Dynamic Firewall Solution Guide

First Published: 2025-08-15

Last Modified: 2025-12-05

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

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

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

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

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

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

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

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

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

CHAPTER 1

About the Dynamic Firewall

The following topics provide general information about the Dynamic Firewall.

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 an 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.

CHAPTER 2

Configure the Dynamic Firewall

- How to configure the dynamic firewall, on page 3
- Create dynamic attributes filters, on page 15

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 1.

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 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 5.

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 **System** (⚙) > **Integration** > **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 (ISE 3.3 or Earlier)
- How to Configure a pxGrid Cloud Identity Source (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 an 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 **Integration** > **Dynamic Attributes Connector** and click **Configure Dynamic Firewall**.

See Create a dynamic firewall instance, on page 7.

8. Associate your identity source with Cisco Identity Intelligence.

See Associate an identity source with Identity Intelligence, on page 9.

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 15.

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 14.

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 Firewall Management Center access control rules.

Procedure

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

Step 2 Click **Integration** > **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.

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 :

- **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**).

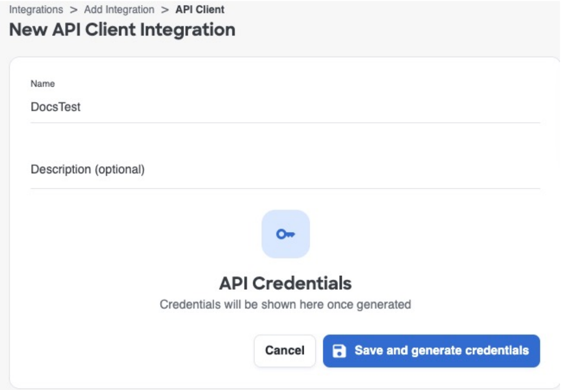
Step 3 Click **Add Integration**.

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

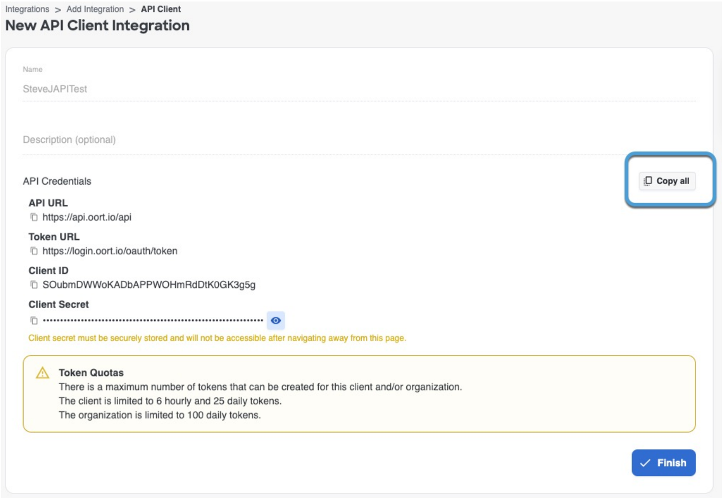
DocsTest

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 Paste the credentials to a text file so they are available later.

Step 9 Click **Finish**.

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 an 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 (ISE 3.3 or earlier)
  - How to configure a pxGrid cloud identity source (ISE 3.4 or later)

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 .
- Create an identity source:
  - 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 (ISE 3.3 or earlier)
    - How to configure a pxGrid cloud identity source (ISE 3.4 or later)

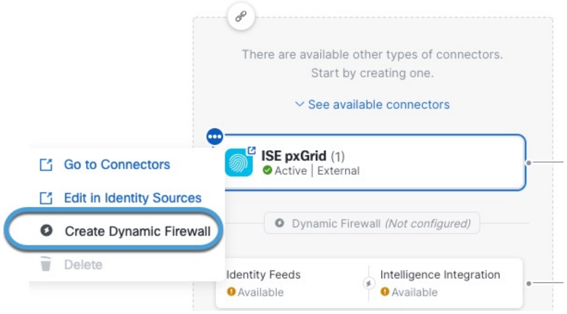
Procedure

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

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

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

The following figure shows an example.



There are available other types of connectors. Start by creating one.

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 (ISE 3.3 or earlier)
- How to configure a pxGrid cloud identity source (ISE 3.4 or later)

Step 4 Click **Create Dynamic Firewall**.

Step 5 Continue with Associate an identity source with Identity Intelligence.

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:

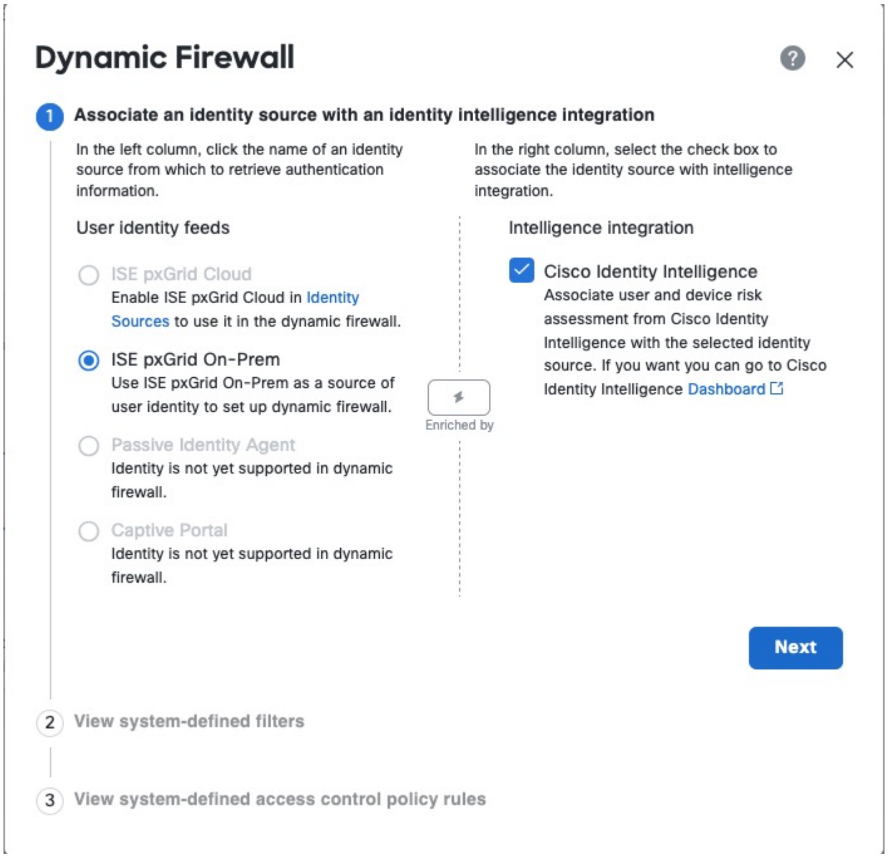
- Understand how the identity realm, identity source, and Identity Intelligence work together as discussed in About the dynamic firewall, on page 1.
- Completed the tasks discussed in Create a dynamic firewall instance, on page 7.

Procedure

Step 1 Start with Create a dynamic firewall instance.

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 10.

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

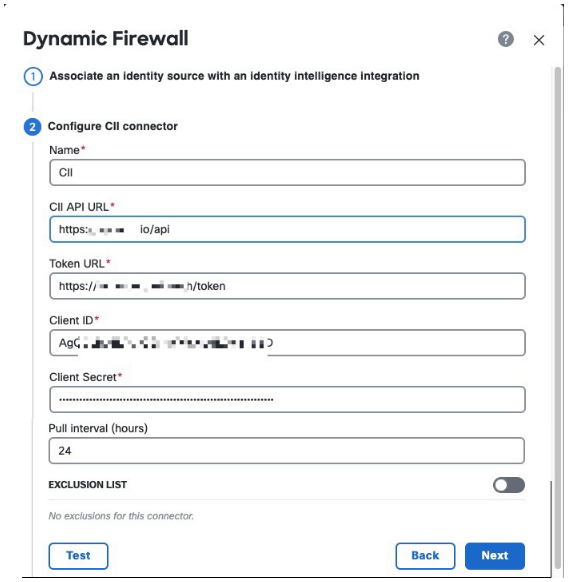
Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 9.

Procedure

Step 1 Complete the tasks discussed in Associate an identity source with Identity Intelligence, on page 9.

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 5.

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 11.

View system-defined filters

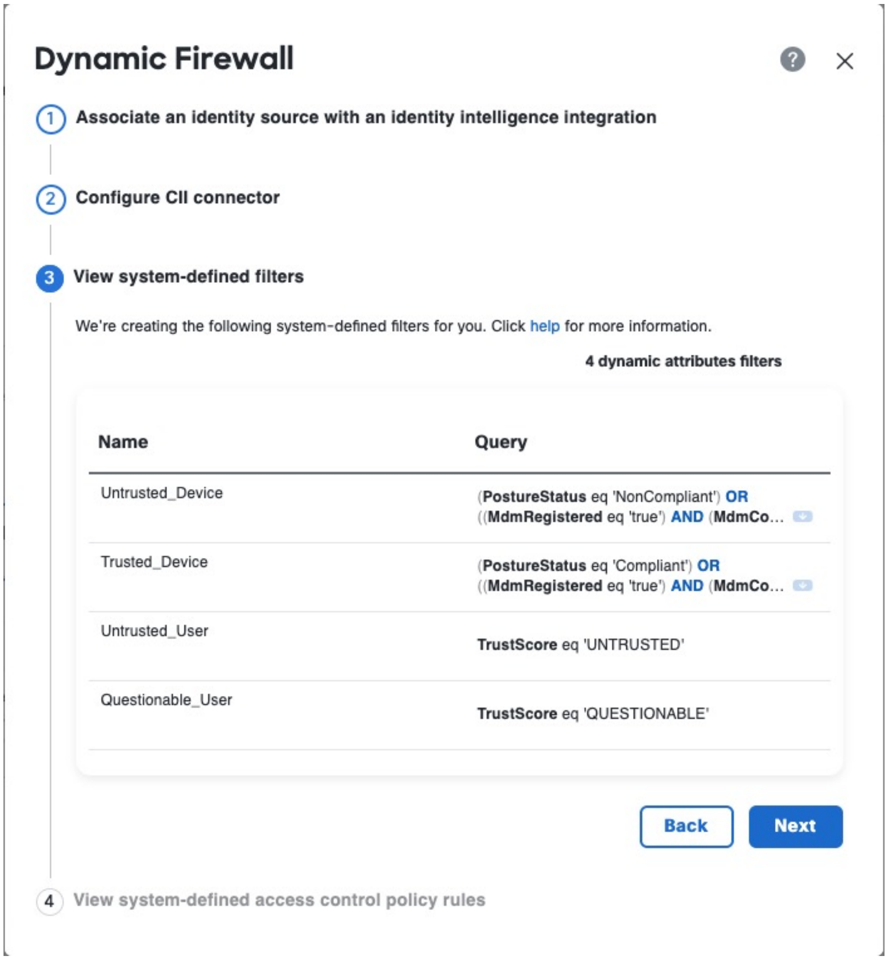
This task discusses how you associate an identity source with Cisco Identity Intelligence, which provides user and device risk ratings to the Secure Firewall Management Center.

Before you begin

See Configure Identity Intelligence.

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 12.

View system-defined access control rules

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

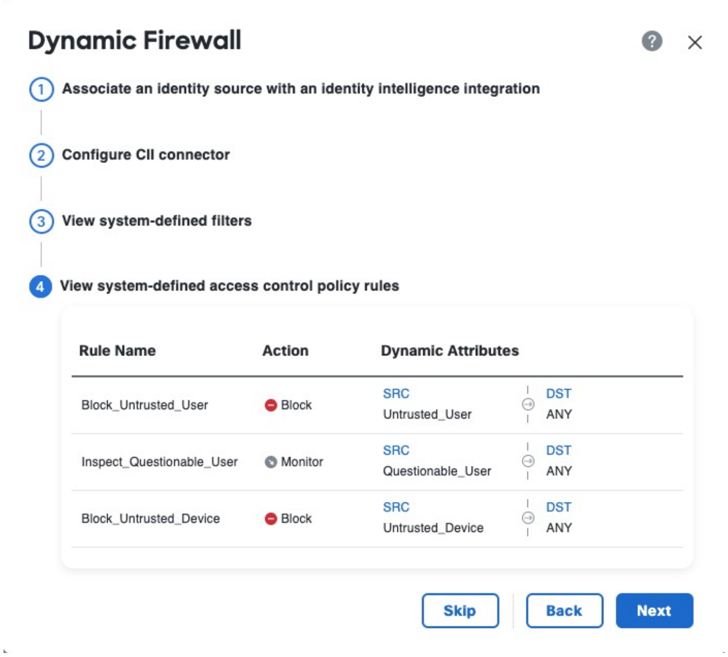
Before you begin

See View system-defined filters, on page 11.

Procedure

Step 1 View the system-created access control rules.

The following figure shows an example.



Dynamic Firewall

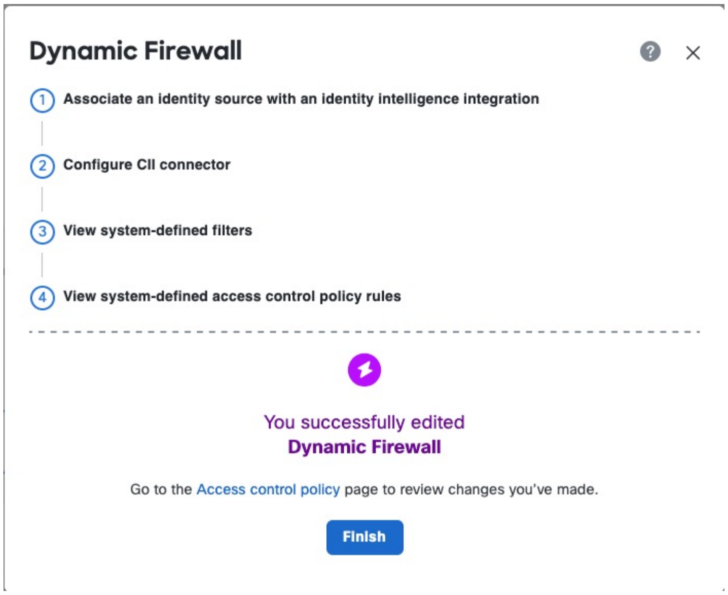
1. Associate an identity source with an identity intelligence integration
2. Configure CII connector
3. View system-defined filters
4. View system-defined access control policy rules

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.

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 7.

Procedure

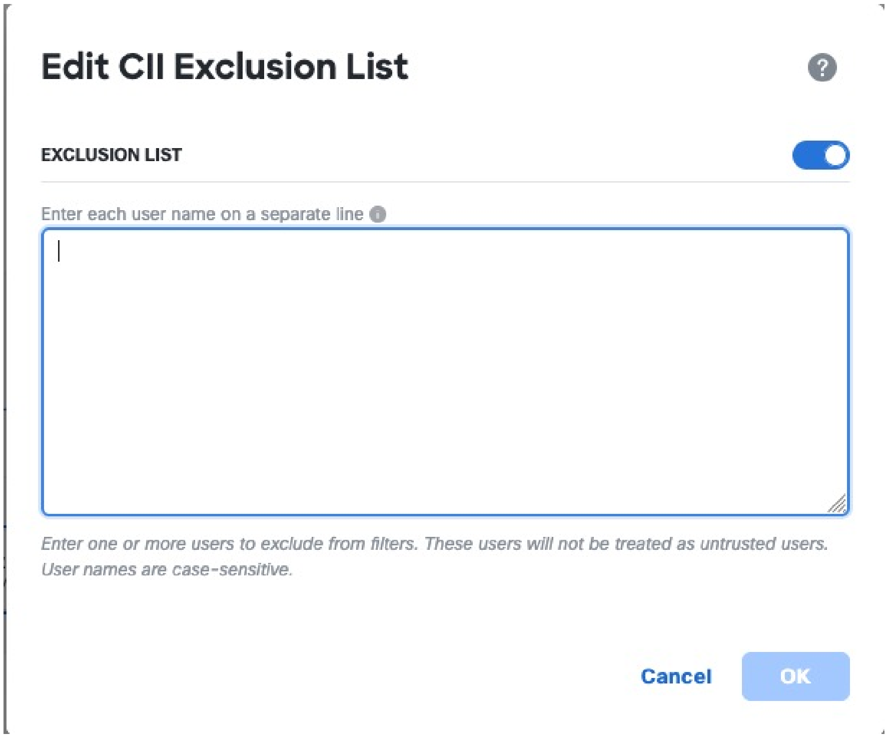
Step 1 If you haven't already done so, log in to the Secure Firewall Management Center.

Step 2 Click **Integration** > **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.
Cancel
OK

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.

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 12.

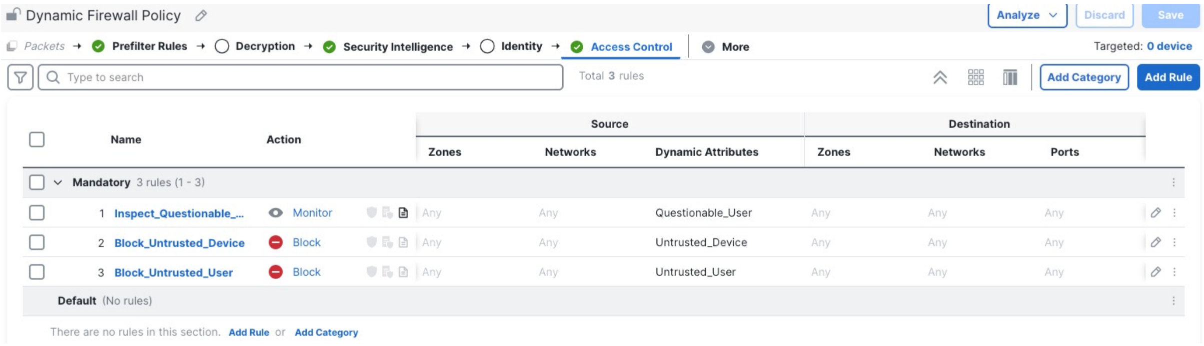
Procedure

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

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



			Source			Destination		
	Name	Action	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, seeLogging 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: Access control policy advanced settings.
- Associate other policies with this access control policy: Associating other policies with access control .

Create dynamic attributes filters

Dynamic attributes filters that you define using the 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.

Procedure

Step 1 Log in to Secure Firewall Management Center.

Step 2 Click **Policies** > **Firewall Threat Defense** > **Integration** > **Other Integrations** > **Dynamic Attributes Connector**.

Step 3 Click **Dynamic Attributes Filters**.

- 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** > **Object Management** > **External Attributes** > **Dynamic Object**.
The dynamic attribute query you created should be displayed as a dynamic object.