

ADFSおよびUPNを使用したSWGのSAML認証の設定

内容

[はじめに](#)

[SAML認証の要件](#)

[ADFSの設定手順](#)

[UPNと電子メールアドレス](#)

はじめに

このドキュメントでは、Active Directory Federated Services(ADFS)を使用してSecure Web Gateway(SWG)のSAML認証を設定する方法について説明します。

SAML認証の要件

包括SAML認証では、SAML応答でエンドユーザのuserPrincipalName(例: [user@domain.local](#))を名前ID要求として含める必要があります。この要件は、すべてのアイデンティティプロバイダーに適用されます。ADFSなどの一部のデバイスでは、この属性を含めるために手動で設定する必要があります。

ADFSの設定手順

1. ADFSで、Umbrella用に作成された証明書利用者信頼 (「ADFS」 > 「証明書利用者信頼」) を選択します。
2. [要求発行ポリシーの編集]をクリックします。
3. 要求templateSend LDAP Attributeを要求として使用して、新しい規則を追加します。
4. LDAP attributeuserPrincipalNameをSAML出力要求typeName IDにマッピングするようにルールを設定します。

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:

UPN to Name ID

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

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
*		

View Rule Language...

OK

Cancel

スクリーンショット_2021-10-20_at_12.33.50.png

5. 設定を保存します。

UPNと電子メールアドレス

ユーザのUPN(たとえば、[user@domain.local](#))は、多くの場合、ユーザの電子メールアドレスと一致します。環境によっては、電子メールアドレス(たとえば、[user@externaldomain.tld](#))がUPNと異なります。

- Umbrellaでは、アイデンティティプロバイダーがUPN値を含むtheName IDclaimを送信する

必要があります。

- これは、Deployments > Users and Groups in Umbrellaでプロビジョニングされたユーザ名と一致している必要があります。
- Umbrellaユーザプロビジョニングツール（ADコネクタなど）は、UPNによってユーザを識別します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。