

使用Okta通过SSO身份验证配置Firepower管理中心访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[限制和限制](#)

[配置步骤](#)

[身份提供程序\(OKTA\)上的配置步骤](#)

[FMC上的配置步骤](#)

[验证](#)

简介

本文档介绍如何配置Firepower管理中心(FMC)以使用单点登录(SSO)进行身份验证以进行管理访问。

先决条件

要求

Cisco 建议您了解以下主题：

- 对单点登录和SAML的基本了解
- 了解身份提供程序(iDP)上的配置

使用的组件

本文档中的信息基于以下软件版本：

- 思科Firepower管理中心(FMC)版本6.7.0
- 确定身份提供者

注意：本文档中的信息是从特定实验环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解任何配置更改的潜在影响。

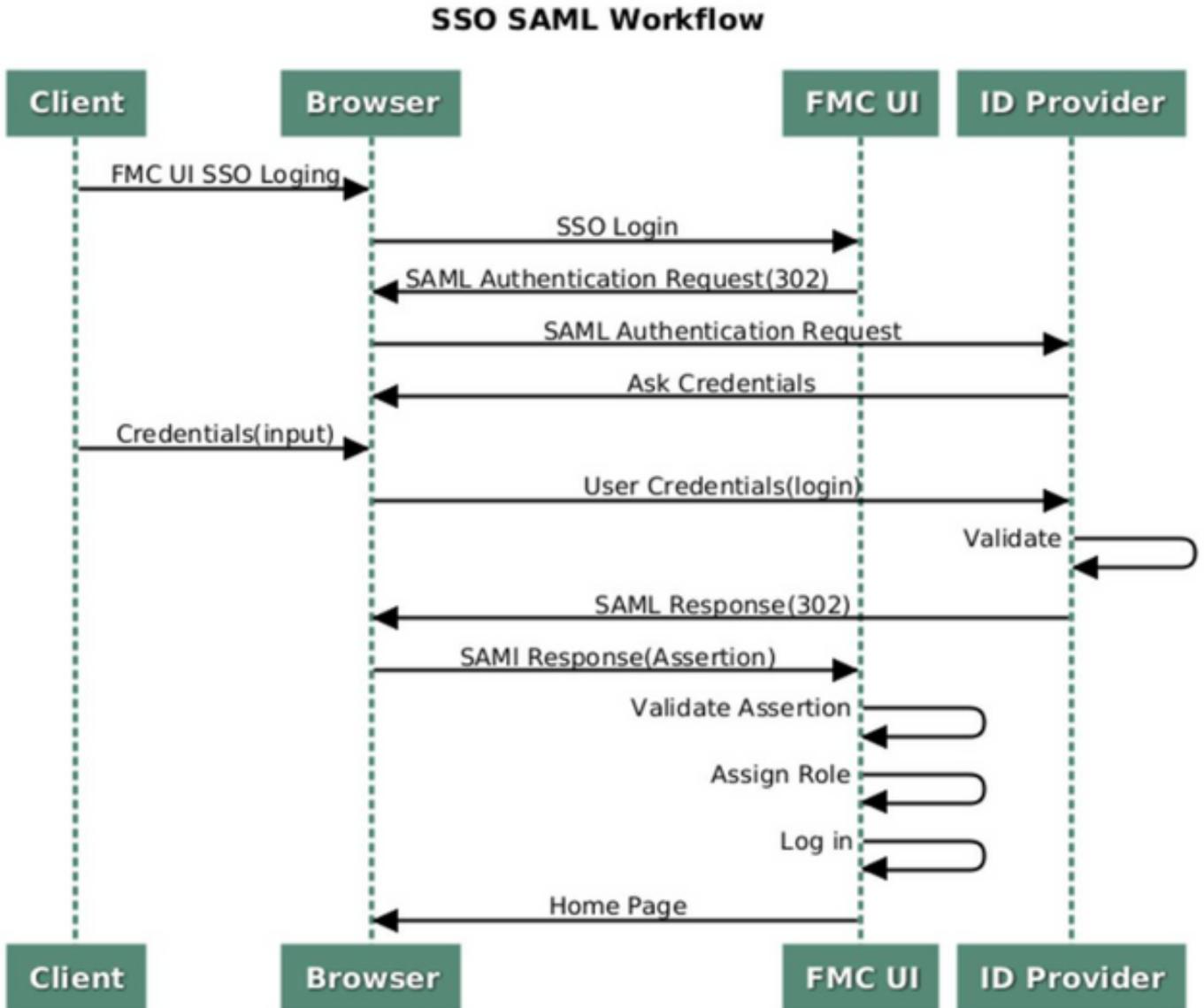
背景信息

单点登录(SSO)是身份和访问管理(IAM)的一个属性，通过仅使用一组凭证（用户名和密码）登录一次，用户就可以安全地使用多个应用和网站进行身份验证。使用SSO时，用户尝试访问的应用或网

站依靠受信任的第三方来验证用户是否是他们所说的用户。

SAML (安全断言标记语言) 是一个基于XML的框架，用于在安全域之间交换身份验证和授权数据。它在用户、服务提供商(SP)和身份提供商(IdP)之间创建信任圈，允许用户一次登录多个服务

服务提供商(SP)是接收并接受由身份提供商(iDP)发出的身份验证断言的实体。如其名称所述，服务提供商提供服务，而身份提供商提供用户身份 (身份验证)。



这些iDP受支持，并经过身份验证测试：

- 奥克塔
- OneLogin
- PingID
- Azure AD
- 其他 (任何符合SAML 2.0的iDP)

注意：无新许可证要求。此功能在许可和评估模式下工作。

限制和限制

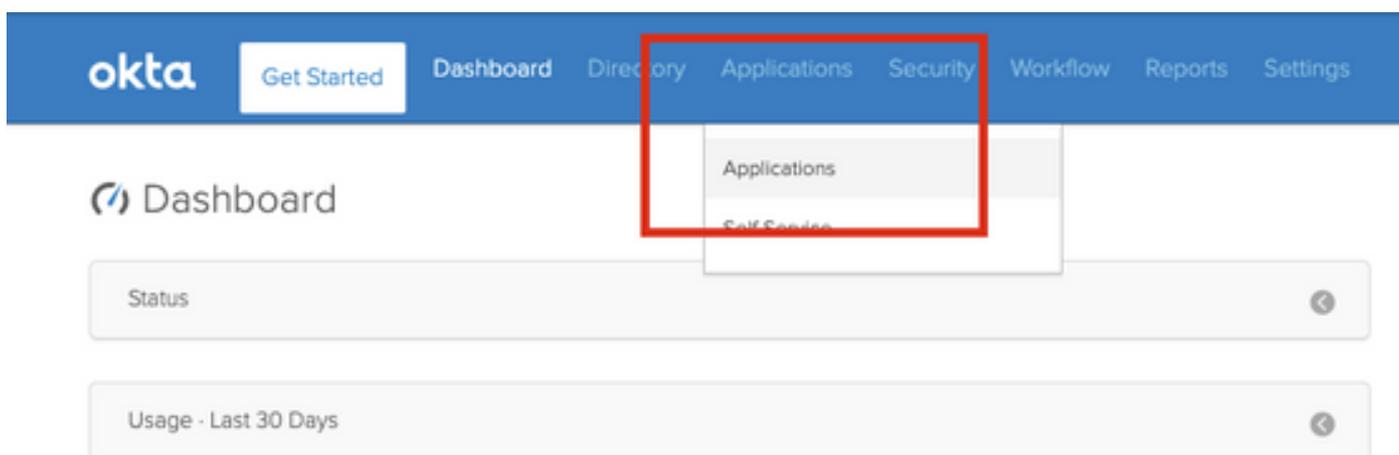
以下是FMC访问的SSO身份验证的已知限制和限制：

- SSO只能配置为全局域
- HA对中的FMC需要单独配置
- 只有本地/AD管理员可以在FMC上配置SSO (SSO管理员用户将无法在FMC上配置/更新SSO设置)。

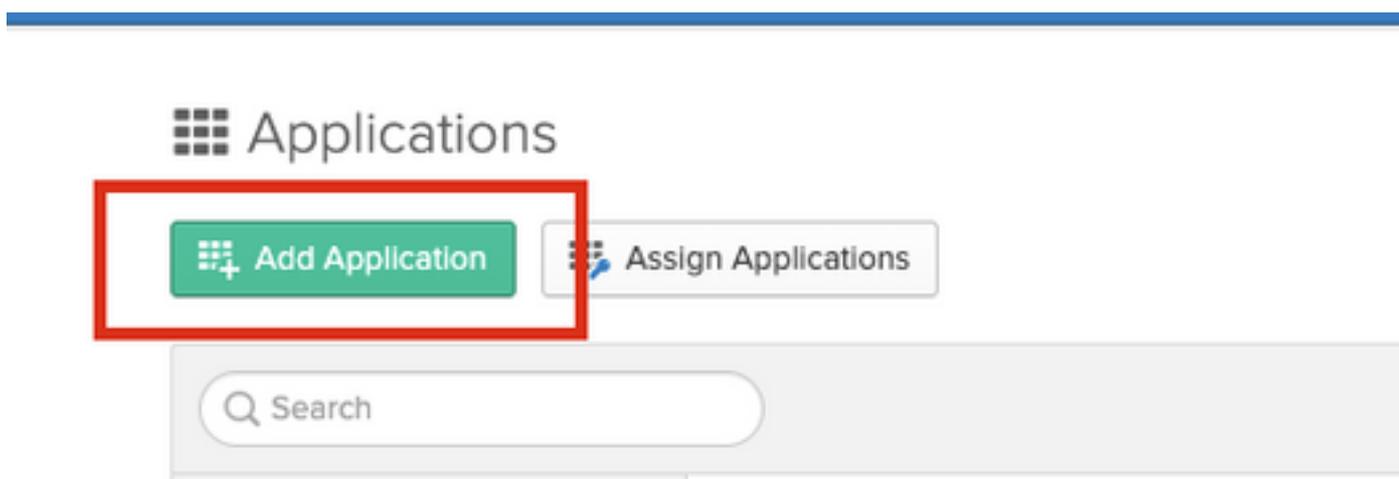
配置步骤

身份提供程序(OKTA)上的配置步骤

步骤1.登录Okta门户。导航至应用程序>应用程序，如下图所示。



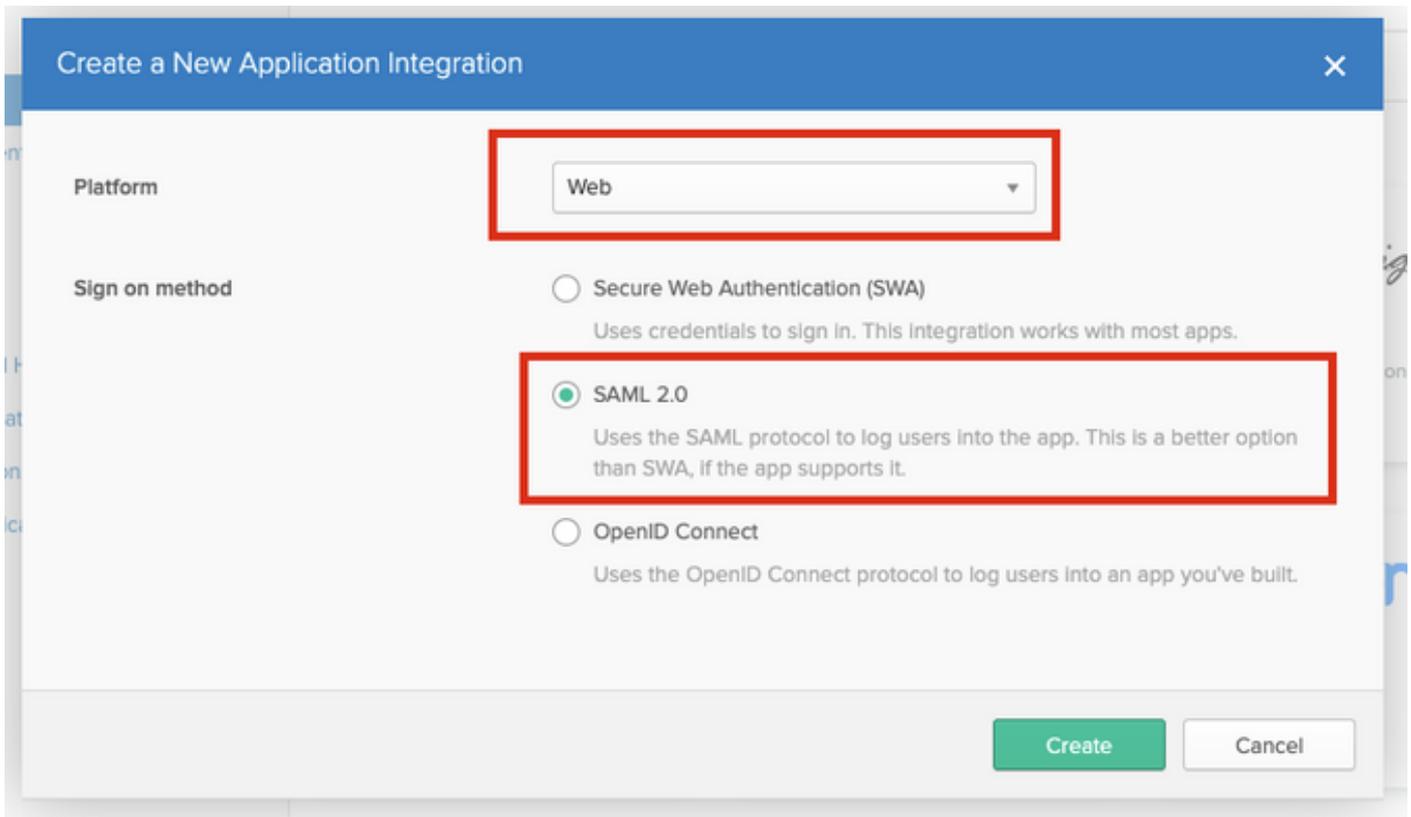
步骤2.如此图所示，单击AddApplication(添加应用)。



步骤3.如此图所示，单击“创建新应用”。



步骤4.将平台选为Web。选择Sign On方法作为SAML 2.0。单击Create，如此图所示。



步骤5.提供应用名称、应用徽标（可选），然后单击下一步，如下图所示。

1 General Settings

App name

FMC-Login

App logo (optional) ?



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

App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

Cancel Next

步骤6.输入SAML Settings。

单点登录URL:https://<fmc URL>/saml/acs

受众URI (SP实体ID) : https://<fmc URL>/saml/metadata

默认中继状态 : /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](#)

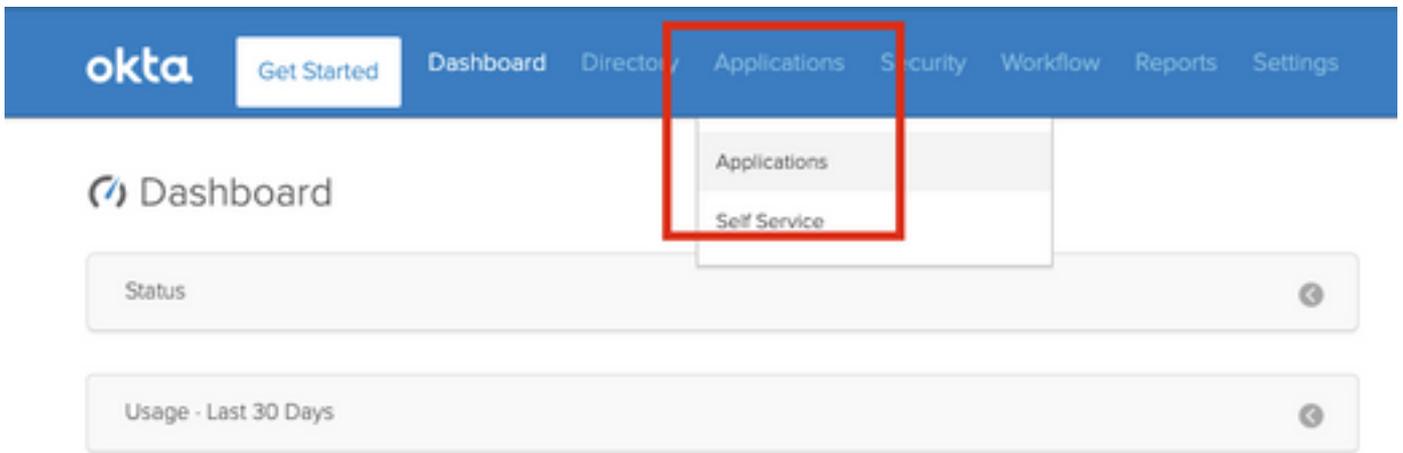
Name

Name format (optional)

Value

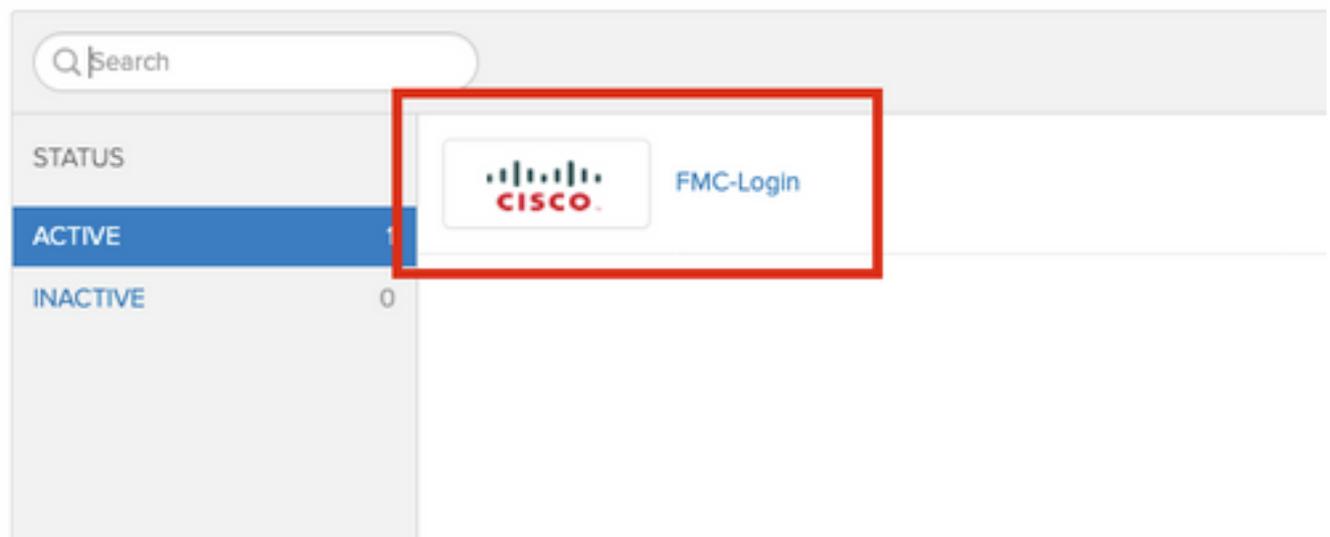
[Add Another](#)

步骤7. 导航回 Applications > Applications，如下图所示。



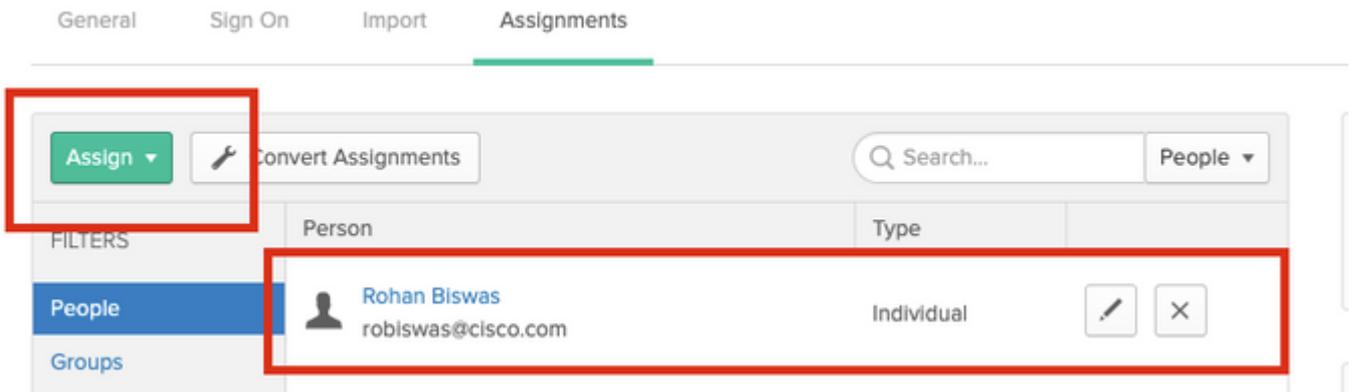
步骤8.单击创建的应用名称。

Applications

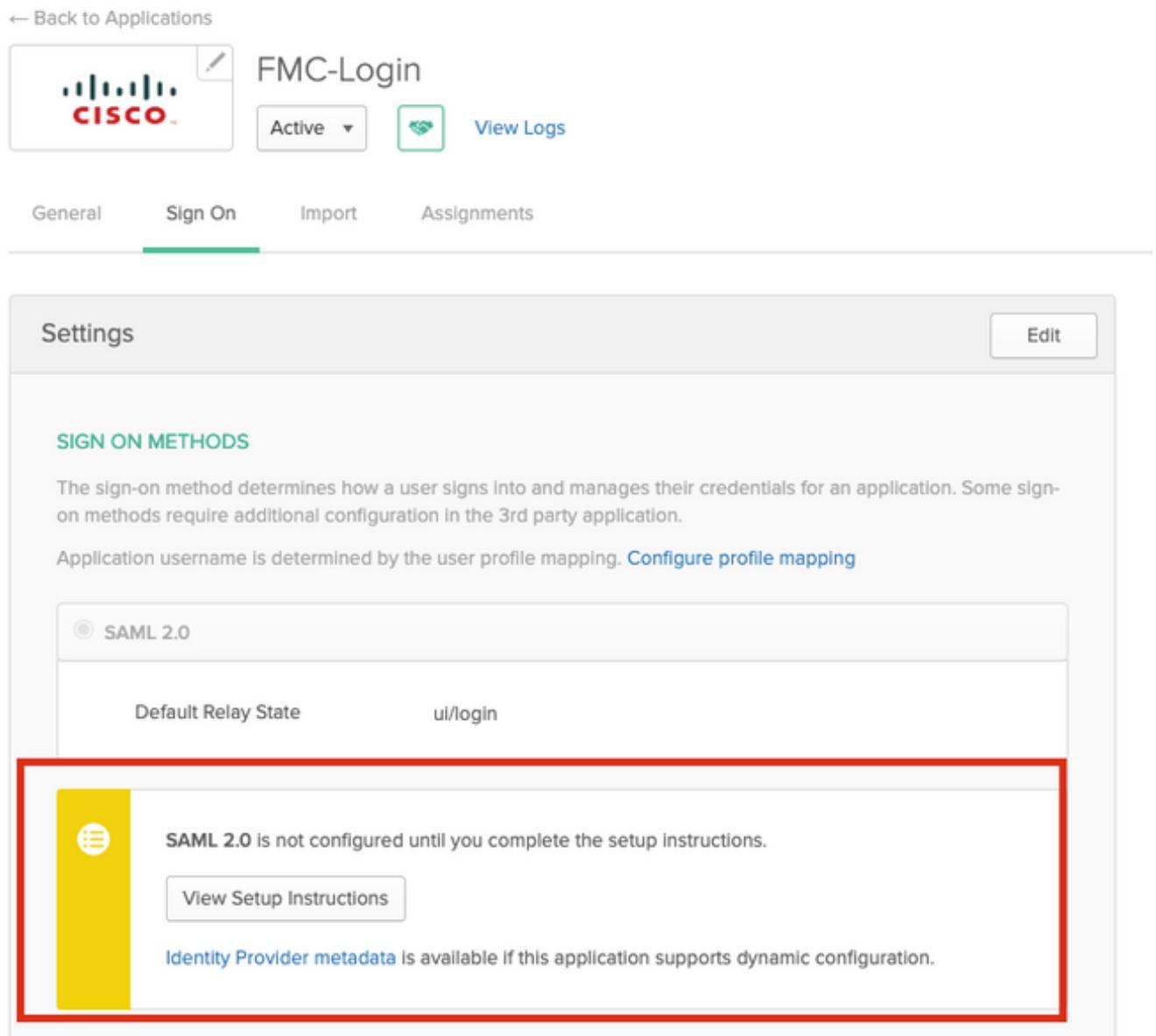


步骤9.定位至“分配”。单击“Assign”。

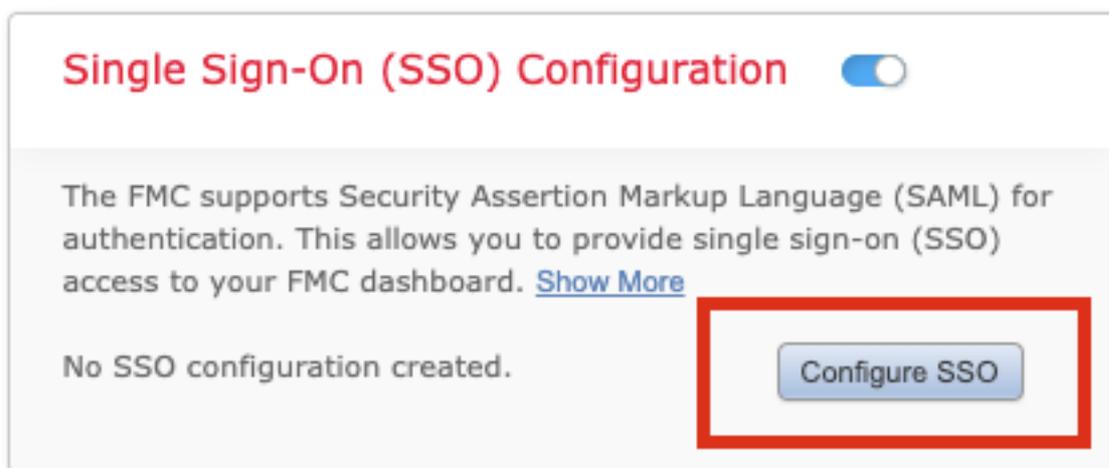
您可以选择将单个用户或组分配给创建的应用名称。



步骤10. 导航至登录。单击“查看设置说明”。单击“身份提供程序”元数据以查看iDP的元数据。



将文件另存为要在FMC上使用的.xml文件。

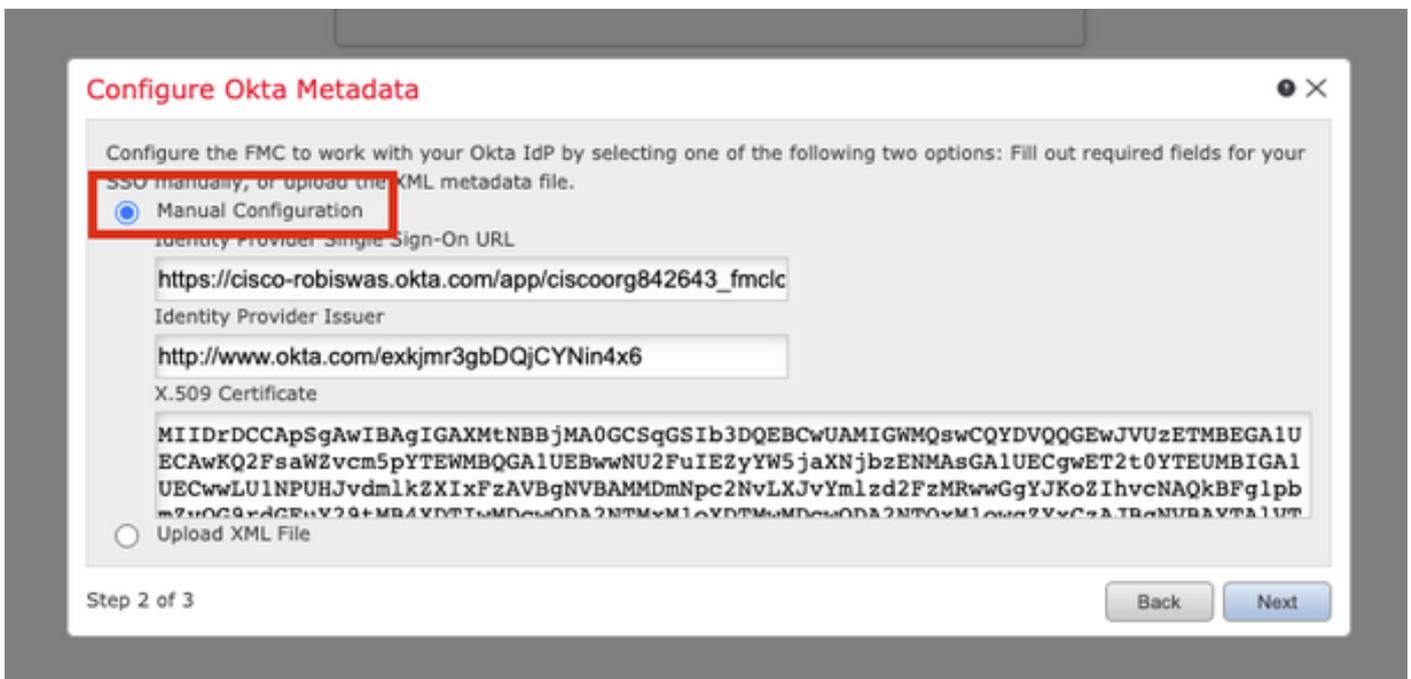


步骤5.选择FMC SAML提供程序。单击 Next。

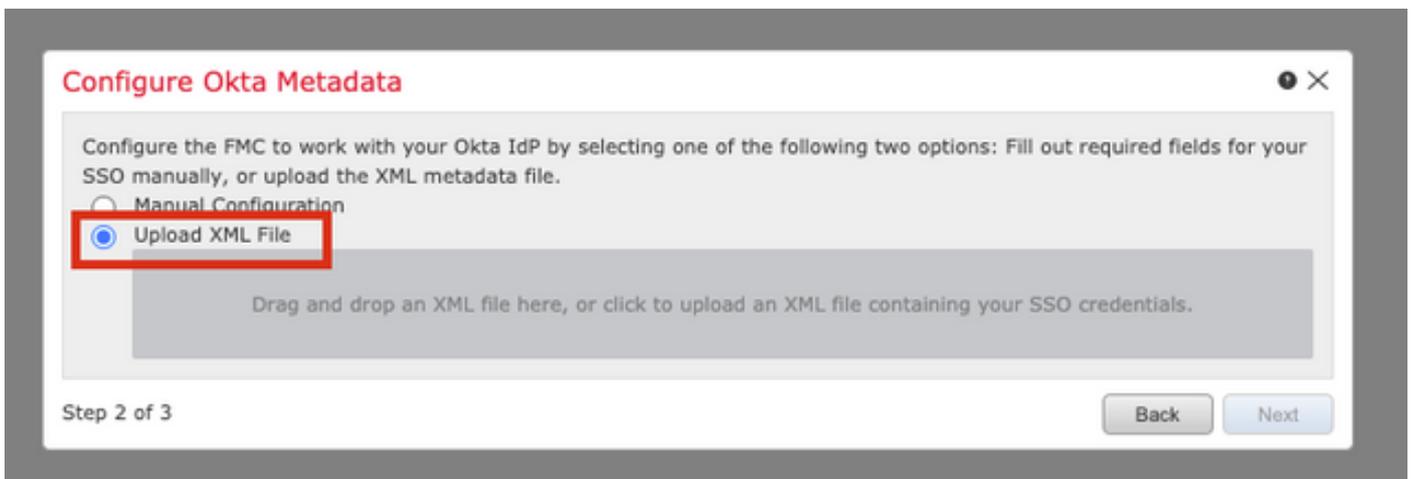
本演示使用Okta。



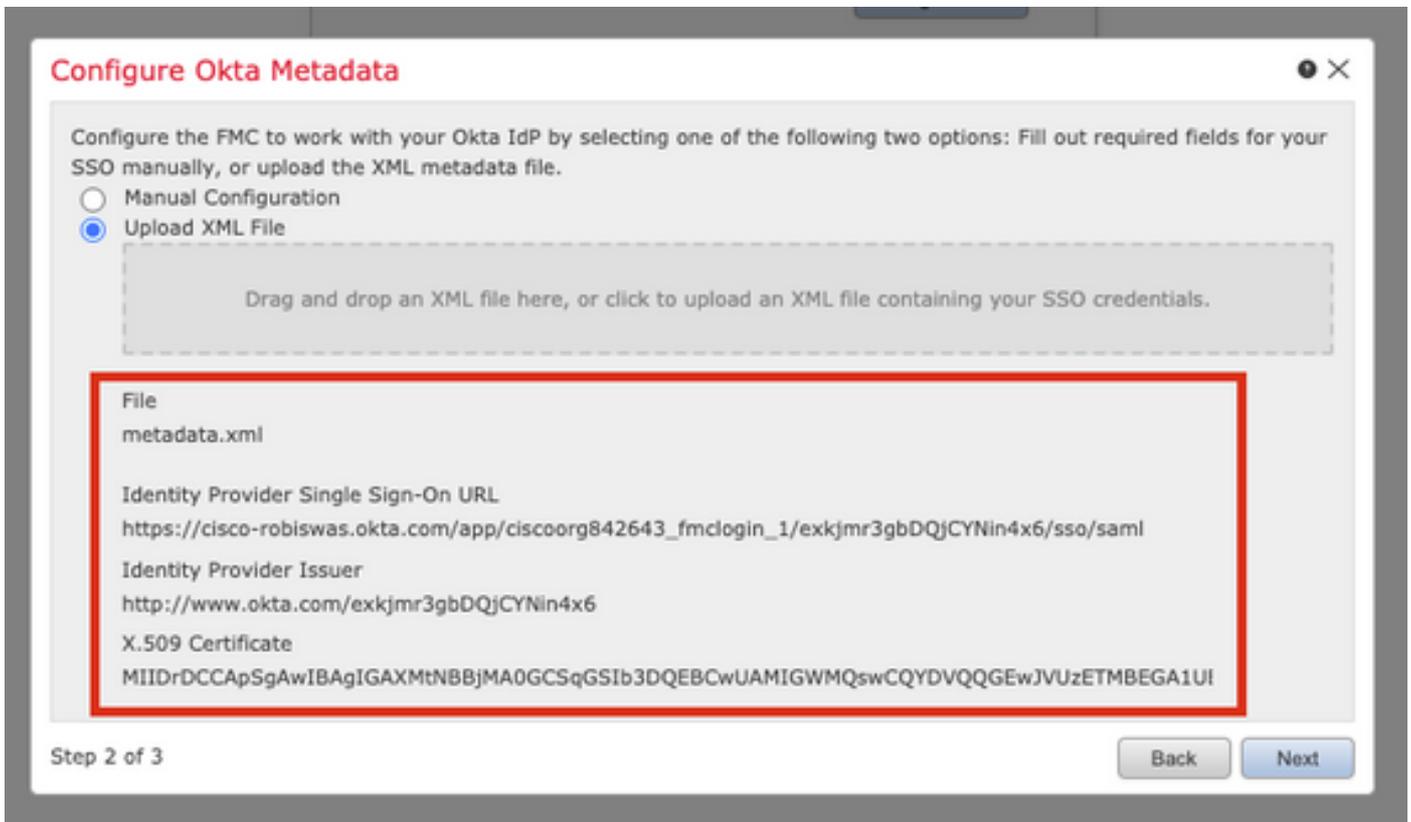
步骤6.您可以选择手动配置并手动输入iDP数据。单击Next，如



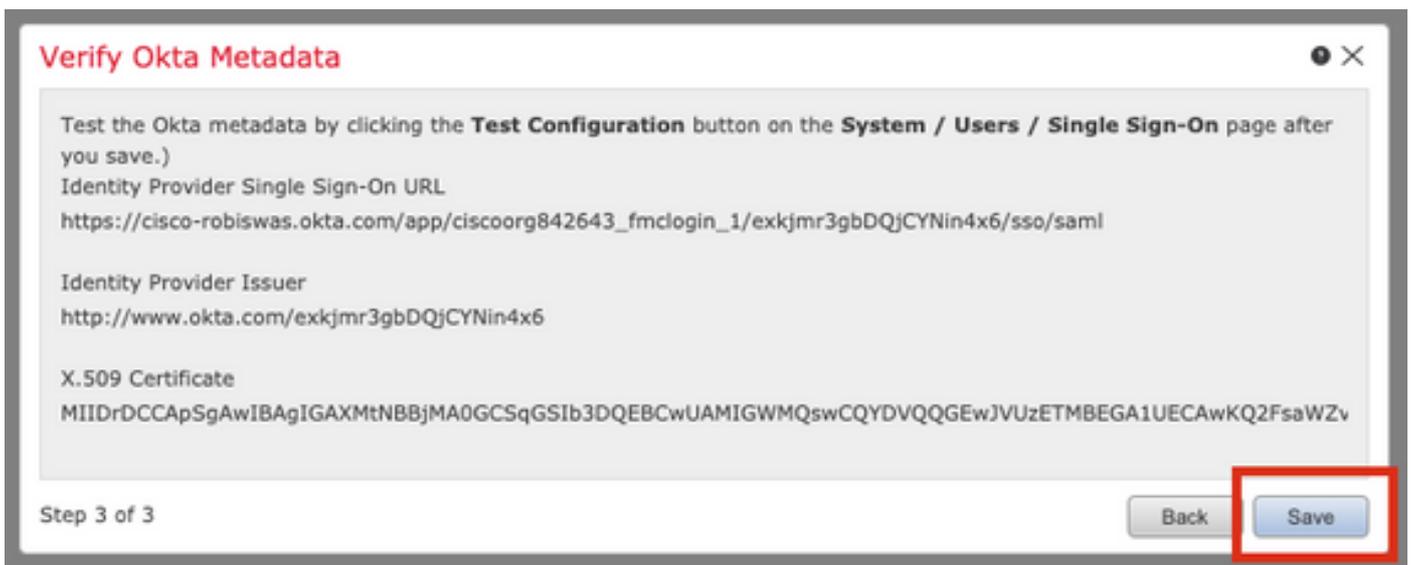
您还可以选择上传XML文件并上传在Okta配置步骤10[中检索](#)的XML文件。



上传文件后，FMC将显示元数据。单击Next，如下图所示。



步骤7. 检验元数据。单击Save，如此图所示。



步骤8. 在Advanced Configuration下配置Role Mapping/Default User Role。

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

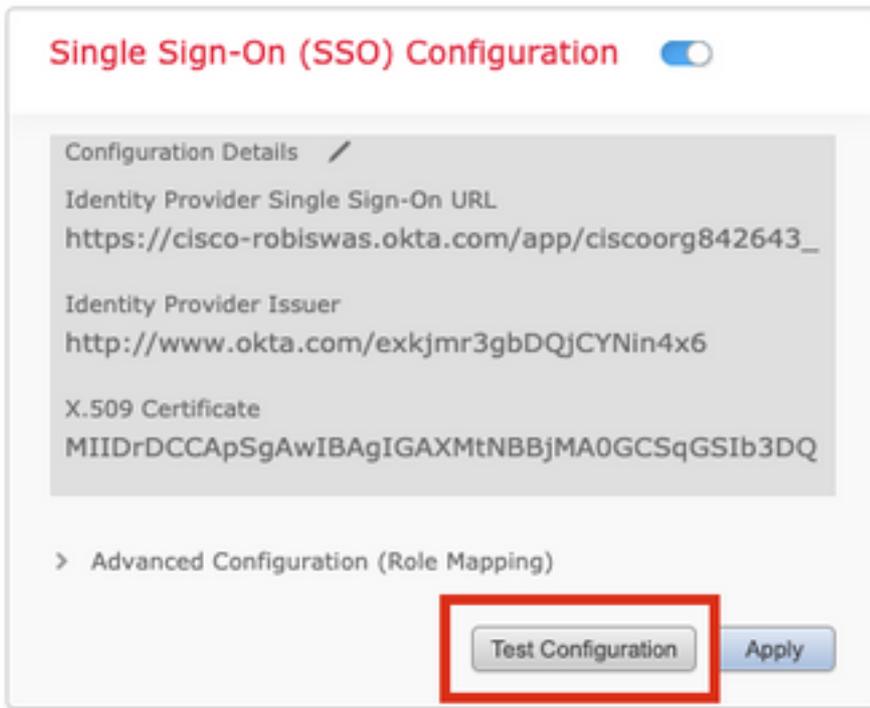
Security Analyst

Security Analyst (Read Only)

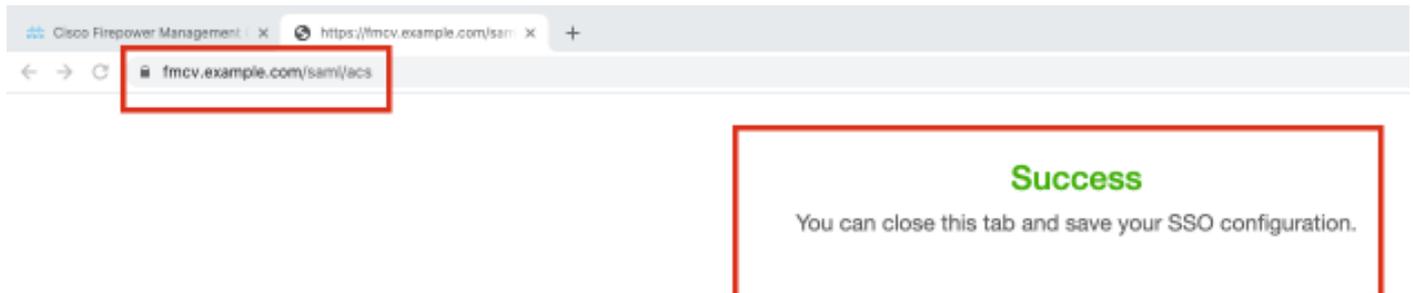
Security Approver

Threat Intelligence Director (TID) User

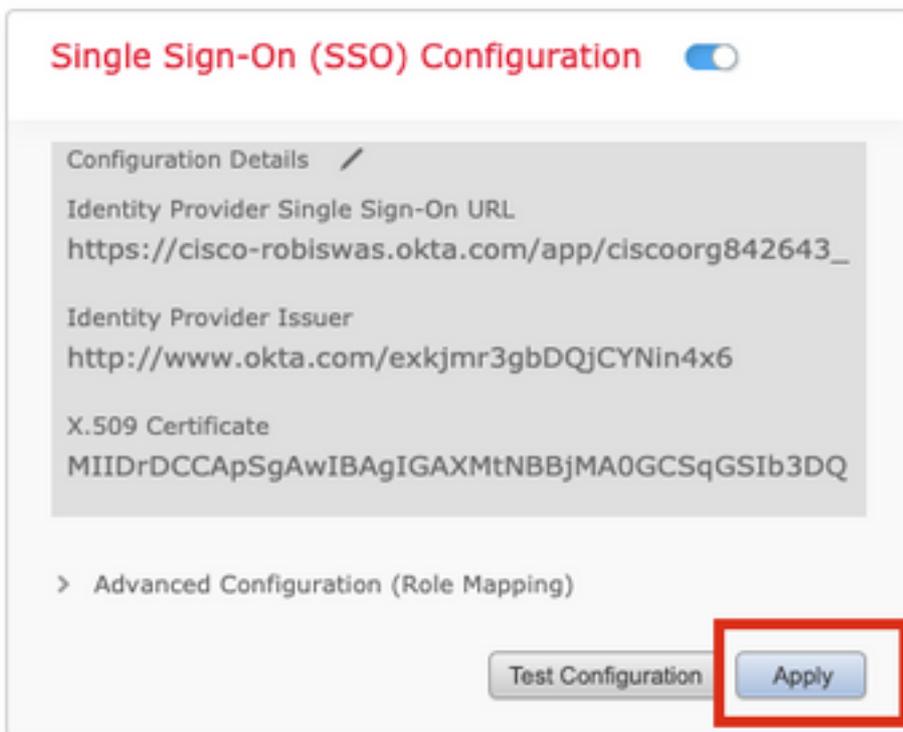
步骤9.要测试配置，请单击**测试配置**，如本图所示。



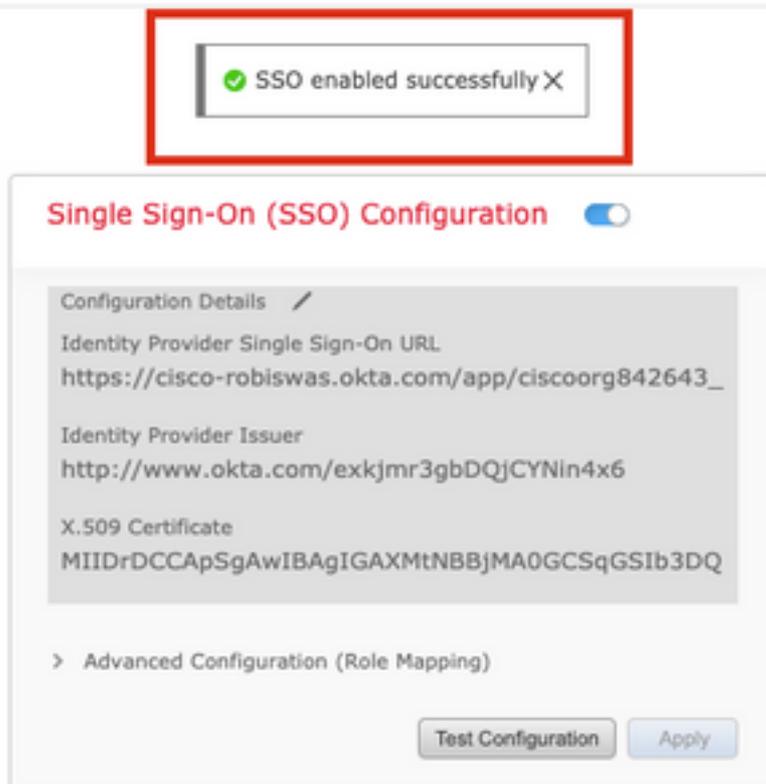
如果测试成功，您应在浏览器的新选项卡上看到此图像中显示的页面。



步骤10.单击“应用”保存配置。



SSO应该已成功启用。



验证

从浏览器导航至FMC URL:https://<fmc URL>。单击Single Sign-On。



Firepower Management Center

Username

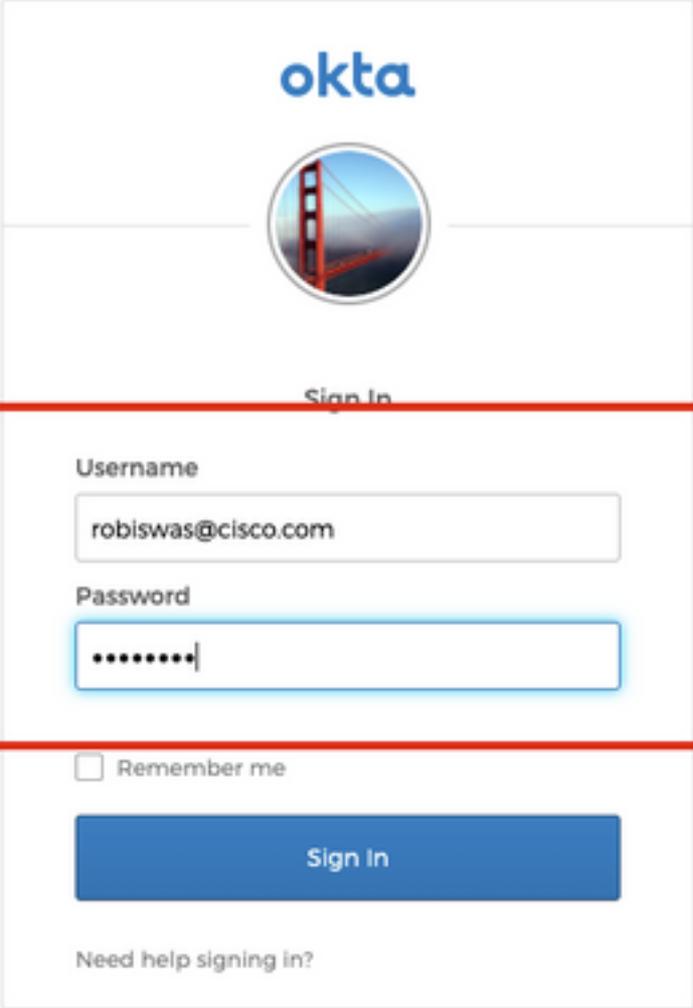
Password

[Single Sign-On](#)

[Log In](#)

您将被重定向到iDP(Okta)登录页。提供您的SSO凭证。单击“**Sign in (登录)**”。

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 text "Sign In" is centered below the profile picture. 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 checkbox labeled "Remember me" which is unchecked. A blue "Sign In" button is positioned below the checkbox. At the bottom of the form, there is a link that says "Need help signing in?".

如果成功，您应该能够登录并查看FMC默认页面。

在FMC上，导航至**System > Users**，查看已添加到数据库的SSO用户。

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