

Configurar o acesso do Firepower Management Center por meio da autenticação SSO com o Okta

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Limitações e restrições](#)

[Configuration Steps](#)

[Etapas de configuração no Provedor de identidade \(Okta\)](#)

[Etapas de configuração no FMC](#)

[Verificar](#)

Introduction

Este documento descreve como configurar o Firepower Management Center (FMC) para autenticação usando o Single Sign-On (SSO) para acesso de gerenciamento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica de login único e SAML
- Compreensão da configuração no provedor de identidade (iDP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center (FMC) versão 6.7.0
- Okta como provedor de identidade

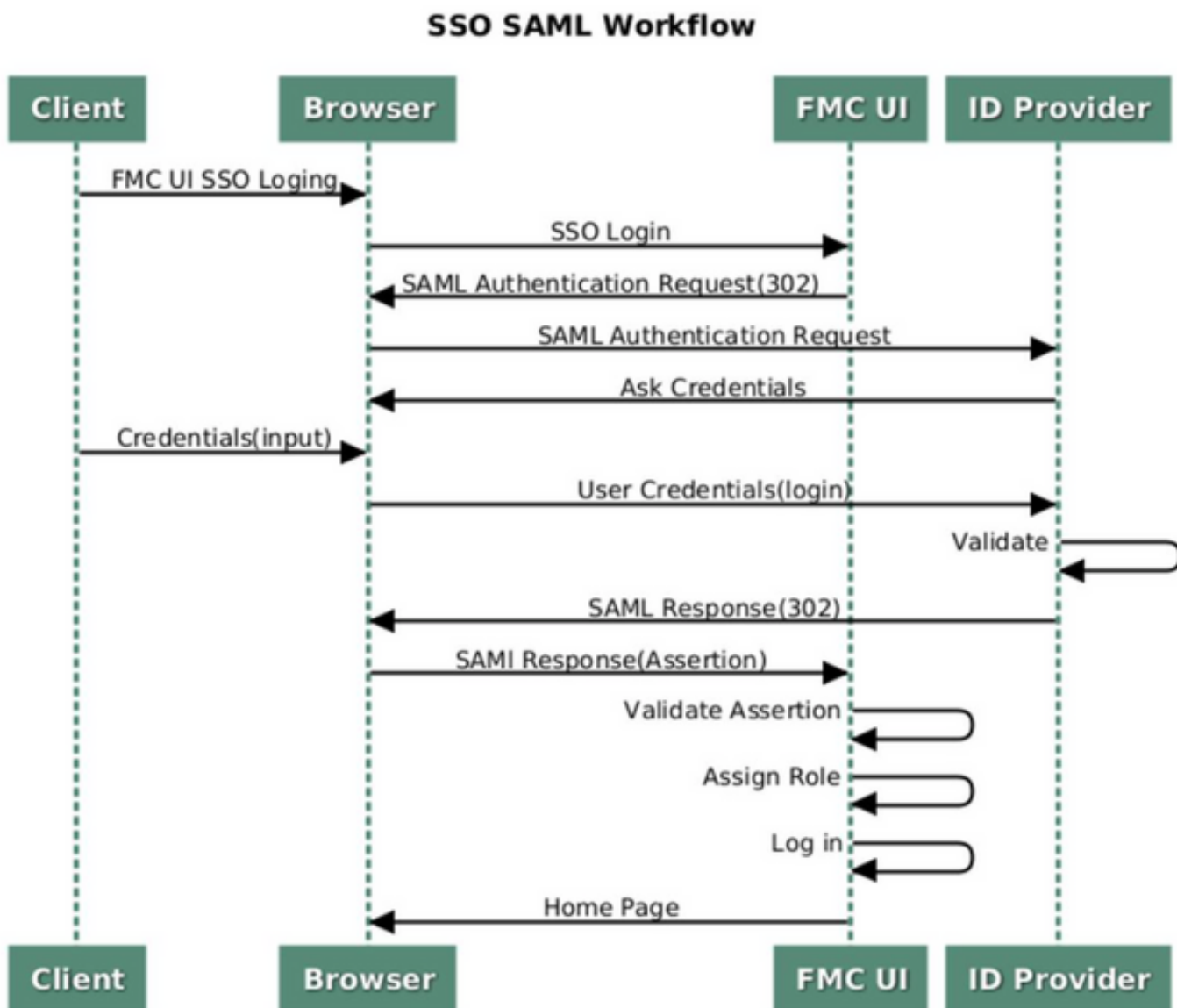
Observação: as informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer alteração de configuração.

Informações de Apoio

O login único (SSO) é uma propriedade do gerenciamento de identidade e acesso (IAM) que permite que os usuários autentiquem com segurança vários aplicativos e sites, fazendo login apenas uma vez com apenas um conjunto de credenciais (nome de usuário e senha). Com o SSO, o aplicativo ou site que o usuário está tentando acessar depende de um terceiro confiável para verificar se os usuários são quem dizem ser.

SAML (Security Assertion Markup Language) é uma estrutura baseada em XML para troca de dados de autenticação e autorização entre domínios de segurança. Ele cria um círculo de confiança entre o usuário, um provedor de serviços (SP) e um provedor de identidade (IdP) que permite que o usuário entre em uma única vez para vários serviços

Um provedor de serviços (SP) é uma entidade que recebe e aceita uma asserção de autenticação emitida por um provedor de identidade (iDP). Conforme descrito pelos nomes, os provedores de serviços fornecem serviços, enquanto os provedores de identidade fornecem a identidade dos usuários (autenticação).



Esses iDPs são suportados e testados para autenticação:

- Okta
- OneLogin
- PingID
- Azure AD
- Outros (qualquer iDP em conformidade com SAML 2.0)

Observação: não há necessidade de novas licenças. Este recurso funciona no modo licenciado e no modo de avaliação.

Limitações e restrições

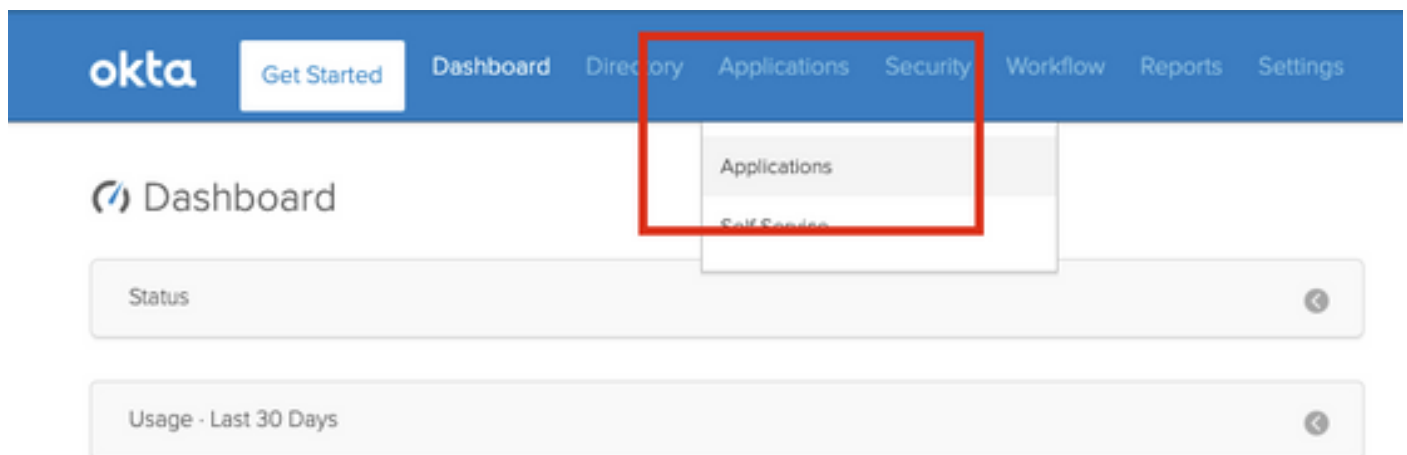
Essas são limitações conhecidas e restrições para autenticação SSO para acesso ao FMC:

- O SSO pode ser configurado somente para o domínio global
- Os FMCs no par HA exigem configuração individual
- Somente administradores locais/AD podem configurar SSO no FMC (os usuários admin SSO não poderão configurar/atualizar as configurações SSO no FMC).

Configuration Steps

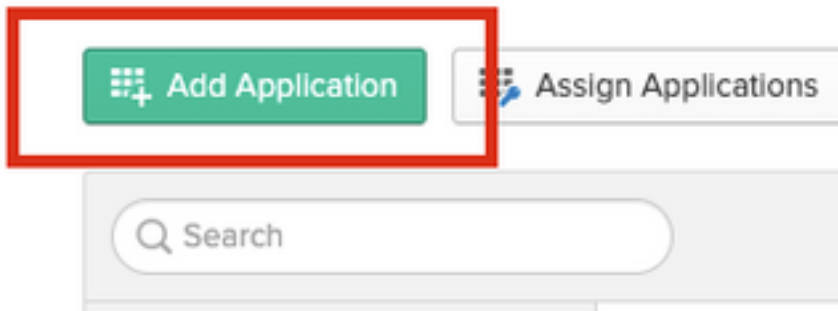
Etapas de configuração no Provedor de identidade (Okta)

Etapa 1. Faça login no portal Okta. Navegue para **Aplicativos > Aplicativos**, como mostrado nesta imagem.

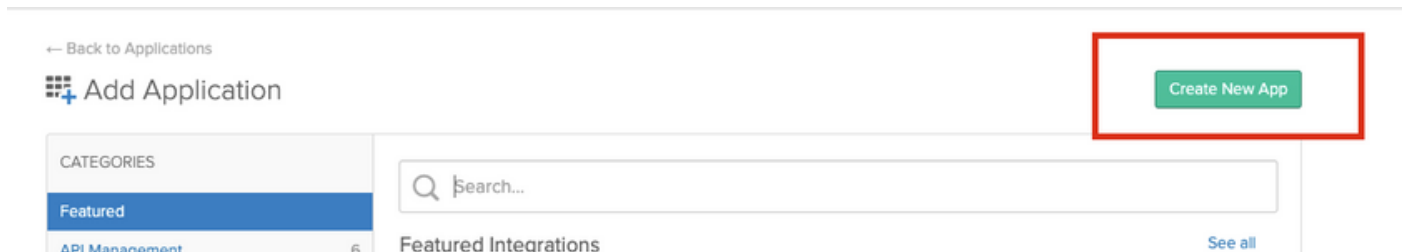


Etapa 2. Como mostrado nesta imagem, clique em **AddApplication**.

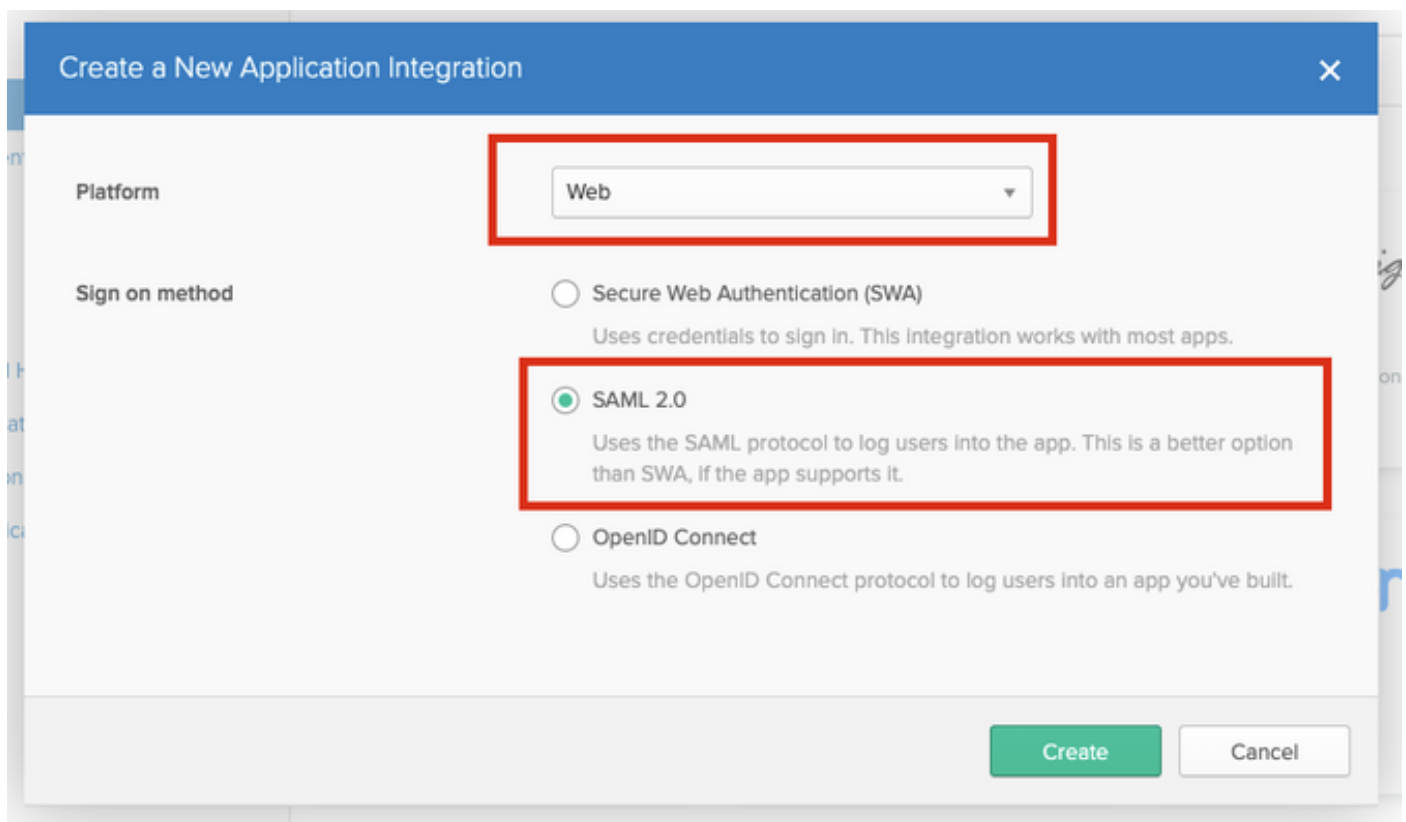
Applications



Etapa 3. Como mostrado nesta imagem, clique em **Create NewApp**.



Etapa 4. Escolha a **plataforma** como **Web**. Escolha o **método de Início de Sessão** como **SAML 2.0**. Clique em **Criar**, conforme mostrado nesta imagem.




Etapa 5. Forneça um **nome de aplicativo**, **logotipo de aplicativo (opcional)** e clique em **Avançar**, como mostrado nesta imagem.

1 General Settings

App name

App logo (optional) ?



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

Etapa 6. Digite as configurações SAML.

URL de início de sessão único: `https://<URL do fmc>/saml/acs`

URI da audiência (ID da entidade da controladora de armazenamento): `https://<URL do fmc>/saml/metadados`

Estado de retransmissão padrão: `/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](#)

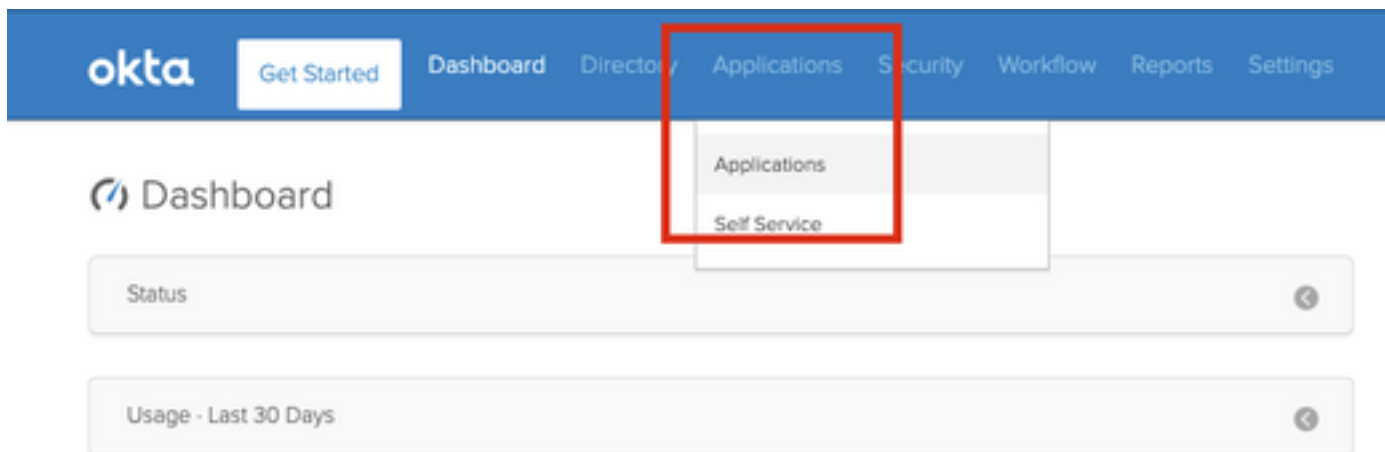
Name

Name format (optional)

Value

[Add Another](#)

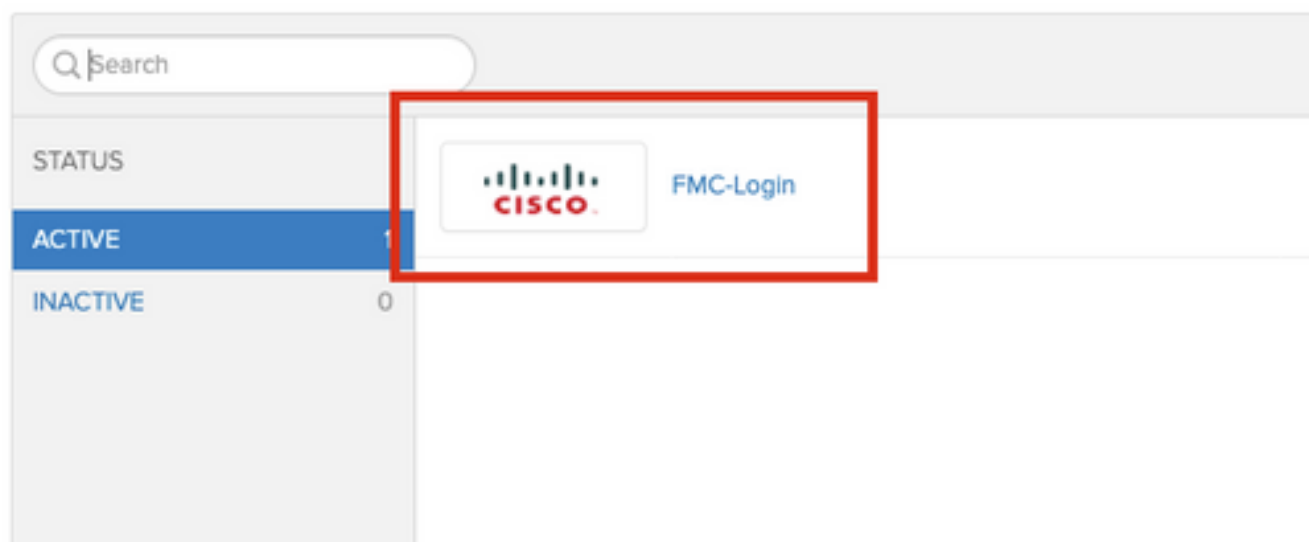
Passo 7. Navegue para **Aplicativos > Aplicativos**, como mostrado nesta imagem.



Etapa 8. Clique no nome do aplicativo que foi criado.

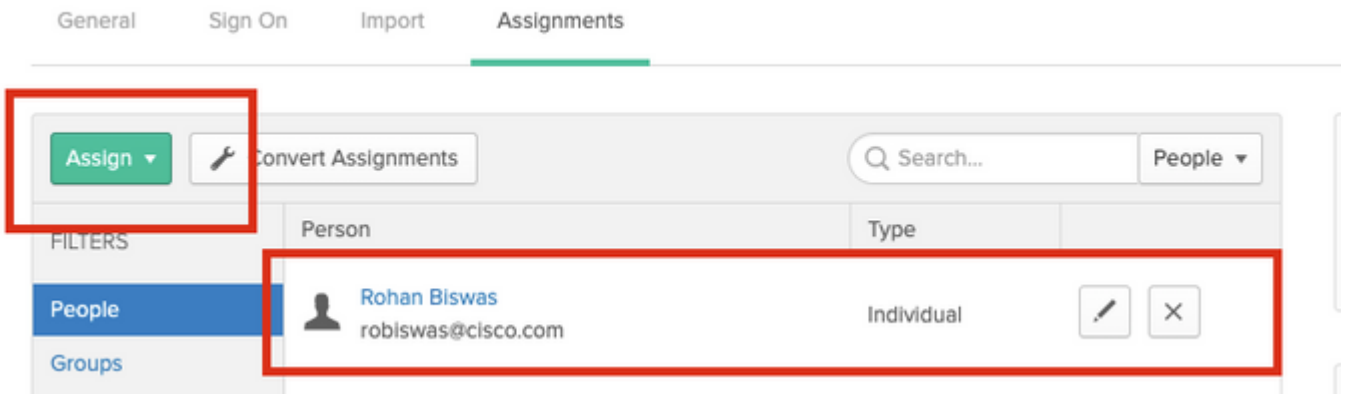
Applications

[Add Application](#) [Assign Applications](#) [More](#)

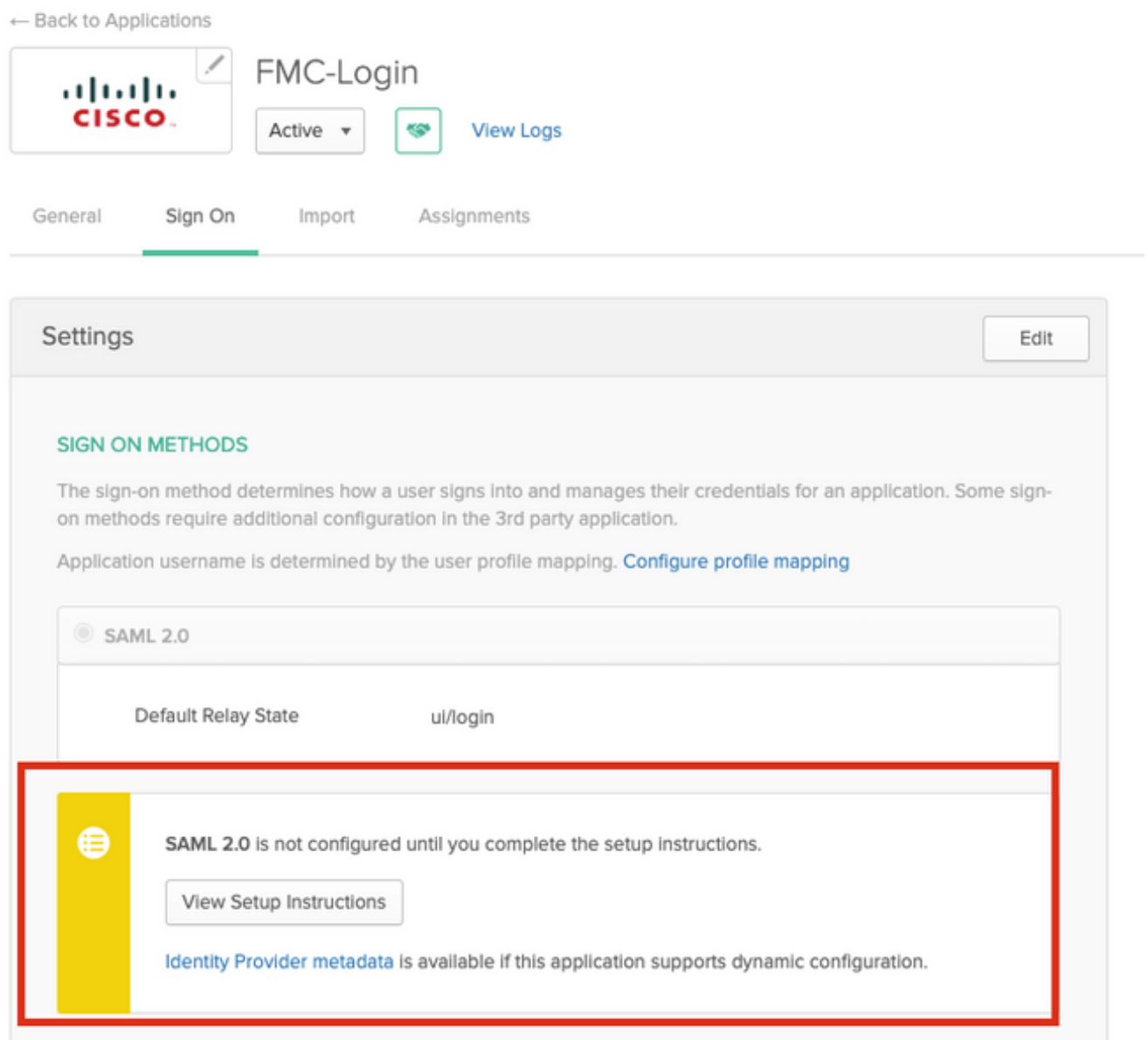


Etapa 9. Navegue até **Atribuições**. Clique em **Atribuir**.

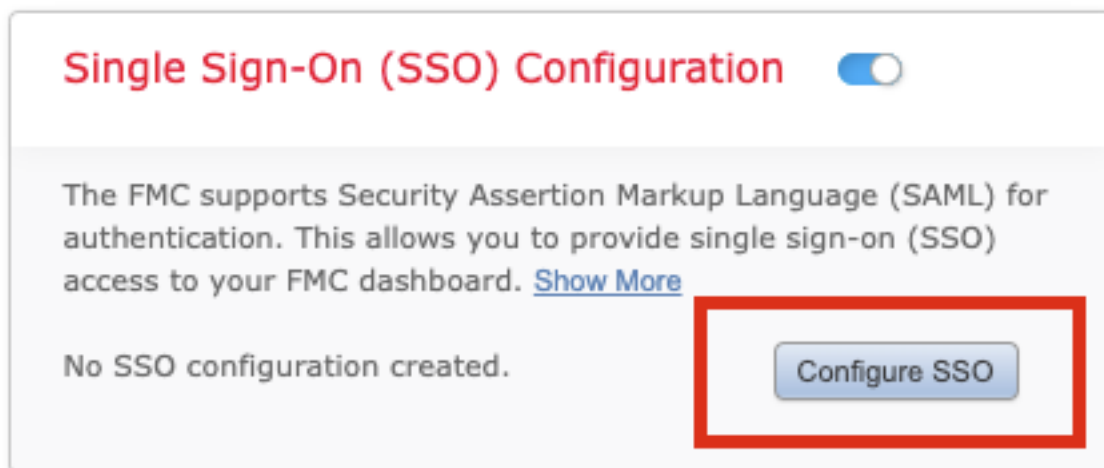
Você pode optar por atribuir usuários individuais ou grupos ao nome do aplicativo criado.



Etapa 10. Navegue para **Iniciar Sessão**. Clique em **Exibir instruções de configuração**. Clique nos **metadados do provedor de identidade** para exibir os metadados do iDP.



Salve o arquivo como um arquivo **.xml** a ser usado no FMC.

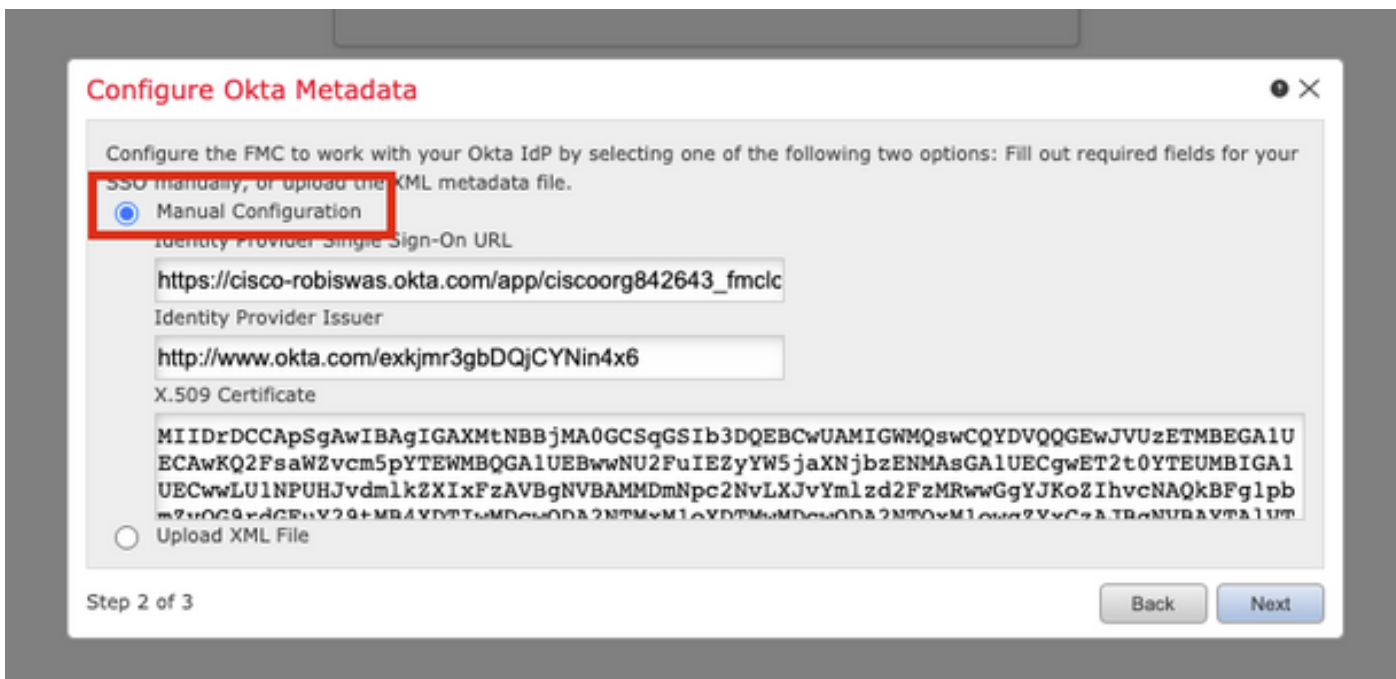


Etapa 5. Selecione o **FMC SAML Provider**. Clique em Next.

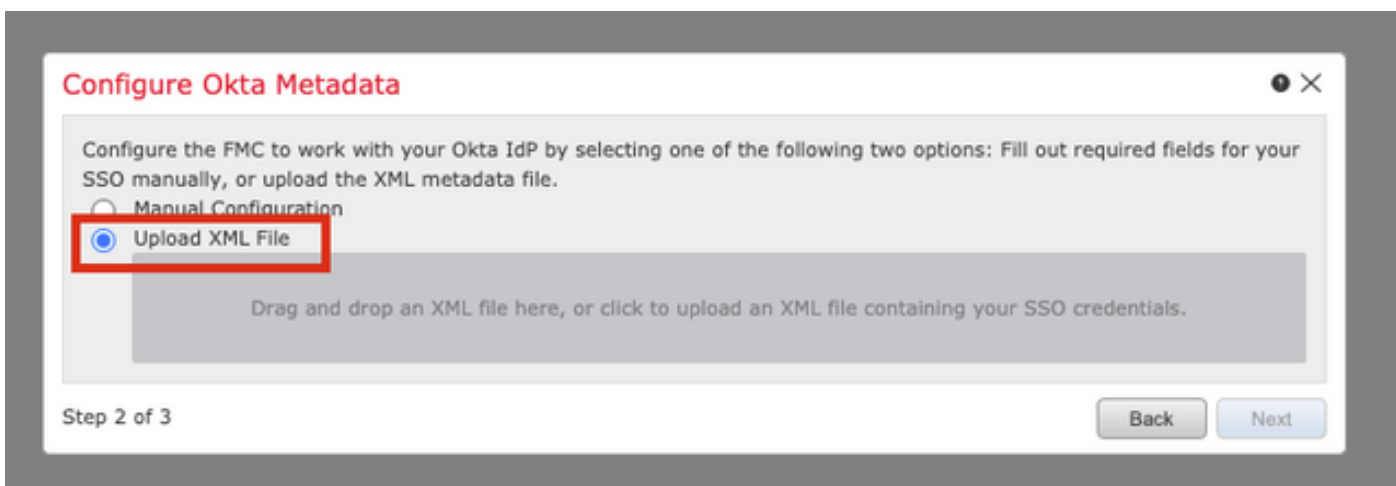
Para o propósito desta demonstração, é usado **Okta**.



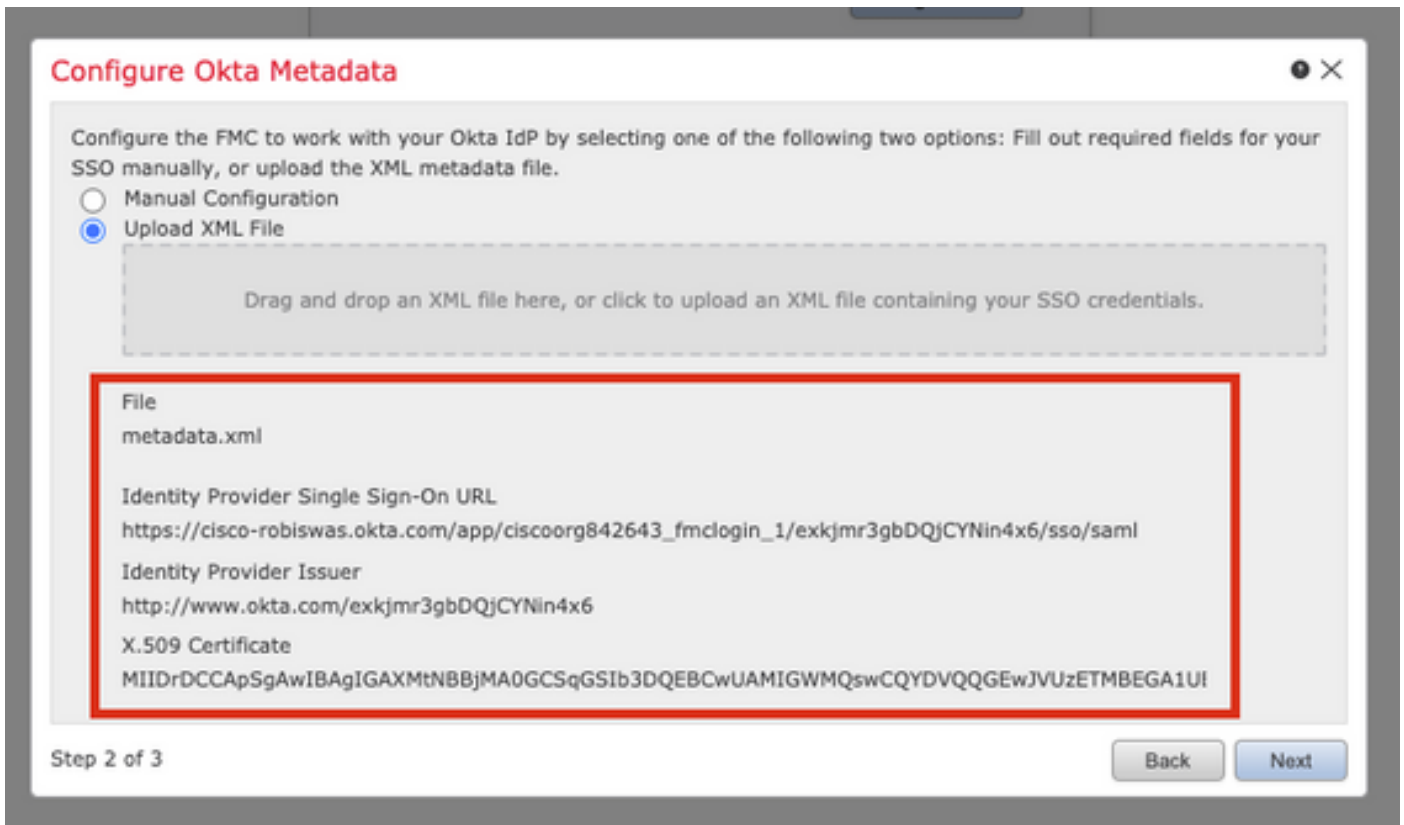
Etapa 6. Você pode escolher **Configuração manual** e inserir os dados iDP manualmente. Clique em **Avançar**, como



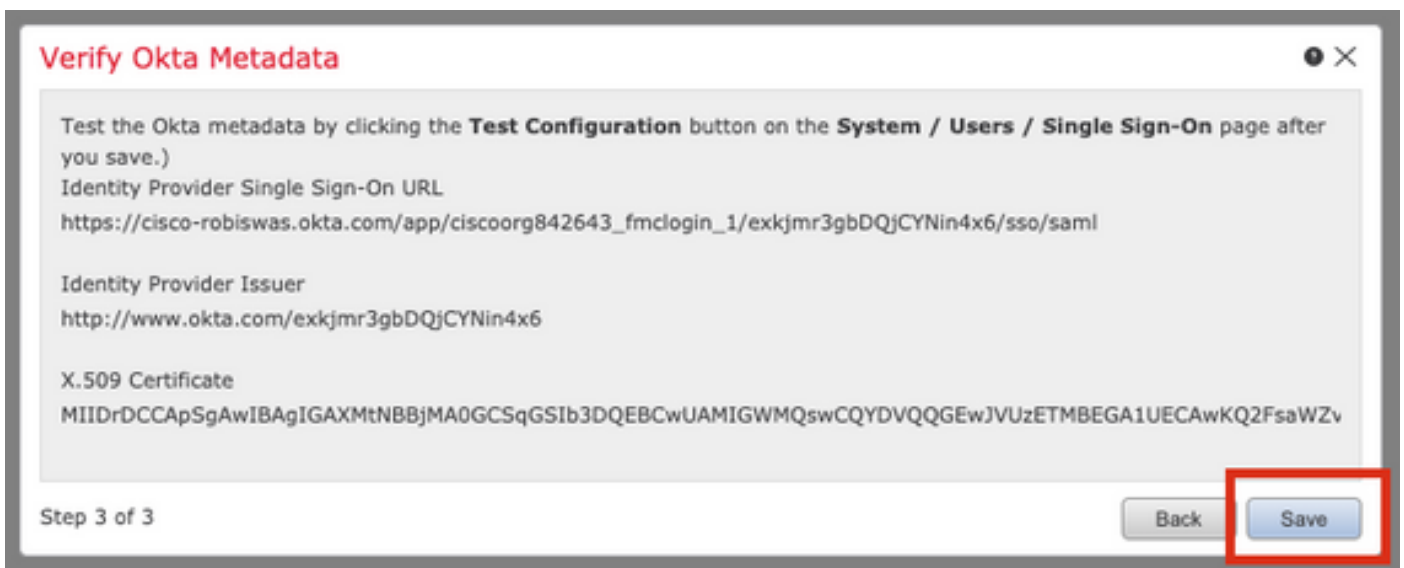
Você também pode escolher **Carregar arquivo XML** e carregar o arquivo XML recuperado na [Etapa 10](#) da Configuração do Okta.



Quando o arquivo é carregado, o FMC exibe os metadados. Clique em **Avançar**, conforme mostrado nesta imagem.



Passo 7. **Verifique** os metadados. Clique em **Salvar**, conforme mostrado nesta imagem.



Etapa 8. Configure o **Mapeamento de funções/Função de usuário padrão** em **Configuração avançada**.

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

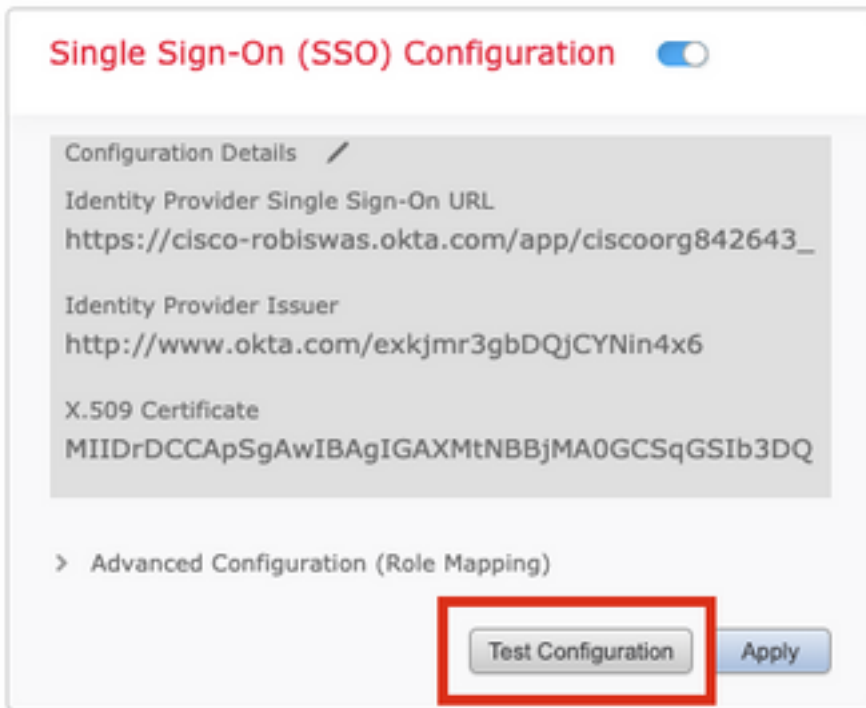
Security Analyst

Security Analyst (Read Only)

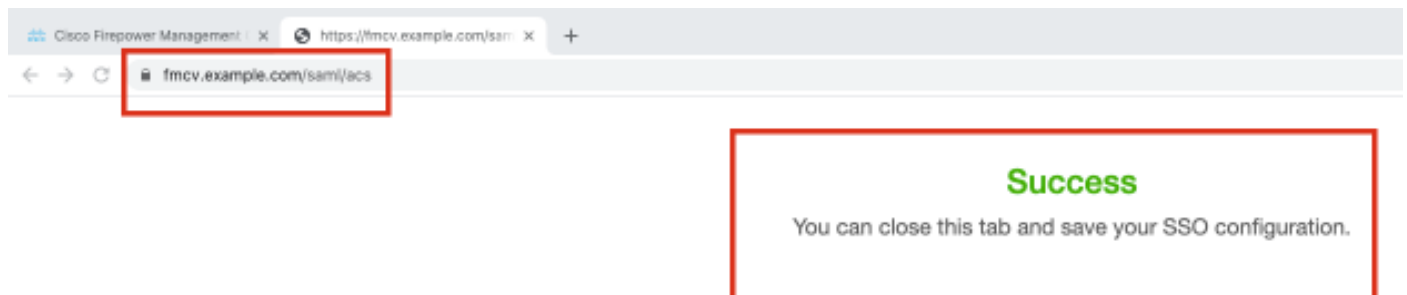
Security Approver

Threat Intelligence Director (TID) User

Etapa 9. Para testar a configuração, clique em **Test Configuration**, como mostrado nesta imagem.



Se o teste for bem-sucedido, você deverá ver a página mostrada nesta imagem, em uma nova guia no navegador.



Etapa 10. Clique em **Apply (Aplicar)** para salvar a configuração.

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 deve ser ativado com êxito.

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

Verificar

Navegue até o URL do FMC no seu navegador: https://<URL do fmc>. Clique em Logon único.



Firepower Management Center


Username

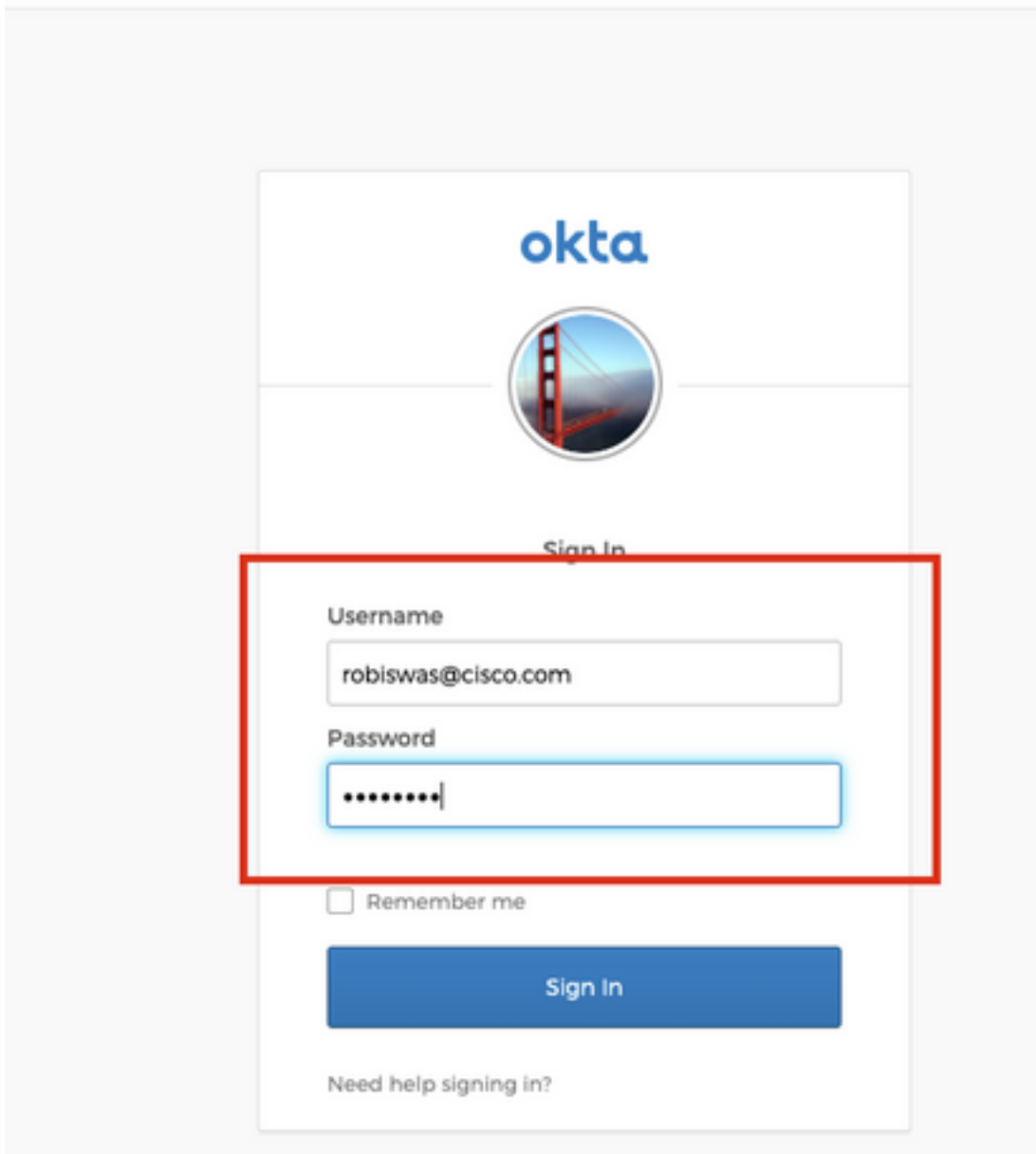
Password

[Single Sign-On](#)

[Log In](#)

Você seria redirecionado para a página de login do iDP (Okta). Forneça suas credenciais SSO. Clique em **Entrar**.

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.

Se tiver êxito, você poderá fazer login e ver a página padrão do FMC.

No FMC, navegue até **System > Users** para ver o usuário SSO adicionado ao banco de dados.

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