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

Sommario

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

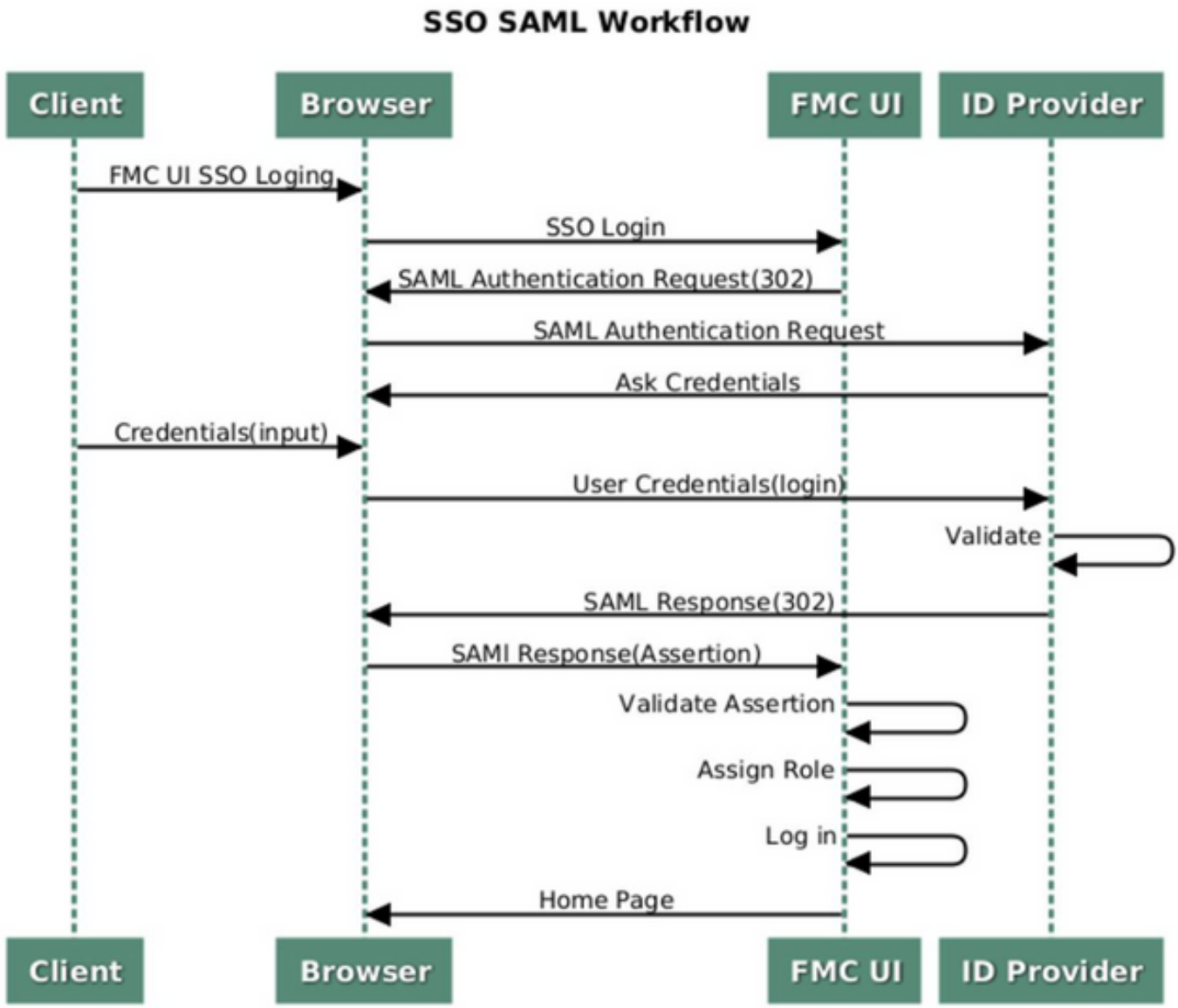
Nota: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali modifiche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



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

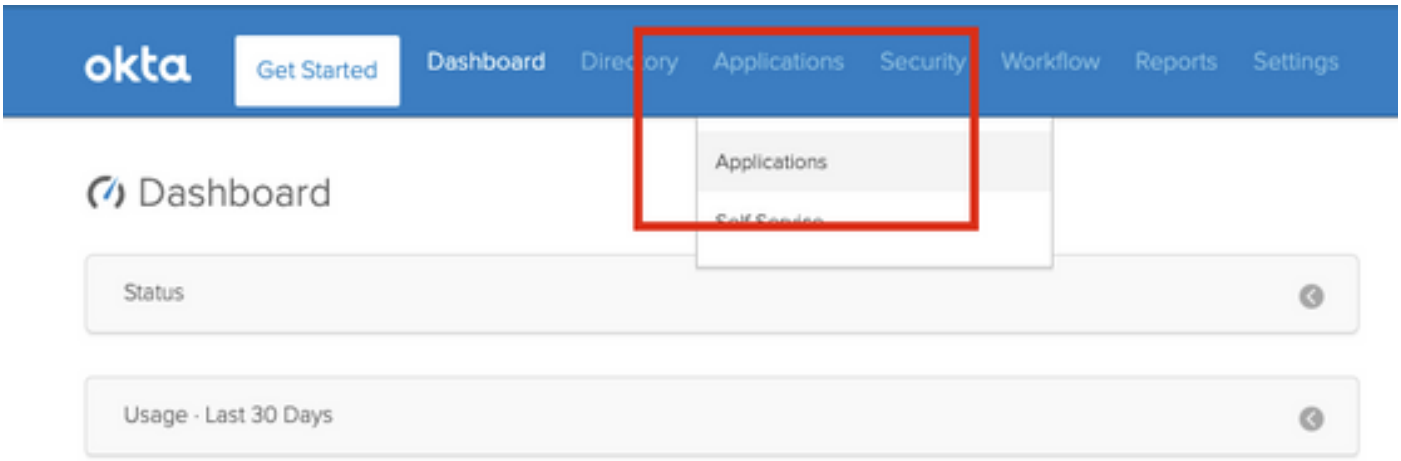
Si tratta di limitazioni e restrizioni note per l'autenticazione SSO per l'accesso FMC:

- 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).

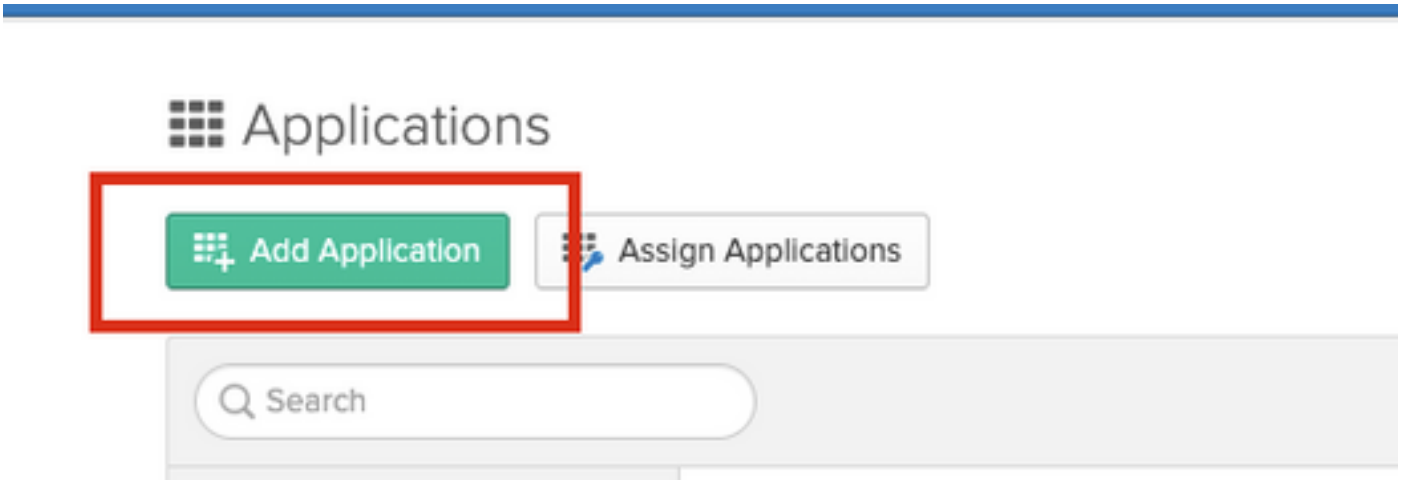
Procedura di configurazione

Procedura di configurazione nel provider di identità (Okta)

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

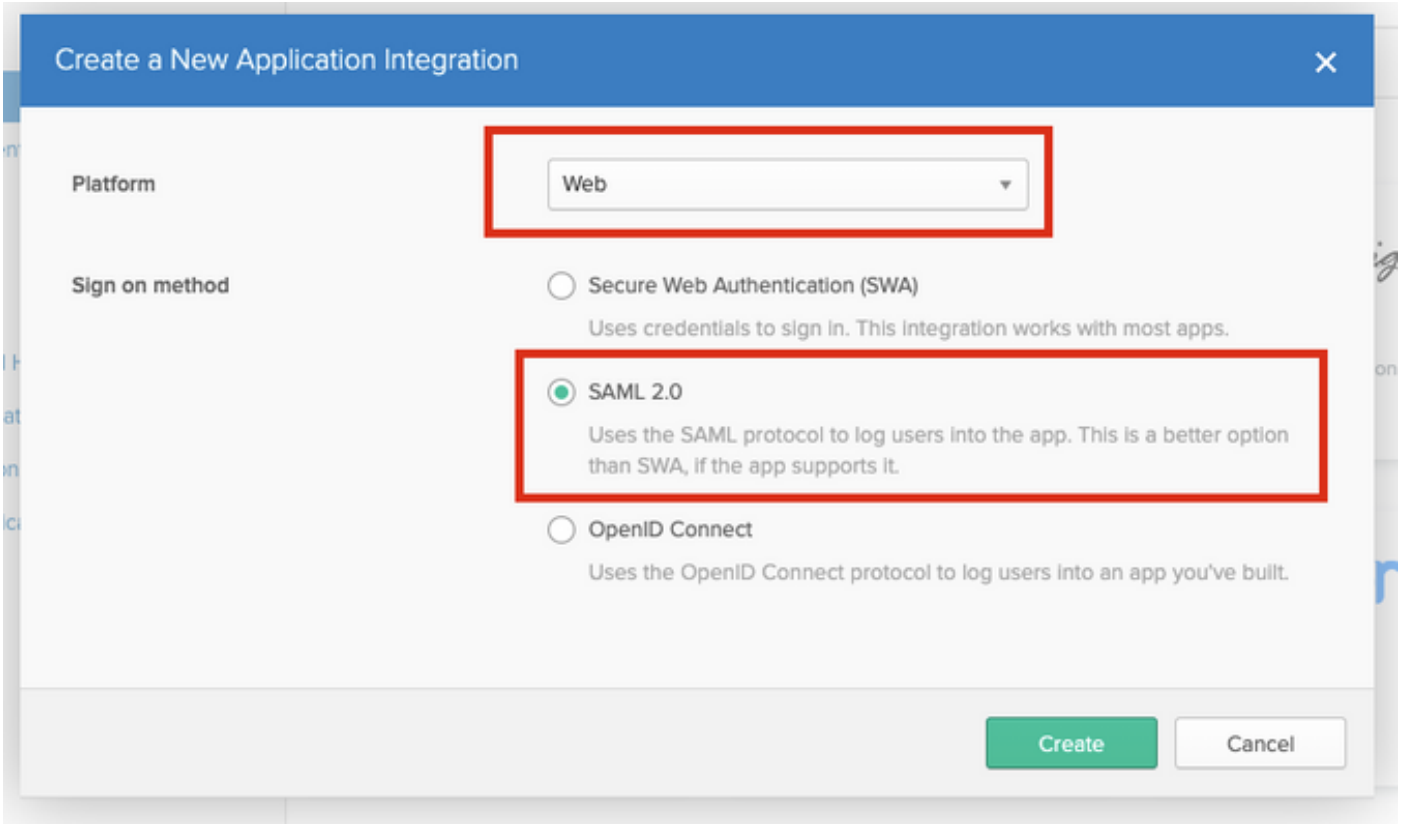


Passaggio 2. Come mostrato nell'immagine, fare clic su **AddApplication**.

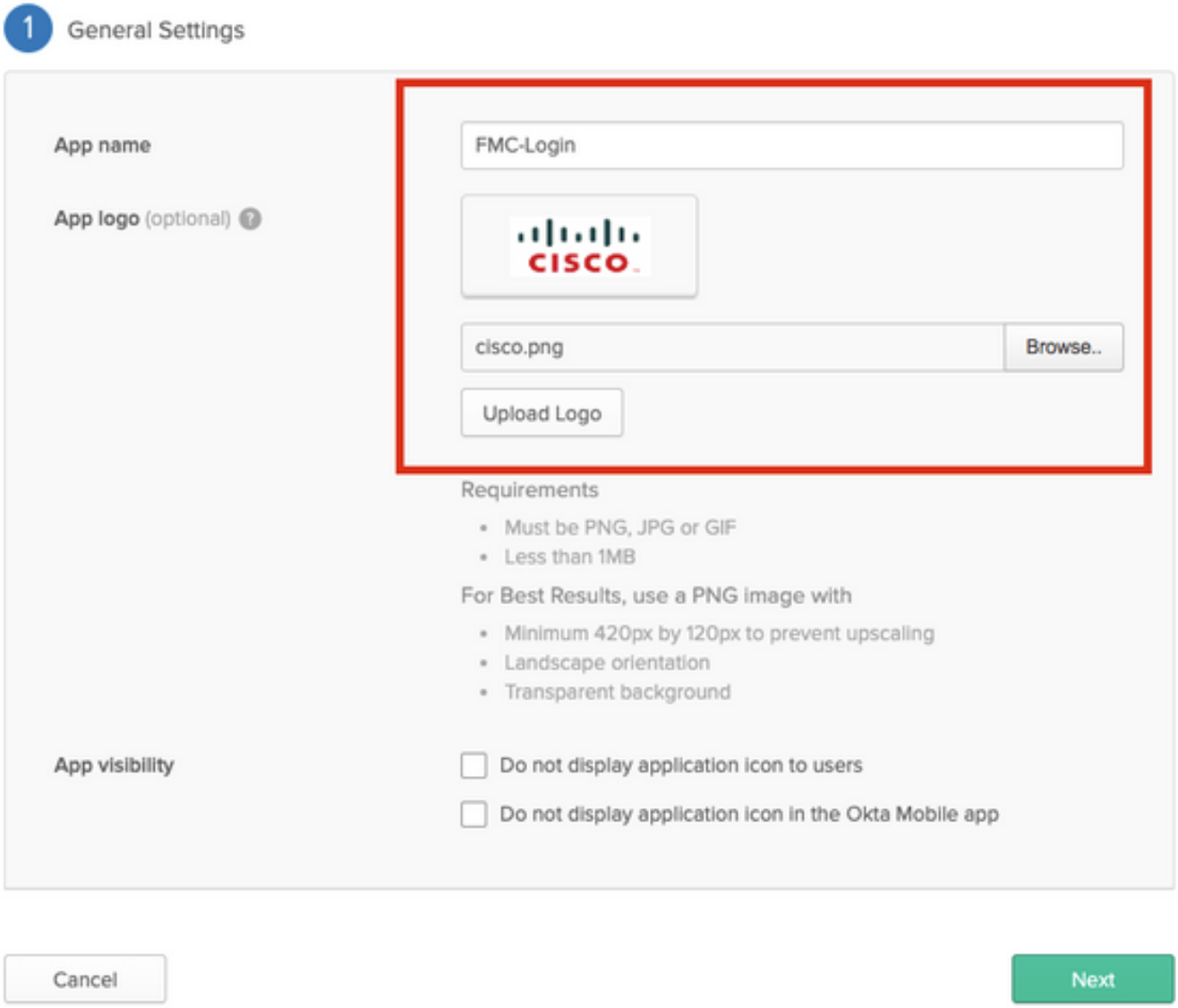


Passaggio 3. Come mostrato in questa immagine, fare clic su **Create NewApp** (Crea nuova app).

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.

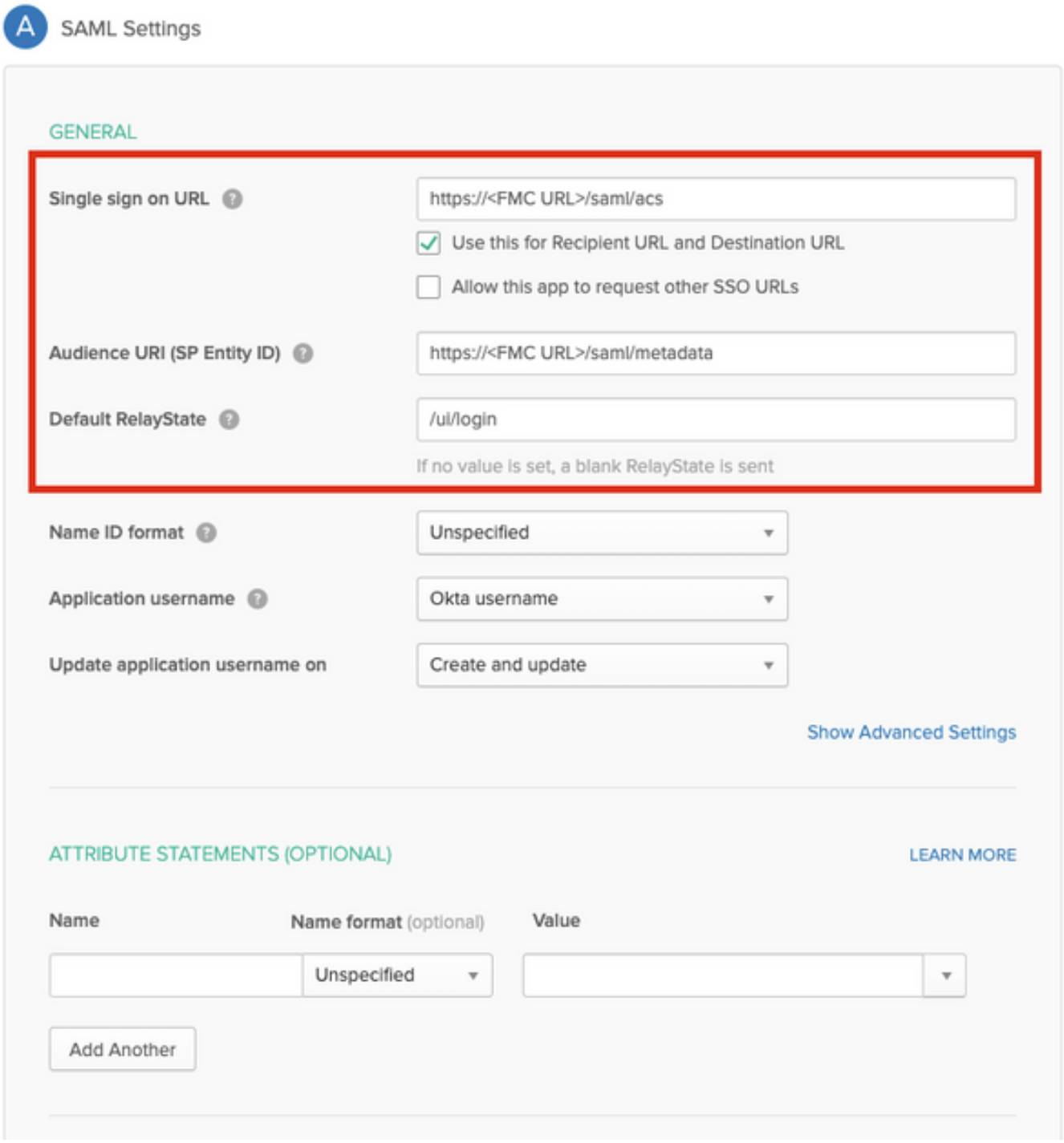


Passaggio 6. Inserire le **impostazioni SAML**.

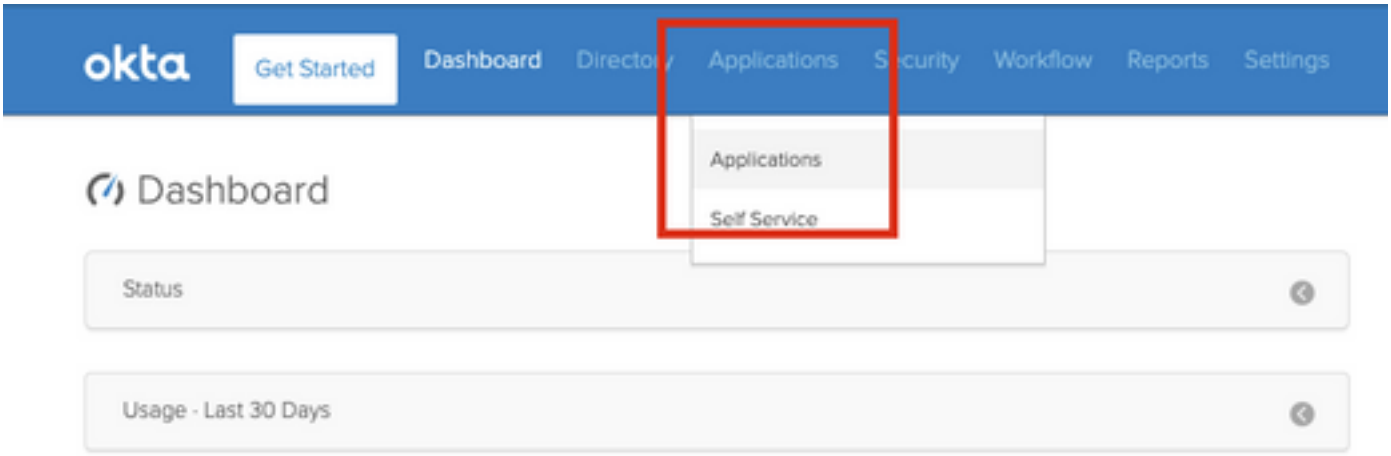
URL Single Sign-On: https://<URL fmc>/saml/acs

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

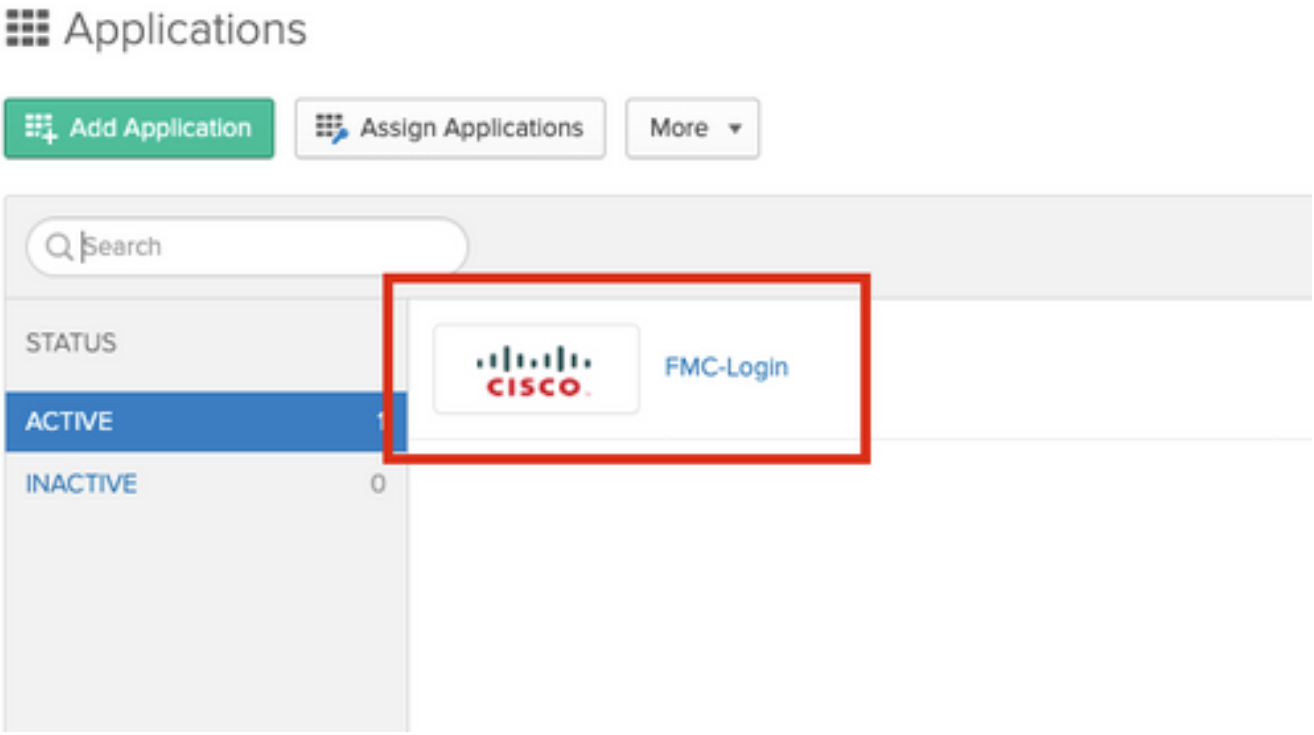
RelayState predefinito: /ui/login



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

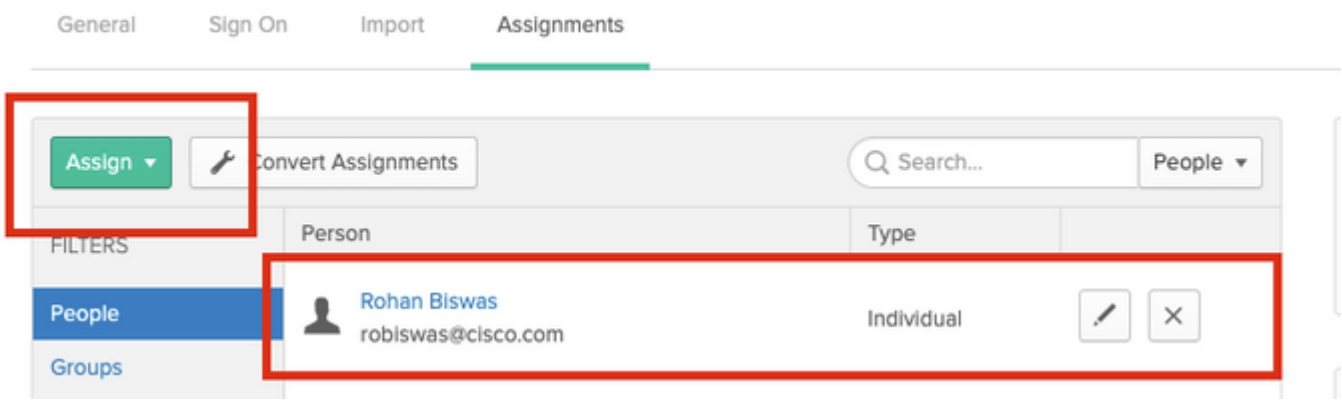


Passaggio 8. Fare clic sul nome dell'app creata.

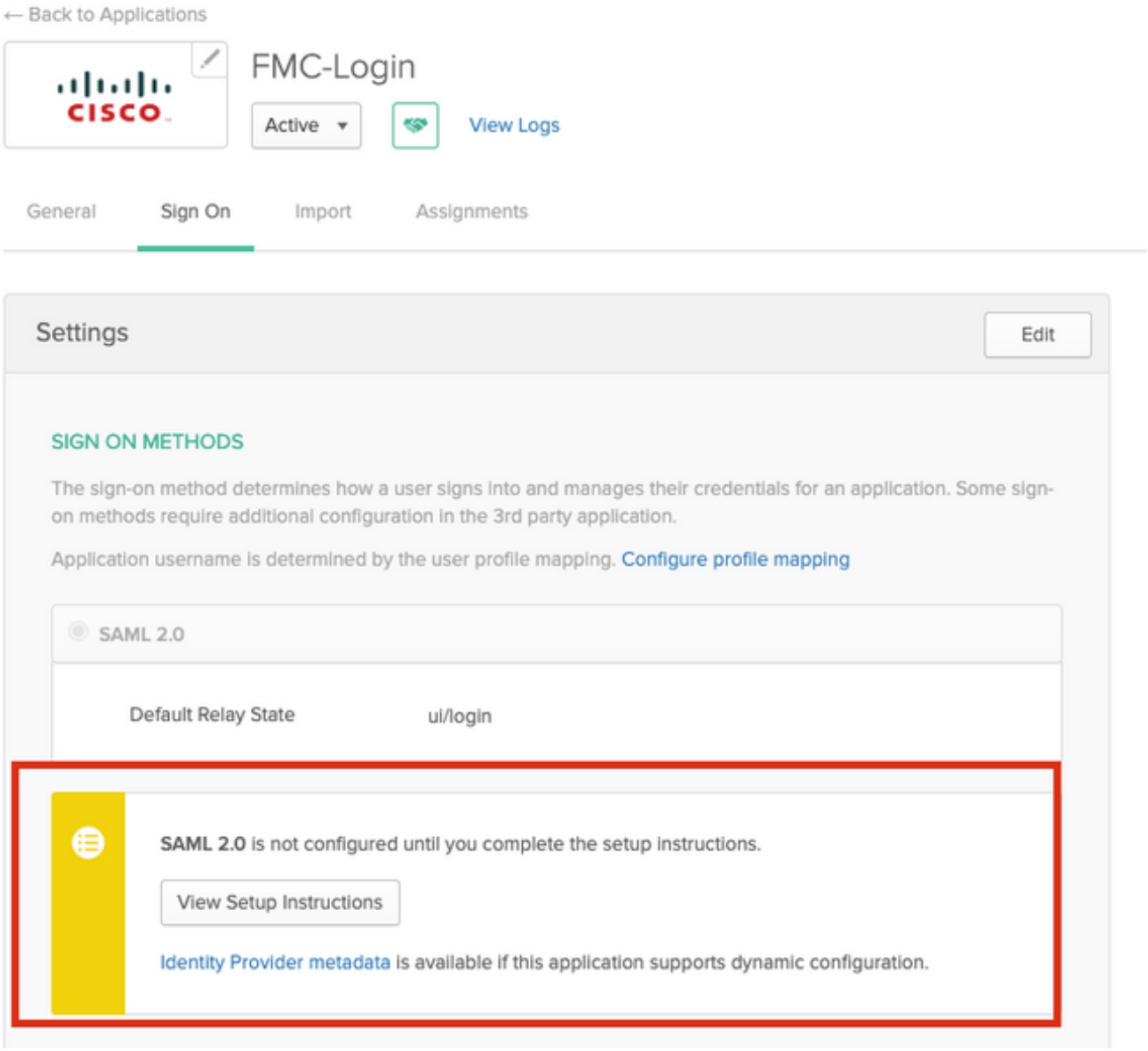


Passaggio 9. Passare ad **Assegnazioni**. Fare clic su **Assegna**.

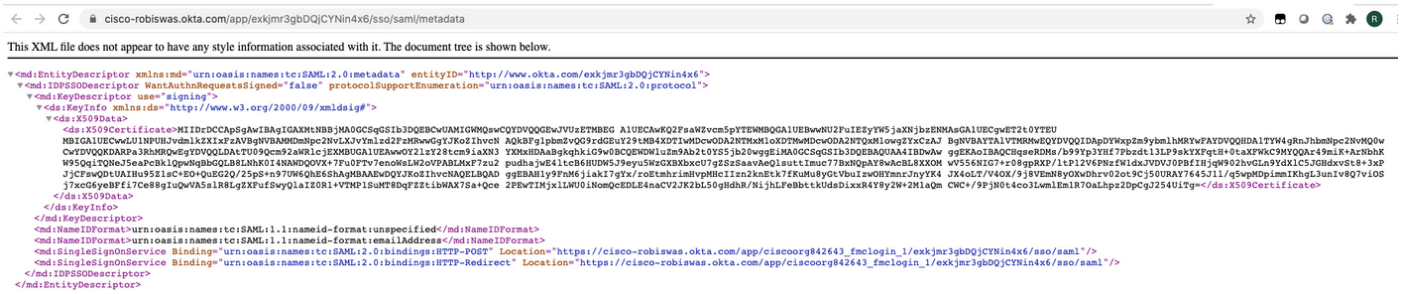
Èpossibile scegliere di assegnare singoli utenti o gruppi al nome dell'app creata.



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.



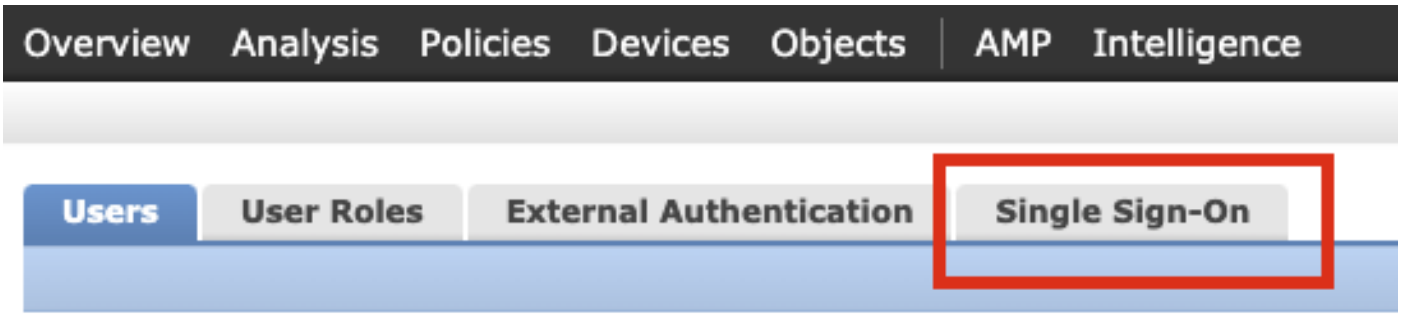
Salvare il file come file **xml** da utilizzare nel CCP.



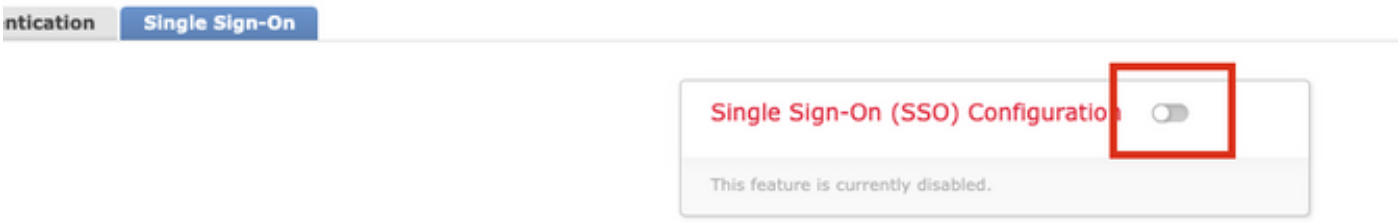
Procedura di configurazione in FMC

Passaggio 1. Accedere al CCP con privilegi di **amministratore**. Passare a **Sistema > Utenti**.

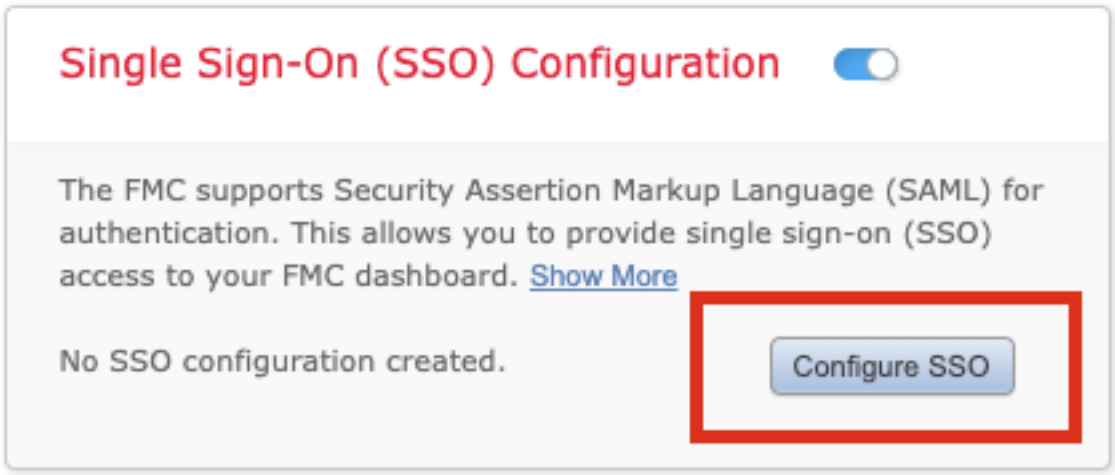
Passaggio 2. Fare clic su **Single Sign-On**, come illustrato nell'immagine.



Passaggio 3. **Abilitare** l'opzione Single Sign-On (disabilitata per impostazione predefinita).



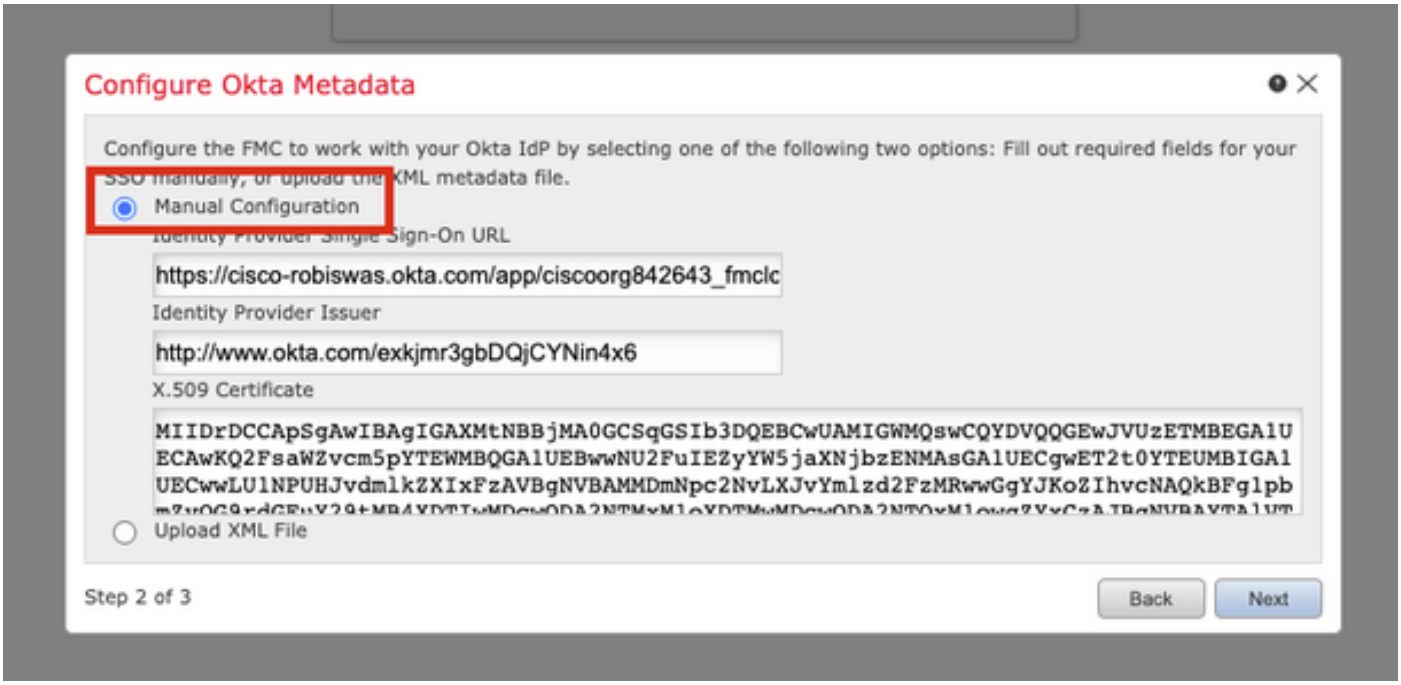
Passaggio 4. Fare clic su **Configura SSO** per avviare la configurazione dell'SSO in FMC.



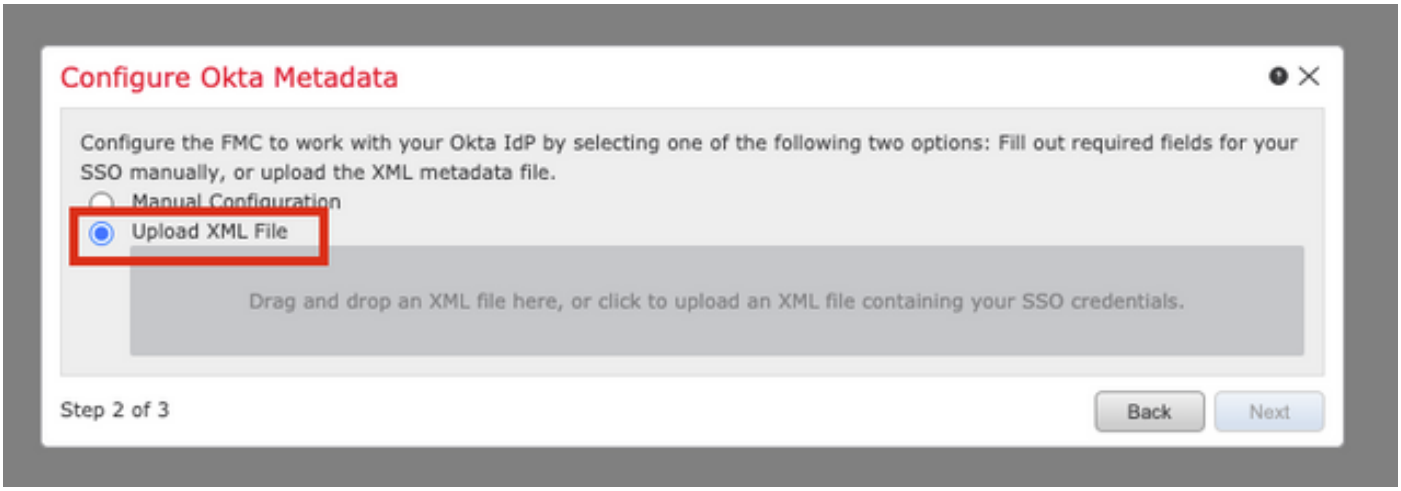
Passaggio 5. Selezionare il **provider SAML FMC**. Fare clic su Next (Avanti).

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

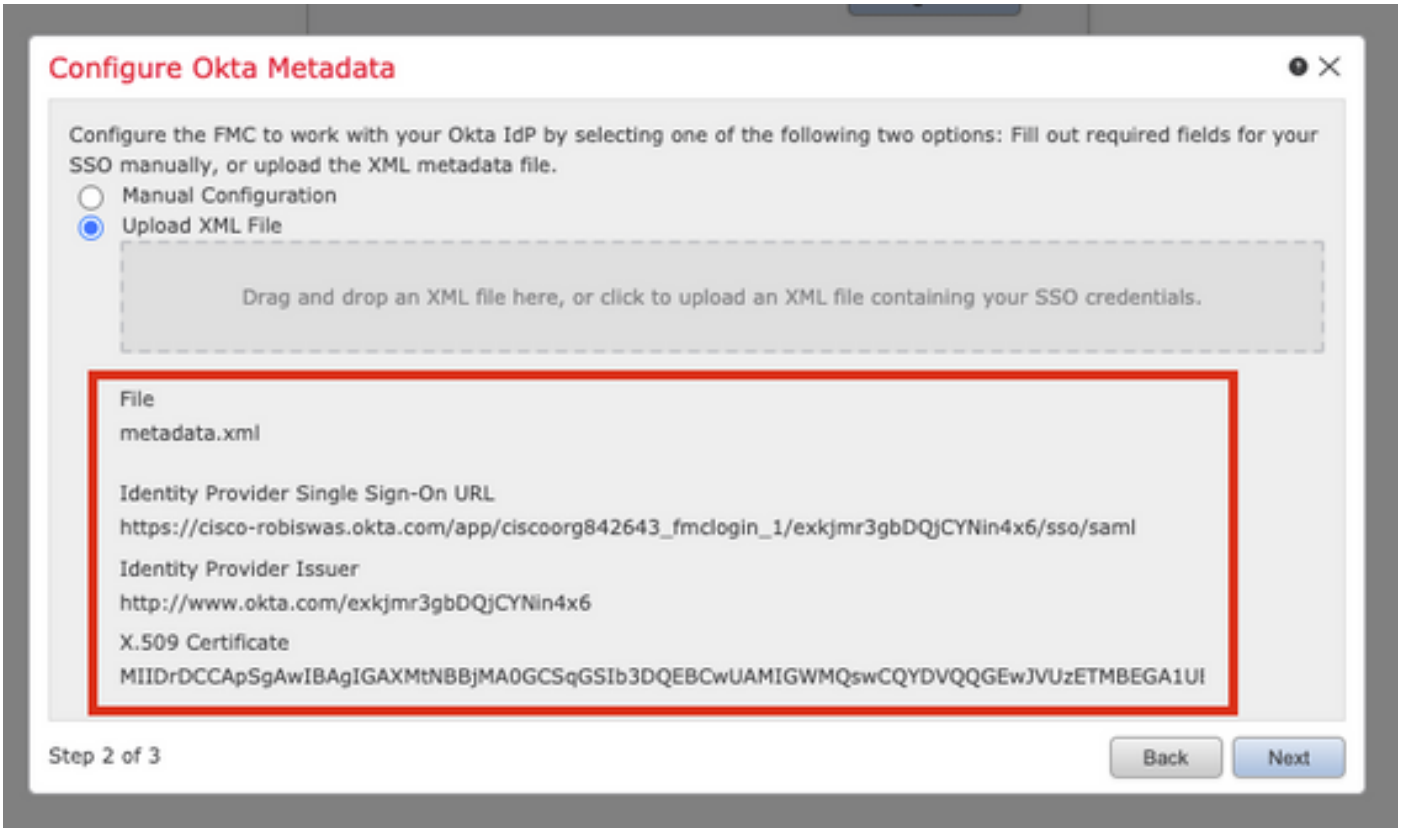
Passaggio 6. È possibile scegliere **Configurazione manuale** e immettere i dati iDP manualmente. Fare clic su **Avanti**, come



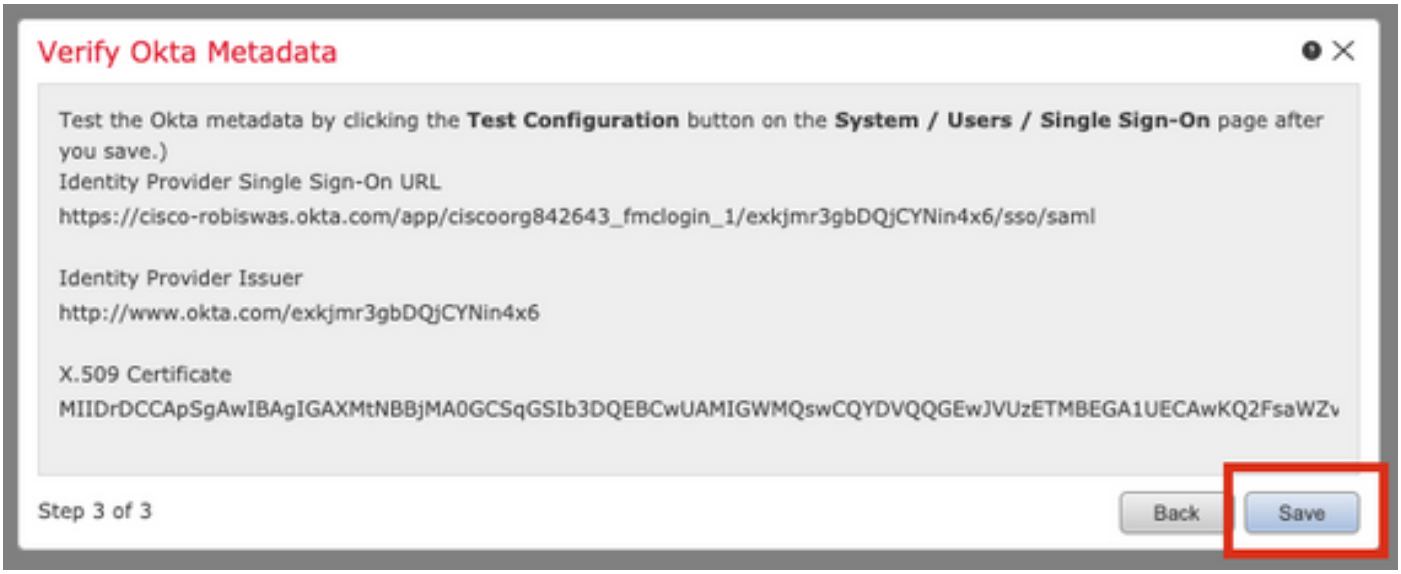
Èinoltre possibile scegliere **Carica file XML** e caricare il file XML recuperato nel passo 10 della configurazione Okta.



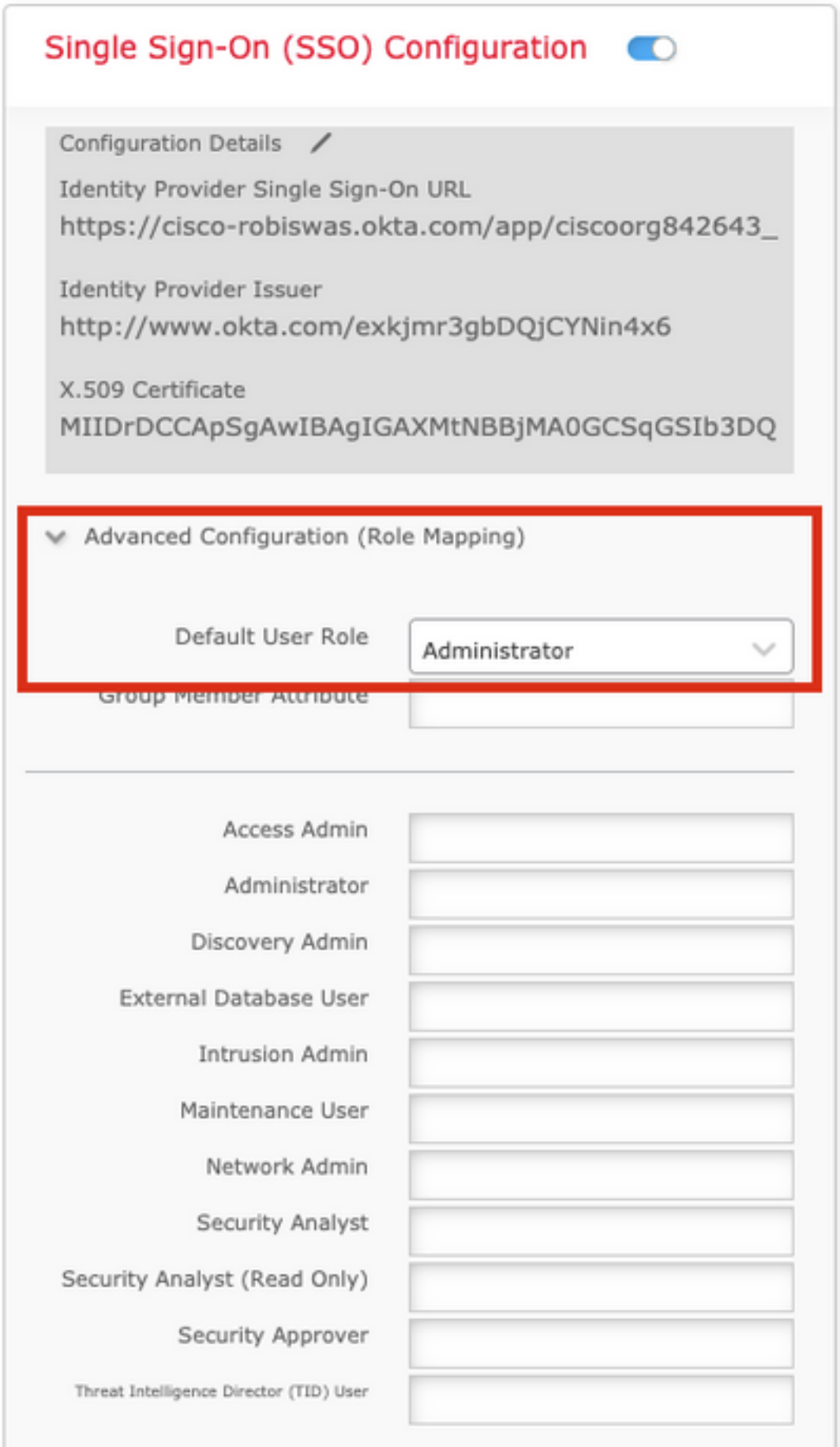
Una volta caricato il file, il FMC visualizza i metadati. Fare clic su **Avanti**, come mostrato nell'immagine.



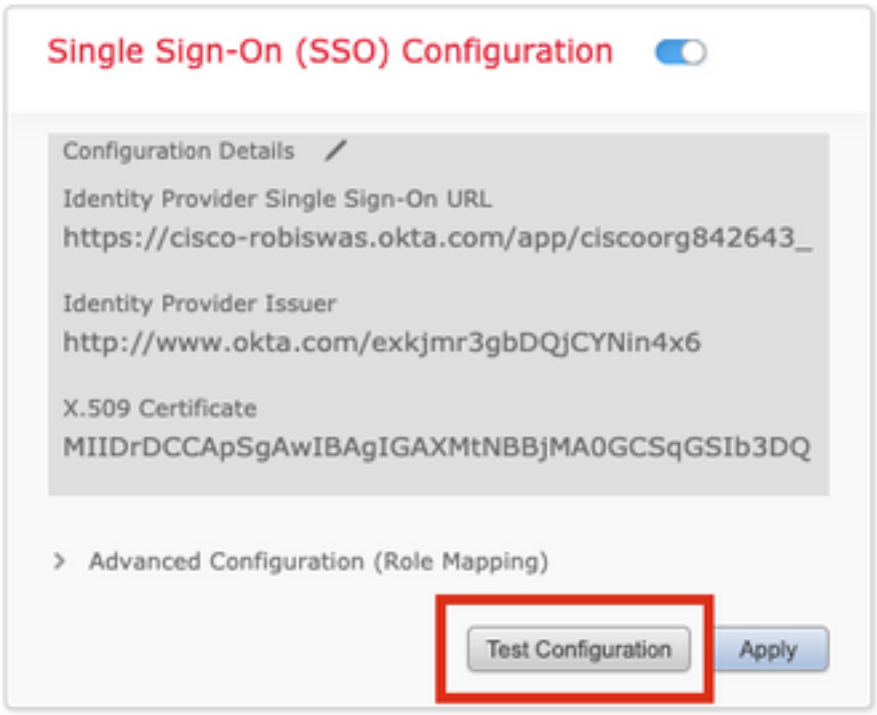
Passaggio 7. **Verificare** i metadati. Fare clic su **Save** (Salva), come mostrato nell'immagine.



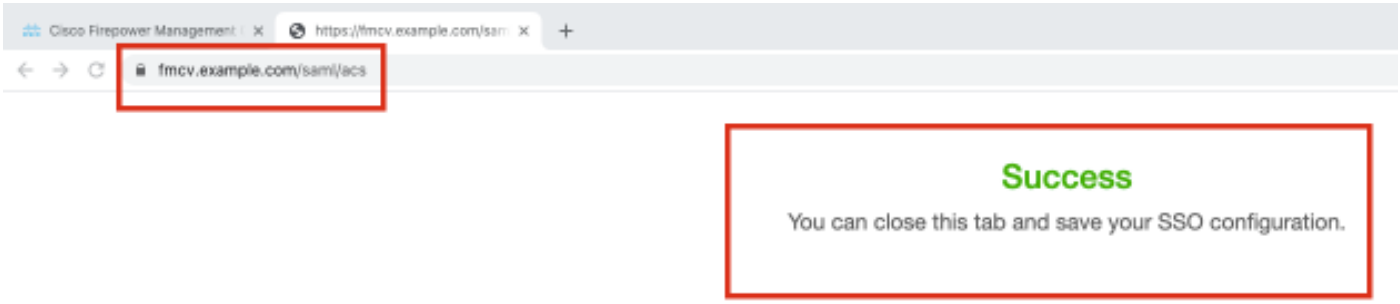
Passaggio 8. Configurare il **mapping ruoli/ruolo utente predefinito** in **Configurazione avanzata**.



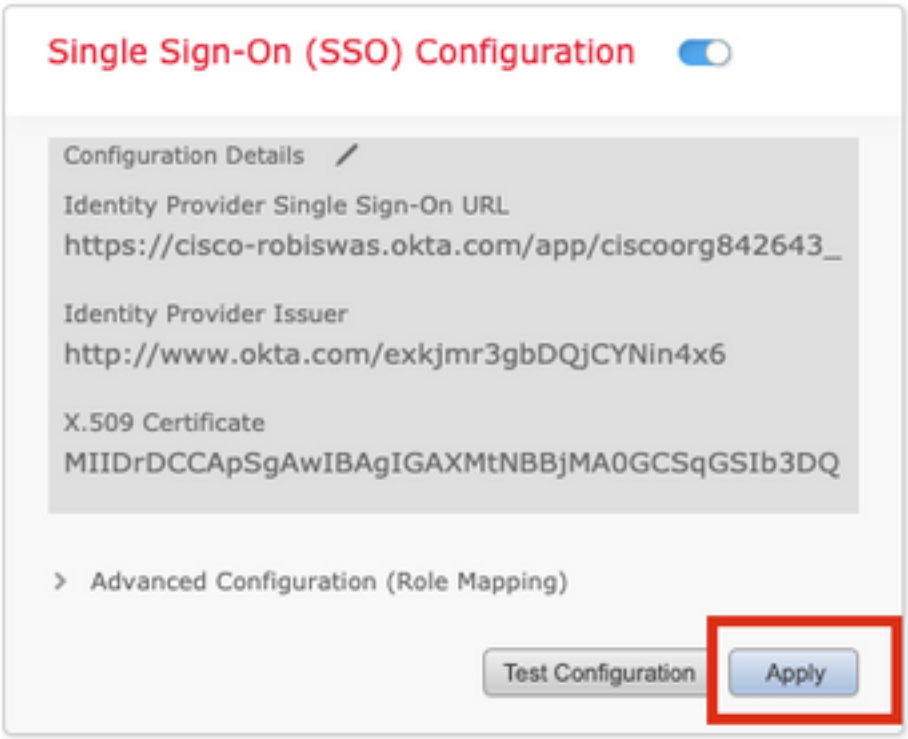
Passaggio 9. Per verificare la configurazione, fare clic su **Test della configurazione**, come mostrato nell'immagine.



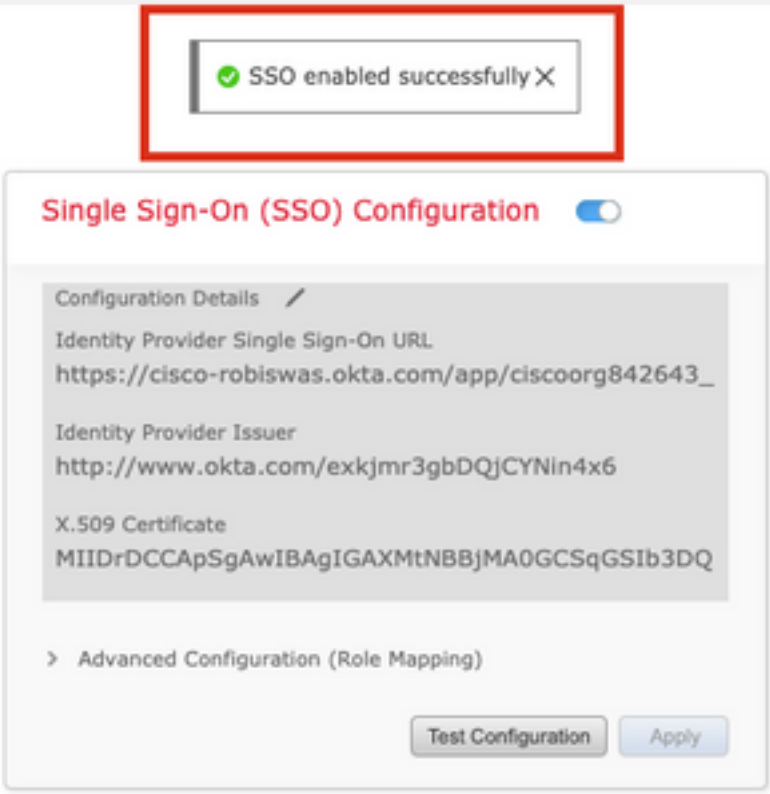
Se il test ha esito positivo, la pagina visualizzata in questa immagine dovrebbe essere una nuova scheda del browser.



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



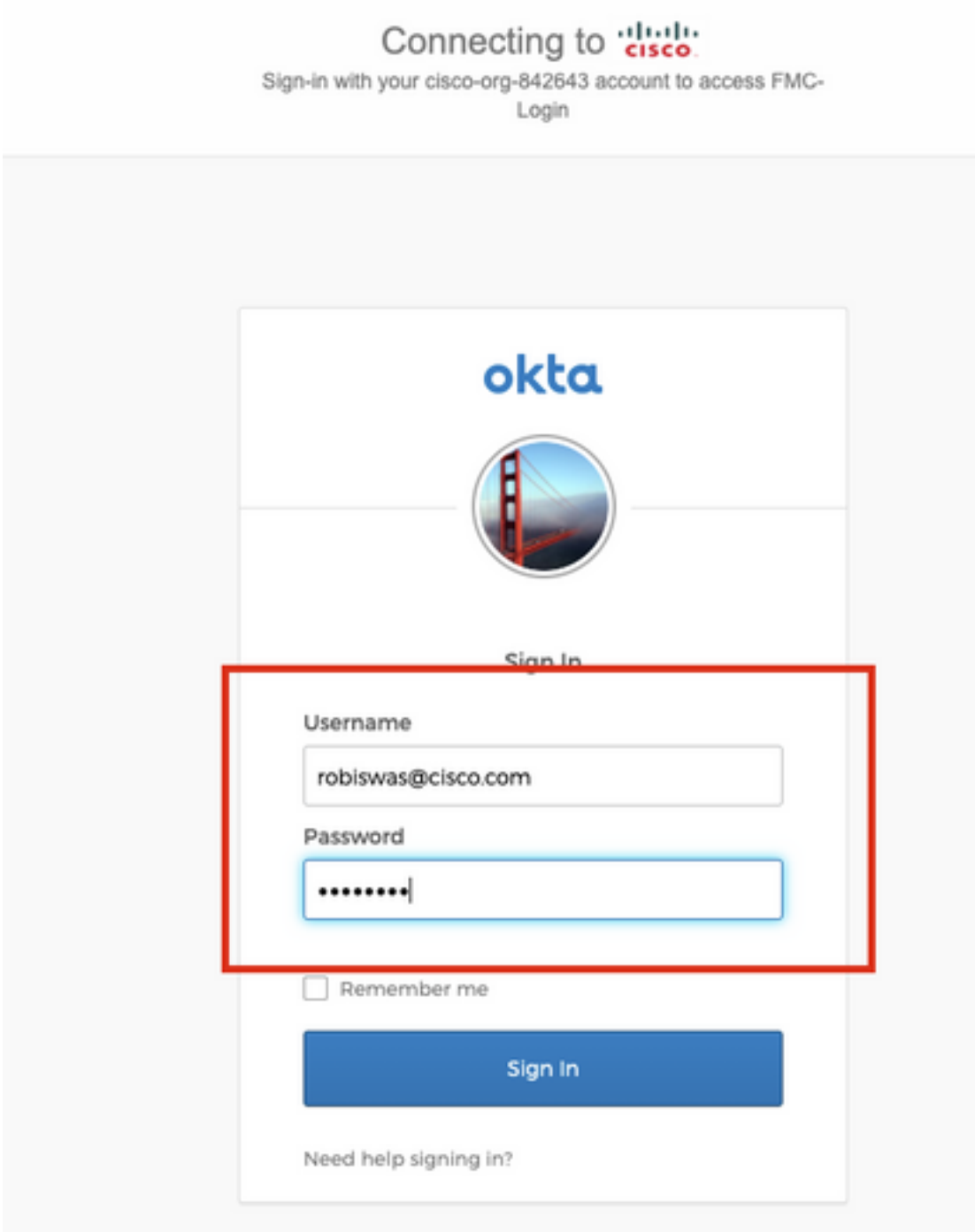
L'SSO deve essere abilitato correttamente.



Verifica

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

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



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.