**Azure AD B2C – Configuring Identity Providers**

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure AD B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

**Diagram:**

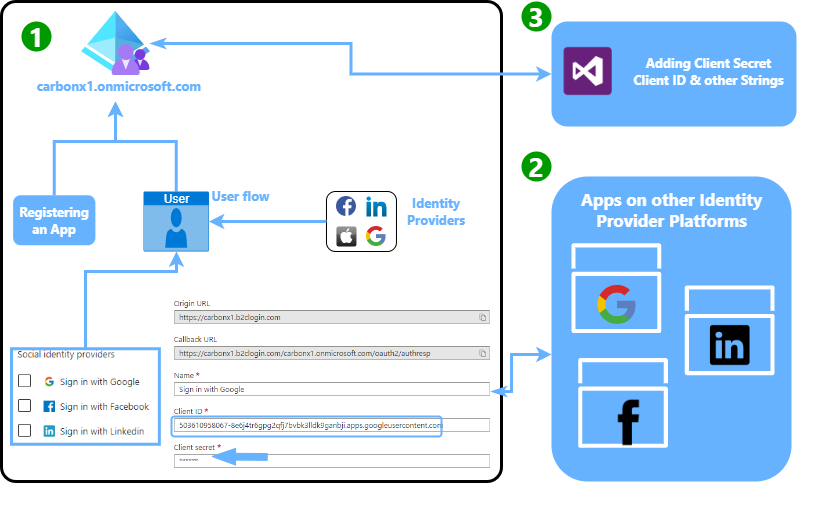
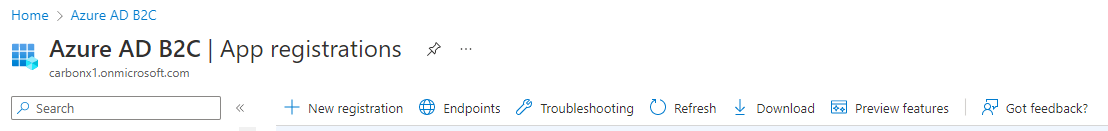


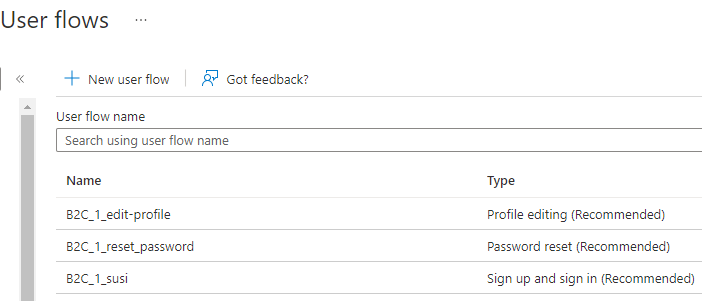
Figure 1

**Step1: Creating Azure AD B2C and doing Configuration**

1. Create and Azure AD B2C
2. Add identity providers i.e Google, Facebook, Linkedin etc
3. Adding Origin & Redirect UrIs in to App of Respective Identity Provider
4. Adding client id and client secret of that App in to you B2C identity Providers
5. Configure Userflows in Policies section by selection userflow type and filling other details
   1. In Social Identity Provider Section of Userflow select the provider you want to use
   2. Select attributes and return claims can also add your custom attributes
6. Select Api and Expose the scopes by registering and APP
   1. In supported account type select “Account in any Identity provider or organizational directory”
7. Now use Expose and API blade to Expose the link
8. In Authentication blade select id tokens and access tokens
9. In userflow properties we can change properties according to our need i.e password complexity, MFA option etc
10. For Page layout we can select already available templates or can use our custom

****

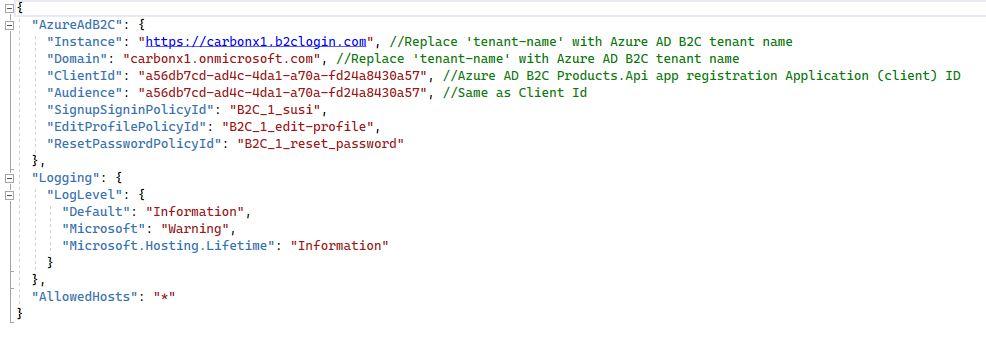
****

****

Creating Userflows 1

**Step2: Configuring Connection in our WebApp i.e Dotnet Web Application**

1. Go to source files in of WebApp in VS
2. In webclient folder of app go to appsettings.json file and add the followings information of Azure AD B2C in to that file
   1. Instance
   2. Domain
   3. Client ID
   4. Client Secret
   5. Base-address
   6. URL
   7. ReadScope
   8. Userflow Name
3. Make the same require change in appsetting.json file in Api folder

****

WebApp API setting 1

****

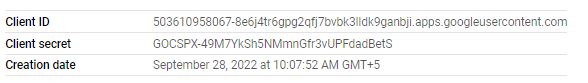
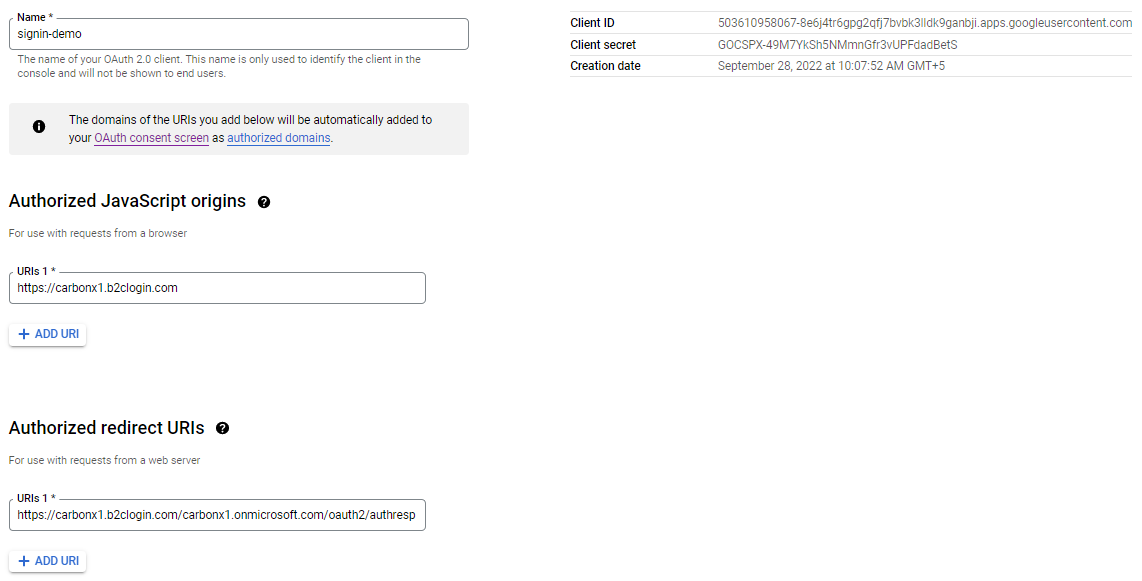
Web client Settings 1

**Step3: Creating and Configuring Apps on Third Party Identity Provider**

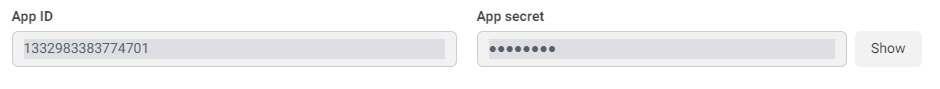
1. Create and App on the provider (social platform you want to use) developer portal
2. Select Authentication option on that App
3. Add Origin URI and Redirect URI of Azure AD B2C in it
4. Add Client ID and Client Secret from App to Identity provider section in Azure AD B2C

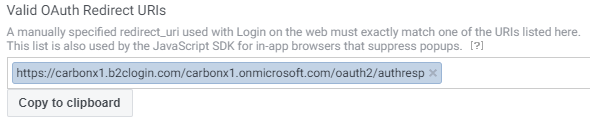
Below are given example of App created on Google, Facebook and Linkedin

1. **For Google Identity**

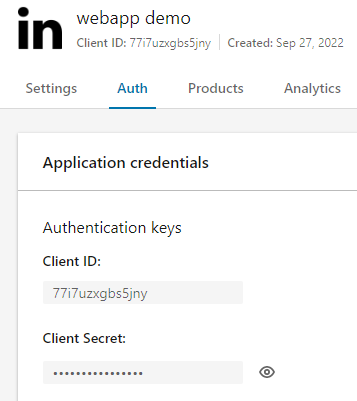


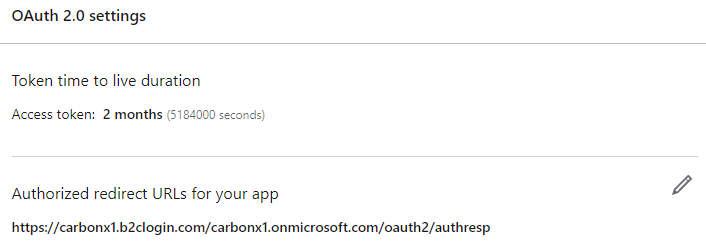
1. **For Facebook Identity**

****

****

1. **For Linkedin Identity**

****



Reference:

GitHub Repository URL:

[Sharp-Programmer/SharpProg.Tutorials.AzureB2C (github.com)](https://github.com/Sharp-Programmer/SharpProg.Tutorials.AzureB2C)

GitHub Repository URL:

[Azure Active Directory B2C documentation | Microsoft Learn](https://learn.microsoft.com/en-us/azure/active-directory-b2c/)