Televic Education

OpenID Connect via Azure AD - Example configuration

23 October 2023

Created by Sylvia Joos

televic education

Table of contents

1 Configuration 4

2 Add configuration for existing applications: 5

This document shows a step-by-step guide on how to configure an Azure Active Directory for connecting with the assessmentQ Identity Provider.

1 Configuration

1. Go to your Azure Portal via https://portal.azure.com.
2. Type "Active Directory" in the search bar on top and click on "Azure Active Directory".
3. Click on "App registrations" in the menu on the left.
4. Click on "New registration" on top.
5. Fill in the form with the following data
   Name **<subdomain>.<environment or blank>.assessmentq.com**
   Who can use this application or access this API? **Accounts in this organizational directory only (XXXXXXX - Single tenant)**
   Redirect URI (optional) ***Copy the callback URL you find in the assessmentQ backoffice*** *(see Module Settings > Integrations > Single-Sign-On)*
6. Make a note of the Application (client) ID and Directory (tenant) ID values.
   You will need them later (cfr. step 14).
7. Go to the Authentication tab.
   - Make sure the redirect URIs contain the "callback URL" you found in the assessmentQ backoffice.
   - Also fill in the front-channel logout URL in Azure with the **entry URL** which you find in the assessmentQ backoffice (see Module Settings > Integrations > Single-Sign-On).
   - Enable "ID tokens" under "Implicit grant and hybrid flows".
8. Go to the "Token Configuration" page.
9. Add the following optional claims:
   a. Access - email
   b. Access - given_name
   c. Access - family_name
   d. ID - email
   e. ID - given_name
   f. ID - family_name
10. (Optional) If you want the language of your organisation to be used in assessmentQ, also add the following claims:
    a. Access - xms_pl (for the user's language)
    b. Access - xms_tpl (for the organisation's preferred language)
    c. ID - xms_pl (for the user's language)
    d. ID - xms_tpl (for the organisation's preferred language)
    If both claims are passed, the user's language will have priority over the organisation language
11. (Optional) If you want the groups of your organisation to come through in assessmentQ:
    - Click "Add groups claim"
    - Choose which group types you want to use in assessmentQ
    - Under "Customize token properties by type", choose "sAMAccountName" for every token type
12. (Optional) If you want to pass a role for users to assessmentQ:
    - Go to "App roles"
    - Create the roles you wish to use in assessmentQ:
      - New role:
        If you create a role that does not yet exist in assessmentQ, the new role will be created in assessmentQ. The permissions and access rights for this role will have to be set manually in the assessmentQ backoffice.
      - Existing role:
        If you create a role that already exists in assessmentQ, no manual intervention is needed in the assessmentQ backoffice to set the permissions and access rights.
    - To assign users/groups to roles, go to the Managed Application that is linked to your App Registration
    - Choose the tab "Users and groups" on the application
    - There, you can choose allowed users and groups, and assign a role to them

13. Go to the "Certificates & Secrets" page
    a. Create a new secret (24 months)
    b. Take a note of the value of the secret.
14. Copy the following information to the assessmentQ backoffice (Module Settings > Integrations > Single-Sign-On):
    a. Discovery URL => **https://login.microsoftonline.com/<TenantId>/v2.0/.well-known/openid-configuration (from step 6).**
    b. ClientID => **Application (client) ID (from step 6).**
    c. Secret => **Value of the secret** created in the previous step.
    d. Scope => **openid profile email** these are the minimal scopes required

2 Add configuration for existing applications:

1. Go to your Azure Portal via https://portal.azure.com.
2. Type "Active Directory" in the search bar on top and click on "Azure Active Directory".
3. Click on "App registrations" in the menu on the left.
4. Select the desired application
5. Go to the "Certificates & Secrets" page
    a. Create a new secret (24 months)
    b. Take a note of the value of the secret.
6. Go to Overview (for the other needed information)
7. Copy the following information to the assessmentQ backoffice:
    a. Discovery URL => https://login.microsoftonline.com/**<TenantId>/v2.0/.well-known/openid-configuration (from step 6).**
    b. ClientID => <**Application (client) ID>.**
    c. Secret => **Value of the secret** created in the previous step.
    d. Scope => **`openid profile email`** these are the minimal scopes required