

通過Okta的SSO身份驗證配置Firepower管理中心訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[限制和限制](#)

[配置步驟](#)

[身份提供程式\(Okta\)上的配置步驟](#)

[FMC的配置步驟](#)

[驗證](#)

簡介

本文檔介紹如何配置Firepower管理中心(FMC)以使用單一登入(SSO)進行身份驗證，以便進行管理訪問。

必要條件

需求

思科建議您瞭解以下主題：

- 對單點登入和SAML的基本瞭解
- 瞭解身份提供程式(iDP)上的配置

採用元件

本檔案中的資訊是根據以下軟體版本：

- 思科Firepower管理中心(FMC)版本6.7.0
- Okta作為身份提供程式

注意：本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何組態變更的潛在影響。

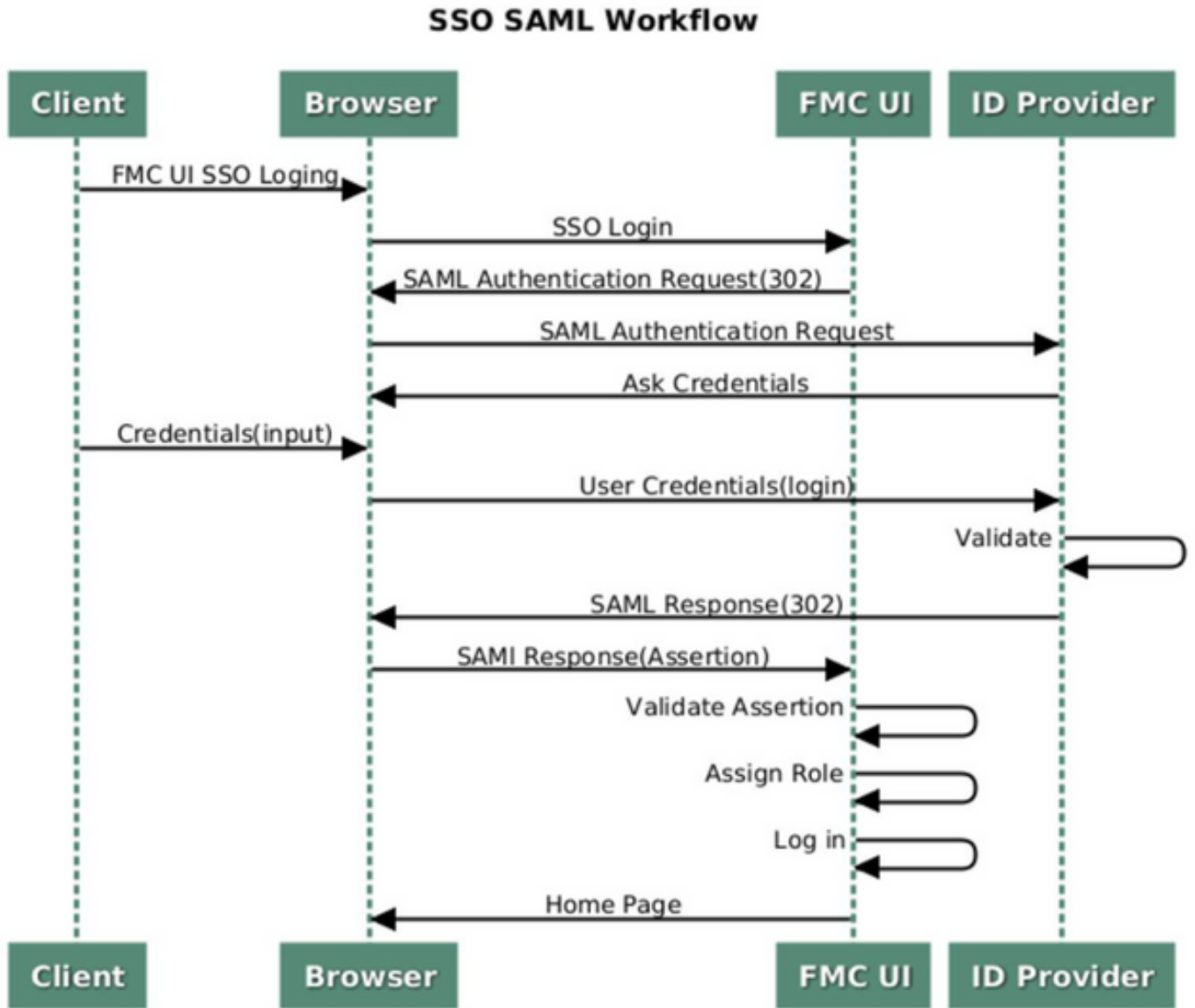
背景資訊

單點登入(SSO)是身份和訪問管理(IAM)的一項屬性，使使用者只需使用一組憑證（使用者名稱和密

碼) 登入一次，即可通過多個應用程式和網站進行安全身份驗證。使用SSO時，使用者嘗試訪問的應用程式或網站依賴於可信的第三方來驗證使用者是否擁有其聲稱的身份。

SAML(Security Assertion Markup Language)是一個基於XML的框架，用於在安全域之間交換驗證和授權資料。它在使用者、服務提供商(SP)和身份提供者(IdP)之間建立一個信任圈，允許使用者一次性登入多個服務

服務提供程式(SP)是接收並接受身份提供程式(iDP)發出的身份驗證斷言的實體。正如其名稱所描述的，服務提供商提供服務，而身份提供者提供使用者的身份(身份驗證)。



這些iDP受支援並進行身份驗證測試：

- 奧克塔
- OneLogin
- PingID
- Azure AD
- 其他 (符合SAML 2.0的任何iDP)

注意：無新許可證要求。此功能在許可模式和評估模式下均可用。

限制和限制

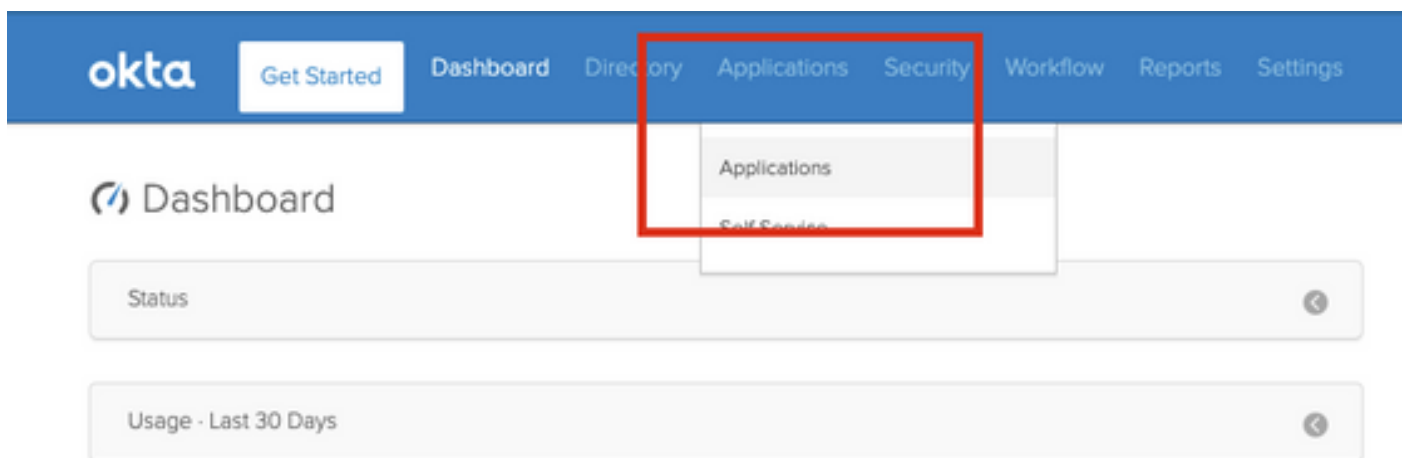
以下是用於FMC訪問的SSO身份驗證的已知限制和限制：

- 只能為全域性域配置SSO
- HA配對中的FMC需要單獨配置
- 只有本地/AD管理員才能在FMC上配置SSO (SSO管理員使用者將無法在FMC上配置/更新SSO設定)。

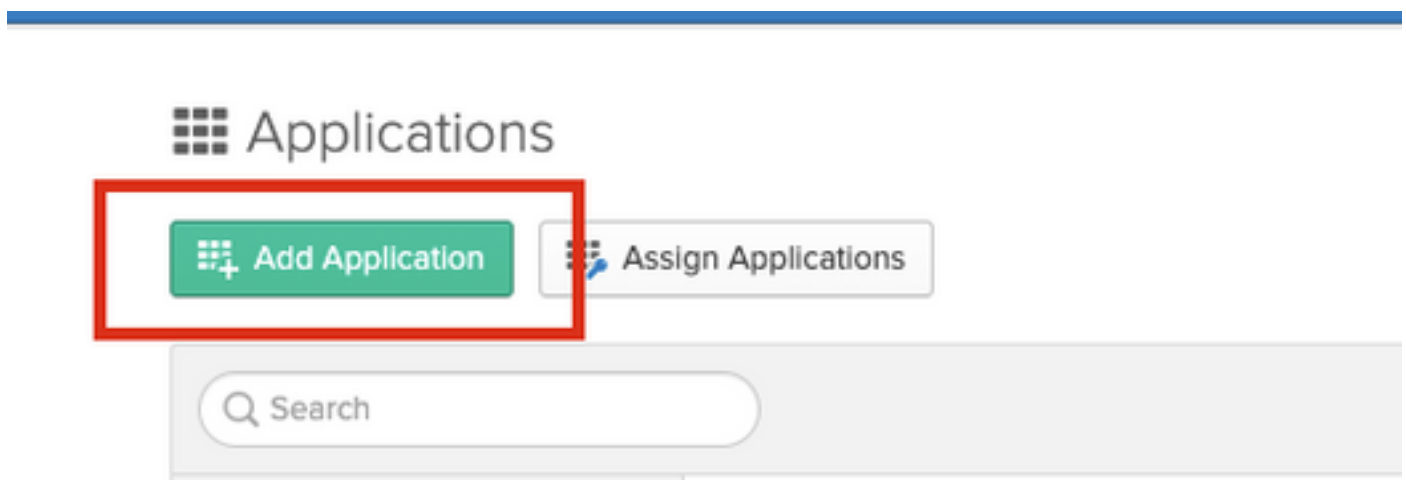
配置步驟

身份提供程式(Okta)上的配置步驟

步驟1.登入Okta門戶。導覽至Applications > Applications，如下圖所示。



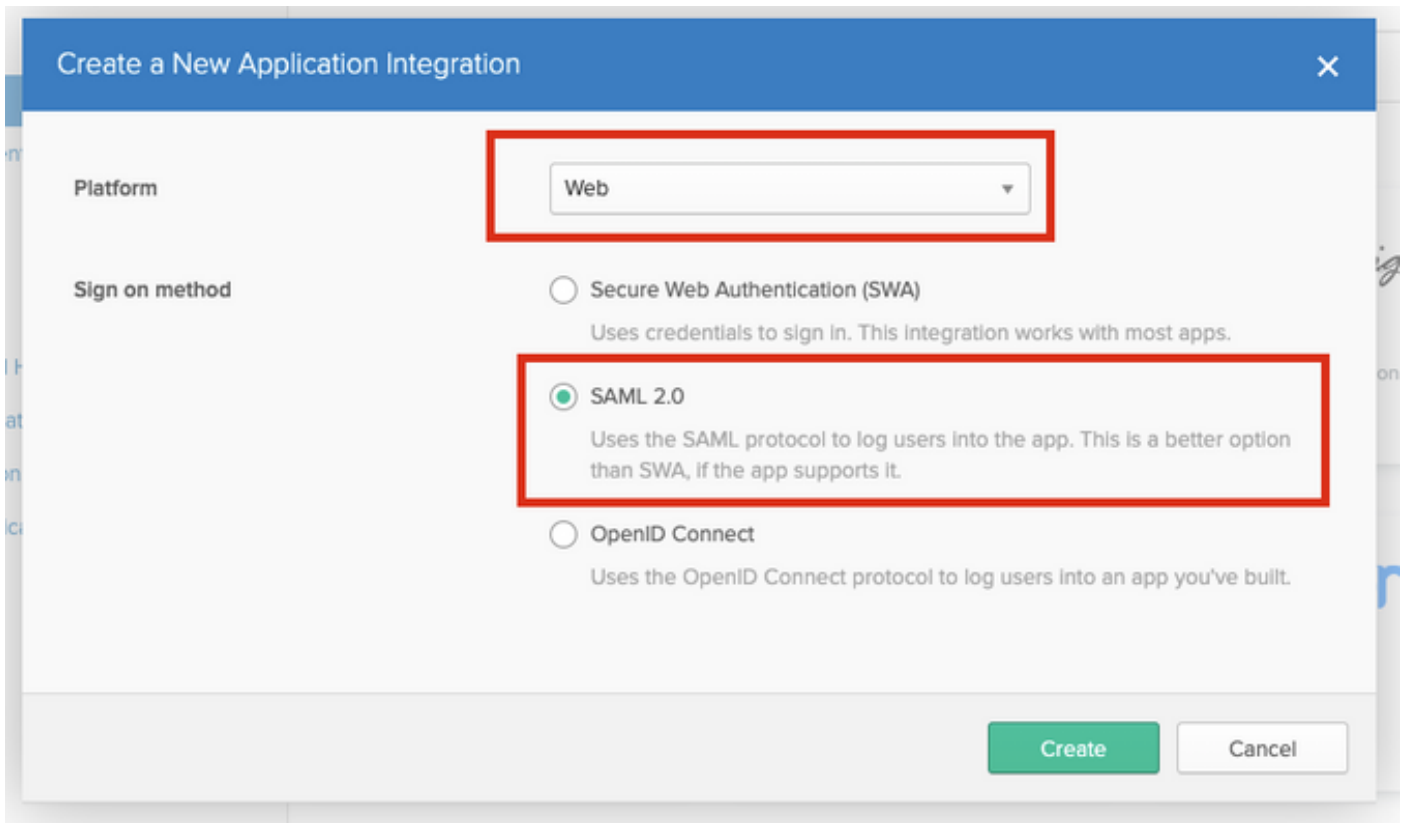
步驟2.如本圖所示，按一下AddApplication。



步驟3.如本圖所示，按一下Create NewApp。



步驟4.選擇Platform作為Web。選擇Sign On method 作為 SAML 2.0。按一下Create，如下圖所示。




步驟5.提供App 名稱、App徽標（可選），然後按一下Next，如下圖所示。

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

步驟6.輸入SAML設定。

單點登入URL:https://<fmc URL>/saml/acs

受眾URI (SP實體ID) : https://<fmc URL>/saml/metadata

預設中繼狀態:/ui/login

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

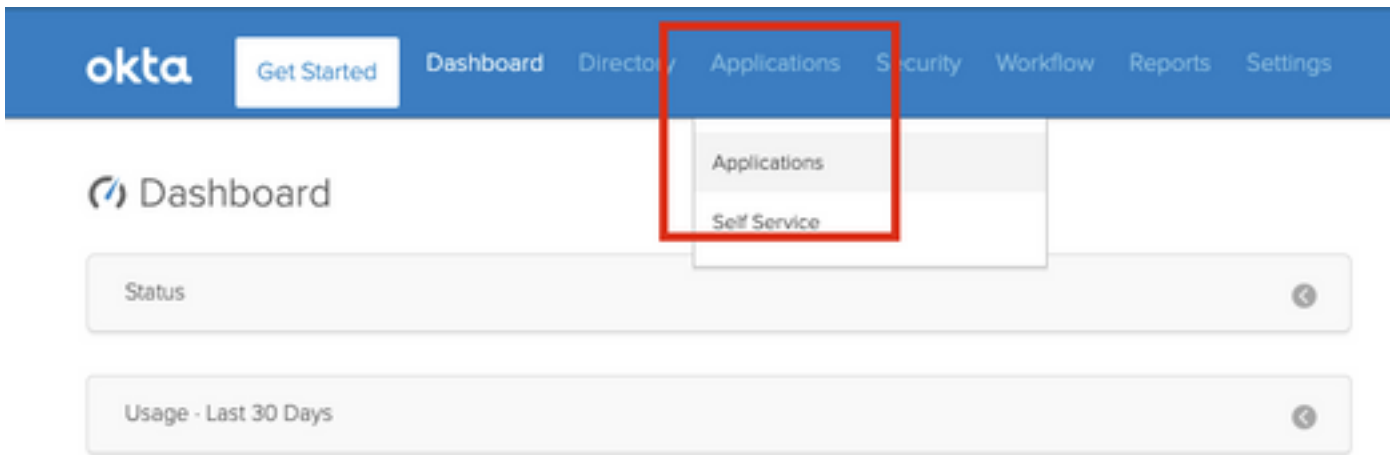
Name format (optional)

Value

Unspecified

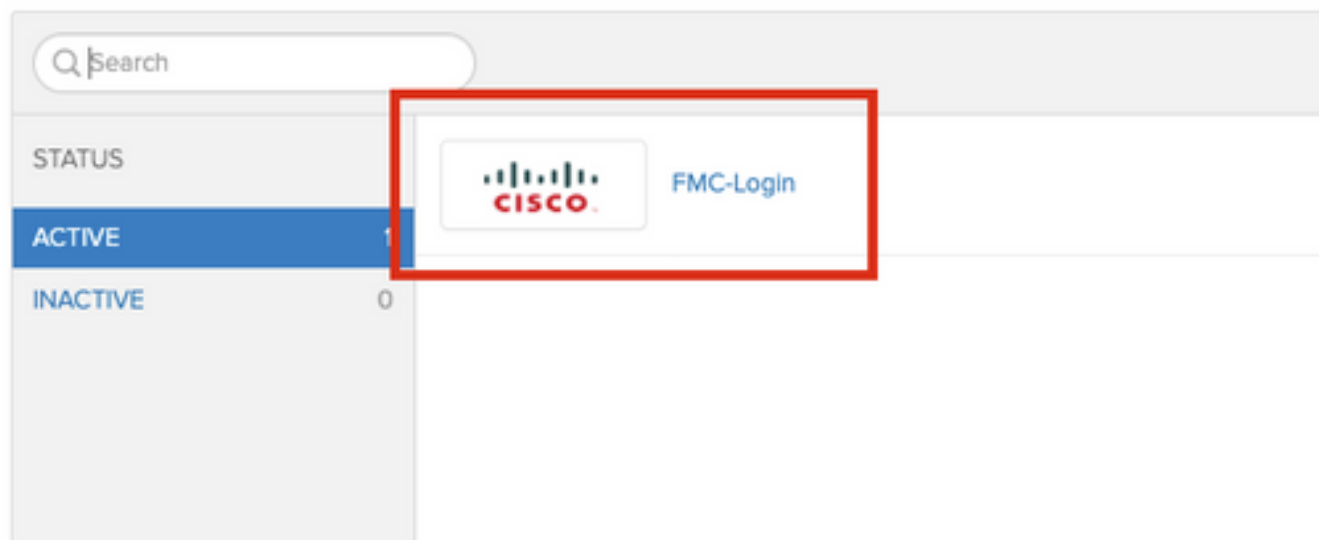
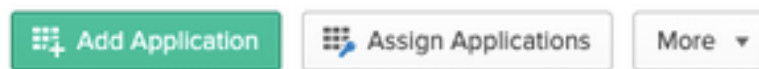
[Add Another](#)

步驟7. 導覽至 Applications > Applications , 如下圖所示。



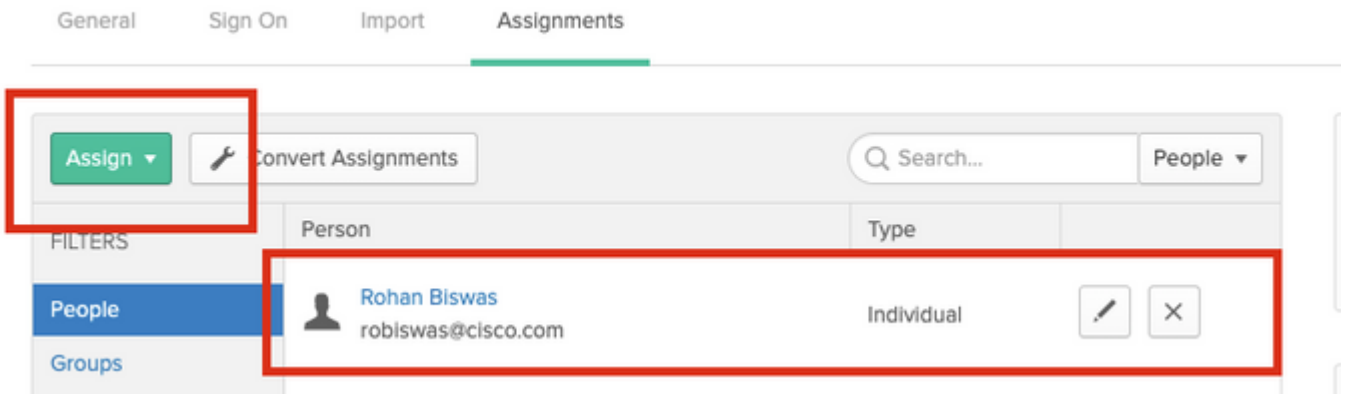
步驟8.按一下建立的應用程式名稱。

Applications

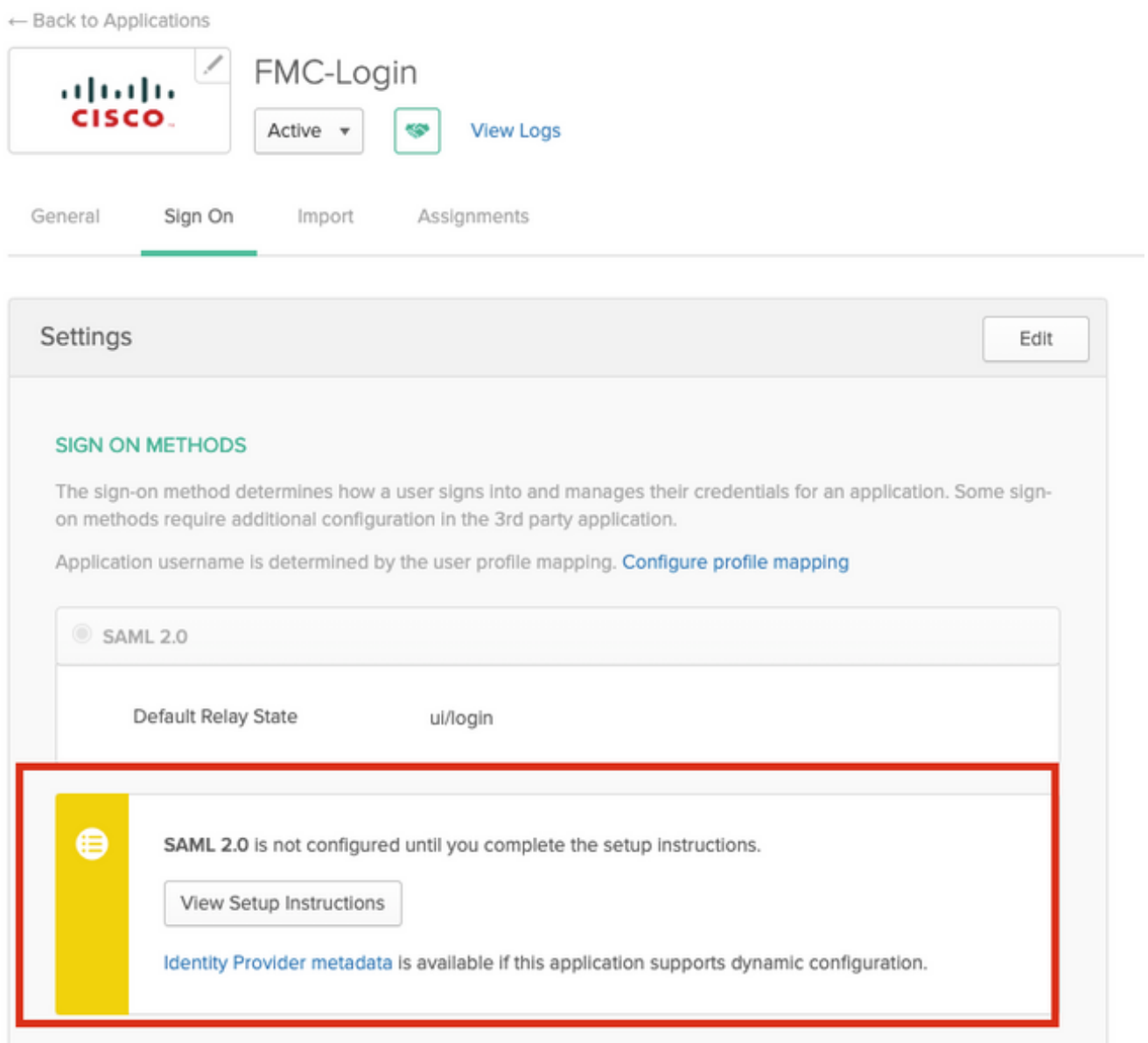


步驟9.定位至分配。按一下Assign。

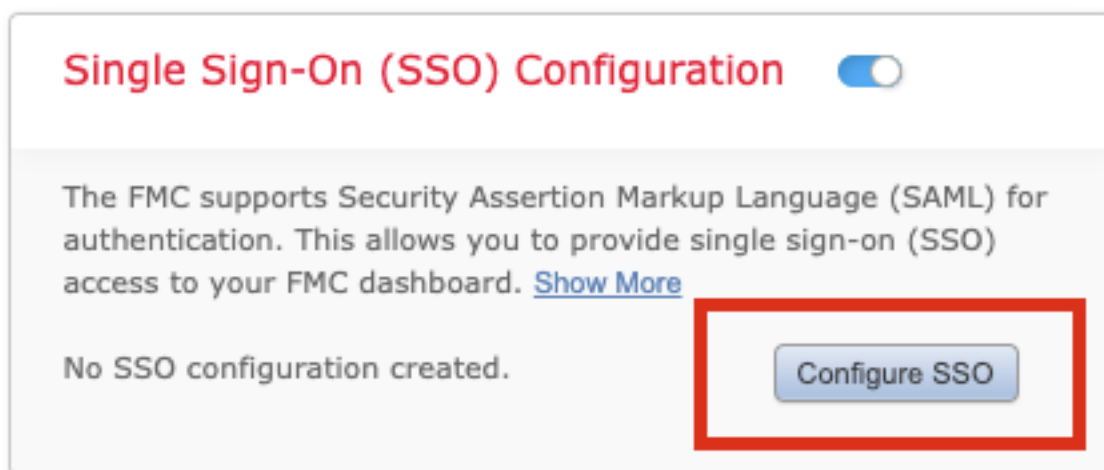
您可以選擇將單個使用者或組分配給建立的應用程式名稱。



步驟10. 導覽至 Sign On。按一下檢視安裝說明。按一下 Identity Provider metadata 檢視 iDP 的後設資料。



將檔案另存為.xml檔案，以便在FMC上使用。

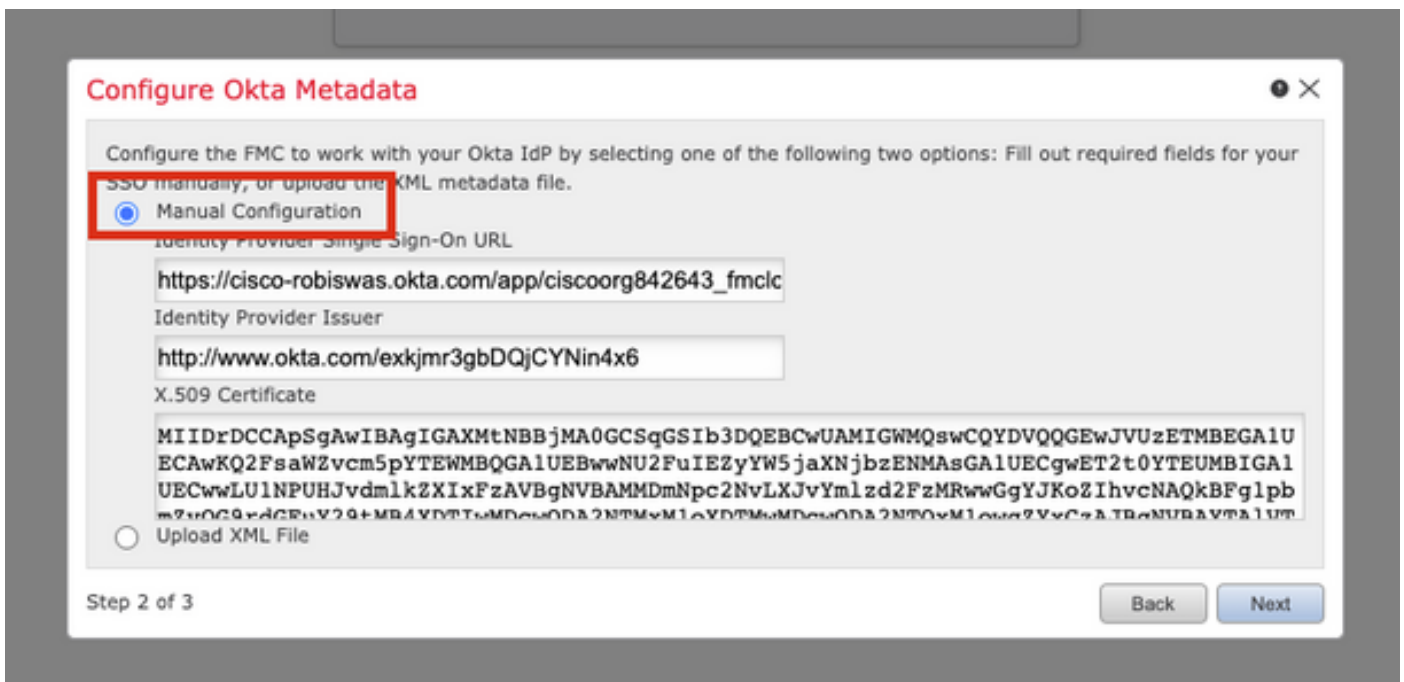


步驟5.選擇FMC SAML提供程式。按「Next」（下一步）。

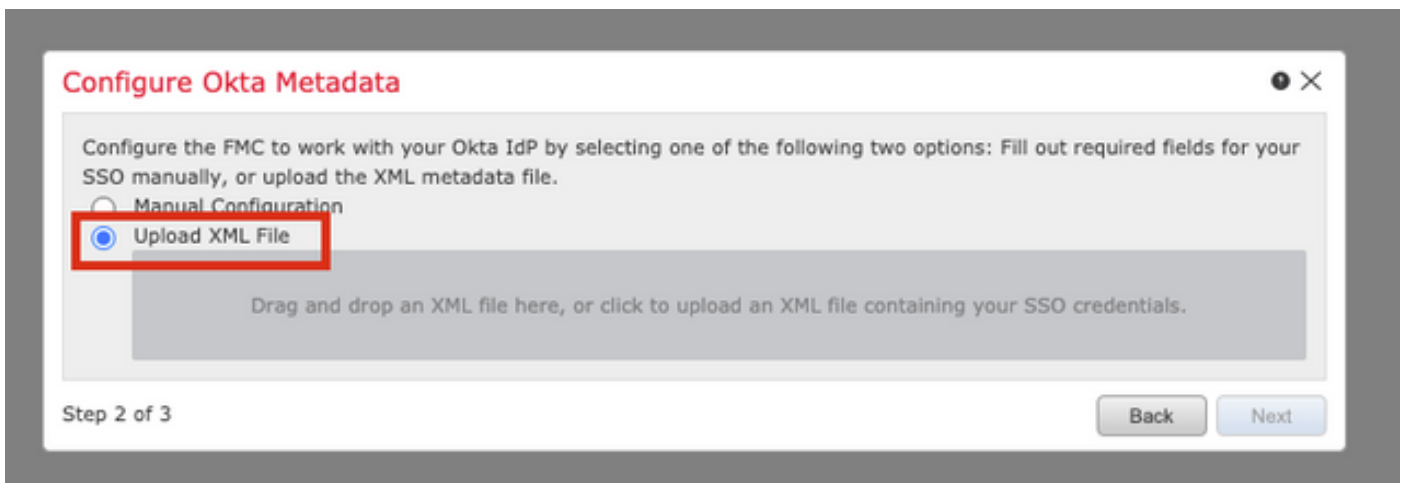
在本演示中，使用Okta。



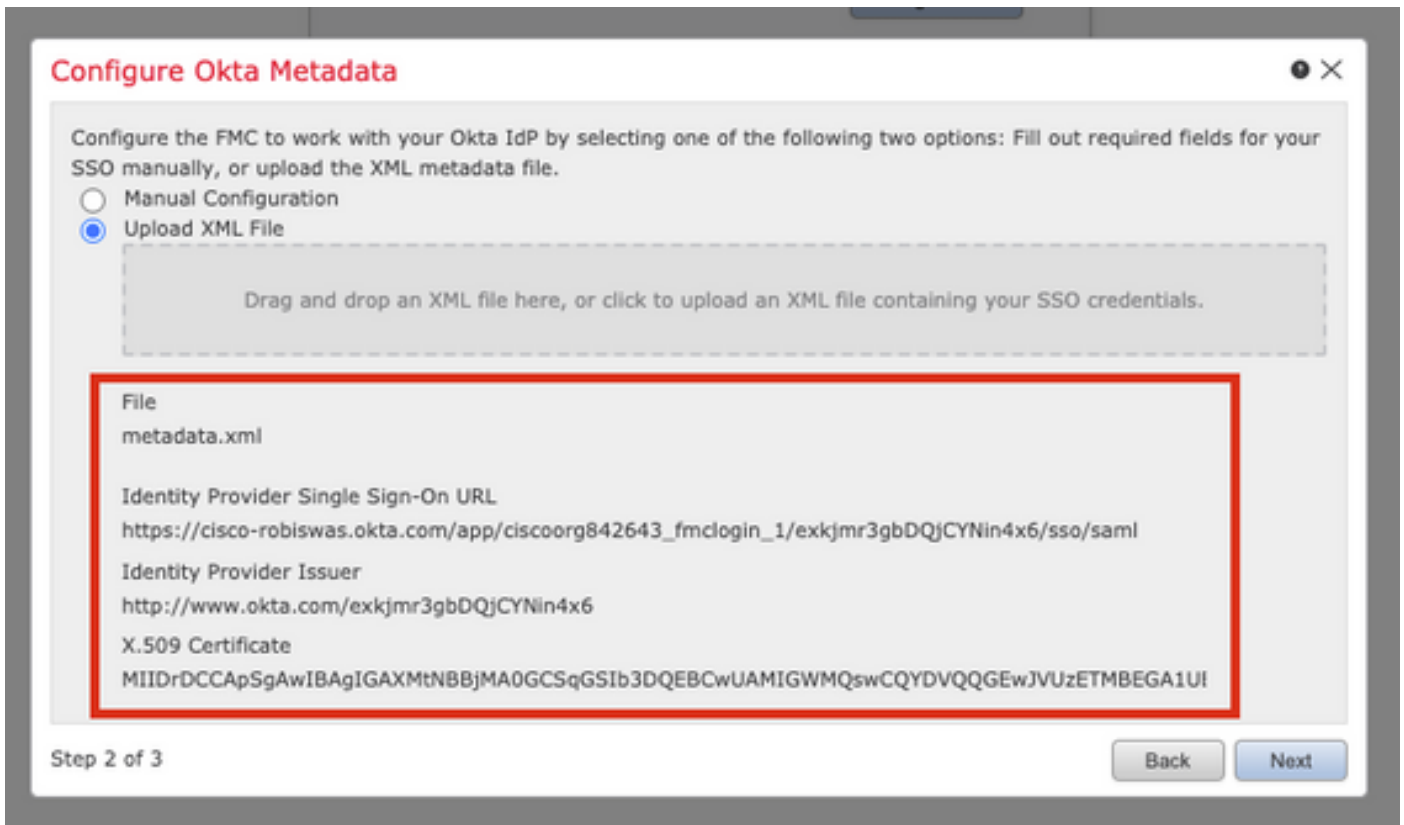
步驟6.您可以選擇**手動配置**，然後手動輸入iDP資料。按一下**Next**，作為



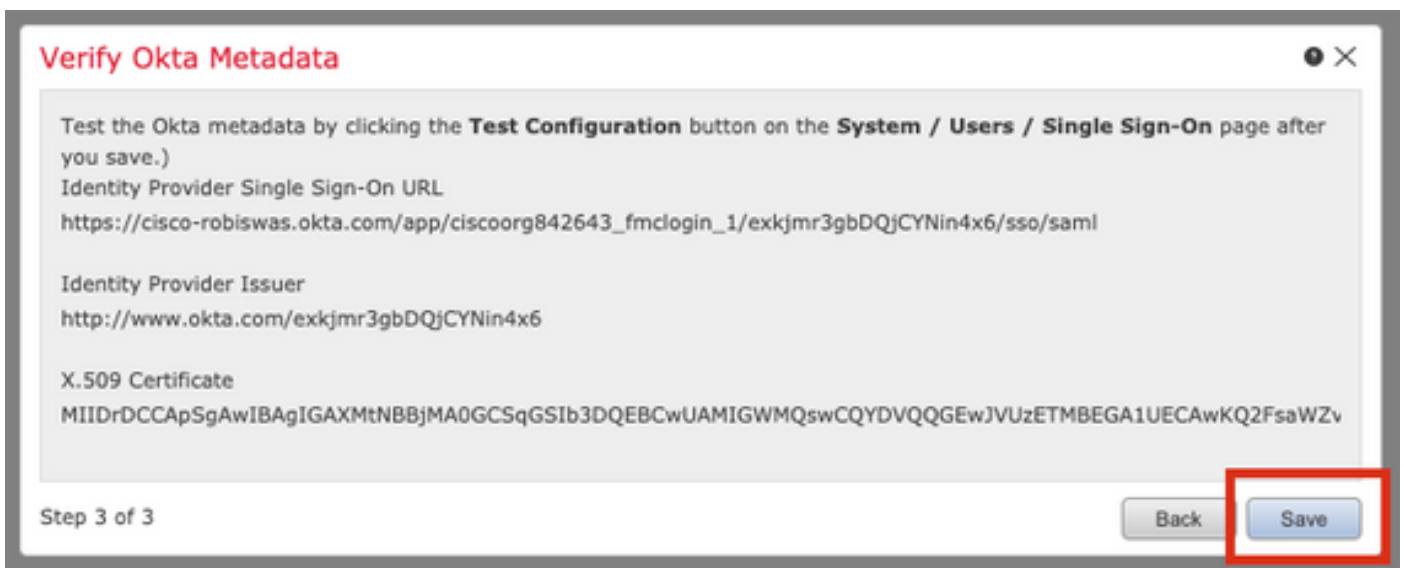
您還可以選擇上傳XML檔案，並上傳在[Okta配置](#)的步驟10中檢索的XML檔案。



一旦上傳檔案，FMC將顯示後設資料。按一下「Next」，如下圖所示。



步驟7. 驗證後設資料。按一下「Save」，如下圖所示。



步驟8. 在高級配置下配置角色對映/預設使用者角色。

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

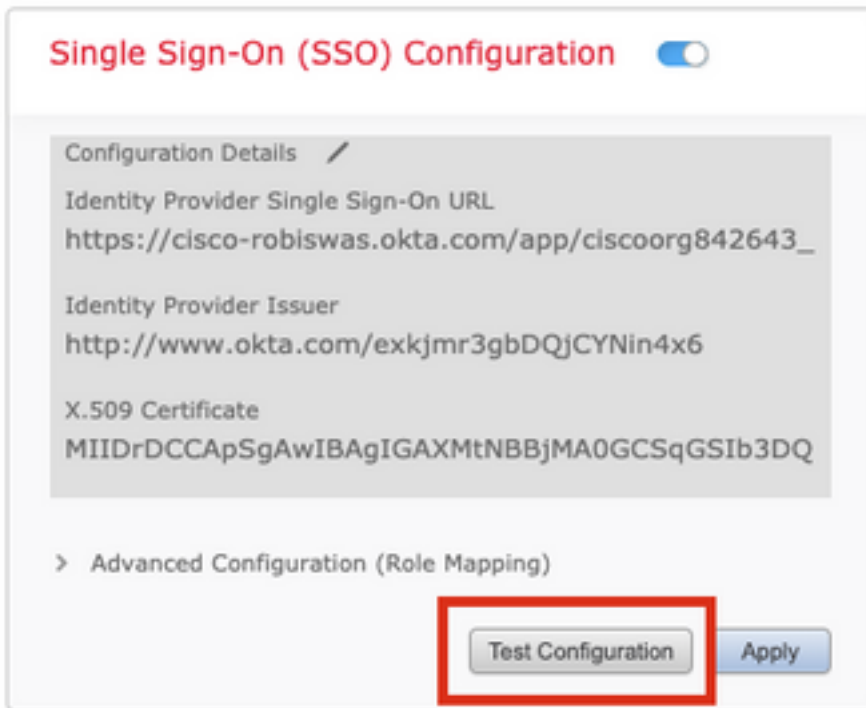
Security Analyst

Security Analyst (Read Only)

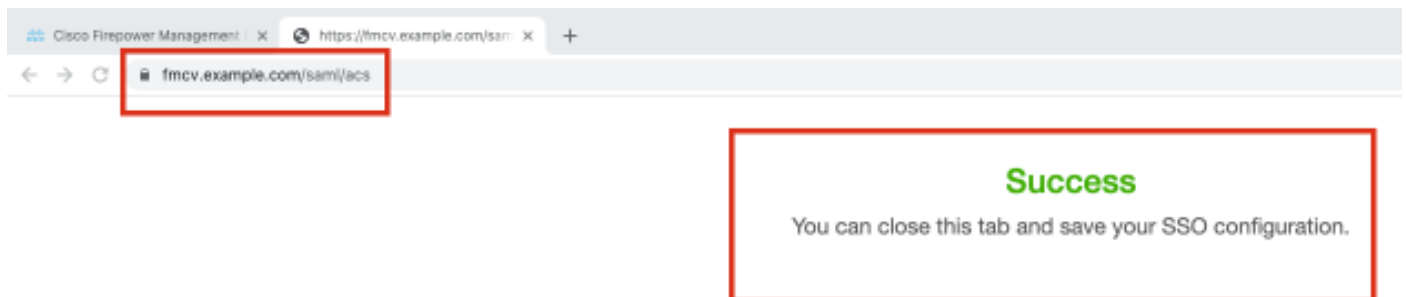
Security Approver

Threat Intelligence Director (TID) User

步驟9.若要測試組態，請按一下**Test Configuration**，如下圖所示。



如果測試成功，您應該會看到此圖中所示的頁面，位於瀏覽器上的新頁籤上。



步驟10. 按一下**Apply** 以儲存組態。

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)

Test Configuration **Apply**

應成功啟用SSO。

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/exkjm3gbDQjCYNin4x6

X.509 Certificate
MIIDrDCCApSgAwIBAgIGAXMtNBBjMA0GCSqGSIb3DQ

> Advanced Configuration (Role Mapping)

Test Configuration Apply

驗證

從瀏覽器導航至FMC URL:https://<fmc URL>。按一下Single Sign-On。



Firepower Management Center


Username

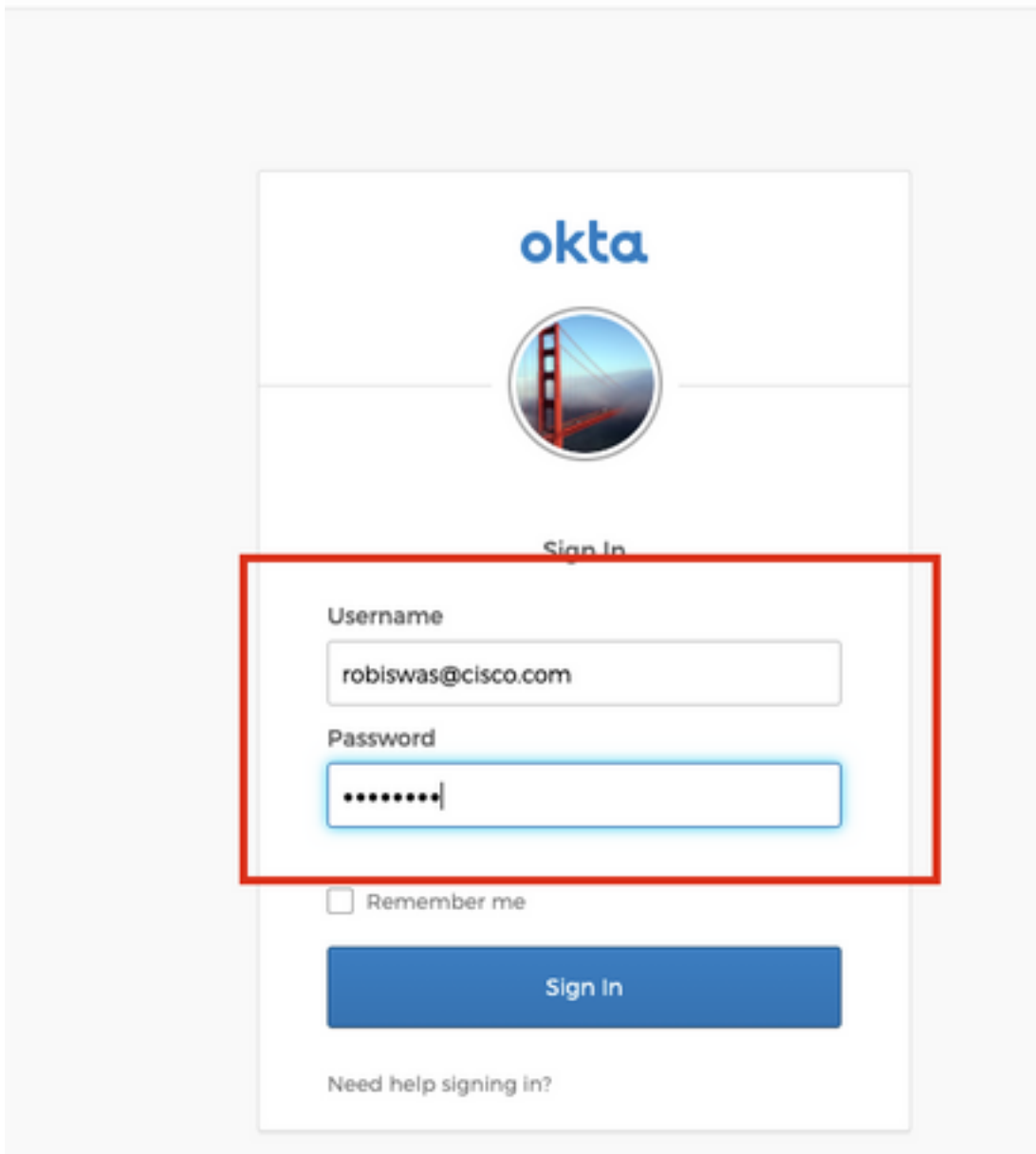
Password

[Single Sign-On](#)

[Log In](#)

系統會將您重新導向至iDP(Okta)登入頁面。提供您的SSO憑據。按一下登入。

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



The image shows an Okta sign-in page. At the top, the Okta logo is displayed in blue. Below the logo 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，您應該能夠登入並檢視FMC預設頁面。

在FMC上，導航到**System > Users**，檢視新增到資料庫的SSO使用者。

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