使用ADFS和UPN配置SWG的SAML身份验证

目录

简介

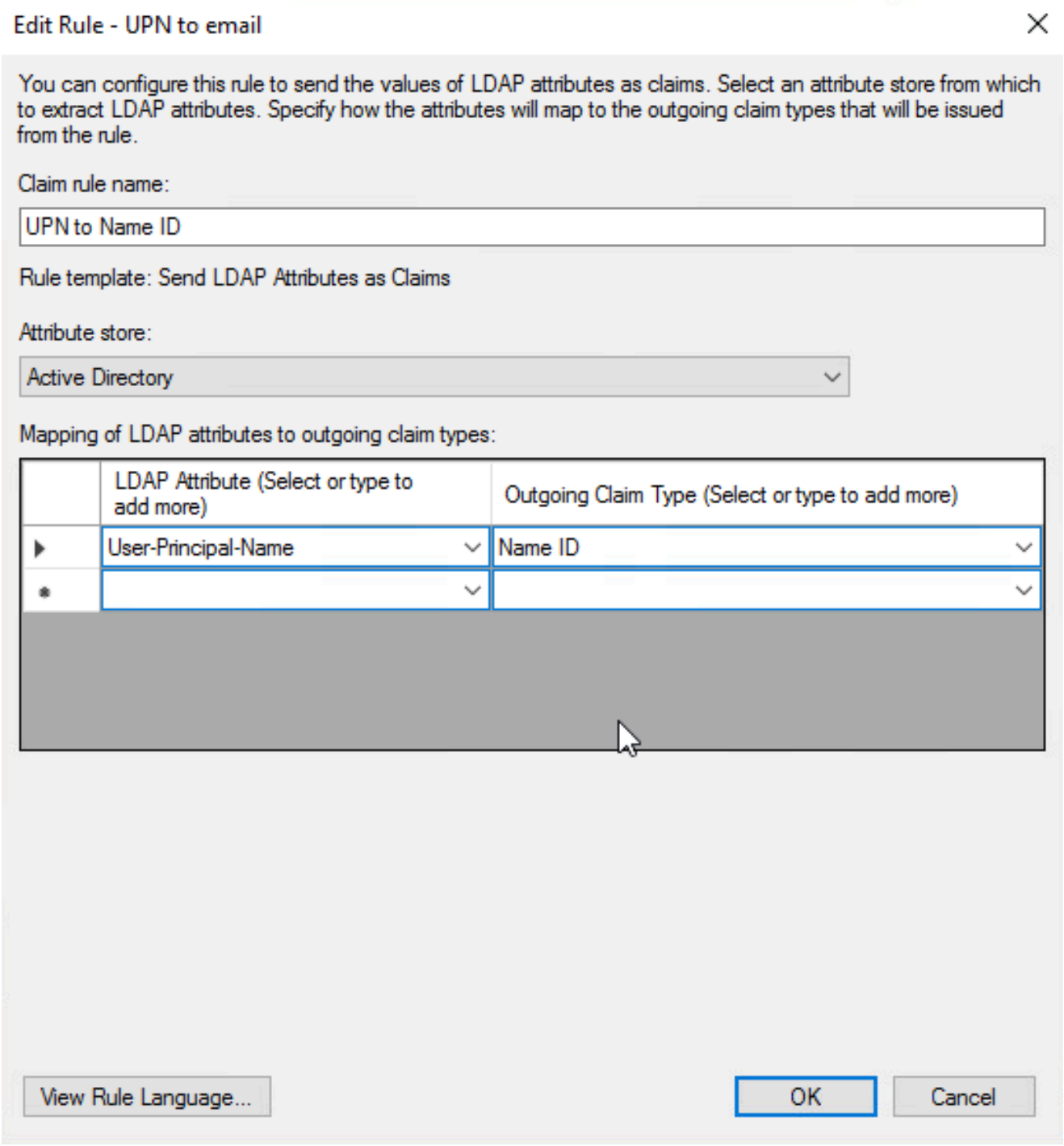
本文档介绍如何使用Active Directory联合服务(ADFS)为安全网络网关(SWG)配置SAML身份验证。

SAML身份验证的要求

Umbrella SAML身份验证要求SAML响应将最终用户的用户userPrincipalName(例如，user@domain.local)作为名称ID声明。此要求适用于所有身份提供程序。有些设备（例如ADFS）需要手动配置才能包括此属性。

ADFS中的配置步骤

1. 在ADFS中，在ADFS > Relying Party Trusts下，选择为Umbrella创建的信赖方信任。
2. 点击Edit Claim Issuance Policy。
3. 使用声明模板添加新规则将LDAP属性作为声明发送。
4. 配置规则以将LDAP属性userPrincipalName映射到SAML传出声明typeName ID。



屏幕截图_2021-10-20_at_12.33.50.png

5. 保存配置。

UPN与电子邮件地址

用户的UPN(例如，user@domain.local)通常与用户的电子邮件地址匹配。在某些环境中，电子邮件地址(例如user@externaldomain.tld)与UPN不同。

- Umbrella要求身份提供程序发送带有UPN值的Name IDclaim。
- 这必须与Deployments > Users and Groupsin Umbrella中设置的用户名匹配。

- Umbrella用户调配工具（如AD连接器）通过用户的UPN识别用户。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。