Configure SAML Authentication for SWG with ADFS and UPN

Contents

Introduction

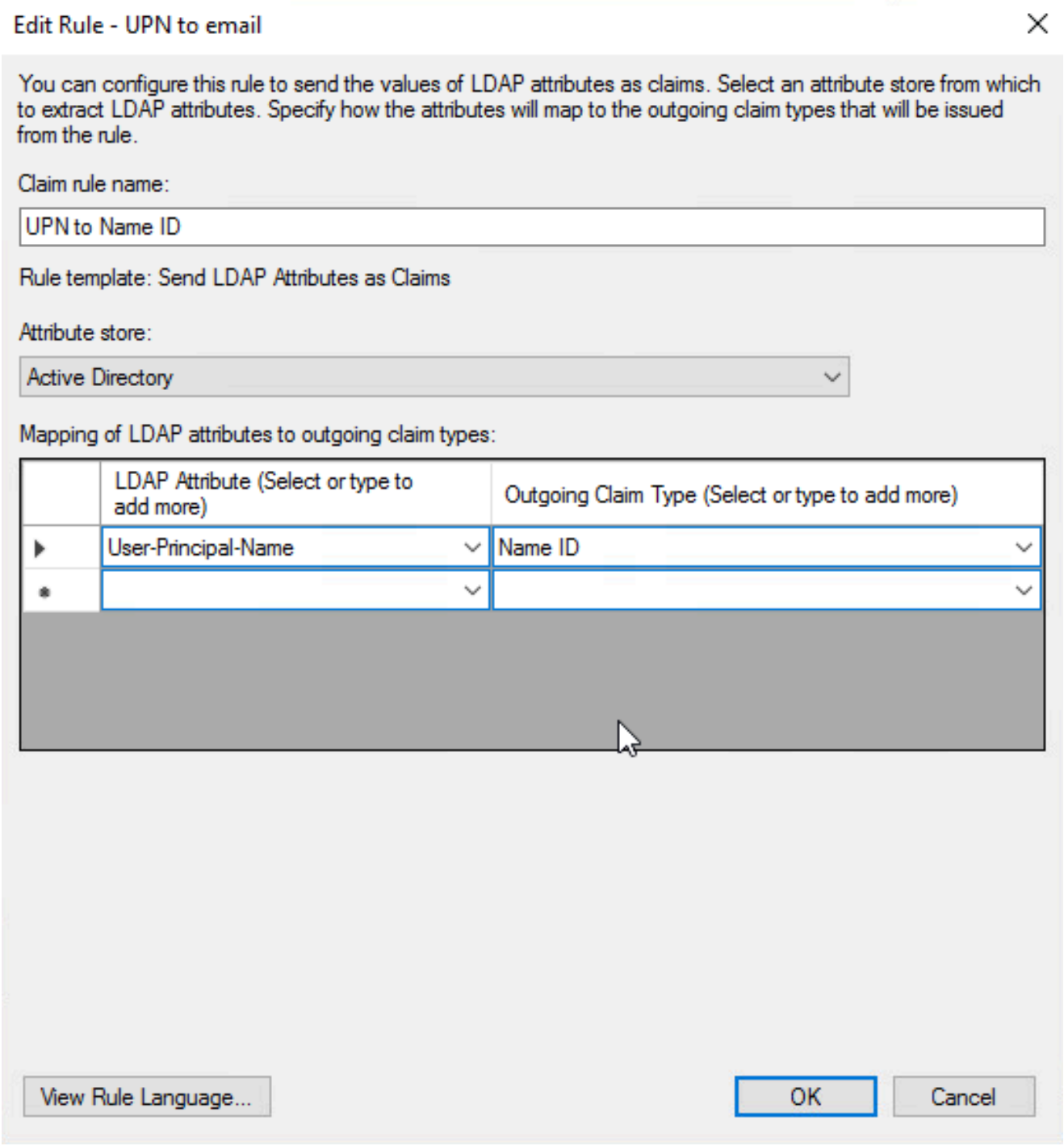
This document describes how to configure SAML authentication for Secure Web Gateway (SWG) using Active Directory Federated Services (ADFS).

Requirement for SAML Authentication

Umbrella SAML authentication requires the SAML response to include the end user's userPrincipalName (for example, user@domain.local) as the Name ID claim. This requirement applies to all Identity Providers. Some, such as ADFS, require manual configuration to include this attribute.

Configuration Steps in ADFS

1. In ADFS, select the**Relying Party Trust**created for Umbrella under**ADFS > Relying Party Trusts**.
2. Click**Edit Claim Issuance Policy**.
3. Add a new rule using the claim template**Send LDAP Attribute as claims**.
4. Configure the rule to map the LDAP attribute**userPrincipalName**to the SAML outgoing claim type**Name ID**.



Screenshot_2021-10-20_at_12.33.50.png

5. Save the configuration.

UPN Versus E-Mail Address

A user's UPN (for example, user@domain.local) often matches the user's e-mail address. In some environments, the e-mail address (for example, user@externaldomain.tld) differs from the UPN.

- Umbrella requires the Identity Provider to send the**Name ID**claim with the UPN value.
- This must match the username provisioned in**Deployments > Users and Groups**in Umbrella.
- Umbrella user provisioning tools (such as the AD Connector) identify users by their UPN.