

# Oktaを使用したSSO認証によるFirepower Management Center(FMC)アクセスの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[制限と制限](#)

[設定手順](#)

[アイデンティティプロバイダー\(Okta\)の設定手順](#)

[FMCの設定手順](#)

[確認](#)

## 概要

このドキュメントでは、管理アクセスにシングルサインオン(SSO)を使用して認証するようにFirepower Management Center(FMC)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- シングルサインオンとSAMLの基礎知識
- アイデンティティプロバイダー(iDP)の設定について

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Firepower Management Center(FMC)バージョン6.7.0
- IDプロバイダーとしてokta

注：このドキュメントの情報は、特定のラボ環境のデバイスから作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、設定変更による潜在的な影響について理解しておいてください。

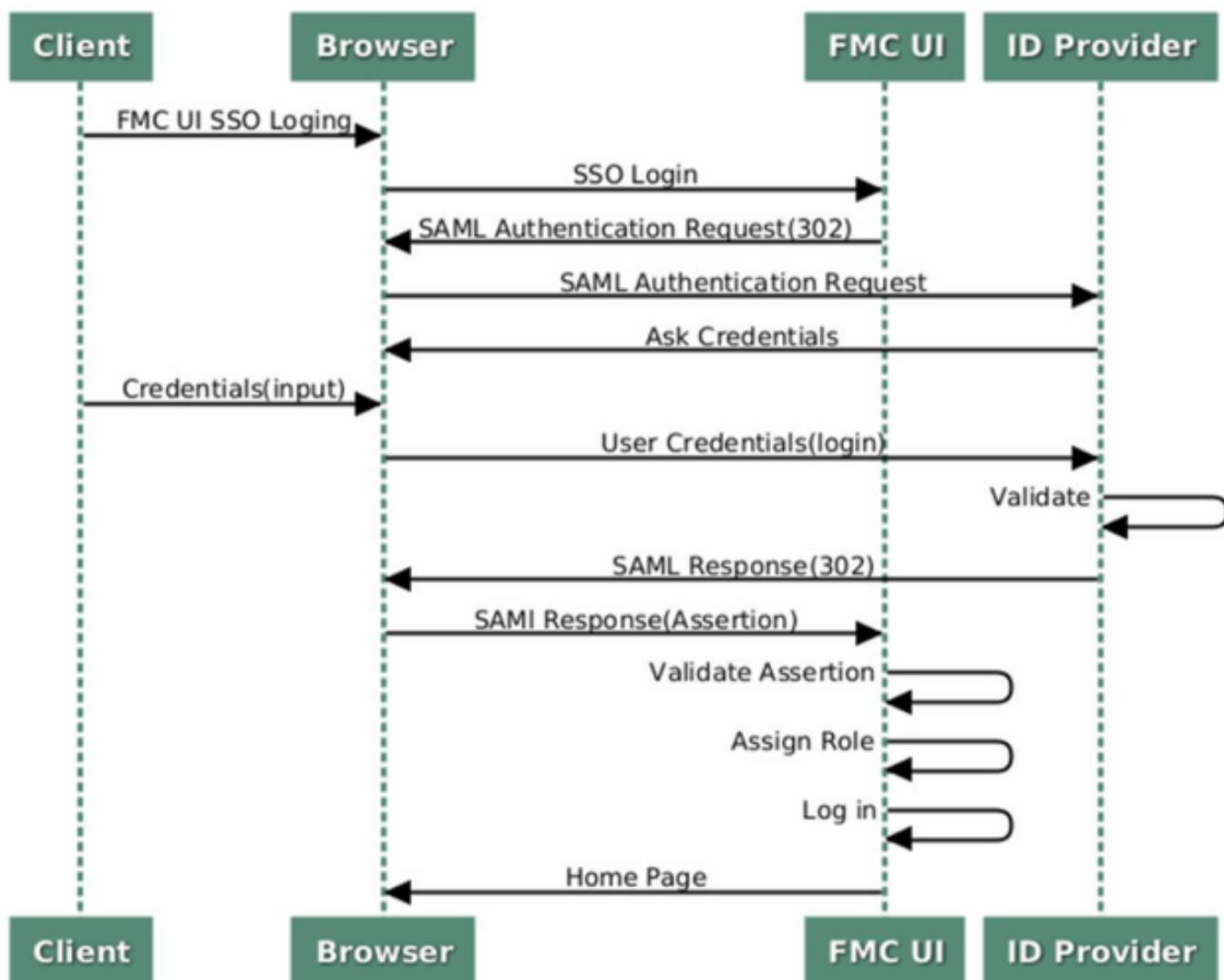
## 背景説明

シングルサインオン(SSO)は、IDおよびアクセス管理(IAM)のプロパティで、1つのクレデンシャル(ユーザ名とパスワード)を使用して1回だけログインするだけで、複数のアプリケーションやWebサイトで安全に認証できます。SSOを使用すると、ユーザがアクセスしようとしているアプリケーションまたはWebサイトは、信頼できるサードパーティに依存して、ユーザが自分が言っているユーザであることを確認します。

SAML(Security Assertion Markup Language)は、セキュリティドメイン間で認証および許可データを交換するためのXMLベースのフレームワークです。ユーザ、サービスプロバイダー(SP)、アイデンティティプロバイダー(IdP)の間に信頼の輪が作成され、ユーザは複数のサービスに対して一度にサインインできます

サービスプロバイダー(SP)は、アイデンティティプロバイダー(iDP)によって発行された認証セッションを受信して受け入れるエンティティです。名前に記載されているように、サービスプロバイダーはサービスを提供し、アイデンティティプロバイダーはユーザのアイデンティティを提供します(認証)。

### SSO SAML Workflow



次のiDPがサポートされ、認証がテストされています。

- 岡田
- OneLogin
- PingID

- Azure AD
- その他 ( SAML 2.0に準拠するiDP )

注：新しいライセンス要件はありません。この機能は、ライセンス供与モードと評価モードで動作します。

## 制限と制限

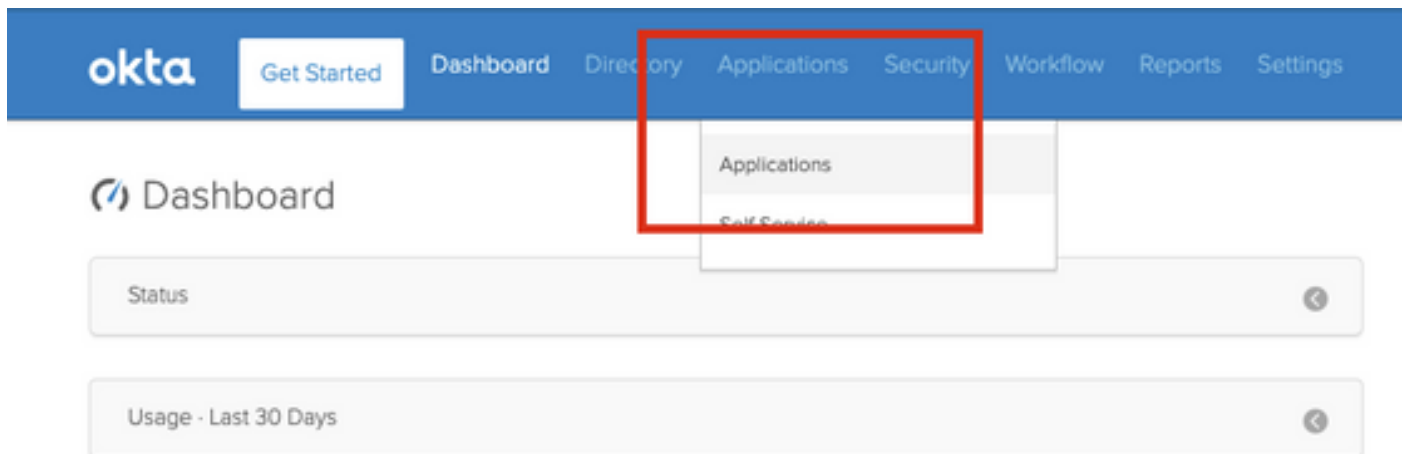
FMCアクセスのSSO認証に関する既知の制限と制限は次のとおりです。

- SSOはグローバルドメインに対してのみ設定できます
- HAペアのFMCでは個別の設定が必要
- ローカル/AD管理者のみがFMCでSSOを設定できます ( SSO管理者ユーザはFMCでSSO設定を設定/更新できません )。

## 設定手順

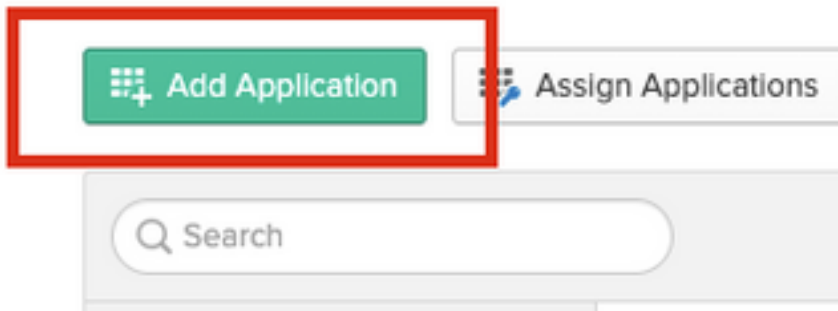
### アイデンティティプロバイダー(Okta)の設定手順

ステップ1:Oktaポータルにログインします。次の図に示すように、[Applications] > [Applications]に移動します。

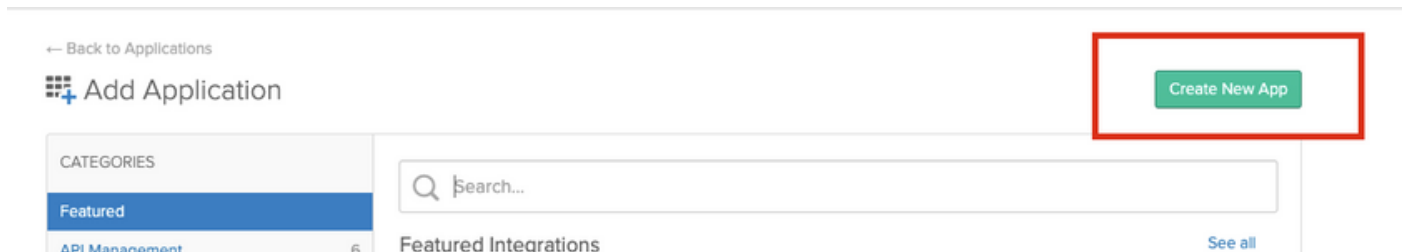


ステップ2：次の図に示すように、[AddApplication]をクリックします。

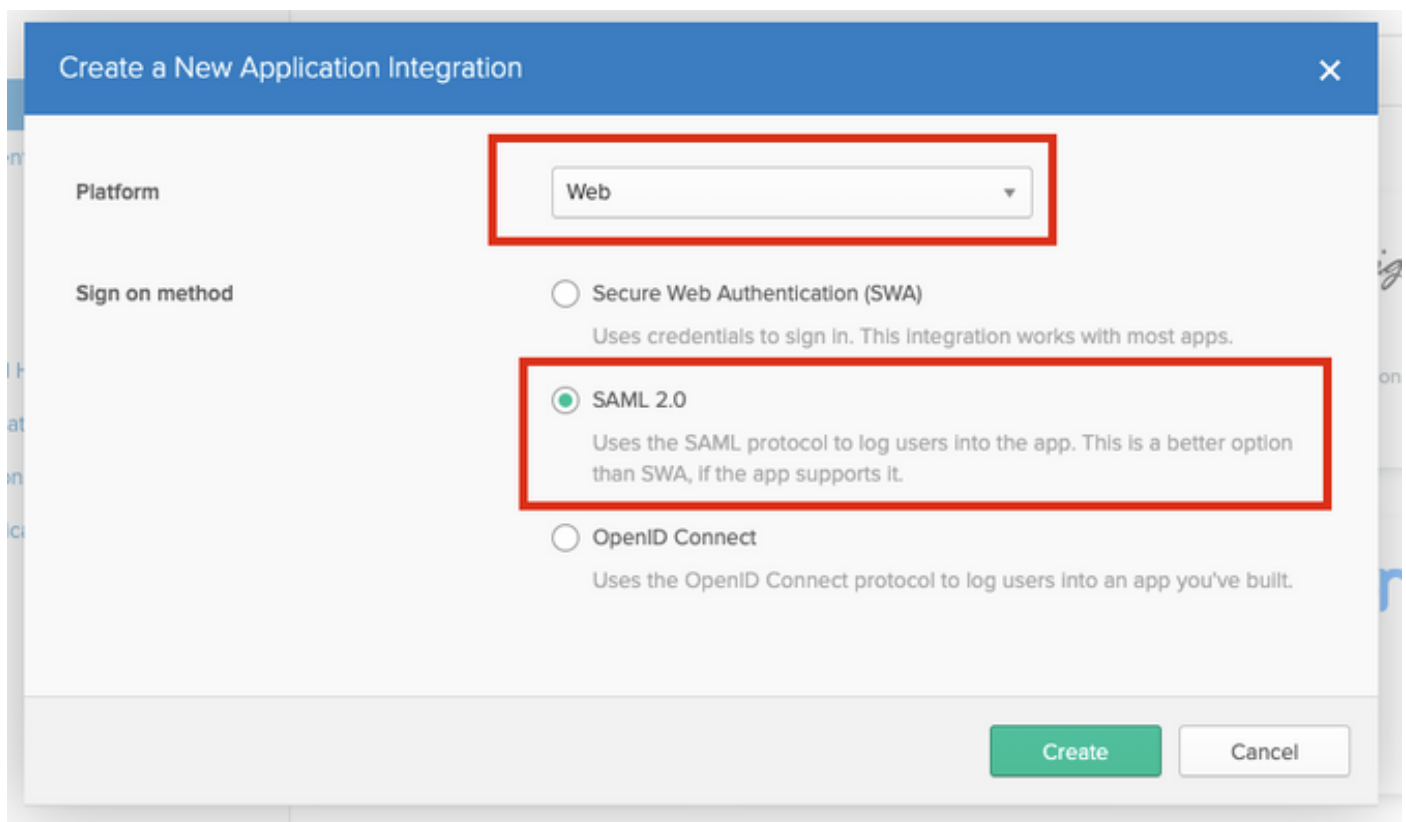
## Applications



ステップ3 : 次の図に示すように、[Create NewApp]をクリックします。



ステップ4:[Platform]を[Web]として選択します。Sign OnメソッドをSAML 2.0と選択します。次の図に示すように[Create]をクリックします。




ステップ5 : 次の図に示すように、[App name]、[App logo](オプション)を指定し、[Next]をクリックします。

## 1 General Settings

App name

App logo (optional) ?

FMC-Login



cisco.png

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

App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

ステップ6:[SAML Settings]を入力します。

シングルサインオンURL:https://<fmc URL>/saml/acs

対象者URI ( SPエンティティID ) : https://<fmc URL>/saml/metadata

既定のリレー状態 : /ui/login

## A SAML Settings

### GENERAL

Single sign on URL ?

 Use this for Recipient URL and Destination URL Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

### ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

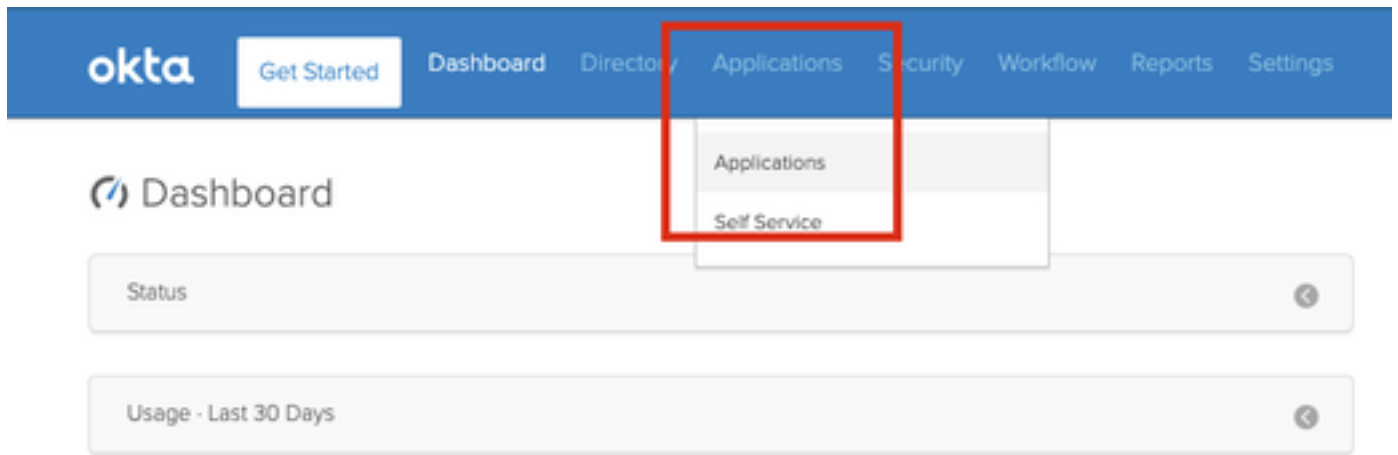
Name

Name format (optional)

Value

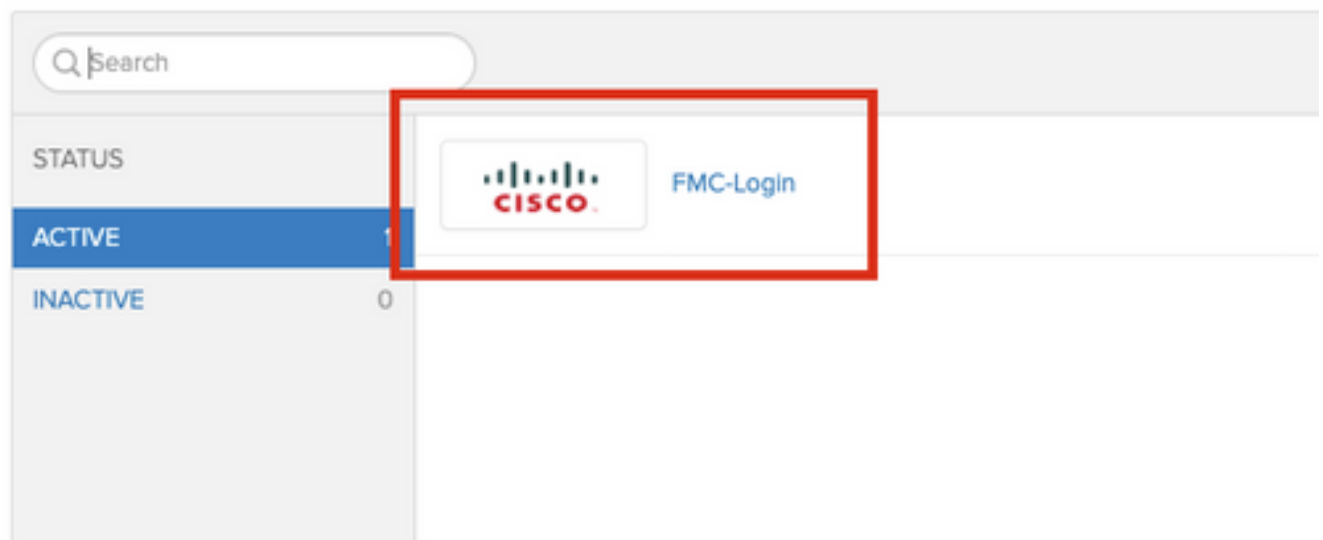
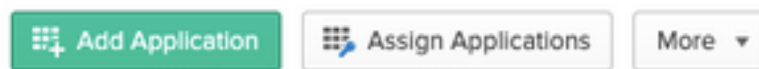
[Add Another](#)

ステップ7：次の図に示すように、[Applications] > [Applications]に戻ります。



ステップ8: 作成されたアプリ名をクリックします。

## Applications




ステップ9: 「割当」にナビゲートします。[割り当て]をクリックします。

作成したアプリ名に個々のユーザーまたはグループを割り当てることができます。

General Sign On Import **Assignments**

Assign Convert Assignments Search... People


FILTERS

Person	Type
 Rohan Biswas robiswas@cisco.com	Individual

People Groups

ステップ10:[サインオン]に移動します。「設定手順の表示」をクリックします。「アイデンティティプロバイダ」メタデータをクリックすると、iDPのメタデータが表示されます。

← Back to Applications

 FMC-Login

Active View Logs

General Sign On Import Assignments

Settings Edit


**SIGN ON METHODS**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State ui/login

 SAML 2.0 is not configured until you complete the setup instructions.

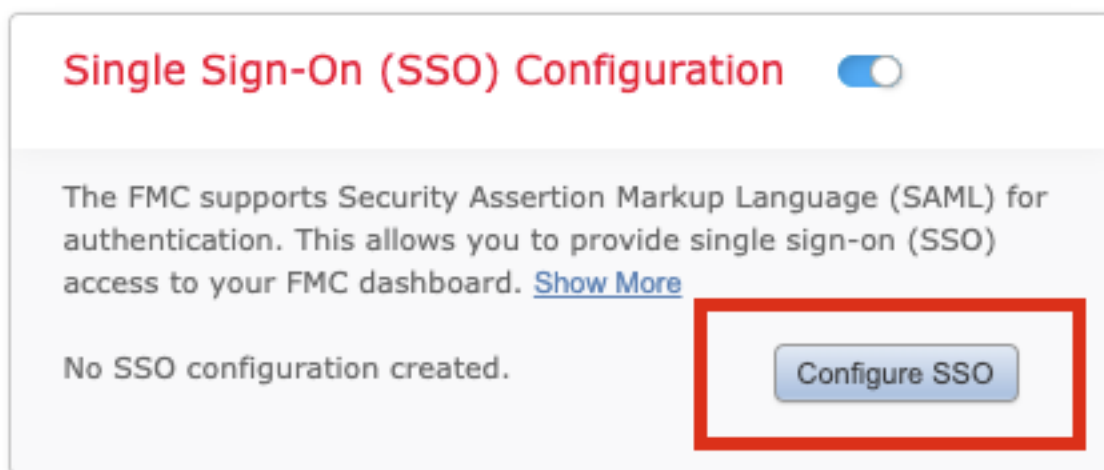
[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

FMCで使用する.xmlファイルとしてファイルを保存します。





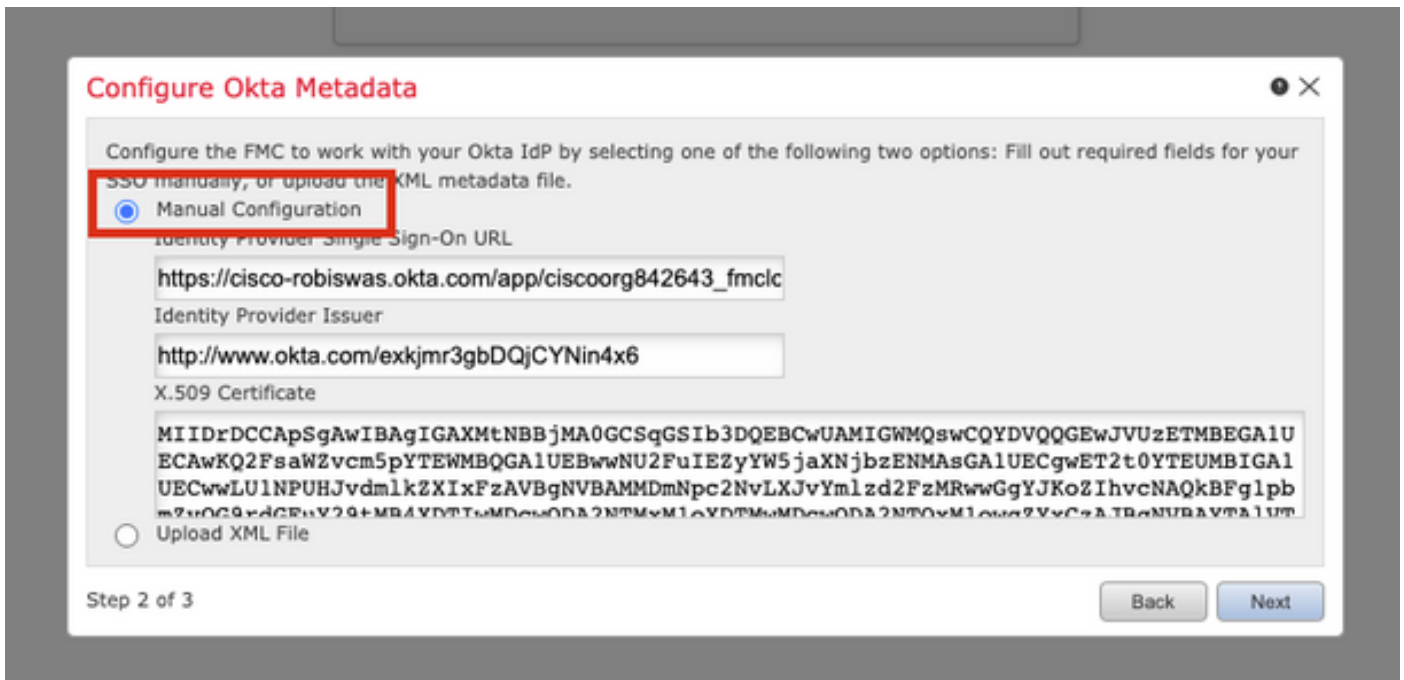


ステップ5:[FMC SAML Provider]を選択します。[next] をクリックします。

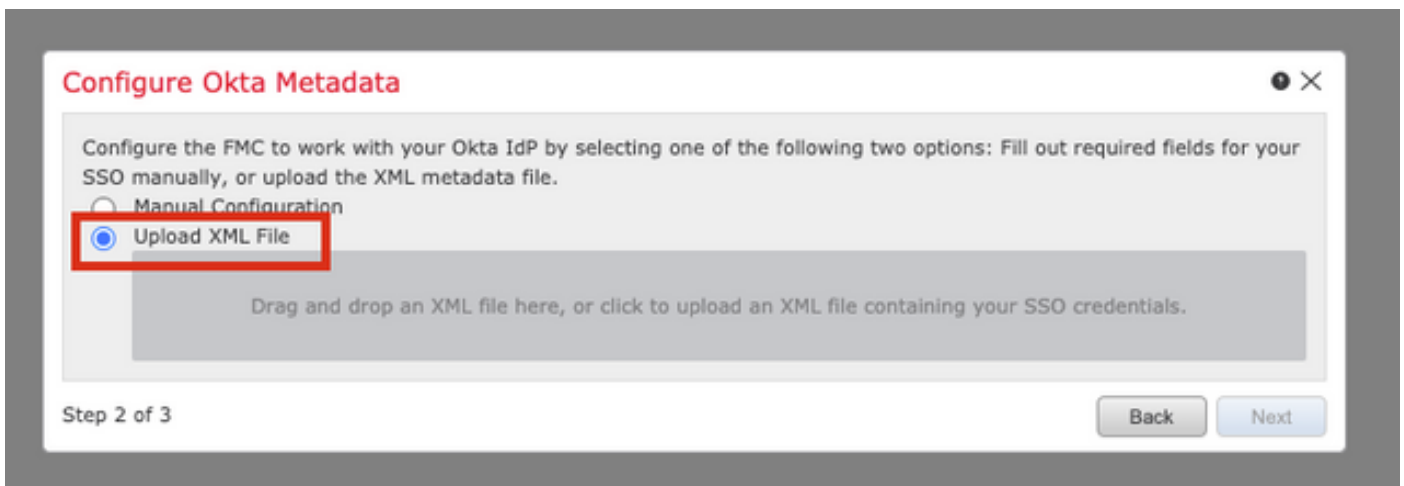
このデモンストレーションの目的はお田です。



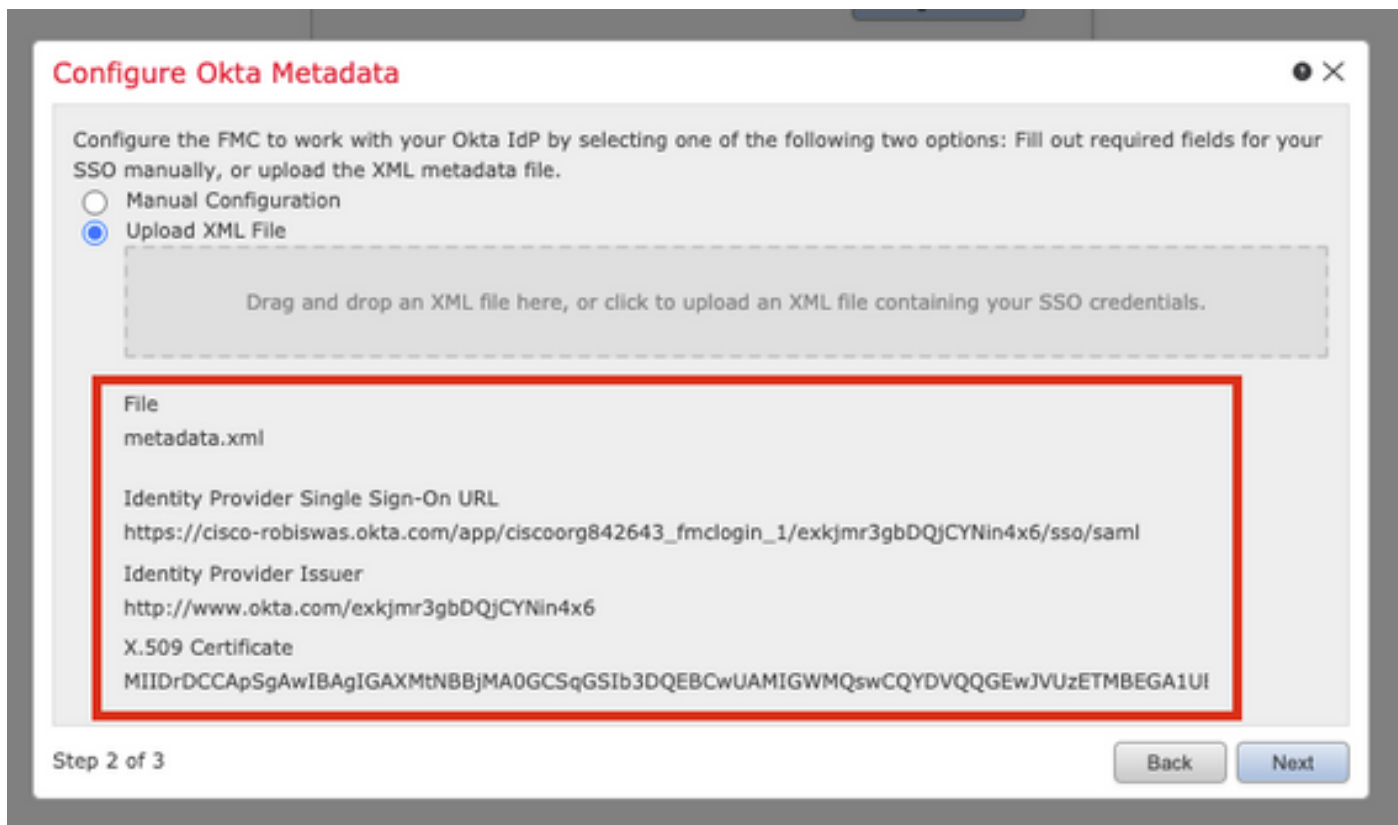
ステップ6:[Manual Configuration]を選択し、iDPデータを手動で入力できます。[次へ]をクリックします。



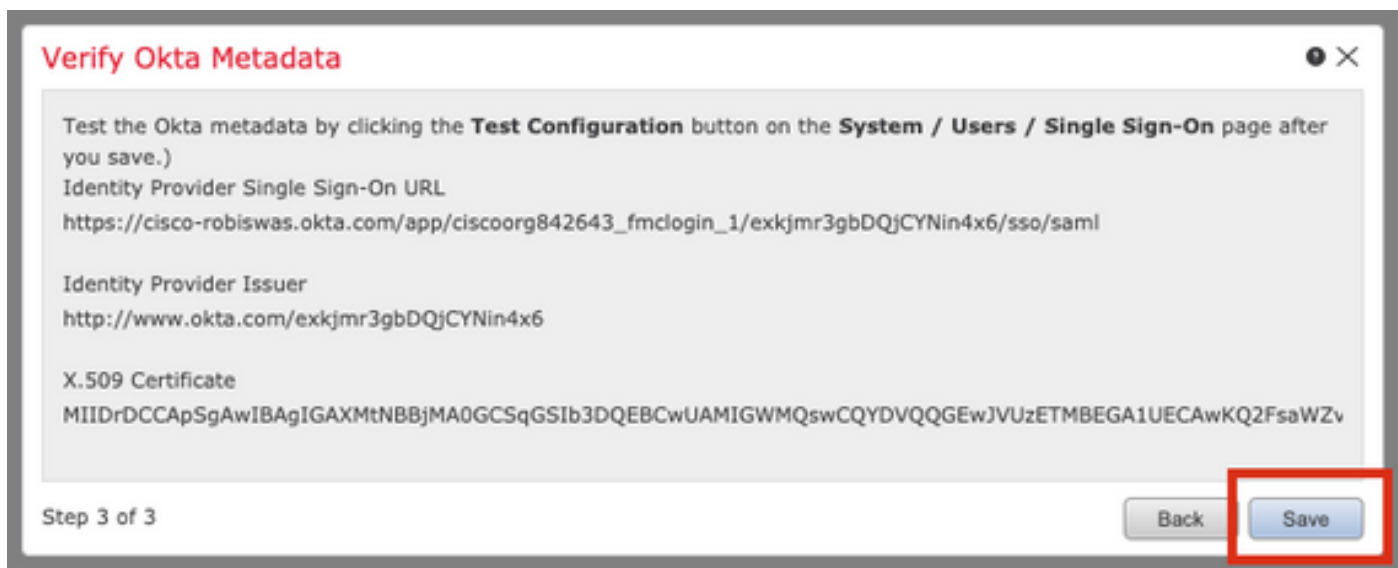
「XMLファイルのアップロード」を選択し、Okta構成のステップ10で取得したXMLファイルを[アップロードする](#)こともできます。



ファイルがアップロードされると、FMCにメタデータが表示されます。次の図に示すように[Next]をクリックします。



ステップ7: メタデータを確認します。次の図に示すように[Save]をクリックします。



ステップ8:[Advanced Configuration]の下で[Role Mapping/Default User Role]を設定します。

## 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)

Default User Role

Administrator

Group Member Attribute

Access Admin

Administrator

Discovery Admin

External Database User

Intrusion Admin

Maintenance User

Network Admin

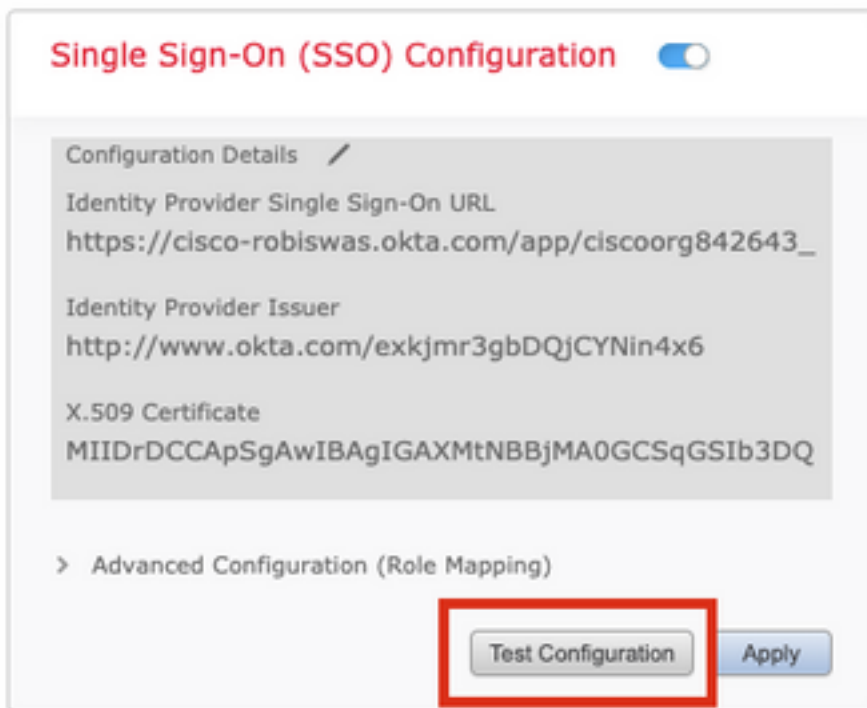
Security Analyst

Security Analyst (Read Only)

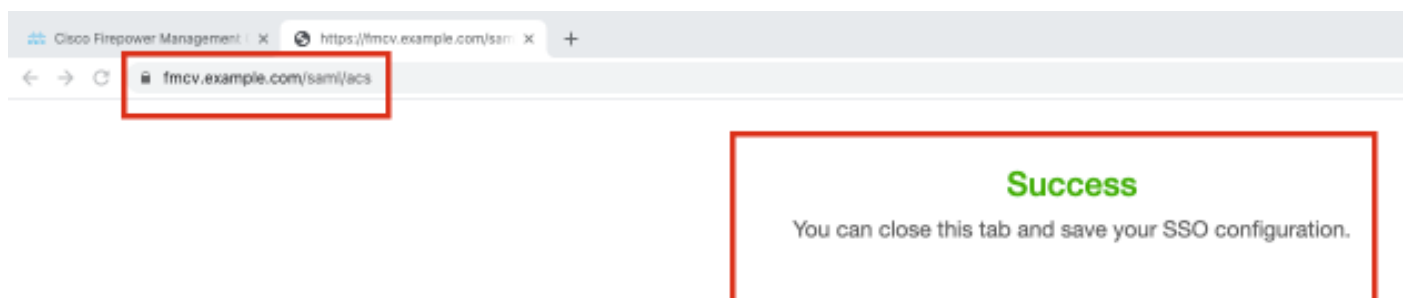
Security Approver

Threat Intelligence Director (TID) User

ステップ9 : 設定をテストするには、次の図に示すように[Test Configuration]をクリックします。



テストが成功した場合は、ブラウザの新しいタブに、次の図に示すページが表示されます。



ステップ10:[Apply]をクリックし、設定を保存します。

**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

SSOを正常に有効にする必要があります。

✔ 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/exkjmr3gbDQjCYNin4x6

X.509 Certificate  
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

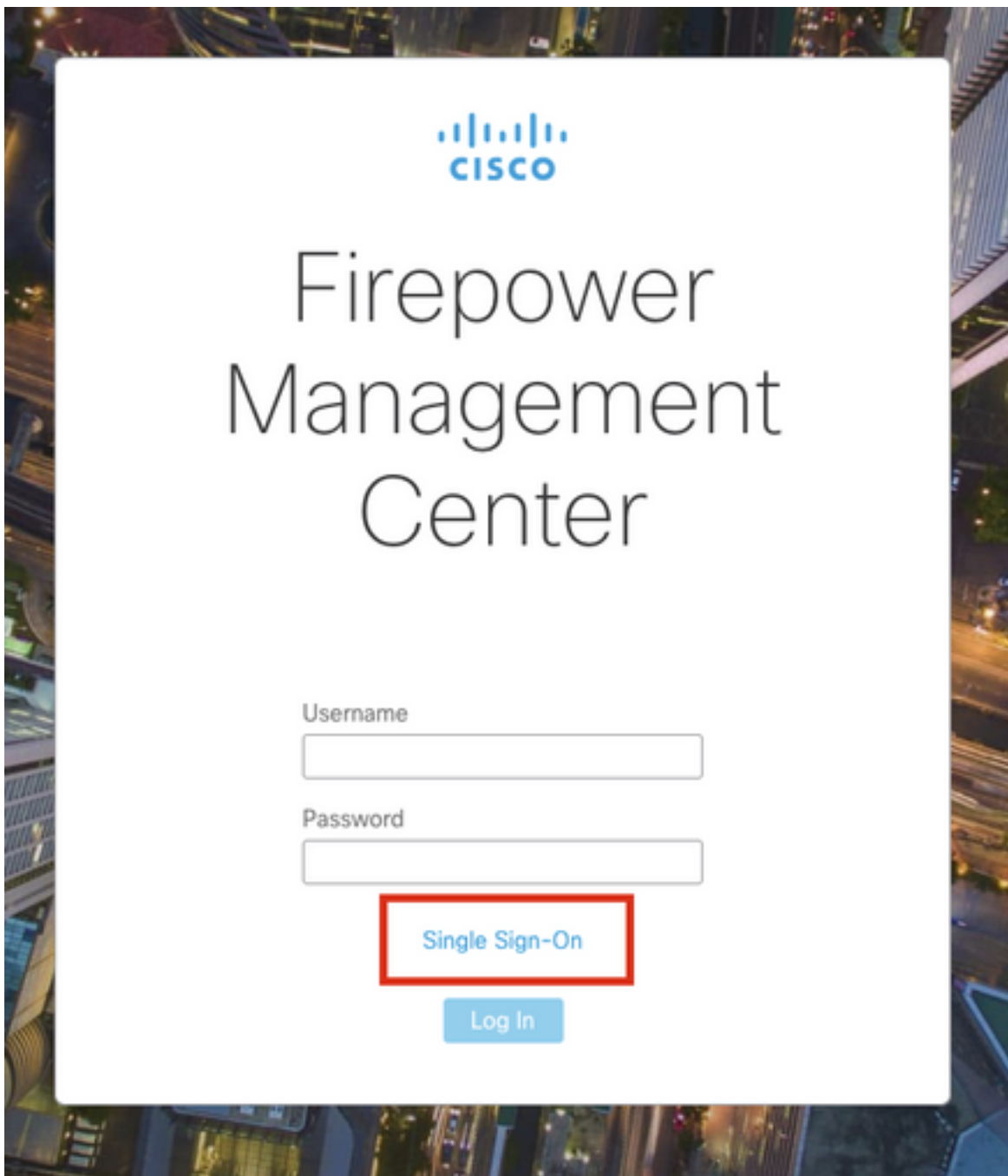
> Advanced Configuration (Role Mapping)

Test Configuration Apply

## 確認


ブラウザからFMC URL <https://<fmc URL>>に移動します。[シングルサインオン]をクリックします

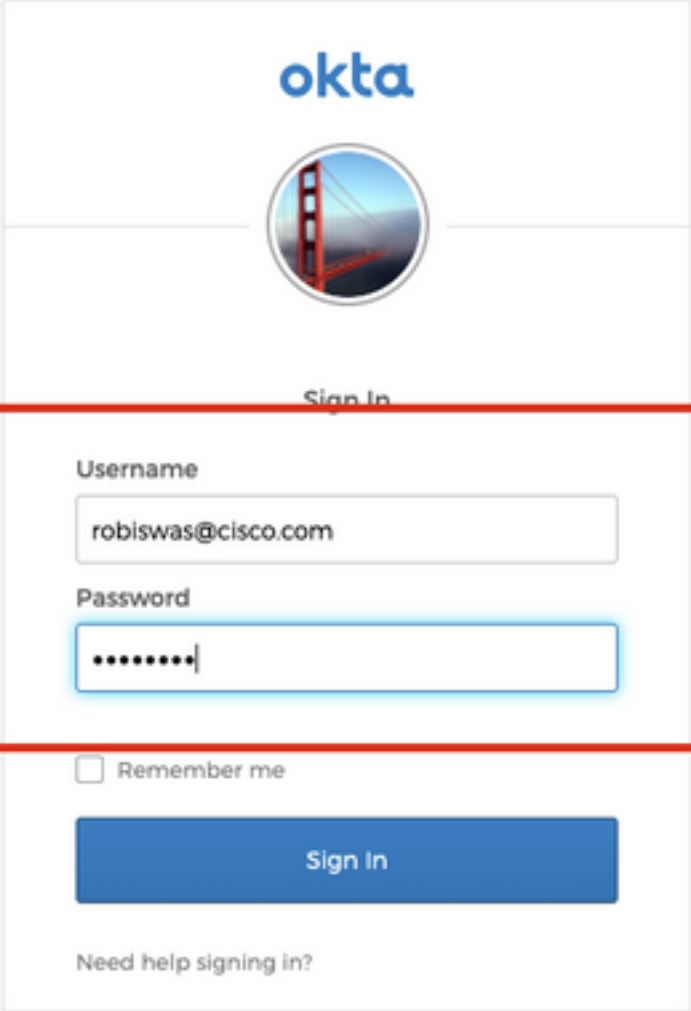
o



iDP(Okta)ログインページにリダイレクトされます。SSOクレデンシャルを入力します。[サインイン]をクリックします。



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



The image shows the Okta sign-in interface. At the top, the Okta logo is displayed. Below it is a circular profile picture of the Golden Gate Bridge. The main heading is "Sign In". A red rectangular box highlights the login fields: "Username" with the value "robiswas@cisco.com" and "Password" with masked characters. Below the password field is a "Remember me" checkbox, which is unchecked. A blue "Sign In" button is positioned below the checkbox. At the bottom, there is a link that says "Need help signing in?".

成功した場合は、ログインしてFMCのデフォルトページを表示できます。

FMCで、[システム(System)] > [ユーザ(Users)]に移動し、データベースに追加されたSSOユーザを確認します。

Username	Real Name	Roles	Authentication Method	Password Lifetime	Enabled	Actions
admin		Administrator	Internal	Unlimited	<input checked="" type="checkbox"/>	
robiswas@cisco.com		Administrator	External (SSO)		<input checked="" type="checkbox"/>	