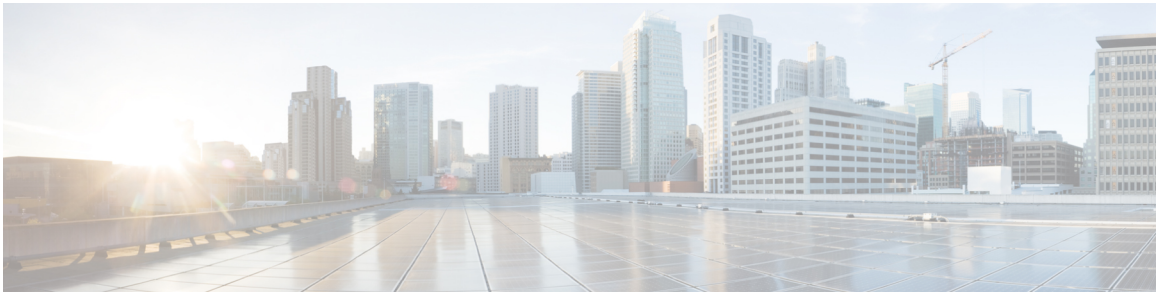
Cisco Secure Dynamic Attributes Connector Configuration Guide

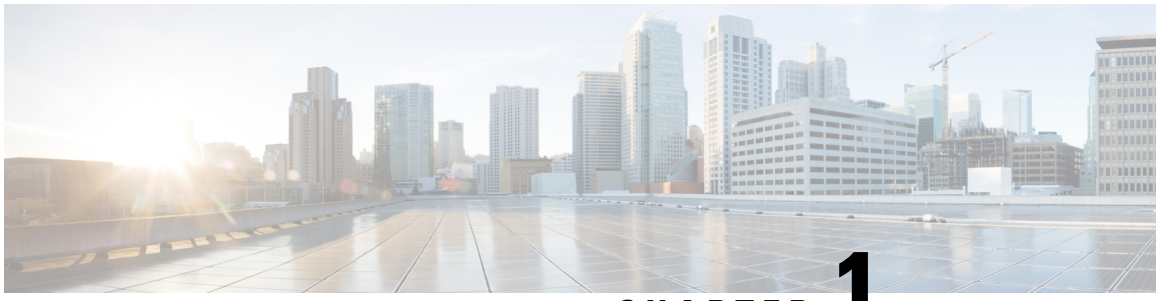
First Published: 2021-06-01

Last Modified: 2022-10-04

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS



CHAPTER 1

About the Cisco Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to collect data (such as networks and IP addresses) from cloud providers and send it to the FMC (FMC) so it can be used in access control rules.

The following topics provide background about the dynamic attributes connector:

About the Cisco Secure Dynamic Attributes Connector

The Cisco Secure Dynamic Attributes Connector enables you to use service tags and categories from various cloud service platforms in Firepower Management Center (FMC) 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	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

More information about connectors:

- Amazon Web Services (AWS)

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

- Microsoft Azure

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

- Microsoft Azure service tags

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

- Office 365

  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

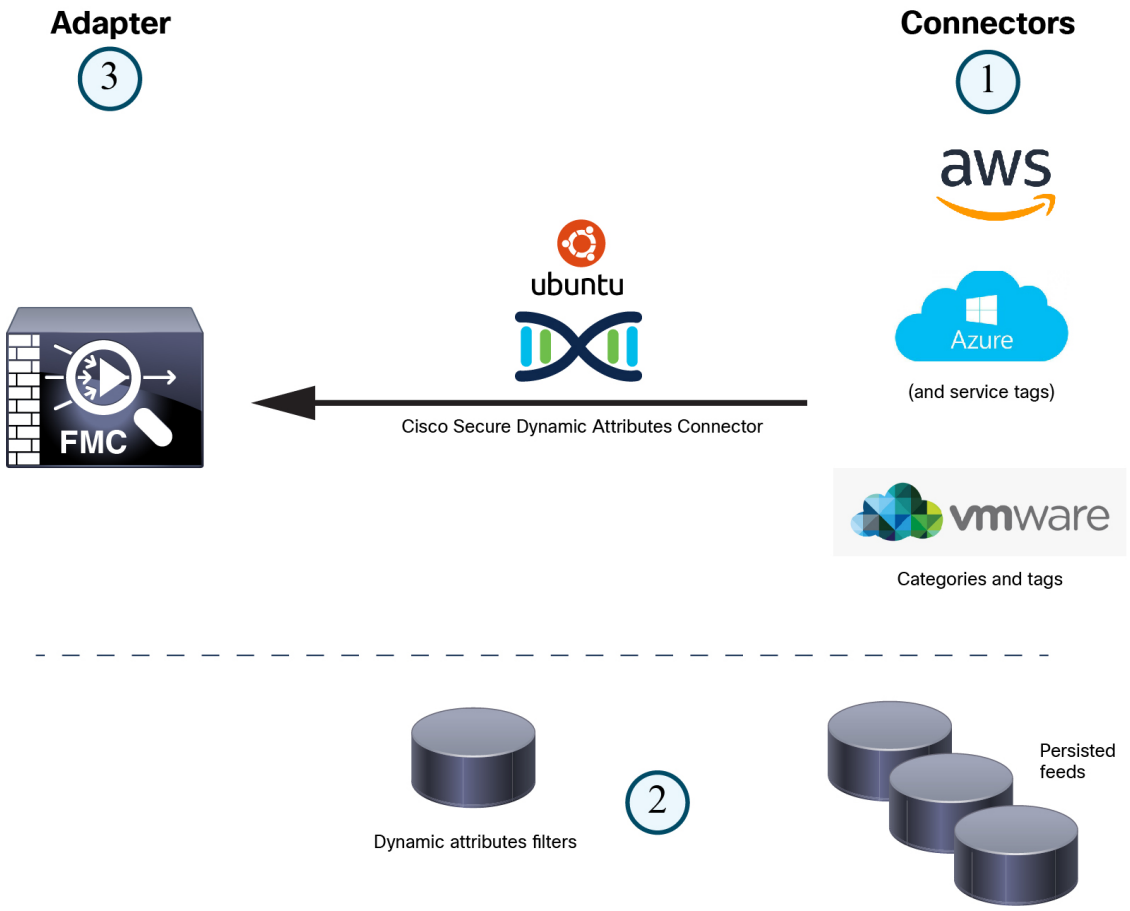
  For more information, see a resource like vSphere Tags and Attributes in the VMware documentation site.

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.

You can collect these tags and attributes using dynamic attributes connector Docker containers running on an Ubuntu virtual machine. Install the dynamic attributes connector on the Ubuntu host using an Ansible collection.

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



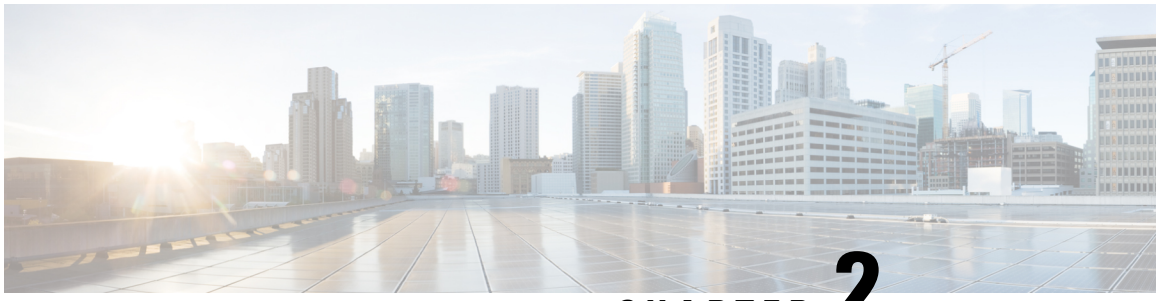
1. *Connectors* contain the tags and containers to query.

For example, typically these tags define dynamically allocated network and IP addresses for which you cannot create access control rules. Persisted feeds from the connectors are stored on the dynamic attributes connector for fast access.

2. Tag information is persisted on the dynamic attributes connector where you create *dynamic attribute filters* that define which information is important to use in access control rules.

   For example, if AWS defines networks for the Accounting and Finance Departments virtual machines, you can create a dynamic attributes filter that specifies only the Finance network.

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



CHAPTER 2

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 5
- Create an Adapter, on page 11
- Create Dynamic Attributes Filters, on page 16

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 2: 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 12.

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.

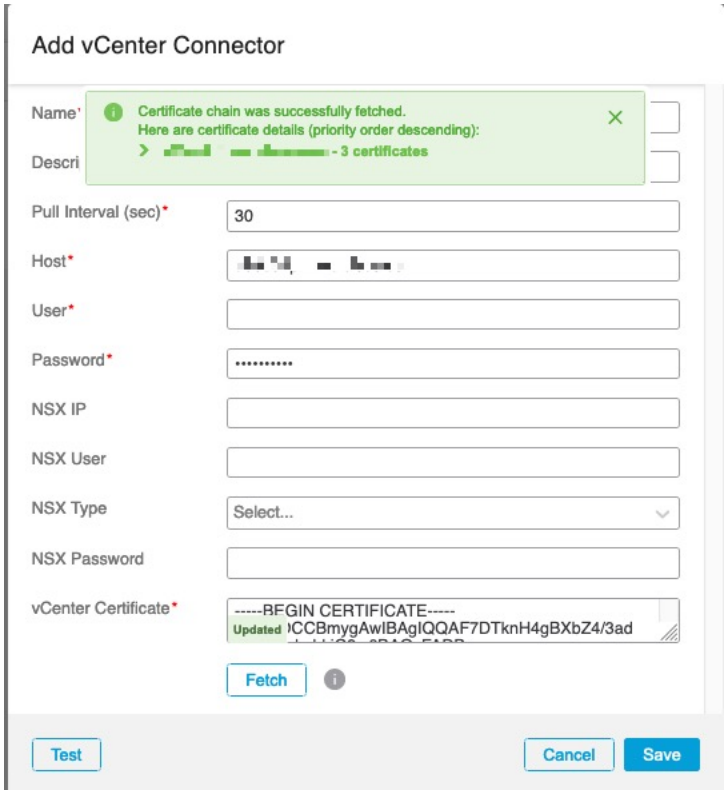
No other information is required to fetch the certificate CA chain.

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 12.

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 11

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**.

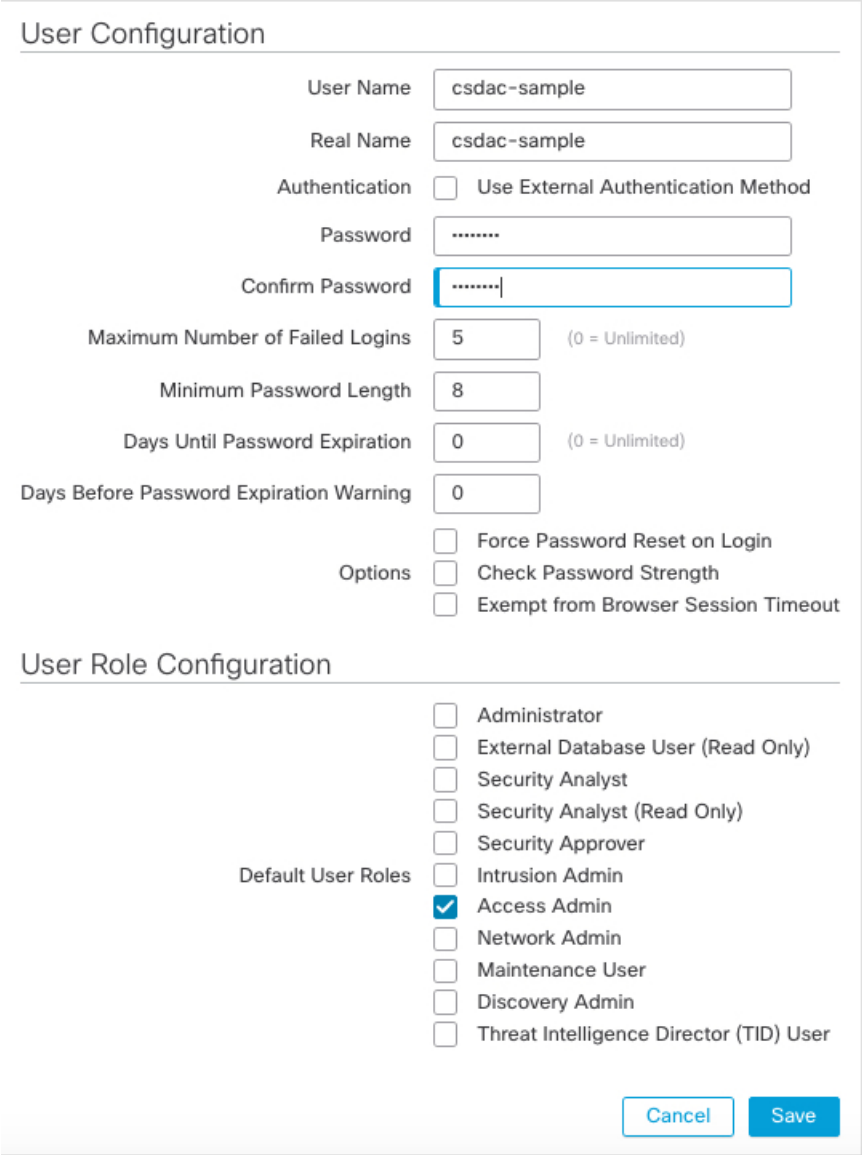
Step 3 Click **Create User**.

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
   ```

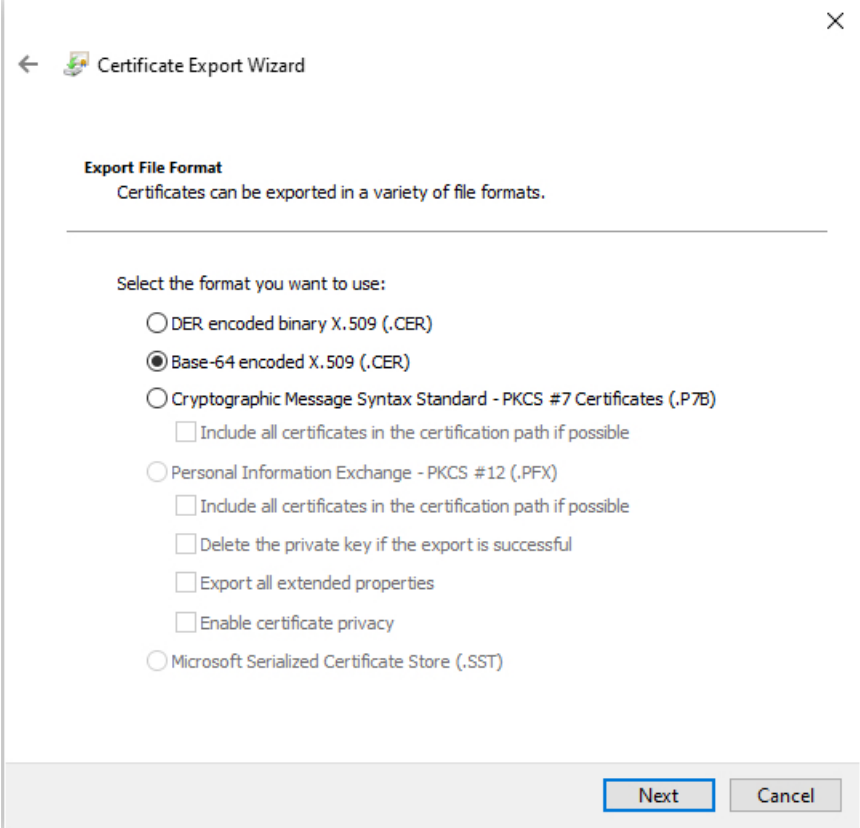
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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



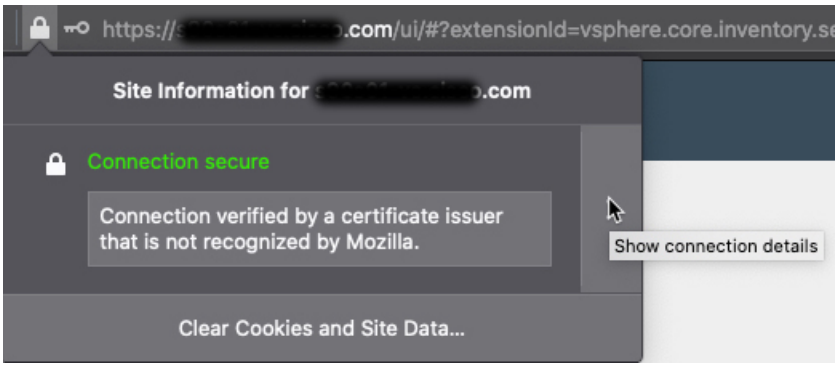
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

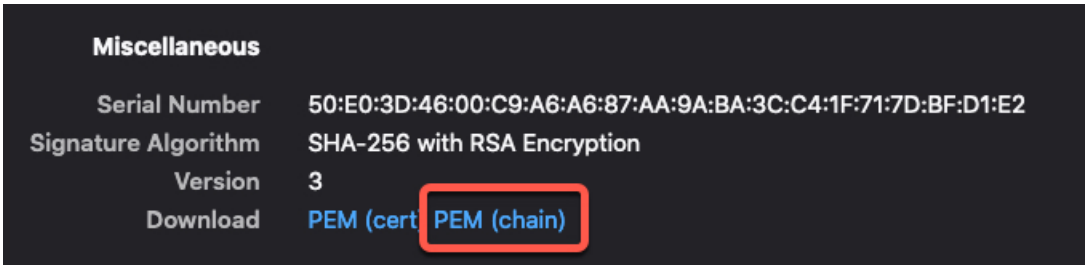
Get a Certificate Chain—Windows Firefox

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 11.

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 12.

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, on page 21.

Before you begin

Complete all of the following tasks:

- Install Prerequisite Software
- Create a Connector, on page 5
- Create an Adapter, on page 11

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.

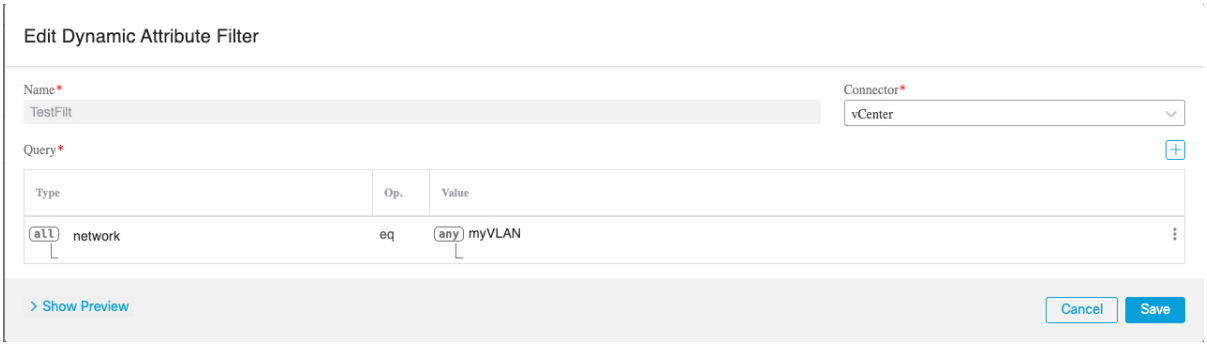
a) Log in to the FMC as a user with the Network Admin role at minimum.
b) Click **Objects** > **Object Manager**.
c) In the left pane, click **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

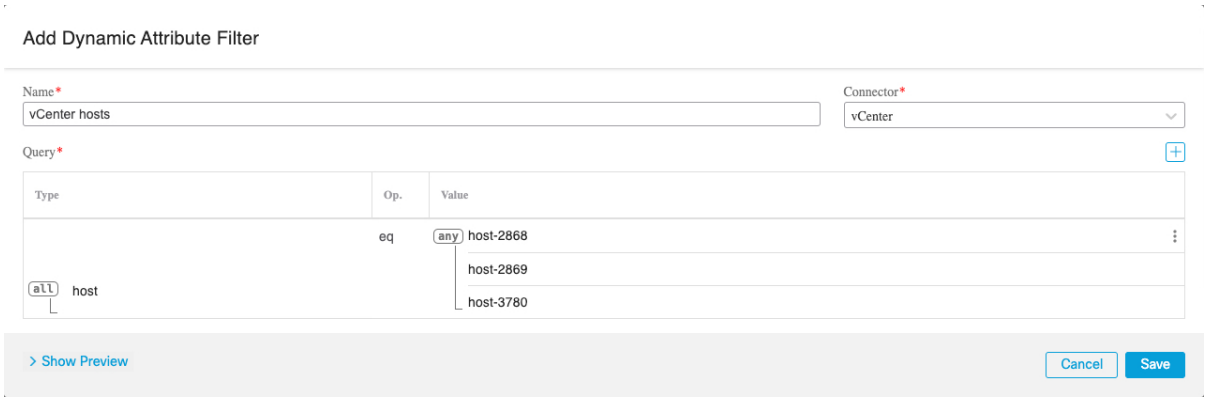
This topic provides some examples of setting up dynamic attribute filters.

Examples: vCenter

The following example shows one criterion: a VLAN.

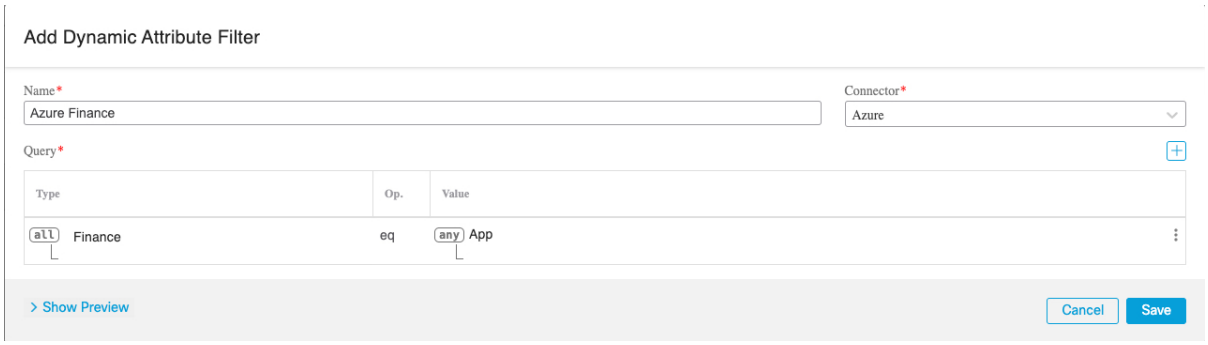


The following example shows three criteria that are joined with OR: the query matches any of three hosts.



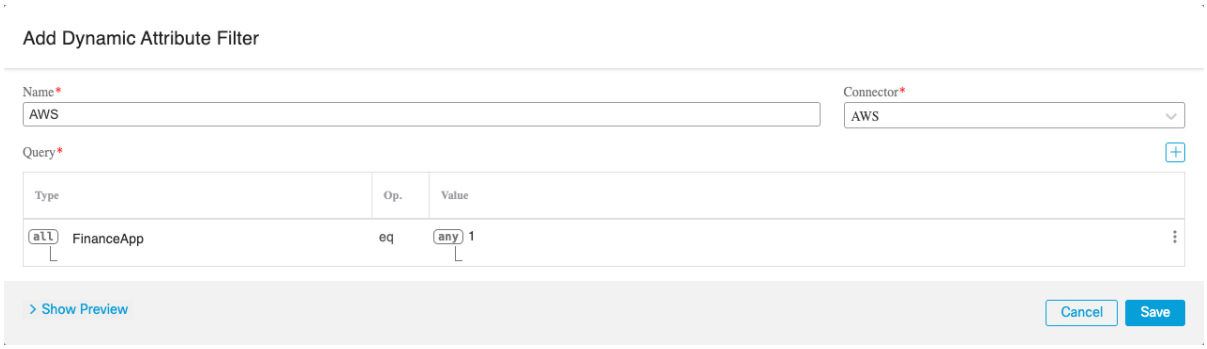
Example: Azure

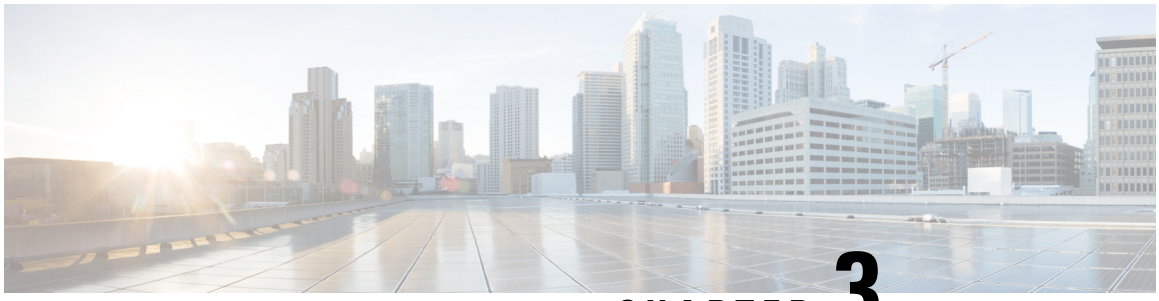
The following example shows one criterion: a server tagged as a Finance app.



Example: AWS

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





CHAPTER 3

Use Dynamic Objects in Access Control Policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the FMC 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 a defined On-Prem Firewall Management Center or adapter after you save a dynamic attributes filter on the connector.

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

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

Create Access Control Rules Using Dynamic Attributes Filters

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

Before you begin

Create dynamic attributes filters as discussed in Create Dynamic Attributes Filters, on page 16.

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

Step 1 Log in to the FMC.

Step 2 Click **Policies** > **Access Control**.

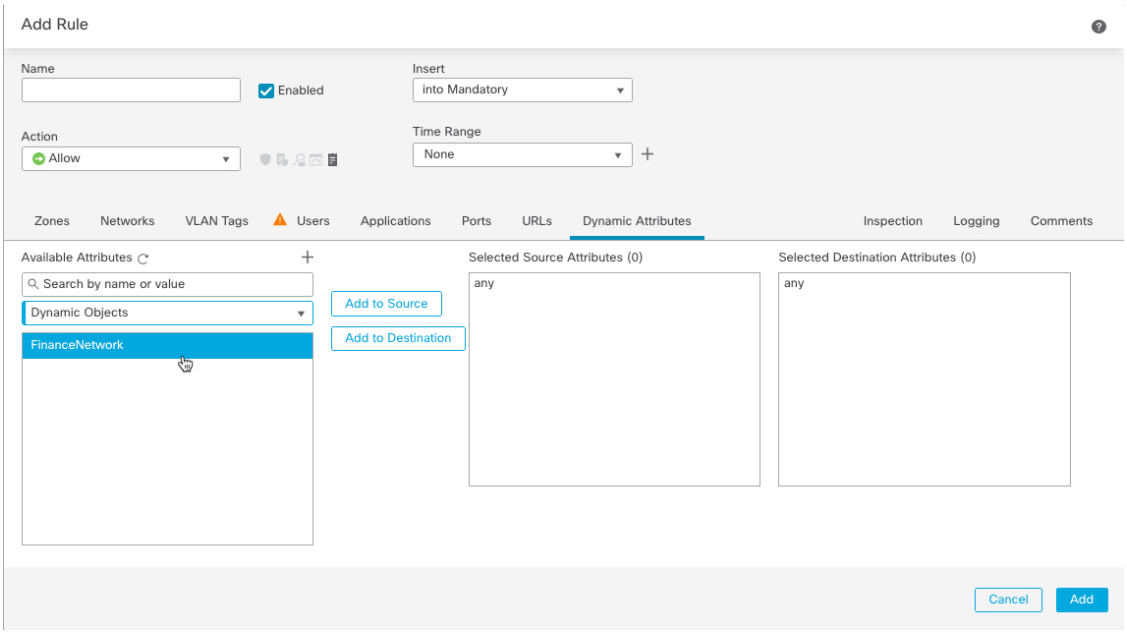
Step 3 Click **Edit** (✎) next to an access control policy.

Step 4 Click **Add Rule**.

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

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

The following figure shows an example.



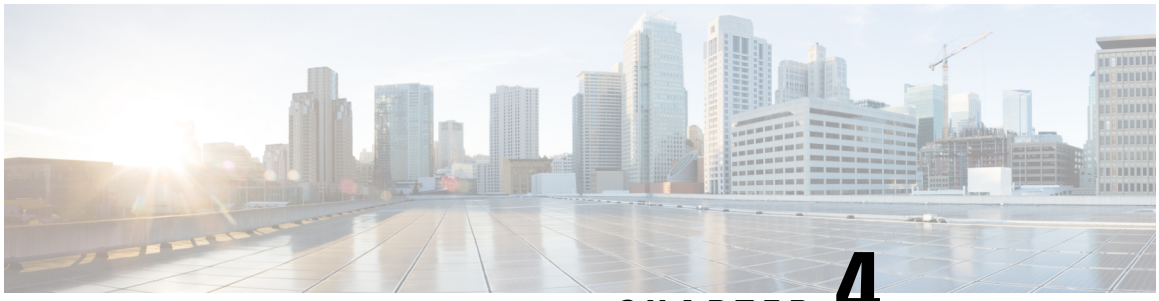
The preceding example shows a dynamic object named `FinanceNetwork` that corresponds to the dynamic attribute filter created in the Dynamic Attributes Connector.

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

Step 8 Add other conditions to the rule if desired.

What to do next

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



CHAPTER 4

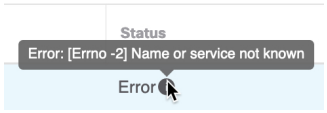
Troubleshoot the Dynamic Attributes Connector

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

Troubleshoot Error Messages

Problem: Name or service not known error

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



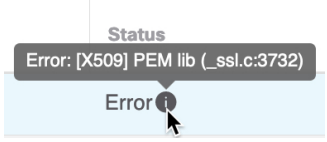
Solution: Edit the connector or adapter and check for:

- A trailing slash on a host name
- (FMC adapter only.) A scheme at the beginning of a host name (for example, `https://`)
- Verify the password is correct
- For an FMC adapter, verify the contents of the **FMC Server Certificate** field.

  For more information, see Manually Get a Certificate Authority (CA) Chain, on page 12.

Problem: [X509 PEM lib]

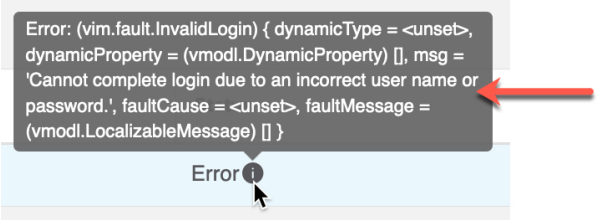
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and check the CA chain. For more information, see Manually Get a Certificate Authority (CA) Chain, on page 12.

Problem: Incorrect username or password

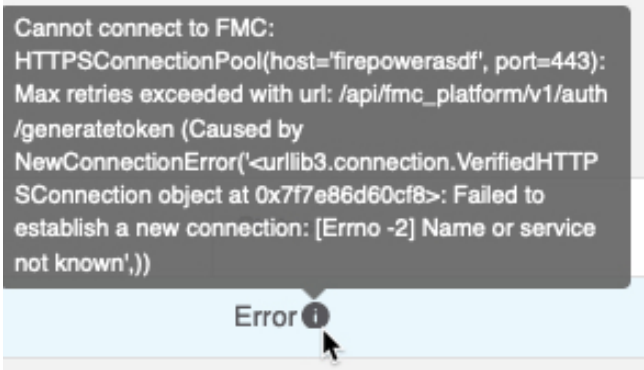
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.

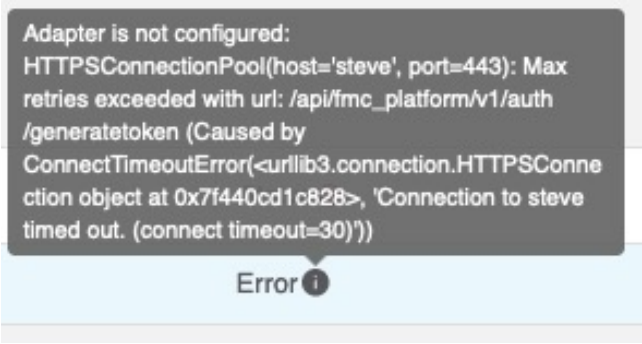


Solution: Edit the connector and change the user name or password.

Problem: Timeout or max retries error for an adapter

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





Solution: Do all of the following:

- Verify the management center is running.
- Verify the contents of the **FMC Server Certificate** field.
- Make sure the value you entered in the **IP** field exactly matches the certificate's Common Name.

For more information, see Manually Get a Certificate Authority (CA) Chain, on page 12.

Troubleshooting Tools

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 ~/csdac/app
sudo ./muster-cli status
```

Sample output follows:

```
============================== CORE SERVICES ==============================
      Name                      Command                  State    Ports
-----------------------------------------------------------------------------------------------------
muster-bee     ./docker-entrypoint.sh run ...   Up             50049/tcp, 50050/tcp

muster-etcd    etcd                             Up             2379/tcp, 2380/tcp

muster-ui      /docker-entrypoint.sh runs ...   Up (healthy)
0.0.0.0:443->8443/tcp,:::443->8443/tcp
muster-ui-backend   ./docker-entrypoint.sh run ...   Up             50031/tcp

========================== CONNECTORS AND ADAPTERS ==========================
          Name                          Command               State     Ports
-------------------------------------------------------------------------------
muster-adapter-fmc.1         ./docker-entrypoint.sh run ...   Up      50070/tcp
muster-connector-vcenter.1   ./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 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
/csdac/app/ts-bundle-*timestamp***/info**	`etcd` database contents
/csdac/app/ts-bundle-*timestamp***/logs**	Container log files
/csdac/app/ts-bundle-*timestamp***/status.log**	Container status, versions, and image status

Verify dynamic objects on the

To verify your connectors and adapters are creating objects on the FMC, you can use the following command on the FMC as an administrator:

```
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.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": []
}
```

Example: Unsuccessful object creation (in this case because the adapter user has insufficient privileges):

```
26-Aug-2021 12:47:50.440,[INFO],(DefenseCenterServiceImpl.java:1442)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-2
** REST Request [ CSM ]
** ID : 58566831-7532-4d61-a579-2bbc3c325b2f
** URL: POST /audit
{
  "version": "7.1.0",
  "requestId": "58566831-7532-4d61-a579-2bbc3c325b2f",
  "data": {
    "userName": "csdac-centos7",
    "subsystem": "API",
    "message": "GET
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/
object/dynamicobjects/vCenter___CentOS_7__4 Forbidden (403) - The server understood the
request, but is refusing to fulfill it",
    "sourceIP": "192.0.2.103",
    "domainUuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f",
    "time": "1629982070404"
  },
  "deleteList": []
}
```

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.

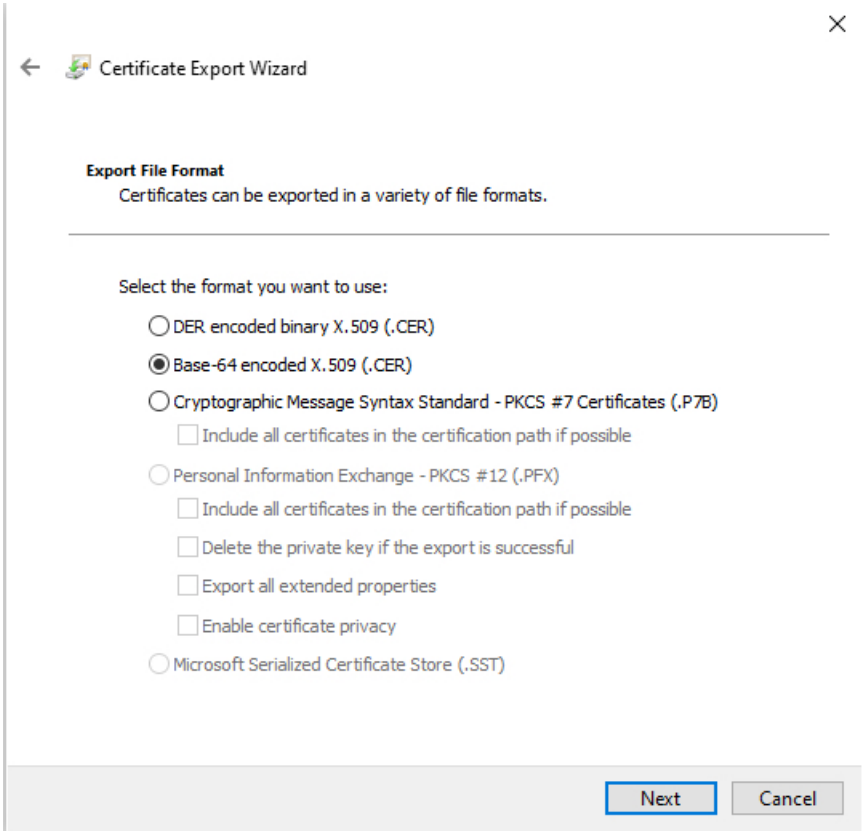
Get a Certificate Chain—Windows Chrome

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.



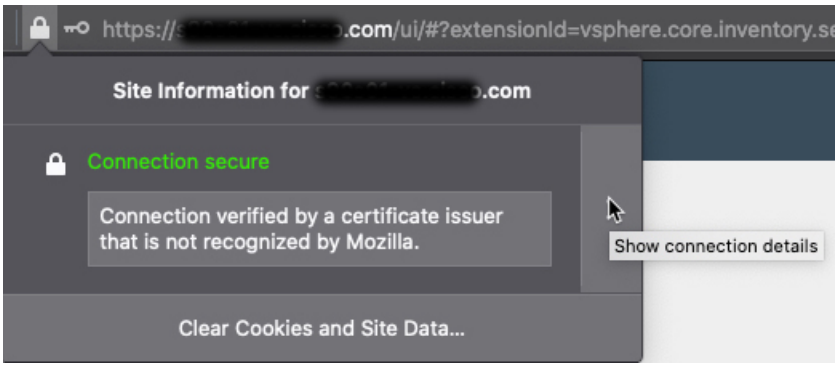
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

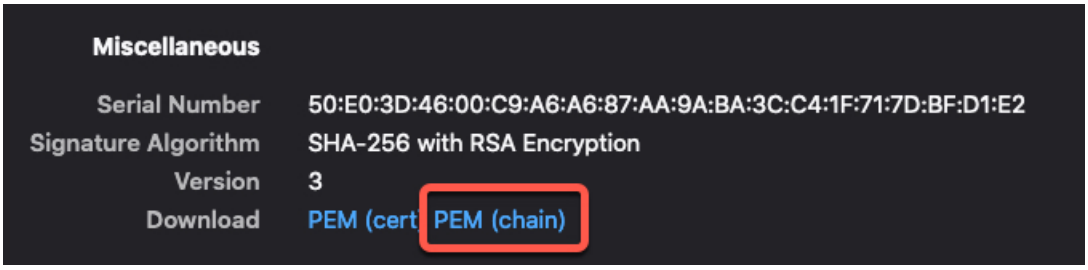
Get a Certificate Chain—Windows Firefox

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

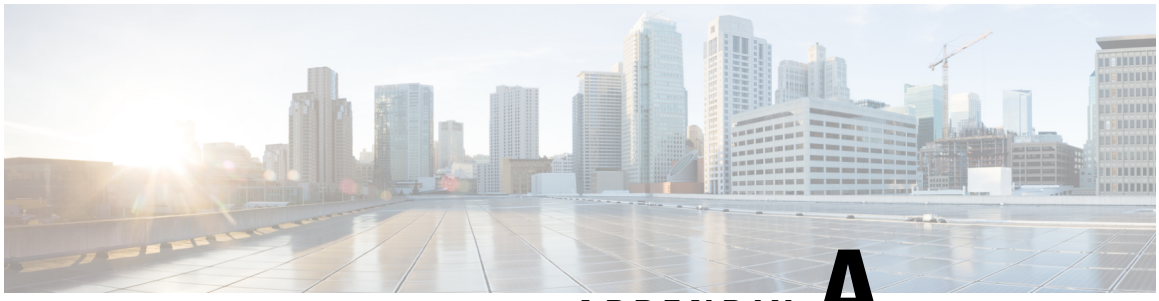
1. Log in to vCenter or the FMC using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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.



APPENDIX A

Security and Internet Access

Lists of URLs used by the dynamic attributes connector when communicating with cloud service providers and the FMC.

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 FMC reside on the same network, you can connect the FMC 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 FMC and with external servers.

Table 3: Dynamic Attributes Connector FMC 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

URL	Reason
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

Dynamic Attributes Connector AWS access requirements

The dynamic attributes connector calls built-in SDK methods to get instance information. These methods internally query service endpoint URLs based on the specified region in the .dynamic attributes connector They are documented in AWS website https://docs.aws.amazon.com/general/latest/gr/ec2-service.html.

Dynamic Attributes Connector Azure access requirements

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