Configurer plusieurs groupes de tunnels avec SAML sur ASA

Table des matières

Introduction

Ce document décrit l'authentification SAML avec Azure Identity Provider pour plusieurs groupes de tunnels sur Cisco ASA.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Appliance de sécurité adaptable (ASA)
- SAML (Security Assertion Markup Language)
- Certificats SSL (Secure Socket Layer)
- Microsoft Azure

Composants utilisés

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

- ASA 9.22(1)1

- Microsoft Azure Entra ID avec SAML 2.0
- Cisco Secure Client 5.1.7.80

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

Microsoft Azure peut prendre en charge plusieurs applications pour le même ID d'entité. Chaque application (mappée à un groupe de tunnels différent) nécessite un certificat unique. Sur ASA, plusieurs groupes de tunnels peuvent être configurés pour utiliser différentes applications protégées par fournisseur d'identité de remplacement (IdP) en raison de la fonctionnalité de certificat IdP. Cette fonctionnalité permet aux administrateurs de remplacer le certificat du fournisseur d'identité principal dans l'objet de serveur SSO (Single Sign-On) par un certificat de fournisseur d'identité spécifique pour chaque groupe de tunnels. Cette fonctionnalité a été introduite sur ASA à partir de la version 9.17.1.

SSO SAML initié par SP

Lorsque l'utilisateur final initie la connexion en accédant à l'ASA, le comportement de connexion se déroule comme suit :

1. Lorsque l'utilisateur VPN accède à un groupe de tunnels activé par SAML ou en choisit un, l'utilisateur final est redirigé vers le fournisseur d'identité SAML pour authentification. L'utilisateur est invité à accéder directement à l'URL du groupe, auquel cas la redirection est silencieuse.

2. L'ASA génère une demande d'authentification SAML, que le navigateur redirige vers le fournisseur d'ID SAML.

3. Le fournisseur d'identité demande à l'utilisateur final de fournir des informations d'identification et l'utilisateur final se connecte. Les informations d'identification saisies doivent satisfaire à la configuration d'authentification IdP.

4. La réponse du fournisseur d'identité est renvoyée au navigateur et publiée sur l'URL de connexion ASA. L'ASA vérifie la réponse pour terminer la connexion.

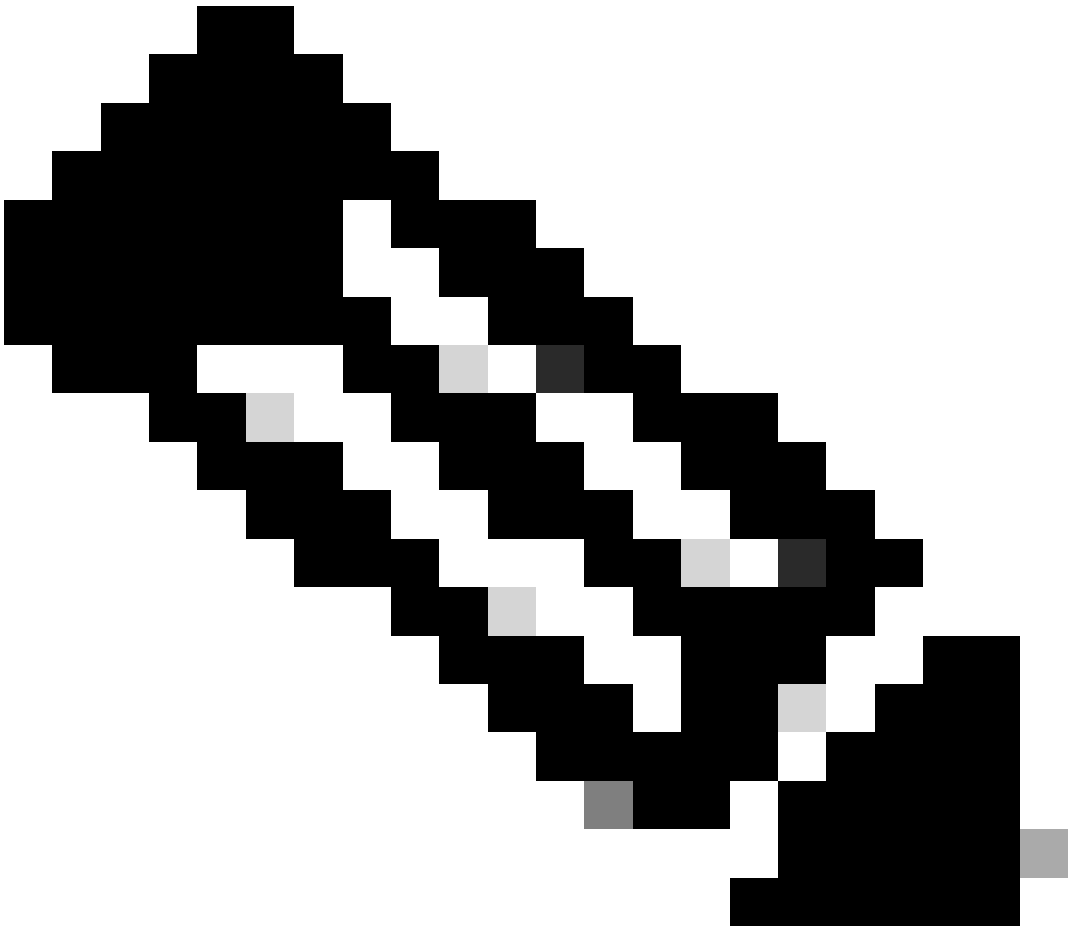
Configurations

Ajout de Cisco Secure Firewall - Secure Client à partir de la galerie

Dans cet exemple, l'intégration de Microsoft Entra SSO avec Cisco Secure Firewall - Secure Client sur Azure est ajoutée pour deux groupes de tunnels configurés sur ASA :

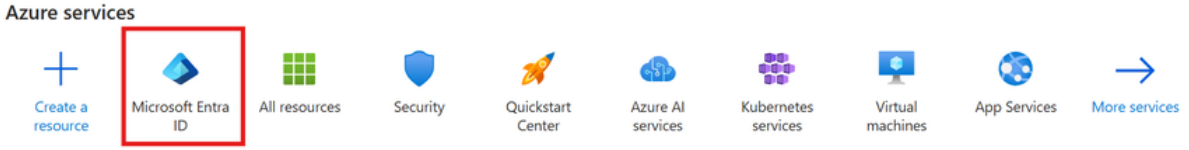
- SAML1
- SAML2

Afin de configurer l'intégration de Cisco Secure Firewall - Secure Client dans Microsoft Entra ID, vous devez ajouter Cisco Secure Firewall - Secure Client de la galerie à votre liste d'applications SaaS gérées.

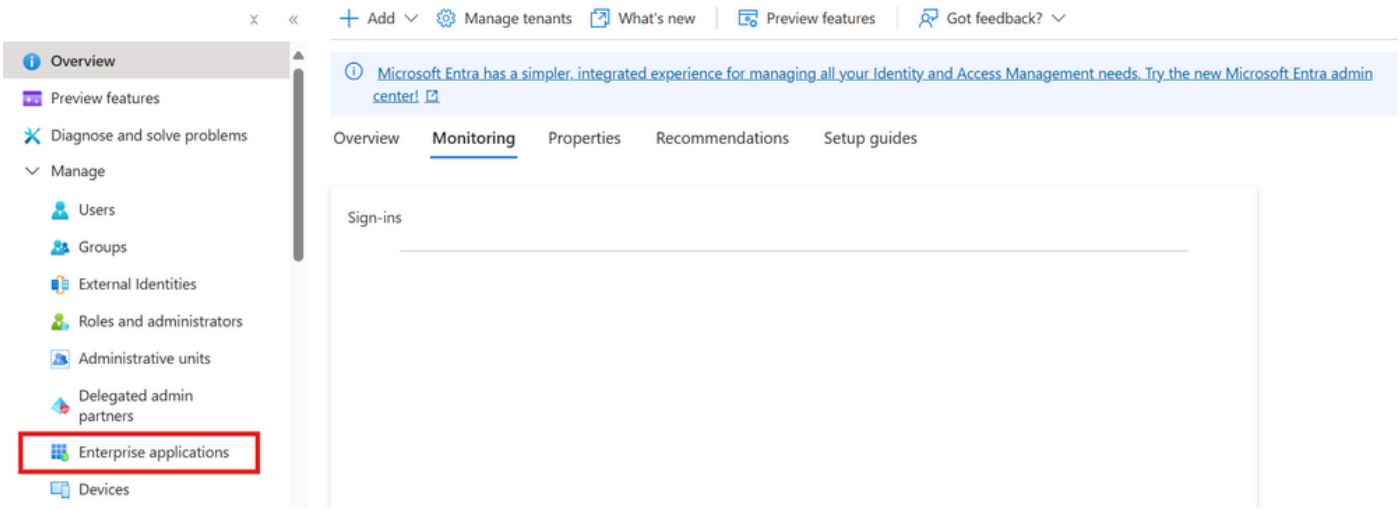


Remarque : Ces étapes permettent d'ajouter Cisco Secure Firewall - Secure Client à la galerie pour le premier groupe de tunnels, SAML1.

Étape 1. Connectez-vous au portail Azure et sélectionnez Microsoft Entra ID.

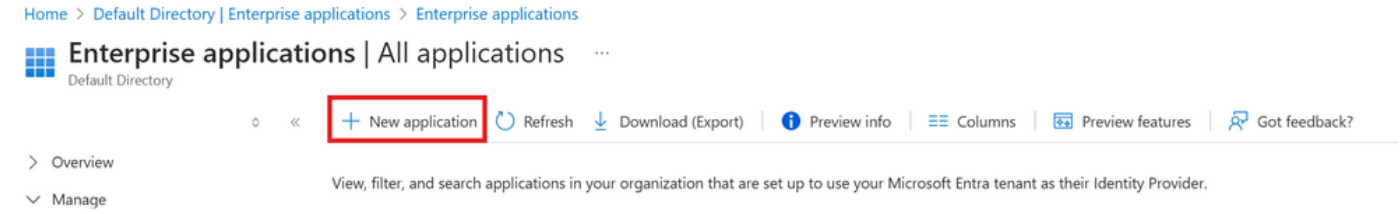


Étape 2. Comme le montre cette image, choisissez Applications d'entreprise.



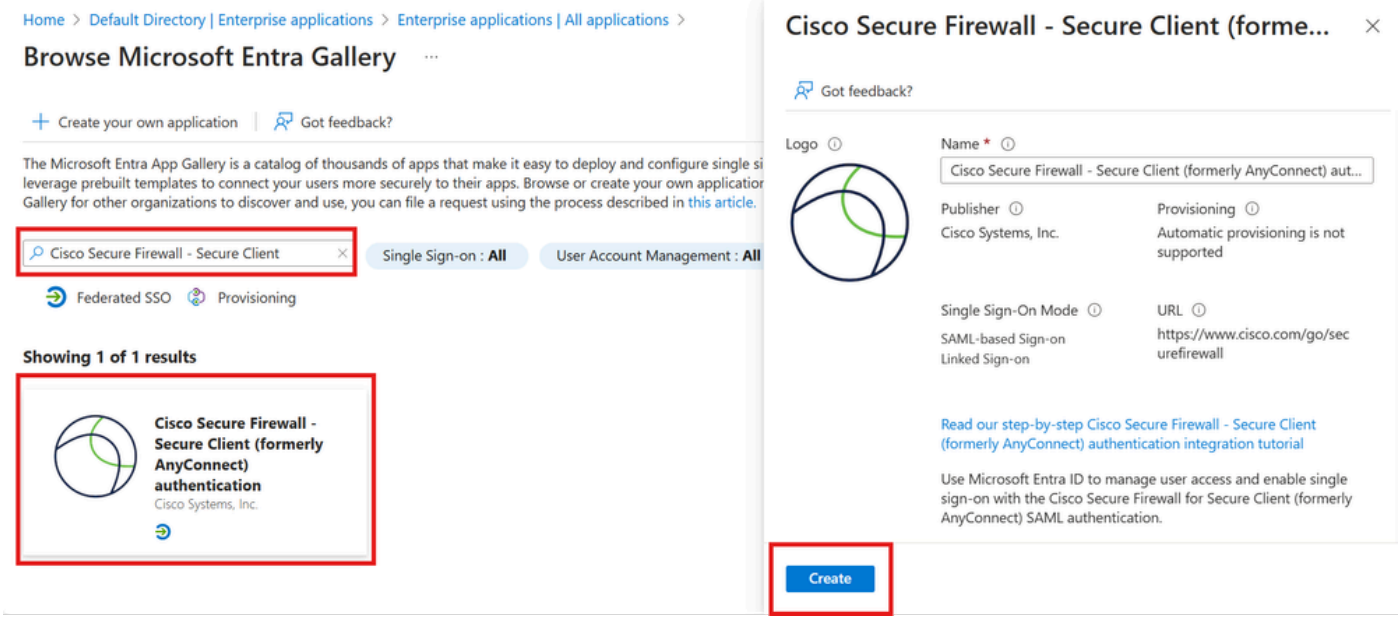
Application d'entreprise

Étape 3. Maintenant, choisissez New Application, comme illustré dans cette image.



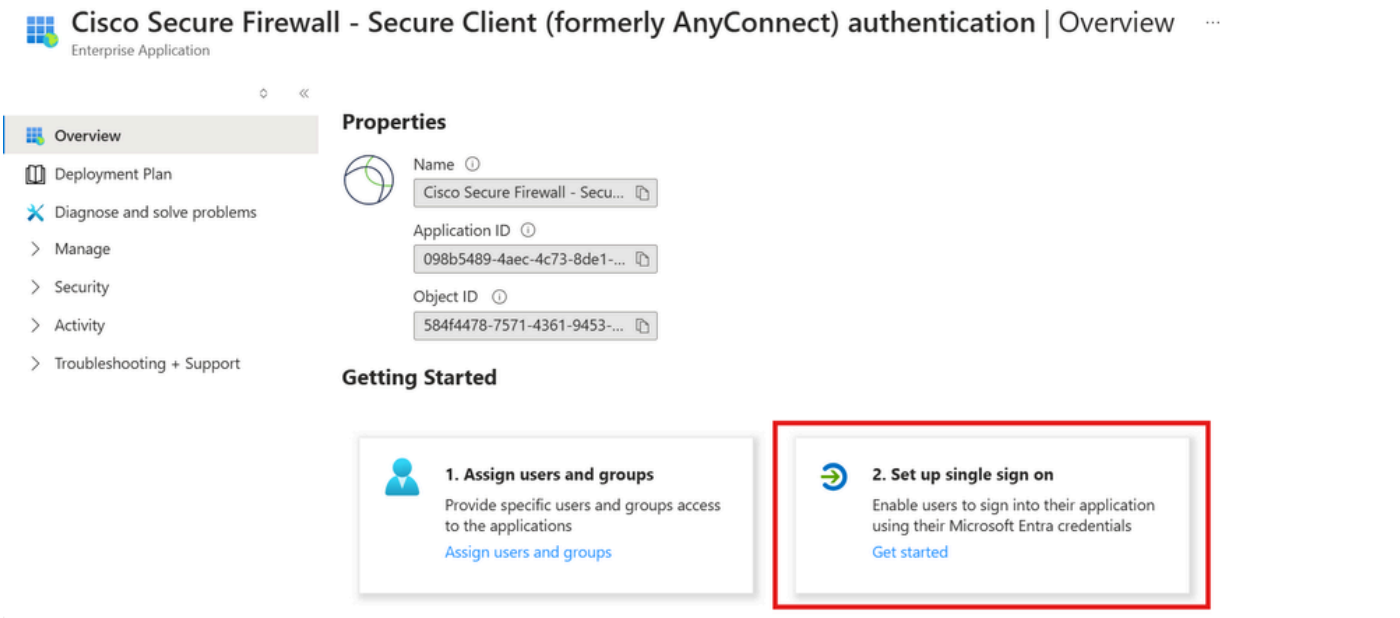
Nouvelle application

Étape 4. Dans la section Ajouter à partir de la galerie, tapez Cisco Secure Firewall - Secure Client dans la zone de recherche, choisissez Cisco Secure Firewall - Secure Client dans le panneau des résultats, puis ajoutez l'application.



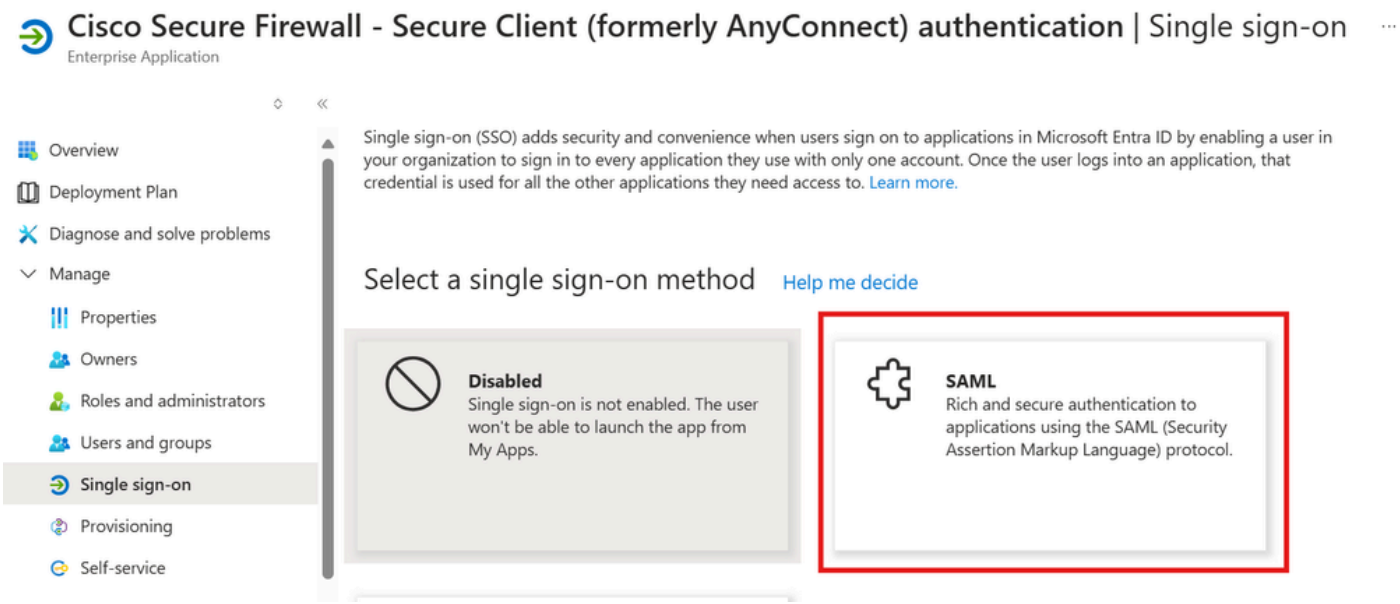
Pare-feu sécurisé Cisco - Client sécurisé

Étape 5. Choisissez l'élément de menu Single Sign-on, comme illustré dans cette image.



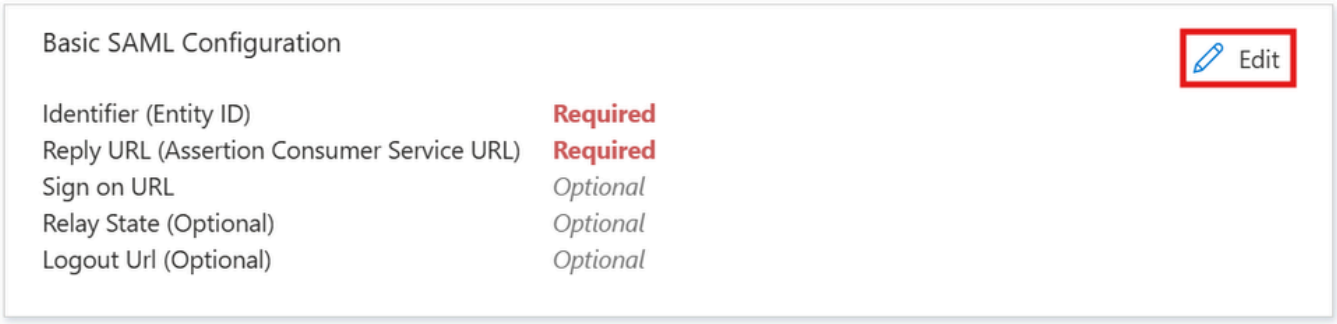
Configurer l'authentification unique

Étape 6. Sur la page Sélectionner une méthode d'authentification unique, sélectionnezSAML.



SAML

Étape 7. Sur la page Configurer l'authentification unique avec SAML, cliquez sur l'icône Modifier/Ouvrir de Configuration SAML de base afin de modifier les paramètres.



Exemple de configuration de base

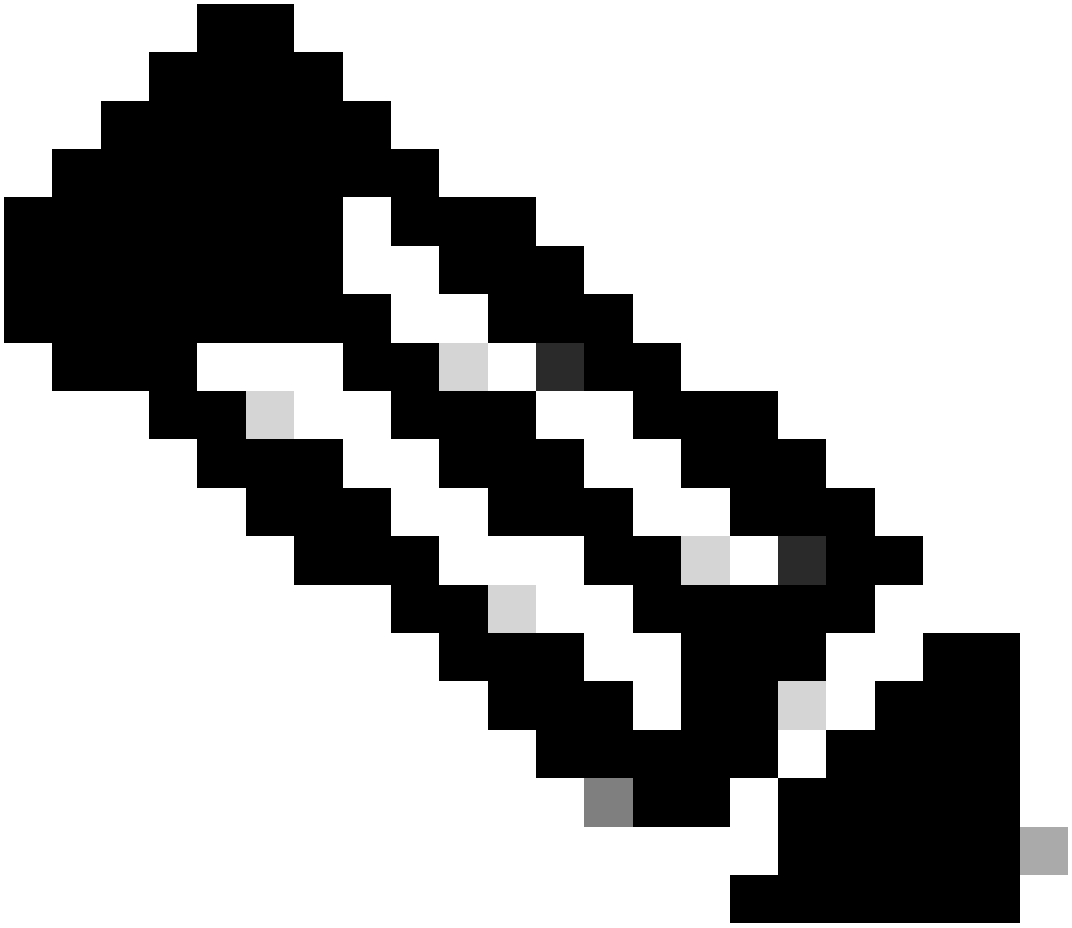
Étape 8. Dans la page Configurer l'authentification unique avec SAML, saisissez les valeurs des champs suivants :

a. Dans la zone de texte Identifier, tapez une URL en utilisant ce modèle :

https://<URL VPN>/saml/sp/metadata/<Nom_Groupe_Tunnel>

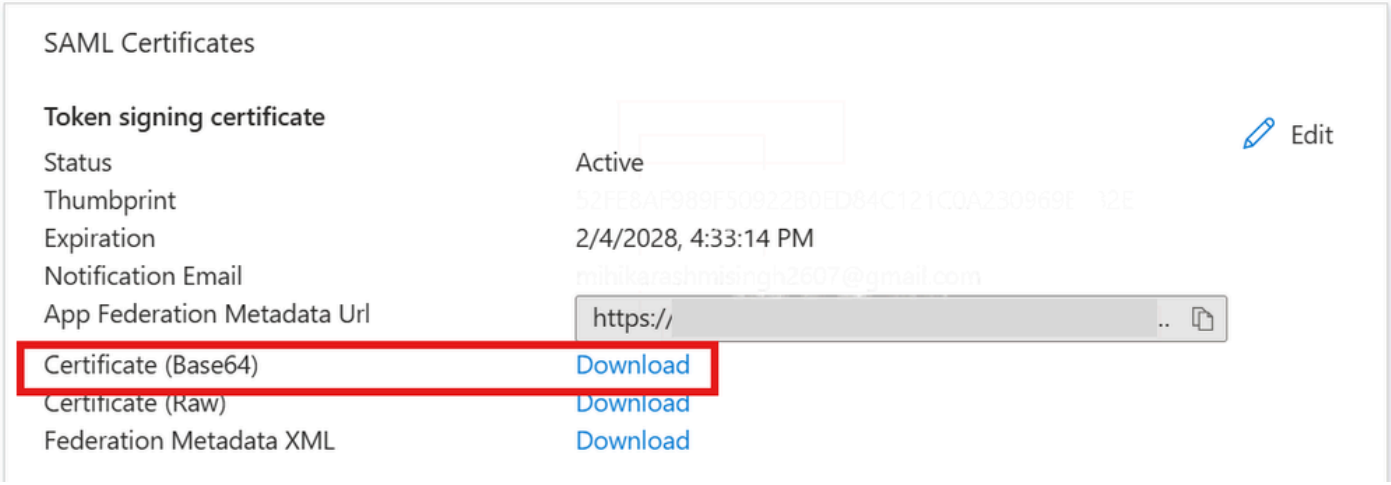
b. Dans la zone de texte URL de réponse, tapez une URL en utilisant ce modèle :

https://<URL VPN>/+CSCOE+/saml/sp/acs?tgname=<Nom_Groupe_Tunnel>
[Nom_Groupe_Tunnel = SAML1]

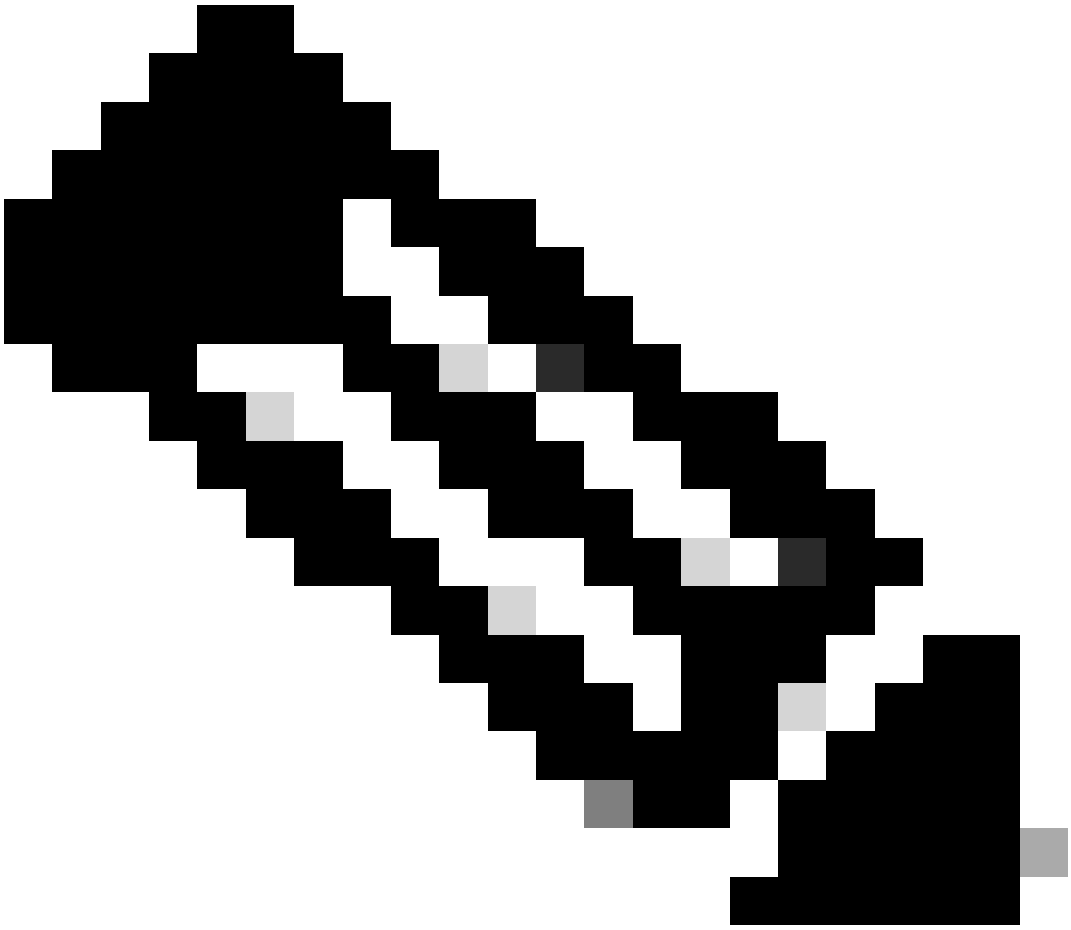


Remarque : Tunnel_Group_Name est sensible à la casse et la valeur ne doit pas contenir de points '.' et les barres obliques '/'.

Étape 9. Sur la page Configurer l'authentification unique avec SAML, dans la section Certificat de signature SAML, recherchez Certificat (Base64) et choisissez Télécharger afin de télécharger le fichier de certificat et de l'enregistrer sur votre ordinateur.



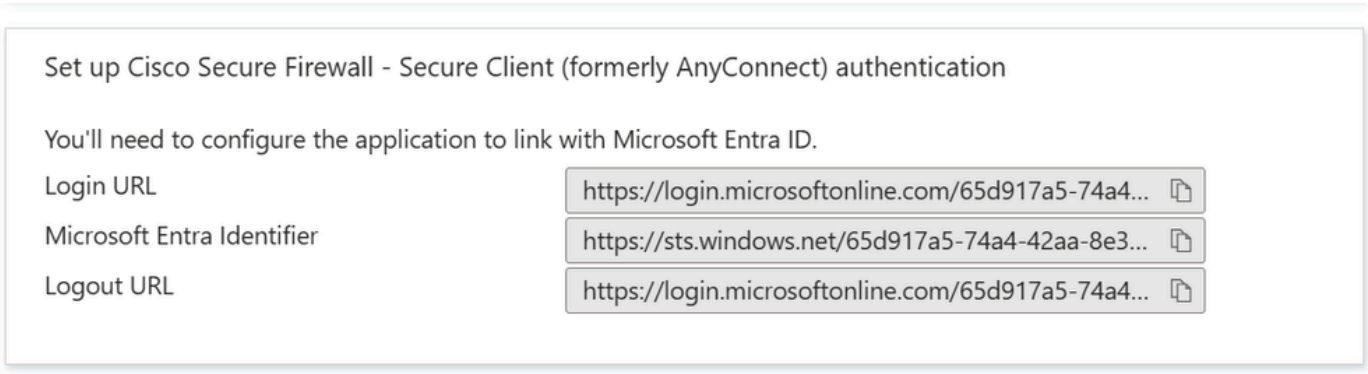
Téléchargement du certificat (Base64)



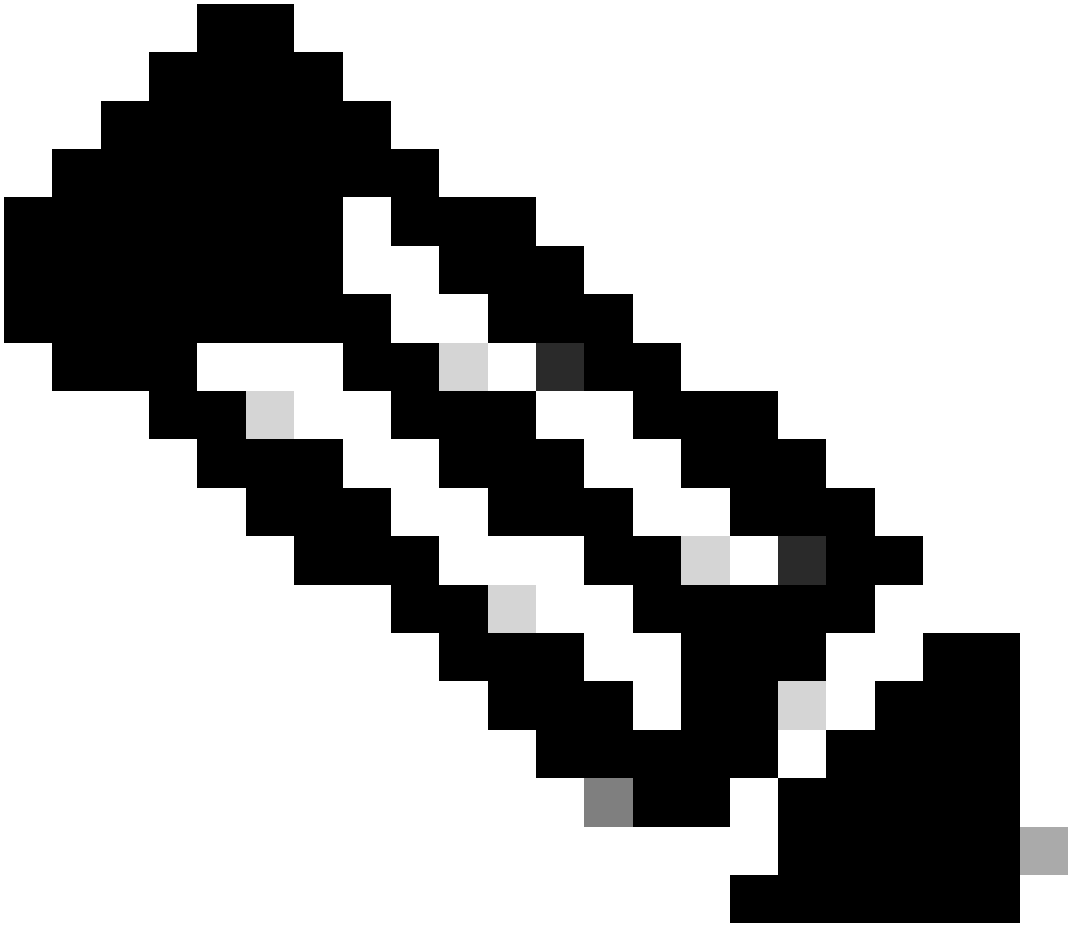
Remarque : ce certificat téléchargé est importé dans le point de confiance ASA AzureAD-AC-SAML1. Reportez-vous à la section Configuration ASA pour plus de détails.

Étape 10. Dans la section Configurer Cisco Secure Firewall - Client sécurisé, copiez la ou les URL appropriées en fonction de vos besoins. Ces URL sont utilisées pour configurer l'objet Serveur SSO sur ASA.

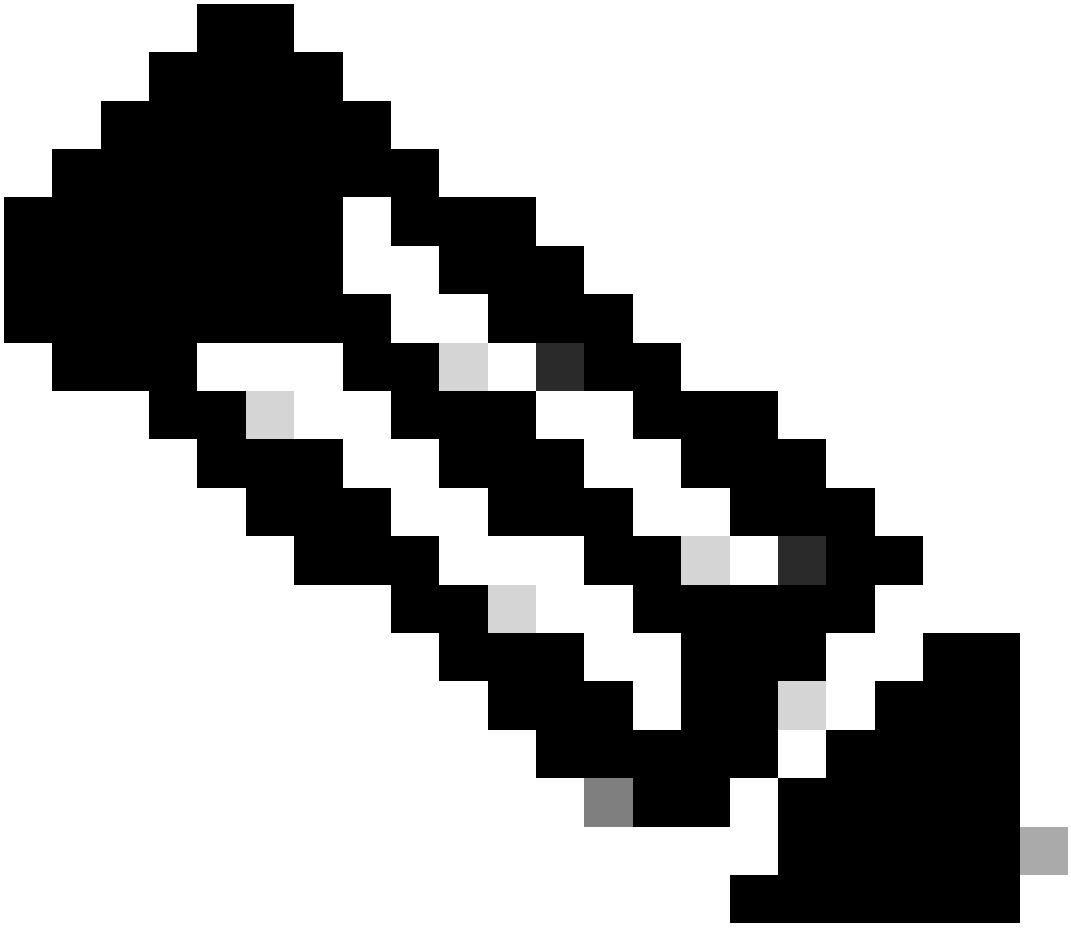
- Microsoft Entra Identifier : il s'agit de l'ID SAML dans la configuration VPN.
- URL de connexion : il s'agit de la connexion à l'URL.
- URL de déconnexion : il s'agit de la déconnexion de l'URL.



URL SSO



Remarque : Répétez les étapes de configuration précédentes afin d'ajouter l'application Cisco Secure Firewall - Secure Client de la galerie pour le deuxième groupe de tunnels. Dans ce cas, le deuxième nom du groupe de tunnels est SAML2.



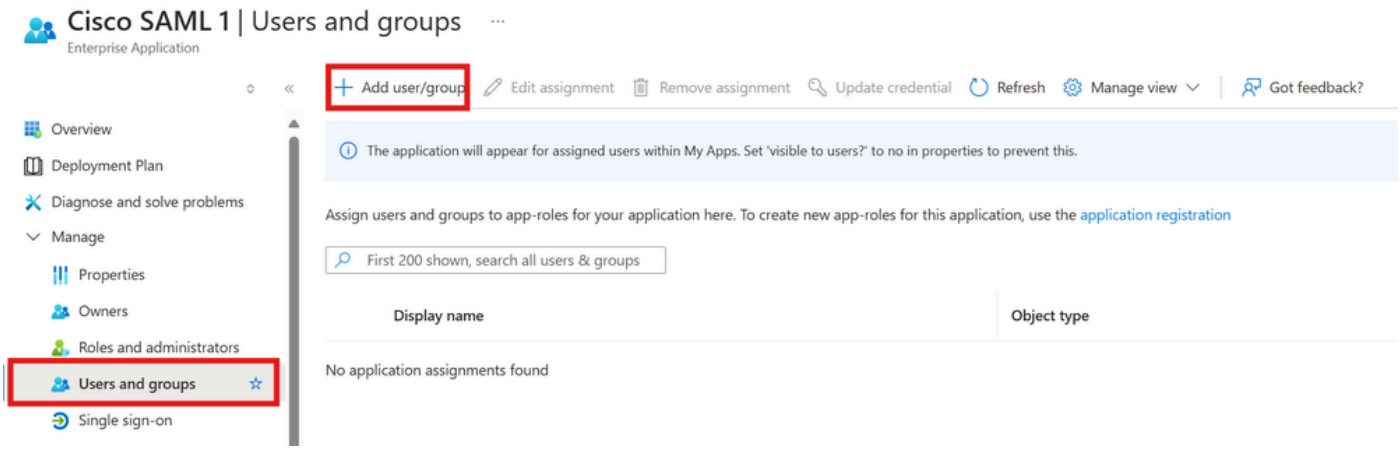
Remarque : lors de l'ajout de l'application Cisco Secure Firewall - Secure Client pour le deuxième groupe de tunnels (SAML 2), le certificat Azure téléchargé à l'étape 8. est importé dans le point de confiance ASA AzureAD-AC-SAML2.

Affecter des utilisateurs Azure AD à l'application

Dans cette section, Test1 et Test2 sont activés pour utiliser Azure SSO, lorsque vous accordez l'accès à l'application Cisco Secure Client.

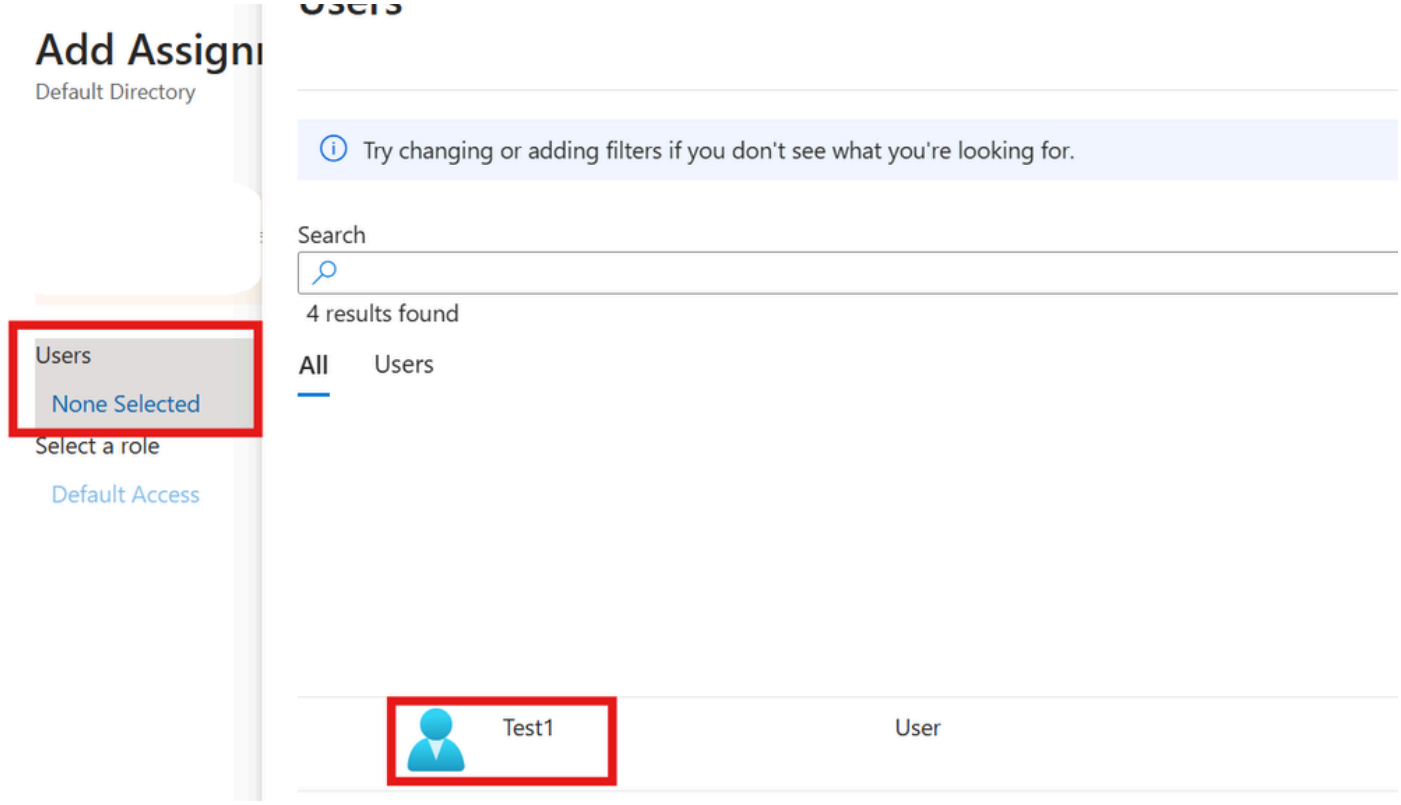
Pour la première application IdP :

Étape 1. Dans la première page de présentation de l'application IdP, sélectionnez Utilisateurs et groupes, puis Ajouter un utilisateur.



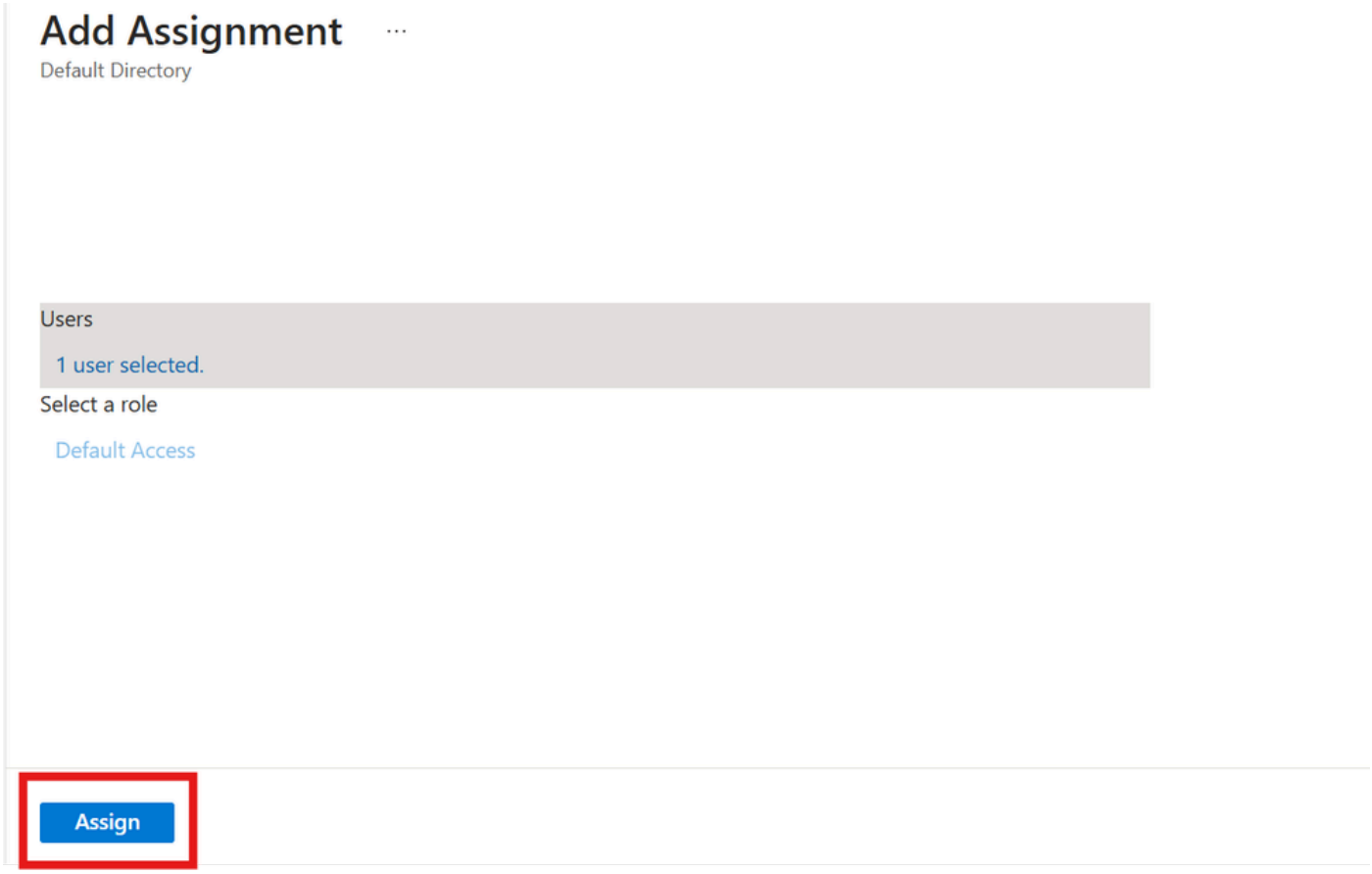
Utilisateurs et groupes

Étape 2. Sélectionnez Utilisateurs ou groupes dans la boîte de dialogue Ajouter une affectation.



Ajouter le devoir 1

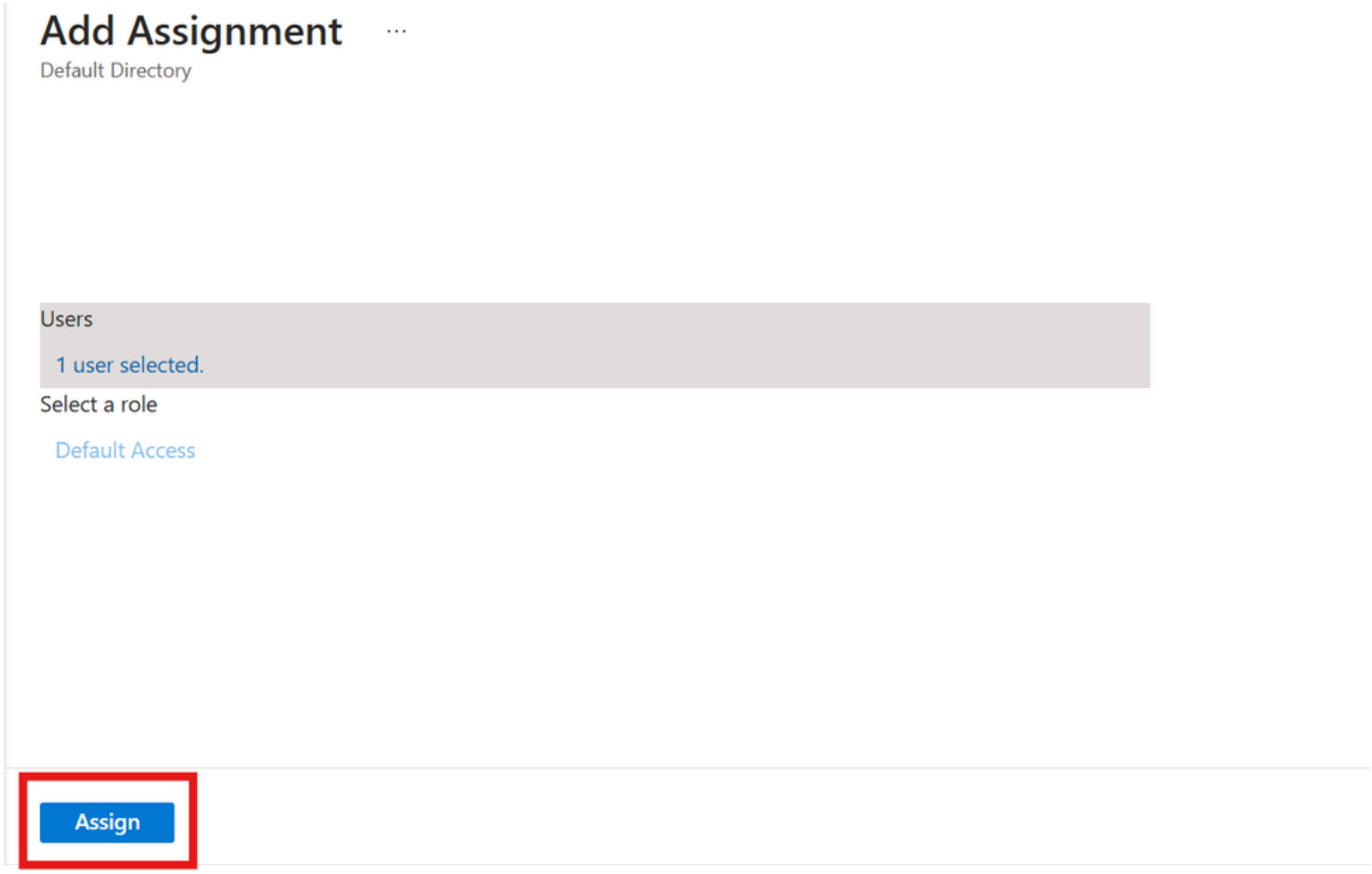
Étape 3. Dans la boîte de dialogue Ajouter une affectation, cliquez sur le bouton Affecter.



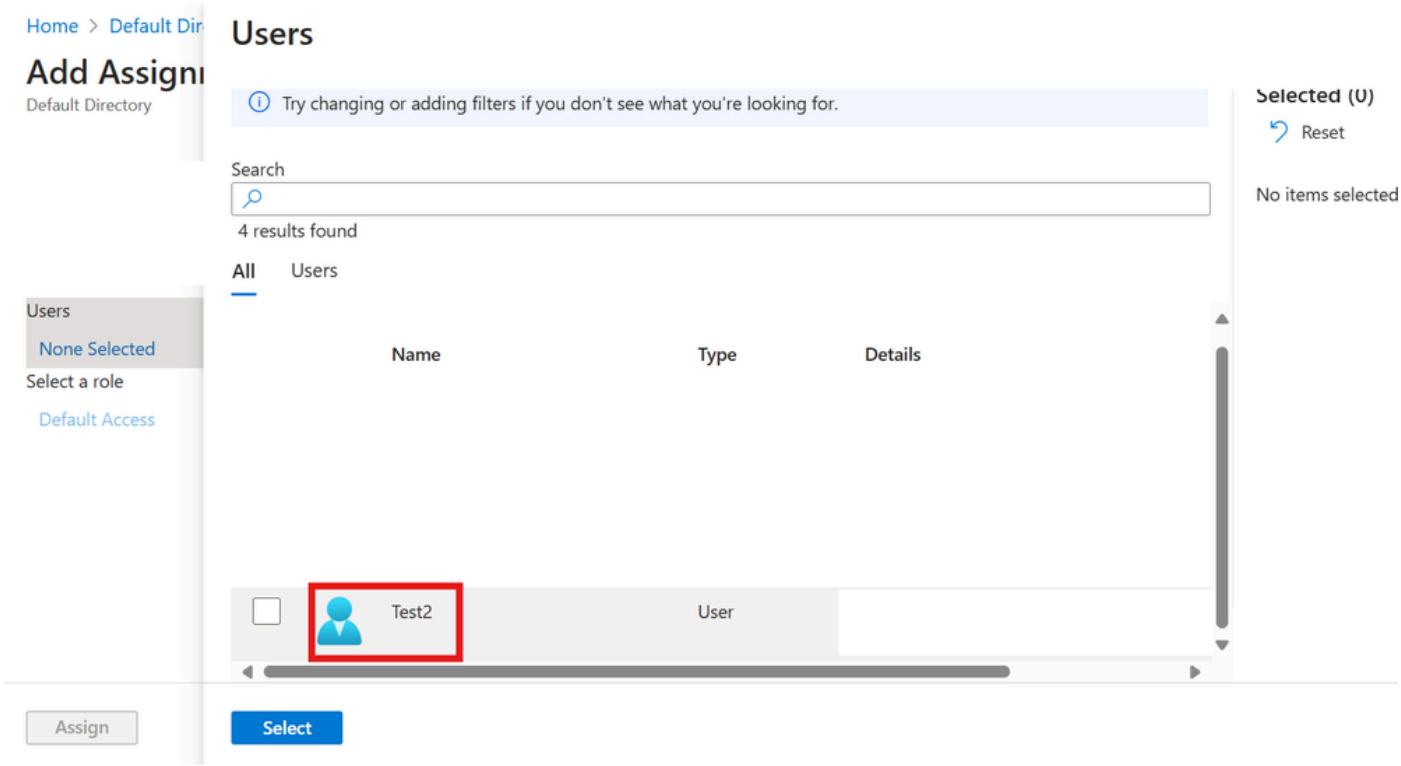
Attribution d'utilisateur Test1

Pour la deuxième application IdP :

Répétez les étapes précédentes pour la deuxième application Idp, comme indiqué dans ces images.

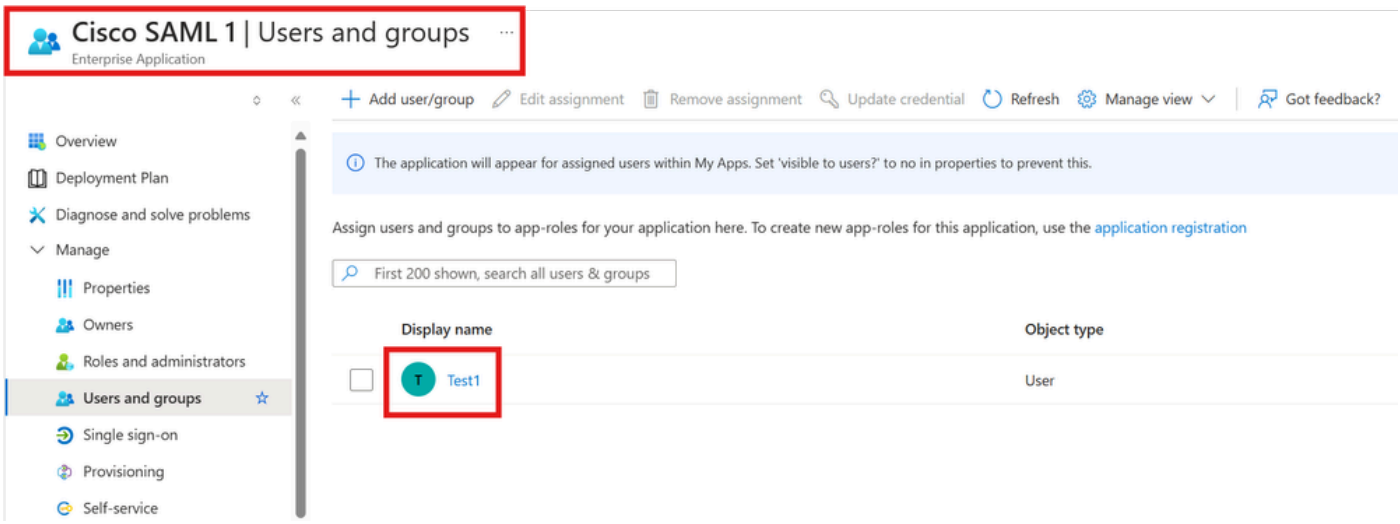


Ajouter le devoir 2



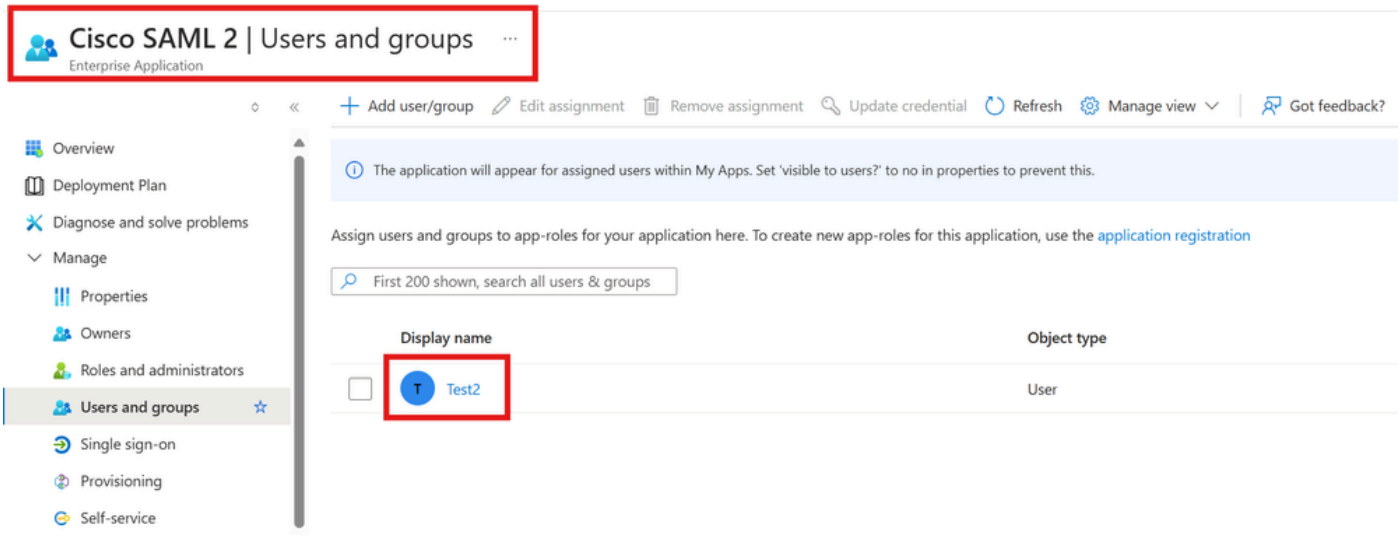
Attribuer un utilisateur Test2

Attribution d'utilisateur Test1 :



Tester 1 affectation d'utilisateur

Attribution d'utilisateur Test2 :



Test 2 - Affectation d'utilisateurs

Configuration ASA via CLI

Étape 1 : création de points de confiance et importation de certificats SAML

Configurez deux points de confiance et importez les certificats SAML respectifs pour chaque groupe de tunnels.

<#root>

```
config t

 crypto ca trustpoint
```

AzureAD-AC-SAML1

```
   revocation-check none
   no id-usage
```

```
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML1

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit

!
!

crypto ca trustpoint
```

AzureAD-AC-SAML2

```
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate
```

AzureAD-AC-SAML2

```
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded from AzureAD goes here
 …
 -----END CERTIFICATE-----
 quit
```

Étape 2 : configuration de l'IdP SAML

Utilisez ces commandes pour provisionner les paramètres du fournisseur d'identité SAML.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxxx/saml2  - [Logout URL]
 trustpoint idp AzureAD-AC-SAML1 - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

Étape 3 : application de l’authentification SAML au premier groupe de tunnels VPN

Configurez le groupe de tunnels SAML1 avec le point de confiance AzureAD-AC-SAML1 IdP.

<#root>

```
tunnel-group SAML1 webvpn-attributes
authentication saml
group-alias SAML1 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML1 <---- Overrides the primary IDP certificate in the Single Sign-On (

Étape 4 : application de l'authentification SAML au deuxième groupe de tunnels VPN

Configurez le groupe de tunnels SAML2 avec le point de confiance AzureAD-AC-SAML2 IdP.

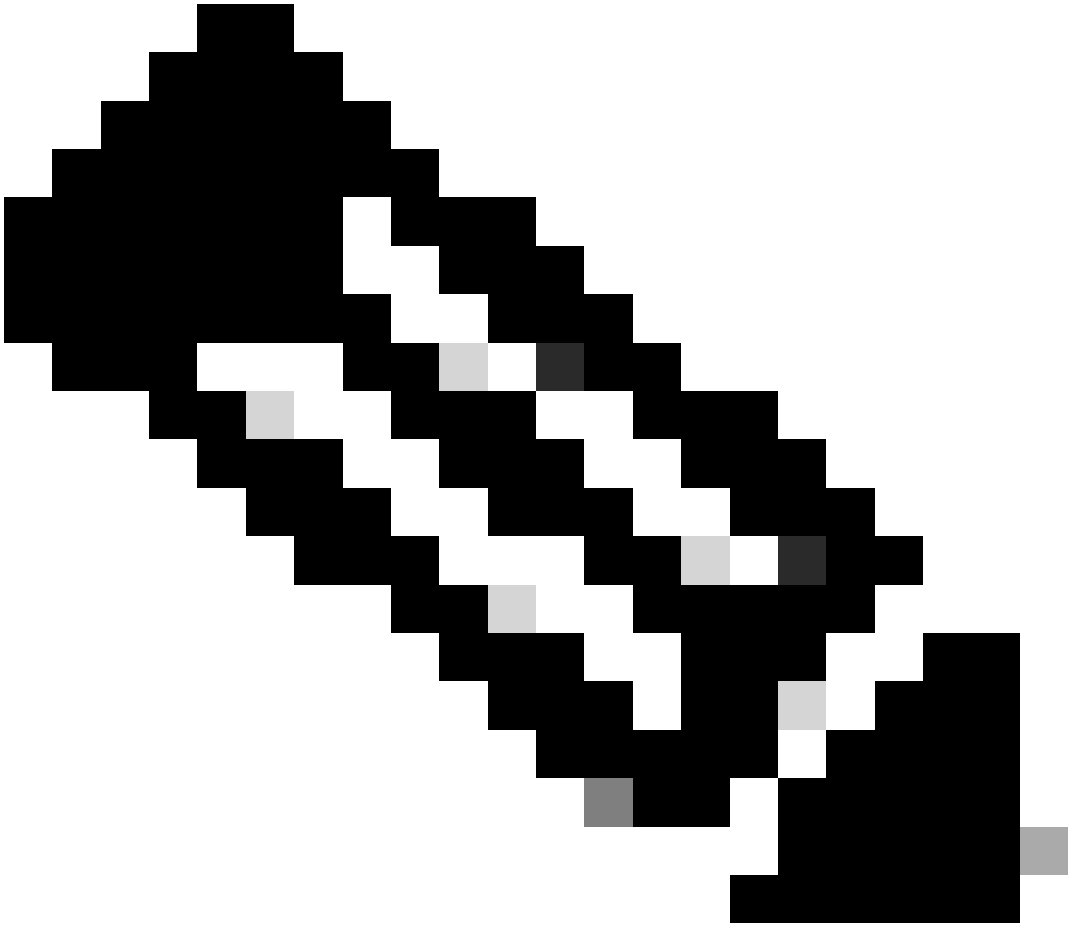
<#root>

```
tunnel-group SAML2 webvpn-attributes
authentication saml
group-alias SAML2 enable
saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
```

saml idp-trustpoint AzureAD-AC-SAML2 <---- Overrides the primary IDP certificate in the Single Sign-On (

Étape 5 : Enregistrez la configuration.

```
write memory
```



Remarque : Si vous apportez des modifications à la configuration du fournisseur d'identité, vous devez supprimer la configuration du fournisseur d'identité SAML de votre groupe de tunnels et la réappliquer pour que les modifications prennent effet.

Vérifier

Testez AnyConnect avec l’authentification SAML.

Étape 1. Connectez-vous à votre URL VPN et entrez vos détails de connexion dans Azure AD.

Étape 2. (Facultatif) Approuvez la demande de connexion.

Étape 3. AnyConnect est connecté.

Dépannage

La plupart des dépannages SAML impliquent une erreur de configuration qui peut être trouvée lorsque la configuration SAML est vérifiée, ou que des débogages sont exécutés. debug webvpn saml 255 peut être utilisé pour dépanner la plupart des problèmes, cependant, dans les scénarios où ce débogage ne fournit pas d'informations utiles, des débogages supplémentaires peuvent être exécutés :

```
debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
```

Informations connexes

- Configurer le RPV AnyConnect d’un ASA avec l’authentification multifactorielle de Microsoft Azure par SAML
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.