使用ADFS和UPN配置SWG的SAML身份驗證

目錄

簡介

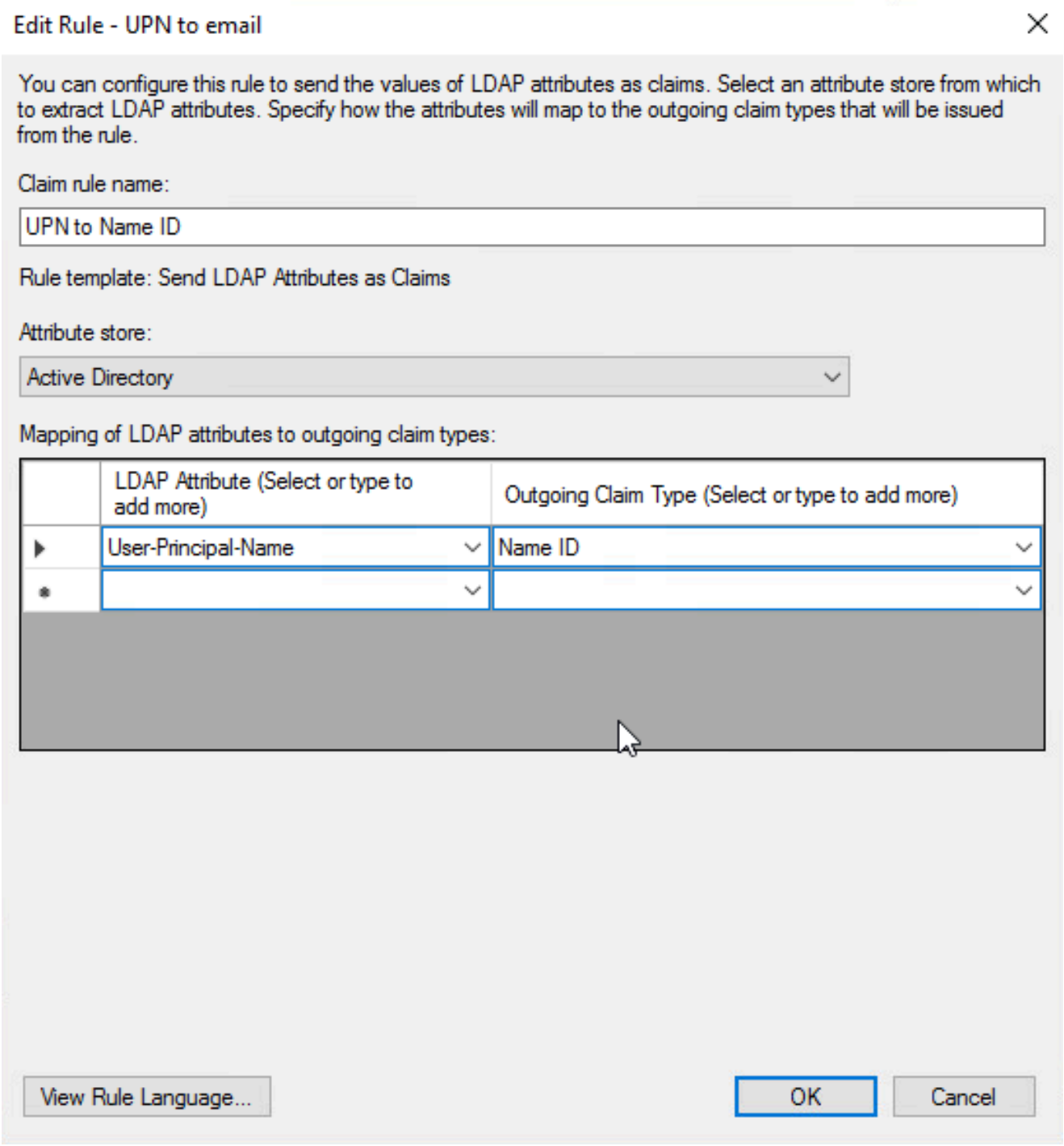
本文檔介紹如何使用Active Directory聯合服務(ADFS)為安全Web網關(SWG)配置SAML身份驗證。

SAML身份驗證的要求

Umbrella SAML身份驗證要求SAML響應將終端使用者的userPrincipalName(例如，user@domain.local)包含為Name ID宣告。此要求適用於所有身份提供程式。某些屬性（例如ADFS）需要手動配置才能包含此屬性。

ADFS中的配置步驟

1. 在ADFS中，在ADFS > Reliing Party Trusts下，選擇為Umbrella建立的信賴方信任。
2. 按一下編輯宣告頒發策略。
3. 使用宣告模板新增新規則將LDAP屬性作為宣告傳送。
4. 配置規則以將LDAP屬性userPrincipalName對映到SAML傳出宣告型別Name ID。



螢幕截圖_2021-10-20_at_12.33.50.png

5. 儲存組態。

UPN與電子郵件地址

使用者的UPN(例如，user@domain.local)通常與使用者的電子郵件地址匹配。在某些環境中，電子郵件地址(例如user@externaldomain.tld)與UPN不同。

- Umbrella要求身份提供程式發送具有UPN值的Name IDclaim。
- 此使用者名稱必須與Deployments > Users and Groupsin Umbrella中設定的使用者名匹配。

- Umbrella使用者調配工具（如AD聯結器）通過UPN識別使用者。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。