Configure the Cisco Secure Dynamic Attributes Connector

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

See the following topics for more information:

- Create a Connector, on page 1
- Create an Adapter, on page 7
- Create Dynamic Attributes Filters, on page 12

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 FMC.

We support the following:

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

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

See one of the following sections for more information.

Create an Azure Service Tags Connector

This topic discusses how to create a connector for Azure service tags to the FMCfor 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 FMC.

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** (+), 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 Office 365 Connector

This task discusses how to create a connector for Office 365 tags to send data to the FMC 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 Log in to the FMC.

Step 3 Click **Integration** > **Cisco Dynamic Attributes Connector**.

Step 4 Click **Connectors**.

Step 5 Do any of the following:

- Add a new connector: click **Add** (+), 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 6 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 7 Click **Save**.

Step 8 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 FMC 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.

Fetch a Certificate Authority (CA) Chain for a vCenter Connector

This topic discusses how to automatically fetch the certificate authority chain for a connector or an adapter. The *certificate authority chain* is the root certificate and all subordinate certificates; it is required to connect securely with vCenter or the FMC.

The dynamic attributes connector enables you to automatically fetch the certificate authority chain but if this procedure does not work for some reason, see Manually Get a Certificate Authority (CA) Chain, on page 8.

Step 1 Log in to the dynamic attributes connector.

Step 2 Do any of the following:

a) To fetch a vCenter CA chain, click **Connectors**.

b) To fetch the FMC adapter CA chain, click **Adapters**.

c) Click **Add** (+).

Step 3 In the **Name** field, enter a name to identify the connector or adapter.

Step 4 In the **Host** field, enter the connector or adapter's host name or IP address without the scheme (such as **https://**).

For example, `myvcenter.example.com` or `192.0.2.100:9090`

The host name or IP you enter must exactly match the Common Name of the CA certificate used to securely connect to it.

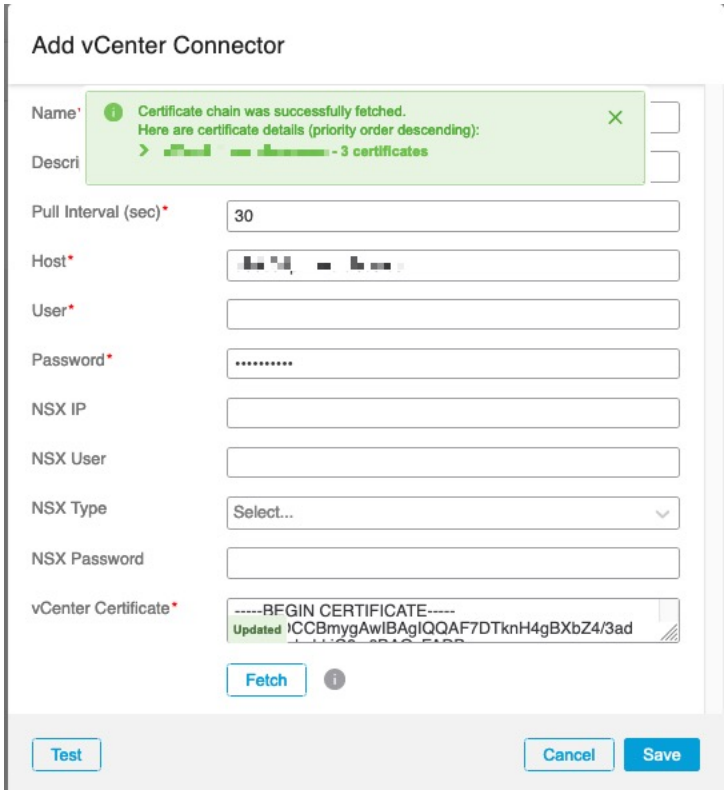
No other information is required to fetch the certificate CA chain.

Step 5 Click **Fetch**.

Step 6 (Optional.) Expand the certificates in the certificate CA chain to verify them.

Example

Following is an example of a successful certificate CA fetch for a vCenter connector.



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

Create a vCenter Connector

This task discusses how to create a connector for VMware vCenter to send data to the FMC 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 8.

Step 1 Log in to the dynamic attributes connector.

Step 2 Log in to the FMC.

Step 3 Click **Connectors**.

Step 4 Click **Integration** > **Cisco Dynamic Attributes Connector**.

Step 5 Do any of the following:

- Add a new connector: click **Add** (+), 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 6 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	

Step 7 Click **Save**.

What to do next

Create an Adapter, on page 7

Create an Adapter

An *adapter* is a secure connection to FMC 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 FMC.

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

Create a Firepower Management Center User for the Dynamic Attributes Connector

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

The FMC user must have Access Admin privileges at least.

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

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

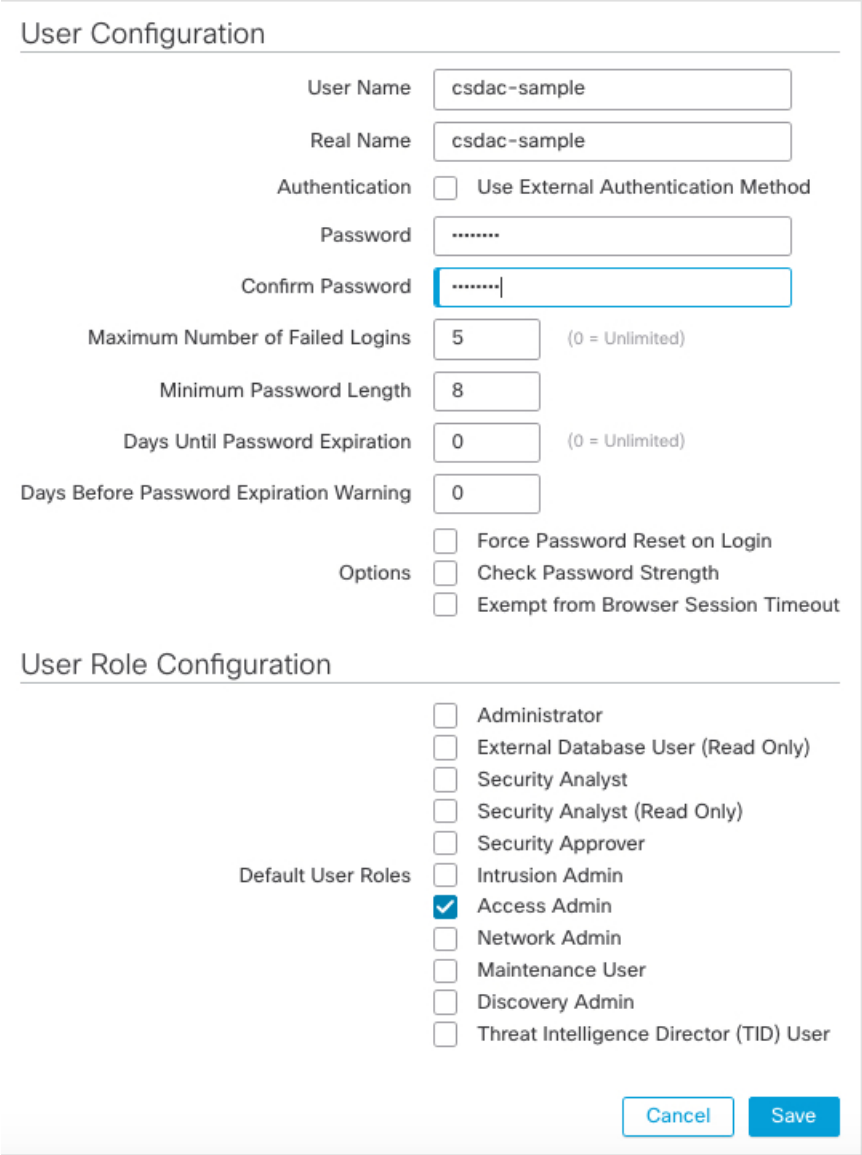
Step 3 Click **Create User**.

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.



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.

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 FMC.

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.

- FMC

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 FMC. For example:

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

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

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

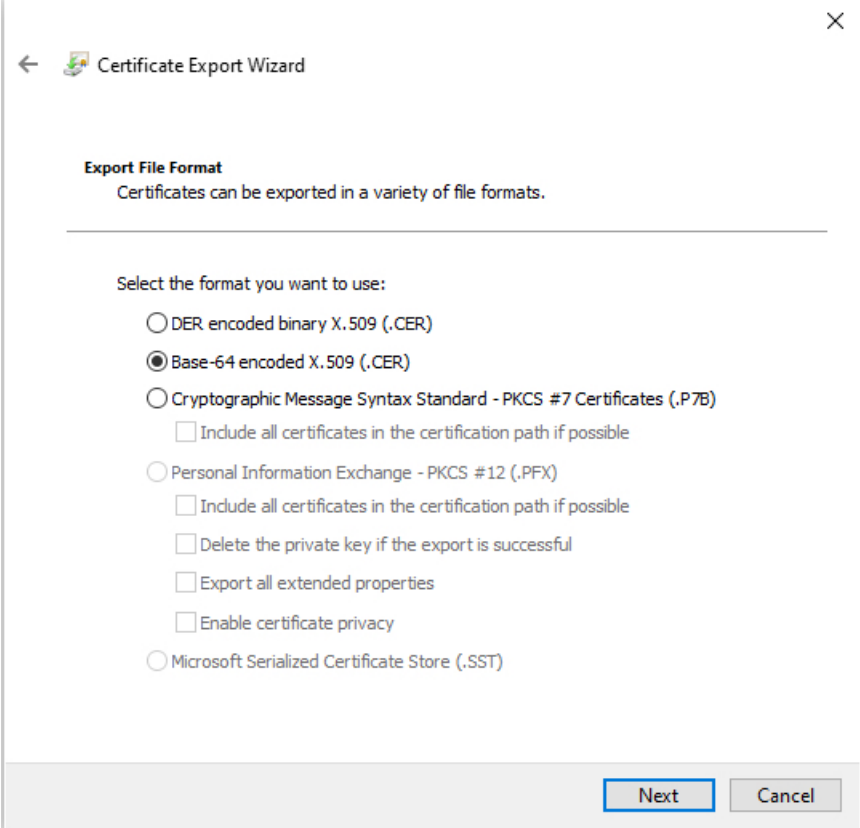
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

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 FMC 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.



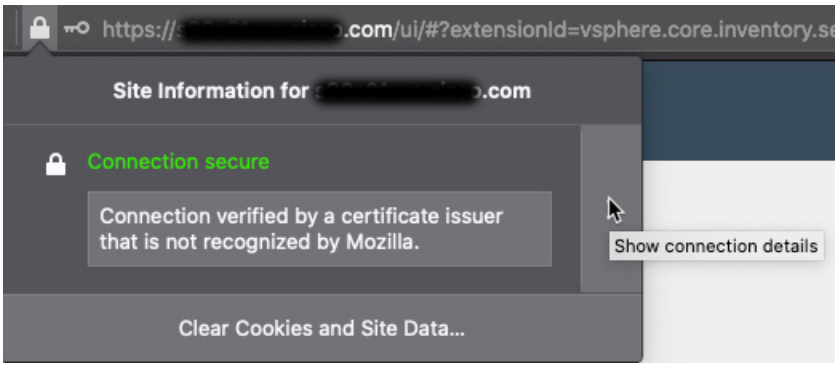
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

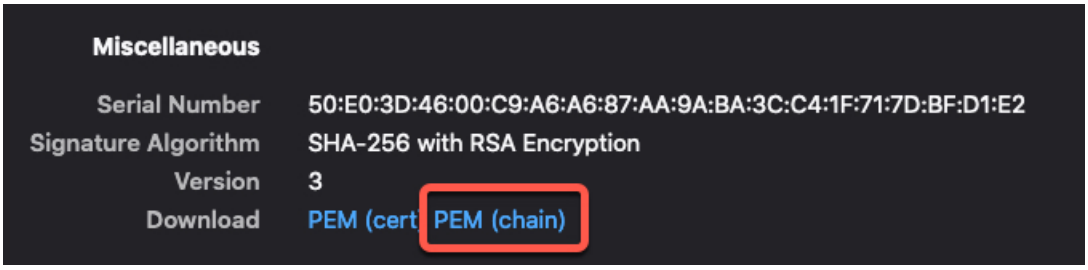
Get a Certificate Chain—Windows Firefox

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 FMC 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 FMC.

How to Create an FMC Adapter

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

Before you begin

See Create a Firepower Management Center User for the Dynamic Attributes Connector, on page 7.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Adapters**.

Step 3 Do any of the following:

- Add a new adapter: click **Add** (+), then click FMC.
- Edit or delete an adapter: 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 Firepower 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 Firepower 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 Firepower Management Center Virtual.
User	(Required.) Enter the name of an Firepower 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 Firepower 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 Firepower Management Center Virtual.
Secondary User	(High availability only.) Enter the name of a secondary Firepower Management Center Virtual user with the Network Admin role at minimum.
Secondary Password	(High availability only.) Enter the user's password.
FMC Server Certificate	Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 8.

Step 5 Click **Save**.

Create Dynamic Attributes Filters

Dynamic attributes filters that you define using the Cisco Secure Dynamic Attributes Connector are exposed in the FMC 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 Office 365, or Azure Service Tags. These types of cloud objects provide their own IP addresses.

For more information about access control rules, see Create Access Control Rules Using Dynamic Attributes Filters.

Before you begin

Complete all of the following tasks:

- Install Prerequisite Software
- Create a Connector, on page 1
- Create an Adapter, on page 7

Step 1 Log in to the dynamic attributes connector.

Step 2 Log in to the FMC.

Step 3 Click **Integration** > **Cisco Dynamic Attributes Connector**.

Step 4 Click **Dynamic Attributes Filters**.

Step 5 Do any of the following:

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

Step 6 Do any of the following:

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

Step 7 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 FMC 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** (+). • Edit or delete a filter: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 8 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 9 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 10 When you're finished, click **Save**.

Step 11 (Optional.) Verify the dynamic object in the FMC.

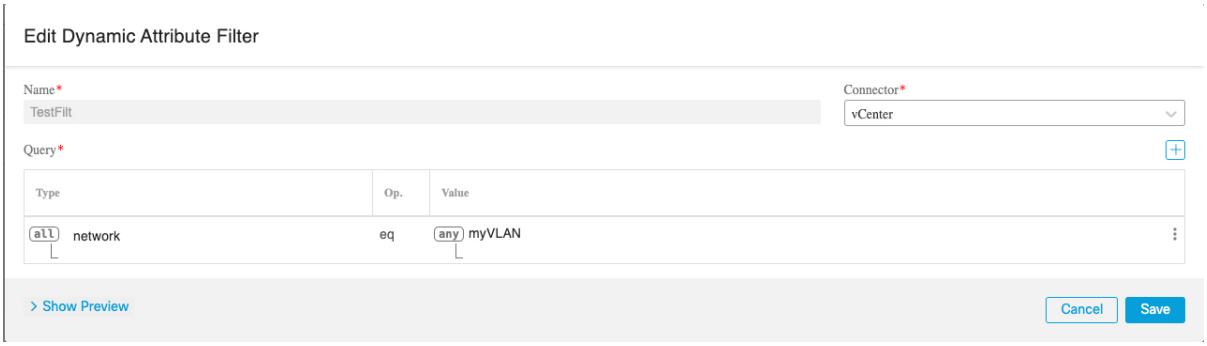
a) Log in to the FMC as a user with the Network Admin role at minimum.
b) Click **Objects** > **Object Manager**.
c) In the left pane, click **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

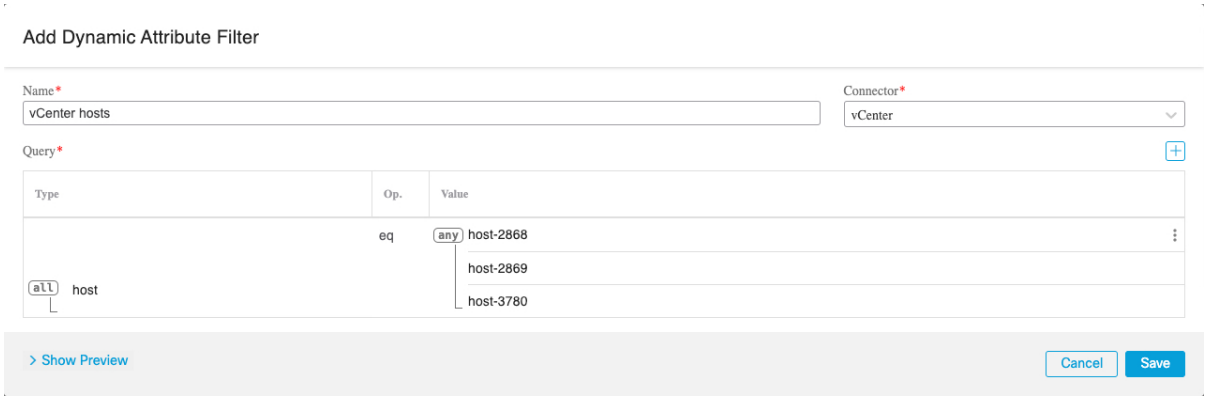
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

The following example shows one criterion: a VLAN.

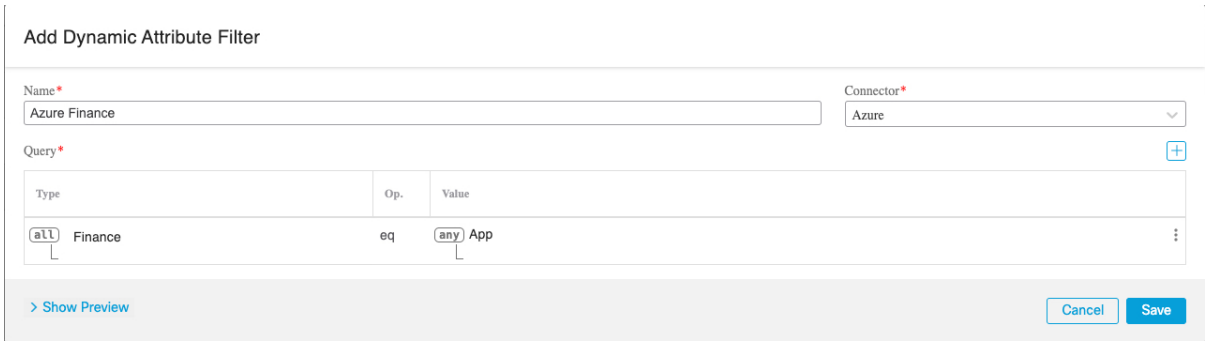


The following example shows three criteria that are joined with OR: the query matches any of three hosts.



Example: Azure

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



Example: AWS

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