Configurer le RPV AnyConnect d’un ASA avec l’authentification multifactorielle de Microsoft Azure par SAML

Table des matières

Introduction

Ce document décrit comment configurer le langage SAML (Security Assertion Markup Language) en mettant l'accent sur ASA AnyConnect via Microsoft Azure MFA.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration VPN RA sur ASA.
- Connaissances de base de SAML et Microsoft Azure.
- Licences AnyConnect activées (APEX ou VPN uniquement).

Composants utilisés

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

- Un abonnement Microsoft Azure AD.
- Cisco ASA 9.7+ et Anyconnect 4.6+
- Utilisation du profil VPN AnyConnect

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

SAML est une structure XML permettant d'échanger des données d'authentification et d'autorisation entre des domaines de sécurité. Il crée un cercle de confiance entre l'utilisateur, un fournisseur de services (SP) et un fournisseur d'identité (IdP) qui permet à l'utilisateur de se connecter en une seule fois pour plusieurs services. Microsoft Azure MFA s'intègre en toute transparence à l'appliance VPN Cisco ASA pour fournir une sécurité supplémentaire pour les connexions VPN Cisco AnyConnect.

Composants SAML

Métadonnées : il s'agit d'un document XML qui garantit une transaction sécurisée entre un fournisseur d'identité et un fournisseur de services. Il permet au fournisseur d'identité et au fournisseur de services de négocier des accords.

Rôles pris en charge par les périphériques (IdP, SP)

Un périphérique peut prendre en charge plusieurs rôles et peut contenir des valeurs à la fois pour un fournisseur de services et un fournisseur d'identité. Sous le champ EntityDescriptor se trouve un IDPSSODescriptor si les informations contenues concernent un fournisseur de services d'identification à authentification unique ou un SPSSODescriptor si les informations contenues concernent un fournisseur de services à authentification unique. Ceci est important car les valeurs correctes doivent être prises dans les sections appropriées pour que la configuration de SAML soit réussie.

ID d'entité : ce champ est un identifiant unique pour un fournisseur de services ou un fournisseur d'identité. Un périphérique unique peut avoir plusieurs services et utiliser différents ID d'entité pour les différencier. Par exemple, ASA a différents ID d'entité pour différents groupes de tunnels qui doivent être authentifiés. Un fournisseur d'identité qui authentifie chaque groupe de tunnels a des entrées d'ID d'entité distinctes pour chaque groupe de tunnels afin d'identifier précisément ces

services.

ASA peut prendre en charge plusieurs IdP et dispose d'un ID d'entité distinct pour chaque IdP afin de les différencier. Si l'une des parties reçoit un message d'un périphérique qui ne contient pas d'ID d'entité précédemment configuré, le périphérique abandonne probablement ce message et l'authentification SAML échoue. L'ID d'entité se trouve dans le champ EntityDescriptor en regard de entityID.

URL de service : elles définissent l'URL d'un service SAML fourni par le SP ou le fournisseur d'identité. Pour les IDp, il s'agit le plus souvent du service de déconnexion unique et du service d'authentification unique. Pour les fournisseurs de services, il s'agit généralement des services Assertion Consumer et Single Logout.

L'URL du service d'authentification unique trouvée dans les métadonnées IdP est utilisée par le fournisseur de services pour rediriger l'utilisateur vers le fournisseur d'identité pour l'authentification. Si cette valeur n'est pas correctement configurée, le fournisseur d'identité ne reçoit pas ou ne peut pas traiter correctement la demande d'authentification envoyée par le fournisseur de services.

L'URL du service consommateur d'assertions trouvée dans les métadonnées SP est utilisée par le fournisseur d'identité pour rediriger l'utilisateur vers le fournisseur de services et fournir des informations sur la tentative d'authentification de l'utilisateur. Si cette configuration est incorrecte, le SP ne reçoit pas l'assertion (la réponse) ou ne peut pas la traiter correctement.

L'URL du service de déconnexion unique se trouve à la fois sur le fournisseur de services et sur le fournisseur d'identité. Il est utilisé pour faciliter la déconnexion de tous les services SSO du SP et est facultatif sur l'ASA. Lorsque l'URL du service SLO à partir des métadonnées IdP est configurée sur le fournisseur de services, lorsque l'utilisateur se déconnecte du service sur le fournisseur de services, le fournisseur de services envoie la demande au fournisseur d'ID. Une fois que l'IdP a réussi à déconnecter l'utilisateur des services, il le redirige vers le SP et utilise l'URL du service SLO trouvée dans les métadonnées du SP.

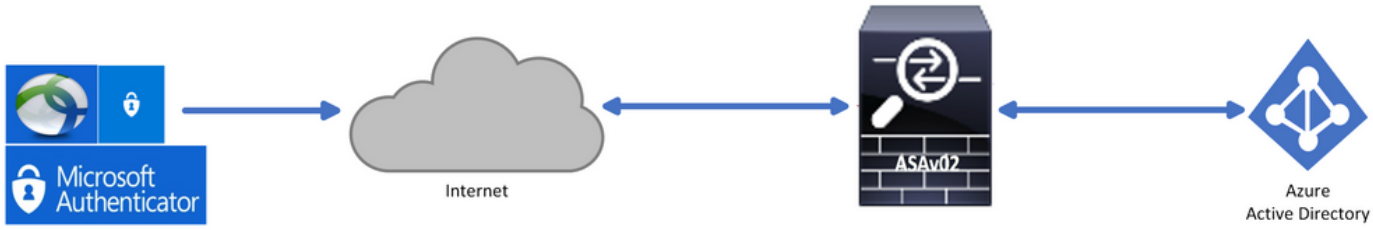
Liaisons SAML pour les URL de service : les liaisons sont la méthode que le SP utilise pour transférer des informations au fournisseur d'identité et vice versa pour les services. Cela inclut HTTP Redirect, HTTP POST et Artifact. Chaque méthode permet de transférer des données différemment. La méthode de liaison prise en charge par le service est incluse dans la définition de ces services. Par exemple : SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=https://saml.example.com/simplesaml/saml2/idp/SSOService.php/ >. L'ASA ne prend pas en charge la liaison d'artefact. ASA utilise toujours la méthode de redirection HTTP pour les demandes d'authentification SAML. Il est donc important de choisir l'URL du service SSO qui utilise la liaison de redirection HTTP afin que le fournisseur d'identité l'attende.

Certificats pour les opérations de signature et de chiffrement

Pour assurer la confidentialité et l'intégrité des messages envoyés entre le SP et le fournisseur d'identité, SAML inclut la possibilité de chiffrer et de signer les données. Le certificat utilisé pour chiffrer et/ou signer les données peut être inclus dans les métadonnées afin que l'extrémité qui

reçoit puisse vérifier le message SAML et s'assurer qu'il provient de la source attendue. Les certificats utilisés pour la signature et le chiffrement se trouvent dans les métadonnées sous KeyDescriptor use="signing" et KeyDescriptor use="encryption", respectivement, puis X509Certificate. L'ASA ne prend pas en charge le chiffrement des messages SAML.

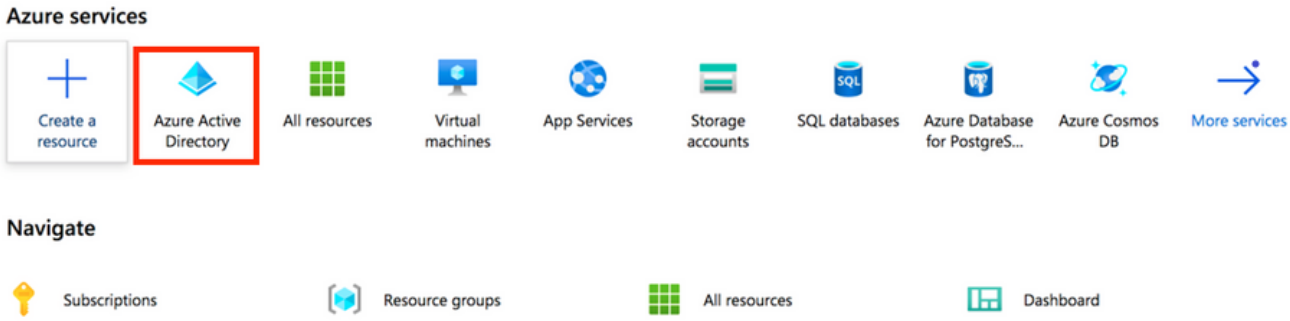
Diagramme du réseau



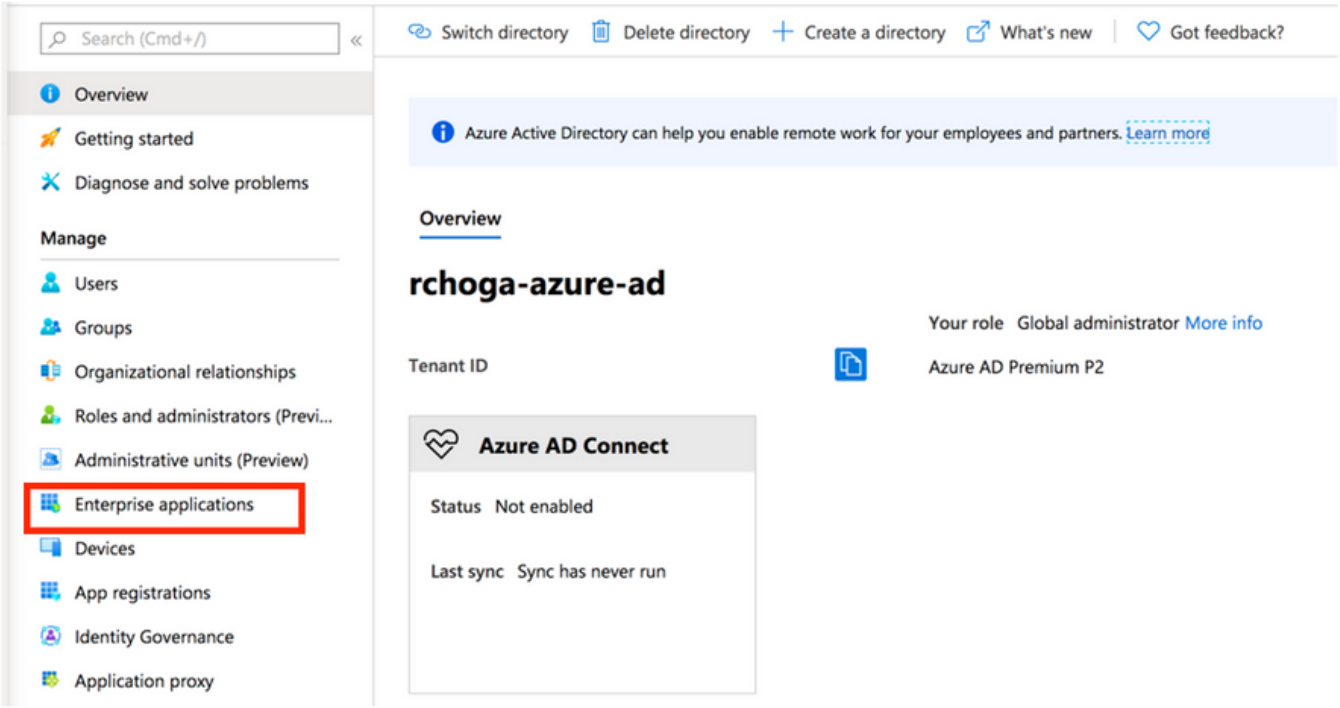
Configurer

Ajouter Cisco AnyConnect à partir de la galerie d'applications Microsoft

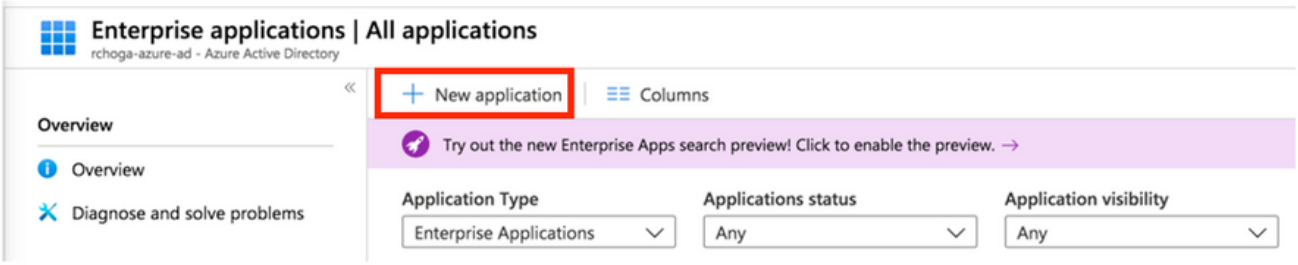
Étape 1. Connectez-vous au portail Azure et choisissez Azure Active Directory.



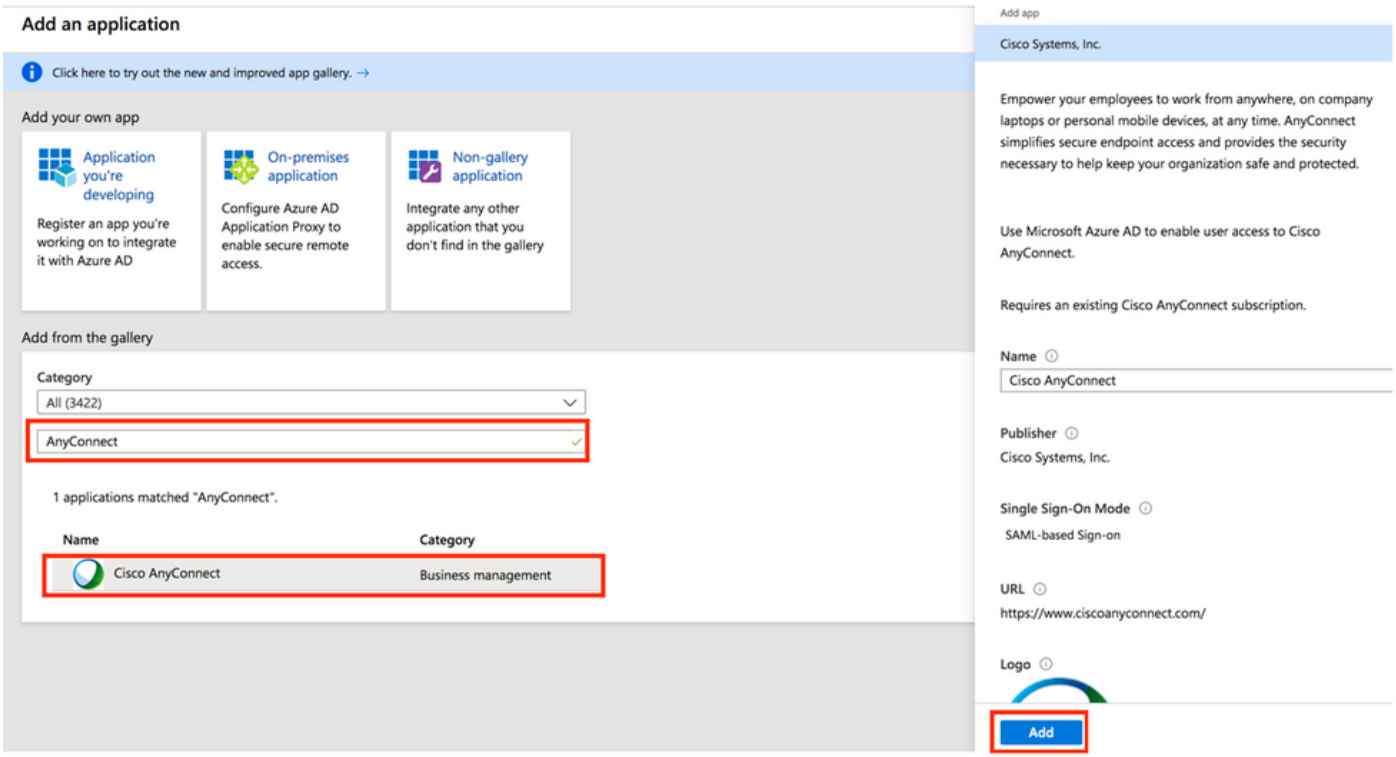
Étape 2. Comme l'illustre cette image, sélectionnez Applications d'entreprise.



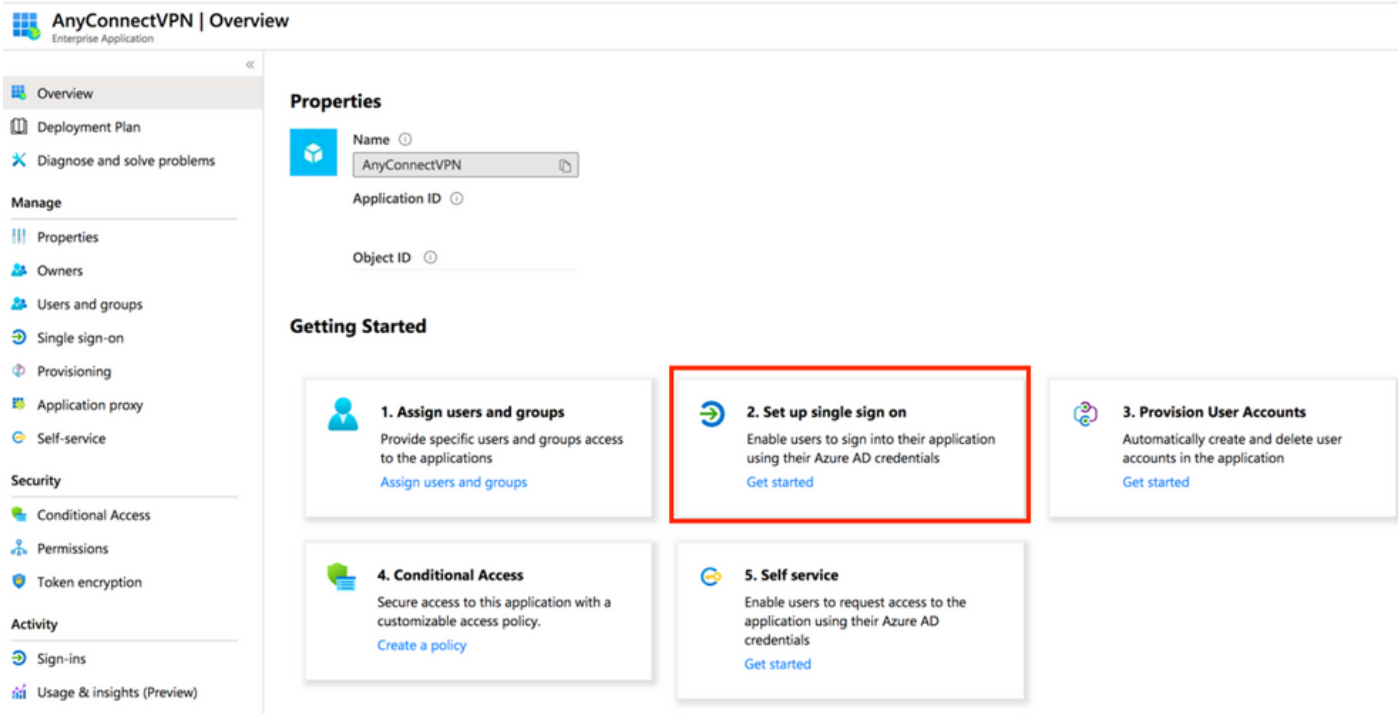
Étape 3. Choisissez maintenant New Application, comme illustré dans cette image.



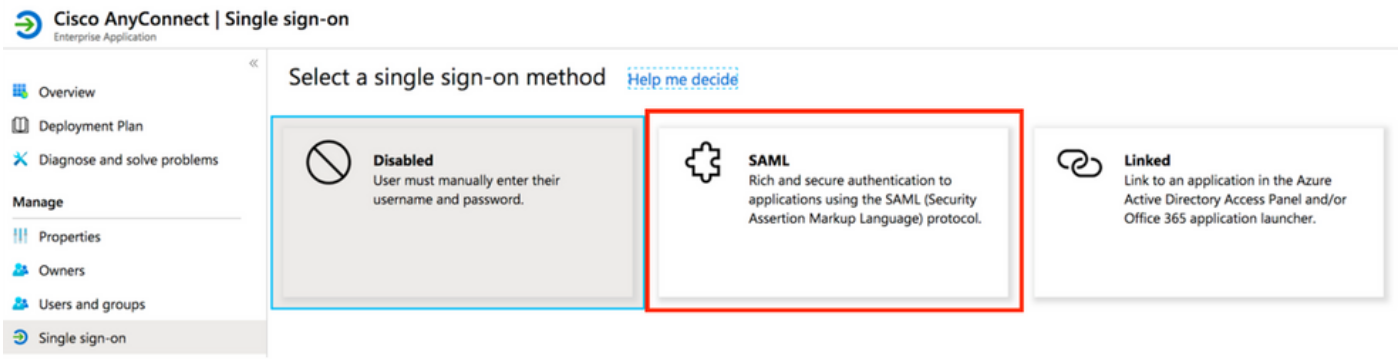
Étape 4. Dans la section Ajouter à partir de la galerie, tapez AnyConnect dans la zone de recherche, choisissez Cisco AnyConnect dans le panneau des résultats, puis ajoutez l'application.



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



Étape 6. Choisissez SAML, comme illustré dans l'image.



Étape 7. Modifiez la section 1 avec ces détails.

<#root>

a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>

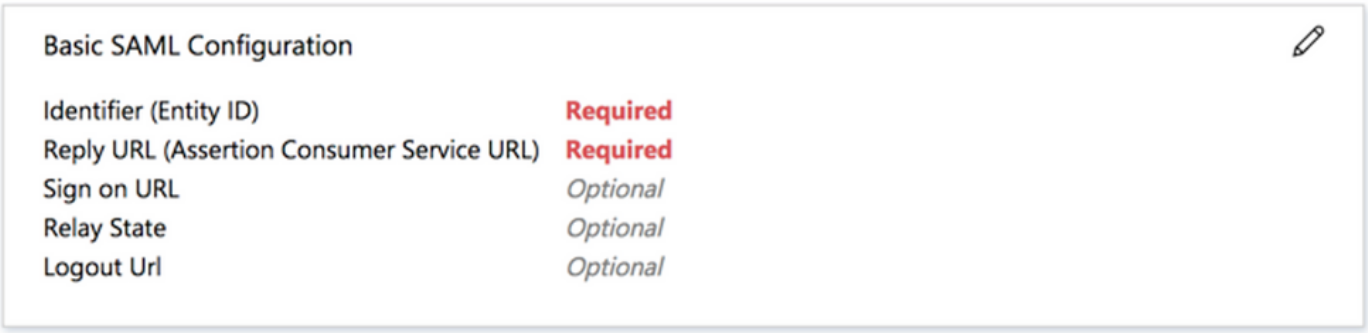
b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G

Example: vpn url called

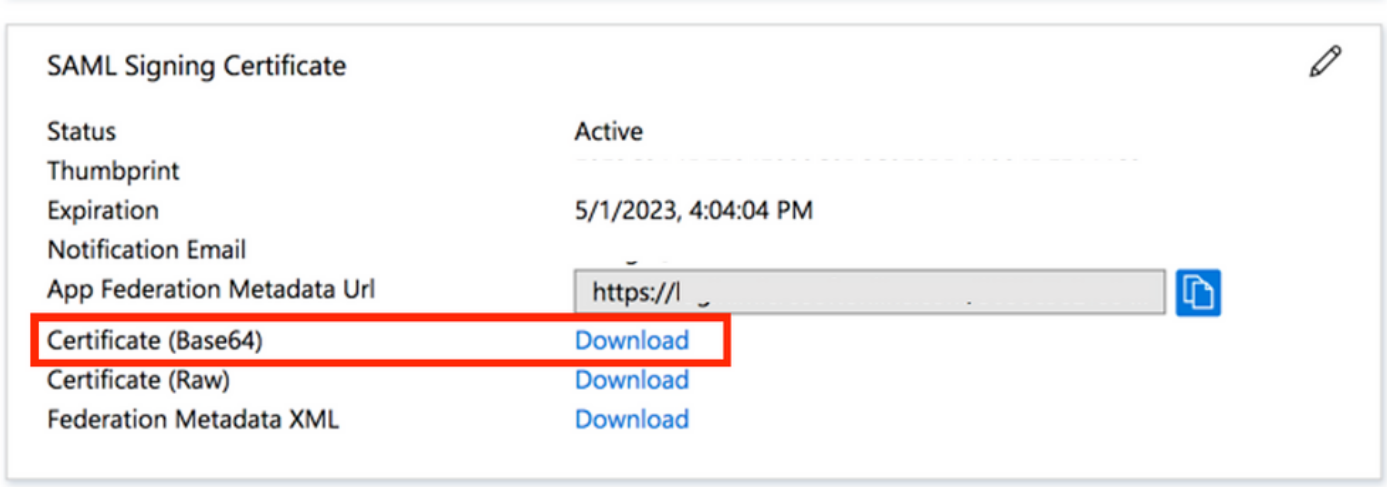
asa.example.com

and tunnel-group called

AnyConnectVPN-1

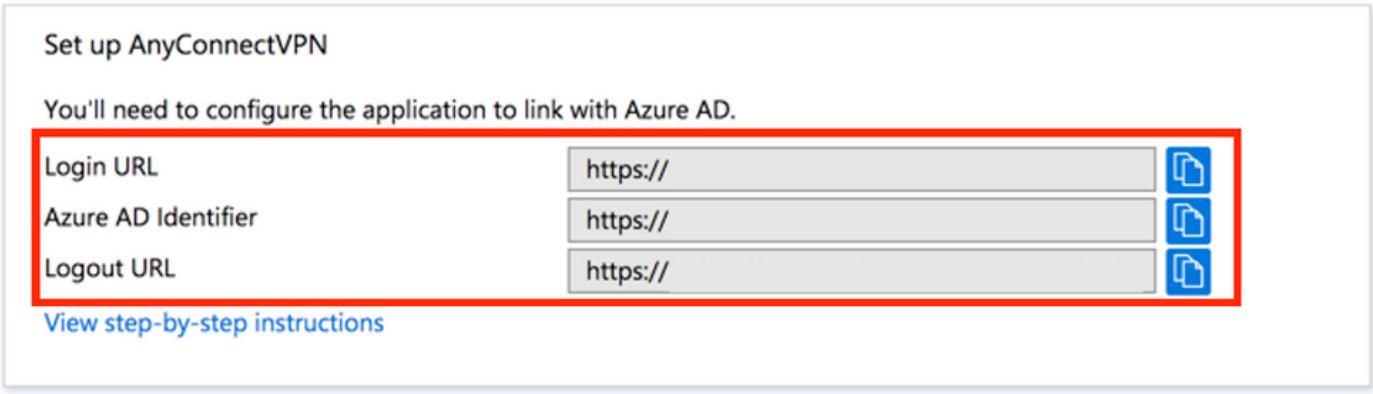


Étape 8. Dans la section Certificat de signature SAML, choisissez Télécharger pour télécharger le fichier de certificat et enregistrez-le sur votre ordinateur.



Étape 9. Ceci est requis pour la configuration ASA.

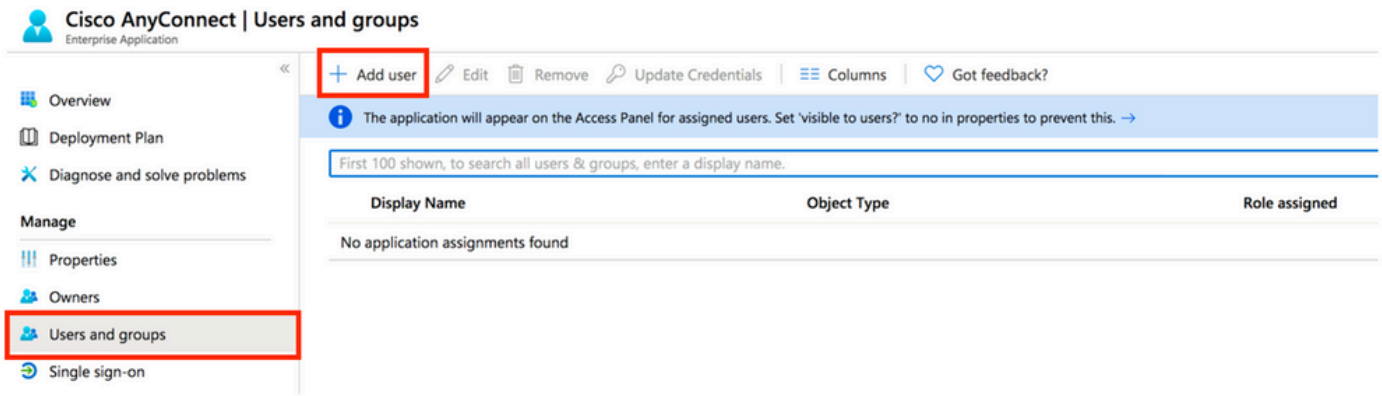
- Identificateur Azure AD : il s'agit du petit ID dans notre configuration VPN.
- URL de connexion : il s'agit de la connexion à l'URL.
- URL de déconnexion : il s'agit de la déconnexion de l'URL.



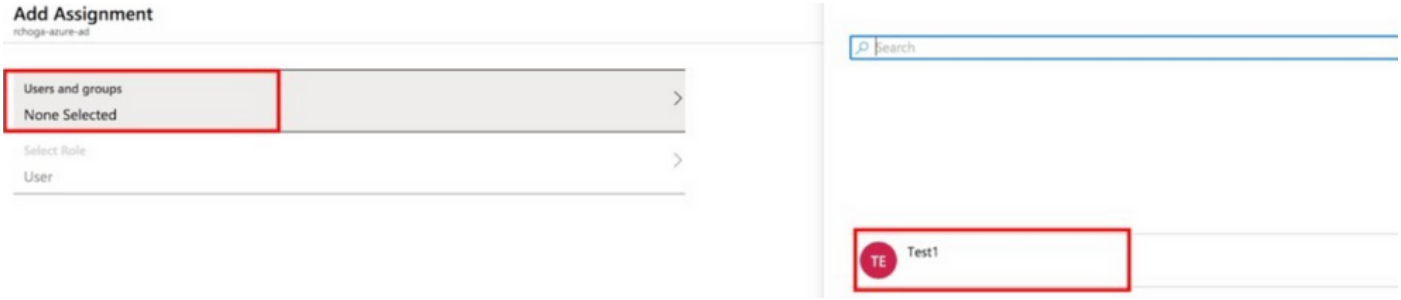
Affecter un utilisateur Azure AD à l'application

Dans cette section, Test1 est activé pour utiliser l'authentification unique Azure, lorsque vous accordez l'accès à l'application Cisco AnyConnect.

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



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



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

Configurer ASA pour SAML via CLI

Étape 1. Créez un Trustpoint et importez votre certificat SAML.

```
config t

 crypto ca trustpoint AzureAD-AC-SAML
   revocation-check none
   no id-usage
   enrollment terminal
   no ca-check
 crypto ca authenticate AzureAD-AC-SAML
 -----BEGIN CERTIFICATE-----
 …
 PEM Certificate Text you downloaded goes here
 …
 -----END CERTIFICATE-----
 quit
```

Étape 2. Ces commandes mettent en service votre IDp SAML.

```
webvpn

 saml idp https://xxx.windows.net/xxxxxxxxxxxx/ - [Azure AD Identifier]
 url sign-in https://login.microsoftonline.com/xxxxxxxxxxxxxxxxxxxxx/saml2 - [Login URL]
 url sign-out https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 - Logout URL
 trustpoint idp AzureAD-AC-SAML - [IdP Trustpoint]
 trustpoint sp ASA-EXTERNAL-CERT - [SP Trustpoint]
 no force re-authentication
 no signature
 base-url https://asa.example.com
```

Étape 3. Appliquer l'authentification SAML à une configuration de tunnel VPN.

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxxxxx/
  authentication saml
end

write memory
```

Remarque : si vous modifiez la configuration du fournisseur d'identité, vous devez supprimer la petite configuration du fournisseur d'identité de votre groupe de tunnels et la réappliquer pour que les modifications prennent effet.

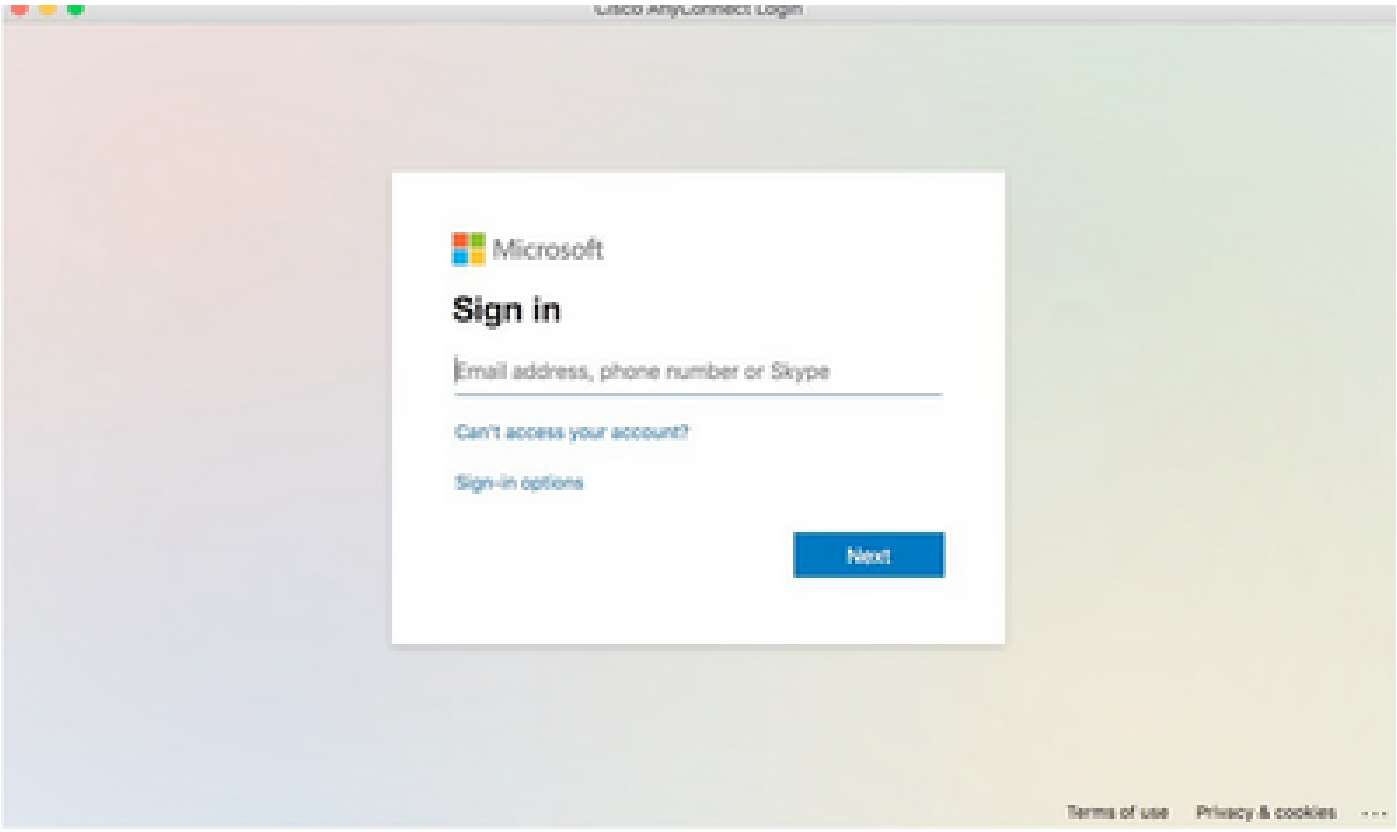
Vérifier

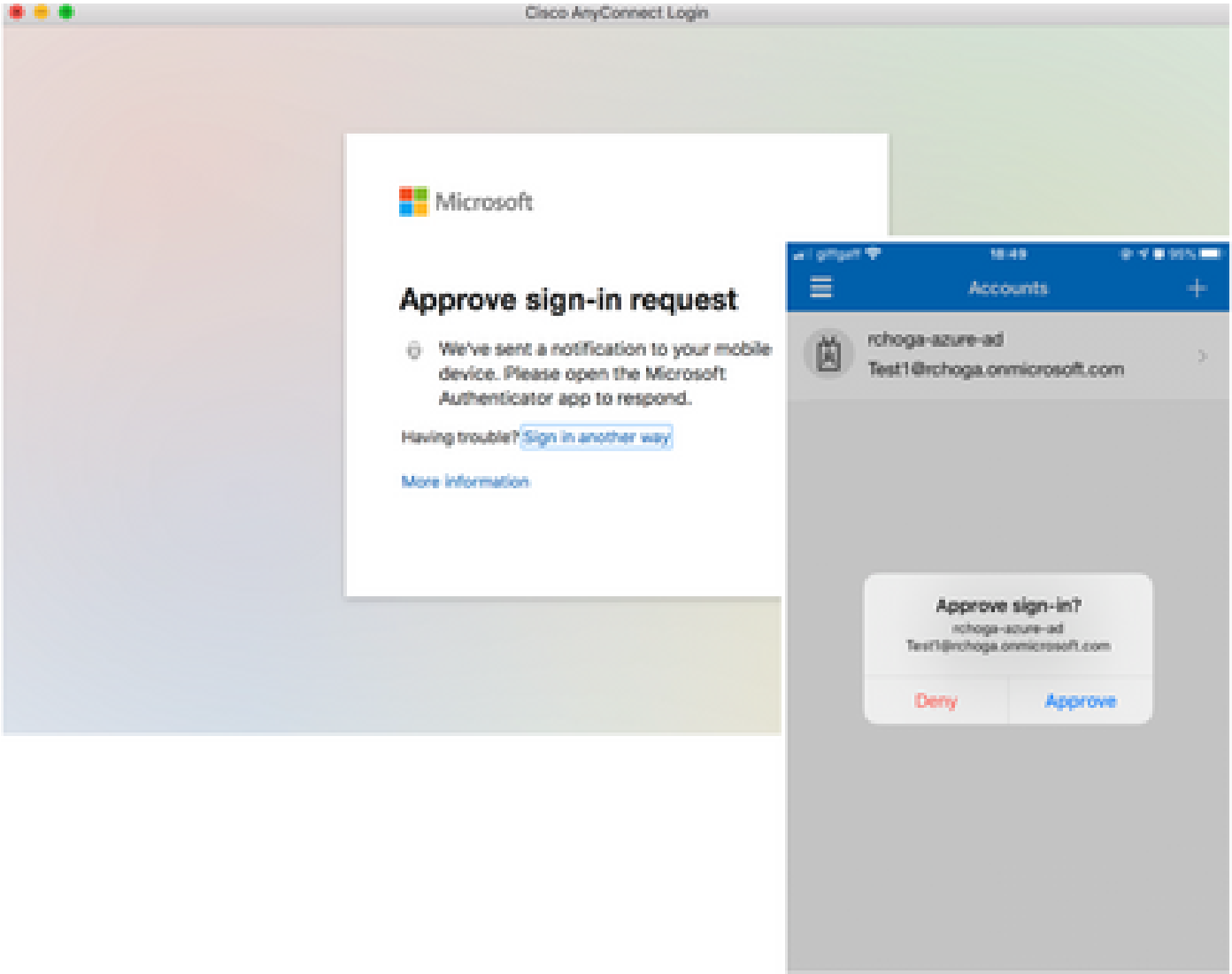
Tester AnyConnect avec l'authentification SAML

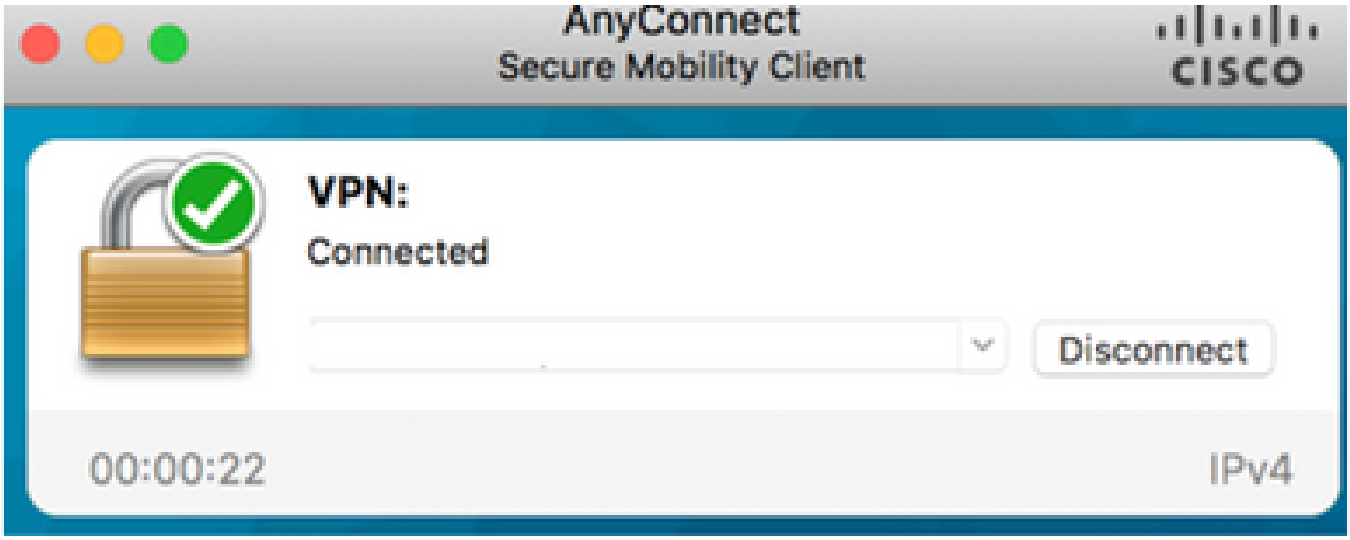
Étape 1. Connectez-vous à votre URL VPN et entrez vos informations de connexion dans Azure AD.

Étape 2 : approbation de la demande de connexion

Étape 3. AnyConnect est connecté.


Cisco AnyConnect Login
Microsoft
Sign in
Email address, phone number or Skype
Can't access your account?
Sign-in options
Next
Terms of use
Privacy & cookies


Cisco AnyConnect Login
Microsoft
Approve sign-in request
We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.
Having trouble? Sign in another way
More information
Accounts
rchoga-azure-ad
Test1@rchoga.onmicrosoft.com
Approve sign-in?
rchoga-azure-ad
Deny
Approve



Problèmes courants

Non-concordance ID entité

Exemple de débogage :

[SAML] consume_assertion : l'identificateur d'un fournisseur est inconnu de #LassoServer. Pour enregistrer un fournisseur dans un objet #LassoServer, vous devez utiliser les méthodes lasso_server_add_provider() ou lasso_server_add_provider_from_buffer() .

Problème : en général, signifie que la commande saml idp [entityID] sous la configuration webvpn de l'ASA ne correspond pas à l'ID d'entité du fournisseur d'identité trouvé dans les métadonnées du fournisseur d'identité.

Solution : Vérifiez l'ID d'entité du fichier de métadonnées du fournisseur d'identités et modifiez la commande saml idp [entity id] pour qu'elle corresponde à ceci.

Non-concordance temporelle

Exemple de débogage :

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Z timeout: 0

[SAML] consume_assertion : assertion expirée ou non valide

Problème 1. Heure ASA non synchronisée avec l'heure du fournisseur d'identité.

Solution 1. Configurez ASA avec le même serveur NTP utilisé par IdP.

Problème 2. L'assertion n'est pas valide entre l'heure spécifiée.

Solution 2. Modifiez la valeur de délai d'attente configurée sur l'ASA.

Certificat de signature IdP incorrect utilisé

Exemple de débogage :

[Lasso] func=xmlSecOpenSLEvpSignatureVerify : file=signatures.c : line=493 : obj=rsa-sha1 : subj=EVP_VerifyFinal : error=18 : les données ne correspondent pas : les signatures ne correspondent pas

[SAML] consume_assertion : le profil ne peut pas vérifier une signature sur le message

Problème : ASA n'a pas pu vérifier le message signé par le fournisseur d'identité ou il n'y a aucune signature à vérifier par l'ASA.

Solution : vérifiez le certificat de signature du fournisseur d'identité installé sur l'ASA pour vous assurer qu'il correspond à ce qui est envoyé par le fournisseur d'identité. Si cela est confirmé, assurez-vous que la signature est incluse dans la réponse SAML.

Audience d'assertions non valide

Exemple de débogage :

[SAML] consume_assertion : assertion audience non valide

Problème : IdP définit l'audience incorrecte.

Solution : corrigez la configuration de l'auditoire sur le fournisseur d'identité. Il doit correspondre à l'ID d'entité de l'ASA.

URL incorrecte pour le service client d'assertion

Exemple de débogage : impossible de recevoir des débogages une fois la demande d'authentification initiale envoyée. L'utilisateur peut entrer des informations d'identification au niveau du fournisseur d'identité, mais ce dernier ne redirige pas vers ASA.

Problème : IdP est configuré pour l'URL du service consommateur d'assertions incorrecte.

Solution(s) : vérifiez l'URL de base dans la configuration et assurez-vous qu'elle est correcte. Vérifiez les métadonnées ASA avec show pour vous assurer que l'URL du service client d'assertion est correcte. Afin de le tester, parcourez-le, Si les deux sont corrects sur l'ASA, vérifiez l'IdP pour vous assurer que l'URL est correcte.

Modifications de la configuration SAML qui ne prennent pas effet

Exemple : une fois qu'une URL d'authentification unique a été modifiée ou modifiée, le certificat SP, SAML ne fonctionne toujours pas et envoie les configurations précédentes.

Problème : ASA doit régénérer ses métadonnées lorsqu'une modification de configuration l'affecte. Il ne le fait pas automatiquement.

Solution : Une fois les modifications apportées, sous le tunnel-group affecté, supprimez et réappliquez la commande saml idp [entity-id].

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

- Authentification unique SAML pour les applications sur site avec le proxy d'application

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.