Cisco Secure Dynamic Attributes Connector Configuration Guide

First Published: 2021-06-01
Last Modified: 2022-01-25

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
Full Cisco Trademarks with Software License

CHAPTER 1
About the Cisco Secure Dynamic Attributes Connector 1
About the Cisco Dynamic Attributes Connector

CHAPTER 2
Configure the Cisco Secure Dynamic Attributes Connector 5
Supported Operating Systems and Third-Party Software 5
Install Prerequisite Software 5
Install Prerequisite Software—Ubuntu 6
Install the Cisco Secure Dynamic Attributes Connector 7
Create a Connector 10
Create an AWS Connector 10
Create an Azure Connector 11
How to Create a vCenter Connector 12
Create a FMC Adapter 13
Create an FMC User for the Dynamic Attributes Connector 13
Manually Get a Certificate Authority (CA) Chain 15
How to Create an FMC Adapter 17
Create Dynamic Attribute Filters 18
Dynamic Attribute Filter Examples 20

CHAPTER 3
Use Dynamic Objects in Access Control Policies 23
About Dynamic Objects in Access Control Rules 23
Create Access Control Rules Using Dynamic Attribute Filters 23
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 Firepower Management Center 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, on page 1

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.

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.

We currently support:

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

- Amazon Web Services (AWS) service tags
  For more information, see a resource like Tagging AWS resources on the Amazon documentation site

- 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

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.
As shown in the figure:

1. **Connectors** (currently, AWS, Azure, and vCenter) contain the tags and containers to query.
   Typically, these tags define dynamically allocated network and IP addresses (for example) that aren't possible to write access control rules for. 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 vCenter defines networks for the Accounting and Finance Departments virtual machines, you can create a filter that specifies only the Finance network.

3. The FMC 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.
Related Topics
   Install Prerequisite Software, on page 5
CHAPTER 2

Configure the Cisco Secure Dynamic Attributes Connector

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

See the following topics for more information:

• Supported Operating Systems and Third-Party Software, on page 5
• Install Prerequisite Software, on page 5
• Install the Cisco Secure Dynamic Attributes Connector, on page 7
• Create a Connector, on page 10
• Create a FMC Adapter, on page 13
• Create Dynamic Attribute Filters, on page 18

Supported Operating Systems and Third-Party Software

The dynamic attributes connector requires the following:

• Ubuntu 18.04
• Python 3.6.x
• Ansible 2.9 or later

If you wish to use vCenter attributes, we also require:

• vCenter 6.7
• VMware Tools must be installed on the virtual machine

Install Prerequisite Software

Before you begin

Make sure you have physical or virtual set up and that the system that can communicate with your FMC. For details, see Supported Operating Systems and Third-Party Software, on page 5.
Step 1  
(Optional.) Use a text editor to edit /etc/environment to export the following variables to enable communication with the internet if your Ubuntu machine is behind an internet proxy.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>export http_proxy</td>
<td>Use with an HTTP proxy.</td>
</tr>
<tr>
<td></td>
<td>user:pass@host-or-ip:port</td>
</tr>
<tr>
<td>export https_proxy</td>
<td>Use this with an HTTPS proxy.</td>
</tr>
<tr>
<td></td>
<td>user:pass@host-or-ip:port</td>
</tr>
<tr>
<td>export no_proxy</td>
<td>Remove the proxy configuration.</td>
</tr>
<tr>
<td></td>
<td>export no_proxy=&quot;localhost,127.0.0.1&quot;</td>
</tr>
</tbody>
</table>

Examples:

HTTP proxy without authentication:

```
vi /etc/environment
export http_proxy="myproxy.example.com:8181"
```

HTTPS proxy with authentication:

```
vi /etc/environment
export https_proxy="ben.smith:bens-password@myproxy.example.com:8181"
```

Step 2  
Use a different command window to confirm the settings:

```
env grep | proxy
```

Example result:

```
http_proxy=myproxy.example.com:8181
```

Step 3  
Continue with one of the following sections.

Related Topics

Install Prerequisite Software—Ubuntu, on page 6

Install Prerequisite Software—Ubuntu

Step 1  
Make sure Docker is not installed and uninstall it if it is.

```
docker --version
```

If Docker is installed, uninstall it as discussed in Uninstall Docker Engine on Ubuntu.

Step 2  
Update your repositories.

```
sudo apt -y update && sudo apt -y upgrade
```

Step 3  
Confirm your Python version.

```
/usr/bin/python3 --version
```
If the version is earlier than 3.6, you must install version 3.6.x.

Step 4  Install Python 3.6.
       sudo apt -y install python3.6

Step 5  Install the common libraries.
       sudo apt -y install software-properties-common

Step 6  Install Ansible.
       sudo apt-add-repository -y -u ppa:ansible/ansible && sudo apt -y install ansible

Step 7  Verify the Ansible version.
       ansible --version

       An example follows.
       ansible --version
       ansible 2.9.19
          config file = /etc/ansible/ansible.cfg
          configured module search path = [u'/home/admin/.ansible/plugins/modules',
                                         u'/usr/share/ansible/plugins/modules']
          ansible python module location = /usr/lib/python2.7/dist-packages/ansible
          executable location = /usr/bin/ansible
          python version = 2.7.17 (default, Feb 27 2021, 15:10:58) [GCC 7.5.0]

       Note  It's normal for Ansible to reference Python 2.x as the preceding output shows. The connector will still use Python 3.6.

What to do next

Install the connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 7.

To optionally stop using a proxy with the dynamic attributes connector, edit /etc/environment and remove the proxy configuration.

Install the Cisco Secure Dynamic Attributes Connector

About the installation

This topic discusses installing the Cisco Secure Dynamic Attributes Connector. You must install the connector as a user with sudo privileges but you can run the connector as a non-privileged user.

Before you begin

Make sure your system has the following prerequisite software:

- Ubuntu 18.04
- Python 3.6.x
- Ansible 2.9 or later

If you wish to use vCenter attributes, we also require:
Install the Cisco Secure Dynamic Attributes Connector

- vCenter 6.7
- VMware Tools must be installed on the virtual machine

To install prerequisite software, see Install Prerequisite Software, on page 5.

View the Readme and Release Notes

For the latest installation information, see the following:

Readme: https://galaxy.ansible.com/cisco/csdac

Release Notes: Cisco Secure Dynamic Attributes Connector Release Notes

Get the Dynamic Attributes Connector software

To get the latest version of the dynamic attributes connector software, run the following command:

```bash
ansible-galaxy collection install cisco.csdac
```

Install the muster service

The muster service is another name for the dynamic attributes connector.

Run the following command from the `~/.ansible/collections/ansible_collections/cisco/csdac` directory.

```bash
ansible-playbook default_playbook.yml [--ask-become-pass] [--extra-vars "vars"]
```

**Syntax Description**

- `--ask-become-pass` Prompts you to enter the `sudo` password. Required if sudo is enabled on your machine.
The following optional extra variables enable the dynamic attributes connector to use a proxy. The value you use must match the value in /etc/environment, which you configured as discussed in Install Prerequisite Software, on page 5.

- csdac_proxy_enabled=true
- csdac_http_proxy_url=http://PROXY_URL
  csdac_https_proxy_url=PROXY_URL

The following optional extra variables create a self-signed certificate you can use to securely connect to the dynamic attributes connector. If you omit these parameters, the dynamic attributes connector uses a default certificate.

- csdac_certificate_domain
domain name for autogenerated certificate. Default value is autodetected hostname of the host (detected by ansible)
- csdac_certificate_country_name
  Two-letter country code. (Default is US)
- csdac_certificate_organization_name
  Organization name. (Default is Cisco)
- csdac_certificate_organization_unit_name
  Organizational unit name (Default is Cisco)

---

**Example installation with a default certificate**

For example, to install the software with default options:

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass
```

**Example installation with optional certificate**

For example, to install the software with an optional certificate:

```
ansible-galaxy collection install cisco.csdac
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-playbook default_playbook.yml --ask-become-pass --extra-vars
''"csdac_certificate_domain-domain.example.com csdac_certificate_country_name-US
csdac_certificate_organization_name=Cisco
csdac_certificate_organization_unit_name=Engineering"
```

After you create the certificate, import it into the web browser you'll use to access the connector. The certificate is created in the ~/csdac/app/config/certs directory.

**View the installation log**

The installation log is located as follows:
Use your certificate to connect to the dynamic attributes connector

If you have a certificate and key, put them in the ~/.csdac/app/config/certs directory on your Ubuntu machine.

After you perform the preceding task, restart the dynamic attributes connector's Docker container by entering the following command:

docker restart muster-ui

Log in to the connector

1. Access the dynamic attributes connector at https://ip-address

2. Log in.

   The initial login is username admin, password admin. You are required to change the password the first time you log in.

Create a Connector

A connector is an interface with a cloud service (currently, Microsoft Azure, Amazon Web Services (AWS), or VMware vCenter). The connector retrieves network information from the cloud service so the network information can be used in access control policies on the FMC.

See one of the following sections for more information.

Related Topics

- Create an AWS Connector, on page 10
- Create an Azure Connector, on page 11
- Troubleshoot Issues with the Cisco Secure Dynamic Attributes Connector, on page 25
- How to Create a vCenter Connector, on page 12

Create an AWS Connector

Step 1 Log in to the dynamic attributes connector.

Step 2 Click Connectors.

Step 3 Do any of the following:

- Add a new connector: click Add (+), then click AWS.

- Edit or delete a connector: Click More ( ), then click Edit or Delete at the end of the row.

Step 4 Enter the following information.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required.) Enter a name to uniquely identify this connector.</td>
</tr>
</tbody>
</table>
Configure the Cisco Secure Dynamic Attributes Connector

## Create an Azure Connector

### What to do next

Create a FMC Adapter, on page 13

---

### Create an Azure Connector

**Step 1** Log in to the dynamic attributes connector.

**Step 2** Click Connectors.

**Step 3** Do any of the following:

- Add a new connector: click Add (＋), then click Azure.

- Edit or delete a connector: Click More (⋯), then click Edit or Delete at the end of the row.

**Step 4** Enter the following information.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>(Required.) Enter a name to uniquely identify this connector.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Optional description.</td>
</tr>
<tr>
<td><strong>Pull Interval</strong></td>
<td>(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure.</td>
</tr>
<tr>
<td><strong>Subscription Id</strong></td>
<td>(Required.) Enter your Azure subscription ID.</td>
</tr>
<tr>
<td><strong>Tenant Id</strong></td>
<td>(Required.) Enter your tenant ID.</td>
</tr>
<tr>
<td><strong>Client Id</strong></td>
<td>(Required.) Enter your client ID.</td>
</tr>
<tr>
<td><strong>Client Secret</strong></td>
<td>(Required.) Enter your client secret.</td>
</tr>
</tbody>
</table>
Step 5  Click Save.
Step 6  Make sure Ok is displayed in the Status column.

What to do next
Create a FMC Adapter, on page 13

How to Create a vCenter Connector

Before you begin
If you use non-trusted certificates to communicate with vCenter, see Manually Get a Certificate Authority (CA) Chain, on page 15.

Step 1  Log in to the dynamic attributes connector.
Step 2  Do any of the following:
   - Add a new connector: click Add (+), then click vCenter.
   - Edit or delete a connector: Click More (⋮), then click Edit or Delete at the end of the row.
Step 3  Enter the following information.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required.) Enter a name to uniquely identify this connector.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>Pull Interval</td>
<td>(Default 30 seconds.) Interval at which IP mappings are retrieved from vCenter.</td>
</tr>
<tr>
<td>Host</td>
<td>(Required.) Enter any of the following:</td>
</tr>
<tr>
<td></td>
<td>• vCenter's fully qualified host name</td>
</tr>
<tr>
<td></td>
<td>• vCenter's IP address</td>
</tr>
<tr>
<td></td>
<td>• (Optional.) A port</td>
</tr>
<tr>
<td></td>
<td>Do not enter a scheme (such as https://) or trailing slash.</td>
</tr>
<tr>
<td></td>
<td>For example, myvcenter.example.com or 192.0.2.100:9090</td>
</tr>
<tr>
<td>User</td>
<td>(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required.) Enter the user's password.</td>
</tr>
<tr>
<td>NSX IP</td>
<td>If you use vCenter Network Security Visualization (NSX), enter its IP address.</td>
</tr>
<tr>
<td>NSX User</td>
<td>Enter the user name of an NSX user with the Auditor role at minimum.</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NSX Type</td>
<td>Enter NSX-T.</td>
</tr>
<tr>
<td>NSX Password</td>
<td>Enter the NSX user's password.</td>
</tr>
<tr>
<td>vCenter Certificate</td>
<td>Paste the certificate authority (CA) chain you got as discussed in <a href="#">Manually Get a Certificate Authority (CA) Chain</a>, on page 15.</td>
</tr>
</tbody>
</table>

**Step 4**  
Click **Test** and make sure **Test connection succeeded** is displayed before you save the connector.

**Step 5**  
Click **Save**.

---

**What to do next**

[Create a FMC Adapter](#), on page 13

---

**Create a FMC Adapter**

An *adapter* is a secure connection to a 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 an FMC host name; creating the adapter requires a user name, password, and other information.

**Related Topics**

- [Create an FMC User for the Dynamic Attributes Connector](#), on page 13
- Fetch the Certificate Authority (CA) Chain
- [How to Create an FMC Adapter](#), on page 17
- [Troubleshoot Issues with the Cisco Secure Dynamic Attributes Connector](#), on page 25

---

**Create an FMC User for the Dynamic Attributes Connector**

**Before you begin**

We recommend you create an 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:
The following figure shows an example.

<table>
<thead>
<tr>
<th>User Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong></td>
</tr>
<tr>
<td><strong>Real Name</strong></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
</tr>
<tr>
<td><strong>Maximum Number of Failed Logins</strong></td>
</tr>
<tr>
<td><strong>Minimum Password Length</strong></td>
</tr>
<tr>
<td><strong>Days Until Password Expiration</strong></td>
</tr>
<tr>
<td><strong>Days Before Password Expiration Warning</strong></td>
</tr>
<tr>
<td><strong>Options</strong></td>
</tr>
<tr>
<td>Force Password Reset on Login</td>
</tr>
<tr>
<td>Check Password Strength</td>
</tr>
<tr>
<td>Exempt from Browser Session Timeout</td>
</tr>
<tr>
<td><strong>User Role Configuration</strong></td>
</tr>
<tr>
<td>Administrator</td>
</tr>
<tr>
<td>External Database User (Read Only)</td>
</tr>
<tr>
<td>Security Analyst</td>
</tr>
<tr>
<td>Security Analyst (Read Only)</td>
</tr>
<tr>
<td>Security Approver</td>
</tr>
<tr>
<td>Intrusion Admin</td>
</tr>
<tr>
<td>Access Admin</td>
</tr>
<tr>
<td>Network Admin</td>
</tr>
<tr>
<td>Maintenance User</td>
</tr>
<tr>
<td>Discovery Admin</td>
</tr>
<tr>
<td>Threat Intelligence Director (TID) User</td>
</tr>
<tr>
<td><strong>Default User Roles</strong></td>
</tr>
</tbody>
</table>

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

**What to do next**

See How to Create an FMC Adapter, on page 17
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.
- The FMC

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

- How to Create a vCenter Connector, on page 12
- Create a FMC Adapter, on page 13

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.
   
   ```bash
   security verify-cert -P url[:port]
   ```
   
   where url is the URL (including scheme) to vCenter or FMC. For example:

   ```bash
   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:

   ```bash
   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.

![Show connection details](image)

4. Click More Information.
5. Click View Certificate.
6. If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA.
7. Scroll to the Miscellaneous section.
8. Click PEM (chain) in the Download row. The following figure shows an example.

![Miscellaneous](image)

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 an FMC User for the Dynamic Attributes Connector](#), on page 13.

---

**Step 1** Log in to the dynamic attributes connector if you have not already done so.
**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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required.) Enter a unique name to identify this adapter.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional description of the adapter.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the FMC domain in which to create dynamic objects. Leave the field blank to create dynamic objects in the Global domain. For example, <strong>Global/MySubdomain</strong></td>
</tr>
<tr>
<td>IP</td>
<td>(Required.) Enter your FMC'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.</td>
</tr>
<tr>
<td>Port</td>
<td>(Required.) Enter the TLS port used by your FMC.</td>
</tr>
<tr>
<td>User</td>
<td>(Required.) Enter the name of an FMC user with the Network Admin role at minimum.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required.) Enter the user's password.</td>
</tr>
<tr>
<td>Secondary IP</td>
<td>(High availability only.) Enter the secondary FMC'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.</td>
</tr>
<tr>
<td>Secondary Port</td>
<td>(High availability only.) Enter the TLS port used by your secondary FMC.</td>
</tr>
<tr>
<td>Secondary User</td>
<td>(High availability only.) Enter the name of a secondary FMC user with the Network Admin role at minimum.</td>
</tr>
<tr>
<td>Secondary Password</td>
<td>(High availability only.) Enter the user's password.</td>
</tr>
<tr>
<td>FMC Server Certificate</td>
<td>Paste the certificate authority (CA) chain you got as discussed in Manually Get a Certificate Authority (CA) Chain, on page 15.</td>
</tr>
</tbody>
</table>

Step 5

Click Save.

Related Topics

Troubleshoot Issues with the Cisco Secure Dynamic Attributes Connector, on page 25

Create Dynamic Attribute Filters

Dynamic attributes filters that you define using the Cisco Secure Dynamic Attributes Connector are exposed in the FMC as dynamic attributes 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.
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, see:

- Tagging AWS resources on the Amazon documentation site

For more information about access control rules, see Create Access Control Rules Using Dynamic Attribute Filters, on page 23.

**Before you begin**

Complete all of the following tasks:

- Install Prerequisite Software, on page 5
- Create a Connector, on page 10
- Create a FMC Adapter, on page 13

---

**Step 1**

Log in to the Dynamic Attributes Connector.

**Step 2**

Click **Dynamic Attributes Filters**.

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 3**

Enter the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the FMC Object Manager (External Attributes &gt; Dynamic Object).</td>
</tr>
<tr>
<td>Connector</td>
<td>From the list, click the name of a connector to use.</td>
</tr>
</tbody>
</table>
| Query    | • Add a new filter query: Click **Add**
              • Edit or delete an existing filter query: Click **More**, then click **Edit** or **Delete** at the end of the row. |

**Step 4**

To add or edit a query, enter the following information.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>Click a key from the list. Keys are fetched from the connector.</td>
</tr>
</tbody>
</table>
**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](image)

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure Finance</td>
<td>Azure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>str</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Example: AWS

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>AWS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>str</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
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, on page 23
- Create Access Control Rules Using Dynamic Attribute Filters, on page 23

About Dynamic Objects in Access Control Rules

A dynamic object is automatically pushed from the dynamic attributes connector to a defined FMC 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.

Create Access Control Rules Using Dynamic Attribute 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 Attribute Filters, on page 18.

Step 1 Log in to the FMC as a user with at least the Network Administrator role.
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 *Firepower Management Center Configuration Guide.* (link to chapter)
Troubleshoot the Dynamic Attributes Connector

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

- Troubleshoot Issues with the Cisco Secure Dynamic Attributes Connector, on page 25
- Troubleshooting Tools, on page 26
- Manually Get a Certificate Authority (CA) Chain, on page 28

Troubleshoot Issues with the Cisco Secure Dynamic Attributes Connector

This topic has suggested solutions to issues you might find while using the dynamic attributes connector.

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 different.

![Error](Error.png)

Solution: Edit the connector or adapter and check for:

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

For more information, see Manually Get a Certificate Authority (CA) Chain, on page 15.

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 15.

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 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 15.

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Command</th>
<th>State</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>muster-bee</td>
<td>./docker-entrypoint.sh run</td>
<td>Up</td>
<td>50049/tcp, 50050/tcp</td>
</tr>
<tr>
<td>muster-etcd</td>
<td>etcd</td>
<td>Up</td>
<td>2379/tcp, 2380/tcp</td>
</tr>
<tr>
<td>muster-ui</td>
<td>/docker-entrypoint.sh runs</td>
<td>Up (healthy)</td>
<td>0.0.0.0:443-&gt;8443/tcp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>:::443-&gt;8443/tcp</td>
</tr>
<tr>
<td>muster-ui-backend</td>
<td>./docker-entrypoint.sh run</td>
<td>Up</td>
<td>50031/tcp</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Location</th>
<th>What it contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>/csdac/app/ts-bundle-timestamp/info</td>
<td>etcd database contents</td>
</tr>
<tr>
<td>/csdac/app/ts-bundle-timestamp/logs</td>
<td>Container log files</td>
</tr>
<tr>
<td>/csdac/app/ts-bundle-timestamp/status.log</td>
<td>Container status, versions, and image status</td>
</tr>
</tbody>
</table>
Verify dynamic objects on FMC

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

```bash
sudo tail f /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
```

**Example: Successful object creation**

```bash
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-bbccbf52a6275
** URL: POST /audit
{
   "version": "7.1.0",
   "requestId": "18b25356-fd6b-4cc4-8d27-bbccbf52a6275",
   "data": {
      "userName": "csdac-centos7",
      "subsystem": "API",
      "message": "POST
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e5-8169-6d9ed49b625f/object/dynamicobjects
Created (201) - The request has been fulfilled and resulted in a new
resource being created",
      "sourceIP": "192.0.2.103",
      "domainUuid": "e276abec-e0f2-11e5-8169-6d9ed49b625f",
      "time": "1629981695431"
   }
},
"deleteList": []
}
```

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

```bash
26-Aug-2021 12:47:50.440, [INFO], (DefenseCenterServiceImpl.java:1442)
** REST Request [ CSM ]
** ID : 58566831-7532-4d61-a579-2bbcc3c325b2f
** URL: POST /audit
{
   "version": "7.1.0",
   "requestId": "58566831-7532-4d61-a579-2bbcc3c325b2f",
   "data": {
      "userName": "csdac-centos7",
      "subsystem": "API",
      "message": "GET
https://myfmc.example.com/api/fmc_config/v1/domain/e276abec-e0f2-11e5-8169-6d9ed49b625f/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-e0f2-11e5-8169-6d9ed49b625f",
      "time": "1629981695431"
   }
},
"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.
- The FMC

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

- How to Create a vCenter Connector, on page 12
- Create a FMC Adapter, on page 13

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.

   ![Certificate Information](image)

9. Save the file.
10. Repeat these tasks for both vCenter and the FMC.
Manually Get a Certificate Authority (CA) Chain
Security and Internet Access

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

- Security Requirements, on page 33
- Internet Access Requirements, on page 33

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 Firepower Management Center (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 1: Dynamic Attributes Connector FMC access requirements**

<table>
<thead>
<tr>
<th>URL</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https://fmc-ip/api/fmc_platform/v1/auth/generatetoken</code></td>
<td>Authentication</td>
</tr>
<tr>
<td><code>https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects</code></td>
<td>GET and POST dynamic objects</td>
</tr>
</tbody>
</table>
Table 2: Dynamic Attributes Connector vCenter access requirements

<table>
<thead>
<tr>
<th>URL</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://vcenter-ip/rest/com/vmware/cis/session">https://vcenter-ip/rest/com/vmware/cis/session</a></td>
<td>Authentication</td>
</tr>
<tr>
<td><a href="https://vcenter-ip/rest/vcenter/vm">https://vcenter-ip/rest/vcenter/vm</a></td>
<td>Get VM information</td>
</tr>
</tbody>
</table>

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 CSDAC UI. They are documented in AWS website [https://docs.aws.amazon.com/general/latest/gr/ec2-service.html](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 [https://login.microsoft.com](https://login.microsoft.com) (for authentication) and [https://management.azure.com](https://management.azure.com) (to get instance information).