Configurer FMC SSO avec Azure comme fournisseur d'identité

Contenu

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.

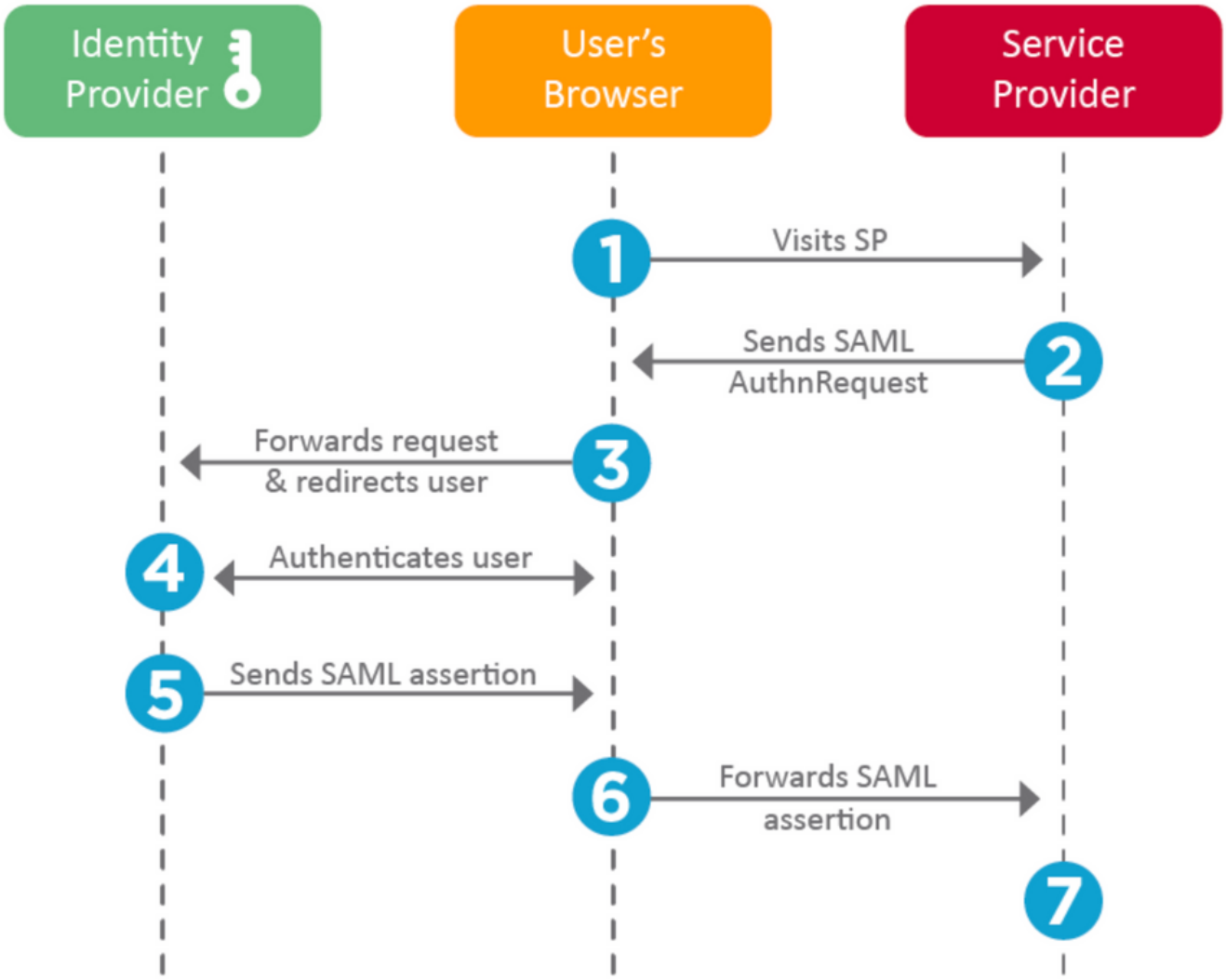
- EntityID : nom unique global pour le SP. Les formats varient, mais il est de plus en plus courant de voir cette valeur formatée comme une URL.
  Exemple : <https://<nom de domaine complet ou adresse IP>/saml/métadonnées>

- 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)

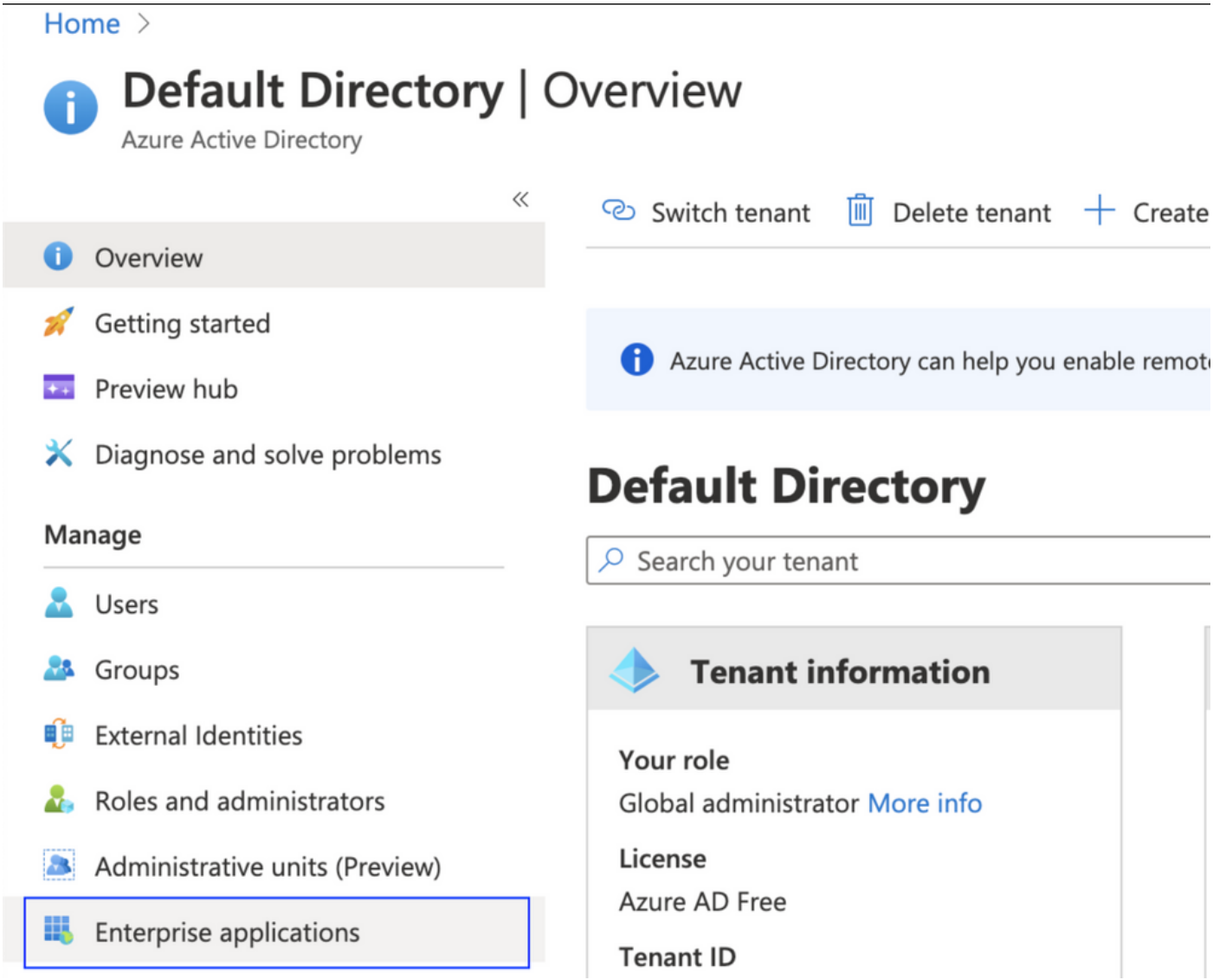
Limitations et cavernes

- 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'Idp n'est pas pris en charge.

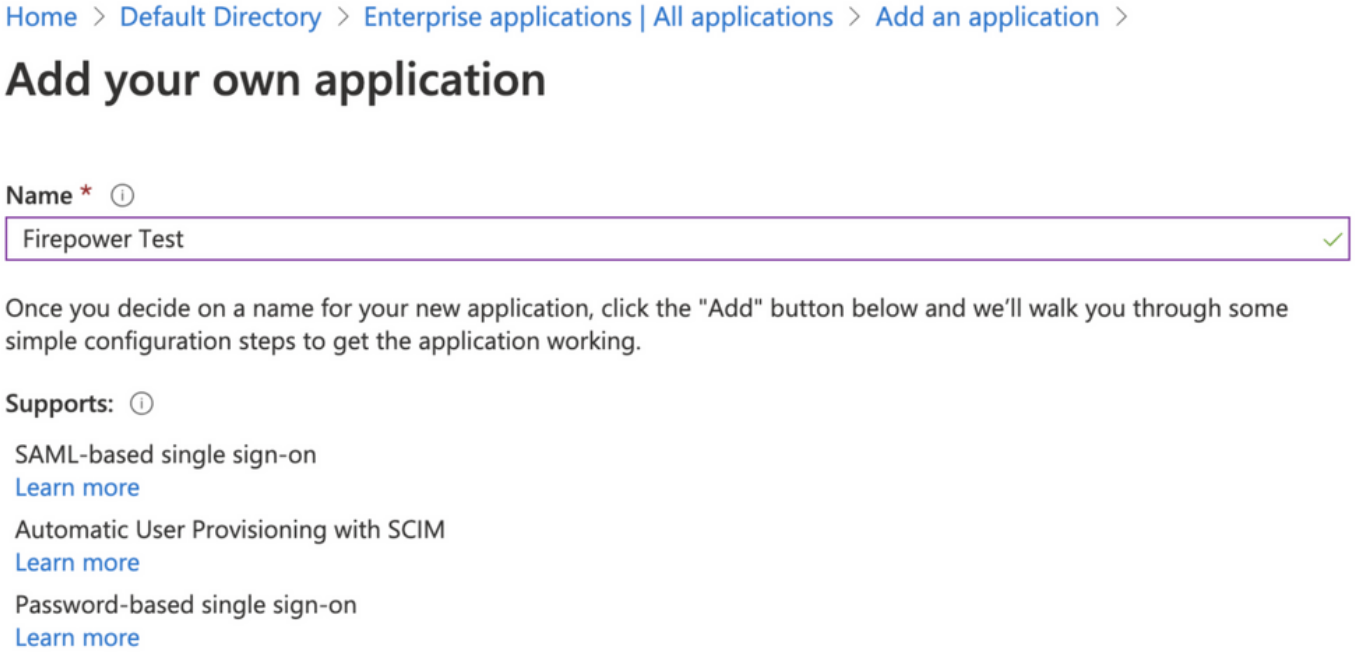
Configuration

Configuration sur le fournisseur d'identités

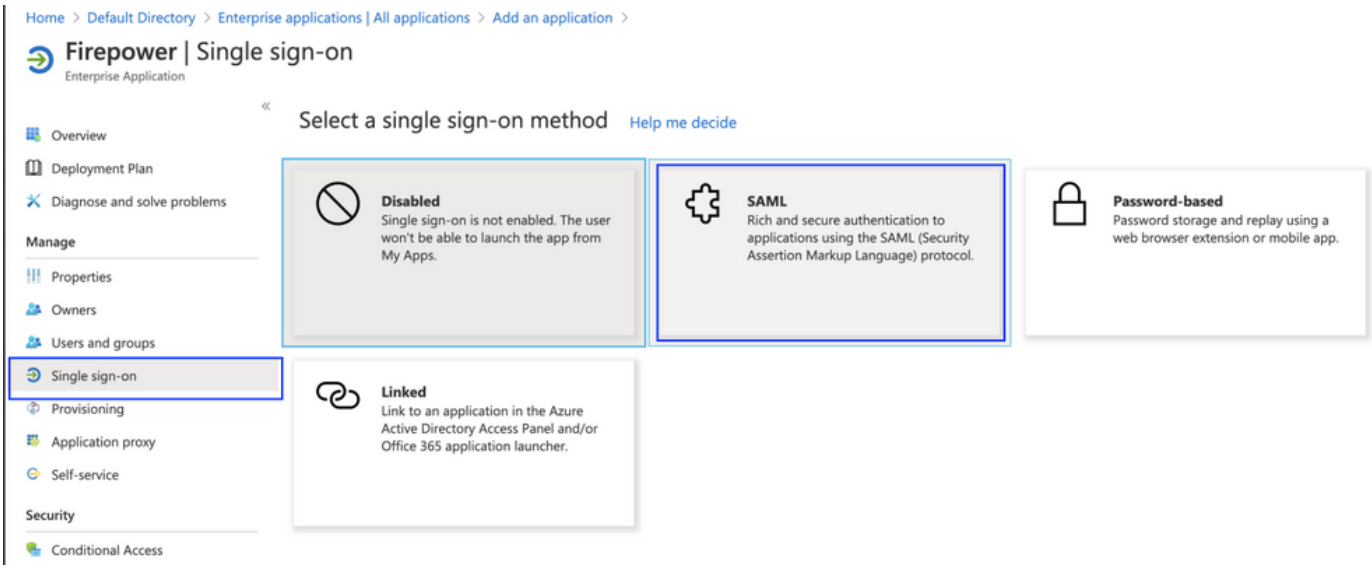
Étape 1. Connectez-vous à Microsoft Azure. Accédez à **Azure Active Directory > Enterprise Application**.



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

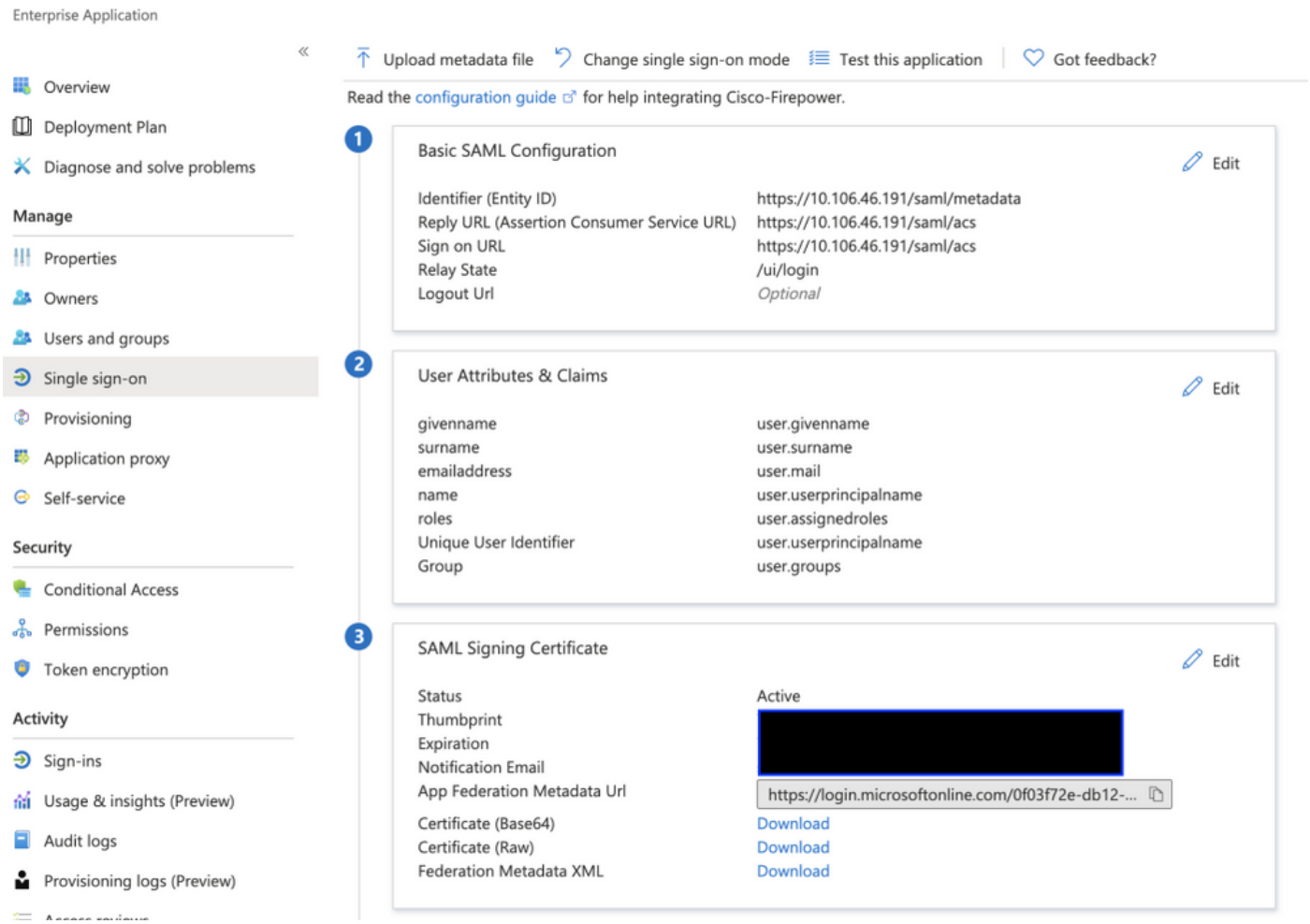


Étape 3. Modifiez l'application créée et accédez à **Configurer une seule connexion sur > SAML**, comme illustré dans cette image.



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-QDN-or-IPaddress>/saml/acs**
- RelayState :**/ui/login**

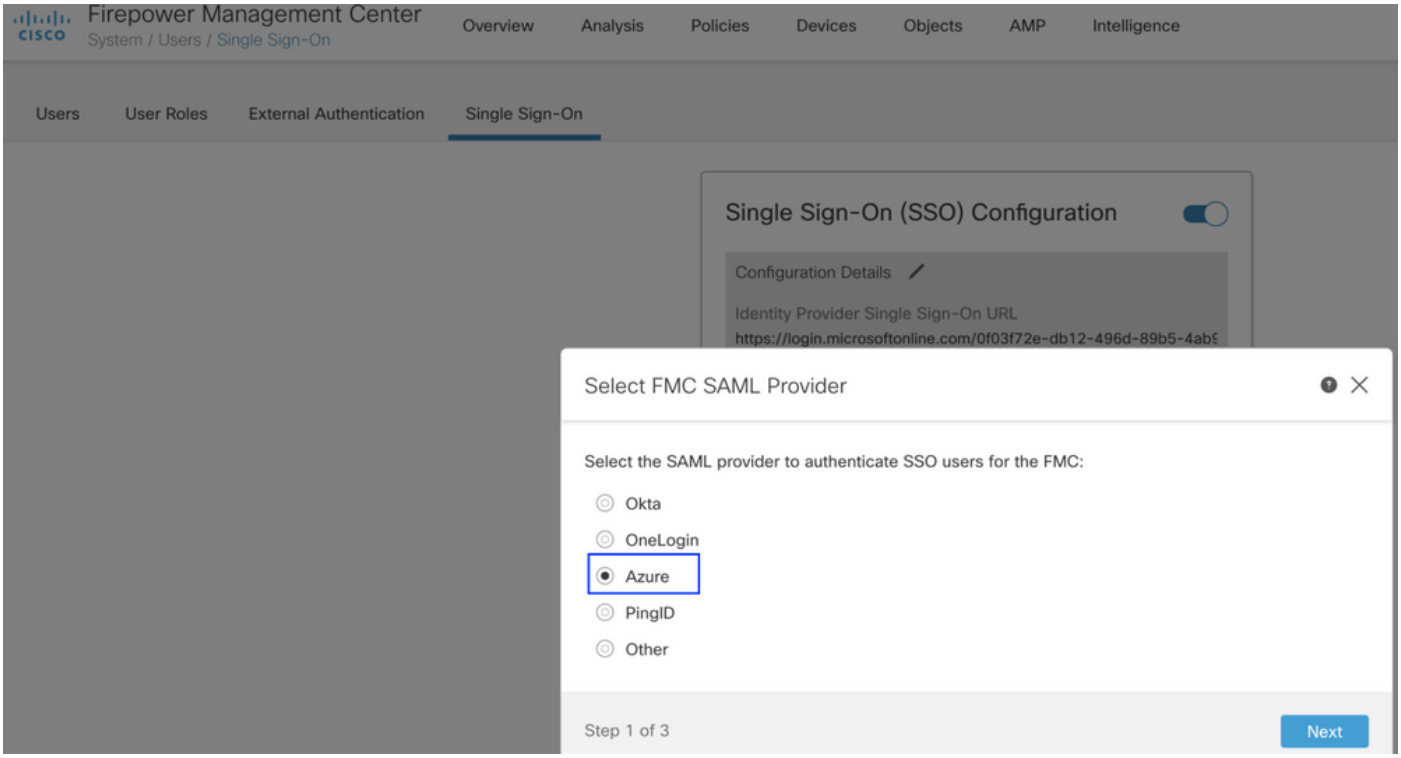


Conservez le reste comme valeur par défaut. Cette section est traitée plus en détail pour l'accès basé sur les rôles.

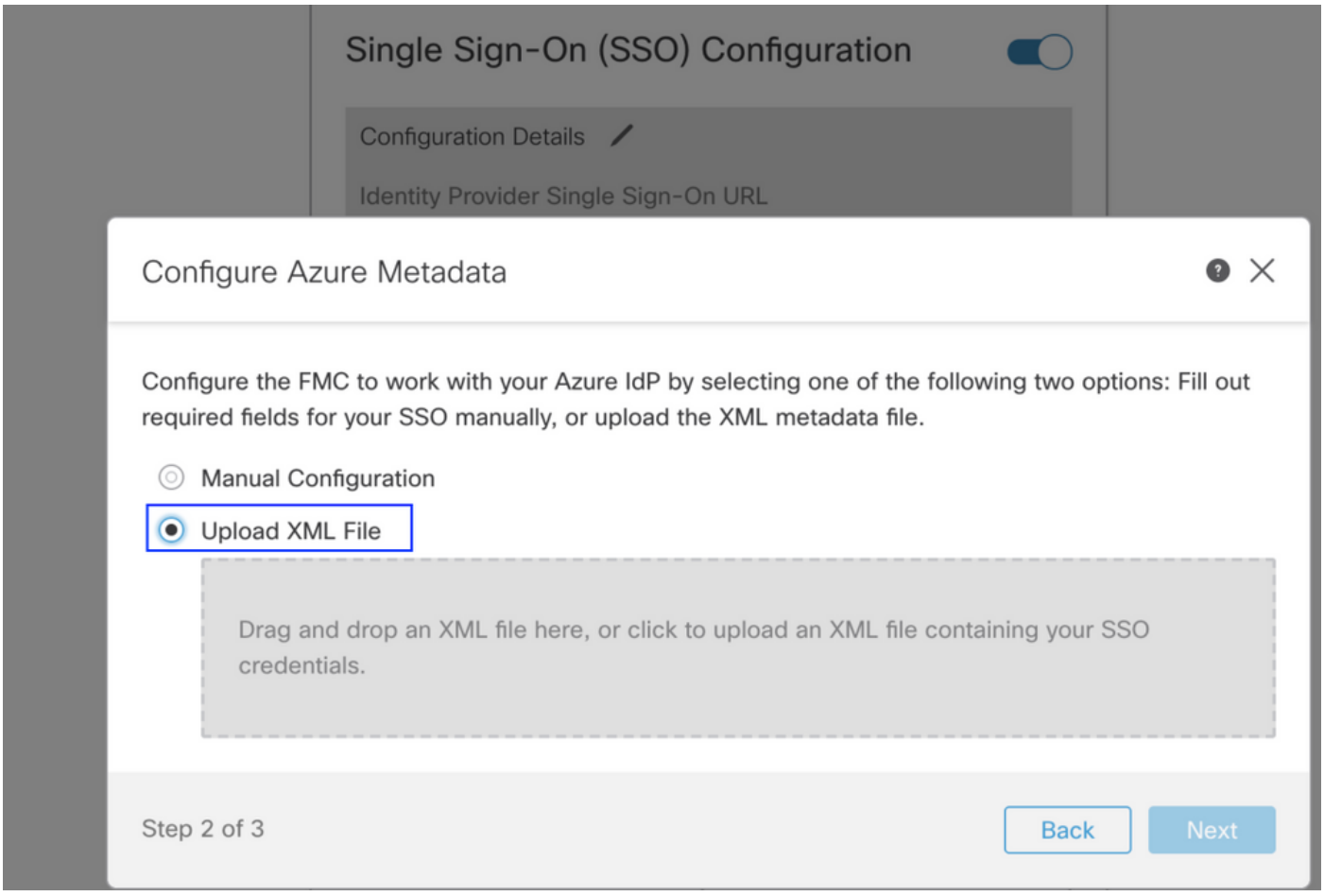
Ceci marque la fin de la configuration du fournisseur d'identité. Téléchargez le XML des métadonnées de fédération qui sera utilisé pour la configuration FMC.

Configuration de Firepower Management Center

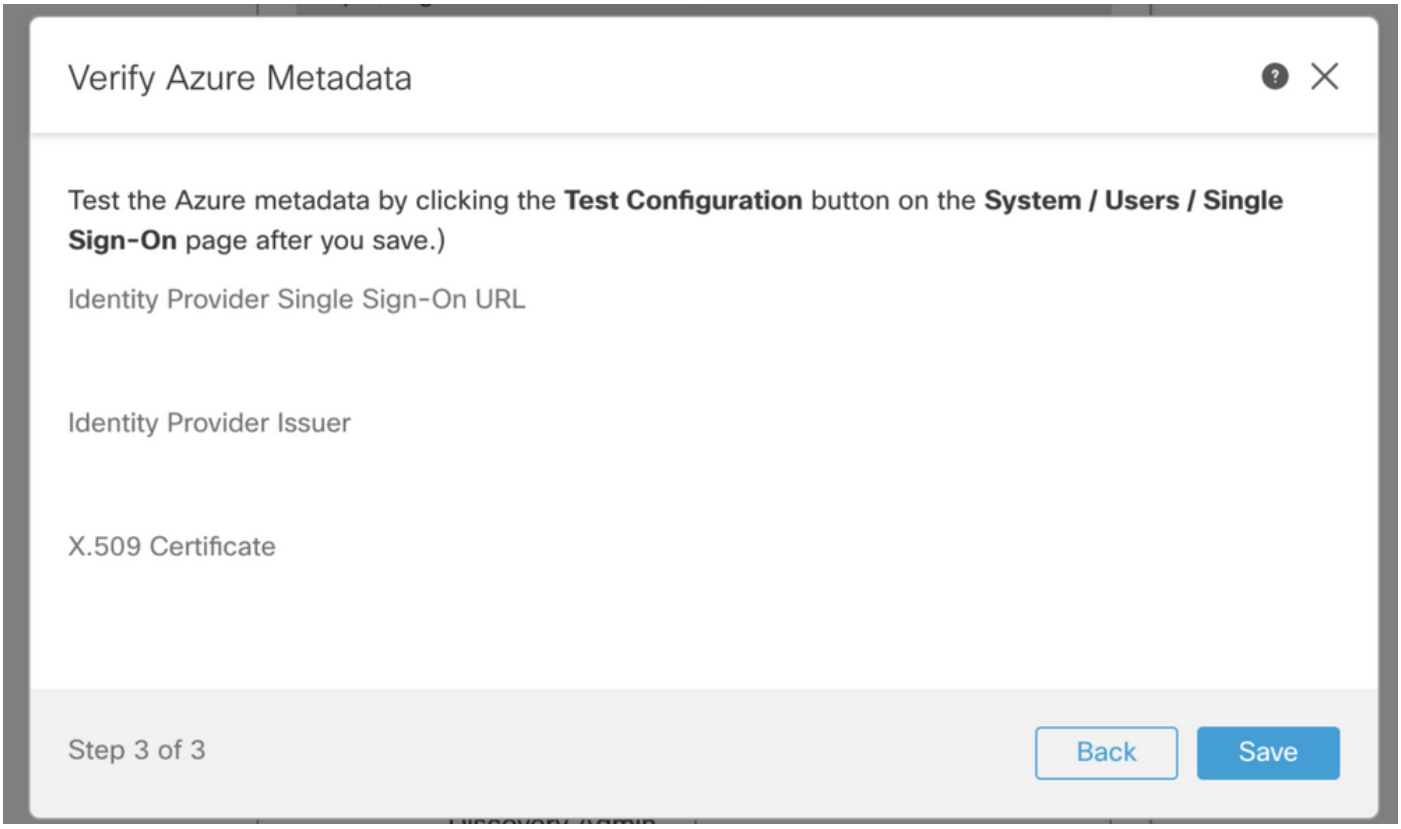
Étape 1. Connectez-vous à FMC, accédez à **Paramètres > Utilisateurs > Authentification unique** et activez SSO. Sélectionnez **Azure** comme fournisseur.



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



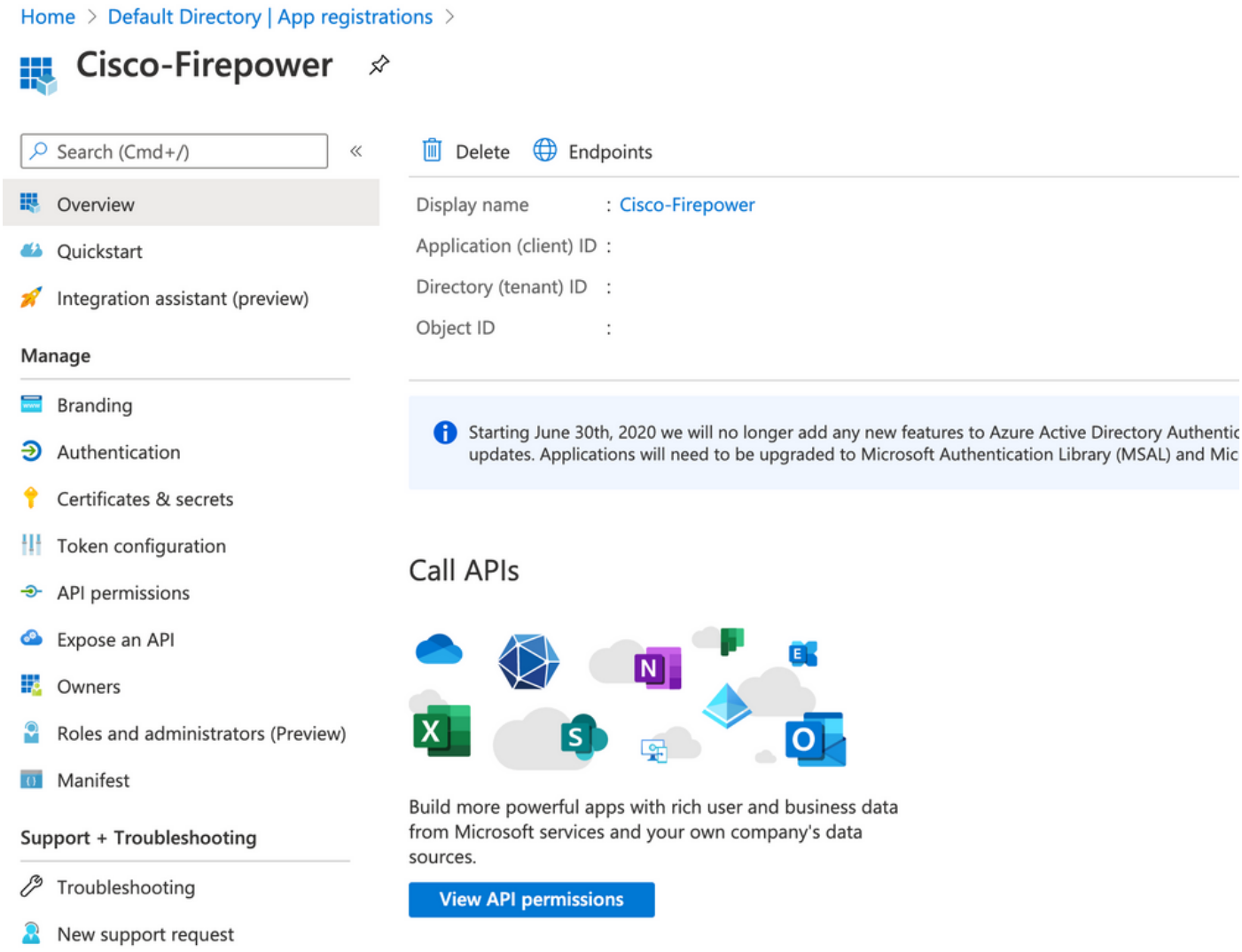
Étape 3. Vérifiez la configuration et cliquez sur **Enregistrer**, comme indiqué dans cette image.



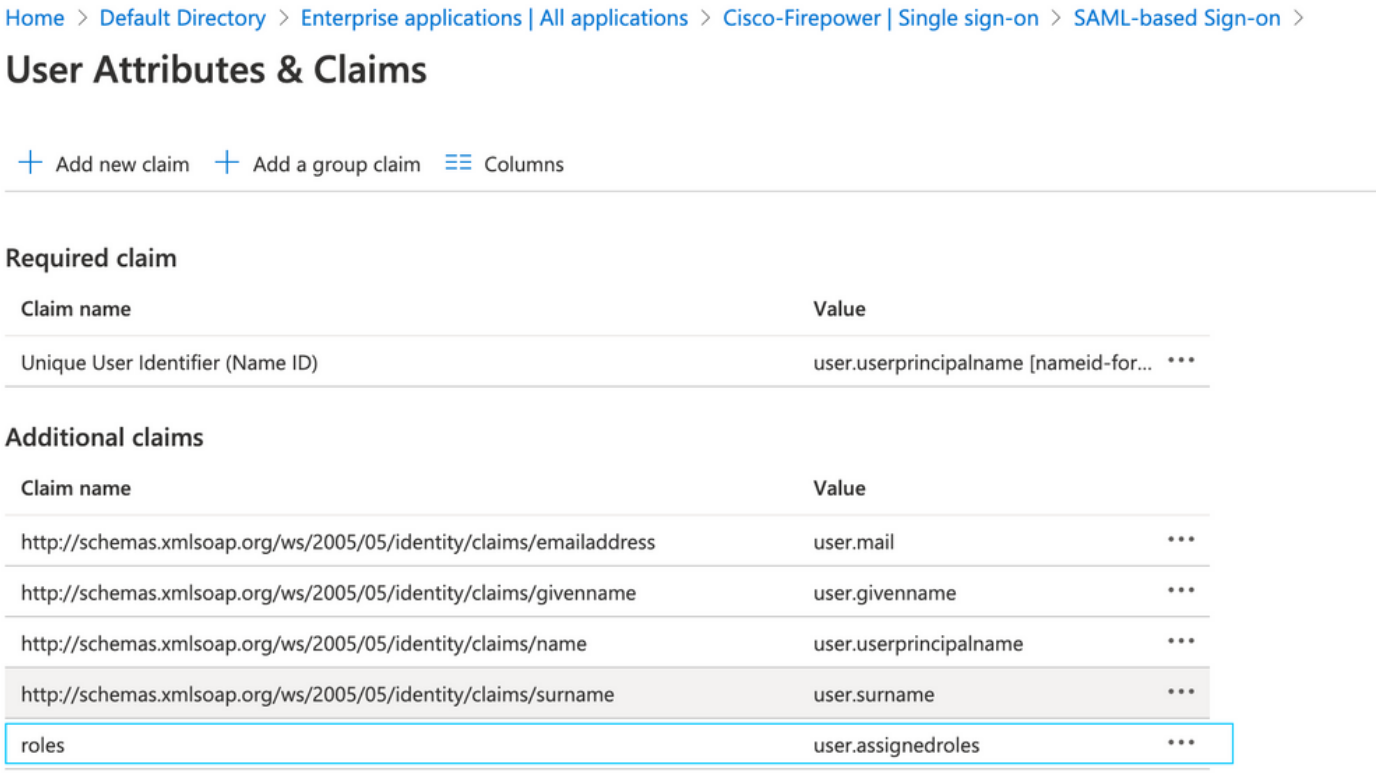
Configuration avancée - RBAC avec Azure

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.

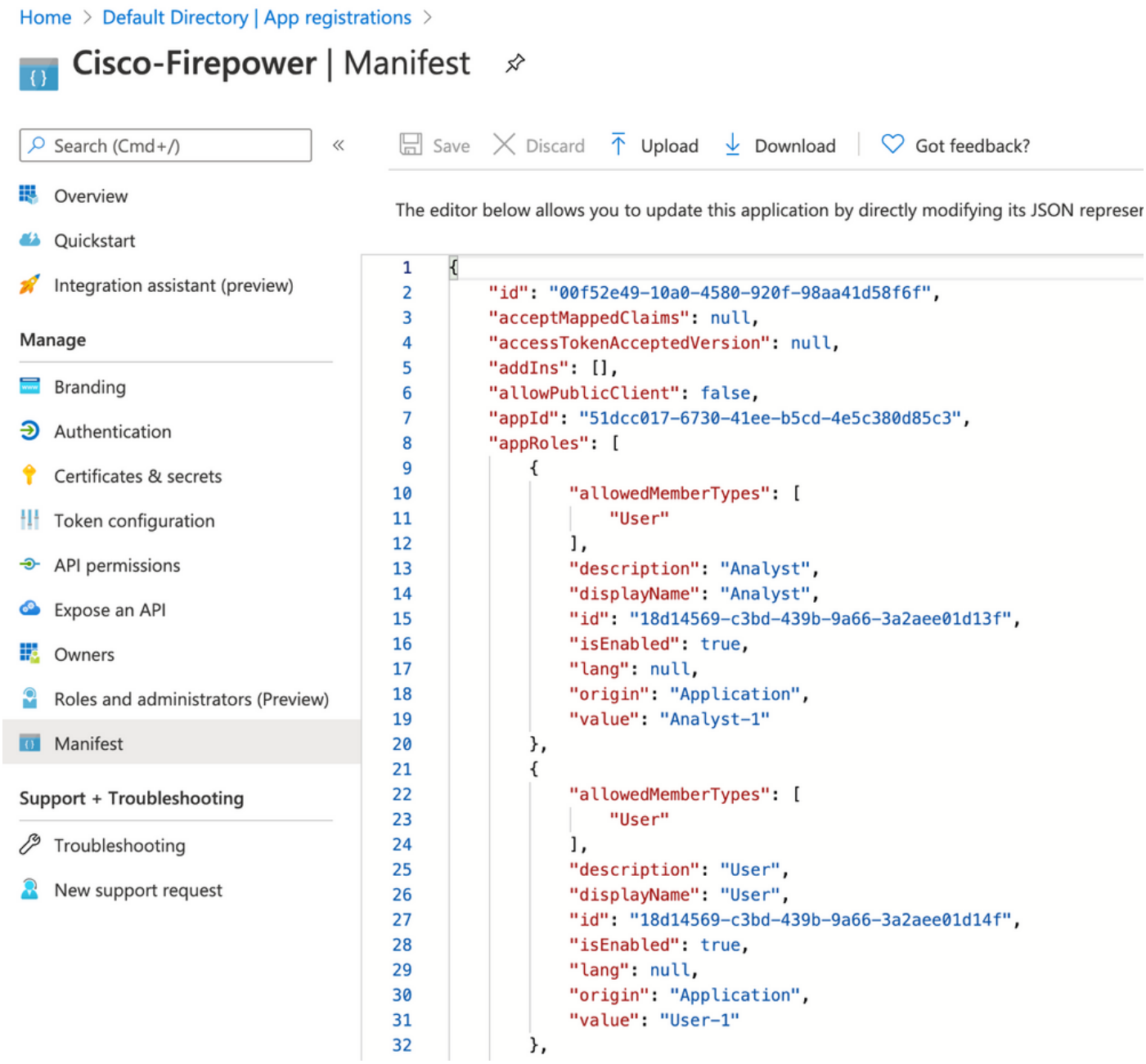
Étape 1. Accédez à l'**application** créée et cliquez sur **Connexion unique**.



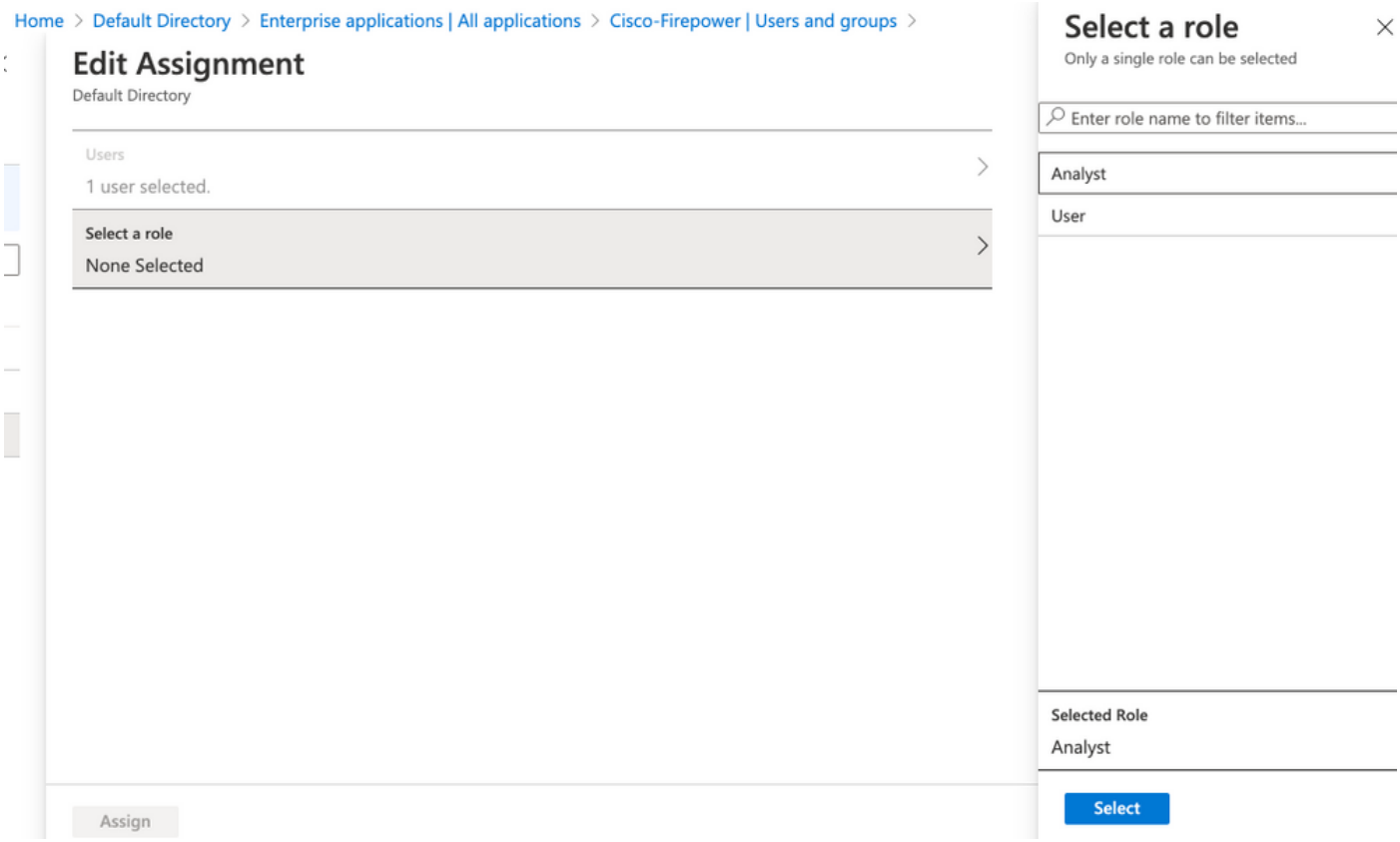
Étape 2. Modifiez les attributs utilisateur et les revendications. Ajouter une nouvelle revendication avec le nom : **rôles** et sélectionnez la valeur en tant que **user.assignedroles**.



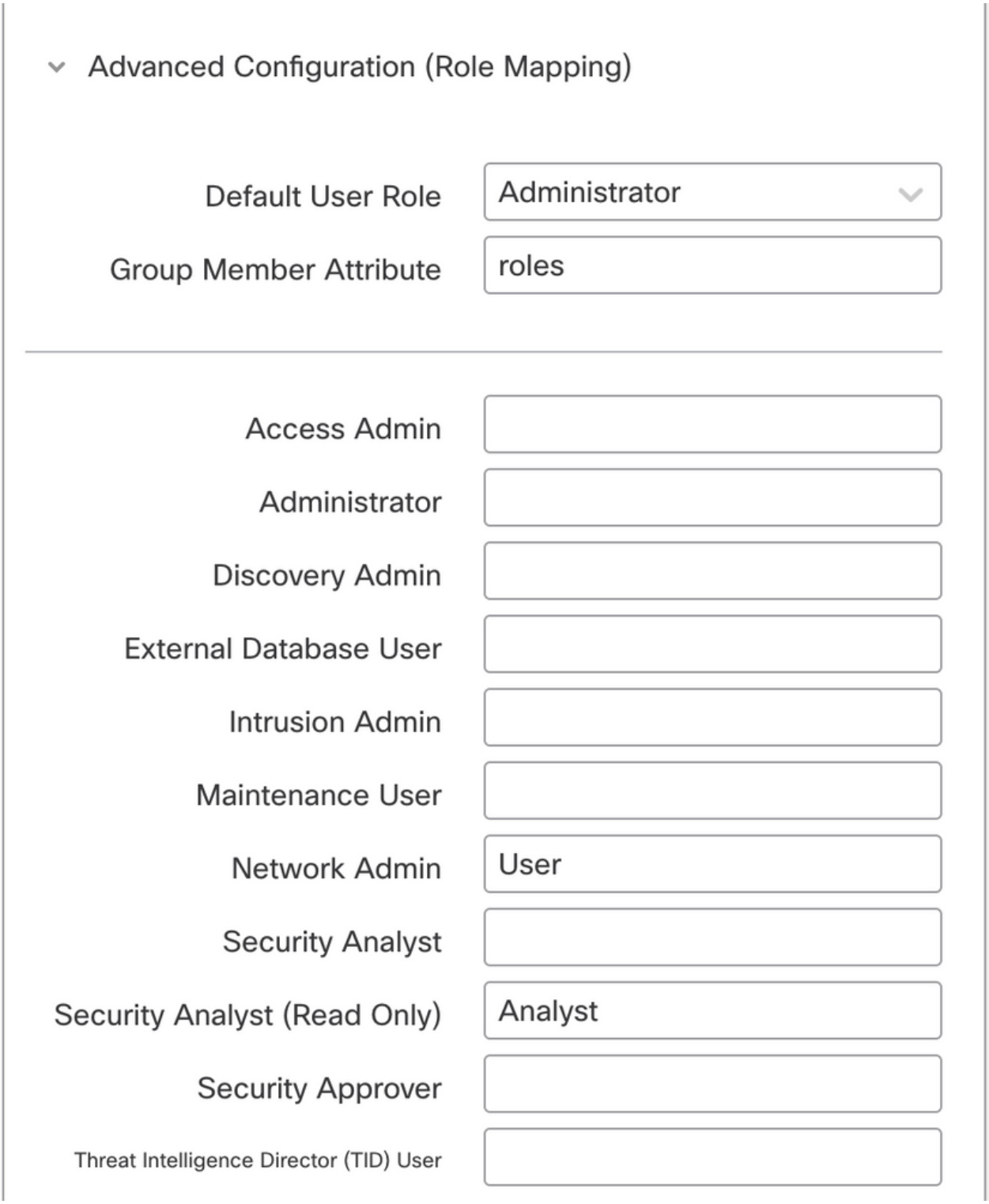
Étape 3. Accédez à **<Application-Name> > Manifest**. Modifiez le manifeste. Le fichier est au format JSON et un utilisateur par défaut est disponible pour la copie. Par exemple, deux rôles sont créés : Utilisateur et analyste.



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



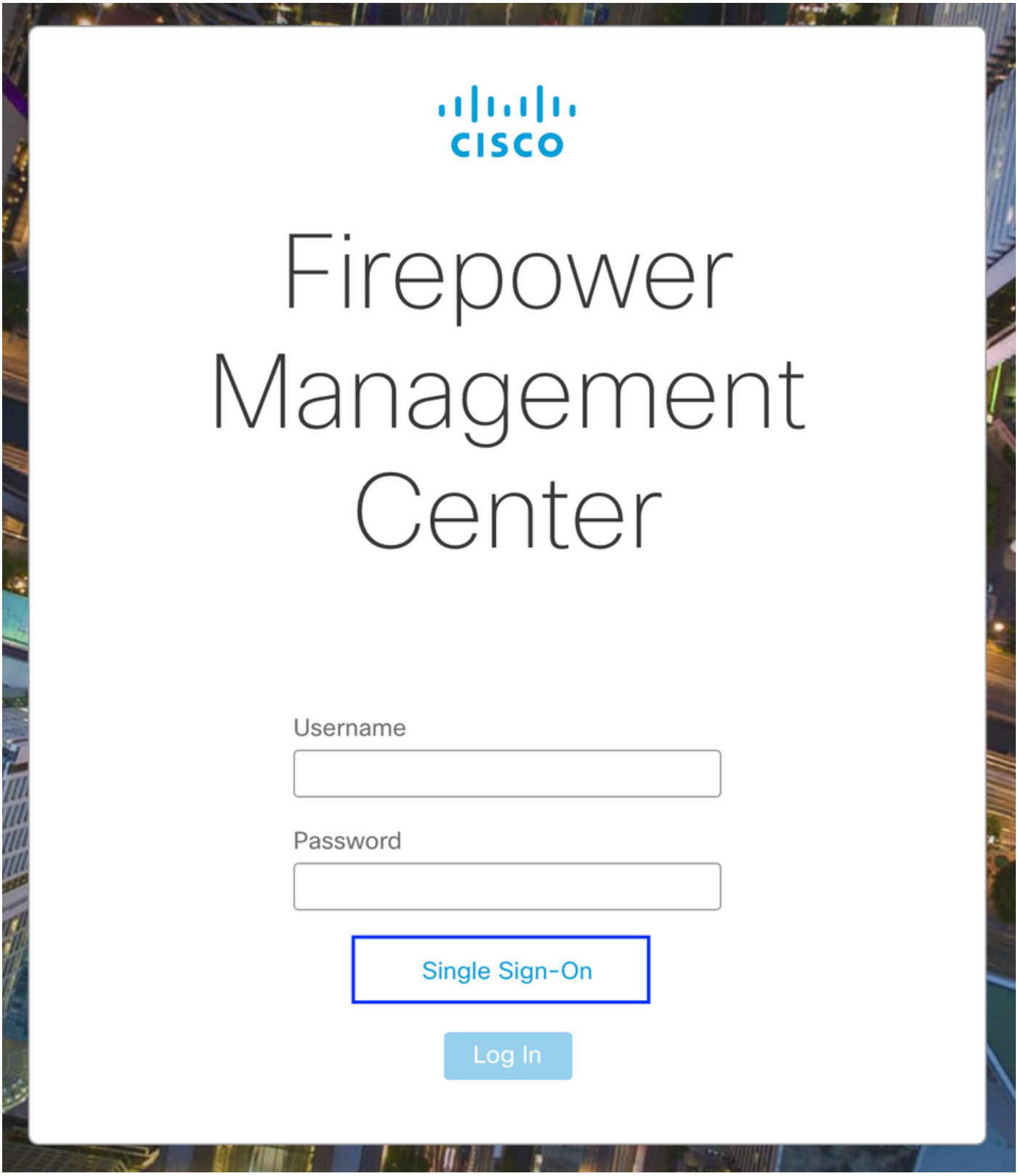
Étape 4. Connectez-vous à FMC et modifiez la configuration avancée dans SSO. Pour : Attribut de membre de groupe : aattribuez le **nom d'affichage** que vous avez fourni dans le manifeste d'application aux rôles.



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.



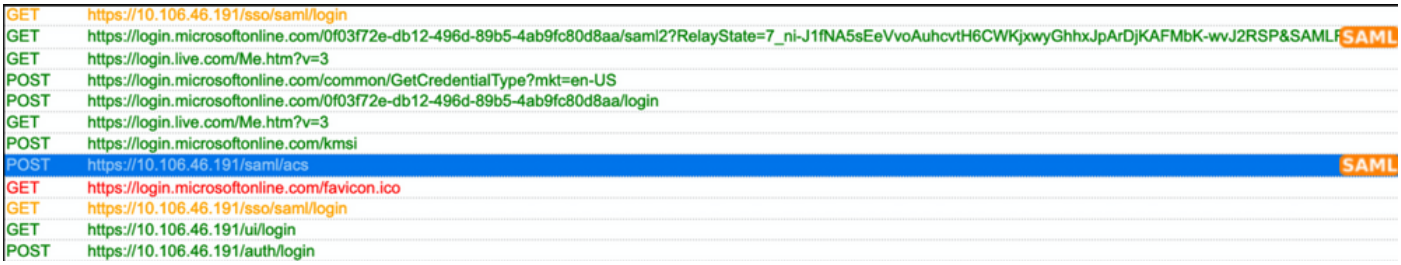
Vous êtes redirigé vers la page de connexion Microsoft et une connexion réussie retournerait la page par défaut de FMC.

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

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



Journaux SAML FMC

Vérifiez les connexions SAML sur FMC à l'adresse **/var/log/auth-daemon.log**