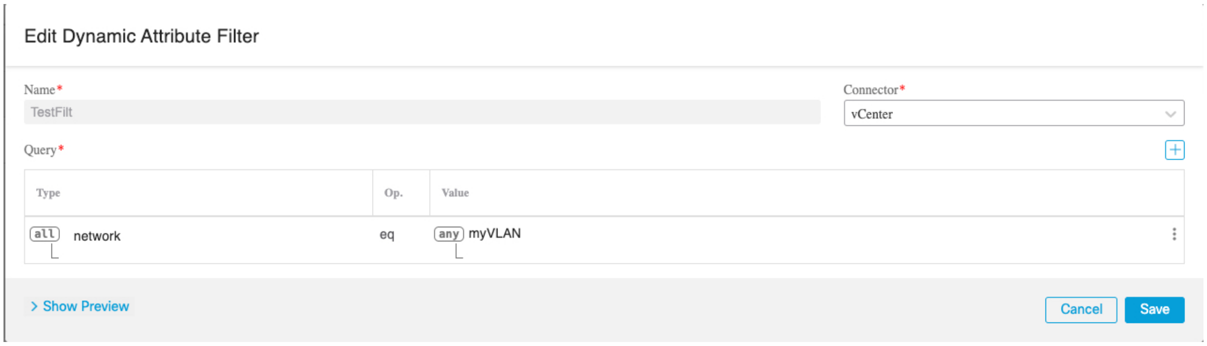
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

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

Examples: vCenter

The following example shows one criterion: a VLAN.



Edit Dynamic Attribute Filter

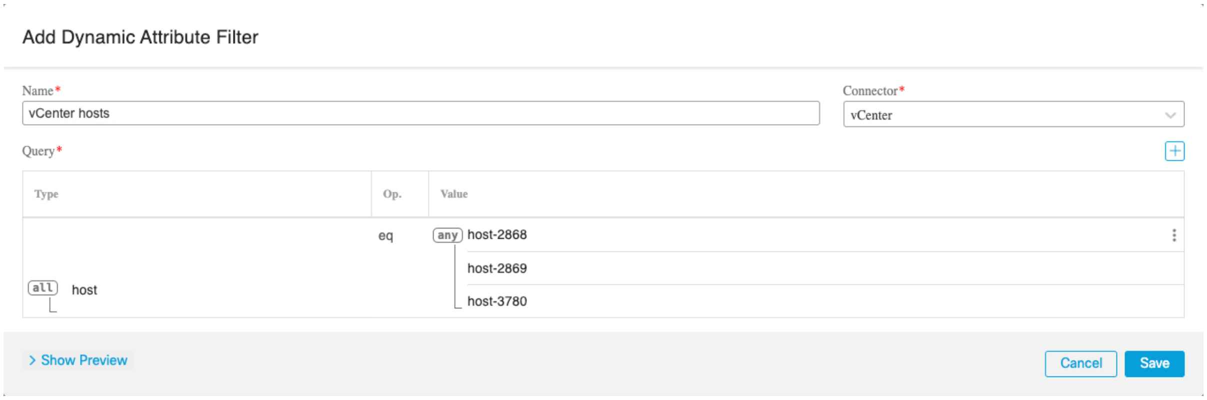
Name* TestFilt

Connector* vCenter

Query*

Type	Op.	Value
all network	eq	any myVLAN

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



Add Dynamic Attribute Filter

Name* vCenter hosts

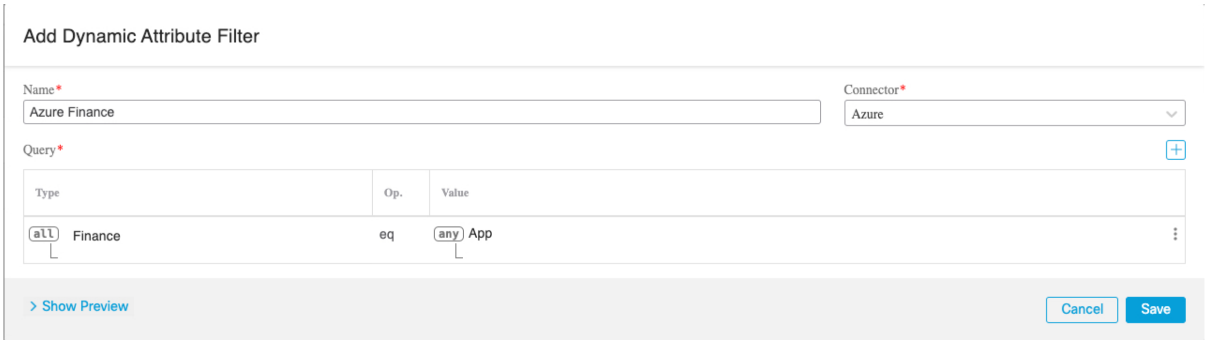
Connector* vCenter

Query*

Type	Op.	Value
all host	eq	any host-2868 host-2869 host-3780

Example: Azure

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


Add Dynamic Attribute Filter

Name* Azure Finance

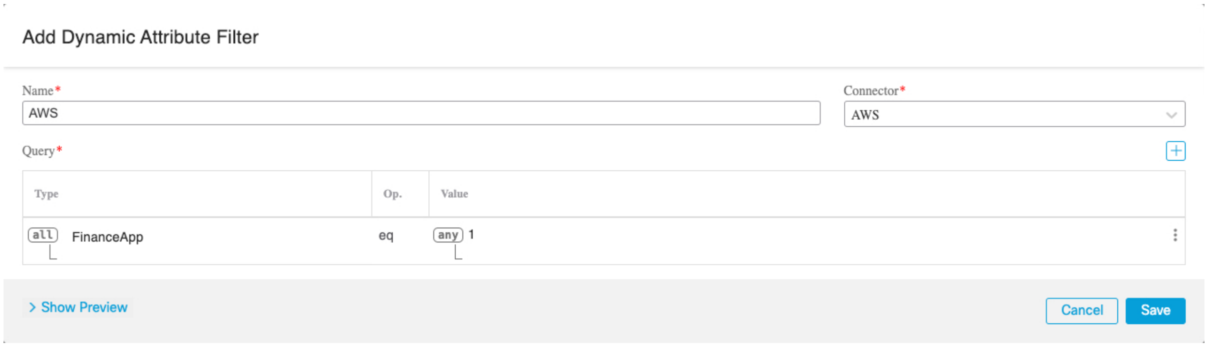
Connector* Azure

Query*

Type	Op.	Value
all Finance	eq	any App

Example: AWS

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


Add Dynamic Attribute Filter

Name* AWS

Connector* AWS

Query*

Type	Op.	Value
all FinanceApp	eq	any 1

Manually Get a Certificate Authority (CA) Chain

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

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

You must use one of these procedures to connect to the following:

- vCenter or NSX

  It is not necessary to get a certificate chain for connecting to Azure or AWS.

- Management Center

Before you use this procedure, see the section on automatically fetching the certificate authority chain in:

- Create a vCenter Connector, on page 12

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.

2. Enter the following command.

   ```
   security verify-cert -P url[:port]
   ```

   where url is the URL (including scheme) to vCenter or Management Center. For example:

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

   If you access vCenter or the management center using NAT or PAT, you can add a port as follows:

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

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

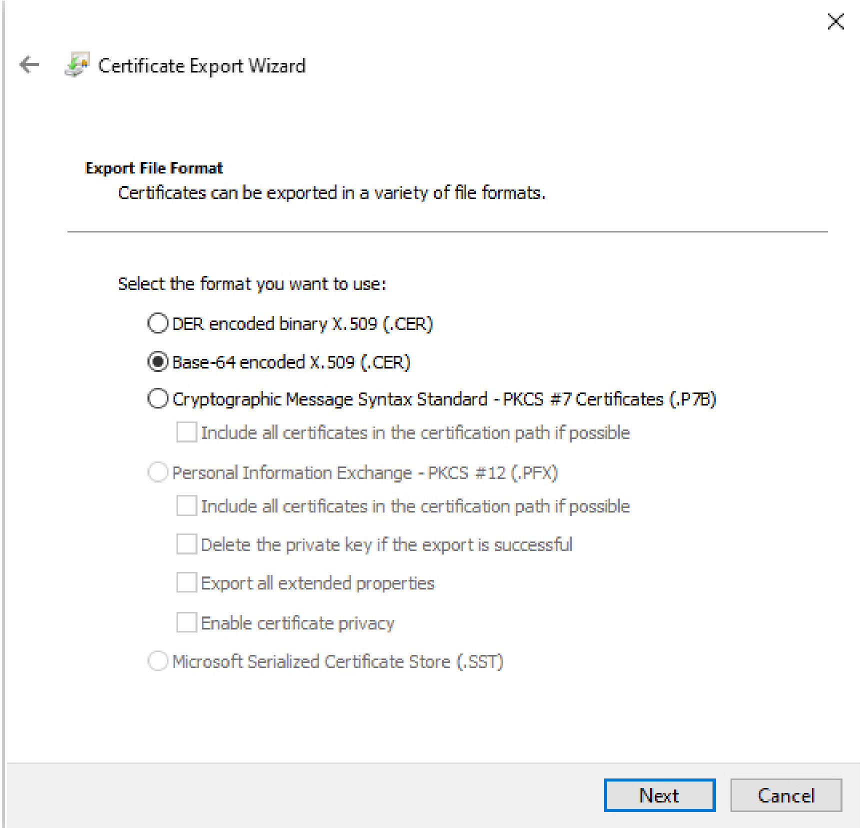
4. Repeat these tasks for both vCenter and the Management Center.

Get a Certificate Chain—Windows Chrome

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

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

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



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

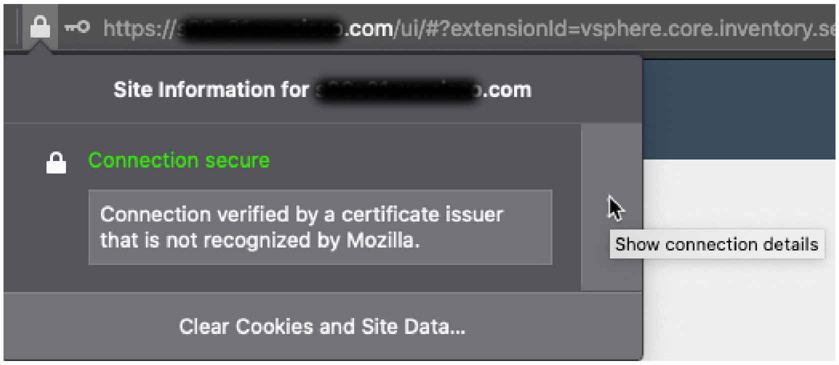
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for both vCenter and the FMC.

Get a Certificate Chain—Windows Firefox

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

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


https://[redacted].com/ui/#?extensionId=vsphere.core.inventory.se
Site Information for [redacted].com
Connection secure
Show connection details
Clear Cookies and Site Data...

Connection verified by a certificate issuer that is not recognized by Mozilla.

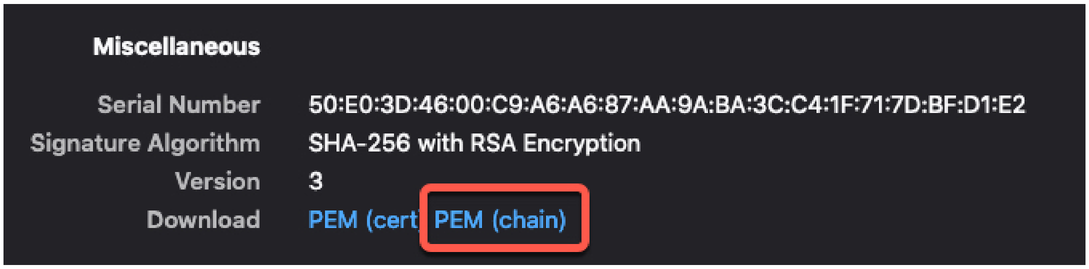
4. Click **More Information**.

5. Click **View Certificate**.

6. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.

7. Scroll to the Miscellaneous section.

8. Click **PEM (chain)** in the Download row. The following figure shows an example.



Miscellaneous

Serial Number	50:E0:3D:46:00:C9:A6:A6:87:AA:9A:BA:3C:C4:1F:71:7D:BF:D1:E2
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert PEM (chain)

9. Save the file.

10. Repeat these tasks for both vCenter and the Management Center.