PROACT 2.0

Azure AD B2C Configuration

09/03/2022

1. Azure initialization

1.1. Create an Azure Active Directory B2C tenant

1. Sign in to the Azure portal.
2. Create an Azure Active Directory B2C tenant.
3. Switch to the new directory.
4. Select Azure AD B2C from resources.

1.2. Create an Signin user flow

1. Select **User Flow** from the side menu.
2. Select **New user flow** button.
3. Select **Sign in** and **Recommended**.
4. Insert a user flow name.
5. Select **Email signin** as Local accounts.
6. Select the following Application claims:

    - Display Name
    - Identity provider

7. Select **Email** as Type of Method.
8. Select Off as MFA enforcement.
9. In Password configuration select this options:

    - Self-service password reset
    - Forced password reset

1.3. Identification of the AuthURL value

1. In Azure Ad B2C page select **App registrations** from the side menu.
2. Select **Endpoint** tab**.**
3. Copy the value of **“Azure AD B2C OAuth 2.0 authorization endpoint (v2)”.**

4. Replace “<policy-name>” with “{0}”.

Example:

```
https://proact.b2clogin.com/proact.onmicrosoft.com/<policy-name>/oauth2/v2.0/authorize

to

https://proact.b2clogin.com/proact.onmicrosoft.com/{0}/oauth2/v2.0/authorize
```

2. Web API app registration (Proact.Service solution)

2.1. App registration

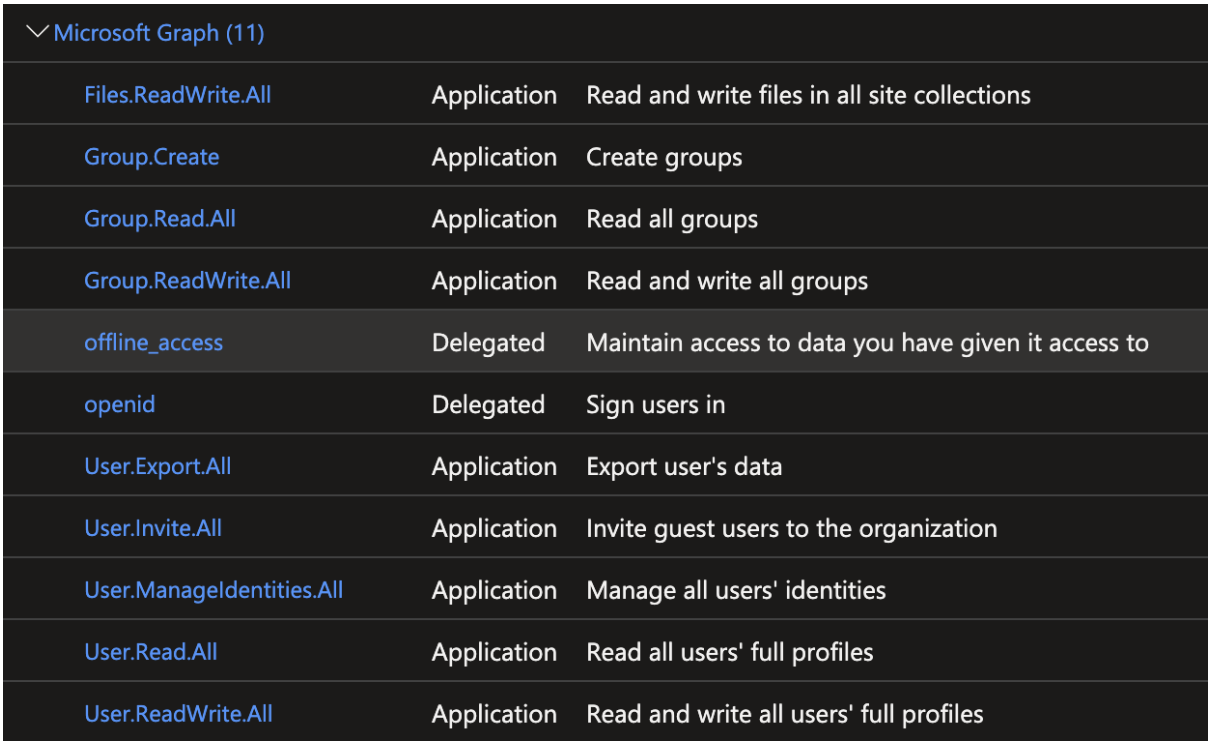
1. In Azure Ad B2C page select **App registrations** from the side menu.
2. Select **New registration**.
3. Insert "API" as app **name**.
4. Select **Create.**
5. Select **Overview** from the side menu.
6. Copy and keep **Application (client) ID.**

2.2. Create an application client Secret

1. Select **Certificates & secrets** from the side menu.
2. Select **New client secret** e inserisci.
3. Inserti "**Description**" and "**expires**".
4. Copy and keep the Secret client Value.

2.3. Configure API permissions

1. Select **API permissions** from the side menu.
2. Select **Add a permission**.
3. Select **Microsoft APIs** > **Microsoft Graph** > **Application permissions.**
4. Select the following permissions:



Microsoft Graph (11)		
Files.ReadWrite.All	Application	Read and write files in all site collections
Group.Create	Application	Create groups
Group.Read.All	Application	Read all groups
Group.ReadWrite.All	Application	Read and write all groups
offline_access	Delegated	Maintain access to data you have given it access to
openid	Delegated	Sign users in
User.Export.All	Application	Export user's data
User.Invite.All	Application	Invite guest users to the organization
User.ManageIdentities.All	Application	Manage all users' identities
User.Read.All	Application	Read all users' full profiles
User.ReadWrite.All	Application	Read and write all users' full profiles

Select **Grant admin consent for Proact.**

2.4. Add a Scope

1. Select **Expose an API** from the side menu.
2. Select "**Set**" to create an **Application ID URI,** then select **save**.
3. Select **Add a scope.**
4. Copy and keep the scope value.

2.5. Create a B2C Extension App Client Id

1. Select **App registrations** from the side menu.
2. Select "**b2c-extensions-app. Do not modify. Used by AADB2C for storing user data**".
3. Select Overview.
4. Copy and keep **Application (client) ID.**

2.6. Swagger app registration

1. Select **App registrations** from the side menu.
2. Select **New registration.**
3. Insert "Swagger" as the app **name**.
4. Insert this redirect **URI**:
    - Platform : Web
    - URI: <YOUR_SWAGGER_URL>/oauth2-redirect.html

5. Select **Create.**

Select **Overview** from the side menu.
Copy and keep **Application (client) ID**

Authentication options:

Select **Authentication** from the side menu.
Check this options:

- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Select **Save.**

API Permissions:

1. Select **API permissions** from the side menu.
2. Select "**Add a permission**".
3. Select **My APIs**, then Select your API.
4. Select the scope.
5. Select **Add permissions**.
6. Select **Grant admin consent for Proact**.

3. Proact.Service solution Settings

Open Proact.Service solution.
Open AppSettings.Production.json (or AppSettings.Development.json) and insert this values:

```
"AzureAdB2C": {
    "Instance": "https://<YOUR_TENANT_NAME>.b2clogin.com",
    "ClientId": "<YOUR_API_APPLICATION_CLIENT_ID>",
    "Domain": "<YOUR_TENANT_NAME>.onmicrosoft.com",
    "SignUpSignInPolicyId": "<YOUR_SIGNIN_USER_FLOW_NAME>"
  }
```

```
"AzureB2CUserGraph": {
    "Tenant": "<YOUR_TENANT_NAME>.onmicrosoft.com",
    "ClientId": "<YOUR_API_APPLICATION_CLIENT_ID>",
    "ClientSecret": "<YOUR_API_APPLICATION_CLIENT_SECRET>",
    "B2CExtentionAppClientId": "<YOUR_B2CExtentionAppClientId>",
    "UserCommonPassword": "<YOUR_DEFAULT_USER_PASSWORD>"
  }
```

```
"Swagger": {
    "ApiName": "Proact Service API",
    "ApiVer": "v1",
```

```
  "AuthUrl":"<YOUR_AUTH_URL>",
  "SignUpSignInPolicyId": "<YOUR_SIGNIN_USER_FLOW_NAME>",
  "ClientId": "<YOUR_SWAGGER_APPLICATION_CLIENT_ID>",
  "Scope": "<YOUR_API_APPLICATION_SCOPE>"
}
```

4. CPanel app registration (Proact-WebApp solution)

4.1. App registration

1. Select **App registrations** from the side menu.
2. Select **New registration.**
3. Insert "Cpanel" as the app **name**.
4. Insert this redirect **URI**:
    - Platform : Web
    - URI: <YOUR_CPANEL_URL>/signin-oidc
5. Select **Create.**

Select **Overview** from the side menu.
Copy and keep **Application (client) ID.**

4.2. Authentication options

1. Select **Authentication** from the side menu.
2. Check this options:
    - Access tokens (used for implicit flows).
    - ID tokens (used for implicit and hybrid flows).

3. Select **Save.**

4.3. API Permissions

1. Select **API permissions** from the side menu.
2. Select "**Add a permission**".
3. Select **My APIs**, then Select your API.
4. Select the scope.
5. Select **Add permissions**.
6. Select **Grant admin consent for Proact**.

4.4. Application client secret

1. Select **Certificates & secrets** from the side menu.
2. Select **New client secret** e inserisci.
3. Inserti “**Description**” and “**expires**”.
4. Copy and keep the Secret client Value.

5. Proact-WebApp solution Settings

Open Proact.WebApp solution.
Open AppSettings.Production.json (or AppSettings.Development.json) and insert this values:

```
"AzureAdB2C": {
   "Instance": "https://<YOUR_TENANT_NAME>.b2clogin.com",
   "ClientId": "<YOUR_CPANEL_CLIENT_ID>",
   "Domain": "<YOUR_TENANT_NAME>.onmicrosoft.com",
   "SignedOutCallbackPath": "/signout/<YOUR_SIGNIN_USER_FLOW_NAME>",
   "SignUpSignInPolicyId": "<YOUR_SIGNIN_USER_FLOW_NAME>",
   "ClientSecret": "<YOUR_CPANEL_CLIENT_SECRET>"
 },

 "ProactWebAppScope": "<YOUR_API_APPLICATION_SCOPE>"
```

6. Mobile app registration (Proact.Mobile solution)

6.1. App registration

1. Select **App registrations** from the side menu.
2. Select **New registration.**
3. Insert “Mobile” as the app **name**.
4. Insert this redirect **URI**:
   - Platform : Public client/native (mobile & desktop).
   - URI: void.
5. Select **Create.**

Select **Overview** from the side menu.
Copy and keep **Application (client) ID.**

6.2. Authentication options

1. Select **Authentication** from the side menu.
2. Select **Add a platform.**
3. Select **mobile & desktop applications.**
4. Select the precompiled Redirect URIs.

6.3. Api permissions

Select **API permissions** from the side menu.
Select “**Add a permission**”.
Select **My APIs**, then Select your API.
Select the scope.
Select **Add permissions**.
Select **Grant admin consent for Proact**.

1. Proact.Mobile solution Settings

Open Proact.Mobile solution.
Open Settings.cs and insert this values:

```
private static readonly string _tenantName = "<YOUR_TENANT_NAME>";
private static readonly string _tenantId ="<YOUR_TENANT_NAME>.onmicrosoft.com";
private static readonly string _clientId = "<YOUR_MOBILE_CLIENT_ID>";
private static readonly string[] _scopes = { "<YOUR_API_APPLICATION_SCOPE>" };

private static readonly string _policySignin = "<YOUR_SIGNIN_USER_FLOW_NAME>";
```

1.1. iOS Project info.plist settings

Open info.plist file in Proact.Mobile.iOS project and add

```
<key>CFBundleURLTypes</key>
<array>
	<dict>
		<key>CFBundleURLSchemes</key>
		<array>
			<string>msal<YOUR_MOBILE_CLIENT_ID></string>
		</array>
		<key>CFBundleURLName</key>
		<string>ADB2C Auth</string>
	</dict>
</array>
```

1.2. Android ProjectManifest update

Open AndroidManifest.xml and add this tag inside application tag:

```
<activity android:name="microsoft.identity.client.BrowserTabActivity">
   <intent-filter>
      <action android:name="android.intent.action.VIEW" />
      <category android:name="android.intent.category.DEFAULT" />
      <category android:name="android.intent.category.BROWSABLE" />
      <data android:scheme="msal<YOUR_MOBILE_CLIENT_ID>" android:host="auth" />
    </intent-filter>
</activity>
```