

Configurer FMC SSO avec Azure comme fournisseur d'identité

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration IdP](#)

[Configuration SP](#)

[SAML sur FMC](#)

[Limitations et cavernes](#)

[Configuration](#)

[Configuration sur le fournisseur d'identités](#)

[Configuration de Firepower Management Center](#)

[Configuration avancée - RBAC avec Azure](#)

[Vérification](#)

[Dépannage](#)

[Journaux SAML du navigateur](#)

[Journaux SAML FMC](#)

Introduction

Ce document décrit comment configurer l'authentification unique (SSO) de Firepower Management Center (FMC) avec Azure en tant que fournisseur d'identité (IdP).

Le langage de balisage d'assertion de sécurité (SAML) est le protocole sous-jacent le plus souvent utilisé pour rendre SSO possible. Une société gère une page de connexion unique, derrière elle se trouve un magasin d'identité et diverses règles d'authentification. Il peut facilement configurer n'importe quelle application web qui prend en charge SAML, ce qui vous permet de vous connecter à toutes les applications web. Elle présente également l'avantage sécuritaire de ne pas forcer les utilisateurs à conserver (et potentiellement à réutiliser) des mots de passe pour chaque application Web à laquelle ils ont besoin d'accéder, ni à exposer des mots de passe à ces applications Web.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base de Firepower Management Center
- Compréhension de base de l'authentification unique

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Cisco Firepower Management Center (FMC) version 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Terminologies SAML

La configuration de SAML doit être effectuée à deux endroits : à l'IDP et au SP. L'IDP doit être configuré de sorte qu'il sache où et comment envoyer les utilisateurs lorsqu'ils veulent se connecter à un SP spécifique. Le SP doit être configuré de sorte qu'il sache qu'il peut faire confiance aux assertions SAML signées par l'IdP.

Définition de quelques termes qui sont au coeur de SAML :

- Fournisseur d'identité (IdP) : outil ou service logiciel (souvent visualisé par une page de connexion et/ou un tableau de bord) qui effectue l'authentification ; vérifie le nom d'utilisateur et les mots de passe, vérifie l'état du compte, appelle deux facteurs, etc.
- Fournisseur de services (SP) : application Web dans laquelle l'utilisateur tente d'accéder à.
- Assertion SAML : message indiquant l'identité d'un utilisateur et souvent d'autres attributs, envoyé via HTTP via des redirections de navigateur

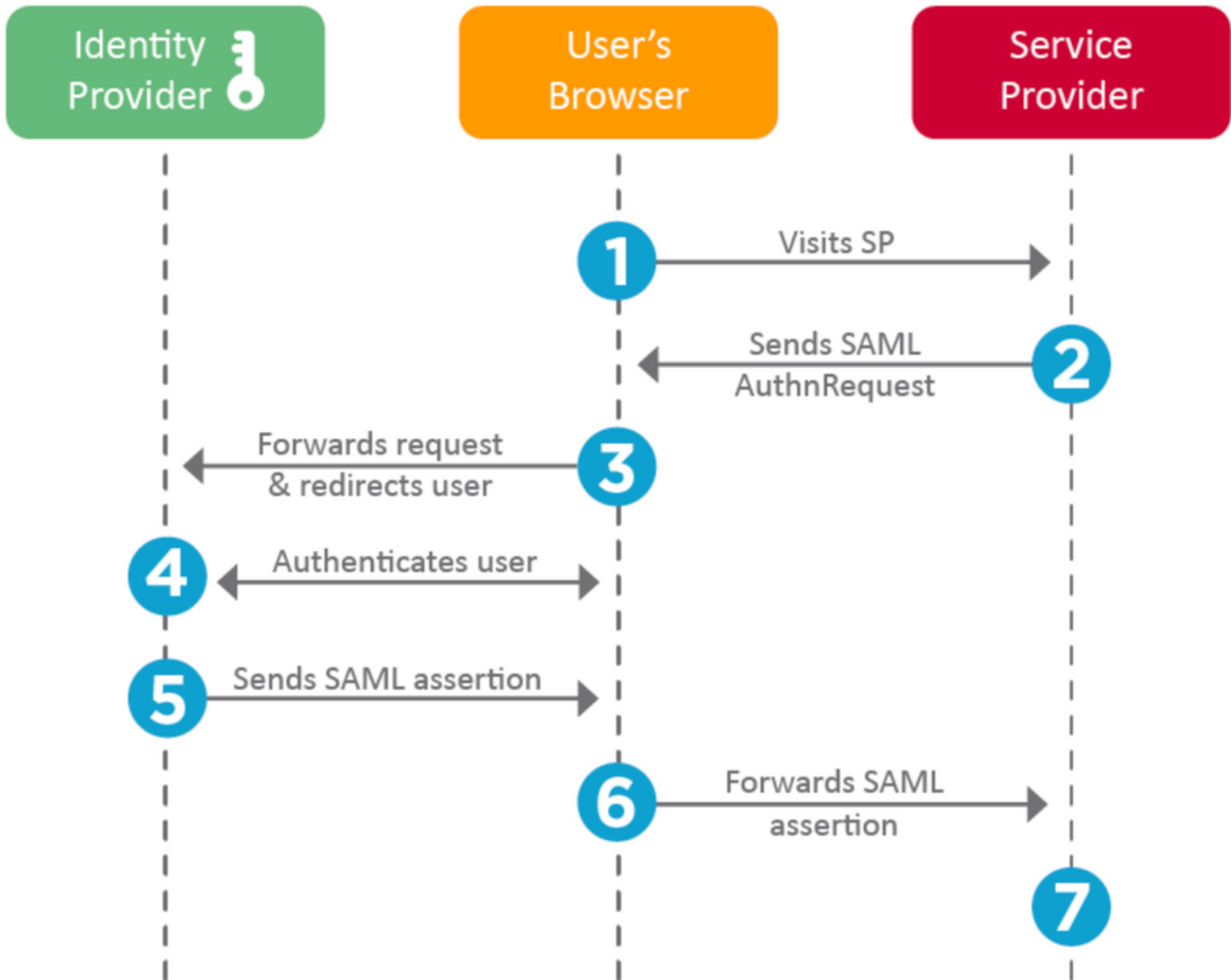
Configuration IdP

Les spécifications d'une assertion SAML, ce qu'elle doit contenir et comment elle doit être formatée sont fournies par le SP et définies à l'IDP.

- EntityID : nom unique global pour le SP. Les formats varient, mais il est de plus en plus courant de voir cette valeur formatée comme une URL.
Exemple : <https://<nom de domaine complet ou adresse IP>/saml/métadonnées>
- Validateur ACS (Assertion Consumer Service) : mesure de sécurité sous forme d'expression régulière (regex) qui garantit que l'assertion SAML est envoyée à l'ACS correct. Cela n'intervient que lors des connexions initiées par le fournisseur de services, lorsque la demande SAML contient un emplacement ACS. Par conséquent, ce validateur ACS s'assure que l'emplacement ACS fourni par la demande SAML est légitime.
Exemple : <https://<FQDN-or-IPaddress>/saml/acs>
- Attributs : le nombre et le format des attributs peuvent varier considérablement. Il existe généralement au moins un attribut, le nameID, qui est généralement le nom d'utilisateur de

l'utilisateur qui tente de se connecter.

- Algorithme de signature SAML - SHA-1 ou SHA-256. Moins souvent SHA-384 ou SHA-512. Cet algorithme est utilisé conjointement avec le certificat X.509 est mentionné ici.



Configuration SP

Au verso de la section ci-dessus, cette section traite des informations fournies par l'IdP et définies sur le SP.

- URL de l'émetteur - Identificateur unique de l'IDP. Formaté en tant qu'URL contenant des informations sur l'IdP afin que le SP puisse valider que les assertions SAML qu'il reçoit sont émises à partir du IdP correct.
Exemple : <saml : Émetteur <https://sts.windows.net/0djgedfasklf-sfadsj123fsdv-c80d8aa/> >
- URL de connexion du point de terminaison SSO SAML / du fournisseur de services : point de terminaison IdP qui lance l'authentification lorsqu'il est redirigé ici par le fournisseur de services avec une requête SAML.
Exemple : <https://login.microsoftonline.com/023480840129412-824812/saml2>
- Point de terminaison SAML SLO (Single Log-out) : point de terminaison IdP qui ferme votre session IdP lorsqu'elle est redirigée ici par le SP, généralement après la **déconnexion**.
Exemple : <https://access.wristbandtent.com/logout>

SAML sur FMC

La fonctionnalité SSO de FMC est introduite à partir de la version 6.7. La nouvelle fonctionnalité simplifie l'autorisation FMC (RBAC), car elle mappe les informations existantes aux rôles FMC. Il s'applique à tous les utilisateurs de l'interface utilisateur FMC et aux rôles FMC. Pour l'instant, il prend en charge la spécification SAML 2.0 et ces personnes déplacées prises en charge

- OKTA
- OneLogin
- PingID
- Azure AD
- Autres (tout PCI conforme à SAML 2.0)

Limitations et cavernes

- SSO peut être configuré uniquement pour le domaine global.
- Les FMC de la paire HA ont besoin d'une configuration individuelle.
- Seuls les administrateurs locaux/AD peuvent configurer l'authentification unique.
- SSO initié à partir d'ldp n'est pas pris en charge.

Configuration

Configuration sur le fournisseur d'identités

Étape 1. Connectez-vous à Microsoft Azure. Accédez à **Azure Active Directory > Enterprise Application**.



Default Directory | Overview

Azure Active Directory



Switch tenant



Delete tenant



Create



Overview



Getting started



Preview hub



Diagnose and solve problems

Manage



Users



Groups



External Identities



Roles and administrators



Administrative units (Preview)



Enterprise applications



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

- Étape 2. Créez **une nouvelle application** sous Application non-Gallery, comme illustré dans cette image.

[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](#)

Étape 3. Modifiez l'application créée et accédez à **Configurer une seule connexion sur > SAML**, comme illustré dans cette image.

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

Firepower | Single sign-on

Enterprise Application

« 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.

Overview
Deployment Plan
Diagnose and solve problems

Manage

- Properties
- Owners
- Users and groups
- Single sign-on**
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access

Étape 4. Modifiez la configuration SAML de base et fournissez les détails FMC :

- URL FMC : <https://<FMC-FQDN-or-IPaddress>>
- Identificateur (ID d'entité) : <https://<FMC-FQDN-or-IPaddress>/saml/métadonnées>
- URL de réponse : <https://<FMC-FQDN-or-IPaddress>/saml/acs>
- URL de connexion : [/https://<FMC-FQDN-or-IPaddress>/saml/acs](https://<FMC-FQDN-or-IPaddress>/saml/acs)
- RelayState : `/ui/login`

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

- [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 \(Preview\)](#)

1

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	<i>Optional</i>

2

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

3

SAML Signing Certificate ✎ Edit

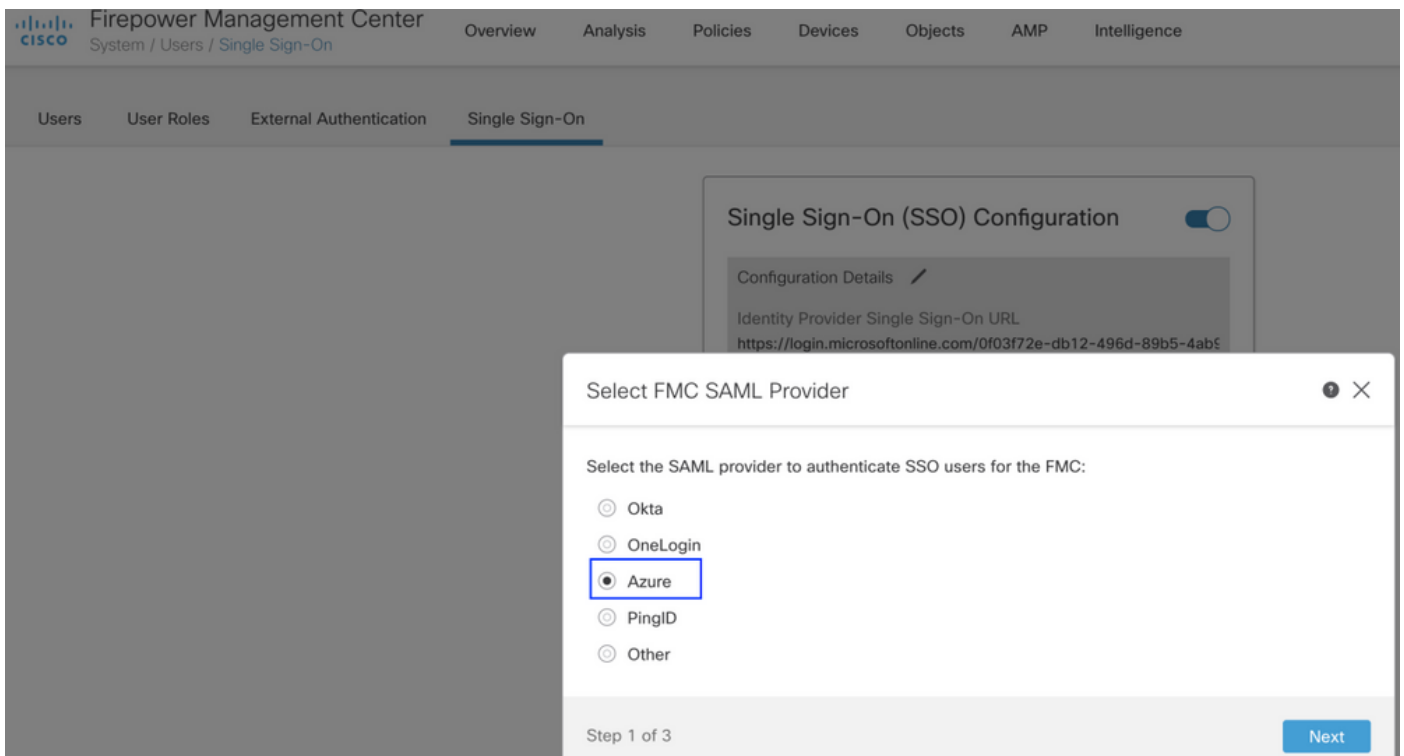
Status	Active
Thumbprint	[REDACTED]
Expiration	
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/0f03f72e-db12-... 📄
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Conservez le reste comme valeur par défaut. Cette section est traitée plus en détail pour l'accès basé sur les rôles.

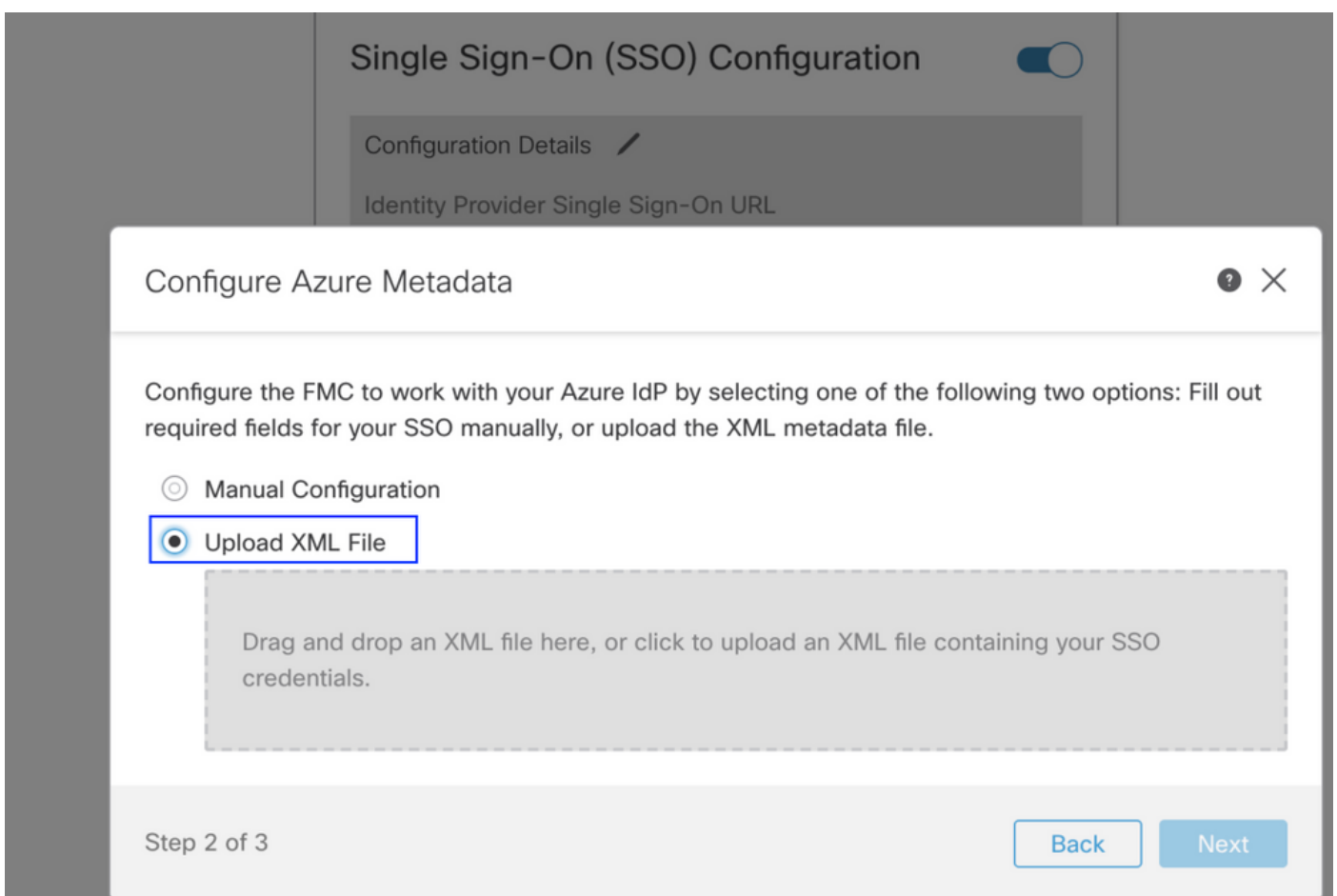
Ceci marque la fin de la configuration du fournisseur d'identité. Téléchargez le XML des métadonnées de fédération qui sera utilisé pour la configuration FMC.

Configuration de Firepower Management Center

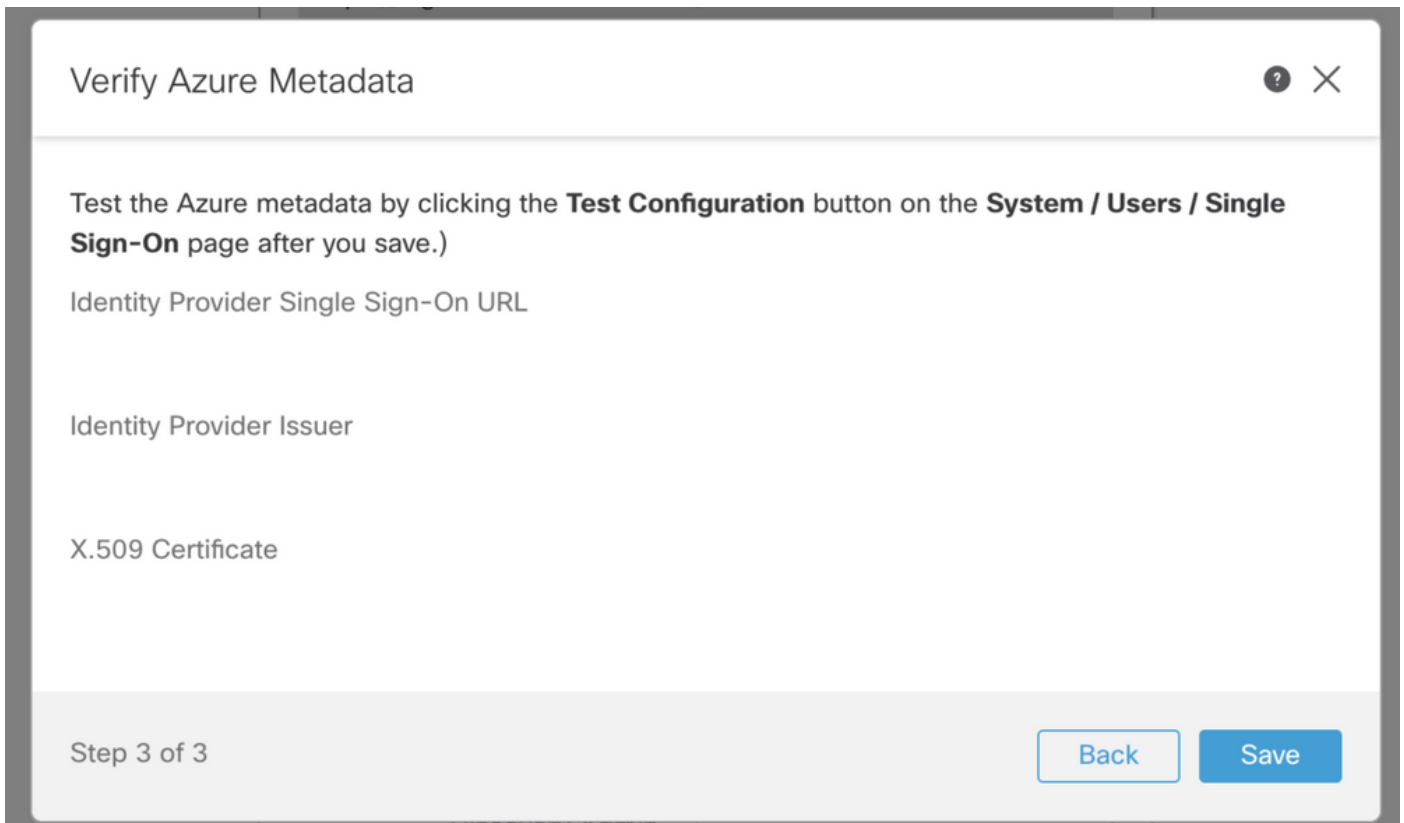
Étape 1. Connectez-vous à FMC, accédez à **Paramètres > Utilisateurs > Authentification unique** et activez SSO. Sélectionnez **Azure** comme fournisseur.



Étape 2. Téléchargez le fichier XML téléchargé depuis Azure ici. Il remplit automatiquement tous les détails nécessaires.



Étape 3. Vérifiez la configuration et cliquez sur **Enregistrer**, comme indiqué dans cette image.



Configuration avancée - RBAC avec Azure

Afin d'utiliser divers types de rôle pour mapper aux rôles de FMC - Vous devez modifier le manifeste de l'application sur Azure pour affecter des valeurs aux rôles. Par défaut, les rôles ont la valeur Null.

Étape 1. Accédez à l'**application** créée et cliquez sur **Connexion unique**.


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](#)

Étape 2. Modifiez les attributs utilisateur et les revendications. Ajouter une nouvelle revendication avec le nom : **rôles** et sélectionnez la valeur en tant que **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 ***

Étape 3. Accédez à **<Application-Name> > Manifest**. Modifiez le manifeste. Le fichier est au format JSON et un utilisateur par défaut est disponible pour la copie. Par exemple, deux rôles sont créés : Utilisateur et analyste.

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 }
```

Étape 4. Accédez à **<Application-Name> > Utilisateurs et groupes**. Modifiez l'utilisateur et affectez les nouveaux rôles, comme illustré dans cette image.

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

Étape 4. Connectez-vous à FMC et modifiez la configuration avancée dans SSO. Pour : Attribut de membre de groupe : attribuez le **nom d'affichage** que vous avez fourni dans le manifeste d'application aux rôles.

▼ Advanced Configuration (Role Mapping)

Default User Role	<input type="text" value="Administrator"/>
Group Member Attribute	<input type="text" value="roles"/>
<hr/>	
Access Admin	<input type="text"/>
Administrator	<input type="text"/>
Discovery Admin	<input type="text"/>
External Database User	<input type="text"/>
Intrusion Admin	<input type="text"/>
Maintenance User	<input type="text"/>
Network Admin	<input type="text" value="User"/>
Security Analyst	<input type="text"/>
Security Analyst (Read Only)	<input type="text" value="Analyst"/>
Security Approver	<input type="text"/>
Threat Intelligence Director (TID) User	<input type="text"/>

Une fois cela fait, vous devriez pouvoir vous connecter à leur rôle désigné.

Vérification

Étape 1. Accédez à l'URL FMC à partir de votre navigateur : <https://<URL FMC>>. Cliquez sur **Connexion unique**, comme illustré dans cette image.



Firepower Management Center

Username

Password

Single Sign-On

Log In

Vous êtes redirigé vers la page de connexion Microsoft et une connexion réussie retournerait la page par défaut de FMC.

Étape 2. Sur FMC, accédez à **System > Users** pour voir l'utilisateur SSO ajouté à la base de données.

test1@shbhartiscisco.onmicrosoft.com

Security Analyst

External (SSO)

test2guy@shbhartiscisco.onmicrosoft.com

Administrator

External (SSO)

Dépannage

Vérifiez l'authentification SAML et voici le flux de travail que vous effectuez pour obtenir une autorisation réussie (cette image provient d'un environnement de travaux pratiques) :

Journaux SAML du navigateur

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	

Journaux SAML FMC

Vérifiez les connexions SAML sur FMC à l'adresse `/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
```