Dynamic Attributes Connector

The following topics discuss how to configure and use the Dynamic Attributes Connector.

About the Dynamic Attributes Connector

The dynamic attributes connector enables your access control and DNS policy to adapt in real time to the changes in public and private cloud workloads and business-critical software-as-a-service (SaaS) applications. It simplifies policy management by keeping rules up to date without tedious manual updates and policy deployment. 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.

Supported connectors

We currently support:

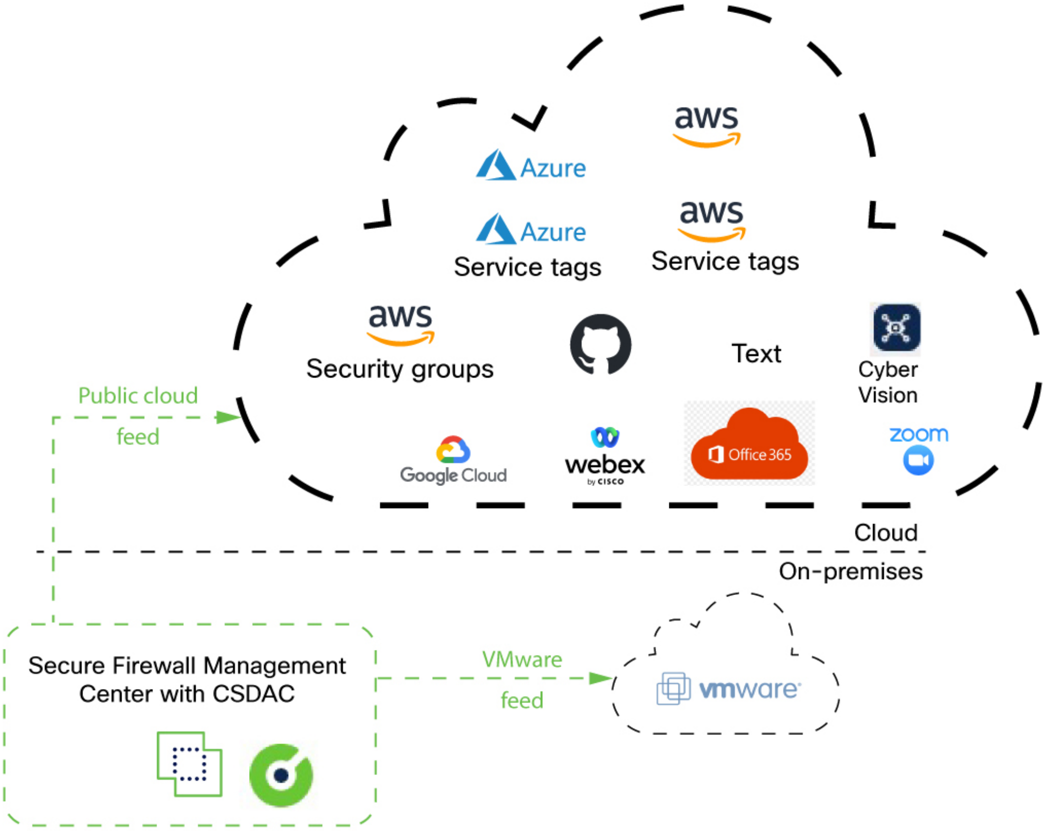
Table 1: List of supported connectors by dynamic attributes connector version and platform

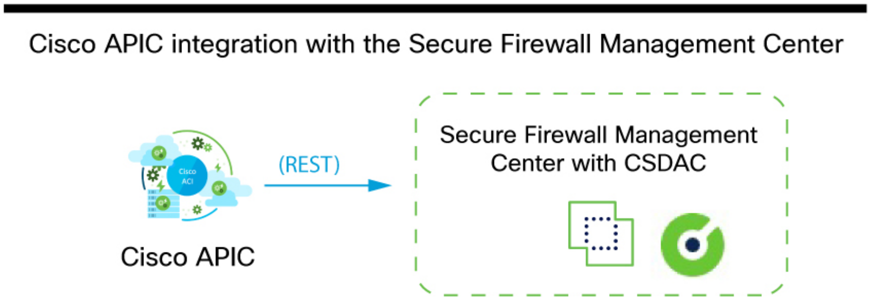
CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

How it works

This topic discusses the architecture of the Dynamic Attributes Connector.

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




Cisco APIC integration with the Secure Firewall Management Center
Cisco ACI
(REST)
Cisco APIC
Secure Firewall Management
Center with CSDAC

- The system supports certain public cloud providers.

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

- The dynamic attributes connector is provided with Secure Firewall Management Center.

Related Topics

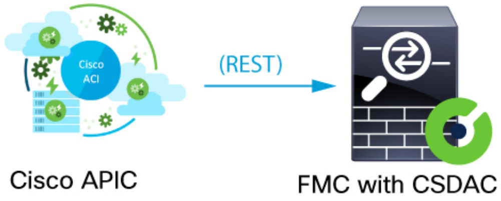
- Enable the dynamic attributes connector
- About the dashboard, on page 10

About the Cisco APIC integration with the Secure Firewall Management Center

The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to the Secure Firewall Management Center.

Cisco APIC defines endpoint groups (EPGs) and endpoint security groups (ESGs) that have network object groups. Create a connector in the dynamic attributes connector that pulls that data from Cisco APIC tenants to the Secure Firewall Management Center on which you can use those objects in access control rules.

The following figure shows how the integration works.



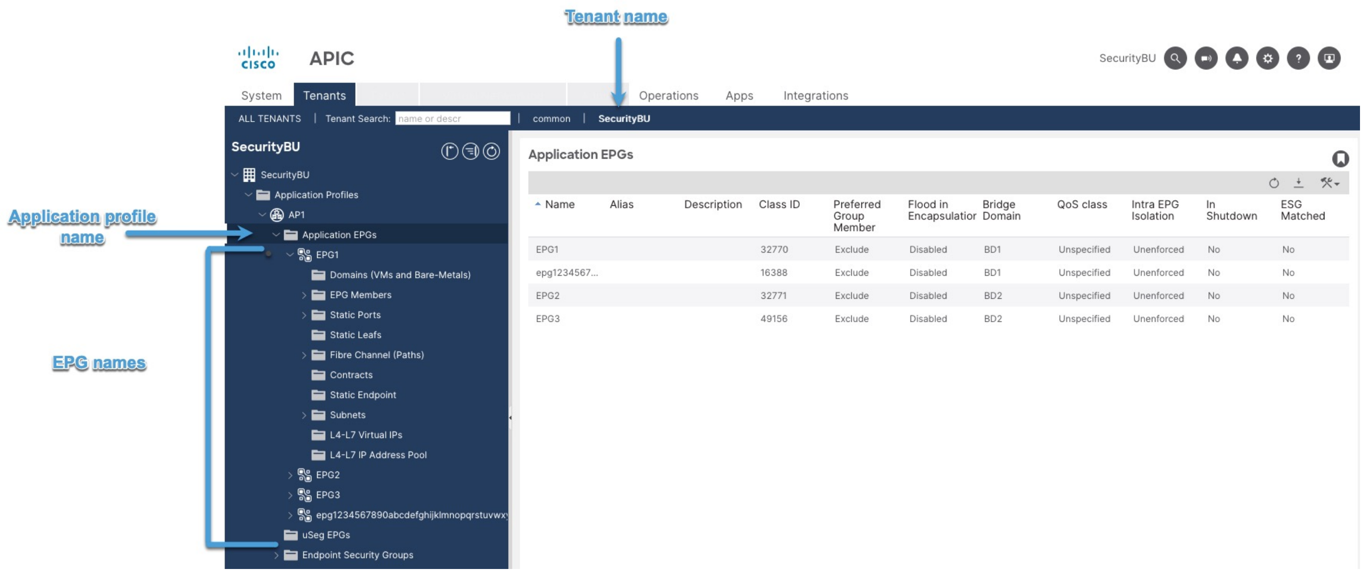
Sample configuration

The following sample configuration shows how network object groups are named in the Secure Firewall Management Center based on names in APIC and the APIC connector (not shown).

Network object group names are a concatenation of (in order):

- Cisco ACI Endpoint Update App **Site Prefix** value

  Cisco APIC tenant name); in this example, `CSDAC`.
- Cisco APIC application profile name (in this example, `AP1`)
- Cisco APIC EPG name (in this example, `EPG1` through `EPG4`)



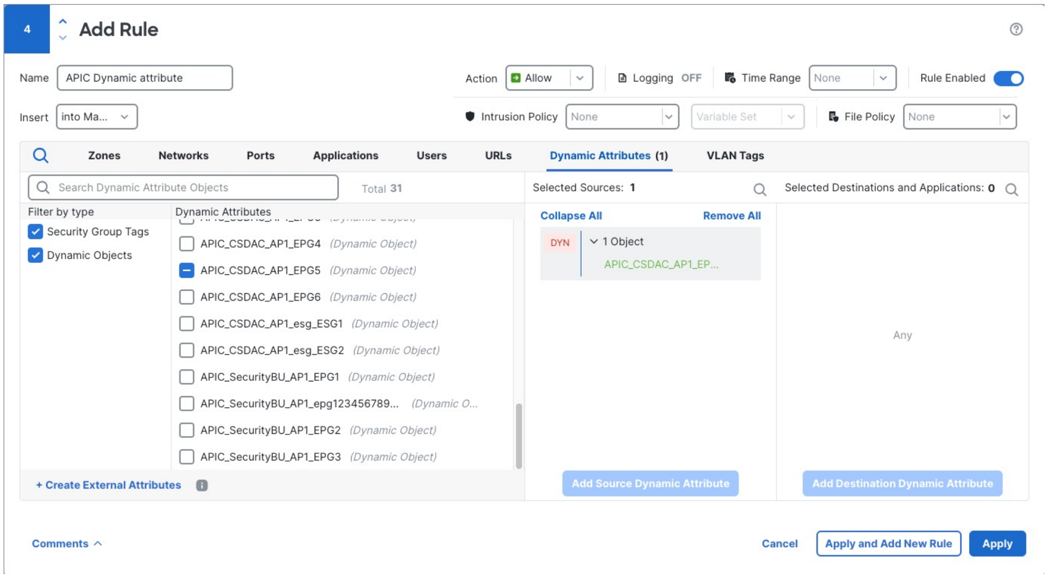
Application EPGs

Name	Alias	Description	Class ID	Preferred Group Member	Flood in Encapsulatior	Bridge Domain	QoS class	Intra EPG Isolation	In Shutdown	ESG Matched
EPG1			32770	Exclude	Disabled	BD1	Unspecified	Unenforced	No	No
epg1234567...			16388	Exclude	Disabled	BD1	Unspecified	Unenforced	No	No
EPG2			32771	Exclude	Disabled	BD2	Unspecified	Unenforced	No	No
EPG3			49156	Exclude	Disabled	BD2	Unspecified	Unenforced	No	No

The following figure shows sample Cisco APIC dynamic object names used in an access control rule.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```



Name: APIC Dynamic attribute

Insert: into Ma...

Action: Allow

Logging: OFF

Time Range: None

Rule Enabled

Intrusion Policy: None

Variable Set

File Policy: None

Total 31

Selected Sources: 1

Selected Destinations and Applications: 0

Filter by type

☑ Security Group Tags

☑ Dynamic Objects

Dynamic Attributes

□ APIC_CSDAC_AP1_EPG4 *(Dynamic Object)*

☑ APIC_CSDAC_AP1_EPG5 *(Dynamic Object)*

□ APIC_CSDAC_AP1_EPG6 *(Dynamic Object)*

□ APIC_CSDAC_AP1_esg_ESG1 *(Dynamic Object)*

□ APIC_CSDAC_AP1_esg_ESG2 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_EPG1 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_epg123456789... *(Dynamic O...*

□ APIC_SecurityBU_AP1_EPG2 *(Dynamic Object)*

□ APIC_SecurityBU_AP1_EPG3 *(Dynamic Object)*

1 Object

APIC_CSDAC_AP1_EP...

More information

- For more information about the dynamic attributes connector in the Secure Firewall Management Center, see Secure Firewall Management Center Device Configuration Guide.
- APIC Roles and Privileges Matrix
- Endpoint Security Groups
- Basic User Tenant Configuration

History for the dynamic attributes connector

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
DNS rule support for dynamic objects and security group tags.	10.0.0	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the Dynamic Attributes tab to the add/edit DNS rule dialog box.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Dynamic firewall	10.0.0	10.0.0	Previously, the Secure Firewall Management CenterSecure Firewall Management Center collected information about users exclusively from the configured identity source, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address. The dynamic firewall enables you to add user risk scores from Cisco Identity Intelligence to identity source-provided information so you can set policies based on always-current user posture and risk. We enable you to pair user identity with intelligence and use that information in reporting and access control policies. **New/modified screens**: • Click **Integrations** > **Dynamic Attributes Connector**. Then click ⋯ next to the name of the identity source and click **Create Dynamic Firewall**.
Cisco APIC connector	10.0.0	10.0.0	The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to . **New/updated screens:** • **Integrations** > **Dynamic Attributes Connector** > **Connectors** > **New Connector**
New connectors	7.6	20241127	AWS security groups, AWS service tags, and Cisco Cyber Vision These connectors can send an on-premises Secure Firewall Management Center dynamic objects as can Security Cloud Control. To receive dynamic objects from an on-premises dynamic attributes connector, version 3.0 of the on-premises dynamic attributes connector is required.
Dynamic Attributes Connector	7.4.0	7.4.0	This feature is introduced. The Dynamic Attributes Connector is now included in the Secure Firewall Management Center. You can use the dynamic attributes connector to get IP addresses from cloud-based platforms such as Microsoft Azure in access control rules without having to deploy to managed devices. More information: • The dynamic attributes connector included with this product: About the Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: *Cisco Secure Dynamic Attributes Connector Configuration Guide* New/modified screen: **Integrations** > **Dynamic Attributes Connector**

System requirements for the Dynamic Attributes Connector

The Dynamic Attributes Connector has the following memory requirements:

FMCv: Amount of RAM	Secure Firewall Management Center hardware model	Maximum number of (connectors + Azure AD realms)
At least 32 GB	Firepower 1000, Firepower 1600, vFMC	10
At least 64 GB	Firepower 2500, Firepower 2600,vFMC 300	20
At least 128 GB	Firepower 4500, Firepower 4600	30

The preceding limits apply to both virtual machines and physical machines.

The system prevents you from exceeding these limits to avoid deployment issues.

Enable the dynamic attributes connector

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access controland DNS rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integrations** > **Dynamic Attributes Connector**.

Step 3 Slide to **Enabled**.

Step 4 Messages are displayed while the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

Configure networks and subnets for Docker containers

The Dynamic Attributes Connector uses Docker containers to retrieve connector data in the Secure Firewall Management Center. To avoid conflicts with the Secure Firewall Management Center management interface and other IP addresses used in your network, you can optionally use the command discussed in this section to change Docker IP addresses and ranges.

About Docker networks

The Docker daemon is used by the dynamic attributes connector requires the following networks:

- `docker0` which is used internally by the Docker daemon.
- A series of IPv6 networks named `veth`*`number`*.

  These are internal bridge networks used by the dynamic attributes connector.
- Docker bridge networks used by dynamic attributes connector connectors named `br-`*`number`*.

Before you enable the dynamic attributes connector, there is only one Docker interface, named `docker0`, set to 172.18.0.1/16 (for a Secure Firewall Management Center Virtual; on-premises managers use different IP address ranges). The table in the Examples section provides details.

Change Docker networks and subnets

First enable the dynamic attributes connector as discussed in Enable the dynamic attributes connector.

To change Docker networks and subnets, run `/usr/local/sf/bin/change_docker_subnet.sh -b` *`CIDR-network`* `-s` *`address-pool-size`* as a user with `root` privileges where:

- `-b` *`CIDR-network`* sets a network base address pool in CIDR notation.
- `-s` *`address-pool-size`* sets a netmask for the network base address. You can use this option to limit the number of addresses in a base address range in the event the network range overlaps existing network ranges; in particular, we recommend certain `-s` values for Secure Firewall Management Center models to make sure you don't exceed the available RAM in the machine. (Docker containers are used by dynamic attributes connector connectors and those limits are shown in System requirements for the Dynamic Attributes Connector, on page 7.)

Important The networks you assign to Docker must be in an internal network range and must *not* conflict with networks used by the Secure Firewall Management Center or by other devices in your internal network.

Examples

The following table shows examples.

Secure Firewall Management Center model	Recommended -s value	Sample -b value	Dynamic Attributes Connector container addresses used
Firepower 1000, Firepower 1600, vFMC	27 (netmask 255.255.255.224)	172.19.0.0/16	30 IP addresses `docker0`: 172.19.0.1 Bridge networks `br-`*`number`* gateway `172.19.0.33` with subnet `172.19.0.32/27` Connectors created in networks like `172.19.0.38/27`, `172.19.0.39/27`, and so on

Secure Firewall Management Center model	Recommended -s value	Sample -b value	Dynamic Attributes Connector container addresses used
Firepower 2500, Firepower 2600, vFMC 300	26 (netmask 255.255.255.192)	192.168.0.0/16	62 IP addresses `docker0`: 192.168.1.1 Bridge networks `br-number` gateway `192.168.1.65`with subnet `192.168.1.64/26` Connectors created in networks like `192.168.1.71/26`, `192.168.1.72/26`, and so on
Firepower 4500, Firepower 4600	25 (netmask 255.255.255.128)	192.168.0.0/16	126 IP addresses `docker0`: 192.168.1.1 Bridge networks `br-number` gateway `192.168.1.129`with subnet `192.168.1.128/25` Connectors created in networks like `192.168.1.136/25`, `192.168.1.135/25`, and so on

For reference, the complete commands follow:

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 27
```

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 26
```

```
sudo /usr/local/sf/bin/change_docker_subnet.sh -b 192.168.0.0/16 -s 25
```

Verify the networks

To verify your network settings, enter `sudo docker network inspect muster-net`. The command results are displayed in JSON format.

Troubleshoot

Following are some solutions to common errors you might encounter using this command.

Error: **`Pull subnet value can not be greater than size`**

Solution: Change the value of `-s` so it is less than the CIDR network value.

For example,

INCORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 8`

CORRECT: `sudo /usr/local/sf/bin/change_docker_subnet.sh -b 172.19.0.0/16 -s 20`

Error: After running the command, the Docker networks are wrong.

Solution: Restart the Docker daemon: `sudo pmtool restartbyid docker`

Error: **`Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?`**

Solution: Restart Docker: `pmtool restartbyid docker`

Error: Input can't be empty

The `-s` parameter is required.

Error: `Pull size - 32 - can not be greater than 32 or less than 0`

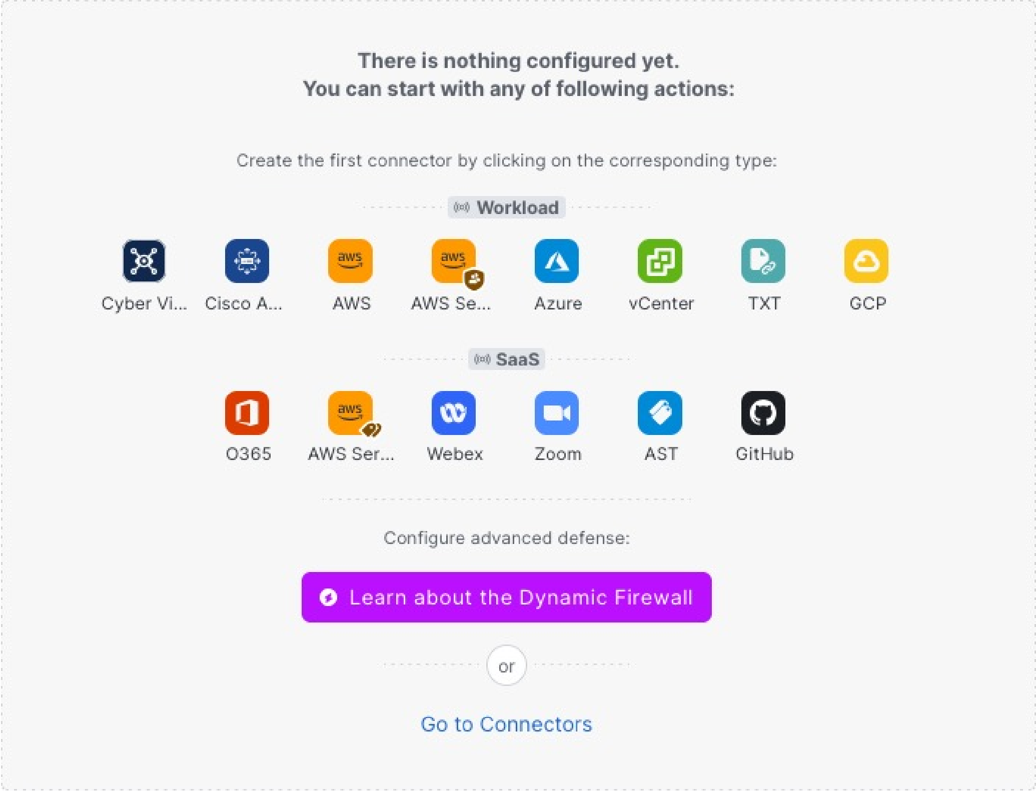
Solution: Change the value of `-s` so it is greater than 0 and less than 32.

About the dashboard

To access the dynamic attributes connector dashboard, log in to the Secure Firewall Manager and click **Integrations** > **Dynamic Attributes Connector** at the top of the page.

If the dynamic attributes connector is not enabled, move the slider to enable it. This process could take several minutes to complete.

The dynamic attributes connector Dashboard page displays the status of your connectors, adapters, and filters at a glance. Following is an example of the Dashboard of an unconfigured system:



There is nothing configured yet.
You can start with any of following actions:

Create the first connector by clicking on the corresponding type:

Configure advanced defense:

Among the things you can do with the Dashboard are:

- Add, edit, and delete connectors and dynamic attributes filters.
- See how connectors and dynamic attributes filters are related to each other.
- View warnings and errors.

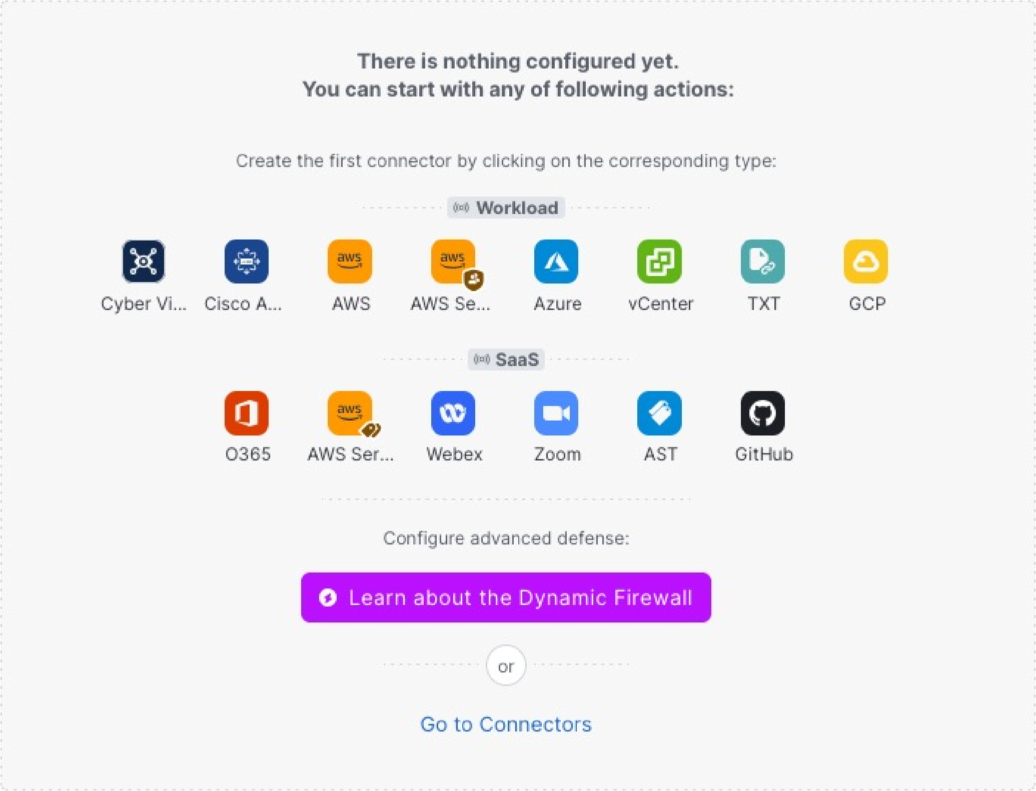
Related Topics

- Dashboard of an unconfigured system, on page 11
- Dashboard of a configured system, on page 12

- Add, edit, or delete connectors, on page 13
- Add, edit, or delete dynamic attributes filters, on page 15

Dashboard of an unconfigured system

Sample dynamic attributes connector Dashboard page of an unconfigured system:

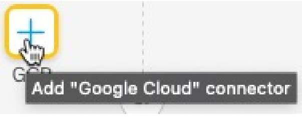


There is nothing configured yet.
You can start with any of following actions:

Create the first connector by clicking on the corresponding type:

Configure advanced defense:

The Dashboard initially displays all the types of connectors you can configure for your system. You can do any of the following:

- Hover the mouse pointer over a connector and click  to create a new one.

- Click **Go to Connectors** to add, edit, or delete connectors (good for creating, editing, or deleting multiple connectors at the same time).

  For more information, see Create a connector, on page 16.

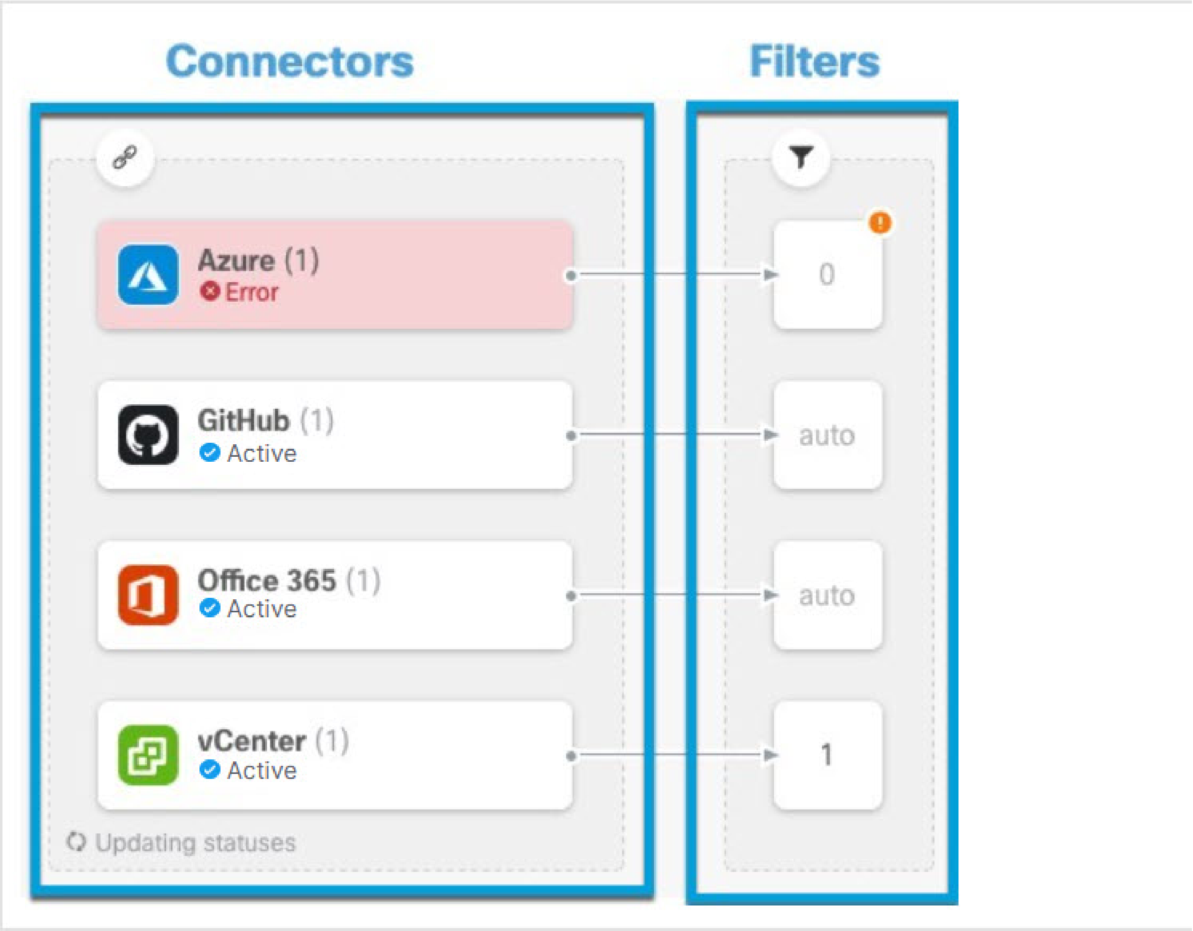
Related Topics:

- Dashboard of a configured system, on page 12
- Add, edit, or delete connectors, on page 13
- Add, edit, or delete dynamic attributes filters, on page 15

Dashboard of a configured system

Sample dynamic attributes connector Dashboard page of a configured system:

Click an area in the figure to learn more about it or click one of the links following the figure.



1 Create a connector, on page 16
2 Create dynamic attributes filters

The Dashboard shows the following (from left to right):

Connectors column	Filters column
List of connectors with a number indicating how many of each type are configured. Connectors collect dynamic attributes that could be sent to the Secure Firewall Manager. Dynamic attributes filters specify what data is sent. Click 🔗 to view more information about all configured connectors. You can also click the name of a connector to add, edit, or delete connectors; or to view detailed information about them. For more information, see Add, edit, or delete connectors, on page 13.	List of dynamic attributes filters associated with each connector with a number indicating how many of each filter are associated with a connector. Click ▼ to view more information about all configured filters. You can also click the name of a filter to add, edit, or delete filters; or to view detailed information about them. For more information, see Add, edit, or delete dynamic attributes filters, on page 15.

Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the ▼ column.

The Dashboard indicates whether or not an object is available. The Dashboard page is refreshed every 15 seconds but you can click **Refresh** (↻) at the top of the page at any time to refresh immediately. If issues persist, check your network connection.

Related Topics:

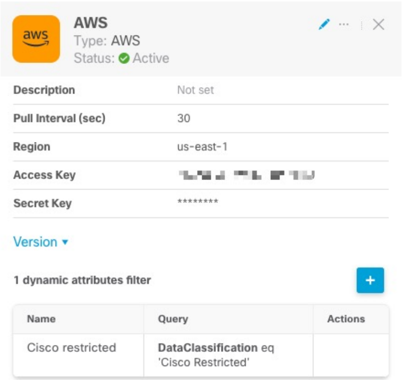
- Add, edit, or delete connectors, on page 13
- Add, edit, or delete dynamic attributes filters, on page 15

Add, edit, or delete connectors

The Dashboard enables you to view or edit connectors. You can click the name of a connector to view all instances of that connector or you can click 🔗 for the following additional options:

- **Go to Connectors** to view all connectors at the same time; you can add, edit, and delete connectors from there.
- **Add Connector** > ***type*** to add a connector of the indicated type.

Click any connector in the connectors column (🔗) to display more information about it; an example follows:



AWS
Type: AWS
Status: ✓ Active

Description	Not set
Pull Interval (sec)	30
Region	us-east-1
Access Key	[redacted]
Secret Key	********

Version ▾

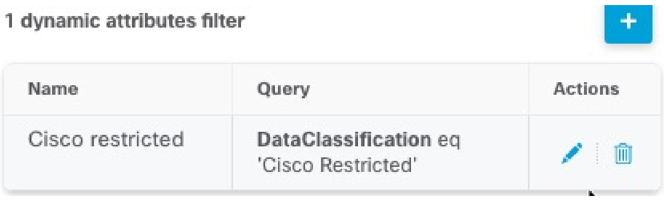
1 dynamic attributes filter +

Name	Query	Actions
Cisco restricted	**DataClassification** eq 'Cisco Restricted'	

You have the following options:

- Click the Edit icon (✎) to edit this connector.
- Click the More icon (⋯) for additional options.
- Click × to close the panel.
- Click **Version** to display the version of the . You can optionally copy the version to the clipboard if necessary for Cisco TAC.

The table at the bottom of the panel enables you to add dynamic attributes filters; or to edit or dynamic attributes connector delete connectors. A sample follows:



1 dynamic attributes filter +

Name	Query	Actions
Cisco restricted	**DataClassification** eq 'Cisco Restricted'	✎ 🗑

Click the Add icon (+ ˅) to add a dynamic attributes filter for this connector. For more information, see Create dynamic attributes filters.

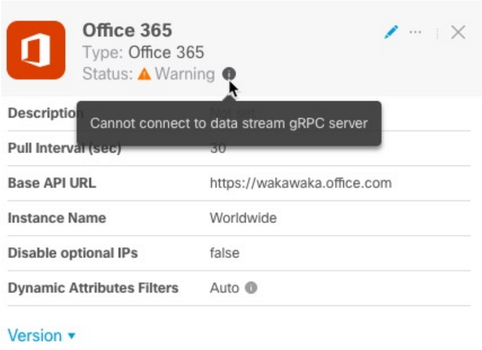
Hover the mouse pointer over the Actions column to either edit or delete the indicated connector.

View error information

To view error information for a connector:

1. On the Dashboard, click the name of the connector that is displaying the error.
2. In the right pane, click **Information** (ⓘ).

   An example follows.



Office 365
Type: Office 365
Status: ⚠ Warning

Cannot connect to data stream gRPC server

Description	
Pull Interval (sec)	30
Base API URL	https://wakawaka.office.com
Instance Name	Worldwide
Disable optional IPs	false
Dynamic Attributes Filters	Auto

Version ▾

3. To resolve this issue, edit the connector settings as discussed in Create an Office 365 connector, on page 43.

4. If you cannot resolve the issue, click **Version** and copy the version to a text file.

5. Provide all of this information to Cisco TAC.

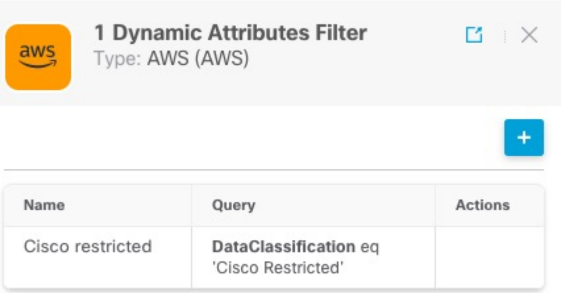
Add, edit, or delete dynamic attributes filters

The dashboard enables you to add, edit, or delete dynamic attributes filters. You can click the name of a filter to view all instances of that filter or you can click for the following additional options:

- **Go to Dynamic Attributes Filters** to view all configured dynamic attributes filters. You can add, edit, or delete dynamic attributes filters from there.
- **Add Dynamic Attributes Filters** to add a filter.

For more information about adding dynamic attributes filters, see Create dynamic attributes filters.

An example follows:



1 Dynamic Attributes Filter
Type: AWS (AWS)

Name	Query	Actions
Cisco restricted	DataClassification eq 'Cisco Restricted'	

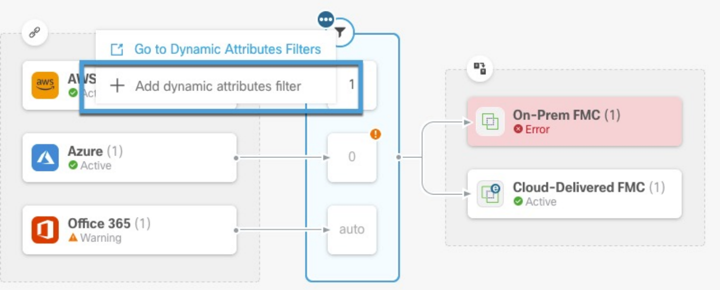
Note Some connectors, such as Outlook 365 and Azure Service tags, automatically pull available dynamic objects without the need for a dynamic attributes filters. Those connectors display **Auto** in the column.

You have the following options:

- Click a filter instance to view summary information about dynamic attributes filters associated with a connector.
- Click the Add icon (+ ⌄) to add a new dynamic attributes filter.

  For more information, see Create dynamic attributes filters.
- Click ! in the filters column (▼) indicates the indicated connector has no associated dynamic attributes filters. Without associated filters, the connector can send nothing to Firewall Management Center.

  One way to resolve the issue is to click ▼ in the filters column and click **Add Dynamic Attributes Filter**. A sample follows.



- Click ↗ to add, edit, or delete filters.
- Click ✕ to close the panel.

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 policies on the Secure Firewall Management Center.

We support the following:

Table 2: List of supported connectors by dynamic attributes connector version and platform

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 1.1 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes	No	Yes	No	No
Version 2.0 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	No	Yes	Yes	No	Yes	No	No
Version 2.2 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	No	No
Version 2.3 (on-premises)	Yes	No	No	Yes	Yes	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes

CSDAC version	AWS	AWS Security Groups	AWS Service Tags	Azure	Azure Service Tags	Cisco APIC	Cisco Cyber Vision	Cisco Multicl. Defense	Generic text	GitHub	Google Cloud	Microsoft Office 365	Tenable	vCenter	Webex	Zoom
Version 3.0 (on-premises)	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Version 3.1 (on-premises)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Cloud-delivered (Security Cloud Control)	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes	Yes	No	No	No
Secure Firewall Management Center 7.4.1	Yes	No	No	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.6	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 7.7	Yes	Yes	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Secure Firewall Management Center 10.0.0	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

Amazon Web Services connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from AWS to Secure Firewall Management Center for use in 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 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 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 17.

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 can grant user access later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

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

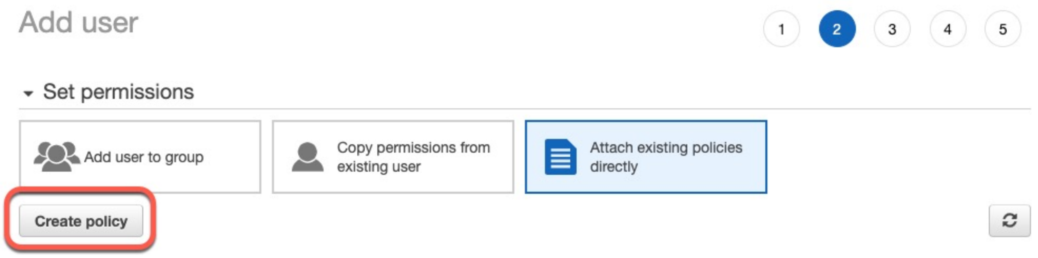
Note
This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

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

Step 13 Click **Create Policy**.

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


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

Step 15 Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "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 19.

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 policies.

Before you begin

Create a user with at least the privileges discussed in Create an AWS user with minimal permissions for the dynamic attributes connector, on page 17.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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.

Value	Description
Access Key	(Required.) Enter your access key.
Secret Key	(Required.) Enter your secret key.

Step 5 Click **Save**.

Step 6 Make sure **Ok** is displayed in the Status column.

Amazon Web Services Security Groups connector—About user permissions

The dynamic attributes connector imports dynamic attributes from AWS to Secure Firewall Management Center for use in policies.

Minimum permissions required

The 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 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 17.

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 can grant user access later.

Step 8 Add tags to the user if desired.

Step 9 Click **Create User**.

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

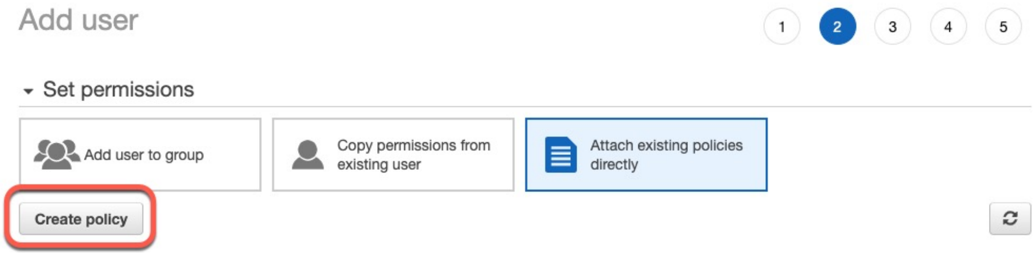
Note
This is the only opportunity you have to retrieve the user's key.

Step 11 Click **Close**.

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

Step 13 Click **Create Policy**.

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


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

Step 15 Enter the following policy in the field:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeTags",
    "ec2:DescribeInstances",
    "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 19.

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 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 dynamic attributes connector, on page 17.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 **Save**.

Step 6 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 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 **Save**.

Step 6 Make sure **Ok** is displayed in the Status column.

Azure connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Azure to Secure Firewall Management Center for use in 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 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 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 23.

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**.

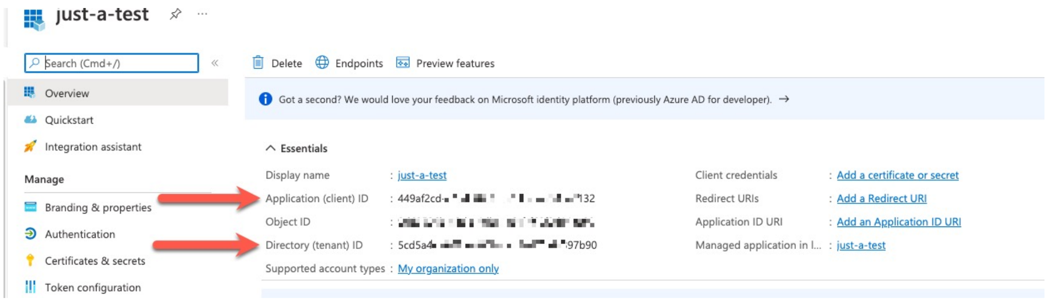
Step 5 In the **Name** field, enter a name to identify this application.

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

Step 7 Click **Register**.

Step 8 On the next page, write down or copy the Client ID (also referred to as *application ID*) and the tenant ID (also referred to as the *directory ID*).

A sample follows.



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

Display name : just-a-test

Application (client) ID : 449af2cd-[redacted]132

Object ID : [redacted]

Directory (tenant) ID : 5cd5a4[redacted]97b90

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

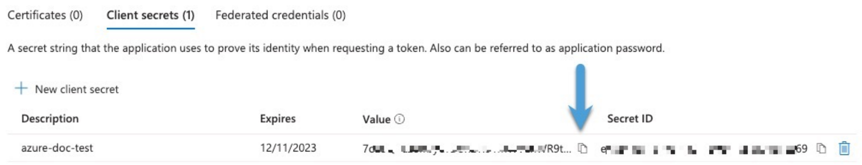
Managed application in l... : just-a-test

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

Step 10 Click **New Client Secret**.

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

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



Certificates (0) | Client secrets (1) | Federated credentials (0)

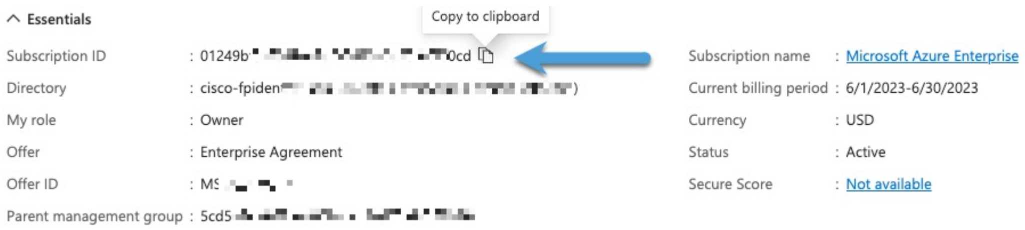
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

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

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

Step 14 Click the name of your subscription.

Step 15 Copy the subscription ID to the clipboard.



Subscription ID : 01249b[redacted]0cd

Directory : cisco-fpiden[redacted])

My role : Owner

Offer : Enterprise Agreement

Offer ID : MS[redacted]

Parent management group : 5cd5[redacted]

Subscription name : Microsoft Azure Enterprise

Current billing period : 6/1/2023-6/30/2023

Currency : USD

Status : Active

Secure Score : Not available

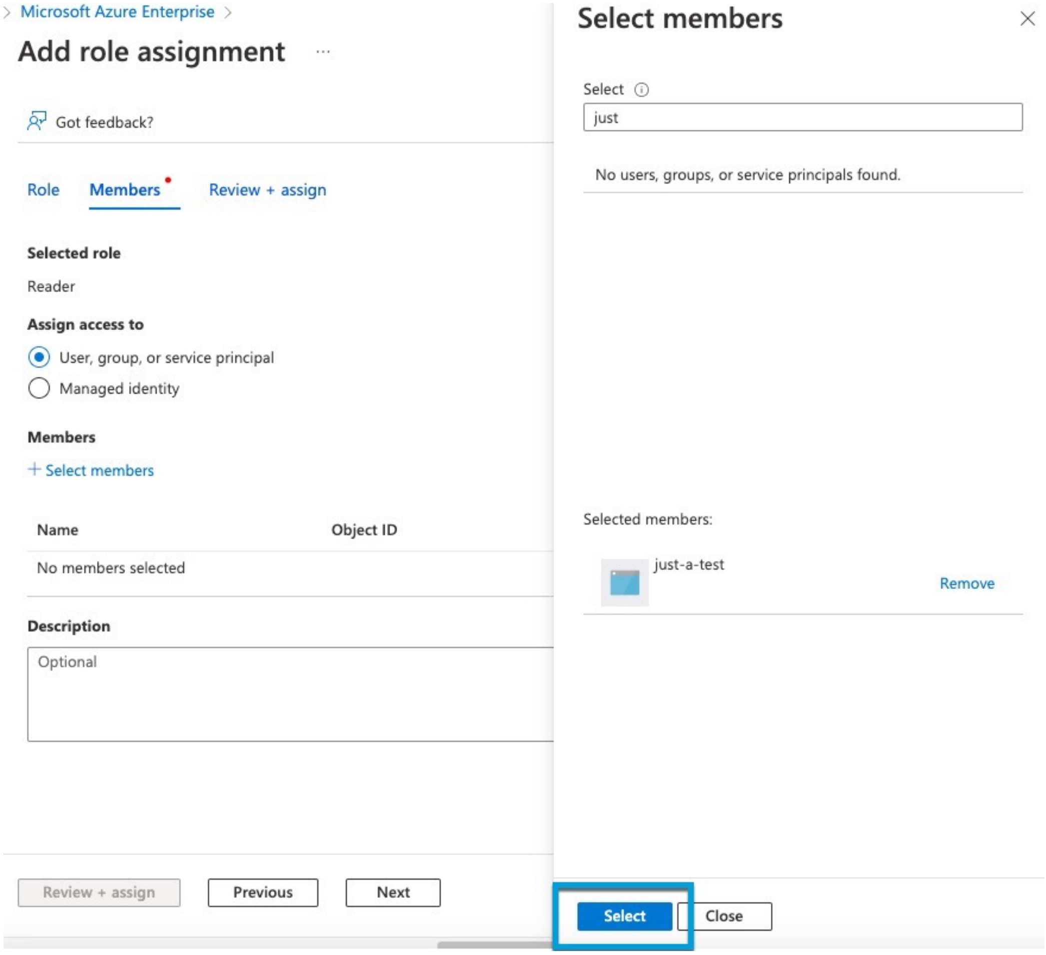
Step 16 Click **Access Control (IAM)**.

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

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

Step 19 Click **Select Members**.

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



> Microsoft Azure Enterprise >

Add role assignment ...

Got feedback?

Role | Members | Review + assign

Selected role

Reader

Assign access to

● User, group, or service principal

○ Managed identity

Members

+ Select members

Name	Object ID
No members selected	

Description

Optional

Review + assign | Previous | Next

Select members

Select ⓘ

just

No users, groups, or service principals found.

Selected members:

just-a-test Remove

Select | Close

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

What to do next

See Create an Azure connector, on page 26.

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 policies.

Before you begin

Create an Azure user with at least the privileges discussed in Create an Azure user with minimal permissions for the dynamic attributes connector, on page 24.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 **Save**.

Step 6 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 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 **Save**.

Step 6 Make sure **Ok** is displayed in the Status column.

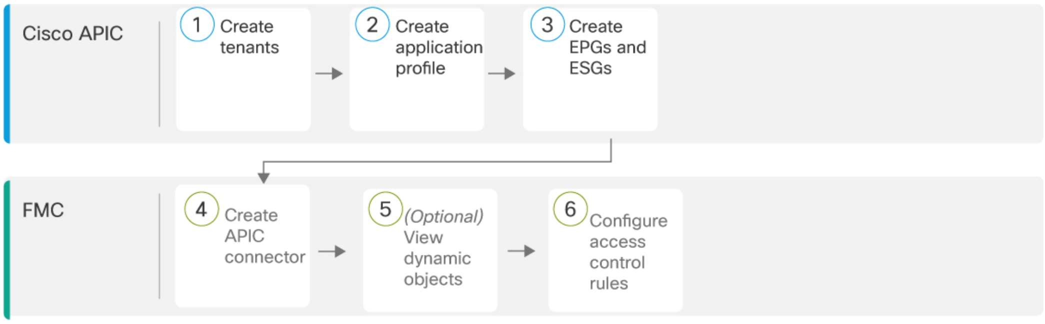
Cisco APIC connector

The following topics discuss how to configure the Cisco APIC Integration with the Secure Firewall Management Center.

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35

How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules


Cisco APIC
1 Create tenants
2 Create application profile
3 Create EPGs and ESGs
FMC
4 Create APIC connector
5 (Optional) View dynamic objects
6 Configure access control rules

1 Basic User Tenant Configuration
2 Basic User Tenant Configuration
3 EPGs
4 Create a Cisco APIC connector, on page 33
5 View dynamic objects in the Secure Firewall Management Center, on page 58
6 Create access control rules or DNS rules using dynamic attributes filters

Table 3: Configure Secure Firewall Management Center access control rules or DNS rules using network object groups

1	Cisco APIC	A tenant allows a Cisco APIC administrator to set up domain-based access control. See Basic User Tenant Configuration
2	Cisco APIC	An application profile is a container for other objects, such as an endpoint group (EPG). See Basic User Tenant Configuration
3	Cisco APIC	An EPG is a container for network objects that serves as the way that devices connect to the network. An ESG is a logical entity that contains a collection of physical or virtual network endpoints. See EPGs and ESGs
	Secure Firewall Management Center	If you haven't done so already, Enable the dynamic attributes connector.
4	Secure Firewall Management Center	Create the Cisco APIC connector which retrieves EPGs and ESGs from Cisco APIC and enables them to be used in Secure Firewall Management Center access control policies or DNS policies. See Create a Cisco APIC connector, on page 33.
5	Secure Firewall Management Center	(Optional.) View the dynamic objects fetched from Cisco APIC. See View dynamic objects in the Secure Firewall Management Center, on page 58.
6	Secure Firewall Management Center	To use dynamic objects in access control policies or DNS policies, you must add them as dynamic objects to those rules. See Create access control rules or DNS rules using dynamic attributes filters.

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35
Cisco APIC connector, on page 28

System requirements for the integration with Cisco APIC

Your system must meet the following requirements:

- Secure Firewall Management Center version: 10.0.0 and later.

  Essentials license or better required; high availability is supported.
- Firewall Threat Defense version: 7.2 and later.
- Cisco APIC version: 3.0(1k) or later.
- If you use the ACI Endpoint Update App, it must be version 2.6.

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35

Get required information for the integration

This section discusses:

- Information required to configure the integration
- Information used in dynamic object names

Cisco ACI Endpoint Update App site prefix and update interval

This information applies to you only if you're currently using the Cisco ACI Endpoint Update App; otherwise, you can skip it.

To find the Cisco ACI Endpoint Update App site prefix and update interval:

1. Log in to Cisco APIC as a user with `admin` privileges.

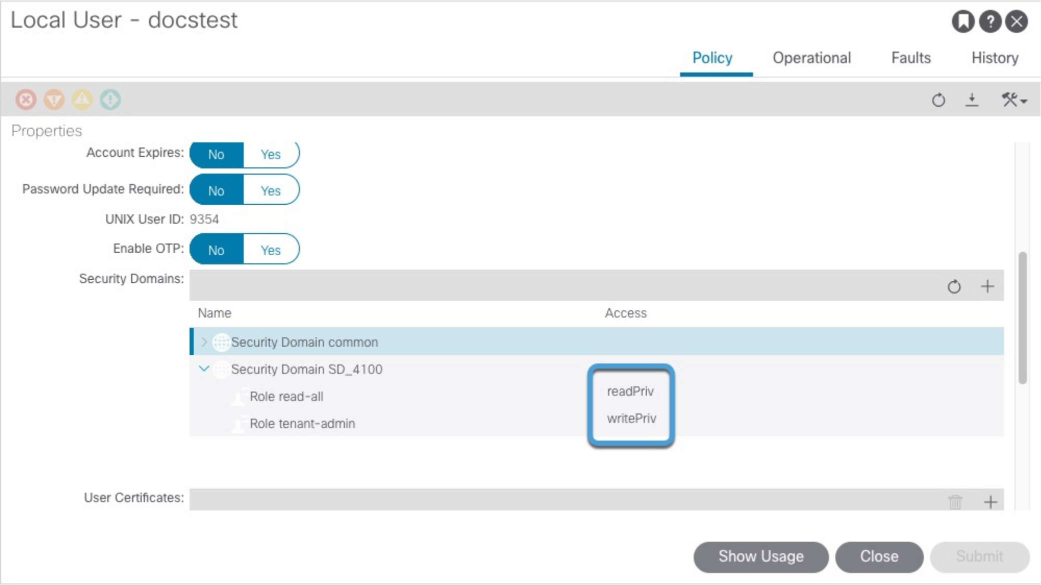
   For more information, see *APIC Roles and Privileges Matrix*.
2. Click **Apps**.
3. Under ACI Endpoint Update app, click **Open**.
4. Click **Edit** (✎).

5. Write down the values of **Update Interval (In seconds)** and **Site Prefix**.

Required to configure the integration: Find a user with appropriate access

To find a user with at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain:

1. Log in to Cisco APIC.
2. Click **Admin**.
3. In the left pane, click **Users**.
4. In the right pane, double-click the name of a user.
5. Scroll to Security Domains.
6. For the relevant security domain, make sure the user has at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain, as the following figure shows.



Local User - docstest

Properties
Account Expires: [✓ No] Yes
Password Update Required: [✓ No] Yes
UNIX User ID: 9354
Enable OTP: [✓ No] Yes
Security Domains:

Name	Access
Security Domain common	
Security Domain SD_4100	
Role read-all	readPriv
Role tenant-admin	writePriv

User Certificates:

Cisco APIC tenant name

The Cisco APIC tenant name is used in the names of dynamic objects created by this integration. To find it:

1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Write down the name of the tenant that contains objects to send to .

Cisco APIC application profile name

The Cisco APIC application profile name is used in the names of dynamic objects created by this integration. To find it:

1. Log in to Cisco APIC.

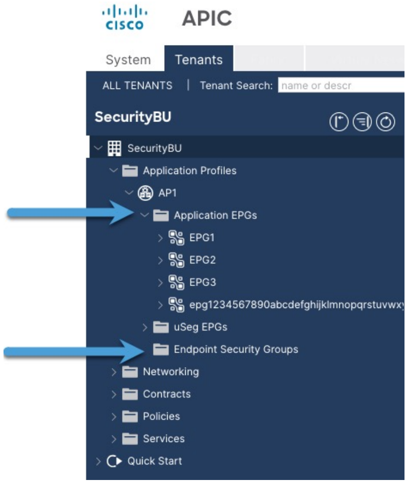
2. Click **Tenants**.
3. Double-click the name of your tenant.
4. Expand your tenant.
5. Expand **Application Profiles**.
6. Write down the name of the application profile that contains EPGs and ESGs to integrate with ASA.

EPG name

The Cisco APIC EPG name is used in the names of dynamic objects created by this integration. To find it:

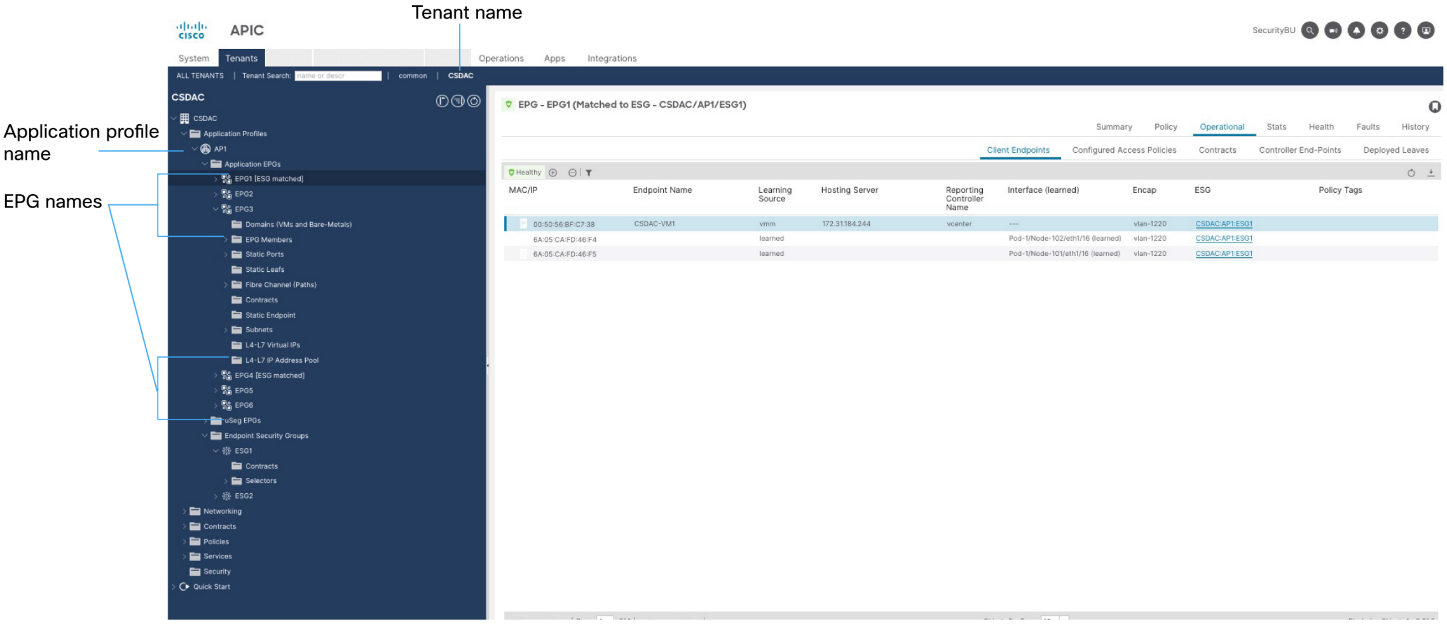
1. Log in to Cisco APIC.
2. Click **Tenants**.
3. Double-click the name of your tenant.
4. Expand your tenant.
5. Expand **Application Profiles**.
6. Expand the name of the application profile.
7. Expand **Application EPGs**.
8. Write down the name of the EPG or ESG that has network object groups to send to ASA.

   The following figure shows an example.



Example

The following figure shows the values in Cisco APIC.



EPG - EPG1 (Matched to ESG - CSDAC/AP1/ESG1)

MAC/IP	Endpoint Name	Learning Source	Hosting Server	Reporting Controller Name	Interface (learned)	Encap	ESG	Policy Tags
00:50:56:BF:C7:38	CSDAC-VM1	vmm	172.31.184.244	vcenter	---	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F4		learned			Pod-1/Node-102/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	
6A:05:CA:FD:46:F5		learned			Pod-1/Node-101/eth1/16 (learned)	vlan-1220	CSDAC:AP1:ESG1	

Related Topics

- System requirements for the integration with Cisco APIC, on page 30
- Get required information for the integration, on page 30
- Create a Cisco APIC connector, on page 33
- How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
- Manually get a certificate authority (CA) chain, on page 35

Create a Cisco APIC connector

This topic discusses creating a Cisco APIC connector that gets network object groups from a configured endpoint group (EPG) on Cisco APIC.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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.

Value	Description
Description	Optional description.
Pull Interval	(Default 60 seconds.) Interval at which IP mappings are retrieved from Cisco APIC. We recommend setting this to 15 seconds.
IP or Hostname	Enter the fully-qualified domain name or IP address of the Cisco APIC server from which to retrieve network object groups from EPGs and ESGs. *Do not* enter a scheme (such as **`https://`**) and *do not* include a trailing slash.
Add another cluster IP	(Optional.) Enter the IP address of other servers in the Cisco APIC cluster.
Username	Enter the name of a Cisco APIC user with at least at least the `read-all` role with `readPriv` access and the `tenant-admin` role with `writePriv` access for the security domain. Objects from all tenants the user has privileges to can be pushed to .
Password	Enter the user's password.
Server Certificate	(Recommended if using fully-qualified domain name.) You have the following options: • Paste the certificate authority (CA) chain you got as discussed in Manually get a certificate authority (CA) chain, on page 35. • 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 35. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

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.

Related Topics

System requirements for the integration with Cisco APIC, on page 30

Get required information for the integration, on page 30

Create a Cisco APIC connector, on page 33

How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29

Manually get a certificate authority (CA) chain, on page 35

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 Firewall 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
- Firewall Management Center
- Cisco APIC

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 Firewall Management Center. For example:

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

   If you access vCenter or Firewall 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 Firewall Management Center.

Get a Certificate Chain—Windows Chrome

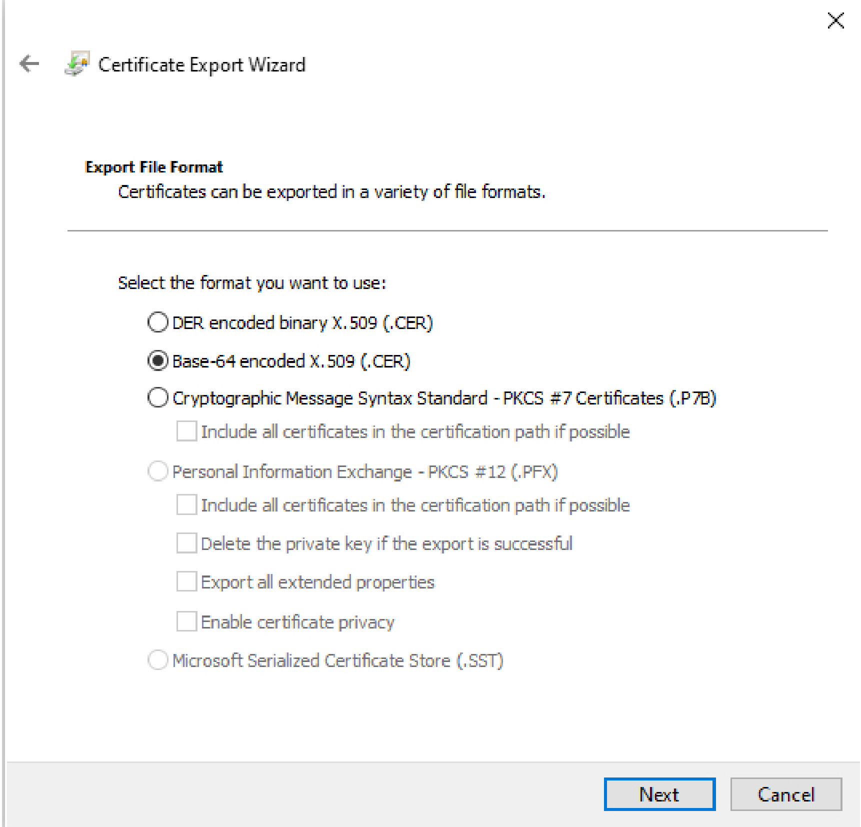
Use this procedure to get a certificate chain using the Chrome browser on Windows.

1. Log in to vCenter or Firewall 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.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

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

10. Follow the prompts to complete the export.

11. Open the certificate in a text editor.

12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for vCenter or Firewall Management Center.

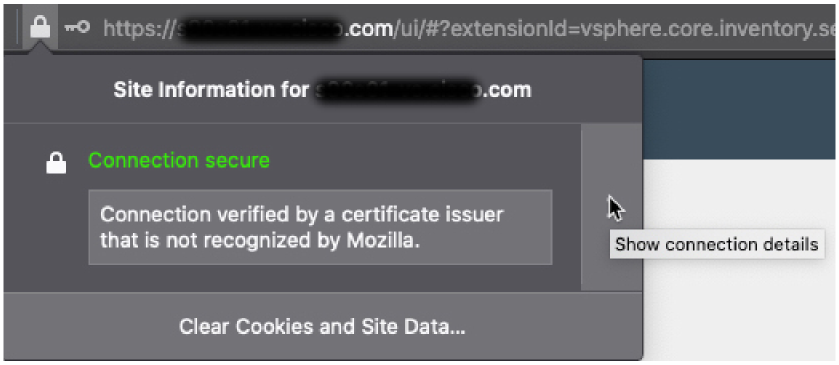
Get a Certificate Chain—Windows Firefox

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 Firewall 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.



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

Site Information for [redacted].com

Connection secure

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

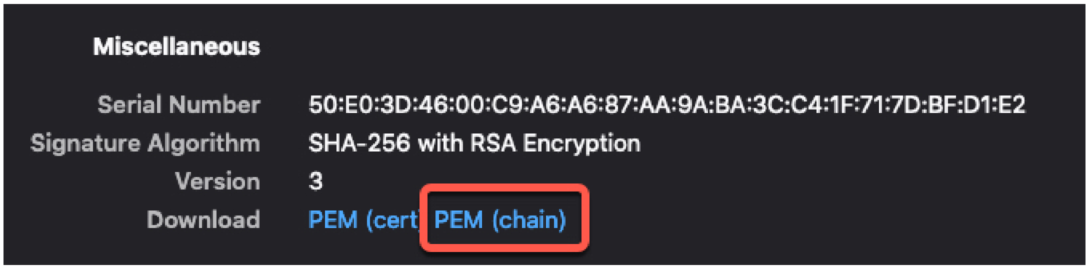
4. Click **More Information**.

5. Click **View Certificate**.

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

7. Scroll to the Miscellaneous section.

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



Miscellaneous

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

Signature Algorithm SHA-256 with RSA Encryption

Version 3

Download PEM (cert) PEM (chain)

9. Save the file.

10. Repeat these tasks for vCenter or Firewall Management Center.

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35
Cisco APIC connector, on page 28

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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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.
Host	(Required.) Enter the Cyber Vision fully qualified host name or 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.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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:

Item	Description
Name	Enter a name to identify the connector.
Description	(Optional.) Enter a description
Pull Interval	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.
URLs	Enter a URL from which to retrieve IP addresses.
Add another URL	(Optional.) Click the link to add more URLs to an existing list.
Username	(Optional.) If the server on which the text file is located uses authentication, enter the user's name in this field. We use Basic authentication.
Password	(Optional.) Enter the user's password.

Item	Description
Certificate	(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 35. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

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 GitHub connector

This section discusses how to create a GitHub connector that sends data to the Secure Firewall Management Center for use in 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 **Save**.

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

Google Cloud connector—About user permissions and imported data

The dynamic attributes connector imports dynamic attributes from Google Cloud to Secure Firewall Management Center for use in 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 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 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 41.

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.

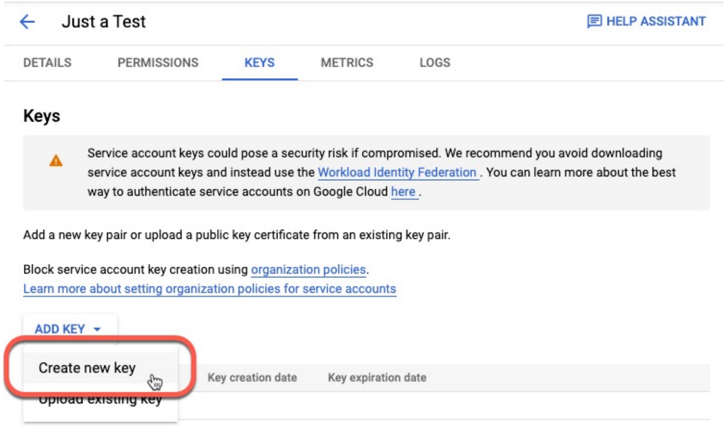
Step 7 Click **Done**.

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**.



Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation . You can learn more about the best way to authenticate service accounts on Google Cloud here .

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

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 42.

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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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.
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 **Save**.

Step 6 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 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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.

Value	Description
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.
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 **Save**.

Step 6 Make sure **Ok** is displayed in the Status column.

vCenter connector—About user permissions and imported data

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

Dynamic attributes imported

We import the following dynamic attributes from vCenter:

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

Minimum permissions required

The 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 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 44.

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**.

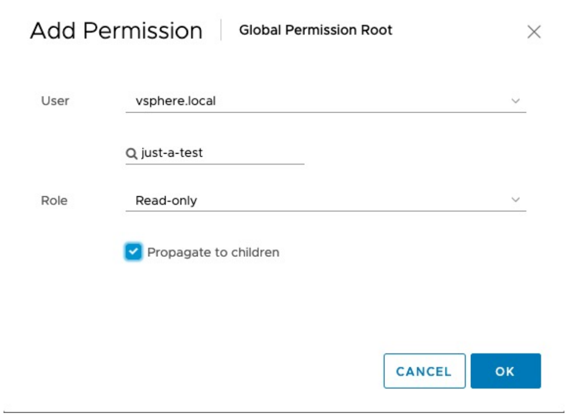
Step 8 Click **Add**(+).

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

just-a-test

Role Read-only

☑ Propagate to children

Step 13 Click **OK**.

What to do next

See Create a vCenter connector, on page 45.

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 policies.

Before you begin

If you use non-trusted certificates to communicate with vCenter, see Manually get a certificate authority (CA) chain, on page 35.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

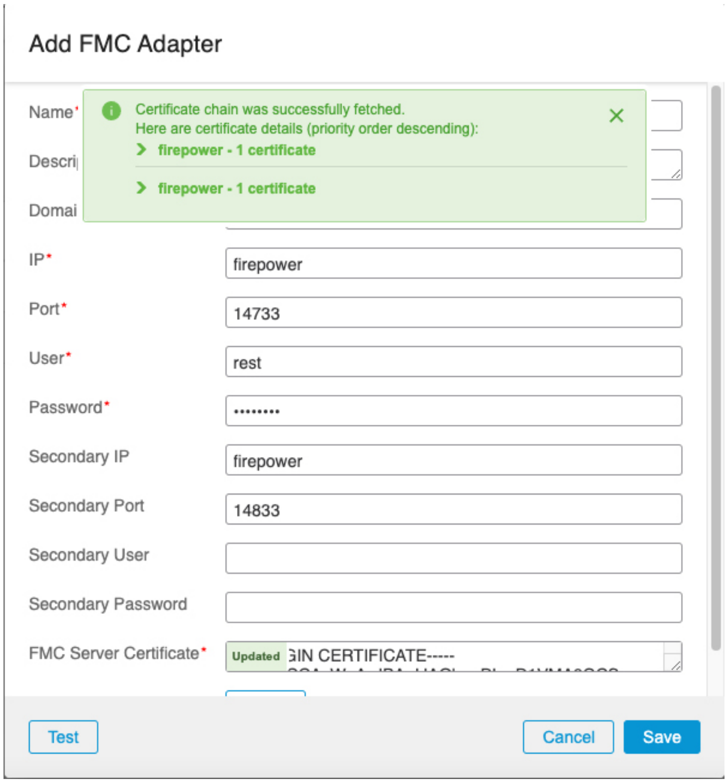
- Add a new connector: click Add icon (+ ⌄), then click the name of the connector.
- Edit or delete a connector: Click **More** (⋮), then click **Edit** or **Delete** at the end of the row.

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: • vCenter's fully qualified host name • vCenter's IP address • (Optional.) A port *Do not* enter a scheme (such as **`https://`**) or trailing slash. For example, **`myvcenter.example.com`** or **`192.0.2.100:9090`**
User	(Required.) Enter the user name of a user with the Read-only role at minimum. User names are case-sensitive.
Password	(Required.) Enter the user's password.
NSX IP	If you use vCenter Network Security Visualization (NSX), enter its IP address.
NSX User	Enter the user name of an NSX user with the Auditor role at minimum.
NSX Type	Enter **NSX-T**.
NSX Password	Enter the NSX user's password.

Value	Description
vCenter Certificate	You have the following options: • Paste the certificate authority (CA) chain you got as discussed in Manually get a certificate authority (CA) chain, on page 35. • Click **Fetch** to automatically fetch the certificate or, if that is not possible, get the certificate manually as discussed in Manually get a certificate authority (CA) chain, on page 35. • 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 35. • Click **Get Certificate** > **Browse from file** to upload a certificate chain you downloaded previously.

Following is an example of successfully fetching a certificate chain:

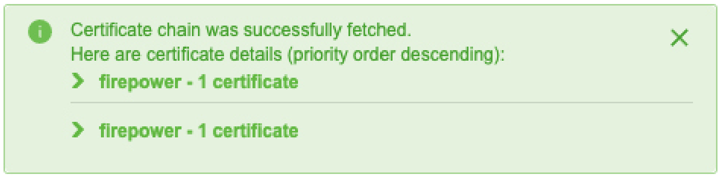


Add FMC Adapter

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

Name*	
Descri	
Domai	
IP*	firepower
Port*	14733
User*	rest
Password*	••••••••
Secondary IP	firepower
Secondary Port	14833
Secondary User	
Secondary Password	
FMC Server Certificate*	Updated 3IN CERTIFICATE-----

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



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

If it's not possible to fetch the certificate this way, you can get the certificate chain manually as discussed in Manually get a certificate authority (CA) chain, on page 35.

Step 5 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 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 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 Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **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 dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, 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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control or DNS rules, see Create access control rules or DNS rules using dynamic attributes filters.

Before you begin

Create a connector, on page 16

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a 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	Click Add ⊞.

Step 5 To add or edit a query, enter the following information.

Item	Description
Key	Click a key from the list. Keys are fetched from the connector.
Operation	Click one of the following: • **Equals** to exactly match the key to the value. • **Contains** to match the key to the value if any part of the value matches.

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

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the Secure Firewall Management Center .

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **External Attributes** > **Dynamic Object**.

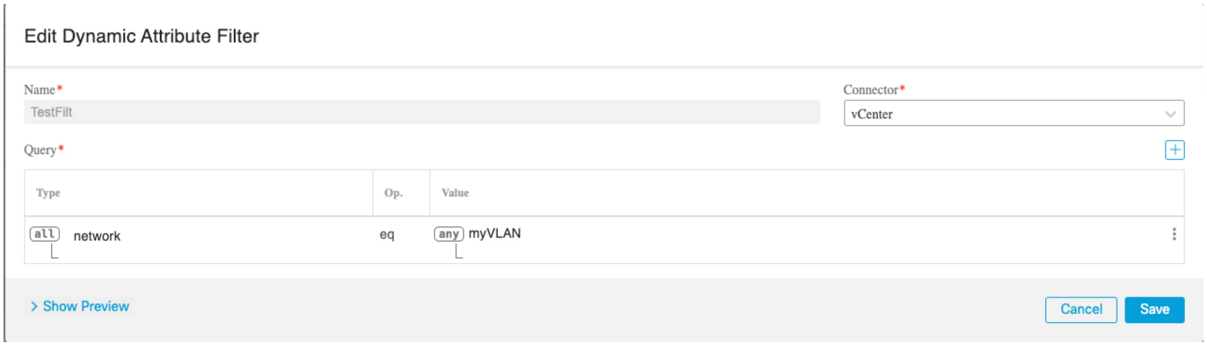
The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attribute filter examples

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

Examples: vCenter

The following example shows one criterion: a VLAN.



Edit Dynamic Attribute Filter

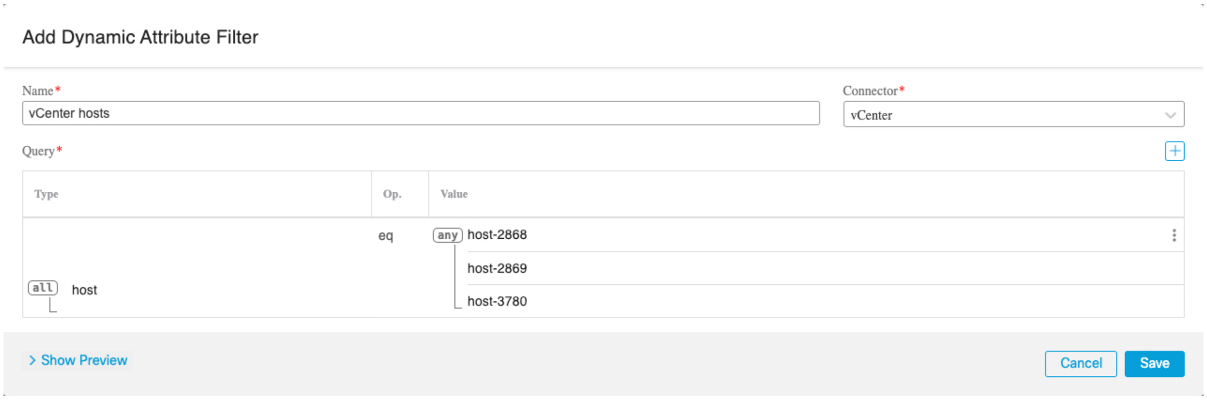
Name* TestFilt

Connector* vCenter

Query*

Type	Op.	Value
all network	eq	any myVLAN

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



Add Dynamic Attribute Filter

Name* vCenter hosts

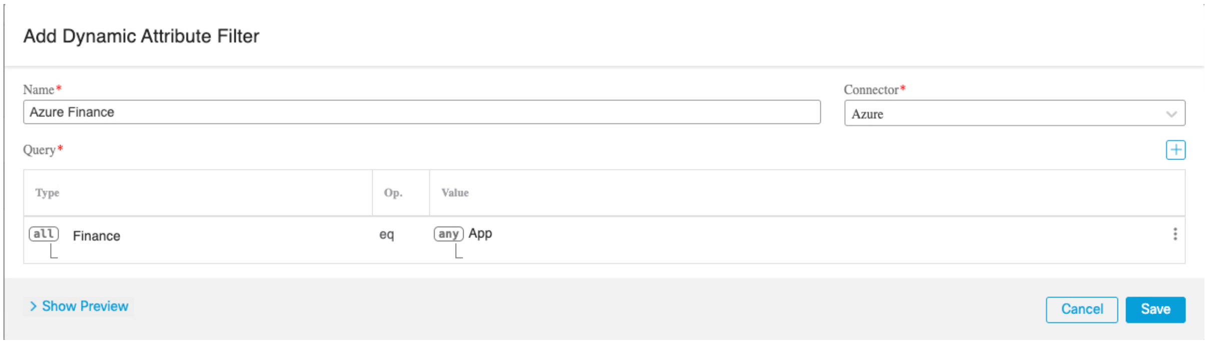
Connector* vCenter

Query*

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

Example: Azure

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



Add Dynamic Attribute Filter

Name*: Azure Finance

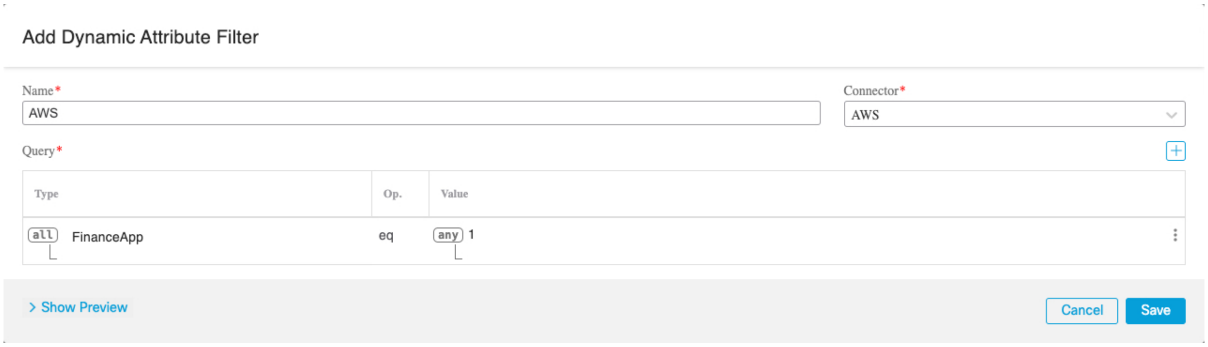
Connector*: Azure

Query*

Type	Op.	Value
all Finance	eq	any App

Example: AWS

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



Add Dynamic Attribute Filter

Name*: AWS

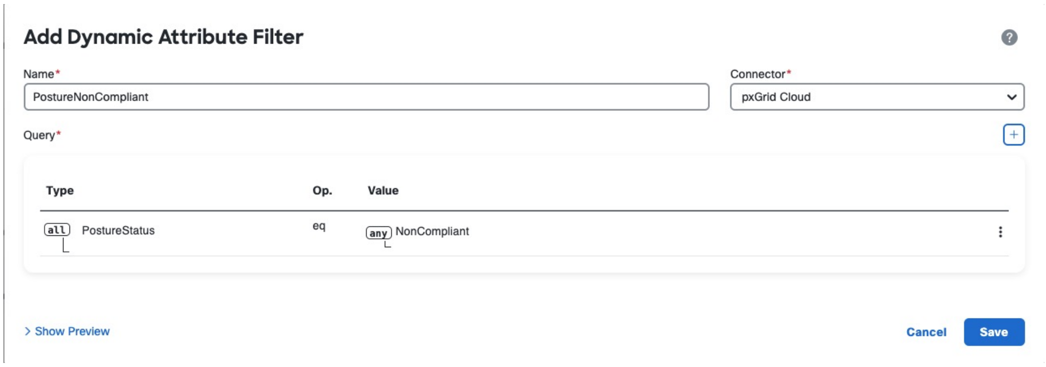
Connector*: AWS

Query*

Type	Op.	Value
all FinanceApp	eq	any 1

Example: pxGrid Cloud

The following example shows one criterion: PostureStatus is NonCompliant.



Add Dynamic Attribute Filter

Name*: PostureNonCompliant

Connector*: pxGrid Cloud

Query*

Type	Op.	Value
all PostureStatus	eq	any NonCompliant

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 Firewall 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
- Firewall Management Center
- Cisco APIC

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 Firewall Management Center. For example:

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

   If you access vCenter or Firewall 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 Firewall Management Center.

Get a Certificate Chain—Windows Chrome

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

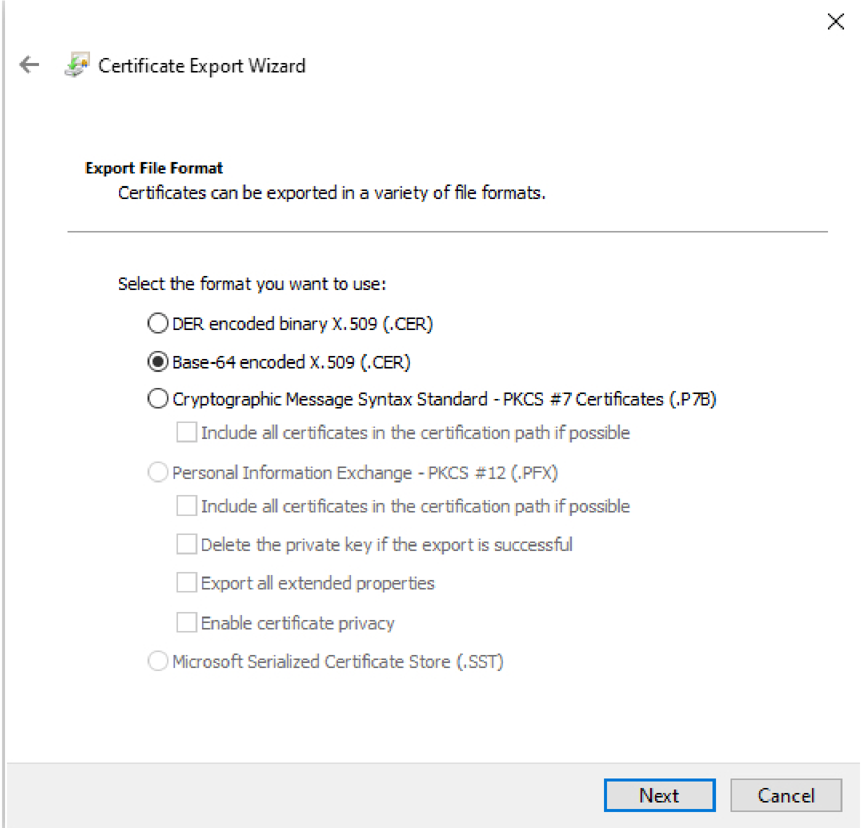
1. Log in to vCenter or Firewall Management Center using Chrome.
2. In the browser address bar, click the lock to the left of the host name.
3. Click **Certificate**.
4. Click the **Certification Path** tab.
5. Click the top (that is, first) certificate in the chain.
6. Click **View Certificate**.

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.



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

10. Follow the prompts to complete the export.

11. Open the certificate in a text editor.

12. Repeat the process for all certificates in the chain.

    You must paste each certificate in the text editor in order, first to last.

13. Repeat these tasks for vCenter or Firewall Management Center.

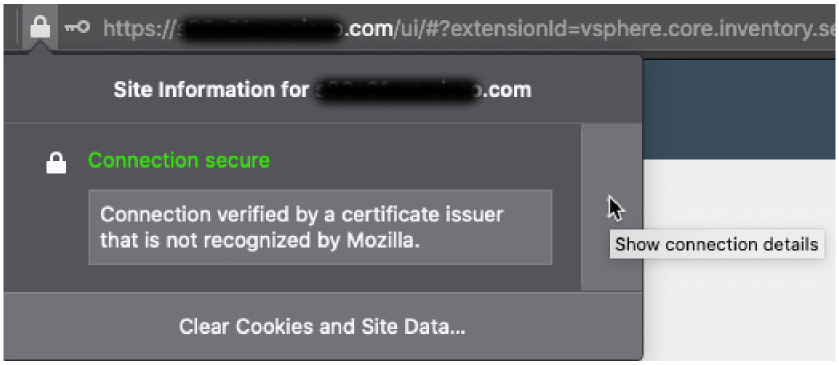
Get a Certificate Chain—Windows Firefox

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 Firewall 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.



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

Site Information for [redacted].com

Connection secure

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

Show connection details

Clear Cookies and Site Data...

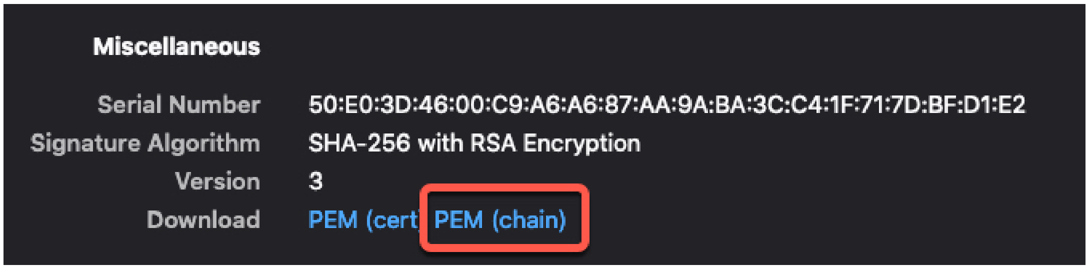
4. Click **More Information**.

5. Click **View Certificate**.

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

7. Scroll to the Miscellaneous section.

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



Miscellaneous

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

9. Save the file.

10. Repeat these tasks for vCenter or Firewall Management Center.

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35
Cisco APIC connector, on page 28

Use Dynamic Objects in Access Control Policies or DNS Policies

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

About dynamic objects in access control rules or DNS 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 or DNS rule's **Dynamic Attributes** tab page. 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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

Create dynamic attributes filters

Dynamic attributes filters that you define using the Dynamic Attributes Connector are exposed in the Secure Firewall Management Center as dynamic objects that can be used in access control policies. For example, 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 Generic Text, Office 365, Azure Service Tags, Webex, or Zoom. These types of cloud objects provide their own IP addresses.

For more information about access control or DNS rules, see Create access control rules or DNS rules using dynamic attributes filters.

Before you begin

Create a connector, on page 16

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **Dynamic Attributes Filters**.

Step 3 Do any of the following:

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

Step 4 Enter the following information.

Item	Description
Name	Unique name to identify the dynamic filter (as a dynamic object) in a 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	Click Add ⊞.

Step 5 To add or edit a query, enter the following information.

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

Step 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the Secure Firewall Management Center .

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **External Attributes** > **Dynamic Object**.

The dynamic attribute query you created should be displayed as a dynamic object.

Dynamic attributes rule conditions

Dynamic attributes include the following:

- (Source or destination.) Dynamic objects (such as from the dynamic attributes connector)

  The 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 they can be used in access control rules.

  For more information about the dynamic attributes connector, see About the Dynamic Attributes Connector, on page 1.

- (Source only.) SGT objects contain tags either manually defined or defined in ISE. For more information, see Source and destination Security Group Tag (SGT) matching and Security Group Tag.
- (Source only.) Location IP objects, defined by Cisco ISE
- (Source only.) Device type objects, defined by Cisco ISE (also referred to as endpoint profile objects)

Dynamic attributes can be used as source criteria and destination criteria in access control rules. Use the following guidelines:

- Objects of different types are ANDd together
- Objects of a similar type are ORd together

For example, if you choose source destination criteria SGT 1, SGT 2, and device type 1; the rule is matched if device type 1 is detected on either SGT 1 or SGT 2. As another example, if you select both a security group tag, and a dynamic object that lists IP addresses, the rule matches if traffic with the tag originates from (or is destined to) one of those IP addresses.

View dynamic objects in the Secure Firewall Management Center

(Optional.) The following task discusses how you can view Cisco APIC network objects in the **Objects** > **External Attributes** > **Dynamic Object**.

Before you begin

Complete all of the previous tasks related to integrating Cisco APIC with the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center

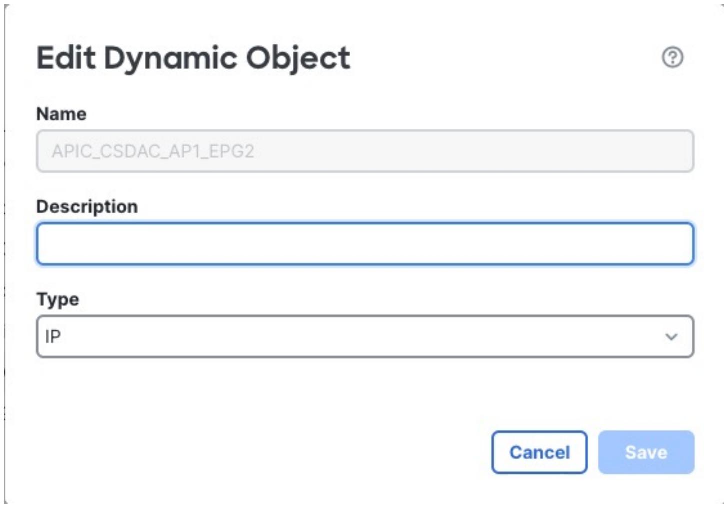
Step 2 Expand **Objects** > **External Attributes** > **Dynamic Object**.

Dynamic objects have their own naming conventions; for example, AWS dynamic objects have names like `aws_AMAZON`.

Dynamic objects created by the integration with Cisco APIC have names matching the pattern:

```
APIC-site-name_tenant-name_application-profile-name_EPG-or-ESG-name
```

Example.



Edit Dynamic Object

Name

APIC_CSDAC_AP1_EPG2

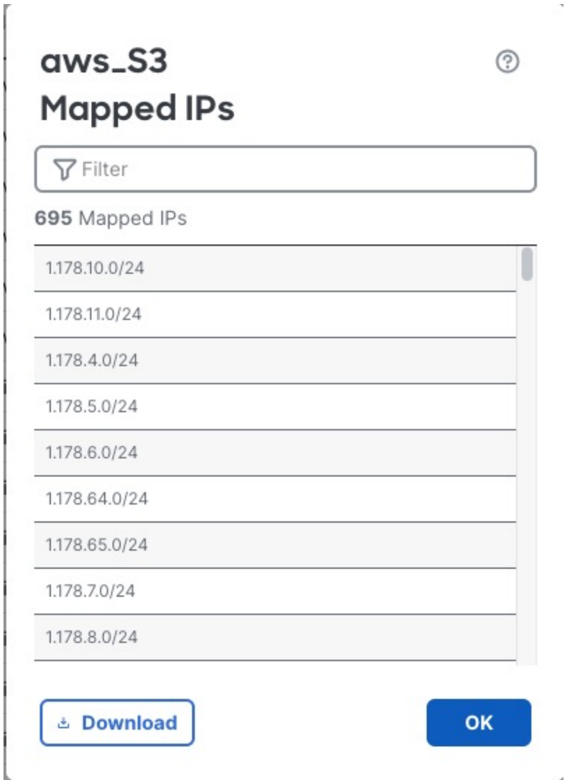
Description

Type

IP

Step 3 To view IP addresses associated with each dynamic object, click (IPs) at the end of the row.

Example:



aws_S3

Mapped IPs

695 Mapped IPs

1.178.10.0/24

1.178.11.0/24

1.178.4.0/24

1.178.5.0/24

1.178.6.0/24

1.178.64.0/24

1.178.65.0/24

1.178.7.0/24

1.178.8.0/24

What to do next

See Create access control rules or DNS rules using dynamic attributes filters.

Create access control rules or DNS 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).

To add dynamic attributes filters to DNS policies, see Creating Basic DNS Policies.

To add dynamic attributes filters to DNS policies, see Creating Basic DNS Policies.

Before you begin

Create dynamic attributes filters as discussed in Create dynamic attributes filters.

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

Procedure

Step 1 Log in to the Secure Firewall Management Center

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

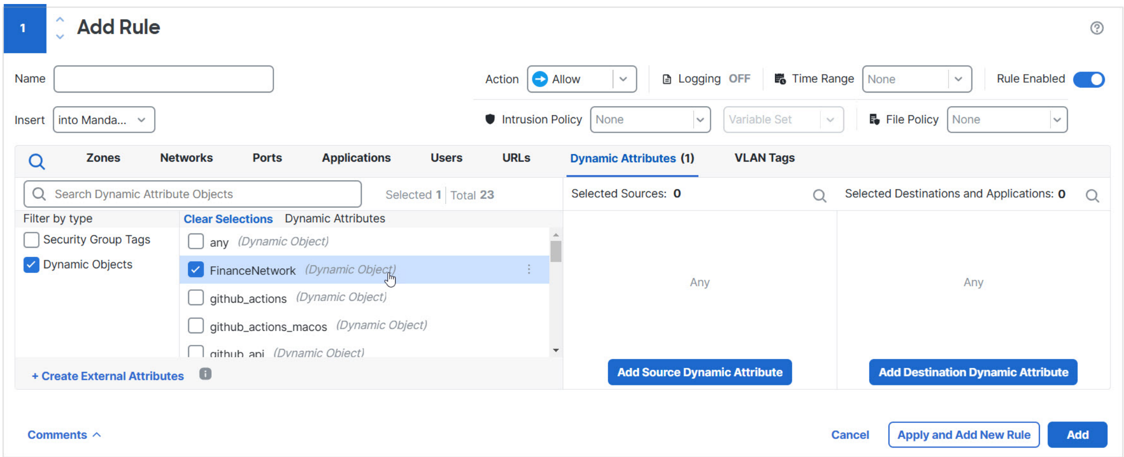
Step 3 Click **Edit** (✎) next to an access control policy.

Step 4 Click **Add Rule**.

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

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

The following figure shows an example.



Name:
Action: Allow
Logging OFF
Time Range: None
Rule Enabled
Insert: into Manda...
Intrusion Policy: None
Variable Set
File Policy: None

Search Dynamic Attribute Objects
Selected 1 | Total 23
Selected Sources: 0
Selected Destinations and Applications: 0

Filter by type
☐ Security Group Tags
☑ Dynamic Objects

Dynamic Attributes
☐ any (Dynamic Object)
☑ FinanceNetwork (Dynamic Object)
☐ github_actions (Dynamic Object)
☐ github_actions_macos (Dynamic Object)
☐ github_api (Dynamic Object)

This example shows a dynamic object named `APIC Dynamic Attribute` that corresponds to the dynamic attribute filter created in the dynamic attributes connector.

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

Step 8 Add other conditions to the rule if desired.

What to do next

See Dynamic attributes rule conditions, on page 57.

Use dynamic objects in DNS policies

The dynamic attributes connector enables you to configure dynamic filters, seen in the Secure Firewall Management Center as dynamic objects, in DNS rules. For information about DNS policies, see DNS Policies for Security Intelligence.

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

You can use these dynamic objects on the DNS rule's Dynamic Attributes tab page, similarly to the way you use Security Group Tags (SGTs). You can add dynamic objects as source or destination attributes, except for endpoint device type objects, which are source only.

Procedure

Step 1 Click **Policies** > **Security policies** > **DNS** and create or edit a DNS policy.

Step 2 Add or edit a rule.

Step 3 Click the **Dynamic Attributes** tab.

Step 4 In the **Dynamic Attributes** list, select the objects you want to use, then add them to the source or destination lists as appropriate. Initially, all security group and dynamic objects are listed, by you can uncheck the Security Group option to see dynamic objects only.

Step 5 On the **DNS** tab, select the appropriate list or feed to match the DNS requests you are targeting.

Step 6 Add other conditions to the rule if desired and set the action.

Step 7 Click **Save**.

Dynamic firewall

These topics describe how to integrate user identity data (including Microsoft AD and ISE) with user trust data provided by Identity Intelligence to enhance your ability to detect identity-based exploits in your network.

Related Topics

- About the dynamic firewall, on page 62
- How to configure the dynamic firewall, on page 62

About the dynamic firewall

Previously, the Secure Firewall Management Center collected information about users exclusively from the configured identity source, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address.

The dynamic firewall enables you to add user risk scores from Cisco Identity Intelligence to identity source-provided information so you can set policies based on always-current user posture and risk. We enable you to pair user identity with intelligence and use that information in reporting and access control policies.

To use the dynamic firewall, you must:

- Have an Identity Intelligence tenant

  See Duo Identity Security with Cisco Identity Intelligence.

- Enable the Dynamic Attributes Connector

- Set up an identity source:

  - Cisco Identity Services Engine (Cisco ISE)

  - pxGrid Cloud

    pxGrid Cloud combines identity and posture in the same feed

    More information: What is pxGrid?

  In addition to providing authentication information, Cisco ISE and pxGrid Cloud can provide the following:

  - SGT Exchange Protocol over TCP (SXP) binding and directory session information if desired. For more information, see the *Cisco Identity Services Engine Administrator Guide*

  - Posture and mobile device management compliance. For more information, see Compliance.

- Set up an identity realm:

  - Create an LDAP realm or an Active Directory realm and realm directory

  - Create a Microsoft Azure AD (SAML) realm for passive authentication

The *identity source* provides authentication information (login, logout) as well as posture. The identity source can also provide SXP binding and session directory information if desired.

The *identity realm* provides user, group, and IP address information.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

How to configure the dynamic firewall

This topic helps you understand the concepts and options to configure the dynamic firewall discussed in About the dynamic firewall, on page 62.

Summary

The dynamic firewall integrates an identity source (such as Cisco ISE) with Cisco Identity Intelligence, which provides user trust information to the Secure Firewall Management Center.

1. Configure Cisco Identity Intelligence to collect user trust information.
2. Configure a supported Secure Firewall Management Center identity source.
3. Configure a supported identity realm.
4. Enable the dynamic attributes connector.
5. Configure the dynamic firewall.

Workflow

The following procedure provides a high-level overview of how to configure the dynamic firewall.

1. As a Duo user with the Owner role, provision a Cisco Identity Intelligence tenant.

   You can provision a tenant from Duo Advantage as discussed in *Provision Your Cisco Identity Intelligence Tenant*.

2. In Cisco Identity Intelligence, create an API integration and use the information to set up the dynamic firewall.

   We use Cisco Identity Intelligence to find user and device risk information in your network.

   For more information about Cisco Identity Intelligence, see How-to Guides.

   For more information about this task, see Get required information for Identity Intelligence, on page 65.

3. (Microsoft Azure AD realm only.) In Identity Intelligence, create a Microsoft Entra ID integration.

   For more information, see Microsoft Entra ID (Azure AD) Data Integration.

4. Create an identity source. (If you already have an identity source, continue with the next step.)

   You can do this in any of the following ways:

   - The Configure Dynamic Firewall dialog box displays **Configure** links to start setting up your identity source.
   - Click **Integrations** > **Identity** > **Identity Sources**.

   For more information about creating identity sources, see:

   - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
   - How to configure a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
   - How to configure a pxGrid Cloud identity source (Cisco ISE 3.4 or later)

5. Create an identity realm.

   We support the following realms:

   - Create an LDAP realm or an Active Directory realm and realm directory

     Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

6. Enable the dynamic attributes connector.

   The dynamic attributes connector is required to use the dynamic firewall. It enables your identity source to integrate with Identity Intelligence to provide enhanced insights into user activity.

   See Enable the dynamic attributes connector.

7. Create the dynamic firewall instance. (If you already have a dynamic firewall instance, continue with the next step.)

   Click **Integrations** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

   See Create a dynamic firewall instance, on page 67.

8. Associate your identity source with Cisco Identity Intelligence.

   See Associate an identity source with Identity Intelligence, on page 68.

9. View system-defined filters.

   We create dynamic attributes filters for the following:

   - Untrusted device
   - Trusted device
   - Untrusted user
   - Questionable user

   You can edit or replace these dynamic attributes filters as discussed in Create dynamic attributes filters, on page 75.

10. View system-defined access control rules.

    We create an access control policy named Dynamic Firewall Policy (or similar) with the following rules:

    - Block an untrusted user from any source network to any destination network.
    - Monitor a questionable user from any source network to any destination network.
    - Block an untrusted device from any source network to any destination network.

    You can edit or delete the access control policy and rules as discussed in View and edit the system-created access control policy, on page 74.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

Enable the dynamic attributes connector

This task discusses how to enable the dynamic attributes connector in the Secure Firewall Management Center. The dynamic attributes connector is an integration that enables objects from cloud networking products to be used in Secure Firewall Management Center access controland DNS rules.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integrations** > **Dynamic Attributes Connector**.

Step 3 Slide to **Enabled**.

Step 4 Messages are displayed while the dynamic attributes connector is enabled.

In the event of errors, try again. If errors persist, contact Cisco TAC.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

Get required information for Identity Intelligence

This task discusses how to create an API client, which provides all the get required information to set up Identity Intelligence in the dynamic firewall.

If you already have an API client and you know the values of all the following, you can skip this procedure and continue with Create a dynamic firewall instance, on page 67:

- **Client ID**
- **API URL**
- **Token URL**
- **Client Secret**

Before you begin

Integrating with the dynamic firewall requires you to create an *API client integration* in Identity Intelligence.

Among the values you must know about your API client integration is the client secret, which is displayed when you create the API client only. For that reason you might need to create the API integration first.

For more information about creating an API cilent integration, see Public API.

Procedure

Step 1 Log in to your Identity Intelligence tenant.

Step 2 Click 🧩 (**Integrations**).

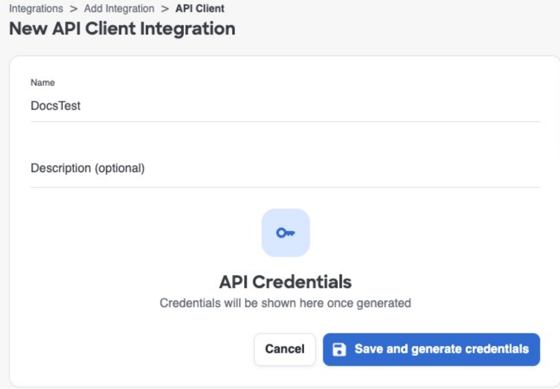
Step 3 Click **Add Integration**.

Step 4 On the next page, under API Clients, click **Add API Client**.

Step 5 Enter a **Name** and an optional **Description**.

Step 6 Click **Save and Generate Credentials**.

The following figure shows an example.



Integrations > Add Integration > API Client

New API Client Integration

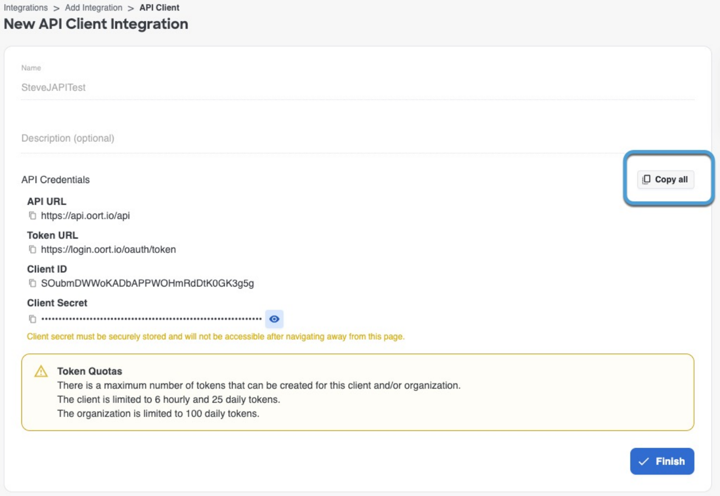
Name: DocsTest

Description (optional)

API Credentials

Credentials will be shown here once generated

Step 7 On the next page, click **Copy all** as the following figure shows.



Integrations > Add Integration > API Client

New API Client Integration

Name: SteveJAPITest

Description (optional)

API Credentials

API URL: https://api.oort.io/api

Token URL: https://login.oort.io/oauth/token

Client ID: SOubmDWWoKADbAPPWOHmRdDtK0GK3g5g

Client Secret: ••

Client secret must be securely stored and will not be accessible after navigating away from this page.

Token Quotas
There is a maximum number of tokens that can be created for this client and/or organization.
The client is limited to 6 hourly and 25 daily tokens.
The organization is limited to 100 daily tokens.

Step 8 Save the credentials for later use.

Step 9 Click **Finish**.

What to do next

See Create a dynamic firewall instance, on page 67.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

Create an identity source and realm for the dynamic firewall

Before you configure the dynamic firewall, you must configure a supported identity realm and identity source.

Configure an identity realm

These identity realms are supported:

- Create an LDAP realm or an Active Directory realm and realm directory

  Only Microsoft AD is supported; LDAP realms are not supported.

- Create a Microsoft Azure AD (SAML) realm for passive authentication

Configure an identity source

These identity sources are supported:

- On-premises Cisco ISE: Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- Single or multiple Cisco ISE clusters:
  - How to configure a pxGrid Cloud identity source (Cisco ISE 3.4 or later)
  - How to configure a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

Create a dynamic firewall instance

This task discusses how to create a new instance of the dynamic firewall, which is an association between an identity source and Identity Intelligence.

Before you begin

Do all of the following:

- Enable the dynamic attributes connector as discussed in Enable the dynamic attributes connector.
- Create an identity source:
  - Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source.
  - Create a pxGrid Cloud identity source.

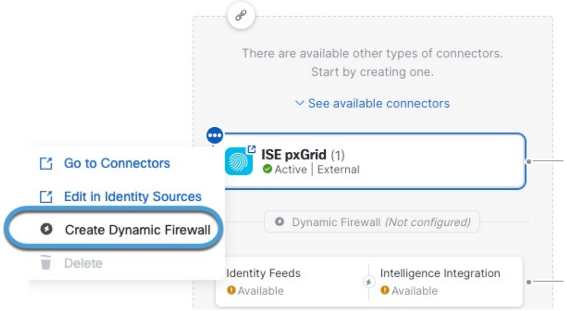
Procedure

Step 1 If you have not already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Administration** > **Dynamic Attributes Connector**.

Step 3 Click ⋯ next to the name of the identity source with which to add the dynamic firewall.

The following figure shows an example.



Note

If you do not see an identity source, create one before continuing:

- Ways to configure the Cisco Identity Services Engine (Cisco ISE) identity source
- How to configure a pxGrid Cloud identity source (Cisco ISE 3.3 or earlier)
- How to configure a pxGrid Cloud identity source (Cisco ISE 3.4 or later)

Step 4 Click **Create Dynamic Firewall**.

Step 5 Continue with Associate an identity source with Identity Intelligence, on page 68.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

Associate an identity source with Identity Intelligence

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device trust ratings to the Secure Firewall Management Center.

For more information, see User Trust Level.

Before you begin

Before you begin, make sure you:

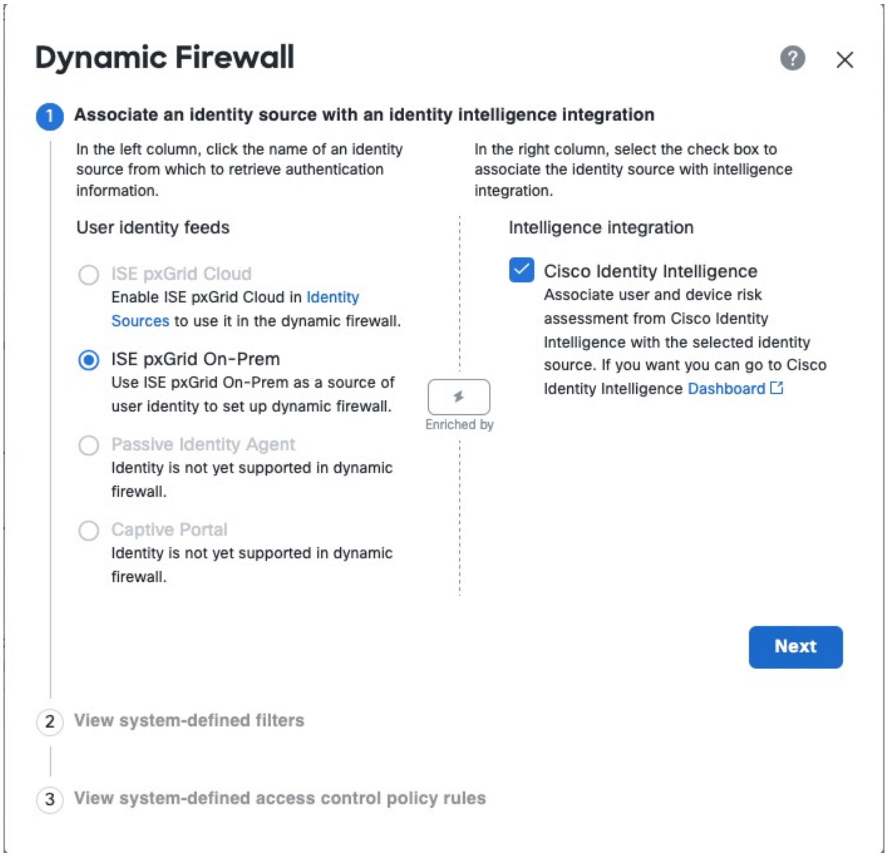
- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in About the dynamic firewall, on page 62.
- Completed the tasks discussed in Create a dynamic firewall instance, on page 67.

Procedure

Step 1 Start with Create a dynamic firewall instance, on page 67.

Step 2 On the next page, from the left column, click your identity source. Then, in the right column, select the **Cisco Identity Intelligence** check box to add user intelligence, including user and device risk.

The following figure shows an example.



Dynamic Firewall

1 Associate an identity source with an identity intelligence integration

In the left column, click the name of an identity source from which to retrieve authentication information.

In the right column, select the check box to associate the identity source with intelligence integration.

User identity feeds

○ ISE pxGrid Cloud
Enable ISE pxGrid Cloud in Identity Sources to use it in the dynamic firewall.

● ISE pxGrid On-Prem
Use ISE pxGrid On-Prem as a source of user identity to set up dynamic firewall.

○ Passive Identity Agent
Identity is not yet supported in dynamic firewall.

○ Captive Portal
Identity is not yet supported in dynamic firewall.

Intelligence integration

☑ Cisco Identity Intelligence
Associate user and device risk assessment from Cisco Identity Intelligence with the selected identity source. If you want you can go to Cisco Identity Intelligence Dashboard

2 View system-defined filters

3 View system-defined access control policy rules

Step 3 Click **Next**.

Step 4 Continue with Configure Identity Intelligence, on page 69.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

Configure Identity Intelligence

This task discusses how you associate an identity source with Identity Intelligence, which provides user and device risk ratings to the Secure Firewall Management Center.

Before you begin

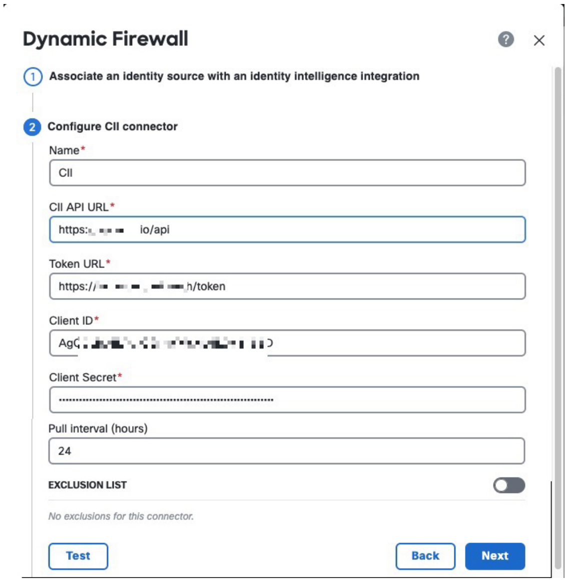
Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 68.

Procedure

Step 1 Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 68.

Step 2 If you selected the **Cisco Identity Intelligence** check box, enter the information you found for Identity Intelligence as described in Get required information for Identity Intelligence, on page 65.

The following figure shows an example.



Dynamic Firewall

1 Associate an identity source with an identity intelligence integration

2 Configure CII connector

Name*: CII

CII API URL*: https:[redacted]io/api

Token URL*: https://[redacted]h/token

Client ID*: AgC[redacted]

Client Secret*: ••

Pull interval (hours): 24

EXCLUSION LIST ○

No exclusions for this connector.

Step 3 (Optional.) For Identity Intelligence to consider a specific set of users as trusted, slide **Exclusion List** to **Slider enabled** (●).

Enter one user name per line in **username@domain.com** format. Users in this list are considered trusted by Identity Intelligence.

Step 4 Click **Test**.

Only if the test succeeds, continue with the next step.

If any errors are displayed, check all of your Identity Intelligence values and try again.

Step 5 Click **Next**.

Step 6 Continue with View system-defined filters, on page 70.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

View system-defined filters

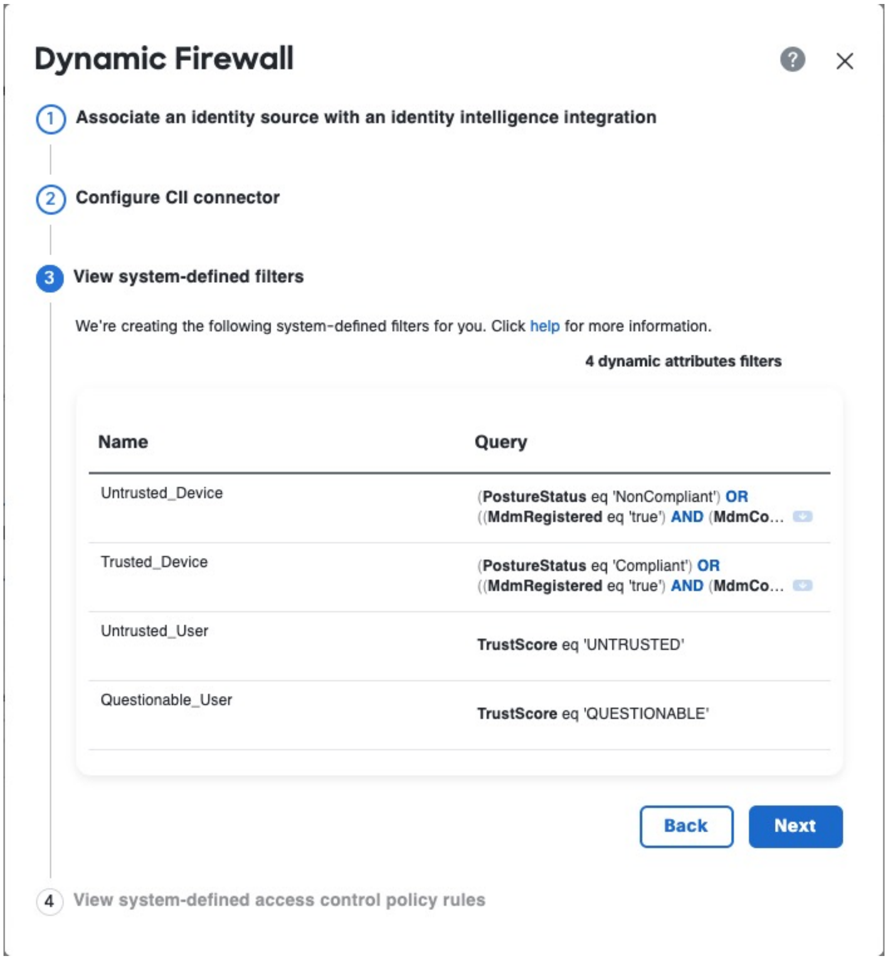
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the Secure Firewall Management Center.

Before you begin

See Configure Identity Intelligence, on page 69.

Procedure

Step 1 The system displays a set of system-defined dynamic attributes filters, as the following figure shows.



Dynamic Firewall

1. Associate an identity source with an identity intelligence integration
2. Configure CII connector
3. View system-defined filters

We're creating the following system-defined filters for you. Click help for more information.

4 dynamic attributes filters

Name	Query
Untrusted_Device	(**PostureStatus** eq 'NonCompliant') **OR** ((**MdmRegistered** eq 'true') **AND** (**MdmCo…**
Trusted_Device	(**PostureStatus** eq 'Compliant') **OR** ((**MdmRegistered** eq 'true') **AND** (**MdmCo…**
Untrusted_User	**TrustScore** eq 'UNTRUSTED'
Questionable_User	**TrustScore** eq 'QUESTIONABLE'

4. View system-defined access control policy rules

Step 2 View the system-created filters. Click ▾ on any row to expand the filter so you can view the filter and see its details.

Step 3 Click **Next**.

Step 4 Continue with View system-defined access control rules, on page 71.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

View system-defined access control rules

This task discusses access control rules created by the dynamic firewall.

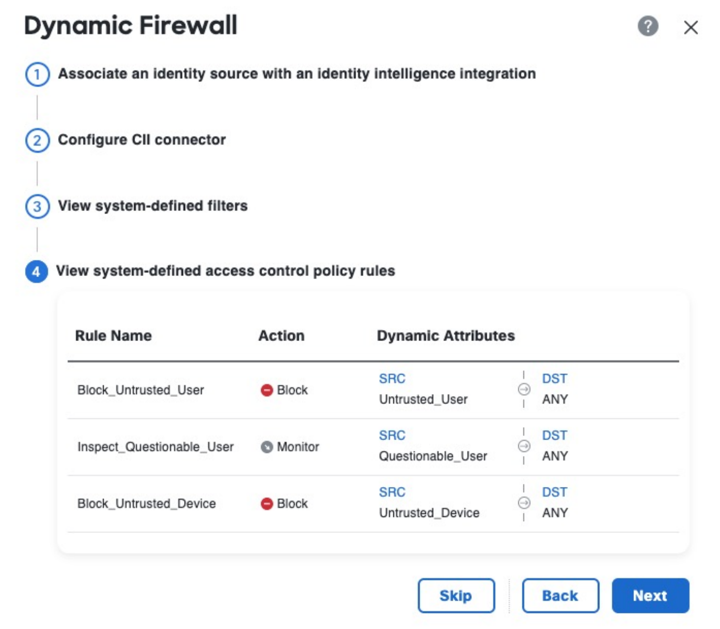
Before you begin

See View system-defined filters, on page 70.

Procedure

Step 1 View the system-created access control rules.

The following figure shows an example.



Dynamic Firewall

1 Associate an identity source with an identity intelligence integration

2 Configure CII connector

3 View system-defined filters

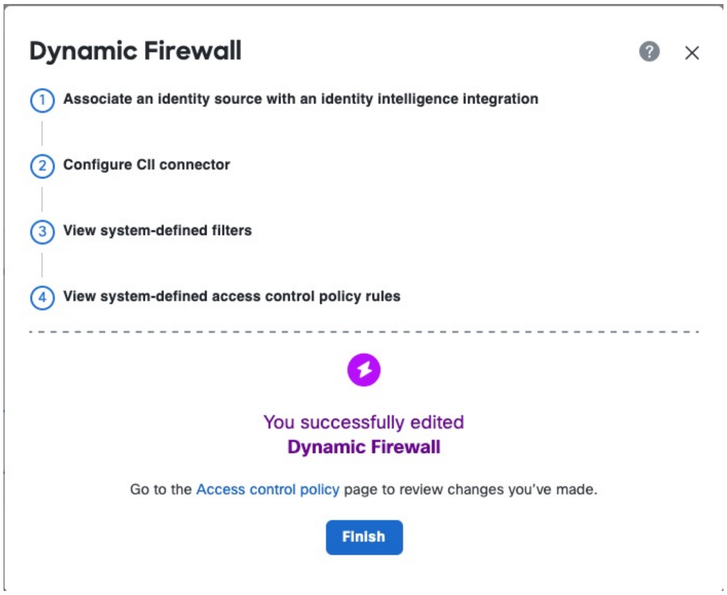
4 View system-defined access control policy rules

Rule Name	Action	Dynamic Attributes
Block_Untrusted_User	⊖ Block	SRC Untrusted_User → DST ANY
Inspect_Questionable_User	Monitor	SRC Questionable_User → DST ANY
Block_Untrusted_Device	⊖ Block	SRC Untrusted_Device → DST ANY

Step 2 Choose one of these options:

- Click **Skip** to skip creating these access control rules. You can create your own anytime.
- Click **Next** to create an access control policy named Dynamic Firewall Policy with the rules shown in the preceding figure.
- Click **Back** to return to system-created filters.

Step 3 After you click **Next**, if you created access control rules successfully, the following page is displayed:



Dynamic Firewall

1. Associate an identity source with an identity intelligence integration
2. Configure CII connector
3. View system-defined filters
4. View system-defined access control policy rules

You successfully edited
Dynamic Firewall

Go to the Access control policy page to review changes you've made.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

Edit the user exclusion list

(Optional.) You can instruct Identity Intelligence to treat specific users as trusted.

Before you begin

Configure the dynamic firewall as discussed in Create a dynamic firewall instance, on page 67.

Procedure

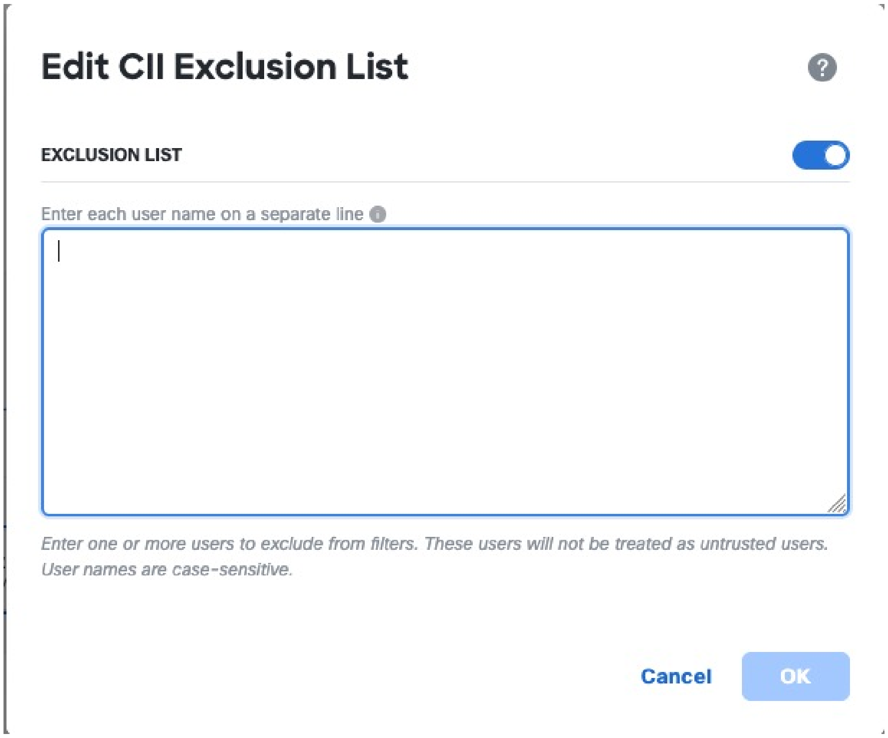
Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector**.

Step 3 Click ••• next to the name of the identity source.

Step 4 Click **Edit CII Exclusion List**.

The following dialog box is displayed.



Edit CII Exclusion List

EXCLUSION LIST

Enter each user name on a separate line

Enter one or more users to exclude from filters. These users will not be treated as untrusted users. User names are case-sensitive.

Step 5 In the provided field, enter one user name in `username@domain.com` format on a line, press Enter, and enter another user name.

Each user name is considered as trusted by Identity Intelligence.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

View and edit the system-created access control policy

This topic discusses how you can edit the system-created access control rules and policy. Initially, the policy isn't associated with any devices but if you want to use it you can add devices, change rules, reorder rules, or delete rules.

Before you begin

Complete the tasks described in View system-defined access control rules, on page 71.

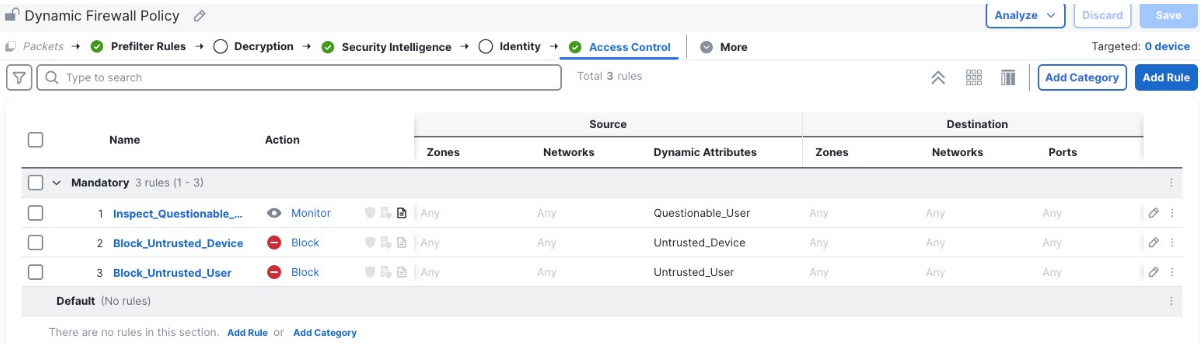
Procedure

Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

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

Step 3 Click **Edit** (✎) next to the policy named Dynamic Firewall Policy (or similar).

The following figure shows a sample access control policy.



	Name	Action	Source			Destination		
			Zones	Networks	Dynamic Attributes	Zones	Networks	Ports
Mandatory 3 rules (1 - 3)								
1	Inspect_Questionable_...	Monitor	Any	Any	Questionable_User	Any	Any	Any
2	Block_Untrusted_Device	Block	Any	Any	Untrusted_Device	Any	Any	Any
3	Block_Untrusted_User	Block	Any	Any	Untrusted_User	Any	Any	Any
Default (No rules)								

There are no rules in this section. Add Rule or Add Category

Note that in this access control policy, only the rule set to monitor questionable users logs anything. To adjust the logging settings, see Logging settings for access control policies.

Step 4 Do any of the following:

- Target the access control policy at devices: Assigning devices to an access control policy.
- Edit the policy, including adding logging: Managing access control policies.
- Edit access control rules: Managing access control rules.
- Set advanced policy options: Configuring advanced settings for the access control policy.
- Associate other policies with this access control policy: Associating other policies with access control.

Related Topics

About the dynamic firewall, on page 62
How to configure the dynamic firewall, on page 62

Create dynamic attributes filters

Dynamic attributes filters that you define using the 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.

For more information about access control rules, see Create access control rules or DNS rules using dynamic attributes filters.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Integrations** > **Dynamic Attributes Connector** > **Connectors**.

Step 3 Do any of the following:

- Add a new filter: click **Add** (+).

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

Step 4 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	Click Add ⊞.

Step 5 To add a query, enter the following information.

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

Step 6 Click **Show Preview** to display a list of networks or IP addresses returned by your query.

Step 7 When you're finished, click **Save**.

Step 8 (Optional.) Verify the dynamic object in the Secure Firewall Management Center .

a) Log in to the Secure Firewall Management Center as a user with the Network Admin role at minimum.

b) Click **Objects** > **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.

Related Topics

About the dynamic firewall, on page 62

How to configure the dynamic firewall, on page 62

Disable the dynamic attributes connector

If you no longer wish to collect dynamic objects from cloud sources, you can disable the Dynamic Attributes Connector in the Secure Firewall Management Center as discussed in the following task.

Procedure

Step 1 Log in to the Secure Firewall Management Center if you have not done so already.

Step 2 Click **Integrations** > **Dynamic Attributes Connector**.

Step 3 Slide to **Disabled**.

Troubleshoot using the Secure Firewall Management Center

This task discusses how to generate troubleshoot files for the Secure Firewall Management Center.

Procedure

Step 1 Log in to the Secure Firewall Management Center.

Step 2 Click **Troubleshooting** > **Health** > **Monitor**.

Step 3 In the left pane, click **Firewall Management Center**.

Step 4 At the top, click **System & Troubleshooting Details**.

Step 5 Click **Generate Troubleshooting Files**.

Step 6 Provide the files to Cisco TAC or to your Beta coordinator.

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 Firewall 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
- Firewall Management Center
- Cisco APIC

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 Firewall Management Center. For example:

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

If you access vCenter or Firewall 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.

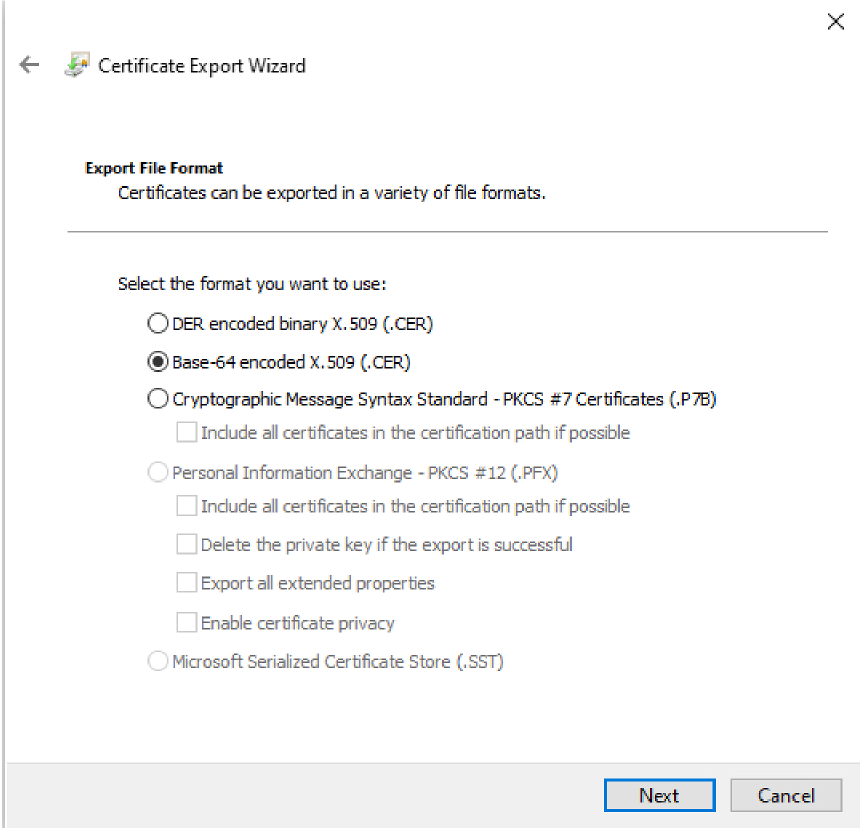
4. Repeat these tasks for vCenter Firewall Management Center.

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 Firewall 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.



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

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

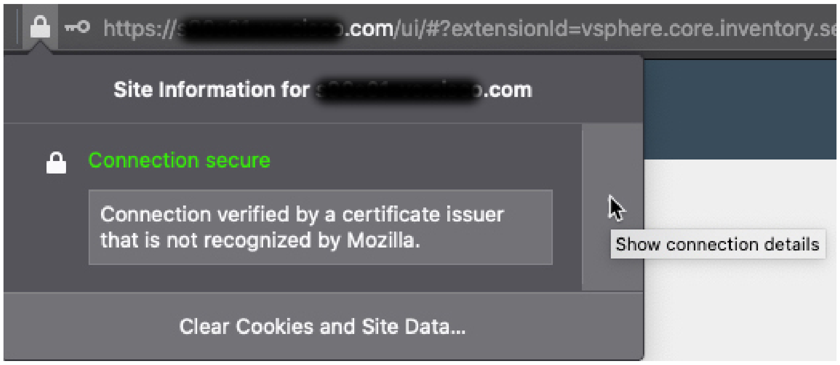
10. Follow the prompts to complete the export.
11. Open the certificate in a text editor.
12. Repeat the process for all certificates in the chain.

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



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

Site Information for [redacted].com

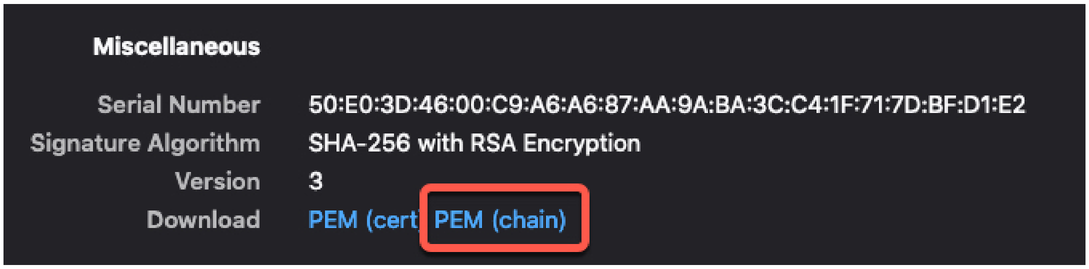
Connection secure

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

Show connection details

Clear Cookies and Site Data...

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



Miscellaneous

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

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

Related Topics

System requirements for the integration with Cisco APIC, on page 30
Get required information for the integration, on page 30
Create a Cisco APIC connector, on page 33
How to use dynamic objects from Cisco APIC in Secure Firewall Management Center access control rules or DNS Rules, on page 29
Manually get a certificate authority (CA) chain, on page 35
Cisco APIC connector, on page 28

Security requirements

To safeguard the 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 4: Dynamic Attributes Connector access requirements

URL	Reason
https://*fmc-ip***/api/fmc_platform/v1/ auth/generatetoken**	Authentication
https://*fmc-ip***/api/fmc_config/ v1/domain/***domain-id***/object/dynamicobjects**	GET and POST dynamic objects
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 5: 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 Dynamic Attributes Connector are being migrated from Docker Hub to Amazon Elastic Container Registry (Amazon ECR).

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

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

Dynamic Attributes Connector Azure access requirements

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

History for the dynamic attributes connector

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
DNS rule support for dynamic objects and security group tags.	10.0.0	10.0.0	You can configure DNS rules in the DNS policy to use dynamic objects or security group tags (SGT). If you are using these types of objects in access control rules already, you can now extend their use to your DNS policy. We added the Dynamic Attributes tab to the add/edit DNS rule dialog box.
Dynamic firewall	10.0.0	10.0.0	Previously, the Secure Firewall Management CenterSecure Firewall Management Center collected information about users exclusively from the configured identity source, such as Microsoft Active Directory, the passive identity agent, Cisco Identity Services Engine (Cisco ISE), and so on. This information generally included user name, group, and IP address. The dynamic firewall enables you to add user risk scores from Cisco Identity Intelligence to identity source-provided information so you can set policies based on always-current user posture and risk. We enable you to pair user identity with intelligence and use that information in reporting and access control policies. **New/modified screens**: • Click **Integrations** > **Dynamic Attributes Connector**. Then click ⋯ next to the name of the identity source and click **Create Dynamic Firewall**.
Cisco APIC connector	10.0.0	10.0.0	The dynamic attributes connector enables you to send Cisco APIC dynamic endpoint group (EPG) and endpoint security group (ESG) data from Cisco APIC tenants to . **New/updated screens:** • **Integrations** > **Dynamic Attributes Connector** > **Connectors** > **New Connector**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
New connectors	7.6	20241127	AWS security groups, AWS service tags, and Cisco Cyber Vision These connectors can send an on-premises Secure Firewall Management Center dynamic objects as can Security Cloud Control. To receive dynamic objects from an on-premises dynamic attributes connector, version 3.0 of the on-premises dynamic attributes connector is required.
Dynamic Attributes Connector	7.4.0	7.4.0	This feature is introduced. The Dynamic Attributes Connector is now included in the Secure Firewall Management Center. You can use the dynamic attributes connector to get IP addresses from cloud-based platforms such as Microsoft Azure in access control rules without having to deploy to managed devices. More information: • The dynamic attributes connector included with this product: About the Dynamic Attributes Connector, on page 1 • The standalone dynamic attributes connector: *Cisco Secure Dynamic Attributes Connector Configuration Guide* New/modified screen: **Integrations** > **Dynamic Attributes Connector**