

Configurar FMC SSO con Azure como proveedor de identidad

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración de IdP](#)

[Configuración SP](#)

[SAML en FMC](#)

[Limitaciones y advertencias](#)

[Configurar](#)

[Configuración en el proveedor de identidad](#)

[Configuración en Firepower Management Center](#)

[Configuración avanzada - RBAC con Azure](#)

[Verificación](#)

[Troubleshoot](#)

[Registros SAML del explorador](#)

[Registros SAML de FMC](#)

Introducción

Este documento describe cómo configurar Firepower Management Center (FMC) Single Sign-On (SSO) con Azure como proveedor de identidad (IdP).

El lenguaje de marcado de aserción de seguridad (SAML) es el protocolo subyacente que hace posible el SSO. Una empresa mantiene una única página de inicio de sesión, detrás de la cual hay un almacén de identidades y varias reglas de autenticación. Puede configurar fácilmente cualquier aplicación web que soporte SAML, lo que le permite iniciar sesión en todas las aplicaciones web. También tiene la ventaja de no obligar a los usuarios a mantener (y potencialmente reutilizar) las contraseñas de cada aplicación web a la que necesiten acceder, ni exponer las contraseñas a esas aplicaciones web.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de Firepower Management Center
- Comprensión básica del inicio de sesión único

Componentes Utilizados

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

- Cisco Firepower Management Center (FMC) versión 6.7.0
- Azure - IdP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Terminologías SAML

La configuración para SAML debe realizarse en dos lugares: en el IdP y en el SP. El IdP debe configurarse para que sepa dónde y cómo enviar a los usuarios cuando deseen iniciar sesión en un SP específico. El SP necesita configurarse para saber que puede confiar en las afirmaciones SAML firmadas por el IdP.

Definición de algunos términos que son fundamentales para SAML:

- Proveedor de identidad (IdP): herramienta o servicio de software (a menudo visualizado por una página de inicio de sesión o panel) que realiza la autenticación; verifica el nombre de usuario y las contraseñas, verifica el estado de la cuenta, invoca dos factores, etc.
- Proveedor de servicios (SP): aplicación web en la que el usuario intenta obtener acceso.
- Afirmación SAML: mensaje que afirma la identidad de un usuario y, a menudo, otros atributos, que se envía a través de HTTP a través de las redirecciones del explorador.

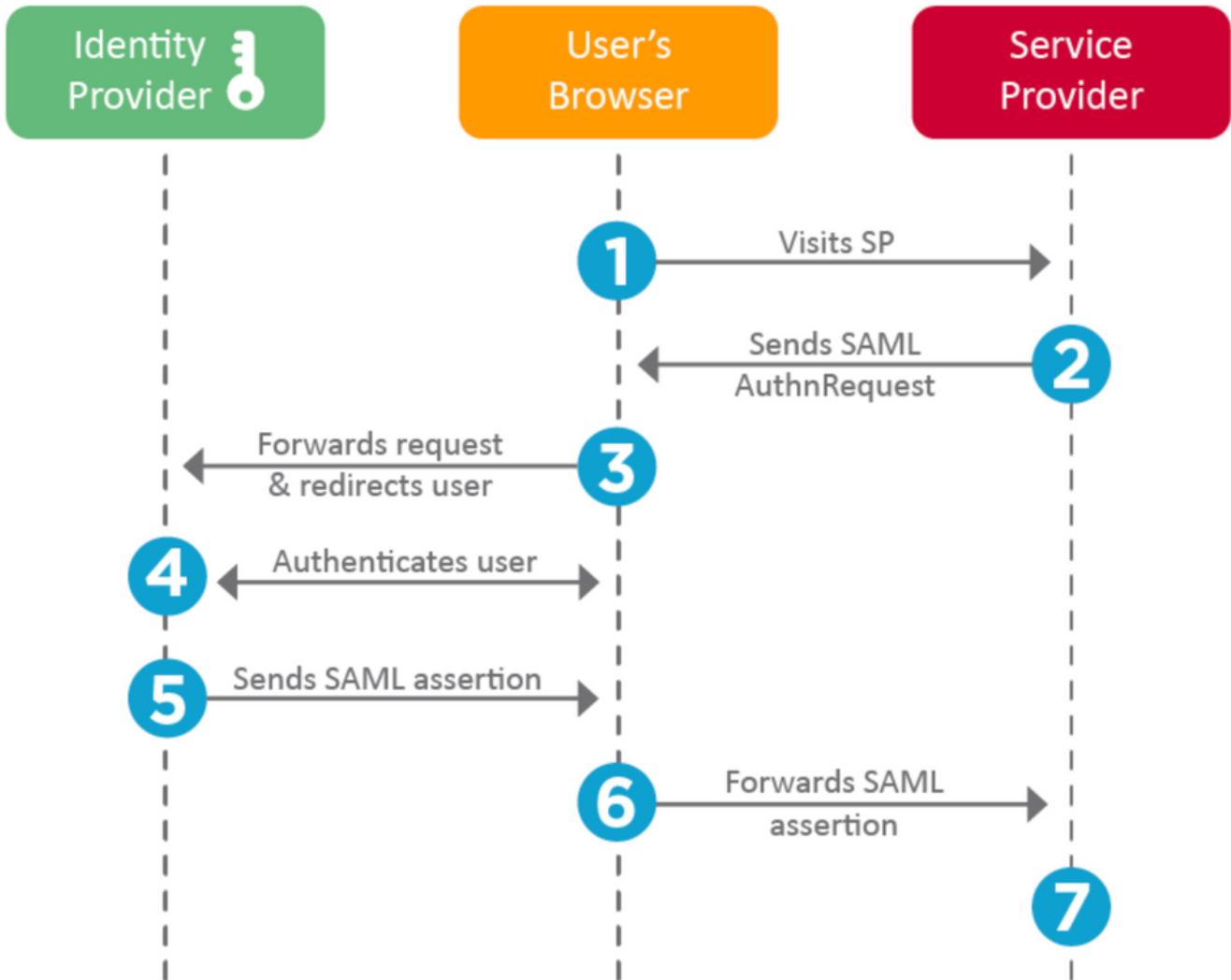
Configuración de IdP

El SP proporciona las especificaciones para una afirmación SAML, lo que debe contener y cómo debe formatearse, y las establece en el IdP.

- EntityID: nombre global único para el SP. Los formatos varían, pero cada vez es más común ver este valor formateado como URL.
Ejemplo: <https://<FQDN-or-IPaddress>/saml/metadata>
- Validador del servicio de consumidor de afirmación (ACS): medida de seguridad en forma de expresión regular (regex) que garantiza que la afirmación SAML se envía al ACS correcto. Esto sólo se aplica durante los inicios de sesión iniciados por SP donde la solicitud SAML contiene una ubicación ACS, por lo que este validador ACS garantizaría que la ubicación ACS proporcionada por la solicitud SAML es legítima.
Ejemplo: <https://<FQDN-or-IPaddress>/saml/acs>
- Atributos: el número y el formato de los atributos pueden variar mucho. Normalmente hay al menos un atributo, el nameID, que suele ser el nombre de usuario del usuario que intenta

iniciar sesión.

- Algoritmo de firma SAML - SHA-1 o SHA-256. Menos comúnmente SHA-384 o SHA-512. Este algoritmo se utiliza junto con el certificado X.509 se menciona aquí.



Configuración SP

A la inversa de la sección anterior, esta sección habla de la información proporcionada por el IdP y establecida en el SP.

- URL del emisor: identificador único del IdP. Formateado como una URL que contiene información sobre el IdP para que el SP pueda validar que las afirmaciones SAML que recibe se emitan del IdP correcto.
Ejemplo: <saml:Emisor <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/> >
- URL de inicio de sesión del proveedor de servicios/punto final SSO de SAML: un punto final de IdP que inicia la autenticación cuando el SP lo redirige aquí con una solicitud SAML.
Ejemplo: <https://login.microsoftonline.com/023480840129412-824812/saml2>
- Extremo SAML SLO (Single Log-out) - Un punto final de IdP que cierra su sesión de IdP cuando el SP lo redirige aquí, normalmente después de **cerrar sesión** se hace clic en él.
Ejemplo: <https://access.wristbandtent.com/logout>

SAML en FMC

La función SSO de FMC se introduce a partir de la versión 6.7. La nueva función simplifica la autorización de FMC (RBAC), ya que asigna la información existente a las funciones de FMC. Se aplica a todos los usuarios de la interfaz de usuario de FMC y a las funciones de FMC. Por ahora, admite la especificación SAML 2.0 y estos IDP soportados

- OKTA
- OneLogin
- PingID
- Azure AD
- Otros (Cualquier IDP que cumpla con SAML 2.0)

Limitaciones y advertencias

- SSO sólo se puede configurar para el dominio global.
- Los FMC en el par HA necesitan una configuración individual.
- Sólo los administradores locales/AD pueden configurar el inicio de sesión único.
- SSO iniciado desde Idp no se soporta.

Configurar

Configuración en el proveedor de identidad

Paso 1. Inicie sesión en Microsoft Azure. Vaya a **Azure Active Directory > Enterprise Application**.

Default Directory | Overview

Azure Active Directory

Overview

Getting started

Preview hub

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units (Preview)

Enterprise applications



Switch tenant Delete tenant Create

Azure Active Directory can help you enable remote

Default Directory

Search your tenant

Tenant information

Your role

Global administrator [More info](#)

License

Azure AD Free

Tenant ID

- Paso 2. Cree **Nueva aplicación** en Aplicación no-Galería, como se muestra en esta imagen.

[Home](#) > [Default Directory](#) > [Enterprise applications | All applications](#) > [Add an application](#) >

Add your own application

Name * ⓘ

Firepower Test ✓

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports: ⓘ

SAML-based single sign-on

[Learn more](#)

Automatic User Provisioning with SCIM

[Learn more](#)

Password-based single sign-on

[Learn more](#)

Paso 3. Edite la Aplicación que se creó y navegue hasta **Configurar inicio de sesión único > SAML**, como se muestra en esta imagen.

Home > Default Directory > Enterprise applications | All applications > Add an application >

Firepower | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access

Select a single sign-on method [Help me decide](#)

Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based

Password storage and replay using a web browser extension or mobile app.

Linked

Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

Paso 4. Edite la configuración básica de SAML y proporcione los detalles de FMC :

- URL de FMC: <https://<FMC-FQDN-or-IPaddress>>
- Identificador (ID de entidad): <https://<FMC-FQDN-or-IPaddress>/saml/metadata>
- URL de respuesta: <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- URL de inicio de sesión: [/https://<FMC-FQDN-or-IPaddress>/saml/acs](https://<FMC-FQDN-or-IPaddress>/saml/acs)
- RelayState:/ui/login

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-ins
 - Usage & insights (Preview)
 - Audit logs
 - Provisioning logs (Preview)

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Read the [configuration guide](#) for help integrating Cisco-Firepower.

- Basic SAML Configuration** [Edit](#)

Identifier (Entity ID)	https://10.106.46.191/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://10.106.46.191/saml/acs
Sign on URL	https://10.106.46.191/saml/acs
Relay State	/ui/login
Logout Url	Optional
- User Attributes & Claims** [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
roles	user.assignedroles
Unique User Identifier	user.userprincipalname
Group	user.groups
- SAML Signing Certificate** [Edit](#)

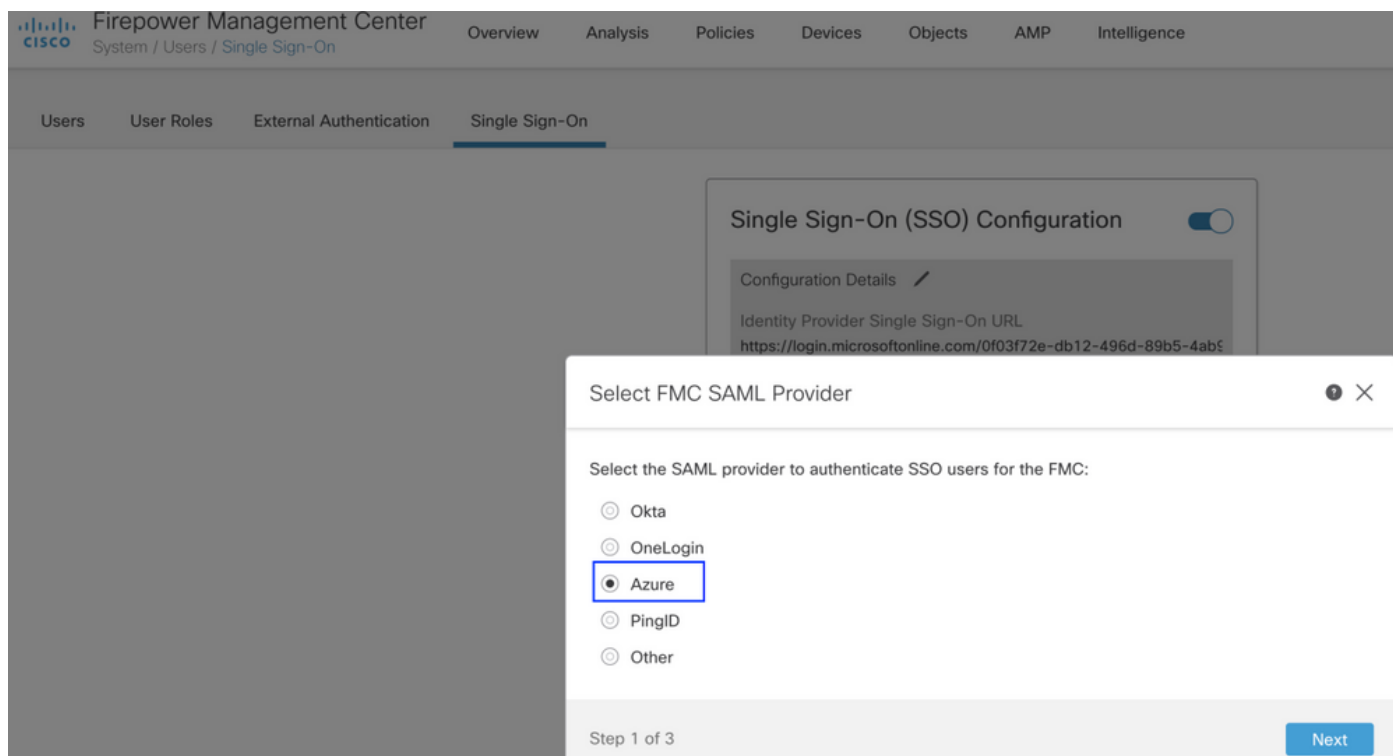
Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Mantenga el resto como valor predeterminado. Esto se analiza más a fondo para el acceso basado en roles.

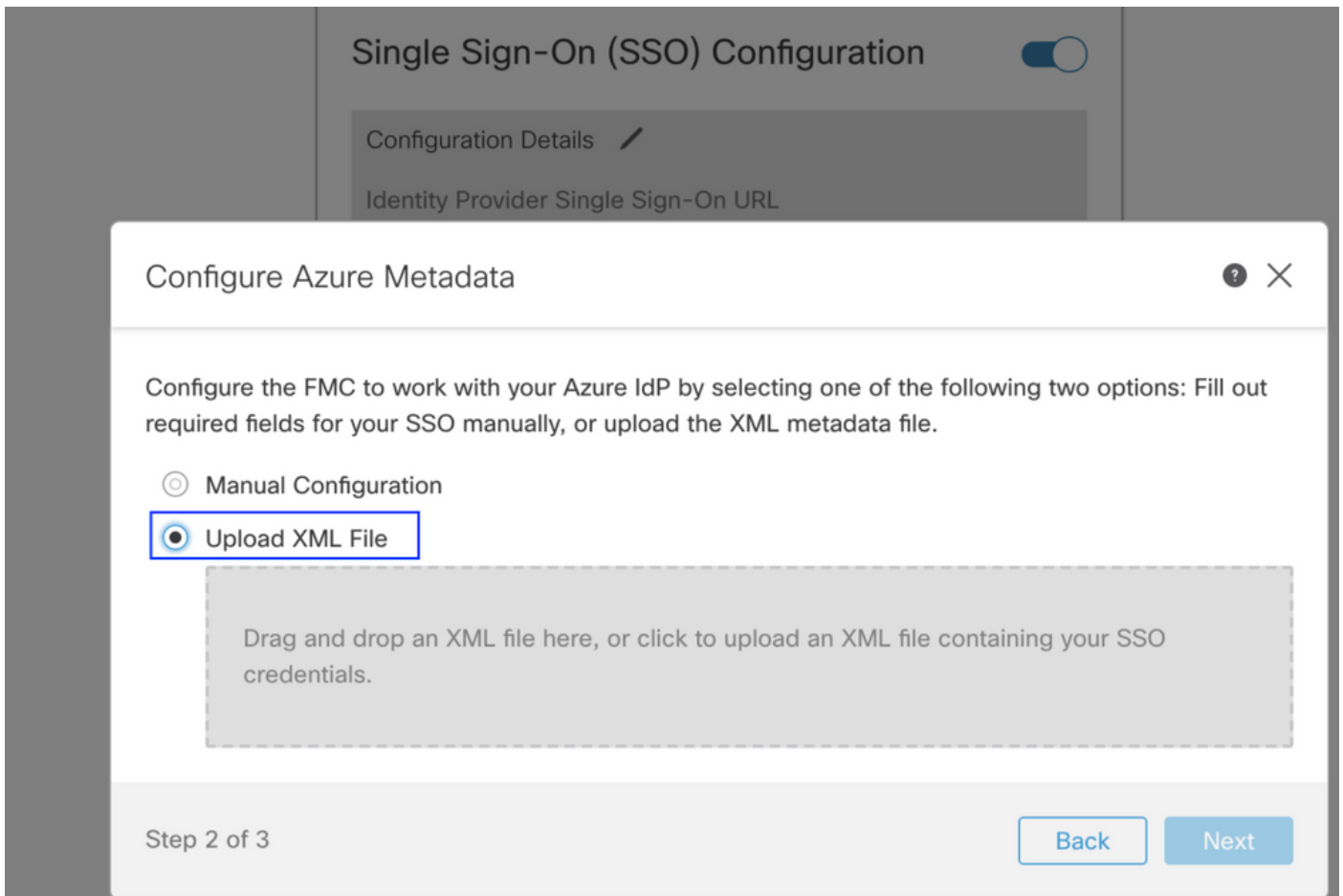
Esto marca el final de la configuración del proveedor de identidad. Descargue el archivo XML de metadatos de federación que se utilizará para la configuración de FMC.

Configuración en Firepower Management Center

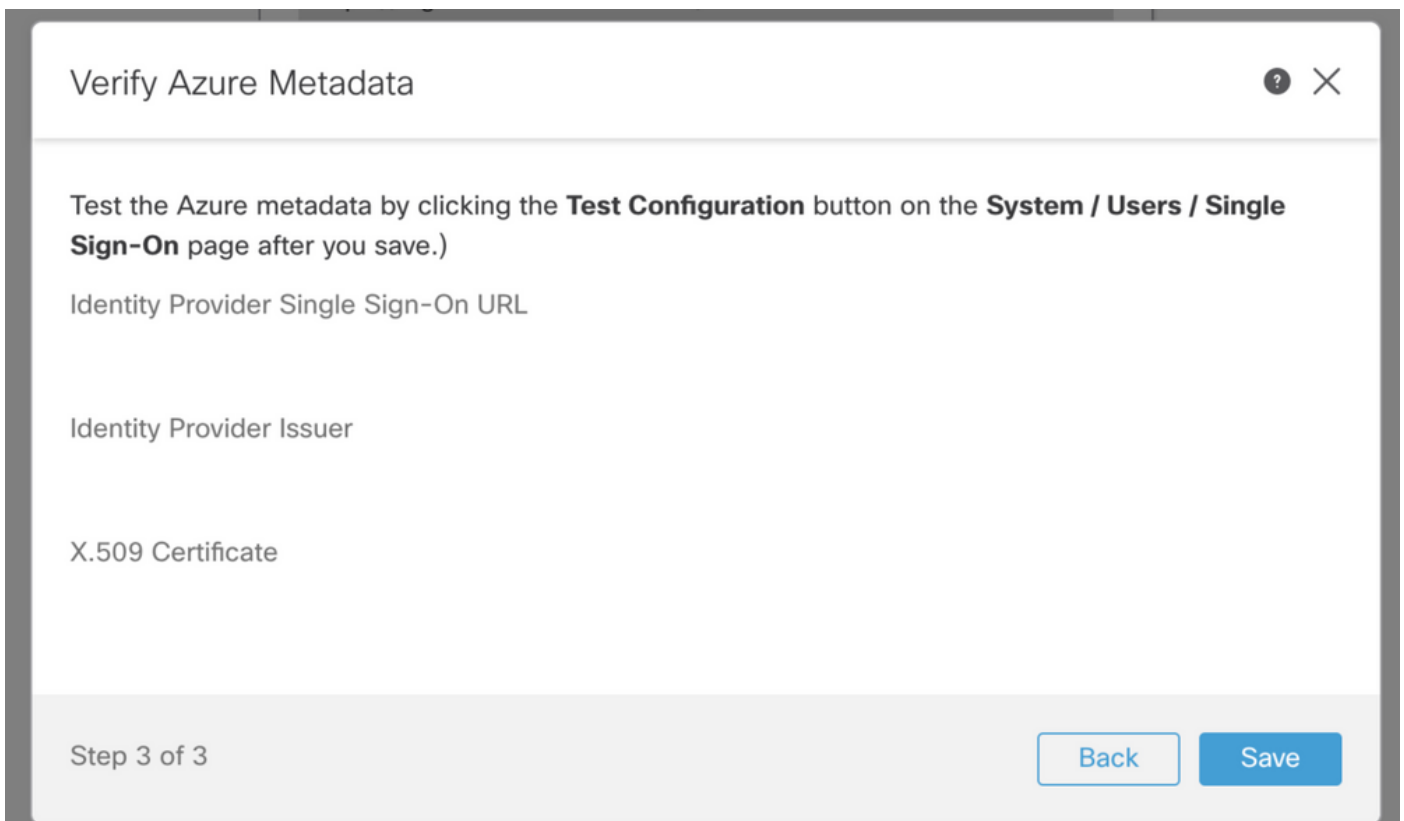
Paso 1. Inicie sesión en FMC, navegue hasta **Settings > Users > Single Sign-On** y Enable SSO. Seleccione **Azure** como Provider.



Paso 2. Cargue el archivo XML descargado de Azure aquí. Rellena automáticamente todos los detalles necesarios.



Paso 3. Verifique la configuración y haga clic en **Guardar**, como se muestra en esta imagen.



Configuración avanzada - RBAC con Azure



Para utilizar varios tipos de funciones para asignar a las funciones de FMC: debe editar el

manifiesto de aplicación en Azure para asignar valores a las funciones. De forma predeterminada, las funciones tienen el valor Null.

Paso 1. Navegue hasta la **Aplicación** que se crea y haga clic en **Inicio de sesión único**.

Home > Default Directory | App registrations >

Cisco-Firepower

Search (Cmd+/) <<  Delete  Endpoints

- Overview
- Quickstart
- Integration assistant (preview)

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest

Support + Troubleshooting


- Troubleshooting
- New support request

Display name : Cisco-Firepower


Application (client) ID :

Directory (tenant) ID :

Object ID :

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Mic

Call APIs



Build more powerful apps with rich user and business data from Microsoft services and your own company's data sources.

[View API permissions](#)

Paso 2. Edite los atributos de usuario y las reclamaciones. Agregar una nueva reclamación con el nombre: **roles** y seleccione el valor como **user.assignedroles**.

User Attributes & Claims

+ Add new claim + Add a group claim ≡ Columns

Required claim






Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for... ***

Additional claims

Claim name	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname ***
roles	user.assignedroles ***

Paso 3. Vaya a **<Application-Name> > Manifest**. Editar el manifiesto. El archivo está en formato JSON y hay un usuario predeterminado disponible para copiar. Por ejemplo, aquí se crean 2 roles: Usuario y analista.

Cisco-Firepower | Manifest

Search (Cmd+/) <<  Save  Discard  Upload  Download |  Got feedback?

- Overview
- Quickstart
- Integration assistant (preview)
- Manage**
- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators (Preview)
- Manifest**
- Support + Troubleshooting**
- Troubleshooting
- New support request

The editor below allows you to update this application by directly modifying its JSON represe

```
1  {
2    "id": "00f52e49-10a0-4580-920f-98aa41d58f6f",
3    "acceptMappedClaims": null,
4    "accessTokenAcceptedVersion": null,
5    "addIns": [],
6    "allowPublicClient": false,
7    "appId": "51dcc017-6730-41ee-b5cd-4e5c380d85c3",
8    "appRoles": [
9      {
10       "allowedMemberTypes": [
11         "User"
12       ],
13       "description": "Analyst",
14       "displayName": "Analyst",
15       "id": "18d14569-c3bd-439b-9a66-3a2aee01d13f",
16       "isEnabled": true,
17       "lang": null,
18       "origin": "Application",
19       "value": "Analyst-1"
20     },
21     {
22       "allowedMemberTypes": [
23         "User"
24       ],
25       "description": "User",
26       "displayName": "User",
27       "id": "18d14569-c3bd-439b-9a66-3a2aee01d14f",
28       "isEnabled": true,
29       "lang": null,
30       "origin": "Application",
31       "value": "User-1"
32     }
33   ]
34 }
```

Paso 4. Vaya a <Application-Name> > Users and Groups. Edite el usuario y asigne las funciones recién creadas, como se muestra en esta imagen.

Edit Assignment

Default Directory

Users

1 user selected. >

Select a role >

None Selected

Assign

Select a role

Only a single role can be selected

Analyst

User

Selected Role

Analyst

Select

Paso 4. Inicie sesión en FMC y edite la configuración avanzada en SSO. Para: Atributo de miembro de grupo: asigne el **nombre de visualización** que ha proporcionado en el manifiesto de aplicación a las funciones.

▼ Advanced Configuration (Role Mapping)

Default User Role

Administrator

Group Member Attribute

roles

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

Una vez hecho esto, debe poder iniciar sesión en su función designada.

Verificación

Paso 1. Acceda a la URL de FMC desde su navegador: <https://<FMC URL>>. Haga clic en **Inicio de sesión único**, como se muestra en esta imagen.



Firepower Management Center

Username

Password

Single Sign-On

Log In

Se le redirige a la página de inicio de sesión de Microsoft y el inicio de sesión correcto devolverá la página predeterminada de FMC.

Paso 2. En FMC, navegue hasta **System > Users** para ver el usuario SSO agregado a la base de datos.

test1@shbhartisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartisco.onmicrosoft.com

Administrator

External (SSO)

Troubleshoot

Verifique la autenticación SAML y este es el flujo de trabajo que consigue para una autorización exitosa (Esta imagen es de un entorno de laboratorio) :

Registros SAML del explorador

GET	https://10.106.46.191/sso/saml/login	
GET	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/saml2?RelayState=7_ni-J1fNA5eEeVvoAuhcviH6CwKjxwyGhnxJpArDjKAFMbK-wvJ2RSP&SAML	SAML
GET	https://login.live.com/Me.htm?v=3	
POST	https://login.microsoftonline.com/common/GetCredentialType?mkt=en-US	
POST	https://login.microsoftonline.com/0f03f72e-db12-496d-89b5-4ab9fc80d8aa/login	
GET	https://login.live.com/Me.htm?v=3	
POST	https://login.microsoftonline.com/kmsi	
POST	https://10.106.46.191/saml/acs	SAML
GET	https://login.microsoftonline.com/favicon.ico	
GET	https://10.106.46.191/sso/saml/login	
GET	https://10.106.46.191/ui/login	
POST	https://10.106.46.191/auth/login	

Registros SAML de FMC

Verifique los registros SAML en FMC en `/var/log/auth-daemon.log`

```
root@shbharti1ffncl1:/var/log# tail -f auth-daemon.log
auth-daemon 2020/08/09 04:59:11 I! Writing Audit Log to DB.
auth-daemon 2020/08/09 04:59:11 I! Parsing SAML ACS Response
auth-daemon 2020/08/09 04:59:11 I! SAML ACS Response Parsed, ID: id-56574e8a5f44bdd58102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! Authorizing Response, ID : id-56574e8a5f44bdd58102743d2cc9350b75f74d8c
auth-daemon 2020/08/09 04:59:11 I! No member value in Data. Using Default Role.
auth-daemon 2020/08/09 04:59:11 I! Attribute Map in the token : map[http://schemas.microsoft.com/claims/authnmethodsreferences:[http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password]
http://schemas.microsoft.com/identity/claims/objectid:[b5-4ab9fc80d8aa/] http://schemas.microsoft.com/identity/claims/objectid:[a] http://schemas.xmlsoap.org/w
/2005/05/identity/claims/givenname:[Test 1] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name:[test@shbhartiCisco.onmicrosoft.com] http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname:[Guy]
mapped_role_uid:[bee2eb18-e129-11df-a04a-42c66f0a3b36]]
auth-daemon 2020/08/09 04:59:11 I! Redirecting ID : id-56574e8a5f44bdd58102743d2cc9350b75f74d8c, URI : /sso/saml/login
```