Configure AD FS in the Umbrella Dashboard

Contents

Introduction

This document describes how to configure AD FS in the Cisco Umbrella Dashboard in order to allow logins with an e-mail address.

Overview

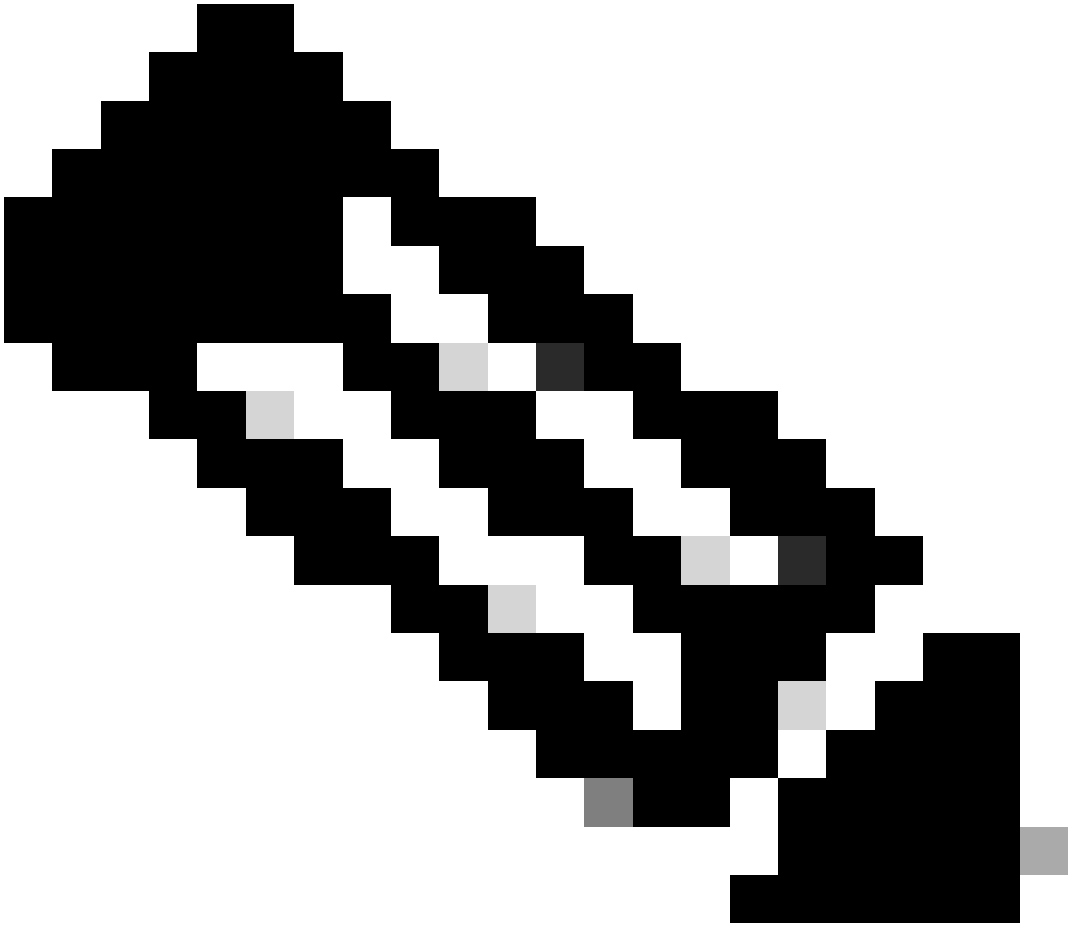
This document applies to users who want to configure single sign-on authentication between the Cisco Umbrella Dashboard and Active Directory Federated Services (AD FS). This document is an appendix to the main AD FS instructions in the Guide to configuring Cisco Umbrella with Active Directory Federation Services (AD FS) version 3.0 using SAML.

This article also provides an example of configuring AD FS to allow login with an e-mail address.

Configure

By default, AD FS authenticates users based on their User Principal Name (UPN). Often this UPN matches both the e-mail address and the Umbrella account e-mail address of the user, therefore no action is required.

However, in some cases, the e-mail address of the user differs from their UPN, and these additional steps are required.



Note: This example is provided 'as is' based on a working AD FS environment. Umbrella Support is unable to help with the configuration of individual AD FS environments.

Step 1. Allow E-mail Address Login (Optional)

Thee PowerShell command configures AD FS to allow the **mail** attribute to be used as the login ID. Replace **<Domain>** with the name of your Active Directory domain:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID mail -LookupForests <Dom
```

This avoids confusion for the end user since they can use the same username for both systems. After this change, the user can log in as:

- Enter the Umbrella username (for example, email@domain.tld)
- Enter email@domain.tld or upn@domain.tld as the AD FS username

If this step is not followed, the end user can need to use a different username for both systems:

- Enter the Umbrella username (for example, email@domain.tld)
- Enter upn@domain.tld as the AD FS username

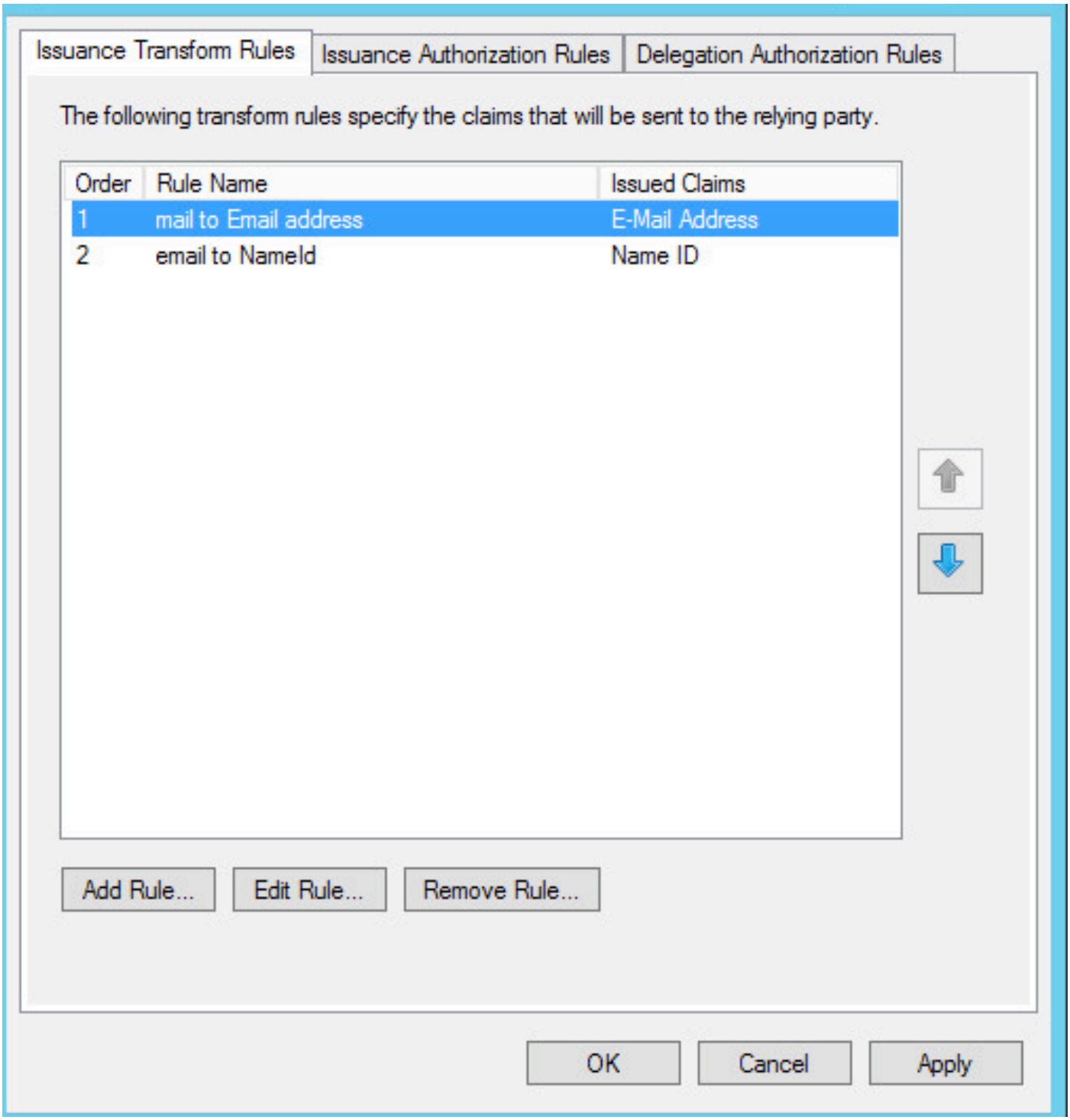
Step 2. Edit Claims Rules (Required)

Review the information in the AD FS instructions in the Guide to configuring Cisco Umbrella with Active Directory Federation Services (AD FS) version 3.0 using SAML. The claims rule **userPrincipalName to Email address** must be deleted and replaced with the rule called **mail to Email address**.

This tells AD FS to include the **mail** attribute in its SAML response:

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

The claims rules must be configured in the correct order with **mail to Email Address** as the first rule:


Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
The following transform rules specify the claims that will be sent to the relying party.
Order
Rule Name
Issued Claims
1
mail to Email address
E-Mail Address
2
email to NameId
Name ID
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply