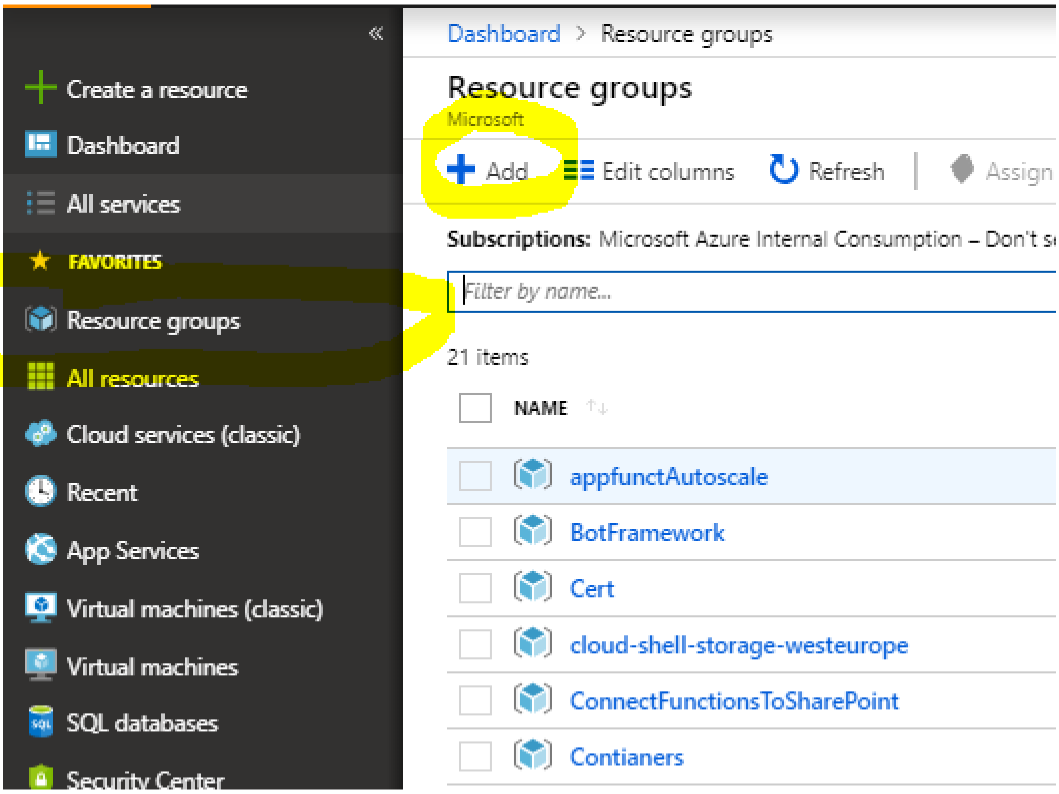
Configure AAD B2C

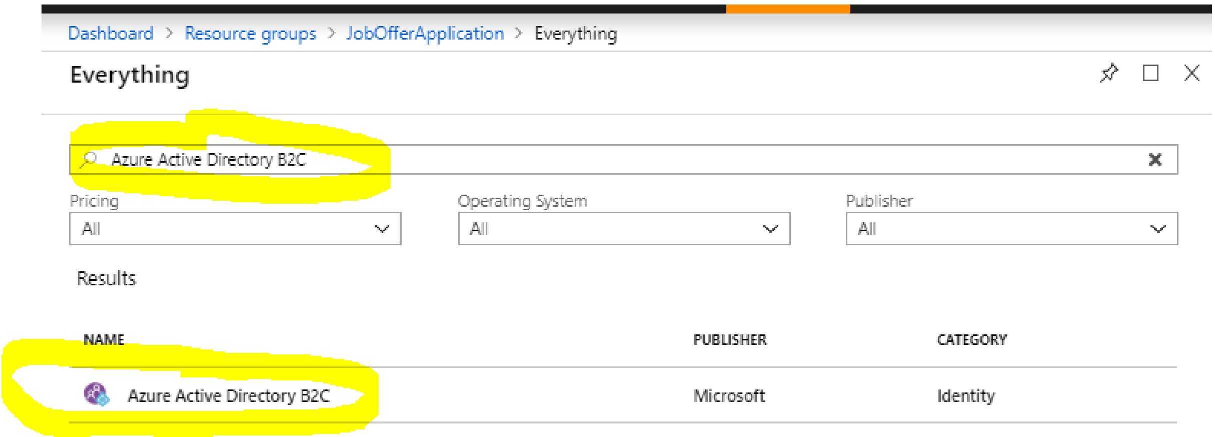
1. Go to portal.azure.com
2. Create resource group “JobOfferApplication”:



Subscriptions: Microsoft Azure Internal Consumption – Don't s

NAME
appfunctAutoscale
BotFramework
Cert
cloud-shell-storage-westeurope
ConnectFunctionsToSharePoint
Contianers

3. Create Azure Active Directory B2C Service inside new resource group:


Dashboard > Resource groups > JobOfferApplication > Everything
Everything
Results

Azure Active Directory B2C

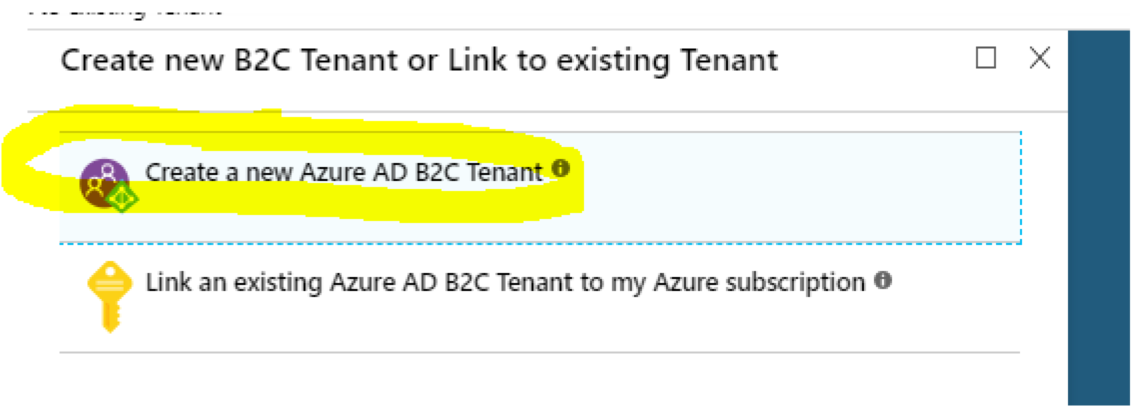
Pricing: All

Operating System: All

Publisher: All

NAME	PUBLISHER	CATEGORY
Azure Active Directory B2C	Microsoft	Identity

4. Select “create” and then “create new”:

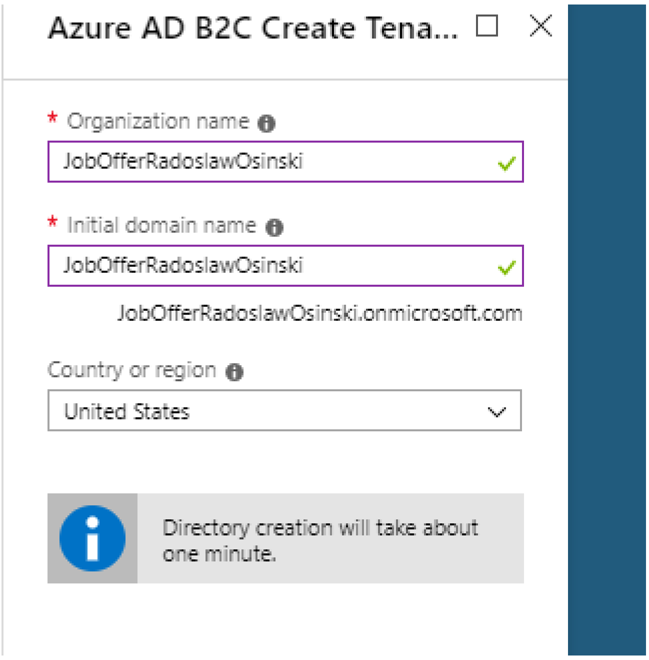


Create new B2C Tenant or Link to existing Tenant

Create a new Azure AD B2C Tenant

Link an existing Azure AD B2C Tenant to my Azure subscription

5. As a organization and initial domain name use “JobOffer” + <<NameSurname>>



Azure AD B2C Create Tena...

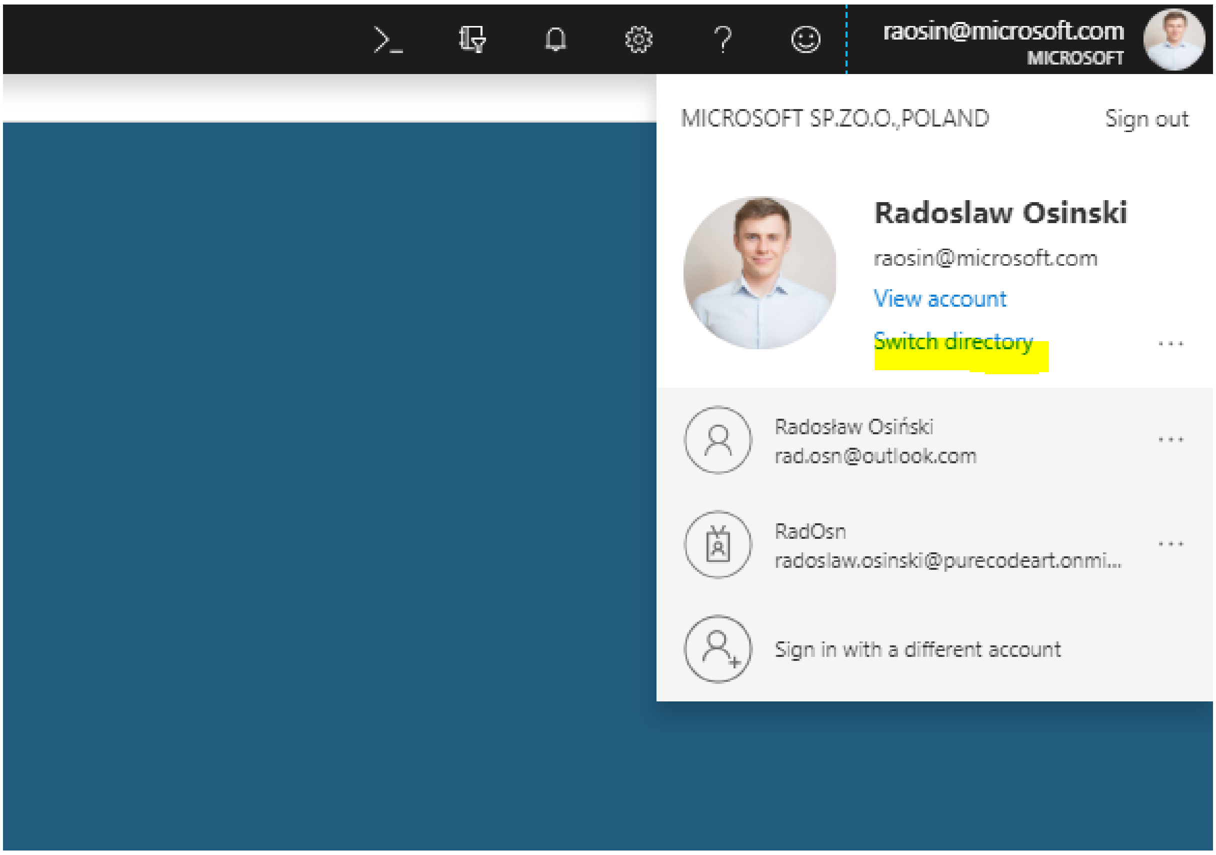
* Organization name
JobOfferRadoslawOsinski

* Initial domain name
JobOfferRadoslawOsinski
JobOfferRadoslawOsinski.onmicrosoft.com

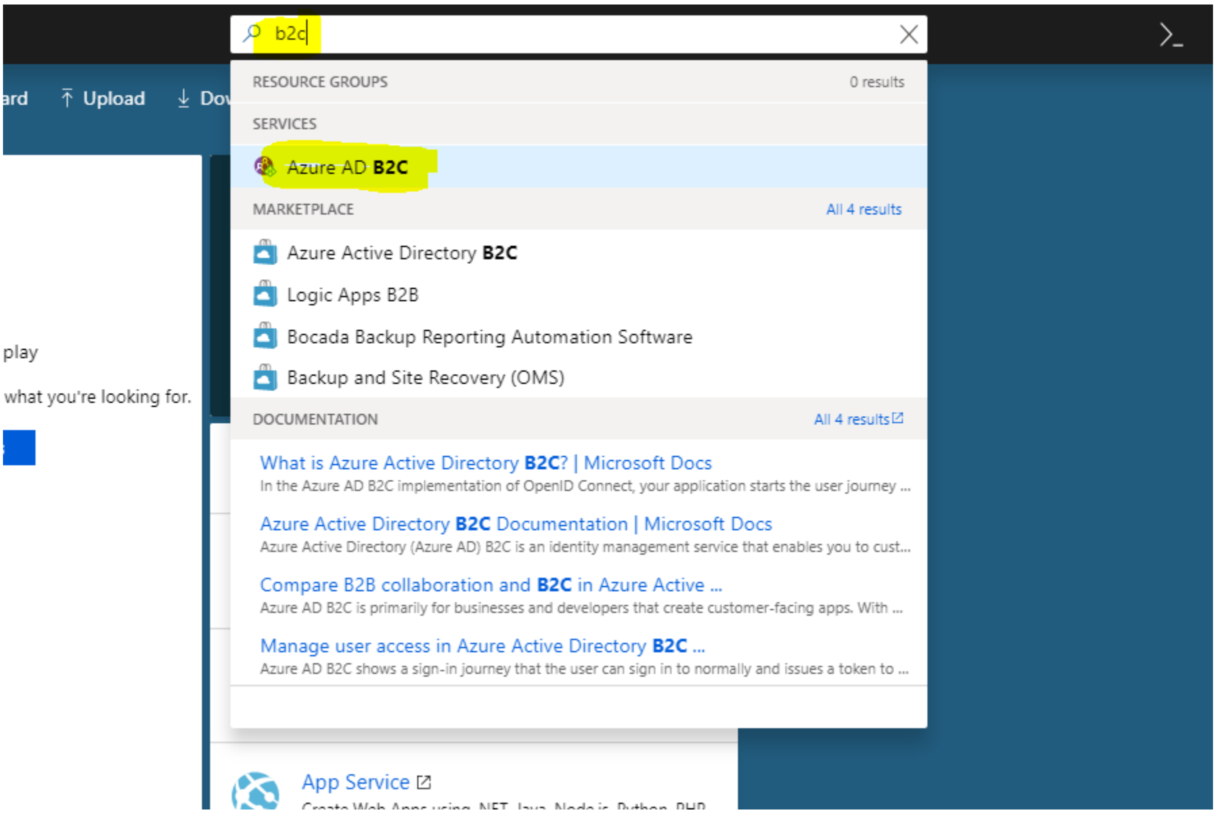
Country or region
United States

Directory creation will take about one minute.

6. When service creation will be finished refresh the page
7. Change directory to newly created:
   Right top corner → switch directory



8. Select new one from the list.
9. When page will reload type B2C in search and select result:



What is Azure Active Directory B2C? | Microsoft Docs
In the Azure AD B2C implementation of OpenID Connect, your application starts the user journey ...

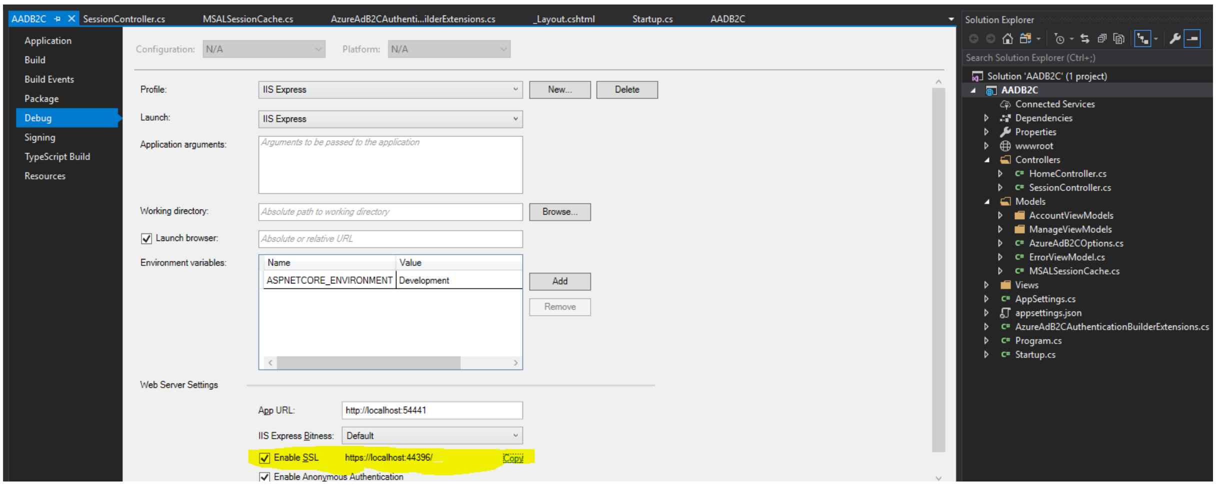
Azure Active Directory B2C Documentation | Microsoft Docs
Azure Active Directory (Azure AD) B2C is an identity management service that enables you to cust...

Compare B2B collaboration and B2C in Azure Active ...
Azure AD B2C is primarily for businesses and developers that create customer-facing apps. With ...

Manage user access in Azure Active Directory B2C ...
Azure AD B2C shows a sign-in journey that the user can sign in to normally and issues a token to ...

Create Web Apps using .NET, Java, Node.js, Python, PHP

10. You are now in Azure B2C
11. Make sure that SSL is enabled in your project properties and copy SSL URL:



Configuration: N/A Platform: N/A

Profile: IIS Express

Launch: IIS Express

Application arguments: Arguments to be passed to the application

Working directory: Absolute path to working directory

☑ Launch browser: Absolute or relative URL

Environment variables:

Name	Value
ASPNETCORE_ENVIRONMENT	Development

Web Server Settings

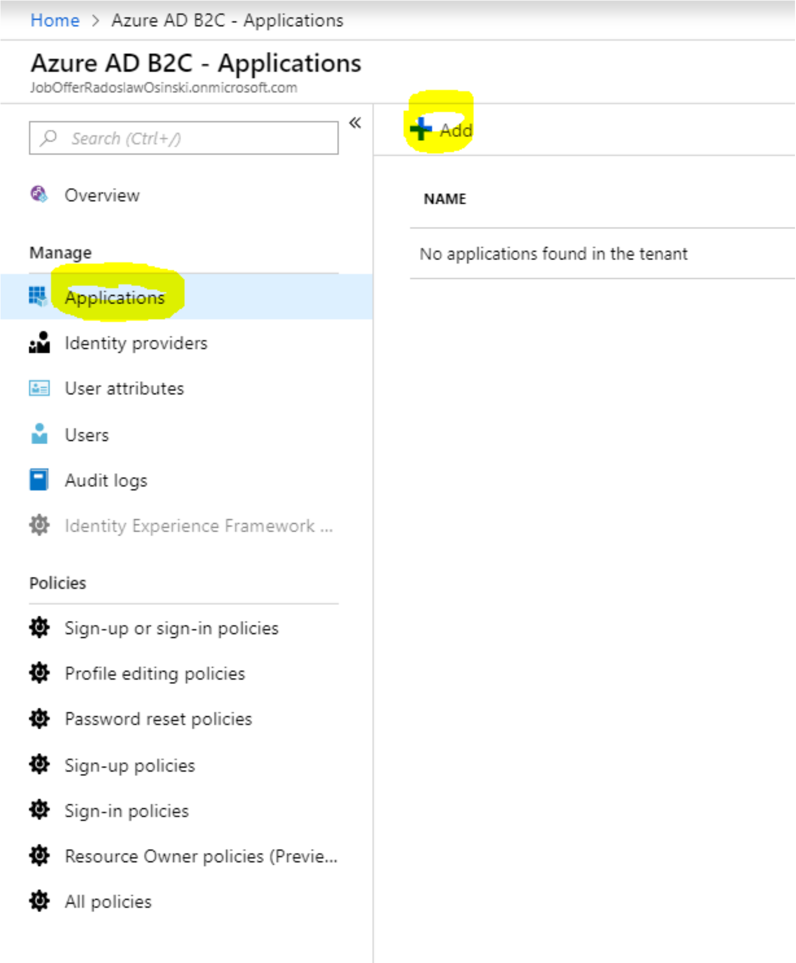
App URL: http://localhost:54441

IIS Express Bitness: Default

☑ Enable SSL https://localhost:44396/

☑ Enable Anonymous Authentication

12. Go back to AAD B2C to "Applications" to register your app:

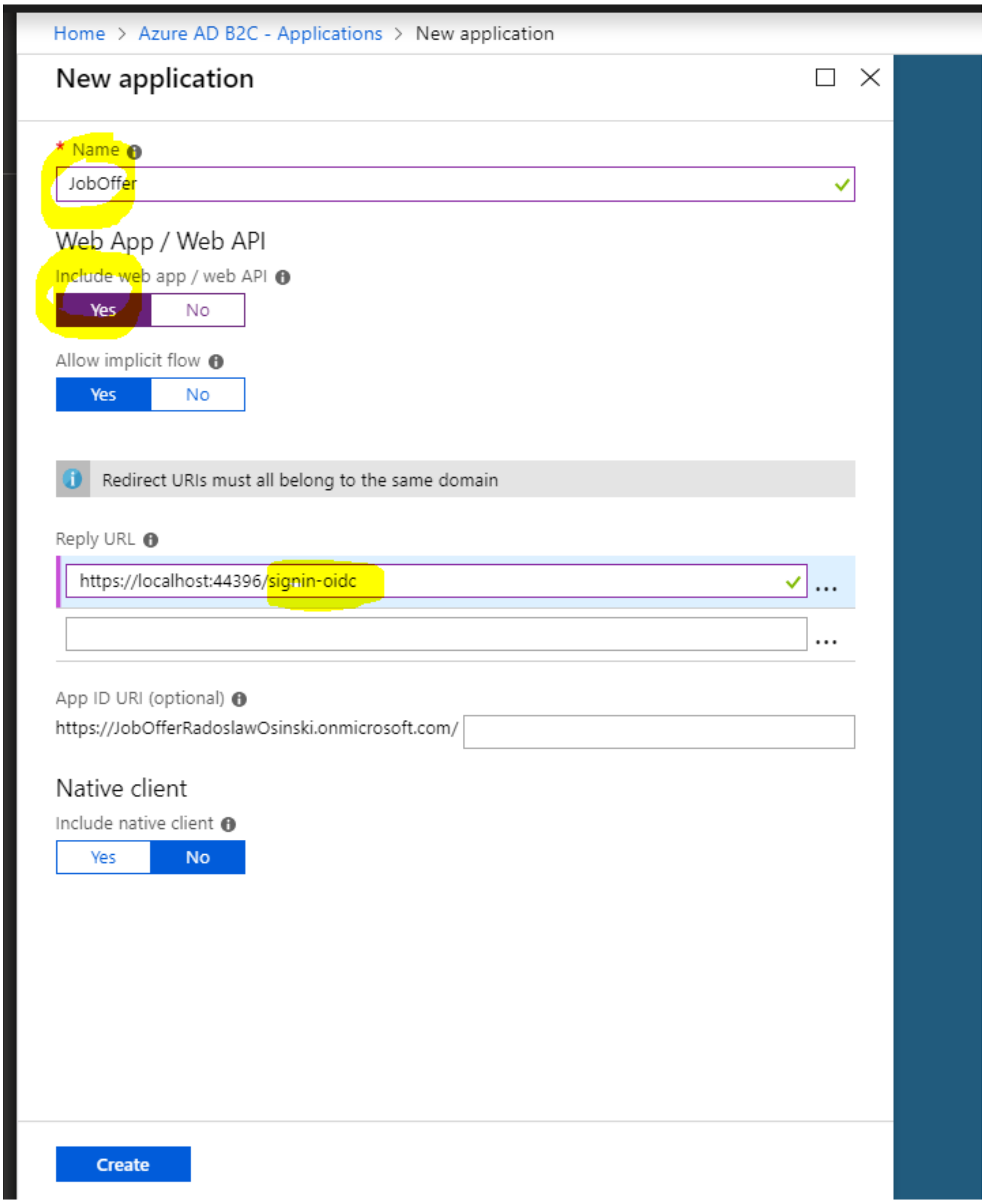


Azure AD B2C - Applications

JobOfferRadoslawOsinski.onmicrosoft.com

No applications found in the tenant

13. Set properties as on the screen.
In URL reply paste copied link from project and add "signin-oidc" at the end:



New application

* Name

JobOffer

Web App / Web API

Include web app / web API: [✓ Yes] No

Allow implicit flow: [✓ Yes] No

Redirect URIs must all belong to the same domain

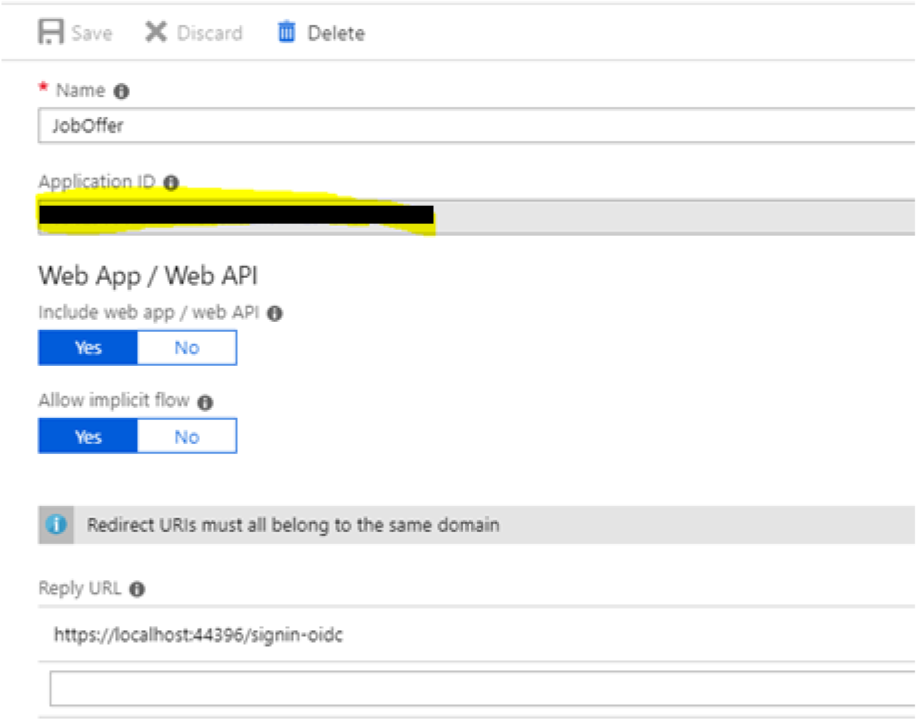
Reply URL: https://localhost:44396/signin-oidc

App ID URI (optional): https://JobOfferRadoslawOsinski.onmicrosoft.com/

Native client

Include native client: Yes [✓ No]

14. When application is created copy “Application ID”



* Name: JobOffer

Application ID: [redacted]

Web App / Web API

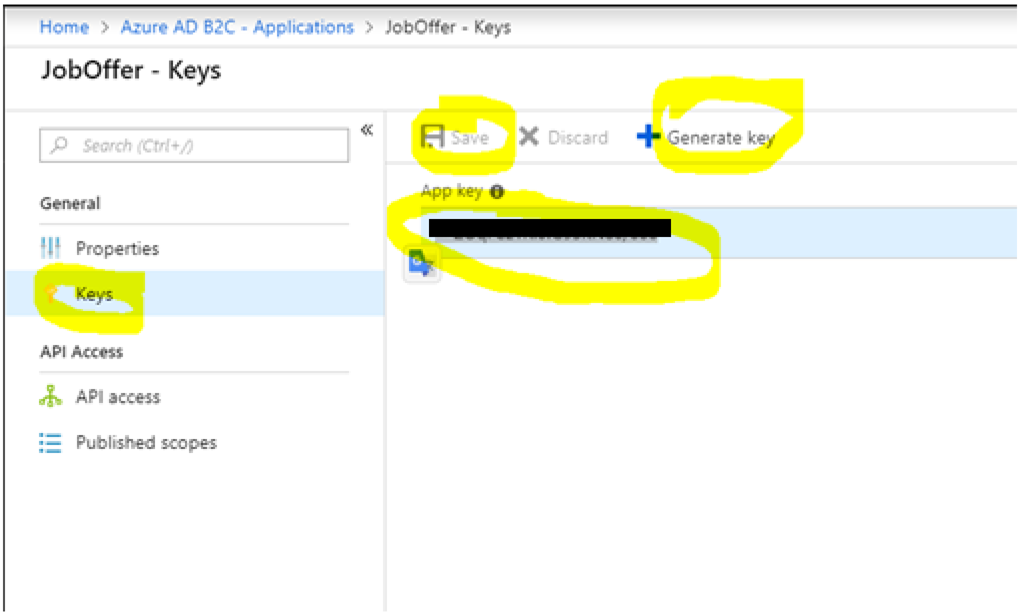
Include web app / web API: Yes

Allow implicit flow: Yes

Redirect URIs must all belong to the same domain

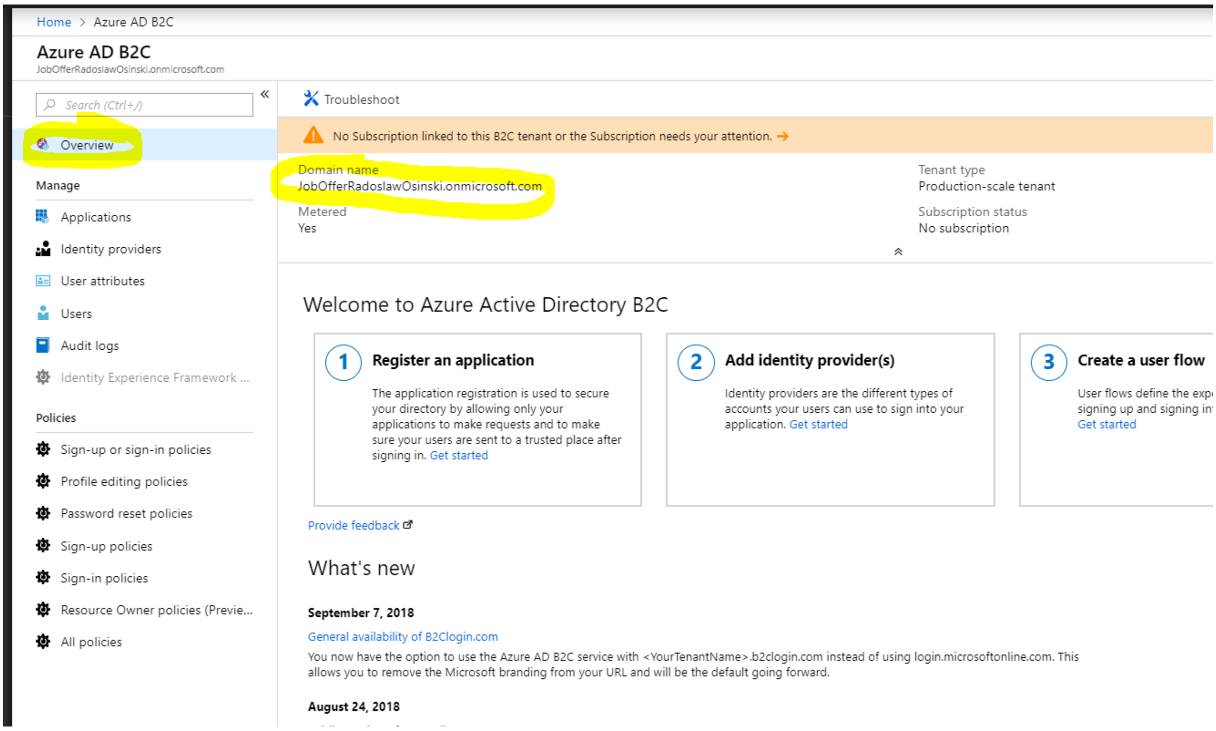
Reply URL: https://localhost:44396/signin-oidc

15. Go to keys klick “Generate key” then without any value in the field “App Key” click Save. That will generate secret automatically. Copy created secret:



App key: [redacted]

16. Go to overview and copy domain name:



Home > Azure AD B2C

Azure AD B2C
JobOfferRadoslawOsinski.onmicrosoft.com

Search (Ctrl+/)

Overview

Manage

Applications

Identity providers

User attributes

Users

Audit logs

Identity Experience Framework ...

Policies

Sign-up or sign-in policies

Profile editing policies

Password reset policies

Sign-up policies

Sign-in policies

Resource Owner policies (Previe...

All policies

Troubleshoot

No Subscription linked to this B2C tenant or the Subscription needs your attention. →

Domain name
JobOfferRadoslawOsinski.onmicrosoft.com

Metered
Yes

Tenant type
Production-scale tenant

Subscription status
No subscription

Welcome to Azure Active Directory B2C

1 Register an application

The application registration is used to secure your directory by allowing only your applications to make requests and to make sure your users are sent to a trusted place after signing in. Get started

2 Add identity provider(s)

Identity providers are the different types of accounts your users can use to sign into your application. Get started

3 Create a user flow

User flows define the exp signing up and signing in Get started

Provide feedback

What's new

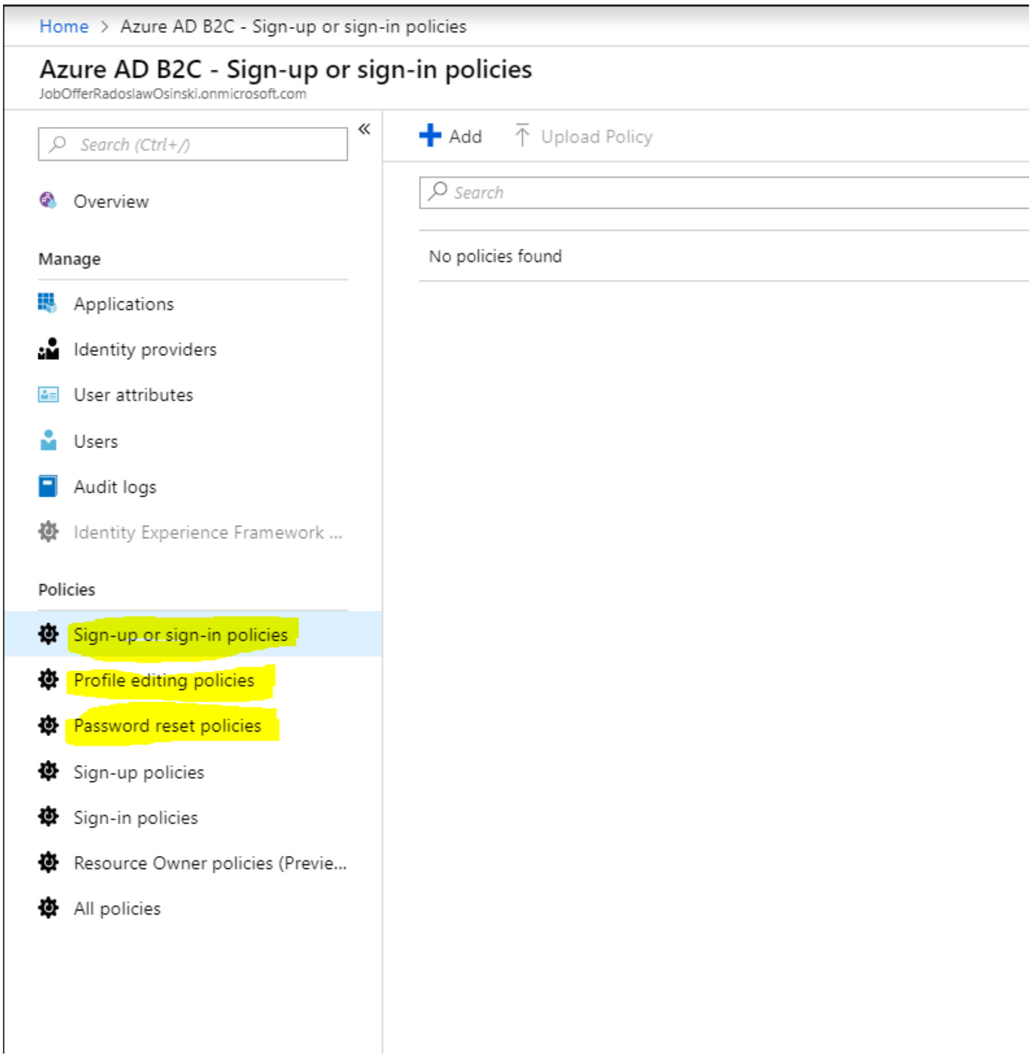
September 7, 2018

General availability of B2Clogin.com

You now have the option to use the Azure AD B2C service with <YourTenantName>.b2clogin.com instead of using login.microsoftonline.com. This allows you to remove the Microsoft branding from your URL and will be the default going forward.

August 24, 2018

17. Now you need to create 3 policies:



Home > Azure AD B2C - Sign-up or sign-in policies

Azure AD B2C - Sign-up or sign-in policies
JobOfferRadoslawOsinski.onmicrosoft.com

Search (Ctrl+/)

Overview

Manage

Applications

Identity providers

User attributes

Users

Audit logs

Identity Experience Framework ...

Policies

Sign-up or sign-in policies

Profile editing policies

Password reset policies

Sign-up policies

Sign-in policies

Resource Owner policies (Previe...

All policies

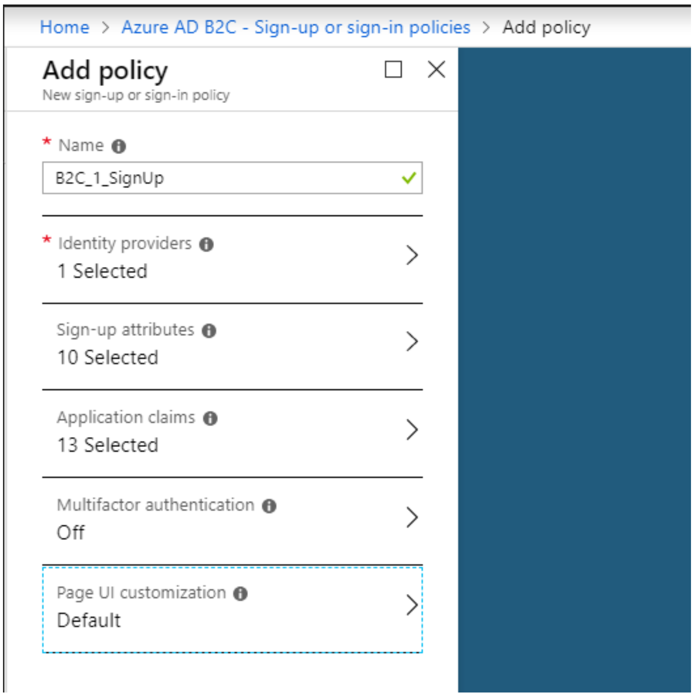
Add Upload Policy

Search

No policies found

18. Create “Sign-up or sign-in policies”

Name it "B2C_1_SignUp", select email identity, all available attributes (10) and claims (13)



Home > Azure AD B2C - Sign-up or sign-in policies > Add policy

Add policy

New sign-up or sign-in policy

* Name

B2C_1_SignUp ✓

* Identity providers

1 Selected

Sign-up attributes

10 Selected

Application claims

13 Selected

Multifactor authentication

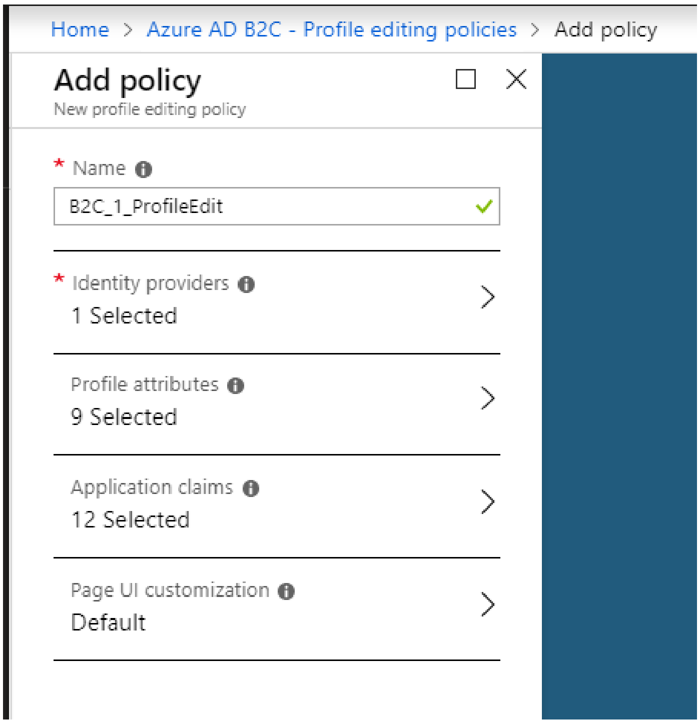
Off

Page UI customization

Default

19. Create "Profile editing policies"

    Name it "B2C_1_ProfileEdit", select "Local Account SignIn" identity, all available attributes (9) and claims (12)



Home > Azure AD B2C - Profile editing policies > Add policy

Add policy

New profile editing policy

* Name

B2C_1_ProfileEdit ✓

* Identity providers

1 Selected

Profile attributes

9 Selected

Application claims

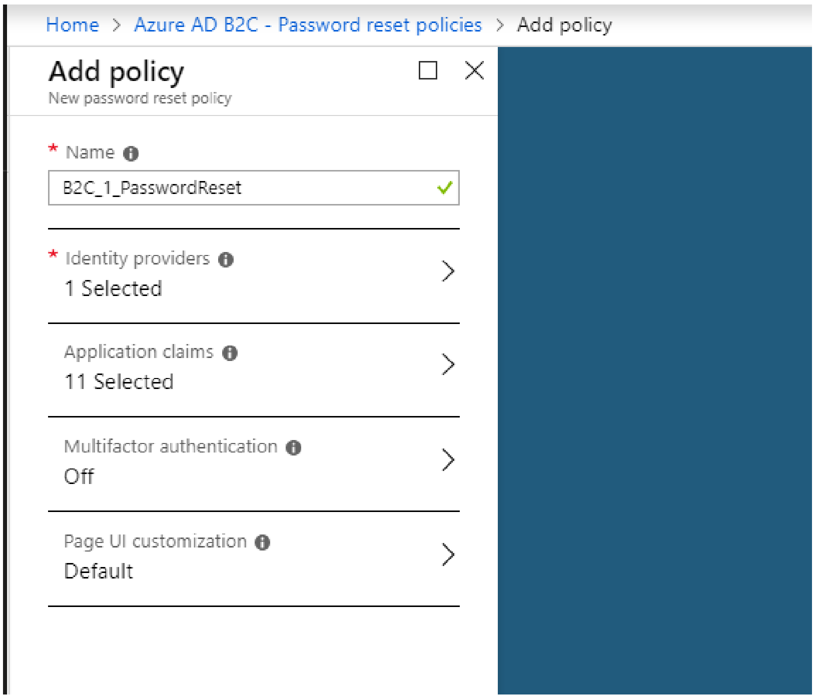
12 Selected

Page UI customization

Default

20. Create "Password reset policies"

    Name it "B2C_1_PasswordReset", select "Reset password using email address" identity, all available attributes (11)



Home > Azure AD B2C - Password reset policies > Add policy

Add policy

New password reset policy

* Name

B2C_1_PasswordReset

* Identity providers

1 Selected

Application claims

11 Selected

Multifactor authentication

Off

Page UI customization

Default

Configure Solution:

21. Copy from the zip fallowing elements to your project:

File: AzureAdB2CAuthenticationBuilderExtensions.cs

Folder: AccountViewModels from Models

Folder: ManageViewModels from Models

File: AzureAdB2COptions.cs from Models

File: MSALSessionCache.cs from Models

Folder: Session from Views

File: _LoginPartial.cshtml from Shared views folder

File: SessionController.cs from Controllers folder

File: AppSettings.cs

22. Add nuget package: `Microsoft.Identity.Client`
23. Put inside appsettings.json authentication section:

```
"Authentication": {
   "AzureAdB2C": {
      "ClientId": "<<taken from Azure (instruction step 14)>>",
      "ClientSecret": "<<taken from Azure (instruction step 15)>>",
      "Tenant": "<<taken from Azure>>.onmicrosoft.com (instruction step 16)",
      "SignUpSignInPolicyId": "B2C_1_SignUp",
      "ResetPasswordPolicyId": "B2C_1_PasswordReset",
      "EditProfilePolicyId": "B2C_1_ProfileEdit",
                "RedirectUri": <<from project (instruction step 11)>>signin-oidc,
              }
            },
```

24. Replace constructor in startup class:

```
public Startup(IHostingEnvironment env)
{
     var builder = new ConfigurationBuilder()
         .SetBasePath(env.ContentRootPath)
         .AddJsonFile("appsettings.json", optional: false, reloadOnChange: true)
         .AddJsonFile($"appsettings.{env.EnvironmentName}.json", optional: true)
         .AddEnvironmentVariables();

          Configuration = builder.Build();
}
```

25. Add at the beginning to ConfigureServices method to startap class:

```
services.AddSingleton<IHttpContextAccessor, HttpContextAccessor>();
          services.Configure<AppSettings>(Configuration.GetSection("AppSettings"));
            services.AddSingleton<IConfiguration>(Configuration);

            services.AddAuthentication(sharedOptions =>
            {
                sharedOptions.DefaultScheme =
CookieAuthenticationDefaults.AuthenticationScheme;
                sharedOptions.DefaultChallengeScheme =
OpenIdConnectDefaults.AuthenticationScheme;
            })
            .AddAzureAdB2C(options => Configuration.Bind("Authentication:AzureAdB2C",
options))
            .AddCookie();

            services.AddMemoryCache();
            services.AddDistributedMemoryCache();
                  services.AddSession();
```

26. Add to startup class:

```
using Microsoft.AspNetCore.Authentication.Cookies;
using Microsoft.AspNetCore.Authentication.OpenIdConnect;
```

27. Add to configure method in startup class:

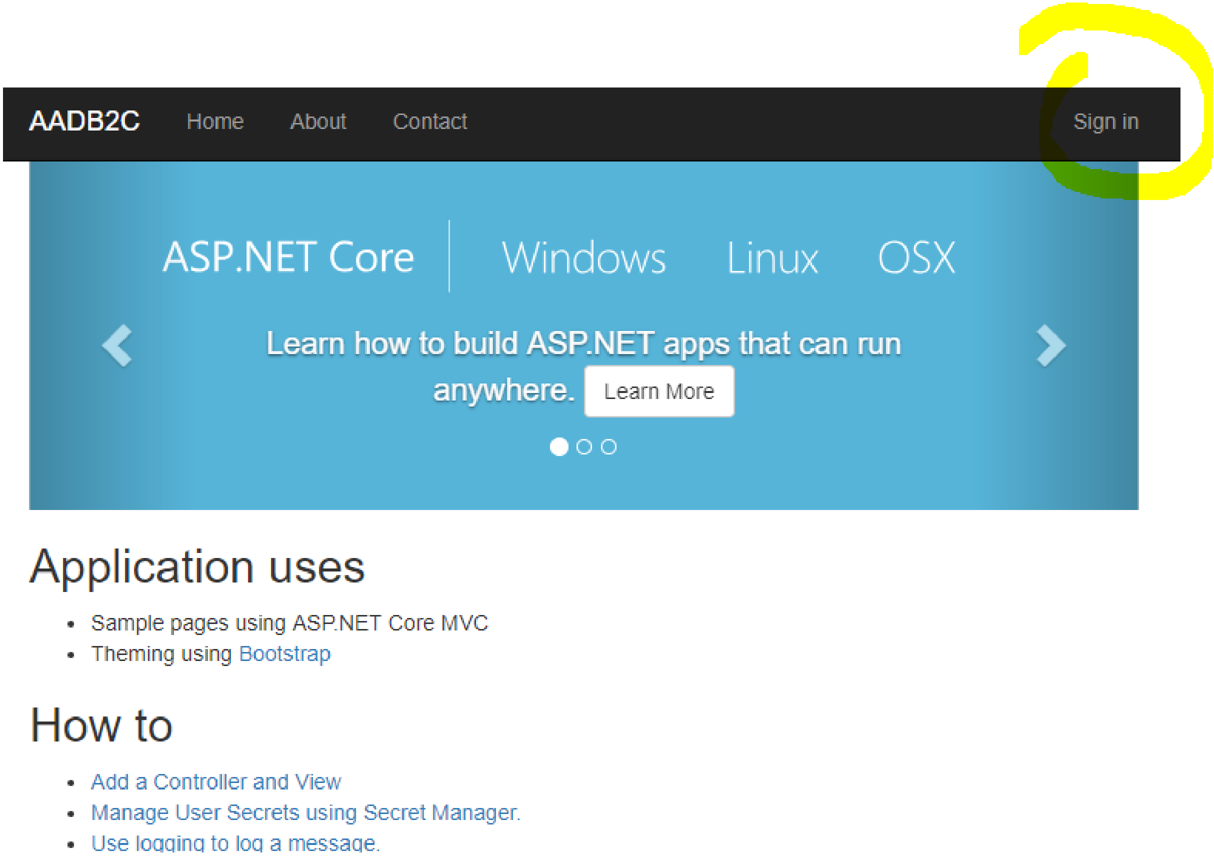
```
app.UseSession();
app.UseAuthentication();
```

28. Paste to _Layout.cshtml

```
@await Html.PartialAsync("_LoginPartial")
```

Just after </ul> navbar

29. Run an app and click “Sign in”



Learn how to build ASP.NET apps that can run anywhere.

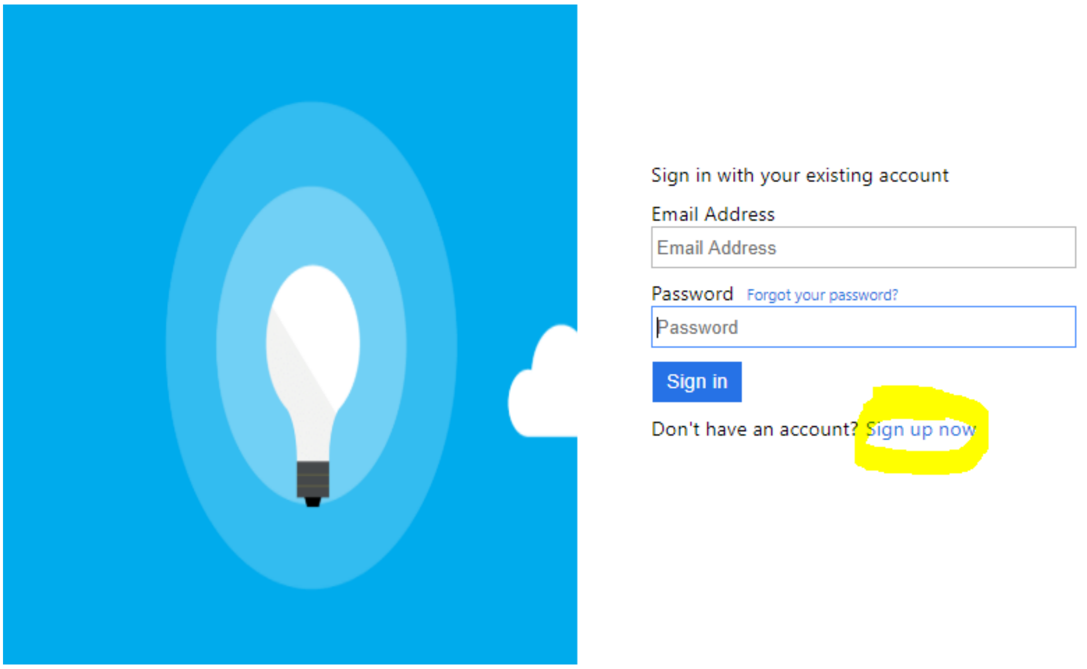
Application uses

- Sample pages using ASP.NET Core MVC
- Theming using Bootstrap

How to

- Add a Controller and View
- Manage User Secrets using Secret Manager.
- Use logging to log a message.

30. Sign up as a new user:

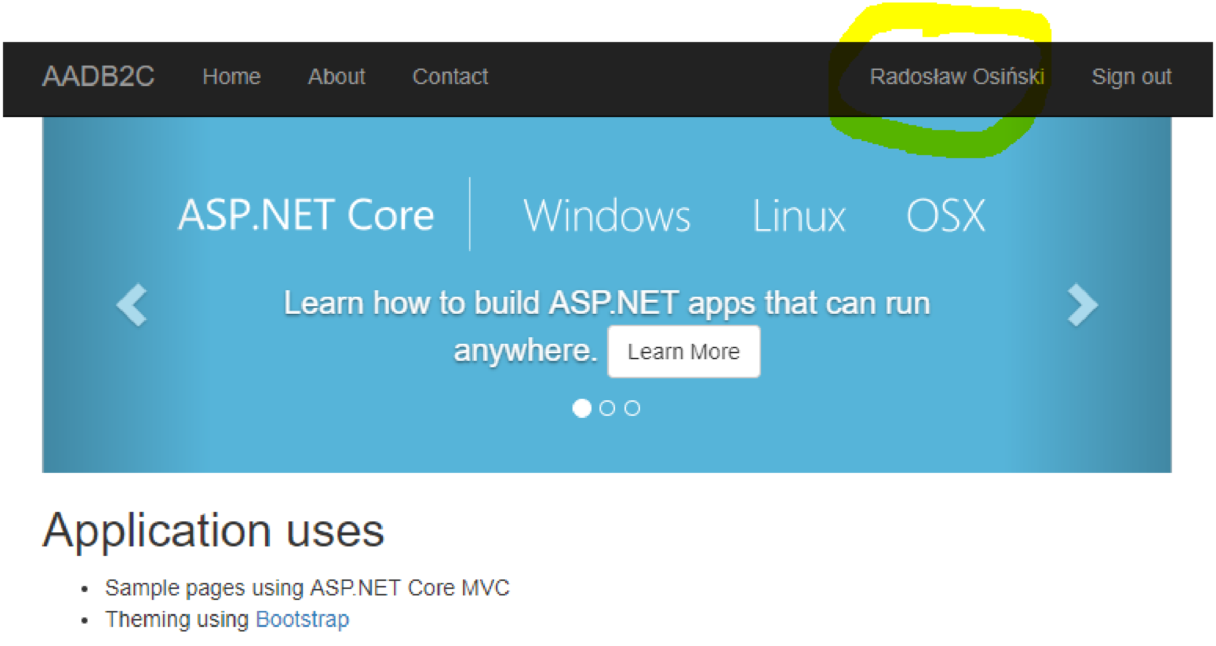


Sign in with your existing account

Email Address

Don't have an account? Sign up now

31. Verify email by code.
32. After log in you should see user name and “Sign out” next to it:



Learn how to build ASP.NET apps that can run anywhere.

Application uses

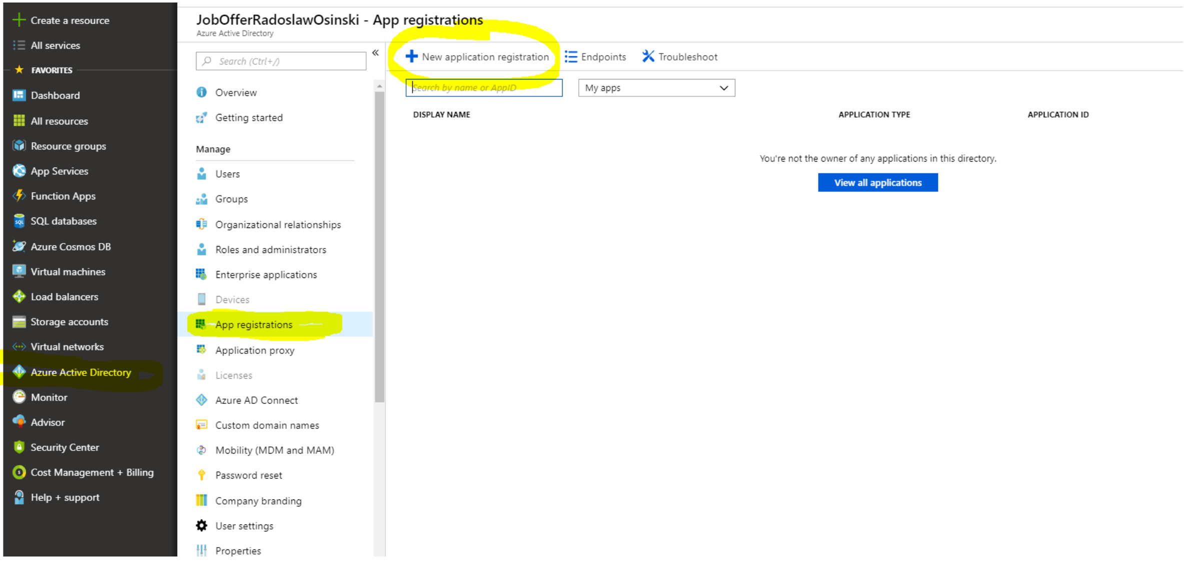
- Sample pages using ASP.NET Core MVC
- Theming using Bootstrap

33. To make sure that user need to be logged in to run controller add an attribute

```
[Authorize]
public IActionResult Profile()
{
        return View();
}
```

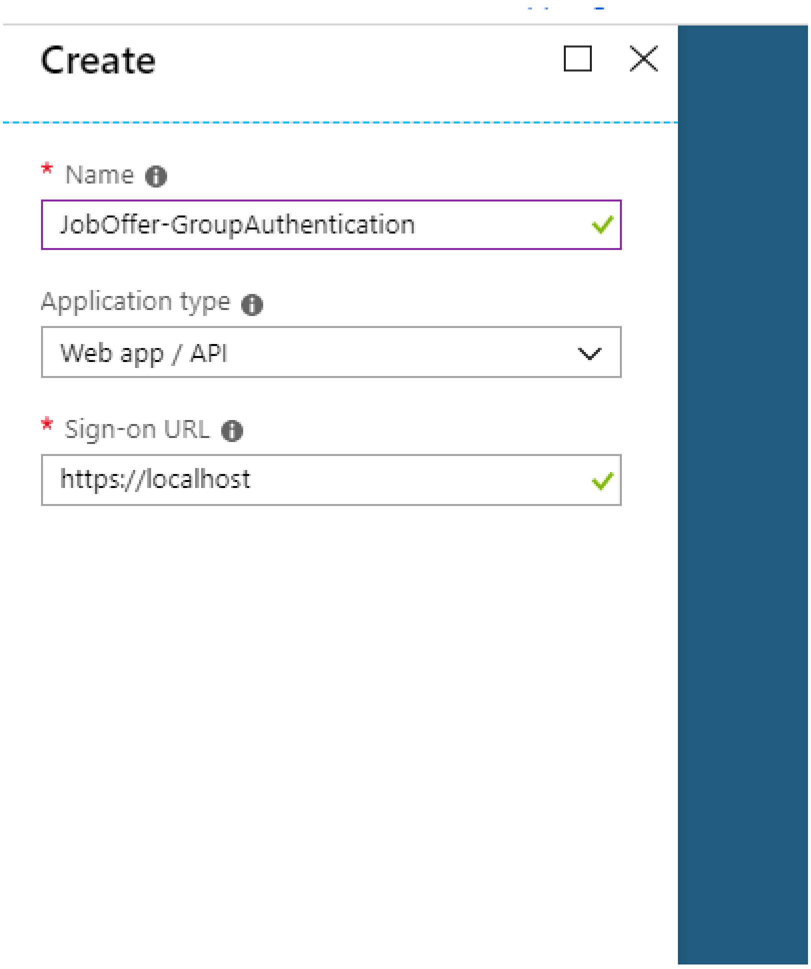
Check if user belong to group

34. Copy Helper Folder
35. Copy AAD folder from Model folder
36. Add NuGet package: Microsoft.IdentityModel.Clients.ActiveDirectory
37. Go to: Azure Active Directory → App Registrations → New Application registration



You're not the owner of any applications in this directory.

38. Provide details and create:



* Name

JobOffer-GroupAuthentication

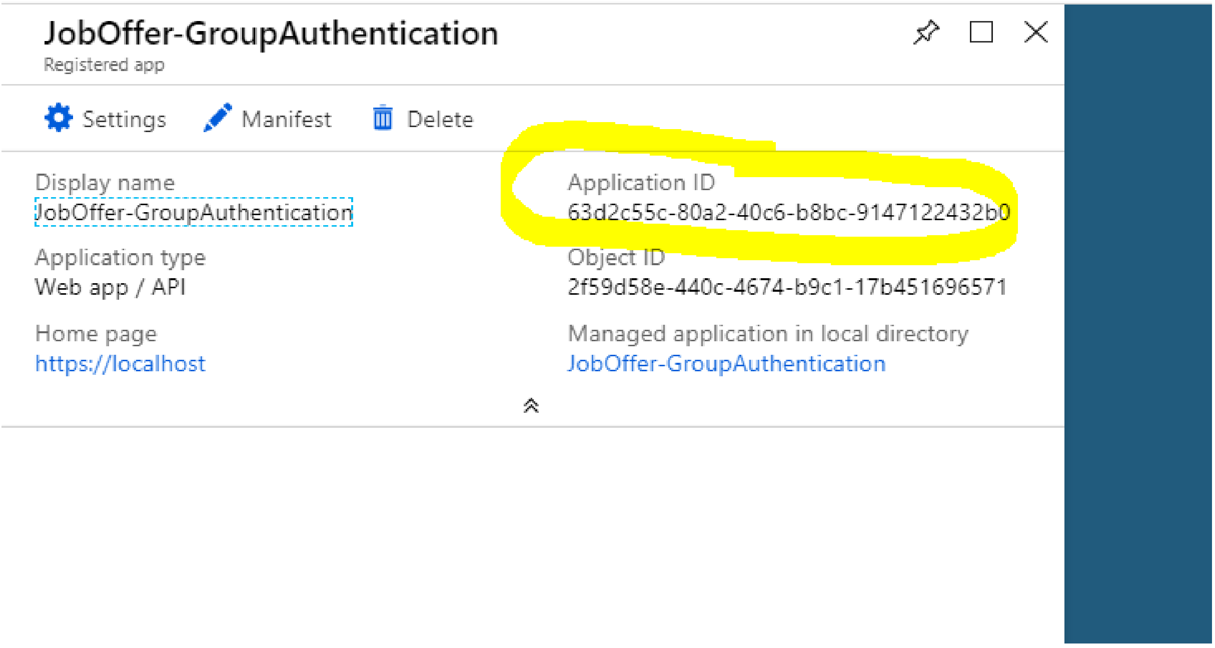
Application type

Web app / API

* Sign-on URL

https://localhost

39. Coppy Application Id :



Display name
JobOffer-GroupAuthentication

Application ID
63d2c55c-80a2-40c6-b8bc-9147122432b0

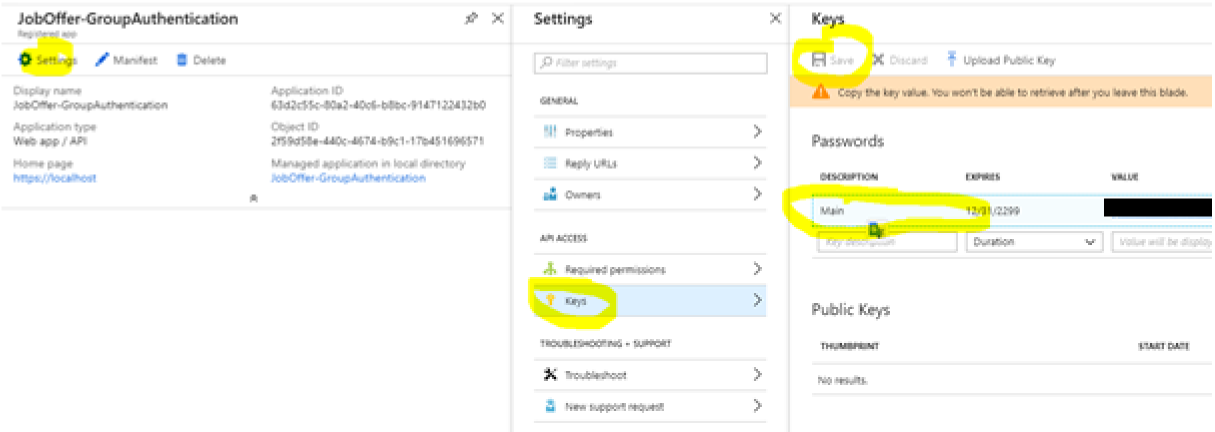
Application type
Web app / API

Object ID
2f59d58e-440c-4674-b9c1-17b451696571

Home page
https://localhost

Managed application in local directory
JobOffer-GroupAuthentication

40. Go to settings, generate new key and copy it:



Display name: JobOffer-GroupAuthentication
Application ID: 63d2c55c-80a2-40c6-b8bc-9147122432b0
Application type: Web app / API
Object ID: 2f59d58e-440c-4674-b9c1-17b451696571
Home page: https://localhost
Managed application in local directory: JobOffer-GroupAuthentication

Copy the key value. You won't be able to retrieve after you leave this blade.

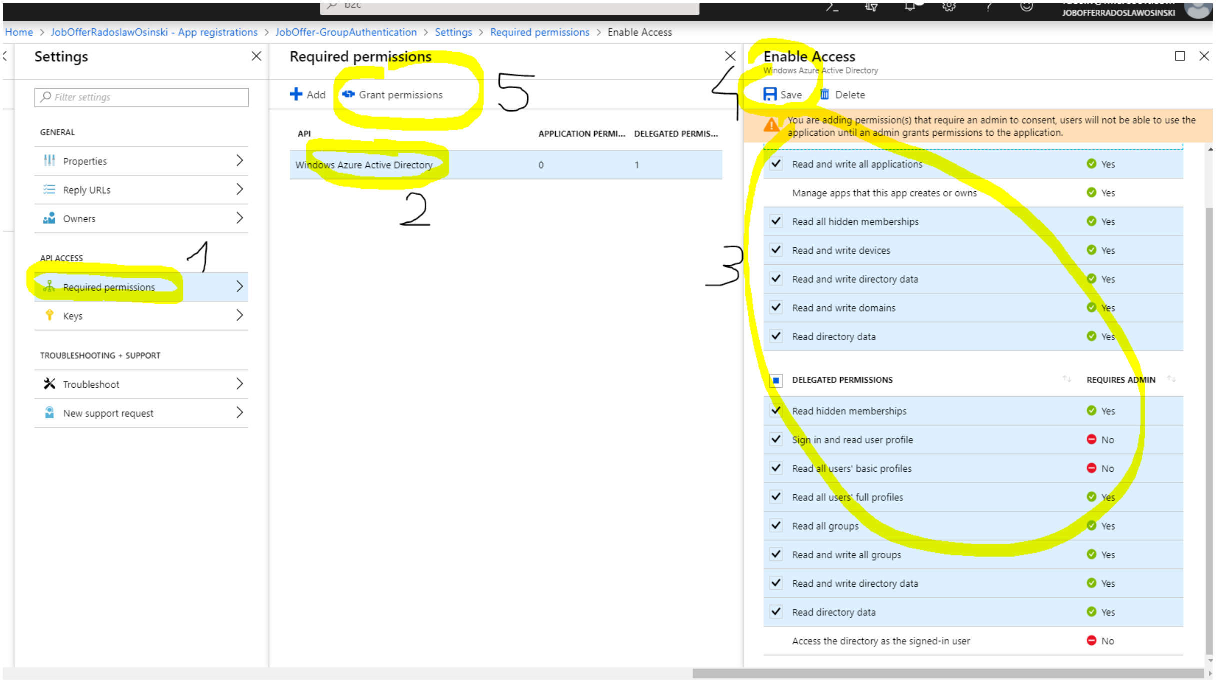
Passwords

DESCRIPTION	EXPIRES	VALUE
Main	12/31/2299	[redacted]
Key description	Duration	Value will be display

Public Keys

THUMBPRINT	START DATE
No results.	

41. Go to Required permissions → Windows Azure Active Directory. Select all read permmisions and Save it. After Save Click “Grand Permissions”:

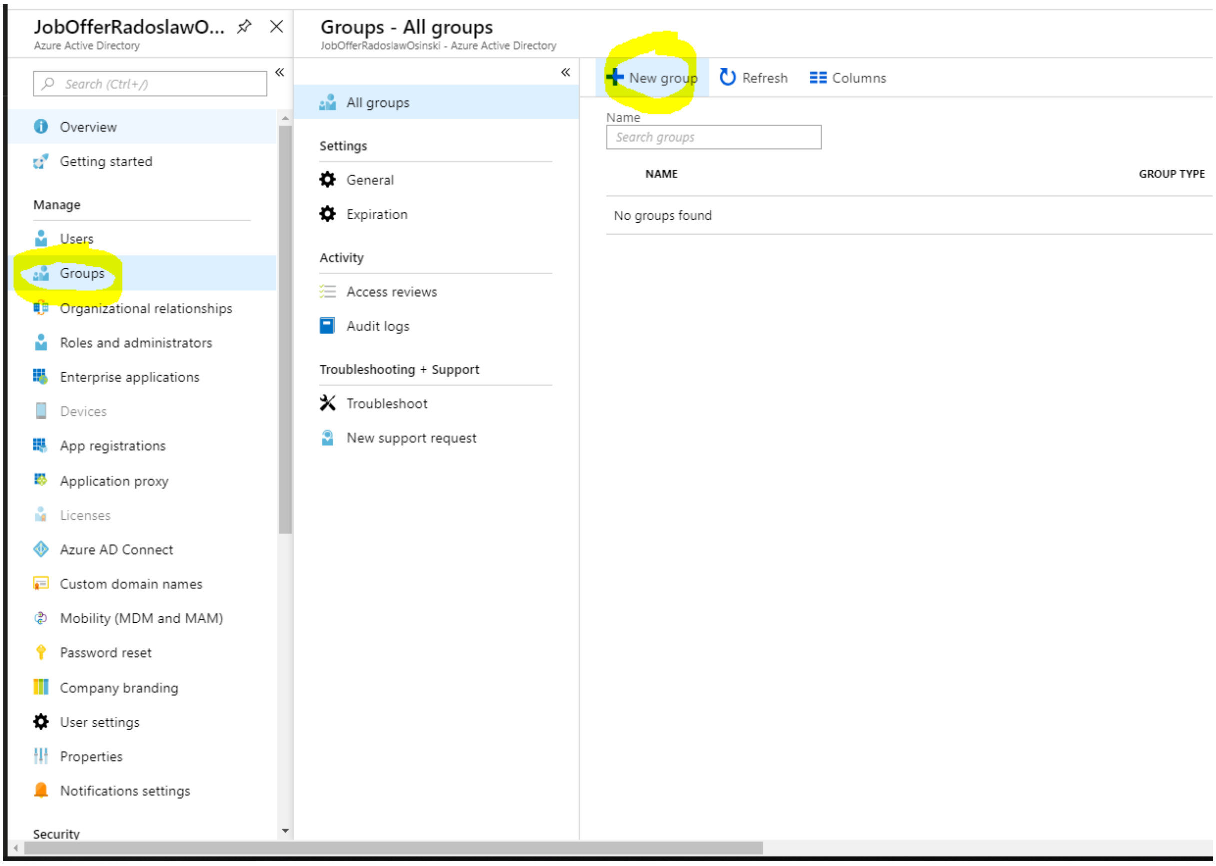


API	APPLICATION PERMI...	DELEGATED PERMIS...
Windows Azure Active Directory	0	1

You are adding permission(s) that require an admin to consent, users will not be able to use the application until an admin grants permissions to the application.

✓	Read and write all applications	Yes
	Manage apps that this app creates or owns	Yes
✓	Read all hidden memberships	Yes
✓	Read and write devices	Yes
✓	Read and write directory data	Yes
✓	Read and write domains	Yes
✓	Read directory data	Yes
■	DELEGATED PERMISSIONS	REQUIRES ADMIN
✓	Read hidden memberships	Yes
✓	Sign in and read user profile	No
✓	Read all users' basic profiles	No
✓	Read all users' full profiles	Yes
✓	Read all groups	Yes
✓	Read and write all groups	Yes
✓	Read and write directory data	Yes
✓	Read directory data	Yes
	Access the directory as the signed-in user	No

42. Go to groups and create one:



JobOfferRadoslawO...
Azure Active Directory

Search (Ctrl+/)

- Overview
- Getting started

Manage

- Users
- Groups
- Organizational relationships
- Roles and administrators
- Enterprise applications
- Devices
- App registrations
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings

Security

Groups - All groups
JobOfferRadoslawOsinski - Azure Active Directory

- All groups

Settings

- General
- Expiration

Activity

- Access reviews
- Audit logs

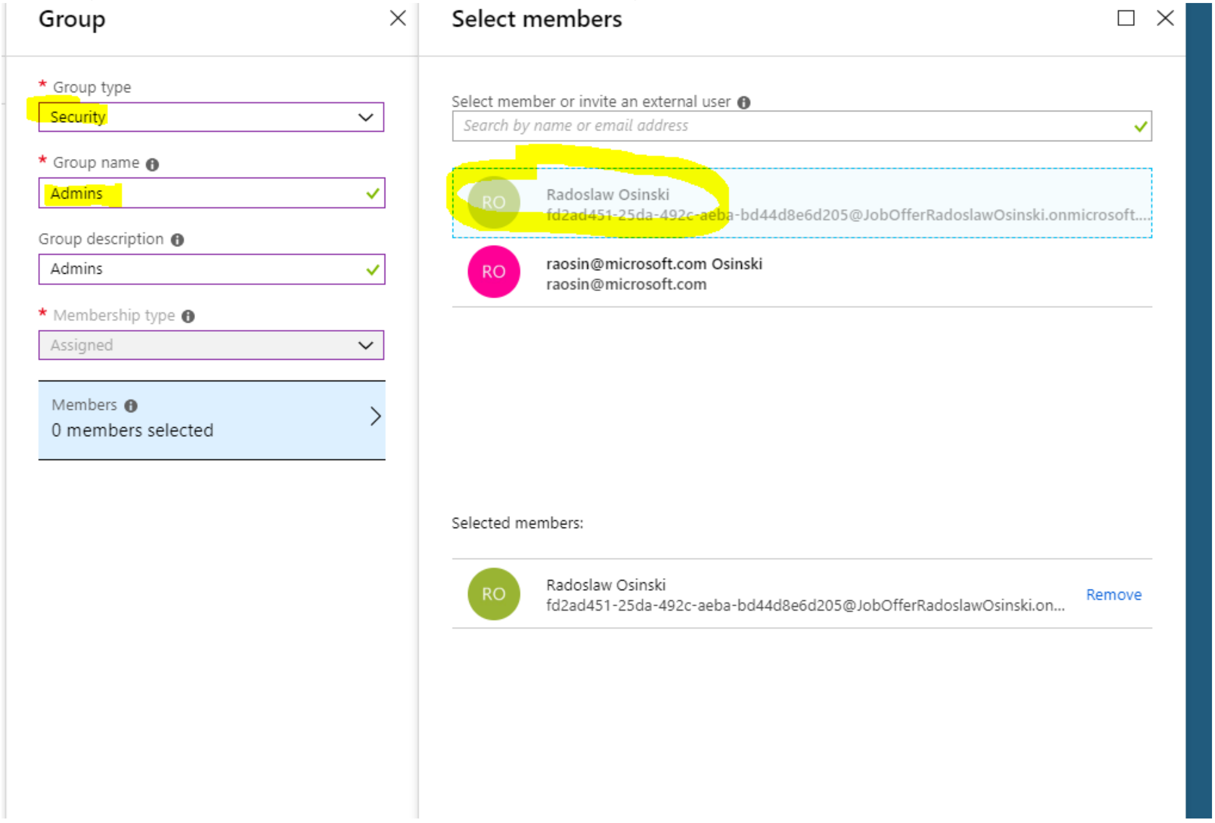
Troubleshooting + Support

- Troubleshoot
- New support request

Name
Search groups

NAME	GROUP TYPE
No groups found	

43. Durring creation select B2C user which you register before:



Group

* Group type
Security

* Group name
Admins

Group description
Admins

* Membership type
Assigned

Members
0 members selected

Select members

Select member or invite an external user
Search by name or email address

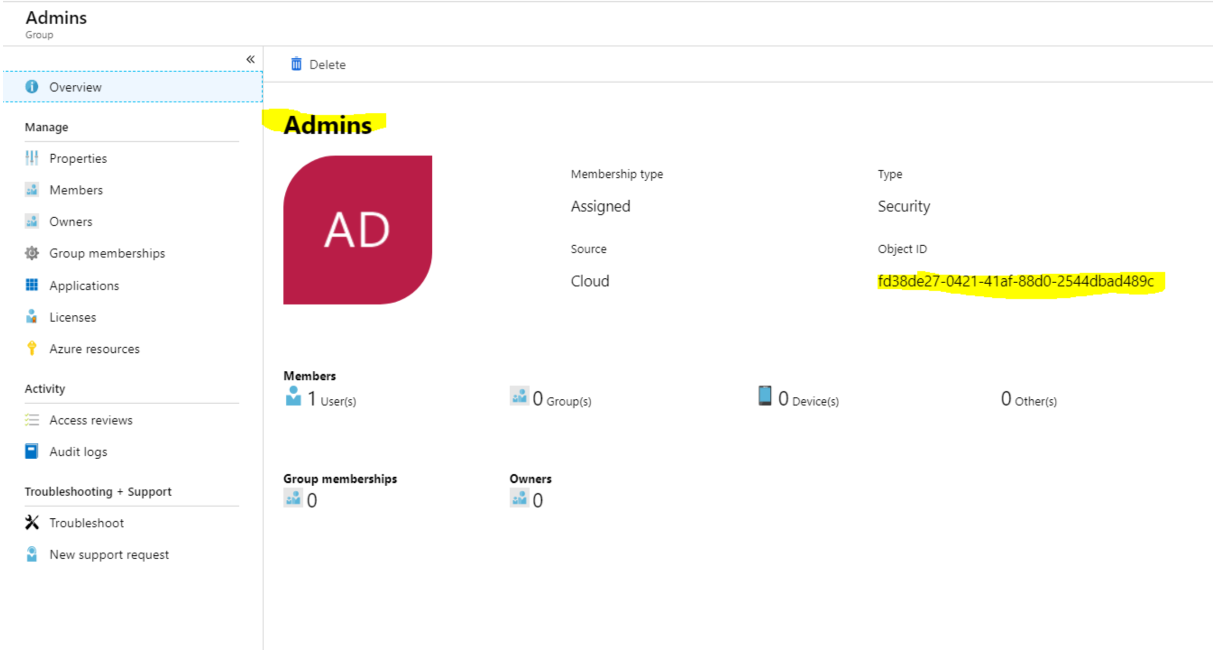
RO Radoslaw Osinski
fd2ad451-25da-492c-aeba-bd44d8e6d205@JobOfferRadoslawOsinski.onmicrosoft....

RO raosin@microsoft.com Osinski
raosin@microsoft.com

Selected members:

RO Radoslaw Osinski
fd2ad451-25da-492c-aeba-bd44d8e6d205@JobOfferRadoslawOsinski.on...
Remove

44. After group creation copy group name and object ID:



Admins

Membership type: Assigned

Type: Security

Source: Cloud

Object ID: fd38de27-0421-41af-88d0-2544dbad489c

Members: 1 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

Group memberships: 0

Owners: 0

45. In appsettings.json add section:

```
"AppSettings": {
   "AADGroups": [
     {
        "Name": "(step 44)",
        "Id": "(step 44)"
      }

    ],
    "GroupApplicationId": "(step 39)",
    "GroupApplicationKey": "(step 40)",
    "AuthenticationContext": "https://login.microsoftonline.com/<<tenant (step
16)>>",
    "UserIdClaimName":
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"
  }
```

46. Copy ApplicationSettings.cs
47. Add [Authorize] attribute on top of the Contact() In Home controller
48. Add constructor to home controller to take reference to app settings object:

```
private IConfiguration _configuration;
private AppSettings AppSettings { get; set; }

public HomeController(IConfiguration Configuration)
{
    _configuration = Configuration;
 AppSettings = _configuration.GetSection("AppSettings").Get<AppSettings>();
}
```

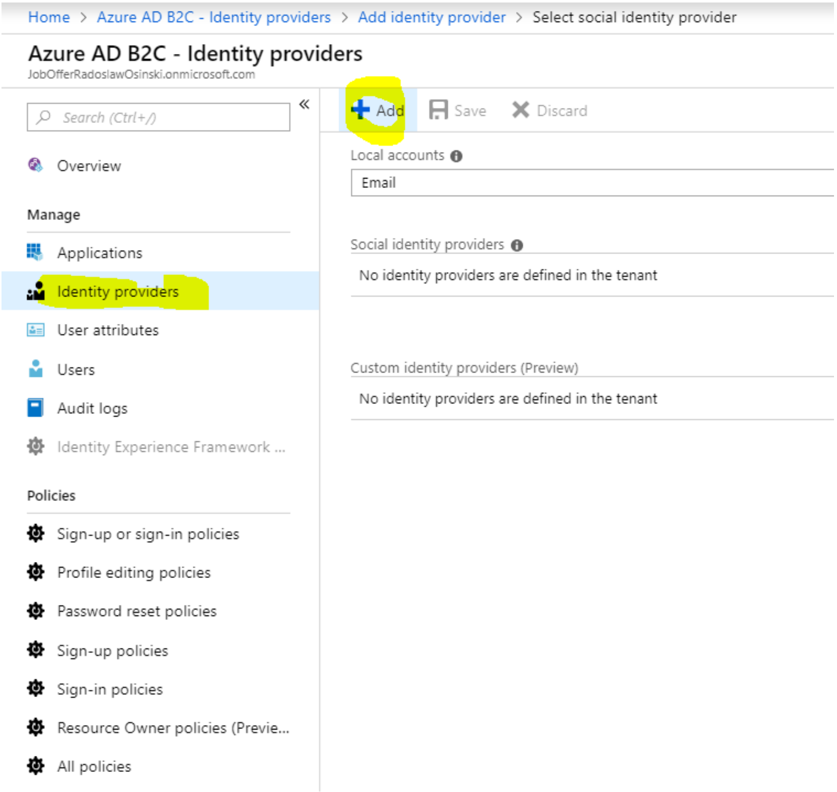
49. Paste code to Contact() action in home controller:

```
AADGraph graph = new AADGraph(AppSettings);
string groupName = "Admins";
string groupId = AppSettings.AADGroups.FirstOrDefault(g =>
String.Compare(g.Name, groupName) == 0).Id;
bool isIngroup = await graph.IsUserInGroup(User.Claims, groupId);
```

50. If user is in group bool value should be true.

Configure Additional Identity Provicers

51. Add additional identity providers:



Home > Azure AD B2C - Identity providers > Add identity provider > Select social identity provider

Azure AD B2C - Identity providers

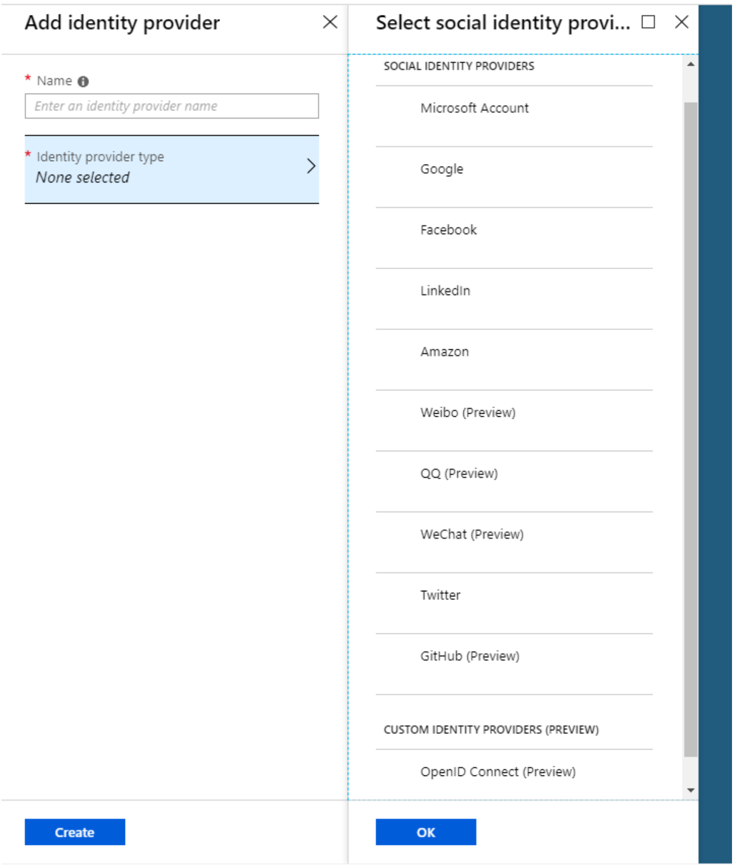
JobOfferRadoslawOsinski.onmicrosoft.com

Local accounts: Email

Social identity providers: No identity providers are defined in the tenant

Custom identity providers (Preview): No identity providers are defined in the tenant

52. Select from the available list.
(Providers required to register an app on their developer portal to receive credentials)



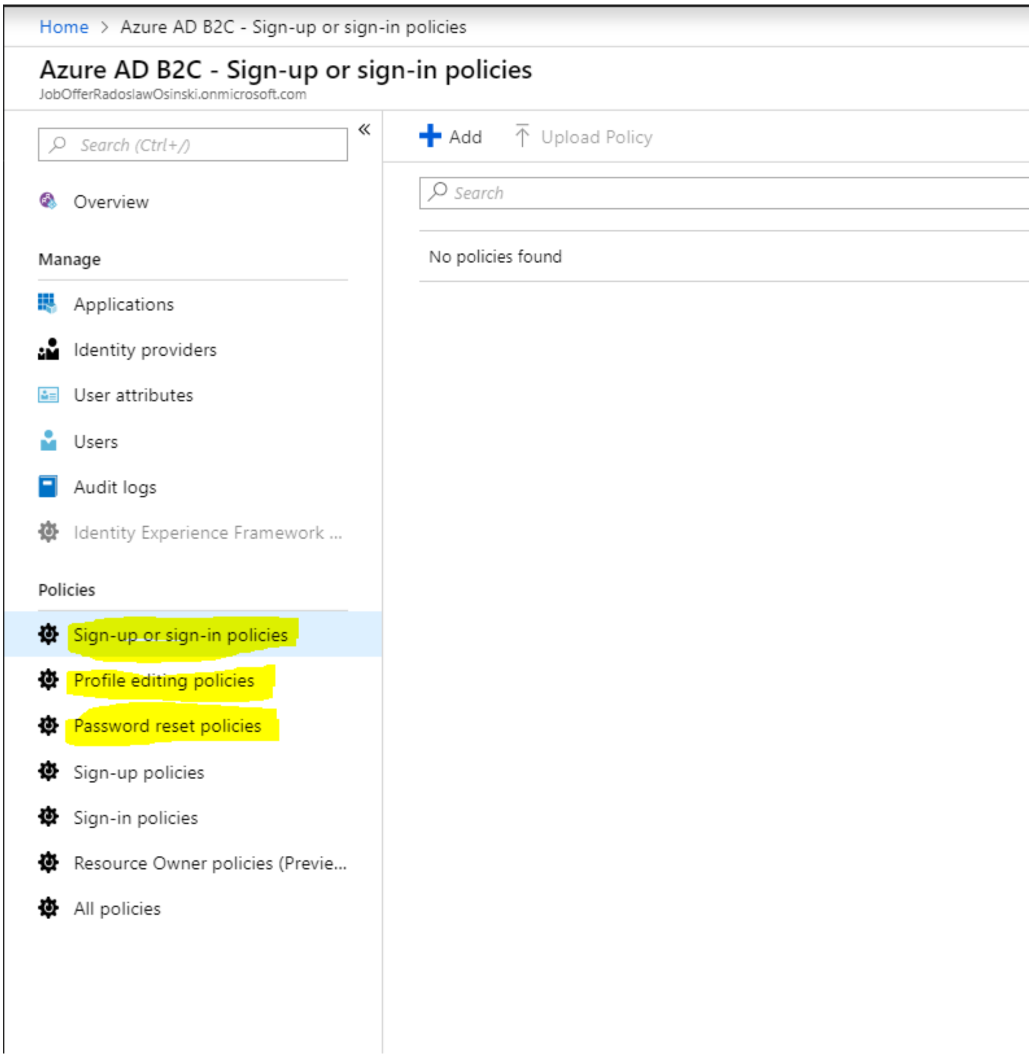
Add identity provider

* Name: Enter an identity provider name

* Identity provider type: None selected

Select social identity provi...

53. Add new identity providers to all politics that have been created:



Azure AD B2C - Sign-up or sign-in policies

JobOfferRadoslawOsinski.onmicrosoft.com

No policies found