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'.

💱 Add Relying Party Trust Wizard			Actions		
Welcome			Rel	ying Party Trusts	
Tressence		5		Add Relying Party Trust	
Steps Welcome to the Add Relying Party Trust Wizard			-	View	
 Welcome Claims, suggest another strong consume claims in security takens to make authentication and 				New Window from Here	
 Select Data Source authorization decisions. Non-claims-aware applications are web-based and use Windows 			a	Refresh	
Choose Access Control Policy Policy Choose Access Control Proxy for extranet access. Learn more			2	Help	
Ready to Add Trust Claims aware					
Finish O Non claims aware					
< Previous Start Cancel					
	_	1			

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

翰 Add Relying Party Trust Wizard

Select Data Source	
Select Data Source Steps • Welcome • Select Data Source • Specify Display Name • Configure Certificate • Configure URL • Configure Identifiers • Choose Access Control Policy • Ready to Add Trust • Finish	Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported to federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Erderation metadata file location: Browse Performance of the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

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

Specify Display Name

Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	Televic Education
Specify Display Name	Ngtes:
 Configure Certificate 	The Televic Education Identity Server
 Configure URL 	
Configure Identifiers	
 Choose Access Control Policy 	
Ready to Add Trust	
 Finish 	



 \times

 \times

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

 This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust. AD ES 2.0 profile This profile supports relying parties that are interoperable with new AD FS 2.0 features, such as security token encryption and the SAML 2.0 protocol. △ D FS 1.0 and 1.1 profile This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1. 					
<u>< P</u> revious <u>N</u> ext > Cancel <u>H</u> elp					
ption certificates (leave blank)					
Image: State of the state o					
Specify an onlineal taken encomion certificate. The taken encomption certificate is used to encomp the claims					

0	Choose	Access	Control
	Policy		

- Ready to Add Trust
- Finish

View	Browse



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

🖬 Add Relying Party Trust Wizard

Configure URL

Steps	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties, #
Welcome	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-Taut optional is always enabled for a relying party.
Select Data Source	Finable support for the WS-Federation Passive protocol
Specify Display Name	The WC Enderstice Descine entered UDL exceeds Web however bread elvice encoders using the
Configure Certificate	WS-Federation Passive protocol. WS-Federation Passive protocol.
Configure URL	Relying party WS-Federation Passive protocol URL:
 Configure Identifiers 	https://www.sign-in.education/e/sso/televic
 Choose Access Control Policy 	Example: https://fs.contoso.com/adfs/ls/
Ready to Add Trust	Engble support for the SAML 2.0 WebSSO protocol
 Finish 	The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.
	Relying party <u>S</u> AML 2.0 SSO service URL:
	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>

 Provide the Relying Party trust identifier (not the one in the screenshot). Specify the display name and identifiers for this relying party trust.

Display name:	
Televic Education	
Relying party identifier:	
um. <mark>televic s</mark> ign-in.education	Add
Example: https://fs.contoso.com/adfs/services/trust	
Relying party identifiers:	
https://www.sign-in.education/e/sso/televic	Remove
OK Cancel	Apply

televic

 \times

urn: < your_identifier>.idp.assessmentq.com

<u>Note:</u> subdomain is case sensitive and should always be lower case.9. Select 'Permit all users to access this relying party'.

🙀 Add Relying Party Trust	Wizard
Choose Issuance Aut	thorization Rules
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure Identifiers Choose Issuance Authorization Rules Ready to Add Trust Finish	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. Permit all users to access this relying party The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access. Deny all users access to this relying party The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party. You must later add issuance authorization rules to rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.
	< <u>Previous</u> <u>Next</u> > Cancel <u>H</u> elp

翰 Add Relying Party Trust Wizard

Choose Access Control Policy

Steps	Choose an access control policy:				
 Welcome Select Data Source Specify Display Name 	Name Permit everyone Permit everyone and require MFA Permit everyone and require MFA for specific group	Description Grant access to everyone. Grant access to everyone and requir	^		
 Configure Certificate Configure URL Configure Identifiers 	Permit everyone and require MPA for specific group Permit everyone and require MFA from extranet access Permit everyone and require MFA from unauthenticated devices Permit everyone and require MFA, allow automatic device registr	Grant access to everyone and requir Grant access to the intranet users ar Grant access to everyone and requir Grant access to everyone and requir			
 Choose Access Control Policy 	Pemit everyone for intranet access Pamit enantics are in <	Grant access to the intranet users.	~		
 Ready to Add Trust Finish 	Policy Permit everyone				

televic

×

- 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'.

🐏 Add Relying Party Trust	Wizard	×
Finish		
Steps	The relying party trust was successfully added.	
 Welcome 		
Select Data Source	Configure claims issuance policy for this application	
Specify Display Name		
Configure Certificate		
Configure URL		
Configure Identifiers		
 Choose Access Control Policy 		
Ready to Add Trust		
Finish		
		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'

📬 AD FS 2.0		
📢 Elle Action Yiew Window Help		
🗢 🔿 🖄 📷 📓 📷		
AD F5 2.0	Claims Provider Trusts	
Service Trust Relationships	Display Name	Enabled
Claims Provider Trusts	Active Directory	Yes
Relying Party Trusts		
Attribute Stores	1	

or

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



- 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
- 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 🗸 🗸
	Sumame ~	Sumame 🗸 🗸
	Given-Name 🗸 🗸	Given Name 🗸 🗸
*	~	~

 \sim

- 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.

	Short Name	Claim Type		^	Cla	im Descriptions
	store	http://schemas.microsoft.com	/ws/2014/	/01/ider		Add Claim Description
	adfs1email	http://schemas.xmlsoap.org/o	laims/Ema	Addres	\sim	10
	adfs1upn	http://schemas.xmlsoap.org/o	laims/UP		I 1	View
	alternateloginid	http://schemas.microsoft.com	/ws/2013/	/11/ate		New Window from Here
Add a Claim Descri	iption	1	×)1/ider	۵	Refresh
You can add a clair	m description to identify and des	cribe this claim for later use.		entifica	?	Help
Display name:				hornett	Dat	e of Birth
Date of Birth				temnet		Properties
Short Name:)6/ider vertificz	×	Delete
dateOfBirth				etifica	?	Help
C				setifica		
Claim identifier:				settrica	I 1	
http://schemas.xml	soap.org/ws/2005/05/identity/o	claims/dateofbirth		equest	I 1	
Example: http://sch	nemas.xmlsoap.org/ws/2005/05	/identity/claims/emailaddress		equest		
Description:				equest		
				nonNa	I 1	
				/identi	I 1	
				/identi	I 1	
Dublish this slais	n deseriation in federation materia	late as a claim has a that this East	lanting)6/ider	I 1	
Service can acc	n description in rederation metad	ata as a ciaim type that this rec	peration	06/ider	I 1	
				evicer	I 1	
Publish this clair	n description in federation metad	lata as a claim type that this Fed	deration	evicer		
Service can ser	ia.			evicer		
		04 0	Incel	evicer		
		UN La	a i dei	evicer		
				evicer		

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.

	S	Short Name Claim Type		^		Clai	m Descriptions	
	st	ore	http://schemas.microsoft.com	n/ws/2014/0)1/ider	Ц	_	Add Claim Description
	a	dfs1email	http://schemas.xmlsoap.org/	claims/Email	Addres			View
	6 (c	Its Tupn temateloginid	http://schemas.xmisoap.org/	claims/UPN	11/ate			New Window from Here
ſ		i i i i i i i i i i i i i i i i i i i	The state and the state of the state)1/ider	Ш		Pafrach
l	Add a Claim Descripti	on		∠ ×	squest	Ш	<u>u</u>	Kerresn
	You can add a claim de	escription to identify and der	cribe this claim for later use.		etifica	Ш	2	Help
1	Display name:				/6/ider		Dat	e of Birth
ħ	Language				nmeth	IIF		Properties
	Chard Names	J6/der					×	Delete
	Short Name:				etfica	Ш	2	Help
I	language						1	ricip
	Claim identifier:					11		
	http://schemas.televic.	.com/2017/02/claims/User	Language		squest	11		
I	Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress							
I	Description:		equest	11				
I	-				tonNa	Ш		
1					/identi	Ш		
					/identi	Ш		
2	Builds this also description is for any first and data are added to be that this Forderation							
I	Publish this claim description in rederation metadata as a claim type that this rederation Service can accept)6/ider	Ш		
I								
	Publish this claim de	Publish this claim description in federation metadata as a claim type that this Federation Service can send						
I	 Service can send 					Ш		
ľ			OK C	ancel	evicer			
1					eviced			

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

Select Rule Templa	te					
Steps	Select the template for the claim rule that you want to create from the following list. The description provides					
Choose Rule Type	details about each claim rule template.					
 Configure Claim Rule 	Claim rule template:					
	Send LDAP Attributes as Claims 🗸					
	Claim rule template description:					
	Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Memberships as Claim rule template.					

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.

from th	act LDAP attributes. Specify how the attrit ne rule.	bute	s will map to the outgoing claim types that will be issued	1	
Claim	rule name:				
Option	nal Claims				
Rule to	emplate: Send LDAP Attributes as Claims				
Attribu	te store:				
Activ	e Directory		~		
Маррі	ng of LDAP attributes to outgoing claim ty	pes	:		
	LDAP Attribute (Select or type to add more) Outgoing Claim Type (Select or type to add more)				
	User-Principal-Name	\sim	Name	\sim	
	dateOfBirth	\sim	Date of Birth	\sim	
•	language	\sim	UserLanguage	\sim	
		\sim		\sim	
· ·					
-					

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:



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).

<u>Tip:</u> 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).



翰 AD FS	
翰 <u>F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp)
🗢 🔿 🞽 🖬 👔 🕞	
AD FS	Attribute Stores
Service Attribute Stores	Name
Authentication Methods	Active Directory
Certificates	Edumatic
Claim Descriptions	
Device Registration	
Endpoints	
Scope Descriptions	
Web Application Proxy	
Access Control Policies	
Claims Provider Trusts	
Application Groups	

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'



 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 (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.

Edit	Claim	Issuance Policy for Televic Educa	ation	×
Issua	ance 1	ransform Rules		
Tł	he follo	wing transform rules specify the claim	ns that will be sent to the relying party.	
(Order	Rule Name	Issued Claims	
	1	Required claims	Name ID,Name,E-Mail Ad	
	2	Optional Claims	Name,Date of Birth,UserL	
	3	Fetch User's Distinguished Name	<see claim="" rule=""></see>	
	4	Fetch the User's Groups	<see claim="" rule=""></see>	
				_IL
	Add R	ule Edit Rule Remove	Rule	
			OK Cancel	Apply

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.

