使用AD FS为ESA和SMA配置SAML SSO外部身份验证

目录

简介

本文档介绍如何将Active Directory联合身份验证服务配置为SAML身份提供程序，以便在Cisco ESA和SMA上进行外部身份验证。

先决条件

本文档提供了工程师无法以其他方式看到的第三方应用程序的视图。

- 思科邮件安全设备(ESA)和安全管理设备(SMA)最新版本的安全声明标记语言(SAML)外部身份验证配置步骤，使用Active Directory联合身份验证服务(AD FS)2012和2016。
- 基于实验室的基本步骤，不包括专门部署特定的配置。
- 不同于生产部署的实验室环境的工作示例。

⚠ 警告：在此过程之前完成服务提供商(SP)配置。请参阅。

要求

- Microsoft Active Directory联合身份验证服务(AD FS)2012或2016
- 思科邮件安全设备(ESA)和安全管理设备(SMA)最新版本。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

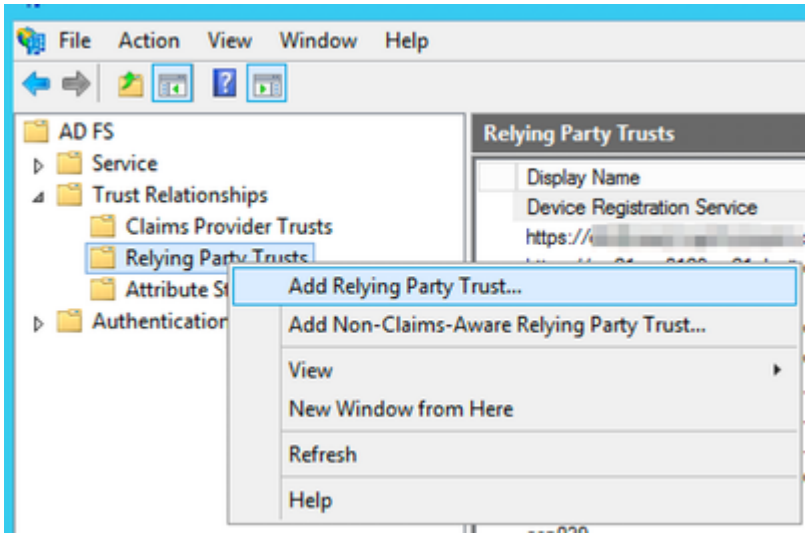
SAML的ADFS IDP配置步骤

配置信赖方信任

使用两个选项之一在AD FS中创建信赖方信任。

方法 A：通过导入SP元数据创建信赖方信任

1. 从管理工具打开AD FS Management控制台。
2. 在AD FS管理控制台中，展开Trusted Relationships，右键单击Relying Party Trusts，然后选择Add Relying Party Trust。



添加信赖方信任

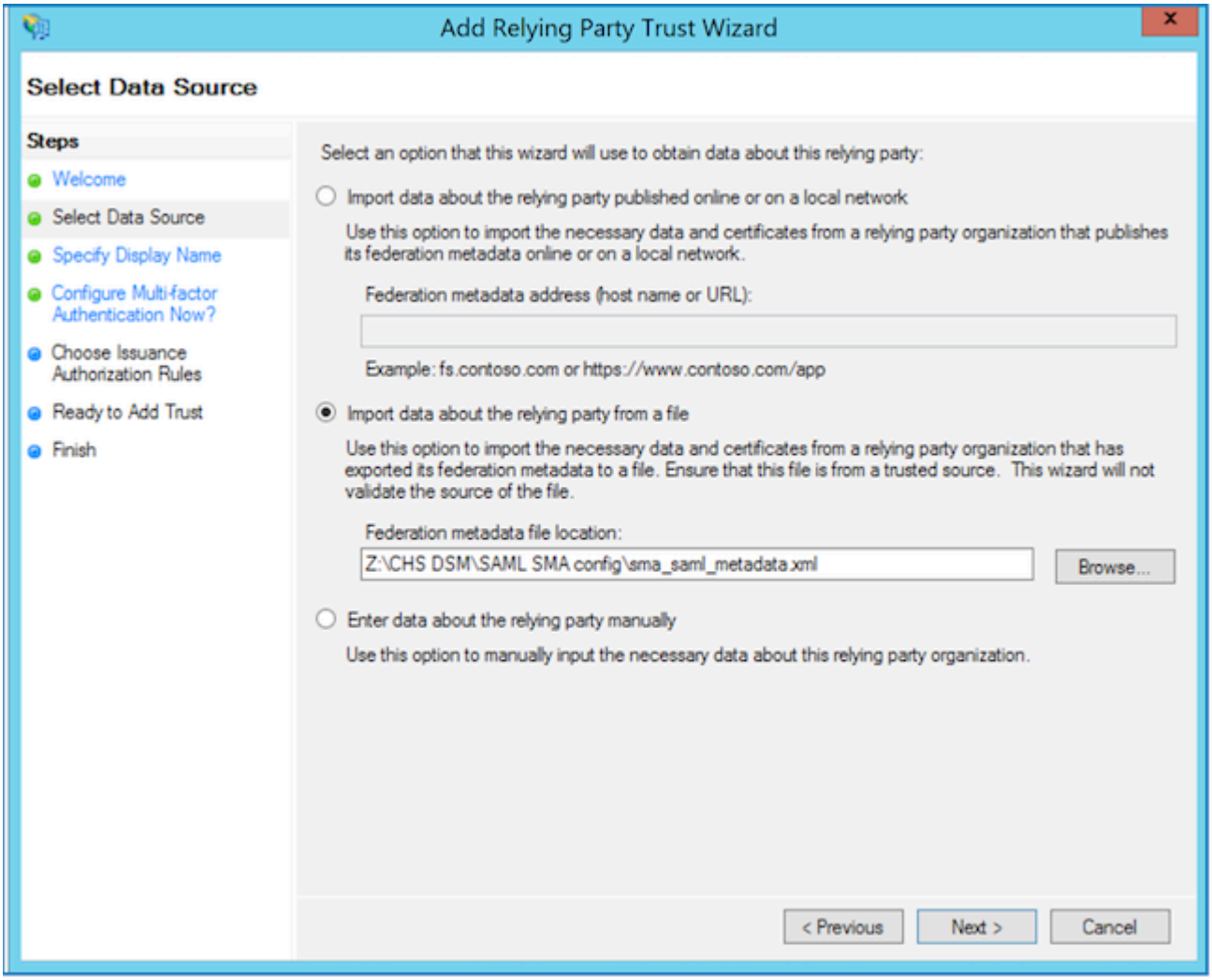
提示：Microsoft信赖方信任

使用以下两个选项之一继续操作：

- 方案 A：从文件导入有关信赖方的数据。上传ESA或SMA服务提供商(SP)metadata.xml文件。
- 方案 B：手动输入有关信赖方的数据。此选项将引导您完成手动配置。

方案 A：从文件导入有关信赖方的数据。上传ESA或SMA服务提供商(SP)metadata.xml文件。

1. 选择选项以从文件导入关于信赖方的数据，然后选择下一步。



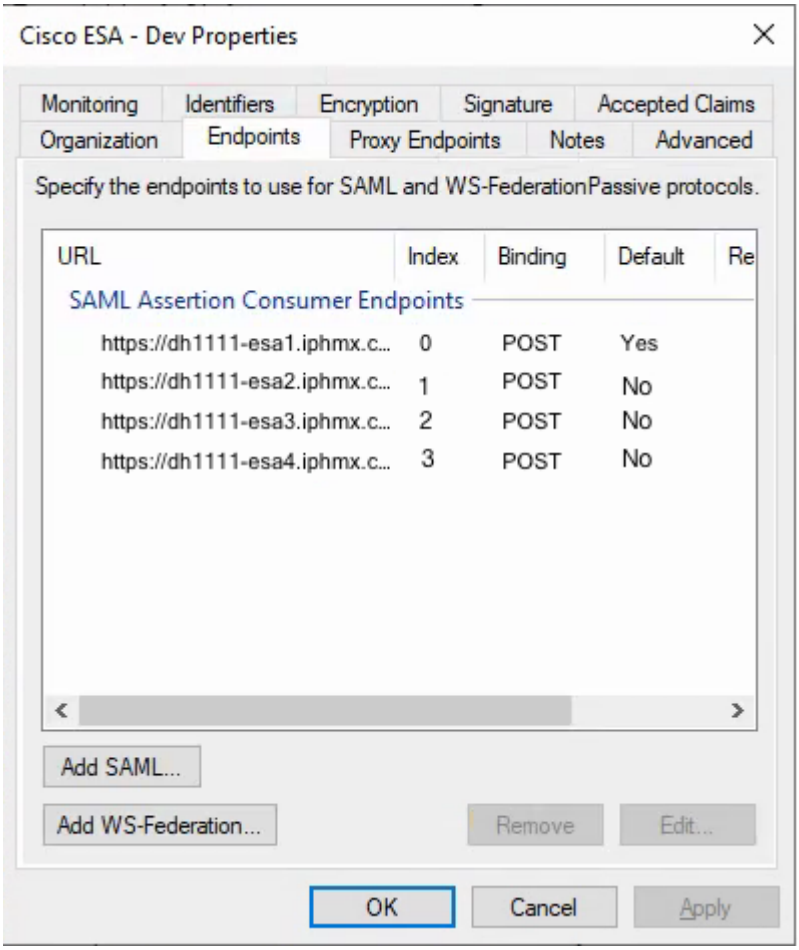
导入ESA/SMA元数据文件

- 指定显示名以标识此信赖方信任，然后选择Next两次。
- 对于颁发授权规则，请选择Permit all users，然后选择Next。
- 在Ready to Add Trust页面上，接受默认设置，然后选择Next。
- 选择完成。这将打开信赖方信任的“编辑声明规则”对话框，该对话框在Issuance Transform Rules - Claims中介绍。

信赖方信任属性 — 终端

仅当集群中存在多个ESA时才执行此步骤。

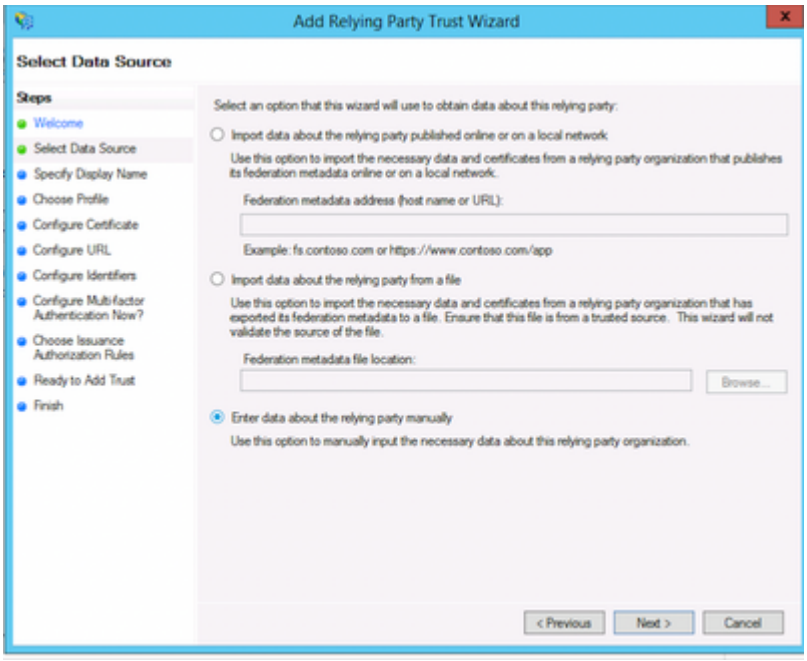
1. 打开信赖方信任属性>端点。
2. 添加每个ESA可访问URL地址，然后选择确定。
3. 索引值从0开始计数，即0、1、2和3。
4. 仅将一个条目设置为Default = Yes。
5. 将剩余条目设置为Default = No。



信赖方信任属性 — 终端

方案 B：手动输入有关信赖方的数据。此选项将引导您完成手动配置。

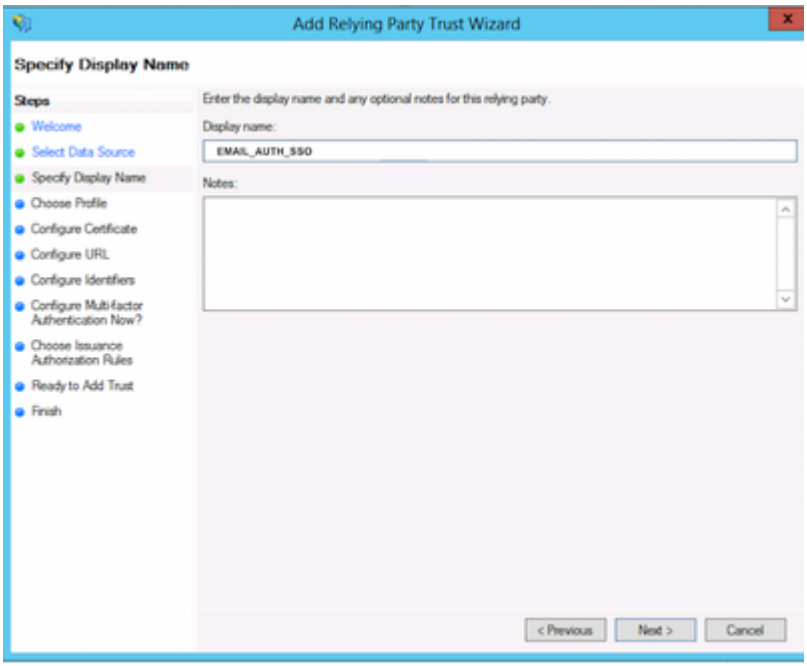
1. 选择手动输入关于信赖方的数据。



手动添加信赖方

提示：Display Name（显示名称）是您选择用于标识ESA或SMA SAML信赖方信任的名称。

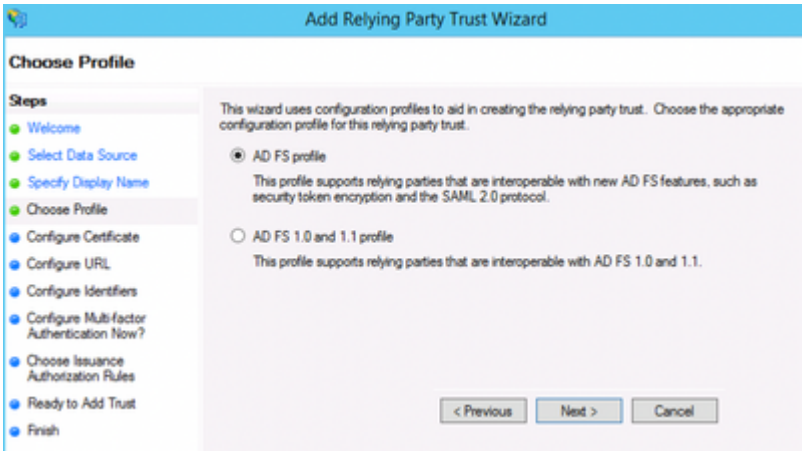
1. 输入服务提供商的显示名称，例如ESA_SP。



为服务提供商配置文件创建名称

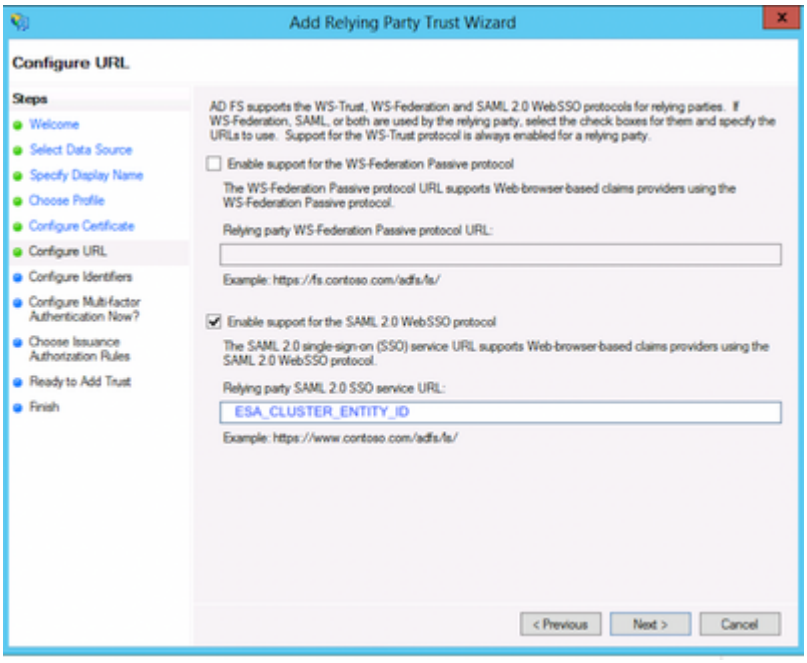
提示：索赔规则和签发转换规则的作用

1. 选择配置文件选项AD FS配置文件。



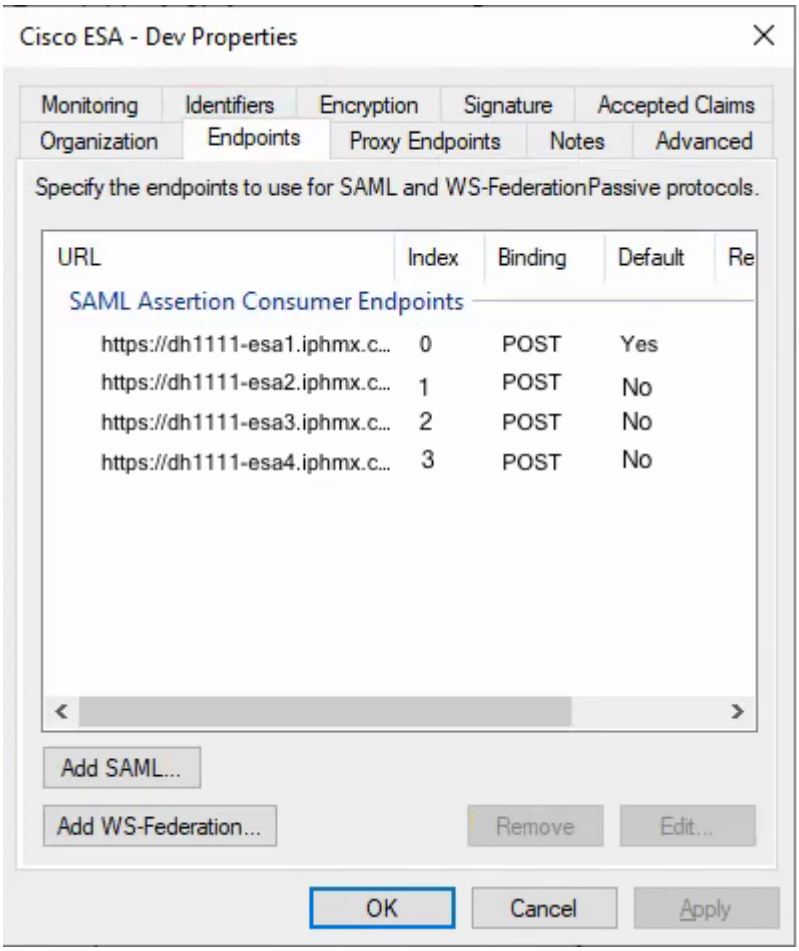
使用SAML 2.0的AD FS配置文件选项

1. 从ESA服务提供商(SP)配置加载公共证书。
2. 对于Configure URL，选择Enable support for the SAML 2.0 single-sign-on(SSO)。
3. 输入具有SP配置文件实体ID值的信赖方SAML 2.0 SSO服务URL。



颁发授权规则 — 允许所有用户

1. 对于颁发授权规则，请选择允许所有用户访问此信赖方。



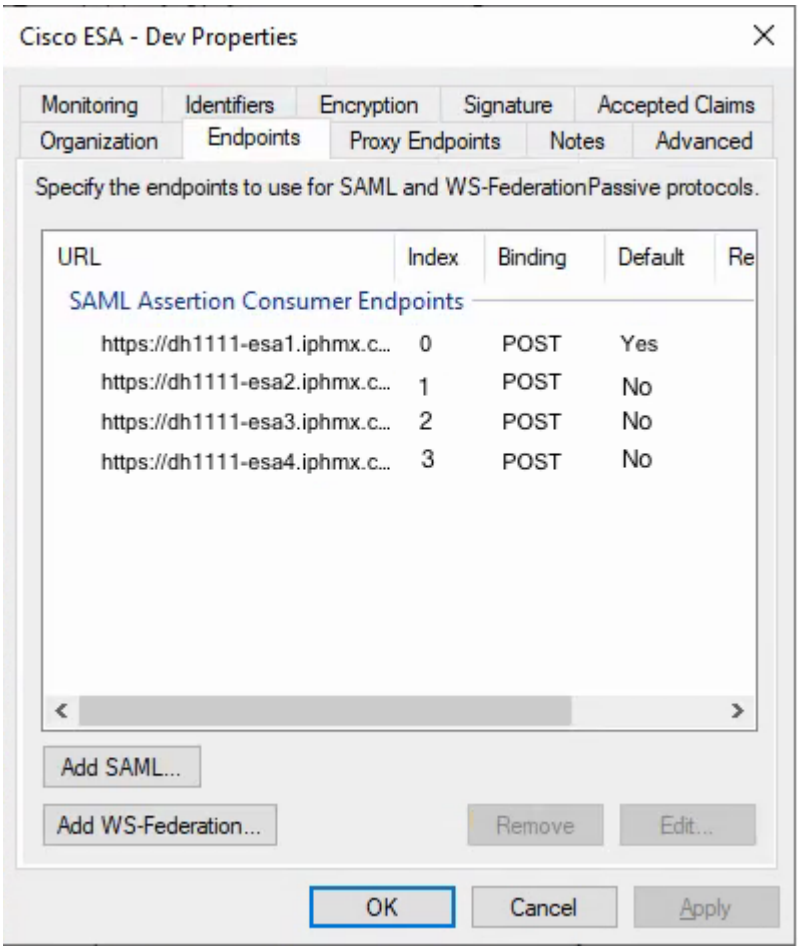
选择Issuance Authorization Rules

1. 选择下一步以转到“完成”页。

配置信赖方信任终端（仅集群）

仅当集群中存在多个ESA时才执行此步骤。

1. 打开信赖方信任属性>端点。
2. 添加每个ESA可访问URL地址，然后单击OK。
3. 设置从0开始的endpoint索引值（例如0、1、2、3）。
4. 仅将一个终端设置为Default = Yes。将剩余终端设置为Default=否

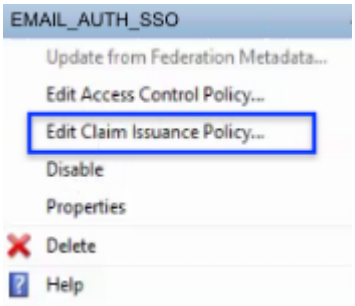


颁发授权规则 — 允许所有用户

- “完成”步骤将启动“编辑声明规则”对话框，供信赖方信任使用（在Issuance Transform Rules中介绍）。

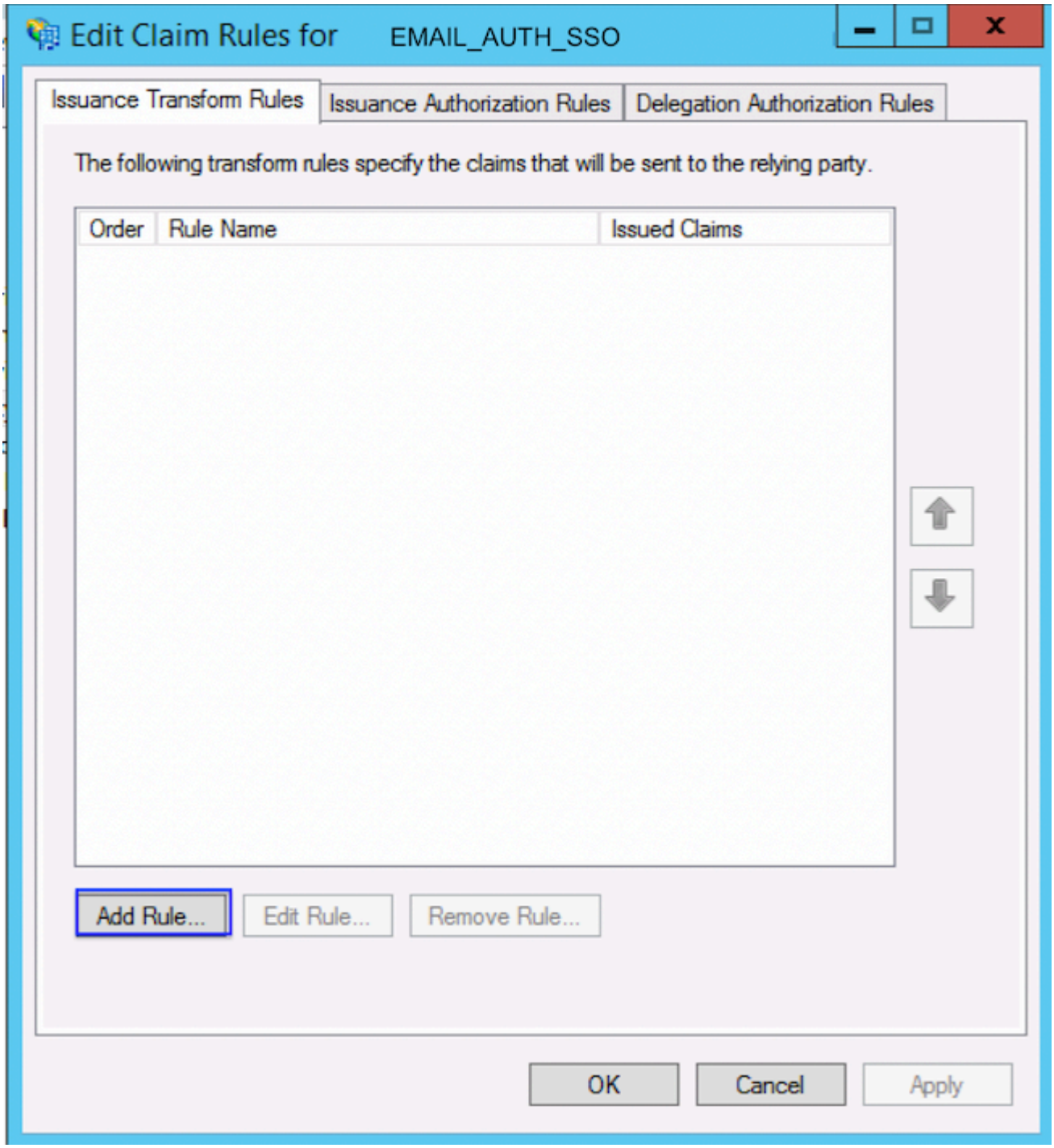
颁发转换规则 — 领款申请

- 选择Edit Claims Issuance Policy。



编辑领款申请颁发策略

- 选择Add Rule。

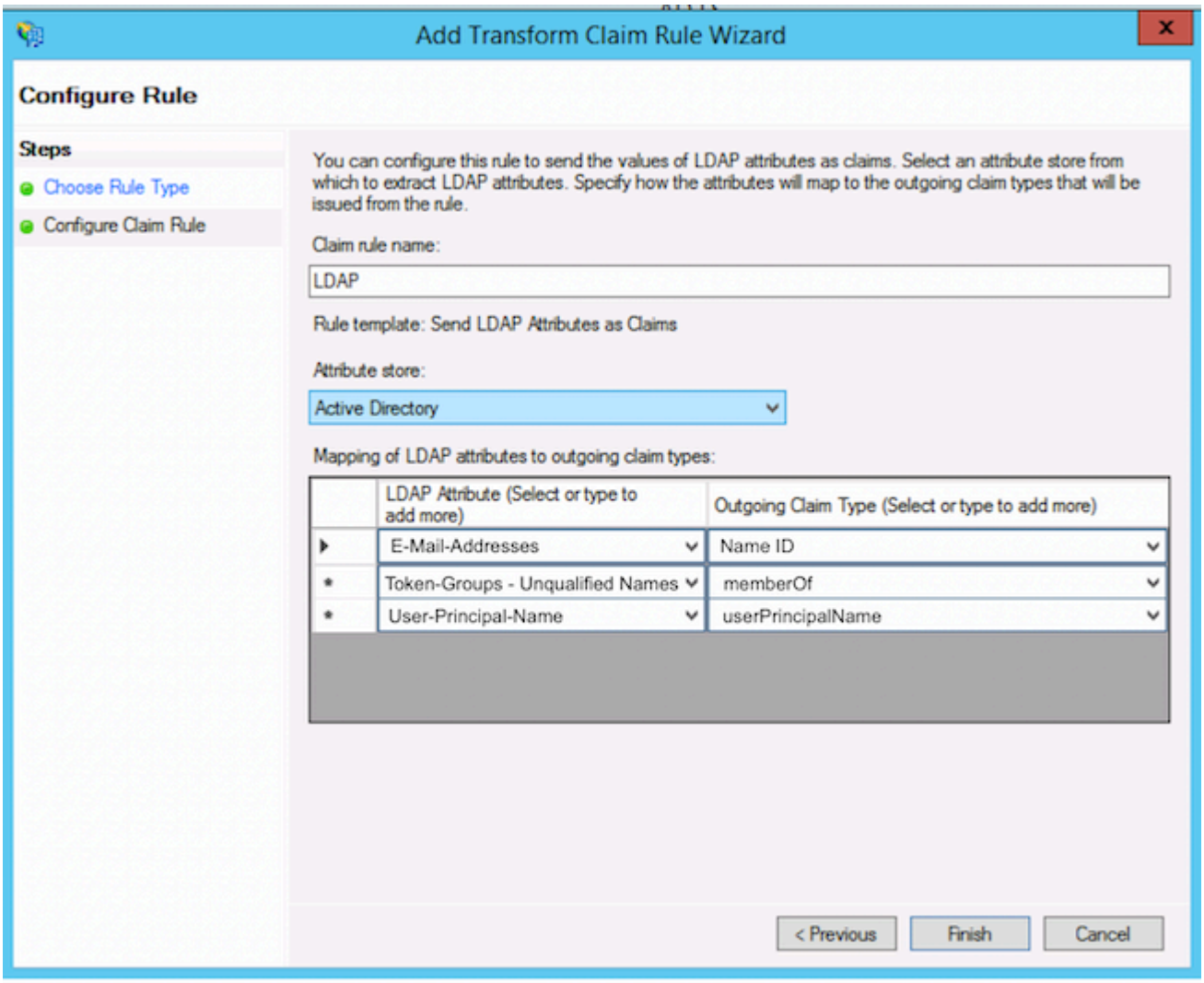


添加颁发转换规则

此处显示的值是允许ESA在外部身份验证设置中填充组名称的通用值。

提示：映射中的值可能因管理员首选项而异。

提示：在列出的示例中，手动输入传出声明类型memberOf和userPrincipalName。从下拉列表中选择Name ID。



转换领款申请规则

- 选择完成。

下载IdP元数据并将其上传到ESA

完成信赖方信任和声明规则配置后，导出身份提供程序(IdP)元数据，并将其上传到ESA。

⚠ 警告：重新启动AD FS服务可能会中断活动的身份验证会话。如果需要，请在维护时段执行此步骤。

- 如果需要，请重新启动AD FS服务。
- 运行以下命令：

```
net stop adfssrv
net start adfssrv
```

- 从此URL下载元数据文件：

https://myserver.domain.com/FederationMetadata/2007-06/FederationMetadata.xml

- 完成并返回ESA集群。

验证

1. 在ESA或SMA中，确认IdP元数据导入成功完成。
2. 使用SAML单点登录(SSO)测试管理登录。
3. 确认已收到预期组声明，且角色映射已按预期填充到外部身份验证配置中。

相关信息

-
- 思科邮件安全设备 — 最终用户指南
- 思科内容安全管理设备 — 最终用户指南

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）。