

Configure Firepower Management Center Access through SSO Authentication with Okta

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Limitations and Restrictions](#)

[Configuration Steps](#)

[Configuration Steps on the Identity Provider \(Okta\)](#)

[Configuration Steps on FMC](#)

[Verify](#)

Introduction

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

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic understanding of Single Sign-On and SAML
- Understanding of the configuration on the Identity Provider (iDP)

Components Used

The information in this document is based on these software versions:

- Cisco Firepower Management Center (FMC) version 6.7.0
- Okta as the Identity Provider

Note: The information in this document was created from 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, make sure that you understand the potential impact of any configuration change.

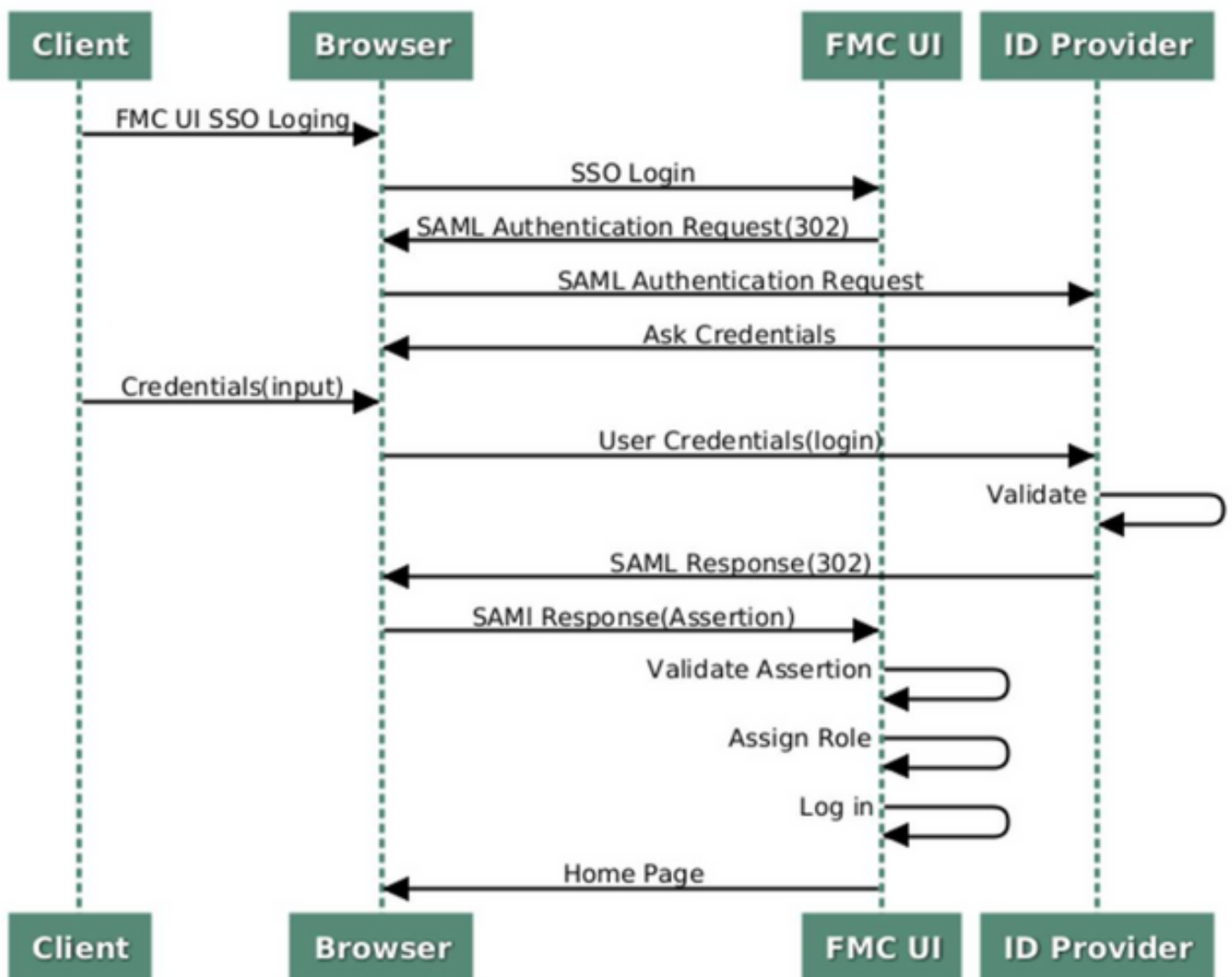
Background Information

Single sign-on (SSO) is a property of identity and access management (IAM) that enables users to securely authenticate with multiple applications and websites by logging in only once with just one set of credentials (username and password). With SSO, the application or website that the user is trying to access relies on a trusted third party to verify that users are who they say they are.

SAML (Security Assertion Markup Language) is an XML-based framework for exchanging authentication and authorization data between security domains. It creates a circle of trust between the user, a service provider (SP), and an Identity Provider (IdP) which allows the user to sign in a single time for multiple services

A Service Provider (SP) is an entity that receives and accepts an authentication assertion issued by an Identity Provider (iDP). As described by their names, service providers provide service while identity providers provide the identity of users (authentication).

SSO SAML Workflow



These iDPs are supported and are tested for authentication:

- Okta
- OneLogin

- PingID
- Azure AD
- 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

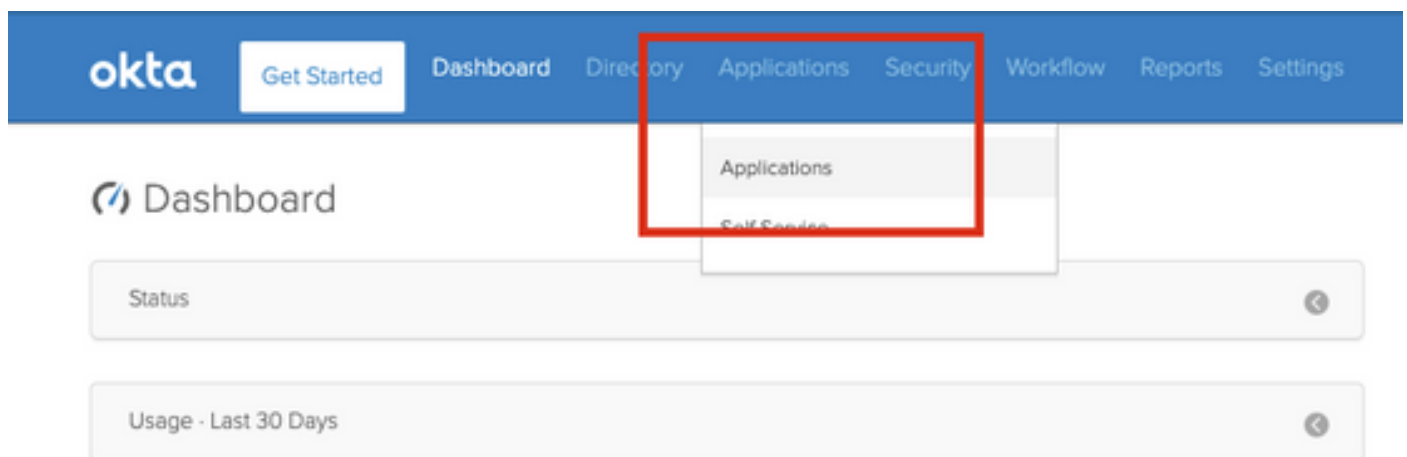
These are known limitations and restrictions for SSO authentication for FMC access:

- SSO can be configured only for the Global Domain
- FMC's in HA Pair requires individual configuration
- Only Local/AD admins can configure SSO on FMC (SSO admin users will not be able to configure/update SSO settings on FMC).

Configuration Steps

Configuration Steps on the Identity Provider (Okta)

Step 1. Login into the Okta portal. Navigate to **Applications > Applications**, as shown in this image.



Step 2. As shown in this image, click on **AddApplication**.

Applications



Add Application



Assign Applications



Search

Step 3. As shown in this image, click on **Create NewApp**.

← Back to Applications

Add Application

Create New App

CATEGORIES

Featured

API Management



Search...

Featured Integrations

See all

Step 4. Choose the **Platform** as **Web**. Choose the **Sign On method** as **SAML 2.0**. Click on **Create**, as shown in this image.

Create a New Application Integration



Platform

Web

Sign on method

☐ Secure Web Authentication (SWA)

Uses credentials to sign in. This integration works with most apps.

☒ SAML 2.0

Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

☐ OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

Step 5. Provide an **App name**, **App logo (optional)**, and click **Next**, as shown in this image.


1 General Settings

App name

App logo (optional) ?

App visibility

FMC-Login


cisco.png Browse..
Upload Logo

Requirements

- Must be PNG, JPG or GIF
- Less than 1MB

For Best Results, use a PNG image with

- Minimum 420px by 120px to prevent upscaling
- Landscape orientation
- Transparent background

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

CancelNext

Step 6. 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`

GENERAL

Single sign on URL ?

https://<FMC URL>/saml/acs

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

https://<FMC URL>/saml/metadata

Default RelayState ?

/ui/login

If no value is set, a blank RelayState is sent

Name ID format ?

Unspecified

Application username ?

Okta username

Update application username on

Create and update

[Show Advanced Settings](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name

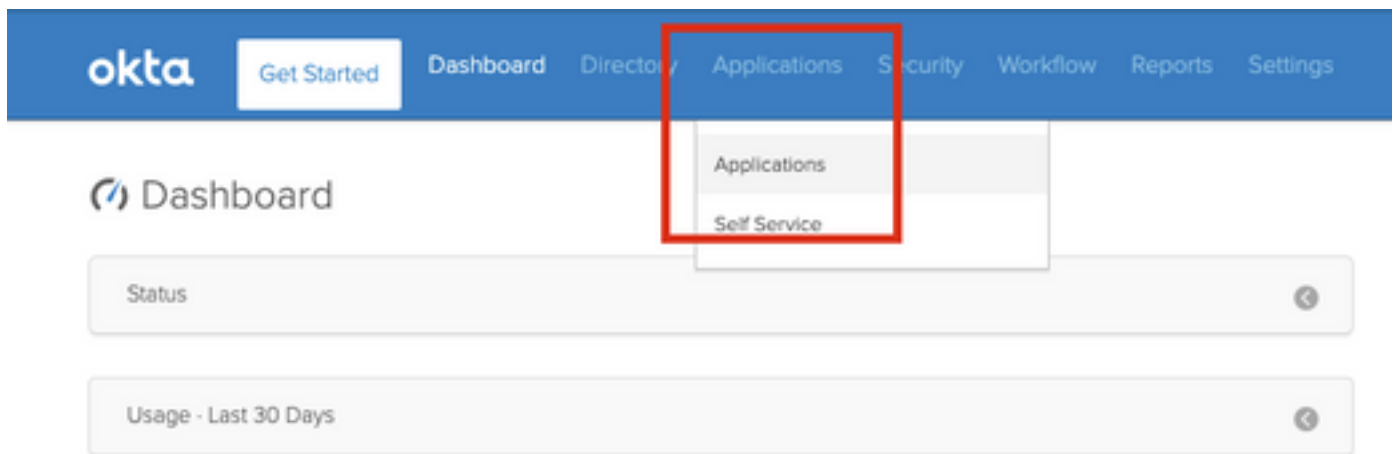
Name format (optional)

Value

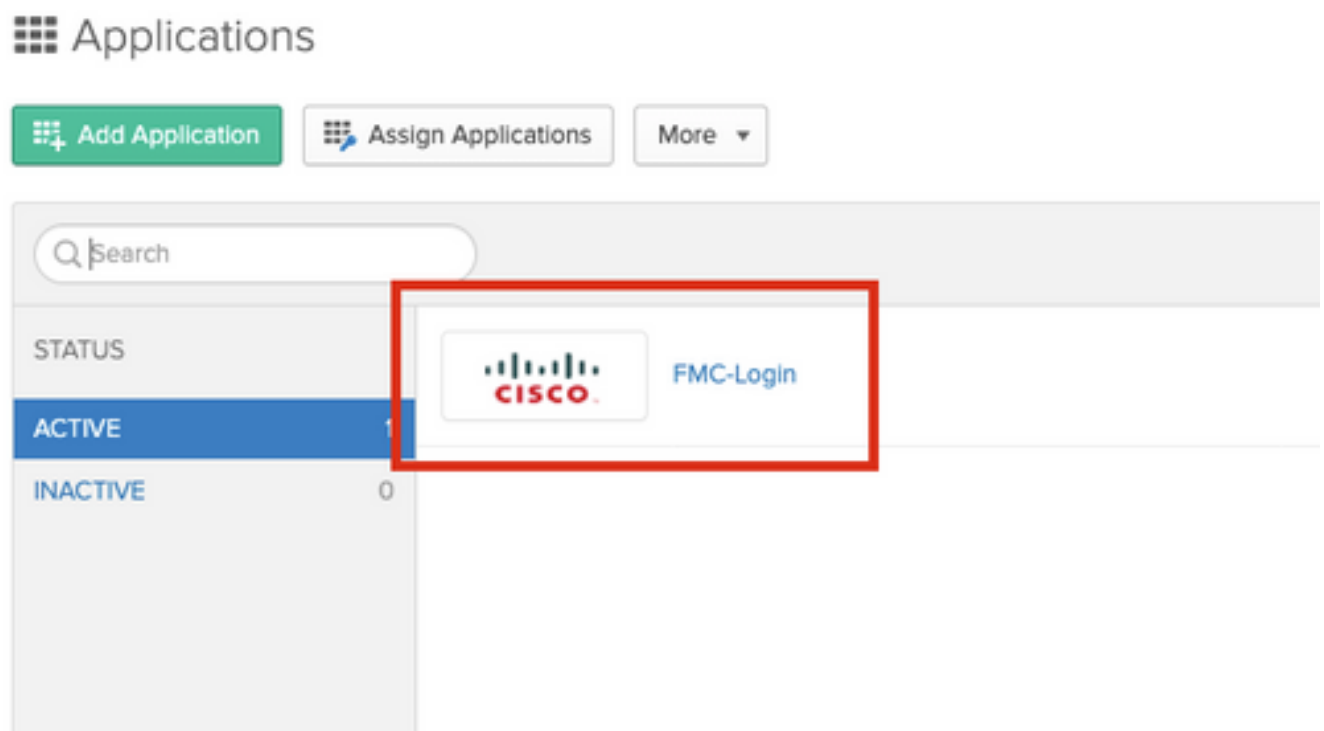
Unspecified

Add Another

Step 7. Navigate back to **Applications > Applications**, as shown in this image.

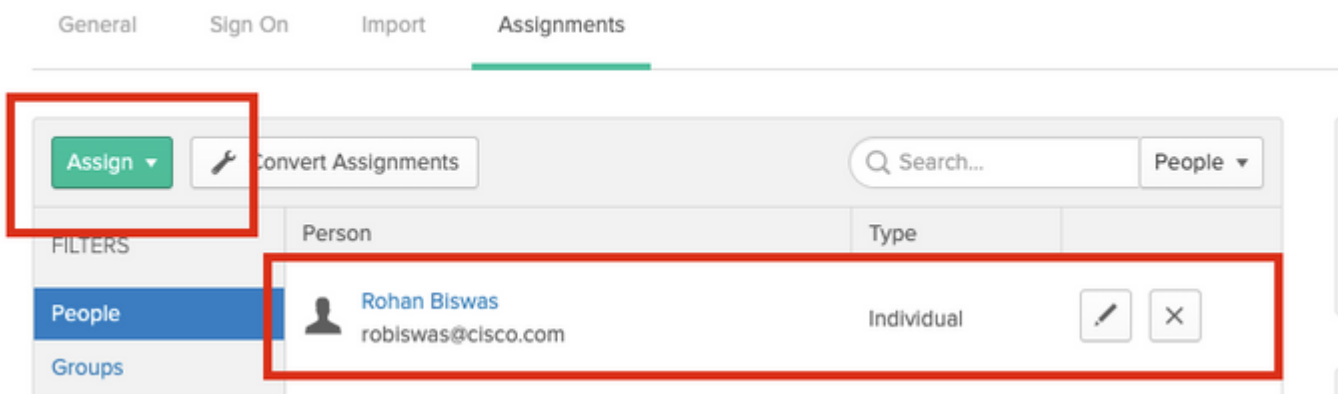


Step 8. Click on the App name that was created.

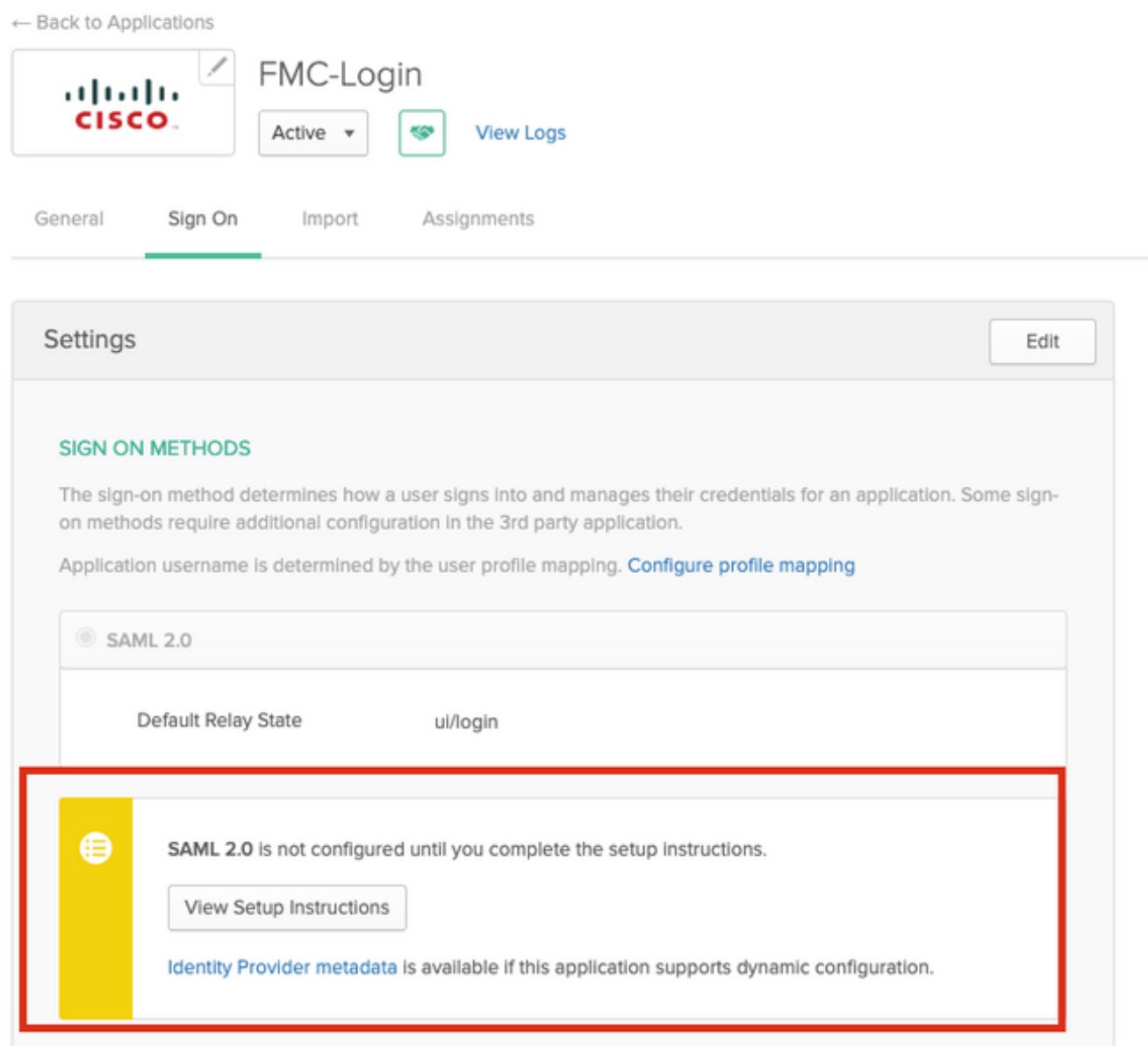


Step 9. Navigate to **Assignments**. Click on **Assign**.

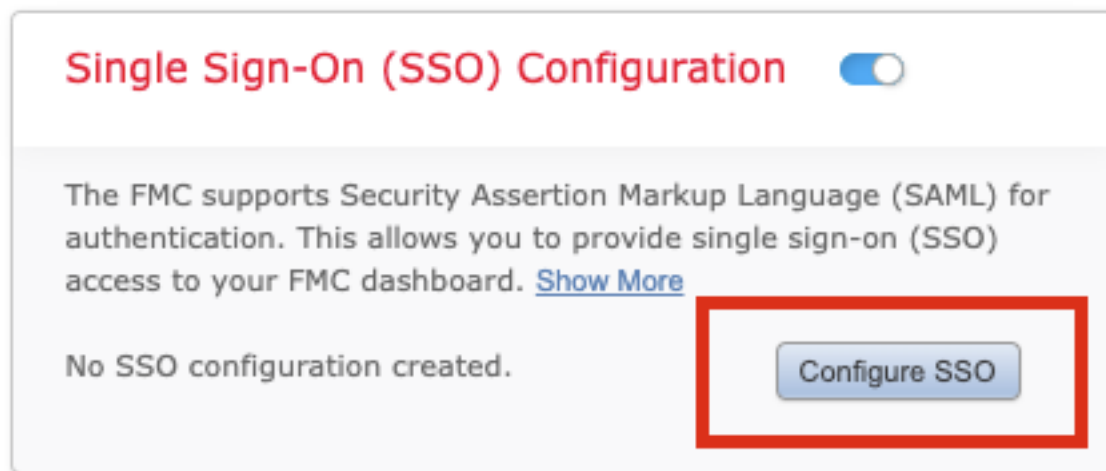
You can choose to assign individual users or groups to the App name created.



Step 10. Navigate to **Sign On**. Click on **View Setup Instructions**. Click on **Identity Provider metadata** to view the metadata of the iDP.



Save the file as a **.xml** file to be used on the FMC.



Step 5. Select the **FMC SAML Provider**. Click **Next**.

For the purpose of this demonstration, **Okta** is used.



Step 6. You can choose **Manual Configuration** and enter the iDP data manually. Click **Next**, as

Configure Okta Metadata

Configure the FMC to work with your Okta 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
metadata.xml

Identity Provider Single Sign-On URL
https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclgin_1/exkjmr3gbDQjCYNin4x6/sso/saml

Identity Provider Issuer
http://www.okta.com/exkjmr3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UI

Step 2 of 3

Back Next

Step 7. **Verify** the metadata. Click **Save**, as shown in this image.

Verify Okta Metadata

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

Identity Provider Single Sign-On URL
https://cisco-robiswas.okta.com/app/ciscoorg842643_fmclgin_1/exkjmr3gbDQjCYNin4x6/sso/saml

Identity Provider Issuer
http://www.okta.com/exkjmr3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZv

Step 3 of 3

Back **Save**

Step 8. Configure the **Role Mapping/Default User Role** under **Advanced Configuration**.

Single Sign-On (SSO) Configuration

Configuration Details

Identity Provider Single Sign-On URL

https://cisco-robiswas.okta.com/app/ciscoorg842643_

Identity Provider Issuer

http://www.okta.com/exkjm3gbDQjCYNin4x6

X.509 Certificate

MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

▼ Advanced Configuration (Role Mapping)

Default User Role

Administrator

Group Member Attribute

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

Security Analyst

Security Analyst (Read Only)

Security Approver

Threat Intelligence Director (TID) User

Step 9. In order to test the Configuration, click on **Test Configuration**, as shown in this image.

Single Sign-On (SSO) Configuration ☒

Configuration Details

Identity Provider Single Sign-On URL
`https://cisco-robiswas.okta.com/app/ciscoorg842643_`

Identity Provider Issuer
`http://www.okta.com/exkjmr3gbDQjCYNin4x6`

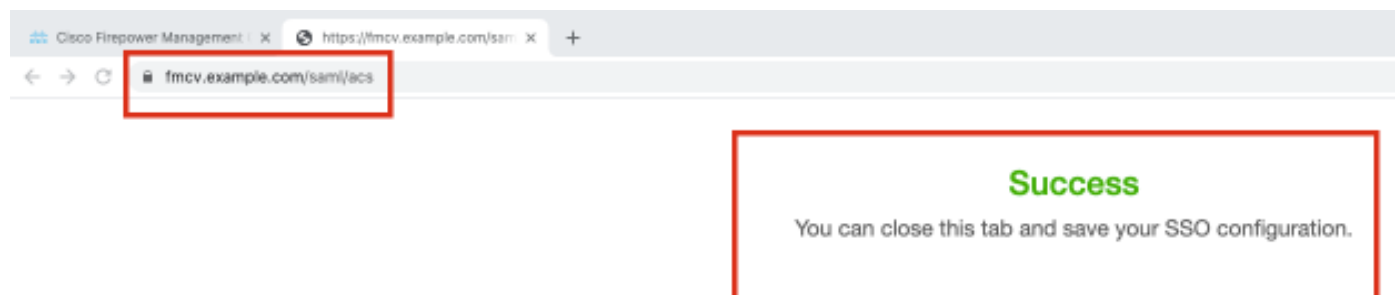
X.509 Certificate
`MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ`

> Advanced Configuration (Role Mapping)

Test Configuration

Apply

If the test is a success, you should see the page shown in this image, on a new tab on the browser.



Step 10. Click on **Apply** to save the configuration.

Single Sign-On (SSO) Configuration ☒

Configuration Details /

Identity Provider Single Sign-On URL
https://cisco-robiswas.okta.com/app/ciscoorg842643_

Identity Provider Issuer
http://www.okta.com/exkjm3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

> Advanced Configuration (Role Mapping)

Test Configuration

Apply

SSO should be enabled successfully.

✔ SSO enabled successfully ✕

Single Sign-On (SSO) Configuration ☒

Configuration Details /

Identity Provider Single Sign-On URL
https://cisco-robiswas.okta.com/app/ciscoorg842643_

Identity Provider Issuer
http://www.okta.com/exkjm3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

> Advanced Configuration (Role Mapping)

Test Configuration

Apply

Verify

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



Firepower Management Center

Username

Password

[Single Sign-On](#)

[Log In](#)

You would be redirected to the iDP (Okta) Login Page. Provide your SSO credentials. Click on **Sign in**.

Connecting to

Sign-in with your cisco-org-842643 account to access FMC-
Login

okta



Sign In

Username

robiswas@cisco.com

Password

.....|

☐ Remember me

Sign In

Need help signing in?

If successful, you should be able to log in and see the FMC default page.

On FMC, navigate to **System > Users** to see the SSO user added to the database.

Users						
User Roles External Authentication Single Sign-On						
Create User						
Filter						
Username	Real Name	Roles	Authentication Method	Password Lifetime	Enabled	Actions
admin		Administrator	Internal	Unlimited		
robiswas@cisco.com		Administrator	External (SSO)			