Enable SAML SSO for Firewall Management Center Using Duo as Identity Provider

Revised: November 30, 2025

Enable SAML SSO for Management Center Using Duo

Is this Guide for You?

This guide helps network administrators configure Security Assertion Markup Language (SAML) Single Sign-On (SSO) in Firewall Management Center with Duo as the Identity Provider (IdP).

Overview of SAML SSO in Firewall Management Center

When you enable SSO in Firewall Management Center, the login page displays an SSO link. Users with SSO access can click this link to sign in through their IdP, in this case, Duo, instead of entering a username and password in the Firewall Management Center login page. After Duo authenticates the user, they are redirected back to the Firewall Management Center web interface and are automatically logged in. Firewall Management Center does not require a direct network connection to Duo because all communication between Firewall Management Center and Duo occurs through the user's browser.

In a multitenant Firewall Management Center, you can configure SSO to assign SAML users to specific subdomains. This configuration must be done at the global domain level. If there is a mismatch between the roles in Duo and Firewall Management Center, the default role, which is that of a security analyst, is assigned to the user. With this default role, a user has access to all domains.

System Requirements

Table 1 lists the platforms and versions for this feature and the example provided in this document.

Product	Version	Version used in this guide
Cisco Secure Firewall Management Center	6.7 or later	10.0
Cisco Secure Firewall Threat Defense	6.7 or later	10.0
Duo Admin Panel	—	Duo 75

Prerequisites for Configuring Duo for SSO in Firewall Management Center

- Ensure that you have a Duo administrator account.
- Log in to Duo Admin Panel at https://admin.duosecurity.com/login using your Duo administrator account credentials.
- Complete two-factor authentication.
- Download Duo Mobile on user's device for two-factor authentication.
- Ensure that Firewall Management Center can reach the Duo IdP.

Guidelines for Using Duo to Enable SAML SSO in Firewall Management Center

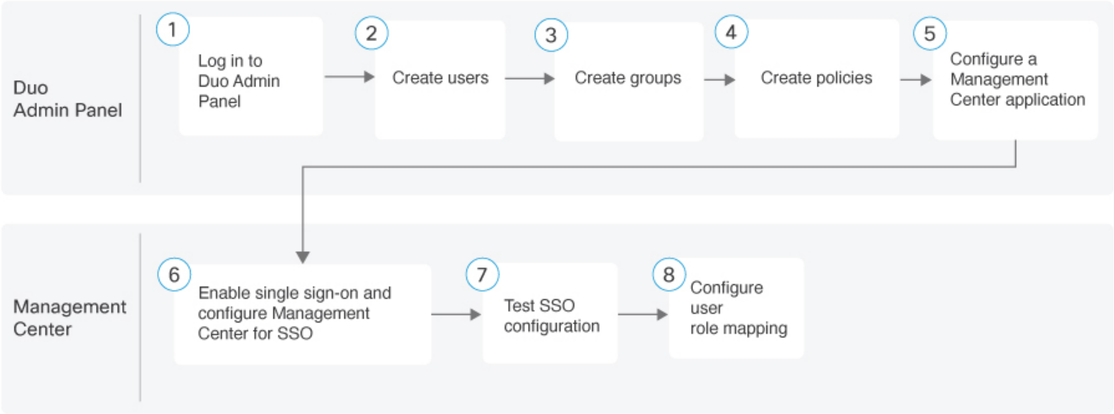
Guidelines

- Only users with the administrator role authenticated internally or by LDAP or RADIUS can configure SSO.
- In Firewall Management Center high-availability configurations, ensure that you follow these guidelines:
  - Since SSO configuration is not synchronized between the members of the high availability pair, you must configure SSO separately on each member of the pair.
  - Both Firewall Management Centers in a high-availability pair must use the same IdP for SSO. You must configure a service provider application in Duo for each Firewall Management Center configured for SSO.
  - Before a user can use SSO to access the secondary Firewall Management Center for the first time, that user must first use SSO to log into the primary Firewall Management Center at least once.
- Do not configure SSO in deployments using CC mode.

Limitations

- Firewall Management Center can support SSO with only one SSO provider at a time—you cannot configure the Firewall Management Center to use, for instance, both Duo and Okta for SSO.
- Firewall Management Center does not support SSO initiated from Duo.
- Firewall Management Center does not support logging in with CAC credentials for SSO accounts.

Workflow for Enabling SAML SSO in Firewall Management Center Using Duo


Duo Admin Panel
1
Log in to Duo Admin Panel
2
Create users
3
Create groups
4
Create policies
5
Configure a Management Center application
Management Center
6
Enable single sign-on and configure Management Center for SSO
7
Test SSO configuration
8
Configure user role mapping

Step	Task	More Information
1	Log in to Duo Admin panel.	—
2	Create users in Duo.	Create a User in Duo, on page 4
3	Create groups in Duo.	Create a Group in Duo, on page 7
4	Create policies in Duo.	Create a Policy, on page 9
5	Configure a Firewall Management Center application in Duo.	Create a Firewall Management Center Application in Duo, on page 10
6	Enable SSO and configure Firewall Management Center for SSO.	Configure Firewall Management Center for Duo SSO, on page 12
7	Test SSO configuration in Firewall Management Center.	—
8	Configure user role mapping in Firewall Management Center.	Configure Firewall Management Center for Duo SSO, on page 12

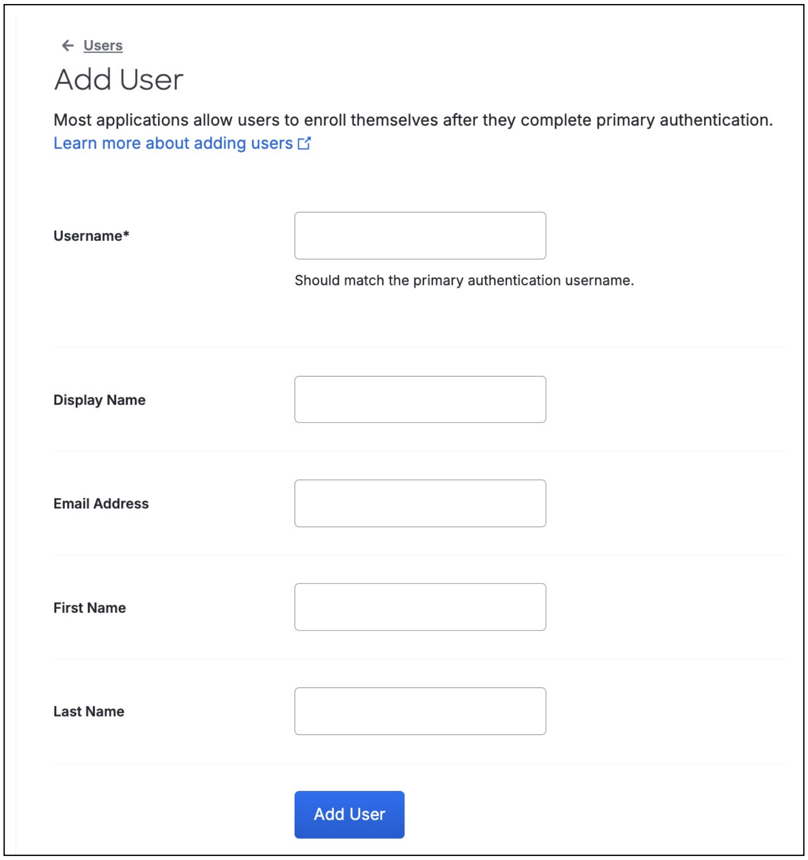
Create a User in Duo

You must create Duo user accounts from the Duo Admin panel. These user accounts allow your end-users to log in to Duo-protected services and applications with two-factor authentication.

Procedure

Step 1 From the Duo Admin panel, choose **Users** > **Users**.

Step 2 Click **Add user**.



← Users

Add User

Most applications allow users to enroll themselves after they complete primary authentication.
Learn more about adding users

Username*

Should match the primary authentication username.

Display Name

Email Address

First Name

Last Name

Add User

Step 3 In the **Username** field, enter the username.

Step 4 In the **Display Name** field, enter the user's display name.

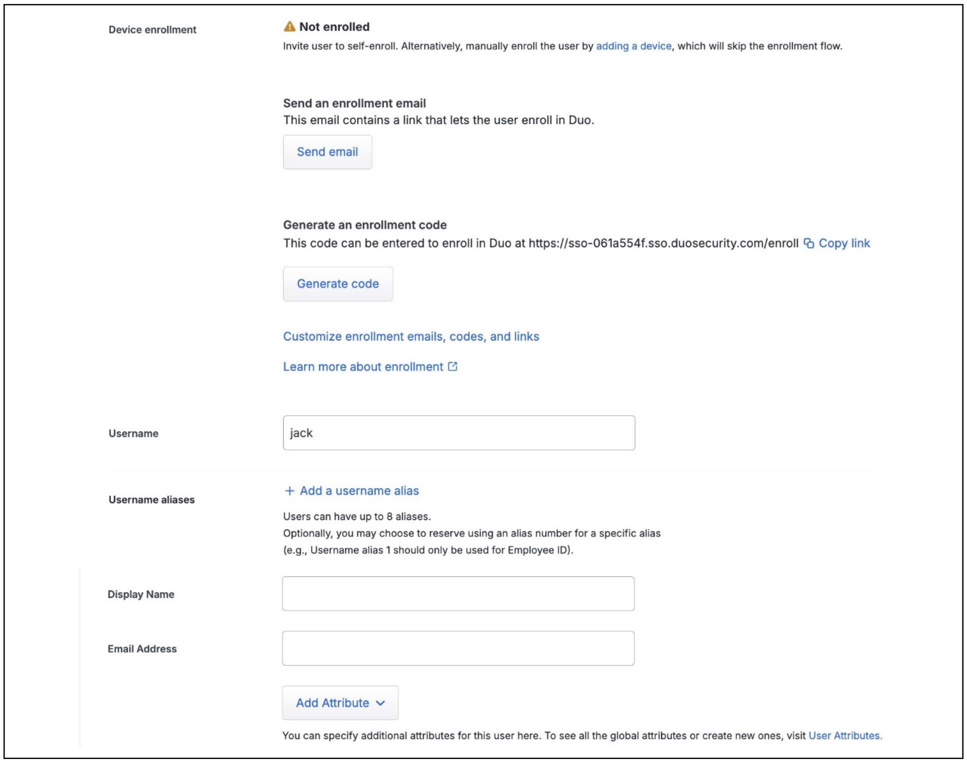
Step 5 In the **Email Address** field, enter the user's email address.

Step 6 Click **Add User**

The user is created and you enter the edit mode for the user.

Step 7 In **Device enrollment**, click **Send email**.

This email contains a link that lets the user enroll in Duo.



Device enrollment

⚠ **Not enrolled**

Invite user to self-enroll. Alternatively, manually enroll the user by adding a device, which will skip the enrollment flow.

Send an enrollment email

This email contains a link that lets the user enroll in Duo.

Generate an enrollment code

This code can be entered to enroll in Duo at https://sso-061a554f.sso.duosecurity.com/enroll Copy link

Generate code
Customize enrollment emails, codes, and links
Learn more about enrollment

Username: jack

Username aliases

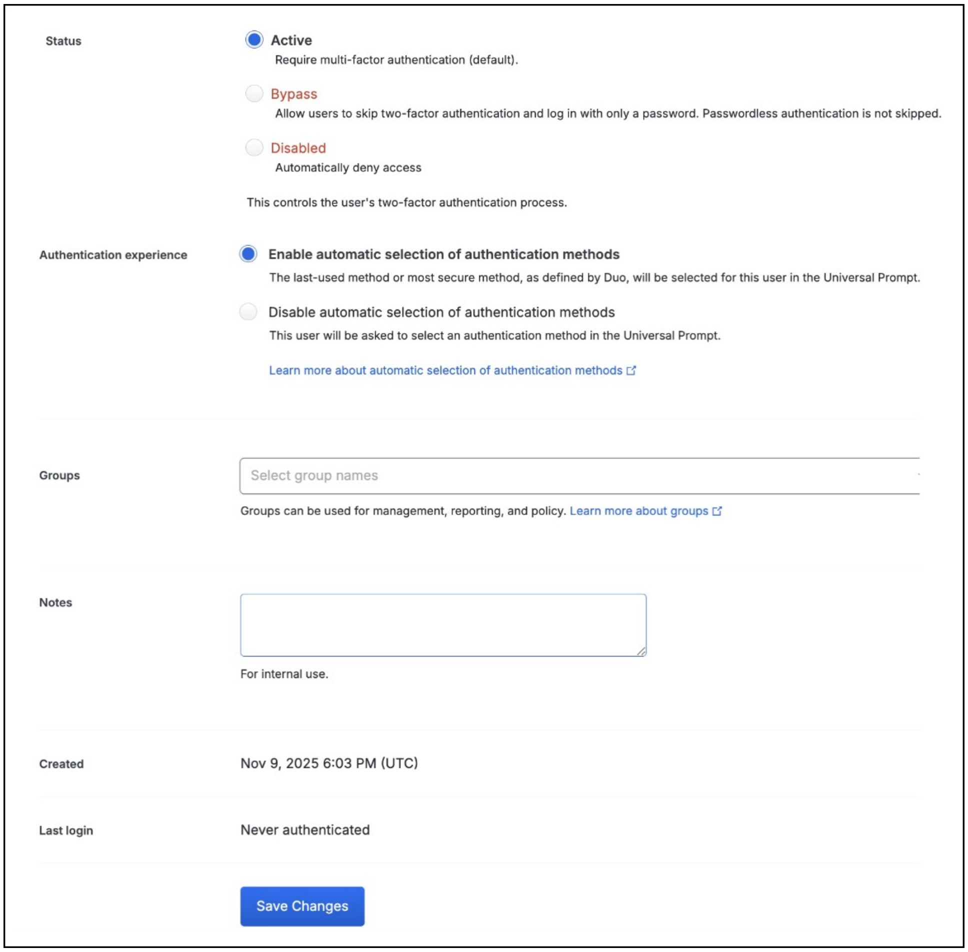
Users can have up to 8 aliases.
Optionally, you may choose to reserve using an alias number for a specific alias
(e.g., Username alias 1 should only be used for Employee ID).

Display Name:

Email Address:

You can specify additional attributes for this user here. To see all the global attributes or create new ones, visit User Attributes.

Step 8 In **Status**, click the **Active** radio button to require multi-factor authentication (MFA) for the user.



Status

● Active
Require multi-factor authentication (default).

○ Bypass
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.

○ Disabled
Automatically deny access

This controls the user's two-factor authentication process.

Authentication experience

● Enable automatic selection of authentication methods
The last-used method or most secure method, as defined by Duo, will be selected for this user in the Universal Prompt.

○ Disable automatic selection of authentication methods
This user will be asked to select an authentication method in the Universal Prompt.

Learn more about automatic selection of authentication methods

Groups

Select group names

Groups can be used for management, reporting, and policy. Learn more about groups

Notes

For internal use.

Created: Nov 9, 2025 6:03 PM (UTC)

Last login: Never authenticated

Step 9 Click **Save Changes**.

The user gets an email from Duo Security to set up a user account for Duo. The user must click the link in the email to create an account.

Create a Group in Duo

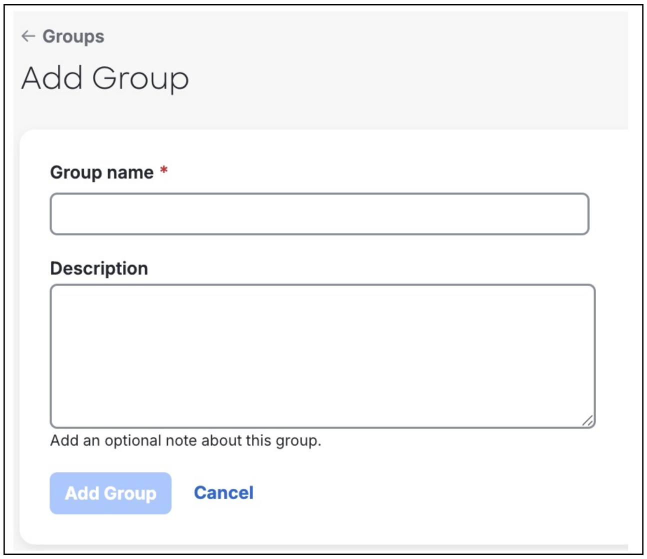
You can use groups to organize and manage users in Duo.

In this example, we create a group, and associate it with the Firewall Management Center application, and configure it such that only users who are members of the group can get authenticated in Firewall Management Center.

Procedure

Step 1 From the Duo Admin panel, choose **Users** > **Groups**.

Step 2 Click **+Add group**.



Add Group

Group name *

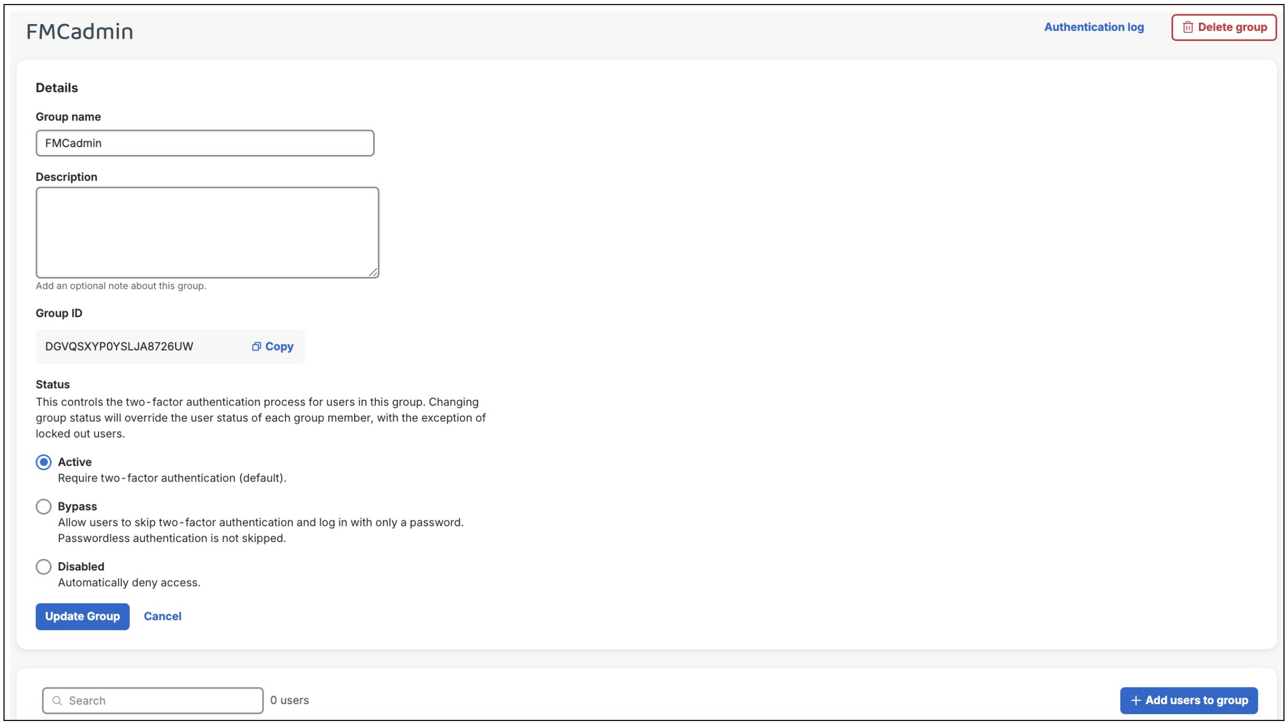
Description

Add an optional note about this group.

Step 3 In the **Group name** field, enter the group name.

Step 4 Click **Add Group**.

The group gets created and you enter the edit mode for the group.



FMCadmin

Details

Group name: FMCadmin

Description

Add an optional note about this group.

Group ID: DGVQSXYP0YSLJA8726UW

Status

This controls the two-factor authentication process for users in this group. Changing group status will override the user status of each group member, with the exception of locked out users.

● Active
Require two-factor authentication (default).

○ Bypass
Allow users to skip two-factor authentication and log in with only a password. Passwordless authentication is not skipped.

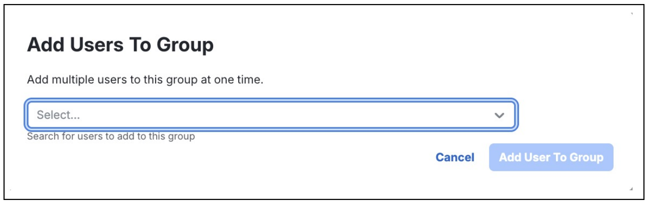
○ Disabled
Automatically deny access.

0 users

Step 5 In **Status**, click **Active** to require two-factor authentication for all users in the group.

Step 6 Click **+Add users to group**.

Step 7 In the **Add Users To Group** dialog box, choose one or more users from the drop-down list.



Add Users To Group

Add multiple users to this group at one time.

Select...

Search for users to add to this group

Step 8 Click **Add User To Group**.

The groups are listed in the **Groups** page. In our example, the groups are:

- FMCadmin
- FMCmaintenance
- FMCreadonly

Create a Policy

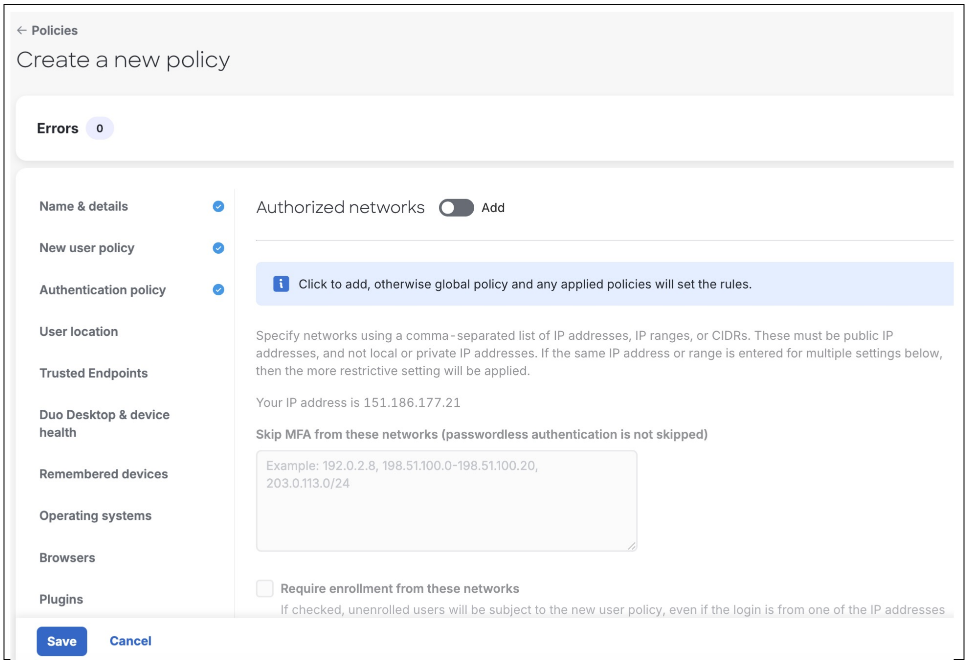
You can create policies and assign them to groups to control how your users get authenticated.

Procedure

Step 1 From the Duo Admin panel, choose **Policies** > **Policies**.

Step 2 Click **+Add Policy**.

The **Create a new policy** dialog box is displayed with rules in the left pane.



← Policies

Create a new policy

Errors 0

Authorized networks Add

Click to add, otherwise global policy and any applied policies will set the rules.

Specify networks using a comma-separated list of IP addresses, IP ranges, or CIDRs. These must be public IP addresses, and not local or private IP addresses. If the same IP address or range is entered for multiple settings below, then the more restrictive setting will be applied.

Your IP address is 151.186.177.21

Skip MFA from these networks (passwordless authentication is not skipped)

Example: 192.0.2.8, 198.51.100.0-198.51.100.20, 203.0.113.0/24

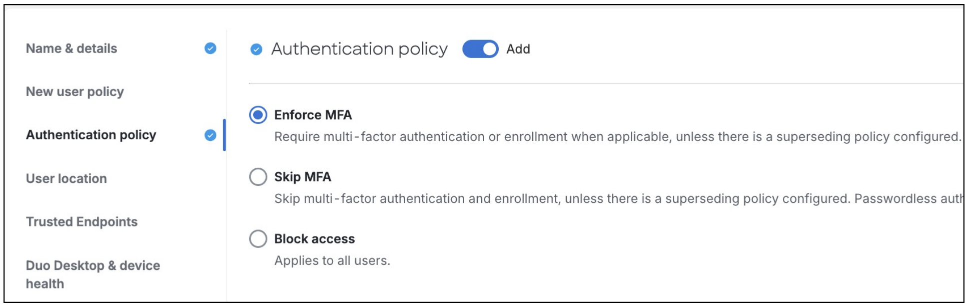
□ Require enrollment from these networks

If checked, unenrolled users will be subject to the new user policy, even if the login is from one of the IP addresses

Step 3 Choose the required rules from the left pane. The parameters corresponding to these rules are displayed on the right pane.

Step 4 Configure rules to enable your company's user authentication requirements.

By selecting **Enforce MFA**, the **Authentication policy** in this example requires all users to use MFA.



Authentication policy Add

● Enforce MFA
Require multi-factor authentication or enrollment when applicable, unless there is a superseding policy configured.

○ Skip MFA
Skip multi-factor authentication and enrollment, unless there is a superseding policy configured. Passwordless auth

○ Block access
Applies to all users.

Step 5 Click **Save**.

Create a Firewall Management Center Application in Duo

To enable SAML SSO for Firewall Management Center with Duo, create a Firewall Management Center application in Duo.

Procedure

Step 1 From the Duo Admin panel, choose **Applications** > **Applications**.

Step 2 Click **+ Add application**.

Step 3 Search for **Generic SAML Service Provider in the Application Catalog** in the search bar.

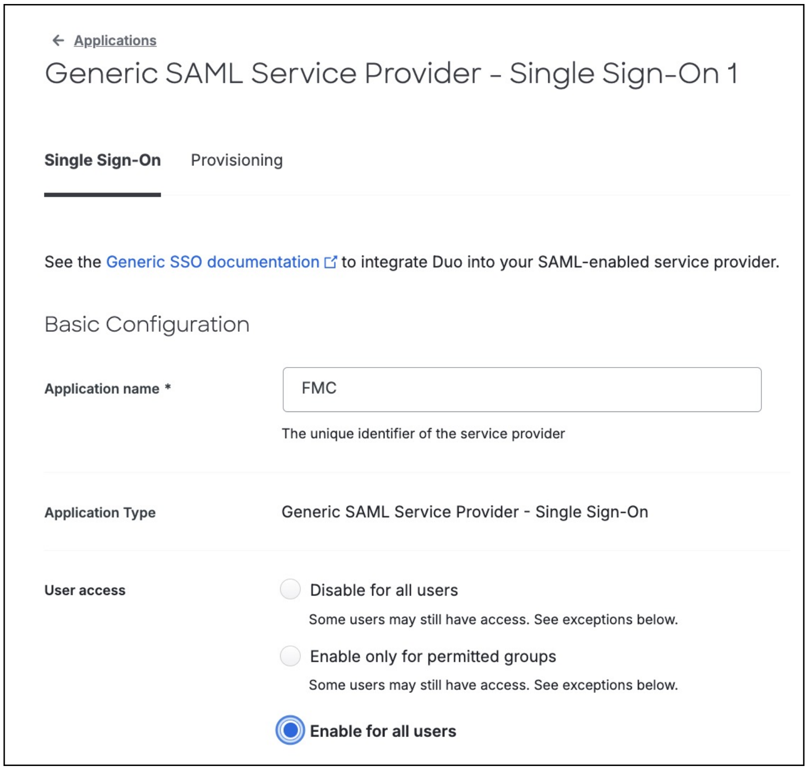
Step 4 Click **+ Add**.

Step 5 Click the **Single Sign-On** tab.

Step 6 In the **Application name** field, enter a name of the application.

Step 7 In **User access**, click the **Enable for all users** or the **Enable only for permitted groups** radio button.

Note
By default, all users are disabled. Ensure that you enable permitted groups or all users.



Generic SAML Service Provider - Single Sign-On 1

See the Generic SSO documentation to integrate Duo into your SAML-enabled service provider.

Basic Configuration

Application name *: FMC

The unique identifier of the service provider

Application Type: Generic SAML Service Provider - Single Sign-On

User access:

○ Disable for all users

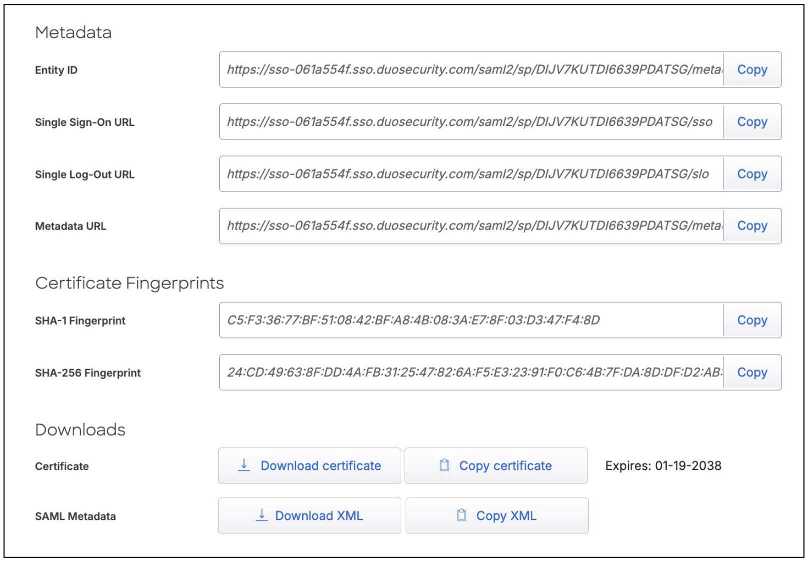
Some users may still have access. See exceptions below.

○ Enable only for permitted groups

Some users may still have access. See exceptions below.

● Enable for all users

Step 8 In **Metadata**, the **Entity ID**, **Single-Sign-On URL**, and **Metadata URL** fields are auto-populated.



Metadata

Entity ID	https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIJV7KUTDI6639PDATSG/meta
Single Sign-On URL	https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIJV7KUTDI6639PDATSG/sso
Single Log-Out URL	https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIJV7KUTDI6639PDATSG/slo
Metadata URL	https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIJV7KUTDI6639PDATSG/meta

Certificate Fingerprints

SHA-1 Fingerprint	C5:F3:36:77:BF:51:08:42:BF:A8:4B:08:3A:E7:8F:03:D3:47:F4:8D
SHA-256 Fingerprint	24:CD:49:63:8F:DD:4A:FB:31:25:47:82:6A:F5:E3:23:91:F0:C6:4B:7F:DA:8D:DF:D2:AB:

Downloads

Certificate — Expires: 01-19-2038

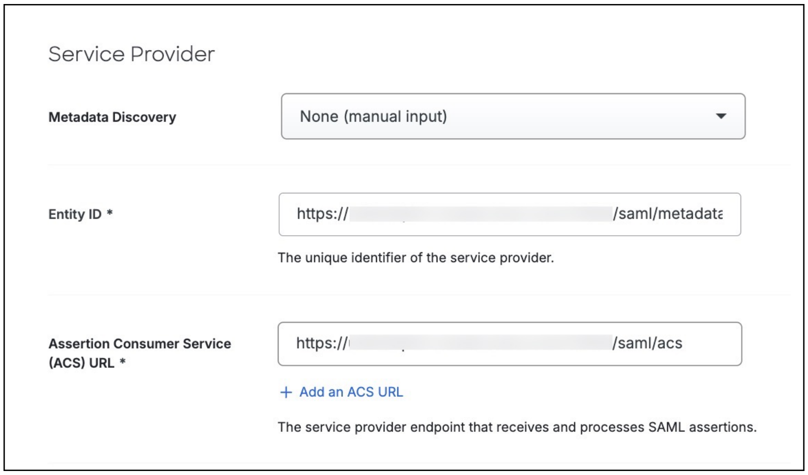
SAML Metadata

Step 9 Click **Download XML** to download this metadata information.

You need to upload this XML to configure Duo metadata in Step 5 in Configure Firewall Management Center for Duo SSO, on page 12.

Step 10 In the **Entity ID** field, enter the FQDN or IP address of the Firewall Management Center and append the `/saml/metadata` string, for example, https://*xxxxxxxxx-xxxxxxx.xxxxx*.com/saml/metadata.

Step 11 In the **Assertion Consumer Service (ACS) URL** field, enter the FQDN or IP address of the Firewall Management Center and append the `/saml/acs` string, for example, https://*xxxxxxxxx-xxxxxxx.xxxxx*.com/saml/acs.



Service Provider

Metadata Discovery: None (manual input)

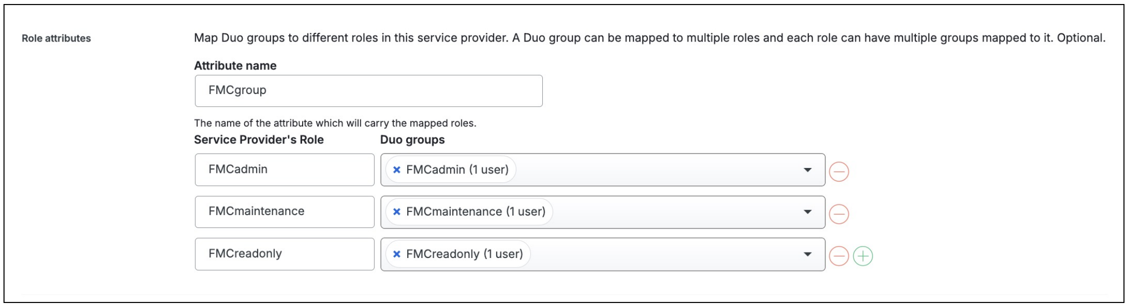
Entity ID *: https://[redacted]/saml/metadat

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL *: https://[redacted]/saml/acs

The service provider endpoint that receives and processes SAML assertions.

Step 12 Configure **Role attributes**.



Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional.

Attribute name: FMCgroup

The name of the attribute which will carry the mapped roles.

Service Provider's Role	Duo groups
FMCadmin	× FMCadmin (1 user)
FMCmaintenance	× FMCmaintenance (1 user)
FMCreadonly	× FMCreadonly (1 user)

a) In the **Attribute name** field, enter an attribute name.

In this example, the **Attribute name** is **FMCgroup**. In Firewall Management Center, you must use this value as the **Group Member Attribute** value (Step 10 in Configure Firewall Management Center for Duo SSO, on page 12).

b) In the **Service Provider's Role** field, enter the Firewall Management Center role.

In this example, the configured roles are **FMCadmin**, **FMCmaintenance**, and **FMCreadonly**.

c) From the **Duo groups** drop-down list, choose the Duo group corresponding to the Firewall Management Center role.

Step 13 In **Policy**, click **Apply a policy to group of users**.

Step 14 Click **Save**.

Configure Firewall Management Center for Duo SSO

Enable SSO on Firewall Management Center and configure the SSO parameters and user role mapping.

Before you begin

Create a Firewall Management Center service provider application in the Duo Admin panel. For more information, see Create a Firewall Management Center Application in Duo, on page 10.

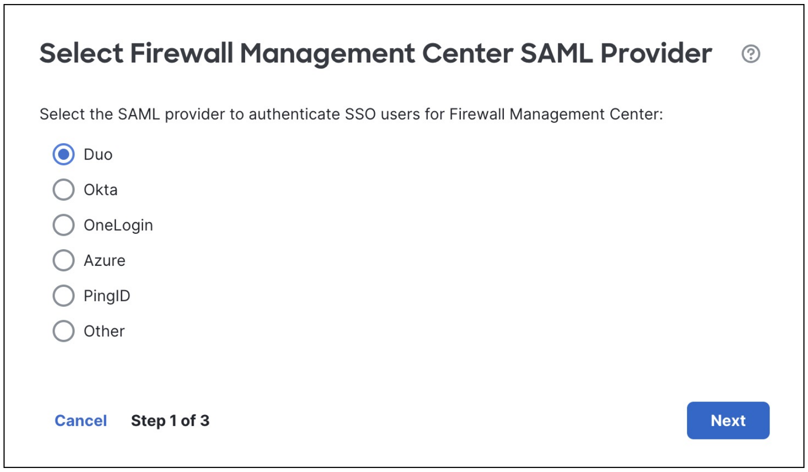
Procedure

Step 1 From Firewall Management Center, choose **Administration** > **Users** > **Single Sign-On**.

Step 2 Click the **Single Sign-On (SSO) Configuration** toggle button to enable SSO.

Step 3 Click **Configure SSO**.

Step 4 In the **Select Firewall Management Center SAML Provider** dialog box, click the **Duo** radio button and click **Next**.



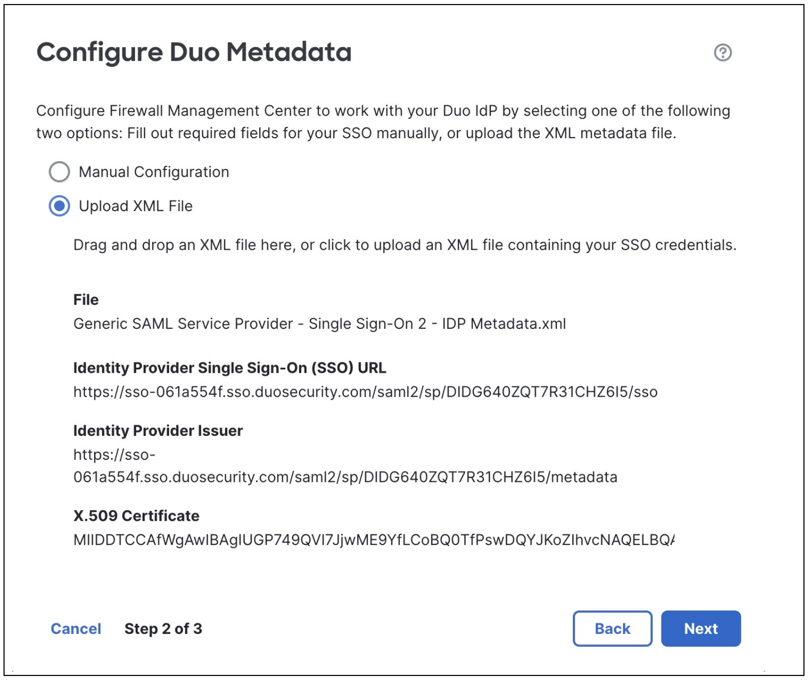
Select Firewall Management Center SAML Provider

Select the SAML provider to authenticate SSO users for Firewall Management Center:

● Duo
○ Okta
○ OneLogin
○ Azure
○ PingID
○ Other

Step 5 In the **Configure Duo Metadata** dialog box, click the **Upload XML File** radio button to upload the metadata file for Duo.

This XML file is the metadata XML file that you downloaded from Duo in Step 9 in Create a Firewall Management Center Application in Duo, on page 10. After you upload the XML file, the metadata gets auto-populated in the **Configure Duo Metadata** dialog box.



Configure Duo Metadata

Configure Firewall Management Center to work with your Duo IdP by selecting one of the following two options: Fill out required fields for your SSO manually, or upload the XML metadata file.

○ Manual Configuration

● Upload XML File

Drag and drop an XML file here, or click to upload an XML file containing your SSO credentials.

File
Generic SAML Service Provider - Single Sign-On 2 - IDP Metadata.xml

Identity Provider Single Sign-On (SSO) URL
https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIDG640ZQT7R31CHZ6I5/sso

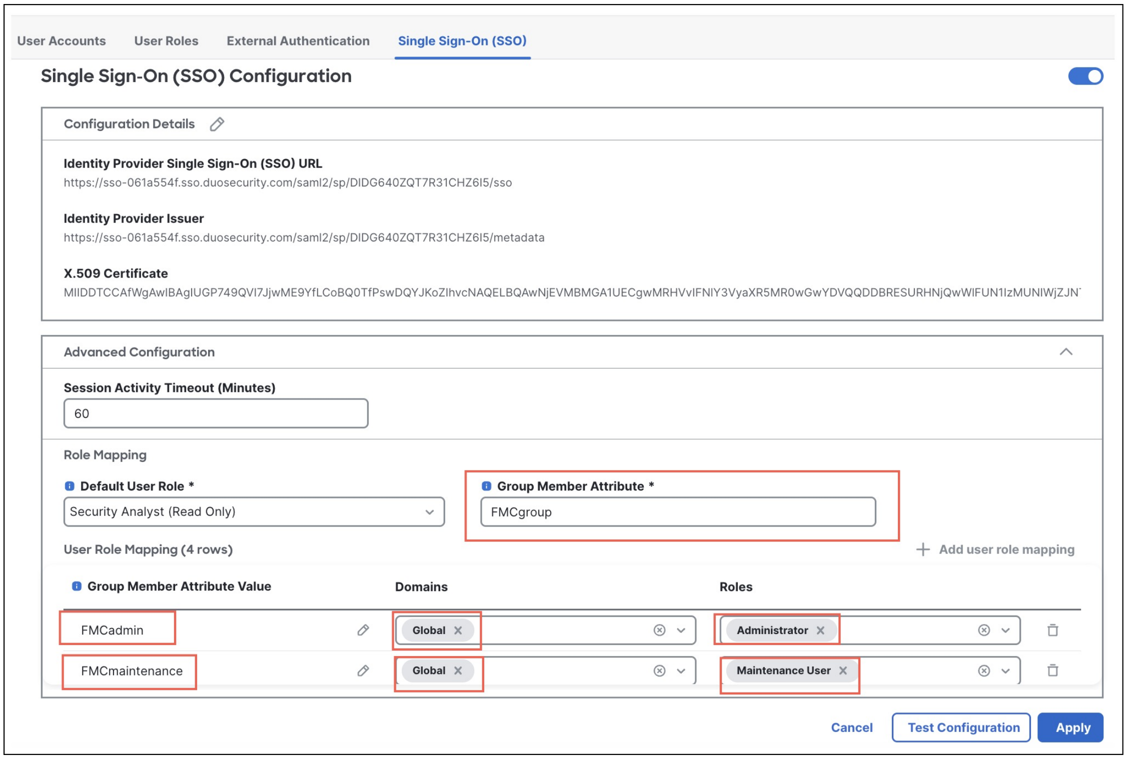
Identity Provider Issuer
https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIDG640ZQT7R31CHZ6I5/metadata

X.509 Certificate
MIIDDTCCAfWgAwIBAgIUGP749QVI7JjwME9YfLCoBQ0TfPswDQYJKoZIhvcNAQELBQ/

Step 6 Click **Next**.

Step 7 Verify the Duo metadata and click **Save**.

Step 8 Expand **Advanced Configuration**.



Single Sign-On (SSO) Configuration

Configuration Details

Identity Provider Single Sign-On (SSO) URL
https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIDG640ZQT7R31CHZ6I5/sso

Identity Provider Issuer
https://sso-061a554f.sso.duosecurity.com/saml2/sp/DIDG640ZQT7R31CHZ6I5/metadata

X.509 Certificate
MIIDDTCCAfWgAwIBAgIUGP749QVI7JjwME9YfLCoBQ0TfPswDQYJKoZIhvcNAQELBQAwNjEVMBMGA1UECgwMRHVvIFNIY3VyaXR5MR0wGwYDVQQDDBRESURHNjQwWIFUN1IzMUNIWjZJN

Advanced Configuration

Session Activity Timeout (Minutes): 60

Role Mapping

Default User Role *: Security Analyst (Read Only)

Group Member Attribute *: FMCgroup

User Role Mapping (4 rows)

Group Member Attribute Value	Domains	Roles
FMCadmin	Global	Administrator
FMCmaintenance	Global	Maintenance User

Step 9 From the **Default User Role** drop-down list, choose a default Firewall Management Center user role to be assigned if there are no other roles configured.

Step 10 In the **Group Member Attribute** field, enter the **Attribute name** configured in Duo for Firewall Management Center role mapping of users or groups (Step 12a in Create a Firewall Management Center Application in Duo, on page 10).

In this example, the group member attribute is **FMCgroup**.

Step 11 Configure one or more user role mappings and associate them to one or more domains:

a) For **Group Member Attribute Value**, click the edit icon and enter the attribute value as a string or a regular expression that matches the attribute value defined in Duo.

b) Click **+ Add user role mapping** to create a new group.

In this example, the group member attribute values are **FMCadmin**, **FMCmaintenance**, and **FMCreadonly**.

c) From the **Domains** drop-down list, choose one or more domains.

In this example, the domain for all the group member attribute values is **Global**.

d) From the **Roles** drop-down list, choose one or more user roles.

The Firewall Management Center compares the attribute value against the user role mapping attribute value that Duo sends to the Firewall Management Center with SSO user information. When a match is found, the Firewall Management Center grants the corresponding role to the user along with access to the configured domains.

In this example, the assigned roles for **FMCadmin**, **FMCmaintenance**, and **FMCreadonly** group member attribute values are **Administrator**, **Maintenance User**, and **Security Analyst** respectively.

e) (Optional) Click **Add user role mapping** to add more user role mappings.

f) Click **Test Configuration**.

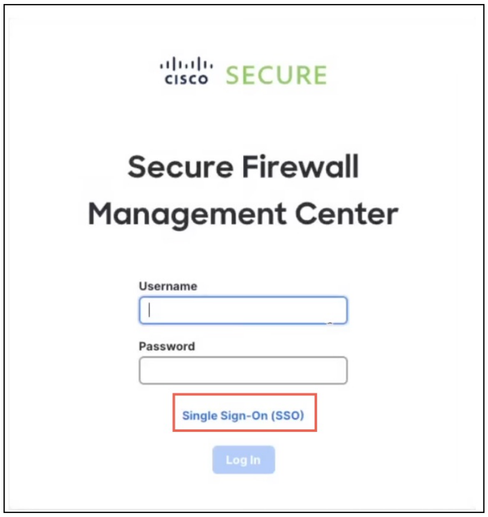
Note
If the system displays an error message, review the SSO configuration for the Firewall Management Center as well as the Duo application configuration. Correct any errors, and try again. If errors persist, contact Cisco Technical Assistance Center.

g) When the system reports a successful configuration test, click **Apply**.

Validate SAML SSO in Firewall Management Center Using Duo

Log in to Firewall Management Center using SSO

1. Click the **Single Sign-On (SSO)** link in the login page of the Firewall Management Center web interface.



2. Enter your email address in Duo Security for two-factor authentication.
3. Click **Next** to get the push notification on your Duo mobile application in your mobile device.
4. Log in to the Firewall Management Center web interface after the two-factor authentication.

Your Firewall Management Center role and domain depends on the user role mapping in Duo. Each Firewall Management Center role is mapped to a group in Duo.

View users in Firewall Management Center

As an administrator, you can verify the users who have logged in to Firewall Management Center using SSO.

1. Log in to the Firewall Management Center with your admin credentials.
2. Choose **Administration** > **Users** > **User Accounts**.

View audit logs in Firewall Management Center to monitor user activity

Firewall Management Center logs audit information about user activity as audit logs. To view these logs, choose **Events & Logs** > **Analysis** > **Audit Logs**.

Troubleshoot SAML SSO in Firewall Management Center

- **Symptom**: User is unable to log in to Firewall Management Center.

  Resolution: Verify the connectivity between Firewall Management Center and Duo.

- **Symptom**: User is unable to log in to the correct domain in Firewall Management Center.

  Resolution: Verify the user role mapping in Firewall Management Center and Duo.

- **Symptom**: `Server Error` message is displayed in the Firewall Management Center **Single Sign-On (SSO)** page.

  Resolution: Verify the connectivity between Firewall Management Center and Duo. If problem persists, contact Cisco TAC.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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