Azure AD B2C lab

(Nov 7th, 2017 – M. Rochon)

# Objective

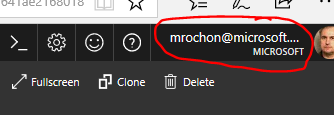
Create and explore your own Azure AD B2C tenant

# Requirements

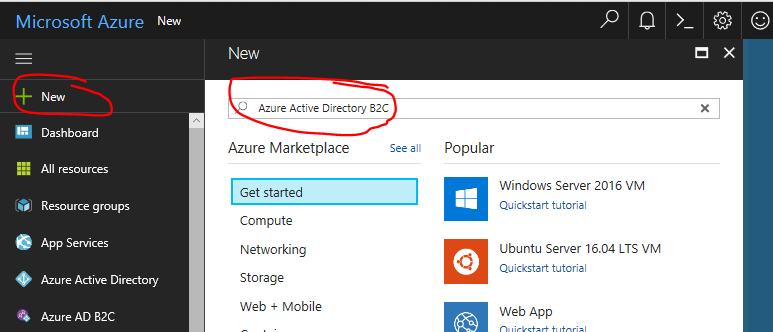
Access to an Azure subscription

# Create an Azure AD B2C tenant

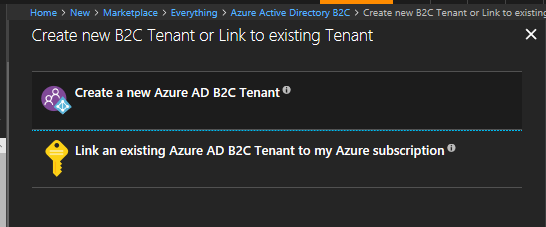
1. Navigate to <https://portal.azure.com>
2. Make sure that the top-right corner of the portal shows the correct Azure AD tenant – the one that owns this subscription. For me it is ‘Microsoft’ as below:



1. Select ‘+ New’ in the resource menu (left-hand side) and enter ‘Azure Active Directory B2C’ in the search field:



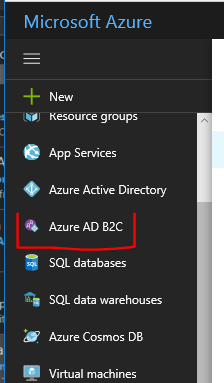
1. Press Enter and select the only displayed option: Azure Active Directory B2C.
2. Press Create button at the bottom of the screen. You should see the following screen. Select ‘Create a new …’ (the other option is for legacy purposes, for those who had created a B2C tenant using the old, classic portal).



1. Complete the tenant details as below. Make sure to use a globally unique name for your tenant domain prefix (the portal will verify that before it lets you do anything further). Press the Create button.
2. Once it is created (a couple of minutes), switch your portal context to view that tenant by changing your account tenancy in the right hand corner (compare to similar view in #2 above). Here, B2C Prod is the descriptive name of my B2C tenant.



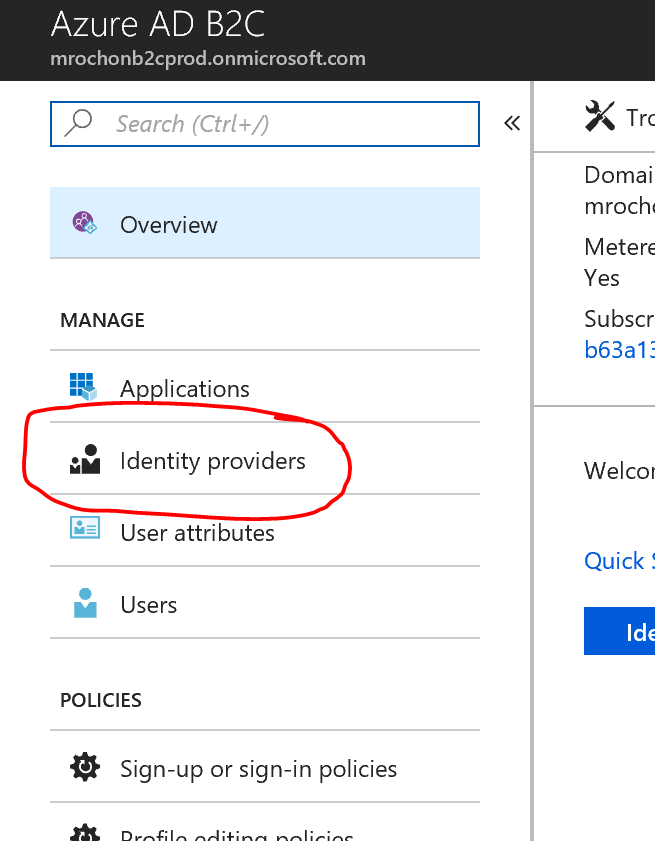
1. Check whether your left-hand side navigation panel contains a link to the ‘Azure AD B2C’ blades.



1. If it does not (it may be at a different vertical location), in the navigation menu of the portal (left-hand side) select ‘More services >’ and enter B2C in the search field. Select the ‘Azure AD 2C’ option. The B2C should now show in the navigation menu. You can use mouse-drag function to reposition it in the vertical list.
2. Select the Azure AD B2C to navigate to the B2C blade. Explore its functionality! Enjoy!
3. Remember to add a local user ([user@mytenant.onmicrosoft.com](mailto:user@mytenant.onmicrosoft.com)) with Global Admin privileges to access the tenant from Graph Explorer.

# Configure IdPs – authentication providers

1. Select the Identity Providers option from the B2C portal blade:



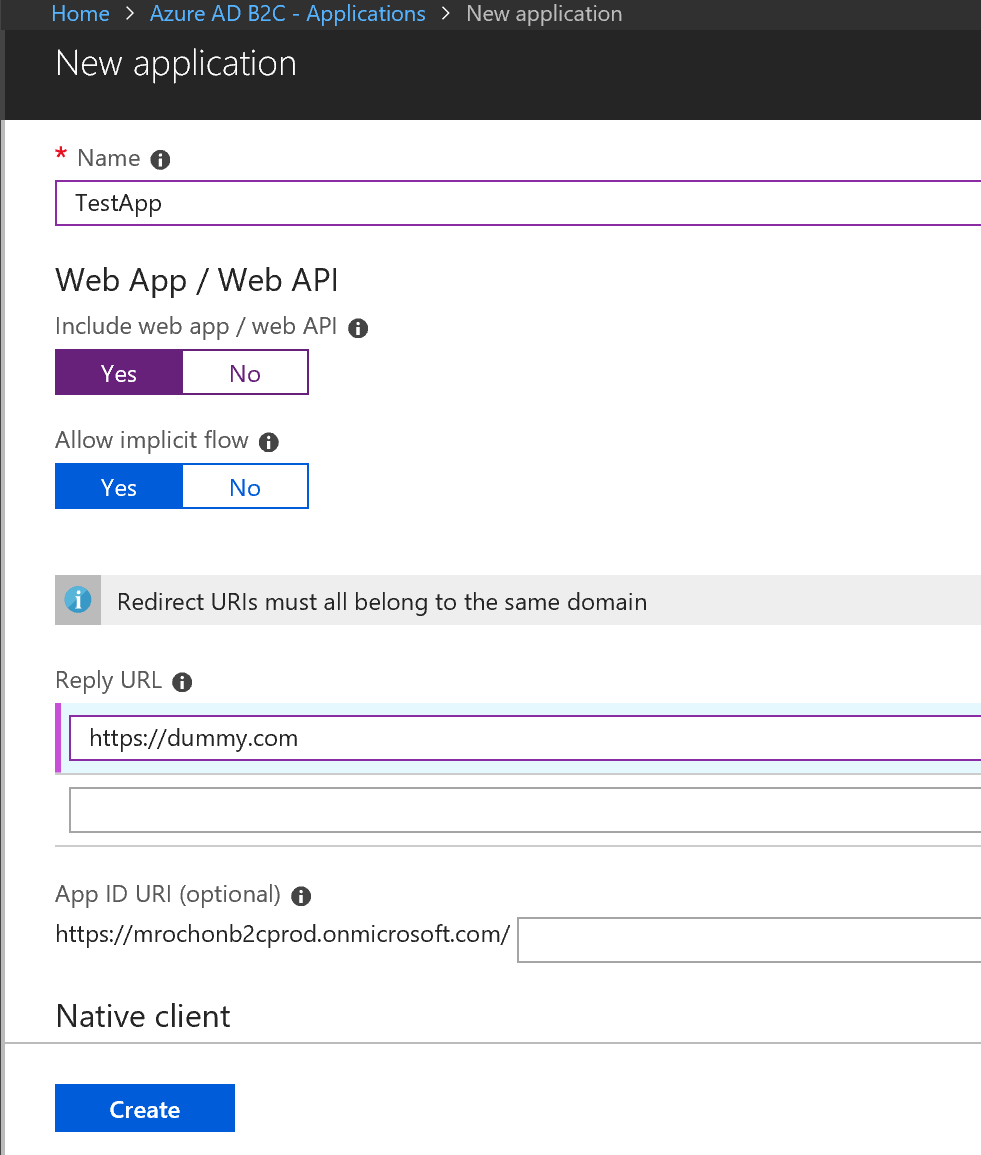
1. Select the type of local account you want to allow (email or username). You can control through the signup/in policies whether a user will in fact be able to use local accounts or only social accounts.
2. Follow instructions on <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-setup-msa-app> to allow users to use their MSA accounts (or use one of the other social account types).

# User attributes

1. Select the User Attributes option from the B2C portal blade.
2. Review existing built-in attributes and add any new attributes you may want to use for your users. For example, you may want to add a LoyaltyId attribute. Note that the selection of which attributes a user is asked to supply and which are passed in a token is configured later on as part of policy definition.

# Test application

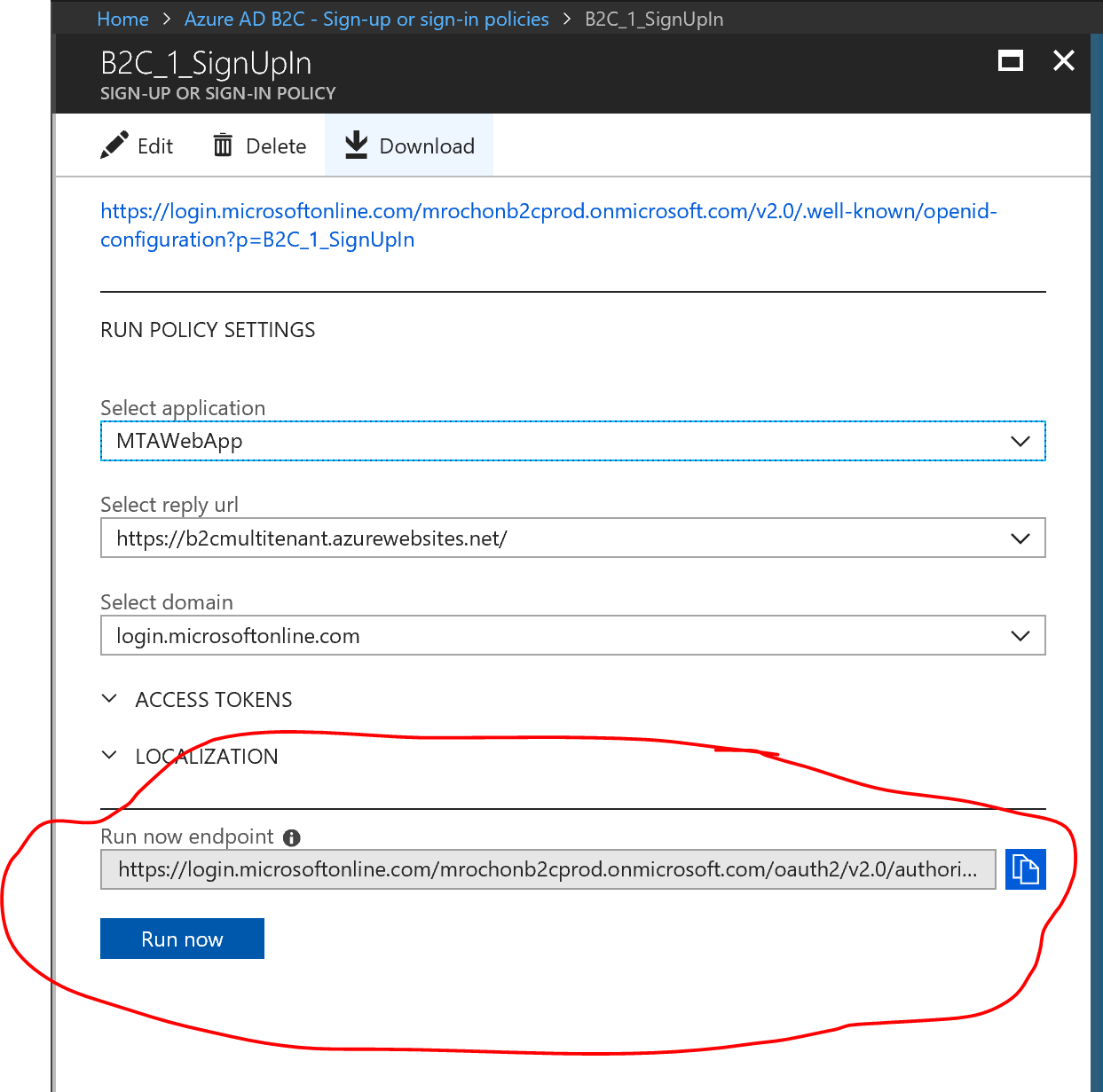
1. Select the Applications option from the B2C portal blade.
2. Click on the Add button to register a new application. For the purpose of this exercise we will register a non-existent application, which will still allow us to do some basic testing of our policies.
3. Give the application a name, e.g. TestApp and select other options as shown below. The reply url value does not need to resolve to a valid IP address (here it is <https://dummy.com>)



1. Click Create to register the application.

# Signup/in policy

1. Select the Sign-up or sign-in policies option from the B2C portal blade.
2. Use the Add button to create a new policy. Individual application will reference specific policies to get B2C to support specific user functionality, in this case signing in or (for new users) signing up to B2C.
   1. Give your policy a name, e.g. ‘SignInUp’ (B2C\_1\_ prefix will be added by B2C later).
   2. Select identity providers you want to allow in this policy, e.g. both local and MSA (or other) social.
   3. Select any sign-up attributes that a new user signing up for the service will need to provide as part of the sign-up process.
   4. Select attributes you want the policy to include in the id\_token sent to the application using this policy. Make sure to include the ‘User is new’ claim to allow the application to do any further processing of new users. You may also include other attributes you selected in as sign-up attributes. These attributes will be stored in B2C and are available through Graph API or to the other policies you may define later.
   5. Do not choose MFA or UI customization for now.
   6. Save the policy.
3. Select the policy you just defined. You should see the following UI.



1. ‘Run now endpoint’ is the url an application will need to redirect the user to (as part of the OIDC Auth Code flow. OWIN or other toolkits will usually take care of formatting the string in your application but you may want to inspect it here anyway).
2. Click on the ‘Run now’ button. This will simulate browser being redirected from your application to B2C to execute the signin/up policy (whose value is the p-parameter in the above url).
3. Use the page to signup as either a local or social user.
4. Once you have signed up B2C will attempt to redirect the browser back to the application. Since it does not exist, browser will show an error page. However the url string will contain the id\_token created by B2C (see below). Copy the value of the token to clipboard and use <https://jwt.ms> to inspect the claims it contains. Does it have the claims/attributes you have configured in the policy?

