Configuración del acceso a Firepower Management Center a través de la autenticación SSO con Okta

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Límites y Restricciones](#)
[Configuration Steps](#)
[Pasos de configuración en el proveedor de identidad (Okta)](#)
[Pasos de configuración en FMC](#)
[Verificación](#)

Introducción

Este documento describe cómo configurar Firepower Management Center (FMC) para la autenticación mediante el inicio de sesión único (SSO) para el acceso a la gestión.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica del inicio de sesión único y SAML
- Comprensión de la configuración en el proveedor de identidad (iDP)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Okta como proveedor de identidad

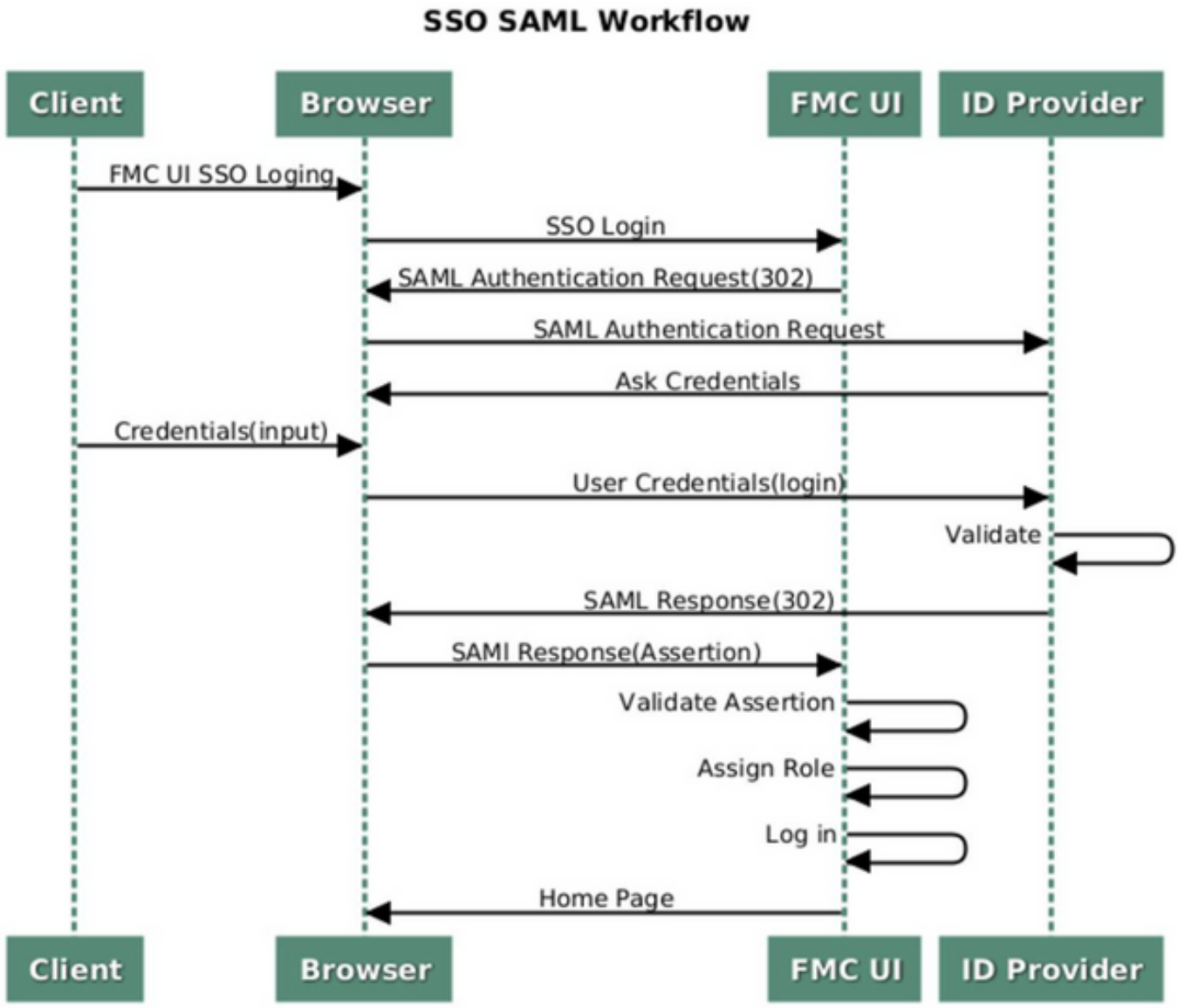
> **Nota:** La información de este documento se creó a partir de dispositivos en un entorno de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio de configuración.

Antecedentes

El inicio de sesión único (SSO) es una propiedad de gestión de identidades y acceso (IAM) que permite a los usuarios autenticarse de forma segura con varias aplicaciones y sitios web iniciando sesión una sola vez con un solo conjunto de credenciales (nombre de usuario y contraseña). Con SSO, la aplicación o el sitio web al que el usuario intenta acceder depende de un tercero de confianza para verificar que los usuarios son quienes dicen ser.

SAML (lenguaje de marcado de aserción de seguridad) es un marco basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad. Crea un círculo de confianza entre el usuario, un proveedor de servicios (SP) y un proveedor de identidad (IdP) que permite al usuario iniciar sesión en una sola vez para varios servicios

Un proveedor de servicios (SP) es una entidad que recibe y acepta una afirmación de autenticación emitida por un proveedor de identidad (iDP). Como se describe en sus nombres, los proveedores de servicios proporcionan servicios mientras que los proveedores de identidad proporcionan la identidad de los usuarios (autenticación).



Estos iDP son compatibles y se prueban para la autenticación:

- Okta
- OneLogin
- PingID
- Azure AD
- Otros (Cualquier iDP que se ajuste a SAML 2.0)

Nota: No se requiere nueva licencia. Esta función funciona tanto en modo de evaluación como de licencia.

Límites y Restricciones

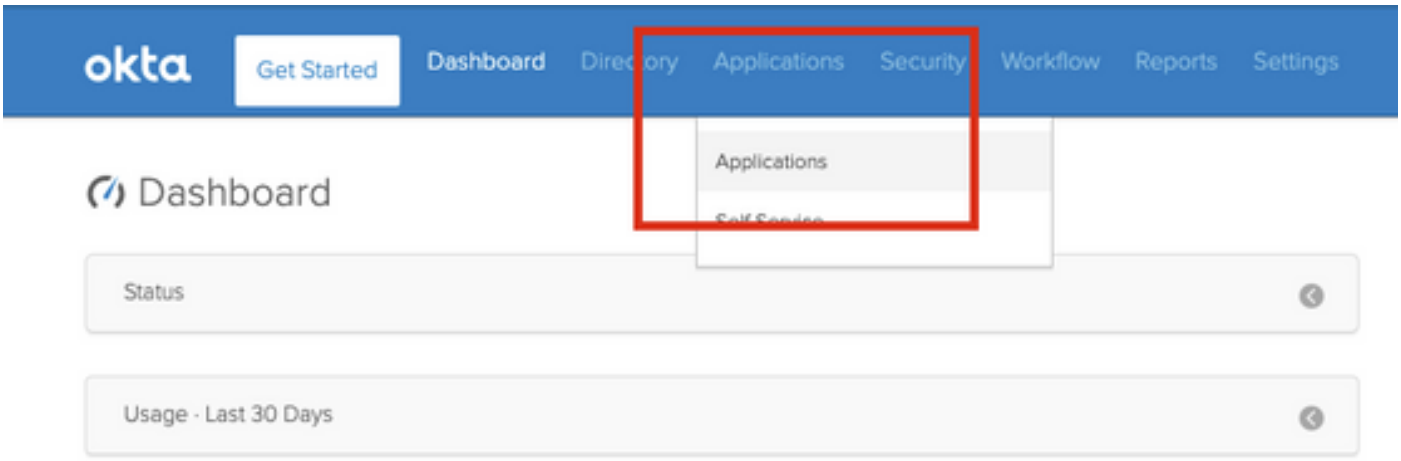
Estas son limitaciones y restricciones conocidas para la autenticación SSO para el acceso FMC:

- SSO sólo se puede configurar para el dominio global
- Los FMC en el par HA requieren configuración individual
- Sólo los administradores locales/AD pueden configurar SSO en FMC (los usuarios administradores de SSO no podrán configurar/actualizar la configuración de SSO en FMC).

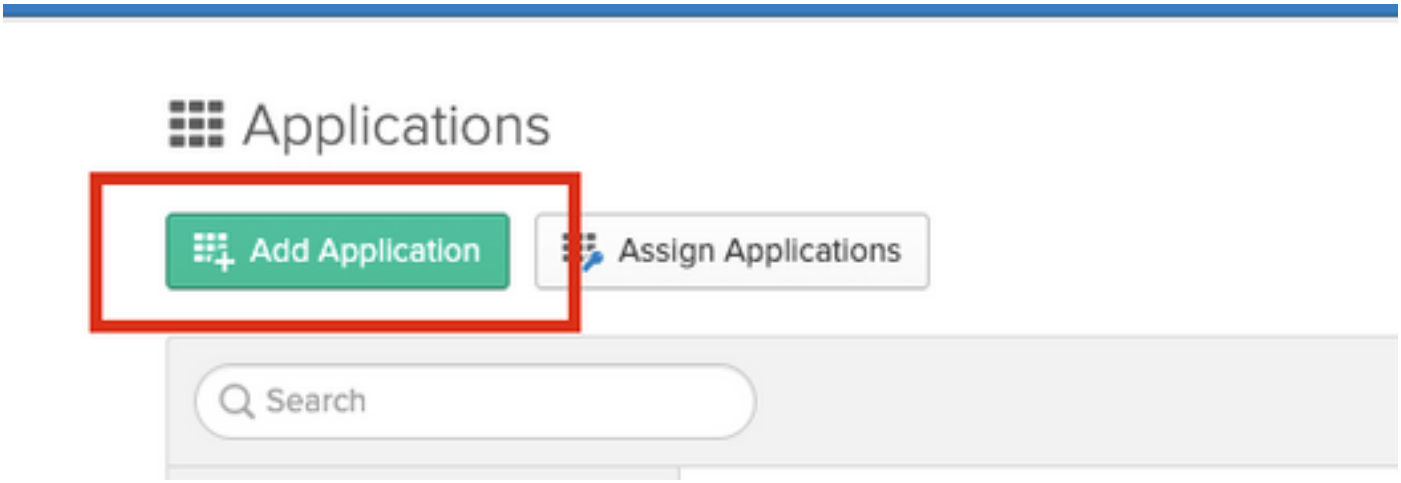
Configuration Steps

Pasos de configuración en el proveedor de identidad (Okta)

Paso 1. Inicie sesión en el portal de Okta. Navegue hasta **Aplicaciones > Aplicaciones**, como se muestra en esta imagen.

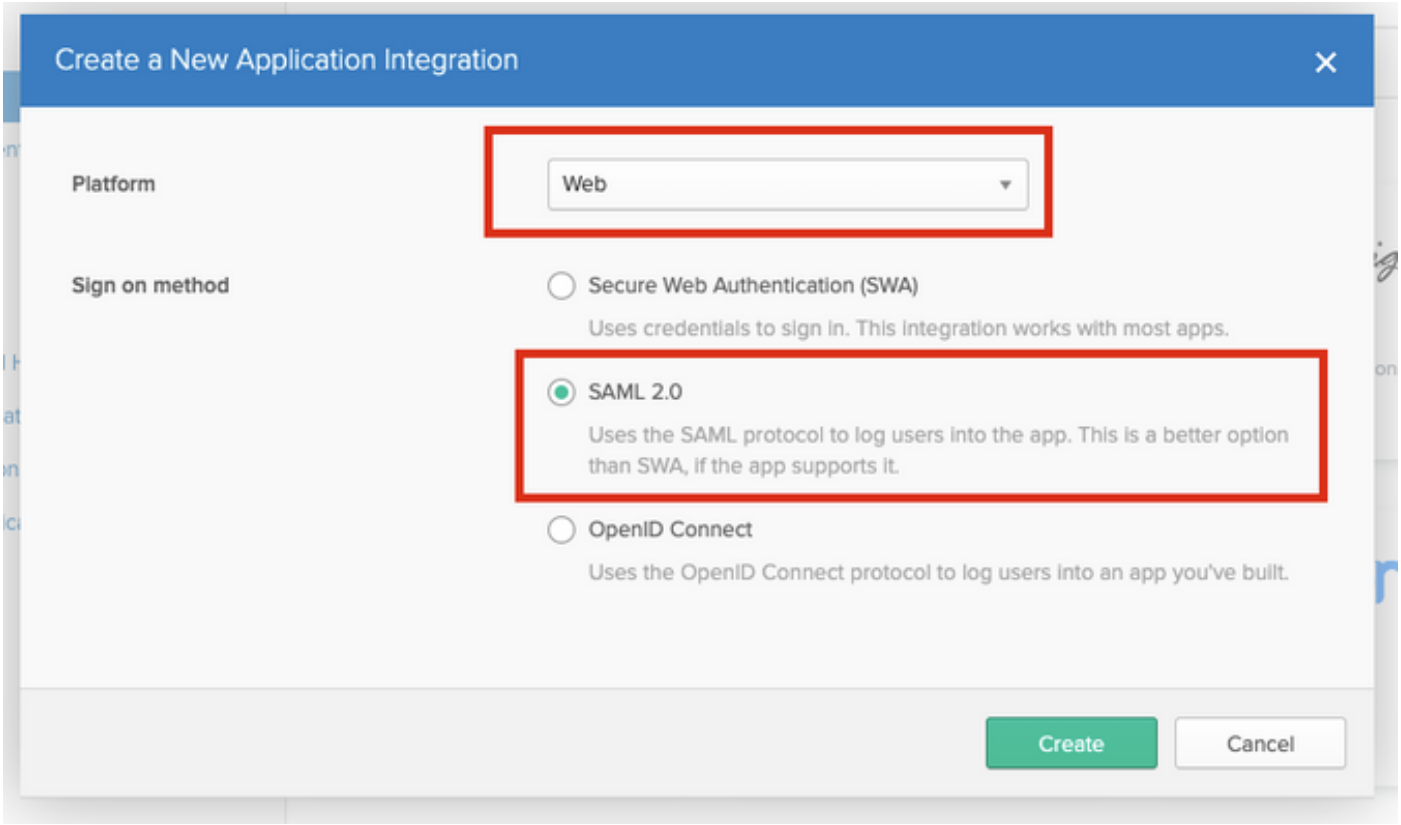


Paso 2. Como se muestra en esta imagen, haga clic en **AddApplication**.

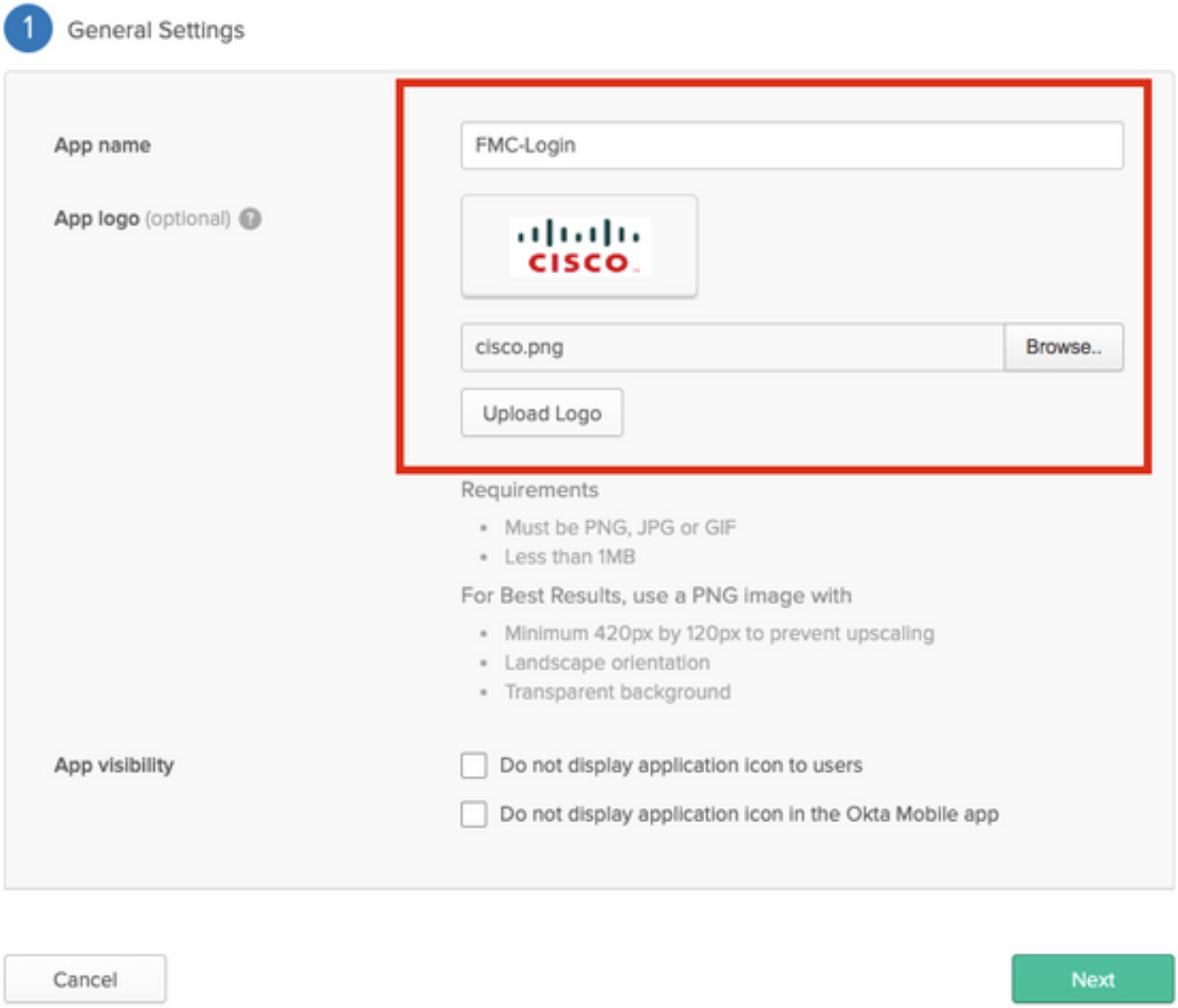


Paso 3. Como se muestra en esta imagen, haga clic en **Create NewApp**.

Paso 4. Elija la **Plataforma** como **Web**. Elija el **método Sign On** como **SAML 2.0**. Haga clic en **Crear**, como se muestra en esta imagen.



Paso 5. Proporcione un **nombre de aplicación**, **logotipo de aplicación (opcional),** y haga clic en **Siguiente**, como se muestra en esta imagen.

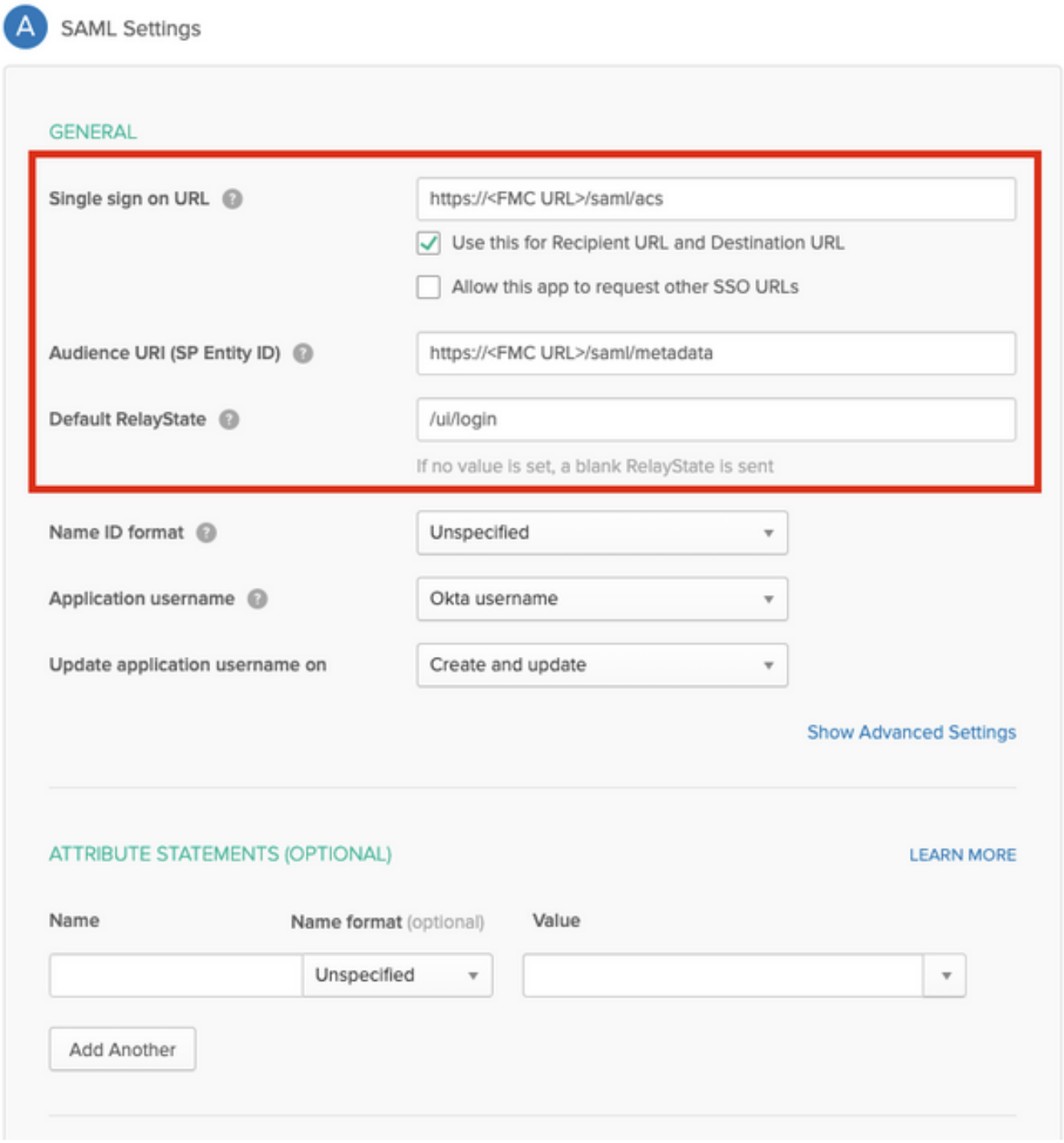


Paso 6. Introduzca la **configuración de SAML**.

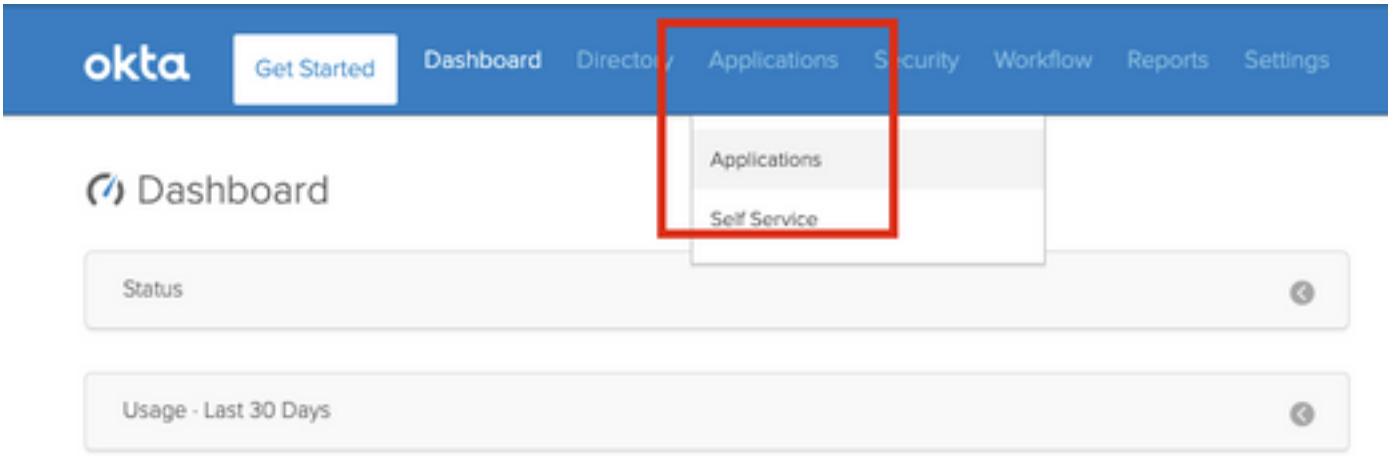
URL de inicio de sesión único: https://<fmc URL>/saml/acs

URI de público (ID de entidad SP): https://<fmc URL>/saml/metadatos

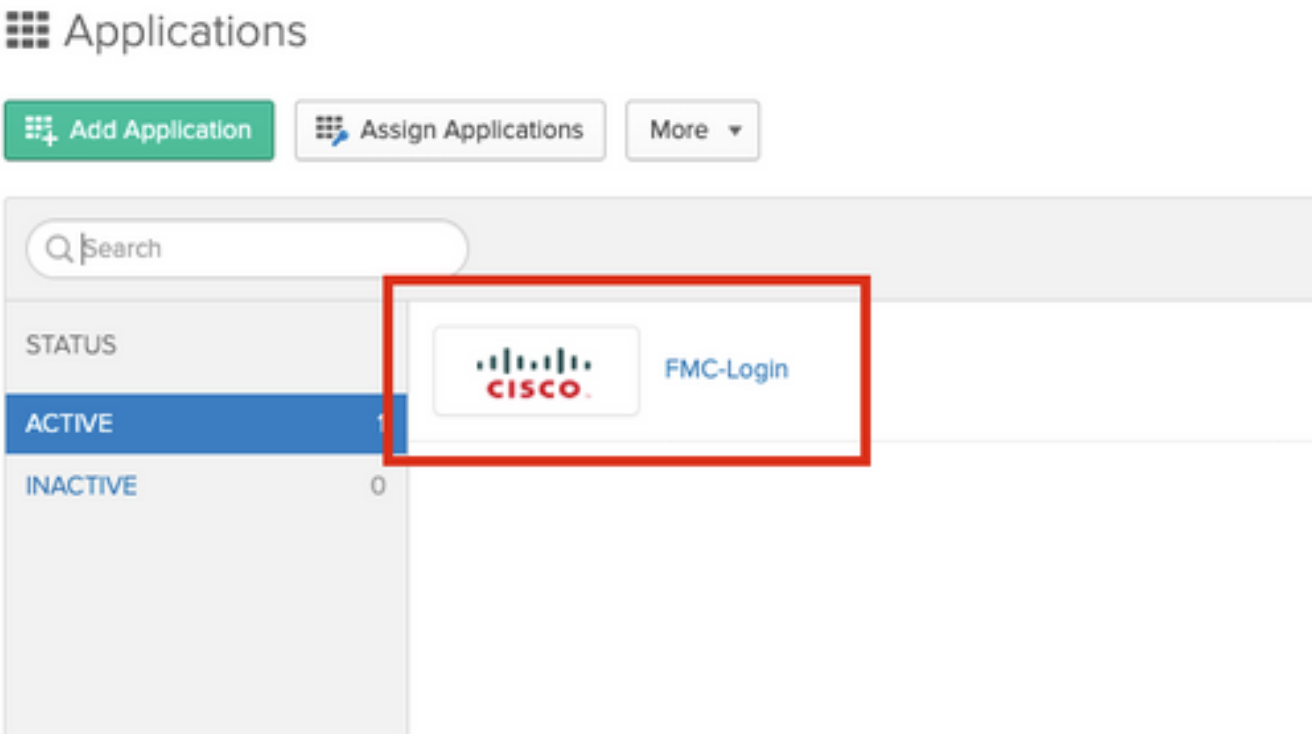
Estado de retransmisión predeterminado: /ui/login



Paso 7. Vuelva a **Aplicaciones > Aplicaciones**, como se muestra en esta imagen.

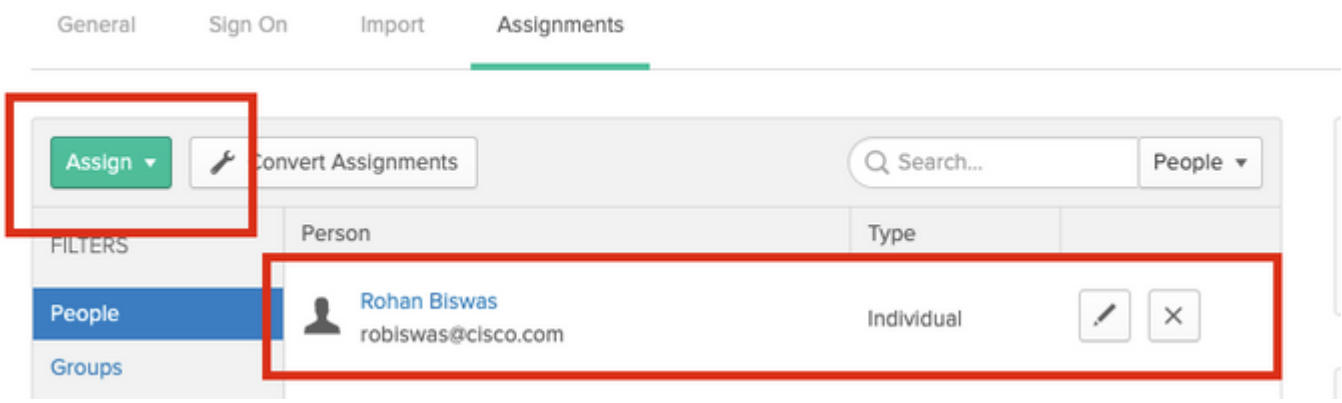


Paso 8. Haga clic en el nombre de la aplicación que se creó.

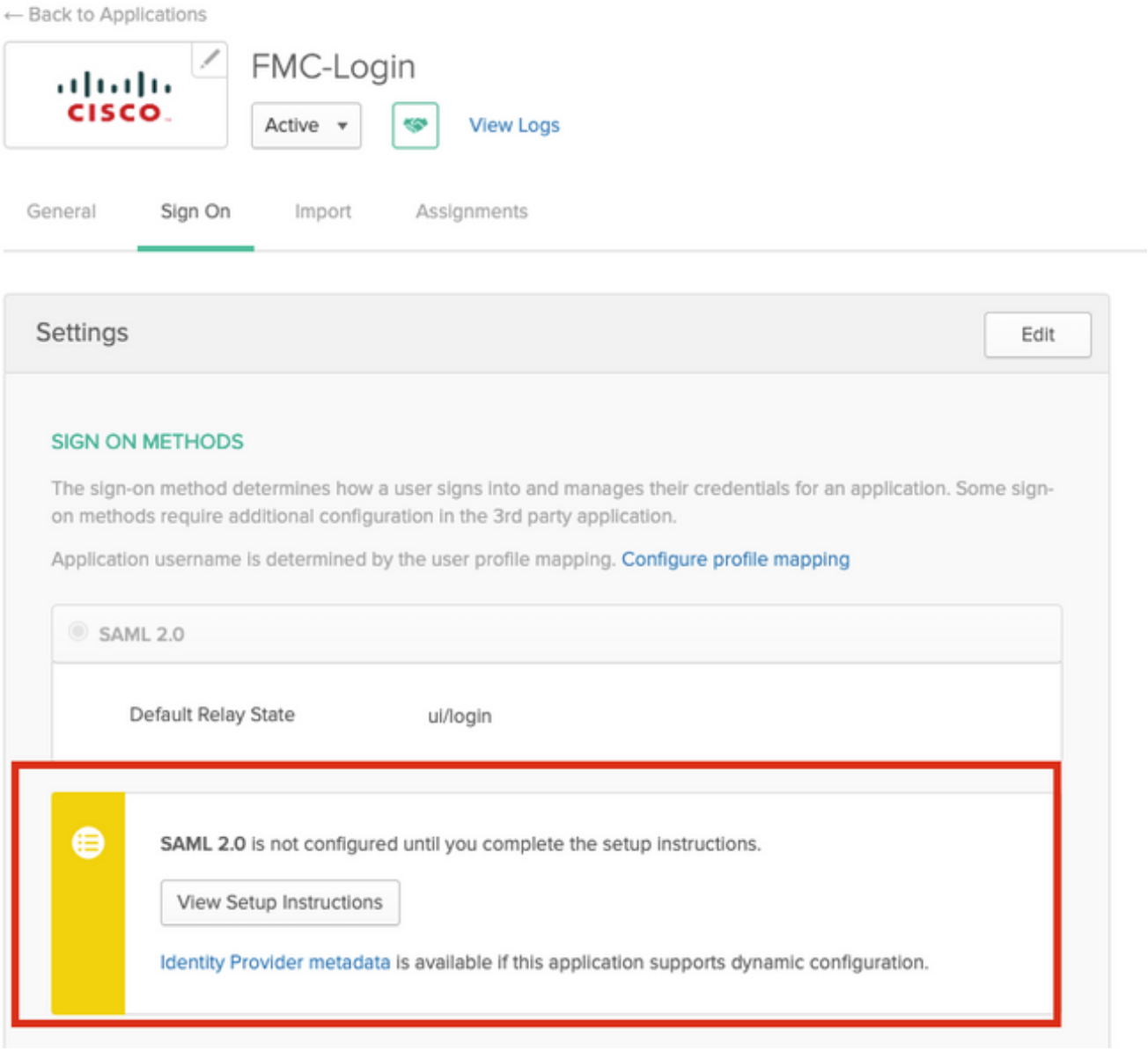


Paso 9. Navegue hasta **Asignaciones**. Haga clic en **Asignar**.

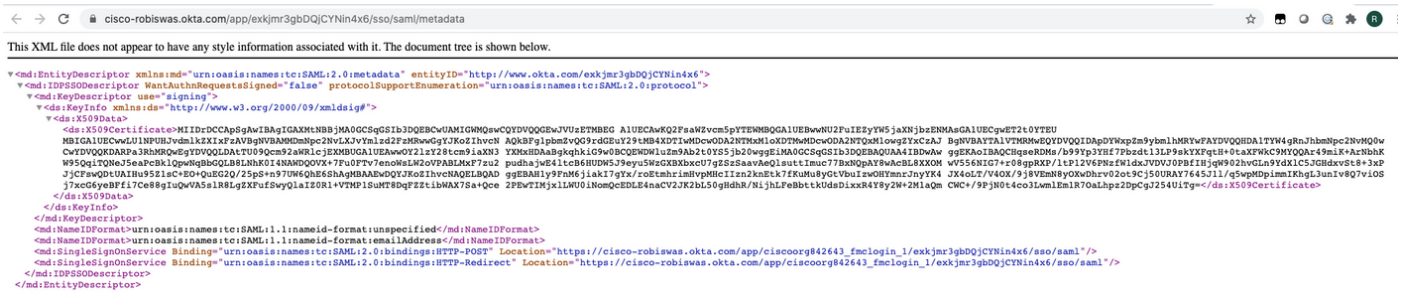
Puede optar por asignar usuarios o grupos individuales al nombre de la aplicación creado.



Paso 10. Navegue hasta **Iniciar sesión**. Haga clic en **Ver instrucciones de configuración**. **Haga clic en los metadatos del proveedor de identidad** para ver los metadatos del iDP.



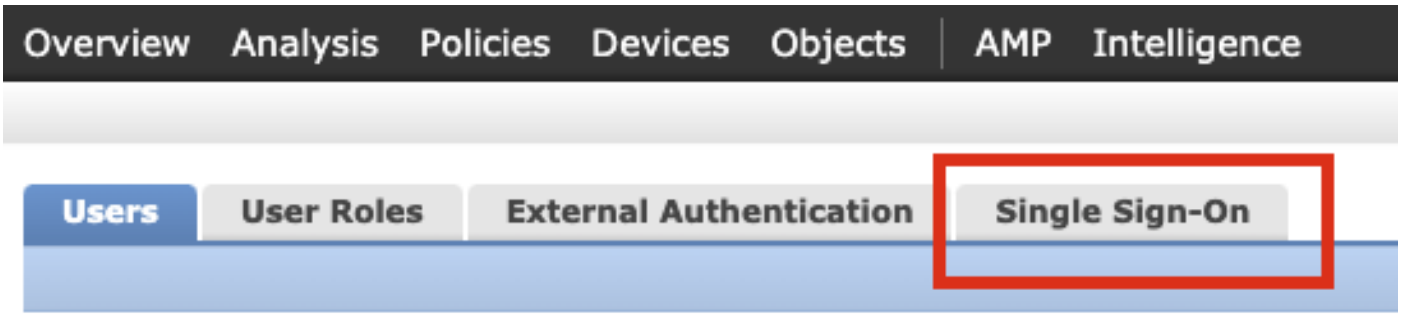
Guarde el archivo como un archivo **.xml** que se utilizará en el FMC.



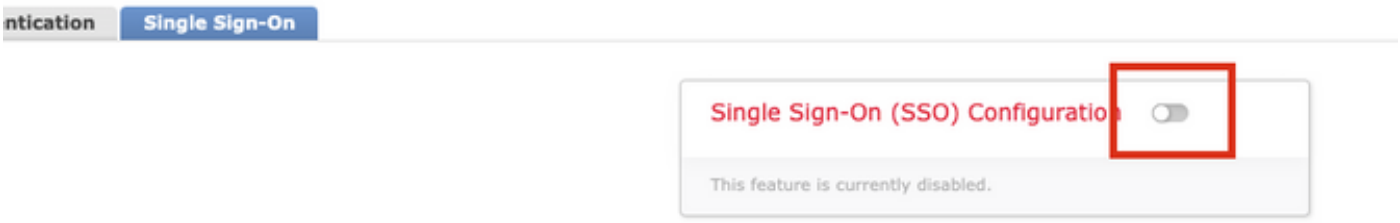
Pasos de configuración en FMC

Paso 1. Inicie sesión en el FMC con privilegios **Admin**. Navegue hasta **Sistema >Usuarios**.

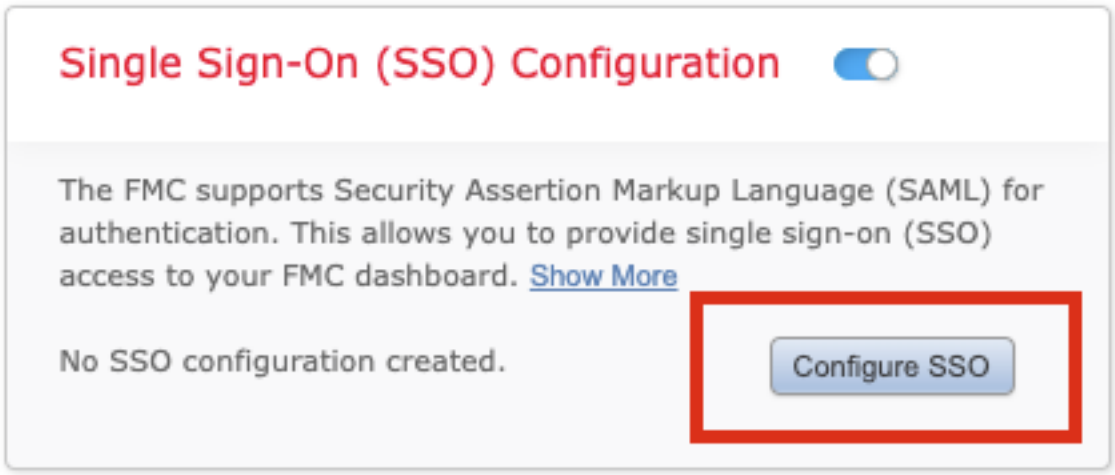
Paso 2. Haga clic en **Inicio de sesión único**, como se muestra en esta imagen.



Paso 3. **Active** la opción Inicio de sesión único (Desactivado de forma predeterminada).



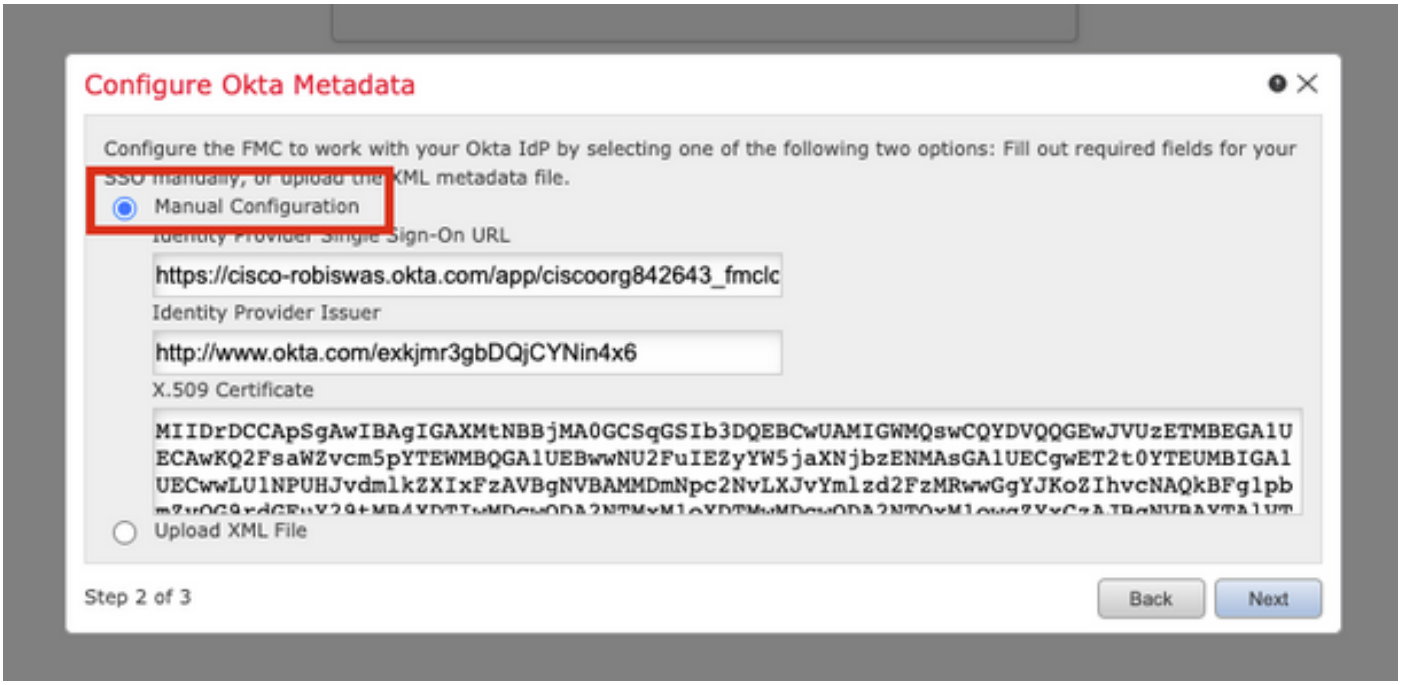
Paso 4. Haga clic en **Configurar SSO** para iniciar la configuración SSO en FMC.



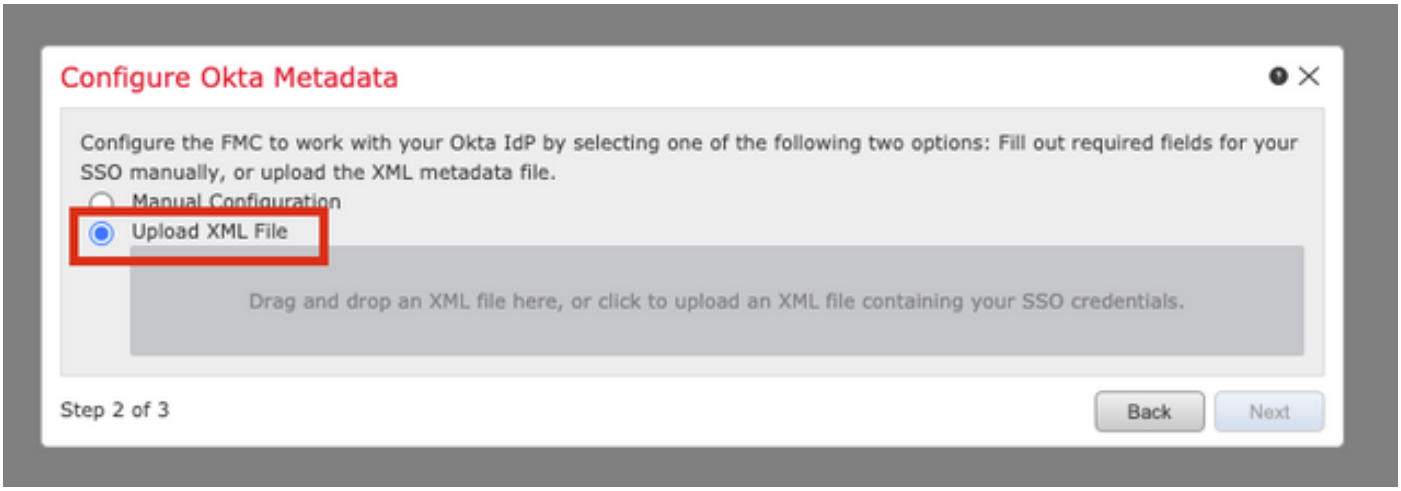
Paso 5. Seleccione el **proveedor SAML de FMC**. Haga clic en Next (Siguiente).

Para el propósito de esta demostración, se utiliza **Okta**.

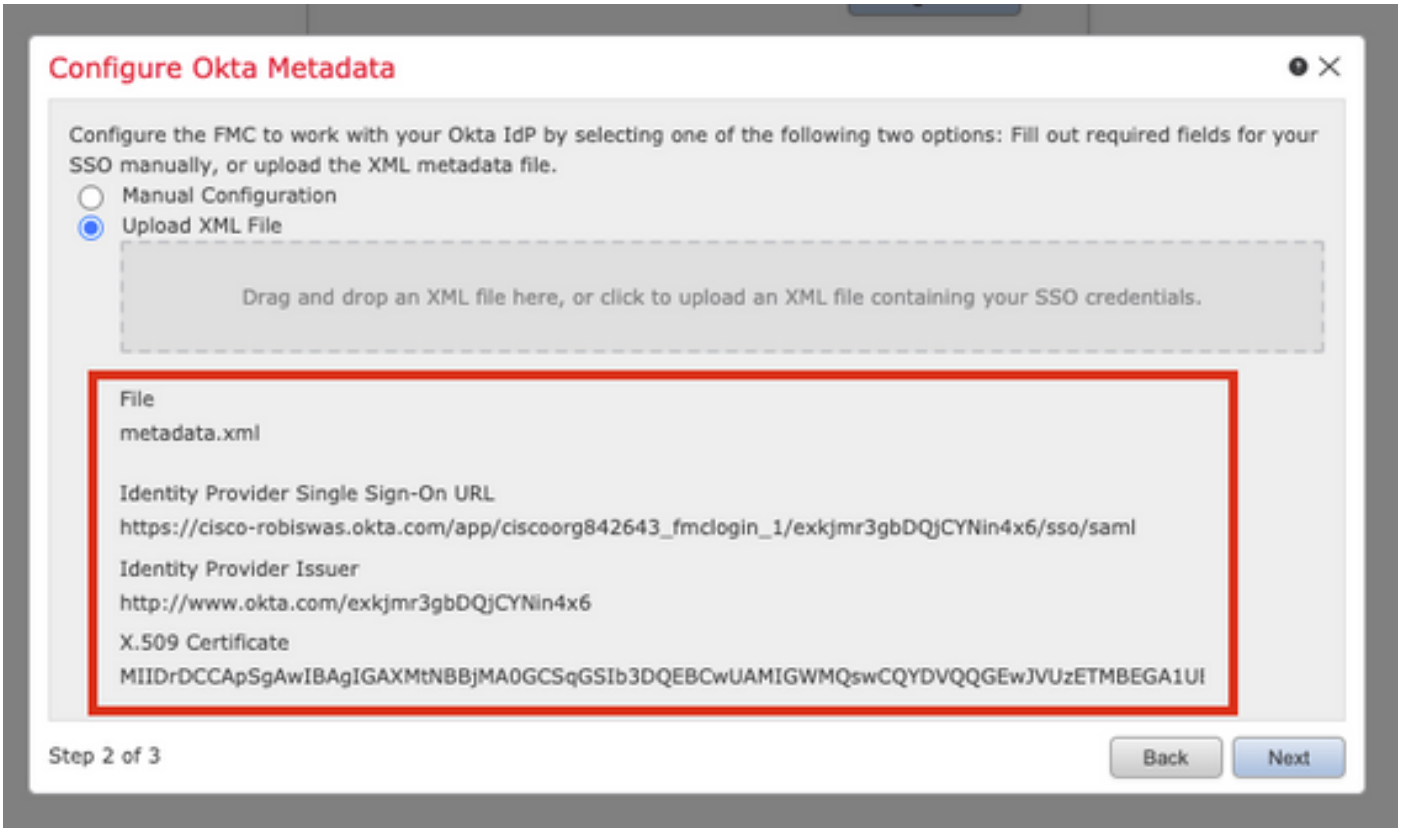
Paso 6. Puede elegir **Configuración manual** e introducir los datos iDP manualmente. Haga clic en **Siguiente**, como



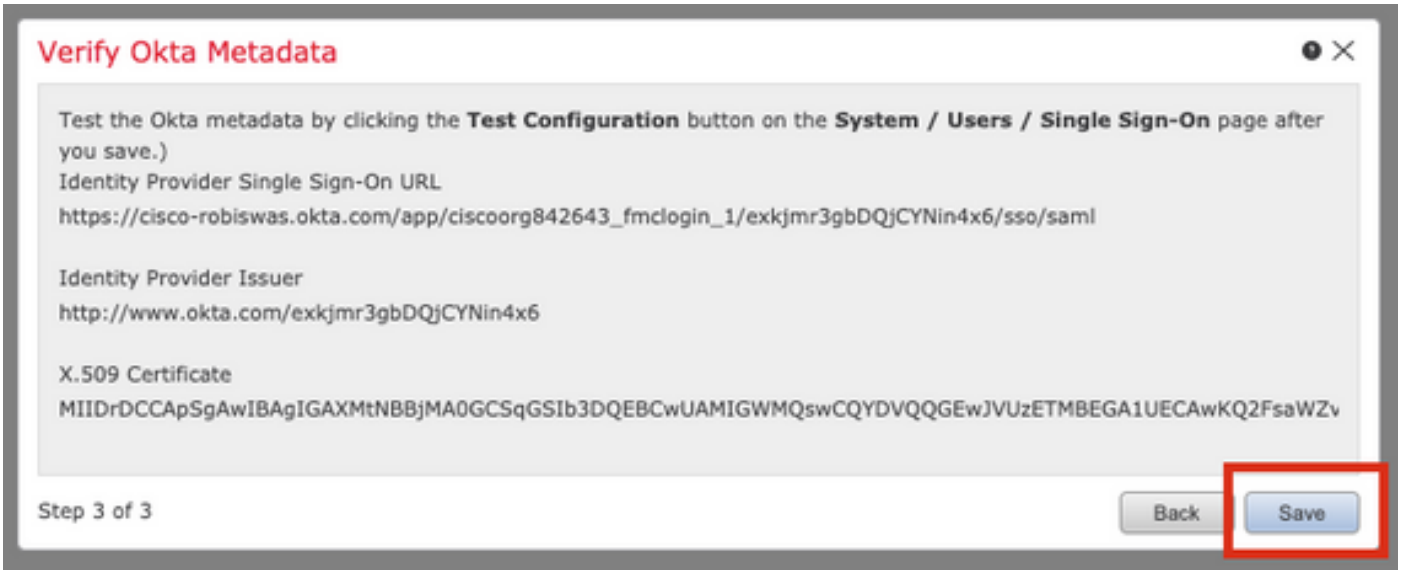
También puede elegir **Cargar archivo XML** y cargar el archivo XML recuperado en el Paso 10 de Configuración de Okta.



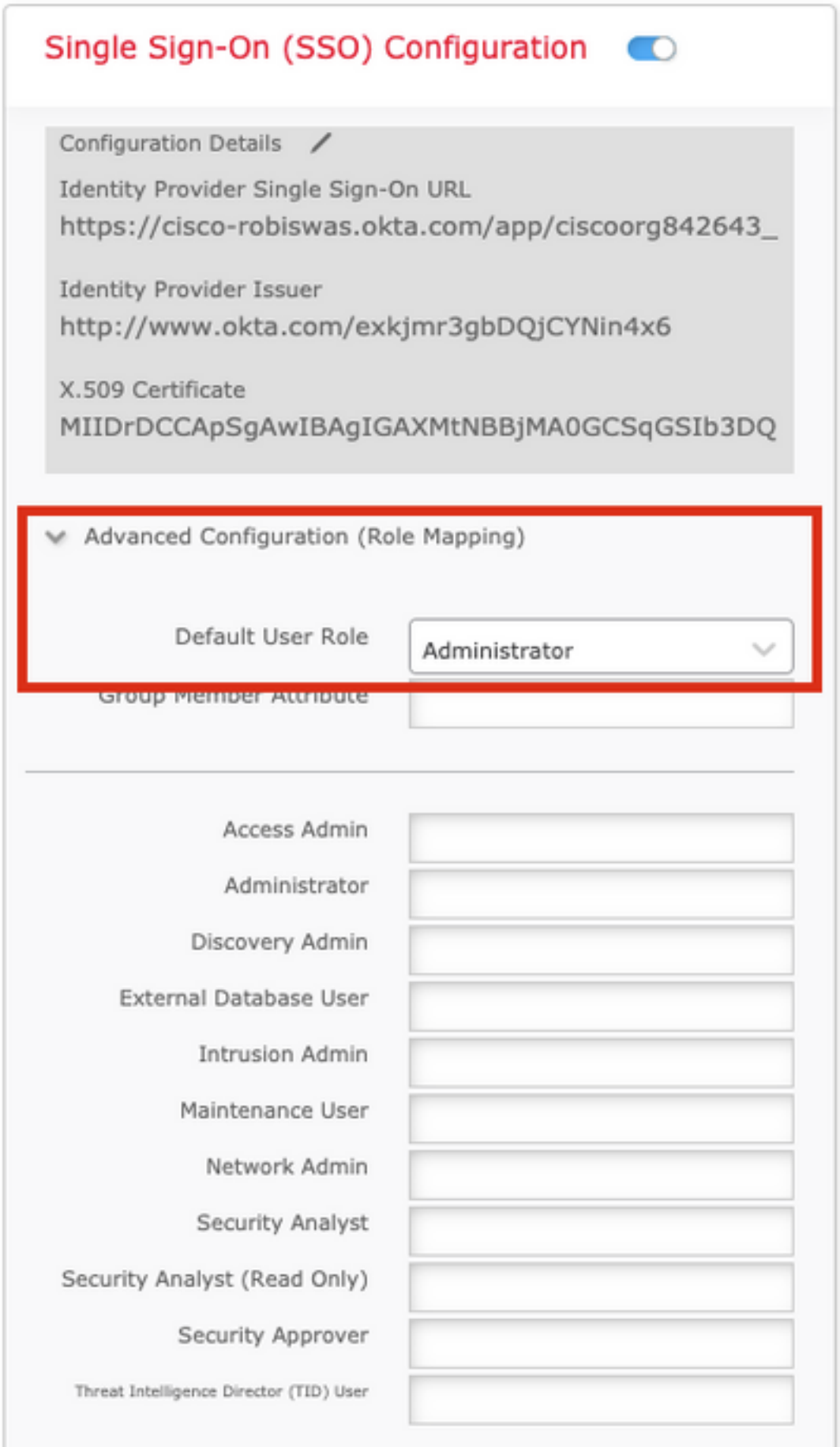
Una vez que se carga el archivo, el FMC muestra los metadatos. Haga clic en **Next**, como se muestra en esta imagen.



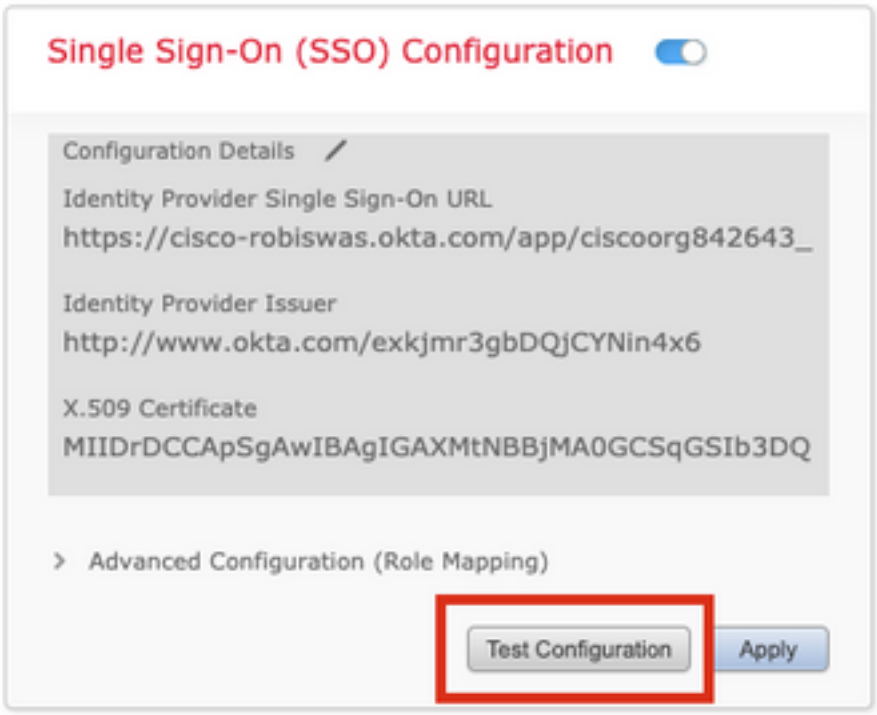
Paso 7. **Verifique** los metadatos. Haga clic en **Guardar**, como se muestra en esta imagen.



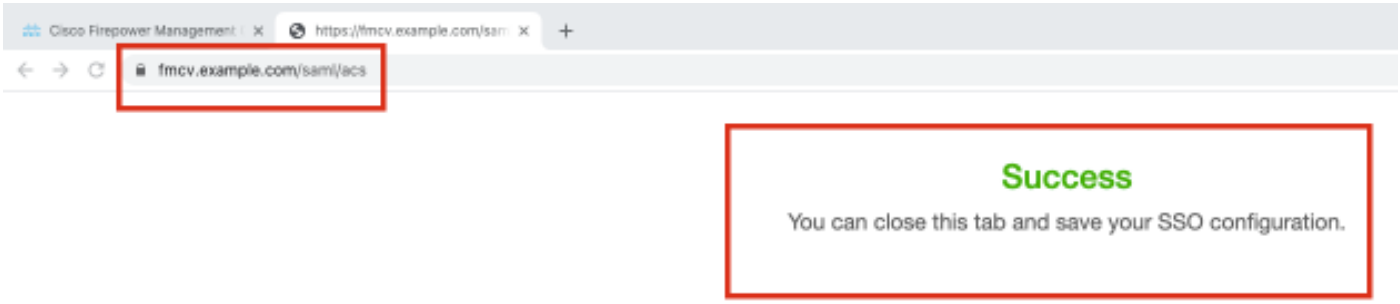
Paso 8. Configure la **Asignación de Función/Función de Usuario Predeterminada** en **Configuración Avanzada**.



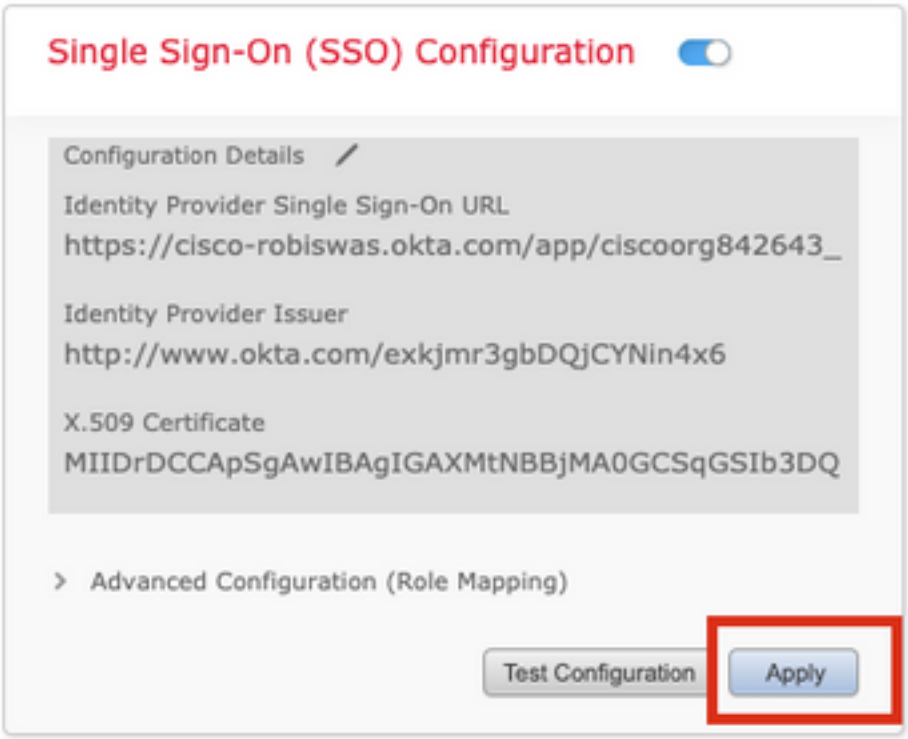
Paso 9. Para probar la configuración, haga clic en **Test Configuration**, como se muestra en esta imagen.



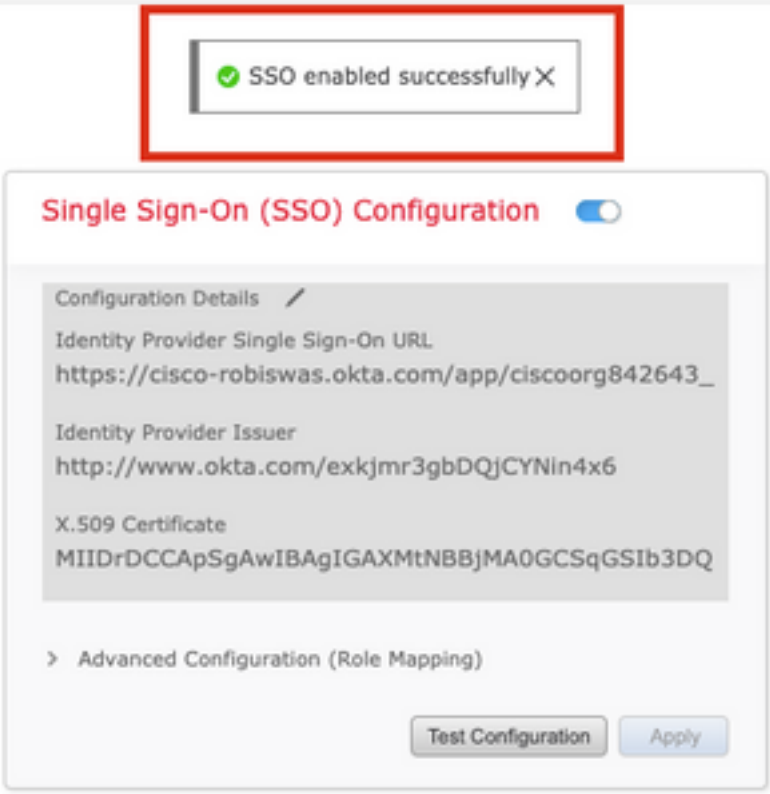
Si la prueba se realiza correctamente, debería ver la página mostrada en esta imagen, en una nueva pestaña del navegador.



Paso 10. Haga clic en **Aplicar** para guardar la configuración.



SSO debe estar habilitado correctamente.

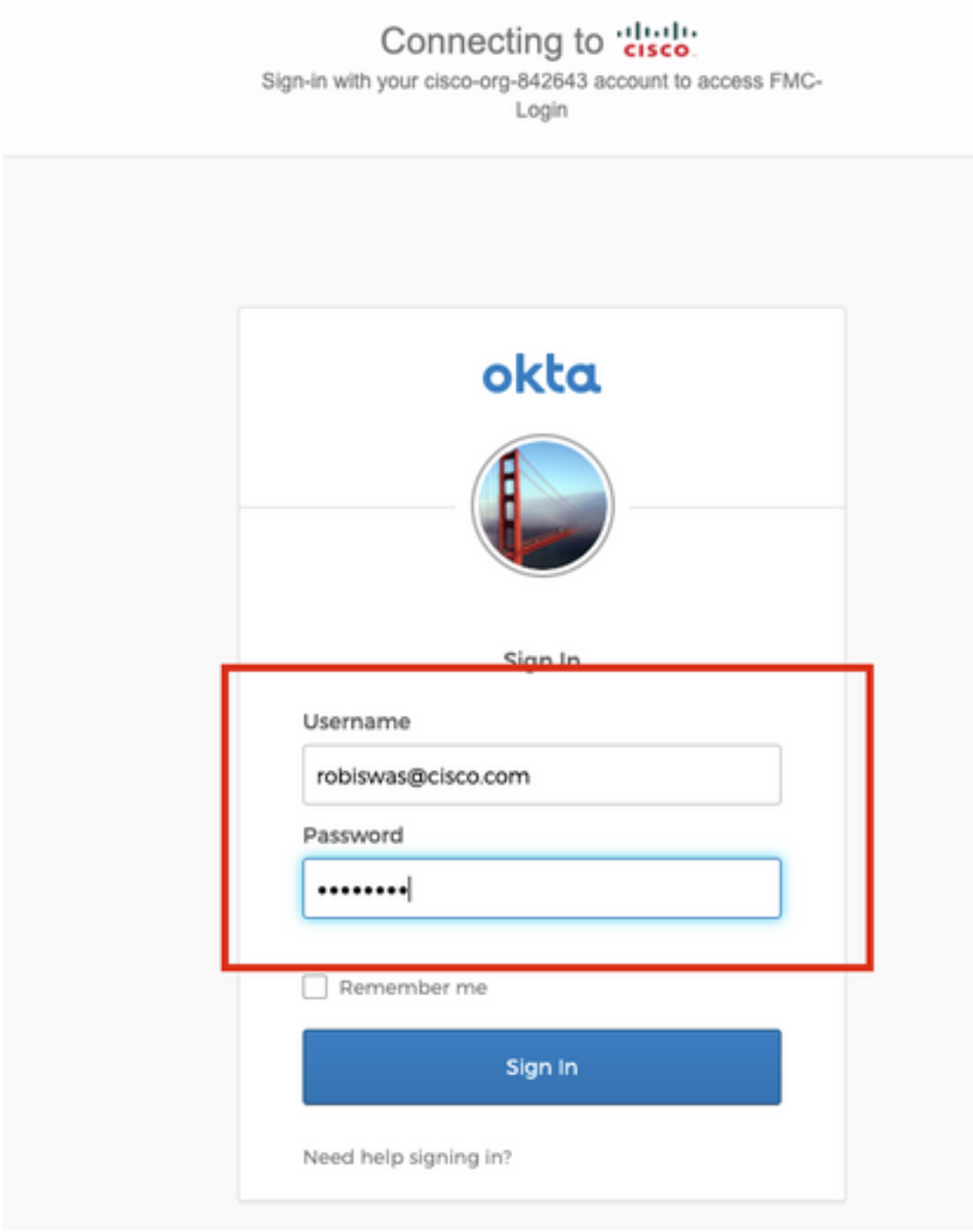


Verificación

Navegue hasta la URL de FMC desde su navegador: https://<fmc URL>. Haga clic en **Inicio de**

sesión único.

Se le redirigirá a la página de inicio de sesión de iDP (Okta). Proporcione sus credenciales de SSO. Haga clic en **Iniciar sesión**.



Si se realiza correctamente, debería poder iniciar sesión y ver la página predeterminada de FMC.

En FMC, navegue hasta **System > Users** para ver el usuario SSO agregado a la base de datos.