使用SAML为Umbrella配置ADFS版本3.0

目录

简介

本文档介绍如何在Cisco Umbrella和Active Directory联合服务(ADFS)版本3.0之间配置SAML。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

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。

概述

本文解释如何在Cisco Umbrella和Active Directory联合服务(ADFS)版本3.0之间配置SAML。使用ADFS配置SAML与Umbrella的其他SAML集成不同，因为它不是向导中的一个或两个点击过程，但需要在ADFS中进行更改才能正常工作。

本文包含为了使SAML和ADFS协同工作而必须做出的详细修改。主要步骤是首先在ADFS环境和Cisco Umbrella之间禁用加密，然后将一些Issuance Transform Custom Claim Rules添加到Umbrella中继方设置。

仅对现有的有效ADFS设置执行这些步骤。Cisco Umbrella支持无法提供帮助或支持，以帮助在特定环境中配置ADFS。

目前这些说明仅支持ADFS 3.0版(Windows Server 2012 R2)。ADFS的早期（2.0或2.1）或晚期(4.0)版本可以与Umbrella SAML集成配合使用，但这一点尚未经过测试或验证。如果您有不同版本的ADFS，并且有兴趣与我们的支持和产品团队合作进行集成，请联系Cisco Umbrella支持。

您可以在Umbrella文档中查找初始SAML设置的必备条件：身份集成：前提条件。完成这些步骤后，您可以继续使用本文中针对ADFS的说明来完成配置。

Umbrella文档中的步骤提及您需要将SAML(ADFS)元数据上传到Umbrella。通过导航到此URL，然后上传XML文件，可以访问元数据。

```
https://{your-ADFS-domain-name}/federationmetadata/2007-06/federationmetadata.xml
```

禁用加密

1.打开AD FS管理。展开信任关系并选择信赖方信任。

2.右键单击Umbrella信赖方（或您为其命名的任意对象），然后选择属性。

3.选择加密选项卡。

4.选择删除以删除要加密的证书。

5.选择确定关闭屏幕。

添加新的颁发转换声明规则

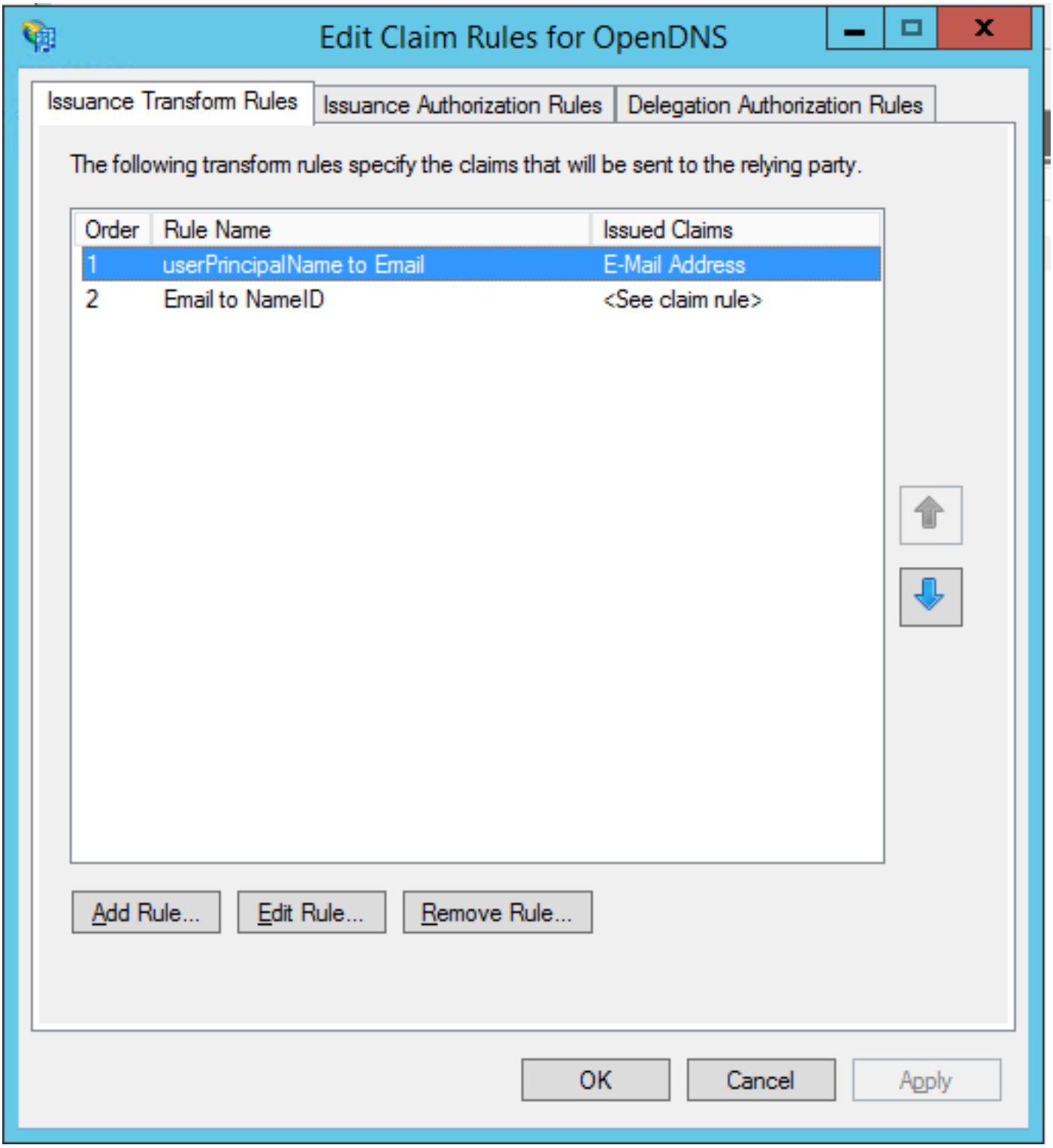
1.打开AD FS管理。展开信任关系并选择中继方信任。

2.右键单击Umbrella中继方（或您为其命名的任意方），然后选择“编辑声明规则”。

3.在Issuance Transform Rules下，选择Add Rule。

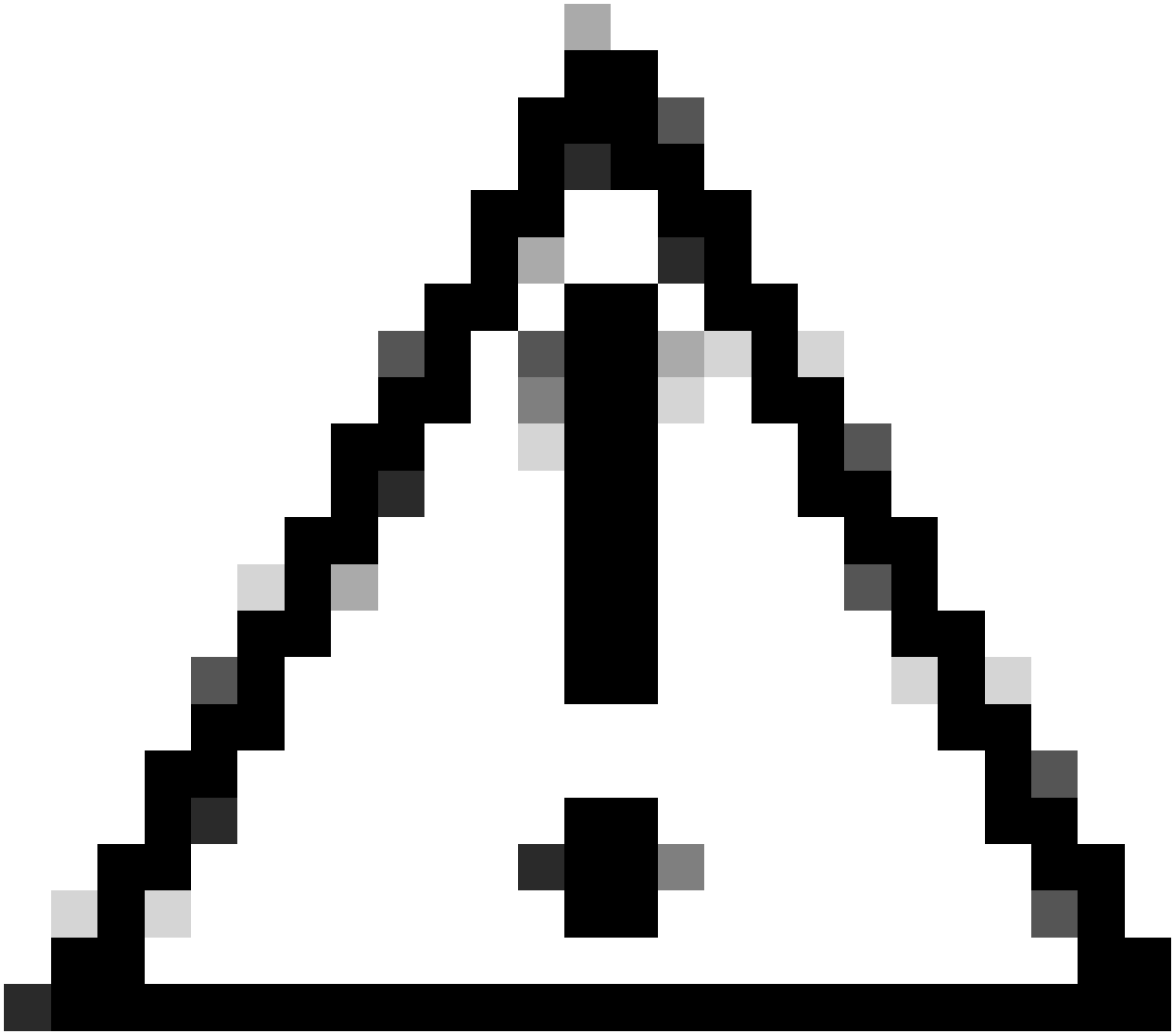
4.选择“使用自定义规则发送索赔”。

查看此屏幕截图，查看可添加的规则列表。



添加这些规则后，集成即可开始工作。

转换规则



警告：这些规则已经过测试，并在Umbrella的ADFS实验室环境中以及一些客户生产环境中运行。请根据您的环境进行修改。

---

userPrincipalName到电子邮件地址

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em
```

发送到名称ID的电子邮件

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

附录：使用“mail”属性登录

默认情况下，ADFS通过用户的UPN（用户主体名称）对用户进行身份验证。 如果您的用户的电子邮件地址（Umbrella帐户名称）与其UPN不匹配，则需要执行其他步骤。请参阅此知识库文章：如何在Cisco Umbrella控制面板中配置AD FS以允许使用电子邮件地址登录？

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）。