Lab: Working with Azure AD B2C Userflows

Overview

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

Objectives

Learn how to:

- Create a new Azure AD B2C tenant.
- Register your web application and create sign-up, sign-in and password reset experiences using userflows.
- Enable multifactor authentication (MFA) to add extra security.
- Provide a sign-up or sign-in experience in 37 different languages.
- Customize the UI of the sign-up and sign-in screens.

Prerequisites

- Microsoft Azure account
- Internet

Table of Contents

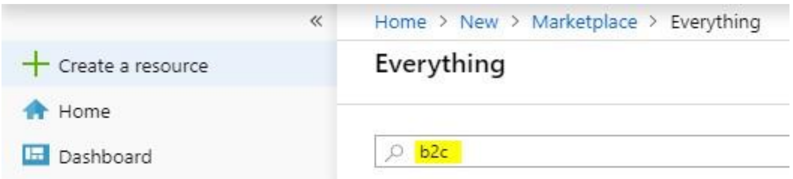
Task 1: Create a new Azure AD B2C tenant

Let's start by creating an Azure AD B2C tenant. A "tenant" (also called a "directory") is a container for all your customers, apps, policies, groups and more.

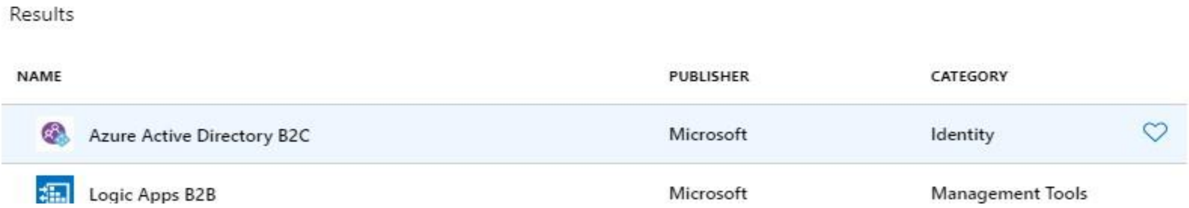
1. First, sign in to the Azure portal at https://portal.azure.com.

   a. Enter your Hotmail or Outlook credentials.

2. Click the **Create a Resource** button and search for **"b2c"**



3. From the search results, click **Azure Active Directory B2C**.



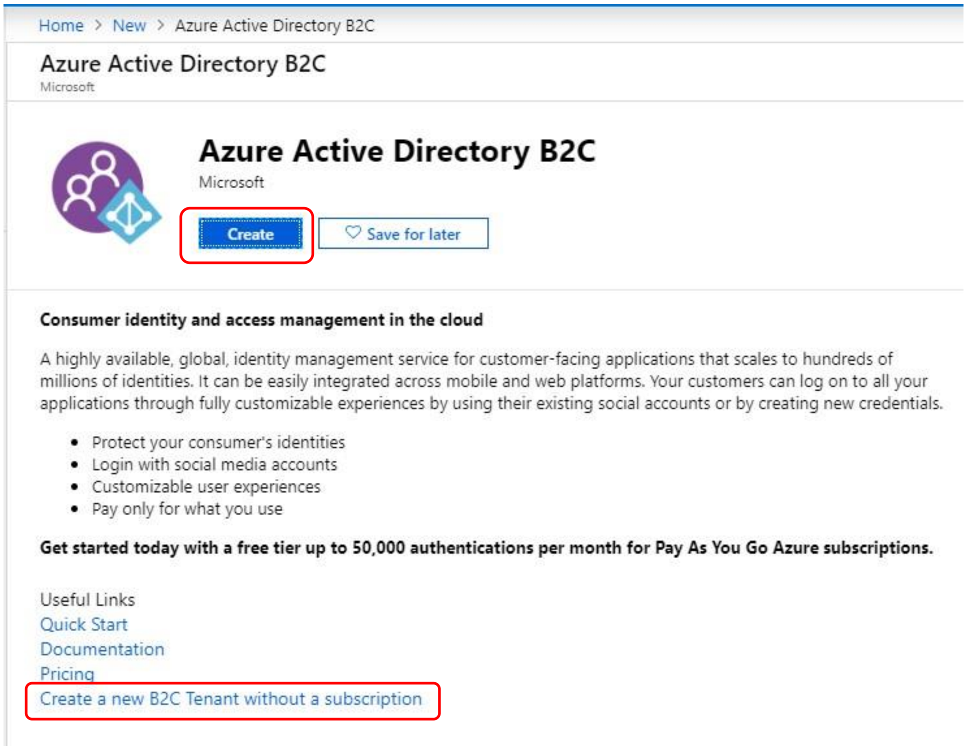
Results

NAME	PUBLISHER	CATEGORY
Azure Active Directory B2C	Microsoft	Identity
Logic Apps B2B	Microsoft	Management Tools

4. Next, if you want to test AAD B2C functionality for free (up to 50,000 authentications per month), you will need an Azure account that is not associated to an Enterprise Agreement.

   a. If you already have such an Azure Account with a subscription, click on **Create** at the next screen and go to step number 5.

   b. If you prefer to add an Azure Account with a subscription later, click on **Create a new B2C Tenant without a subscription** at the next screen and go to step number 5.



Azure Active Directory B2C

Microsoft

Azure Active Directory B2C

Microsoft

Consumer identity and access management in the cloud

A highly available, global, identity management service for customer-facing applications that scales to hundreds of millions of identities. It can be easily integrated across mobile and web platforms. Your customers can log on to all your applications through fully customizable experiences by using their existing social accounts or by creating new credentials.

- Protect your consumer's identities
- Login with social media accounts
- Customizable user experiences
- Pay only for what you use

Get started today with a free tier up to 50,000 authentications per month for Pay As You Go Azure subscriptions.

Useful Links

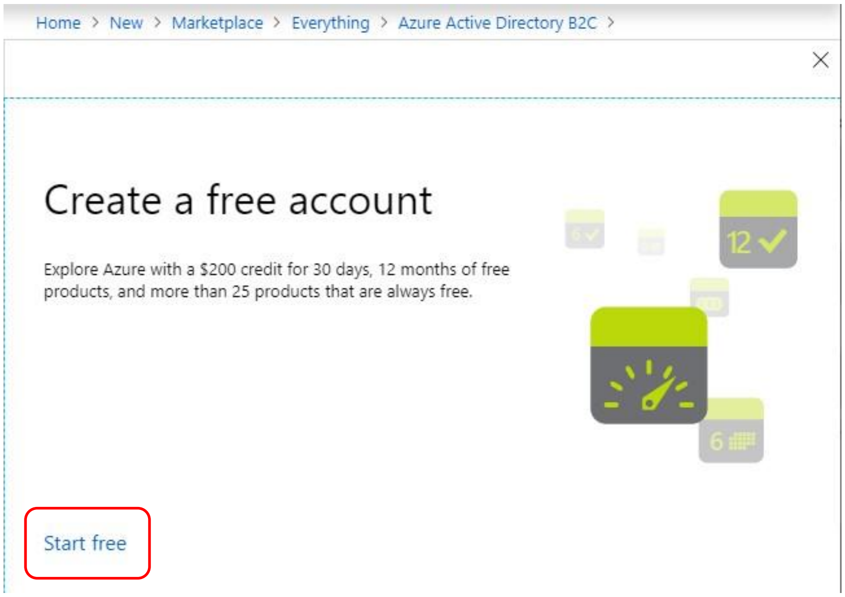
Quick Start

Documentation

Pricing

Create a new B2C Tenant without a subscription

c. Otherwise, if your current Azure account is tied to an Enterprise Agreement or if you don’t already have an account, select **Start free.** Then, go to step D in this section.


Home > New > Marketplace > Everything > Azure Active Directory B2C >

Create a free account

Explore Azure with a $200 credit for 30 days, 12 months of free products, and more than 25 products that are always free.

With your Azure free account, you get all of this—and you won’t be charged until you choose to upgrade.

12 months	+	$200 credit	+	Always free
of popular free services		to explore any Azure service for 30 days		25+ services

IMPORTANT - Note that in order to create your new Azure free account, you are required to provide your credit card information. Azure needs to keep a credit card on file in the event you decide to upgrade or in case you use non-free resources.

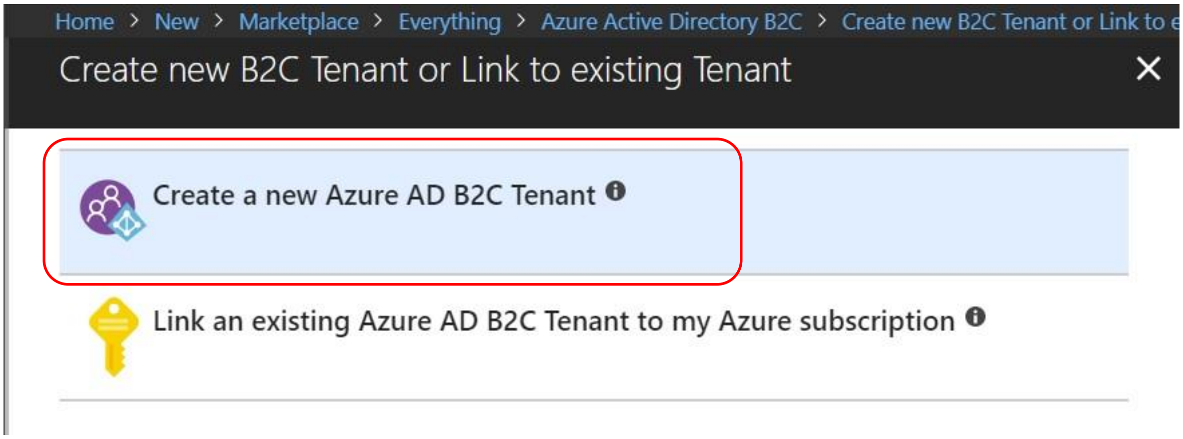
With Azure AD B2C, you account gets 50,000 free authentications per month. However, Azure Multi-Factor Authentication for Azure AD B2C users will be charged at a flat fee of $0.03 per authentication. Go to http://aka.ms/aadb2cpricing for more details.

To avoid any charges to your credit card:

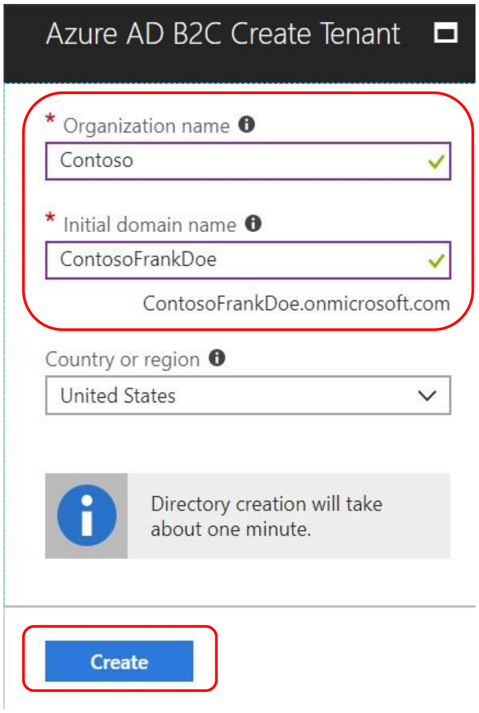
- **Don't authenticate more than 50,000 times per month.**
- **Don't enable MFA in your AAD B2C tenant.**

d. After you have created your new free account, open a new window and go to the Azure portal at https://portal.azure.com. Repeat steps 2 and 3.

5. Click on the **Create a new Azure AD B2C Tenant** link to create a new directory.


Home > New > Marketplace > Everything > Azure Active Directory B2C > Create new B2C Tenant or Link to e
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

6. Enter an **Organization name** of **"Contoso"** and an **Initial domain name** that's globally unique. For example, you may want to include your name, such as **"ContosoFrankDoe"**. This will be the subdomain of the tenant. Which we also called the tenant name, such as **"ContosoFrankDoe.onmicrosoft.com"**, and will be used to configure the application later. Click **Create**.



Azure AD B2C Create Tenant

* Organization name

Contoso

* Initial domain name

ContosoFrankDoe

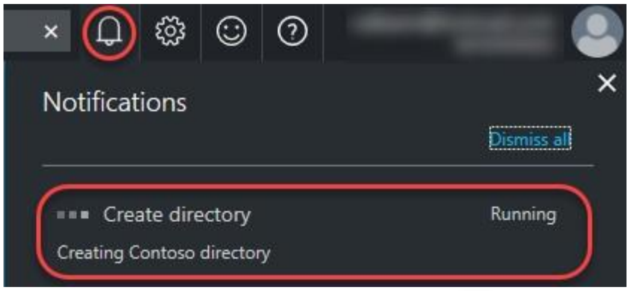
ContosoFrankDoe.onmicrosoft.com

Country or region

United States

Directory creation will take about one minute.

7. It will take a minute or so for the directory to be created. You can track progress using the notifications dropdown in the top right corner of the portal.



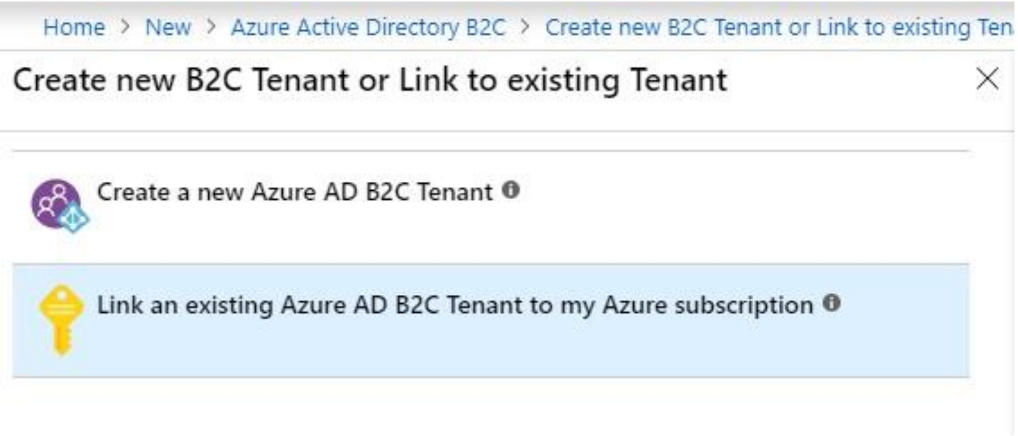
Notifications

Create directory — Running

Creating Contoso directory

8. Once the directory has been created, ↻ **Refresh** your browser to reflect all the changes.

9. select **Link an existing Azure AD B2 Tenant to my Azure Subscription.**



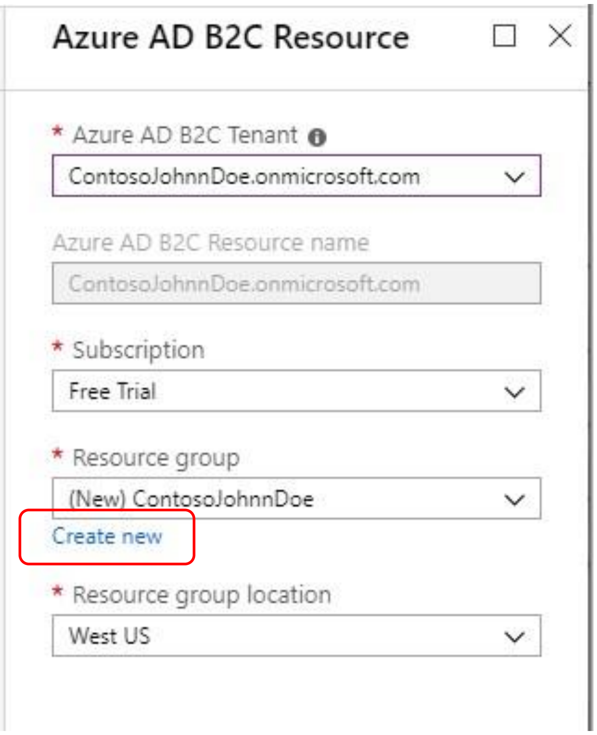
Home > New > Azure Active Directory B2C > Create new B2C Tenant or Link to existing Ten

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

10. From the drop-down menus, select your tenant**, create a new resource group** if you don't already have one, and select the resource group location that you consider is closer to you. Click **create**.



Azure AD B2C Resource

* Azure AD B2C Tenant
ContosoJohnnDoe.onmicrosoft.com

Azure AD B2C Resource name
ContosoJohnnDoe.onmicrosoft.com

* Subscription
Free Trial

* Resource group
(New) ContosoJohnnDoe
Create new

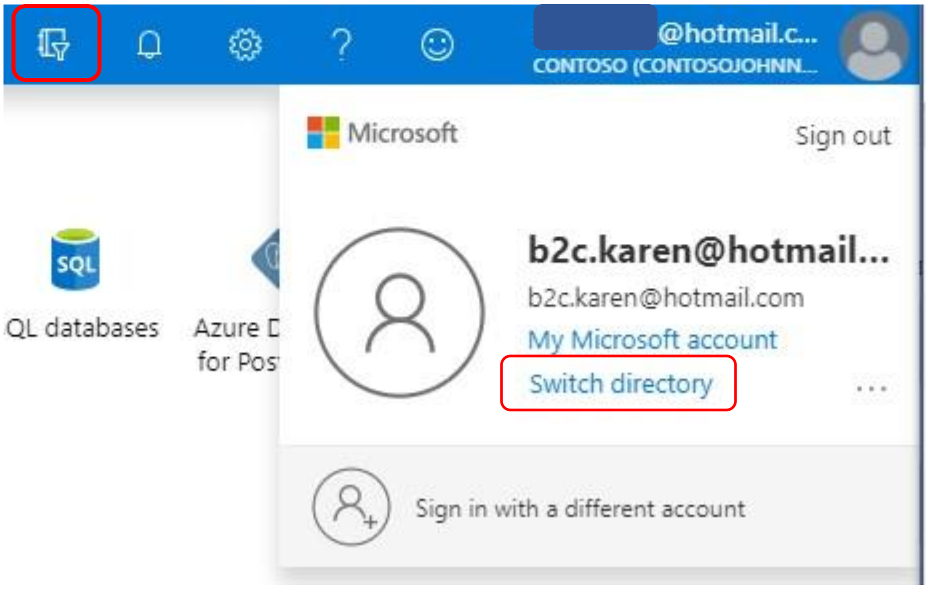
* Resource group location
West US

11. It will take a minute or so for the resource group to be created. You can track progress using the notifications dropdown in the top right corner of the portal.

12. After the resource group is created, ↻ **Refresh** your browser or **sign out from the portal and sign in again**.

13. Click on your name, on the top right corner and select Switch directory.

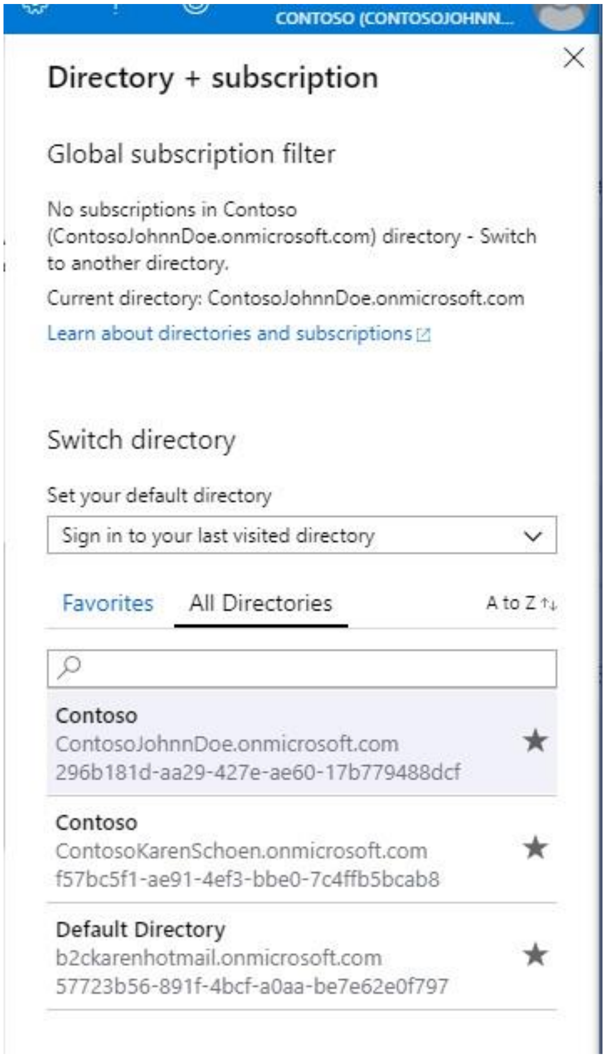
    Or select the switch directory symbol



[redacted]@hotmail.c...
CONTOSO (CONTOSOJOHNN...

b2c.karen@hotmail...
b2c.karen@hotmail.com

14. You will see your Default Directory and your newly created AAD B2C directory, in this case called Contoso. These two directories are completely independent from each other. Select your AAD B2C directory.



No subscriptions in Contoso (ContosoJohnnDoe.onmicrosoft.com) directory - Switch to another directory.

Current directory: ContosoJohnnDoe.onmicrosoft.com

Set your default directory: Sign in to your last visited directory

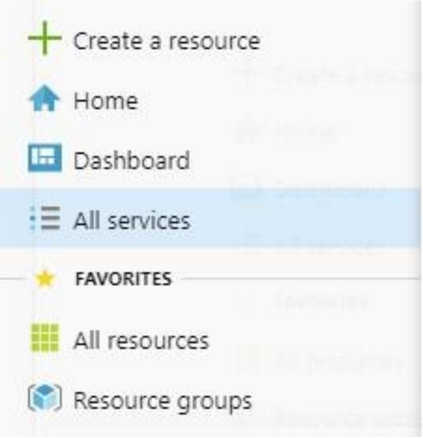
Contoso
ContosoJohnnDoe.onmicrosoft.com
296b181d-aa29-427e-ae60-17b779488dcf ★

Contoso
ContosoKarenSchoen.onmicrosoft.com
f57bc5f1-ae91-4ef3-bbe0-7c4ffb5bcab8 ★

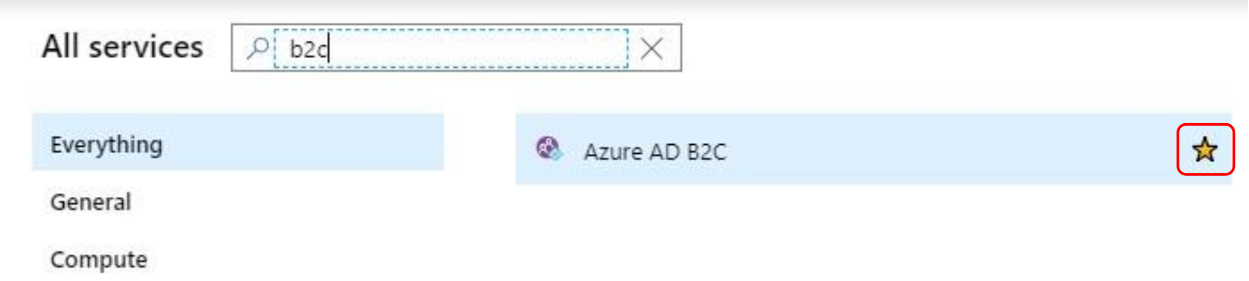
Default Directory
b2ckarenhotmail.onmicrosoft.com
57723b56-891f-4bcf-a0aa-be7e62e0f797 ★

IMPORTANT: you need to be in the AAD B2C directory in order to have access to AAD B2C functionality and user directory.

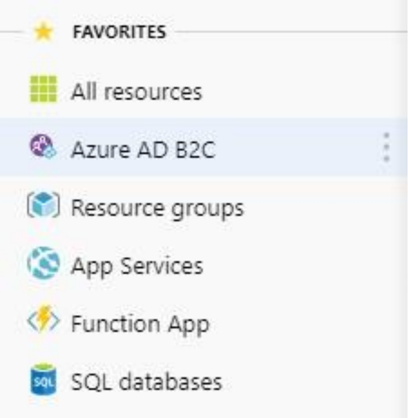
15. To make it easier to access your new AAD B2C tenant, select **All services**.



16. Enter “**b2c**” in the search bar. Then, **click on the star** symbol to add Azure AD B2C to your favorites.



17. Look for **Azure AD B2C** blade under your Favorites menu on the left-hand side of the portal and click on it. For easy access, you can **drag it to the top** of the list.

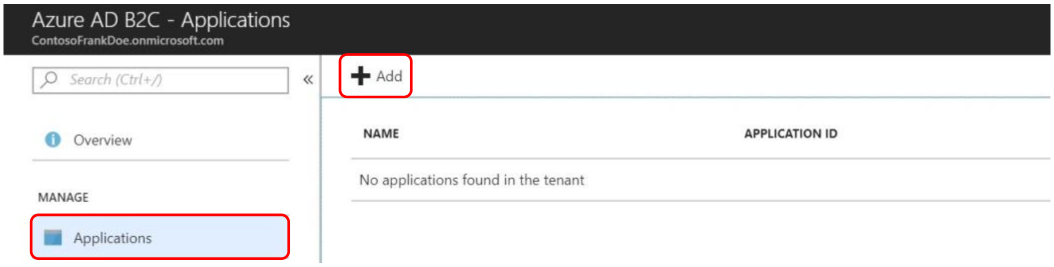


Task 2: Register your web app

You should now be on the page that lets you configure Azure AD B2C. If you are not, see the instructions in the appendix.

The first thing we will do is register an application. This is necessary for Azure AD B2C to identify which application is making the sign-in request.

1. Select the **Applications** tab and click **Add**.

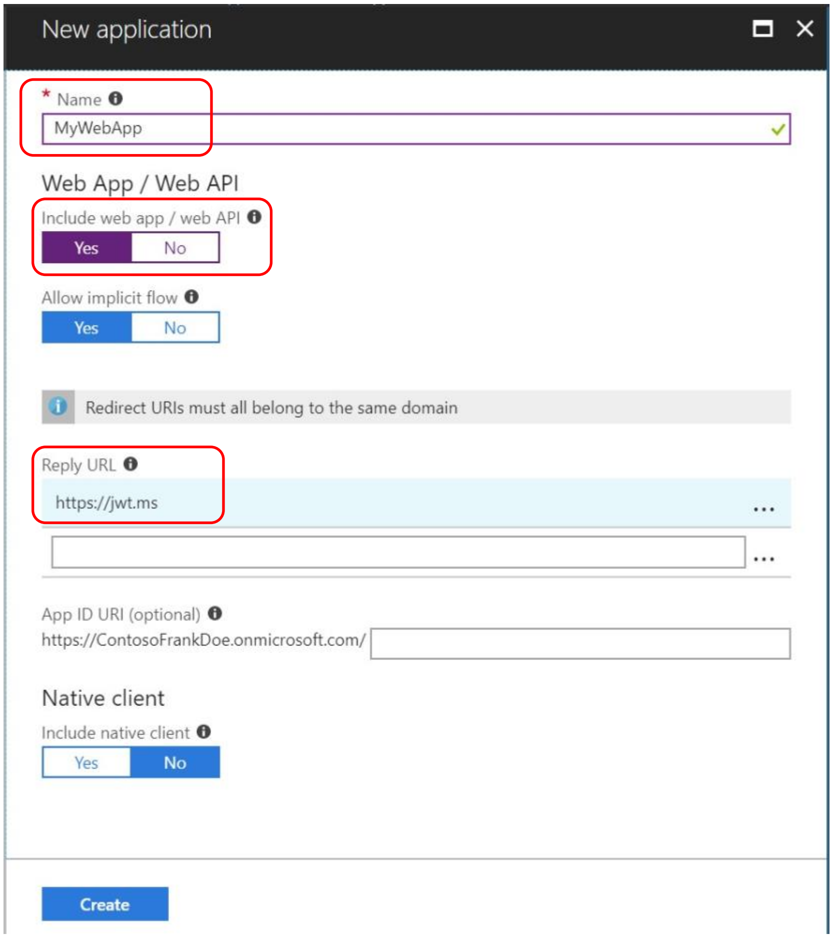


No applications found in the tenant

2. Enter **“MyWebApp”** as the **Name** of the application. Select **Yes** for **Include Web App / Web API**.

3. Add **“https://jwt.ms”** as a **Reply URL**. This is where Azure AD B2C will send tokens back after a successful sign up or sign in. Because we do not have an application built yet, we will use https://jwt.ms temporarily. This web application simply displays the claims in the minted token.

4. Click **Create** to create the application.



New application

* Name

MyWebApp

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://jwt.ms

App ID URI (optional)

https://ContosoFrankDoe.onmicrosoft.com/

Native client

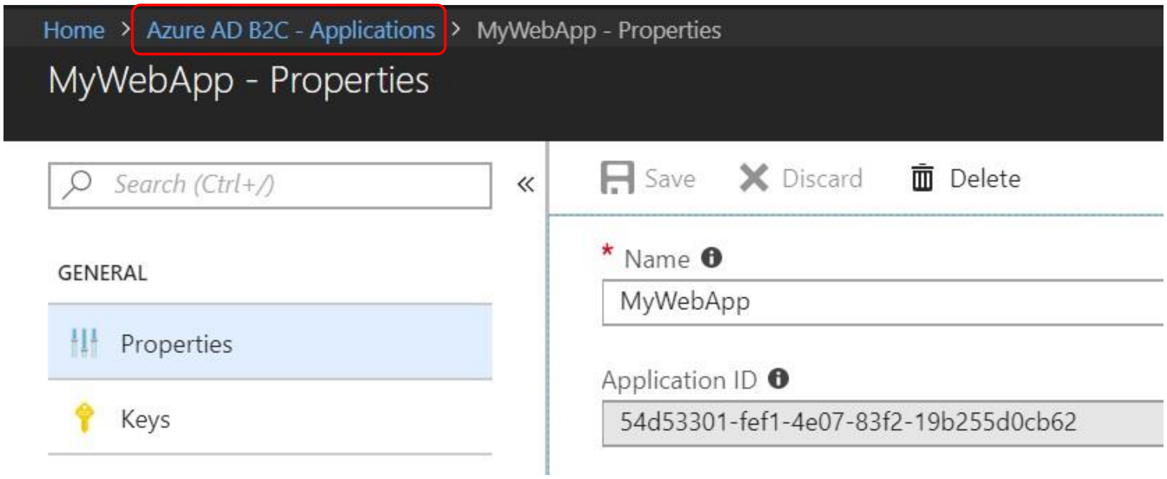
Include native client

Yes [✓ No]

Task 3: Create your sign-in/sign-up policy

Next, you need to create a sign up or sign in policy. Policies are settings that fully describes customer identity experiences such as sign-up, sign-in, profile edit and password reset. Your app can trigger the appropriate experience by invoking the right policy as part of the authentication request.

1. Use the breadcrumb at the top of the portal to return to the **Overview** menu for Azure AD B2C.



Home > Azure AD B2C - Applications > MyWebApp - Properties

MyWebApp - Properties

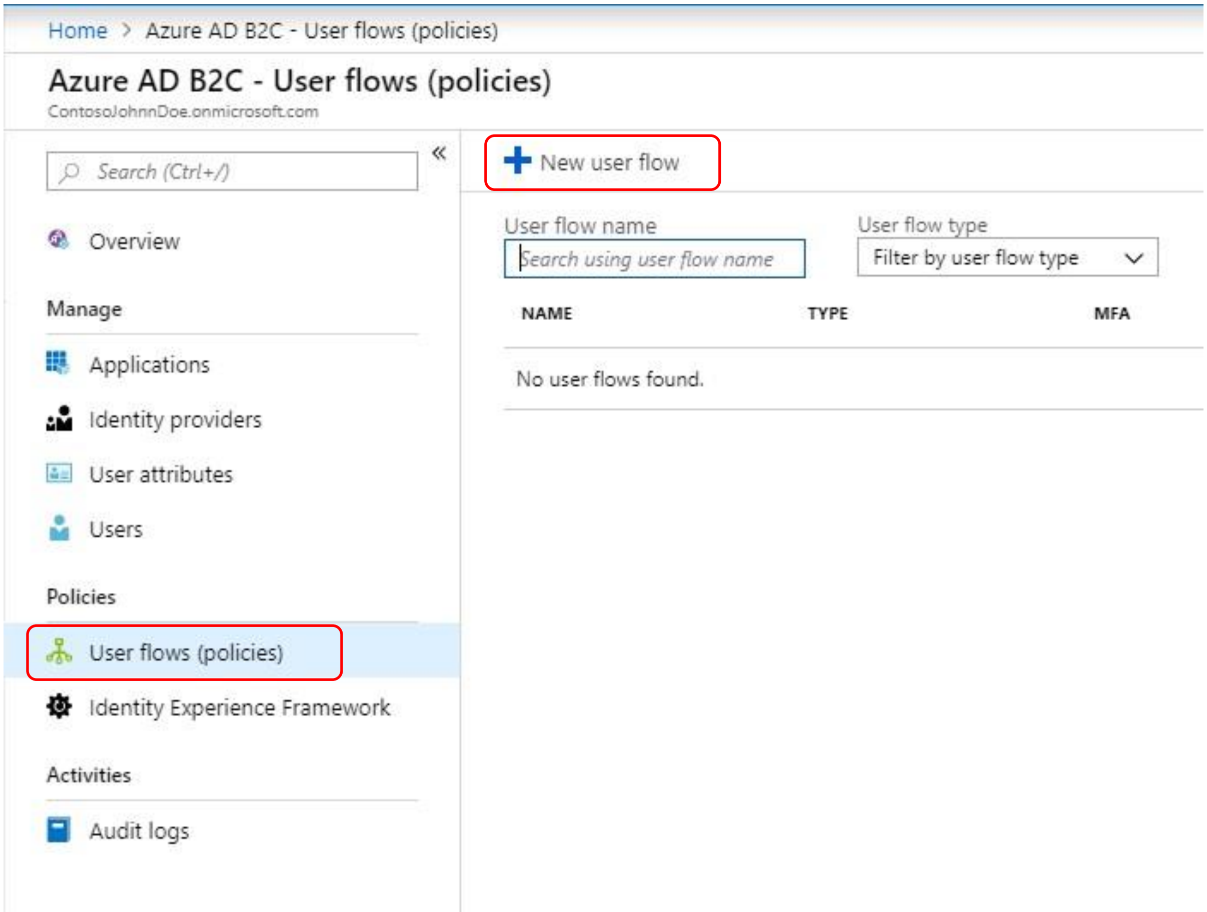
* Name

MyWebApp

Application ID

54d53301-fef1-4e07-83f2-19b255d0cb62

2. Select the **User flows (policies)** tab and click **New user flow**.



Home > Azure AD B2C - User flows (policies)

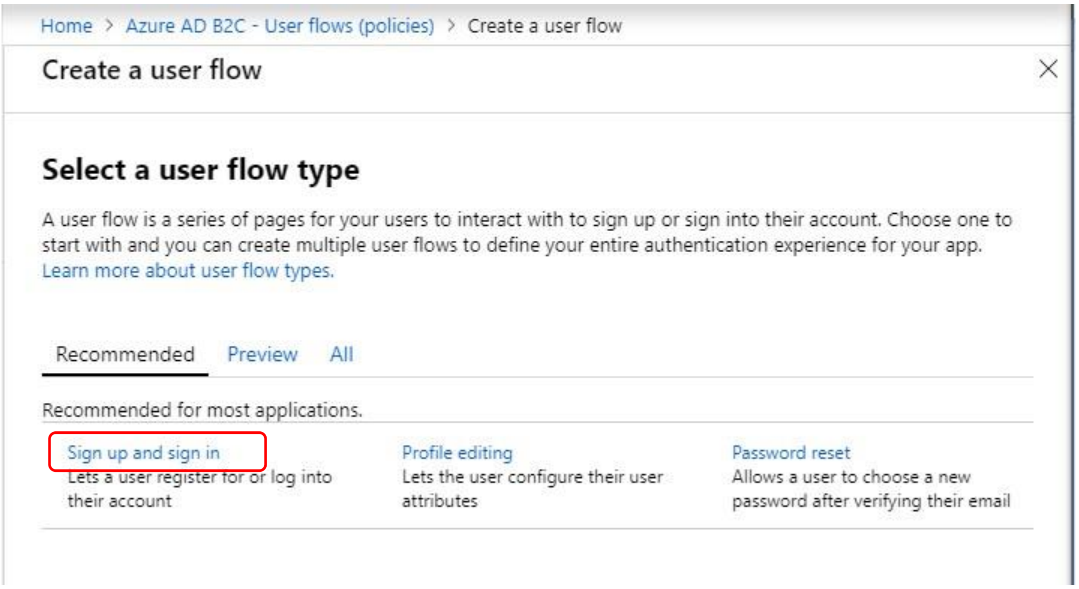
Azure AD B2C - User flows (policies)

ContosoJohnnDoe.onmicrosoft.com

NAME	TYPE	MFA
No user flows found.		

3.

Select **Sign up and sign in**.



Home > Azure AD B2C - User flows (policies) > Create a user flow

Create a user flow

Select a user flow type

A user flow is a series of pages for your users to interact with to sign up or sign into their account. Choose one to start with and you can create multiple user flows to define your entire authentication experience for your app. Learn more about user flow types.

Recommended for most applications.

Sign up and sign in
Lets a user register for or log into their account

Profile editing
Lets the user configure their user attributes

Password reset
Allows a user to choose a new password after verifying their email

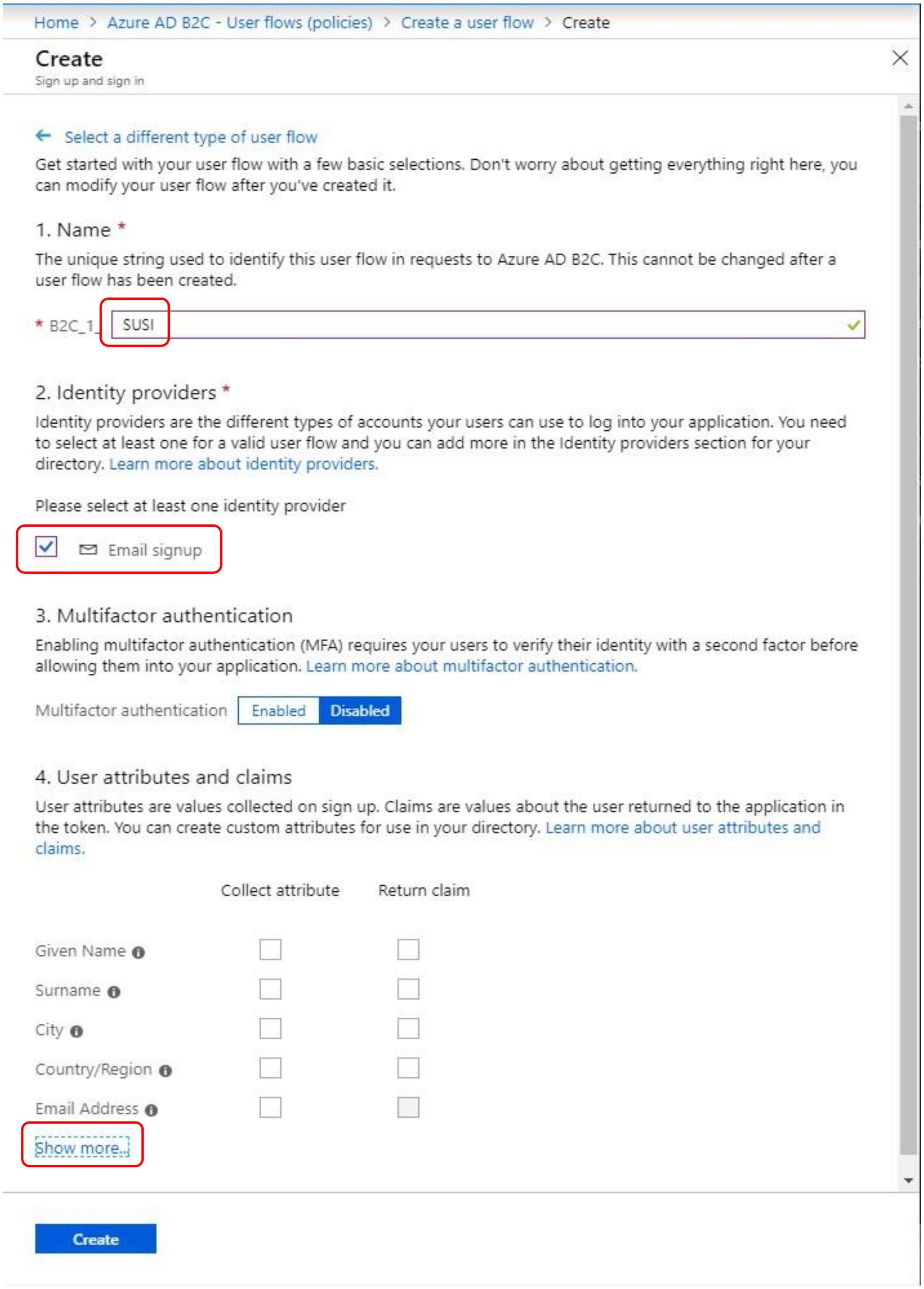
In step number 1, enter **"SUSI"** as the **Name** for the Sign-Up or Sign-In (SUSI) policy. (Once created, your policy name will be automatically prefixed with "B2C_1_" to become "B2C_1_SUSI)

In step number 2, from the **Identity providers** check **Email signup**. This will allow users to sign up (or sign in) using an email address and password. No other identity providers have been configured yet.

In step number 3, You can ignore **Multifactor authentication** for now.

In step number 4, click on **Show more…**

4.



Home > Azure AD B2C - User flows (policies) > Create a user flow > Create

Create

Sign up and sign in

← Select a different type of user flow

Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.

1. Name *

The unique string used to identify this user flow in requests to Azure AD B2C. This cannot be changed after a user flow has been created.

* B2C_1_ SUSI ✓

2. Identity providers *

Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you can add more in the Identity providers section for your directory. Learn more about identity providers.

Please select at least one identity provider

☑ ✉ Email signup

3. Multifactor authentication

Enabling multifactor authentication (MFA) requires your users to verify their identity with a second factor before allowing them into your application. Learn more about multifactor authentication.

Multifactor authentication: Enabled [✓ Disabled]

4. User attributes and claims

User attributes are values collected on sign up. Claims are values about the user returned to the application in the token. You can create custom attributes for use in your directory. Learn more about user attributes and claims.

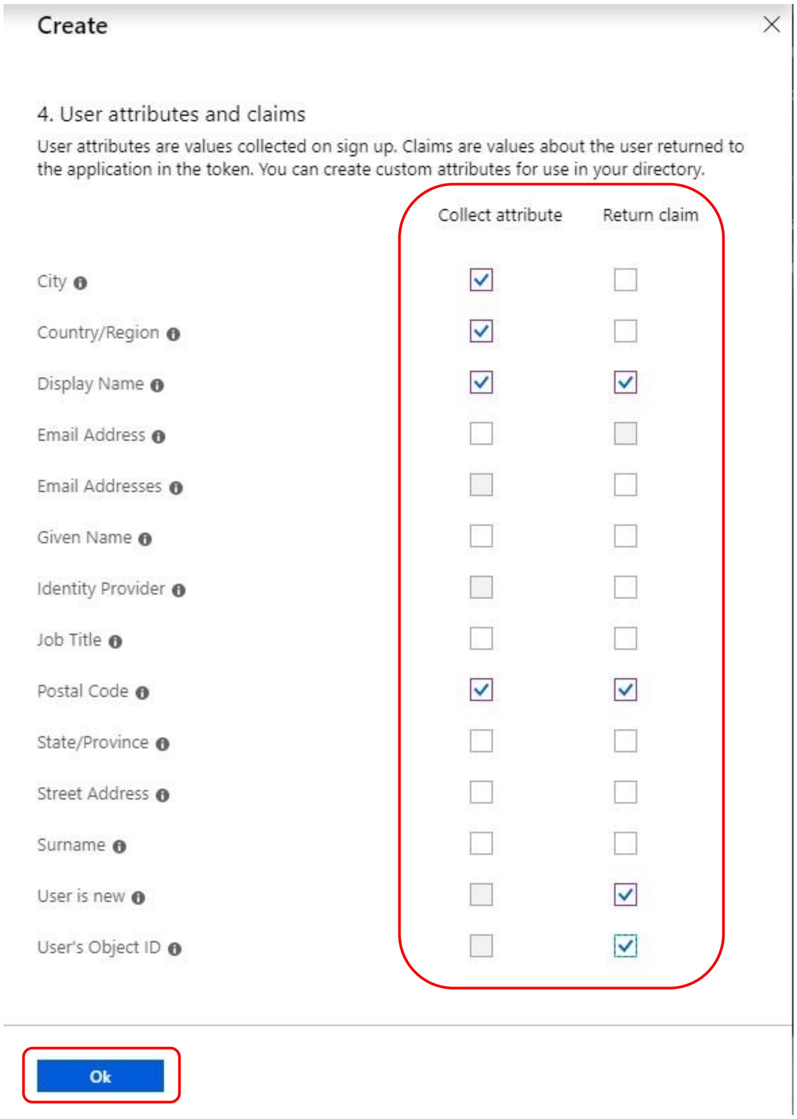
	Collect attribute	Return claim
Given Name ℹ	□	□
Surname ℹ	□	□
City ℹ	□	□
Country/Region ℹ	□	□
Email Address ℹ	□	□

Show more...

From **collect attributes**, check **City, Country/Region, Display Name, and Postal Code**. This represents the data that will be collected from the user when the user is going through the sign up process.

6. Then, from the **return claim** check **Display Name, Postal Code, User is new, and User's Object ID** and click **OK**. This represents the data about the user that will be returned to the application in the token as claims. Click **Create**.

5.



Create

4. User attributes and claims

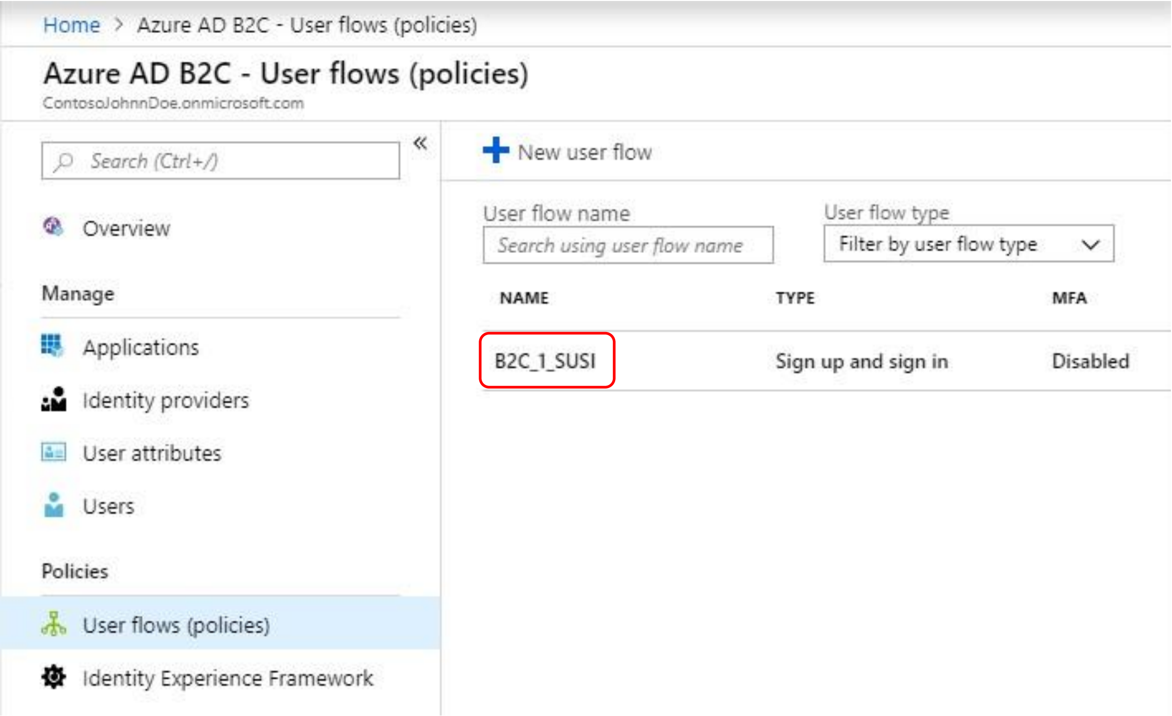
User attributes are values collected on sign up. Claims are values about the user returned to the application in the token. You can create custom attributes for use in your directory.

	Collect attribute	Return claim
City	☑	□
Country/Region	☑	□
Display Name	☑	☑
Email Address	□	□
Email Addresses	□	□
Given Name	□	□
Identity Provider	□	□
Job Title	□	□
Postal Code	☑	☑
State/Province	□	□
Street Address	□	□
Surname	□	□
User is new	□	☑
User's Object ID	□	☑

Task 4: Try out the newly created user experience

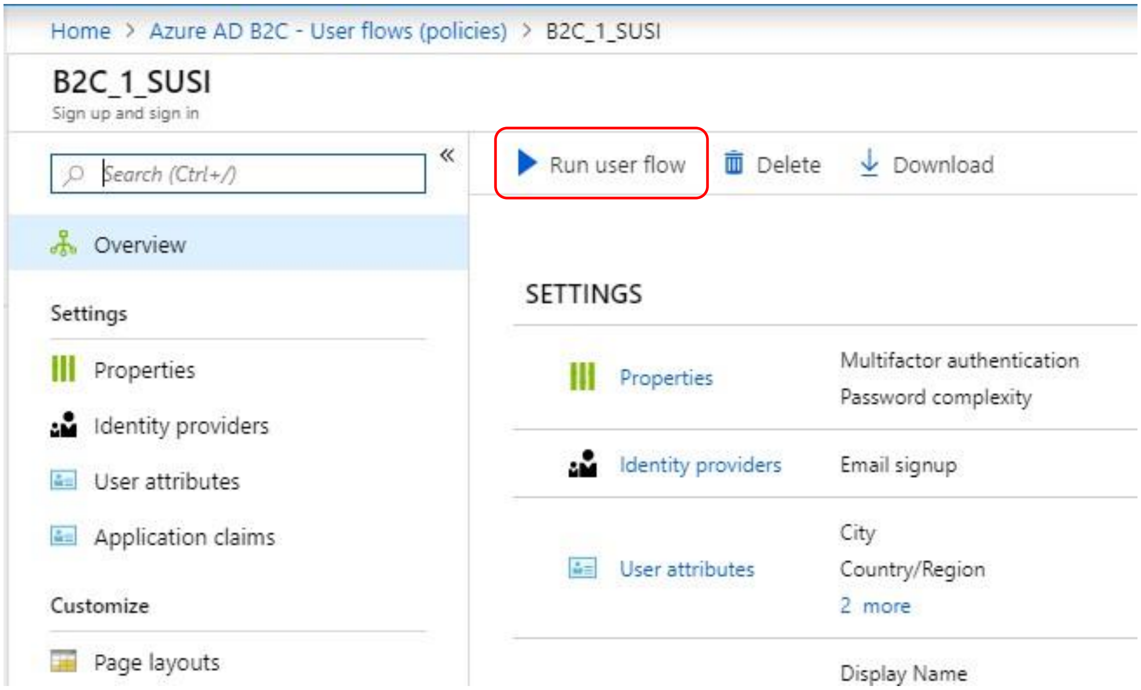
Now that you have created a sign-up or sign-in policy, you can run the policy to see what the user experience will be like when a user is redirected to Azure AD B2C from the application.

1. Open the policy that you just created (**B2C_1_SUSI**).



NAME	TYPE	MFA
B2C_1_SUSI	Sign up and sign in	Disabled

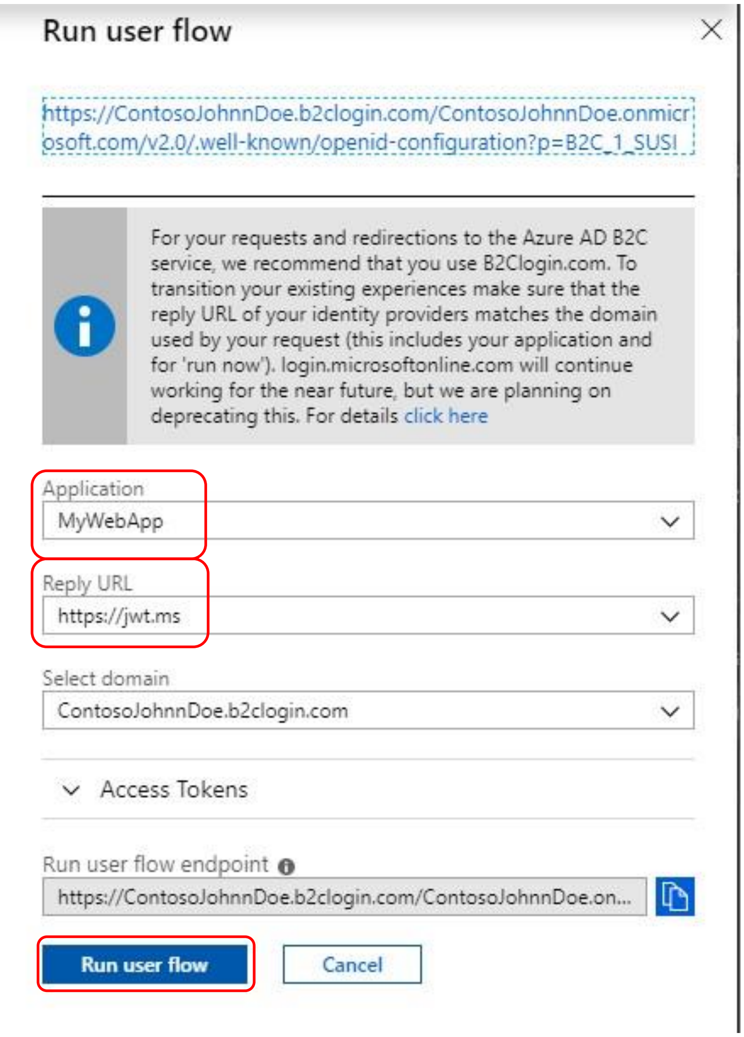
2. You will see an overview of your new policy. Click **Run user flow** to test it.



SETTINGS

Properties	Multifactor authentication Password complexity
Identity providers	Email signup
User attributes	City Country/Region 2 more
	Display Name

3. If not already selected by default, use the “**MyWebApp**” application with the reply URL set to https://jwt.ms (the Reply URL that you registered when creating that application). Click on **Run user flow.** This will open a new tab and take you to the sign up/in experience that you just created.



Run user flow

https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.onmicrosoft.com/v2.0/.well-known/openid-configuration?p=B2C_1_SUSI

For your requests and redirections to the Azure AD B2C service, we recommend that you use B2Clogin.com. To transition your existing experiences make sure that the reply URL of your identity providers matches the domain used by your request (this includes your application and for 'run now'). login.microsoftonline.com will continue working for the near future, but we are planning on deprecating this. For details click here

Application: MyWebApp

Reply URL: https://jwt.ms

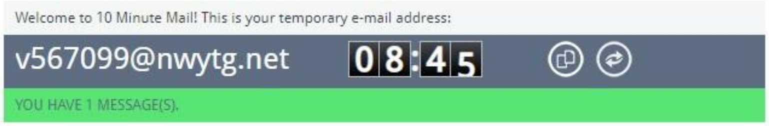
Select domain: ContosoJohnnDoe.b2clogin.com

Access Tokens

Run user flow endpoint: https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.on...

Note: The request made by clicking on “Run user flow” has information that indicates to Azure AD B2C that the application “MyWebApp” wishes to let users sign into Azure AD B2C using the policy “B2C_1_SUSI”, and that when the user successfully signs into Azure AD B2C, the resulting token should be sent to https://jwt.ms. This is similar to the web request that will be made by our web application, except the Reply URL in that request will have the token be sent back to the web app.

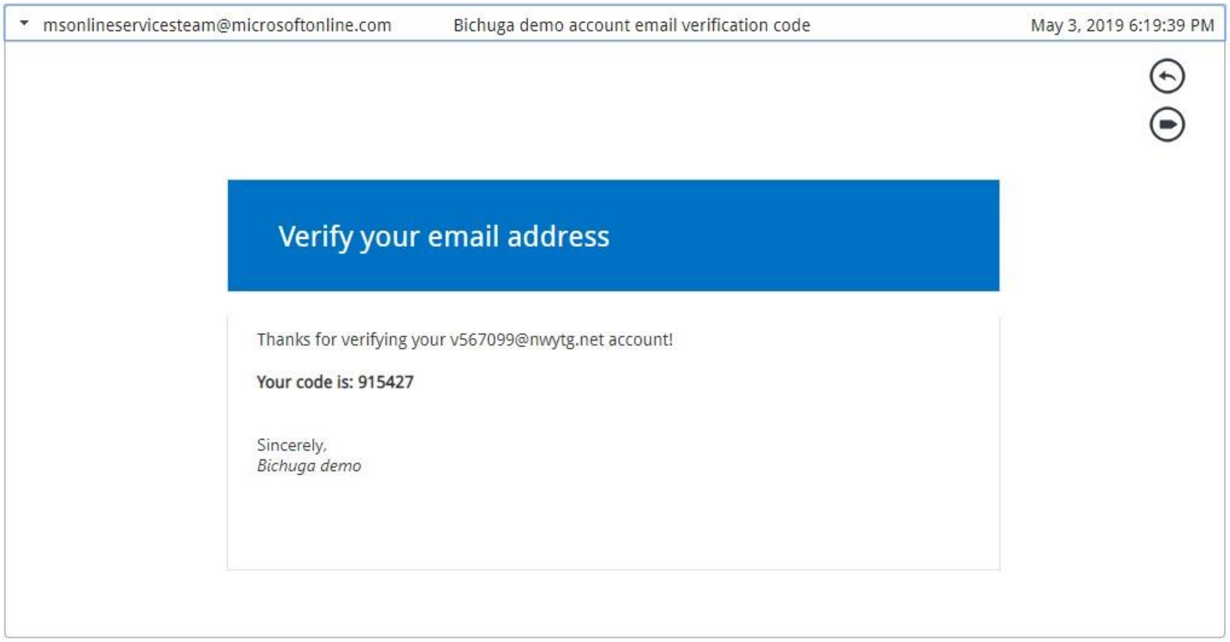
4. In order to test your newly created user experience, you will need a real email address and access to its inbox. To make this task easier, you can use a temporary email service that creates a short-term email/inbox for you. For example, https://10minutemail.com/10MinuteMail/index.html



Welcome to 10 Minute Mail! This is your temporary e-mail address:

v567099@nwytg.net 08:45

YOU HAVE 1 MESSAGE(S).



msonlineservicesteam@microsoftonline.com Bichuga demo account email verification code May 3, 2019 6:19:39 PM

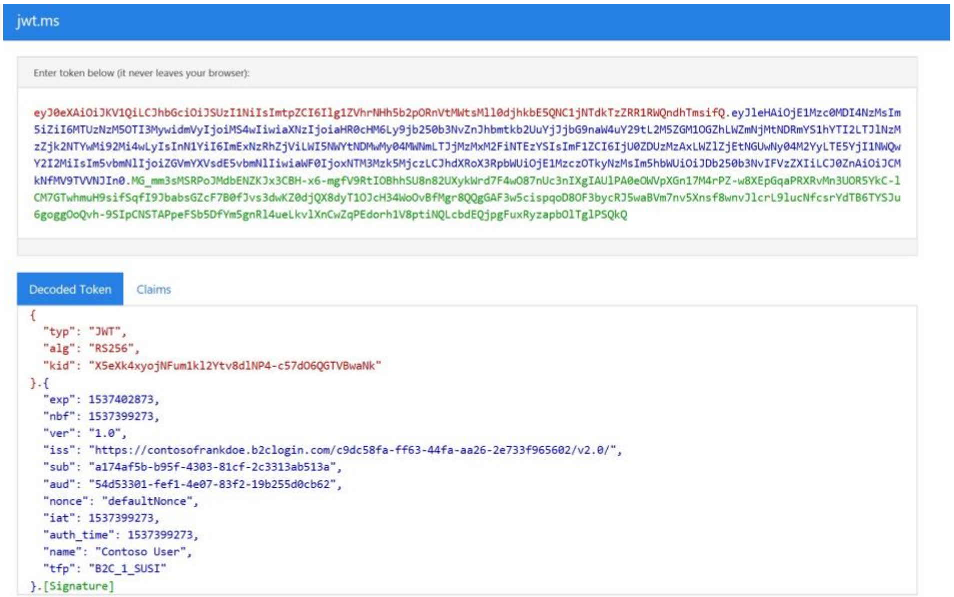
Verify your email address

Thanks for verifying your v567099@nwytg.net account!

Your code is: 915427

Sincerely,
Bichuga demo

5. Go ahead and sign up! Once you've signed up, you will be redirected to https://jwt.ms. This site will decode the Azure AD B2C token for you and show you the claims that are in the token.



Enter token below (it never leaves your browser):

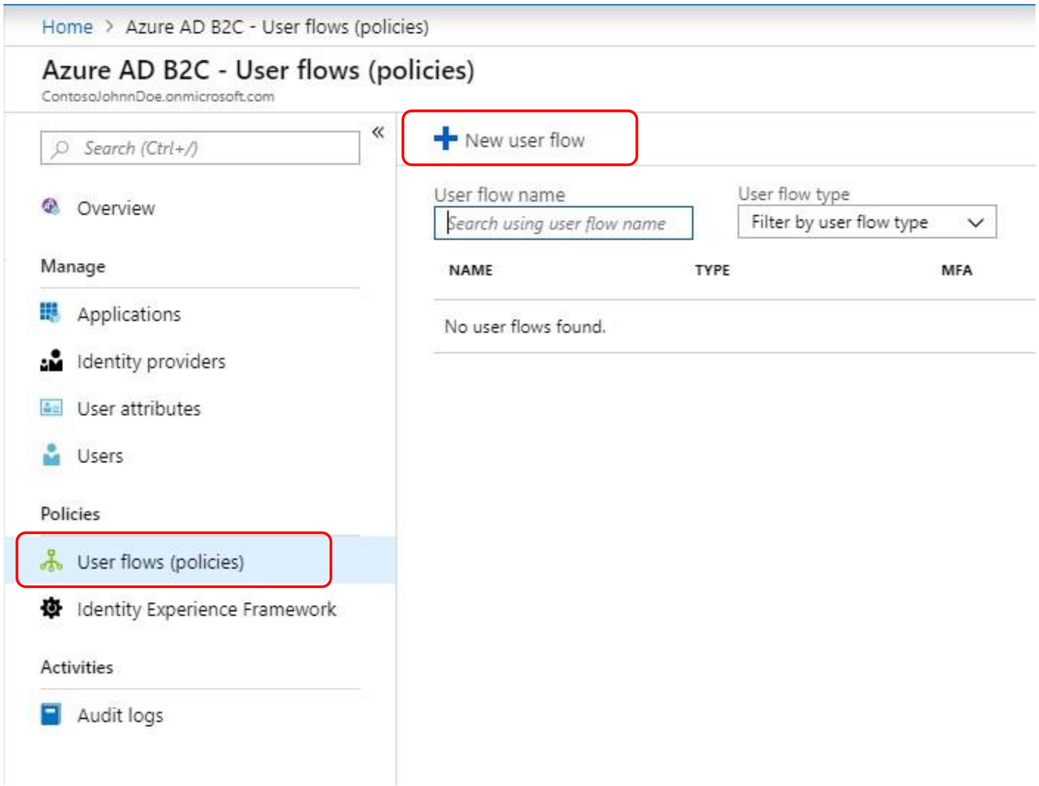
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ilg1ZVhrNHh5b2pORnVtMWtsMll0djhkbE5QNC1jNTdkTzZRR1RWQndhTmsifQ.eyJleHAiOjE1Mzc0MDI4NzMsIm
5iZiI6MTUzNzM5OTI3MywidmVyIjoiMS4wIiwiaXNzIjoiaHR0cHM6Ly9jb250b3NvZnJhbmtkb2UuYjJjbG9naW4uY29tL2M5ZGM1OGZhLWZmNjMtNDRmYS1hYTI2LTJlNzM
zZjk2NTYwMi92Mi4wLyIsInN1YiI6ImExNzRhZjViLWI5NWYtNDMwMy04MWNmLTJjMzMxM2FiNTEzYSIsImF1ZCI6IjU0ZDUzMzAxLWZlZjEtNGUwNy04M2YyLTE5YjI1NWQw
Y2I2MiIsIm5vbmNlIjoiZGVmYXVsdE5vbmNlIiwiaWF0IjoxNTM3Mzk5MjczLCJhdXRoX3RpbWUiOjE1MzczOTkyNzMsIm5hbWUiOiJDb250b3NvIFVzZXIiLCJ0ZnAiOiJCM
kNfMV9TVVNJIn0.MG_mm3sMSRPoJMdbENZKJx3CBH-x6-mgfV9RtIOBhhSU8n82UXykWrd7F4wO87nUc3nIXgIAUlPA0eOWVpXGn17M4rPZ-w8XEpGqaPRXRvMn3UOR5YkC-l
CM7GTwhmuH9sifSqfI9JbabsGZcF7B0fJvs3dwKZ0djQX8dyT1OJcH34WoOvBfMgr8QQgGAF3w5cispqoD8OF3bycRJ5waBVm7nv5Xnsf8wnvJlcrL9lucNfcsrYdTB6TYSJu
6goggOoQvh-9SIpCNSTAPpeFSb5DfYm5gnRl4ueLkvlXnCwZqPEdorh1V8ptiNQLcbdEQjpgFuxRyzapbOlTglPSQkQ
```

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "X5eXk4xyojNFum1kl2Ytv8dlNP4-c57dO6QGTVBwaNk"
}.{
  "exp": 1537402873,
  "nbf": 1537399273,
  "ver": "1.0",
  "iss": "https://contosofrankdoe.b2clogin.com/c9dc58fa-ff63-44fa-aa26-2e733f965602/v2.0/",
  "sub": "a174af5b-b95f-4303-81cf-2c3313ab513a",
  "aud": "54d53301-fef1-4e07-83f2-19b255d0cb62",
  "nonce": "defaultNonce",
  "iat": 1537399273,
  "auth_time": 1537399273,
  "name": "Contoso User",
  "tfp": "B2C_1_SUSI"
}.[Signature]
```

Task 5: Create your password reset policy

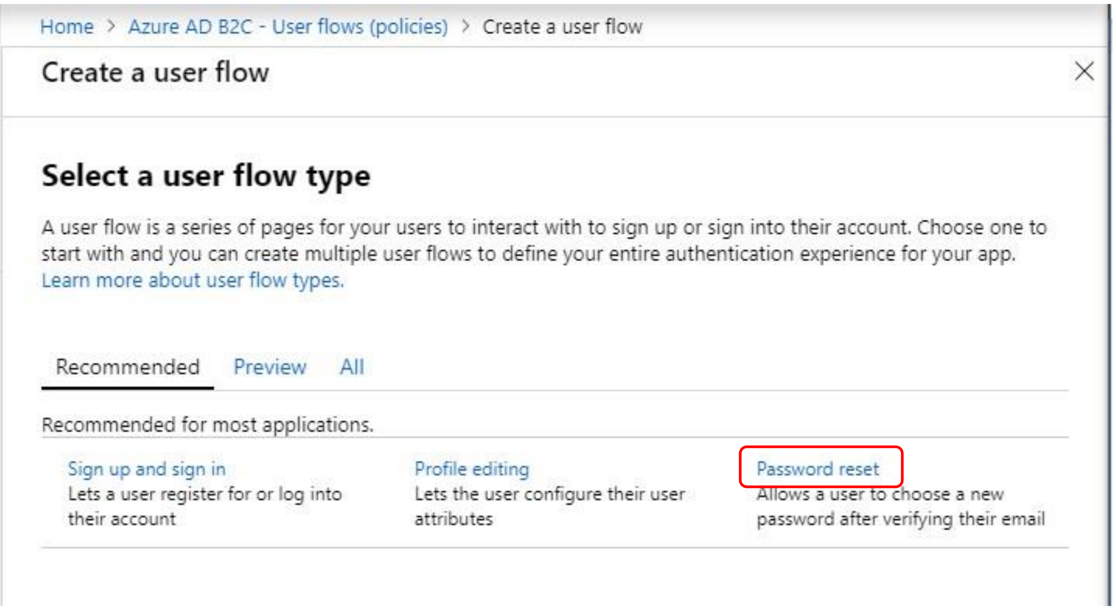
Like the sign-up or sign-in policy that you created, you will need to create a password reset policy as well to give your users the ability to reset their passwords.

1. Return to the **Overview** page of Azure AD B2C and click on **User flows (policies)**. Click **New user flow.**



No user flows found.

2. Select **Password reset**.



A user flow is a series of pages for your users to interact with to sign up or sign into their account. Choose one to start with and you can create multiple user flows to define your entire authentication experience for your app.

Recommended for most applications.

Sign up and sign in: Lets a user register for or log into their account

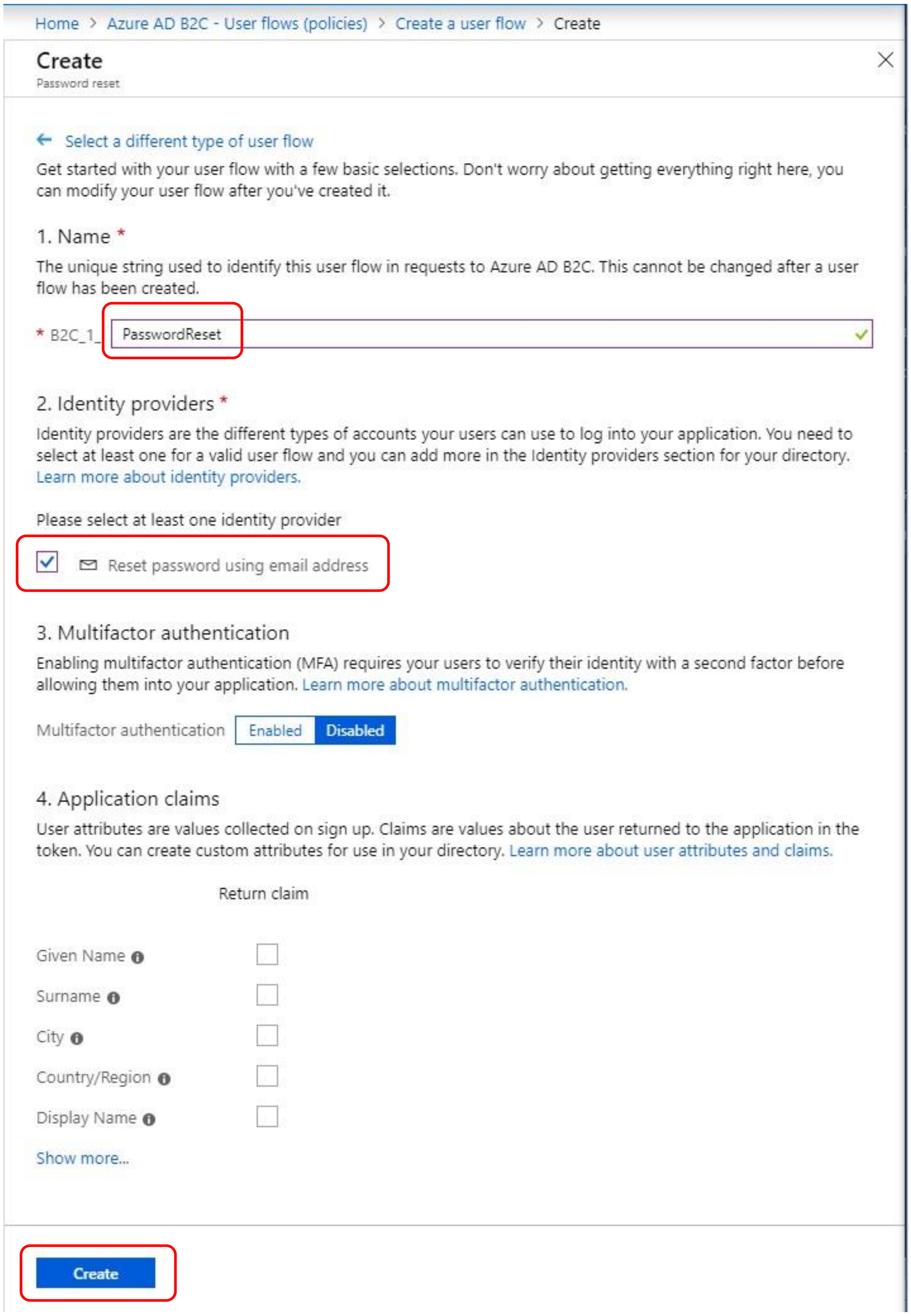
Profile editing: Lets the user configure their user attributes

Password reset: Allows a user to choose a new password after verifying their email

3. In step number 1, enter **"PasswordReset"** as the **Name** for the password reset policy. (Once created, your policy name will be automatically prefixed with "B2C_1_" to become "B2C_1_PasswordReset)

4. In step number 2, from the **Identity providers** tab check **Reset password using email address**.

5. Ignore step 3 and 4 for now. Click **Create** to create the password reset policy.



Home > Azure AD B2C - User flows (policies) > Create a user flow > Create

Create

Password reset

← Select a different type of user flow

Get started with your user flow with a few basic selections. Don't worry about getting everything right here, you can modify your user flow after you've created it.

1. Name *

The unique string used to identify this user flow in requests to Azure AD B2C. This cannot be changed after a user flow has been created.

* B2C_1_ PasswordReset ✓

2. Identity providers *

Identity providers are the different types of accounts your users can use to log into your application. You need to select at least one for a valid user flow and you can add more in the Identity providers section for your directory. Learn more about identity providers.

Please select at least one identity provider

☑ ✉ Reset password using email address

3. Multifactor authentication

Enabling multifactor authentication (MFA) requires your users to verify their identity with a second factor before allowing them into your application. Learn more about multifactor authentication.

Multifactor authentication Enabled [✓ Disabled]

4. Application claims

User attributes are values collected on sign up. Claims are values about the user returned to the application in the token. You can create custom attributes for use in your directory. Learn more about user attributes and claims.

	Return claim
Given Name	□
Surname	□
City	□
Country/Region	□
Display Name	□

Show more...

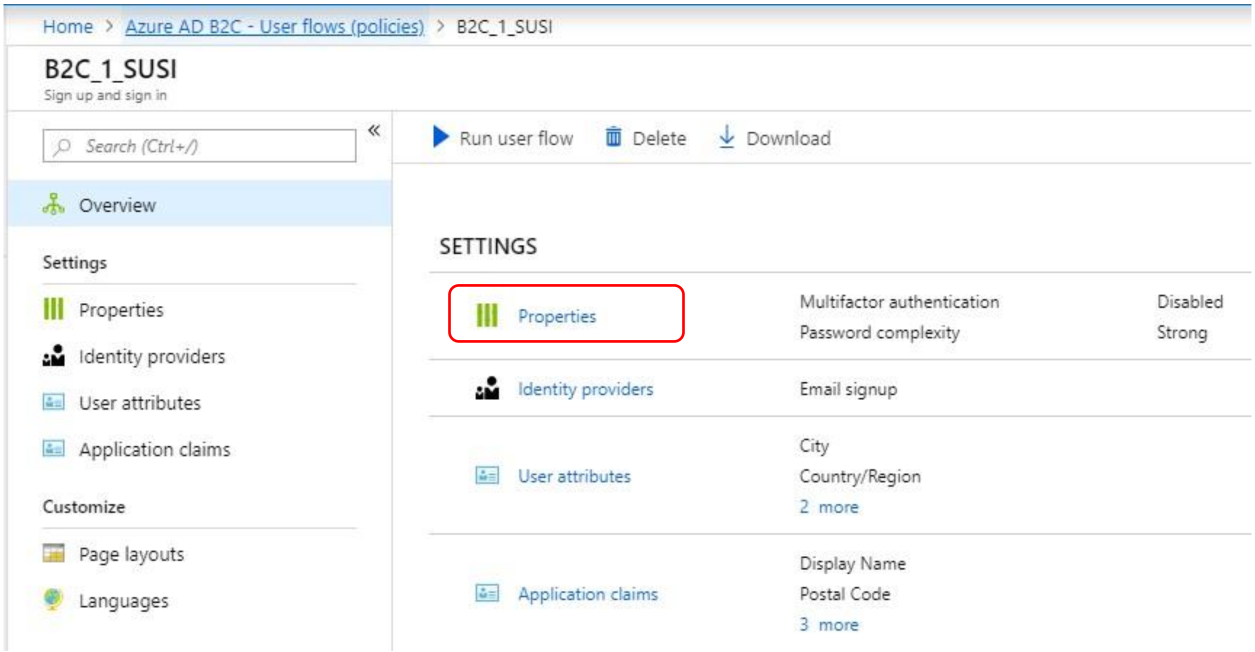
6. Test out the new policy by repeating Task 4 (use the newly recreated password reset policy instead of the sign-up or sign-in policy).

Now that you have a basic setup, let’s work on customizing the user experience a bit more. The next set of tasks will show you how to enable multifactor authentication (MFA), display experiences in multiple languages, and add your own branding. Although the following set of tasks are independent from each other, we recommend going in order.

Task 6: Enable multifactor authentication (MFA)

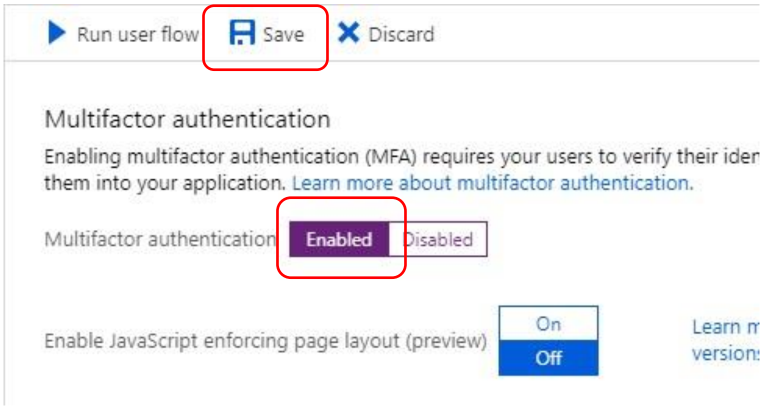
Suppose your new application displays sensitive information to your users, such as their account balance. You need additional security and so let's enable MFA.

1. Open the sign-up or sign-in policy that you created (e.g. B2C_1_SUSI)
2. Click on **Properties**.



Properties	Multifactor authentication Password complexity	Disabled Strong
Identity providers	Email signup	
User attributes	City Country/Region 2 more	
Application claims	Display Name Postal Code 3 more	

3. On the Multifactor authentication section, switch it to **Enabled** and click **Save**.



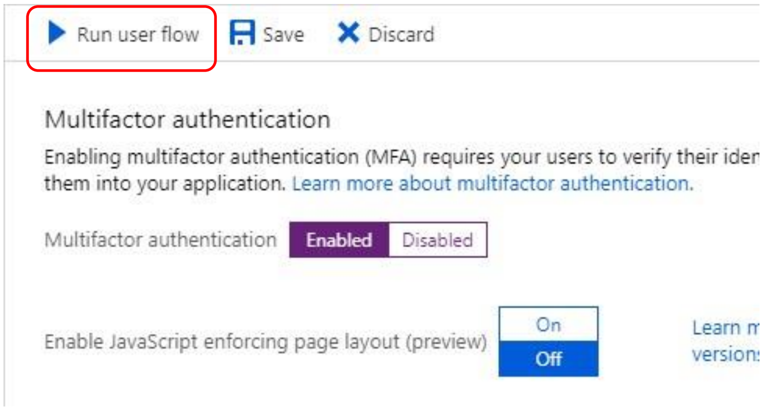
Multifactor authentication

Enabling multifactor authentication (MFA) requires your users to verify their ider
them into your application. Learn more about multifactor authentication.

Multifactor authentication [✓ Enabled] Disabled

Enable JavaScript enforcing page layout (preview) On [✓ Off]

4. Try out the new settings by clicking on **Run user flow** and going through a sign in or sign up experience.



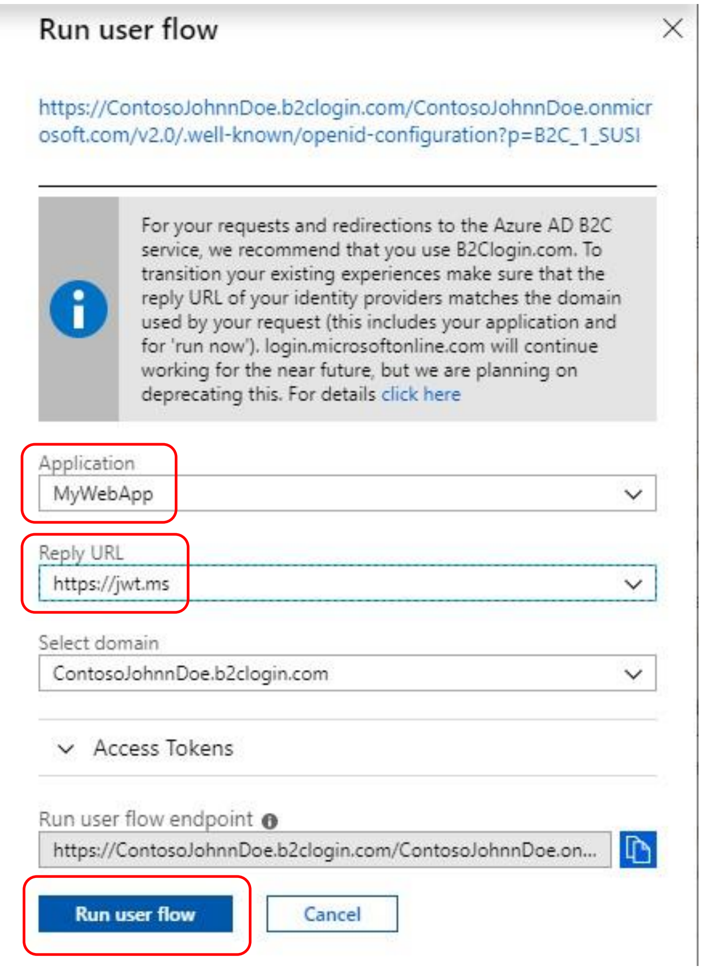
Multifactor authentication

Enabling multifactor authentication (MFA) requires your users to verify their ider
them into your application. Learn more about multifactor authentication.

Multifactor authentication: Enabled | Disabled

Enable JavaScript enforcing page layout (preview): On | Off

Ensure that the **reply URL** is set to https://jwt.ms. Click on **Run user flow**.



Run user flow

https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.onmicrosoft.com/v2.0/.well-known/openid-configuration?p=B2C_1_SUSI

For your requests and redirections to the Azure AD B2C service, we recommend that you use B2Clogin.com. To transition your existing experiences make sure that the reply URL of your identity providers matches the domain used by your request (this includes your application and for 'run now'). login.microsoftonline.com will continue working for the near future, but we are planning on deprecating this. For details click here

Application: MyWebApp

Reply URL: https://jwt.ms

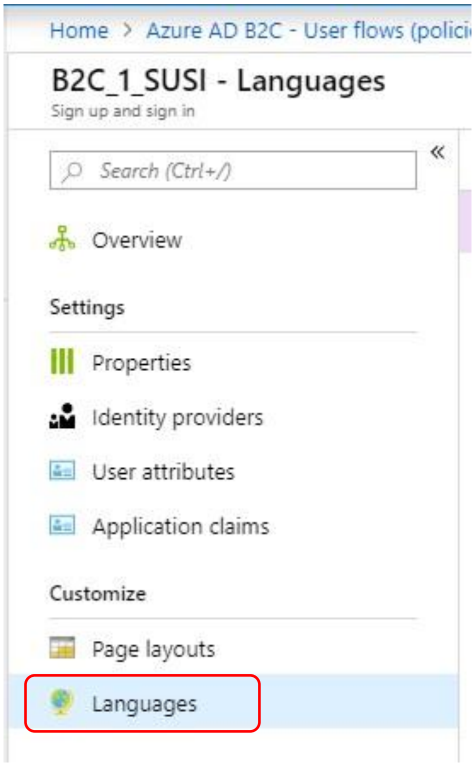
Select domain: ContosoJohnnDoe.b2clogin.com

Run user flow endpoint: https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.on...

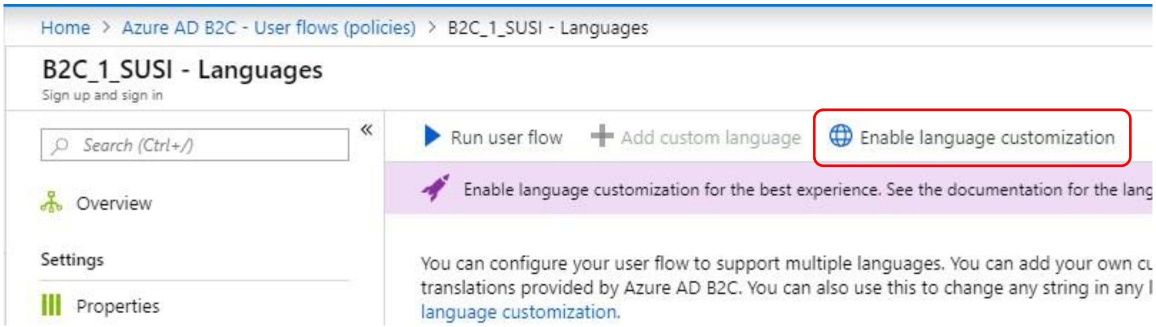
Task 7: Provide sign-in experiences in 37 different languages

Suppose your new application will have users around the world, some who may not use English as the primary language. Azure AD B2C provides sign-in experiences that can be localized up to 36 different languages. This task will show you how you can modify the sign-in request to show the experience in Spanish and French.

1. Open the sign-up or sign-in policy that you created (e.g. B2C_1_SUSI)
2. Click on **Languages**.



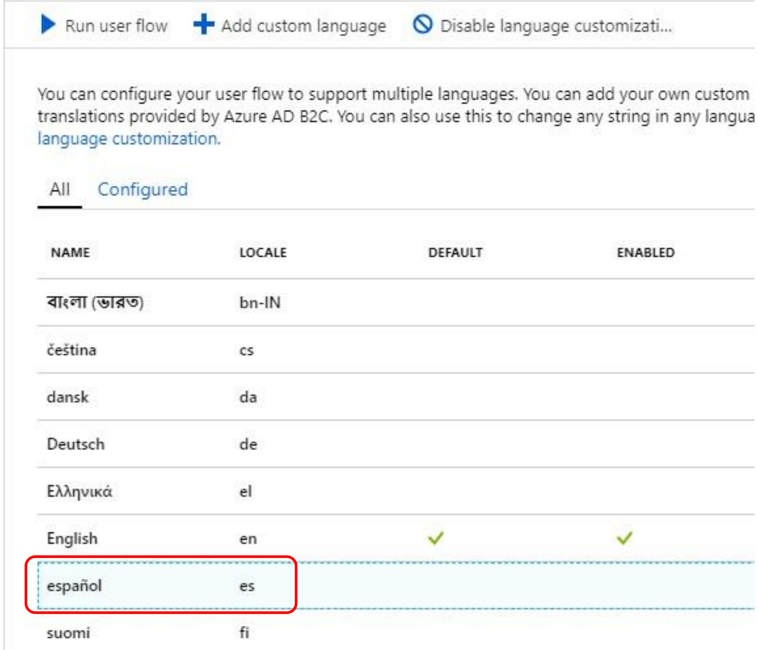
3. Click **Enable language customization**.



Enable language customization for the best experience. See the documentation for the lang

You can configure your user flow to support multiple languages. You can add your own cu translations provided by Azure AD B2C. You can also use this to change any string in any l language customization.

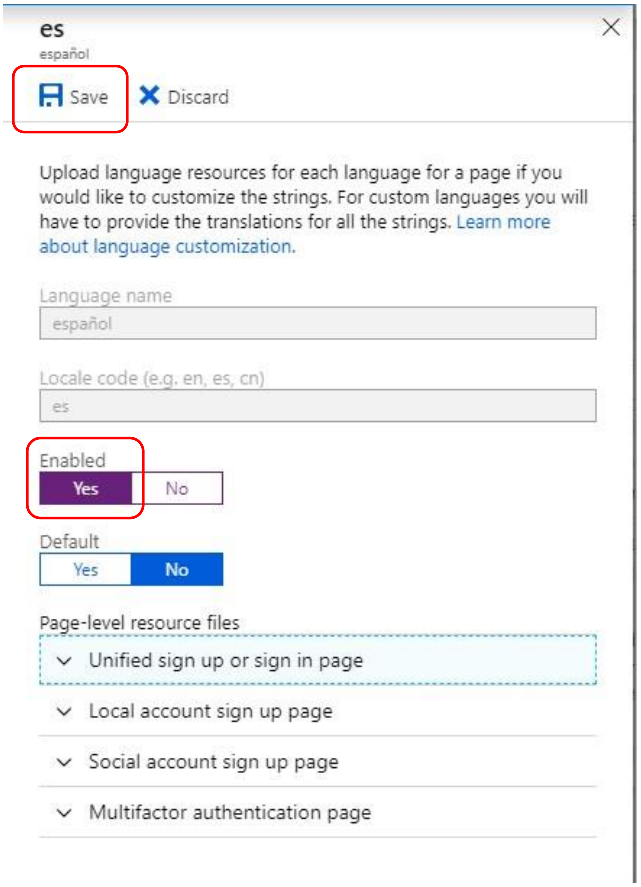
4. Click **español**.



You can configure your user flow to support multiple languages. You can add your own custom translations provided by Azure AD B2C. You can also use this to change any string in any langua language customization.

NAME	LOCALE	DEFAULT	ENABLED
বাংলা (ভারত)	bn-IN		
čeština	cs		
dansk	da		
Deutsch	de		
Ελληνικά	el		
English	en	✓	✓
español	es		
suomi	fi		

5. Switch Enabled to **Yes** and **Save**.



Upload language resources for each language for a page if you would like to customize the strings. For custom languages you will have to provide the translations for all the strings. Learn more about language customization.

Language name: español

Locale code (e.g. en, es, cn): es

Enabled: [✓ Yes] No

Default: Yes [✓ No]

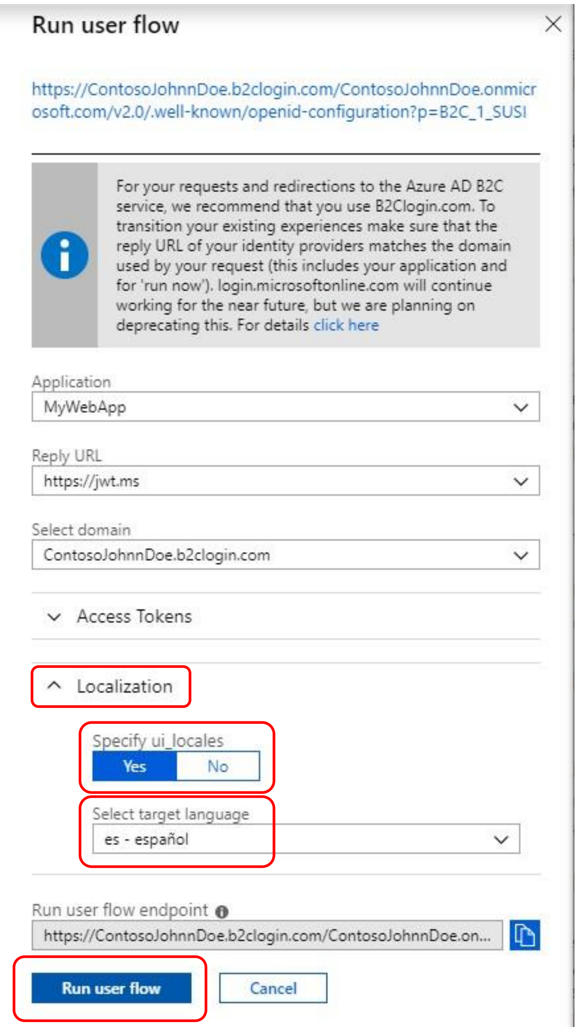
Page-level resource files

- Unified sign up or sign in page
- Local account sign up page
- Social account sign up page
- Multifactor authentication page

6. Now try your new language. Select **Run user flow**.

7. Click **Localization** and switch Specify ui_locales to **Yes** and select **es – español** from the dropdown menu.

   Ensure that the **reply URL** is set to https://jwt.ms. Click on **Run user flow**.



Run user flow

https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.onmicrosoft.com/v2.0/.well-known/openid-configuration?p=B2C_1_SUSI

For your requests and redirections to the Azure AD B2C service, we recommend that you use B2Clogin.com. To transition your existing experiences make sure that the reply URL of your identity providers matches the domain used by your request (this includes your application and for 'run now'). login.microsoftonline.com will continue working for the near future, but we are planning on deprecating this. For details click here

Application: MyWebApp

Reply URL: https://jwt.ms

Select domain: ContosoJohnnDoe.b2clogin.com

Access Tokens

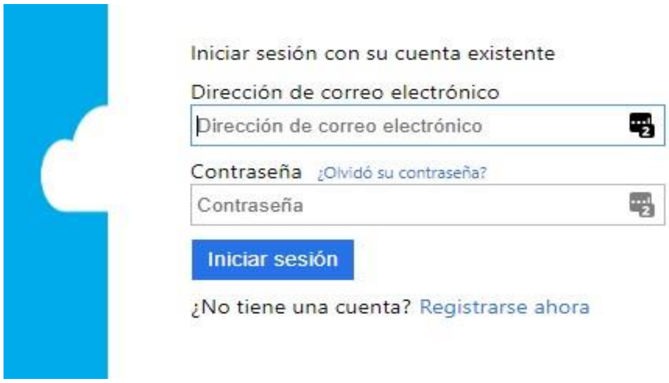
Localization

Specify ui_locales: Yes | No

Select target language: es - español

Run user flow endpoint: https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.on...

A new tab will open, and you should now see the sign-up and sign-in experiences in Spanish.



Iniciar sesión con su cuenta existente

Dirección de correo electrónico

Dirección de correo electrónico

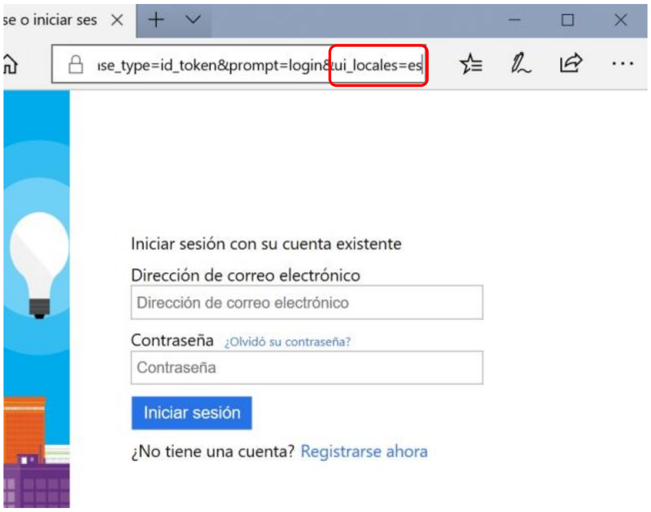
Contraseña ¿Olvidó su contraseña?

Contraseña

¿No tiene una cuenta? Registrarse ahora

Nice! Now let’s change the experience to French.

8. In the URL of the sign in page that just opened, scroll to the end and find the parameter **ui_locales=es**.



se o iniciar ses

ıse_type=id_token&prompt=login&ui_locales=es

Iniciar sesión con su cuenta existente

Dirección de correo electrónico

Dirección de correo electrónico

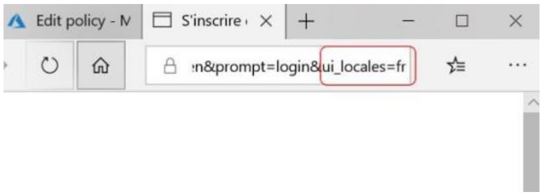
Contraseña ¿Olvidó su contraseña?

Contraseña

Iniciar sesión

¿No tiene una cuenta? Registrarse ahora

9. Change the parameter to **ui_locales=fr** and hit enter to load the new URL.



ın&prompt=login&ui_locales=fr

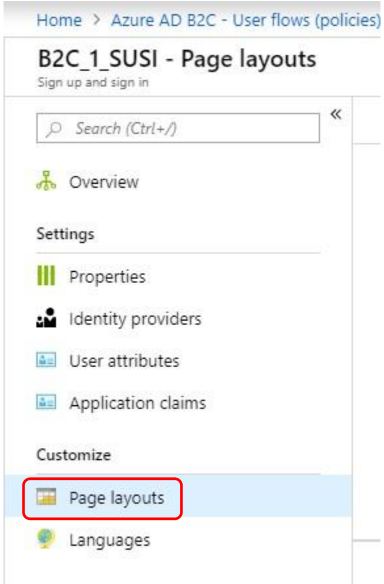
You should now see the sign-up and sign-in experiences in French.

The ui_locales parameter controls which language the sign in experience renders in. To try out any one of the other 36 different languages, just enter the corresponding code. You can find the full list of codes in the **Supported Languages** section here.

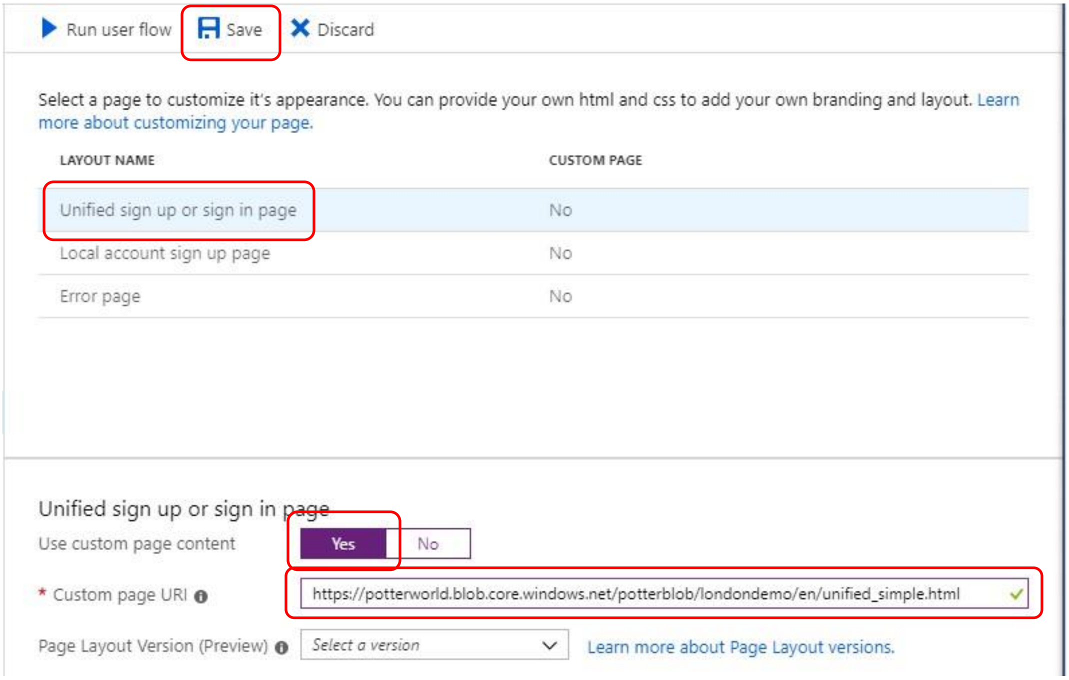
Task 8: Add branding to your sign-in experience

As the developer for a customer-facing application, you want to ensure that your sign in experience doesn't look different than the rest of your application. Specifically, it needs to maintain your brand. In this task, you will customize your sign-in experience to add a branded template. 1. Open the sign-up or sign-in policy that you created (e.g. B2C_1_SUSI)

2. Click on **Page layouts**.



3. If not already selected, select **Unified sign-up or sign-in page**.
   Switch "Use custom page content" to **Yes**. Then, enter the following URL for the **Custom page URI**. https://potterworld.blob.core.windows.net/potterblob/londondemo/en/unified_simple.html



Select a page to customize it's appearance. You can provide your own html and css to add your own branding and layout. Learn more about customizing your page.

LAYOUT NAME	CUSTOM PAGE
Unified sign up or sign in page	No
Local account sign up page	No
Error page	No

Unified sign up or sign in page

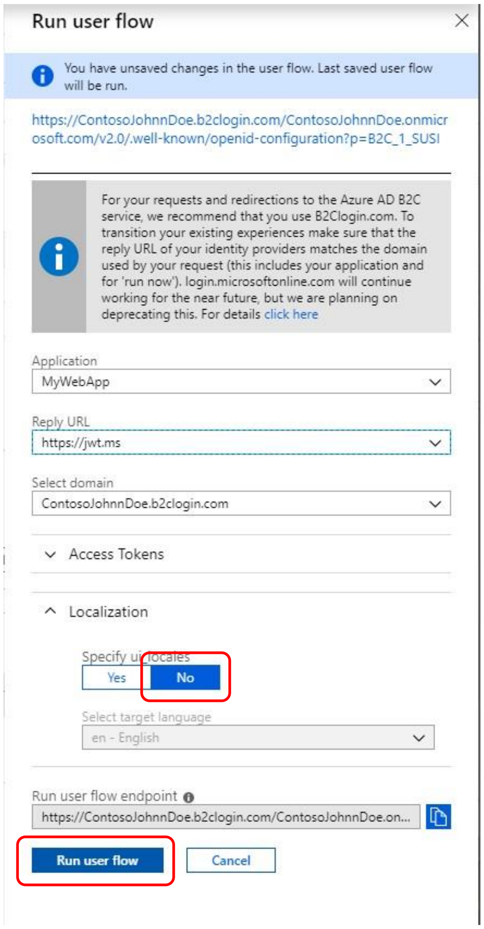
Use custom page content: [✓ Yes] No

* Custom page URI: https://potterworld.blob.core.windows.net/potterblob/londondemo/en/unified_simple.html ✓

Page Layout Version (Preview): Select a version

Learn more about Page Layout versions.

4. **Save** your policy and click on **Run now.**
   Note: Since the provided template has English strings hardcoded into the HTML, we recommend switching off **Localization**.



Run user flow

You have unsaved changes in the user flow. Last saved user flow will be run.

https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.onmicrosoft.com/v2.0/.well-known/openid-configuration?p=B2C_1_SUSI

For your requests and redirections to the Azure AD B2C service, we recommend that you use B2Clogin.com. To transition your existing experiences make sure that the reply URL of your identity providers matches the domain used by your request (this includes your application and for 'run now'). login.microsoftonline.com will continue working for the near future, but we are planning on deprecating this. For details click here

Application: MyWebApp

Reply URL: https://jwt.ms

Select domain: ContosoJohnnDoe.b2clogin.com

Access Tokens

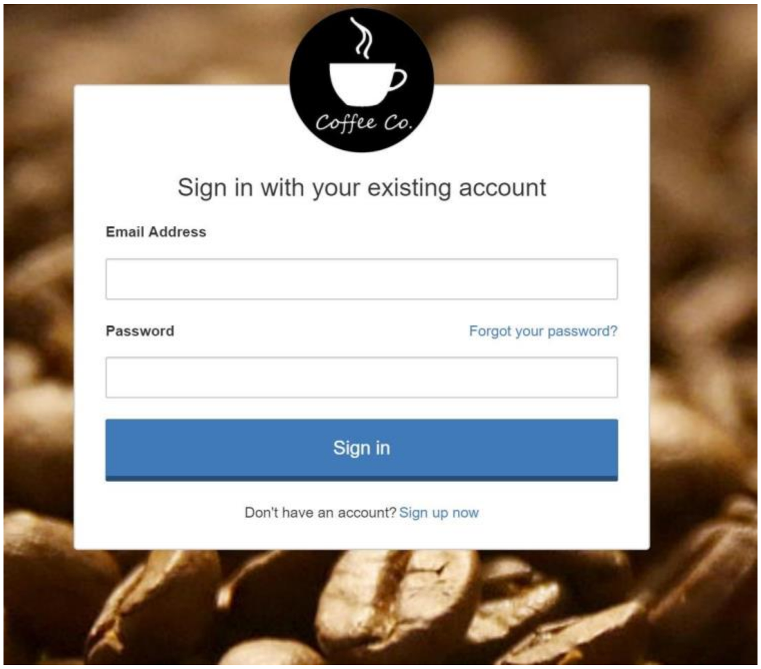
Localization

Specify ui locales: Yes [✓ No]

Select target language: en - English

Run user flow endpoint: https://ContosoJohnnDoe.b2clogin.com/ContosoJohnnDoe.on...

You should now see your sign-in experience branded.



Sign in with your existing account

Email Address

Password

Forgot your password?

Don't have an account? Sign up now

How UI customization works

Azure AD B2C brands the sign-in experiences by taking your HTML and CSS files (this is the link that you provided) and injecting the sign-in elements into a pre-specified location (an empty <div id="api"></div> element somewhere in the <body>). You can inspect the source code of the URL above to find the <div> element. Azure AD B2C pulls the HTML and CSS files from the link, inserts the necessary fields (such as the email and password fields), and presents the final UI to the user.

Lab Summary

Congratulations on completing this lab! You've learned how to use Azure AD B2C to add rich, secure & scalable customer sign-up & sign-in experiences to your web app.

Additional Tasks

- Add a Facebook identity provider
- Add an Azure AD identity provider https://docs.microsoft.com/en-us/azure/active-directory-b2c/tutorial-add-identity-providers •
- Customize the complexity of the password

Resources

If you are interested in learning more about Azure AD B2C, you can refer to the following resources:

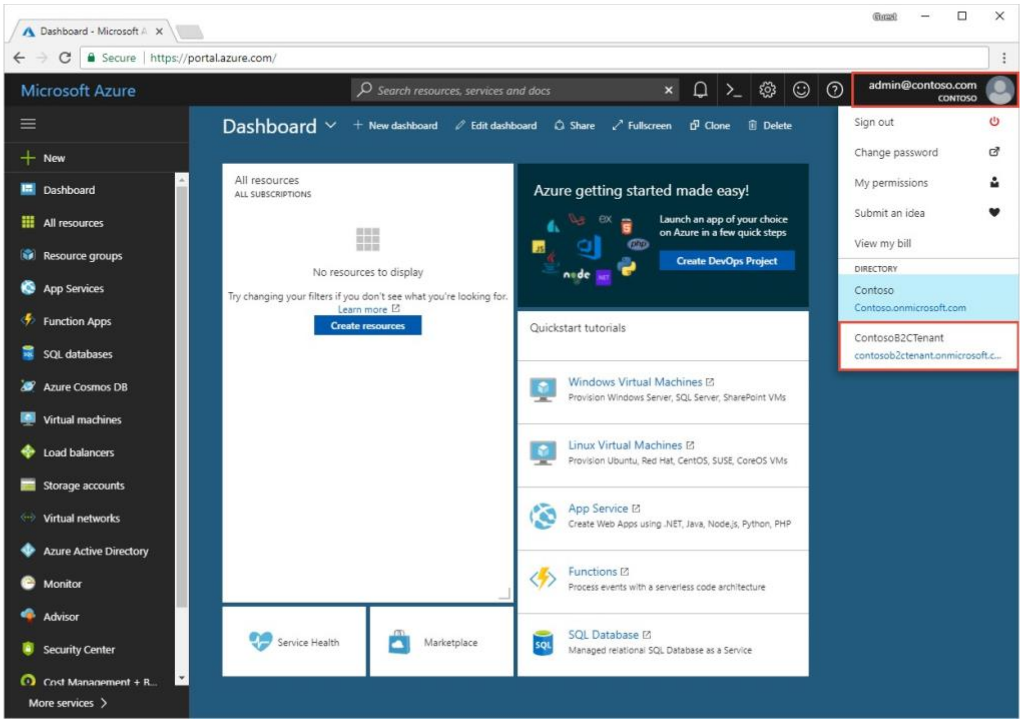
Documentation: http://aka.ms/aadb2c

Samples: http://aka.ms/aadb2csamples

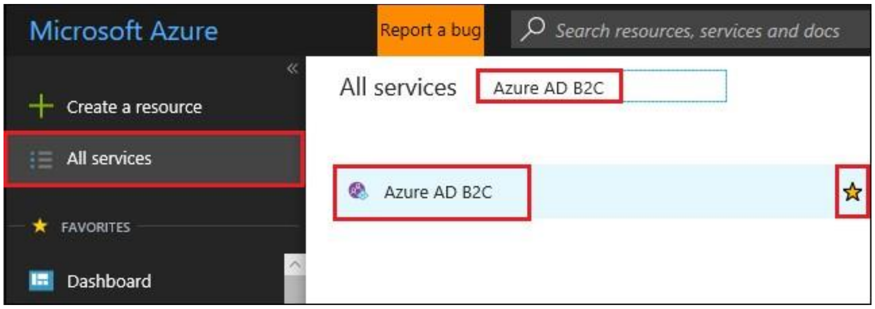
Appendix

Navigating to the Azure AD B2C settings

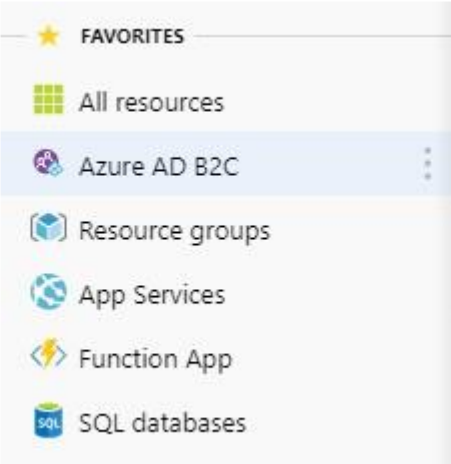
Select the Azure AD B2C directory in the top-right corner of the portal.



If Azure AD B2C isn't in the services list, expand **All services** in the navigation bar at the top-left side of the portal. Search for **Azure AD B2C** and select **Azure AD B2C** in the result list. You can also select the **star icon** to add Azure AD B2C it your favorite services list.



If you have already added AAD B2C to your favorite services list, then click on the Azure AD B2C blade on the left side menu, under favorites.



You can also access the blade by entering **Azure AD B2C** in **Search** resources at the top of the portal. In the results list, select **Azure AD B2C** to access the Azure AD B2C settings blade.