

Configurazione dell'accesso a Firepower Management Center tramite autenticazione SSO con Okta

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Limitazioni e restrizioni](#)

[Procedura di configurazione](#)

[Procedura di configurazione nel provider di identità \(Okta\)](#)

[Procedura di configurazione in FMC](#)

[Verifica](#)

Introduzione

In questo documento viene descritto come configurare Firepower Management Center (FMC) per l'autenticazione tramite Single Sign-On (SSO) per l'accesso di gestione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Single Sign-On e SAML
- Informazioni sulla configurazione del provider di identità (iDP)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco Firepower Management Center (FMC) versione 6.7.0
- Okta come provider di identità

Nota: Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali modifiche alla configurazione.

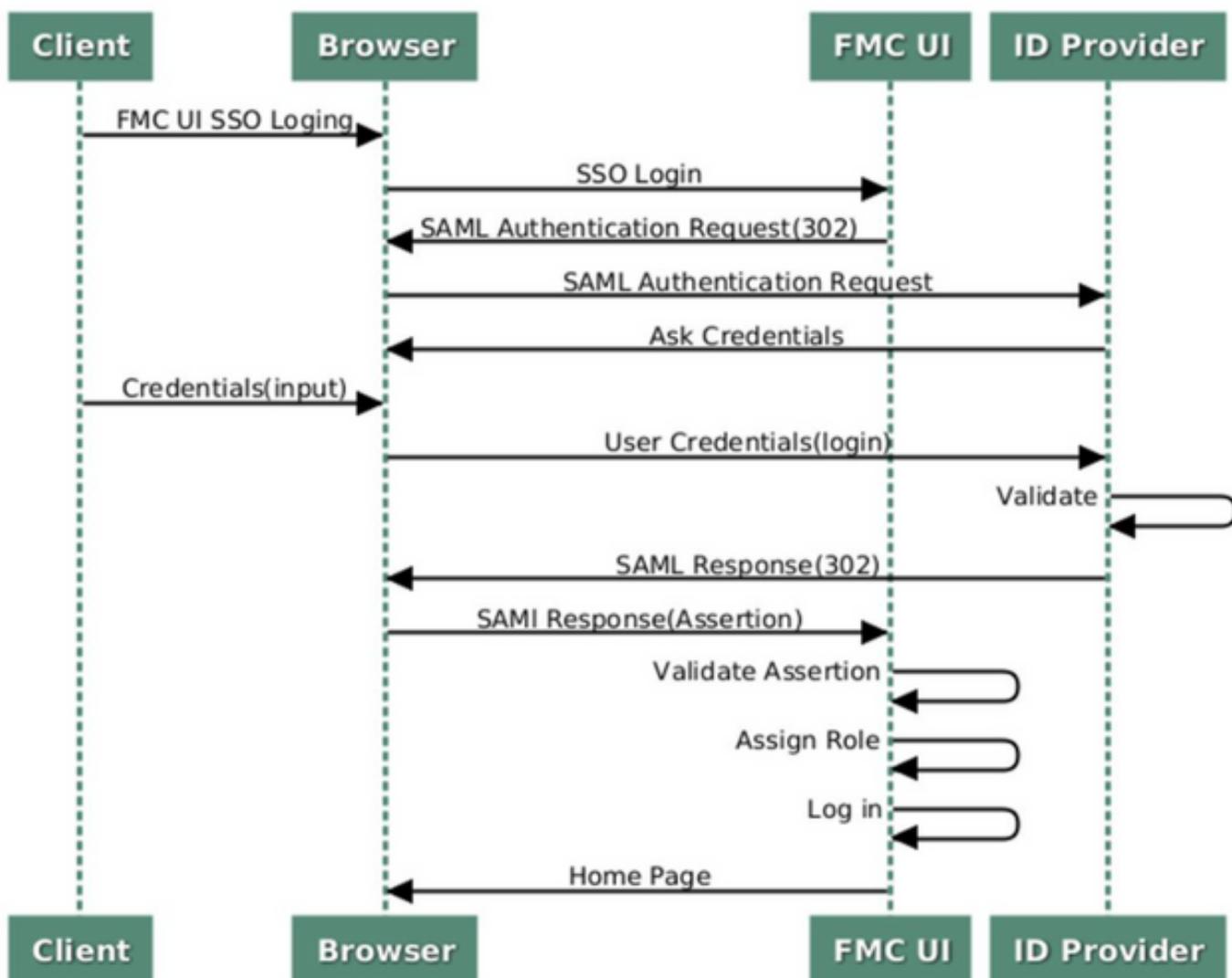
Premesse

Single Sign-On (SSO) è una proprietà di gestione delle identità e degli accessi (IAM) che consente agli utenti di autenticarsi in modo sicuro con più applicazioni e siti Web eseguendo l'accesso una sola volta con un solo insieme di credenziali (nome utente e password). Con SSO, l'applicazione o il sito Web a cui l'utente sta tentando di accedere si basa su una terza parte attendibile per verificare che gli utenti siano chi dicono di essere.

SAML (Security Assertion Markup Language) è un framework basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza. Crea un cerchio di fiducia tra l'utente, un provider di servizi (SP) e un provider di identità (IdP) che consente all'utente di accedere una sola volta a più servizi

Un provider di servizi (SP) è un'entità che riceve e accetta un'asserzione di autenticazione emessa da un provider di identità (iDP). Come descritto dai rispettivi nomi, i provider di servizi forniscono i servizi mentre i provider di identità forniscono l'identità degli utenti (autenticazione).

SSO SAML Workflow



Questi iDP sono supportati e testati per l'autenticazione:

- Okta

- OneLogin
- IDping
- Azure AD
- Altri (qualsiasi iDP conforme a SAML 2.0)

Nota: nessuna nuova licenza richiesta. Questa funzione funziona sia in modalità di valutazione che in modalità con licenza.

Limitazioni e restrizioni

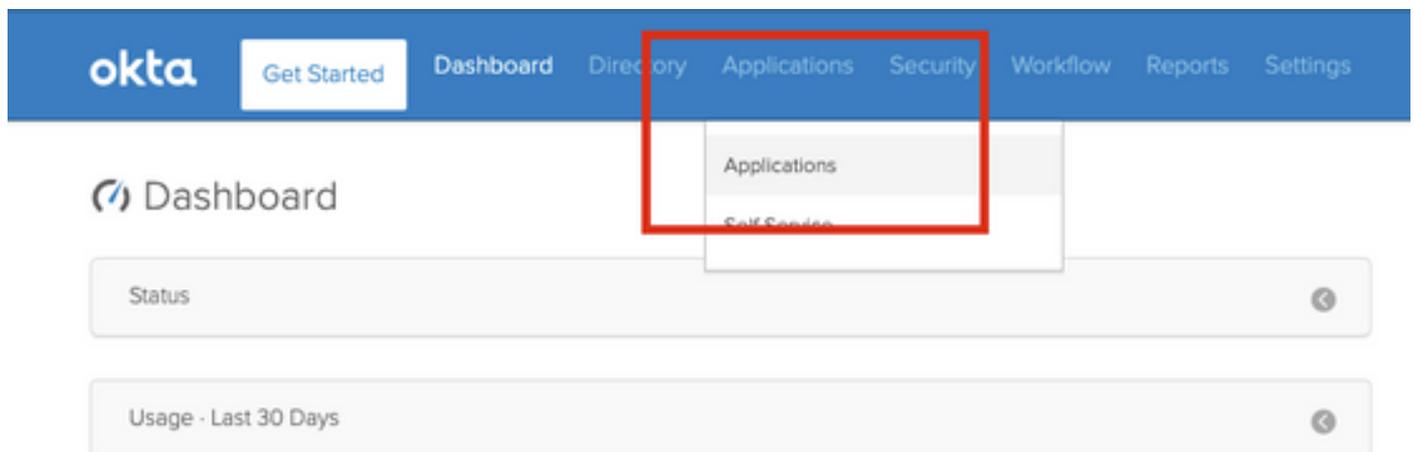
Si tratta di limitazioni e restrizioni note per l'autenticazione SSO per l'accesso FMC:

- SSO può essere configurato solo per il dominio globale
- I FMC in coppia HA richiedono una configurazione individuale
- Solo gli amministratori locali/AD possono configurare SSO su FMC (gli utenti amministratori SSO non potranno configurare/aggiornare le impostazioni SSO su FMC).

Procedura di configurazione

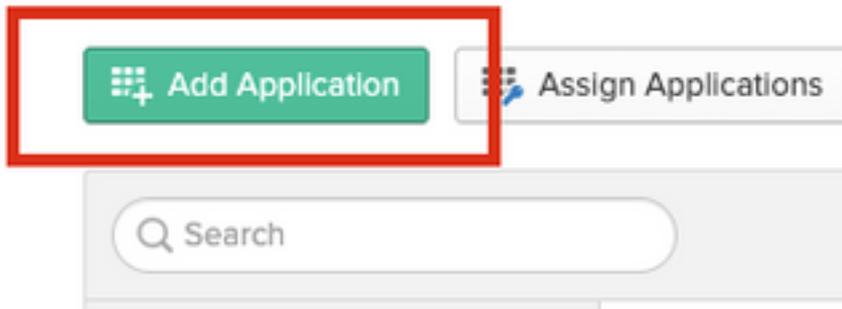
Procedura di configurazione nel provider di identità (Okta)

Passaggio 1. Accedere al portale Okta. Passare a **Applicazioni > Applicazioni**, come mostrato in questa immagine.



Passaggio 2. Come mostrato nell'immagine, fare clic su **AddApplication**.

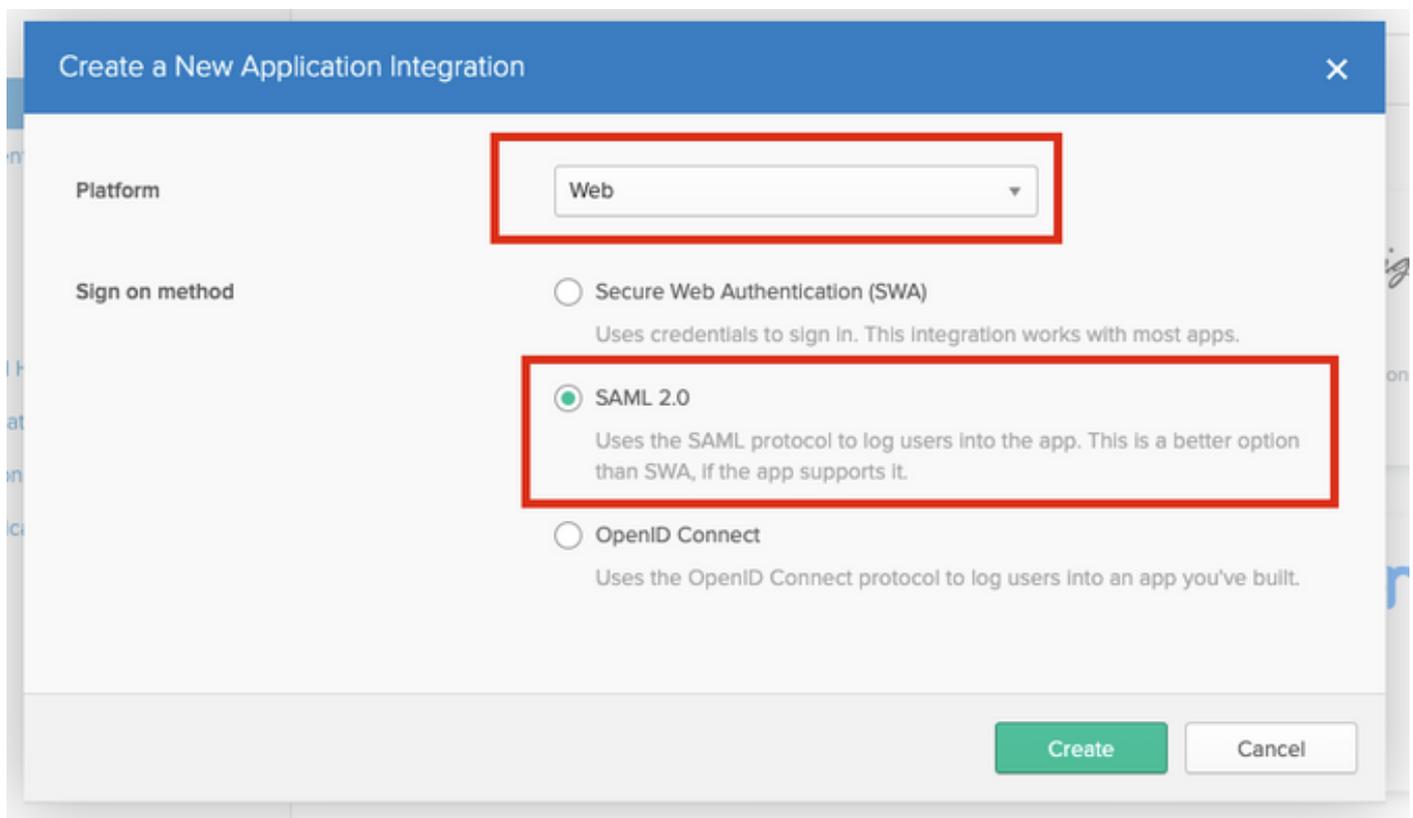
Applications



Passaggio 3. Come mostrato in questa immagine, fare clic su **Create NewApp** (Crea nuova app).



Passaggio 4. Scegliere **Piattaforma** come **Web**. Scegliere il metodo **Sign On** come **SAML 2.0**. Fare clic su **Create** (Crea), come mostrato nell'immagine.



Passaggio 5. Fornire un **nome di app**, il **logo dell'app** (facoltativo) e fare clic su **Avanti**, come mostrato nell'immagine.

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

Passaggio 6. Inserire le impostazioni SAML.

URL Single Sign-On: <https://<URL fmc>/saml/acs>

URI gruppo di destinatari (ID entità SP): <https://<URL fmc>/saml/metadata>

RelayState predefinito: /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](#)

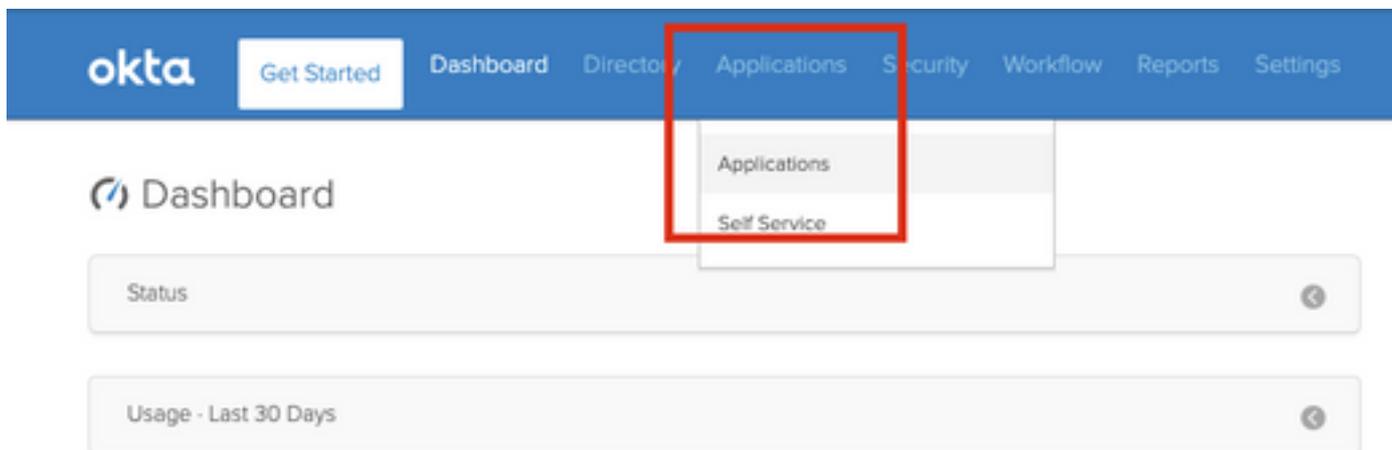
Name

Name format (optional)

Value

[Add Another](#)

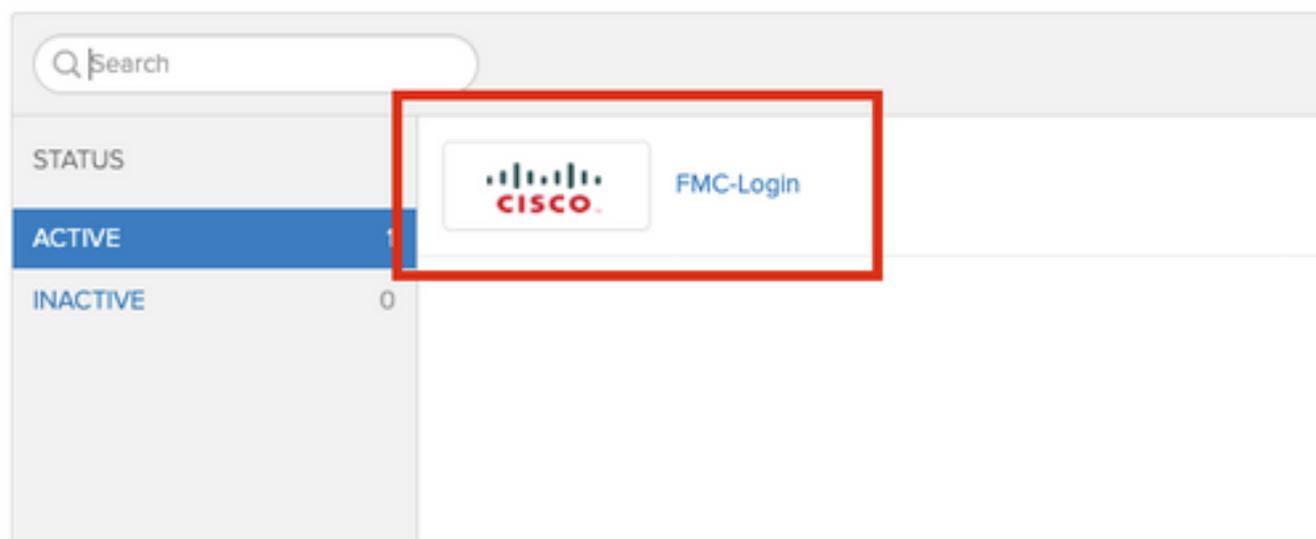
Passaggio 7. Tornare a **Applicazioni > Applicazioni**, come mostrato in questa immagine.



Passaggio 8. Fare clic sul nome dell'app creata.

Applications

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



Passaggio 9. Passare ad **Assegnazioni**. Fare clic su **Assegna**.

È possibile scegliere di assegnare singoli utenti o gruppi al nome dell'app creata.

General Sign On Import **Assignments**

Assign Convert Assignments Search... People

FILTERS

Person	Type
 Rohan Biswas robiswas@cisco.com	Individual

Passaggio 10. Passare a **Sign On**. Fare clic su **Visualizza istruzioni di installazione**. Fare clic sui **metadati del provider di identità** per visualizzare i metadati dell'iDP.

← 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

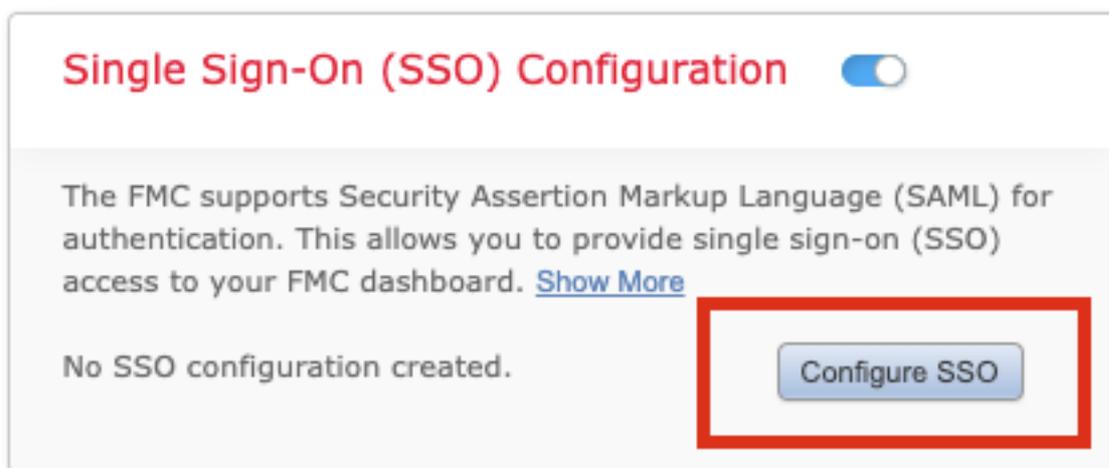
Default Relay State: ui/login

 **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.

Salvare il file come file **xml** da utilizzare nel CCP.

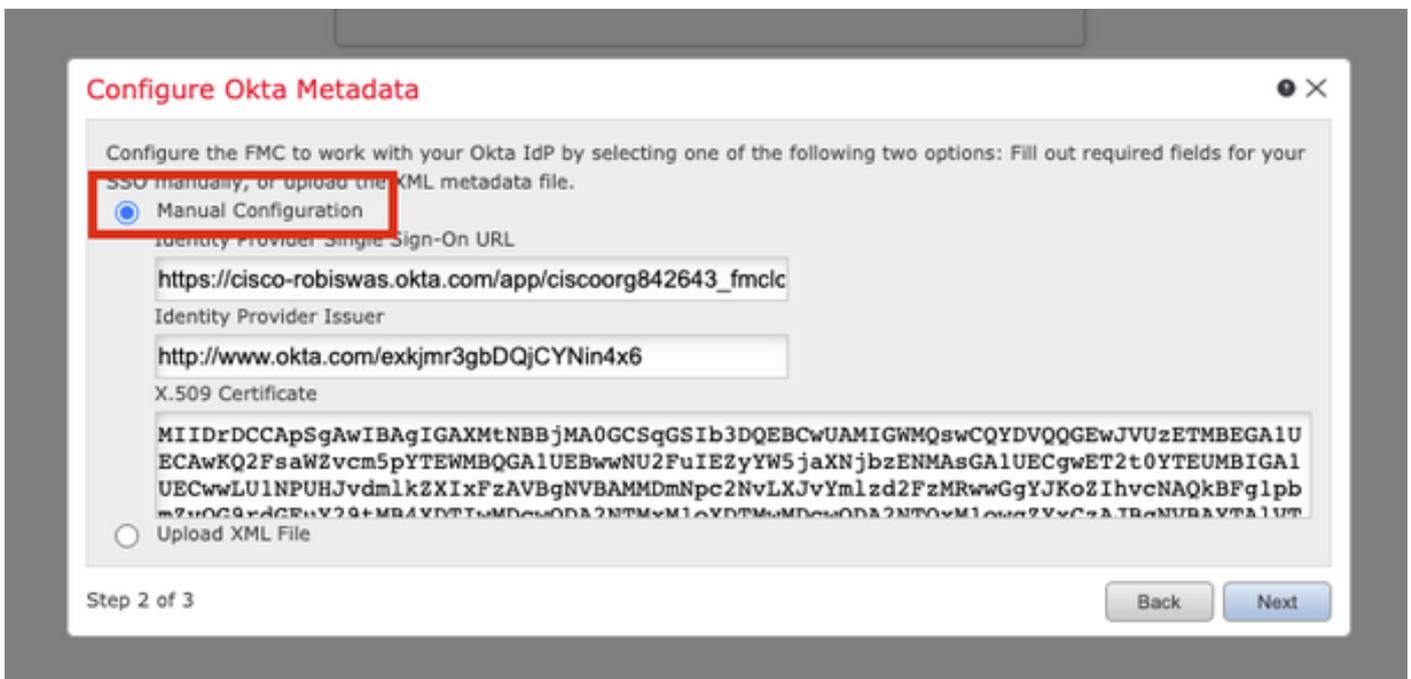


Passaggio 5. Selezionare il **provider SAML FMC**. Fare clic su Next (Avanti).

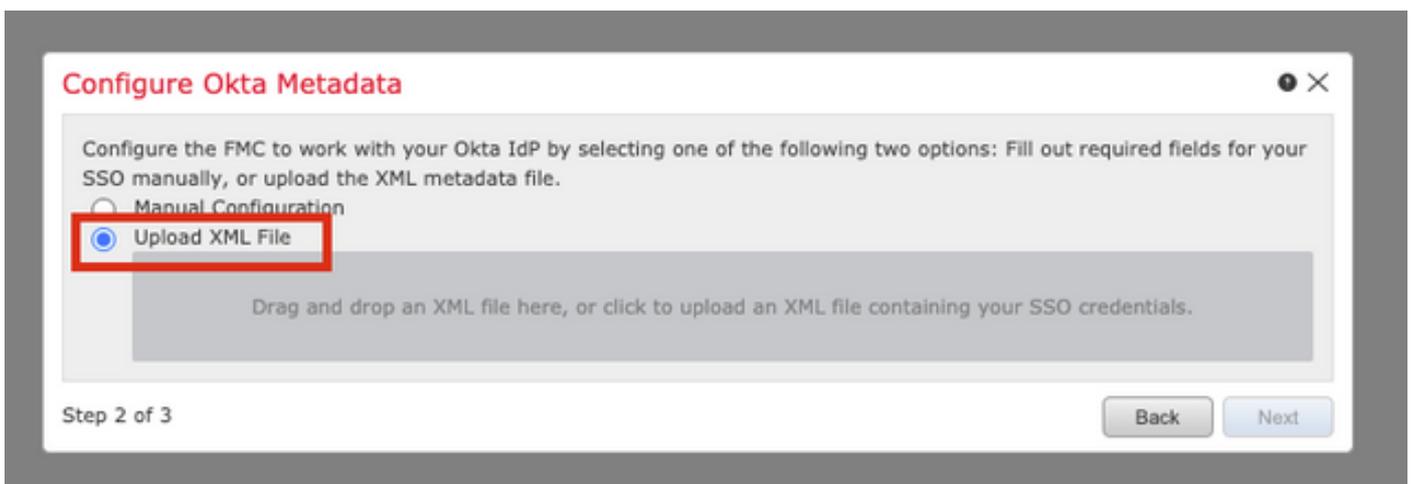
Ai fini della presente dimostrazione, viene utilizzato **Okta**.



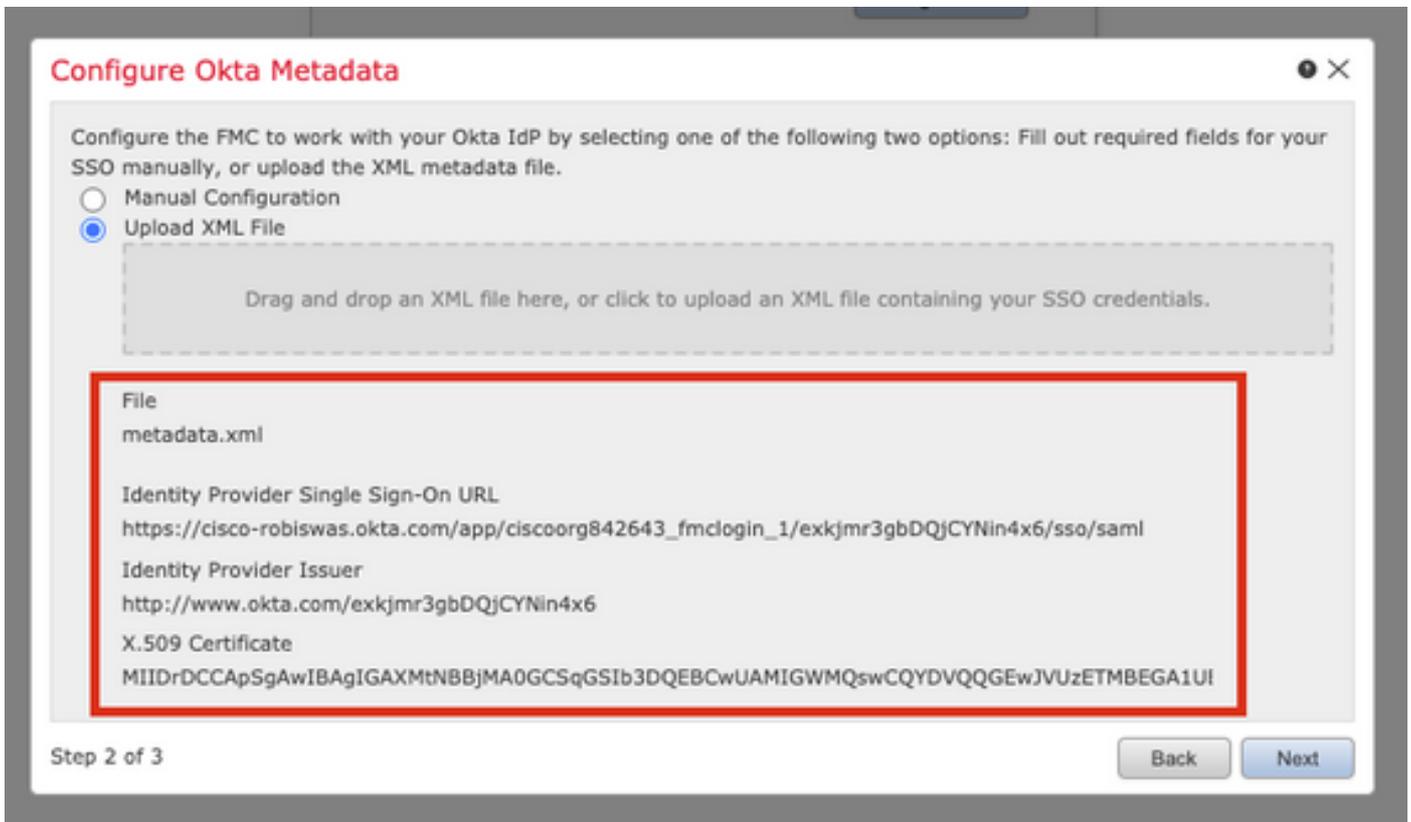
Passaggio 6. È possibile scegliere **Configurazione manuale** e immettere i dati iDP manualmente. Fare clic su **Avanti**, come



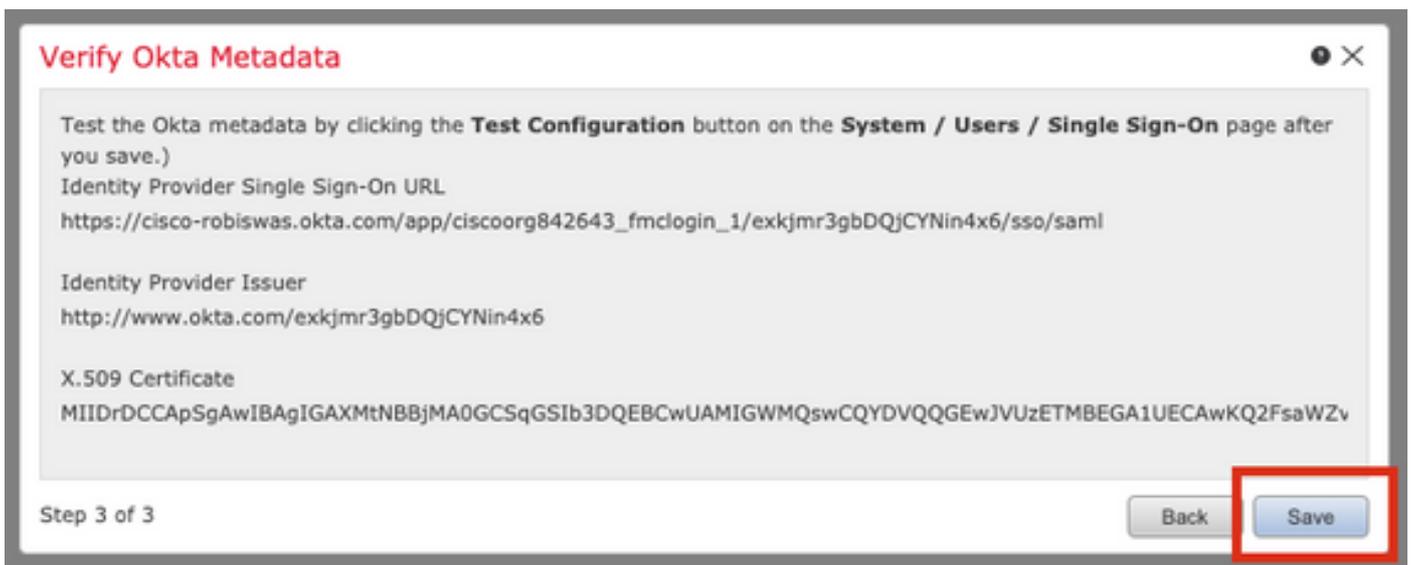
È inoltre possibile scegliere **Carica file XML** e caricare il file XML recuperato nel [passo 10](#) della configurazione Okta.



Una volta caricato il file, il FMC visualizza i metadati. Fare clic su **Avanti**, come mostrato nell'immagine.



Passaggio 7. **Verificare** i metadati. Fare clic su **Save** (Salva), come mostrato nell'immagine.



Passaggio 8. Configurare il **mapping ruoli/ruolo utente predefinito** in **Configurazione avanzata**.

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

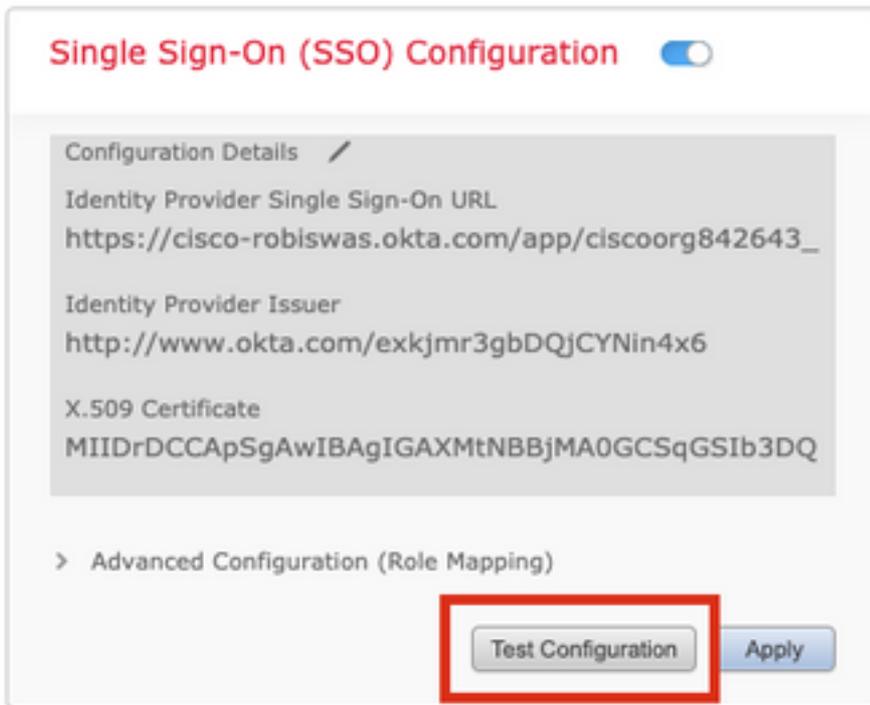
Security Analyst

Security Analyst (Read Only)

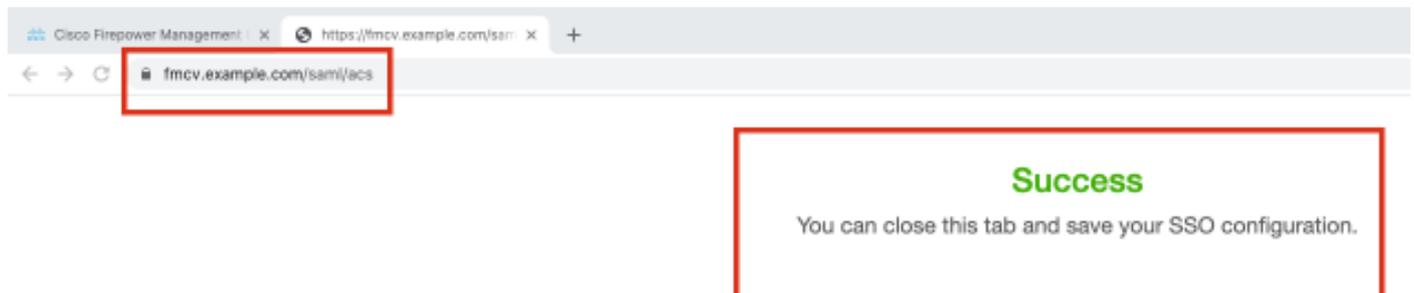
Security Approver

Threat Intelligence Director (TID) User

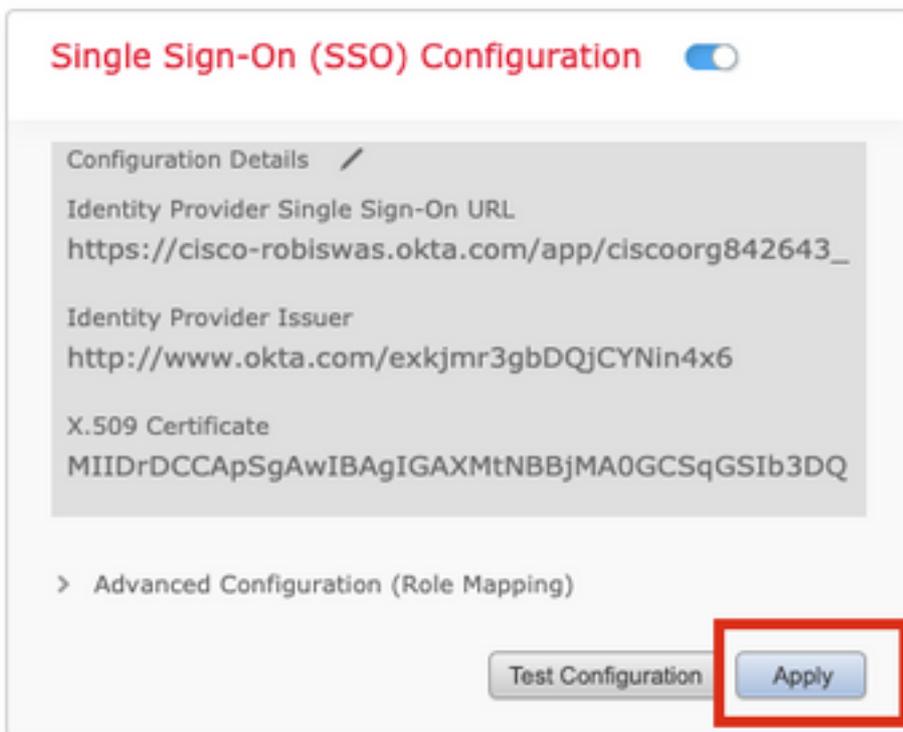
Passaggio 9. Per verificare la configurazione, fare clic su **Test della configurazione**, come mostrato nell'immagine.



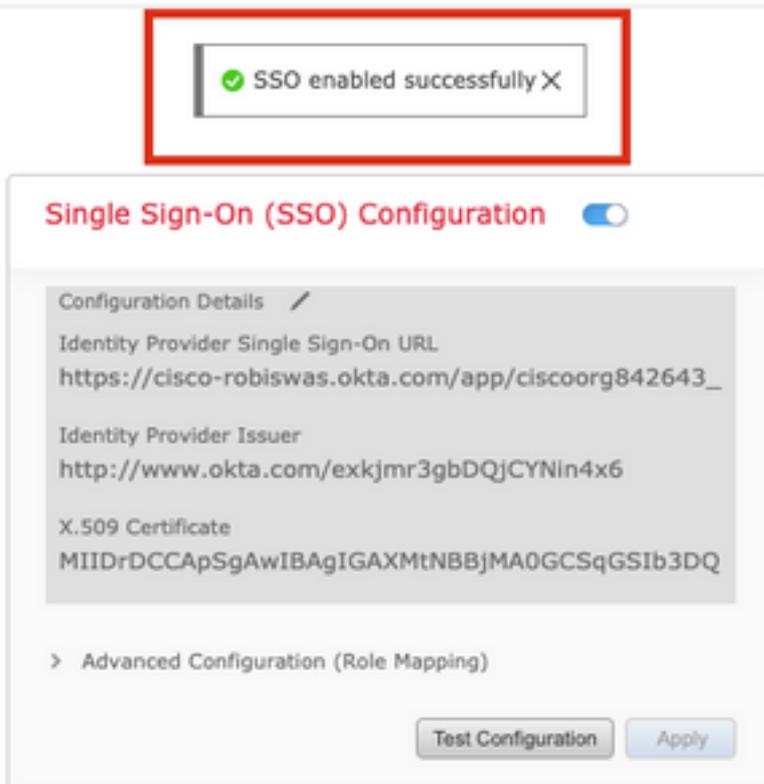
Se il test ha esito positivo, la pagina visualizzata in questa immagine dovrebbe essere una nuova scheda del browser.



Passaggio 10. Fare clic su **Apply** (Applica) per salvare la configurazione.



L'SSO deve essere abilitato correttamente.



Verifica

Accedere all'URL FMC dal browser: <https://<URL fmc>>. Fare clic su **Single Sign-On**.



Firepower Management Center

Username

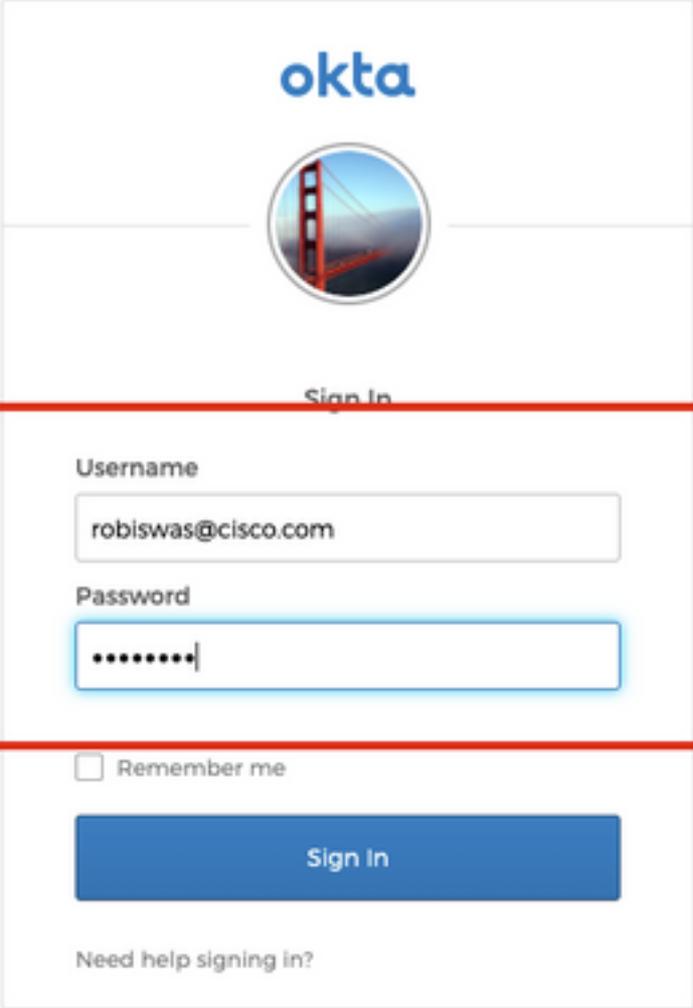
Password

[Single Sign-On](#)

[Log In](#)

Verrai reindirizzato alla pagina di accesso iDP (Okta). Fornire le credenziali SSO. Fare clic su **Accedi**.

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 "Remember me" checkbox, 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?".

Se l'operazione ha esito positivo, sarà possibile accedere e visualizzare la pagina predefinita del CCP.

In FMC, passare a **Sistema > Utenti** per visualizzare l'utente SSO aggiunto al database.

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