



Cisco Secure Dynamic Attributes Connector Configuration Guide 2.3

First Published: 2023-12-01

Last Modified: 2025-01-17

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

Full Cisco Trademarks with Software License ?

CHAPTER 1

About the Cisco Dynamic Attributes Connector 1

About the Cisco Secure Dynamic Attributes Connector 1

How It Works 2

CHAPTER 2

Install and Upgrade the Cisco Secure Dynamic Attributes Connector 5

Supported Operating Systems and Third-Party Software 5

Requirements and Prerequisites for the Cisco APIC Integration with ASA 6

Install Prerequisite Software 7

Install Prerequisite Software—RHEL 8

Install Prerequisite Software—Ubuntu 9

Install the Cisco Secure Dynamic Attributes Connector 10

Upgrade the Cisco Secure Dynamic Attributes Connector 13

CHAPTER 3

Configure the Cisco Secure Dynamic Attributes Connector 15

Create a Connector 15

Amazon Web Services Connector—About User Permissions and Imported Data 16

Create an AWS User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector 16

Create an AWS Connector 17

Amazon Web Services Security Groups Connector—About User Permissions and Imported Data 18

Create an AWS User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector 19

Create an AWS Security Groups Connector 20

Create an AWS Service Tags Connector	21
Azure Connector—About User Permissions and Imported Data	22
Create an Azure User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector	22
Create an Azure Connector	24
Create an Azure Service Tags Connector	25
Create a Cisco Cyber Vision Connector	26
Create a Generic Text Connector	27
Create a GitHub Connector	29
Google Cloud Connector—About User Permissions and Imported Data	29
Create a Google Cloud User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector	30
Create a Google Cloud Connector	31
Create an Office 365 Connector	32
vCenter Connector—About User Permissions and Imported Data	33
Create a vCenter User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector	33
Create a vCenter Connector	34
Create a Webex Connector	37
Create a Zoom Connector	37
Create an Adapter	38
Create a Secure Firewall Management Center User for the Dynamic Attributes Connector	39
How to Create an On-Prem Firewall Management Center Adapter	41
Create a Cloud-delivered Firewall Management Center Adapter	44
Get Your Base URL and API Token	44
How to Create a Cloud-delivered Firewall Management Center Adapter	45
Manually Get a Certificate Authority (CA) Chain	46
Create Dynamic Attributes Filters	49
Dynamic Attribute Filter Examples	51
Manually Get a Certificate Authority (CA) Chain	52
CHAPTER 4	
Use Dynamic Objects in Access Control Policies	57
About Dynamic Objects in Access Control Rules	57
Create Access Control Rules Using Dynamic Attributes Filters	57

CHAPTER 5	Troubleshoot the Dynamic Attributes Connector	59
	Troubleshoot Error Messages	59
	Troubleshoot Using the Command Line	61
	Manually Get a Certificate Authority (CA) Chain	63

APPENDIX A	Security and Internet Access	67
	Security Requirements	67
	Internet Access Requirements	67

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



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 Secure Firewall 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

This topic discusses support and architecture for the Cisco Secure Dynamic Attributes Connector.

Supported connectors

We currently support:

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

CSDAC version/platform	AWS	AWS security groups	AWS service tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Generic Text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

More information about connectors:

- Amazon Web Services security groups.

See [Amazon Web Services Security Groups Connector—About User Permissions and Imported Data](#), on page 18.

- Amazon Web Services service tags.

For more information, see a resource like [What are tags?](#).

- Generic text list of IP addresses you specify

For more information, see [Create a Generic Text Connector, on page 27](#).

- GitHub

For more information, see [Create a GitHub Connector, on page 29](#).

- Google Cloud

For more information, see [Setting Up Your Environment](#) in the Google Cloud documentation.

See [Google Cloud Connector—About User Permissions and Imported Data, on page 29](#).

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

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

- Webex IP addresses

For more information, see [Create a Webex Connector, on page 37](#).

- Zoom IP addresses

For more information, see [Create a Zoom Connector, on page 37](#).

Related Topics

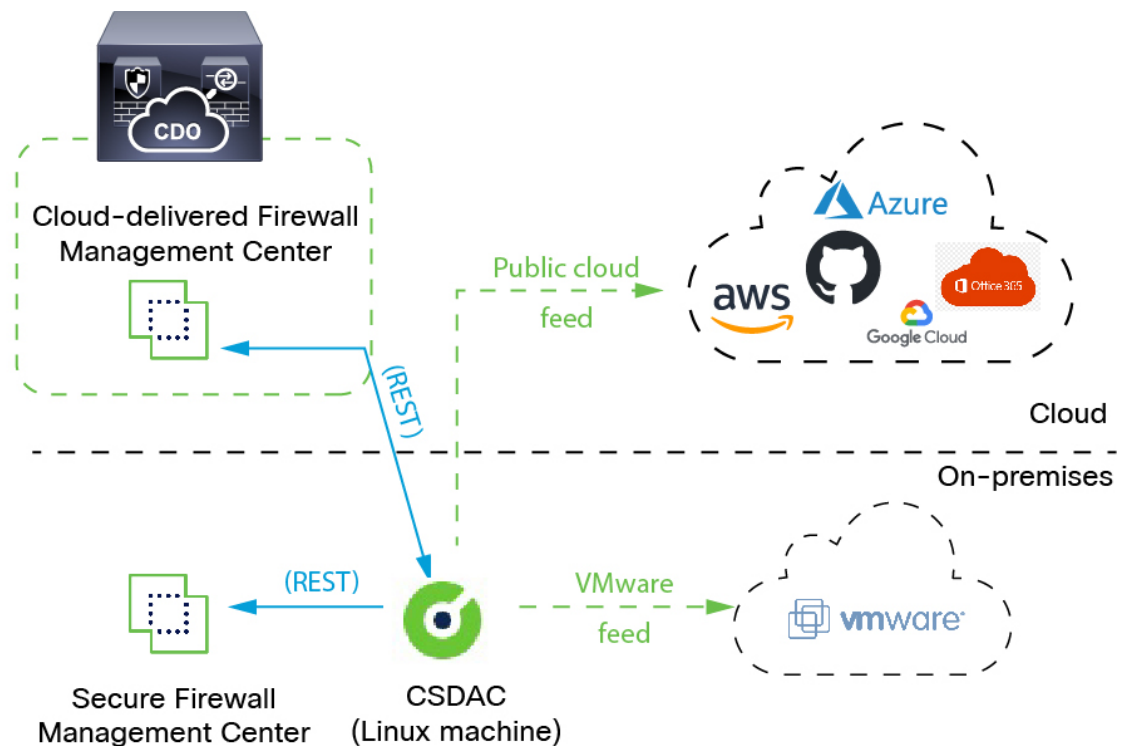
[Install Prerequisite Software, on page 7](#)

How It Works

Network constructs such as IP address are not reliable in virtual, cloud and container environments due to the dynamic nature of the workloads and the inevitability of IP address overlap. Customers require policy rules to be defined based on non-network constructs such as VM name or security group, so that firewall policy is persistent even when the IP address or VLAN changes.

You can collect these tags and attributes using dynamic attributes connector Docker containers running on an Ubuntu, CentOS, or Red Hat Enterprise Linux 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.



- 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:

- *On-Prem Firewall Management Center* for an on-premises Management Center device.

This type of Management Center device might be managed by CDO or it might be a standalone.

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



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, on page 5](#)
- [Requirements and Prerequisites for the Cisco APIC Integration with ASA, on page 6](#)
- [Install Prerequisite Software, on page 7](#)
- [Install the Cisco Secure Dynamic Attributes Connector, on page 10](#)
- [Upgrade the Cisco Secure Dynamic Attributes Connector, on page 13](#)

Supported Operating Systems and Third-Party Software

The dynamic attributes connector requires the following:

- Ubuntu 18.04 to 22.04.2
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x or later
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8 GB RAM
- For new installations, 100 GB available disk space to install the dynamic attributes connector

If you use a hypervisor:

VMware ESX or ESXi up to 8

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

- vCenter up to 8
- VMware Tools must be installed on the virtual machine

Virtual machine sizing

We recommend you size your virtual machines as follows:

- 50 connectors, assuming 5 filters per connector and 20,000 workloads: 4 CPUs; 8 GB RAM; 100 GB available disk space
- 125 connectors, assuming 5 filters per connector and 50,000 workloads: 8 CPUs, 16 GB RAM, 100 GB available disk space

**Note**

Failure to size your virtual machines properly can cause the dynamic attributes connector to fail or not to start.

Requirements and Prerequisites for the Cisco APIC Integration with ASA

Following are requirements and prerequisites to use Cisco APIC to send dynamic objects to ASA:

- Network communication: All of the following must be able to communicate with each other securely:
 - ASA 9.16 and later
 - Cisco APIC 4.2(7q) and later
 - Cisco Secure Dynamic Attributes Connector virtual machine, version 3.1 and later
- ASA requirements
 - License: Essentials
For more information about licensing, see [Smart Software Licensing](#).
 - FQDN: Supported
 - Multi-context: Supported
 - Multi-instance: Supported
 - High availability: Supported
 - Clustering: Supported
- Permissions required:
 - ASA: privilege 15
 - Cisco APIC: `readPriv` role for retrieving objects from tenants and `tenant-admin` role for the relevant security domains

Install Prerequisite Software

Before you begin

Make sure you have physical or virtual set up and that the system that can communicate with your the On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center.

Procedure

- 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. <i>user:pass@host-or-ip:port</i>
export https_proxy	Use this with an HTTPS proxy. <i>user:pass@host-or-ip:port</i>
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—RHEL](#), on page 8

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 7](#).

Procedure

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.

Procedure

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 or later.

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 dynamic attributes 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 to 22.04.2
- Red Hat Enterprise Linux (RHEL) 7 or 8
- Python 3.6.x or later
- Ansible 2.9 or later

Minimum requirements for all operating systems:

- 4 CPUs
- 8 GB RAM
- For new installations, 100 GB available disk space to install the dynamic attributes connector

We recommend you size your virtual machines as follows:

- 50 connectors, assuming 5 filters per connector and 20,000 workloads: 4 CPUs; 8 GB RAM; 100 GB available disk space
- 125 connectors, assuming 5 filters per connector and 50,000 workloads: 8 CPUs, 16 GB RAM, 100 GB available disk space



Note Failure to size your virtual machines properly can cause the dynamic attributes connector to fail or not to start.

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

- vCenter up to 8
- VMware Tools must be installed on the virtual machine

To install prerequisite software, see [Install Prerequisite Software, on page 7](#).

View the Readme and Release Notes

For the latest installation information, see the following:

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

Release Notes: [Release Notes](#)

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 7](#).

- **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 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.

Procedure

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 7](#).

- **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
```



CHAPTER 3

Configure the Cisco Secure Dynamic Attributes Connector

Install the dynamic attributes connector and configure connectors, dynamic attributes filters, and adapters to provide Secure Firewall Management Center or the 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 38](#)
- [Create Dynamic Attributes Filters, on page 49](#)
- [Manually Get a Certificate Authority \(CA\) Chain, on page 52](#)

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 Secure Firewall Management Center.

We support the following:

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

CSDAC version/platform	AWS	AWS security groups	AWS service tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Generic Text	GitHub	Google Cloud	Microsoft Office 365	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes

For more information about connectors, see the [configuration guide](#).

Amazon Web Services Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from AWS to Secure Firewall Management Center for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from AWS:

- *Tags*, user-defined key-value pairs you can use to organize your AWS EC2 resources.
For more information, see [Tag your EC2 Resources](#) in the AWS documentation
- *IP addresses* of virtual machines in AWS.

Minimum permissions required

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

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

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center. 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.

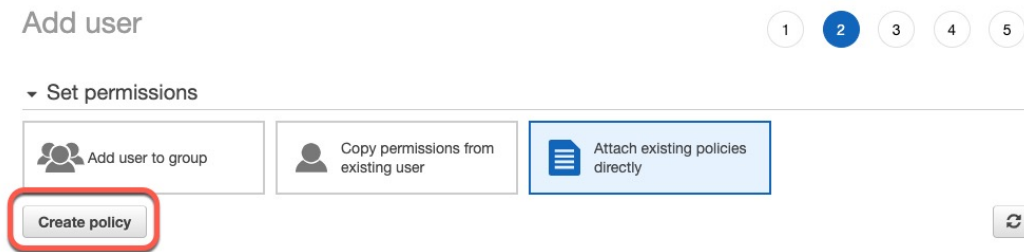
Procedure

-
- Step 1** Log in to the AWS console as a user with the admin role.
 - Step 2** From the Dashboard, click **Security, Identity & Compliance > IAM**.
 - Step 3** Click **Access Management > Users**.
 - Step 4** Click **Add Users**.
 - Step 5** In the **User Name** field, enter a name to identify the user.
 - Step 6** Click **Access Key - Programmatic Access**.
 - Step 7** At the Set permissions page, click **Next** without granting the user access to anything; you'll do this later.
 - Step 8** Add tags to the user if desired.
 - Step 9** Click **Create User**.
 - Step 10** Click **Download .csv** to download the user's key to your computer.

Note

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

- Step 11** Click **Close**.
- Step 12** At the Identity and Access Management (IAM) page in the left column, click **Access Management > Policies**.
- Step 13** Click **Create Policy**.
- Step 14** On the Create Policy page, click **JSON**.



- Step 15** Enter the following policy in the field:

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

- Step 16** Click **Next**.
- Step 17** Click **Review**.
- Step 18** On the Review Policy page, enter the requested information and click **Create Policy**.
- Step 19** On the Policies page, enter all or part of the policy name in the search field and press Enter.
- Step 20** Click the policy you just created.
- Step 21** Click **Actions > Attach**.
- Step 22** If necessary, enter all or part of the user name in the search field and press Enter.
- Step 23** Click **Attach Policy**.

What to do next

[Create an AWS Connector, on page 17.](#)

Create an AWS Connector

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

Before you begin



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

Procedure

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.

Amazon Web Services Security Groups Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from AWS to Secure Firewall Management Center for use in access control policies.

Minimum permissions required

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

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

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center. 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.

Procedure

- Step 1** Log in to the AWS console as a user with the admin role.
- Step 2** From the Dashboard, click **Security, Identity & Compliance > IAM**.
- Step 3** Click **Access Management > Users**.
- Step 4** Click **Add Users**.
- Step 5** In the **User Name** field, enter a name to identify the user.
- Step 6** Click **Access Key - Programmatic Access**.
- Step 7** At the Set permissions page, click **Next** without granting the user access to anything; you'll do this later.
- Step 8** Add tags to the user if desired.
- Step 9** Click **Create User**.
- Step 10** Click **Download .csv** to download the user's key to your computer.

Note

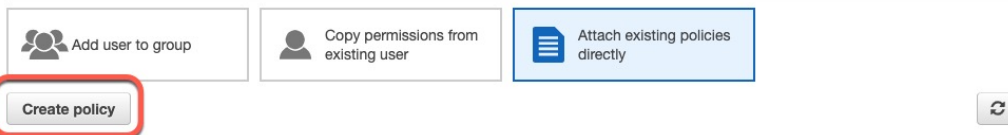
This is the only opportunity you have to retrieve the user's key.

- Step 11** Click **Close**.
- Step 12** At the Identity and Access Management (IAM) page in the left column, click **Access Management > Policies**.
- Step 13** Click **Create Policy**.
- Step 14** On the Create Policy page, click **JSON**.

Add user



Set permissions



- Step 15** Enter the following policy in the field:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```

    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "ec2:DescribeVpcs"
  ],
  "Resource": "*"
}
]
}

```

- Step 16** Click **Next**.
- Step 17** Click **Review**.
- Step 18** On the Review Policy page, enter the requested information and click **Create Policy**.
- Step 19** On the Policies page, enter all or part of the policy name in the search field and press Enter.
- Step 20** Click the policy you just created.
- Step 21** Click **Actions > Attach**.
- Step 22** If necessary, enter all or part of the user name in the search field and press Enter.
- Step 23** Click **Attach Policy**.

What to do next

[Create an AWS Connector, on page 17.](#)

Create an AWS Security Groups Connector



This task discusses how to configure a connector that sends [AWS security groups](#) data to the Secure Firewall Management Center for use in access control policies.

Before you begin

Do all of the following:

- Create AWS security groups as discussed in [Work with security groups](#) on the AWS documentation site.
- 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.](#)

Procedure

- 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. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Region	(Required.) Enter your AWS region code.
AWS Access Key	(Required.) Enter your access key.
AWS 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.

Create an AWS Service Tags Connector

This topic discusses how to create a connector for Amazon Web Services (AWS) service tags to the Secure Firewall Management Center for use in access control policies.

For more information, see resources like the following on the AWS documentation site:



- [What are tags?](#)
- [AWS IP address ranges](#)
- [Tagging your AWS resources](#)
- [Guidance for Tagging on AWS](#)
- [AWS service points](#)

Procedure

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.
URL	(Required.) Do not change the URL unless advised to do so.

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.

Azure Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from Azure to Secure Firewall Management Center for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from Azure:

- *Tags*, key-value pairs associated with resources, resource groups, and subscriptions.
For more information, see [this page](#) in the Microsoft documentation.
- *IP addresses* of virtual machines in Azure.

Minimum permissions required

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

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

This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center. For a list of these attributes, see [Azure Connector—About User Permissions and Imported Data, on page 22](#).

Before you begin

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

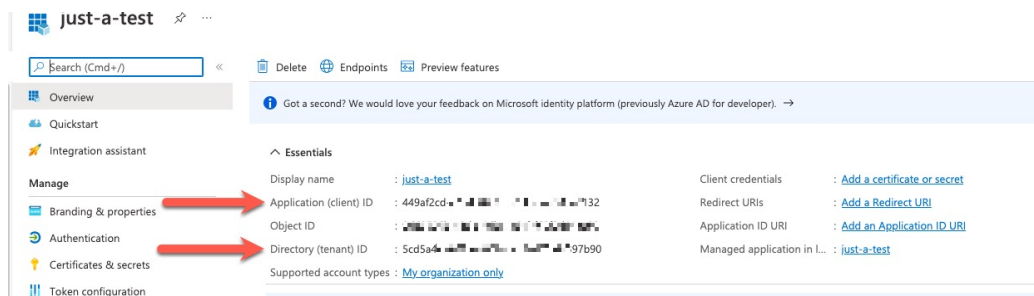
Procedure

Step 1 Log in to the [Azure Portal](#) as the owner of the subscription.

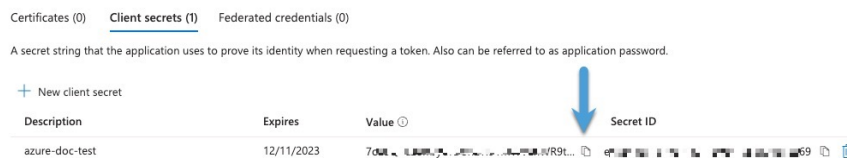
Step 2 Click **Azure Active Directory**.

- 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*).

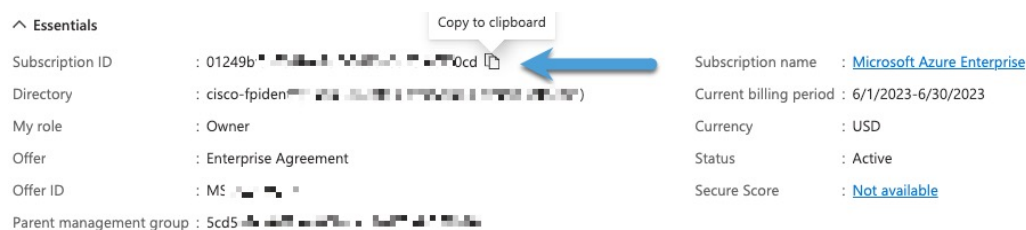
A sample follows.



- 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.



- 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.



- 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 ¹

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 24](#).

Create an Azure Connector

This task discusses how to create a connector to send data from Azure to Secure Firewall Management Center for use in access control policies.

Before you begin



Create an Azure user with at least the privileges discussed in [Create an Azure User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector, on page 22](#).

Procedure

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. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
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.

Create an Azure Service Tags Connector

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



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

Procedure

Step 1 Log in to the 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. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
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.

Create a Cisco Cyber Vision Connector

This task discusses how to send data from [Cisco Cyber Vision](#) to the Secure Firewall Management Center .

Before you begin

Cisco Cyber Vision must be reachable from the machine on which the dynamic attributes connector is running. You must know its IP address, port, and API key.



To find the API key in the Cyber Vision management console, click **Admin > API > Token**, then click **Show** to display the token and  to copy the token to the clipboard.

Procedure

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.
Cyber Vision Prefix	Enter an alphanumeric string to identify dynamic objects from this Cyber Vision's IP address when objects are sent to Secure Firewall Management Center . If you have one Cyber Vision IP address, you can enter any value such as 1 .
Pull Interval	(Default 60 seconds.) Interval at which data mappings are retrieved from Cyber Vision. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
IP	(Required.) Enter the Cyber Vision IP address.
Port	(Required.) Enter the Cyber Vision listen port.
Token	(Required.) Enter the API token.

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.

Create a Generic Text Connector

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

Before you begin

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



For example, you might have a list of IP addresses for an "allow list" in access control rules and another list of IP addresses for a "block list" in access control rules.

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



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

Procedure

-
- Step 1** Log in to the 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 a **Name** and an optional description.
- Step 5** (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from the text file. The default is 30 seconds.
- The minimum value for **Pull Interval** is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
- Step 6** In the **URLs** field, enter each URL from which to retrieve IP addresses, one URL per line.
- Step 7** (Optional.) Click **Add another URL** to add an additional URL to monitor.
- Step 8** (Optional.) If a certificate chain is required for a secure connection to the web server, you have the following options:
- Click **Get Certificate** > **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in [Manually Get a Certificate Authority \(CA\) Chain, on page 46](#).
 - Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.
- Step 9** Click **Test** and make sure the test succeeds before you save the connector.
- Step 10** Click **Save**.
- Step 11** Make sure **Ok** is displayed in the Status column.
-

Create a GitHub Connector



This section discusses how to create a GitHub connector that sends data to the Secure Firewall Management Center for use in access control policies. The IP addresses associated with these tags are maintained by GitHub. You do not have to create a dynamic attributes filters.

For more information, see [About GitHub's IP addresses](#).



Note Do not change the URL because doing so will fail to retrieve any IP addresses.

Procedure

-
- Step 1** Log in to the 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 a **Name** and an optional description.
- Step 5** (Optional.) In the **Pull Interval** field, change the frequency, in seconds, at which the dynamic attributes connector retrieves IP addresses from GitHub. The default is 21,600 seconds (6 hours).
- Step 6** Click **Test** and make sure the test succeeds before you save the connector.
- Step 7** Click **Save**.
- Step 8** Make sure **Ok** is displayed in the Status column.
-

Google Cloud Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from Google Cloud to Secure Firewall Management Center for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from Google Cloud:

- *Labels*, key-value pairs you can use to organize your Google Cloud resources.
For more information, see [Creating and Managing Labels](#) in the Google Cloud documentation.
- *Network tags*, key-value pairs associated with an organization, folder, or project.
For more information, see [Creating and Managing Tags](#) in the Google Cloud documentation.
- *IP addresses* of virtual machines in Google Cloud.

Minimum permissions required

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

Create a Google Cloud User with Minimal Permissions for the Cisco Secure Dynamic Attributes Connector

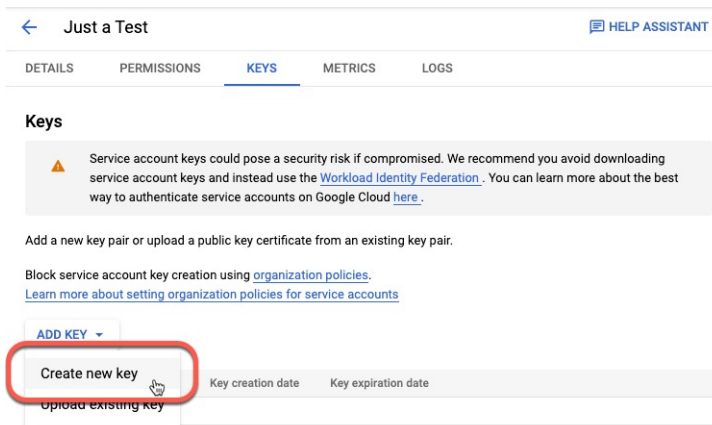
This task discusses how to set up a service account with minimum permissions to send dynamic attributes to Secure Firewall Management Center. For a list of these attributes, see [Google Cloud Connector—About User Permissions and Imported Data](#), on page 29.

Before you begin

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

Procedure

-
- Step 1** Log in to your Google Cloud account as a user with the owner role.
- Step 2** Click **IAM & Admin > Service Accounts > Create Service Account**.
- Step 3** Enter the following information:
- **Service account name:** A name to identify this account; for example, **CSDAC**.
 - **Service account ID:** Should be populated with a unique value after you enter the service account name.
 - **Service account description:** Enter an optional description.
- For more information about service accounts, see [Understanding Service Accounts](#) in the Google Cloud documentation.
- Step 4** Click **Create and Continue**.
- Step 5** Follow the prompts on your screen until the Grant users access to this service account section is displayed.
- Step 6** Grant the user the **Basic > Viewer** role.
- Step 7** Click **Done**.
- A list of service accounts is displayed.
- Step 8** Click **More** (⋮) at the end of the row of the service account you created.
- Step 9** Click **Manage Keys**.
- Step 10** Click **Add Key > Create New Key**.



Step 11 Click **JSON**.

Step 12 Click **Create**.

The JSON key is downloaded to your computer.

Step 13 Keep the key handy when you configure the GCP connector.

What to do next

See [Create a Google Cloud Connector](#), on page 31.

Create a Google Cloud Connector

Before you begin



Have your Google Cloud JSON-formatted service account data ready; it's required to set up the connector.

Procedure

Step 1 Log in to the 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.

Value	Description
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from AWS. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
GCP region	(Required.) Enter the GCP region in which your Google Cloud is located. For more information, see Regions and Zones in the Google Cloud documentation.
Service account	Paste the JSON code for your Google Cloud service account.

Step 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.

Create an Office 365 Connector

This task discusses how to create a connector for Office 365 tags to send data to the Secure Firewall Management Center for use in access control policies. The IP addresses associated with these tags are updated every week by Microsoft. You do not have to create a dynamic attributes filter to use the data.



For more information, see [Office 365 URLs and IP address ranges](#) on docs.microsoft.com.

Procedure

Step 1 Log in to the 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.

Value	Description
Pull Interval	(Default 30 seconds.) Interval at which IP mappings are retrieved from Azure. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
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.

vCenter Connector—About User Permissions and Imported Data

The Cisco Secure Dynamic Attributes Connector imports dynamic attributes from vCenter to Secure Firewall Management Center for use in access control policies.

Dynamic attributes imported

We import the following dynamic attributes from vCenter:

- *Operating system*
- *MAC address*
- *IP addresses*
- *NSX tags*

Minimum permissions required

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

Create a vCenter 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 Secure Firewall Management Center. For a list of these attributes, see [vCenter Connector—About User Permissions and Imported Data](#), on page 33.

Before you begin

You must already have set up your vCenter Server account. For more information about doing that, see [About vCenter Server Installation and Setup](#) in the vCenter documentation.

Procedure

-
- Step 1** Log into vCenter as an administrator.
- Step 2** Click **Menu > Administration**.
- Step 3** In the left pane, click **Single Sign On > Users and Groups**.
- Step 4** From the **Domain** list, click the name of a domain to add the user.
- Step 5** Click **Add User**.
- Step 6** Enter the requested information and click **Add**.
- Step 7** In the left pane, click **Access Control > Global Permissions**.
- Step 8** Click **Add**(+).
- Step 9** From the **User** field, click the name of the vCenter domain in which you created the user.
- Step 10** In the search field, enter part of the user's name.
- Step 11** From the **Role** list, click **Read-only**.
- Step 12** Select the **Propagate to children** check box.

Add Permission | Global Permission Root

User vsphere.local

Q just-a-test

Role Read-only

☒ Propagate to children

CANCEL OK

- Step 13** Click **OK**.
-

What to do next

See [Create a vCenter Connector](#), on page 34.

Create a vCenter Connector

This task discusses how to create a connector for VMware vCenter to send data to the Secure Firewall Management Center 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 46](#).

Procedure

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. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Host	(Required.) Enter any of the following: <ul style="list-style-type: none"> • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port <p><i>Do not</i> enter a scheme (such as https://) or trailing slash. For example, myvcenter.example.com or 192.0.2.100:9090</p>
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter NSX-T .
NSX Password	Enter the NSX user's password.

Value	Description
vCenter Certificate	<p>You have the following options:</p> <ul style="list-style-type: none"> Click Get Certificate > Fetch to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 46. Click Get Certificate > Browse from file to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:

Add FMC Adapter

Name *

Description

Domain

IP *

Port *

User *

Password *

Secondary IP

Secondary Port

Secondary User

Secondary Password

FMC Server Certificate *

firepower

14733

rest

firepower

14833

Updated 3IN CERTIFICATE-----

Test

Cancel

Save

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 46](#).

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

Step 6 Click **Save**.

Create a Webex Connector

This section discusses how to create a Webex connector that sends data to the Secure Firewall Management Center for use in access control policies. The IP addresses associated with these tags are maintained by Webex. You do not have to create a dynamic attributes filters.



For more information, see [Port Reference for Webex Calling](#).

Procedure

Step 1 Log in to the 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 Webex. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) (Required.) Slide to enabled to retrieve any reserved IP addresses.

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.

Create a Zoom Connector

This section discusses how to create a Zoom connector that sends data to the Secure Firewall Management Center for use in access control policies. The IP addresses associated with these tags are maintained by Zoom. You do not have to create a dynamic attributes filters.



For more information, see [Zoom network firewall or proxy server settings](#).

Procedure

Step 1 Log in to the 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 Zoom. The minimum value for Pull Interval is 1 second. You can set the maximum to any value you want. We recommend against setting the minimum to a low value because it can generate a lot of traffic, and, when applicable, can result in your being billed for the traffic.
Provider Reserved IPs	(Required.) Slide to enabled to retrieve any reserved IP addresses.

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.

Create an Adapter

An *adapter* is a secure connection to management center 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 Secure Firewall Management Center .

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



Note Deleting an adapter does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

Related Topics

[How to Create an On-Prem Firewall Management Center Adapter](#), on page 41

[How to Create a Cloud-delivered Firewall Management Center Adapter](#), on page 45

[Create an Adapter](#), on page 38

[Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39

[Create a Cloud-delivered Firewall Management Center Adapter](#), on page 44

[Get Your Base URL and API Token](#), on page 44

[Manually Get a Certificate Authority \(CA\) Chain](#), on page 46

Create a Secure Firewall Management Center User for the Dynamic Attributes Connector

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

The Secure Firewall Management Center user must have Access Admin privileges at least.

Procedure

- Step 1** Log in to the Secure Firewall Management Center 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

☐ 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

Default User Roles

Cancel

Save

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 38](#)

Related Topics

[How to Create an On-Prem Firewall Management Center Adapter, on page 41](#)

[How to Create a Cloud-delivered Firewall Management Center Adapter, on page 45](#)

[Create an Adapter, on page 38](#)

[Create a Secure Firewall Management Center User for the Dynamic Attributes Connector, on page 39](#)

[Create a Cloud-delivered Firewall Management Center Adapter, on page 44](#)

[Get Your Base URL and API Token](#), on page 44

[Manually Get a Certificate Authority \(CA\) Chain](#), on page 46

How to Create an On-Prem Firewall Management Center Adapter

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to the Secure Firewall Management Center .



Note Deleting an adapter does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

Before you begin



See [Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39.

Procedure

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.

Note

Deleting an adapter does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

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 Secure Firewall Management Center domain in which to create dynamic objects. Leave the field blank to create dynamic objects in the Global domain. For example, Global/MySubdomain

Value	Description
IP	(Required.) Enter your Secure Firewall Management Center'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 Secure Firewall Management Center.
User	(Required.) Enter the name of an Secure Firewall Management Center user with the Network Admin role at minimum.
Password	(Required.) Enter the user's password.
Secondary IP	(High availability only.) Enter the secondary Secure Firewall Management Centers 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 Secure Firewall Management Center.
Secondary User	(High availability only.) Enter the name of a secondary Secure Firewall Management Center user with the Network Admin role at minimum.
Secondary Password	(High availability only.) Enter the user's password.
Server Certificate	<p>You have the following options:</p> <ul style="list-style-type: none"> • Click Get Certificate > Fetch to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually Get a Certificate Authority (CA) Chain, on page 46. • Click Get Certificate > Browse from file to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:

Add FMC Adapter

Name *

Describe *

Domain *

IP *

Port *

User *

Password *

Secondary IP

Secondary Port

Secondary User

Secondary Password

FMC Server Certificate *

firepower

14733

rest

firepower

14833

Updated 3IN CERTIFICATE-----

Test

Cancel

Save

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

Information

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 46.

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

Step 6 Click **Save**.

Related Topics

- [How to Create an On-Prem Firewall Management Center Adapter](#), on page 41
- [How to Create a Cloud-delivered Firewall Management Center Adapter](#), on page 45
- [Create an Adapter](#), on page 38
- [Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39
- [Create a Cloud-delivered Firewall Management Center Adapter](#), on page 44
- [Get Your Base URL and API Token](#), on page 44
- [Manually Get a Certificate Authority \(CA\) Chain](#), on page 46

Create a Cloud-delivered Firewall Management Center Adapter

This topic discusses how to create an adapter to push dynamic objects from the dynamic attributes connector to a managed management center on the Secure Firewall Management Center.

You can create the following adapters:

- *On-Prem Firewall Management Center* for an on-premises Secure Firewall Management Center
- *Cloud-delivered Firewall Management Center* for devices managed by CDO

Before you can create a Cloud-delivered Firewall Management Center, get the following information first: [Get Your Base URL and API Token, on page 44](#).

Related Topics

[How to Create an On-Prem Firewall Management Center Adapter, on page 41](#)

[How to Create a Cloud-delivered Firewall Management Center Adapter, on page 45](#)

[Create an Adapter, on page 38](#)

[Create a Secure Firewall Management Center User for the Dynamic Attributes Connector, on page 39](#)

[Create a Cloud-delivered Firewall Management Center Adapter, on page 44](#)

[Get Your Base URL and API Token, on page 44](#)

[Manually Get a Certificate Authority \(CA\) Chain, on page 46](#)

Get Your Base URL and API Token

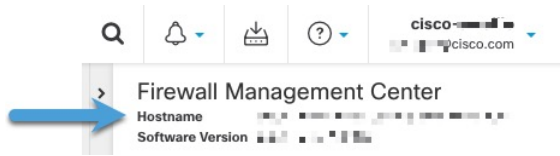
This task dicusses how to get the URL and API token from CDO that are required to create a Cloud-delivered Firewall Management Center adapter.

Before you begin

You must be a CDO Super Admin to complete the tasks discussed in this section.

Procedure

-
- Step 1** Log in to CDO as a user with the Super Admin role.
 - Step 2** In the upper right corner of the page, click **Settings**.
 - Step 3** Click **General Settings**.
 - Step 4** Next to API Token, click **Refresh**.
 - Step 5** Copy the API token to a text file for later use.
 - Step 6** Click .
 - Step 7** Click the name of the management center to which to send dynamic attributes connector data.
 - Step 8** The value of **Hostname**, preceded by **https://**, is the base URL.
An example follows:



What to do next

[How to Create a Cloud-delivered Firewall Management Center Adapter, on page 45.](#)

Related Topics

[How to Create an On-Prem Firewall Management Center Adapter, on page 41](#)

[How to Create a Cloud-delivered Firewall Management Center Adapter, on page 45](#)

[Create an Adapter, on page 38](#)

[Create a Secure Firewall Management Center User for the Dynamic Attributes Connector, on page 39](#)

[Create a Cloud-delivered Firewall Management Center Adapter, on page 44](#)

[Get Your Base URL and API Token, on page 44](#)

[Manually Get a Certificate Authority \(CA\) Chain, on page 46](#)

How to Create a Cloud-delivered Firewall Management Center Adapter

This task discusses how to create a Cloud-delivered Firewall Management Center adapter that sends data from the dynamic attributes connector to a device managed by CDO.

Before you begin



You must get the management center base URL and API token from CDO before you can complete this task. For more information, see [Get Your Base URL and API Token, on page 44.](#)

Procedure

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.

Note

Deleting an adapter does not delete dynamic objects created by the adapter. If you wish to delete those objects permanently, do so on the device associated with the adapter.

Editing an adapter does not push updated objects to the associated device. If you must change the adapter's settings, delete the adapter and add it again.

Step 4 Enter the following information.

Value	Description
Name	(Required.) Enter a unique name to identify this adapter.
Description	Optional description of the adapter.
Base Url	(Required.) Use the Base URL you found in Get Your Base URL and API Token, on page 44 .
API Token	(Required.) Use the API token you found in Get Your Base URL and API Token, on page 44 .

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

Step 6 Click **Save**.

What to do next

[Create Dynamic Attributes Filters, on page 49](#).

Related Topics

[How to Create an On-Prem Firewall Management Center Adapter, on page 41](#)

[How to Create a Cloud-delivered Firewall Management Center Adapter, on page 45](#)

[Create an Adapter, on page 38](#)

[Create a Secure Firewall Management Center User for the Dynamic Attributes Connector, on page 39](#)

[Create a Cloud-delivered Firewall Management Center Adapter, on page 44](#)

[Get Your Base URL and API Token, on page 44](#)

[Manually Get a Certificate Authority \(CA\) Chain, on page 46](#)

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 or Management Center.

The *certificate chain* is the root certificate and all subordinate certificates.

You can optionally use one of these procedures to connect to the following:

- vCenter or NSX
- Management Center

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.
2. Enter the following command.

```
security verify-cert -P url[:port]
```

where url is the URL (including scheme) to vCenter or Management Center. For example:

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

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

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

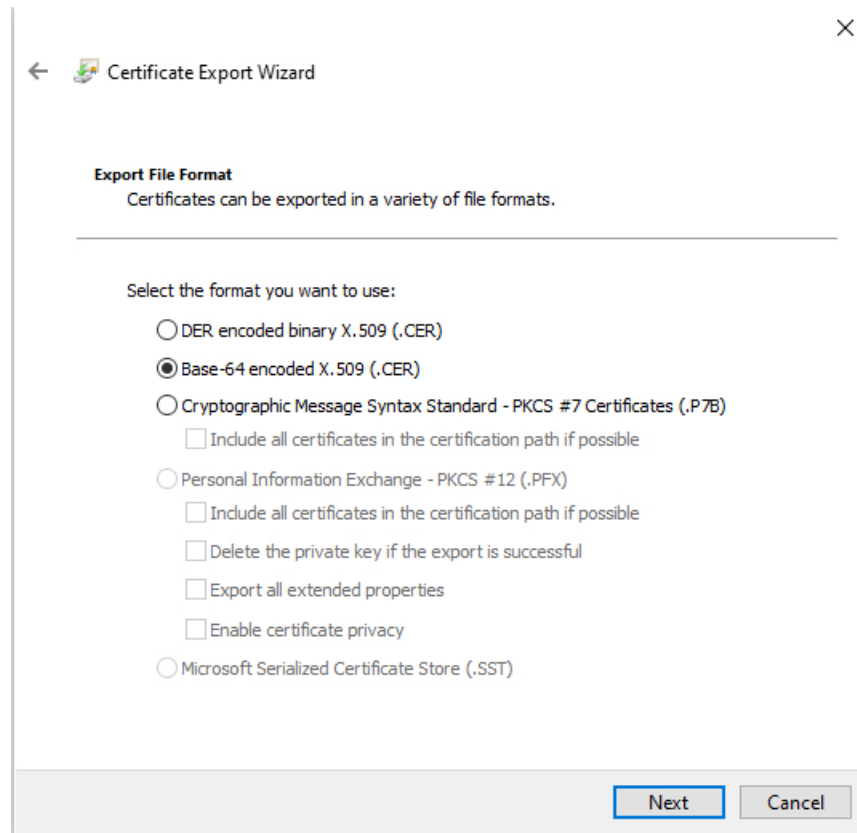
3. Save the entire certificate chain to a plaintext file.
 - *Include* all -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- delimiters.
 - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >)) as well as the angle brackets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

Get a Certificate Chain—Windows Chrome

Use this procedure to get a certificate chain using the Chrome browser on Windows.

1. Log in to vCenter or Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.
8. Click **Copy to File**.
9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)** as the following figure shows.

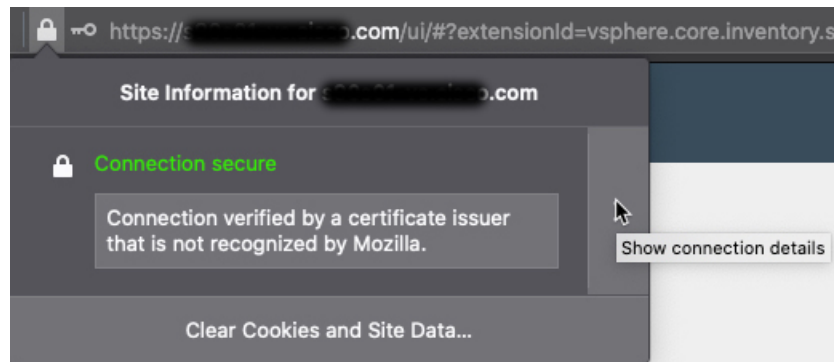


10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.
You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter or Management Center.

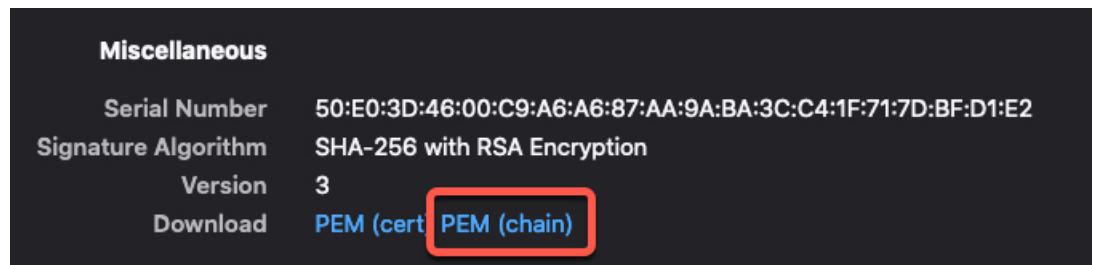
Get a Certificate Chain—Windows Firefox

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 Management Center using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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



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

Related Topics

- [How to Create an On-Prem Firewall Management Center Adapter](#), on page 41
- [How to Create a Cloud-delivered Firewall Management Center Adapter](#), on page 45
- [Create an Adapter](#), on page 38
- [Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39
- [Create a Cloud-delivered Firewall Management Center Adapter](#), on page 44
- [Get Your Base URL and API Token](#), on page 44
- [Manually Get a Certificate Authority \(CA\) Chain](#), on page 46

Create Dynamic Attributes Filters

Dynamic attributes filters that you define using the Cisco Secure Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, you could restrict access to an AWS server for the Finance Department to only members of the Finance group defined in Microsoft Active Directory.



Note You cannot create dynamic attributes filters for AWS, Azure, Azure Service Tags, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.



Before you begin

[Create a Connector, on page 15](#)



Procedure

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 Secure Firewall Management Center Object Manager (External Attributes > Dynamic Object).
Connector	From the list, click the name of a connector to use.
Query	<ul style="list-style-type: none"> • Add a new filter: click Add icon (). • Edit or delete a filter: Click More (), then click Edit or Delete at the end of the row.

Step 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: <ul style="list-style-type: none"> • Equals to exactly match the key to the value. • Contains to match the key to the value if any part of the value matches.

Item	Description
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 Secure Firewall Management Center .

- Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.
- Click **Objects > Object Management**.
- In the left pane, click **External Attributes > Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic Attribute Filter Examples

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

Examples: vCenter

The following example shows one criterion: a VLAN.

Edit Dynamic Attribute Filter

Name* TestFilter Connector* vCenter

Query* +

Type	Op.	Value
all network	eq	any myVLAN

> Show Preview Cancel Save

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

Add Dynamic Attribute Filter

Name* vCenter hosts Connector* vCenter

Query* +

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

> Show Preview Cancel Save

Example: Azure

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

Add Dynamic Attribute Filter

Name *		Connector *	
<input type="text" value="Azure Finance"/>		<input type="text" value="Azure"/>	
Query *			
Type	Op.	Value	
<input type="text" value="all"/> Finance	eq	<input type="text" value="any"/> App	

> Show Preview Cancel Save

Example: AWS

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

Add Dynamic Attribute Filter

Name *		Connector *	
<input type="text" value="AWS"/>		<input type="text" value="AWS"/>	
Query *			
Type	Op.	Value	
<input type="text" value="all"/> FinanceApp	eq	<input type="text" value="any"/> 1	

> Show Preview Cancel Save

Manually Get a Certificate Authority (CA) Chain

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

The *certificate chain* is the root certificate and all subordinate certificates.

You can optionally use one of these procedures to connect to the following:

- vCenter or NSX
- Management Center

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.
2. Enter the following command.

```
security verify-cert -P url[:port]
```

where url is the URL (including scheme) to vCenter or Management Center. For example:

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

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

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

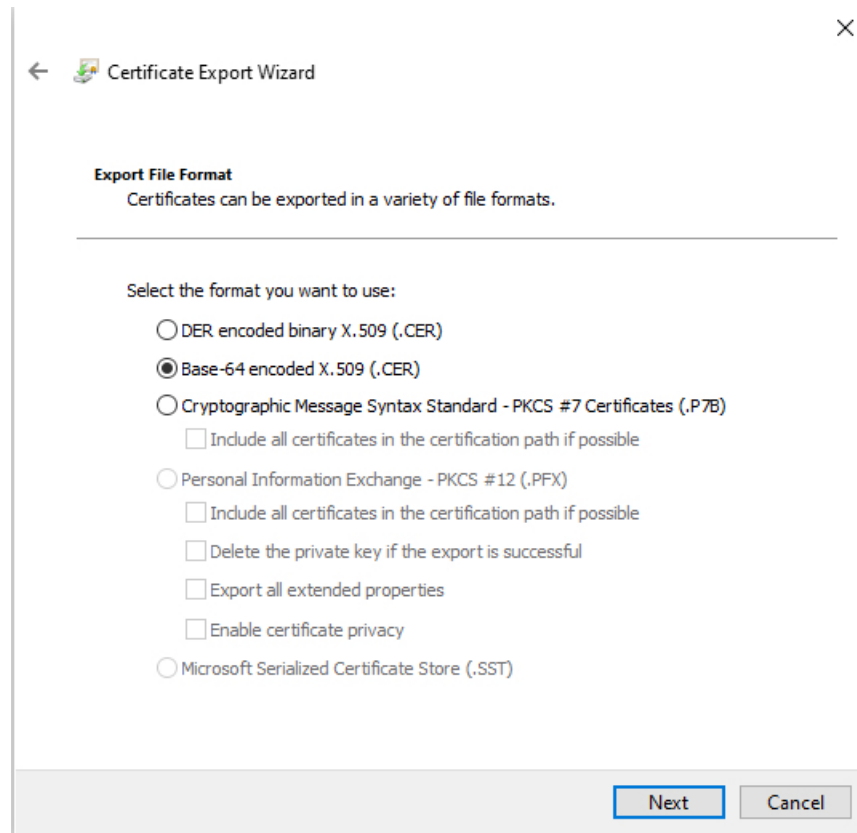
3. Save the entire certificate chain to a plaintext file.
 - *Include* all -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- delimiters.
 - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

Get a Certificate Chain—Windows Chrome

Use this procedure to get a certificate chain using the Chrome browser on Windows.

1. Log in to vCenter or Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.
8. Click **Copy to File**.
9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.

When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)** as the following figure shows.

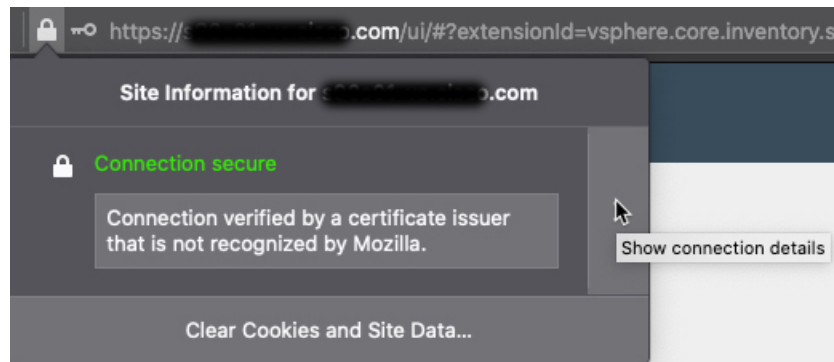


10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.
You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter or Management Center.

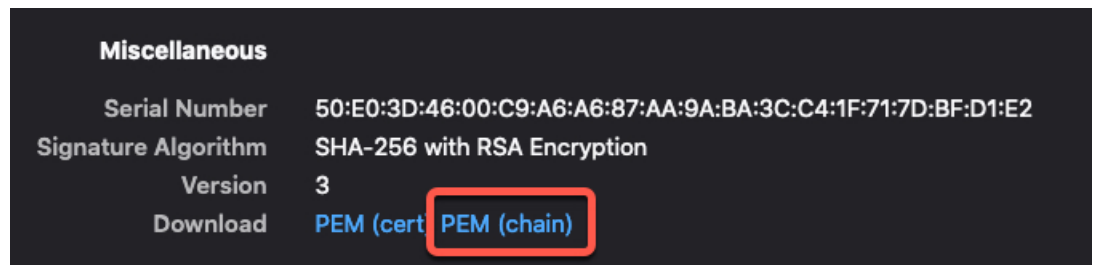
Get a Certificate Chain—Windows Firefox

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 Management Center using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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



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

Related Topics

- [How to Create an On-Prem Firewall Management Center Adapter](#), on page 41
- [How to Create a Cloud-delivered Firewall Management Center Adapter](#), on page 45
- [Create an Adapter](#), on page 38
- [Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39
- [Create a Cloud-delivered Firewall Management Center Adapter](#), on page 44
- [Get Your Base URL and API Token](#), on page 44
- [Manually Get a Certificate Authority \(CA\) Chain](#), on page 46



CHAPTER 4

Use Dynamic Objects in Access Control Policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the Secure Firewall Management Center as dynamic objects, in access control rules.

- [About Dynamic Objects in Access Control Rules, on page 57](#)
- [Create Access Control Rules Using Dynamic Attributes Filters, on page 57](#)

About Dynamic Objects in Access Control Rules

A *dynamic object* is automatically pushed from the dynamic attributes connector to the Secure Firewall Manager after you create connectors and save a dynamic attributes filter on the connector.

You can use 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 AWS, Azure, Azure Service Tags, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create Access Control Rules Using Dynamic Attributes Filters

This topic discusses how to create access control rules using dynamic objects (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 49](#).



Note You cannot create dynamic attributes filters for AWS, Azure, Azure Service Tags, GitHub, Google Cloud, Office 365, vCenter, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Procedure

- Step 1** Log in to Secure Firewall Management Center .
- Step 2** Click **Policies > Access Control heading > 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 screenshot shows the 'Add Rule' configuration interface. At the top, there are fields for 'Name', 'Enabled' (checked), 'Insert' (set to 'into Mandatory'), 'Action' (set to 'Allow'), and 'Time Range' (set to 'None'). Below these are tabs for 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes' (selected), 'Inspection', 'Logging', and 'Comments'. The 'Available Attributes' section on the left has a search bar and a list where 'Dynamic Objects' is expanded, showing 'FinanceNetwork' as a selectable item. To the right are two empty boxes for 'Selected Source Attributes (0)' and 'Selected Destination Attributes (0)', each with an 'Add to Source' or 'Add to Destination' button. At the bottom right are 'Cancel' and 'Add' buttons.

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

- Step 7** Add the desired object to source or destination attributes.
- Step 8** Add other conditions to the rule if desired.

What to do next

[Dynamic Attributes Rule Conditions](#) in the *Cisco Secure Firewall Management Center Device Configuration Guide*.



CHAPTER 5

Troubleshoot the Dynamic Attributes Connector

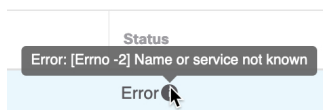
How to troubleshoot issues with the dynamic attributes connector, including using provided tools.

- [Troubleshoot Error Messages, on page 59](#)
- [Troubleshoot Using the Command Line, on page 61](#)
- [Manually Get a Certificate Authority \(CA\) Chain, on page 63](#)

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 a connector. An example follows; yours might look different.



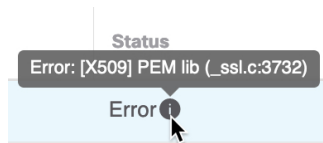
Solution: Edit the connector and check for:

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

For more information, see [Manually Get a Certificate Authority \(CA\) Chain, on page 46](#).

Problem: [X509 PEM lib]

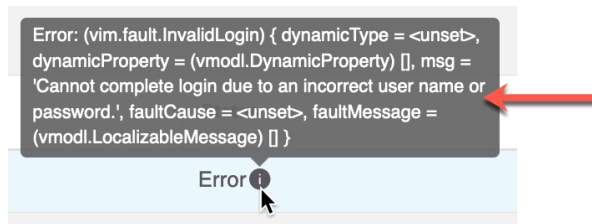
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and check the CA chain. For more information, see [Manually Get a Certificate Authority \(CA\) Chain](#), on page 46.

Problem: Incorrect username or password

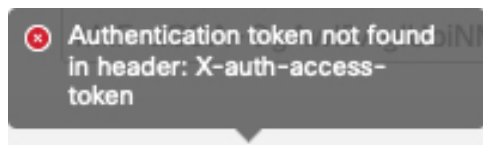
This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



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

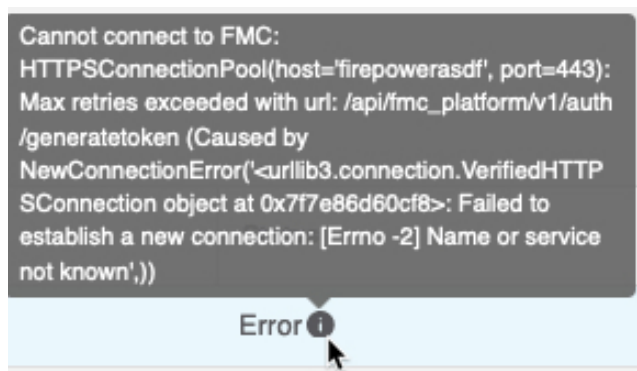
Problem: Authentication token not found in header

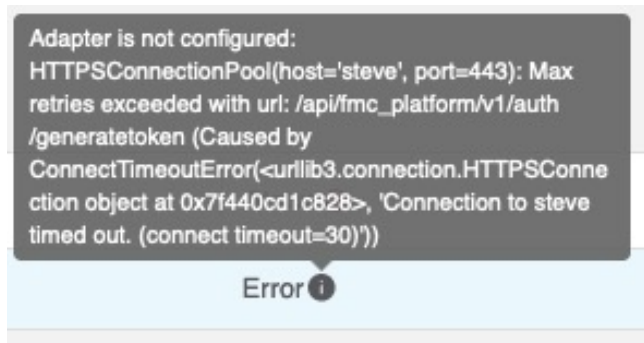
This error is displayed when you attempt to test the connection with an adapter user that does not have sufficient privileges on the Secure Firewall Management Center :



Problem: Timeout or max retries error for an adapter

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





Solution: Do all of the following:

- Verify the management center is running 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 46.

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 Cisco Secure 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 Secure Firewall Management Center

To verify your connectors are creating objects on the Secure Firewall Management Center, you can use the following command on the Secure Firewall Management Center 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": []
}
```

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 or Management Center.

The *certificate chain* is the root certificate and all subordinate certificates.

You can optionally use one of these procedures to connect to the following:

- vCenter or NSX
- Management Center

Get a Certificate Chain—Mac (Chrome and Firefox)

Use this procedure to get a certificate chain using the Chrome and Firefox browsers on Mac OS.

1. Open a Terminal window.
2. Enter the following command.

```
security verify-cert -P url[:port]
```

where url is the URL (including scheme) to vCenter or Management Center. For example:

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

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

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

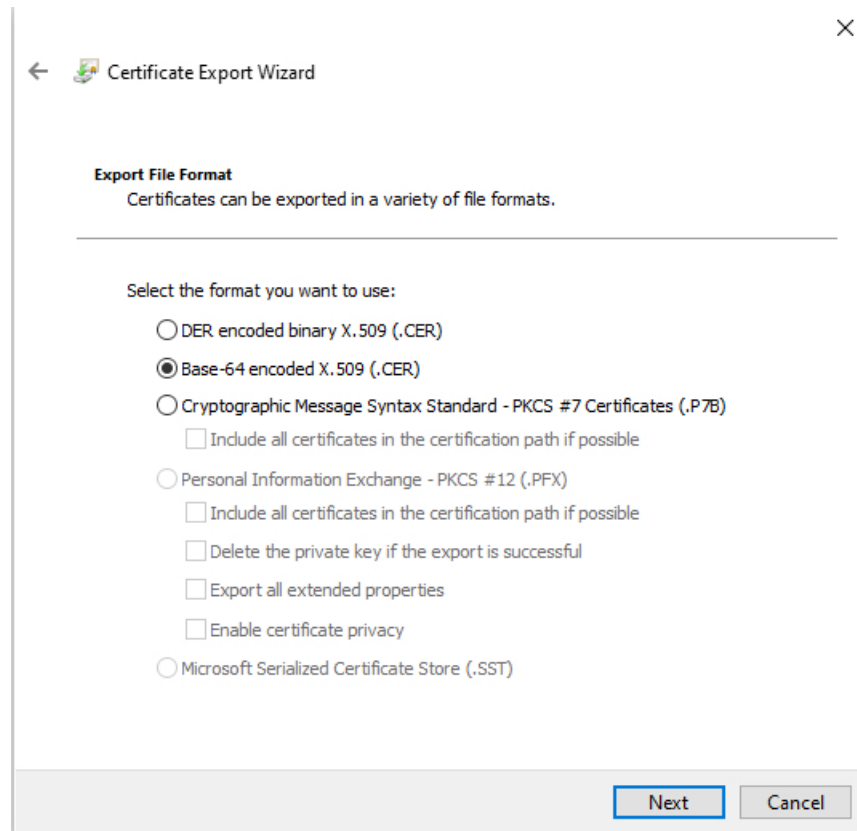
3. Save the entire certificate chain to a plaintext file.
 - *Include* all -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- delimiters.
 - *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets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

Get a Certificate Chain—Windows Chrome

Use this procedure to get a certificate chain using the Chrome browser on Windows.

1. Log in to vCenter or Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.
7. Click the **Details** tab.

8. Click **Copy to File**.
9. Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain.
When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)** as the following figure shows.

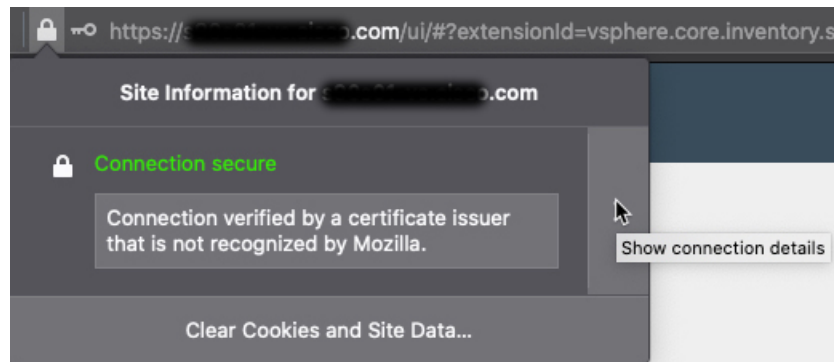


10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.
You must paste each certificate in the text editor in order, first to last.
13. Repeat these tasks for vCenter or Management Center.

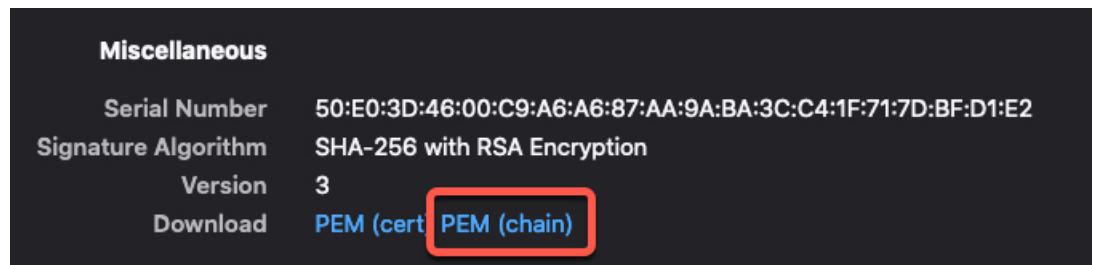
Get a Certificate Chain—Windows Firefox

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 Management Center using Firefox.
2. Click the lock to the left of the host name.
3. Click the right arrow (**Show connection details**). The following figure shows an example.



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



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

Related Topics

- [How to Create an On-Prem Firewall Management Center Adapter](#), on page 41
- [How to Create a Cloud-delivered Firewall Management Center Adapter](#), on page 45
- [Create an Adapter](#), on page 38
- [Create a Secure Firewall Management Center User for the Dynamic Attributes Connector](#), on page 39
- [Create a Cloud-delivered Firewall Management Center Adapter](#), on page 44
- [Get Your Base URL and API Token](#), on page 44
- [Manually Get a Certificate Authority \(CA\) Chain](#), on page 46



APPENDIX **A**

Security and Internet Access

Lists of URLs used by the dynamic attributes connector when communicating with cloud service providers and the Secure Firewall Management Center .

- [Security Requirements, on page 67](#)
- [Internet Access Requirements, on page 67](#)

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 Secure Firewall Management Center reside on the same network, you can connect the Secure Firewall Management Center to the same protected internal network as the dynamic attributes connector.

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

Internet Access Requirements

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

The following information informs you of the URLs the dynamic attributes connector use to communicate with the Secure Firewall Management Center and with external servers.

Table 3: Cisco Secure Dynamic Attributes Connector access requirements

URL	Reason
<code>https://fmc-ip/api/fmc_platform/v1/auth/generatetoken</code>	Authentication
<code>https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects</code>	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: Cisco Secure 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>

Cisco Secure Dynamic Attributes Connector Azure access requirements

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