为ESA和SMA配置Duo IdP SAML SSO

目录

简介

本文档介绍如何为Cisco ESA和SMA的SAML SSO配置Duo Access Gateway。

环境

- Cisco ESA/SMA:AsyncOS最新版本
- Duo接入网关：可从ESA/SMA管理接口部署和访问
- 身份验证源：Active Directory、OpenLDAP、Azure AD或其他SAML身份提供程序（用于属性映射）

问题

本文档仅介绍双端配置。它不包括Cisco ESA/SMA服务提供商(SP)配置。

先决条件

术语

- 身份提供程序(IdP)
- 单点登录(SSO)
- 邮件安全设备(ESA)
- 安全管理设备(SMA)
- 断言消费者服务(ACS)
- 服务提供商(SP)

要求

开始使用前:

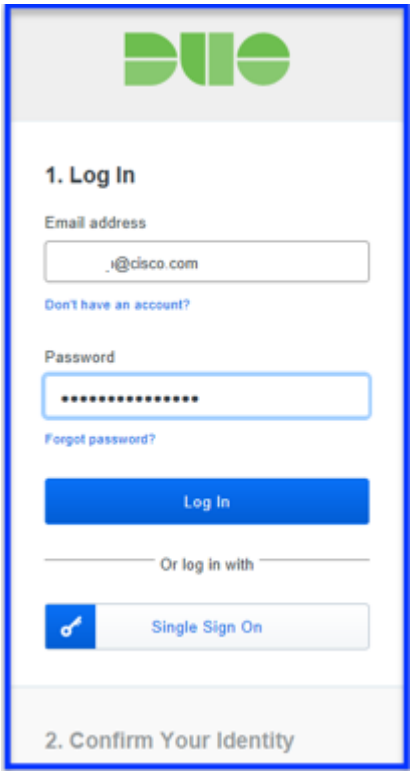
- 确保已部署Duo接入网关并已配置身份验证源。
- 使用已配置的身份验证源部署Duo接入网关。
- 如果不支持多个Assertion Consumer Service(ACS)URL，Duo可能需要为每个ESA提供单独的应用程序。

配置包括两个阶段：

1. 配置Duo云应用。
2. 将新的云应用添加到Duo接入网关。

创建云应用

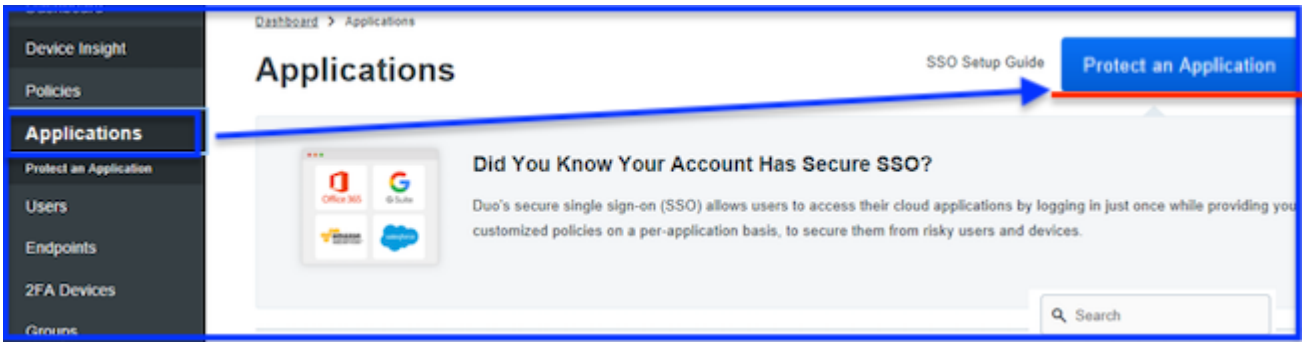
1.登录https://admin.duosecurity.com/。



duo.com

duo.com

2.定位至“应用程序”>“保护应用程序”。

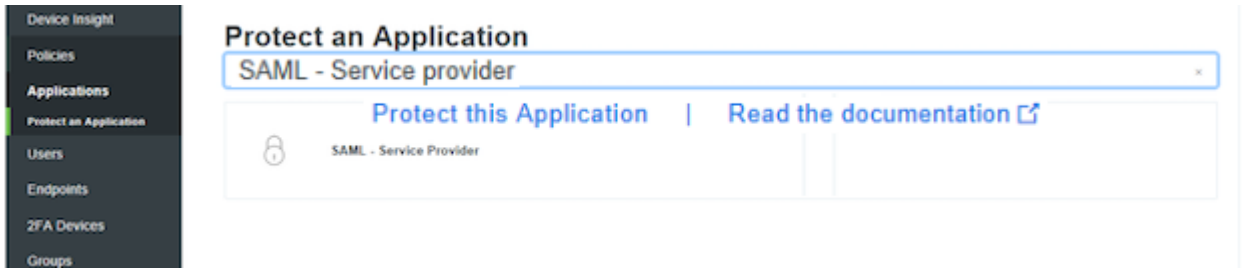


保护应用

保护应用

3.搜索SAML — 服务提供商。

4.出现SAML图标时，选择保护此应用程序。



保护此应用程序

保护此应用程序

5.填写服务提供商配置文件：

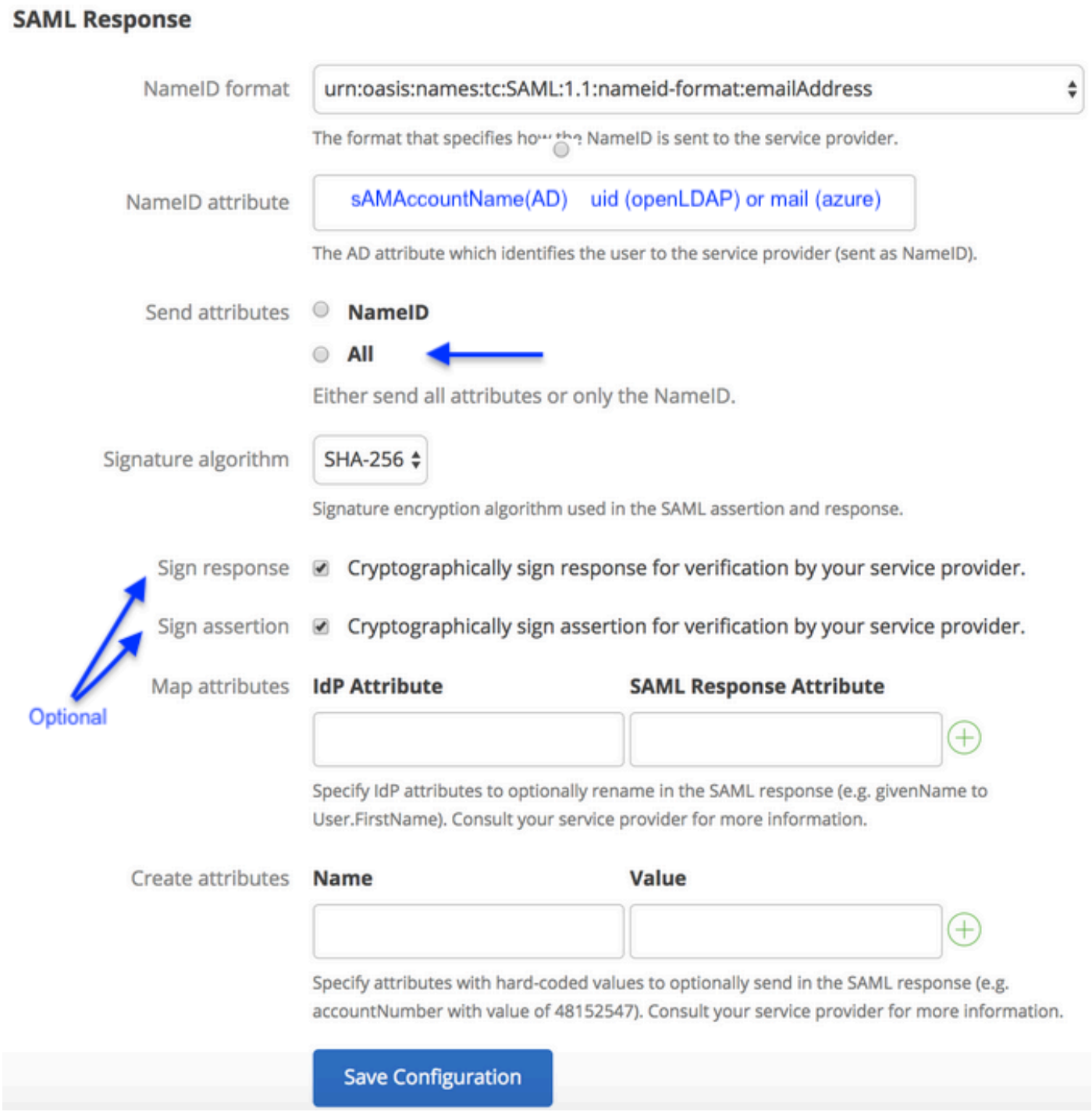
- 服务提供商名称：输入您选择的名称。
- 实体ID:输入用于标识ESA/SMA的公用名称。
- 断言消费者服务：输入可访问的ESA/SMA URL。

6.根据身份验证源使用以下NameID属性值：

属性	Active Directory	OpenLDAP	SAML身份提供程序(IdP)	Azure AD
邮件属性	邮件	邮件	邮件	邮件
用户名属性	sAMAccountName	uid	邮件	邮件
名字属性	给定名称	gn	给定名称	给定名称
姓氏属性	sn	sn	sn	姓

- 发送属性是可选的。选择NameID或ALL。
- 签名响应和签名断言是可选的。IdP和SP上的这些设置必须匹配。

7.选择保存配置。



SAML响应

SAML响应

8.最后，下载配置文件。

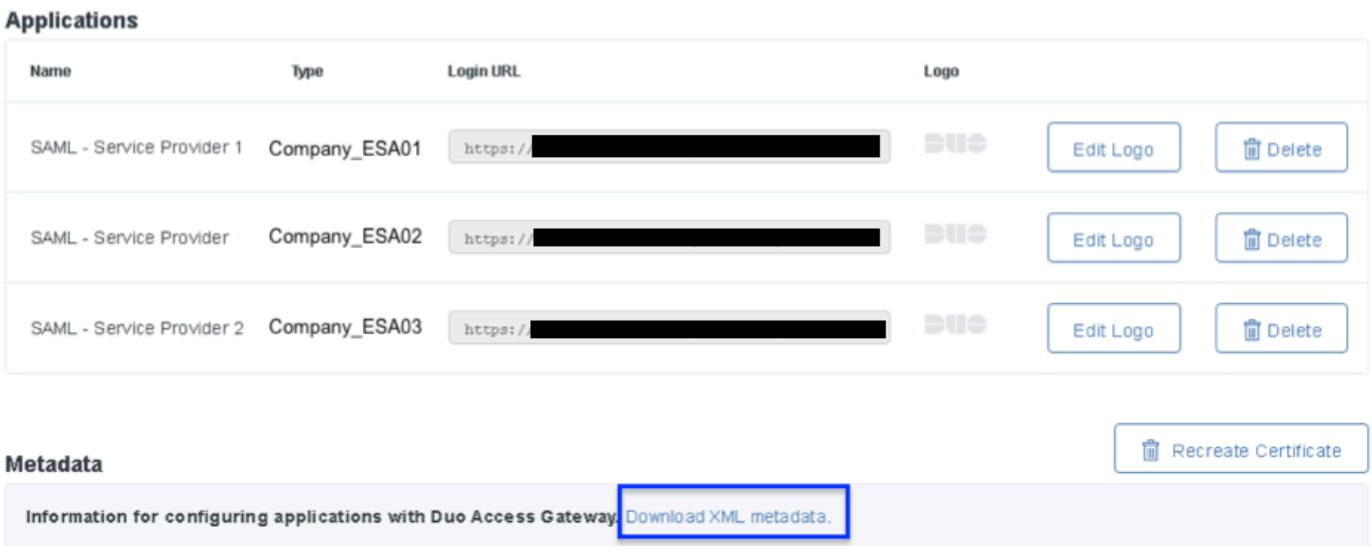
向Duo接入网关添加新的云应用

1.登录到Duo接入网关。

2.定位至应用>添加应用>配置文件>选择文件。

3.选择在步骤1中创建的应用程序配置，然后选择UPLOAD。

4.下载XML元数据，作为IdP配置用于SP主机。



应用视图和下载XML元数据

应用视图和下载XML元数据

5.返回ESA/SMA以完成SAML SSO配置。

- 预期结果：创建了Duo Access Gateway应用程序，IdP XML元数据已准备好导入到ESA/SMA。

6.在后续的ESA/SMA流程中使用下载的元数据。

后续步骤（ESA/SMA配置）

本文仅介绍双端配置。要在ESA/SMA上完成设置，请按照说明操作。

确认

- 确认应用程序显示在Applications下的Duo Access Gateway中。
- 确认IdP XML元数据已成功下载，并且已准备好在ESA/SMA上导入。

相关信息

- SAML SSO的双核文档

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）。