

Configurer l'accès à Firepower Management Center via l'authentification SSO avec Okta

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Limitations et restrictions](#)

[Configuration Steps](#)

[Étapes de configuration sur le fournisseur d'identité \(Okta\)](#)

[Étapes de configuration sur FMC](#)

[Vérification](#)

Introduction

Ce document décrit comment configurer Firepower Management Center (FMC) pour l'authentification à l'aide de l'authentification unique (SSO) pour l'accès à la gestion.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base de l'authentification unique et de SAML
- Présentation de la configuration sur le fournisseur d'identité (iDP)

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Management Center (FMC) version 6.7.0
- Okta en tant que fournisseur d'identité

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute modification de configuration.

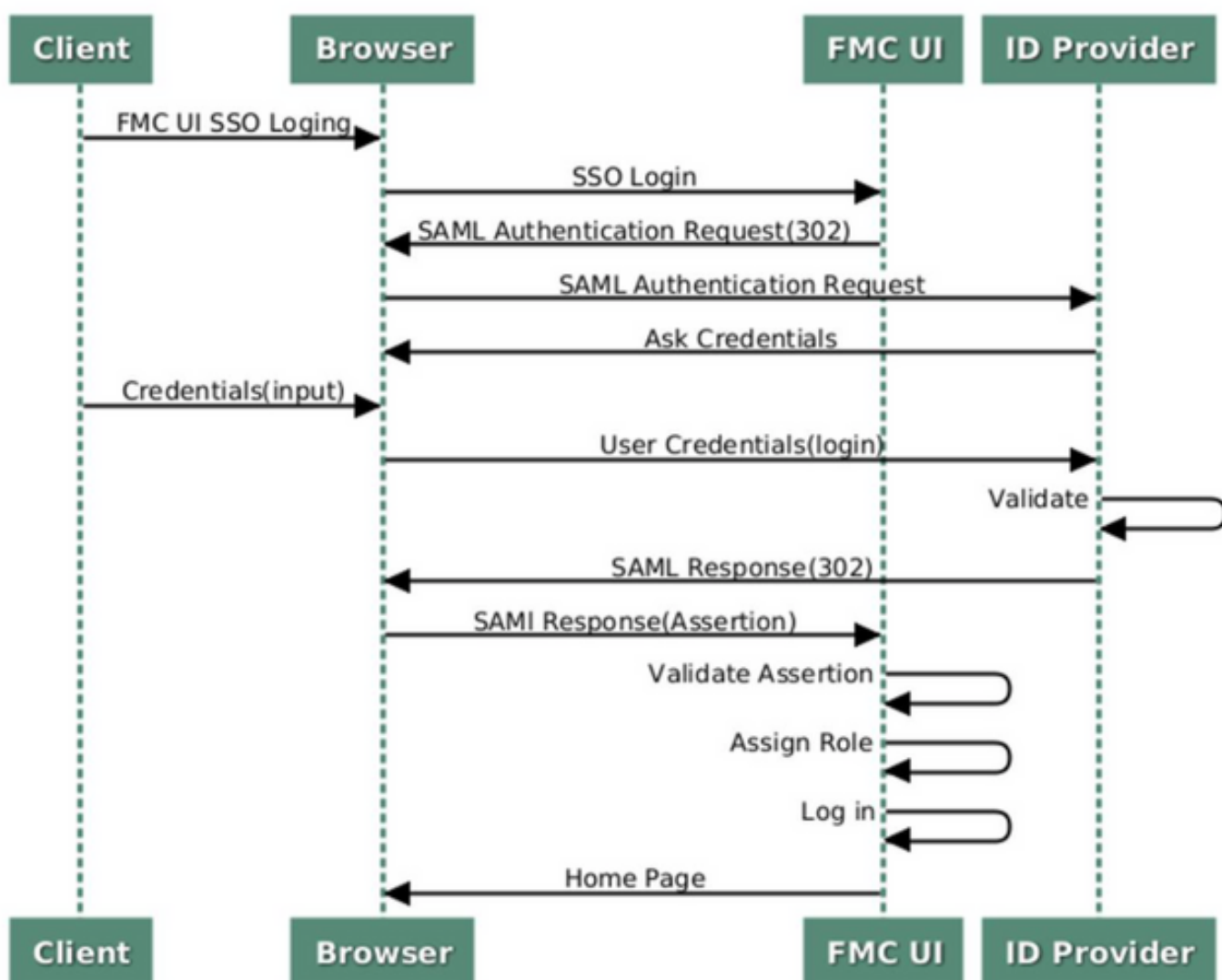
Informations générales

L'authentification unique (SSO) est une propriété de gestion des identités et des accès (IAM) qui permet aux utilisateurs de s'authentifier en toute sécurité avec plusieurs applications et sites Web en se connectant une seule fois avec un seul ensemble d'informations d'identification (nom d'utilisateur et mot de passe). Avec SSO, l'application ou le site Web auquel l'utilisateur tente d'accéder dépend d'un tiers de confiance pour vérifier que les utilisateurs sont ceux qu'ils disent être.

SAML (Security Assertion Markup Language) est un cadre XML permettant d'échanger des données d'authentification et d'autorisation entre des domaines de sécurité. Il crée un cercle de confiance entre l'utilisateur, un fournisseur de services (SP) et un fournisseur d'identité (IdP) qui permet à l'utilisateur de se connecter à une seule heure pour plusieurs services

Un fournisseur de services (SP) est une entité qui reçoit et accepte une assertion d'authentification émise par un fournisseur d'identité (iDP). Comme l'indiquent leurs noms, les fournisseurs de services fournissent des services tandis que les fournisseurs d'identité fournissent l'identité des utilisateurs (authentification).

SSO SAML Workflow



Ces iDP sont pris en charge et testés pour l'authentification :

- Okta
- OneLogin

- PingID
- Azure AD
- Autres (tout iDP conforme à SAML 2.0)

Remarque : Aucune nouvelle licence n'est requise. Cette fonctionnalité fonctionne en mode licence et évaluation.

Limitations et restrictions

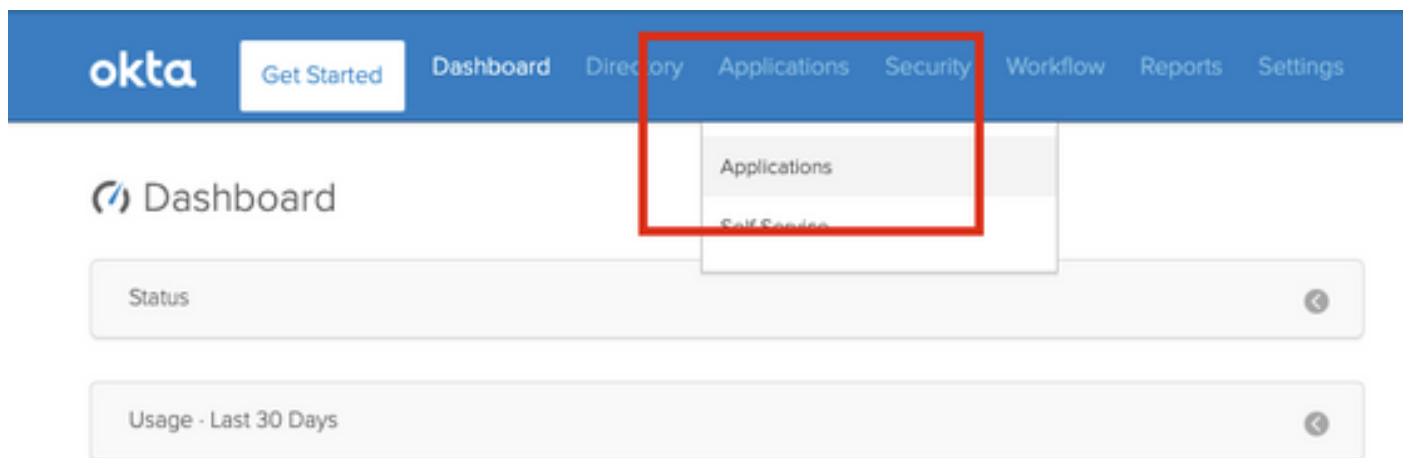
Voici les limitations et restrictions connues pour l'authentification SSO pour l'accès FMC :

- SSO ne peut être configuré que pour le domaine global
- La paire FMC en HA nécessite une configuration individuelle
- Seuls les administrateurs locaux/AD peuvent configurer SSO sur FMC (les utilisateurs de l'administrateur SSO ne pourront pas configurer/mettre à jour les paramètres SSO sur FMC).

Configuration Steps

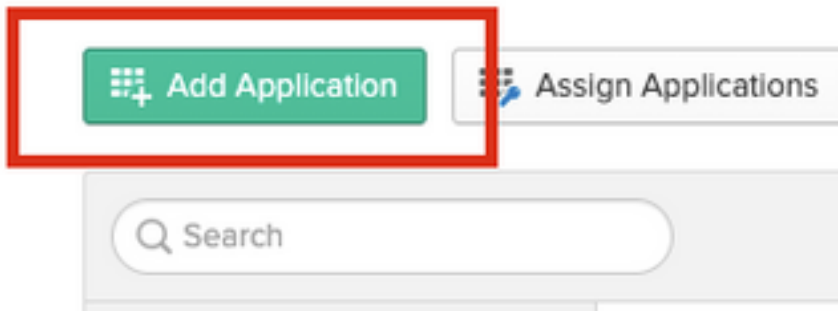
Étapes de configuration sur le fournisseur d'identité (Okta)

Étape 1. Connectez-vous au portail Okta. Accédez à **Applications > Applications**, comme illustré dans cette image.



Étape 2. Comme le montre cette image, cliquez sur **AddApplication**.

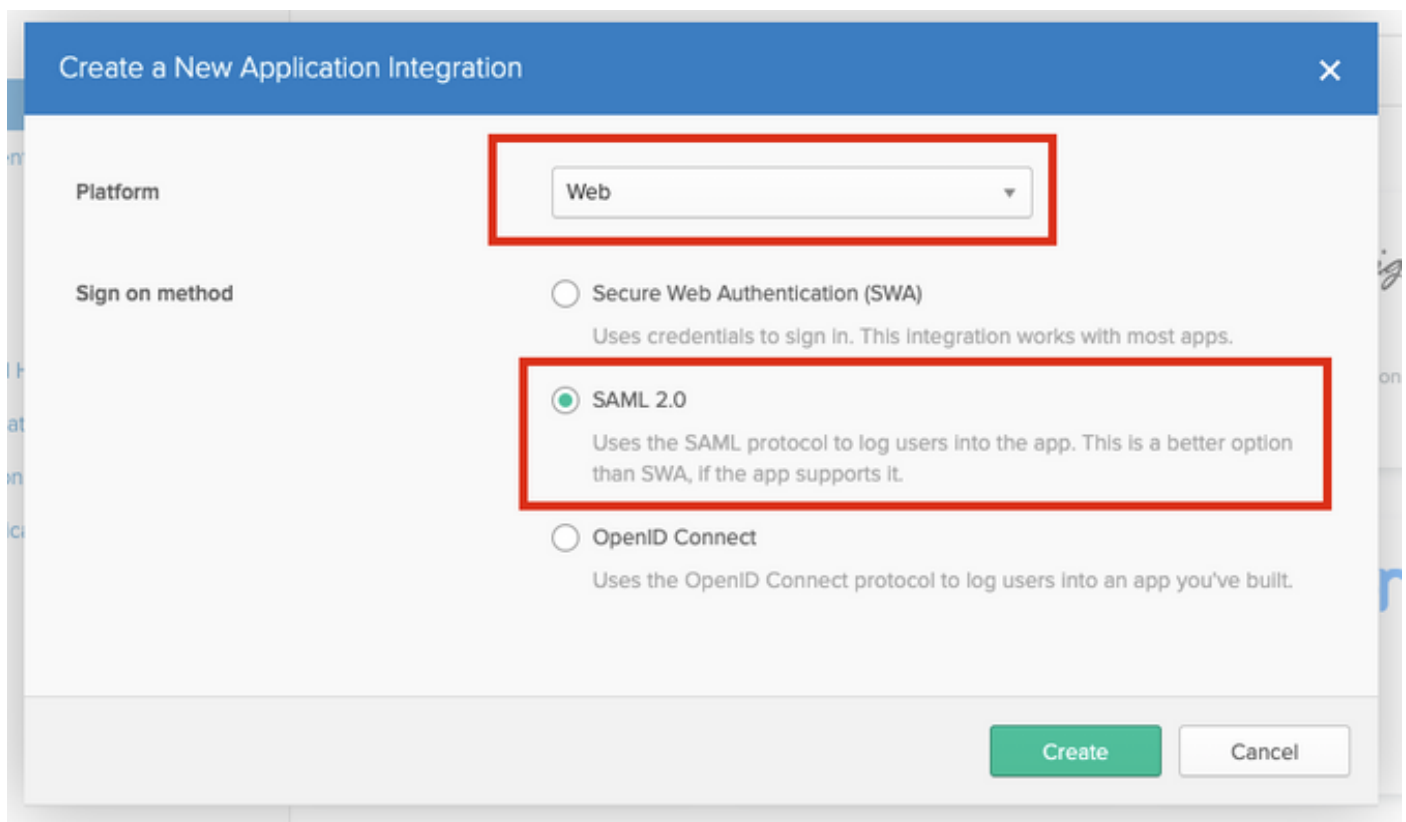
Applications



Étape 3. Comme le montre cette image, cliquez sur **Create NewApp**.



Étape 4. Sélectionnez la **plate-forme** en tant que **Web**. Choisissez la **méthode Sign On** en tant que **SAML 2.0**. Cliquez sur **Créer**, comme illustré dans cette image.




Étape 5. Indiquez un **nom d'application**, un **logo d'application (facultatif)**, puis cliquez sur **Suivant**, comme indiqué dans cette image.

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

Étape 6. Entrez les **paramètres SAML**.

URL de connexion unique : `https://<URL fmc>/saml/acs`

URI d'audience (ID d'entité SP) : `https://<URL fmc>/saml/métadonnées`

État de relais par défaut : `/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](#)

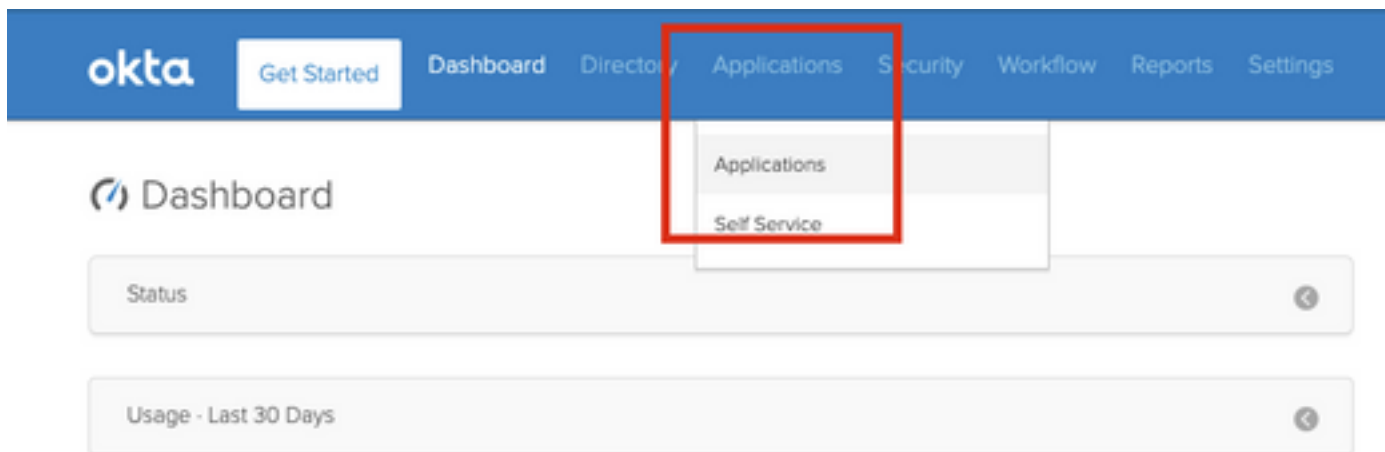
Name

Name format (optional)

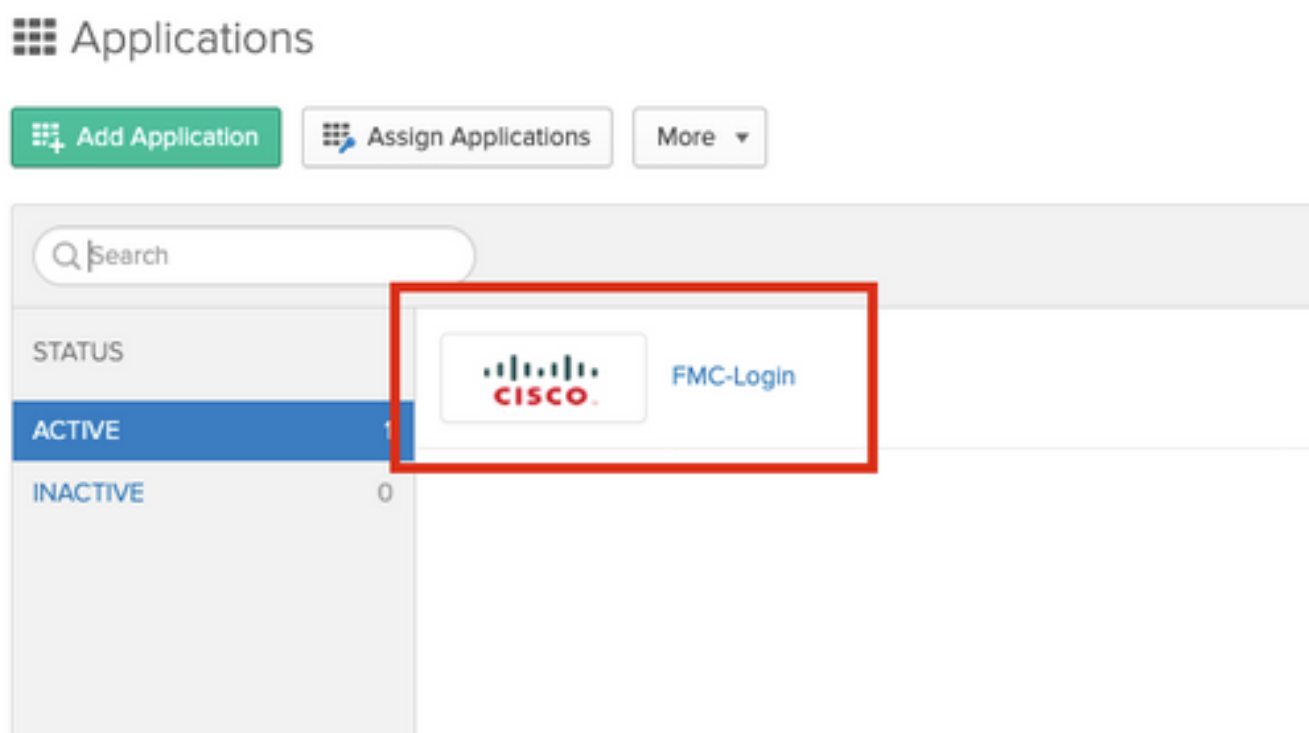
Value

[Add Another](#)

Étape 7. Revenez à **Applications > Applications**, comme illustré dans cette image.

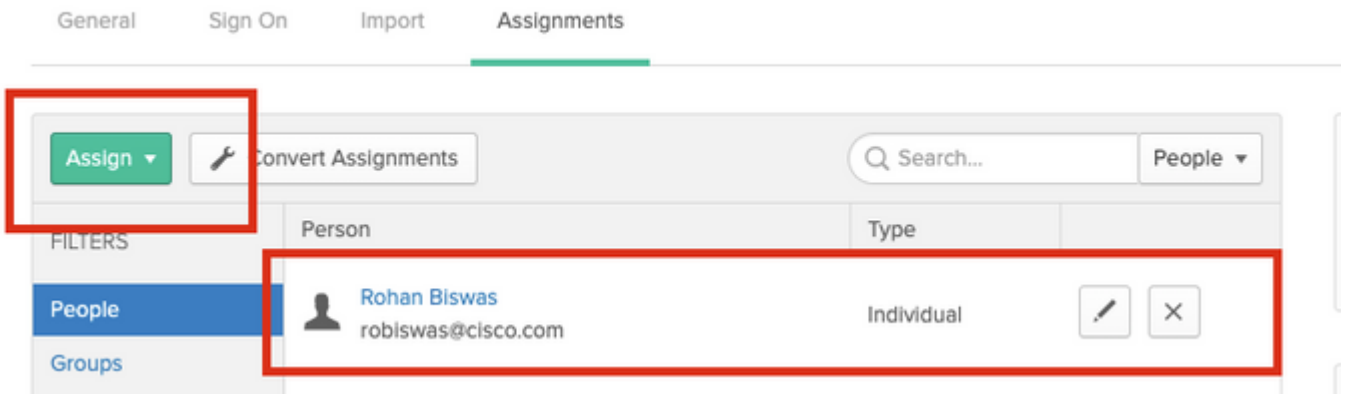


Étape 8. Cliquez sur le nom de l'application qui a été créé.

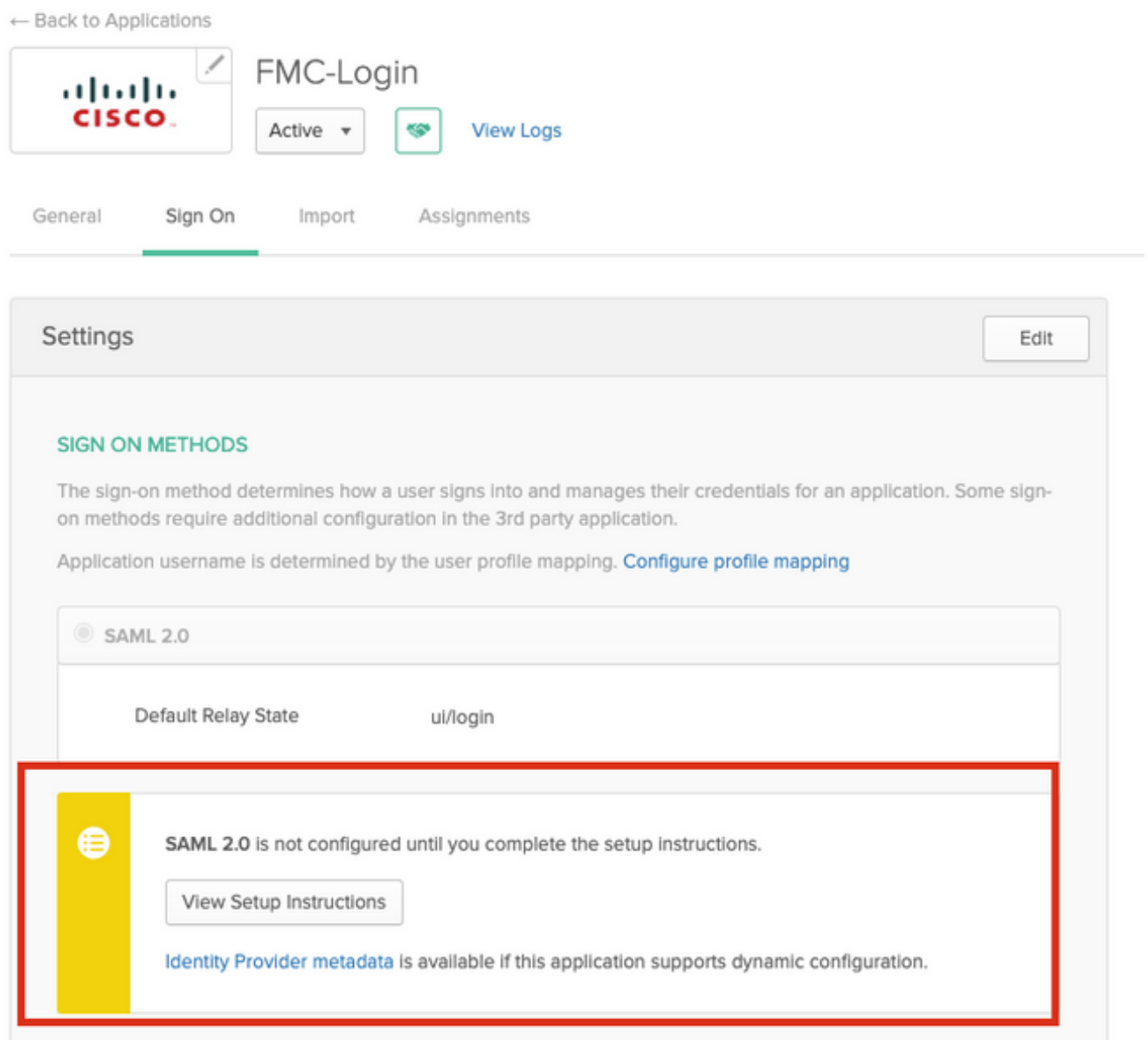


Étape 9. Accédez à **Affectations**. Cliquez sur **Affecter**.

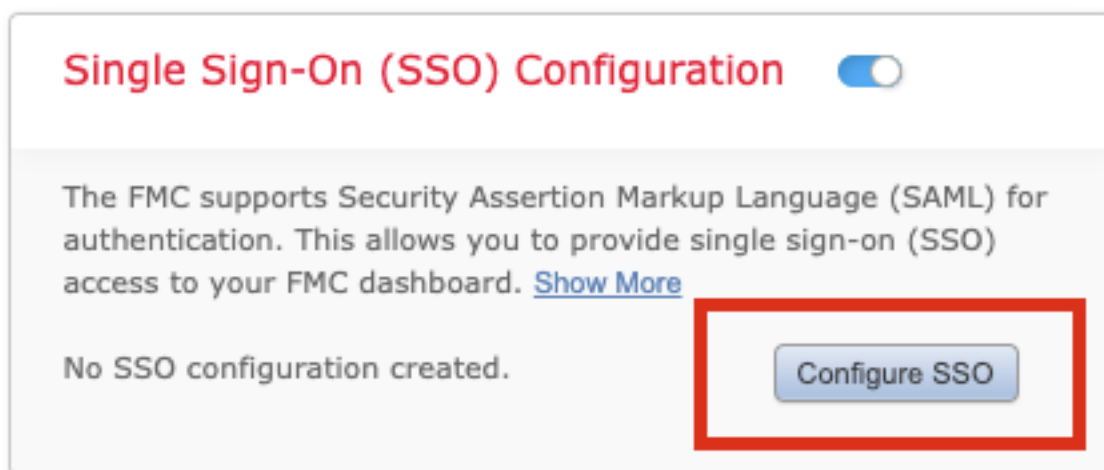
Vous pouvez choisir d'affecter des utilisateurs ou des groupes individuels au nom d'application créé.



Étape 10. Accédez à **Connexion**. Cliquez sur **Afficher les instructions de configuration**. Cliquez sur **les métadonnées du fournisseur d'identité** pour afficher les métadonnées de l'iDP.



Enregistrez le fichier en tant que fichier **.xml** à utiliser sur le FMC.

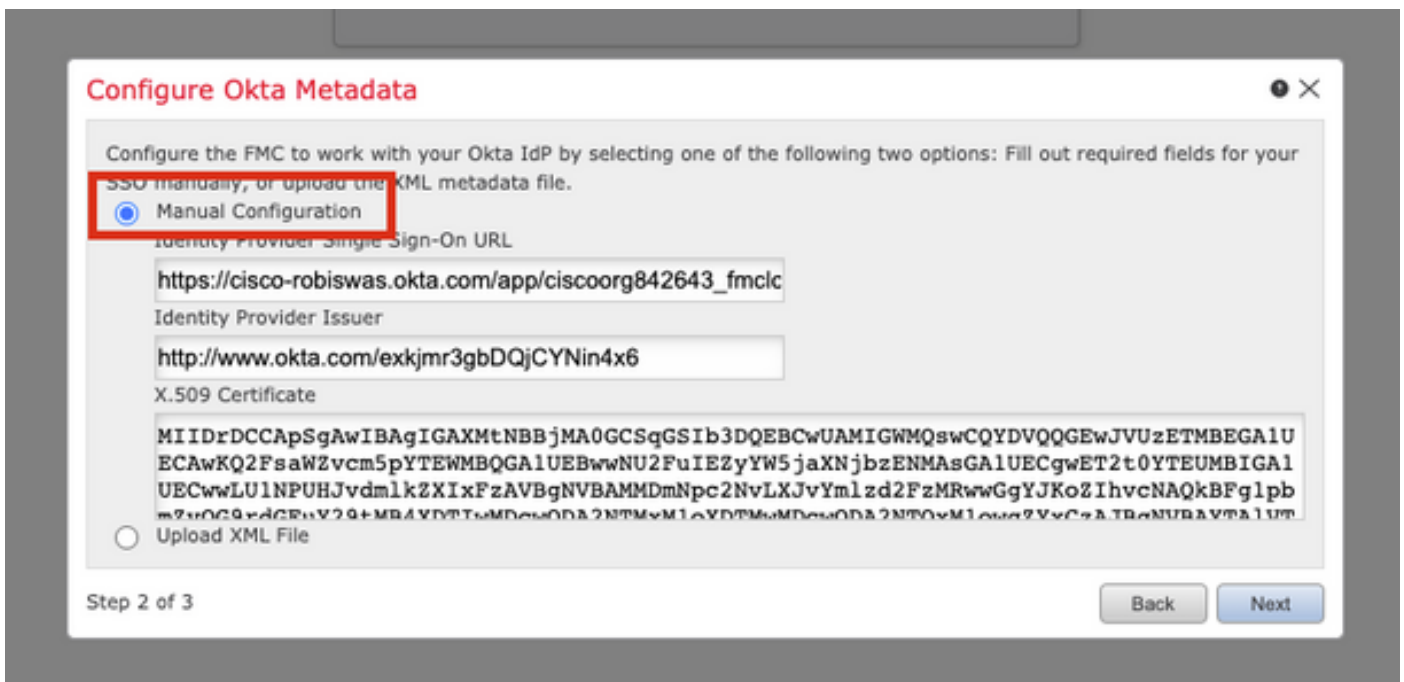


Étape 5. Sélectionnez le **fournisseur SAML FMC**. Cliquez sur Next (Suivant).

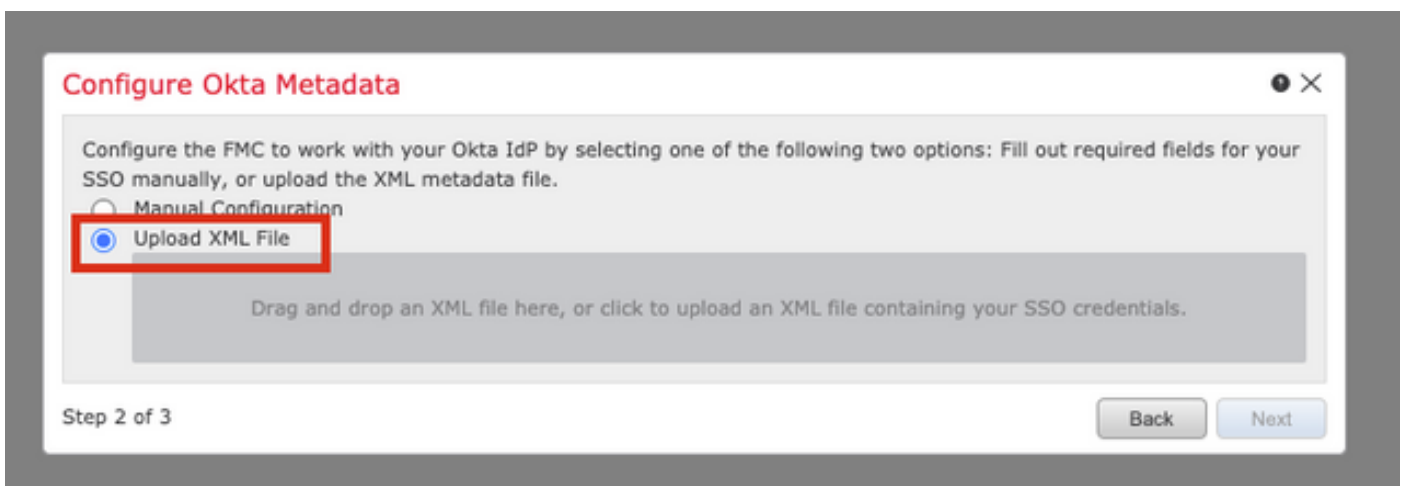
Aux fins de cette démonstration, **Okta** est utilisé.



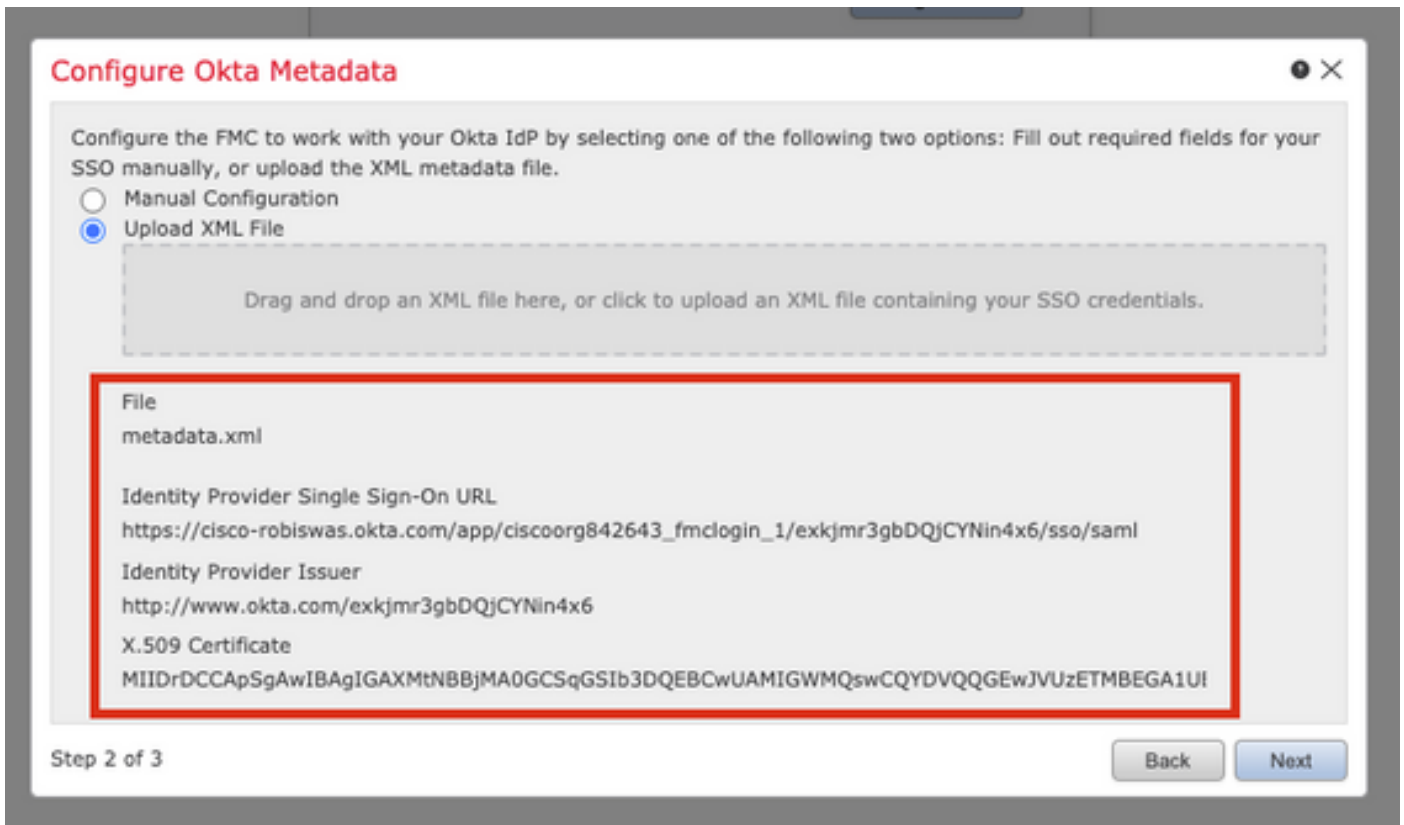
Étape 6. Vous pouvez choisir **Configuration manuelle** et saisir les données iDP manuellement. Cliquez sur **Suivant**, comme



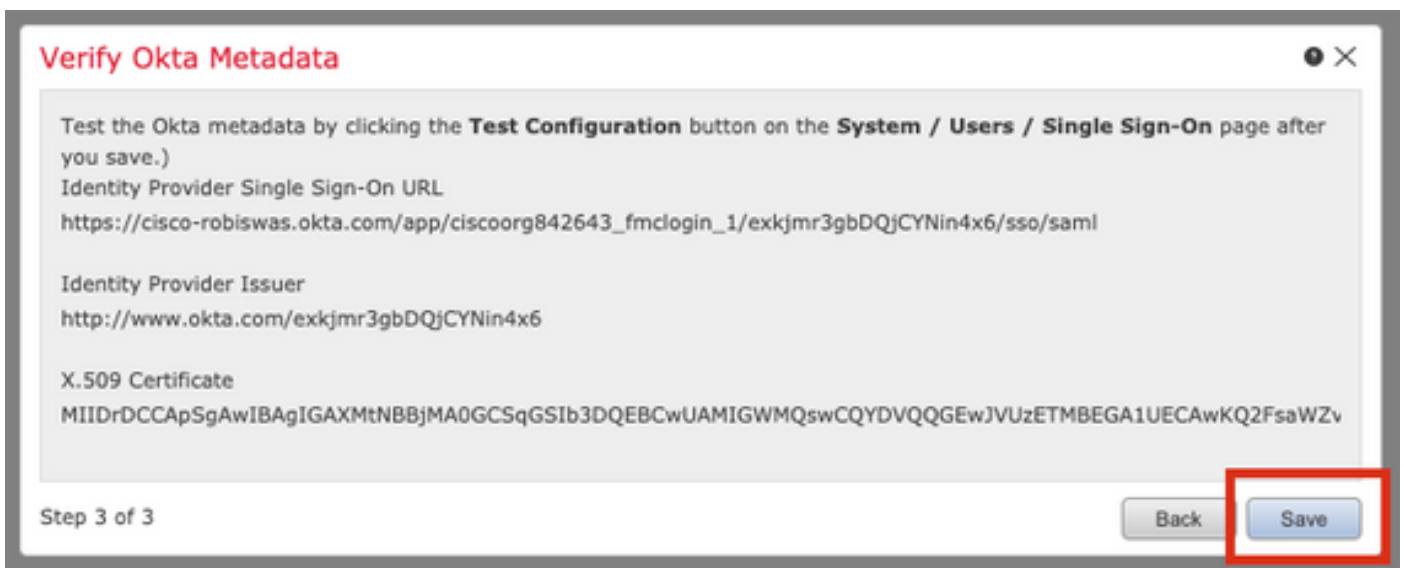
Vous pouvez également choisir **Télécharger le fichier XML** et télécharger le fichier XML récupéré à l'[étape 10](#) de Configuration Okta.



Une fois le fichier téléchargé, le FMC affiche les métadonnées. Cliquez sur **Suivant**, comme illustré dans cette image.



Étape 7. **Vérifiez** les métadonnées. Cliquez sur **Enregistrer**, comme illustré dans cette image.



Étape 8. Configurez le rôle **Mappage de rôle/Rôle utilisateur** par défaut sous **Configuration avancée**.

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

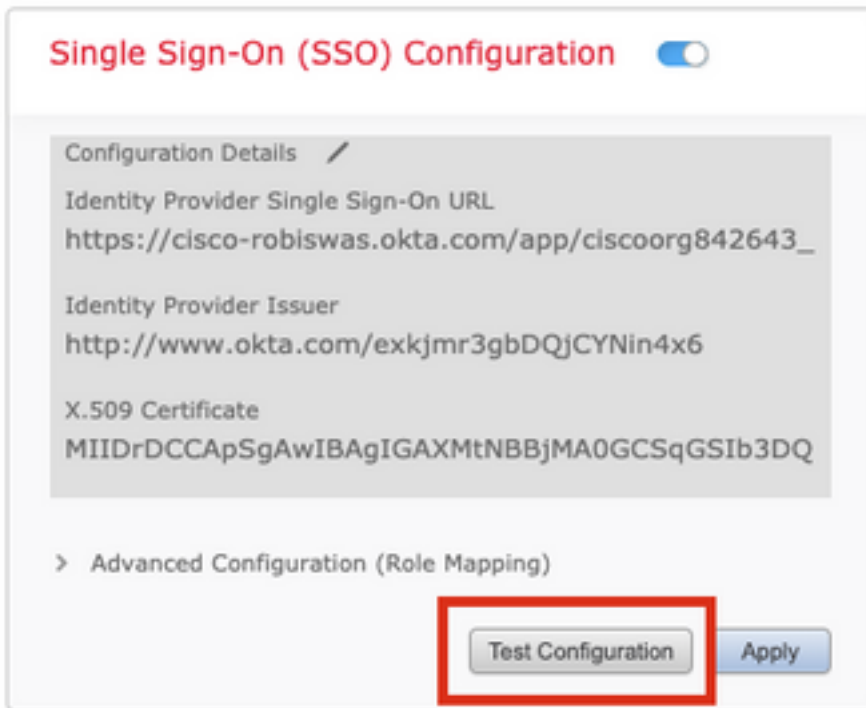
Security Analyst

Security Analyst (Read Only)

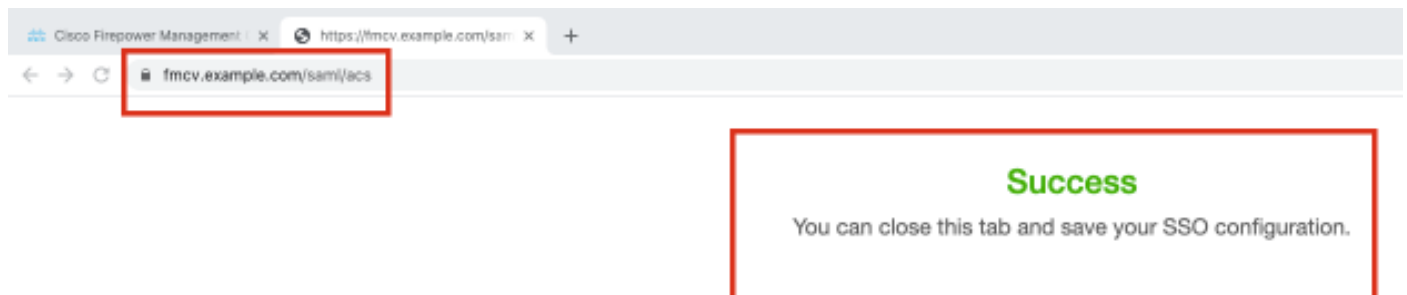
Security Approver

Threat Intelligence Director (TID) User

Étape 9. Afin de tester la configuration, cliquez sur **Test Configuration**, comme indiqué dans cette image.



Si le test est réussi, vous devriez voir la page affichée dans cette image, sur un nouvel onglet du navigateur.



Étape 10. Cliquez sur **Apply** pour enregistrer la 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/exkjmr3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

> Advanced Configuration (Role Mapping)

Test Configuration Apply

SSO doit être activé avec succès.

✔ 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

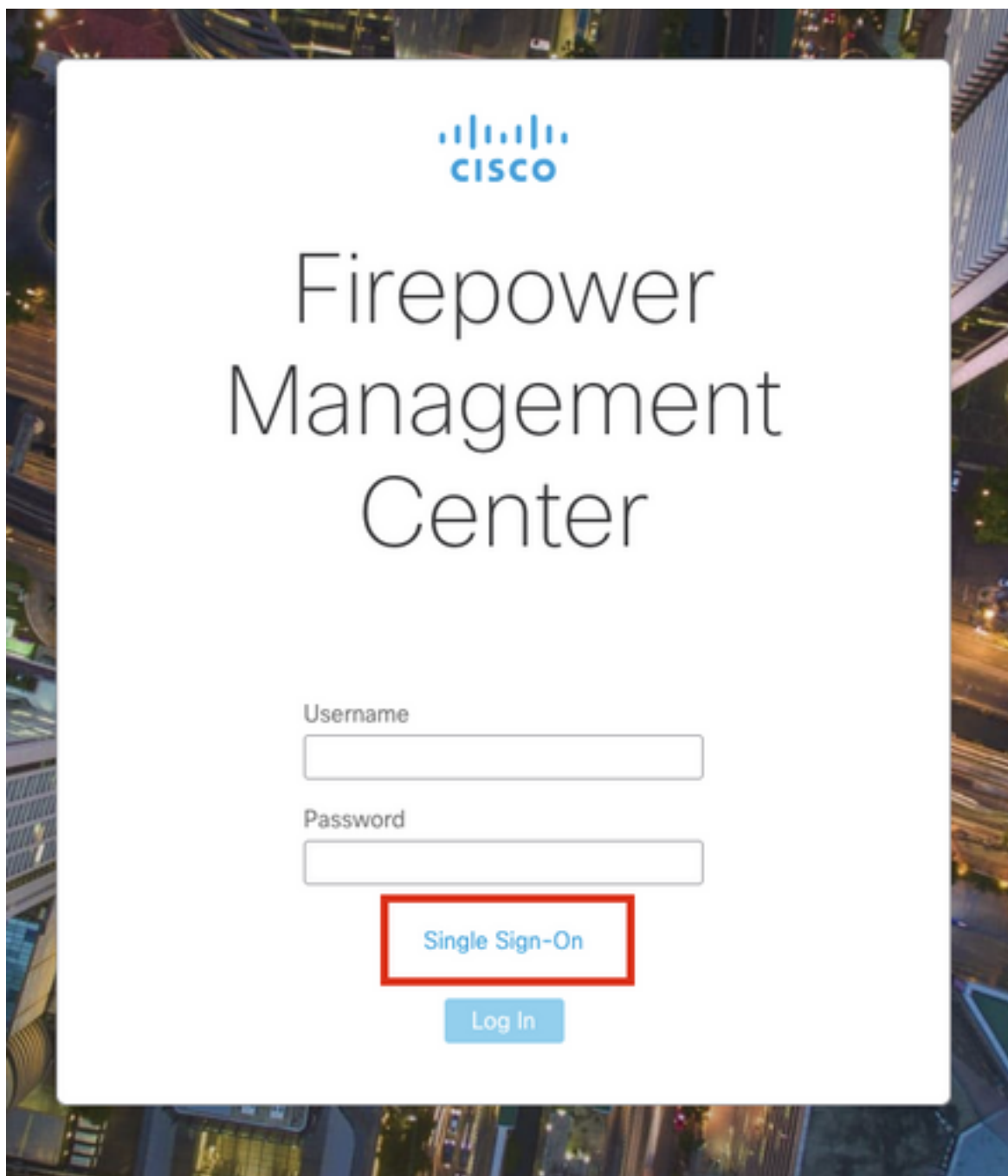
> Advanced Configuration (Role Mapping)

Test Configuration Apply

Vérification


Accédez à l'URL FMC à partir de votre navigateur : https://<URL fmc>. Cliquez sur **Connexion**

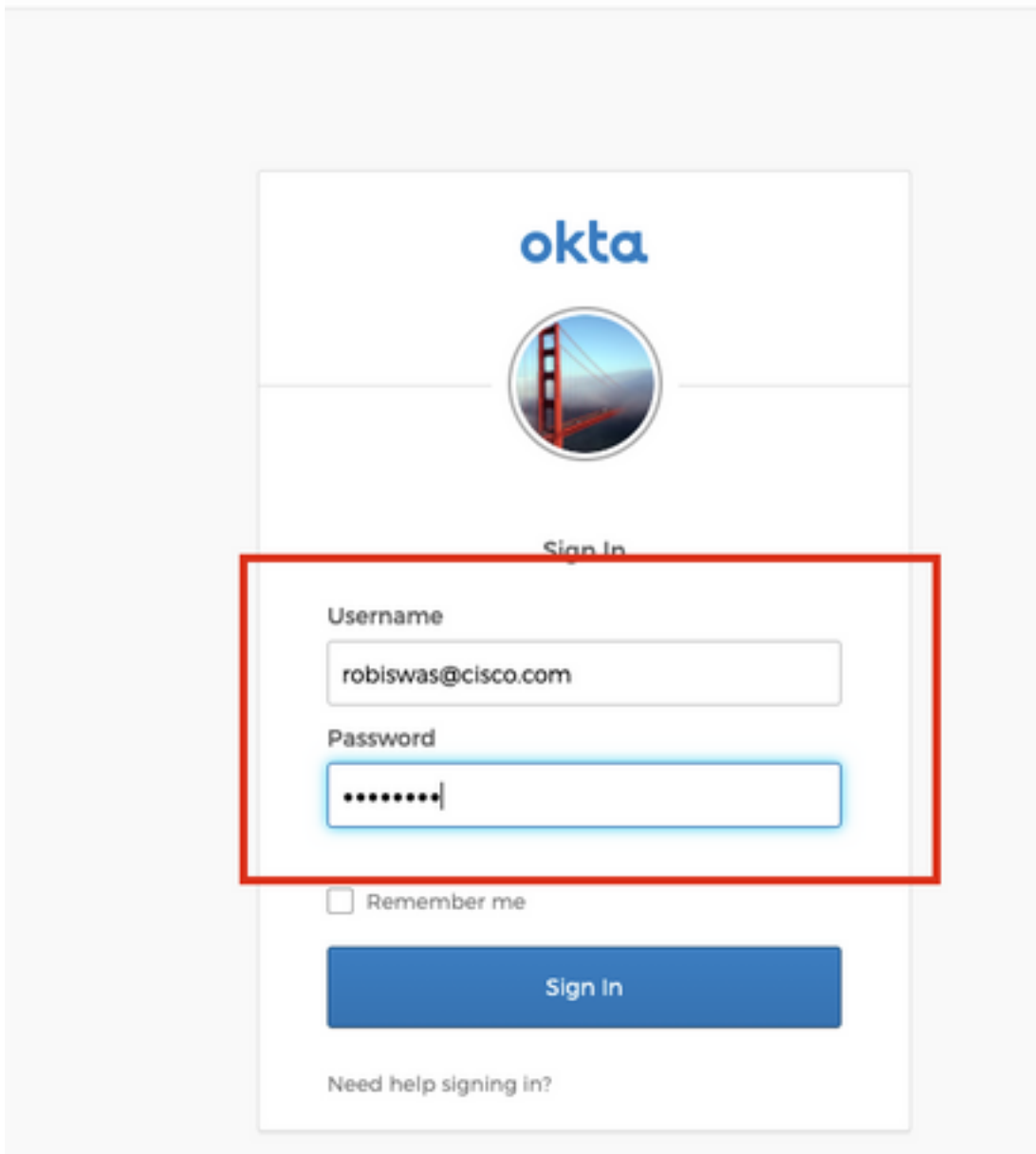
unique.



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 title "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 red rectangular box containing the text "Single Sign-On" in blue. At the bottom center, there is a blue button with the text "Log In". The entire login form is centered on a white background, which is overlaid on a blurred background image of a city at night.

Vous serez redirigé vers la page de connexion iDP (Okta). Fournissez vos informations d'identification SSO. Cliquez sur **Connexion**.

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 content is a "Sign In" form. The form has two input fields: "Username" with the value "robiswas@cisco.com" and "Password" with masked characters ".....". Below the password field is a checkbox for "Remember me" which is unchecked. A blue "Sign In" button is at the bottom of the form. Below the button is a link that says "Need help signing in?". A red rectangular box highlights the username and password input fields.

Si vous réussissez, vous devriez pouvoir vous connecter et voir la page par défaut de FMC.

Sur FMC, accédez à **System > Users** pour voir l'utilisateur SSO ajouté à la base de données.

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