

Configuration de l'authentification SAML pour SWG avec ADFS et UPN

Table des matières

[Introduction](#)

[Configuration requise pour l'authentification SAML](#)

[Étapes de configuration dans ADFS](#)

[UPN et adresse e-mail](#)

Introduction

Ce document décrit comment configurer l'authentification SAML pour la passerelle Web sécurisée (SWG) à l'aide des services AD FS (Active Directory Federated Services).

Configuration requise pour l'authentification SAML

L'authentification SAML d'Umbrella nécessite que la réponse SAML inclue le userPrincipalName de l'utilisateur final (par exemple, [user@domain.local](#)) en tant que revendication d'ID de nom. Cette exigence s'applique à tous les fournisseurs d'identité. Certains, comme ADFS, nécessitent une configuration manuelle pour inclure cet attribut.

Étapes de configuration dans ADFS

1. Dans ADFS, sélectionnez la Confiance de partie de confiance créée pour Umbrella sous ADFS > Confiances de partie de confiance.
2. Cliquez sur Modifier la stratégie d'émission de demande.
3. Ajoutez une nouvelle règle en utilisant le modèle de revendication Envoyer l'attribut LDAP en tant que revendications.
4. Configurez la règle pour mapper l'attribut userPrincipalName LDAP à l'ID typeName de la revendication sortante SAML.

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

| | LDAP Attribute (Select or type to add more) | Outgoing Claim Type (Select or type to add more) |
|---|---|--|
| ▶ | User-Principal-Name | Name ID |
| * | | |

Capture d'écran_2021-10-20_at_12.33.50.png

5. Enregistrez la configuration.

UPN et adresse e-mail

L'UPN d'un utilisateur (par exemple, [user@domain.local](#)) correspond souvent à son adresse e-mail. Dans certains environnements, l'adresse e-mail (par exemple, [user@externaldomain.tld](#)) diffère de l'UPN.

- Umbrella exige que le fournisseur d'identité envoie la revendication Name IDclaim avec la

valeur UPN.

- Ce nom d'utilisateur doit correspondre à celui fourni dans Déploiements > Utilisateurs et groupes dans Umbrella.
- Les outils de mise en service d'utilisateurs généraux (tels que le connecteur AD) identifient les utilisateurs par leur UPN.

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.