

Televic Education

ADFS - Example configuration

17 August 2023

Created by Lynn Van den Broeck



Table of contents

1	Introduction.....	3
2	Requirements	3
3	Configuration	3
3.1	Configuring the Relying Party Trust	3
3.2	Configuring claims	9
3.3	Adding support for synchronizing groups between ADFS and Edumatic	13
3.3.1	Organizing Groups within the AD	13
3.3.2	Limitations	15
3.3.3	Passing on groups to assessmentQ	16
3.4	Overview of the Issuance Transform Rules	20
4	Testing	21

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

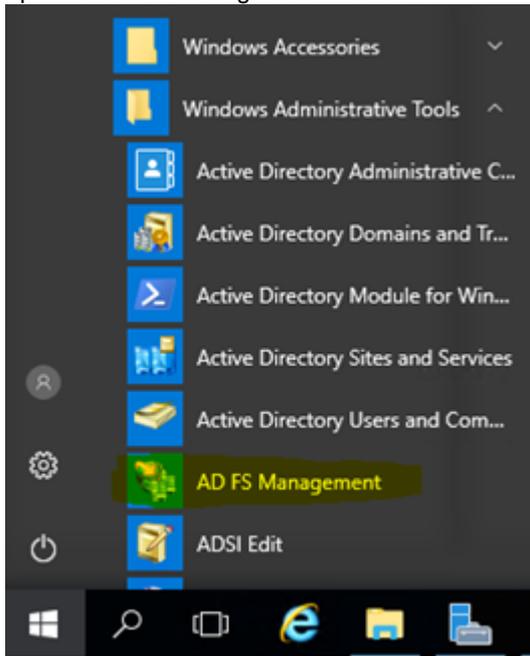
- ADFS 2.0 or higher
- OAuth SHA-2 signature encoding
- Access to the IdP metadata file via direct URL access

3 Configuration

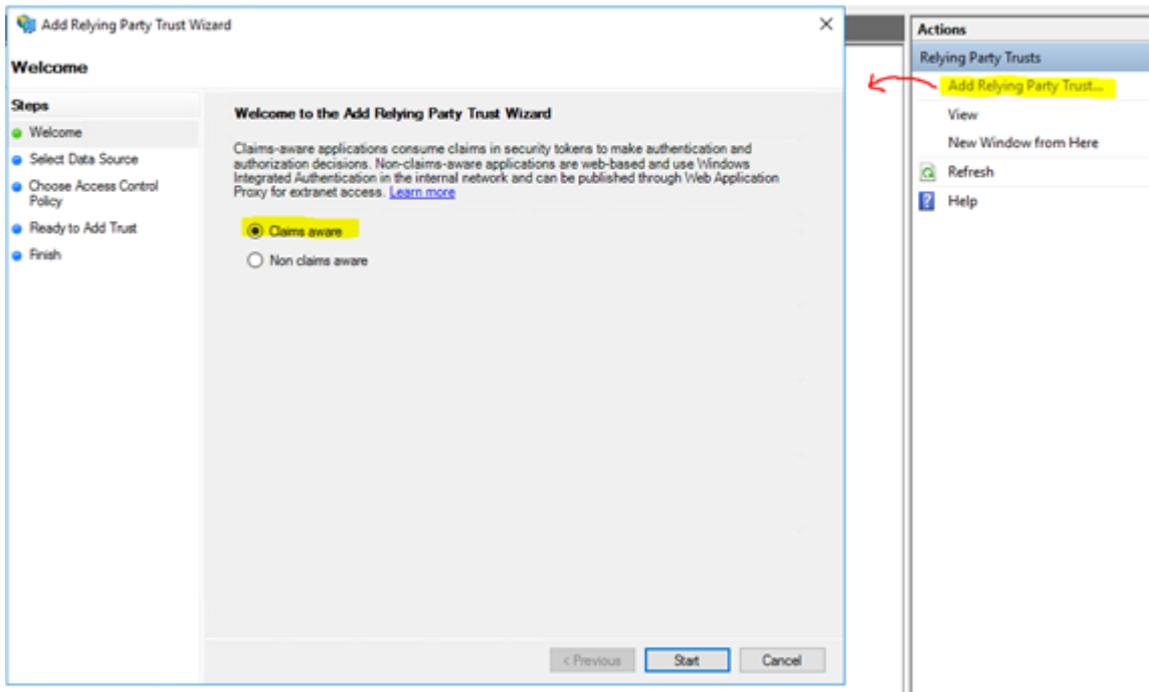
3.1 Configuring the Relying Party Trust

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'.



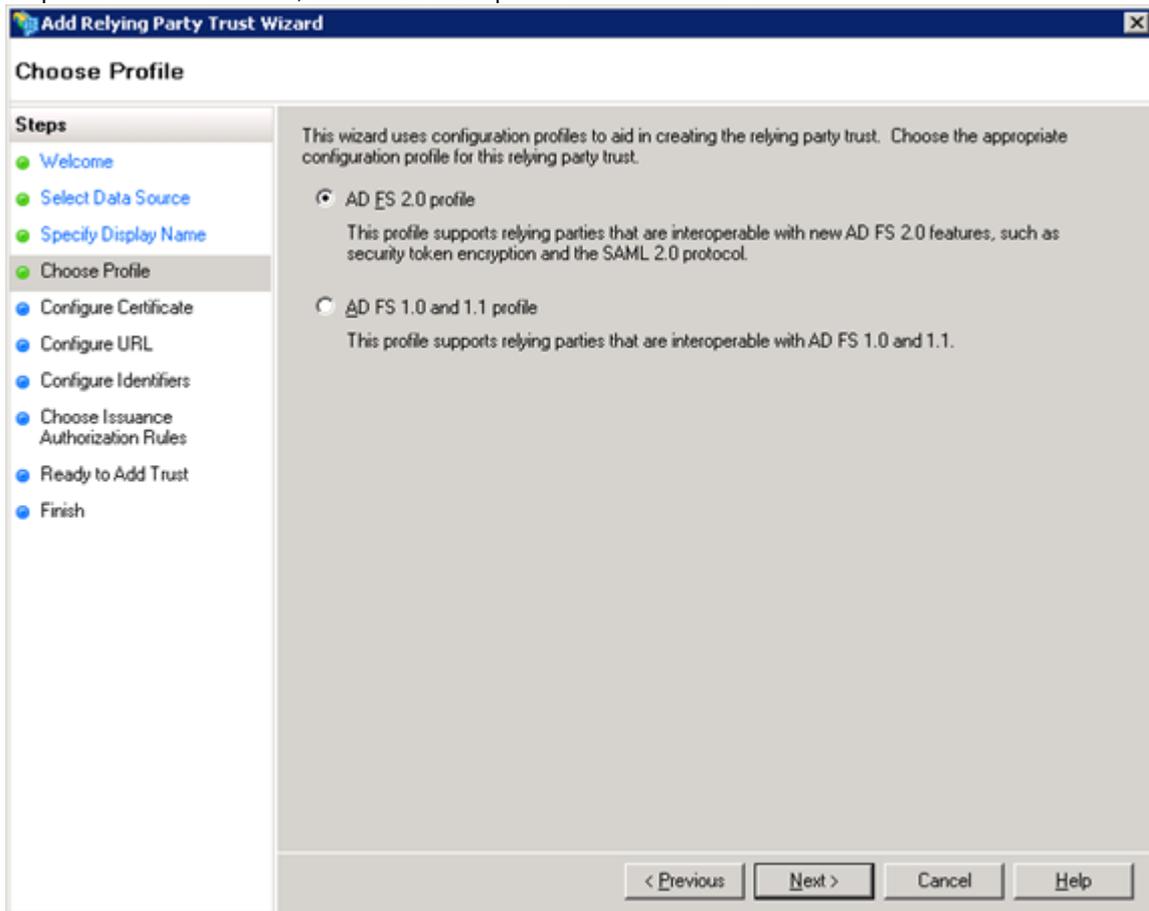
3. Select 'Enter data about the relying party manually' and click 'Next >'.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists: Welcome, Select Data Source (highlighted), Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options: 1. 'Import data about the relying party published online or on a local network' with a text box for 'Federation metadata address (host name or URL):' and an example 'fs.contoso.com or https://www.contoso.com/app'. 2. 'Import data about the relying party from a file' with a text box for 'Federation metadata file location:' and a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected and highlighted in yellow) with a description: 'Use this option to manually input the necessary data about this relying party organization.' At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

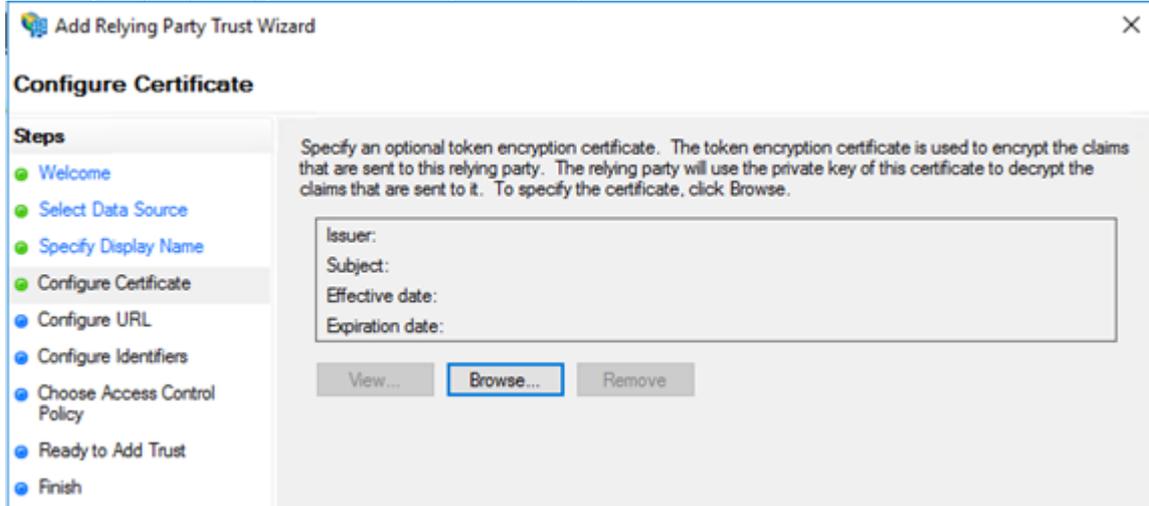
4. Provide a display name for the RP and optional description for the Relying Party and click 'Next >'.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Specify Display Name'. On the left, a 'Steps' pane lists: Welcome, Select Data Source, Specify Display Name (highlighted), Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains a text box for 'Display name:' with the text 'Televic Education' and a larger text area for 'Notes:' with the text 'The Televic Education Identity Server'. At the bottom are '< Previous', 'Next >', and 'Cancel' buttons.

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'

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Configure URL' step. The 'Steps' list on the left includes: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL (highlighted), Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main content area contains the following text: 'AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.' There are two checked options: 'Enable support for the WS-Federation Passive protocol' and 'Enable support for the SAML 2.0 WebSSO protocol'. The 'Relying party WS-Federation Passive protocol URL:' field contains 'https://www.sign-in.education/e/sso/televic'. Below it is an example: 'Example: https://fs.contoso.com/adfs/ls/'. The 'Relying party SAML 2.0 SSO service URL:' field is empty, with an example: 'Example: https://www.contoso.com/adfs/ls/'.

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).

The screenshot shows the 'Specify the display name and identifiers for this relying party trust' dialog box. It contains the following fields and buttons: 'Display name:' with the value 'Televic Education'; 'Relying party identifier:' with the value 'um.televic|sign-in.education' and an 'Add' button; 'Relying party identifiers:' with the value 'https://www.sign-in.education/e/sso/televic' and a 'Remove' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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'.

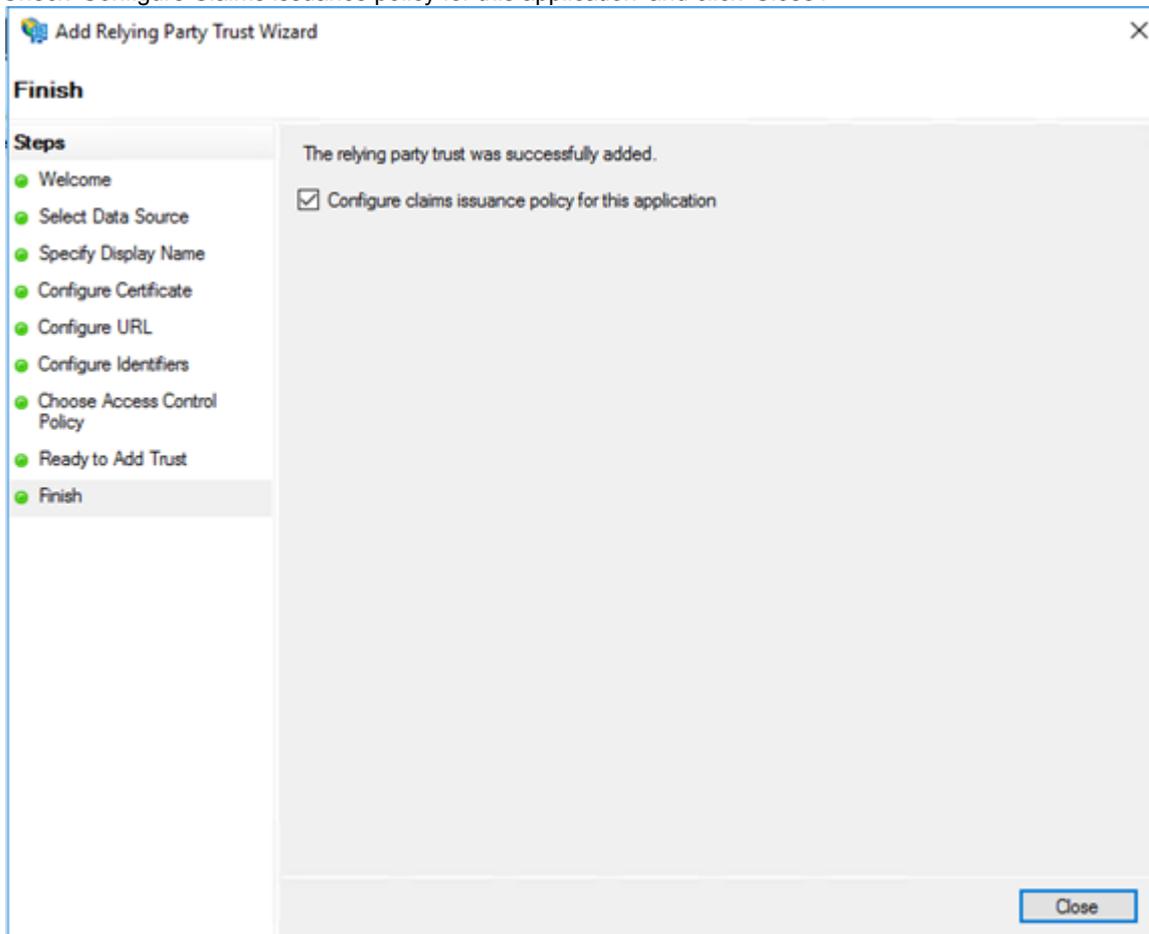
The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Choose Issuance Authorization Rules' step. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Choose Issuance Authorization Rules (highlighted), Ready to Add Trust, and Finish. The main area contains the following text: 'Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.' There are two radio button options: 'Permit all users to access this relying party' (selected) and 'Deny all users access to this relying party'. Below these options is a note: 'You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.' At the bottom, there are buttons for '< Previous', 'Next >', 'Cancel', and 'Help'.

or

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box, specifically the 'Choose Access Control Policy' step. The 'Steps' pane on the left lists the following steps: Welcome, Select Data Source, Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy (highlighted), Ready to Add Trust, and Finish. The main area contains the following text: 'Choose an access control policy:'. Below this is a table with two columns: 'Name' and 'Description'. The table lists several policies, with 'Permit everyone' selected. Below the table is a 'Policy' field containing the text 'Permit everyone'.

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for a specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registr...	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

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.

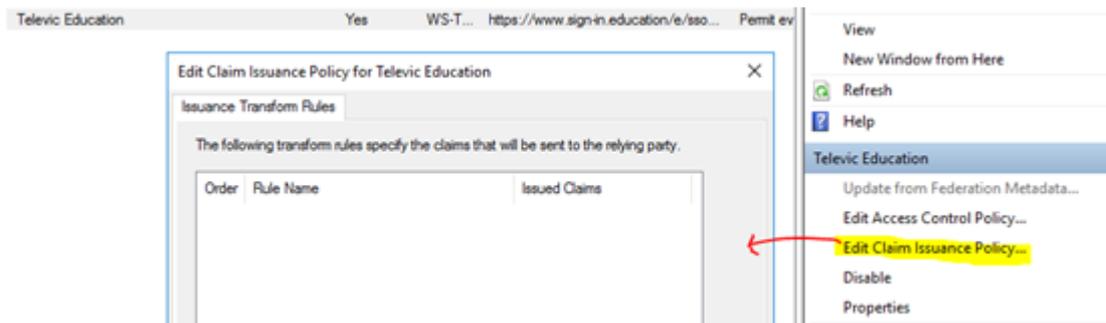
Important note: before continuing, check if the claims is already present.

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



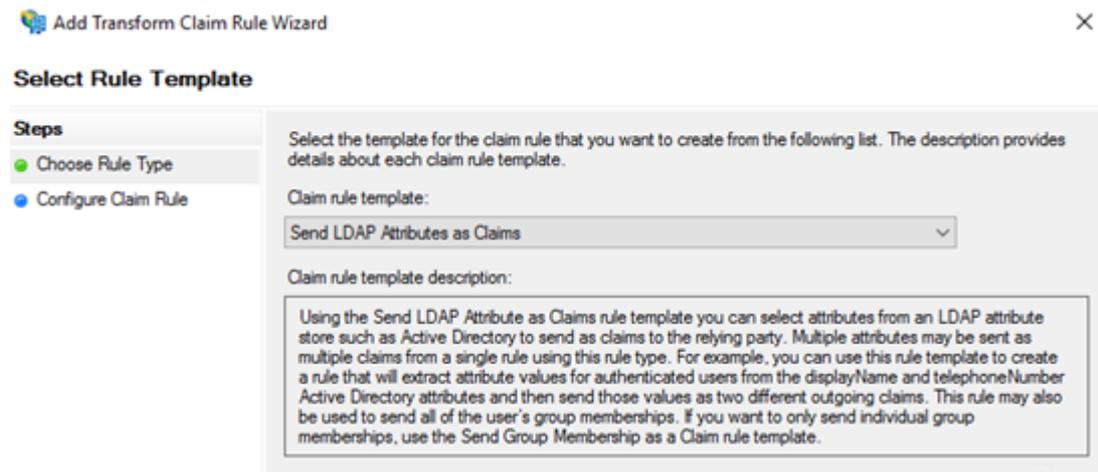
OR

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

Nameld claim.

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:

Required claims

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	Name ID
▶	E-Mail-Addresses	E-Mail Address
	Surname	Surname
	Given-Name	Given Name
*		

4. Optionally another Claim rule can be added to provide for:

- a. User name

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>

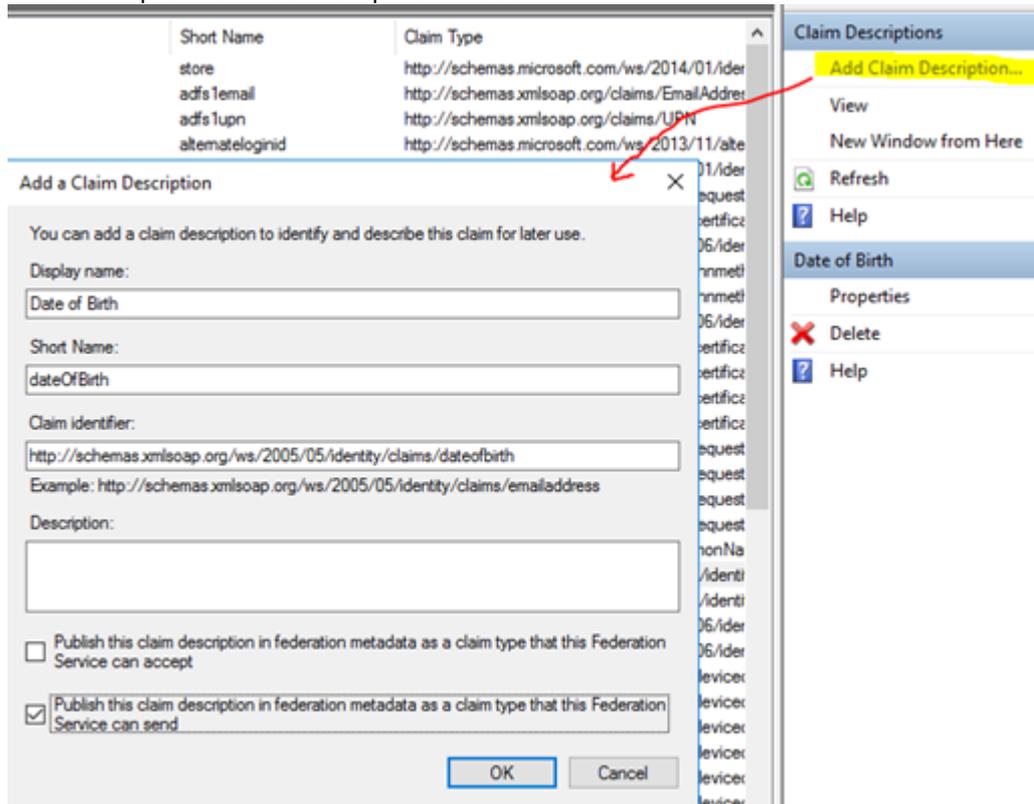
This claim is added to the Claim Descriptions by default.

- 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 >

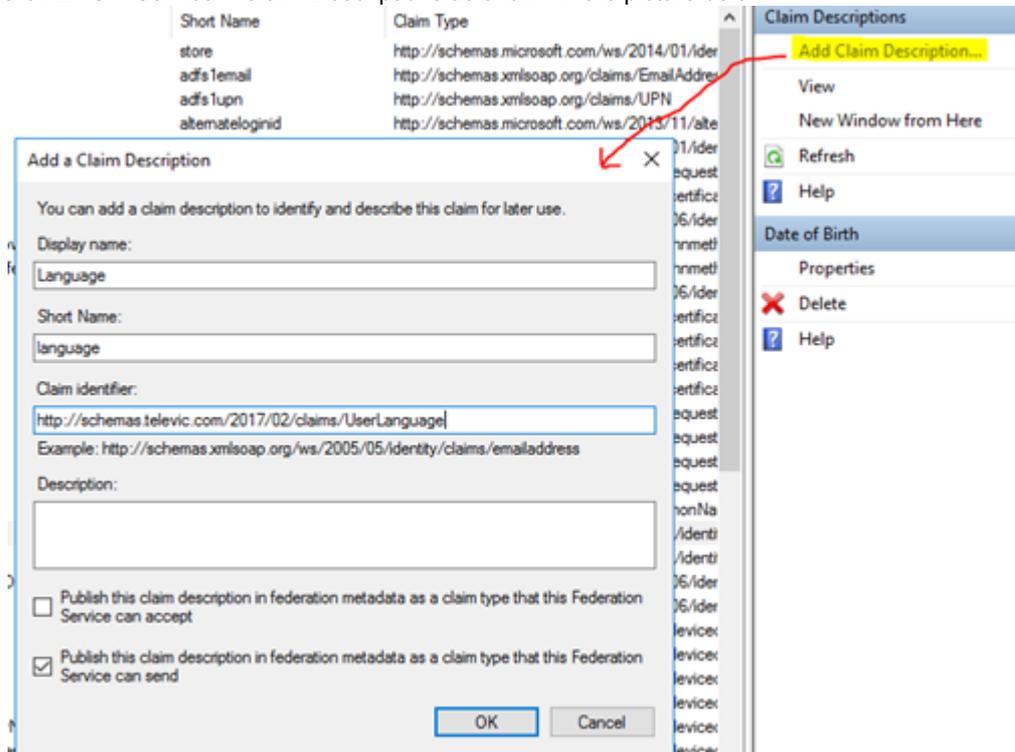
Claim Descriptions as show in the picture below.



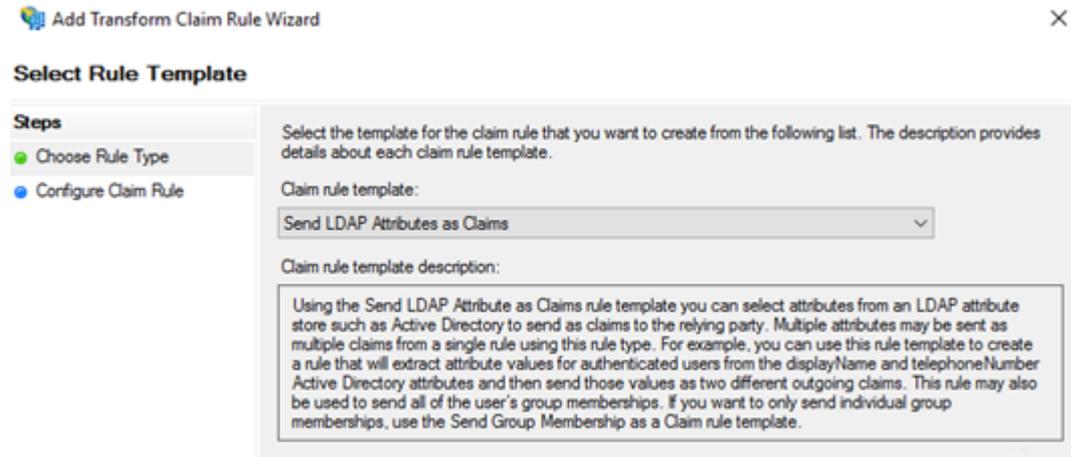
c. UserLanguage

<http://schemas.televic.com/2017/02/claims/UserLanguage>

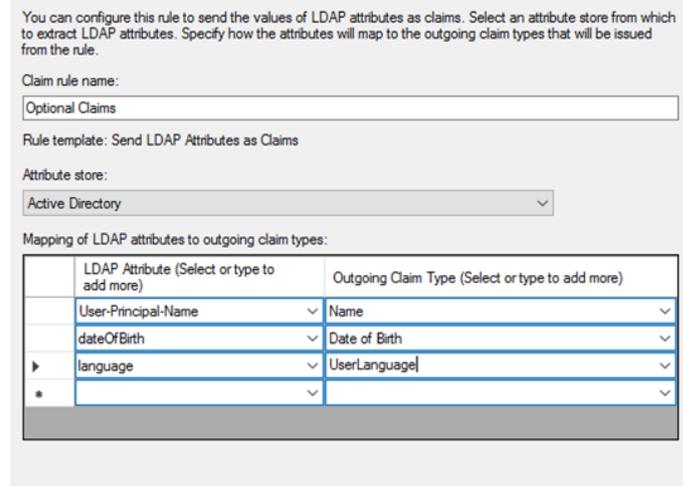
This claim is defined by Televic and is not added to the Claim Descriptions by default. It can be added in the ADFS > Service > Claim Descriptions as shown in the picture below.



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

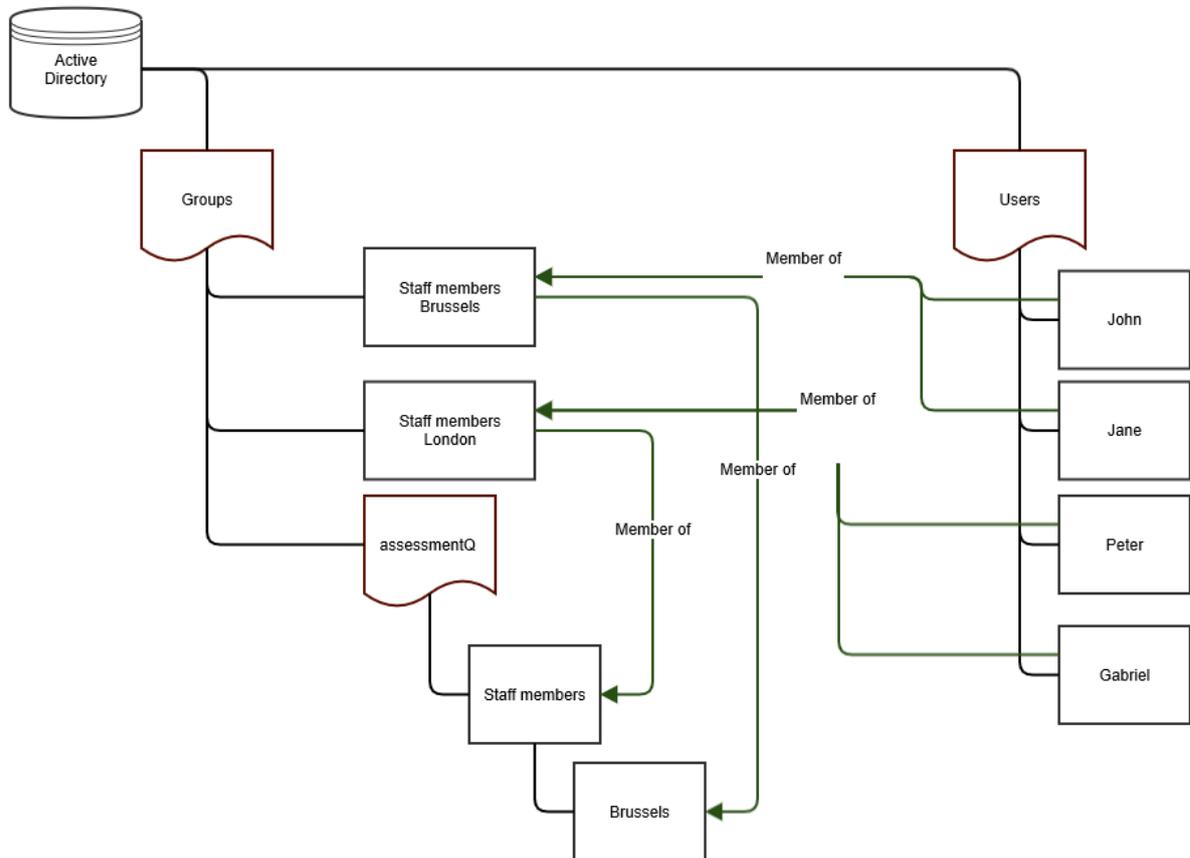
The diagram below depicts the coupling between users and groups in Active Directory (AD) and assessmentQ.

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*.

- Peter and Gabriel are members of the AD group *Staff members London*. This group, in turn, is member 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.

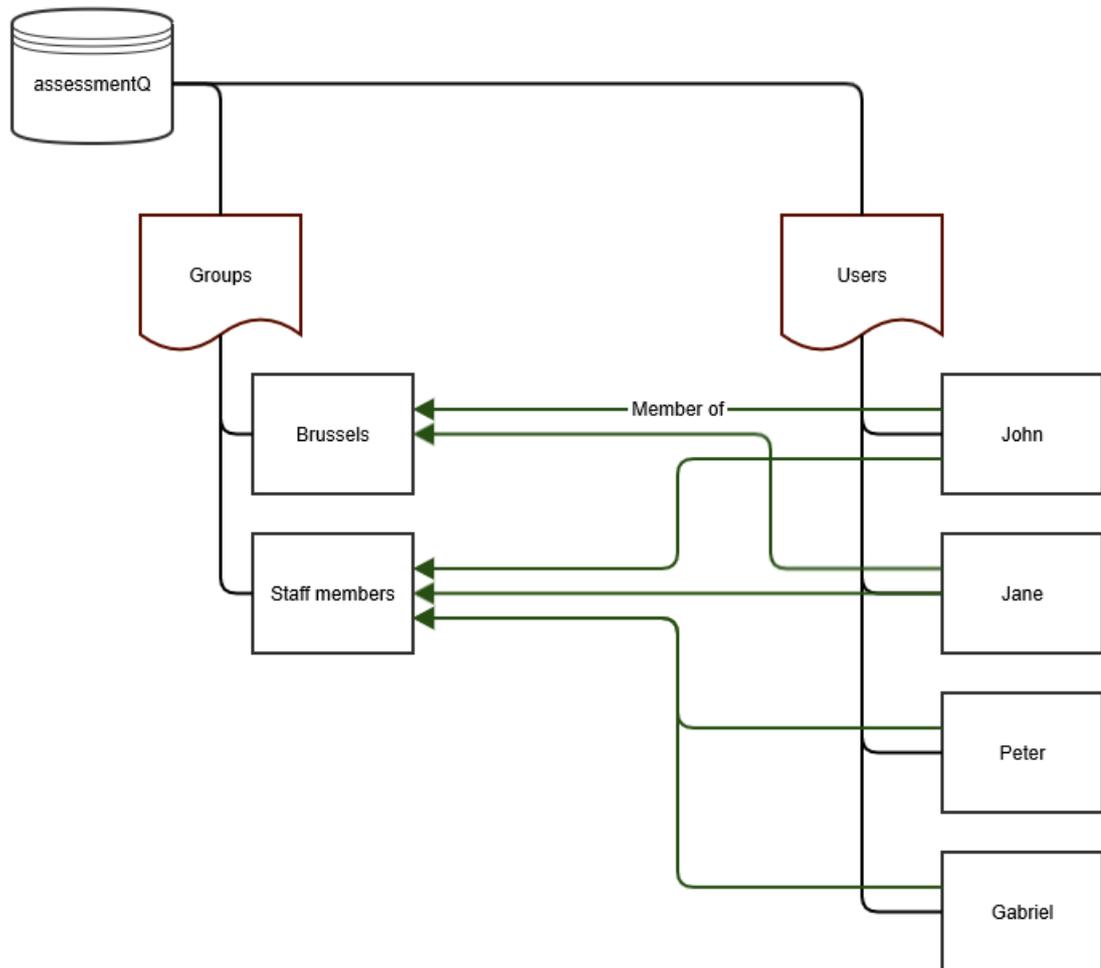
When John signs in to *assessmentQ* (via the ADFS coupling), the groups *Staff members* and *Brussels* are automatically created in *assessmentQ* and John is added to these groups. These groups will not be nested in *assessmentQ* and will exist next to each other.

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:



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.

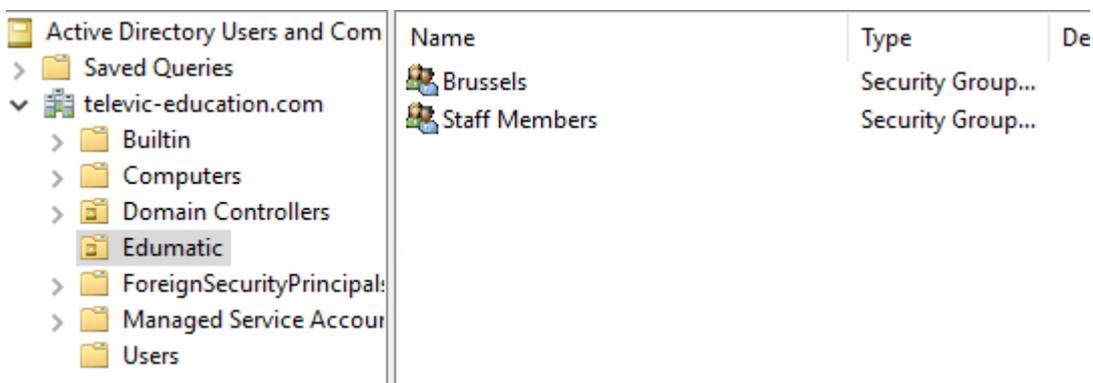
Automatically deleting a user from groups is not supported through ADFS. Also, this could have an impact on reporting and obtained results. As such, if users change groups in AD, they should **manually be removed** from the corresponding assessmentQ group (if needed).

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.

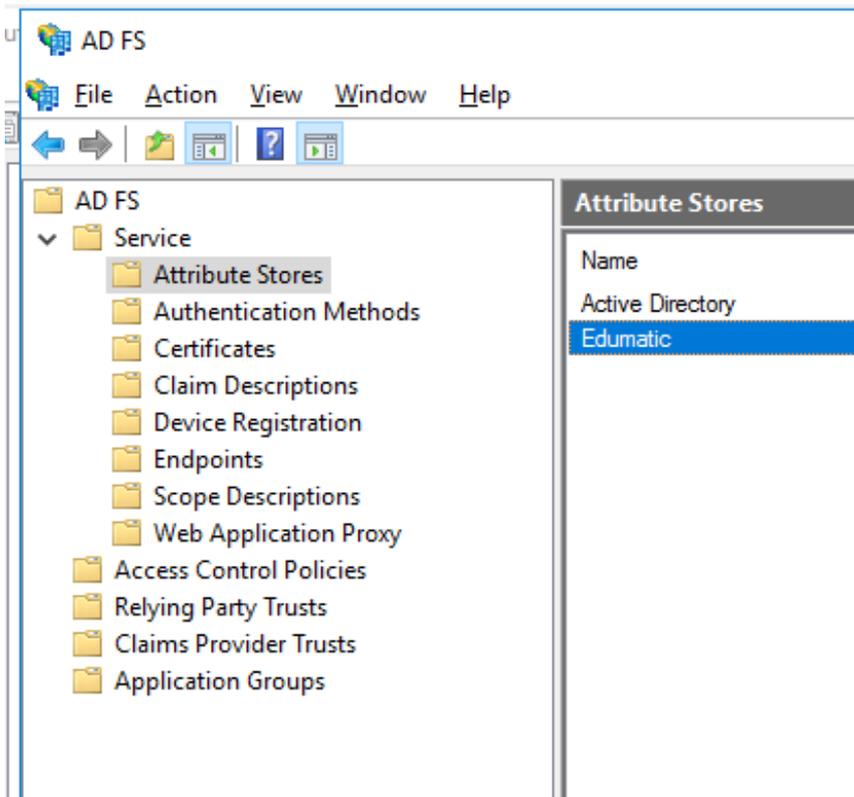
 assessmentQ was formerly called Edumatic. In the screenshots below the name Edumatic is still used instead of assessmentQ.



	Name	Type	De
Active Directory Users and Com			
> Saved Queries			
▼ televic-education.com			
> Builtin			
> Computers			
> Domain Controllers			
Edumatic	Brussels	Security Group...	
> ForeignSecurityPrincipal:	Staff Members	Security Group...	
> Managed Service Account			
Users			

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).

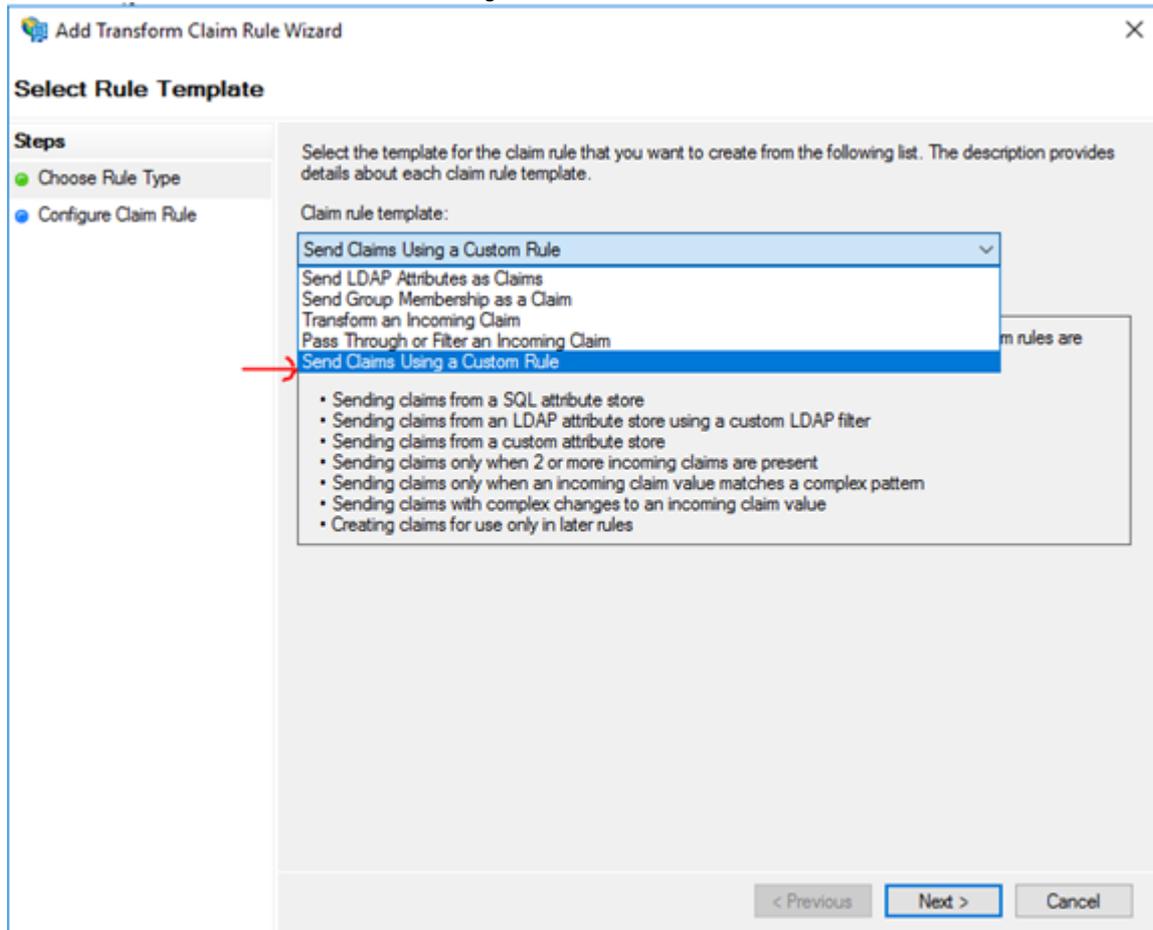


As type choose, LDAP and enter the full LDAP path to the assessmentQ OU. You can see an example in the picture below.

Display name:	Edumatic
Attribute store type:	LDAP
Connection string:	LDAP://televic-education.com/OU=Edumatic,DC=televic-education,DC=com

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);
```

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Fetch User's Distinguished Name

Rule template: Send Claims Using a Custom Rule

Custom rule:

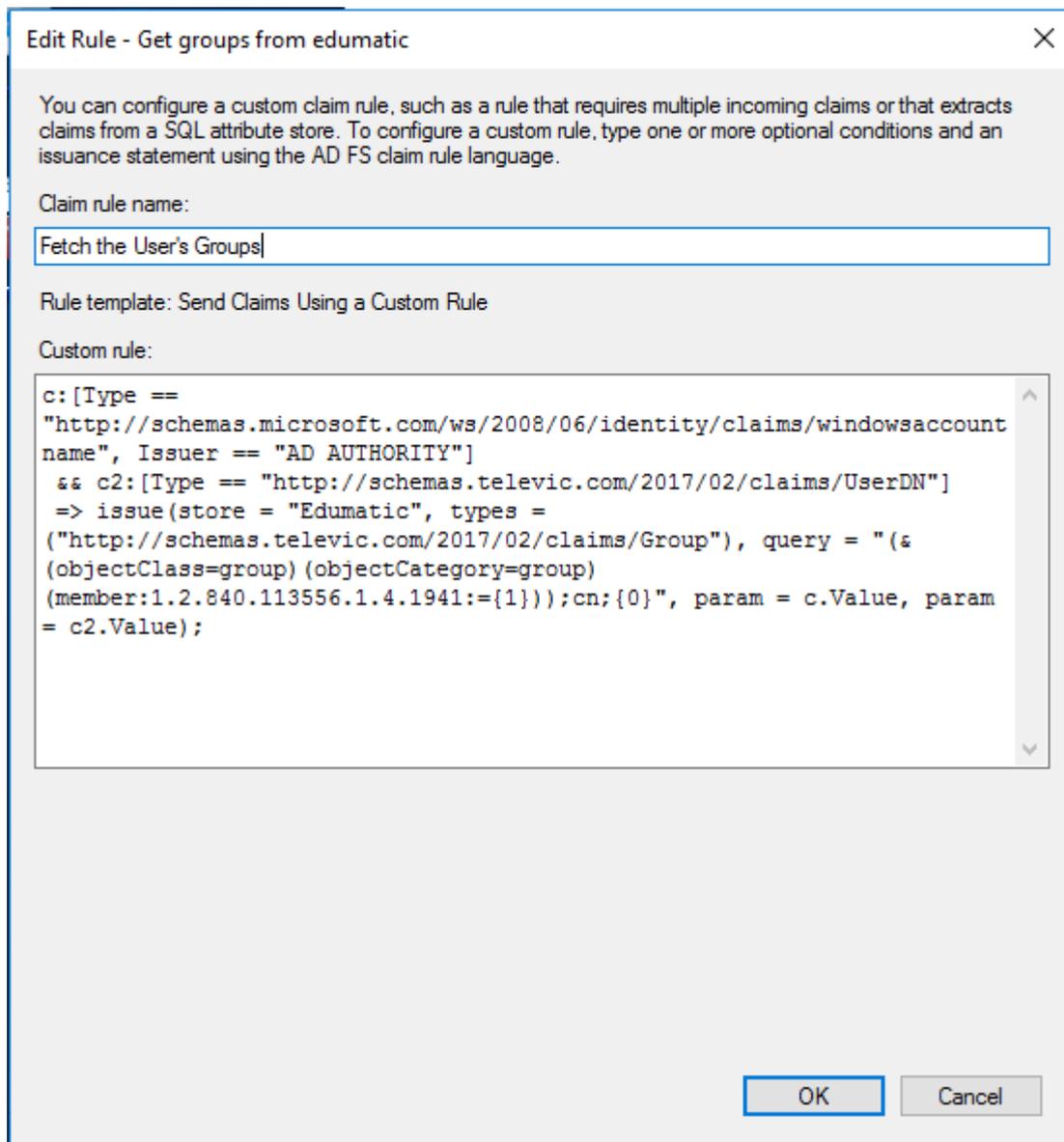
```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types =
("http://schemas.televic.com/2017/02/claims/UserDN"), query =
";distinguishedName;{0}", param = c.Value);|
```

3. Add another custom rule like above.

Name it 'Fetch the User's Groups'.

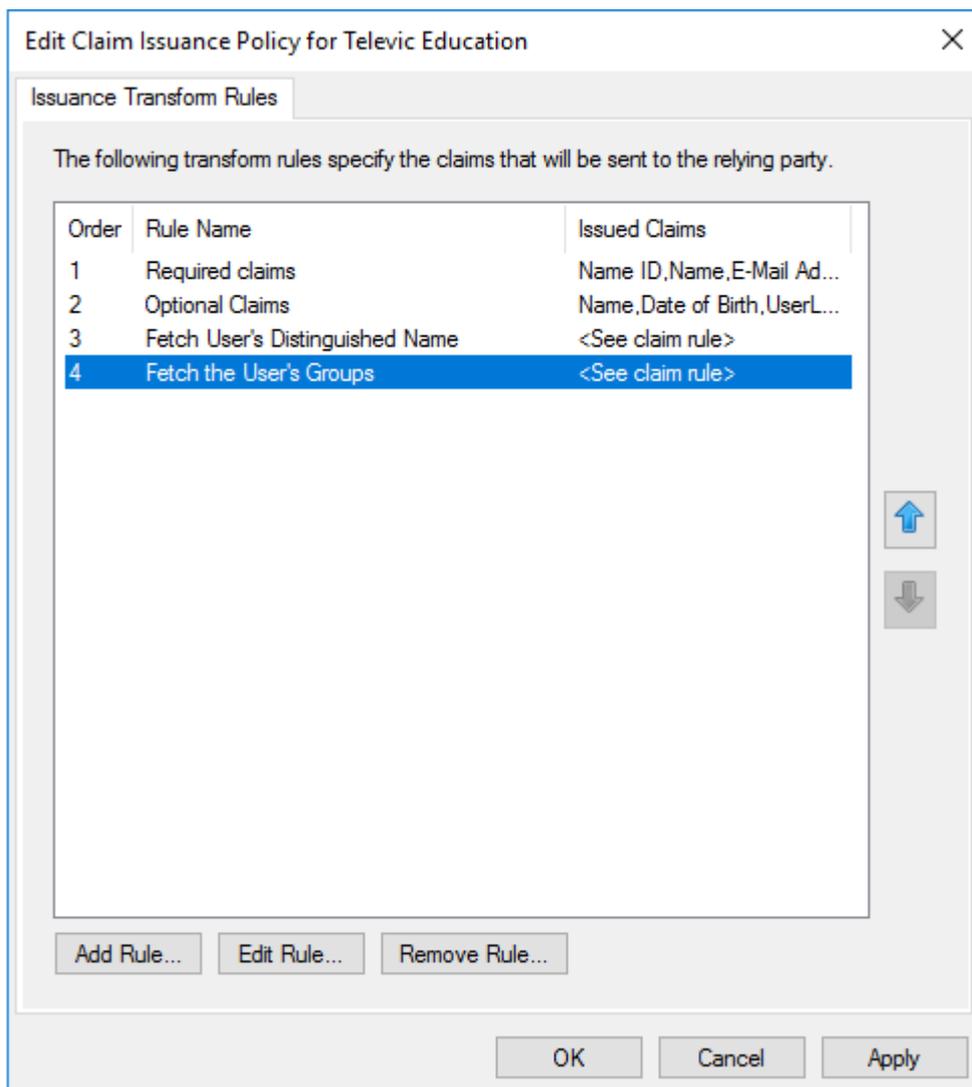
For the rule body, copy and paste the code below. This query will fetch the groups (recursively) of a user (depending on the UserDN) in the assessment Attribute store. This will limit only the groups in the OU.

```
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.