Configure Secure Firewall Management Center Access with Duo SSO

Contents

Introduction

This document describes how to configure the Secure Firewall Management Center (FMC) to authenticate via Single Sign-On (SSO) for management access.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:
â€¢ Basic understanding of Single Sign-On and SAML
â€¢ Understanding of the configuration on the Identity Provider (iDP)

Components Used

The information in this document is based on these software versions:
â€¢ Cisco Secure Firewall Management Center (FMC) version 7.2.4
â€¢ Duo as the Identity Provider

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

These iDPs are supported and are tested for authentication:
â€¢ Okta
â€¢ OneLogin
â€¢ PingID
â€¢ Azure AD
â€¢ Others (Any iDP that conforms to SAML 2.0)

Note: No new license requirement. This feature works in licensed as well as evaluation mode.

Limitations and Restrictions

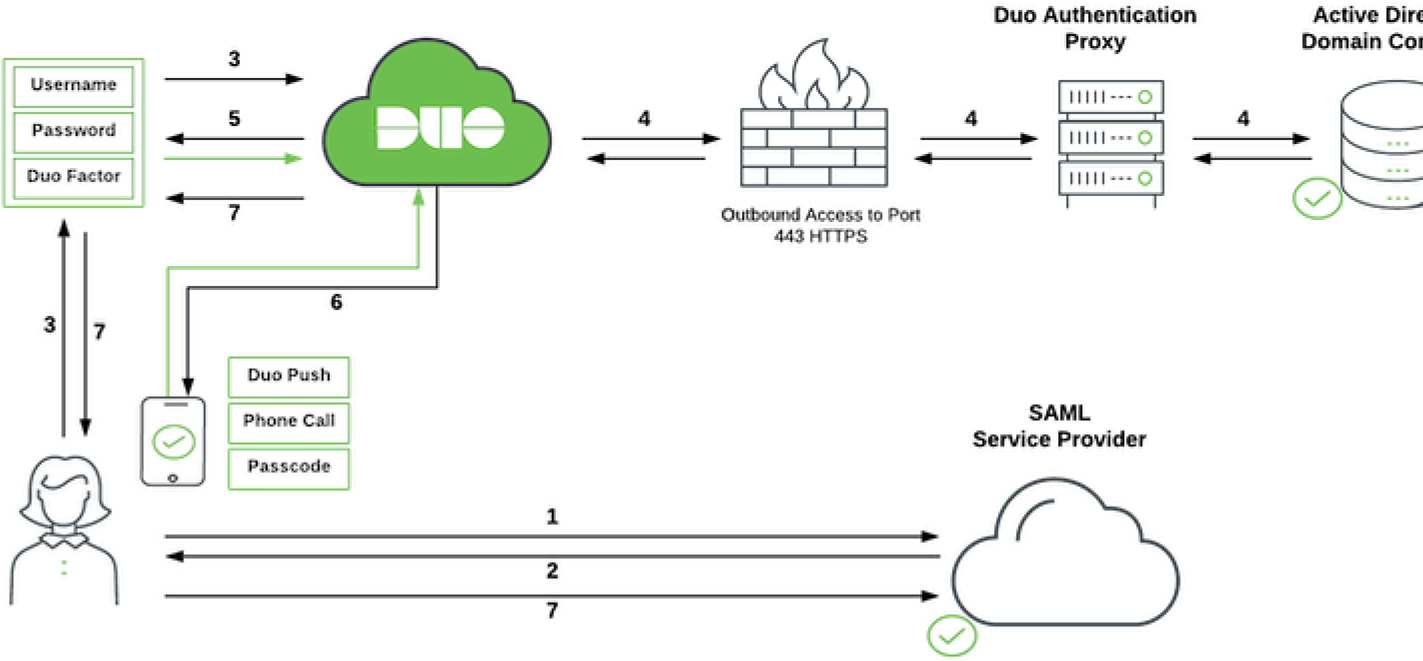
These are known limitations and restrictions for SSO authentication for FMC access:

â€¢ SSO can be configured only for the Global Domain.

â€¢ FMC devices participating in HA Pair requires individual configuration.

â€¢ Only Local/AD admins can configure SSO on FMC (SSO admin users are unable to configure/update SSO settings on FMC).

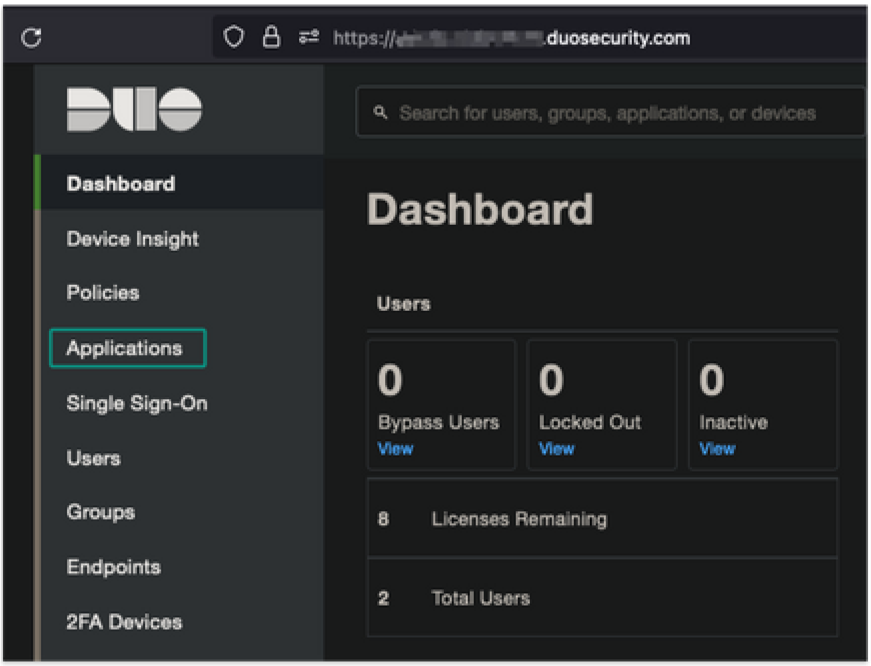
Network Diagram



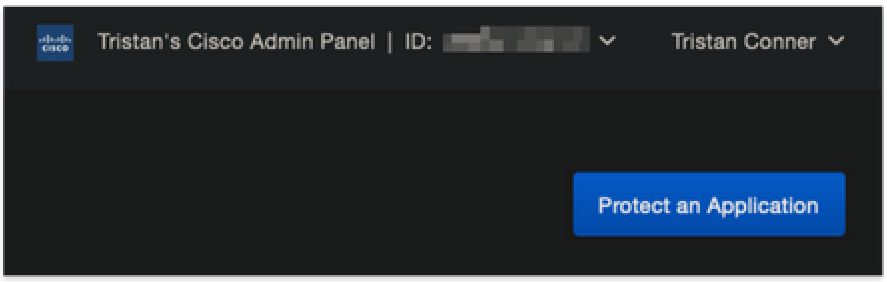
Configuration Steps on the Identity Provider (Duo)

From the Dashboard, navigate to **Applications**:

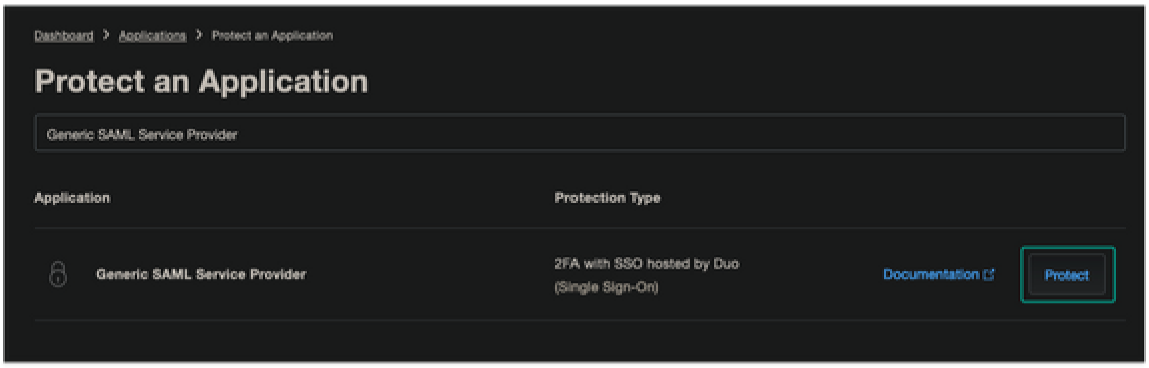
Example url: https://admin-debXXXXX.duosecurity.com/applications



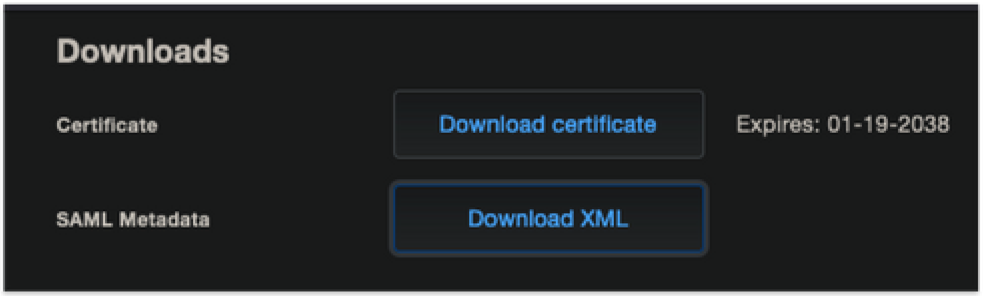
Select **Protect an Application**.



Search for **Generic SAML Service Provider**.

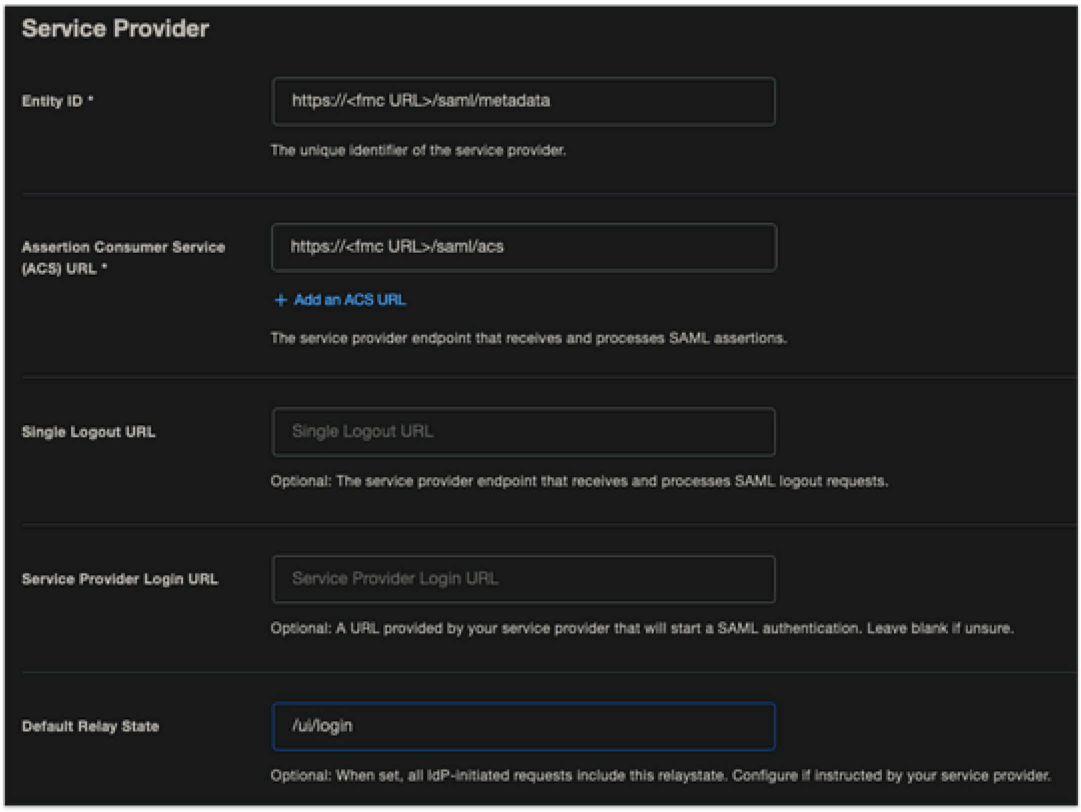

Dashboard > Applications > Protect an Application
Protect an Application
Generic SAML Service Provider
Application
Protection Type
Generic SAML Service Provider
2FA with SSO hosted by Duo (Single Sign-On)
Documentation
Protect

Download Certificate and XML.



Configure Service Provider.

Enter the SAML Settings:
Single sign on URL: https://<fmc URL>/saml/acs
Audience URI (SP Entity ID): https://<fmc URL>/saml/metadata
Default RelayState: /ui/login



Service Provider

Entity ID * https://<fmc URL>/saml/metadata

The unique identifier of the service provider.

Assertion Consumer Service (ACS) URL * https://<fmc URL>/saml/acs

The service provider endpoint that receives and processes SAML assertions.

Single Logout URL: Single Logout URL

Optional: The service provider endpoint that receives and processes SAML logout requests.

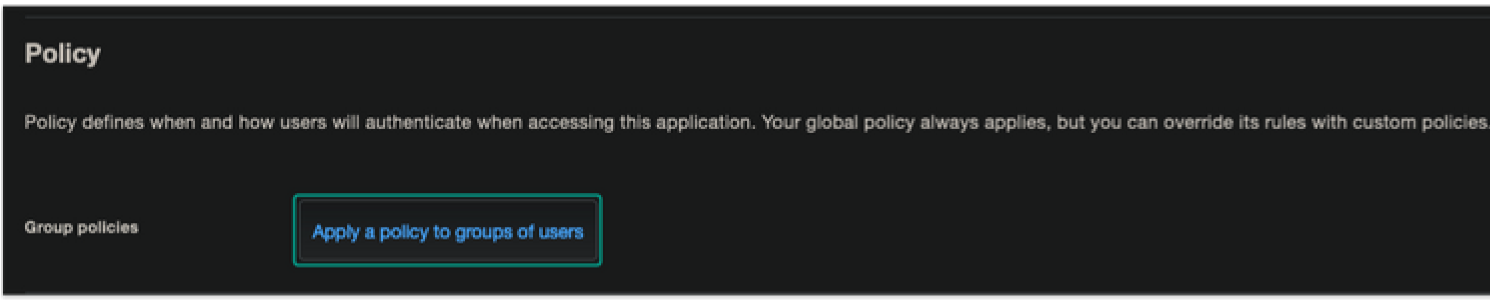
Service Provider Login URL: Service Provider Login URL

Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.

Default Relay State /ui/login

Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.

Configure **Apply Policy to All Users**.



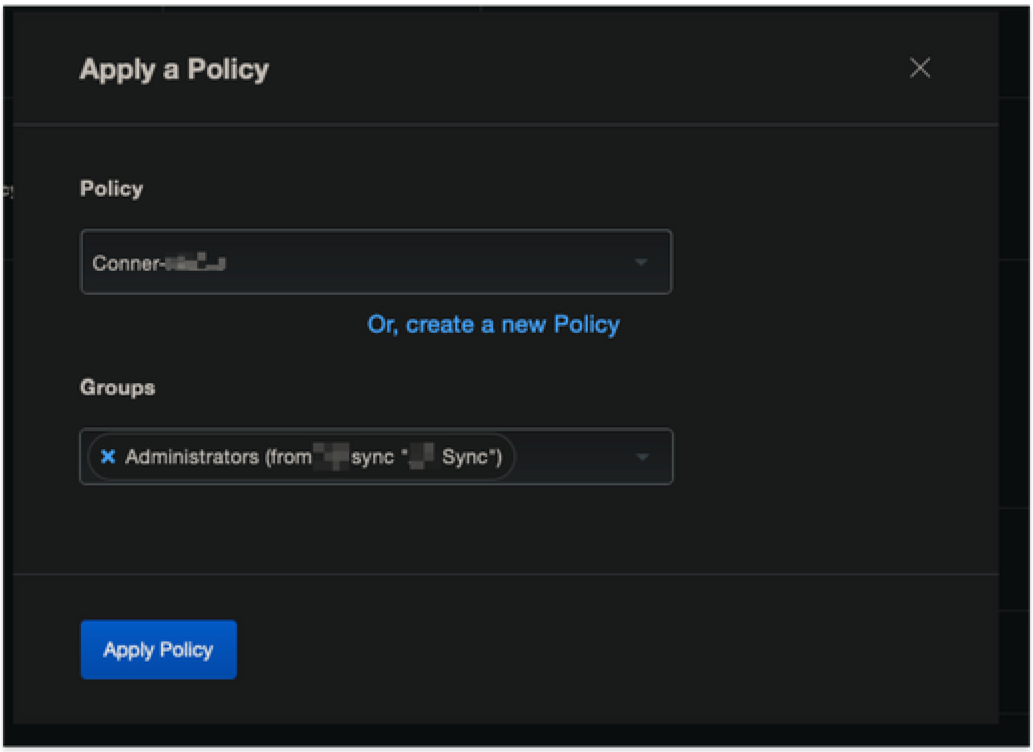
Policy

Policy defines when and how users will authenticate when accessing this application. Your global policy always applies, but you can override its rules with custom policies.

Group policies

Detailed **Apply a Policy**.

Choose necessary administrator group from the appropriate Custom Policy.



Apply a Policy

Policy

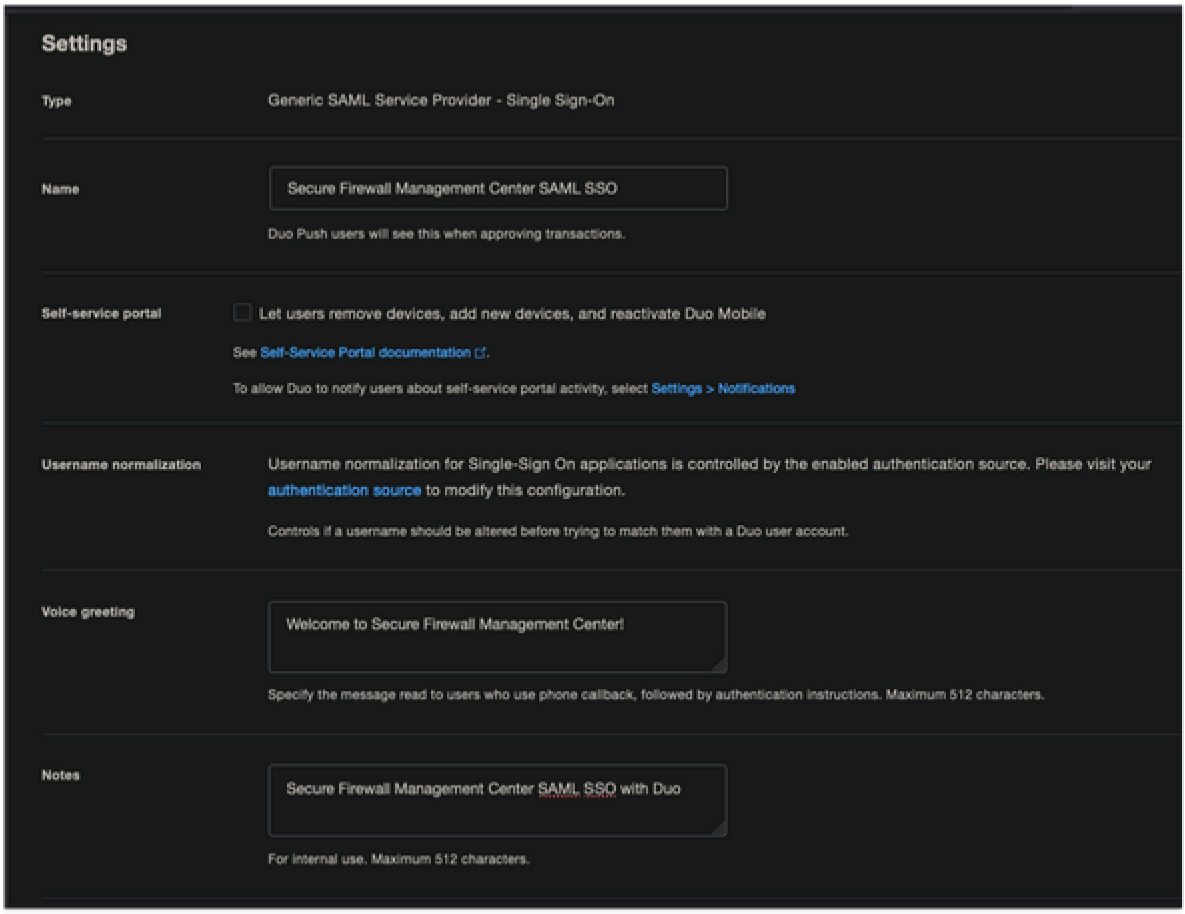
Conner-[redacted]

Or, create a new Policy

Groups

× Administrators (from [redacted] sync "[redacted] Sync")

Configure necessary administrative settings.



Settings

Type: Generic SAML Service Provider - Single Sign-On

Name: Secure Firewall Management Center SAML SSO

Duo Push users will see this when approving transactions.

Self-service portal: □ Let users remove devices, add new devices, and reactivate Duo Mobile

See Self-Service Portal documentation.

To allow Duo to notify users about self-service portal activity, select Settings > Notifications

Username normalization: Username normalization for Single-Sign On applications is controlled by the enabled authentication source. Please visit your authentication source to modify this configuration.

Controls if a username should be altered before trying to match them with a Duo user account.

Voice greeting: Welcome to Secure Firewall Management Center!

Specify the message read to users who use phone callback, followed by authentication instructions. Maximum 512 characters.

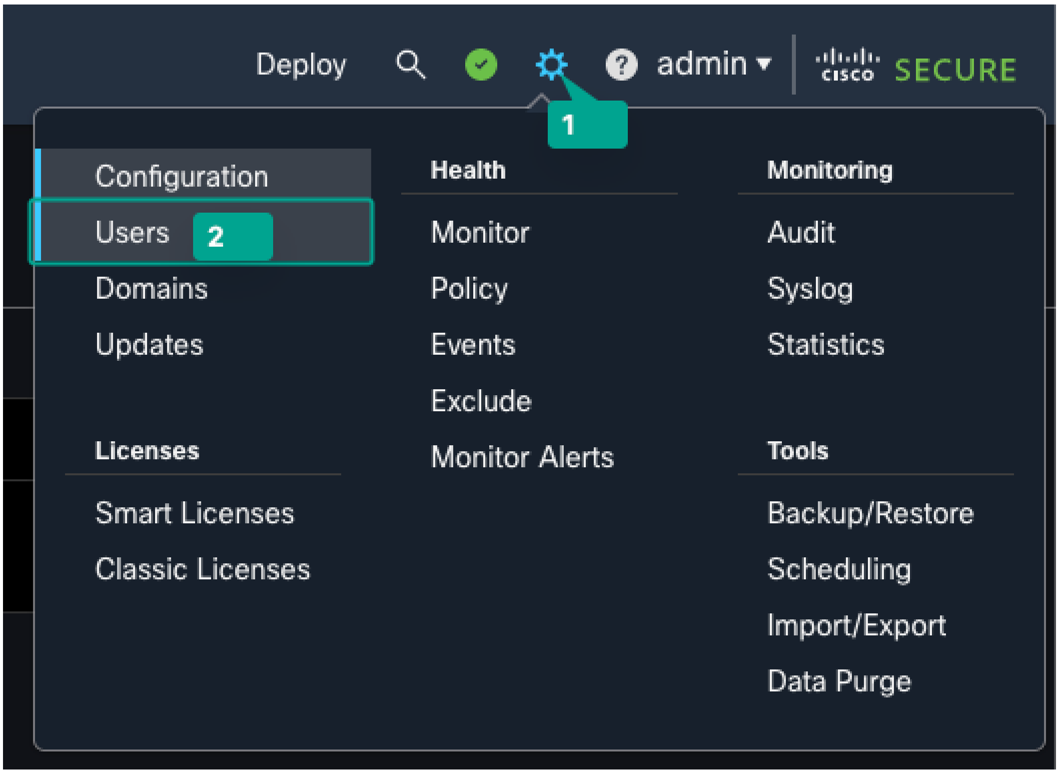
Notes: Secure Firewall Management Center SAML SSO with Duo

For internal use. Maximum 512 characters.

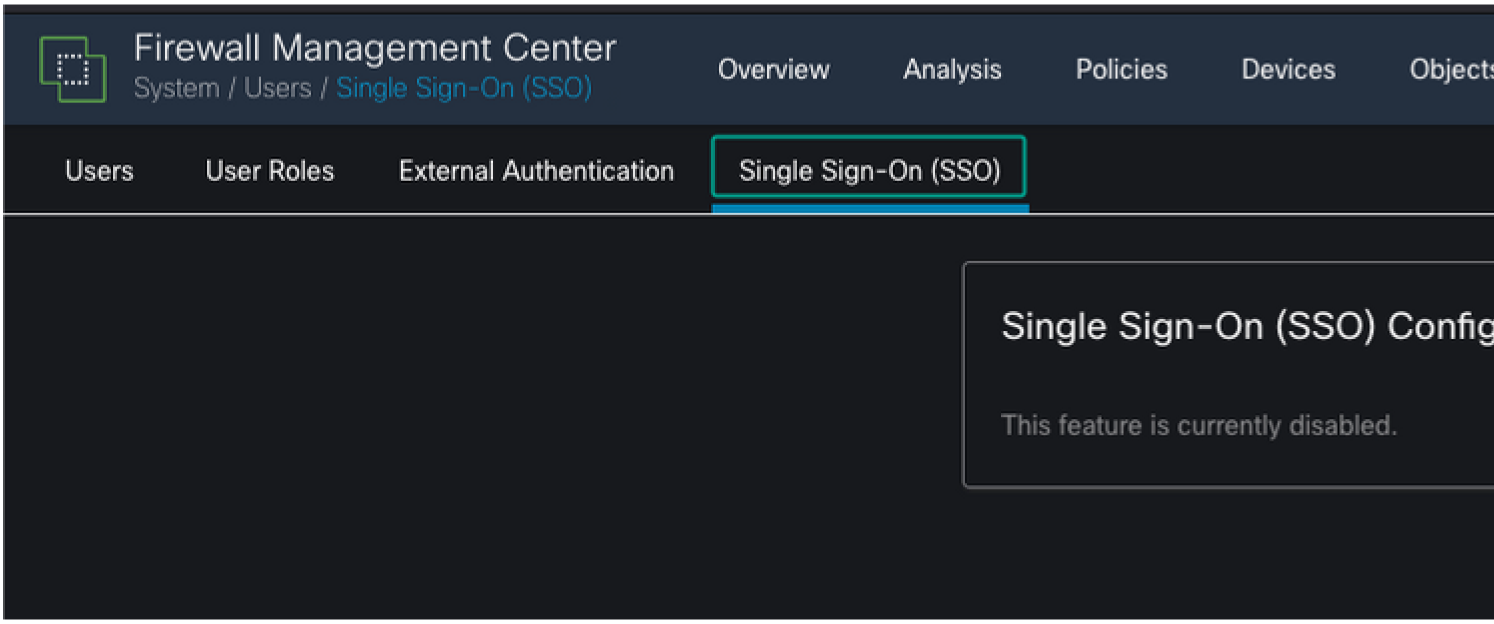
Save Application.

Configuration Steps on Secure Firewall Management Center

Log in to the FMC with Admin privileges. Navigate to **System** > **Users**.

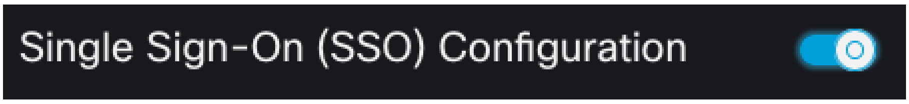


Click Single Sign-On, as shown in this image.



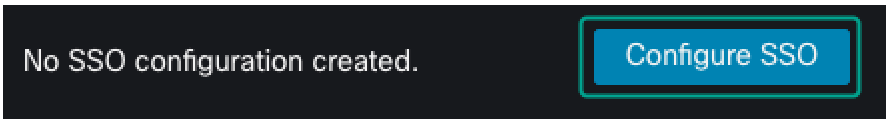
This feature is currently disabled.

Enable the Single Sign-On option (Disabled by default).



Single Sign-On (SSO) Configuration

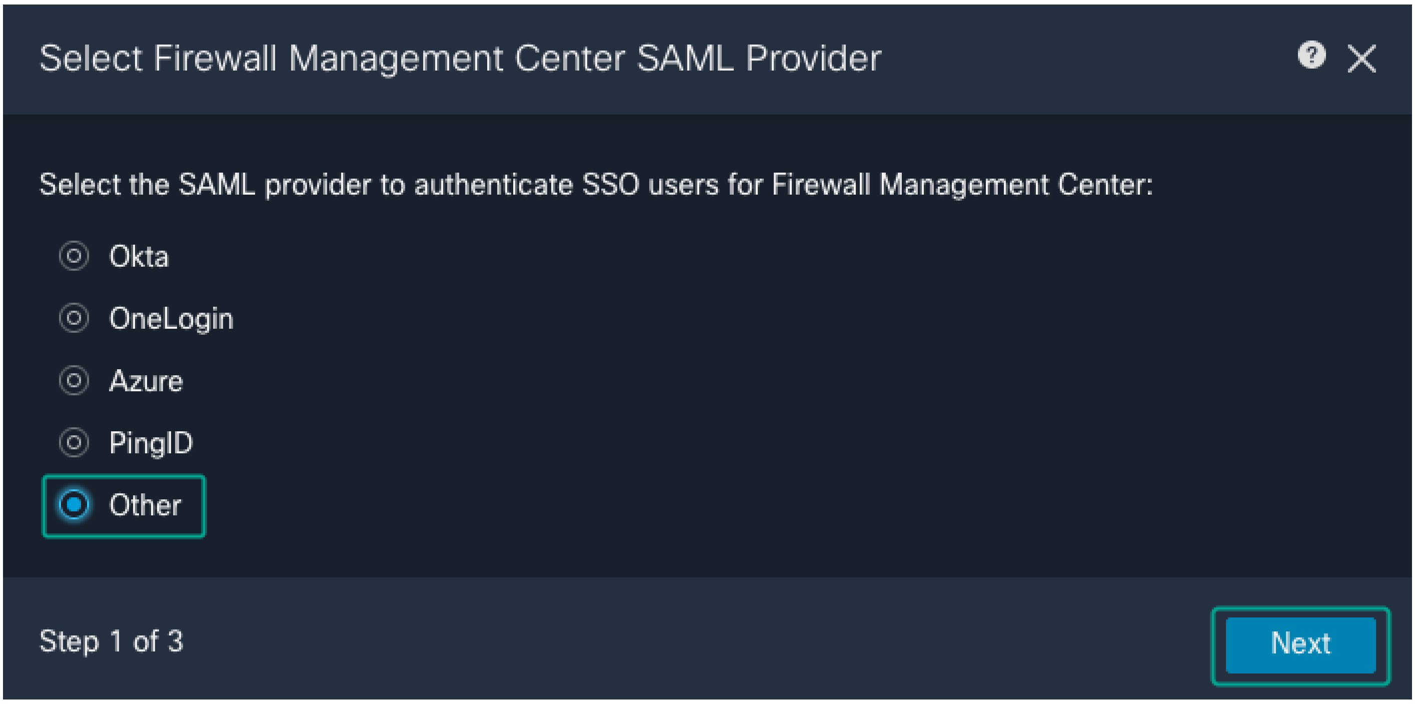
Click **Configure SSO** to begin SSO configuration on FMC.



No SSO configuration created.

Select the Firewall Management Center SAML Provider. Click **Next**.

For the purpose of this demonstration, Other is used.



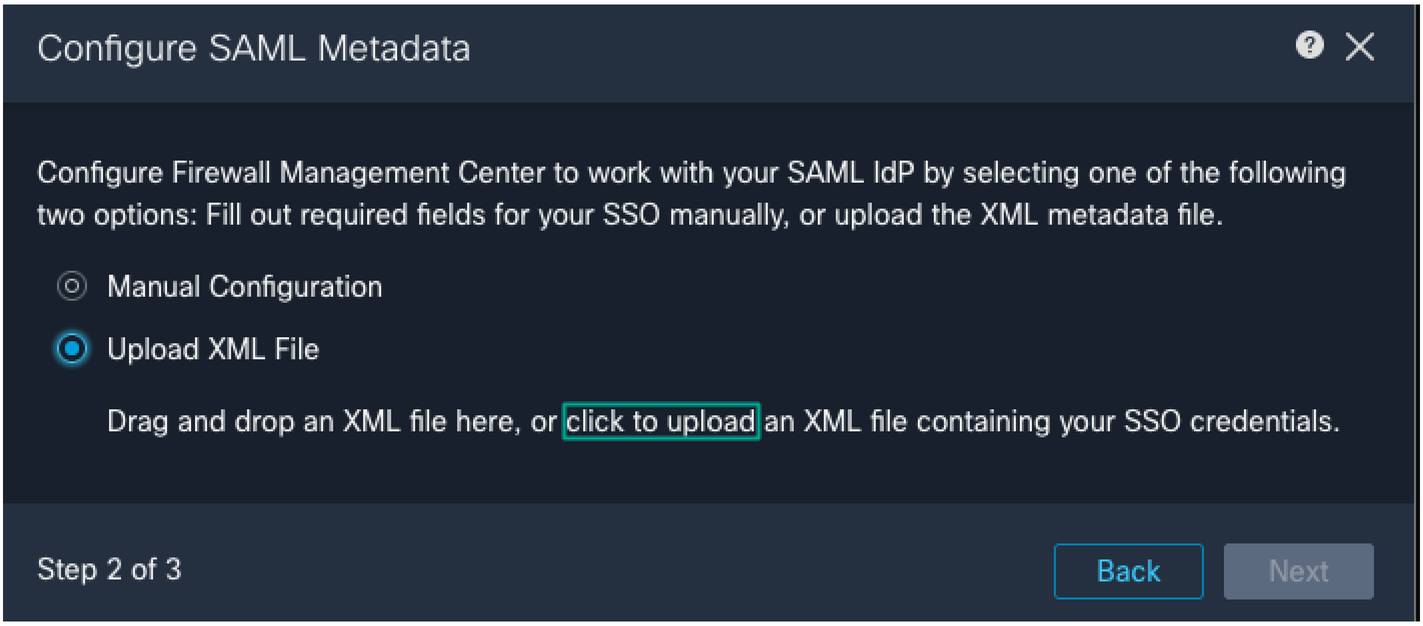
Select Firewall Management Center SAML Provider

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

- ○ Okta
- ○ OneLogin
- ○ Azure
- ○ PingID
- ● Other

Step 1 of 3

You can also choose Upload XML file and upload the XML file retrieved earlier from Duo Configuration.



Configure SAML Metadata

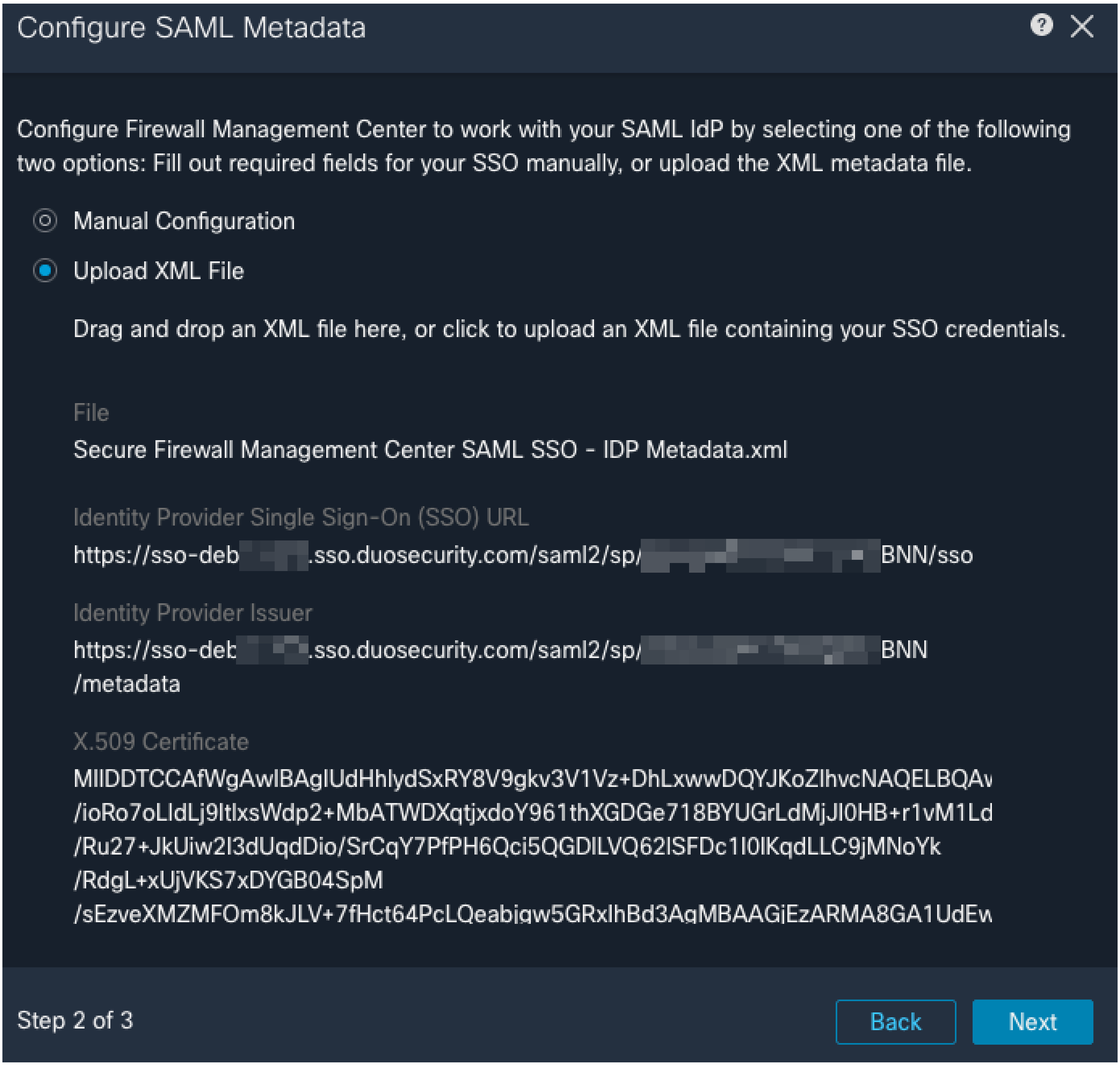
Configure Firewall Management Center to work with your SAML IdP by selecting one of the following two options: Fill out required fields for your SSO manually, or upload the XML metadata file.

○ Manual Configuration

● Upload XML File

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

Once the file is uploaded, the FMC displays the metadata. Click **Next**, as shown in this image.



Configure SAML Metadata

Configure Firewall Management Center to work with your SAML 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
Secure Firewall Management Center SAML SSO - IDP Metadata.xml

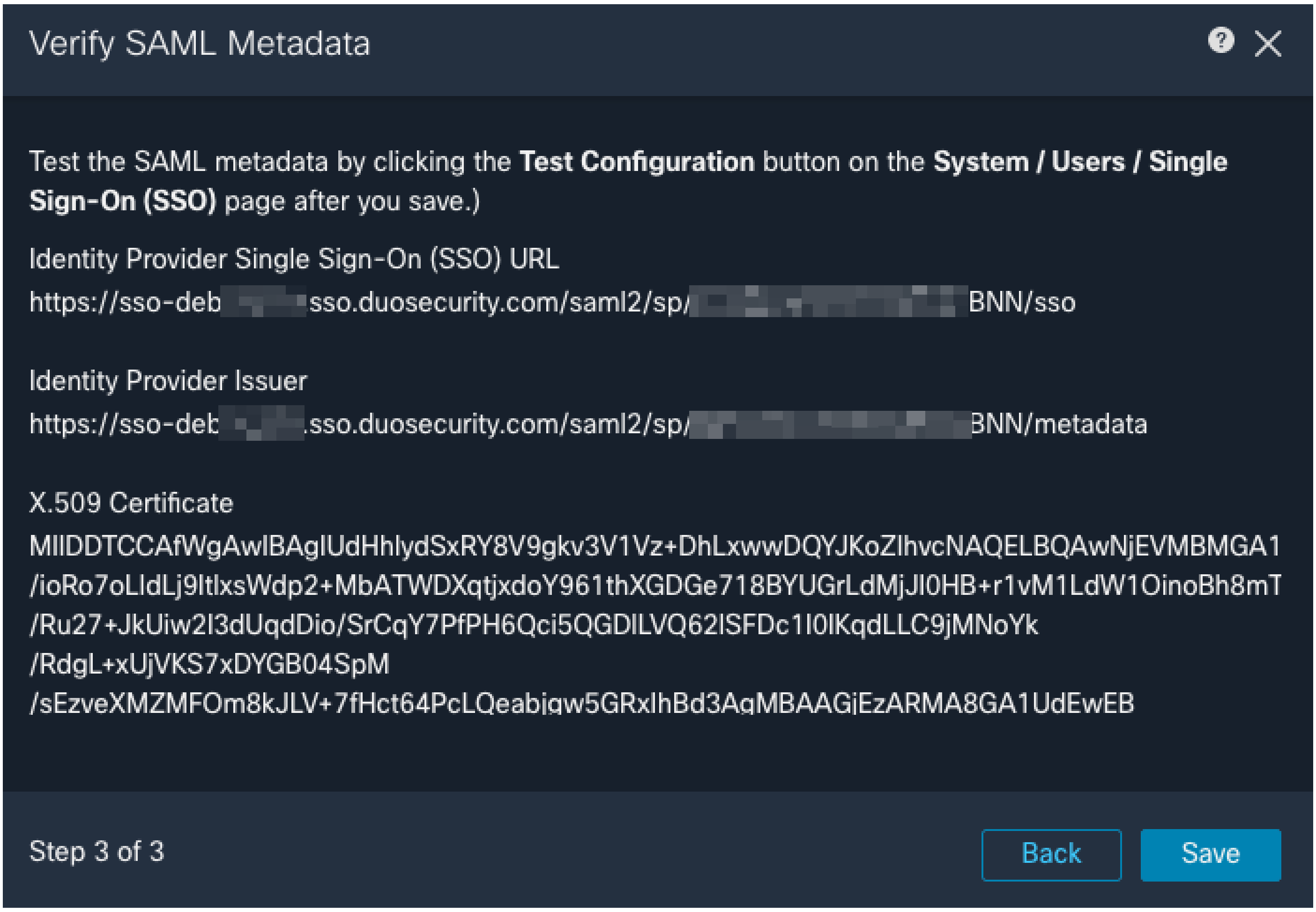
Identity Provider Single Sign-On (SSO) URL
https://sso-deb[redacted].sso.duosecurity.com/saml2/sp/[redacted]BNN/sso

Identity Provider Issuer
https://sso-deb[redacted].sso.duosecurity.com/saml2/sp/[redacted]BNN
/metadata

X.509 Certificate
MIIDDTCCAfWgAwIBAgIUdHhlydSxRY8V9gkv3V1Vz+DhLxwwDQYJKoZIhvcNAQELBQAw
/ioRo7oLldLj9ltlxsWdp2+MbATWDXqtjxdoY961thXGDGe718BYUGrLdMjJI0HB+r1vM1Ld
/Ru27+JkUiw2I3dUqdDio/SrCqY7PfPH6Qci5QGDILVQ62ISFDc1I0IKqdLLC9jMNoYk
/RdgL+xUjVKS7xDYGB04SpM
/sEzveXMZMFOm8kJLV+7fHct64PcLQeabjqw5GRxlhBd3AqMBAAGjEzARMA8GA1UdEw

Step 2 of 3

Verify the metadata. Click **Save**, as shown in this image.



Verify SAML Metadata

Test the SAML metadata by clicking the **Test Configuration** button on the **System / Users / Single Sign-On (SSO)** page after you save.)

Identity Provider Single Sign-On (SSO) URL
https://sso-deb[redacted]sso.duosecurity.com/saml2/sp/[redacted]BNN/sso

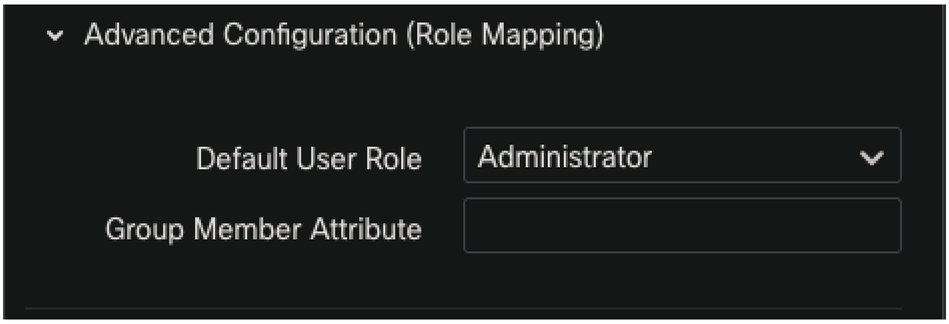
Identity Provider Issuer
https://sso-deb[redacted].sso.duosecurity.com/saml2/sp/[redacted]BNN/metadata

X.509 Certificate

MIIDDTCCAfWgAwIBAgIUdHhlydSxRY8V9gkv3V1Vz+DhLxwwDQYJKoZIhvcNAQELBQAwNjEVMBMGA1
/ioRo7oLIdLj9ItlxsWdp2+MbATWDXqtjxdoY961thXGDGe718BYUGrLdMjJI0HB+r1vM1LdW1OinoBh8mT
/Ru27+JkUiw2I3dUqdDio/SrCqY7PfPH6Qci5QGDILVQ62ISFDc1I0IKqdLLC9jMNoYk
/RdgL+xUjVKS7xDYGB04SpM
/sEzveXMZMFOm8kJLV+7fHct64PcLQeabjqw5GRxlhBd3AqMBAAGjEzARMA8GA1UdEwEB

Step 3 of 3

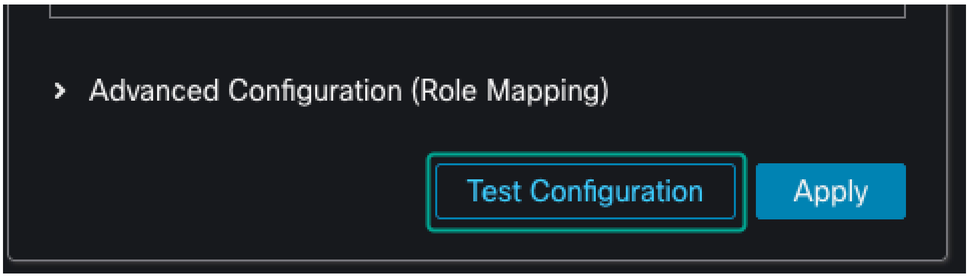
Configure the Role Mapping/Default User Role under Advanced Configuration.



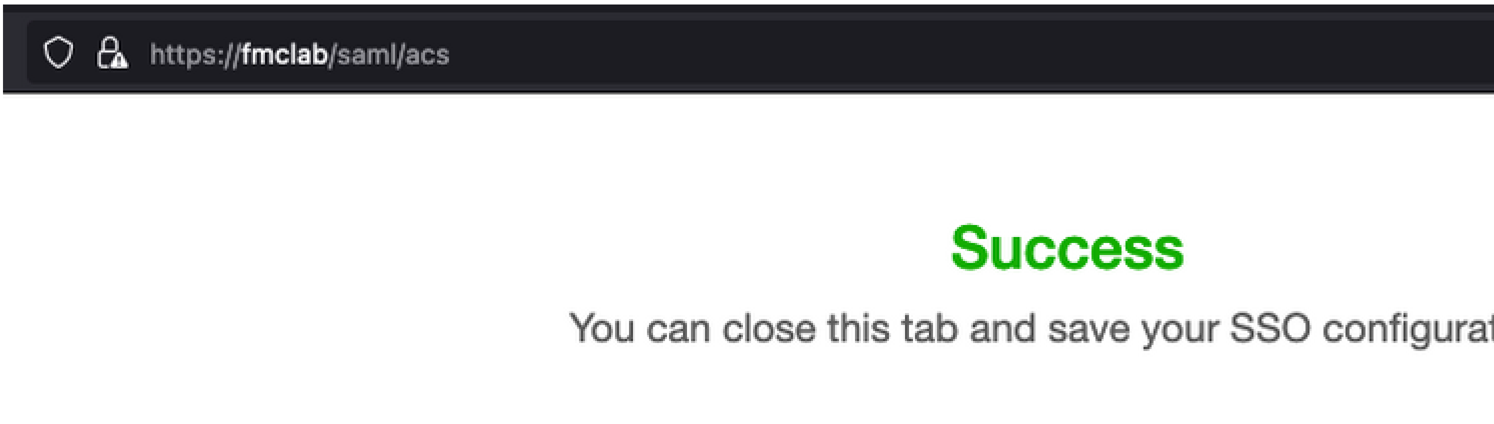
Default User Role: Administrator

Group Member Attribute:

In order to test the Configuration, click **Test Configuration**, as shown in this image.



Example shown of a successful test connection.

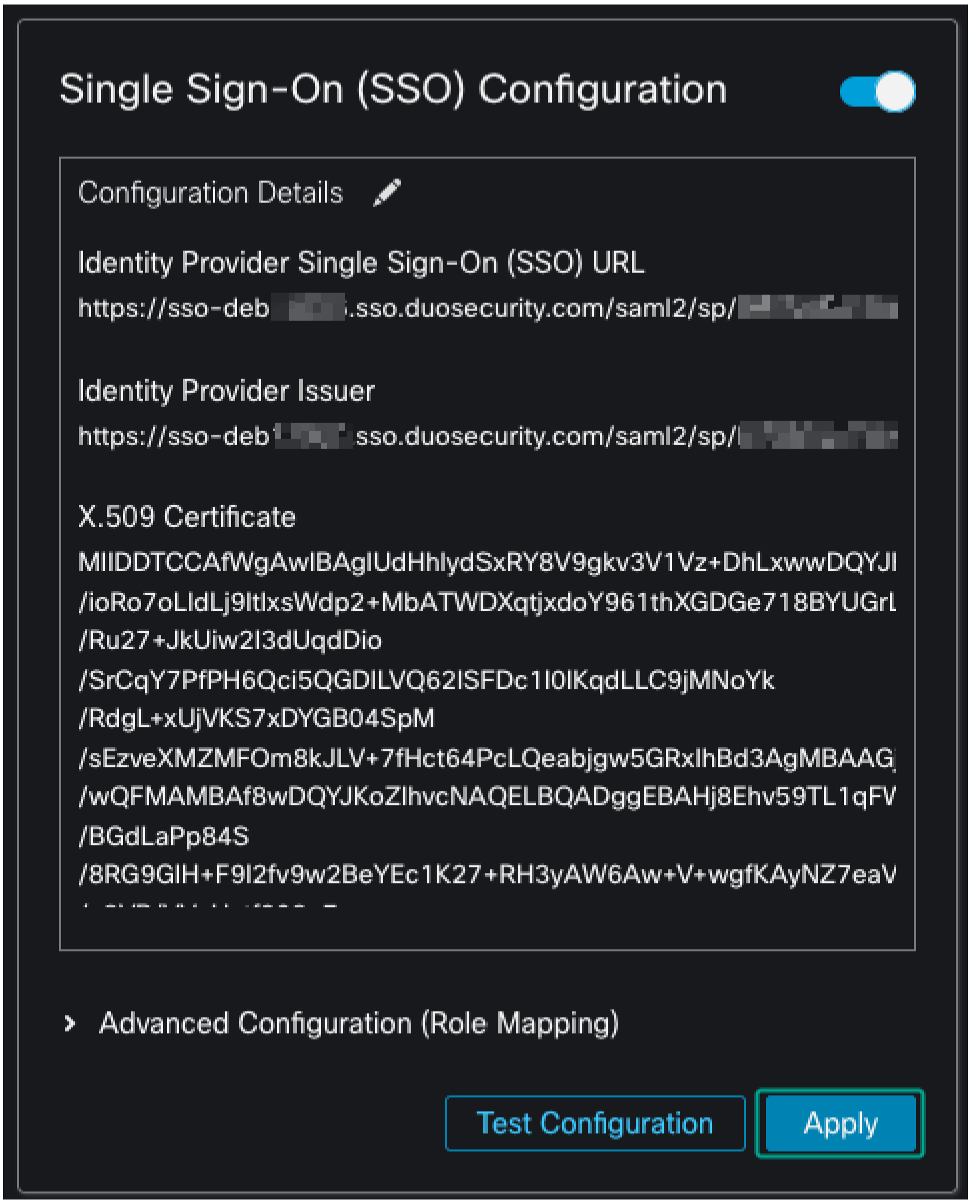


https://fmclab/saml/acs

Success

You can close this tab and save your SSO configurat

Click **Apply** to save the configuration.



Single Sign-On (SSO) Configuration

Configuration Details

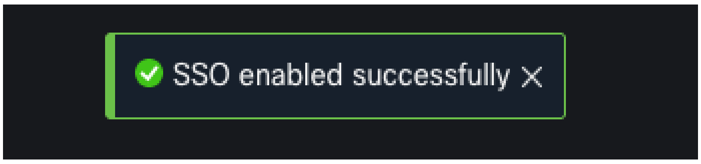
Identity Provider Single Sign-On (SSO) URL
https://sso-deb[redacted].sso.duosecurity.com/saml2/sp/[redacted]

Identity Provider Issuer
https://sso-deb[redacted]sso.duosecurity.com/saml2/sp/[redacted]

X.509 Certificate

```
MIIDDTCCAfWgAwIBAgIUdHhlydSxRY8V9gkv3V1Vz+DhLxwwDQYJI
/ioRo7oLIdLj9ltIxsWdp2+MbATWDXqtjxdoY961thXGDGe718BYUGrL
/Ru27+JkUiw2I3dUqdDio
/SrCqY7PfPH6Qci5QGDILVQ62ISFDc1I0IKqdLLC9jMNoYk
/RdgL+xUjVKS7xDYGB04SpM
/sEzveXMZMFOm8kJLV+7fHct64PcLQeabjgw5GRxIhBd3AgMBAAG
/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAHj8Ehv59TL1qFV
/BGdLaPp84S
/8RG9GIH+F9I2fv9w2BeYEc1K27+RH3yAW6Aw+V+wgfKAyNZ7eaV
```

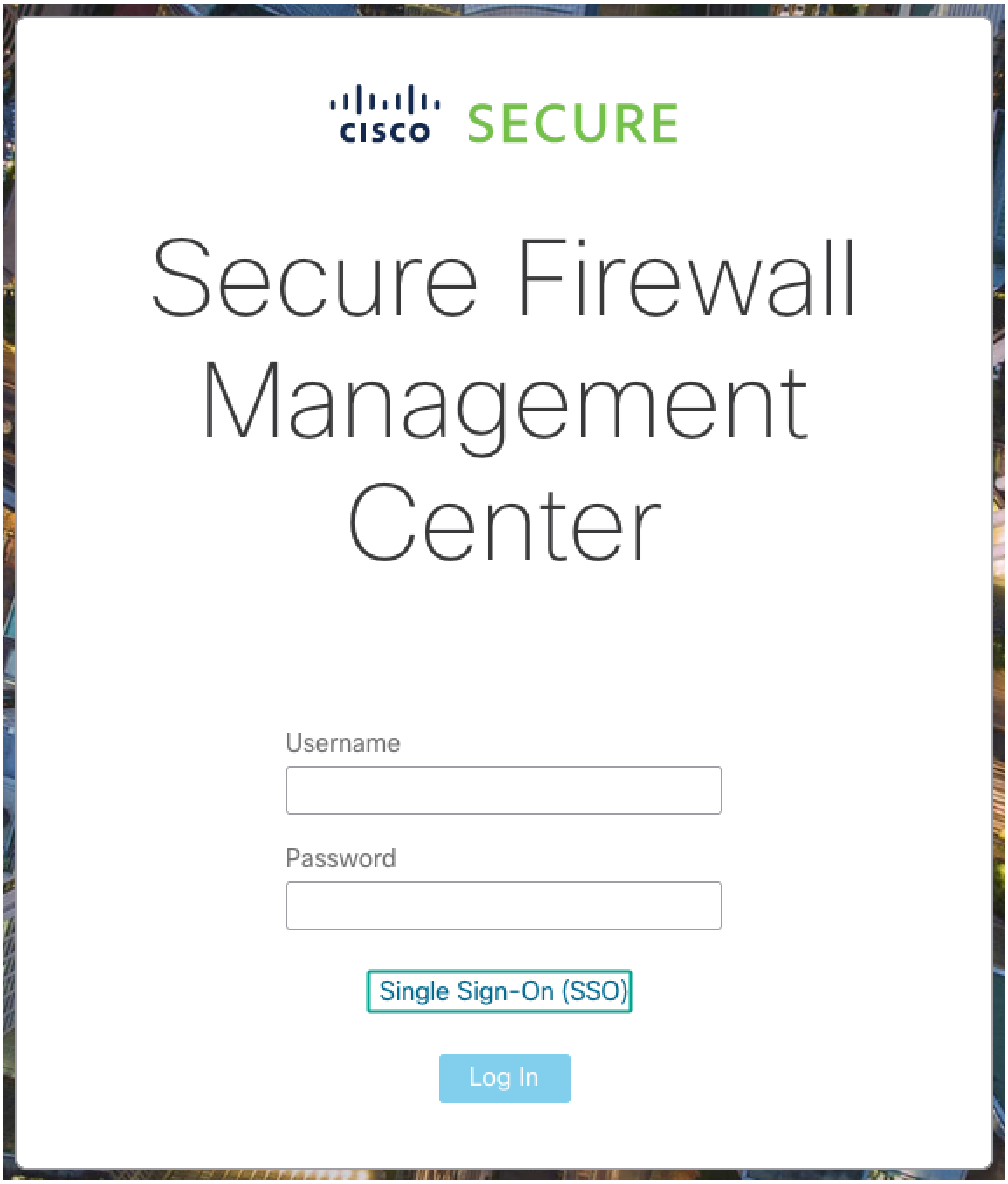
SSO is enabled successfully.



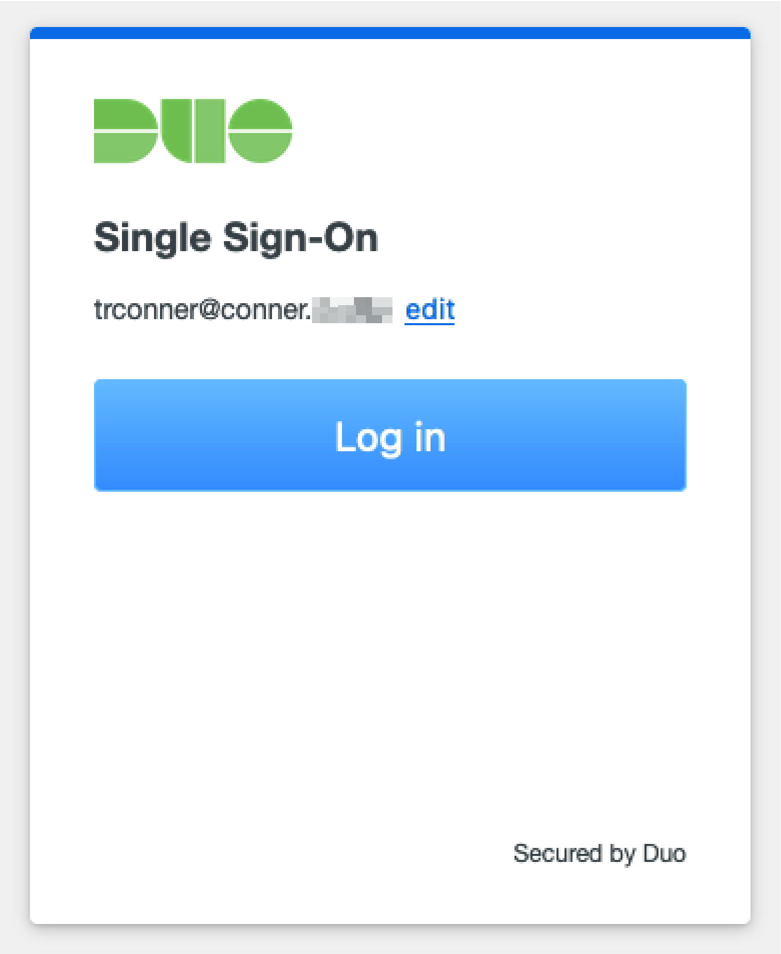
SSO enabled successfully

Verify

Navigate to the FMC URL from your browser: **https://<fmc URL>**. Click **Single Sign-On**.



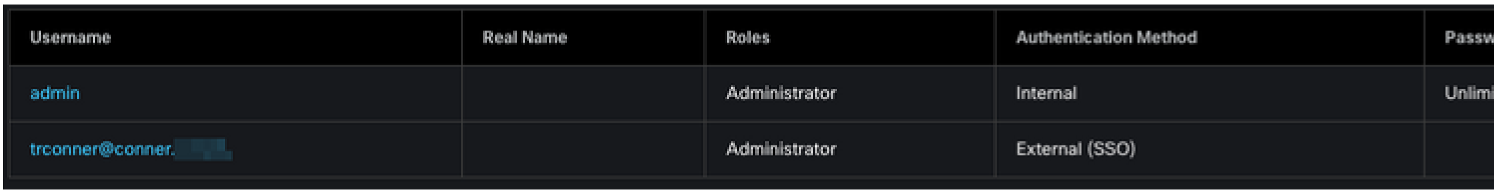
You are directed to the iDP (Duo) Login Page. Provide your SSO credentials. Click **Sign in**.



Single Sign-On

trconner@conner.[redacted]

If successful, you are be able to log in and see the FMC default page.
In FMC, navigate to **System** > **Users** to see the SSO user added to the database.



Username	Real Name	Roles	Authentication Method	Passw
admin		Administrator	Internal	Unlimi
trconner@conner.[redacted]		Administrator	External (SSO)	