

Firepower Management Center Access via SSO-verificatie met Okta configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen en beperkingen](#)

[Configuratiestappen](#)

[Configuratiestappen op de Identity Provider \(Okta\)](#)

[Configuratiestappen op FMC](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u het FireSIGHT Management Center (FMC) kunt configureren om te bevestigen met behulp van Single Sign-On (SSO) voor beheertoegang.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basis begrip van single aanmelding en SAML
- Inzicht in de configuratie van de Identity Provider (iDP)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco Firepower Management Center (FMC) versie 6.7.0
- Okta als Identity Provider

Opmerking: de informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg ervoor dat u de potentiële impact van elke configuratie verandering begrijpt.

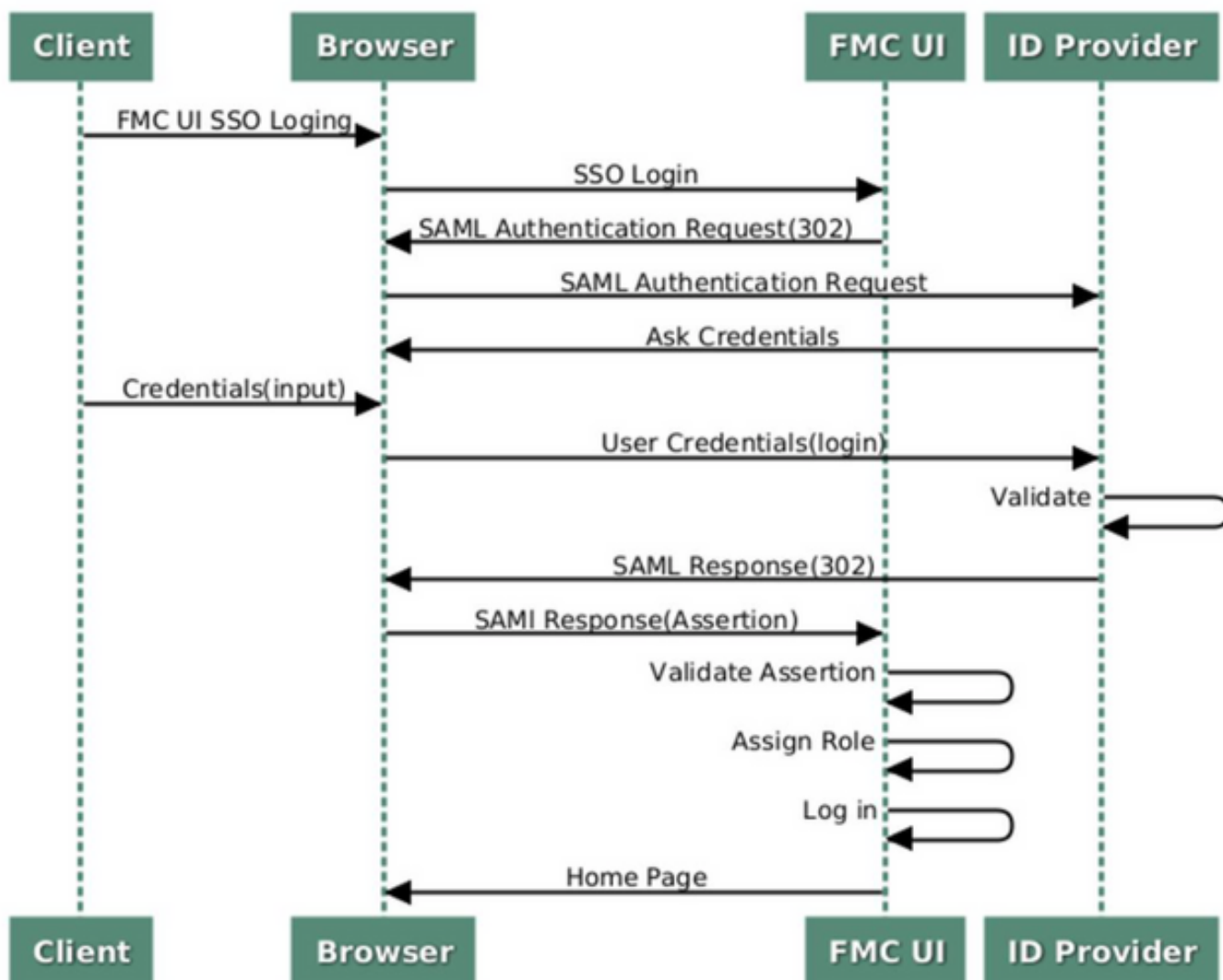
Achtergrondinformatie

Single Sign-on (SSO) is een eigenschap van identiteit en toegangsbeheer (IAM), die gebruikers in staat stelt om beveiligd te authenticeren met meerdere toepassingen en websites door slechts eenmaal in te loggen met één reeks aanmeldingsgegevens (gebruikersnaam en wachtwoord). Met SSO is de toepassing of website die de gebruiker probeert te bereiken afhankelijk van een vertrouwde derde om te controleren of de gebruikers zijn wie ze zeggen dat ze zijn.

SAML (Security Assertion Markup Language) is een op XML gebaseerd kader voor het uitwisselen van gegevens over authenticatie en autorisatie tussen veiligheidsdomeinen. Er wordt een vertrouwenscirkel gecreëerd tussen de gebruiker, een dienstverlener (SP) en een Identity Provider (IDP) waardoor de gebruiker op één moment voor meerdere diensten kan tekenen

Een serviceprovider (SP) is een entiteit die een door een Identity Provider (iDP) afgegeven verklaring van echtheidscontrole ontvangt en accepteert. Zoals door hun namen wordt beschreven, bieden dienstverleners diensten aan terwijl identiteitsaanbieders de identiteit van gebruikers verschaffen (authenticatie).

SSO SAML Workflow



Deze iDP's worden ondersteund en getest op authenticatie:

- Okta
- OneLogin
- PingID

- AD
- Overige (elke iDP die voldoet aan SAML 2.0)

Opmerking: Geen nieuwe vergunning vereist. Deze optie werkt onder licentie en in de evaluatiemodus.

Beperkingen en beperkingen

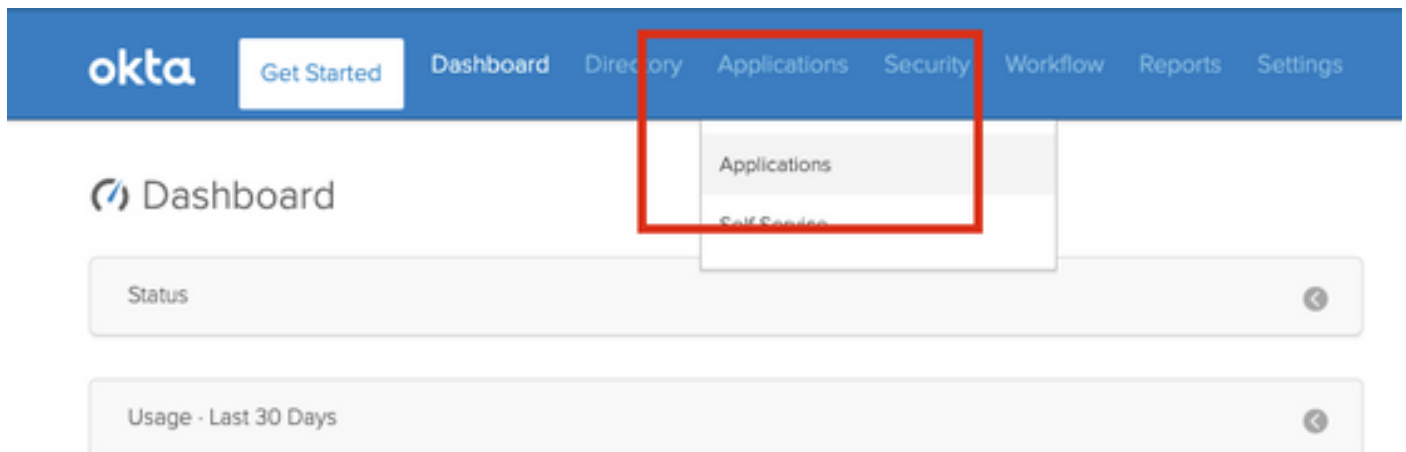
Dit zijn bekende beperkingen en beperkingen voor SSO-authenticatie voor FMC-toegang:

- SSO kan alleen worden ingesteld voor het Global Domain
- FMC's in HA-paar moeten individueel worden geconfiguren
- Alleen lokale/AD-managers kunnen de SSO op FMC configureren (SSO-beheergebruikers kunnen geen SSO-instellingen op FMC configureren of bijwerken).

Configuratiestappen

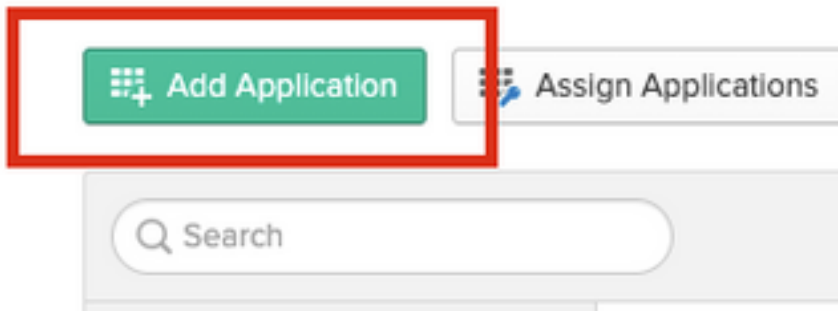
Configuratiestappen op de Identity Provider (Okta)

Stap 1. Meld u aan bij het Okta-portaal. Navigeer naar **Toepassingen > Toepassingen**, zoals in deze afbeelding.



Stap 2. Zoals in deze afbeelding, klik op **AddApplication**.

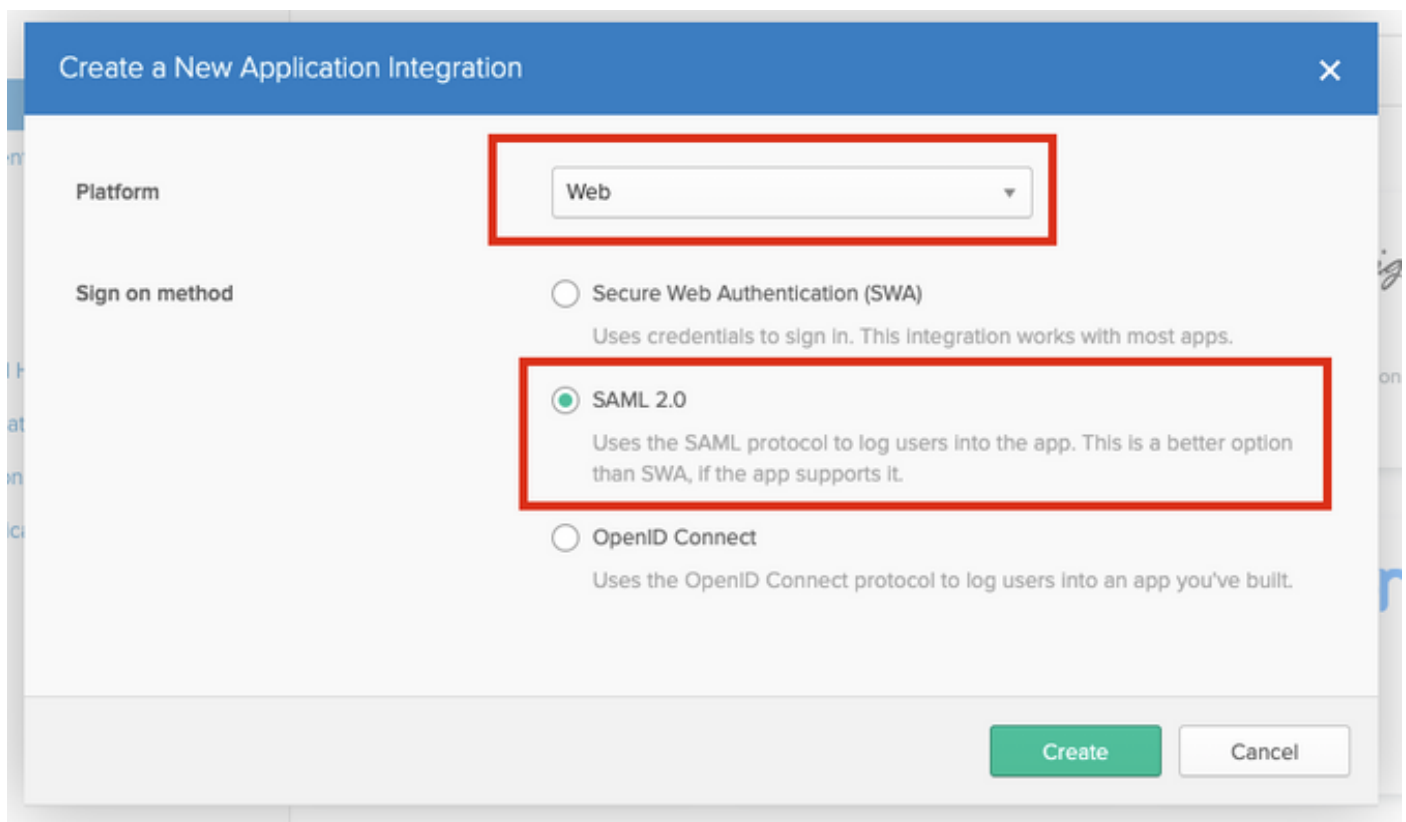
Applications



Stap 3. Zoals in deze afbeelding, klik op **Create NewApp**.



Stap 4. Kies het **platform** als **web**. Kies de **inlogmethode** als **SAML 2.0**. Klik op **Maken**, zoals in deze afbeelding.




Stap 5. Geef een **naam** van de **app**, **App-logo** (optioneel), en klik op **Volgende**, zoals in deze afbeelding.

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

Stap 6. Voer de **SAML-instellingen** in.

Enkelvoudig teken op URL: `https://<fmc URL>/saml/acs`

Publiek URI (SP Entiteit ID): `https://<fmc URL>/saml/metadata`

Standaard RelayState: `/ui/aanmelding`

A SAML Settings

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

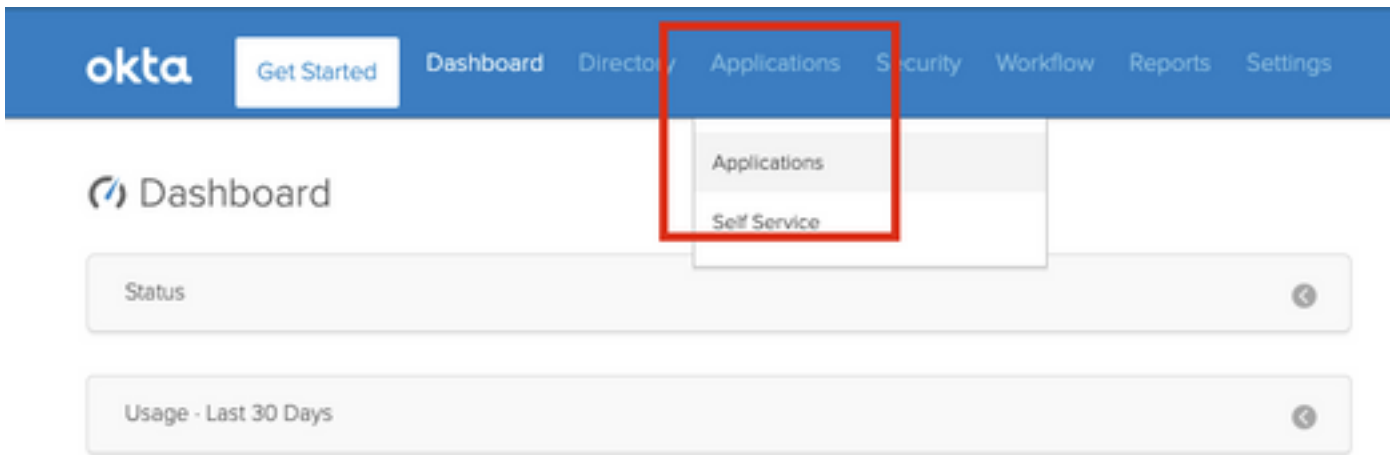
Name format (optional)

Value

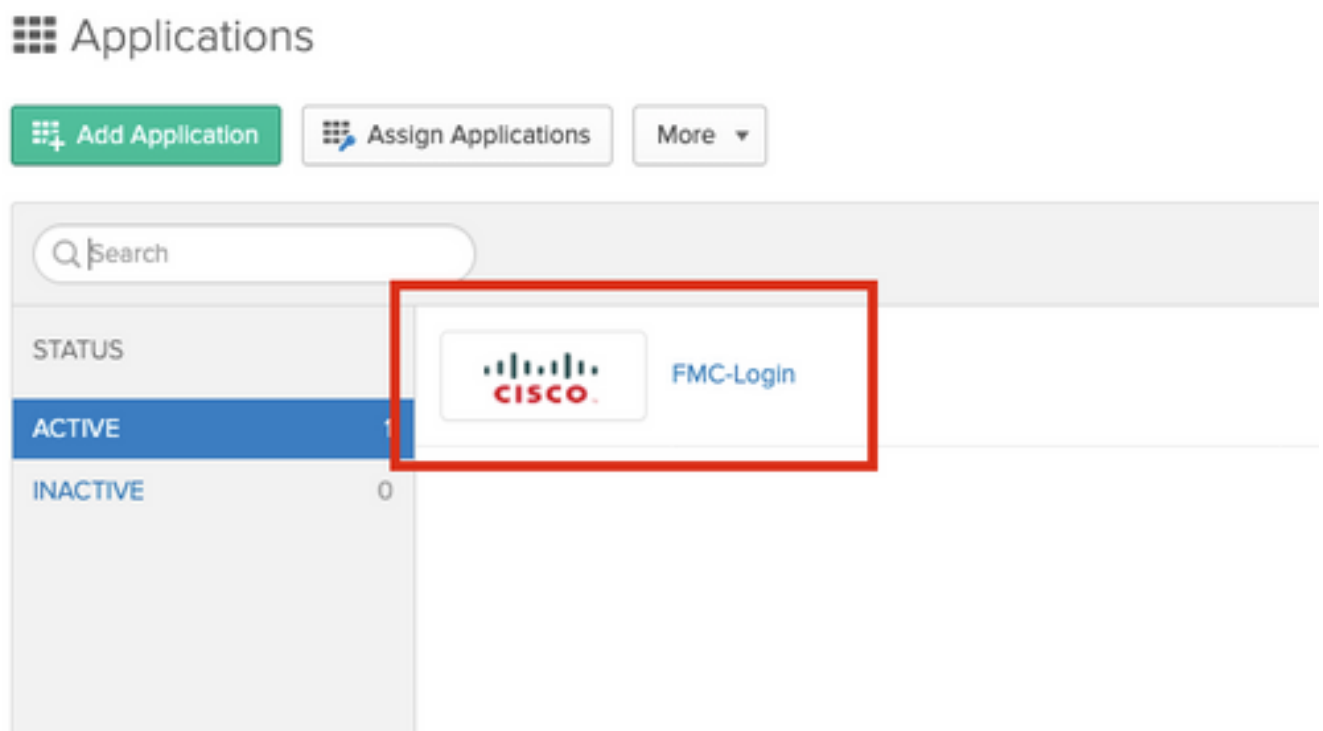
Unspecified

[Add Another](#)

Stap 7. Navigeer terug naar **Toepassingen > Toepassingen**, zoals in deze afbeelding.



Stap 8. Klik op de App-naam die is gemaakt.




Stap 9. Navigeer naar opdrachten. Klik op Toewijzen.

U kunt ervoor kiezen afzonderlijke gebruikers of groepen toe te wijzen aan de App-naam die gemaakt is.

General Sign On Import **Assignments**


Assign Convert Assignments Search... People

FILTERS

Person	Type
 Rohan Biswas robiswas@cisco.com	Individual

Stap 10. Navigeer om **aan te tekenen**. Klik op **Instellen-instructies bekijken**. Klik op de **metagegevens van Identity Provider** om de iDP-metagegevens te bekijken.

← 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

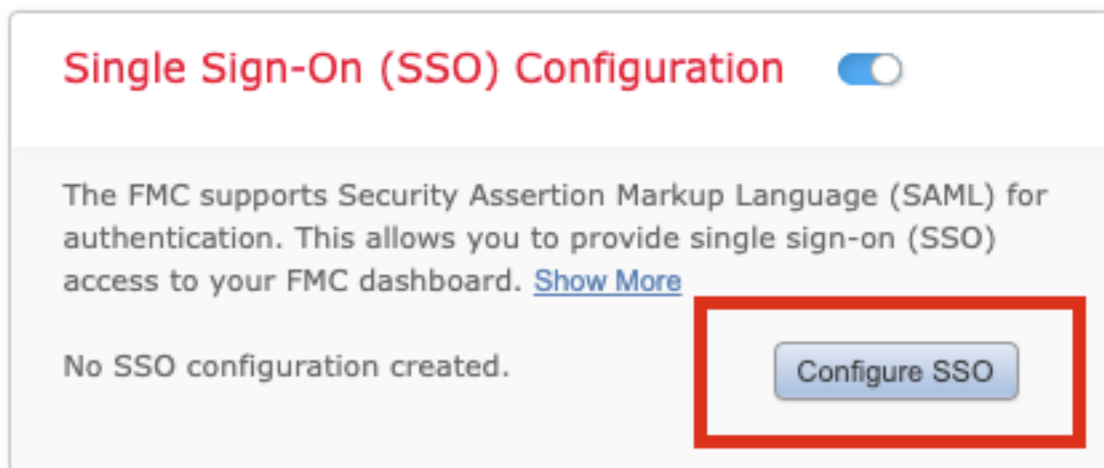
Default Relay State ui/login

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

[View Setup Instructions](#)

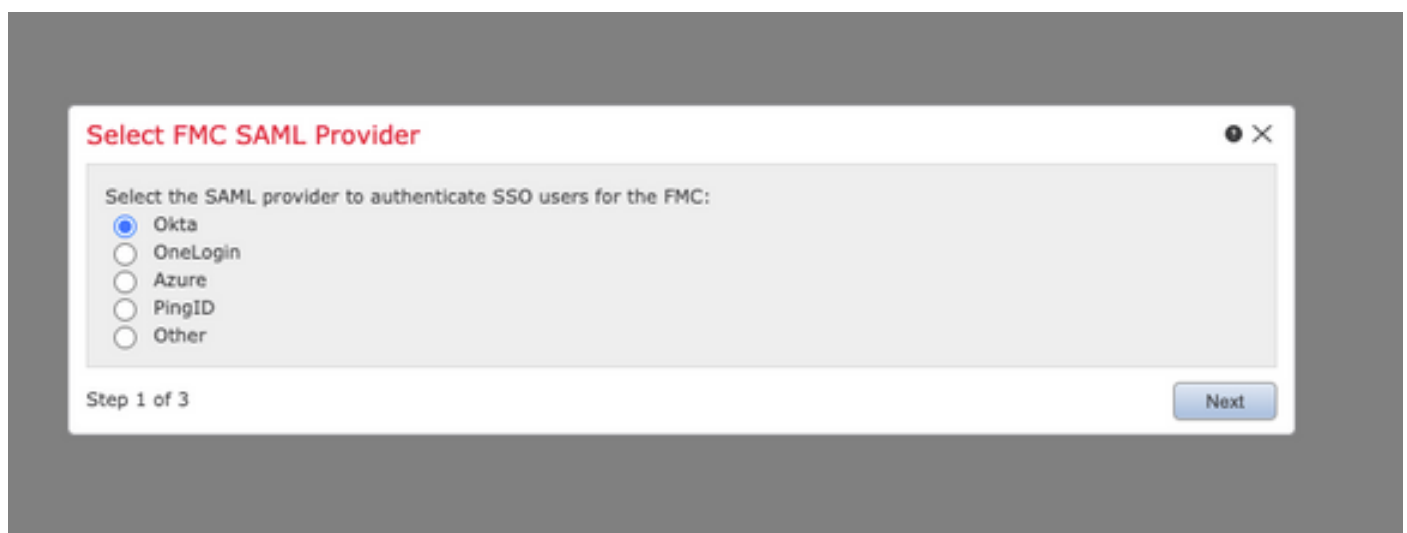
[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Sla het bestand op als een bestand .xml dat op het FMC moet worden gebruikt.

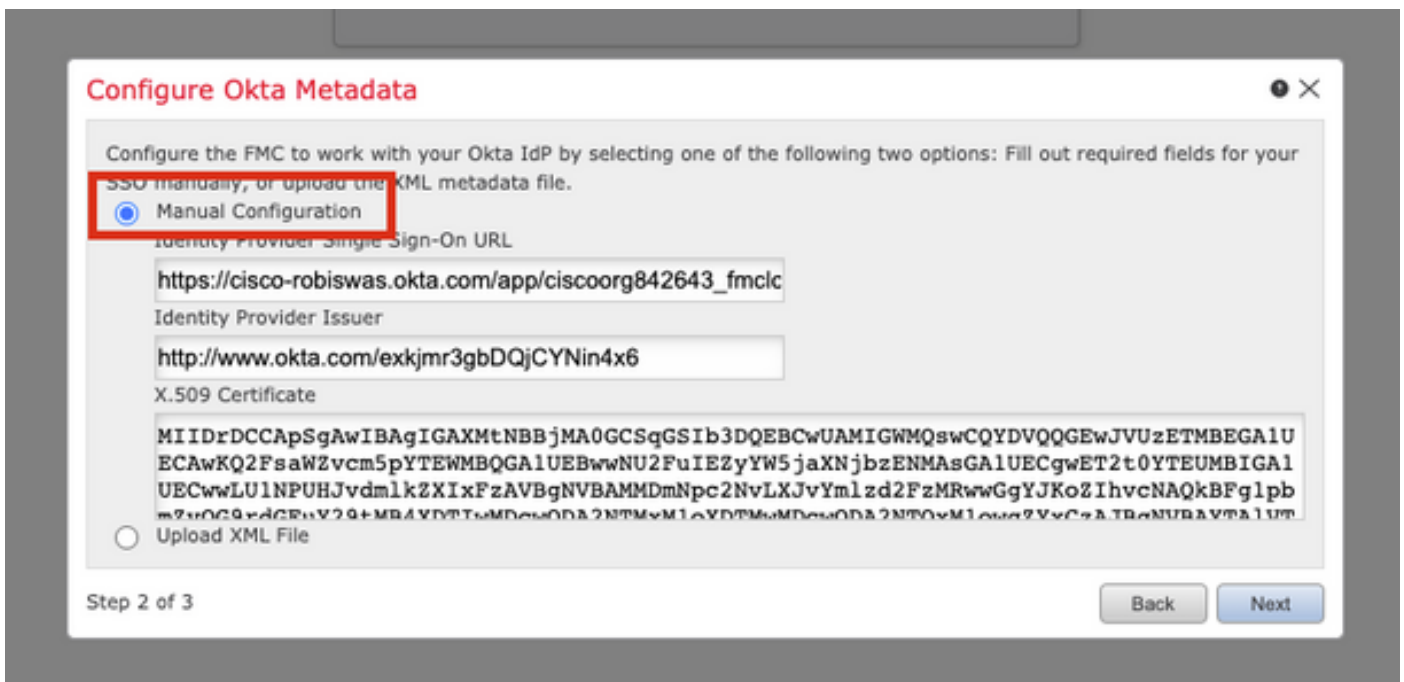


Stap 5. Selecteer de **FMC SAML Provider**. Klik op **Volgende**.

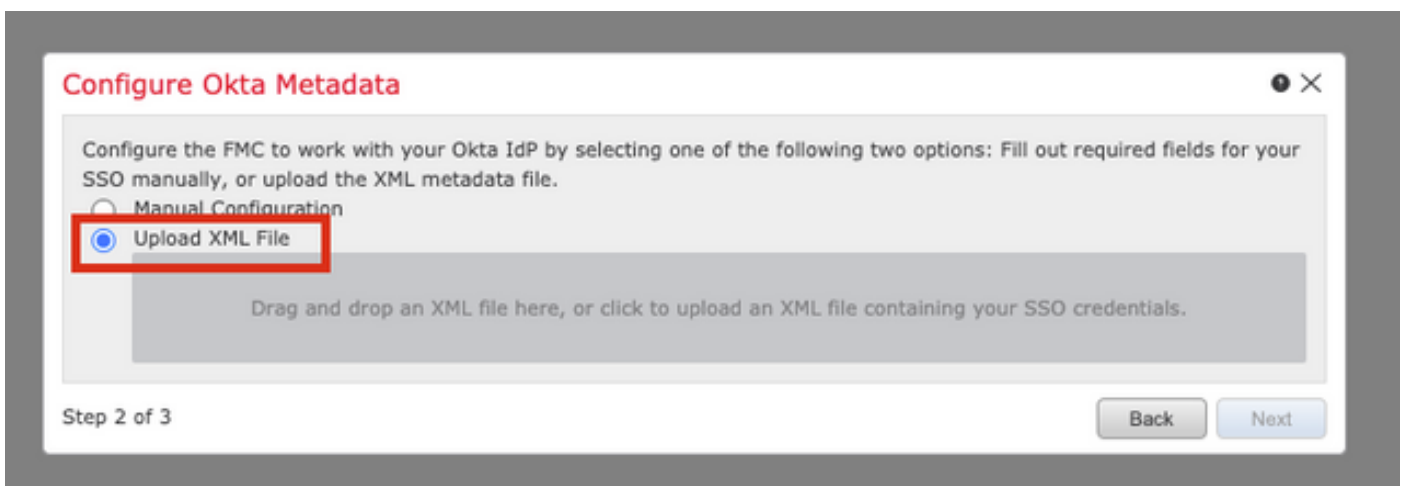
Voor deze demonstratie wordt **Okta** gebruikt.



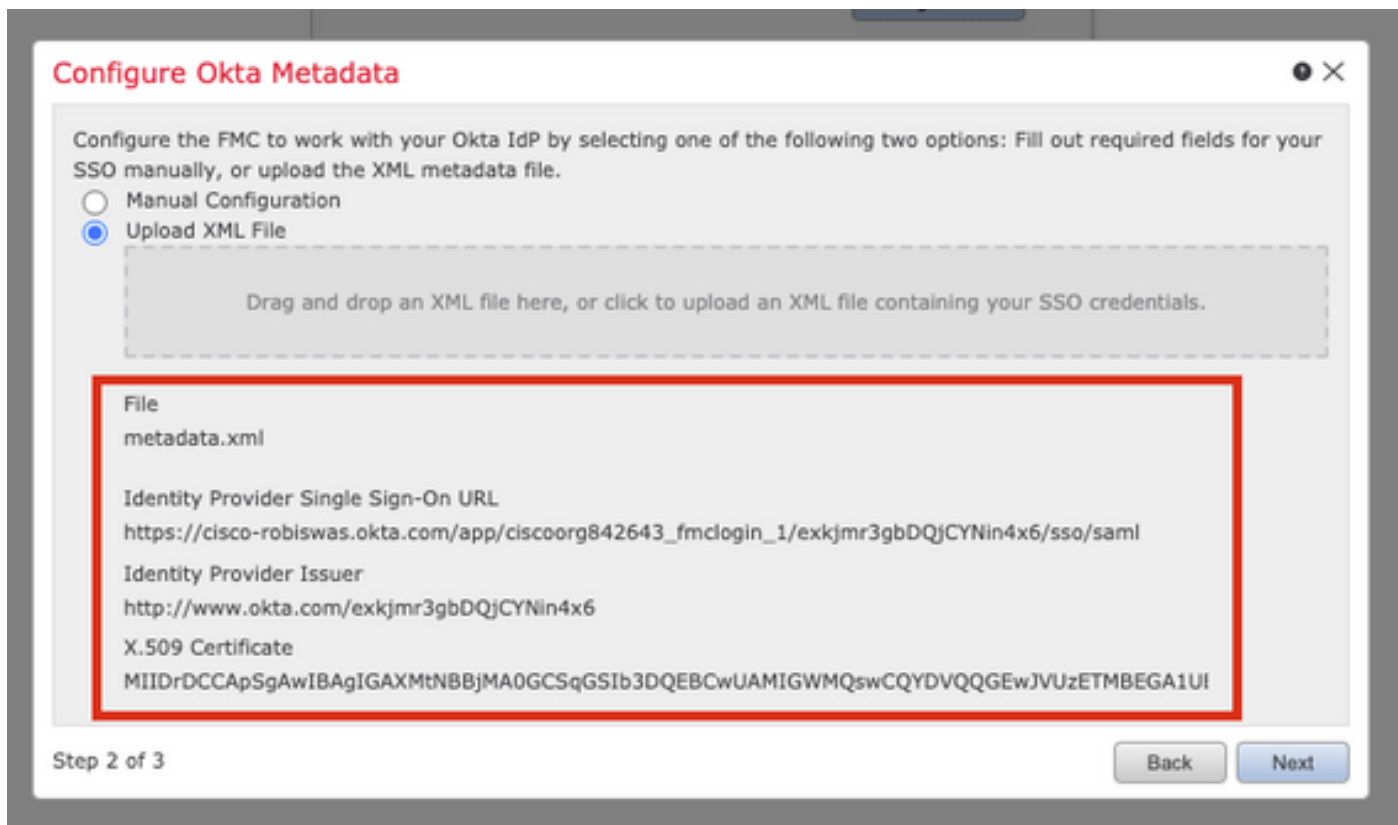
Stap 6. U kunt **Handmatige configuratie** kiezen en de iDP-gegevens handmatig invoeren. Klik op **Volgende**, zoals



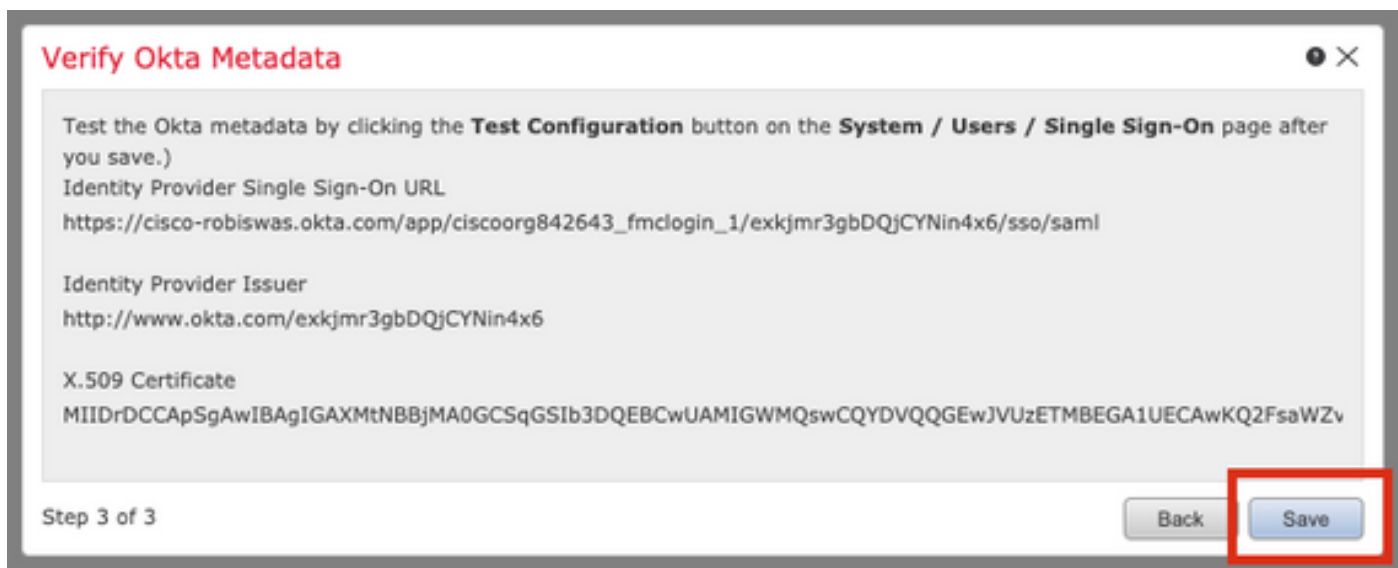
U kunt ook het XML-bestand uploaden en het XML-bestand uploaden dat u in [Stap 10](#) van de Okta-configuratie hebt opgeroepen.



Zodra het bestand is geüpload, geeft het FMC de metagegevens weer. Klik op **Volgende**, zoals in deze afbeelding weergegeven.



Stap 7. **Controleer** de metagegevens. Klik op **Opslaan**, zoals in deze afbeelding.



Stap 8. Configureer de rol van de gebruiker in kaart brengen/standaardinstellen bij geavanceerde configuratie.

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

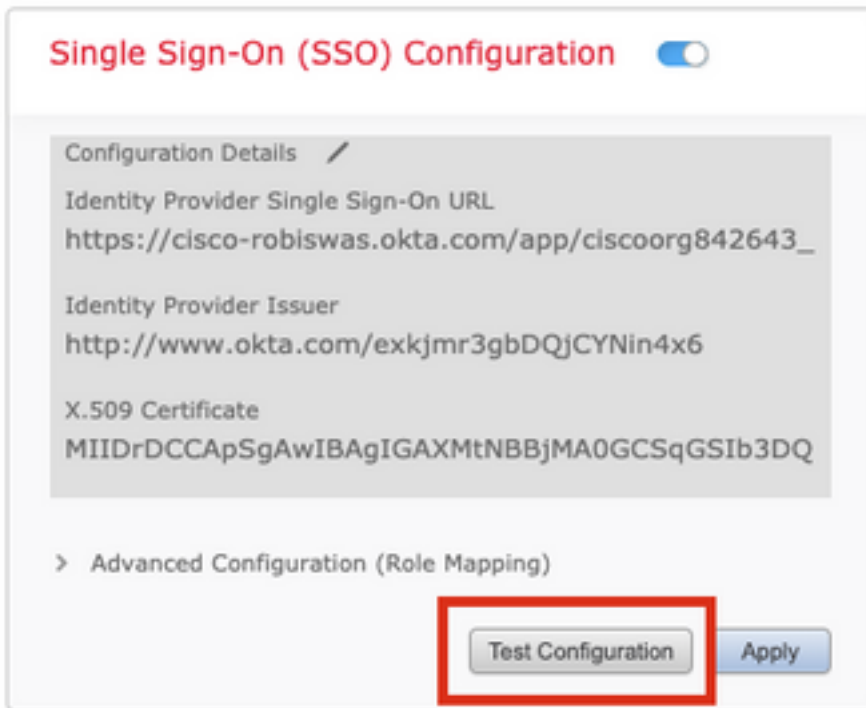
Security Analyst

Security Analyst (Read Only)

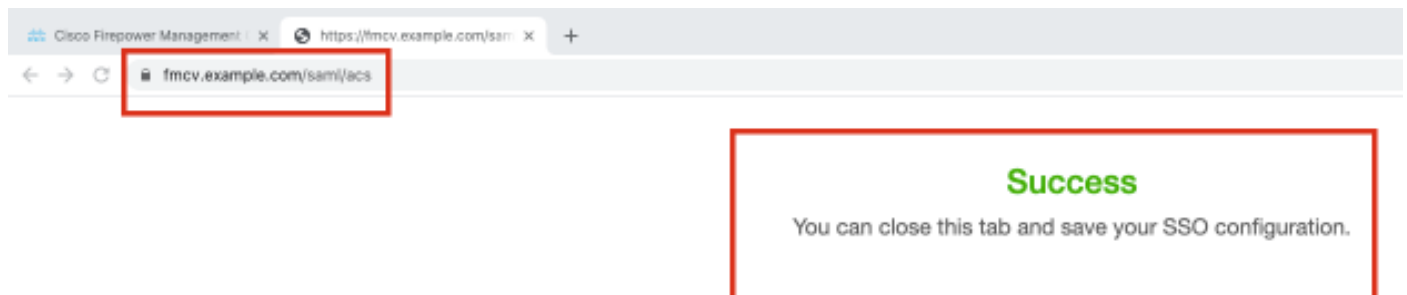
Security Approver

Threat Intelligence Director (TID) User

Stap 9. Klik om de configuratie te testen op **Test Configuration**, zoals in deze afbeelding.



Als de test een succes is, zou u de pagina moeten zien die in deze afbeelding wordt getoond, op een nieuw tabblad in de browser.



Stap 10. Klik op **Toepassen** om de configuratie op te slaan.

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 moet worden ingeschakeld.

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

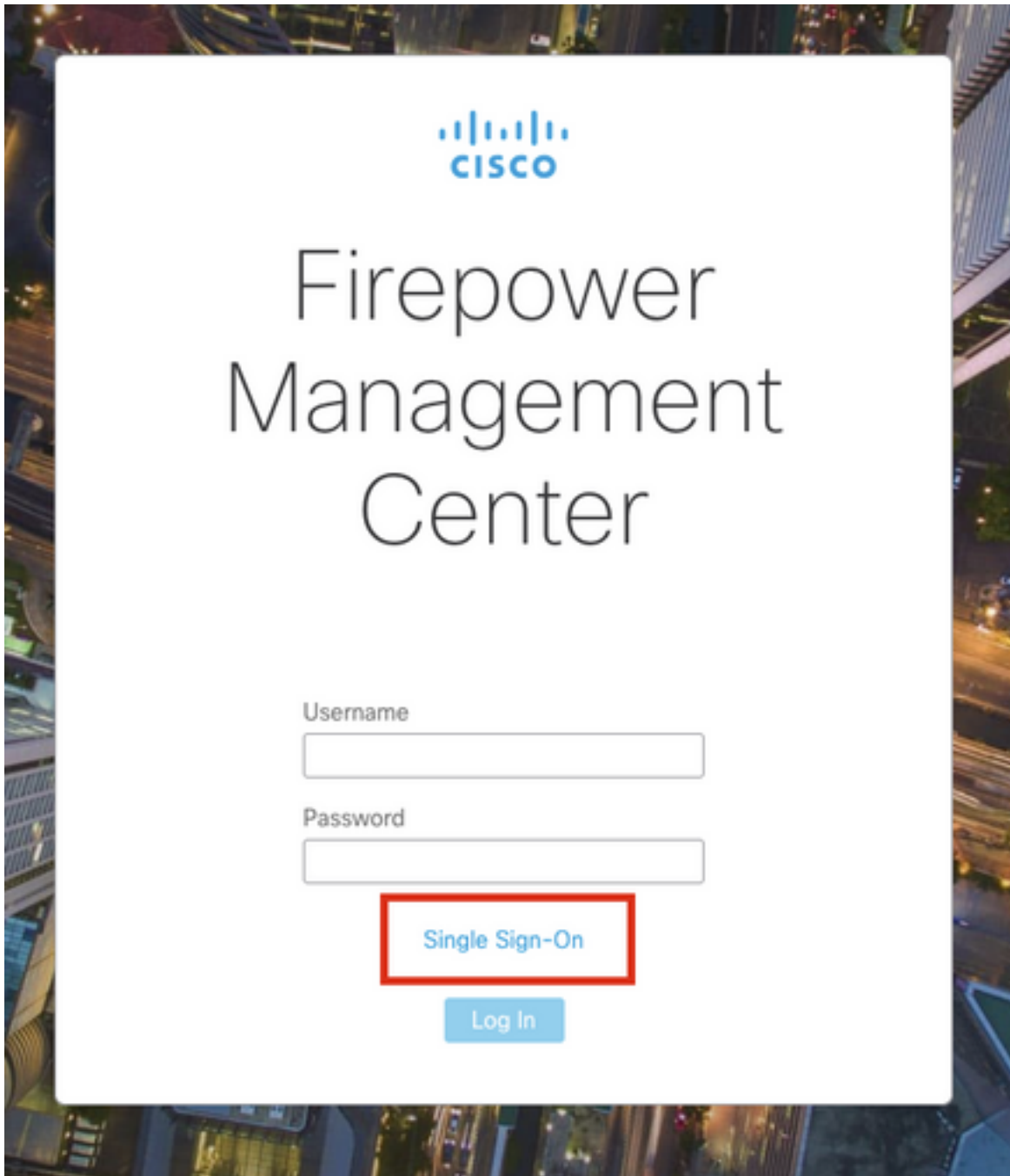
> Advanced Configuration (Role Mapping)

Test Configuration Apply

Verifiëren


Navigeer naar de FMC URL van uw browser: <https://<fmc URL>>. Klik op **Enkelvoudige**

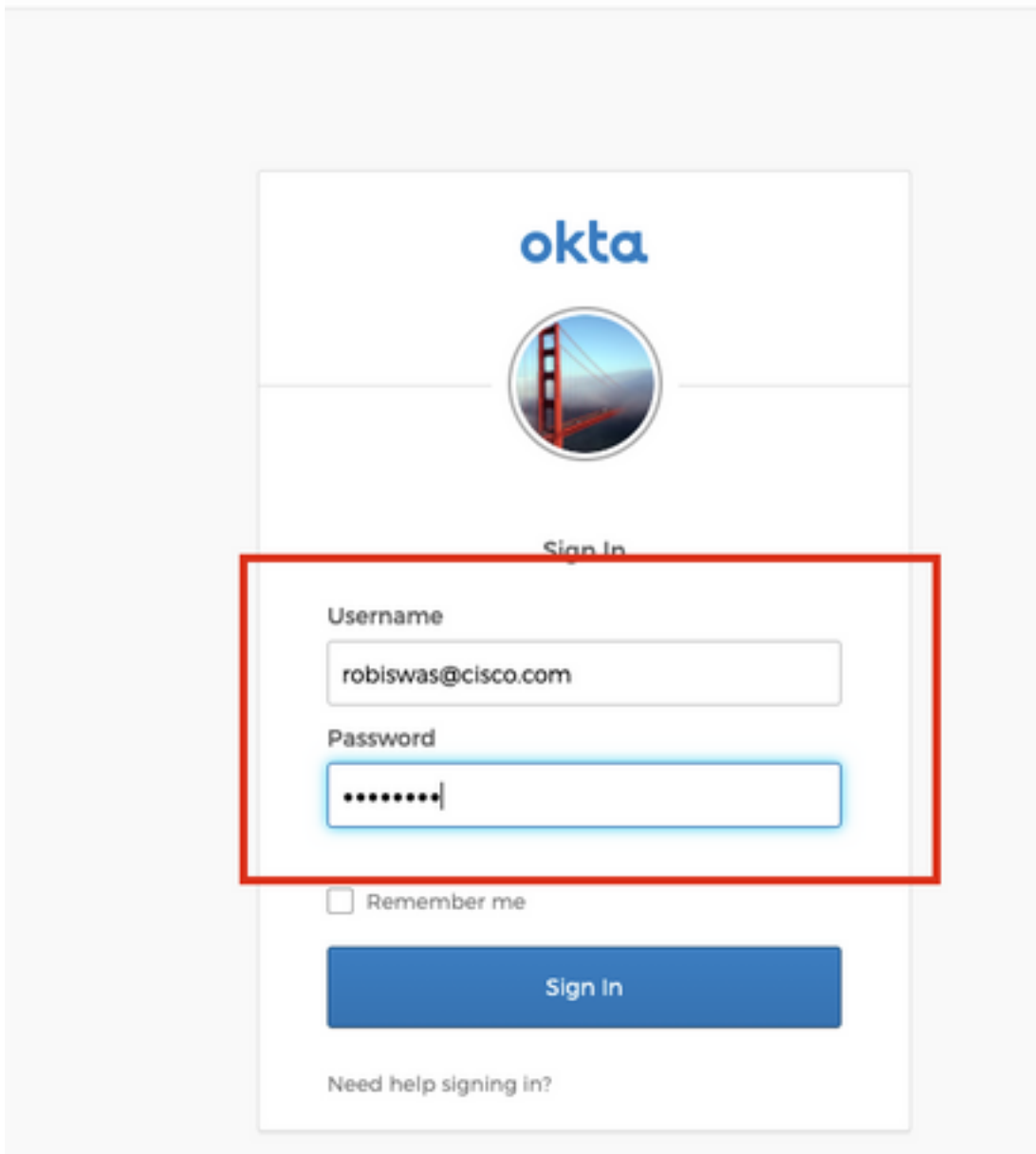
aanmelding.



The image shows the login page for the Cisco Firepower Management Center. At the top center is the Cisco logo, consisting of a stylized bridge icon above the word "CISCO". Below the logo, the text "Firepower Management Center" is displayed in a large, dark grey font. Underneath the title, there are two input fields: "Username" and "Password". Below the password field, there is a blue button labeled "Single Sign-On" which is highlighted with a red rectangular border. At the bottom of the form area, there is another blue button labeled "Log In". The entire form is set against a white background with a cityscape at night visible in the background.

U wordt terugverwezen naar de logpagina iDP (Okta). Geef uw SSO-gegevens op. Klik op **Inloggen**.

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



The image shows an Okta login page. At the top, it says "Connecting to" followed by the Cisco logo and "Sign-in with your cisco-org-842643 account to access FMC-Login". Below this is the Okta logo and a circular profile picture of the Golden Gate Bridge. The main form is titled "Sign In" and contains the following fields:

- Username:** robiswas@cisco.com
- Password:** [masked with dots]
- Remember me
- Sign In** button
- [Need help signing in?](#)

Indien geslaagd, zou u in staat moeten zijn om in te loggen en de standaardpagina van FMC te zien.

Op FMC, navigeer naar **Systeem > Gebruikers** om de SSO-gebruiker aan de database te zien toevoegen.

Username	Real Name	Roles	Authentication Method	Password Lifetime	Enabled	Actions
admin		Administrator	Internal	Unlimited		
robiswas@cisco.com		Administrator	External (SSO)			