

Televic Education

OpenID Connect

17 August 2023

Created by Lynn Van den Broeck



Table of contents

- 1 Introduction.....3
- 2 Requirements3
- 3 Configuration of the Identity Provider3
 - 3.1 Scopes 3
 - 3.2 Mapping users 5
- 4 Connection details and settings6
 - 4.1 Information provided by Televic Education 6
 - 4.2 Information to provide by the Identity Provider 7

1 Introduction

OIDC or OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. (OpenID.net)

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

assessmentQ uses OpenID Connect through [IdentityServer](#) to authenticate users.

2 Requirements

The requirements are straightforward:

- An OIDC enabled Identity Provider (Televic Education's recommendation is [IdentityServer](#)) supporting the Authorization Code Grant Flow
- Public access to the Identity Provider
- Support for the following scopes (will be detailed in the next section)
 - openid
 - profile and email (or edumatic_profile)
 - edumatic_info *[optional]*


3 Configuration of the Identity Provider

In this section, we will provide sample instructions on how to configure the Identity Provider in the case of IdentityServer.

3.1 Scopes

The service provider will ask access to the different scopes as detailed in the requirements.

The table below provides more information on the different scopes.

Scope	Description
openid	<p>Informs the Authorization Server that the Client is making an OpenID Connect request.</p> <p>It grants access to the 'subject' or 'nameid' claim which is required. (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier)</p>
profile	<p>This scope value requests access to the End-User's default profile Claims, which are:</p> <p>name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, and updated_at.</p>
email	<p>This scope value requests access to the <code>email</code> and <code>email_verified</code> Claims.</p>
edumatic_profile	<p>This scope is a custom scope for the interoperability between the Identity Provider and the Service Provider. All claims in this scope are required. It grants access to following claims:</p> <ul style="list-style-type: none"> • <code>given_name</code> - <i>A user's first name</i> • <code>email</code> - <i>A valid email address for the user, must be unique</i> • <code>family_name</code> - <i>A user's last name</i> <p>In the case of IdentityServer, this scope would be defined as follows.</p> <pre> new Scope { Name = "edumatic_profile", Description = "The required edumatic profile data. These are Email, GivenName, FamilyName", Required = true, Type = ScopeType.Identity, Claims = new List<ScopeClaim> { new ScopeClaim(Constants.ClaimType.Email, true), new ScopeClaim(Constants.ClaimType.GivenName, true), new ScopeClaim(Constants.ClaimType.FamilyName, true) } } </pre> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> In case of providing the 'edumatic_profile' scope, the scopes 'profile' and 'email' can be omitted.</p> </div>
edumatic_info	<p>This scope is a custom (and optional) scope for adding extra information to a user.</p> <p>It grants access to following claims:</p> <ul style="list-style-type: none"> • <code>Name</code> (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name) - <i>A user's username, this can be used to store an employeeld, or a unique name for a user. If omitted, the email is used.</i>

Scope	Description
	<ul style="list-style-type: none"> • BirthDate (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth) - A user's birthdate, format should be 'yyyyMMdd' e.g. 19880921 means 'sept 21st, 1988'. • UserLanguage (http://schemas.televic.com/2017/02/claims/UserLanguage) - A user's interface language. Supported values are: <ul style="list-style-type: none"> • nl = Dutch • fr = French • de = German • en = English • es = Spanish • it = Italian • ar = Arabic • Group (http://schemas.televic.com/2017/02/claims/Group) - This claimtype supports multiple values, this claim defines a user's membership in an assessmentQ group. For example: "Authors". <p>In the case of IdentityServer, this scope would be defined as follows.</p> <pre data-bbox="571 853 1425 1303"> new Scope { Name = "edumatic_info", Description = "The optional edumatic profile data. These are Username, Birthdate, Language and Groups", Type = ScopeType.Identity, Claims = new List<ScopeClaim> { new ScopeClaim(Constants.ClaimType.Name), new ScopeClaim(Constants.ClaimType.BirthDate), new ScopeClaim("http://schemas.televic.com/2017/02/claims/UserLanguage"), new ScopeClaim("http://schemas.televic.com/2017/02/claims/Group") } } </pre>

3.2 Mapping users

It is up to the Identity Provider to ensure the user's properties are mapped to the correct claims:

- Subject: a unique identifier for the user withing the IdentityProvider. This is not stored in assessmentQ.
- Email: the valid email address for the user (must be unique)
- GivenName: the user's first name
- FamilyName: the user's last name
- Name: the user's username (this can be used to store an employeeld, or a unique name for a user), if omitted the email address will be used
- Birthdate: the user's birth date, format should be 'yyyyMMdd' e.g. 19880921 means 'sept 21st, 1988'
- UserLanguage: the user's interface language (the assessmentQ interface will be displayed in this language)
 - Supported values are:
 - nl = Dutch
 - fr = French
 - de = German
 - en = English
 - es = Spanish

- it = Italian
- ar = Arabic
- Spanish, Italian and arabic are not supported as an interface language. Users with these languages will see the interface in English.
- Groups: this claimtype supports multiple values, this claim defines the user's membership in an assessmentQ group.

4 Connection details and settings

⚠ Important note: The information provided in this section is strictly personal and bound to your assessmentQ environment/channel. Please do not share this information. The information in this section will allow you to setup an SSO in the assessmentQ **DEMO|PRODUCTION** environment for the channel **CHANNEL_NAME**.

In this section, we list the information Televic Education will provide to you (as Identity Provider) and also need to receive from you in order to successfully setup the SSO between both platforms.

4.1 Information provided by Televic Education

In order to configure assessmentQ as a client in the Identity Provider, we provide following connection details:

Entry URL =

`https://<channel>.assessmentq.com (PRODUCTION)`
`https://<channel>.demo.assessmentq.com (DEMO)`

Callback URL =

`https://idp.assessmentq.com/sso/<channel> (PRODUCTION)`
`https://idp.demo.assessmentq.com/sso/<channel> (DEMO)`

Post logout redirect URI *(optional - if supported)* =

`https://idp.assessmentq.com/slo/<channel> (PRODUCTION)`
`https://idp.demo.assessmentq.com/slo/<channel> (DEMO)`

Discovery URL =

<https://idp.assessmentq.com/.well-known/openid-configuration> (PRODUCTION)

<https://idp.demo.assessmentq.com/.well-known/openid-configuration> (DEMO)

Flow =

Authorization Code Flow

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

4.2 Information to provide by the Identity Provider

In order to configure the Identity Provider within assessmentQ, Televic Education requires following information from you:

Client ID =

CLIENT ID

Client Secret =

CLIENT SECRET

Discovery URL of the Identity Provider =

DISCOVERY URL

Scopes (cfr. section '3.1. Scopes') =

SCOPES (e.g. openid, profile, email)

Test account =

TEST ACCOUNT DETAILS (in order to verify the SSO integration)

Please note that for this test account, the first name, last name and e-mail address must be configured correctly as these are required fields for the integration.