

# Konfiguration der SAML-Authentifizierung für SWG mit ADFS und UPN

## Inhalt

---

[Einleitung](#)

[SAML-Authentifizierungsanforderung](#)

[Konfigurationsschritte in ADFS](#)

[UPN und E-Mail-Adresse im Vergleich](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie die SAML-Authentifizierung für Secure Web Gateway (SWG) mithilfe von Active Directory Federated Services (ADFS) konfigurieren.

## SAML-Authentifizierungsanforderung

Bei der Umbrella SAML Authentication muss die SAML-Antwort den userPrincipalName des Endbenutzers (z. B. user@domain.local) als Namen-ID enthalten. Diese Anforderung gilt für alle Identitätsanbieter. Einige, z. B. ADFS, erfordern eine manuelle Konfiguration, um dieses Attribut einzuschließen.

## Konfigurationsschritte in ADFS

1. Wählen Sie in ADFS die Vertrauenspartei für Umbrella unter ADFS > Vertrauenspartei erstellen aus.
2. Klicken Sie auf Richtlinie zur Anspruchsausstellung bearbeiten.
3. Fügen Sie eine neue Regel hinzu, indem Sie die Anspruchsvorlage verwendenLDAP-Attribut als Ansprüche senden.
4. Konfigurieren Sie die Regel so, dass das LDAP-AttributUserPrincipalName der ausgehenden SAML-AnspruchstypName-ID zugeordnet wird.

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
*		

Screenshot\_2021-10-20\_at\_12.33.50.png

5. Speichern Sie die Konfiguration.

## UPN und E-Mail-Adresse im Vergleich

Das UPN eines Benutzers (z. B. [user@domain.local](#)) entspricht häufig der E-Mail-Adresse des Benutzers. In einigen Umgebungen unterscheidet sich die E-Mail-Adresse (z. B. [user@externaldomain.tld](#)) vom UPN.

- Umbrella erfordert, dass der Identitätsanbieter denName-IDclaim mit dem UPN-Wert sendet.

- Dies muss mit dem Benutzernamen übereinstimmen, der in Deployments > Users and Groups (Bereitstellungen > Benutzer und Gruppen in Umbrella) bereitgestellt wird.
- Umbrella User Provisioning Tools (wie der AD Connector) identifizieren Benutzer anhand ihres UPN.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.