Configure Umbrella with ADFS Version 3.0 Using SAML

Contents

Introduction

This document describes how to configure SAML between Cisco Umbrella and Active Directory Federation Services (ADFS) version 3.0.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

This article explains how to configure SAML between Cisco Umbrella and Active Directory Federation Services (ADFS) version 3.0. Configuring SAML with ADFS differs from Umbrella's other SAML integrations as it is not a one or two click process in the wizard but requires changes in ADFS to work correctly.

This article has detailed modifications that you must make in order to get SAML and ADFS working together. The primary steps are to first disable encryption between your ADFS environment and Cisco Umbrella, and then add some Issuance Transform Custom Claim Rules to the Umbrella relaying party setting.

Only perform these steps with an existing, working ADFS set up. Cisco Umbrella Support is unable to provide assistance or support in helping configure ADFS in a particular environment.

Only ADFS version 3.0 is supported (Windows Server 2012 R2) by these instructions at this time. It is possible earlier (2.0 or 2.1) or later (4.0) versions of ADFS can work with the Umbrella SAML integration, but this has not been tested or proven. If you have a different version of ADFS and are interested in working with our Support and Product teams to integrate, please contact Cisco Umbrella Support.

You can find the prerequisites for the initial SAML setup in the Umbrella documentation: Identity Integrations: Prerequisites. Once you complete those steps, you can continue using the ADFS specific instructions in this article to complete the configuration.

The steps in the Umbrella documentation mention that you need to upload your SAML (ADFS) metadata to Umbrella. You can access your metadata by navigating to this URL and then uploading the XML file.

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

Disable Encryption

1. Open AD FS Management. Expand **Trust Relationships** and select **Relying Party Trusts**.

2. Right-click the Umbrella relying party (or whatever you named it) and select **Properties**.

3. Select the **Encryption** tab.

4. Select **Remove** to remove the certificate for encryption.

5. Select **OK** to close the screen.

Adding New Issuance Transform Claim Rules

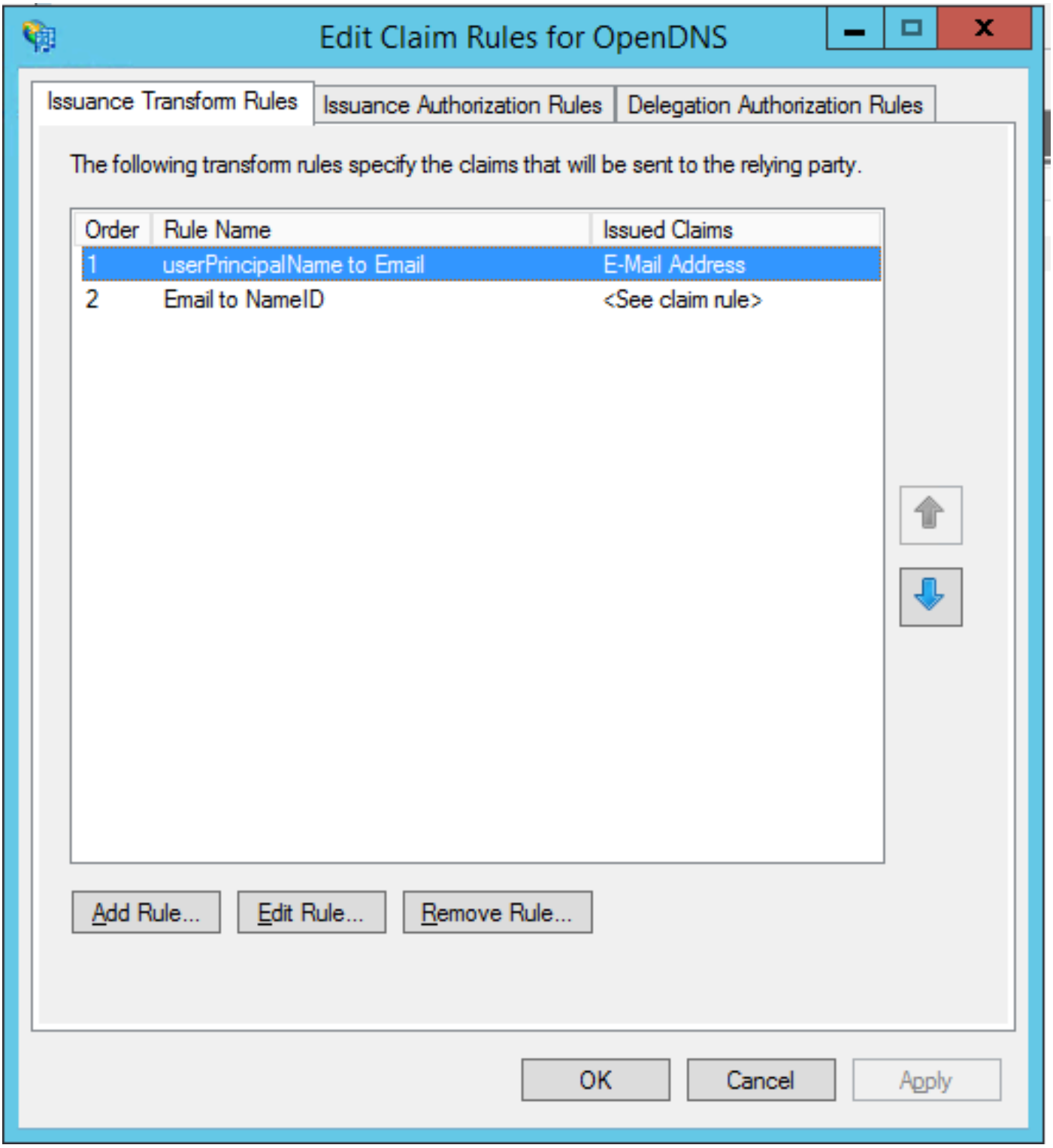
1. Open AD FS Management. Expand **Trust Relationships** and select **Relaying Party Trusts**.

2. Right-click the Umbrella relaying party (or whatever you named it) and select **Edit Claim Rules**.

3. Under **Issuance Transform Rules**, select **Add Rule**.

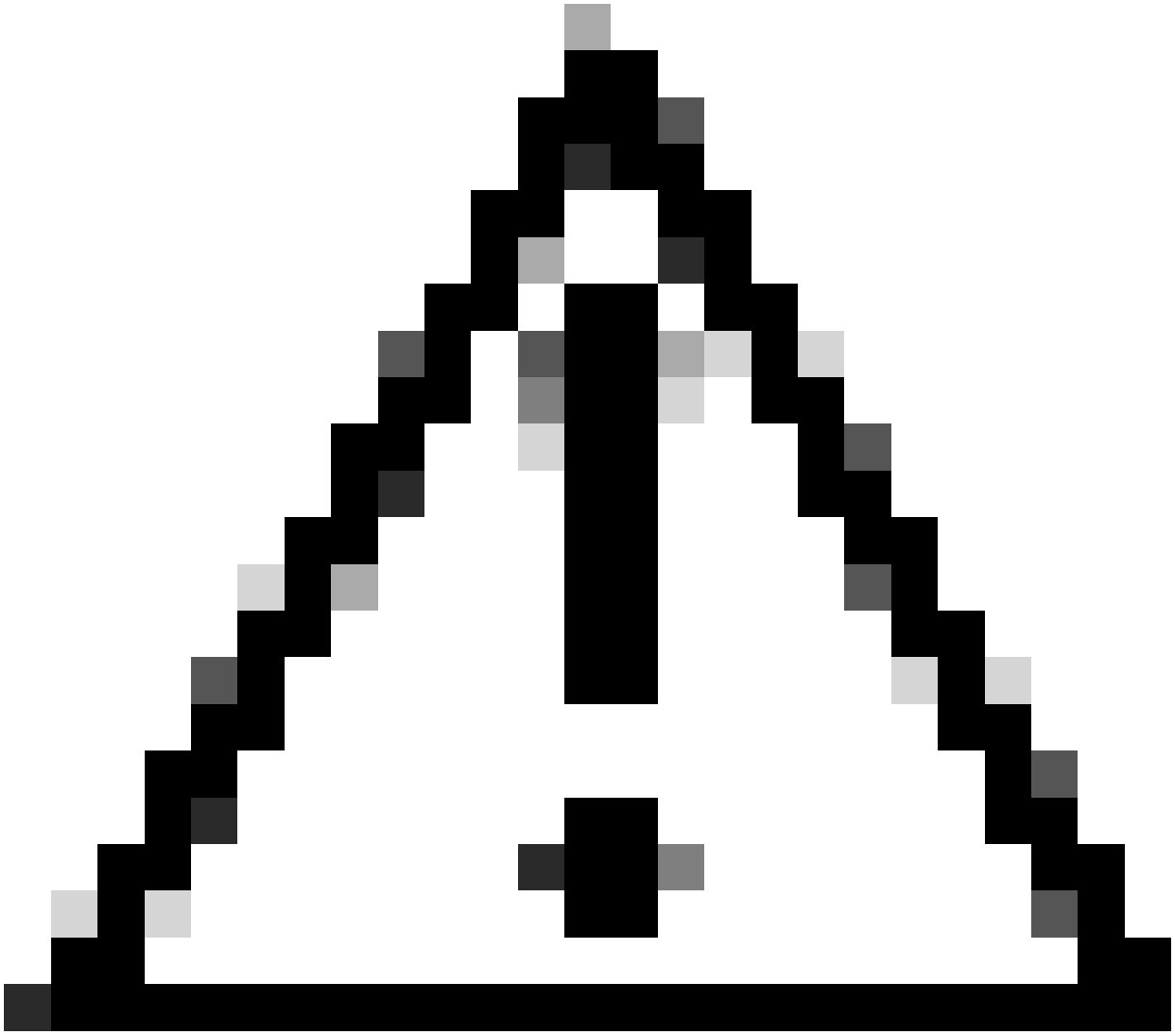
4. Select **Send Claims Using a Custom Rule**.

See this screenshot for the list of rules you can add.



Once you add each of these rules, the integration can begin to work.

Transform Rules



Caution: These rules were tested and working in Umbrella's ADFS lab environment as well as in a few customer production environments. Please modify them to fit your environment.

---

userPrincipalName to Email Address

```
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
```

Email to NameID

```
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");
```

Appendix: Login with 'mail' Attribute

By default ADFS authenticates users by their UPN (User Principal Name). If your user's e-mail address (Umbrella account name) does not match their UPN then additional steps are required. Please see this Knowledge Base article: How do I configure AD FS in the Cisco Umbrella Dashboard to allow logins with an e-mail address?