# **Azure Active Directory B2C**

## **Pre-work for the B2C Partner Conference (May 2016)**

### Overview

# Azure Active Directory (Azure AD) B2C is a cloud identity service for your consumer-facing web & mobile apps. It is highly-available, secure and scales to millions of consumer identities. Consumers can use their social accounts (Facebook, Google, Microsoft account, etc.) or create new credentials to access your apps.

# This document describes the pre-work for the Azure AD B2C Partner Conference. Completing these steps will help you learn about the service and set you up for a productive conference. The exercise should take you 1-2 hours to complete.

# If you are stuck, check out this intro video (<https://channel9.msdn.com/Events/Build/2016/P423>) to see where all the relevant B2C Admin portal settings are.

### Ask

# After you’ve completed this exercise, email **AADB2CPreview@microsoft.com** (subject: **Whitelist tenant** **for Azure AD B2C Partner Conference**) your B2C tenant name, i.e., “**yourb2ctenant.onmicrosoft.com**”. We need to whitelist the tenant for Premium features. Send us any feedback that you may have on documentation.

### Pre-requisites

* Windows 10
* Azure subscription (Sign up for a free account [here](https://azure.microsoft.com/free/). Use a Microsoft account (e.g. xyz@outlook.com))
* Visual Studio 2015 (to complete app-side work)

### Step 1: Create an Azure AD B2C tenant

Follow these steps to get yourself an Azure AD B2C tenant: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-get-started/>.

### Step 2: Create a Global Admin user in your B2C tenant and manage users in classic Azure

Create a Global Admin user in your B2C tenant (e.g. **admin@*yourtenant*.onmicrosoft.com**). You’ll need this for the B2C Premium lab later on. For now, you can continue to use the Microsoft account that you have signed-in with. To create the user and easily add/delete user objects as you complete this exercise, use classic Azure portal at <http://manage.windowsazure.com>. Select your B2C Directory, Select “USERS” tab.

### Step 3: Register a web app

Register a web app in your B2C tenant: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-app-registration/>. Make sure that you have:

* Name your app “**b2ctestapp**”
* Toggled the “**Include web app / web API**” switch to “**Yes**”.
* In **Reply URLs**, you have plugged in “**https://localhost:44321/**” (to use in your Visual Studio .NET MVC app) and “**https://aadb2cplayground.azurewebsites.net**” (to use with the **Run now** option on the B2C Admin Portal; see later for more details).
* Copied the “**Application Client ID**” value of the web app that you just created.

### Step 4: Create a sign-up or sign-in policy

Next, you’ll need to create a sign-up or sign-in policy (<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-reference-policies/#create-a-sign-up-or-sign-in-policy>). Policies fully describes consumer identity experiences such as sign-up, sign-in, profile editing and password reset. Your app triggers the appropriate experience by invoking the right policy (as a query parameter ‘p’) as part of the authentication request. You’ll need the policy name (for e.g., b2c\_1\_susi) for this purpose.

You can use the **Run now** option to test the policy. Make sure you choose “**b2ctestapp**” under “**Select application to run policy**” and “**https://aadb2cplayground.azurewebsites.net**” under “**Select Redirect URI**”

After the execution of the policy you will see the claims selected.

### Step 5: Create a password reset policy

Create a password reset policy (<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-reference-policies/#create-a-password-reset-policy>) and test it out as well.

### Step 6: Add Facebook support

Register a Facebook application and add its details to your B2C tenant using the steps outlined here: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-setup-fb-app/>. Now, add Facebook support to your sign-up or sign-in policy by:

* Click the sign-up or sign-in policy created in Step 4.
* Click **Edit** at the top.
* Click **Identity Providers** and select **Facebook** (in addition to **Email signup**).
* Click **OK** and then **Save**.
* Use **Run now** and test out the experience (first-time sign-up & subsequent sign-ins).

### Steps 7 & 8: Add Google & Microsoft account support (optional)

Similar to Step 6. Instructions are here (<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-setup-goog-app/> and <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-setup-msa-app/>).

### Step 9: Add MFA support to your sign-up or sign-in policy

Enable MFA on your policy (<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-reference-mfa/>). Test it out.

### Step 10: Customize one of the sign-up or sign-in pages in your policy

Use these guides (<https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-reference-ui-customization/>, <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-reference-ui-customization-helper-tool/>) to customize one of the pages in the sign-up or sign-in policy. Even if you don’t get a chance to complete this step, do read up on the basics.

### Step 11: Wire up a .NET MVC app in Visual Studio with your policies (optional)

The sample + instructions are here: <https://github.com/azureadquickstarts/b2c-webapp-openidconnect-dotnet-susi>.

### Step 12: Use Azure AD Graph API to create, read, update & delete users (optional)

The sample + instructions are here: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-b2c-devquickstarts-graph-dotnet/>.