Cisco Secure Dynamic Attributes Connector Configuration Guide 1.1

First Published: 2021-06-01

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	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No

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 IP addresses

  For more information, see Office 365 URLs and IP address ranges on docs.microsoft.com.

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

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

Related Topics

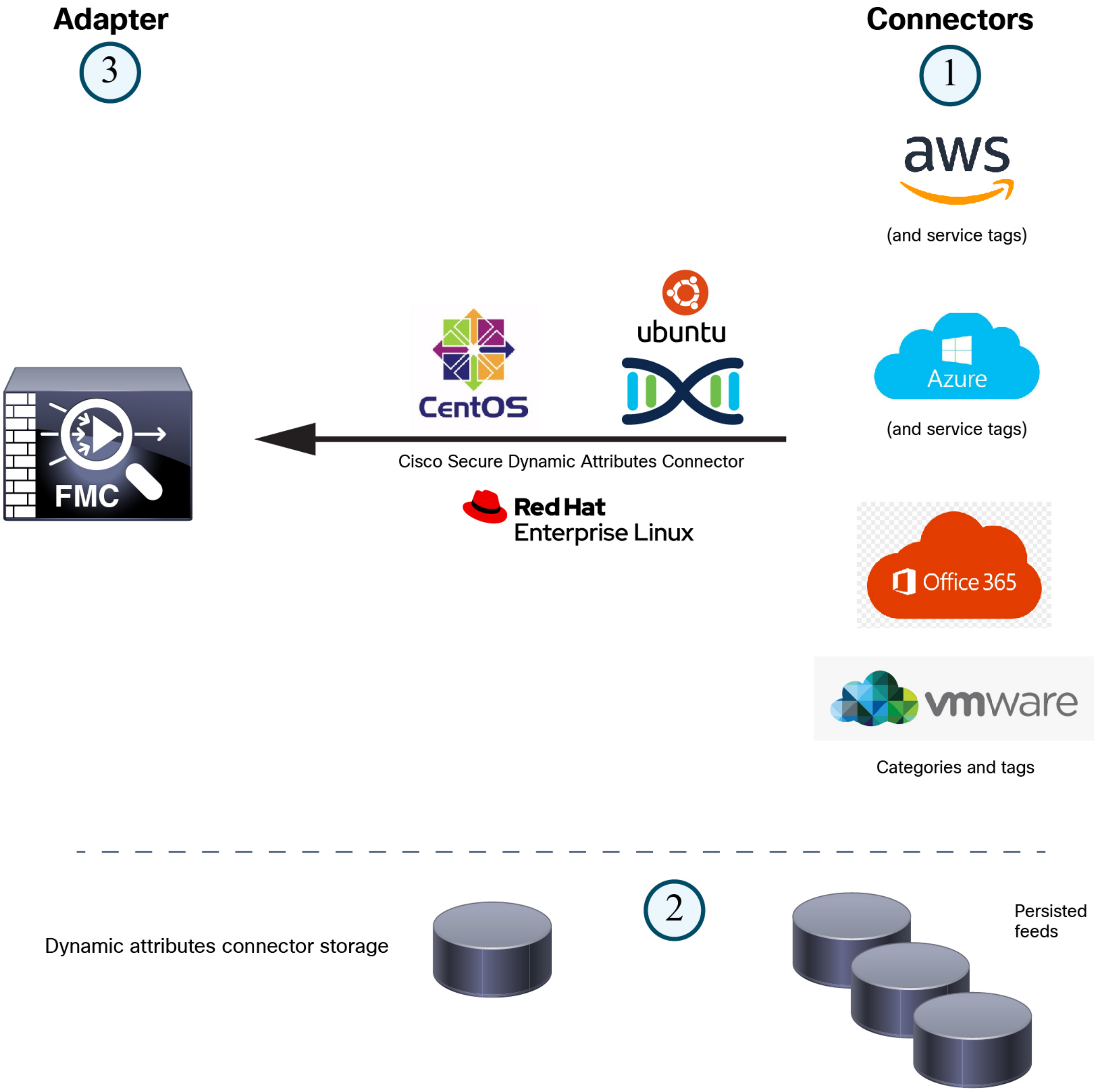
Install Prerequisite Software, on page 6

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 Docker containers running on an Ubuntu virtual machine. Install the Cisco Secure Dynamic Attributes Connector on the Ubuntu host using an Ansible collection.

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



- Install the dynamic attributes connector on a supported Linux virtual machine.

  For more information, see Supported Operating Systems and Third-Party Software, on page 5.

- The system supports certain public cloud providers.

  This topic discusses supported *connectors* (which are the connections to those providers).

- 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.

  You can create the following types of adapters:

  - *FMC* for an on-premises FMC device.

    This type of FMC device might be managed by Cisco Defense Orchestrator (CDO) or it might be a standalone.

  - *Cloud-delivered Firewall Management Center* for devices managed by CDO.

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.

   You can create the following types of adapters:

CHAPTER 2

Install and Upgrade the Cisco Secure Dynamic Attributes Connector

This chapter discusses how to install and upgrade the Cisco Secure Dynamic Attributes Connector on all supported operating systems.

Supported Operating Systems and Third-Party Software

The dynamic attributes connector requires the following:

- Ubuntu 18.04 or 20.04
- CentOS 7 Linux
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8GB RAM
- For new installations, 100GB available disk space

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

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

Virtual machine sizing

Install Prerequisite Software

Before you begin

Make sure you have physical or virtual set up and that the system that can communicate with your Firepower Management Center.

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.

Variable	Value
export http_proxy	Use with an HTTP proxy. *user***:***pass@host-or-ip***:***port*
export https_proxy	Use this with an HTTPS proxy. *user***:***pass@host-or-ip***:***port*
export no_proxy	Remove the proxy configuration. **export no_proxy="localhost,127.0.0.1"**

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 9
Install Prerequisite Software—CentOS, on page 7
Install Prerequisite Software—RHEL, on page 8

Install Prerequisite Software—CentOS

Before you begin

Do all of the following:

- Make sure your system meets the prerequisites discussed in Supported Operating Systems and Third-Party Software, on page 5.
- (Optional.) If you need proxy access to the dynamic attributes connector, see Install Prerequisite Software, on page 6.

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 and upgrade your repositories.

CentOS 7:

```
sudo yum -y update && sudo yum -y upgrade
```

Step 3 Install the epel repository.

CentOS 7:

```
sudo yum -y install epel-release
```

Step 4 (CentOS 7 only.) Install Python 3.

```
sudo yum install -y python3 libselinux-python3
```

Step 5 Install Ansible.

CentOS 7:

```
sudo yum install -y ansible
```

Step 6 Verify the Ansible version is 2.9 or later.

CentOS 7:

```
ansible --version
  ansible 2.9.24
  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/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Apr  2 2020, 13:16:51) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

Note It's normal for Ansible to reference Python 2.x as the preceding output shows. The connector will still use Python 3.

What to do next

Install the connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 10.

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

Install Prerequisite Software—RHEL

Before you begin

Do all of the following:

- Make sure your system meets the prerequisites discussed in Supported Operating Systems and Third-Party Software, on page 5.
- (Optional.) If you need proxy access to the dynamic attributes connector, see Install Prerequisite Software, on page 6.

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.

RHEL 7:

```
sudo yum -y update && sudo yum -y upgrade
```

RHEL 8:

```
sudo dnf -y update && sudo dnf -y upgrade
```

Step 3 Install the epel repository.

RHEL 7:

```
sudo yum -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

RHEL 8:

```
sudo dnf -y install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

Step 4 (RHEL 7 only.) Install Python 3.

```
sudo yum install -y python3 libselinux-python3
```

Step 5 Install Ansible.

RHEL 7:

```
sudo yum -y install ansible
```

RHEL 8:

```
sudo dnf install -y ansible
```

Step 6 Verify the Ansible version.

```
ansible --version
```

An example follows.

RHEL 7:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = [u'/home/stevej/.ansible/plugins/modules',
u'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python2.7/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 2.7.5 (default, Mar 20 2020, 17:08:22) [GCC 4.8.5 20150623 (Red Hat 4.8.5-39)]
```

Note It's normal for Ansible to reference Python 2.x as the preceding output shows. The connector will still use Python 3.

RHEL 8:

```
ansible 2.9.24
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/home/stevej/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/lib/python3.6/site-packages/ansible
  executable location = /usr/bin/ansible
  python version = 3.6.8 (default, Mar 18 2021, 08:58:41) [GCC 8.4.1 20200928 (Red Hat 8.4.1-1)]
```

What to do next

Install the connector as discussed in Install the Cisco Secure Dynamic Attributes Connector, on page 10.

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

Install Prerequisite Software—Ubuntu

This task discusses how to install prerequisite software on 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 10.

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 or 20.04
- CentOS 7 Linux
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8GB RAM

- For new installations, 100GB available disk space

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

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

To install prerequisite software, see Install Prerequisite Software, on page 6.

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:

```
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.

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.

--extra-vars

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 6.

- **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:

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

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 virtual 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.

Upgrade the Cisco Secure Dynamic Attributes Connector

This topic discusses how to upgrade to Cisco Secure Dynamic Attributes Connector version 1.1 from version 1.0. Version 1.0 was available only on Ubuntu 18.04 so that is the only operating system to which these instructions apply.

This topic discusses how to upgrade from any earlier Cisco Secure Dynamic Attributes Connector to the current version. These tasks can be performed regardless of Cisco Secure Dynamic Attributes Connector version or operating system.

Step 1 Log in to the machine you want to upgrade.

Step 2 Enter the following commands:

```
cd ~/.ansible/collections/ansible_collections/cisco/csdac
ansible-galaxy collection install cisco.csdac --force
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.

--extra-vars	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 6. • **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`)

Step 3 Wait for the upgrade to complete.

Step 4 Upgrade logs are available in the following location:

```
~/.ansible/collections/ansible_collections/cisco/csdac/logs/csdac.log
```

What to do next

See Create a Connector, on page 15.

CHAPTER 3

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 15
- Create an Adapter, on page 26
- Create Dynamic Attributes Filters, on page 32

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	GitHub	Google Cloud	Azure	Azure Service Tags	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No

See one of the following sections for more information.

Amazon Web Services Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from AWS to the FMC for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from AWS:

- *Tags*, user-defined key-value pairs you can use to organize your AWS EC2 resources.

  For more information, see Tag your EC2 Resources in the AWS documentation
- *IP addresses* of virtual machines in AWS.

Minimum permissions required

The Cisco Secure Dynamic Attributes Connector requires a user at minimum with a policy that permits `ec2:DescribeTags` and `ec2:DescribeInstances` to be able to import dynamic attributes.

Create an AWS User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to the FMC. For a list of these attributes, see Amazon Web Services Connector—About User Permissions and Imported Data, on page 16.

Before you begin

You must already have set up your Amazon Web Services (AWS) account. For more information about doing that, see this article in the AWS documentation.

Step 1 Log in to the AWS console as a user with the admin role.

Step 2 From the Dashboard, click **Security, Identity & Compliance** > **IAM**.

Step 3 Click **Access Management** > **Users**.

Step 4 Click **Add Users**.

Step 5 In the **User Name** field, enter a name to identify the user.

Step 6 Click **Access Key - Programmatic Access**.

Step 7 At the Set permissions page, click **Next** without granting the user access to anything; you'll do this later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

Step 10 Click **Download .csv** to download the user's key to your computer.

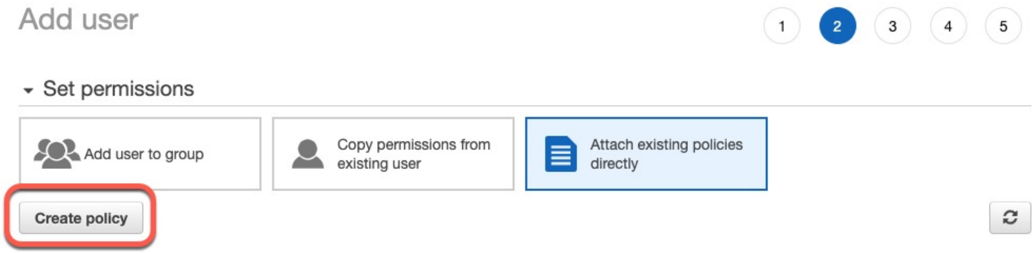
Note This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

Step 12 At the Identity and Access Management (IAM) page in the left column, click **Access Management** > **Policies**.

Step 13 Click **Create Policy**.

Step 14 On the Create Policy page, click **JSON**.


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

Step 15 Enter the following policy in the field:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeTags",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Step 16 Click **Next**.

Step 17 Click **Review**.

Step 18 On the Review Policy page, enter the requested information and click **Create Policy**.

Step 19 On the Policies page, enter all or part of the policy name in the search field and press Enter.

Step 20 Click the policy you just created.

Step 21 Click **Actions** > **Attach**.

Step 22 If necessary, enter all or part of the user name in the search field and press Enter.

Step 23 Click **Attach Policy**.

What to do next

Create an AWS Connector, on page 17.

Create an AWS Connector

This task discusses how to configure a connector that sends data from AWS to the FMC for use in access control policies.

Before you begin

Create a user with at least the privileges discussed in Create an AWS User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector, on page 16.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

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

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

Step 6 Click **Save**.

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

What to do next

Create an Adapter, on page 26

Azure Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from Azure to the FMC for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from Azure:

- *Tags*, key-value pairs associated with resources, resource groups, and subscriptions.

  For more information, see this page in the Microsoft documentation.

- *IP addresses* of virtual machines in Azure.

Minimum permissions required

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

Create an Azure User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to the FMC. For a list of these attributes, see Azure Connector—About User Permissions and Imported Data, on page 18.

Before you begin

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

Step 1 Log in to the Azure Portal as the owner of the subscription.

Step 2 Click **Azure Active Directory**.

Step 3 Find the instance of Azure Active Directory for the application you want to set up.

Step 4 Click **Add** > **App registration**.

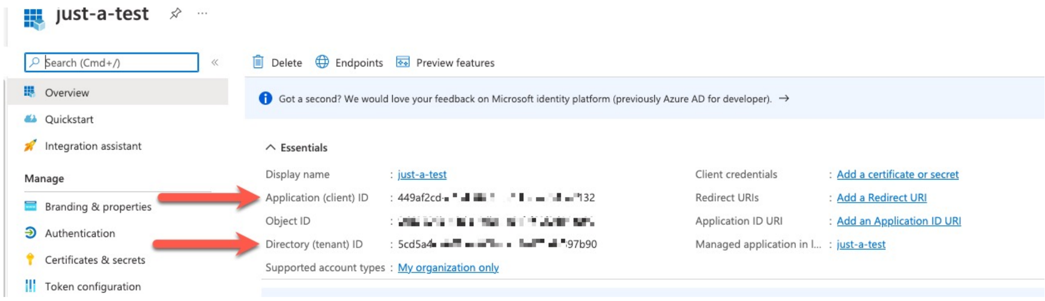
Step 5 In the **Name** field, enter a name to identify this application.

Step 6 Enter other information on this page as required by your organization.

Step 7 Click **Register**.

Step 8 On the next page, make note of the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

A sample follows.



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

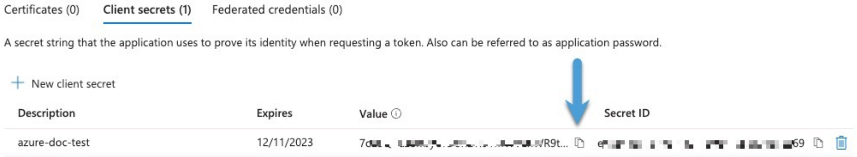
Display name : just-a-test
Application (client) ID : 449af2cd[redacted]132
Object ID : [redacted]
Directory (tenant) ID : 5cd5a4[redacted]97b90
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an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

Step 9 Next to Client Credentials, click **Add a certificate or secret**.

Step 10 Click **New Client Secret**.

Step 11 Enter the requested information and click **Add**.

Step 12 Copy the value of the **Value** field to the clipboard. This value, *and not the **Secret ID***, is the client secret.



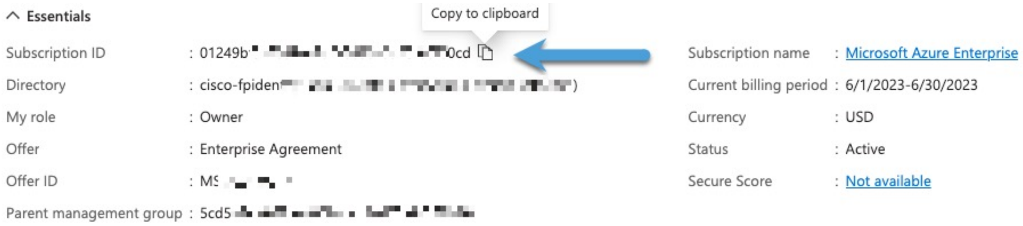
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

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

Step 13 Go back to the main Azure Portal page and click **Subscriptions**.

Step 14 Click the name of your subscription.

Step 15 Copy the subscription ID to the clipboard.



Essentials

Copy to clipboard

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

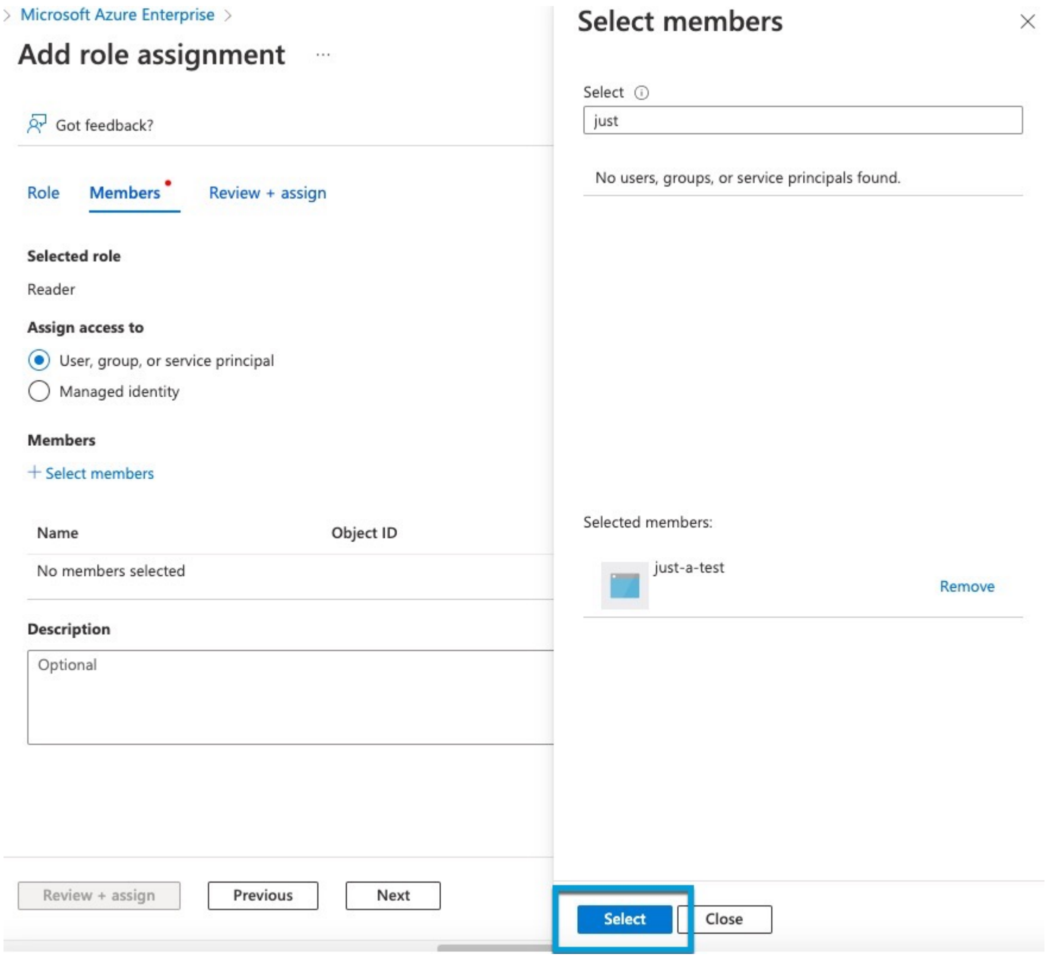
Step 16 Click **Access Control (IAM)**.

Step 17 Click **Add** > **Add role assignment**.

Step 18 Click **Reader** and click **Next**.

Step 19 Click **Select Members**.

Step 20 On the right side of the page, click the name of the app you registered and click **Select**.



> Microsoft Azure Enterprise >

Add role assignment ...

Got feedback?

Role | Members | Review + assign

Selected role

Reader

Assign access to

● User, group, or service principal

○ Managed identity

Members

+ Select members

Name	Object ID
No members selected	

Description

Optional

Review + assign | Previous | Next

Select members

Select ⓘ

just

No users, groups, or service principals found.

Selected members:

just-a-test Remove

Select | Close

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

What to do next

See Create an Azure Connector, on page 21.

Create an Azure Connector

This task discusses how to create a connector to send data from Azure to FMC for use in access control policies.

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector, on page 19.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

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

Step 6 Click **Save**.

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

What to do next

Create an Adapter, on page 26

Create an Azure Service Tags Connector

This topic discusses how to create a connector for Azure service tags to the FMC for use in access control policies. The IP addresses association with these tags are updated every week by Microsoft.

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

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure.
Subscription Id	(Required.) Enter your Azure subscription ID.
Tenant Id	(Required.) Enter your tenant ID.
Client Id	(Required.) Enter your client ID.
Client Secret	(Required.) Enter your client secret.

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

Step 6 Click **Save**.

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

What to do next

Create an Adapter, on page 26

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 Click **Connectors**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure.
Base API URL	(Required.) Enter the URL from which to retrieve Office 365 information, if it's different from the default. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Instance name	(Required.) From the list, click an instance name. For more information, see Office 365 IP Address and URL web service on the Microsoft documentation site.
Disable optional IPs	(Required.) Enter **true** or **false**.

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

Step 6 Click **Save**.

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

What to do next

Create an Adapter, on page 26

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.

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 29.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Connectors**.

Step 3 Do any of the following:

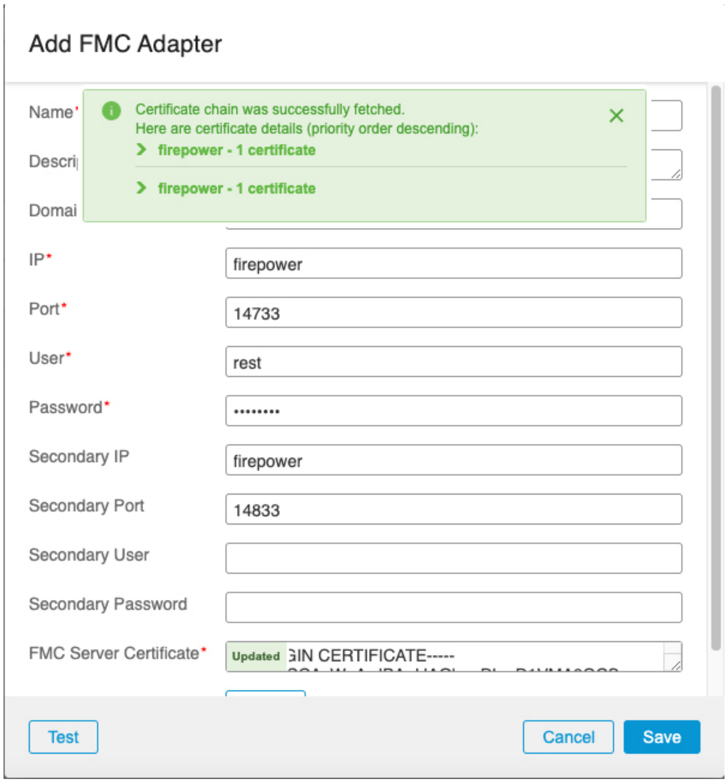
- Add a new connector: click Add icon (+), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a name to uniquely identify this connector.
Description	Enter an optional description.
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from vCenter.
Host	(Required.) Enter any of the following: • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port *Do not* enter a scheme (such as **`https://`**) or trailing slash. For example, **`myvcenter.example.com`** or **`192.0.2.100:9090`**
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.

Value	Description
NSX Password	Enter the NSX user's password.
vCenter Certificate	You have the following options: • Click **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 29.

Following is an example of successfully fetching a certificate chain:



Add FMC Adapter

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

- firepower - 1 certificate
- firepower - 1 certificate

Name*

Descri

Domai

IP*: firepower

Port*: 14733

User*: rest

Password*: ••••••••

Secondary IP: firepower

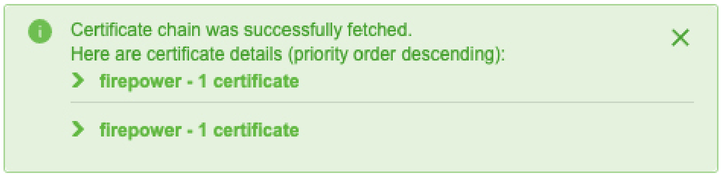
Secondary Port: 14833

Secondary User:

Secondary Password:

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

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



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

- firepower - 1 certificate
- firepower - 1 certificate

If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 29.

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

Step 6 Click **Save**.

What to do next

Create an Adapter, on page 26

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**.

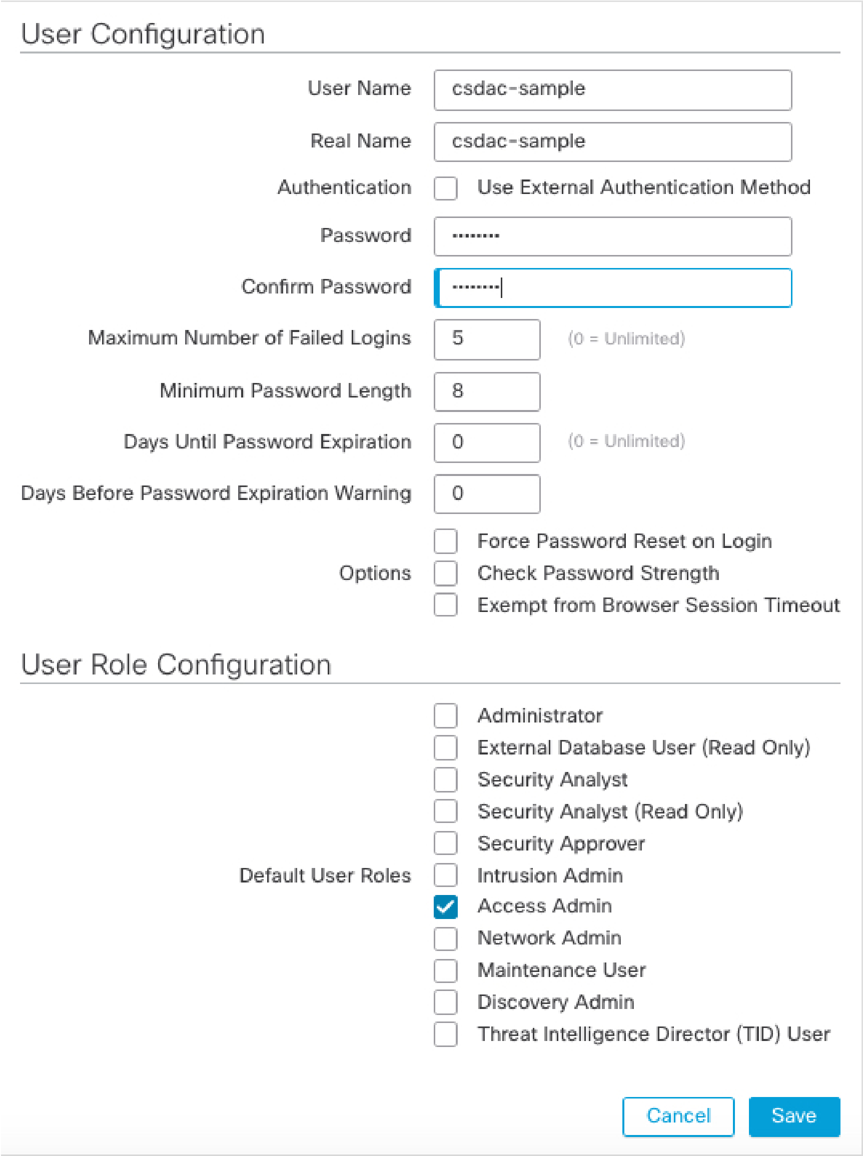
Step 3 Click **Create User**.

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.



User Configuration

User Name: csdac-sample

Real Name: csdac-sample

Authentication: □ Use External Authentication Method

Password: ••••••••

Confirm Password: ••••••••

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

Minimum Password Length: 8

Days Until Password Expiration: 0 (0 = Unlimited)

Days Before Password Expiration Warning: 0

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

User Role Configuration

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

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

What to do next

Create an Adapter, on page 26

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 26.

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Adapters**.

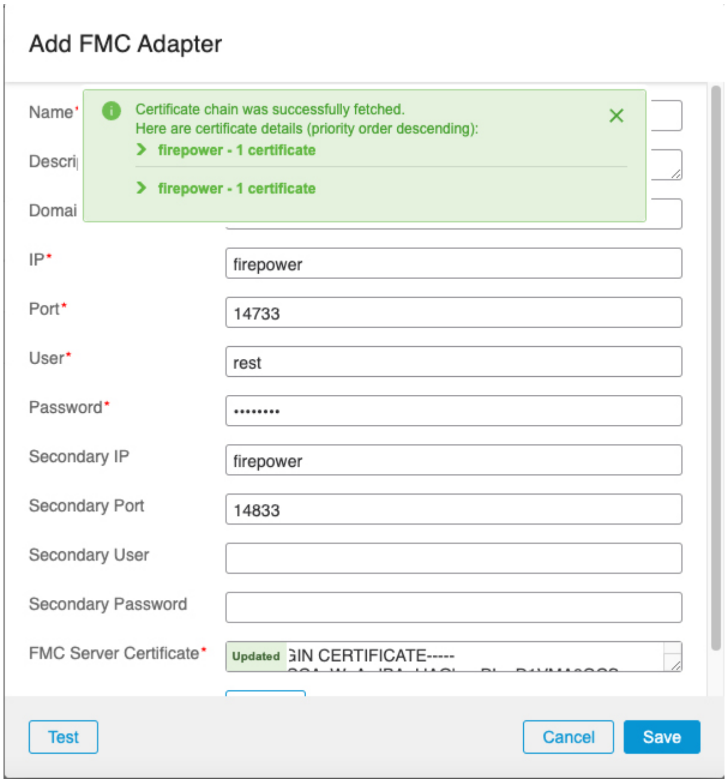
Step 3 Do any of the following:

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

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Domain	Enter the 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	You have the following options: • Click **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 29.

Following is an example of successfully fetching a certificate chain:



Add FMC Adapter

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

Name*

Descri

Domai

IP* firepower

Port* 14733

User* rest

Password* ••••••••

Secondary IP firepower

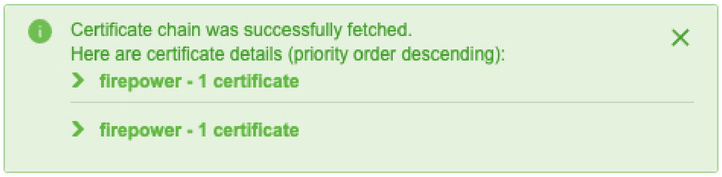
Secondary Port 14833

Secondary User

Secondary Password

FMC Server Certificate* Updated 3IN CERTIFICATE-----

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



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

If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 29.

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

Step 6 Click **Save**.

Manually Get a Certificate Authority (CA) Chain

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

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

- Create a vCenter Connector, on page 24

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
   ```

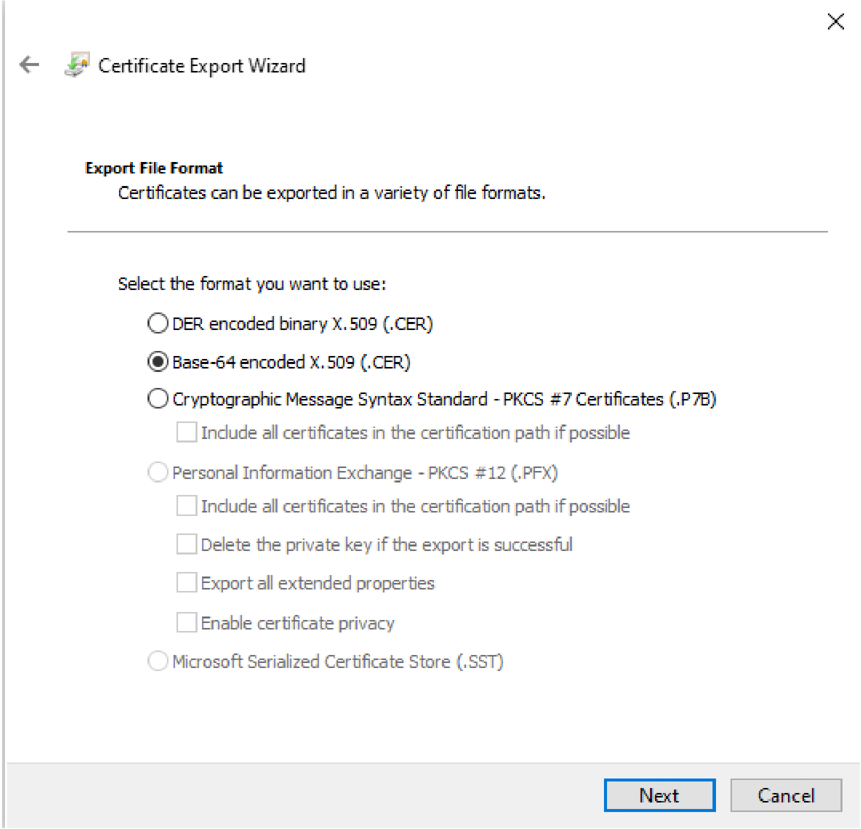
3. Save the entire certificate chain to a plaintext file.
   - *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
   - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)

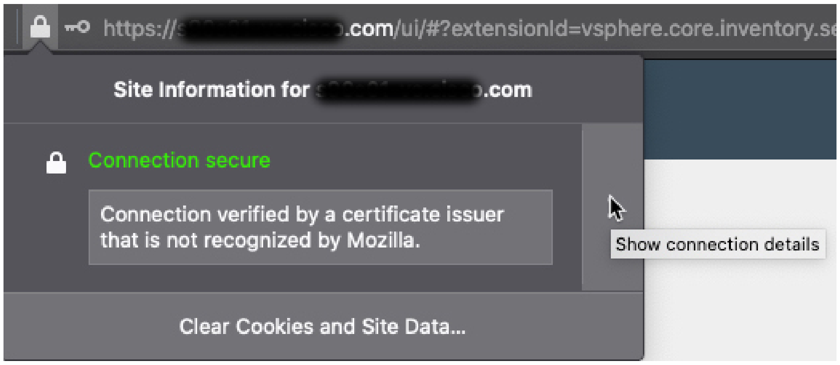
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter or the 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.



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

Site Information for [redacted].com

Connection secure

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

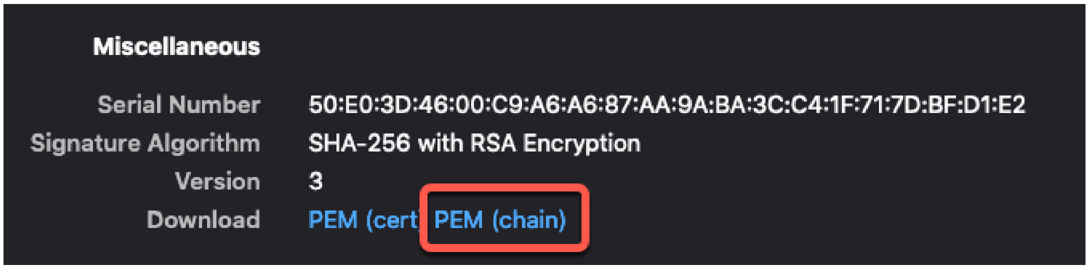
4. Click **More Information**.

5. Click **View Certificate**.

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

7. Scroll to the Miscellaneous section.

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



Miscellaneous

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

9. Save the file.

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

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 37.

Before you begin

Complete all of the following tasks:

- Install Prerequisite Software, on page 6
- Create a Connector, on page 15
- Create an Adapter, on page 26

Step 1 Log in to the dynamic attributes connector.

Step 2 Click **Dynamic Attributes Filters**.

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

Step 3 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in access control policy and in the 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 icon (⊞). • Edit or delete a filter: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

Step 4 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.
Values	Click either **Any** or **All** and click one or more values from the list. Click **Add another value** to add values to your query.

Step 5 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 6 When you're finished, click **Save**.

Step 7 (Optional.) Verify the dynamic object in the FMC.

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

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

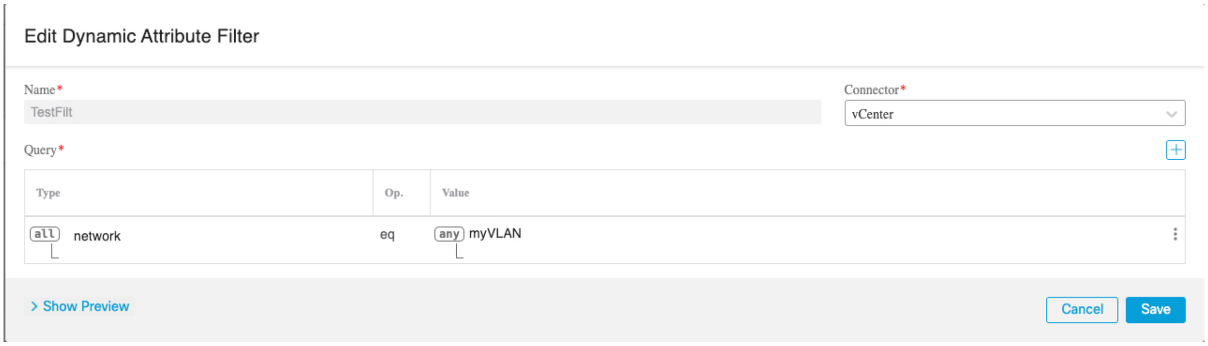
c) In the left pane, click **External Attributes** > **Dynamic Object**.
   The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

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

Examples: vCenter

The following example shows one criterion: a VLAN.



Edit Dynamic Attribute Filter

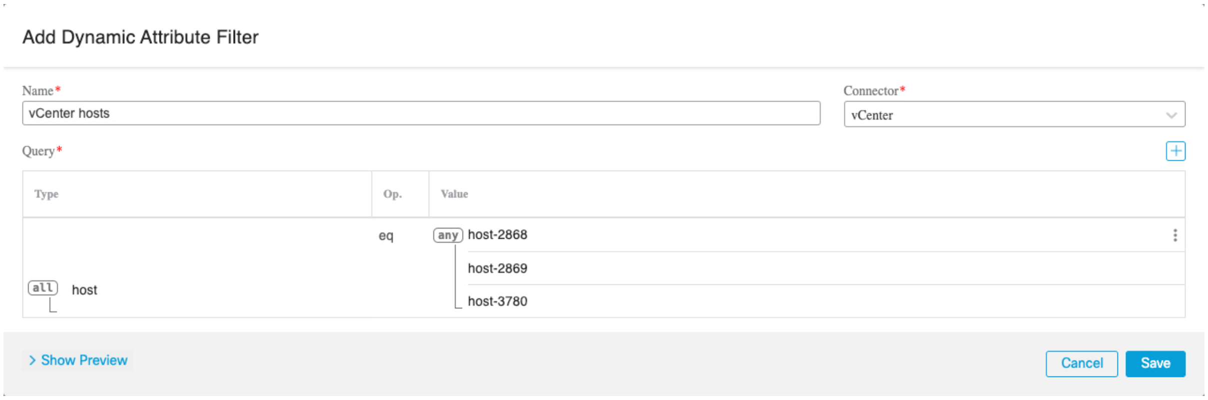
Name*: TestFilt

Connector*: vCenter

Query*

Type	Op.	Value
all network	eq	any myVLAN

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



Add Dynamic Attribute Filter

Name*: vCenter hosts

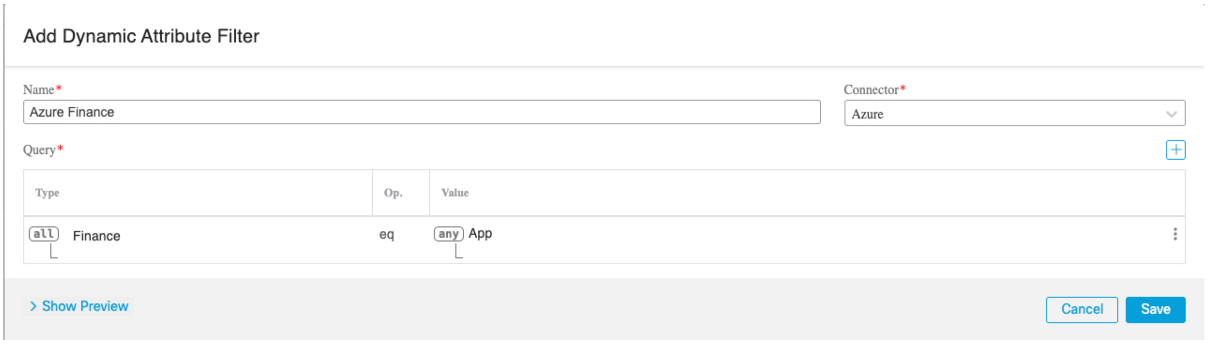
Connector*: vCenter

Query*

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

Example: Azure

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



Add Dynamic Attribute Filter

Name* Azure Finance

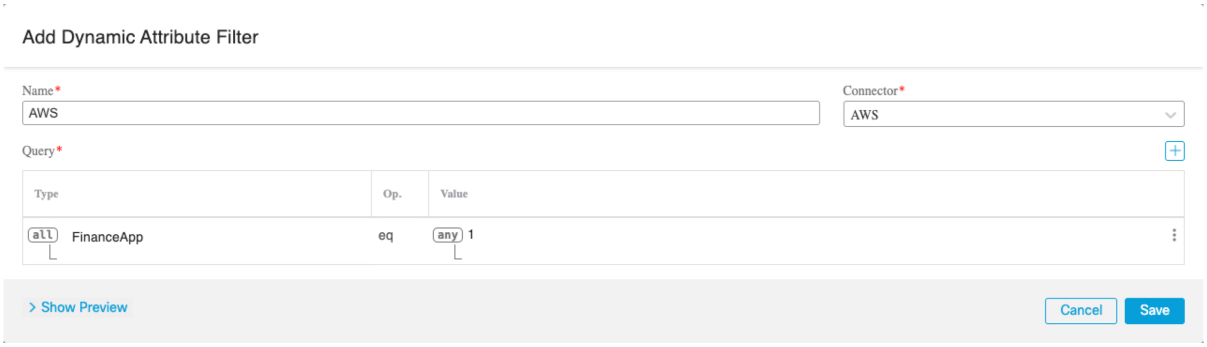
Connector* Azure

Query*

Type	Op.	Value
all Finance	eq	any App

Example: AWS

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



Add Dynamic Attribute Filter

Name* AWS

Connector* AWS

Query*

Type	Op.	Value
all FinanceApp	eq	any 1

CHAPTER 4

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 FMC or Cloud-delivered Firewall Management Center 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 32.

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**.

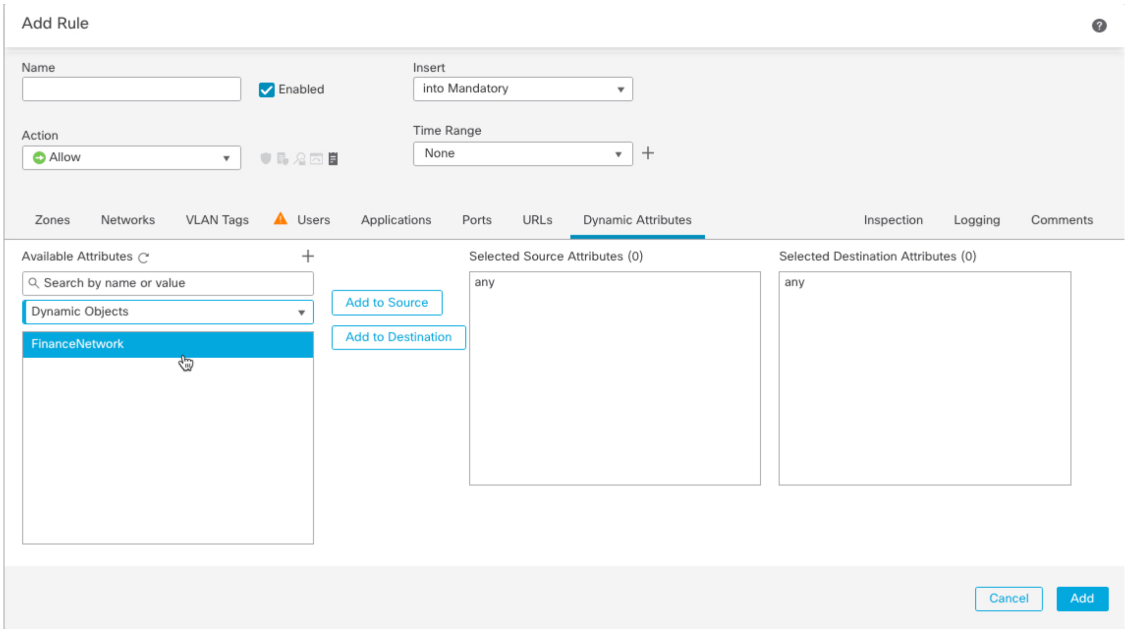
Step 3 Click **Edit** (✎) next to an access control policy.

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.



Add Rule

Name:

☑ Enabled

Insert: into Mandatory

Action: Allow

Time Range: None

Available Attributes: Dynamic Objects

FinanceNetwork

Selected Source Attributes (0): any

Selected Destination Attributes (0): any

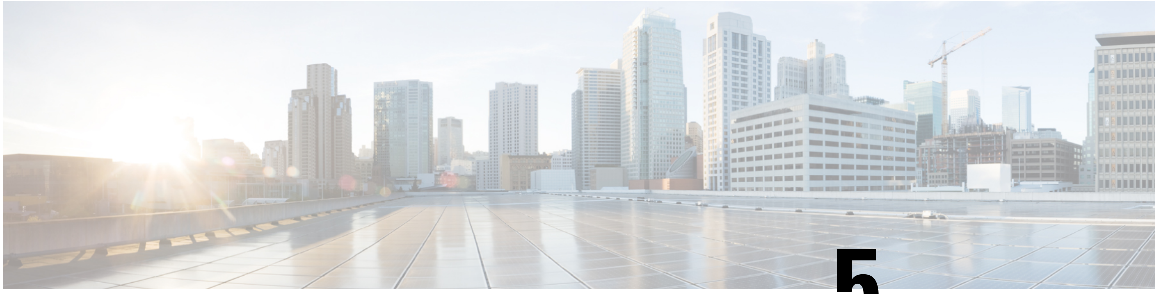
The preceding example shows a dynamic object named `FinanceNetwork` that corresponds to the dynamic attribute filter created in the Cisco Secure Dynamic Attributes Connector.

Step 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 5

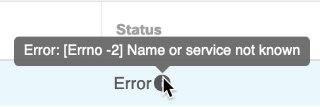
Troubleshoot the Dynamic Attributes Connector

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 different.



Error: [Errno -2] Name or service not known

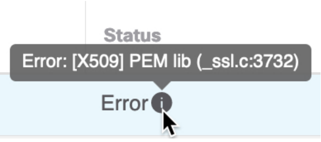
Solution: Edit the connector or adapter and check for:

- 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 29.

Problem: [X509 PEM lib]

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

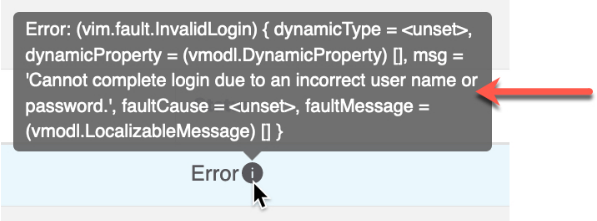


Error: [X509] PEM lib (_ssl.c:3732)

Solution: Edit the connector and check the CA chain. For more information, see Manually Get a Certificate Authority (CA) Chain, on page 29.

Problem: Incorrect username or password

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

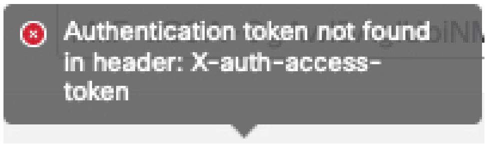


Error: (vim.fault.InvalidLogin) { dynamicType = <unset>, dynamicProperty = (vmodl.DynamicProperty) [], msg = 'Cannot complete login due to an incorrect user name or password.', faultCause = <unset>, faultMessage = (vmodl.LocalizableMessage) [] }

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

Problem: Authentication token not found in header

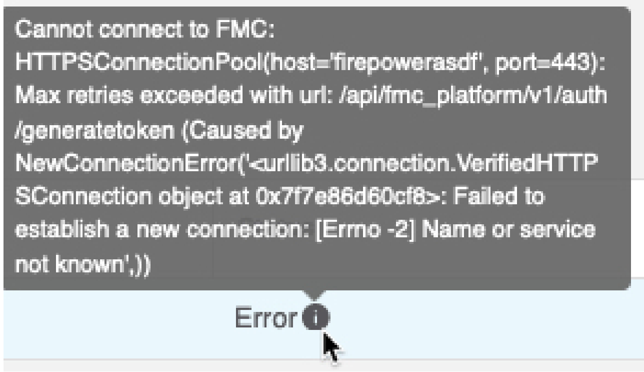
This error is displayed when you attempt to test the connection with an adapter user that does not have sufficient privileges on the FMC:



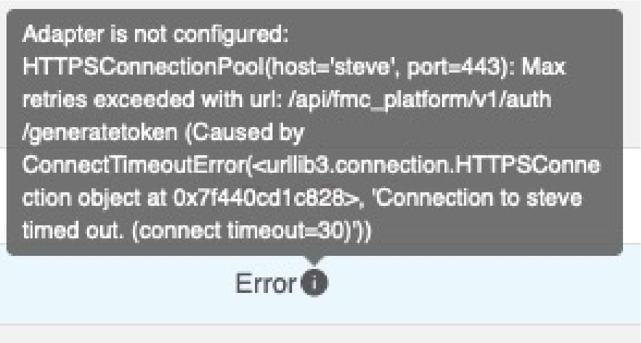
Authentication token not found in header: X-auth-access-token

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.



Cannot connect to FMC: HTTPSConnectionPool(host='firepowerasdf', port=443): Max retries exceeded with url: /api/fmc_platform/v1/auth/generatetoken (Caused by NewConnectionError('<urllib3.connection.VerifiedHTTPSConnection object at 0x7f7e86d60cf8>: Failed to establish a new connection: [Errno -2] Name or service not known',))



Adapter is not configured: HTTPSConnectionPool(host='steve', port=443): Max retries exceeded with url: /api/fmc_platform/v1/auth/generatetoken (Caused by ConnectTimeoutError(<urllib3.connection.HTTPSConnection object at 0x7f440cd1c828>, 'Connection to steve timed out. (connect timeout=30)'))

Solution: Do all of the following:

- Verify the management center is running and that it can be reached from the dynamic attributes connector.
- 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 29.

Troubleshoot Using the Command Line

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

Check container status

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

```
cd ~/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 application debug logging and generate troubleshoot files

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

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

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

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

Location	What it contains
/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

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

- Create a vCenter Connector, on page 24

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.

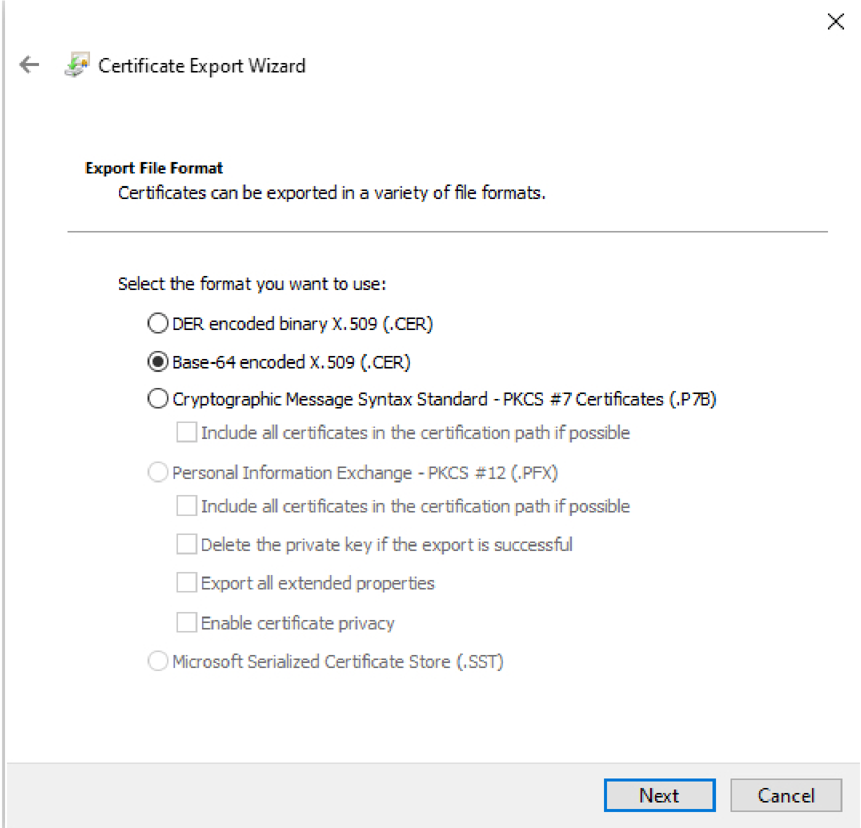
6. Click **View Certificate**.

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.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ○ DER encoded binary X.509 (.CER)
- ● Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Delete the private key if the export is successful
  - □ Export all extended properties
  - □ Enable certificate privacy
- ○ Microsoft Serialized Certificate Store (.SST)

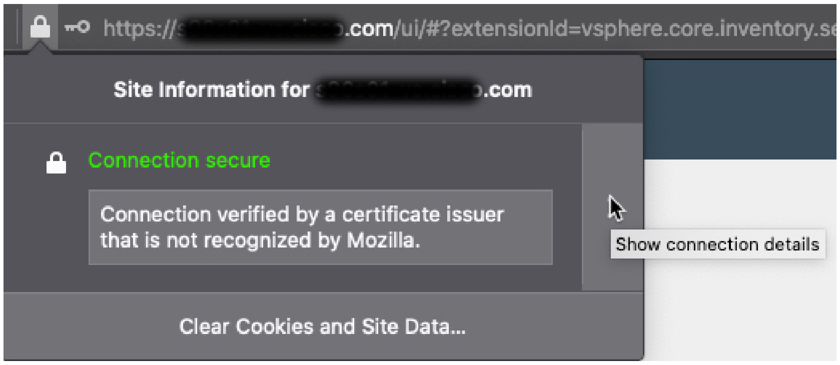
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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

Get a Certificate Chain—Windows Firefox

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

1. Log in to vCenter or the 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.



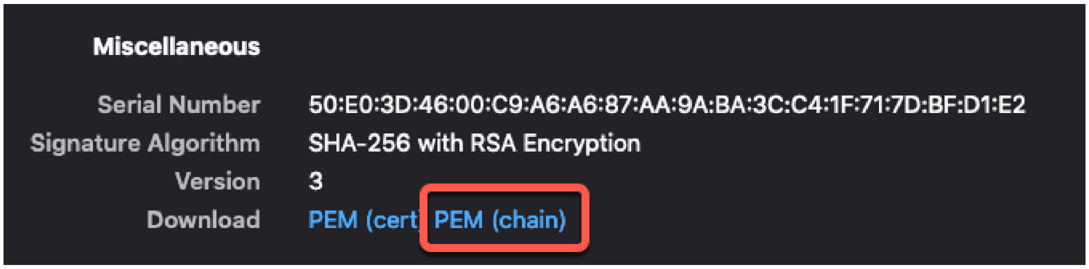
https://[redacted].com/ui/#?extensionId=vsphere.core.inventory.se

Site Information for [redacted].com

Connection secure

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

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



Miscellaneous

Serial Number 50:E0:3D:46:00:C9:A6:A6:87:AA:9A:BA:3C:C4:1F:71:7D:BF:D1:E2

Signature Algorithm SHA-256 with RSA Encryption

Version 3

Download PEM (cert PEM (chain)

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

Migration from DockerHub to Amazon ECR

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

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

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

Dynamic Attributes Connector Azure access requirements

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