Add Required Attribute UID in ADFS Server Manually

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Scenario 1
- Scenario 2
- Configurations

Add a Custom Claim Rule in the ADFS Server under Webex Relying Party Trust

- Steps to Create This Rule

Introduction

This document describes how to manually add an Attribute UID in ADFS relying party trust using a syntex.

Prerequisites

Requirements

- ADFS server
- Control Hub

Components Used

- ADFS server
- Cisco Webex Control Hub
- On-Prem AD

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.

Configure

This is something that is useful in case there is an issue adding an Attribute Claim in ADFS due to an existing attribute.

Scenario 1

You have an existing relying party trust which has a Claim rule created with attribute named UID or Uid.

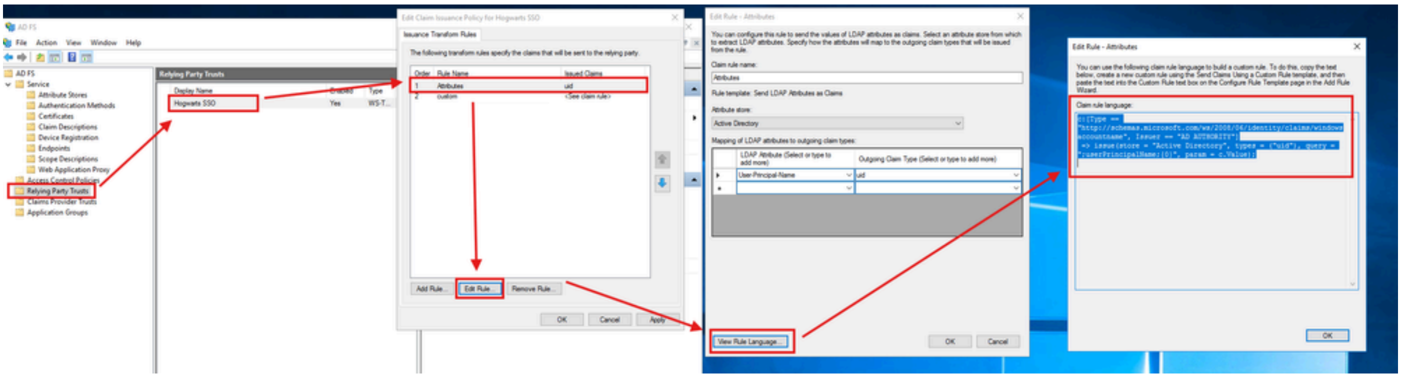
This fails the Authentication since Webex (SP) is case sensitive about the required attribute and it has to be **uid** and must pass the emailAddress of the user in SAML response.

Scenario 2

You have a party trust which has a Claim rule passing an attribute named **uid** but associated with different attribute in AD than what is needed (emailAddress/UserPrincipleName). This creates issues.

Configurations

In an ideal configuration as per the Cisco Webex Guide, ADFS configuration must look like this:



Display Name	Enabled	Type
Hogwarts SSO	Yes	WS-T...

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Attributes	uid
2	custom	<See claim rule>

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: Attributes

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	uid

You can use the following claim rule language to build a custom rule. To do this, copy the text below, create a new custom rule using the Send Claims Using a Custom Rule template, and then paste the text into the Custom Rule text box on the Configure Rule Template page in the Add Rule Wizard.

Claim rule language:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windows
accountname", Issuer == "AD AUTHORITY"]
 => issue(store = "Active Directory", types = ("uid"), query =
";userPrincipalName;{0}", param = c.Value);
```

ADFS Admins can visit this from their **Relying Party Trusts-> Trust they created for Webex -> Edit Claim Issuance Policy -> Edit Rule -> Attributes -> View Rule Language**.

The rule language in plain text is:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types = ("uid"), query = ";userPrincipalName;{0}", param = c.Value);

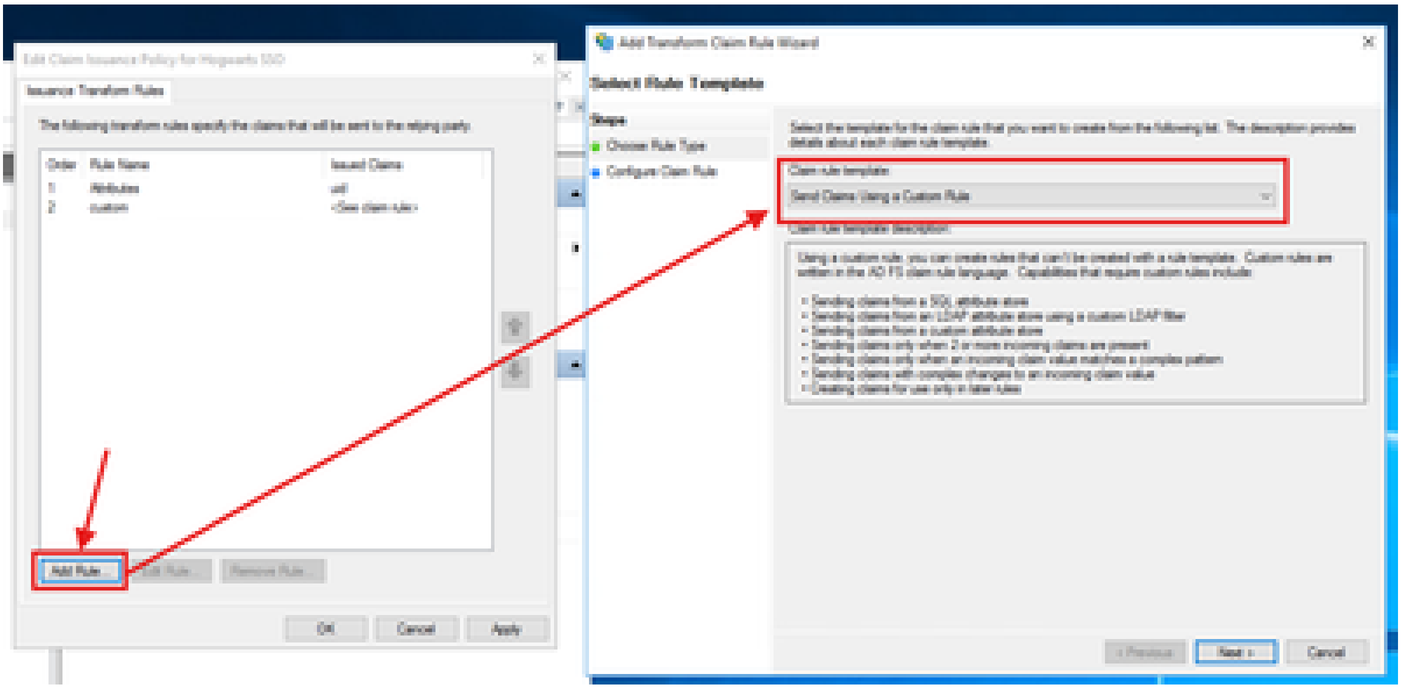
Since the configuration does not display properly, manually create this rule by using the plain text of the rule language.

Add a Custom Claim Rule in the ADFS Server under Webex Relying Party Trust

Steps to Create This Rule

1. In the main ADFS pane, select the trust relationship that you created, and then select **Edit Claim Rules**. Under the **Issuance Transform Rules** tab, select **Add Rule**.
2. Select **Send Claims Using a Custom Rule**, and then select **Next**.
3. Copy the rule from your text editor (starting at c:) and paste it in to the custom rule box on your ADFS server.

This must look like this:



The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Attributes	uid
2	custom	<See claim rule>

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

Once this is done you can test SSO from the Control Hub and that must work as expected.