**Tutorial: Create an Azure Active Directory B2C tenant**

Before your applications can interact with Azure Active Directory B2C (Azure AD B2C), they must be registered in a tenant that you manage.

In this article, you learn how to:

* Create an Azure AD B2C tenant
* Link your tenant to your subscription
* Switch to the directory containing your Azure AD B2C tenant
* Add the Azure AD B2C resource as a **Favorite** in the Azure portal

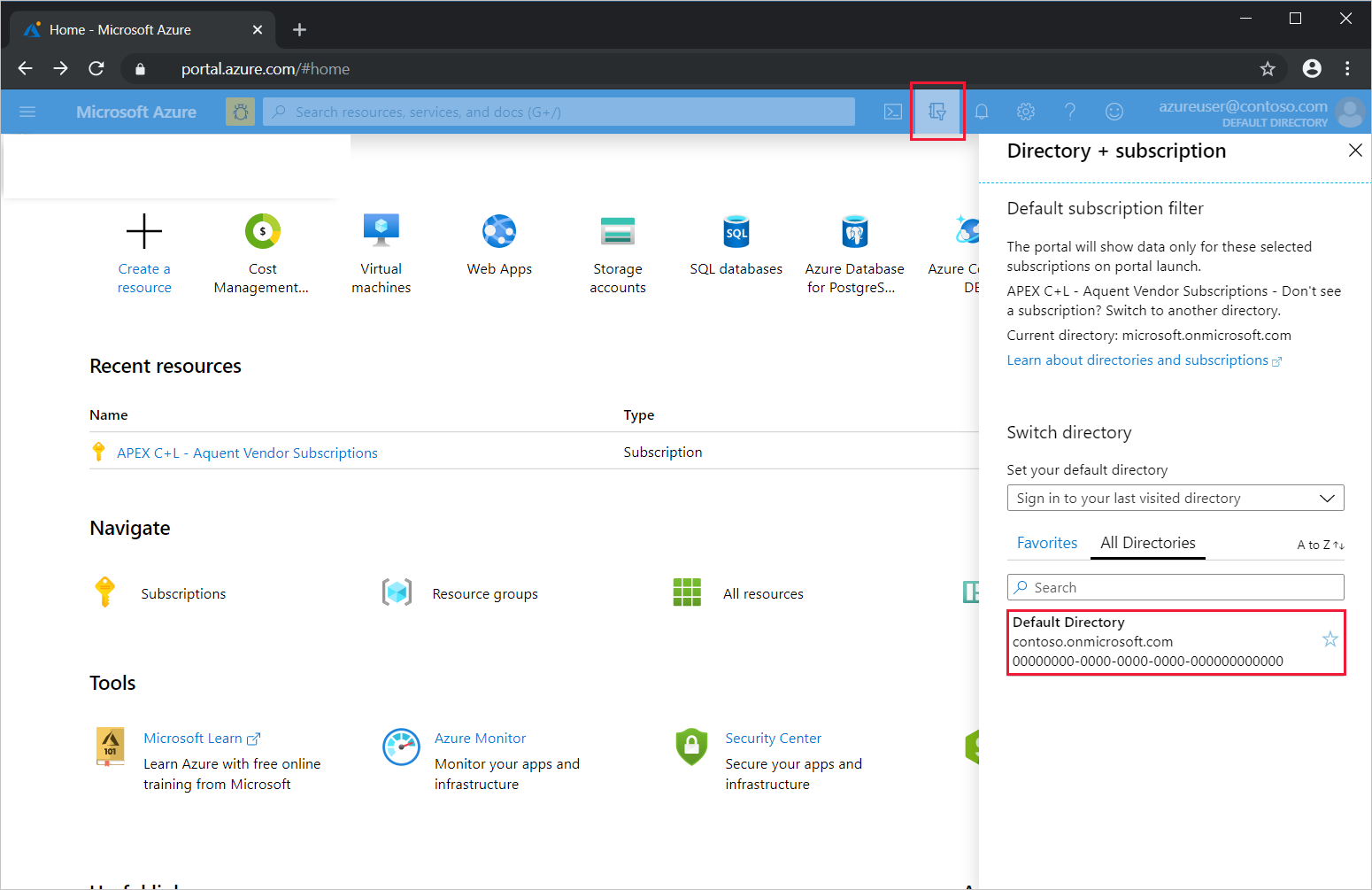
You learn how to register an application in the next tutorial.

If you don't have an Azure subscription, create a free account before you begin.

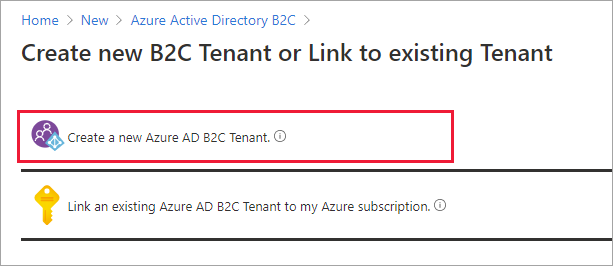
## Create an Azure AD B2C tenant

1. Sign in to the [Azure portal](https://portal.azure.com/). Sign in with an Azure account that's been assigned at least the Contributor role within the subscription or a resource group within the subscription.
2. Select the directory that contains your subscription.

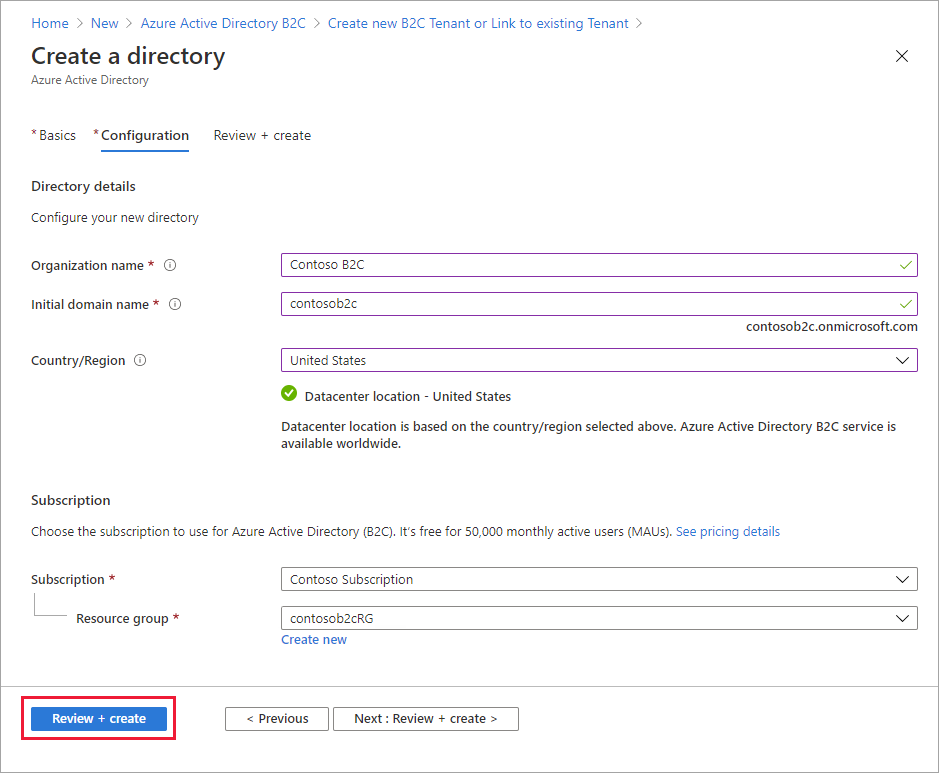
In the Azure portal toolbar, select the **Directory + Subscription** icon, and then select the directory that contains your subscription. This directory is different from the one that will contain your Azure AD B2C tenant.



1. On the Azure portal menu or from the **Home** page, select **Create a resource**.
2. Search for **Azure Active Directory B2C**, and then select **Create**.
3. Select **Create a new Azure AD B2C Tenant**.



1. On the **Create a directory** page, enter the following:
   * **Organization name** - Enter a name for your Azure AD B2C tenant.
   * **Initial domain name** - Enter a domain name for your Azure AD B2C tenant.
   * **Country or region** - Select your country or region from the list. This selection can't be changed later.
   * **Subscription** - Select your subscription from the list.
   * **Resource group** - Select a resource group that will contain the tenant. Or select **Create new**, enter a **Name** for the resource group, select the **Resource group location**, and then select **OK**.



1. Select **Review + create**.
2. Review your directory settings. Then select **Create**.

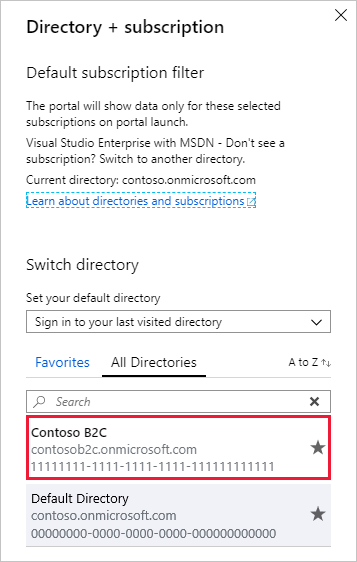
You can link multiple Azure AD B2C tenants to a single Azure subscription for billing purposes. To link a tenant, you must be an admin in the Azure AD B2C tenant and be assigned at least a Contributor role within the Azure subscription.

## Select your B2C tenant directory

To start using your new Azure AD B2C tenant, you need to switch to the directory that contains the tenant.

Select the **Directory + subscription** filter in the top menu of the Azure portal, then select the directory that contains your Azure AD B2C tenant.

If at first you don't see your new Azure B2C tenant in the list, refresh your browser window, then select the **Directory + subscription** filter again in the top menu.



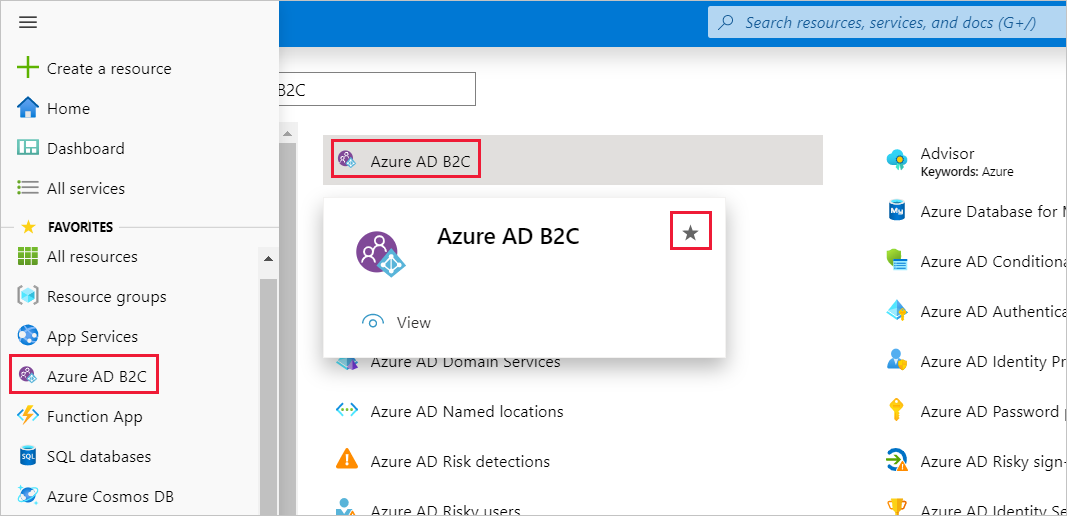
## Add Azure AD B2C as a favorite (optional)

This optional step makes it easier to select your Azure AD B2C tenant in the following and all subsequent tutorials.

Instead of searching for Azure AD B2C in **All services** every time you want to work with your tenant, you can instead favorite the resource. Then, you can select it from the portal menu's **Favorites** section to quickly browse to your Azure AD B2C tenant.

You only need to perform this operation once. Before performing these steps, make sure you've switched to the directory containing your Azure AD B2C tenant as described in the previous section, Select your B2C tenant directory.

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal menu, select **All services**.
3. In the **All services** search box, search for **Azure AD B2C**, hover over the search result, and then select the star icon in the tooltip. **Azure AD B2C** now appears in the Azure portal under **Favorites**.
4. If you want to change the position of your new favorite, go to the Azure portal menu, select **Azure AD B2C**, and then drag it up or down to the desired position.



# Tutorial: Register a web application in Azure Active Directory B2C

Before your applications can interact with Azure Active Directory B2C (Azure AD B2C), they must be registered in a tenant that you manage. This tutorial shows you how to register a web application using the Azure portal.

In this article, you learn how to:

* Register a web application
* Create a client secret

If you don't have an Azure subscription, create a free account before you begin.

## Prerequisites

If you haven't already created your own Azure AD B2C Tenant, create one now. You can use an existing Azure AD B2C tenant.

## Register a web application

* App registrations

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Select the **Directory + Subscription** icon in the portal toolbar, and then select the directory that contains your Azure AD B2C tenant.
3. In the Azure portal, search for and select **Azure AD B2C**.
4. Select **App registrations**, and then select **New registration**.
5. Enter a **Name** for the application. For example, webapp1.
6. Under **Supported account types**, select **Accounts in any organizational directory or any identity provider. For authenticating users with Azure AD B2C**.
7. Under **Redirect URI**, select **Web**, and then enter https://jwt.ms in the URL text box.

The redirect URI is the endpoint to which the user is sent by the authorization server (Azure AD B2C, in this case) after completing its interaction with the user, and to which an access token or authorization code is sent upon successful authorization. In a production application, it's typically a publicly accessible endpoint where your app is running, like https://contoso.com/auth-response. For testing purposes like this tutorial, you can set it to https://jwt.ms, a Microsoft-owned web application that displays the decoded contents of a token (the contents of the token never leave your browser). During app development, you might add the endpoint where your application listens locally, like https://localhost:5000. You can add and modify redirect URIs in your registered applications at any time.

The following restrictions apply to redirect URIs:

* + The reply URL must begin with the scheme https.
  + The reply URL is case-sensitive. Its case must match the case of the URL path of your running application. For example, if your application includes as part of its path .../abc/response-oidc, do not specify .../ABC/response-oidc in the reply URL. Because the web browser treats paths as case-sensitive, cookies associated with .../abc/response-oidc may be excluded if redirected to the case-mismatched .../ABC/response-oidc URL.

1. Under **Permissions**, select the Grant admin consent to openid and offline\_access permissions check box.
2. Select **Register**.

Once the application registration is complete, enable the implicit grant flow:

1. Under **Manage**, select **Authentication**.
2. Under **Implicit grant**, select both the **Access tokens** and **ID tokens** check boxes.
3. Select **Save**.

## Create a client secret

If your application exchanges an authorization code for an access token, you need to create an application secret.

1. In the **Azure AD B2C - App registrations** page, select the application you created, for example webapp1.
2. Under **Manage**, select **Certificates & secrets**.
3. Select **New client secret**.
4. Enter a description for the client secret in the **Description** box. For example, clientsecret1.
5. Under **Expires**, select a duration for which the secret is valid, and then select **Add**.
6. Record the secret's **Value**. You use this value as the application secret in your application's code.

# Tutorial: Create user flows in Azure Active Directory B2C

In your applications you may have user flows that enable users to sign up, sign in, or manage their profile. You can create multiple user flows of different types in your Azure Active Directory B2C (Azure AD B2C) tenant and use them in your applications as needed. User flows can be reused across applications.

In this article, you learn how to:

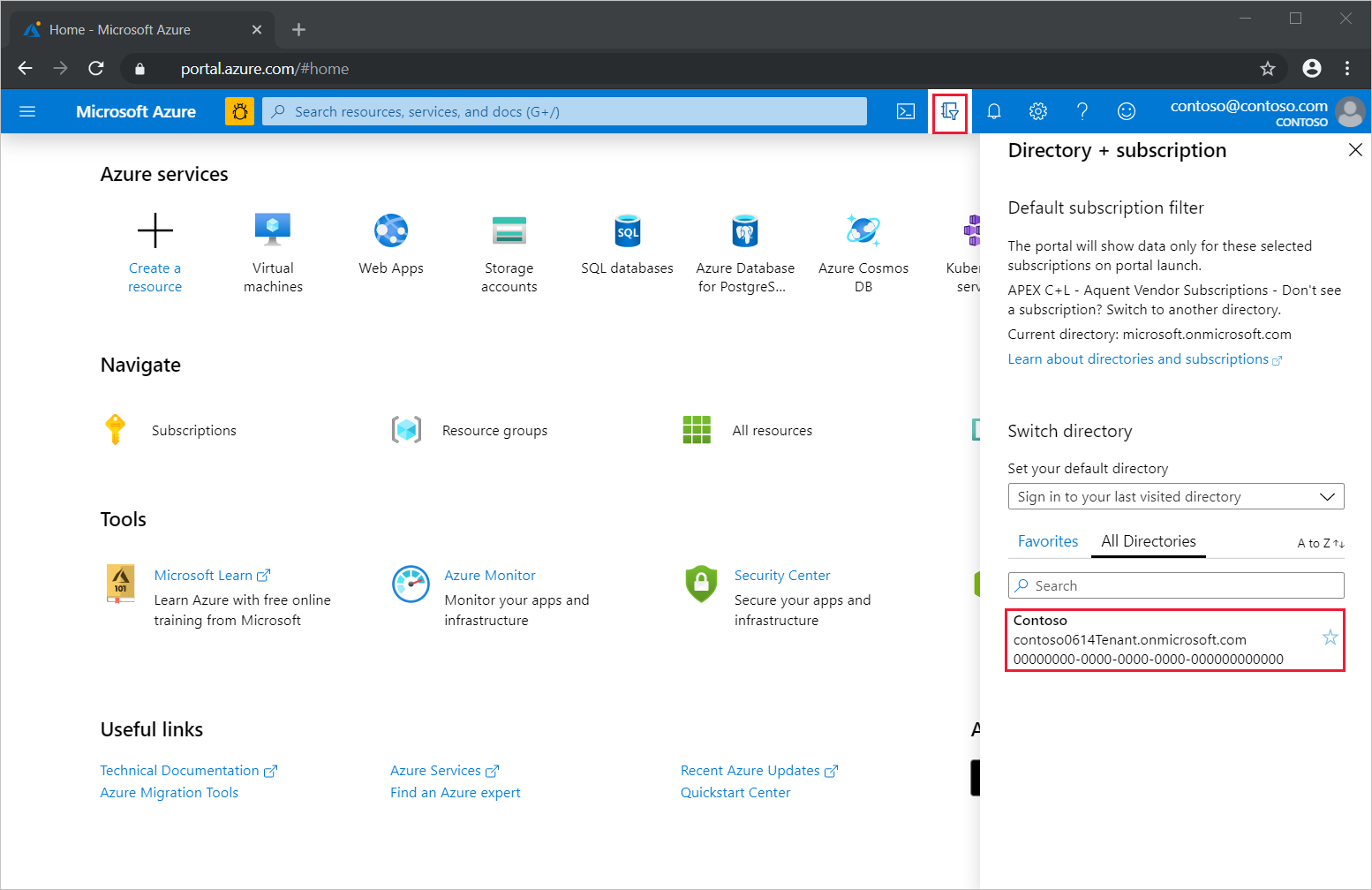
* Create a sign-up and sign-in user flow
* Create a profile editing user flow
* Create a password reset user flow

This tutorial shows you how to create some recommended user flows by using the Azure portal.

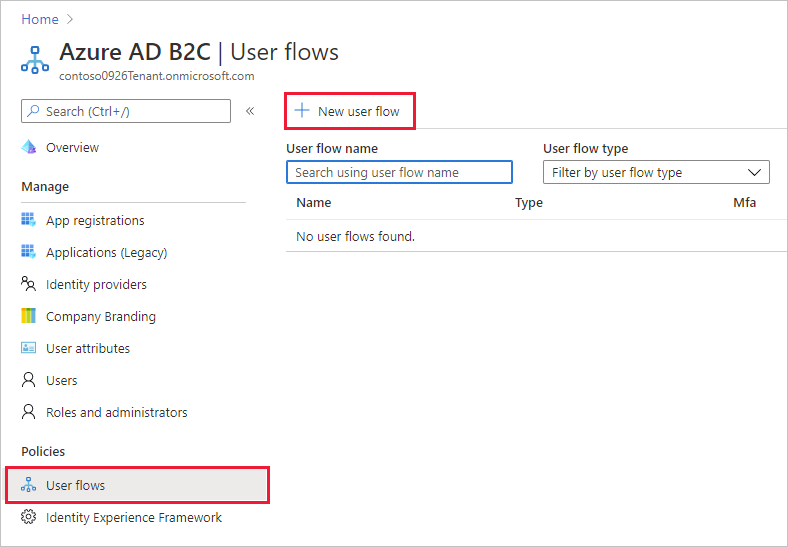
## Create a sign-up and sign-in user flow

The sign-up and sign-in user flow handles both sign-up and sign-in experiences with a single configuration. Users of your application are led down the right path depending on the context.

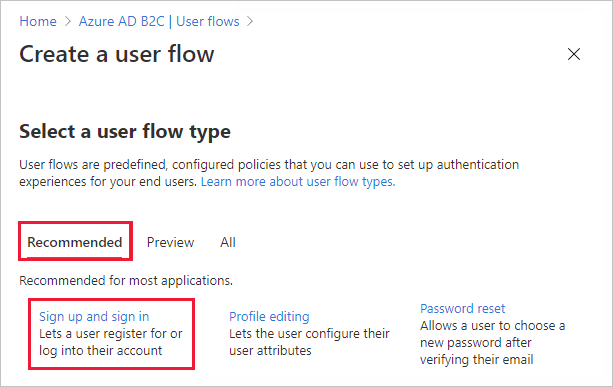
1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Select the **Directory + Subscription** icon in the portal toolbar, and then select the directory that contains your Azure AD B2C tenant.



1. In the Azure portal, search for and select **Azure AD B2C**.
2. Under **Policies**, select **User flows**, and then select **New user flow**.



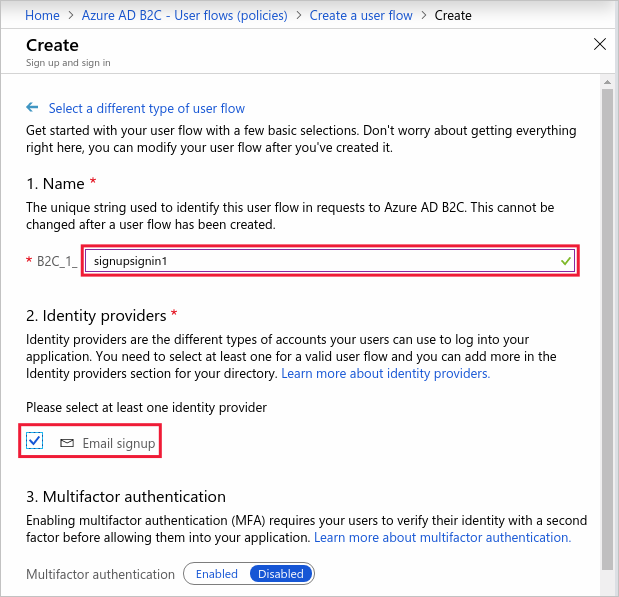
1. On the **Recommended** tab, select the **Sign up and sign in** user flow.



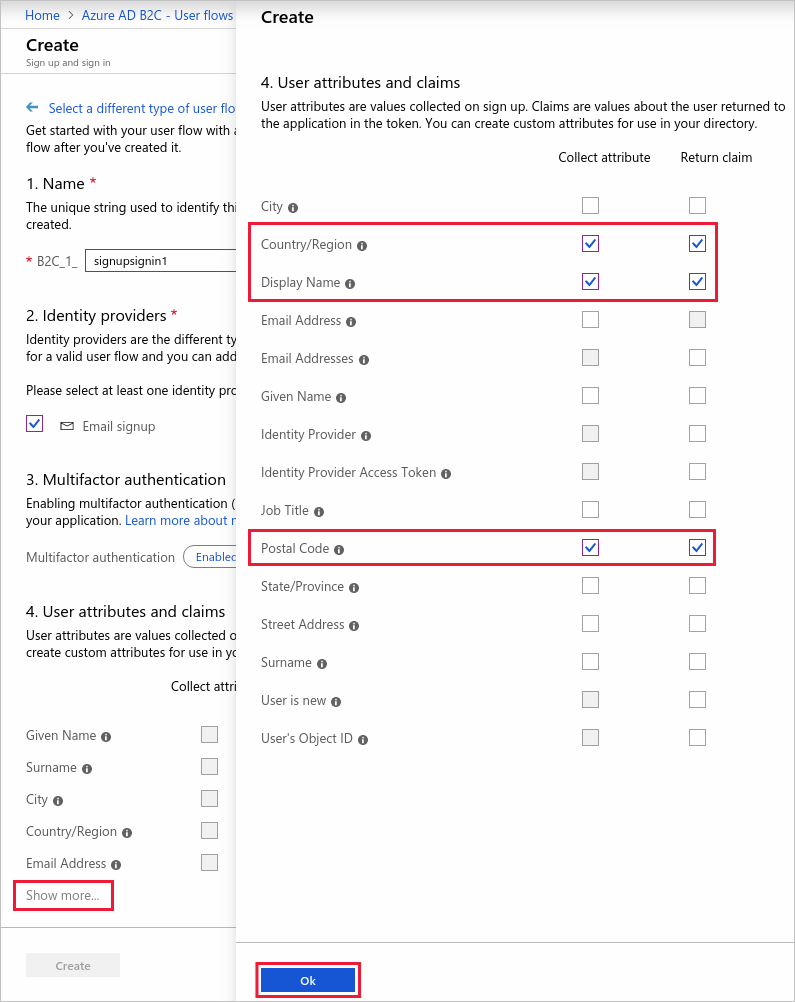
1. Enter a **Name** for the user flow. For example, signupsignin1.
2. For **Identity providers**, select **Email signup**.

# Tutorial: Add identity providers to your applications in Azure Active Directory B2C

n your applications, you may want to enable users to sign in with different identity providers. An identity provider creates, maintains, and manages identity information while providing authentication services to applications. You can add identity providers that are supported by Azure Active Directory B2C (Azure AD B2C) to your user flows using the Azure portal.



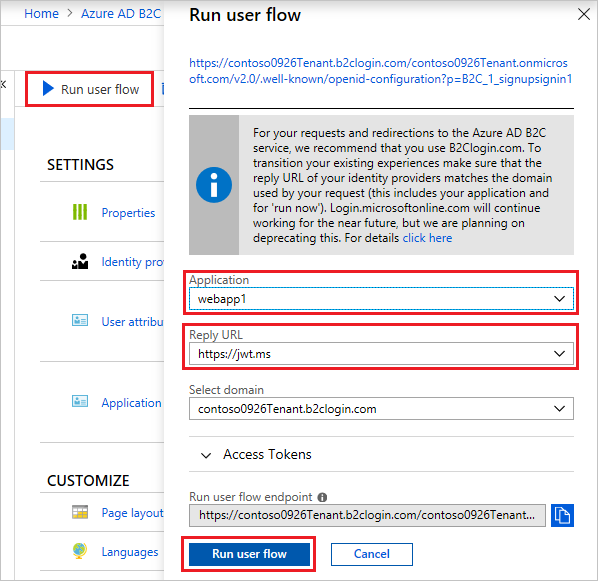
1. For **User attributes and claims**, choose the claims and attributes that you want to collect and send from the user during sign-up. For example, select **Show more**, and then choose attributes and claims for **Country/Region**, **Display Name**, and **Postal Code**. Click **OK**.



1. Click **Create** to add the user flow. A prefix of B2C\_1 is automatically prepended to the name.

### Test the user flow

1. Select the user flow you created to open its overview page, then select **Run user flow**.
2. For **Application**, select the web application named webapp1 that you previously registered. The **Reply URL** should show https://jwt.ms.
3. Click **Run user flow**, and then select **Sign up now**.



1. Enter a valid email address, click **Send verification code**, enter the verification code that you receive, then select **Verify code**.
2. Enter a new password and confirm the password.
3. Select your country and region, enter the name that you want displayed, enter a postal code, and then click **Create**. The token is returned to https://jwt.ms and should be displayed to you.
4. You can now run the user flow again and you should be able to sign in with the account that you created. The returned token includes the claims that you selected of country/region, name, and postal code.

## Create a profile editing user flow

If you want to enable users to edit their profile in your application, you use a profile editing user flow.

1. In the menu of the Azure AD B2C tenant overview page, select **User flows**, and then select **New user flow**.
2. Select the **Profile editing** user flow on the **Recommended** tab.
3. Enter a **Name** for the user flow. For example, profileediting1.
4. For **Identity providers**, select **Local Account SignIn**.
5. For **User attributes**, choose the attributes that you want the customer to be able to edit in their profile. For example, select **Show more**, and then choose both attributes and claims for **Display name** and **Job title**. Click **OK**.
6. Click **Create** to add the user flow. A prefix of B2C\_1 is automatically appended to the name.

### Test the user flow

1. Select the user flow you created to open its overview page, then select **Run user flow**.
2. For **Application**, select the web application named webapp1 that you previously registered. The **Reply URL** should show https://jwt.ms.
3. Click **Run user flow**, and then sign in with the account that you previously created.
4. You now have the opportunity to change the display name and job title for the user. Click **Continue**. The token is returned to https://jwt.ms and should be displayed to you.

## Create a password reset user flow

To enable users of your application to reset their password, you use a password reset user flow.

1. In the Azure AD B2C tenant overview menu, select **User flows**, and then select **New user flow**.
2. Select the **Password reset** user flow on the **Recommended** tab.
3. Enter a **Name** for the user flow. For example, passwordreset1.
4. For **Identity providers**, enable **Reset password using email address**.
5. Under Application claims, click **Show more** and choose the claims that you want returned in the authorization tokens sent back to your application. For example, select **User's Object ID**.
6. Click **OK**.
7. Click **Create** to add the user flow. A prefix of B2C\_1 is automatically appended to the name.

### Test the user flow

1. Select the user flow you created to open its overview page, then select **Run user flow**.
2. For **Application**, select the web application named webapp1 that you previously registered. The **Reply URL** should show https://jwt.ms.
3. Click **Run user flow**, verify the email address of the account that you previously created, and select **Continue**.
4. You now have the opportunity to change the password for the user. Change the password and select **Continue**. The token is returned to https://jwt.ms and should be displayed to you.

## Create applications

Identity provider applications provide the identifier and key to enable communication with your Azure AD B2C tenant. In this section of the tutorial, you create an Azure AD application and a Facebook application from which you get identifiers and keys to add the identity providers to your tenant. If you're adding just one of the identity providers, you only need to create the application for that provider.

### Create an Azure Active Directory application

To enable sign-in for users from Azure AD, you need to register an application within the Azure AD tenant. The Azure AD tenant is not the same as your Azure AD B2C tenant.

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Make sure you're using the directory that contains your Azure AD tenant by selecting the **Directory + subscription** filter in the top menu and choosing the directory that contains your Azure AD tenant.
3. Choose **All services** in the top-left corner of the Azure portal, and then search for and select **App registrations**.
4. Select **New registration**.
5. Enter a name for your application. For example, Azure AD B2C App.
6. Accept the selection of **Accounts in this organizational directory only** for this application.
7. For the **Redirect URI**, accept the value of **Web** and enter the following URL in all lowercase letters, replacing your-B2C-tenant-name with the name of your Azure AD B2C tenant.

https://your-B2C-tenant-name.b2clogin.com/your-B2C-tenant-name.onmicrosoft.com/oauth2/authresp

For example,

 https://contoso.b2clogin.com/contoso.onmicrosoft.com/oauth2/authresp.

All URLs should now be using b2clogin.com.

1. Select **Register**, then record the **Application (client) ID** which you use in a later step.
2. Under **Manage** in the application menu, select **Certificates & secrets**, then select **New client secret**.
3. Enter a **Description** for the client secret. For example, Azure AD B2C App Secret.
4. Select the expiration period. For this application, accept the selection of **In 1 year**.
5. Select **Add**, then record the value of the new client secret which you use in a later step.

### Create a Facebook application

To use a Facebook account as an identity provider in Azure AD B2C, you need to create an application at Facebook. If you don’t already have a Facebook account, you can get it at <https://www.facebook.com/>.

1. Sign in to Facebook for developers with your Facebook account credentials.
2. If you haven't already done so, you need to register as a Facebook developer. To do this, select **Get Started** on the upper-right corner of the page, accept Facebook's policies, and complete the registration steps.
3. Select **My Apps** and then **Create App**.
4. Enter a **Display Name** and a valid **Contact Email**.
5. Click **Create App ID**. This may require you to accept Facebook platform policies and complete an online security check.
6. Select **Settings** > **Basic**.
7. Choose a **Category**, for example Business and Pages. This value is required by Facebook, but isn't used by Azure AD B2C.
8. At the bottom of the page, select **Add Platform**, and then select **Website**.
9. In **Site URL**, enter https://your-tenant-name.b2clogin.com/ replacing your-tenant-name with the name of your tenant.
10. Enter a URL for the **Privacy Policy URL**, for example http://www.contoso.com/. The privacy policy URL is a page you maintain to provide privacy information for your application.
11. Select **Save Changes**.
12. At the top of the page, record the value of **App ID**.
13. Next to **App Secret**, select **Show** and record its value. You use both the App ID and App Secret to configure Facebook as an identity provider in your tenant. **App Secret** is an important security credential which you should store securely.
14. Select the plus sign next to **PRODUCTS**, then under **Facebook Login**, select **Set up**.
15. Under **Facebook Login** in the left-hand menu, select **Settings**.
16. In **Valid OAuth redirect URIs**, enter https://your-tenant-name.b2clogin.com/your-tenant-name.onmicrosoft.com/oauth2/authresp. Replace your-tenant-name with the name of your tenant. Select **Save Changes** at the bottom of the page.
17. To make your Facebook application available to Azure AD B2C, click the **Status** selector at the top right of the page and turn it **On** to make the Application public, and then click **Confirm**. At this point, the Status should change from **Development** to **Live**.

## Add the identity providers

After you create the application for the identity provider that you want to add, you add the identity provider to your tenant.

### Add the Azure Active Directory identity provider

1. Make sure you're using the directory that contains Azure AD B2C tenant. Select the **Directory + subscription** filter in the top menu and choose the directory that contains your Azure AD B2C tenant.
2. Choose **All services** in the top-left corner of the Azure portal, and then search for and select **Azure AD B2C**.
3. Select **Identity providers**, and then select **New OpenID Connect provider**.
4. Enter a **Name**. For example, enter Contoso Azure AD.
5. For **Metadata url**, enter the following URL replacing your-AD-tenant-domain with the domain name of your Azure AD tenant:

Copy

https://login.microsoftonline.com/your-AD-tenant-domain/.well-known/openid-configuration

For example, https://login.microsoftonline.com/contoso.onmicrosoft.com/.well-known/openid-configuration.

1. For **Client ID**, enter the application ID that you previously recorded.
2. For **Client secret**, enter the client secret that you previously recorded.
3. Leave the default values for **Scope**, **Response type**, and **Response mode**.
4. (Optional) Enter a value for **Domain\_hint**. For example, ContosoAD. Domain hints are directives that are included in the authentication request from an application. They can be used to accelerate the user to their federated IdP sign-in page. Or they can be used by a multi-tenant application to accelerate the user straight to the branded Azure AD sign-in page for their tenant.
5. Under **Identity provider claims mapping**, enter the following claims mapping values:
   * **User ID**: oid
   * **Display name**: name
   * **Given name**: given\_name
   * **Surname**: family\_name
   * **Email**: unique\_name
6. Select **Save**.

### Add the Facebook identity provider

1. Select **Identity providers**, then select **Facebook**.
2. Enter a **Name**. For example, Facebook.
3. For the **Client ID**, enter the App ID of the Facebook application that you created earlier.
4. For the **Client secret**, enter the App Secret that you recorded.
5. Select **Save**.

## Update the user flow

In the tutorial that you completed as part of the prerequisites, you created a user flow for sign-up and sign-in named B2C\_1\_signupsignin1. In this section, you add the identity providers to the B2C\_1\_signupsignin1 user flow.

1. Select **User flows (policies)**, and then select the B2C\_1\_signupsignin1 user flow.
2. Select **Identity providers**, select the **Facebook** and **Contoso Azure AD** identity providers that you added.
3. Select **Save**.

## Test the user flow

1. On the Overview page of the user flow that you created, select **Run user flow**.
2. For **Application**, select the web application named webapp1 that you previously registered. The **Reply URL** should show https://jwt.ms.
3. Select **Run user flow**, and then sign in with an identity provider that you previously added.
4. Repeat steps 1 through 3 for the other identity providers that you added.

If the sign in operation is successful, you're redirected to https://jwt.ms which displays the Decoded Token, similar to:

JSON

{

"typ": "JWT",

"alg": "RS256",

"kid": "<key-ID>"

}.{

"exp": 1562346892,

"nbf": 1562343292,

"ver": "1.0",

"iss": "https://your-b2c-tenant.b2clogin.com/10000000-0000-0000-0000-000000000000/v2.0/",

"sub": "20000000-0000-0000-0000-000000000000",

"aud": "30000000-0000-0000-0000-000000000000",

"nonce": "defaultNonce",

"iat": 1562343292,

"auth\_time": 1562343292,

"name": "User Name",

"idp": "facebook.com",

"postalCode": "12345",

"tfp": "B2C\_1\_signupsignin1"

}.[Signature]

# Tutorial: Customize the interface of user experiences in Azure Active Directory B2C

## Create customization files

You create an Azure storage account and container and then place basic HTML and CSS files in the container.

### Create a storage account

Although you can store your files in many ways, for this tutorial, you store them in [Azure Blob storage](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction).

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Make sure you're using the directory that contains your Azure subscription. Select the **Directory + subscription** filter in the top menu and choose the directory that contains your subscription. This directory is different than the one that contains your Azure B2C tenant.
3. Choose All services in the top-left corner of the Azure portal, search for and select **Storage accounts**.
4. Select **Add**.
5. Under **Resource group**, select **Create new**, enter a name for the new resource group, and then click **OK**.
6. Enter a name for the storage account. The name you choose must be unique across Azure, must be between 3 and 24 characters in length, and may contain numbers and lowercase letters only.
7. Select the location of the storage account or accept the default location.
8. Accept all other default values, select **Review + create**, and then click **Create**.
9. After the storage account is created, select **Go to resource**.

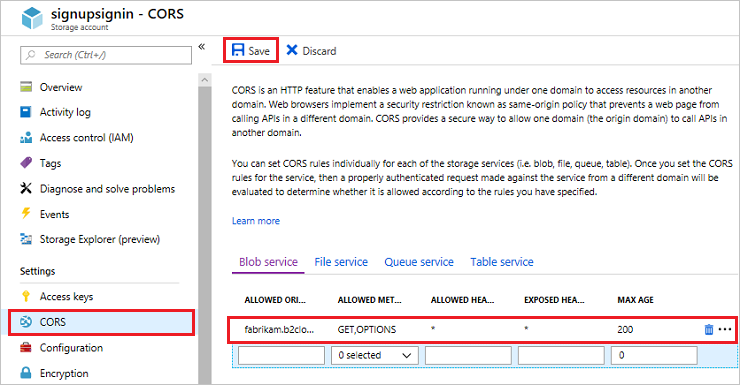
### Create a container

1. On the overview page of the storage account, select **Blobs**.
2. Select **Container**, enter a name for the container, choose **Blob (anonymous read access for blobs only)**, and then click **OK**.

### Enable CORS

Azure AD B2C code in a browser uses a modern and standard approach to load custom content from a URL that you specify in a user flow. Cross-origin resource sharing (CORS) allows restricted resources on a web page to be requested from other domains.

1. In the menu, select **CORS**.
2. For **Allowed origins**, enter https://your-tenant-name.b2clogin.com. Replace your-tenant-name with the name of your Azure AD B2C tenant. For example, https://fabrikam.b2clogin.com. You need to use all lowercase letters when entering your tenant name.
3. For **Allowed Methods**, select GET,PUT, and OPTIONS.
4. For **Allowed Headers**, enter an asterisk (\*).
5. For **Exposed Headers**, enter an asterisk (\*).
6. For **Max age**, enter 200.



1. Click **Save**.

### Create the customization files

To customize the UI of the sign-up experience, you start by creating a simple HTML and CSS file. You can configure your HTML any way you want, but it must have a **div** element with an identifier of api. For example, <div id="api"></div>. Azure AD B2C injects elements into the api container when the page is displayed.

1. In a local folder, create the following file and make sure that you change your-storage-account to the name of the storage account and your-container to the name of the container that you created. For example, https://store1.blob.core.windows.net/b2c/style.css. <!DOCTYPE html>

<html>

<head>

<title>My B2C Application</title>

<link rel="stylesheet" href="https://your-storage-account.blob.core.windows.net/your-container/style.css">

</head>

<body>

<h1>My B2C Application</h1>

<div id="api"></div>

</body>

</html>

1. The page can be designed any way that you want, but the **api** div element is required for any HTML customization file that you create.
2. Save the file as custom-ui.html.
3. Create the following simple CSS that centers all elements on the sign-up or sign-in page including the elements that Azure AD B2C injects.

h1 {

color: blue;

text-align: center;

}

.intro h2 {

text-align: center;

}

.entry {

width: 300px ;

margin-left: auto ;

margin-right: auto ;

}

.divider h2 {

text-align: center;

}

.create {

width: 300px ;

margin-left: auto ;

margin-right: auto ;

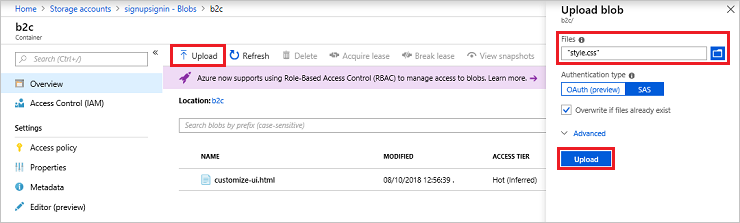
}

1. Save the file as style.css.

### Upload the customization files

In this tutorial, you store the files that you created in the storage account so that Azure AD B2C can access them.

1. Choose **All services** in the top-left corner of the Azure portal, search for and select **Storage accounts**.
2. Select the storage account you created, select **Blobs**, and then select the container that you created.
3. Select **Upload**, navigate to and select the custom-ui.html file, and then click **Upload**.



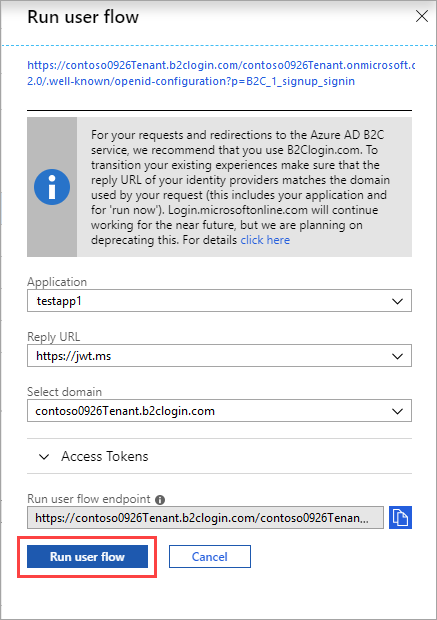
1. Copy the URL for the file that you uploaded to use later in the tutorial.
2. Repeat step 3 and 4 for the style.css file.

## Update the user flow

1. Choose **All services** in the top-left corner of the Azure portal, and then search for and select **Azure AD B2C**.
2. Select **User flows (policies)**, and then select the B2C\_1\_signupsignin1 user flow.
3. Select **Page layouts**, and then under **Unified sign-up or sign-in page**, click **Yes** for **Use custom page content**.
4. In **Custom page URI**, enter the URI for the custom-ui.html file that you recorded earlier.
5. At the top of the page, select **Save**.

## Test the user flow

1. In your Azure AD B2C tenant, select **User flows** and select the B2C\_1\_signupsignin1 user flow.
2. At the top of the page, click **Run user flow**.
3. Click the **Run user flow** button.



You should see a page similar to the following example with the elements centered based on the CSS file that you created:

