Azure AD B2C Configuration

[Overview 1](#_Toc57449408)

[Azure AD B2C Configuration 2](#_Toc268448848)

[Create an Azure AD B2C tenant 2](#_Toc700558030)

[Select your B2C tenant directory 4](#_Toc865890247)

[Register an Application 5](#_Toc1251761993)

[Register the IdentityExperienceFramework application 5](#_Toc10156469)

[Register the ProxyIdentityExperienceFramework application 6](#_Toc1272130983)

[Add signing and encryption keys for Identity Experience Framework applications 7](#_Toc1070793286)

[Create the signing key 7](#_Toc1985403234)

[Create the encryption key 7](#_Toc1267157493)

[Upload the Policy files to the B2C tenant 8](#_Toc372722053)

[Conditional Access Policy 9](#_Toc1002915094)

# Overview

Azure AD B2C is a customer identity access management (CIAM) solution capable of supporting millions of users and billions of authentications per day. It takes care of the scaling and safety of the authentication platform, monitoring, and automatically handling threats like denial-of-service, password spray, or brute force attacks.

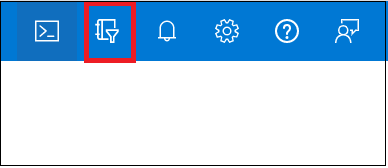
The proposed solution is having an Azure Active directory B2C tenant configured with the users flows to register a new user, login using password, login using OTP, login using UAE PASS, self-service password reset. As we integrate the UAE PASS identity provider with the AD B2C, the user can use their UAE PASS authentication to login to the application. The application is used by the closed set of users and not intended for all the audiences, so the EmiratesId is collected in the user registration phase, and it is validated against the CRM. To align the look and feel of the B2C pages with application, branding is done by customizing the logo and background image in the pages. The URL of the B2C page endpoint is enhanced to have the custom domain.

# Azure AD B2C Configuration

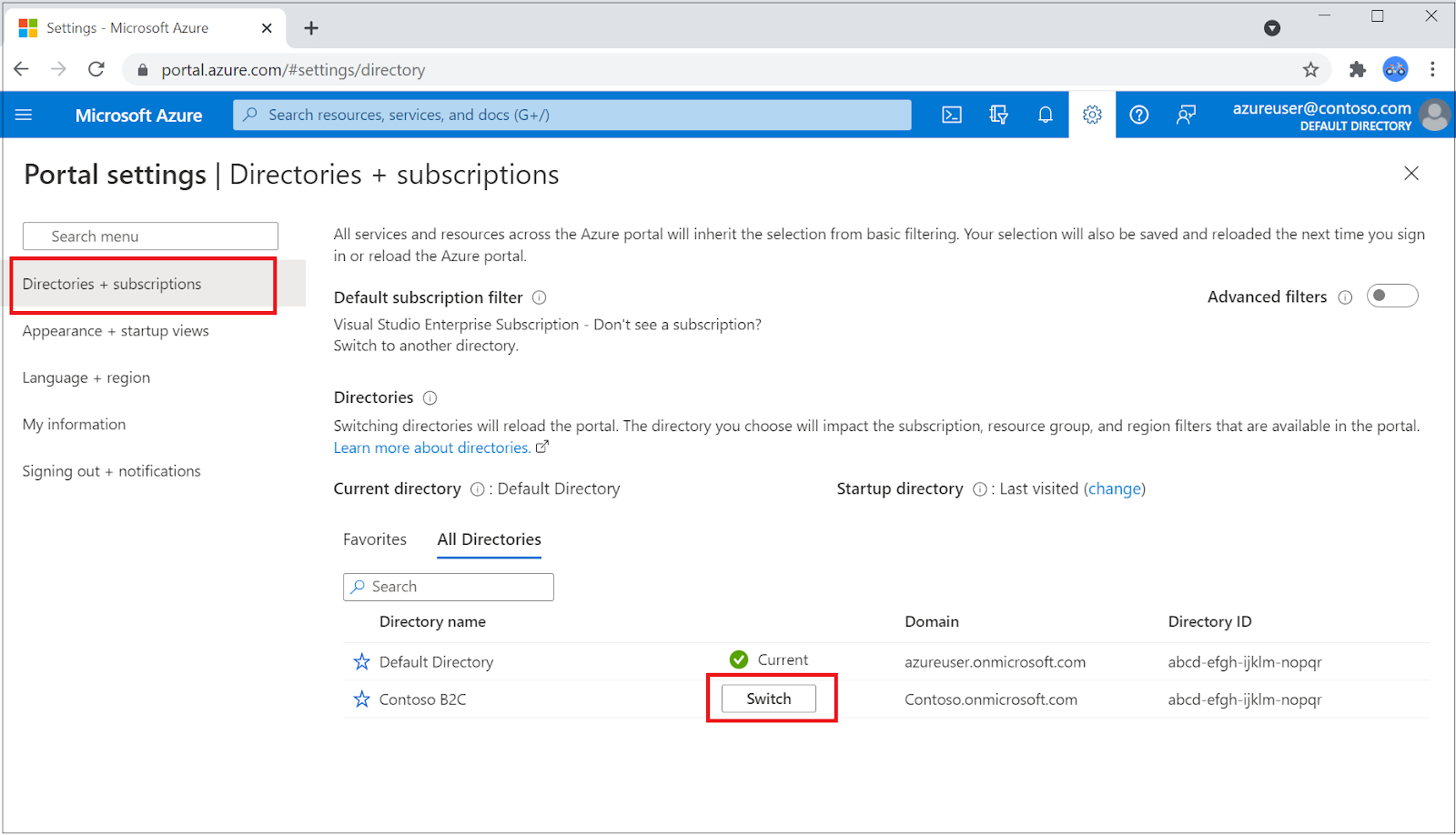
## Create an Azure AD B2C tenant

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Switch to the directory that contains your subscription:

* In the Azure portal toolbar, select the Directories + subscriptions filter icon.



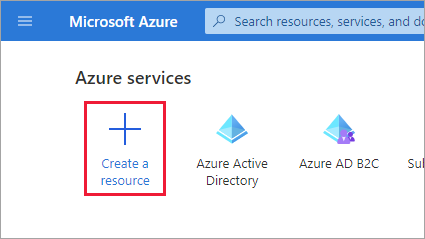
* Find the directory that contains your subscription and select the Switch button next to it. Switching a directory reloads the portal.

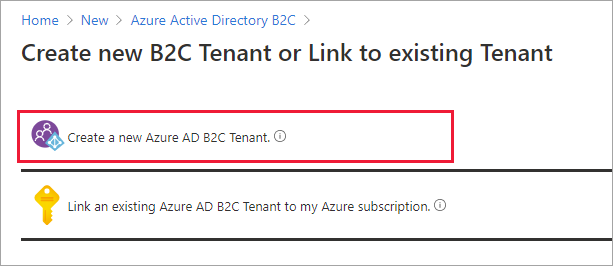


1. Add Microsoft.AzureActiveDirectory as a resource provider for the Azure subscription you're using ([learn more](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types?WT.mc_id=Portal-Microsoft_Azure_Support#register-resource-provider-1)):

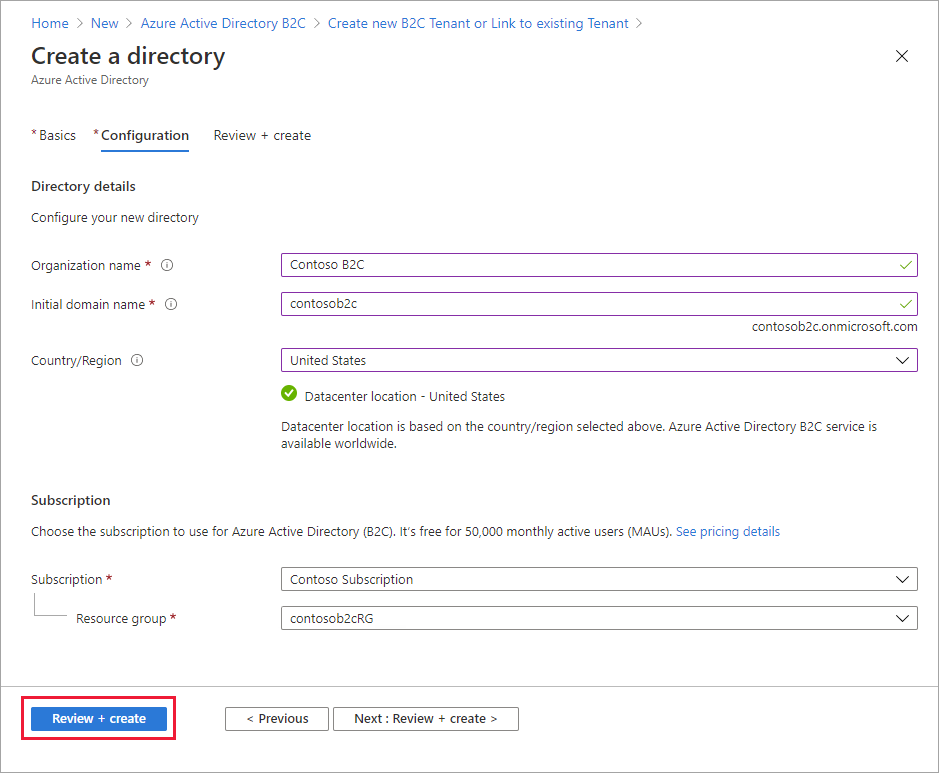
* On the Azure portal, search for and select Subscriptions.
* Select your subscription, and then in the left menu, select Resource providers. If you don't see the left menu, select the Show the menu for < name of your subscription > icon at the top left part of the page to expand it.
* Make sure the Microsoft.AzureActiveDirectory row shows a status of Registered. If it doesn't, select the row, and then select Register.

1. On the Azure portal menu or from the Home page, select Create a resource.



1. Search for Azure Active Directory B2C, and then select Create.
2. Select Create a new Azure AD B2C Tenant.
3. 
4. On the Create a directory page, enter the following:

* Organization name - Enter a name for your Azure AD B2C tenant **DIEZ B2C**
* Initial domain name - Enter a domain name for your Azure AD B2C tenant. **diezb2c**
* Country or region - Select your country or region from the list. This selection can't be changed later. - **UAE North**
* Subscription - Select your subscription from the list.
* Resource group - Select or search for the resource group that will contain the tenant. **diexb2c**



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

## 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:

1. In the Azure portal toolbar, select the Directories + subscriptions filter icon.
2. On the All-Directories tab, find the directory that contains your Azure AD B2C tenant and then select the Switch button next to it.

If at first you don't see your new Azure B2C tenant in the list, refresh your browser window or sign out and sign back in. Then in the Azure portal toolbar, select the Directories + subscriptions filter again.

## Register an Application

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Make sure you're using the directory that contains your Azure AD B2C tenant. Select the Directories + subscriptions icon in the portal toolbar.
3. On the Portal settings | Directories + subscriptions page, find your Azure AD B2C directory in the Directory name list, and then select Switch.
4. In the Azure portal, search for and select Azure AD B2C.
5. Select App registrations, and then select New registration.
6. Enter a Name for the application as **DIEZ**
7. Under Supported account types, s**elect Accounts in any identity provider or organizational directory** (for authenticating users with user flows).
8. Under Redirect URI, select Web, and then enter [https://jwt.ms](https://jwt.ms/) or the application URL in the URL text box.

## Register the IdentityExperienceFramework application

To register an application in your Azure AD B2C tenant, you can use the App registrations experience.

1. Select App registrations, and then select New registration.
2. For Name, enter **IdentityExperienceFramework**.
3. Under Supported account types, select Accounts in this organizational directory only.
4. Under Redirect URI, select Web, and then enter **https:// diezb2c.b2clogin.com/ diezb2c.onmicrosoft.com**,
5. Under Permissions, select the *Grant admin consent to* ***openid*** *and* ***offline\_access*** *permissions* check box.
6. Select Register.
7. Record the Application (client) ID for use in a later step.

Next, expose the API by adding a scope:

1. In the left menu, under **Manage**, select **Expose an API.**
2. Select **Add a scope**, then select **Save** and continue to accept the default application ID URI.
3. Enter the following values to create a scope that allows custom policy execution in your Azure AD B2C tenant:

* Scope name: **user\_impersonation**
* Admin consent display name: Access **IdentityExperienceFramework**
* Admin consent description: **Allow the application to access IdentityExperienceFramework on behalf of the signed-in user.**

1. Select **Add scope**

## Register the ProxyIdentityExperienceFramework application

1. Select App registrations, and then select New registration.
2. For Name, enter **ProxyIdentityExperienceFramework**.
3. Under Supported account types, select **Accounts in this organizational directory only.**
4. Under **Redirect URI**, use the drop-down to select **Public client/native (mobile & desktop)**.
5. For Redirect URI, save the redirect uri with default details.
6. Under Permissions, select the ***Grant admin consent to openid and offline\_access permissions*** check box.
7. Select **Register**.
8. Record the Application (client) ID for use in a later step.

Next, specify that the application should be treated as a public client:

1. In the left menu, under **Manage**, select **Authentication**.
2. Under Advanced settings, in the Allow public client flows section, set Enable the following mobile and desktop flows to Yes.
3. Select **Save**.
4. Ensure that "**allowPublicClient**": true is set in the application manifest:
5. In the left menu, under Manage, select Manifest to open application manifest.
6. Find **allowPublicClient** key and ensure its value is set to true.

Now, grant permissions to the API scope you exposed earlier in the ***IdentityExperienceFramework*** registration:

1. In the left menu, under **Manage**, select **API permissions**.
2. Under Configured permissions, select **Add a permission**.
3. Select the **My APIs tab**, then select the **IdentityExperienceFramework** application.
4. Under Permission, select the **user\_impersonation** scope that you defined earlier.
5. Select **Add permissions**. As directed, wait a few minutes before proceeding to the next step.
6. Select **Grant admin consent for *diezb2c***.
7. Select **Yes**.
8. Select Refresh, and then verify that "Granted for ..." appears under Status for the scope.

## Add signing and encryption keys for Identity Experience Framework applications

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. Make sure you're using the directory that contains your Azure AD B2C tenant. Select the Directories + subscriptions icon in the portal toolbar.
3. On the Portal settings | Directories + subscriptions page, find your Azure AD B2C directory in the Directory name list, and then select Switch.
4. In the Azure portal, search for and select Azure AD B2C.
5. On the overview page, under Policies, select Identity Experience Framework.

### Create the signing key

1. Select Policy Keys and then select **Add**.
2. For Options, choose **Generate**.
3. In Name, enter **TokenSigningKeyContainer**. The prefix B2C\_1A\_ might be added automatically.
4. For Key type, select **RSA**.
5. For Key usage, select **Signature**.
6. Select **Create**.

### Create the encryption key

1. Select Policy Keys and then select **Add**.
2. For Options, choose **Generate**.
3. In Name, enter **TokenEncryptionKeyContainer**. The prefix B2C\_1A\_ might be added automatically.
4. For Key type, select **RSA**.
5. For Key usage, select **Encryption**.
6. Select **Create**.

## Upload the Policy files to the B2C tenant

The shared XML policy files should be uploaded to the B2C Tenant in the Identity Experience Framework Section.

The policies should be upload in the following order.

1. TRUSTFRAMEWORKBASE
2. TRUSTFRAMEWORKLOCALIZATION
3. TRUSTFRAMEWORKEXTENSIONS
4. SIGNIN

# Conditional Access Policy