ADFS 및 UPN을 사용하여 SWG에 대한 SAML 인증 구성

목차

소개

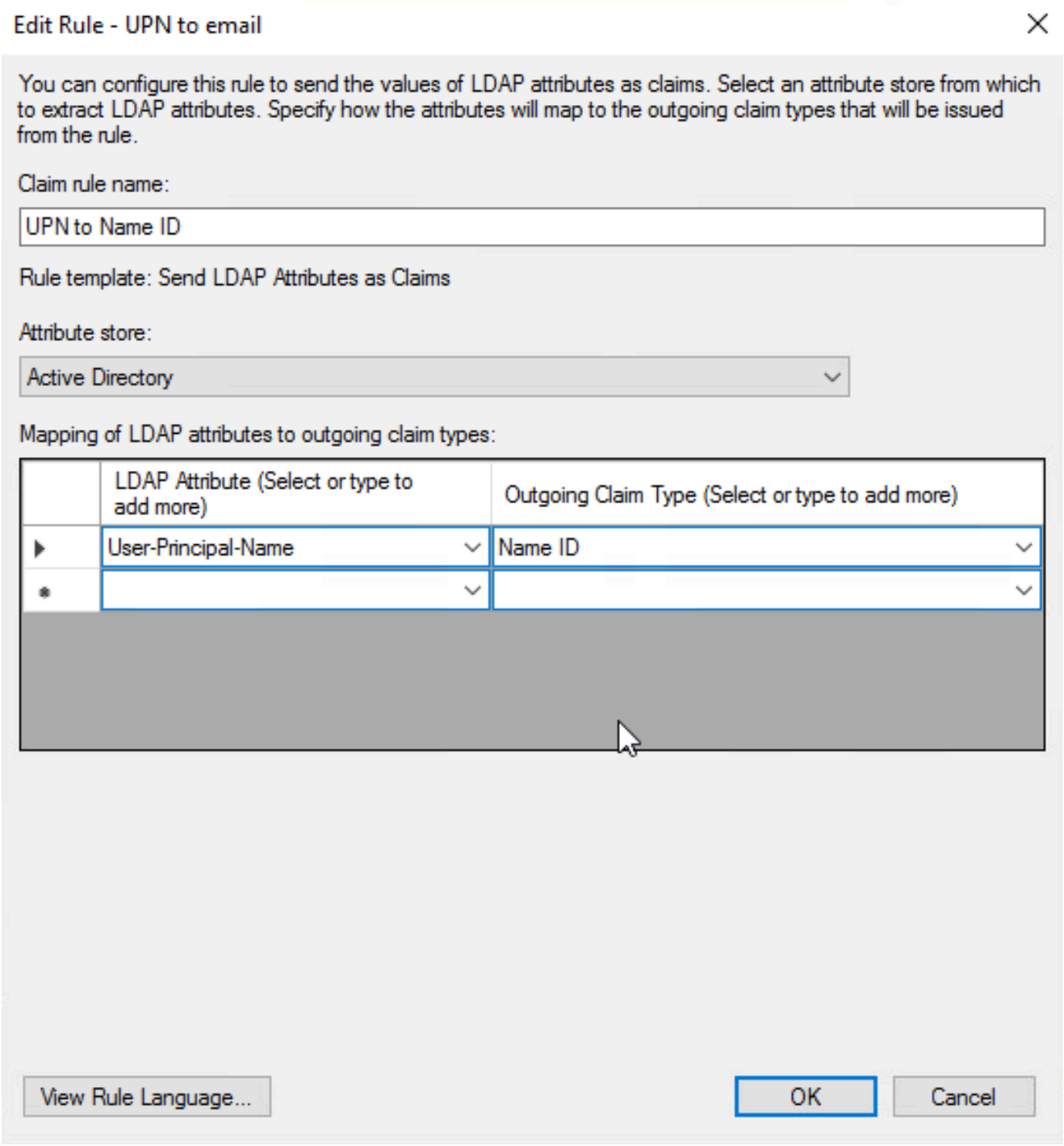
이 문서에서는 ADFS(Active Directory Federated Services)를 사용하여 SWG(Secure Web Gateway)에 대한 SAML 인증을 구성하는 방법에 대해 설명합니다.

SAML 인증 요구 사항

Umbrella SAML 인증에서는 최종 사용자의 userPrincipalName(예: user@domain.local)을 Name ID 클레임으로 포함하려면 SAML 응답이 필요합니다. 이 요구 사항은 모든 ID 제공자에 적용 됩니다. ADFS와 같은 일부 기능은 이 특성을 포함하도록 수동 컨피그레이션이 필요합니다.

AD FS의 컨피그레이션 단계

1. AD FS의 AD FS > Relying Party Trusts(신뢰 당사자 트러스트)에서 Umbrella에 대해 생성된 신뢰 당사자 트러스트를 선택합니다.
2. Edit Claim Issuance Policy를 클릭합니다.
3. 클레임 템플릿LDAP 특성을 클레임으로 보내기를 사용하여 새 규칙을 추가합니다.
4. LDAP attributeuserPrincipalName을 SAML 발신 클레임 유형Name ID에 매핑하도록 규칙을 구성합니다.



스크린샷_2021-10-20_at_12.33.50.png

5. 설정 저장.

UPN 대 전자 메일 주소

사용자의 UPN(예: user@domain.local)은 종종 사용자의 이메일 주소와 일치합니다. 일부 환경에서는 이메일 주소(예: user@externaldomain.tld)가 UPN과 다릅니다.

- Umbrella에서는 ID 공급자가 UPN 값과 함께 Name IDclaim을 전송해야 합니다.
- 이는 Deployments(구축) > Users and Groups in Umbrella(Umbrella의 사용자 및 그룹)에서

프로비저닝된 사용자 이름과 일치해야 합니다.

- Umbrella 사용자 프로비저닝 툴(예: AD 커넥터)은 UPN을 통해 사용자를 식별합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.