

Configurar o SSO do FMC com o Azure como provedor de identidade

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração do IdP](#)

[Configuração do SP](#)

[SAML no FMC](#)

[Limitações e caveats](#)

[Configurar](#)

[Configuração no provedor de identidade](#)

[Configuração do Firepower Management Center](#)

[Configuração avançada - RBAC com Azure](#)

[Verificar](#)

[Troubleshoot](#)

[Logs SAML do navegador](#)

[Logs SAML do FMC](#)

Introduction

Este documento descreve como configurar o SSO (Single Sign-On, logon único) do Firepower Management Center (FMC) com o Azure como provedor de identidade (IdP).

O Security Assertion Markup Language (SAML) é com mais frequência o protocolo subjacente que torna o SSO possível. Uma empresa mantém uma única página de login, atrás dela está um repositório de identidade e várias regras de autenticação. Ele pode facilmente configurar qualquer aplicativo da Web que suporte SAML, o que permite que você faça login em todos os aplicativos da Web. Ele também tem o benefício de segurança de não forçar os usuários a manter (e potencialmente reutilizar) senhas para cada aplicativo da Web ao qual eles precisam acessar, nem expor senhas a esses aplicativos da Web.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Compreensão básica do Firepower Management Center
- Compreensão básica do login único

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center (FMC) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Terminologias SAML

A configuração do SAML deve ser feita em dois locais: no IdP e no SP. O IdP precisa ser configurado para que ele saiba para onde e como enviar usuários quando desejam fazer login em uma controladora específica. O SP precisa ser configurado para que ele saiba que pode confiar em asserções SAML assinadas pelo IdP.

Definição de alguns termos centrais para o SAML:

- Provedor de identidade (IdP) - A ferramenta ou serviço de software (geralmente visualizado por uma página de login e/ou painel) que executa a autenticação; verifica o nome de usuário e as senhas, verifica o status da conta, invoca dois fatores, etc.
- Provedor de serviços (SP) - O aplicativo da Web no qual o usuário tenta obter acesso.
- SAML Assertion - Uma mensagem que afirma a identidade de um usuário e, muitas vezes, outros atributos, enviada por HTTP via redirecionamentos do navegador

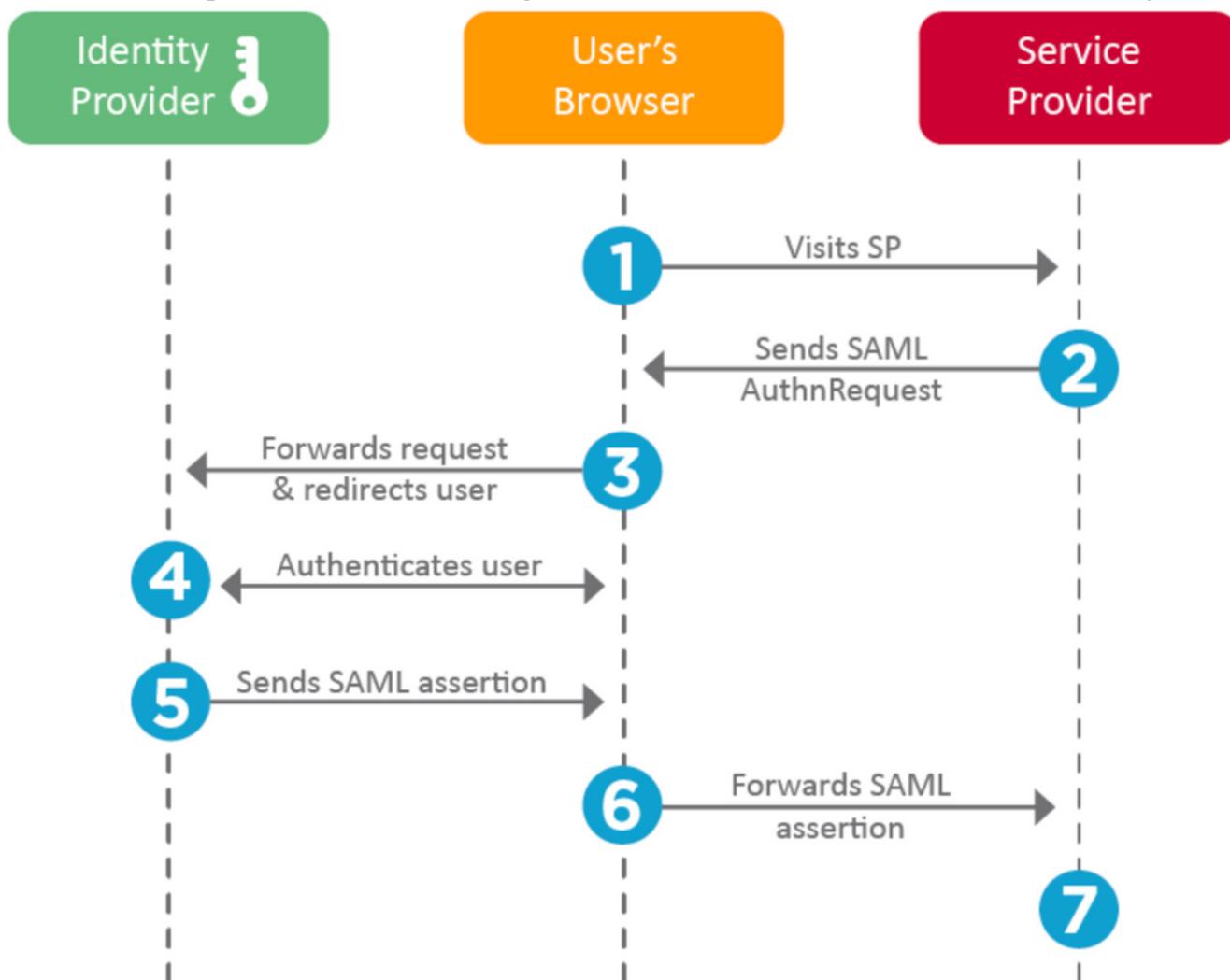
Configuração do IdP

As especificações de uma asserção SAML, o que ela deve conter e como deve ser formatada são fornecidas pelo SP e definidas no IdP.

- EntityID - um nome globalmente exclusivo para o SP. Os formatos variam, mas é cada vez mais comum ver esse valor formatado como um URL.
Exemplo: <https://<FQDN-or-IPaddress>/saml/metadados>
- Validador do Serviço de Consumidor de Asserção (ACS) - Uma medida de segurança na forma de uma expressão regular (regex) que garante que a asserção SAML seja enviada para o ACS correto. Isso só é executado durante os logins iniciados por SP em que a solicitação SAML contém um local ACS, portanto, esse validador ACS garante que o local ACS fornecido pela solicitação SAML é legítimo.
Exemplo: <https://<FQDN-or-IPaddress>/saml/acs>
- Atributos - O número e o formato dos atributos podem variar muito. Geralmente, há pelo menos um atributo, o nameID, que normalmente é o nome de usuário do usuário que está

tentando fazer login.

- Algoritmo de assinatura SAML - SHA-1 ou SHA-256. Menos comumente SHA-384 ou SHA-512. Este algoritmo é usado em conjunto com o certificado X.509 é mencionado aqui.



Configuração do SP

No verso da seção acima, esta seção fala sobre as informações fornecidas pelo IdP e definidas na controladora de armazenamento.

- URL do emissor - Identificador exclusivo do IdP. Formatado como um URL que contém informações sobre o IdP para que a controladora possa validar se as asserções SAML que recebe são emitidas do IdP correto.
Exemplo: <saml:Issuer <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/> >
- Ponto de Extremidade SSO SAML / URL de Login do Provedor de Serviços - Um ponto de extremidade IdP que inicia a autenticação quando redirecionado aqui pelo SP com uma solicitação SAML.
Exemplo: <https://login.microsoftonline.com/023480840129412-824812/saml2>
- Ponto de Extremidade SAML SLO (Logoff Único) - Um ponto de extremidade IdP que fecha sua sessão IdP quando redirecionada aqui pela controladora de armazenamento, geralmente após o **logoff** ser clicado.

Exemplo: <https://access.wristbandtent.com/logout>

SAML no FMC

O recurso SSO no FMC é apresentado a partir da versão 6.7. O novo recurso simplifica a RBAC (Autorização de FMC), pois mapeia as informações existentes para as funções de FMC. Ele se aplica a todos os usuários de IU do FMC e às funções do FMC. Por enquanto, ele suporta a especificação SAML 2.0 e esses IDPs suportados

- OKTA
- OneLogin
- PingID
- Azure AD
- Outros (qualquer IDP compatível com SAML 2.0)

Limitações e caveats

- O SSO pode ser configurado somente para o domínio global.
- Os FMCs no par HA precisam de configuração individual.
- Somente administradores locais/AD podem configurar o Logon único.
- SSO iniciado a partir de Idp não é suportado.

Configurar

Configuração no provedor de identidade

Etapa 1. Faça login no Microsoft Azure. Navegue para **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

- Etapa 2. Criar **Novo Aplicativo** em Aplicativo Não Galeria, como mostrado nesta imagem.

[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](#)

Etapa 3. Edite o Aplicativo que foi criado e navegue para **Configurar logon único > SAML**, como mostrado nesta imagem.

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.

Etapa 4. Edite a Configuração SAML básica e forneça os detalhes do FMC:

- URL do FMC: <https://<FMC-FQDN-or-IPaddress>>
- Identificador (ID da entidade): <https://<FMC-FQDN-or-IPaddress>/saml/metadados>
- URL de resposta: <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- URL de início de sessão: <https://<FMC-QDN-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/metadados
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](#)

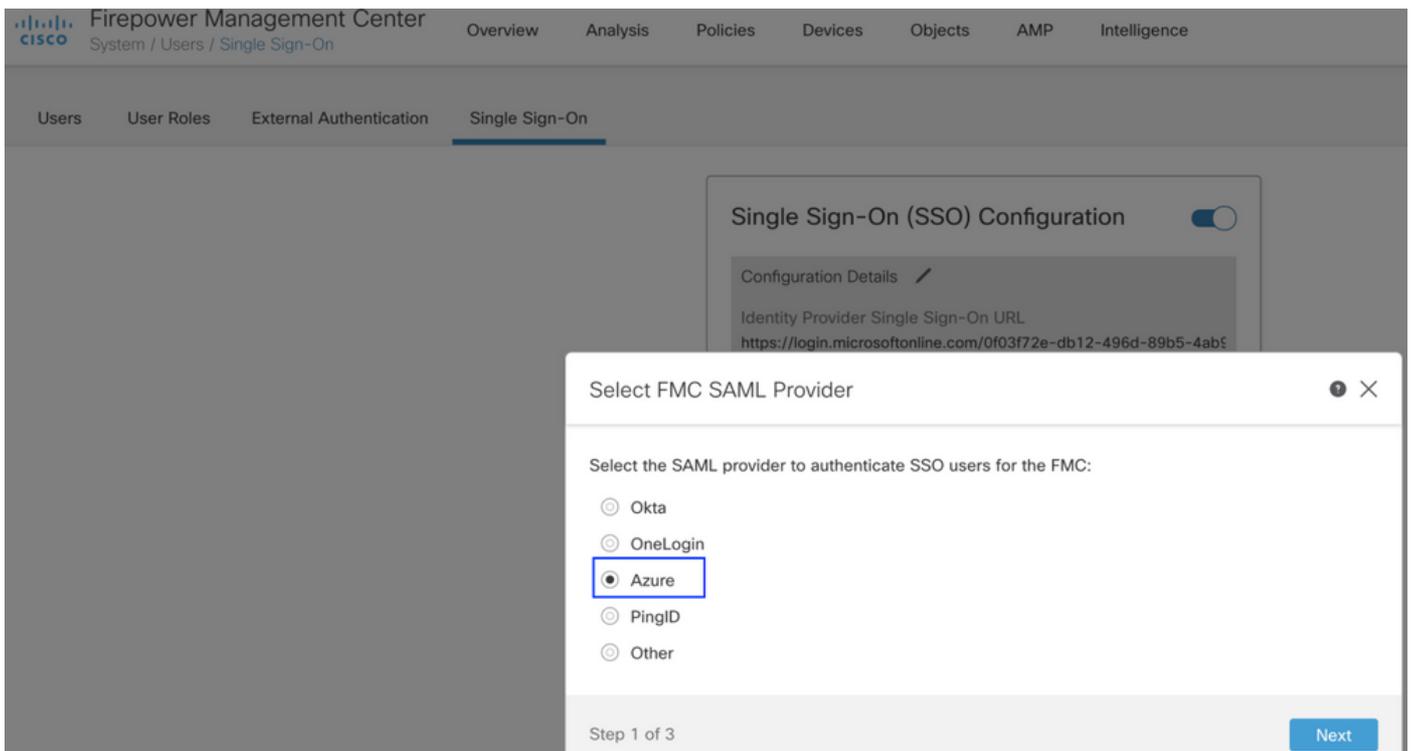
Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Mantenha o restante como padrão - isso é discutido com mais detalhes sobre o acesso baseado em função.

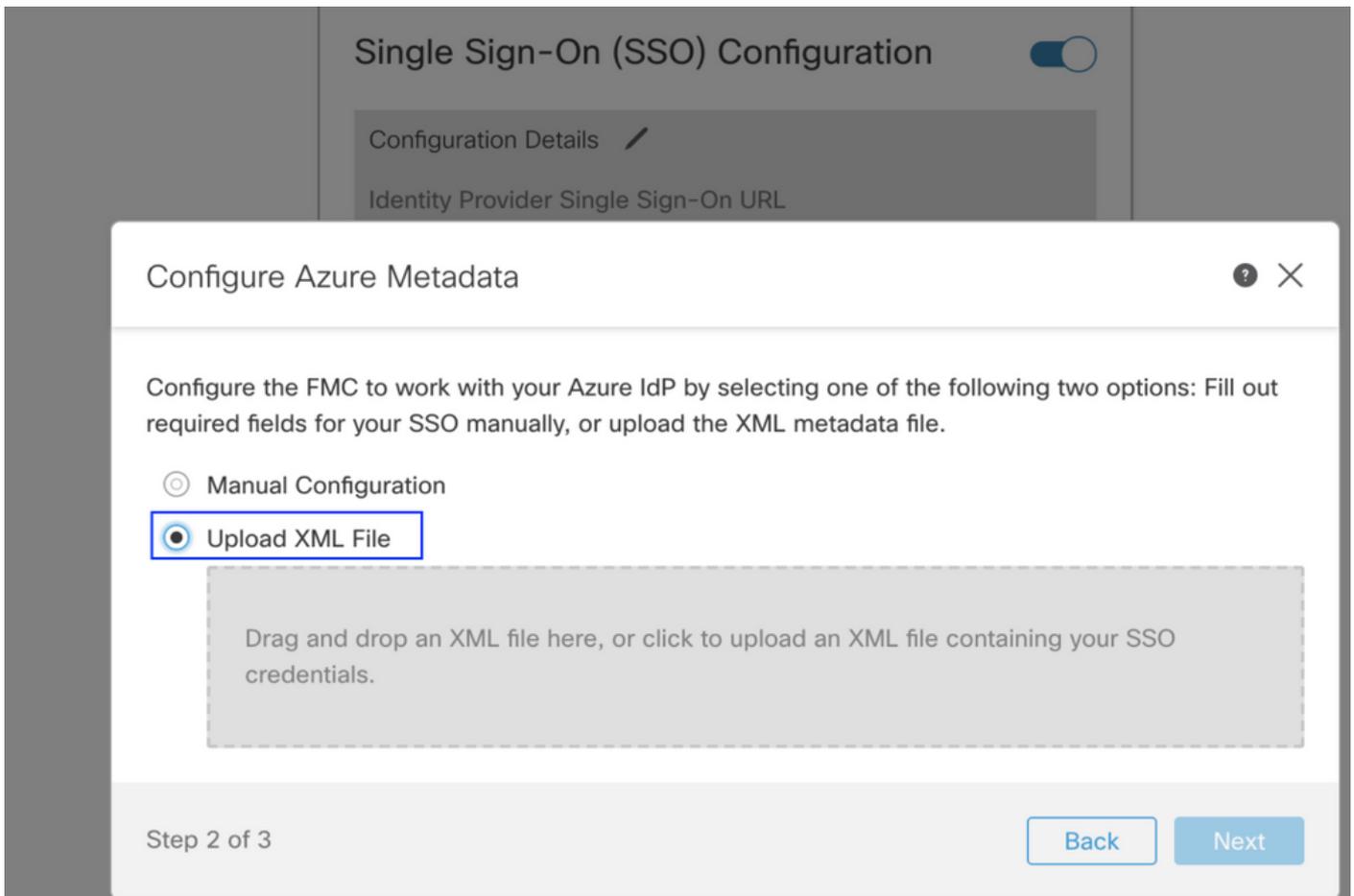
Isso marca o fim da configuração do provedor de identidade. Faça o download do XML de metadados de federação que será usado para a configuração do FMC.

Configuração do Firepower Management Center

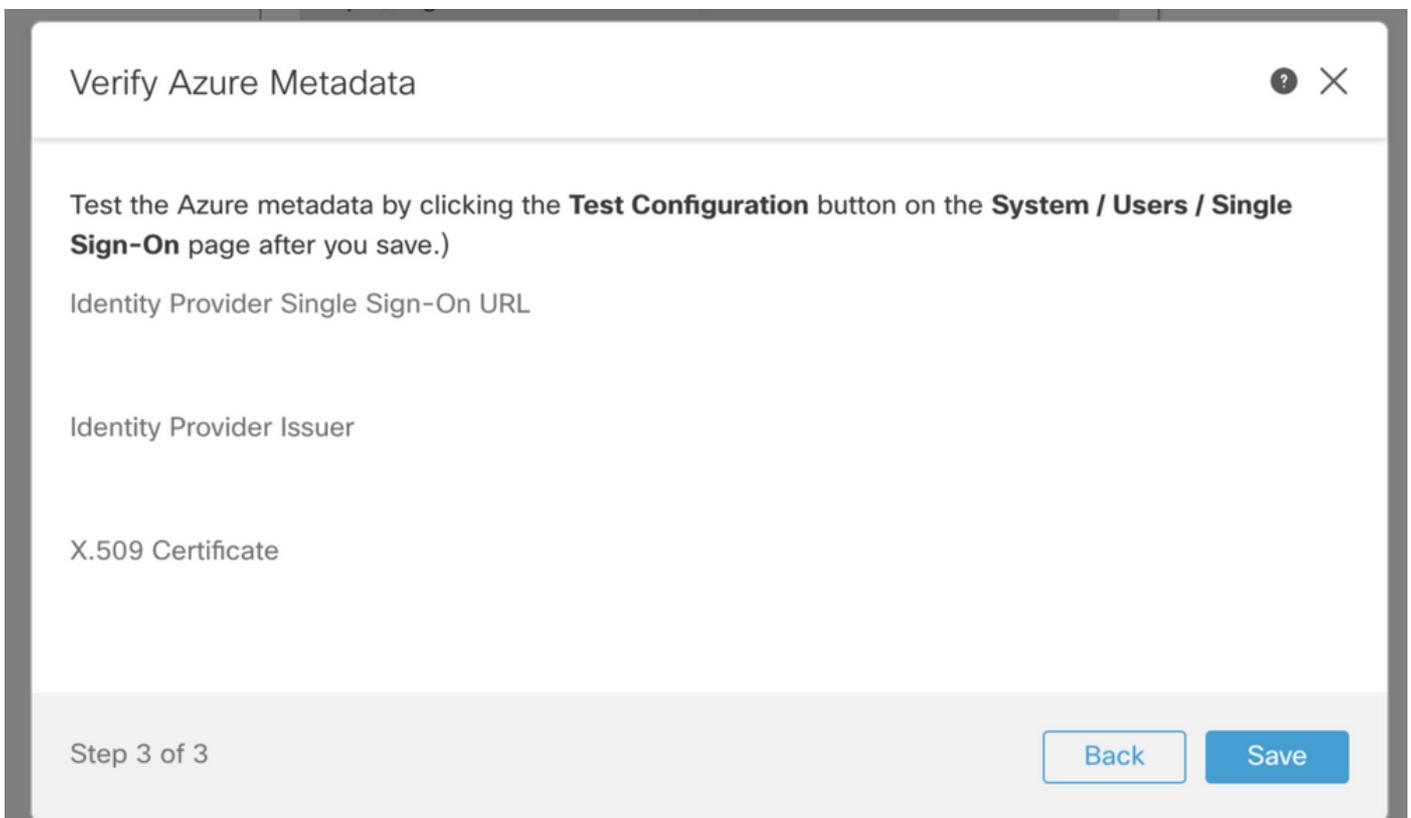
Etapa 1. Faça login no FMC, navegue para **Settings > Users > Single Sign-On** e Enable SSO. Selecione **Azure** como Provedor.



Etapa 2. Carregue o arquivo XML baixado do Azure aqui. Ele preenche automaticamente todos os detalhes necessários.



Etapa 3. Verifique a configuração e clique em **Salvar**, como mostrado nesta imagem.



Configuração avançada - RBAC com Azure

Para usar vários tipos de função para mapear para Funções do FMC - Você precisa editar o

manifesto do Aplicativo no Azure para atribuir valores a funções. Por padrão, as funções têm valor como Nulo.

Etapa 1. Navegue até o **Aplicativo** criado e clique em **Logon 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 Authentic 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](#)

Etapa 2. Edite os atributos do usuário e as reivindicações. Adicionar uma nova reivindicação com o nome: **funções** e seleccione o 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 ***

Etapa 3. Navegue até **<Application-Name> > Manifest**. Edite o Manifesto. O arquivo está no formato JSON e um usuário padrão está disponível para cópia. Por exemplo - aqui 2 funções são criadas: Usuário e analista.

Cisco-Firepower | Manifest



 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 }
```

Etapa 4. Navegue até **<Application-Name> > Users and Groups (Usuários e grupos)**. Edite o usuário e atribua as funções recém-criadas, como mostrado nesta imagem.

Edit Assignment

Default Directory

Users
1 user selected.

Select a role
None Selected

Assign

Select a role

Only a single role can be selected

Enter role name to filter items...

Analyst

User

Selected Role
Analyst

Select

Etapa 4. Faça login no FMC e edite a Configuração avançada no SSO. Para, Atributo do membro do grupo: atribua o **nome de exibição** que você forneceu no Manifesto do aplicativo às funções.

▼ Advanced Configuration (Role Mapping)

Default User Role

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

Depois que isso for feito, você poderá fazer login na função designada.

Verificar

Etapa 1. Navegue até a URL do FMC no seu navegador: <https://<URL do FMC>>. Clique em **Logon único**, como mostrado nesta imagem.



Firepower Management Center

Username

Password

Single Sign-On

Log In

Você é redirecionado para a página de login da Microsoft e o login bem-sucedido retornará a página padrão do FMC.

Etapa 2. No FMC, navegue até **System > Users** para ver o usuário SSO adicionado ao banco de dados.

test1@shbharticisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbharticisco.onmicrosoft.com

Administrator

External (SSO)

Troubleshoot

Verifique a autenticação SAML e este é o fluxo de trabalho que você obtém para uma autorização bem-sucedida (esta imagem é de um ambiente de laboratório):

Logs SAML do navegador

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	

Logs SAML do FMC

Verifique os registros SAML no FMC em `/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/ws/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
```