



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](#)
- [System Requirements for the Cisco Secure Dynamic Attributes Connector, on page 4](#)
- [Enable the Cisco Secure Dynamic Attributes Connector, on page 4](#)
- [About the Dashboard, on page 7](#)
- [Create a Connector, on page 13](#)
- [Create Dynamic Attributes Filters, on page 29](#)
- [Manually Get a Certificate Authority \(CA\) Chain, on page 32](#)
- [Use Dynamic Objects in Access Control Policies, on page 35](#)
- [Disable the Cisco Secure Dynamic Attributes Connector, on page 37](#)
- [Troubleshoot Using the Command Line, on page 37](#)
- [Troubleshoot Using the Management Center, on page 39](#)
- [Manually Get a Certificate Authority \(CA\) Chain, on page 40](#)
- [Security Requirements, on page 42](#)
- [Internet Access Requirements, on page 43](#)
- [History for the Cisco Secure Dynamic Attributes Connector, on page 44](#)

About the Cisco Secure Dynamic Attributes Connector

The dynamic attributes connector enables you to use service tags and categories from various cloud service platforms in Secure Firewall Management Center 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	Azure	Azure Service Tags	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No

CSDAC version/platform	AWS	Azure	Azure Service Tags	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 2.0 (on-premises)	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Cisco Defense Orchestrator)	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	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 13.

- Generic text list of IP addresses you specify.

For more information, see [Create a Generic Text Connector](#), on page 20.

- Microsoft Azure

For more information, see [this page](#) on the Azure documentation site.

See [Azure Connector—About User Permissions and Imported Data](#), on page 16.

- 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.

- VMware categories and tags managed by vCenter and NSX-T

For more information, see a resource like [vSphere Tags and Attributes in the VMware documentation site](#).

- Webex IP addresses

For more information, see [Create a Webex Connector](#), on page 28.

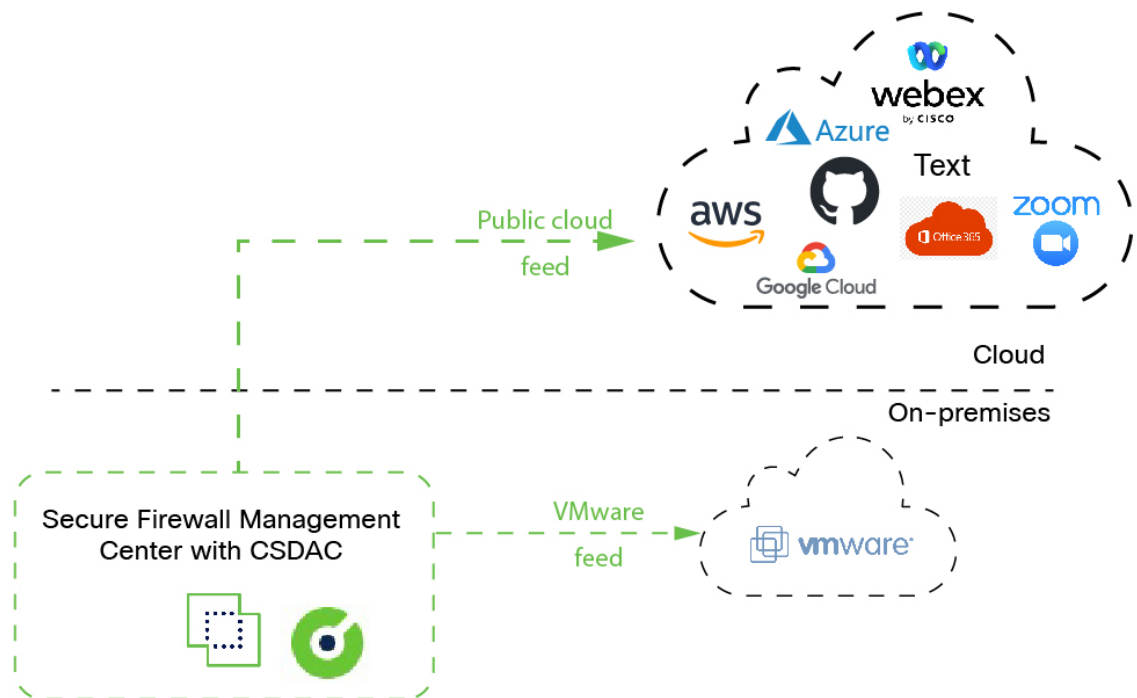
- Zoom IP addresses

For more information, see [Create a Zoom Connector](#), on page 28.

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).

Related topics

- [Enable the Cisco Secure Dynamic Attributes Connector, on page 4](#)
- [About the Dashboard, on page 7](#)

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	7.4.0	7.4.0	<p>This feature is introduced.</p> <p>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.</p> <p>More information:</p> <ul style="list-style-type: none"> 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 <p>New/modified screen: Integration > Cisco Dynamic Attributes Connector</p>

System Requirements for the Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector has the following memory requirements:

FMCv: Amount of RAM	Secure Firewall Management Center hardware model	Maximum number of (connectors + Azure AD realms)
At least 32GB	Firepower 1000, Firepower 1600, vFMC	10
At least 64GB	Firepower 2500, Firepower 2600, vFMC 300	20
At least 128GB	Firepower 4500, Firepower 4600	30

The preceding limits apply to both virtual machines and physical machines.

The system prevents you from exceeding the preceding limits because deployment issues could result.

Enable the Cisco Secure Dynamic Attributes Connector

This task discusses how to enable the Cisco Secure Dynamic Attributes Connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in management center access control rules.

Procedure

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

- Step 2** Click **Integration > Cisco Dynamic Attributes Connector**.
- Step 3** Slide to **Enabled**.
- Step 4** Messages are displayed while the dynamic attributes connector is enabled.
In the event of errors, try again. If errors persist, contact Cisco TAC.
-

Configure Networks and Subnets for Docker Containers

The Cisco Secure Dynamic Attributes Connector uses Docker containers to retrieve connector data in the Secure Firewall Management Center. To avoid conflicts with the Secure Firewall Management Center management interface and other IP addresses used in your network, you can optionally use the command discussed in this section to change Docker IP addresses and ranges.

About Docker networks

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

- `docker0` which is used internally by the Docker daemon.
- A series of IPv6 networks named `vethnumber`.
These are internal bridge networks used by the dynamic attributes connector.
- Docker bridge networks used by dynamic attributes connector connectors named `br-number`.

Before you enable the dynamic attributes connector is enabled, there is only one Docker interface, named `docker0`, set to 172.18.0.1/16.

Change Docker networks and subnets

First enable the dynamic attributes connector as discussed in [Enable the Cisco Secure Dynamic Attributes Connector, on page 4](#).

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

- `-b CIDR-network` sets a network base address pool in CIDR notation.
- `-s address-pool-size` sets a netmask for the network base address. You can use this option to limit the number of addresses in a base address range in the event the network range overlaps existing network ranges; in particular, we recommend certain `-s` values for Secure Firewall Management Center models to make sure you don't exceed the available RAM in the machine. (Docker containers are used by dynamic attributes connector connectors and those limits are shown in [System Requirements for the Cisco Secure Dynamic Attributes Connector, on page 4](#).)



Important The networks you assign to Docker must be in an internal network range and must *not* conflict with networks used by the Secure Firewall Management Center or by other devices in your internal network.

Examples

The following table shows examples.

Secure Firewall Management Center model	Recommended -s value	Sample -b value	Cisco Secure Dynamic Attributes Connector container addresses used
Firepower 1000, Firepower 1600, vFMC	27 (netmask 255.255.255.224)	172.19.0.0/16	30 IP addresses docker0: 172.19.0.1 Bridge networks <i>br-number</i> gateway 172.19.0.33 with subnet 172.19.0.32/27 Connectors created in networks like 172.19.0.38/27, 172.19.0.39/27, and so on
Firepower 2500, Firepower 2600, vFMC 300	26 (netmask 255.255.255.192)	192.168.0.0/16	62 IP addresses docker0: 192.168.1.1 Bridge networks <i>br-number</i> gateway 192.168.1.65 with subnet 192.168.1.64/26 Connectors created in networks like 192.168.1.71/26, 192.168.1.72/26, and so on
Firepower 4500, Firepower 4600	25 (netmask 255.255.255.128)	192.168.0.0/16	126 IP addresses docker0: 192.168.1.1 Bridge networks <i>br-number</i> gateway 192.168.1.129 with subnet 192.168.1.128/25 Connectors created in networks like 192.168.1.136/25, 192.168.1.135/25, and so on

For reference, the complete commands follow:

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

Verify the networks

To verify your network settings, enter `sudo docker network inspect muster-net`. The command results are displayed in JSON format.

Troubleshoot

Following are some solutions to common errors you might encounter using this command.

Error: Pull subnet value can not be greater than size

Solution: Change the value of `-s` so it is less than the CIDR network value.

For example,

INCORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

CORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

Error: After running the command, the Docker networks are wrong.

Solution: Restart the Docker daemon: `sudo systemctl restart docker`

Error: Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?

Solution: Restart Docker: `systemctl restart docker`

Error: Input can't be empty

The `-s` parameter is required.

Error: Pull size - 32 - can not be greater than 32 or less than 0

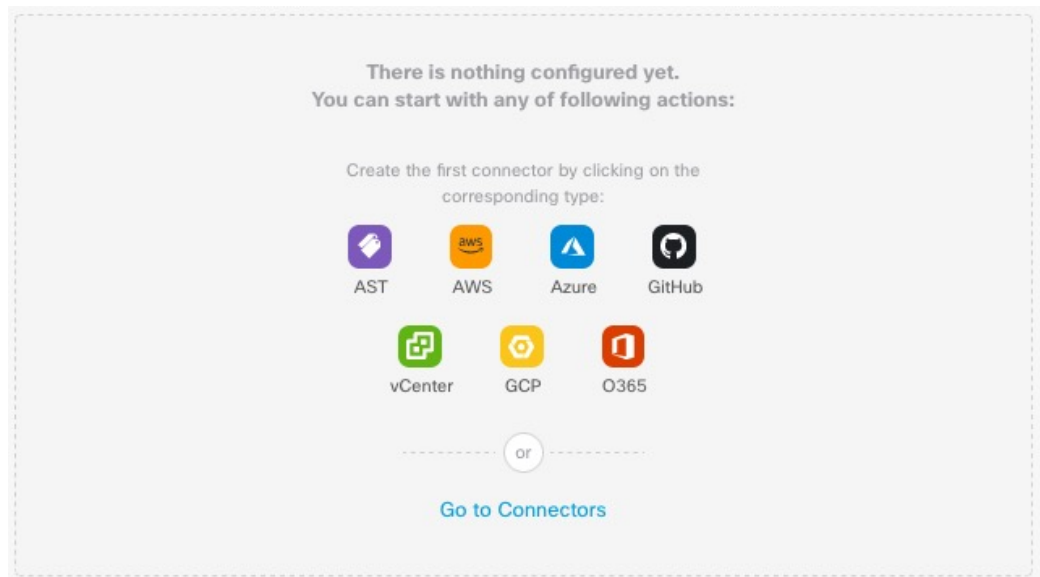
Solution: Change the value of `-s` so it is greater than 0 and less than 32.

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:

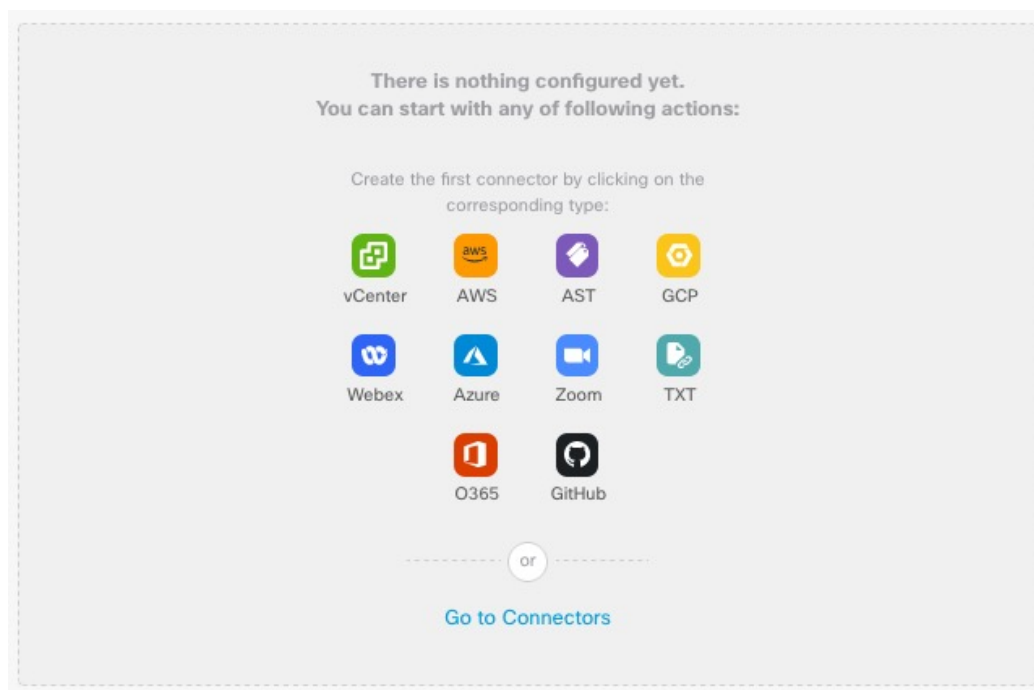
- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

Related Topics

- [Dashboard of an Unconfigured System, on page 8](#)
- [Dashboard of a Configured System, on page 9](#)
- [Add, Edit, or Delete Connectors, on page 10](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 11](#)

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 **Add** 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 13](#).

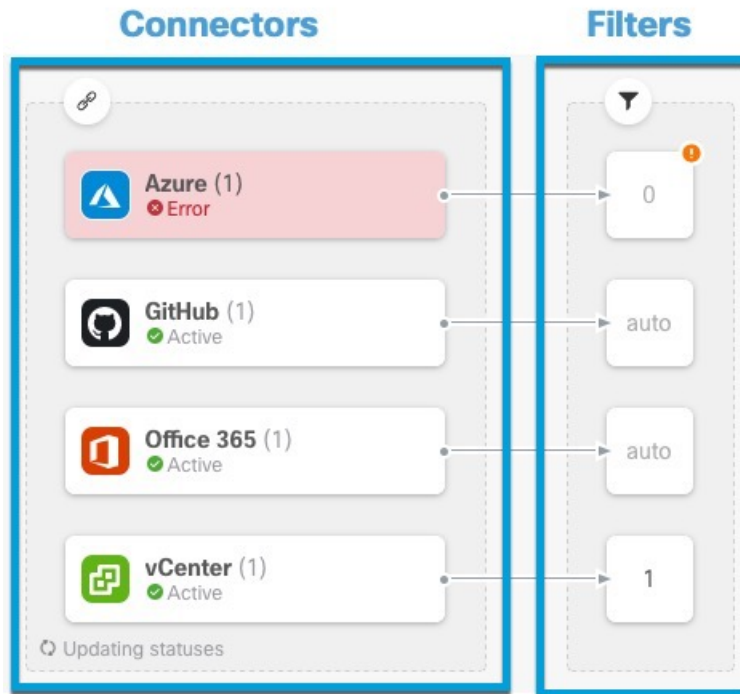
Related Topics:

- [Dashboard of a Configured System, on page 9](#)
- [Add, Edit, or Delete Connectors, on page 10](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 11](#)

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 13](#)


[2 Create Dynamic Attributes Filters, on page 29](#)

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

Connectors column	Filters 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 Secure Firewall Manager. 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 10.</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 11.</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 10](#)
- [Add, Edit, or Delete Dynamic Attributes Filters, on page 11](#)

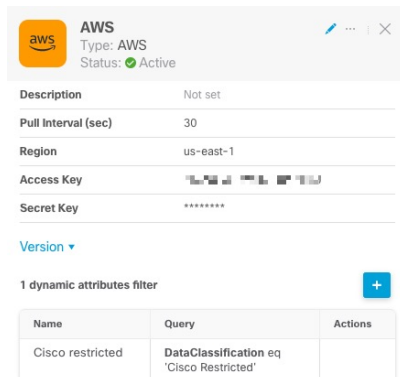
Add, Edit, or Delete Connectors

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:





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 . 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:

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 29](#).

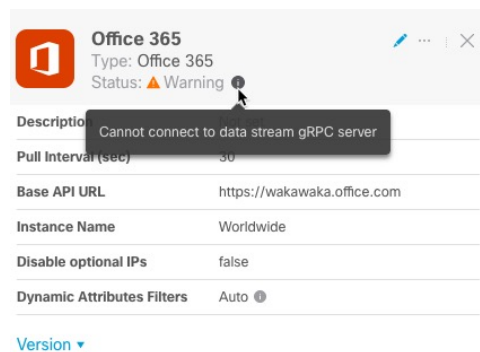
Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

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 24](#).
4. If you cannot resolve the issue, click **Version** and copy the version to a text file.
5. Provide all of this information to [Cisco TAC](#).

Add, Edit, or Delete Dynamic Attributes Filters

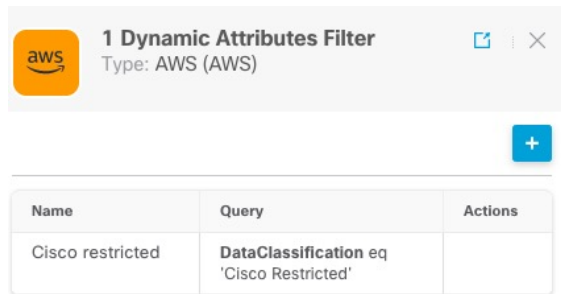
The Dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter

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 29](#).

An example follows:







Name	Query	Actions
Cisco restricted	DataClassification eq 'Cisco Restricted'	

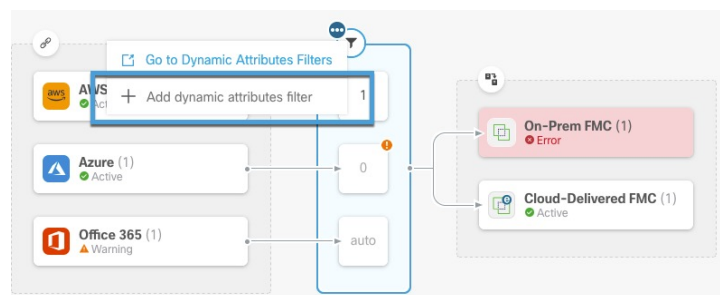




Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the  column.

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 29](#).
- 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 management center.

We support the following:

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

CSDAC version/platform	AWS	Azure	Azure Service Tags	Generic text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	Yes	Yes	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	Yes	Yes	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Cloud-delivered (Cisco Defense Orchestrator)	Yes	Yes	Yes	No	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	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 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`, `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 the management center. For a list of these attributes, see [Amazon Web Services Connector—About User Permissions and Imported Data](#), on page 13.

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.

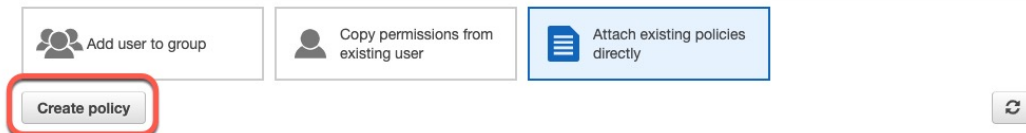
Procedure

- 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",
    "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 15.](#)

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 14.](#)

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Integration > Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** 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 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 16](#).

Before you begin

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

- A sample follows.

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 ⓘ
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 18](#).

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 16.

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Integration** > **Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** 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 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 associated with these tags are updated every week by Microsoft.

For more information, see [Virtual network service tags on Microsoft TechNet](#).

Procedure

- Step 1** Log in to the management center.

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

Step 3 Click **Connectors**.

Step 4 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 5 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 6 Click **Save**.

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

Create a Generic Text Connector

This task discusses how to create an ad hoc list of IP addresses you maintain manually and retrieve at an interval you select (30 seconds by default). You can update the list of addresses anytime you want.

Before you begin

Create a text file with IP addresses and put it on a web server that is accessible from the management center. IP addresses can include CIDR notation. The text file must have only one IP address per line.

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



Note Do not include a scheme (**http://** or **https://**) in your IP addresses.

Procedure

Step 1 Log in to the management center.

- Step 2** Click **Integration > Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** Enter a **Name** and an optional description.
- Step 6** (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 30 seconds.
- Step 7** In the **URLs** field, enter each URL from which to retrieve IP addresses, one URL per line.
- Step 8** (Optional.) If a certificate chain is required for a secure connection to the web server, 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 32](#).
 - Click **Get Certificate > Browse from file** to upload a certificate chain you downloaded previously.
- Step 9** Click **Test** and make sure the test succeeds before you save the connector.
- Step 10** Click **Save**.
- Step 11** 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.

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Integration > Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** Enter a **Name** and an optional description.
- Step 6** (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 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 22](#).

Before you begin

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

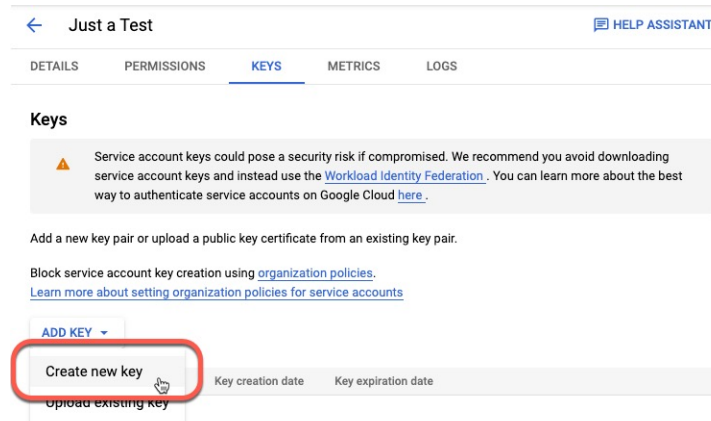
Procedure

- Step 1** Log in to your Google Cloud account as a user with the owner role.
- Step 2** Click **IAM & Admin > Service Accounts > Create Service Account**.
- Step 3** Enter the following information:
- **Service account name:** A name to identify this account; for example, **CSDAC**.

- **Service account ID:** Should be populated with a unique value after you enter the service account name.
- **Service account description:** Enter an optional description.

For more information about service accounts, see [Understanding Service Accounts](#) in the Google Cloud documentation.

- 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 23](#).

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 the management center.
- Step 2** Click **Integration** > **Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** 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 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.

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Integration** > **Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5 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 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.

Procedure

Step 1 Log in to the management center.

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

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: <ul style="list-style-type: none"> • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port <i>Do not</i> 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.

Value	Description
vCenter Certificate	<p>You have the following options:</p> <ul style="list-style-type: none"> • Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 32. • Click Fetch to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 32. • 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 32. • 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

Name* Certificate chain was successfully fetched. Here are certificate details (priority order descending):

Description* > firepower - 1 certificate

Domain* > firepower - 1 certificate

IP*

Port*

User*

Password*

Secondary IP

Secondary Port

Secondary User

Secondary Password

FMC Server Certificate* Updated SIN 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 32](#).

Step 5 Click **Save**.

Create a Webex Connector

This section discusses how to create a Webex connector that sends data to the management center for 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 Log in to the management center.

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

Step 3 Click **Connectors**.

Step 4 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 5 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 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.

Create a Zoom Connector

This section discusses how to create a Zoom connector that sends data to the management center for 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** Log in to the management center.
- Step 2** Click **Integration** > **Cisco Dynamic Attributes Connector**.
- Step 3** Click **Connectors**.
- Step 4** 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 5** 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 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.

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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see [Create Access Control Rules Using Dynamic Attributes Filters, on page 36](#).

Before you begin

[Create a Connector, on page 13](#)

Procedure

Step 1 Log in to the management center.

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

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

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 management center.

- Log in to the management center as a user with the Network Admin role at minimum.
- Click **Objects > Object Management**.
- 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* Connector*

Query* +

Type	Op.	Value
all network	eq	any myVLAN

[Show Preview](#) Cancel Save

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

Add Dynamic Attribute Filter

Name* Connector*

Query* +

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

[Show Preview](#) Cancel Save

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

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

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
```

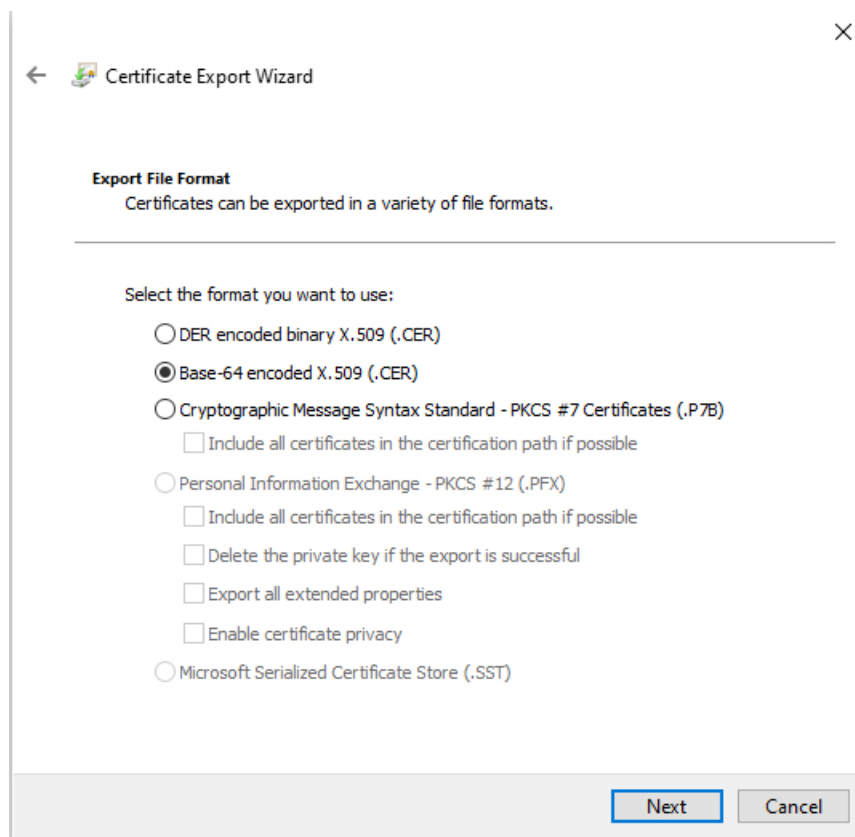
3. Save the entire certificate chain to a plaintext file.
 - *Include* all -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- delimiters.
 - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >)) as well as the angle brackets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

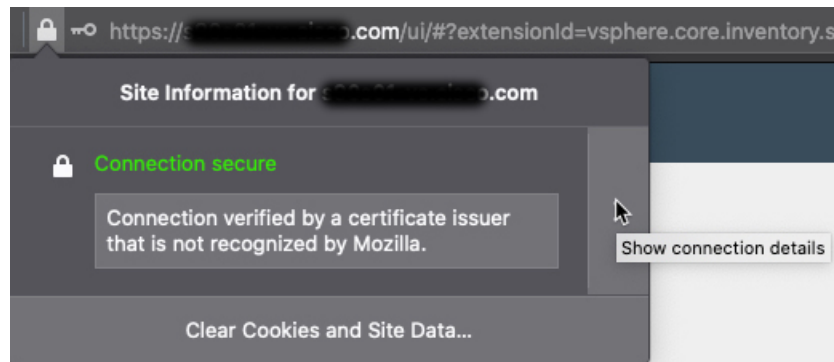


10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.
You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for both vCenter and the FMC.

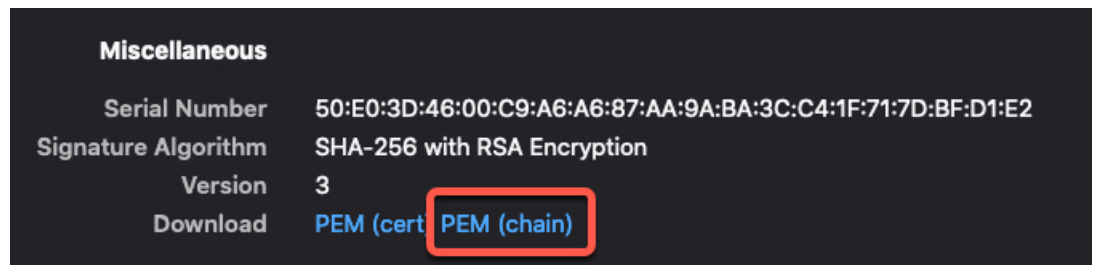
Get a Certificate Chain—Windows Firefox

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.



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.



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

Use Dynamic Objects in Access Control Policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the management center 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 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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. 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.

Procedure

- Step 1** Log in to the management center.
- Step 2** Click **Edit** (✎) next to an access control policy.
- Step 3** Click **Add Rule**.
- Step 4** Click the **Dynamic Attributes** tab.
- Step 5** In the Available Attributes section, from the list, click **Dynamic Objects**.

The following figure shows an example.

The screenshot displays the 'Add Rule' configuration interface. At the top, there are fields for 'Name', 'Enabled' (checked), 'Insert' (set to 'into Mandatory'), 'Action' (set to 'Allow'), and 'Time Range' (set to 'None'). Below these are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes' (selected), 'Inspection', 'Logging', and 'Comments'. The 'Available Attributes' section on the left has a search bar and a list where 'Dynamic Objects' is selected, and 'FinanceNetwork' is highlighted. To the right of this list are 'Add to Source' and 'Add to Destination' buttons. The 'Selected Source Attributes (0)' and 'Selected Destination Attributes (0)' sections are empty. At the bottom right, there are 'Cancel' and 'Add' buttons.

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 6** Add the desired object to source or destination attributes.
- Step 7** 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](#))

Disable the Cisco Secure Dynamic Attributes Connector

If you no longer wish to collect dynamic objects from cloud sources, you can disable the Cisco Secure Dynamic Attributes Connector in the Secure Firewall Management Center as discussed in the following task.

Procedure

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

Troubleshoot Using the Command Line

To assist you with advanced troubleshooting and working with Cisco TAC, we provide the following troubleshooting tools. To use these tools, log in as any user to the Ubuntu host on which the dynamic attributes connector is running.

Check container status

To check the status of the dynamic attributes connector Docker containers, enter the following commands:

```
cd /usr/local/sf/csdac
sudo ./muster-cli status
```

Sample output follows:

```
===== CORE SERVICES =====
=====
      Name                                Command                                State                                Ports
-----
muster-bee                               /bin/sh -c /app/bee                               Up
127.0.0.1:15050->50050/tcp, 50443/tcp
muster-envoy                             /docker-entrypoint.sh runs ...   Up      127.0.0.1:6443->8443/tcp

muster-local-fmc-adapter                 ./docker-entrypoint.sh run ...   Up

muster-ui-backend                       ./docker-entrypoint.sh run ...   Up      50031/tcp

muster-user-analysis                    ./docker-entrypoint.sh run ...   Up      50070/tcp

===== CONNECTORS AND ADAPTERS =====
=====
      Name                                Command                                State                                Ports
-----
muster-connector-o365.1.muster          ./docker-entrypoint.sh run ...   Up      50070/tcp
```

Stop, start, or restart the Dynamic Attributes Connector Docker containers

If the `./muster-cli status` indicates containers are down or to restart containers in the event of issues, you can enter the following commands:

Stop and restart:

```
cd ~/csdac/app
sudo ./muster-cli stop
sudo ./muster-cli start
```

Start only:

```
cd ~/csdac/app
sudo ./muster-cli start
```

Enable application debug logging and generate troubleshoot files

If advised to do so by Cisco TAC, enable debug logging and generate troubleshoot files as follows:

```
cd ~/csdac/app
sudo ./muster-cli debug-on
sudo ./muster-cli ts-gen
```

The troubleshoot file name is **ts-bundle-timestamp.tar** and is created in the same directory.

The following table shows the location of troubleshoot files and logs in the troubleshoot file.

Location	What it contains
<code>/csdac/app/ts-bundle-timestamp/info</code>	etcd database contents
<code>/csdac/app/ts-bundle-timestamp/logs</code>	Container log files
<code>/csdac/app/ts-bundle-timestamp/status.log</code>	Container status, versions, and image status

Enable debugging for a container

You can optionally enable debugging for individual containers if you first get the name of the container as follows:

```
cd /usr/local/sf/csdac
sudo ./muster-cli versions
```

Sample output follows:

```
CSDAC version: 1.0.0
CONTAINERS VERSIONS
CONTAINER                                | APP VERSION          | COMMIT
=====
muster-bee                               | fmc7.4-13            |
944d50c6c384567693d6ecc5a31420de57f6ce2f
muster-envoy                             | fmc7.4-25            |
5e5f6d83164a4acbef5b106aa39e2e3f68fa738f
muster-local-fmc-adapter                  | fmc7.4-17            |
c5902f818baa8e27d7c0b8027490dcacc28c0168
muster-ui-backend                         | fmc7.4-64            |
165a1f5f0d763aa75829a30b5ffbddf0012682b6
muster-user-analysis                      | fmc7.4-43            |
63cd64e29a92599908c3eb684d91e9f685d8c740
muster-connector-o365.1.muster           | fmc7.4-8             |
28f075d315c8867f667b828970c9fbad35fa89cc
```

To enable debugging for the Office 365 connector, for example, enter the following command.

```
sudo ./muster-cli container-debug-on muster-connector-o365.1.muster
```

To disable debugging for that connector, enter the following command.

```
sudo ./muster-cli container-debug-off muster-connector-o365.1.muster
```

Verify dynamic objects on the

To verify your connectors are creating objects on the management center, you can use the following command on the management center as an administrator:

```
sudo tail -f /var/opt/CSCOpX/MDC/log/operation/usmshreddsvcs.log
```

Example: Successful object creation

```
26-Aug-2021 12:41:35.912, [INFO], (DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-10
** REST Request [ CSM ]
** ID : 18b25356-fd6b-4cc4-8d27-bbccb52a6275
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "18b25356-fd6b-4cc4-8d27-bbccb52a6275",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f
/object/dynamicobjects Created (201) - The request has been fulfilled and resulted in a new
resource being created",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629981695431"
  },
  "deleteList": []
}
```

Troubleshoot Using the Management Center

This task discusses how to generate troubleshoot files for the Secure Firewall Management Center.

Before you begin

For complete details about troubleshooting, see the troubleshooting chapter in the [Cisco Secure Firewall Management Center Administration Guide](#).

Procedure

- Step 1** Log in to the Secure Firewall Management Center.
- Step 2** Click **System** (⚙️) > **Health** > **Monitor**.
- Step 3** In the left pane, click **Firewall Management Center**.
- Step 4** At the top, click **System & Troubleshooting Details**.
- Step 5** Click **Generate Troubleshooting Files**.

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

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

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.

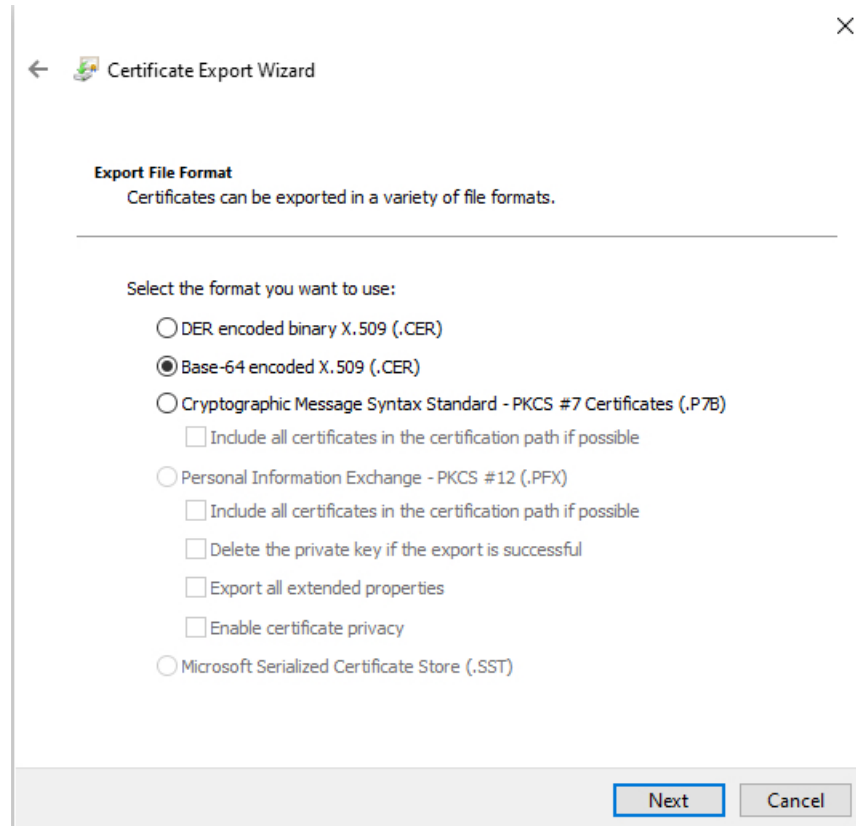
Get a Certificate Chain—Windows Chrome

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.



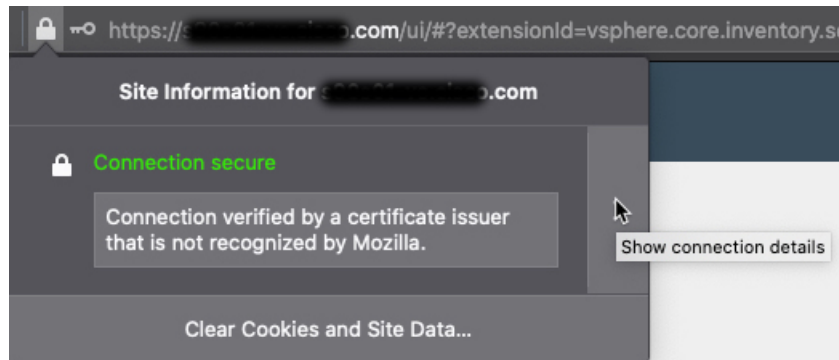
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.
You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for both vCenter and the FMC.

Get a Certificate Chain—Windows Firefox

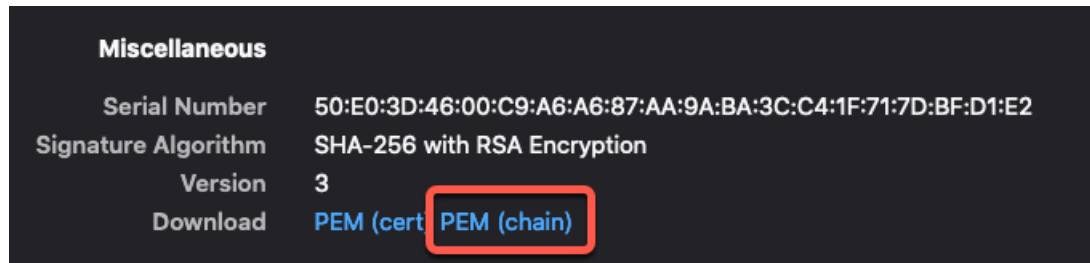
Use the following procedure to get a certificate chain for the Firefox browser on either Windows or Mac OS.

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.



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.



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

Security Requirements

To safeguard the Cisco Secure Dynamic Attributes Connector, you should install it on a protected internal network. Although the dynamic attributes connector is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it.

If the dynamic attributes connector and the management center reside on the same network, you can connect the management center to the same protected internal network as the dynamic attributes connector.

Regardless of how you deploy your appliances, inter-system communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Internet Access Requirements

By default, the dynamic attributes connector is configured to communicate with the Firepower System over the internet using HTTPS on port 443/tcp (HTTPS). If you do not want the dynamic attributes connector to have direct access to the internet, you can configure a proxy server.

The following information informs you of the URLs the dynamic attributes connector use to communicate with the management center and with external servers.

Table 3: Dynamic Attributes Connector management center access requirements

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

Table 4: Dynamic Attributes Connector vCenter access requirements

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

Migration from DockerHub to Amazon ECR

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

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

- <https://public.ecr.aws>
- <https://csdac-cosign.s3.us-west-1.amazonaws.com>

Dynamic Attributes Connector Azure access requirements

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

History for the Cisco Secure Dynamic Attributes Connector

Feature	Minimum Management Center	Minimum Threat Defense	Details
Cisco Secure Dynamic Attributes Connector	7.4.0	7.4.0	<p>This feature is introduced.</p> <p>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.</p> <p>More information:</p> <ul style="list-style-type: none"> • 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 <p>New/modified screen: Integration > Cisco Dynamic Attributes Connector</p>