Televic Education

ADFS - Example configuration

17 August 2023

Created by Lynn Van den Broeck

televic education

Table of contents

This document shows a step-by-step guide on how to configure an ADFS server for connecting with the assessmentQ Identity Provider. This document uses ADFS 4.0 as example.

1 Introduction

With respect to setting up the ADFS coupling, the customer takes the role of the Identity Provider (IdP) and Edumatic takes the role of the Service Provider (SP).

assessmentQ uses Open ID Connect through Identity Server to authenticate users.

Identity Server is to be configured as a Relying Party in ADFS.
WS-Federation Protocol is used for the communication between ADFS and assessmentQ.

2 Requirements

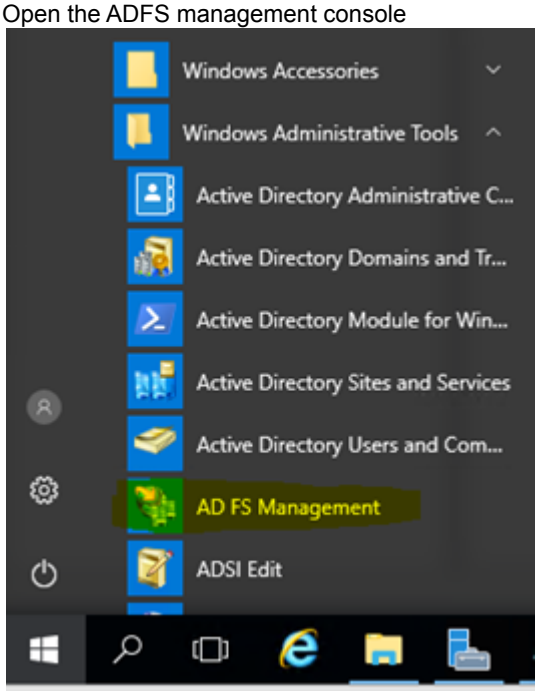
- ADFS 2.0 or higher
- OAuth SHA-2 signature encoding
- Access to the IdP metadata file via direct URL access

3 Configuration

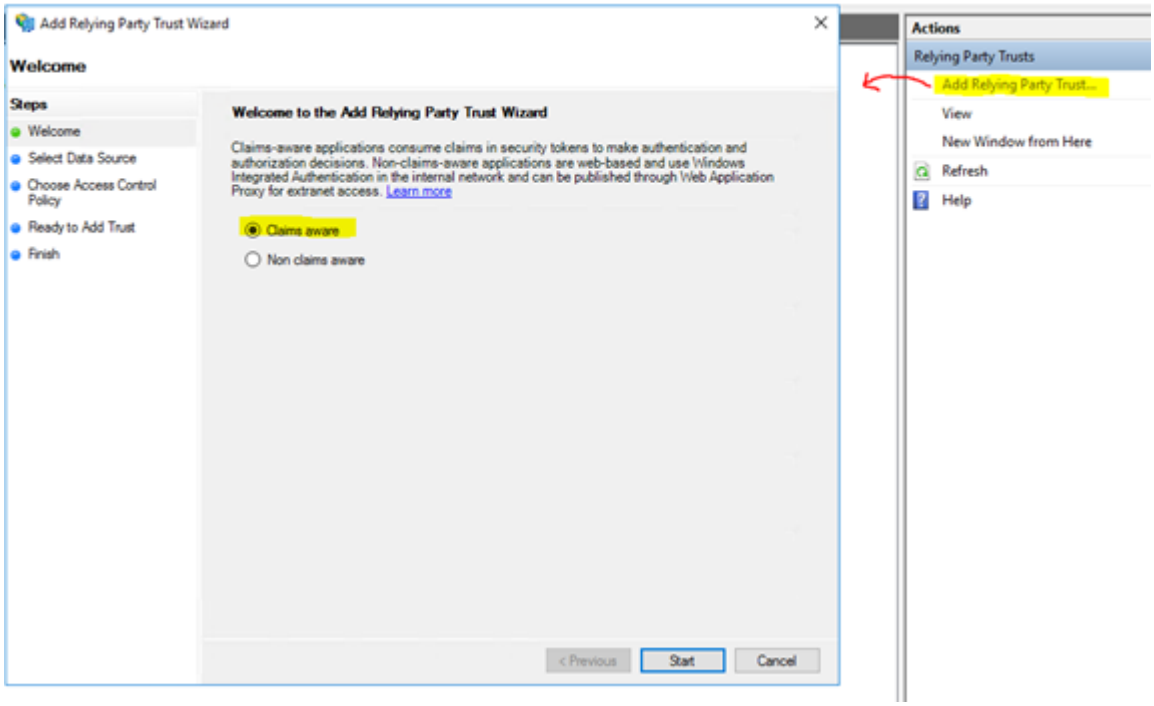
3.1 Configuring the Relying Party Trust

A Relying Party (RP) Trust needs to be configured for the Televic SP.

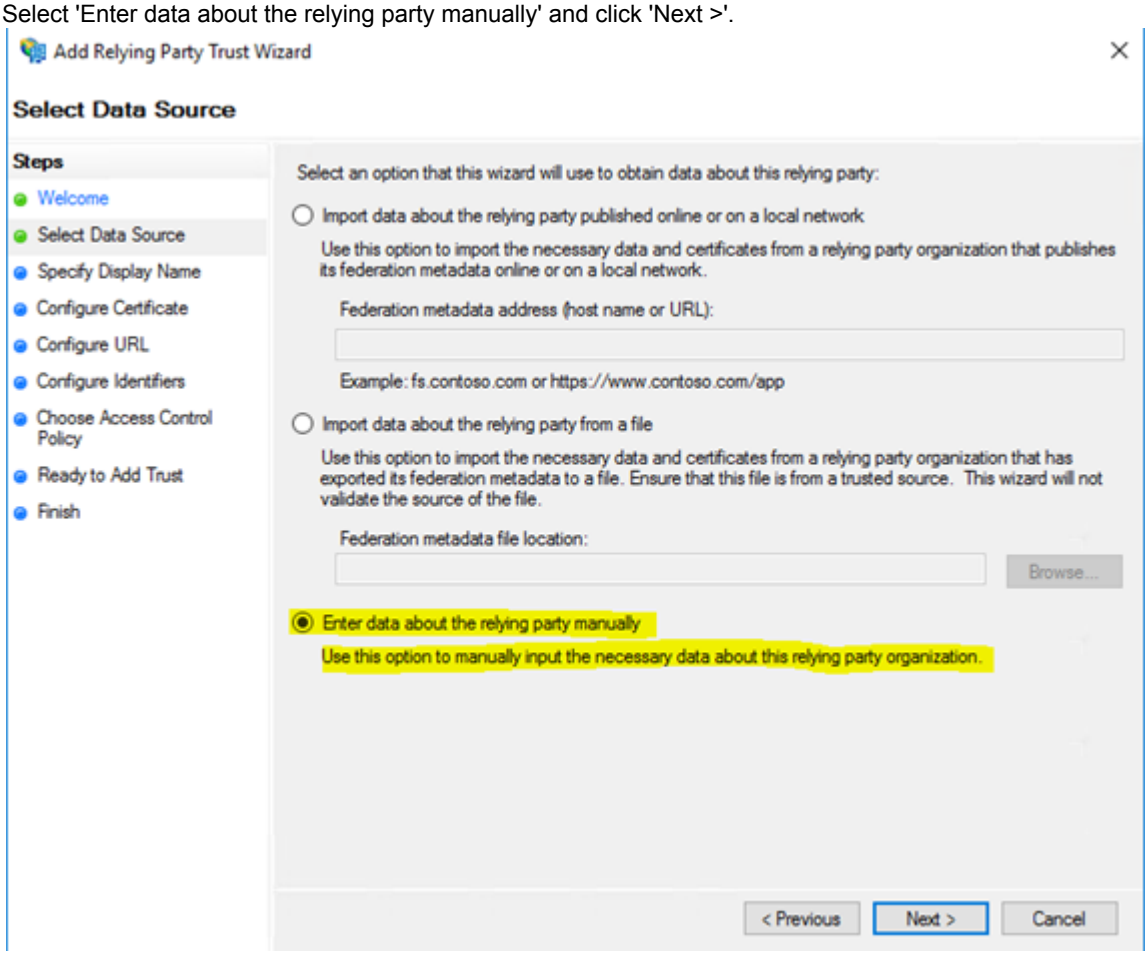
1. Open the ADFS management console



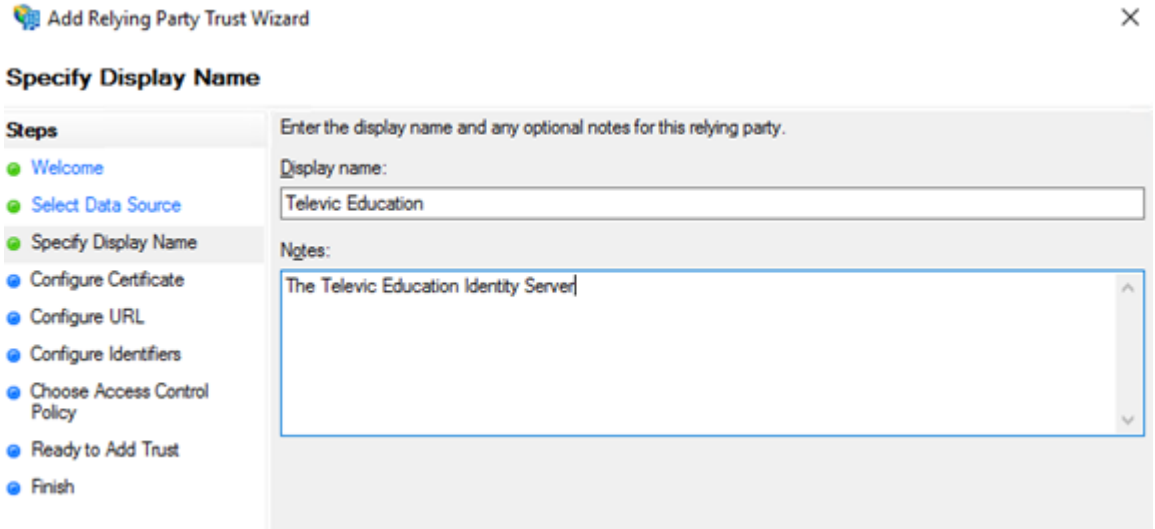
2. Click 'Add Relying Party Trust', select 'Claims Aware' in the first window and click 'Start'.



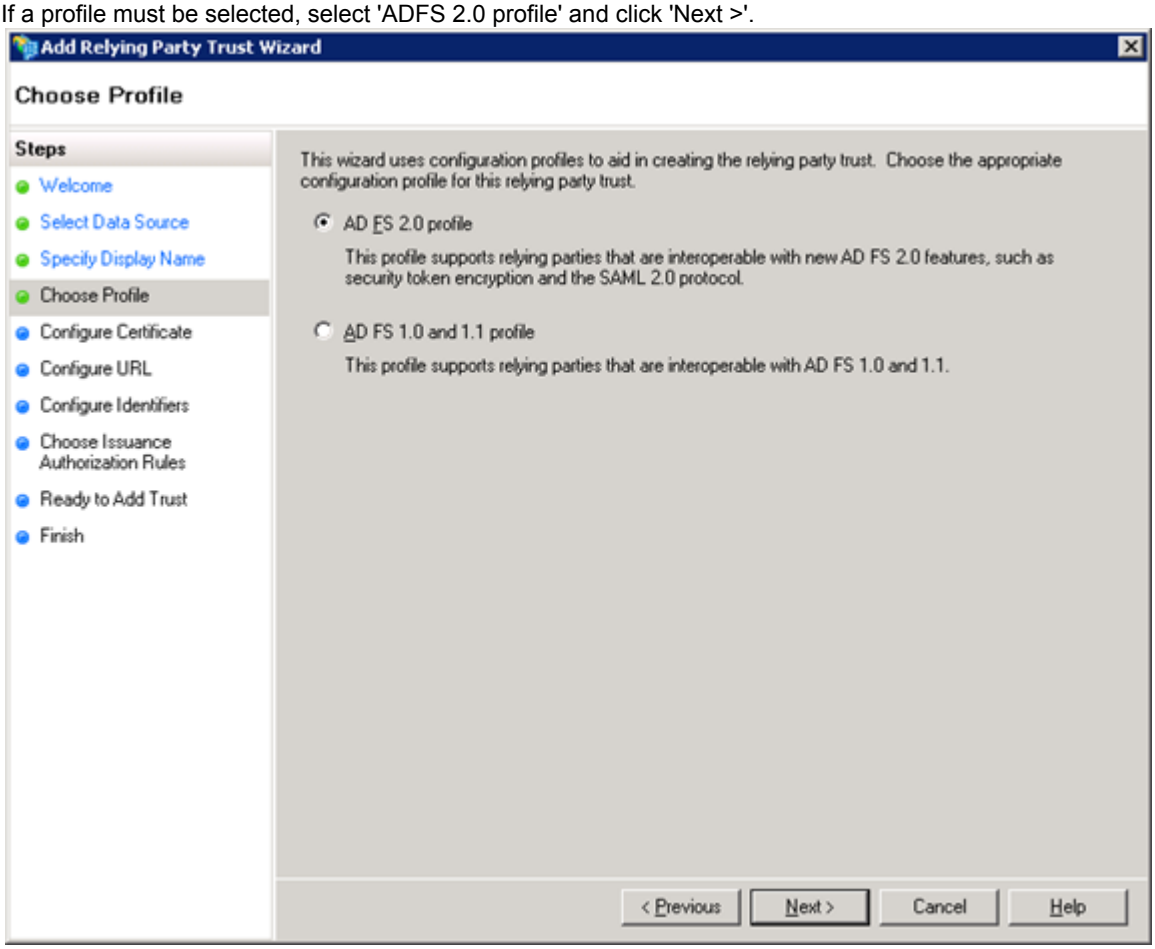
3. Select 'Enter data about the relying party manually' and click 'Next >'.



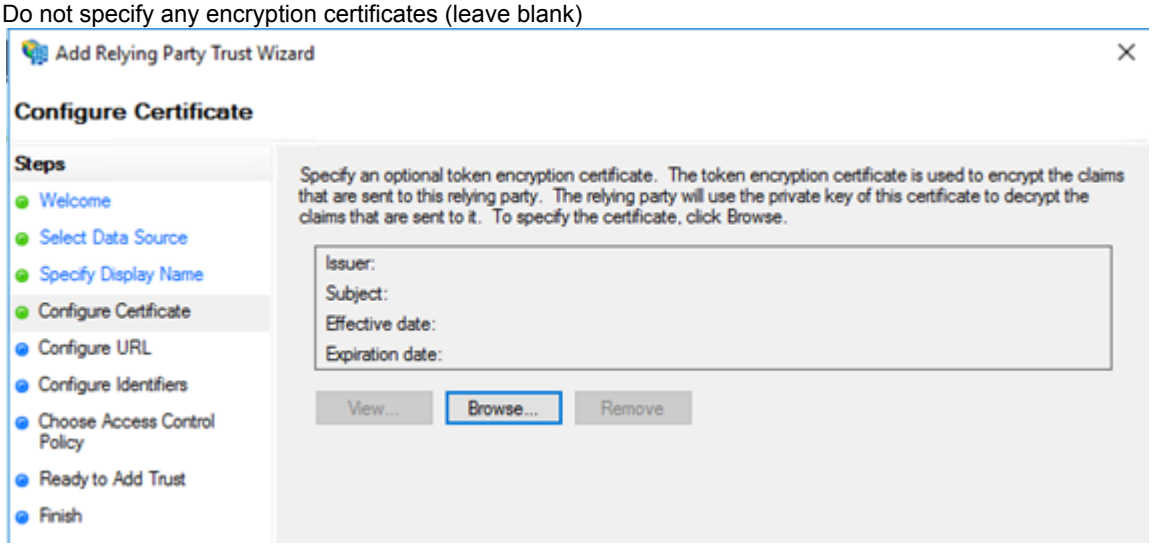
4. Provide a display name for the RP and optional description for the Relying Party and click 'Next >'.



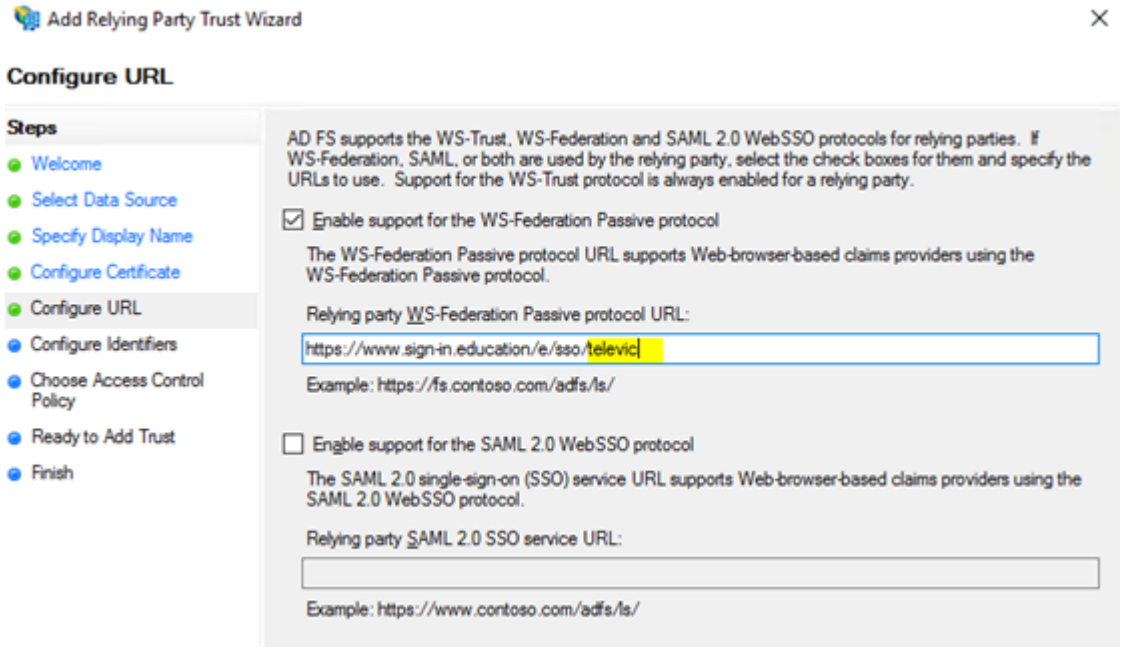
5. If a profile must be selected, select 'ADFS 2.0 profile' and click 'Next >'.



6. Do not specify any encryption certificates (leave blank)



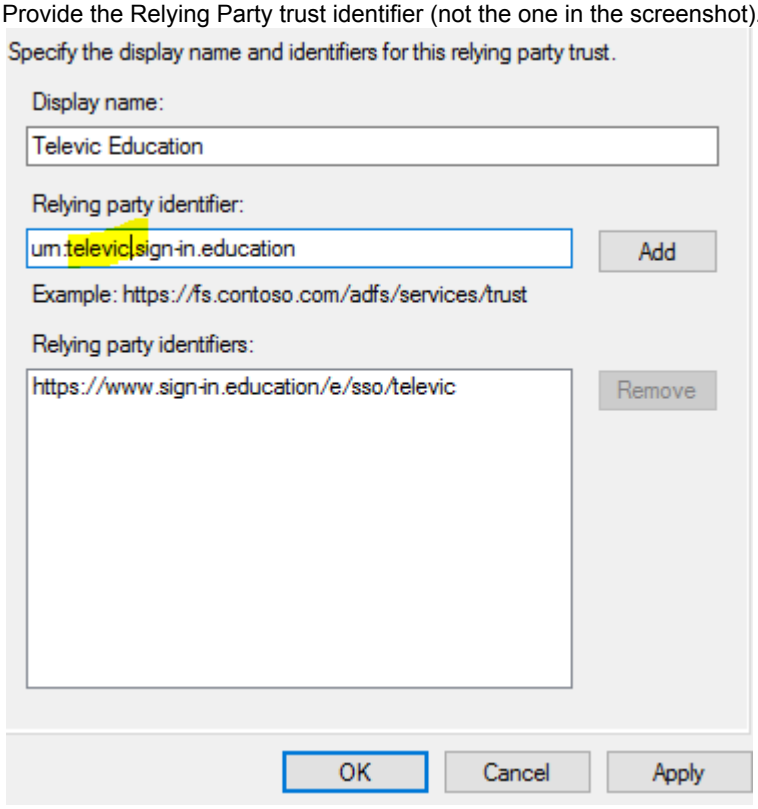
7. Select 'Enable support for the WS-Federation Passive protocol'



Enter the following URL for the 'Relying Party WS-Federation Passive Protocol URL' (not the one in the screenshot):

https://idp.assessmentq.com/sso/*<your_identifier>*

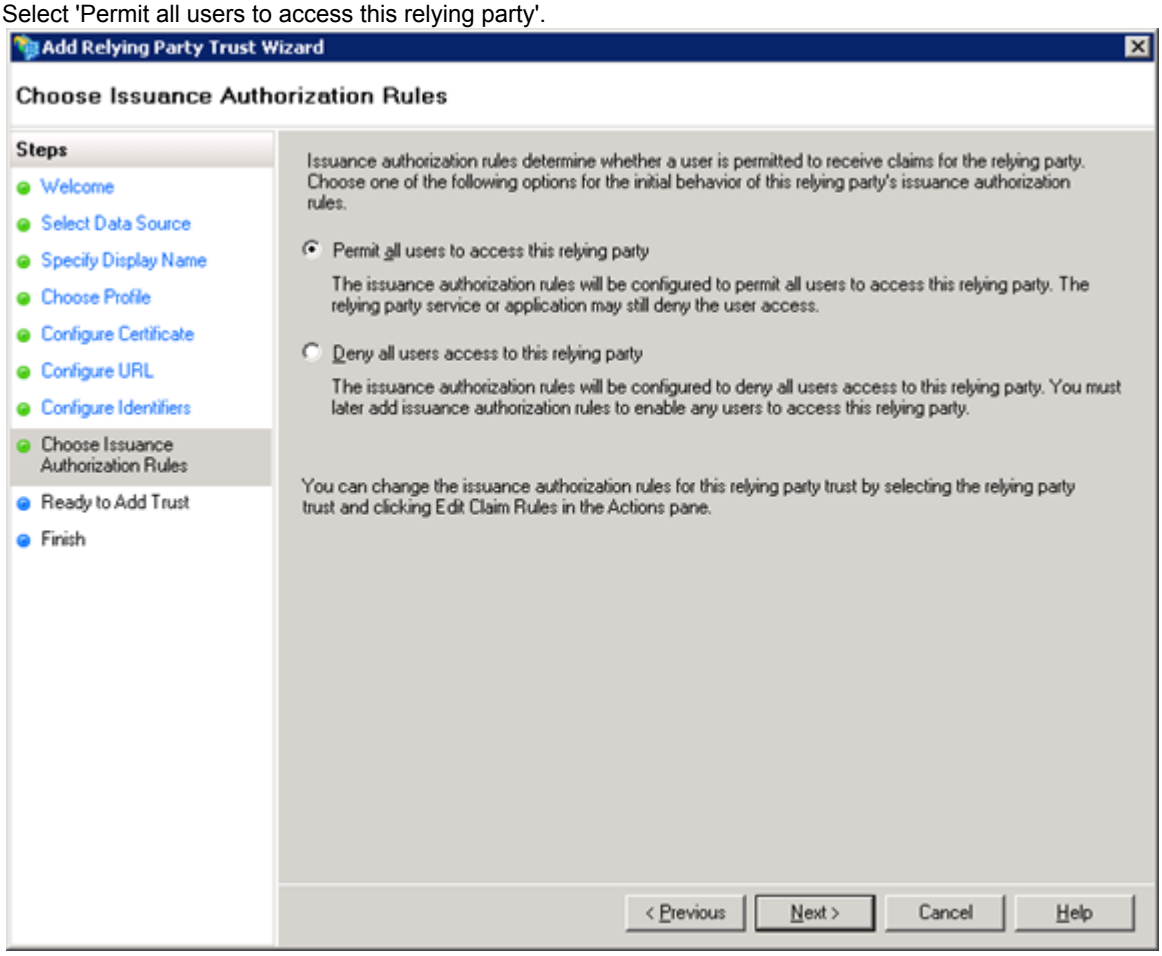
8. Provide the Relying Party trust identifier (not the one in the screenshot).



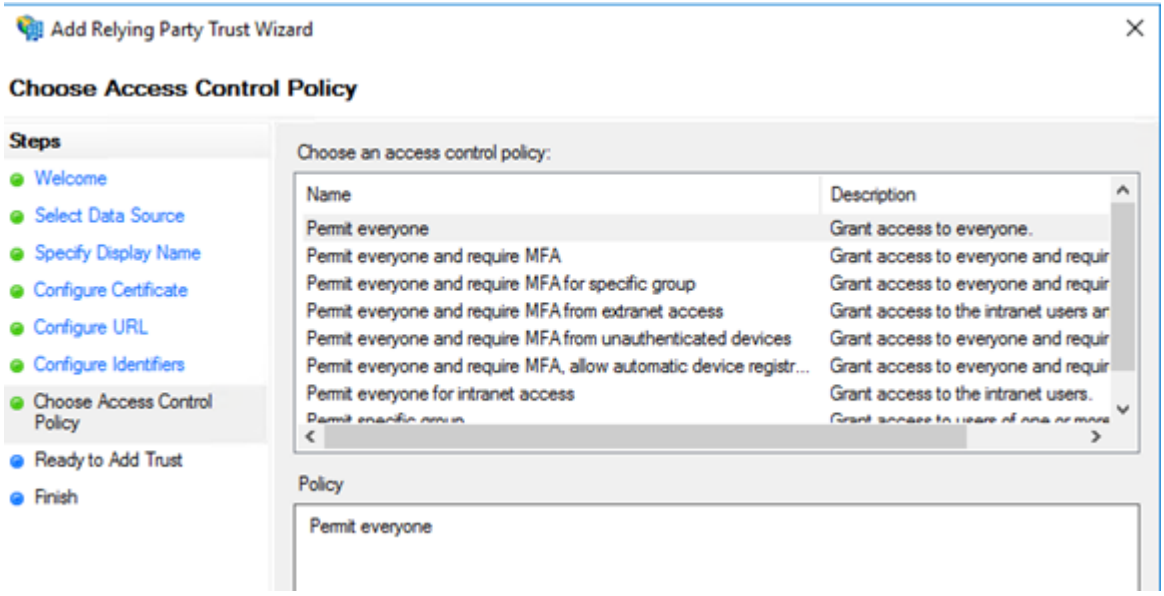
urn:<*your_identifier*>.idp.assessmentq.com

Note: subdomain is case sensitive and should always be lower case.

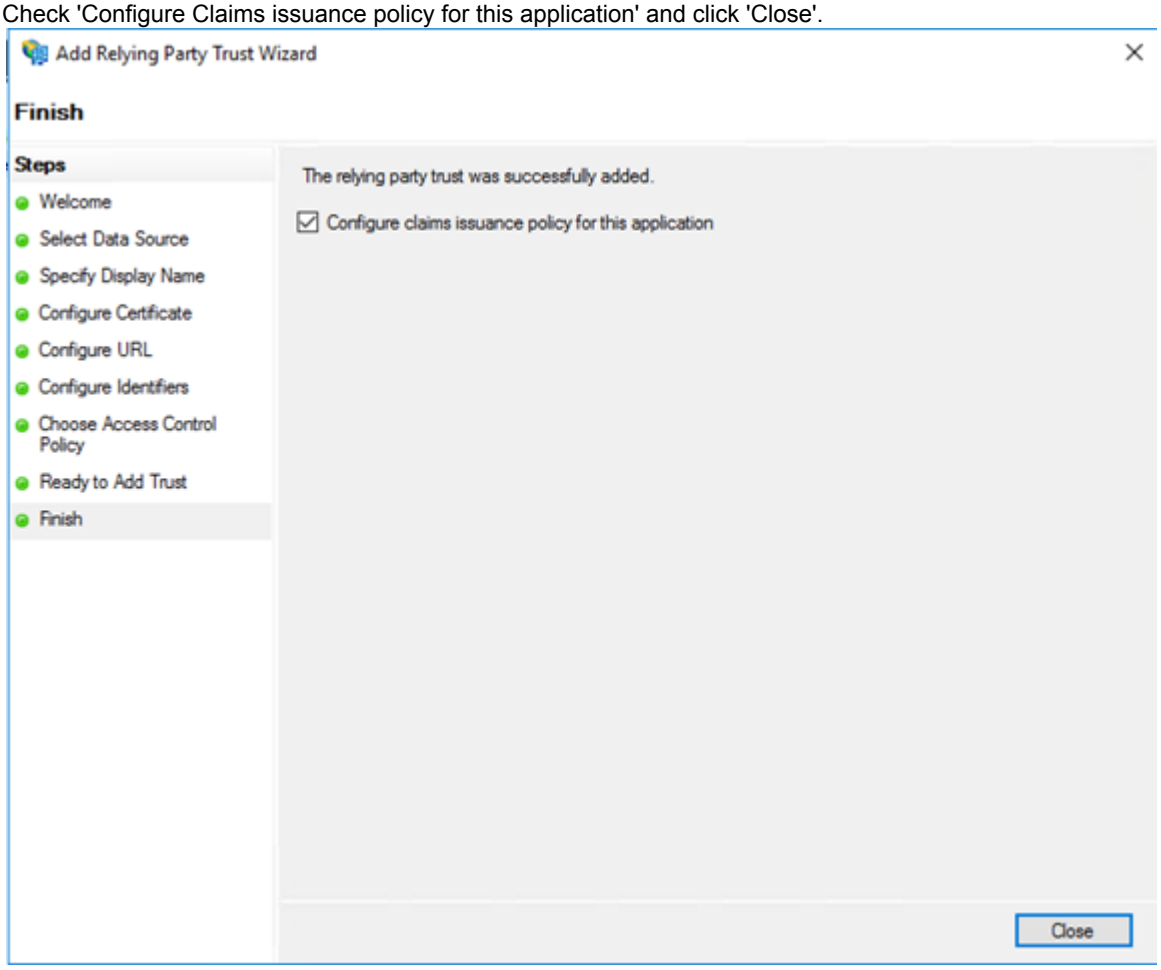
9. Select 'Permit all users to access this relying party'.



or



10. On the 'Ready to Add Trust' screen, you can review all settings. If all is correct, click 'Next >'.
11. Check 'Configure Claims issuance policy for this application' and click 'Close'.



3.2 Configuring claims

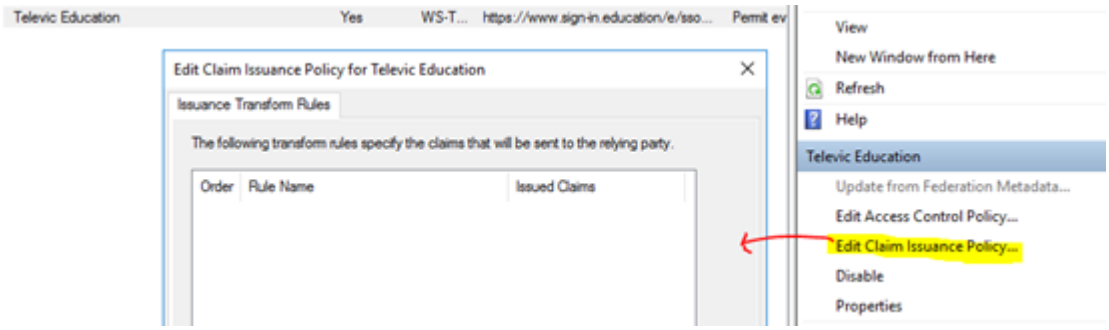
Claims need to be configured in order to map users between ADFS and assessmentQ. Important: the user's Windows name needs to be passed without domain prefix as Name ID. In order to accomplish this, the Active Directory Claims Provider Trust need to be changed accordingly.

By default, there is no claim rule on this provider to pass the Windows user. So one should be add.

Important note: before continuing, check if the claims is already present.

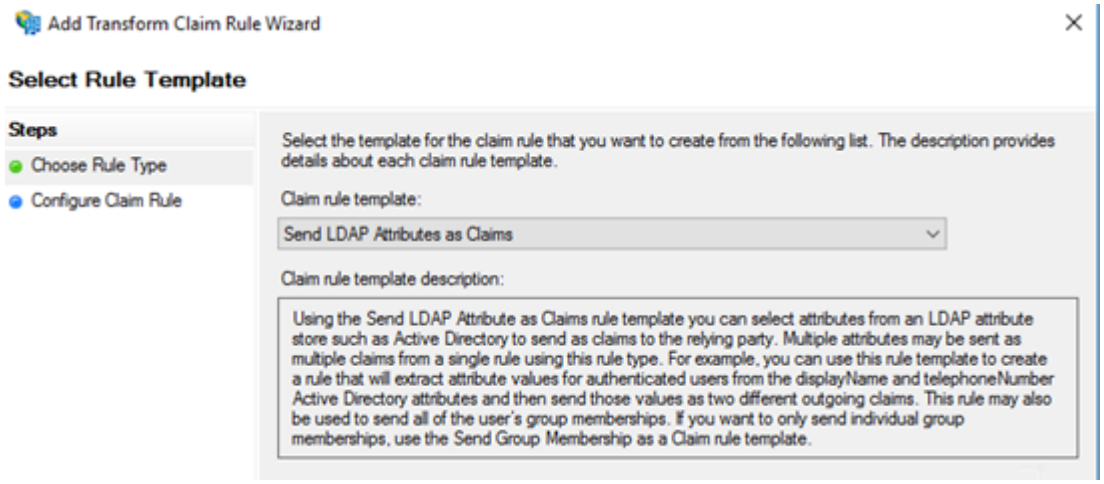
1. Right-click Active Directory and Select 'Edit Claim Rules'

or
Select the Relying Party from the list and click 'Edit Claims Issuance Policy' in the right pane.



and select 'Add Rule'.

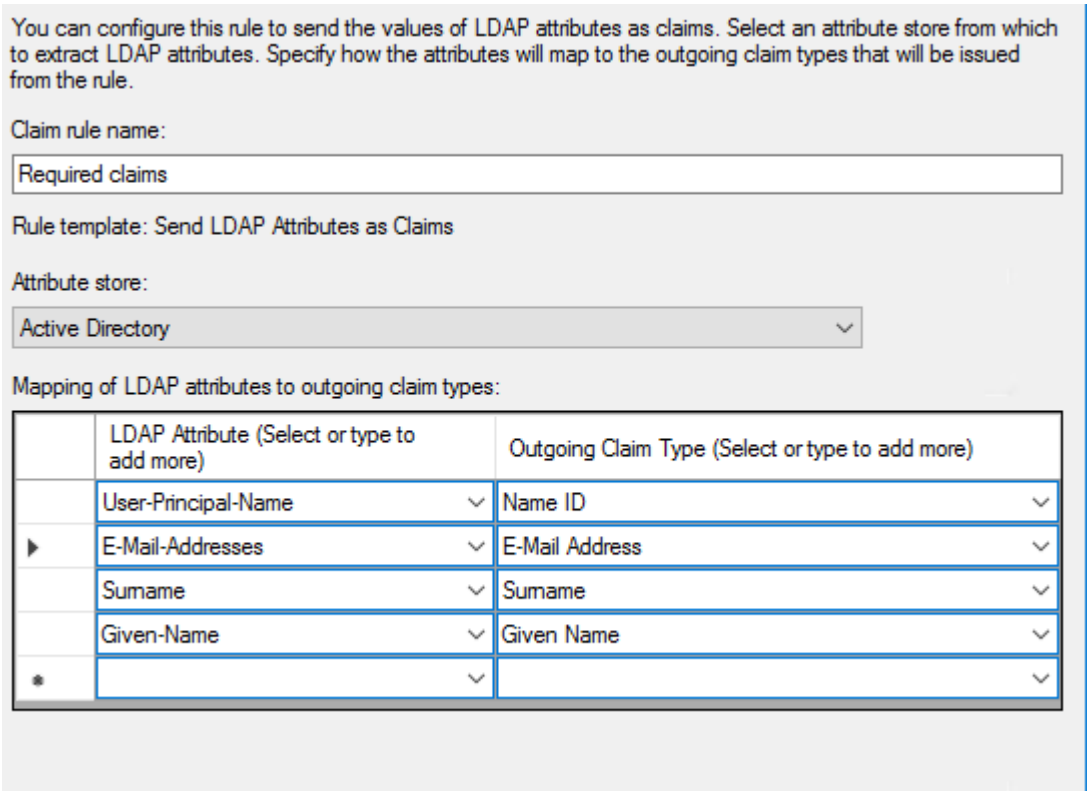
2. Add a new 'Send LDAP Attributes as Claims' rule



3. Enter a name for the claims rule, and map LDAP Attributes to the required claims. The required claims for the SP are:
    a. Name Id or Sub
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
    b. E-mail Address
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
    c. Surname
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
    d. Given Name
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

    These claims are configured by default in the ADFS > Service > Claim Descriptions section of the ADFS Management console.
    An example of how to map them is shown in the figure below. Note that the Name ID Claim can be mapped from anything you wish, as long as it is unique. Another example could be to map the SamAccountName to the

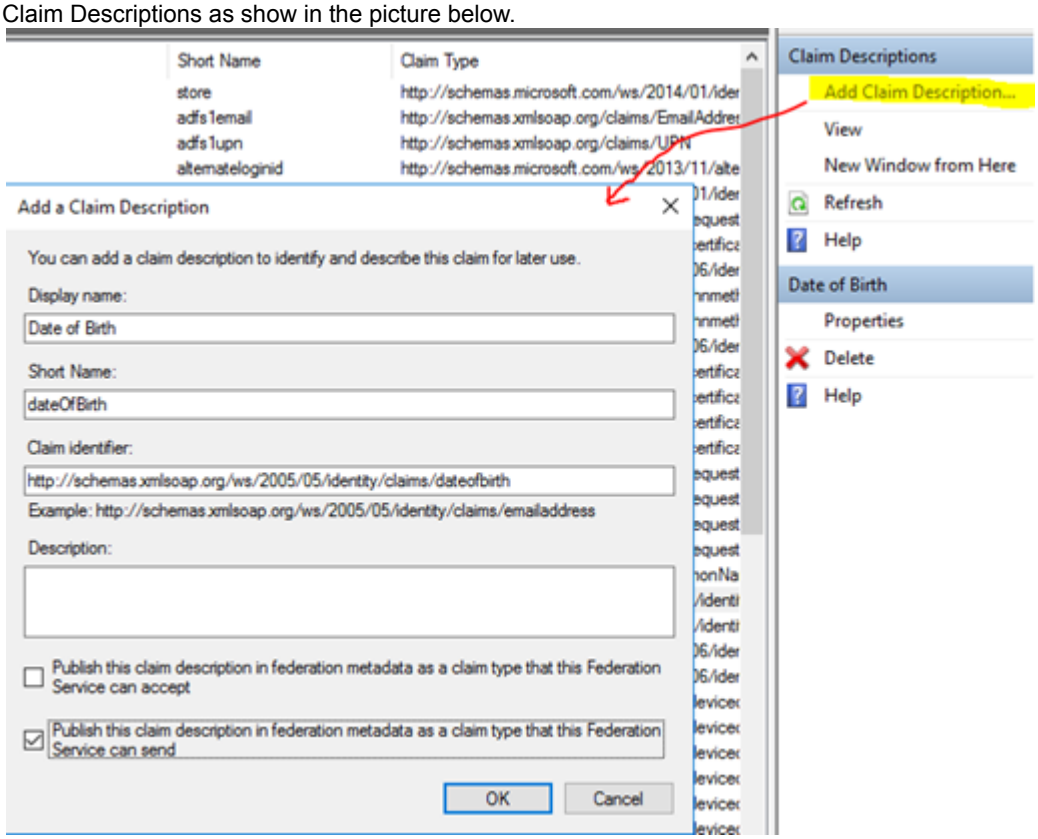
NameId claim.



4. Optionally another Claim rule can be added to provide for:
    a. User name
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
    This claim is added to the Claim Descriptions by default.
    b. Date of Birth
    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth

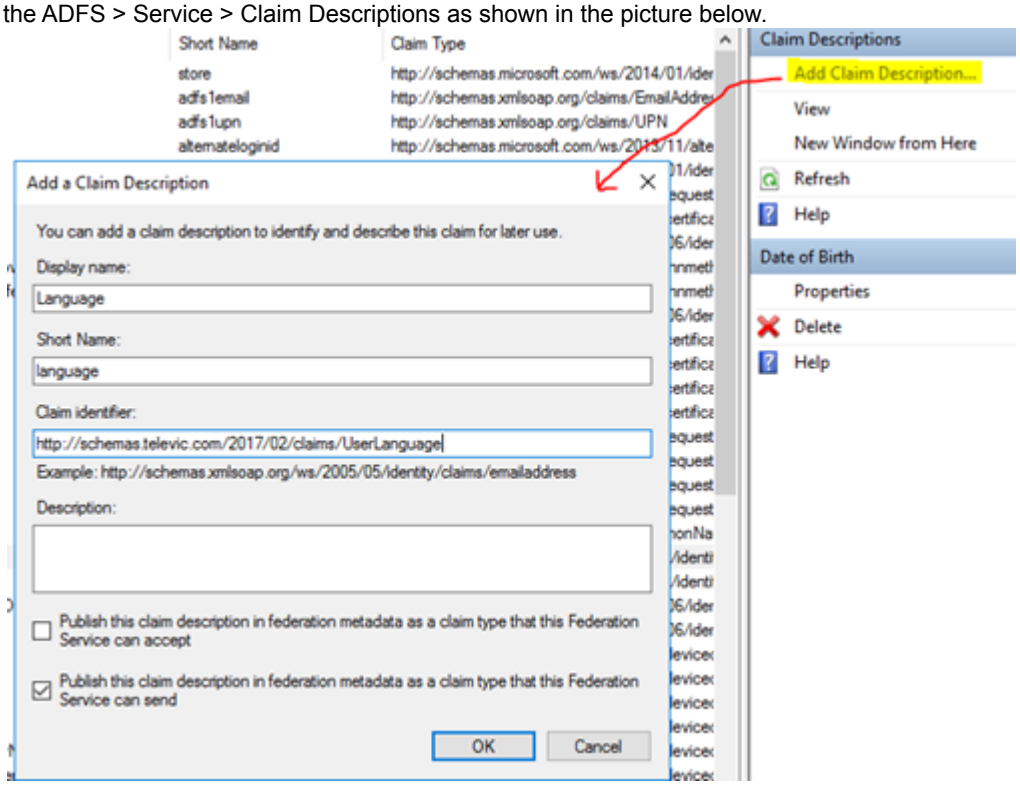
    This claim is not added to the Claim Descriptions by default. It can be added in the ADFS > Service >

Claim Descriptions as show in the picture below.

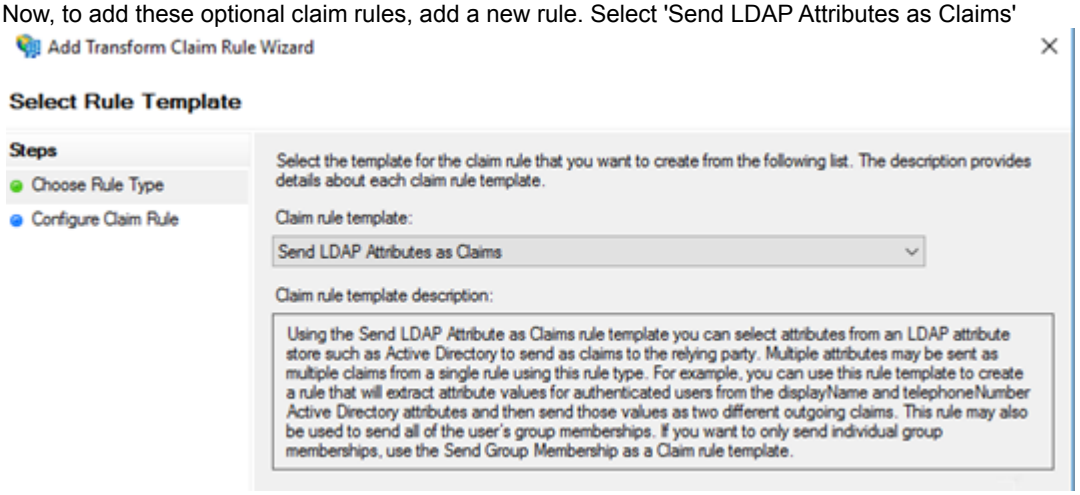


c. UserLanguage
http://schemas.televic.com/2017/02/claims/UserLanguage

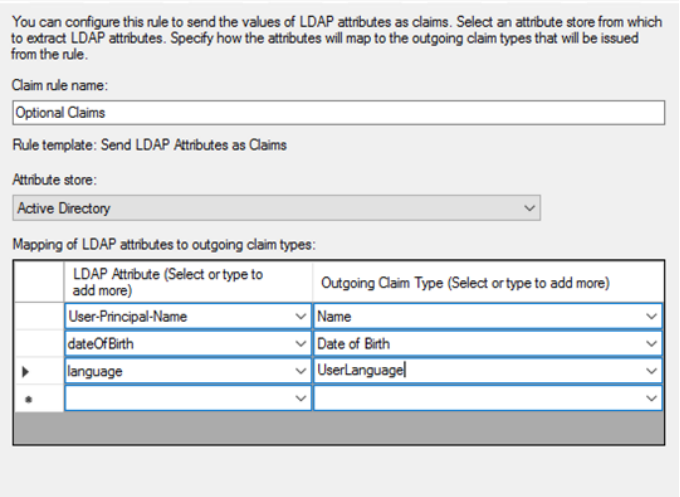
This claim is defined by Televic and is not added to the Claim Descriptions by default. It can be added in the ADFS > Service > Claim Descriptions as shown in the picture below.



Now, to add these optional claim rules, add a new rule. Select 'Send LDAP Attributes as Claims'



And add map the attributes in the picture below. Note that the Name claim can also be chosen from any LDAP Attribute you like. Uniqueness is not required. The 'Date of Birth' and 'language' Attributes are non-standard AD attributes and can be added by an AD Administrator. Adding custom AD Attributes is not covered in this manual.



3.3 Adding support for synchronizing groups between ADFS and Edumatic

3.3.1 Organizing Groups within the AD

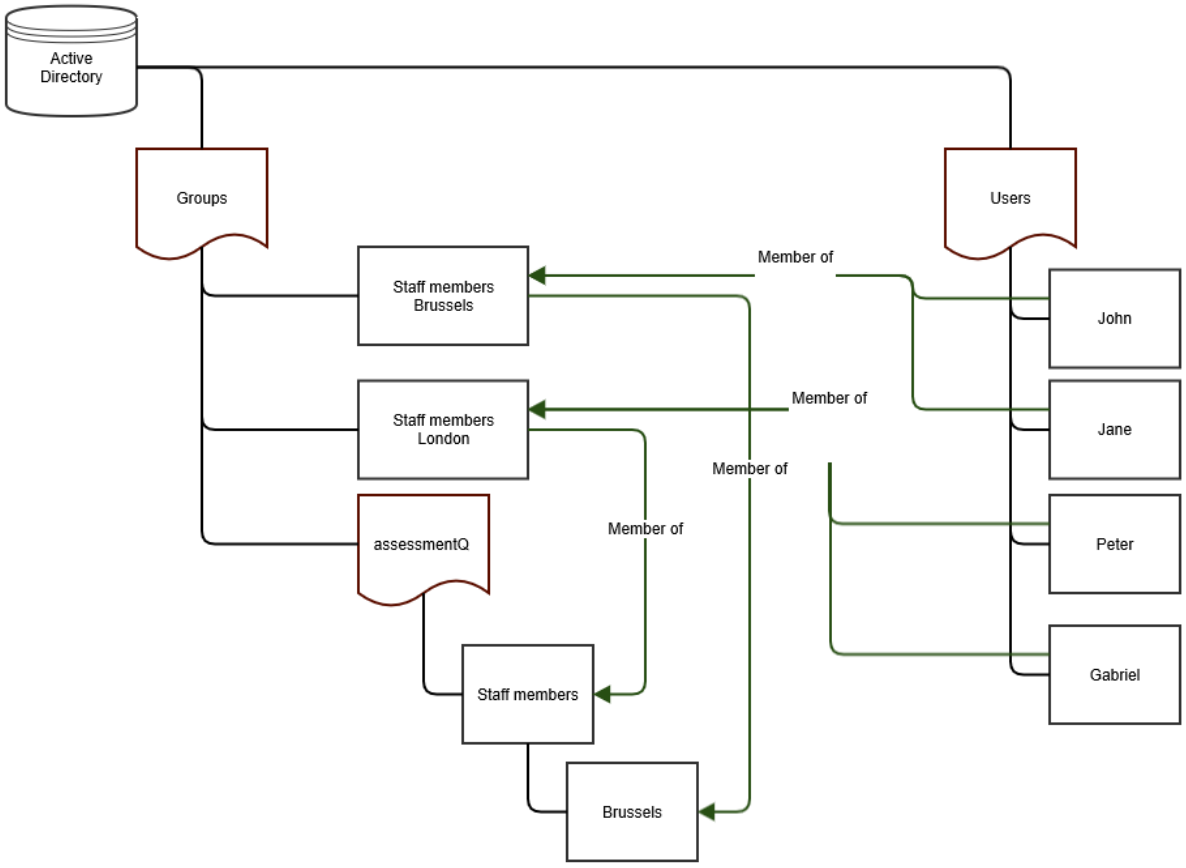
The diagram below depicts the coupling between users and groups in Active Directory (AD) and assessmentQ.

Within the AD structure, you create an Organization Unit (OU) *assessmentQ*. Within this OU, you define all the groups that need to be synchronized with assessmentQ. Subsequently you add the users to these groups, either by linking the user directly to an OU group or by linking an existing AD group to an OU group.

For example:

1. John and Jane are members of the AD group *Staff members Brussels*. This group, in turn, is member of the OU group *Brussels*. As a result, John and Jane are members of the OU groups *Brussels* and Staff members within the OU *assessmentQ.*

2. Peter and Gabriel are members of the AD group *Staff members London*. This group, in turn, is member of the OU group *Staff members*. As a result, Peter and Gabriel are members of the OU group *Staff members* within the OU *assessmentQ*.



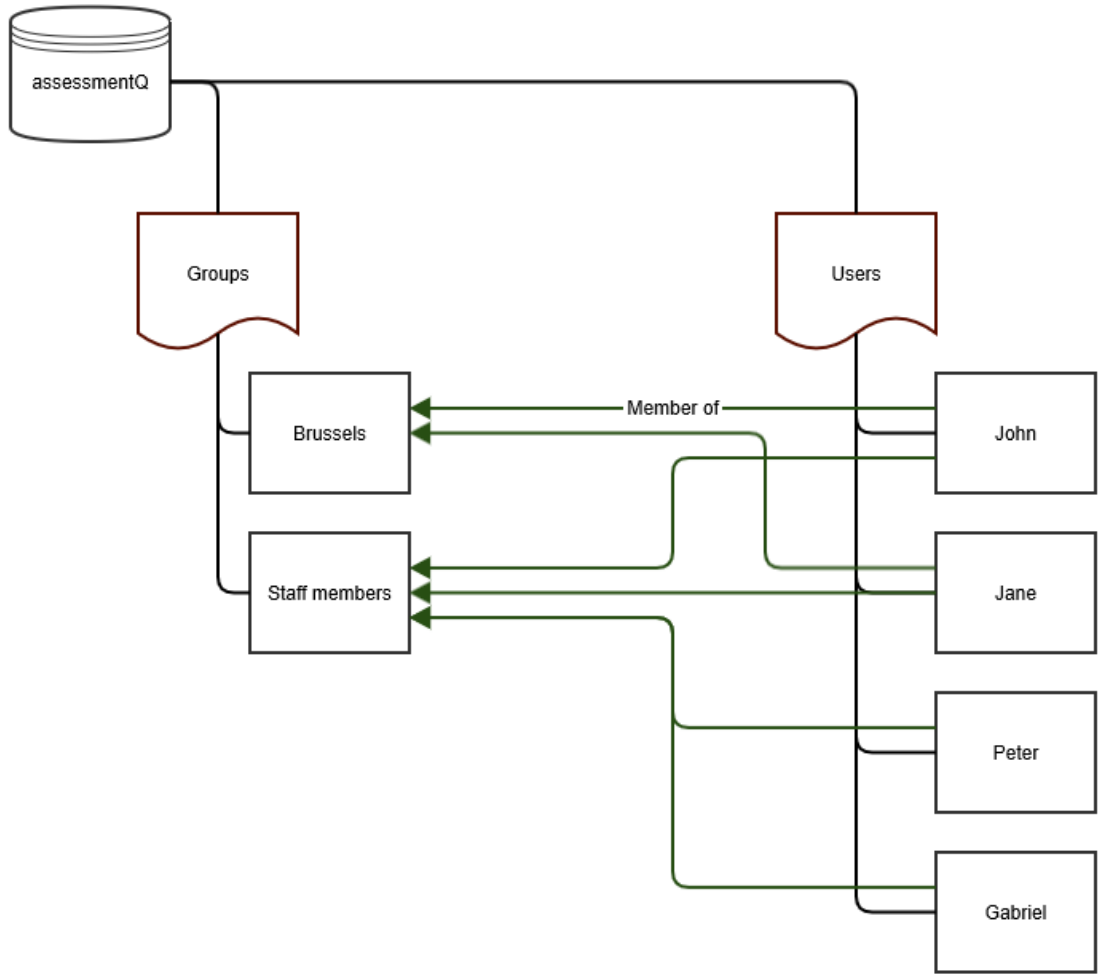
FOUT Gliffy is zonder licentie. installeer een licentie om diagrammen in uw wiki te tekenen.

When John signs in to assessmentQ (via the ADFS coupling), the groups *Staff members* and *Brussels* are automatically created in assessmentQ and John is added to these groups. These groups will not be nested in assessmentQ and will exist next to each other.
When Jane signs in to assessmentQ, she will be added to the groups *Staff members* and *Brussels* (which are already present in the system).

When Peter signs in to assessmentQ, he will only be added to the group *Staff members*. No group *Staff members London* will be created.

As such, groups not part of the OU assessmentQ will not be created in assessmentQ.

In assessmentQ, this will result in the following structure of groups and users:



FOUT Gliffy is zonder licentie. installeer een licentie om diagrammen in uw wiki te tekenen.

3.3.2 Limitations

There are some restrictions and limitations related to syncing groups between AD and assessmentQ:

1. Groups within the OU assessmentQ should all have unique names as groups are not nested in assessmentQ.
2. In case groups already exist within assessmentQ, the same name must be used within the OU assessmentQ.
3. If a group name is changed in assessmentQ, it should also be manually changed in the OU assessmentQ and vice versa.
4. Users are never deleted from groups in assessmentQ.
   Example:
   a. In AD, *Jane* is initially member of the group *Staff members.*
   b. *Jane* signs in to assessmentQ (using ADFS). As a result, *Jane* is also added to the group *Staff members* in assessmentQ.
   c. Some time later, In AD, *Jane* is moved to group *Brussels*. Hence, in AD, *Jane* is no longer member of the group *Staff members.*
   d. *Jane* signs in to assessmentQ again (using ADFS). As a result, *Jane* will be added to the group *Brussels*.
   Important: *Jane* is still a member of the *Staff members* group in assessmentQ as well.

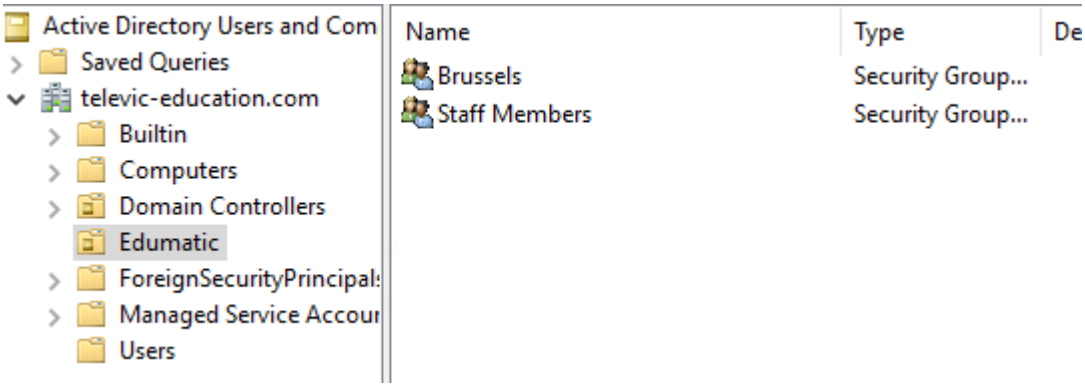
Automatically deleting a user from groups is not supported through ADFS. Also, this could have an impact on reporting and obtained results. As such, if users change groups in AD, they should **manually be removed** from the corresponding assessmentQ group (if needed).

Tip: create a dummy user which is member of all the OU groups and sign in with that particular user in assessmentQ via ADFS. As a result, all assessmentQ groups will be created at once.

3.3.3 Passing on groups to assessmentQ

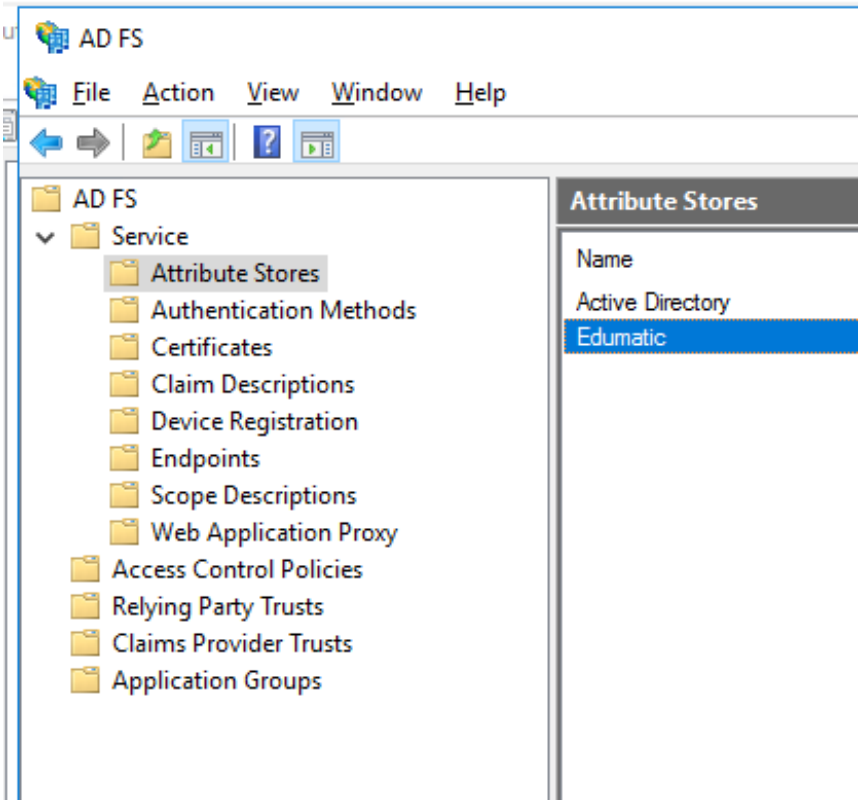
As detailed in the previous section, the groups passed on the assessmentQ need to be defined in an OU as depicted in the picture below.

> ⚠ assessmentQ was formerly called Edumatic. In the screenshots below the name Edumatic is still used instead of assessmentQ.

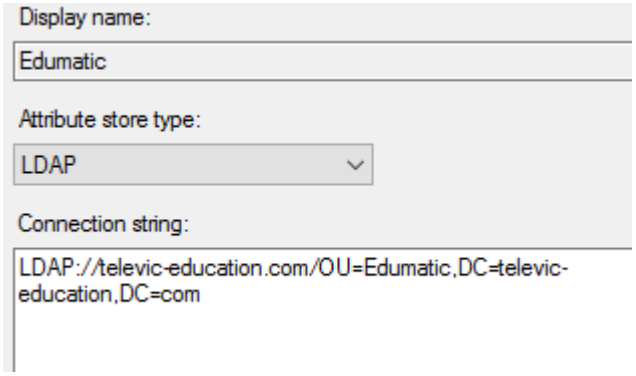


To find all groups for a user, which are member of this assessmentQ OU, we need a custom Attribute Store and 2 custom rules.

First we define a custom attribute store, let's call it assessmentQ (formerly called Edumatic).

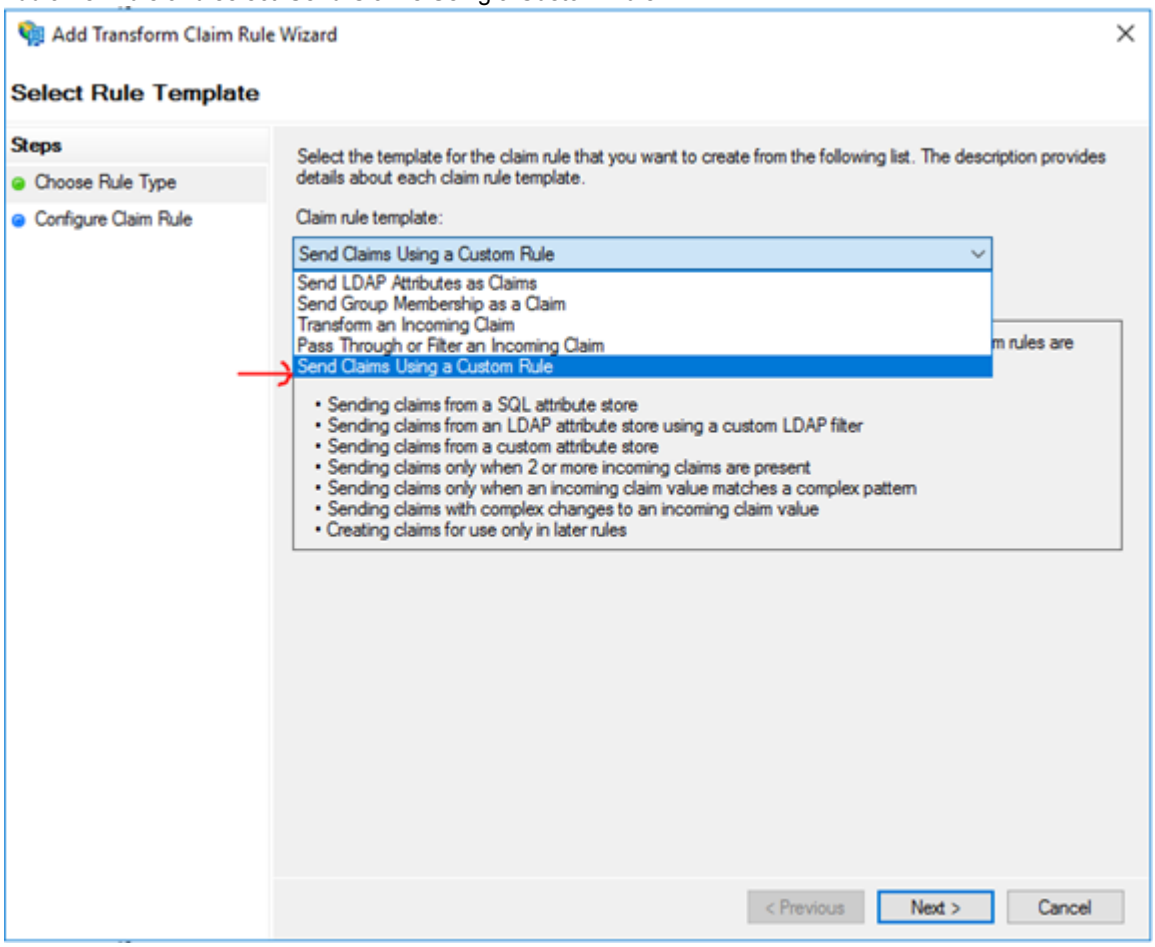


As type choose, LDAP and enter the full LDAP path to the assessmentQ OU. You can see an example in the picture below.



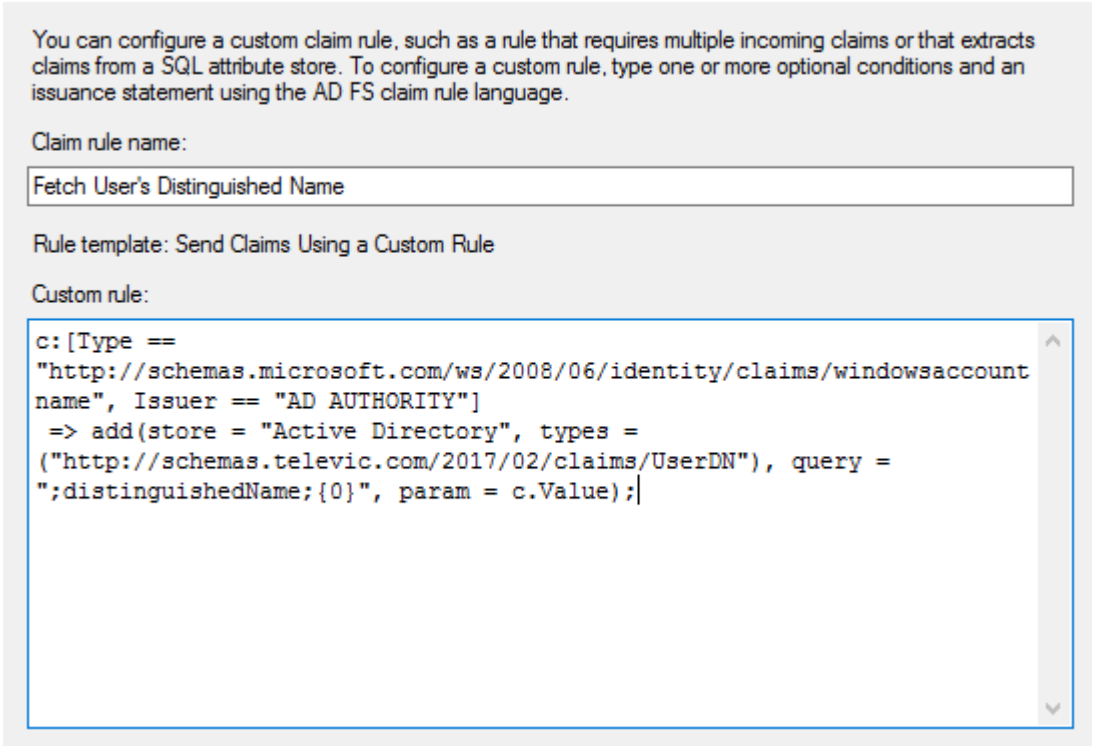
Then we add 2 rules. The first rule is to find the current user's Distinguished Name. The second is to find all groups which this user is member of inside the assessmentQ OU.

1. Add a new rule and select 'Send Claims Using a Custom Rule'



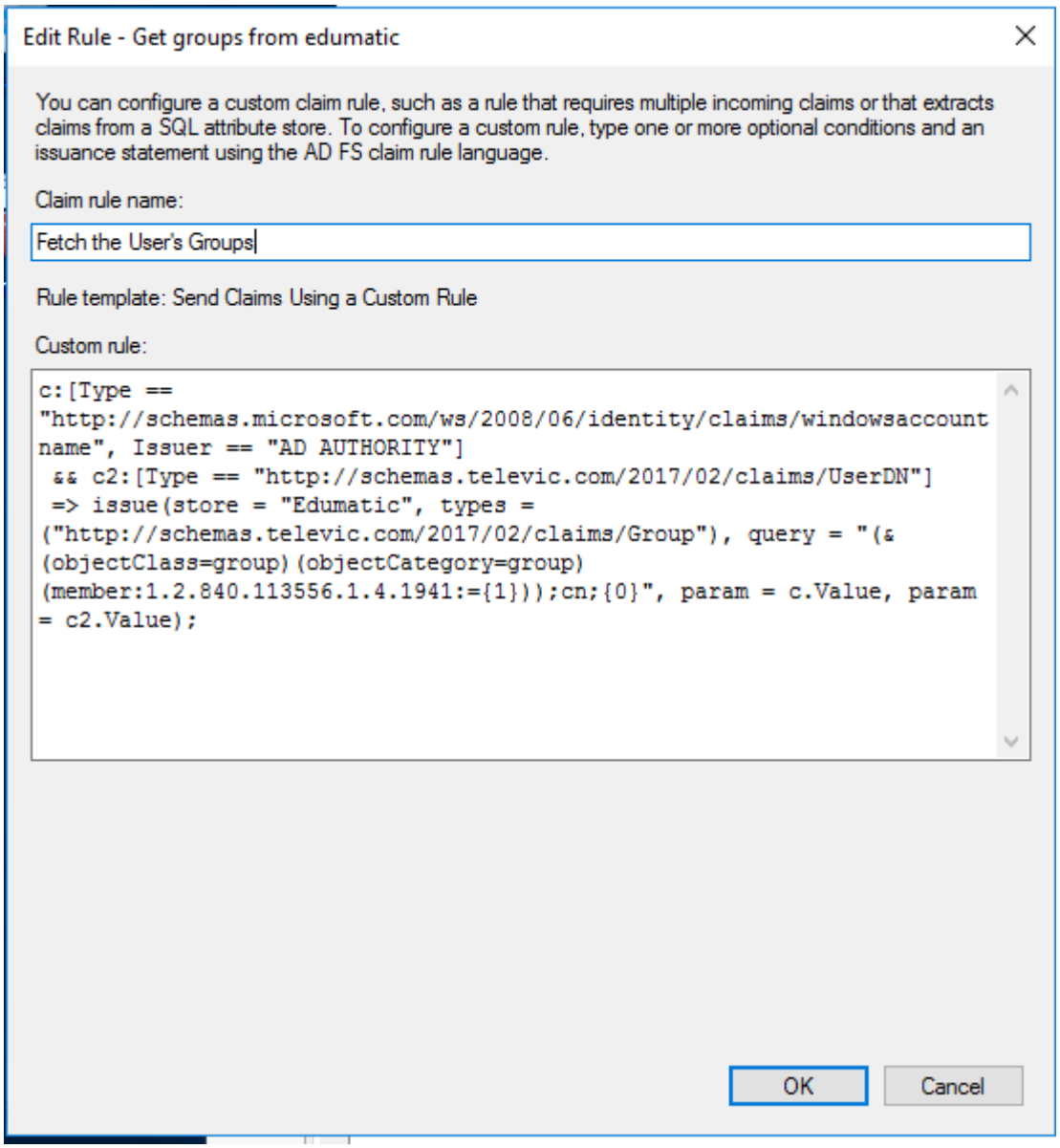
2. Name the rule 'Fetch User's Distinguished Name'.
   For the rule body, copy and post the code below. This query will fetch the User's Distinguished Name and store it in the UserDN claim.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"] => add(store = "Active Directory", types = ("http://schemas.televic.com/2017/02/claims/UserDN"),
query = ";distinguishedName;{0}", param = c.Value);
```



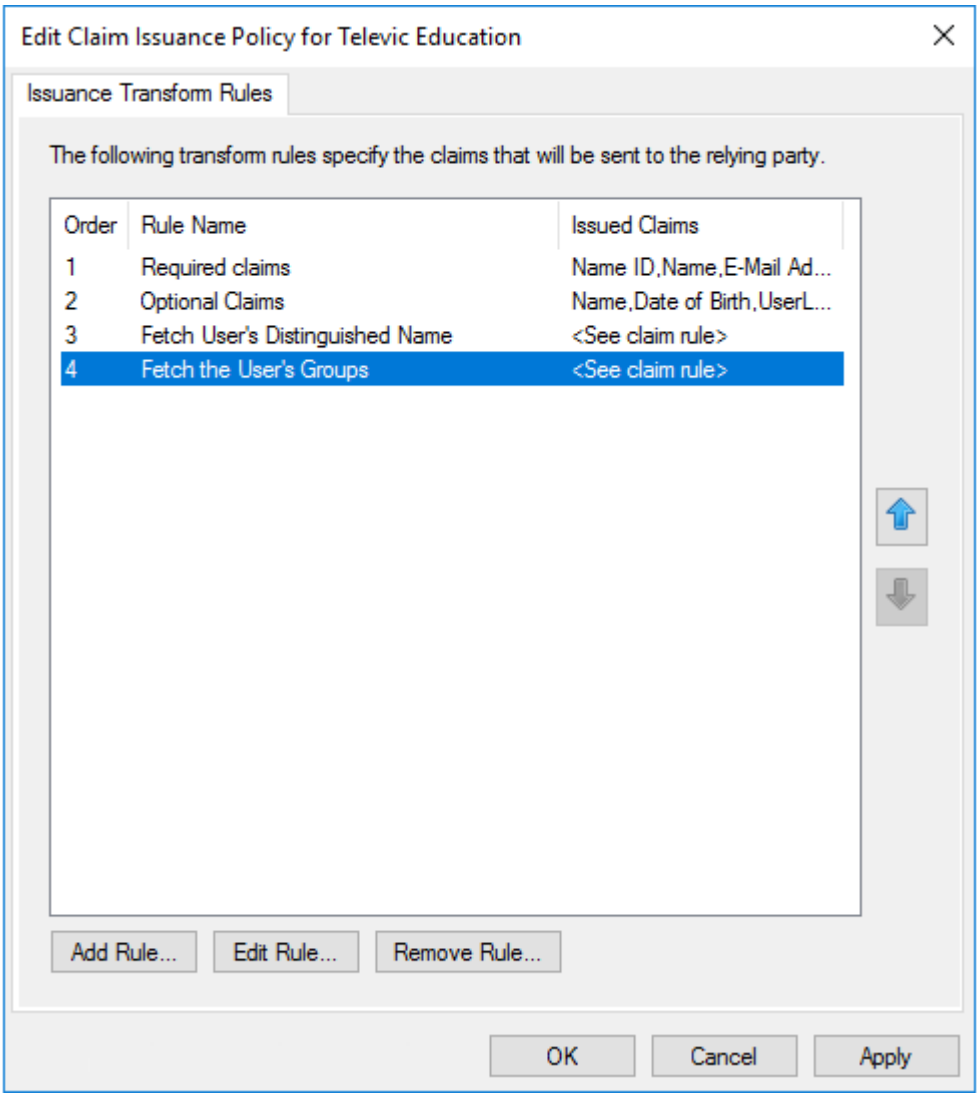
3. Add another custom rule like above.
   Name it 'Fetch the User's Groups'.
   For the rule body, copy and paste the code below. This query will fetch the groups (recursivly) of a user (depending on the UserDN) in the assessment Attribute store. This will limit only the groups in the OU.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
 && c2:[Type == "http://schemas.televic.com/2017/02/claims/UserDN"]
 => issue(store = "Edumatic", types = ("http://schemas.televic.com/2017/02/claims/Group"), query = "(&(objectClass=group)(objectCategory=group)(member:1.2.840.113556.1.4.1941:={1}));cn;{0}", param = c.Value, param = c2.Value);
```



3.4 Overview of the Issuance Transform Rules

Finally the 'Issuance Transform Rules' should look something like below.



4 Testing

The following URLs can be used for testing.

For authors (content-creators) and coaches (who need to see the reporting) the url will be:

https://*<your_identifier>*.backoffice.assessmentq.com

For candidates (who take the tests) the url will be:

https://*<your_identifier>*.assessmentq.com

[1] In this case it is the responsibility of the customer to signal changes in the metadata file to Televic.