

# Introduction:

Welcome to our documentation on integrating Auth0 with Microsoft Identity to develop a login and registration feature for our web application. This guide is designed to streamline the setup process, emphasize key configurations, outline integration steps, and provide a user-friendly guide for leveraging the login and registration functionality.

Integrating Auth0 with Microsoft Identity offers a secure and scalable authentication solution, enabling users to easily log in and register using their Microsoft accounts. This documentation serves as a comprehensive resource, empowering us to create a proof of concept (POC) that demonstrates the seamless integration of these authentication services into our web application.

*Before we delve into the integration process, it's important to understand what **Auth0** and **Microsoft Identity** are:*

## Auth0

Auth0 is a popular *Identity-as-a-Service* (IDaaS) platform that provides authentication, authorization, and identity management services for web, mobile, and single-page applications (SPAs). It offers developers a simple and secure way to add authentication and authorization features to their applications without having to build them from scratch.

### **Key aspects of Auth0 include:**

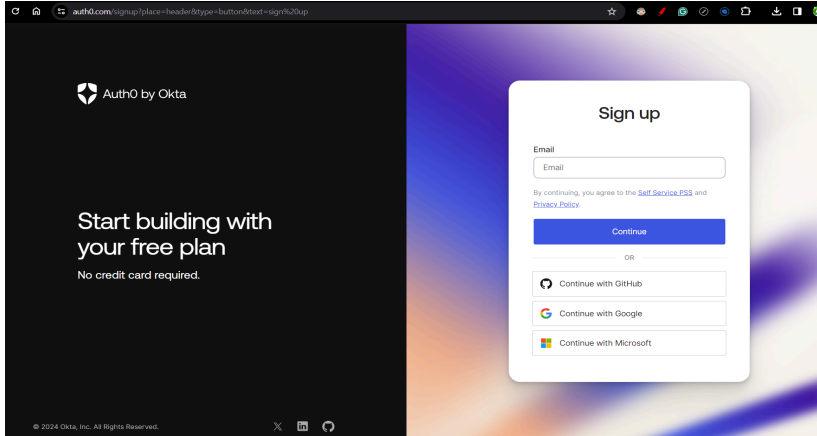
- **Authentication and Authorization:** Provides robust authentication and authorization solutions for applications.
- **Identity Provider Integration:** Supports integration with various identity providers including social media and enterprise solutions.
- **User Management:** Offers features for user registration, password resets, and user profile management.

## Microsoft Identity

Microsoft Identity refers to a set of services and technologies provided by Microsoft for managing user identities and enabling secure authentication and authorization within applications and services. It encompasses various components and protocols designed to facilitate identity management and access control for Microsoft accounts.

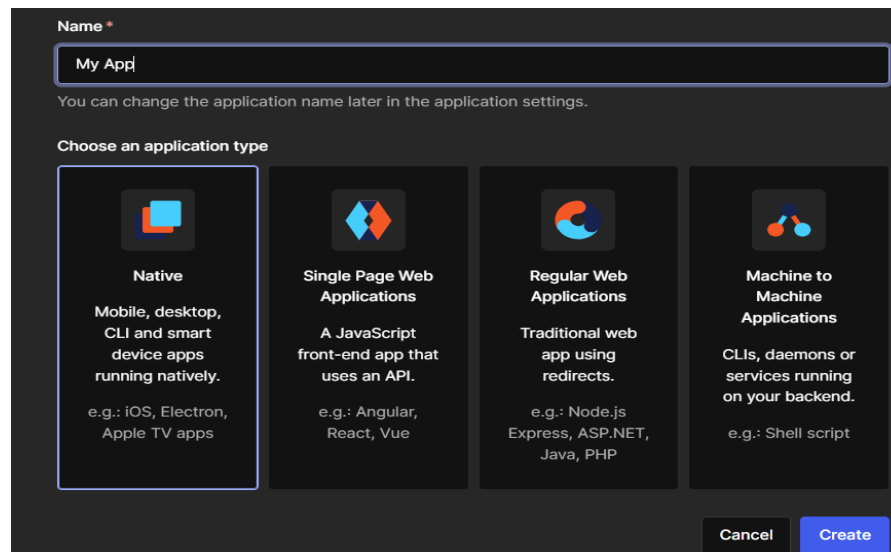
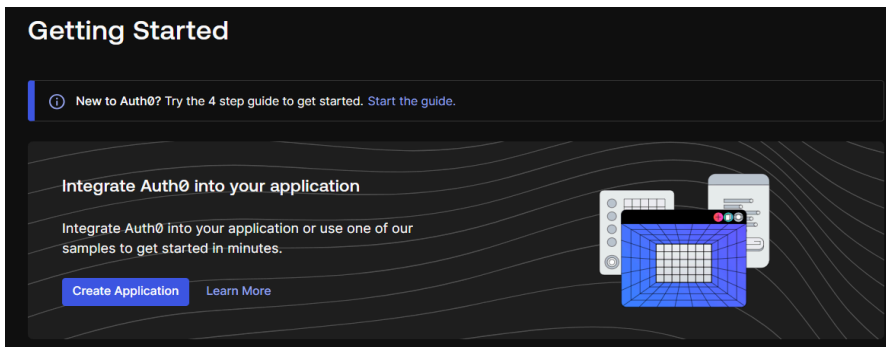
# 1. Setup Process:

★ Create an Auth0 Account: [Auth0 website](#)



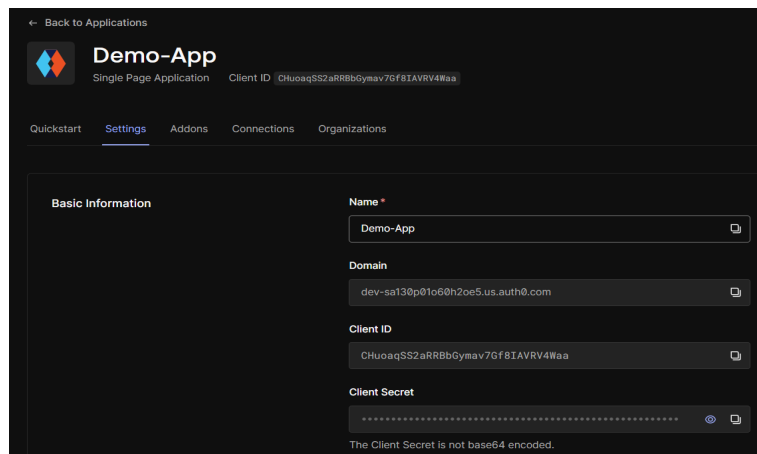
★ Create an Application in Auth0:

1. Log in to your Auth0 dashboard.
2. Navigate to the Applications section and click on "Create Application."
3. Choose the application type (Single Page Application, Regular Web Application, etc.).
4. Follow the prompts to configure your application settings.



## ★ Set up Microsoft Identity in Auth0:

1. In the Auth0 dashboard, go to the Connections tab.
2. Click on "Social" and then select "Microsoft Identity Platform."
3. Enter the Application (client) ID and Application (client) Secret obtained from the Azure portal when registering your app with Microsoft Identity.
4. Save the changes.



← Back to Applications

**Demo-App**  
Single Page Application Client ID CHuoagSS2aRRBbGymav7Gf8IAVRV4Waa

Quickstart Settings Addons Connections Organizations

**Basic Information**

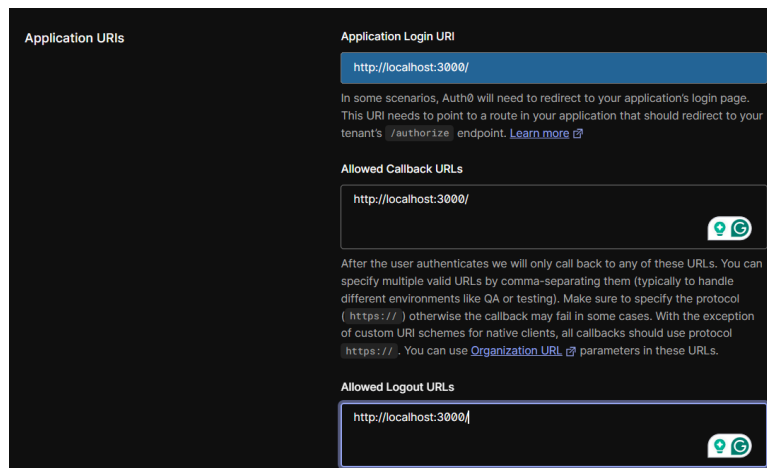
Name \*  
Demo-App

Domain  
dev-sa130p01o60h2oe5.us.auth0.com

Client ID  
CHuoagSS2aRRBbGymav7Gf8IAVRV4Waa

Client Secret  
.....  
The Client Secret is not base64 encoded.

## ★ Configure Callback/Application URLs:



Application URIs

**Application Login URI**  
http://localhost:3000/

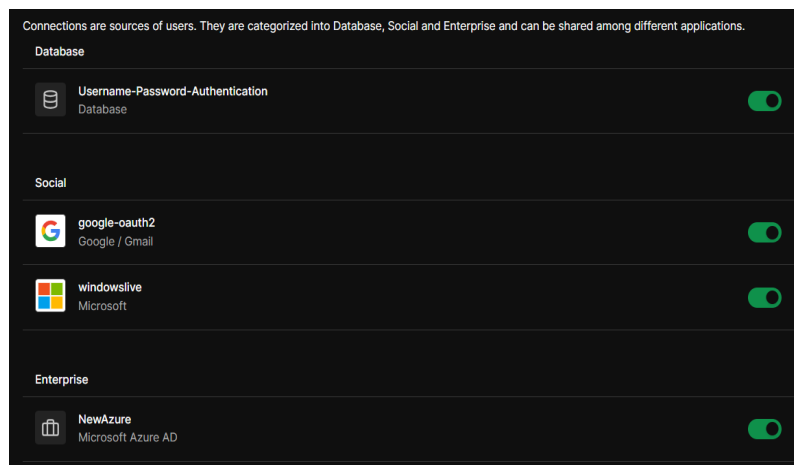
In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. [Learn more](#)

**Allowed Callback URLs**  
http://localhost:3000/

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://`. You can use [Organization URL](#) parameters in these URLs.


**Allowed Logout URLs**  
http://localhost:3000/

## ★ Enable Services





Connections are sources of users. They are categorized into Database, Social and Enterprise and can be shared among different applications.

**Database**


 **Username-Password-Authentication**  
Database ☒

**Social**

 **google-oauth2**  
Google / Gmail ☒

 **windowslive**  
Microsoft ☒

**Enterprise**

 **NewAzure**  
Microsoft Azure AD ☒

## 2. Key Configurations:

### ★ Auth0 Application Settings:

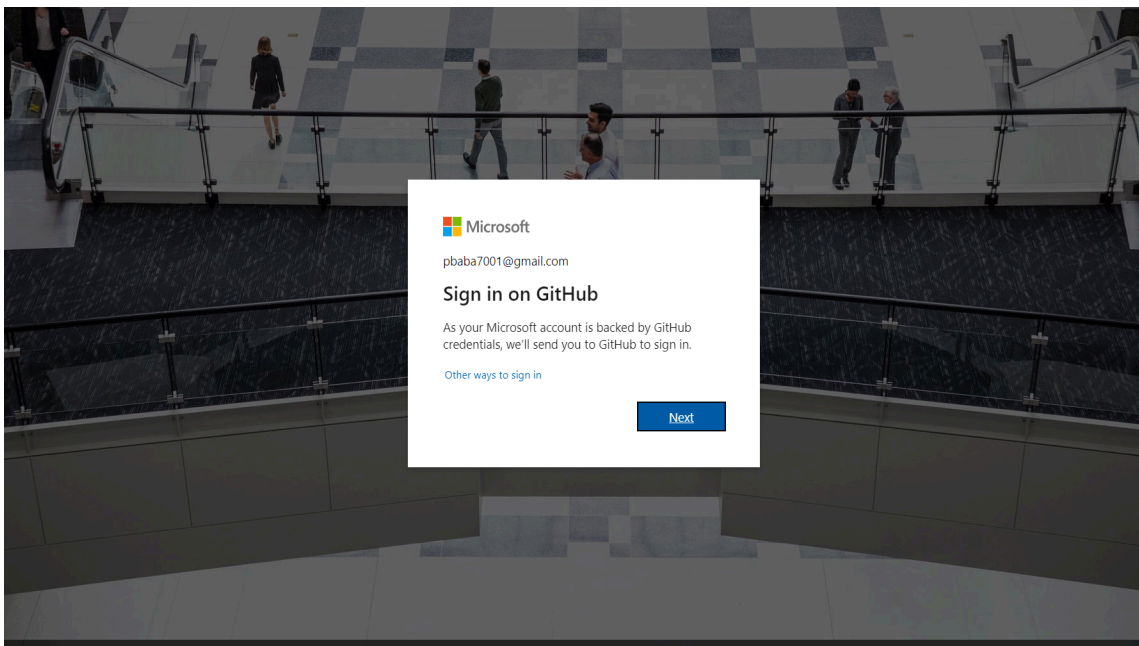
- **Client ID:** Unique identifier for Auth0 application.
- **Client Secret:** Secret key used for secure communication between application and Auth0.
- **Allowed Callback URLs:** URLs where Auth0 redirects users after authentication.
- **Allowed Logout URLs:** URLs where Auth0 redirects users after they log out.
- **Allowed Web Origins:** URLs from which Auth0 accepts requests.

### ★ Microsoft Identity Settings:

- **Application (client) ID:** Unique identifier for Microsoft Identity application.
- **Application (client) Secret:** Secret key used for secure communication between your application and Microsoft Identity.

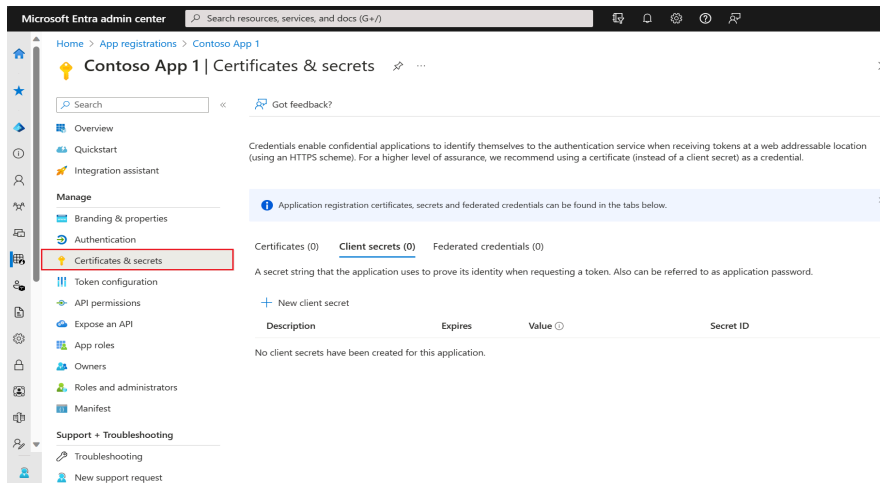
## 3. Integration Steps:

### ★ Log in to the Azure [portal](#)

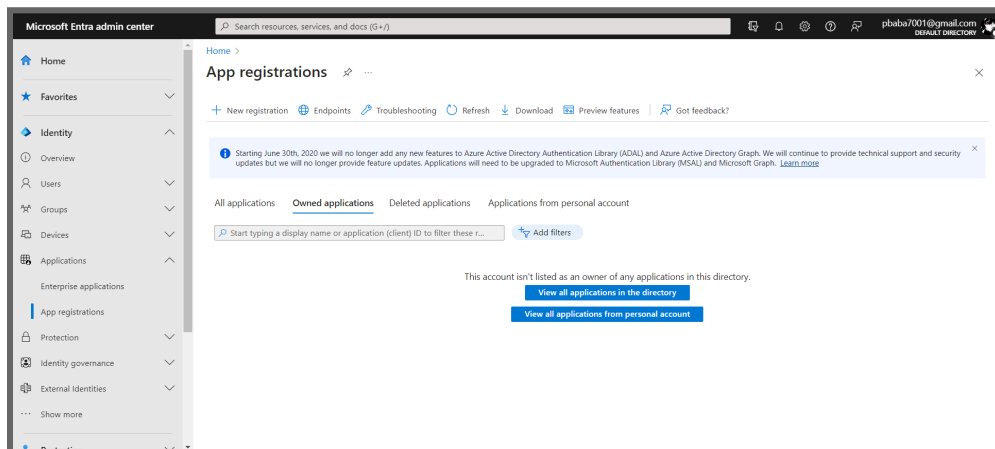


## ★ Register the app with Azure AD

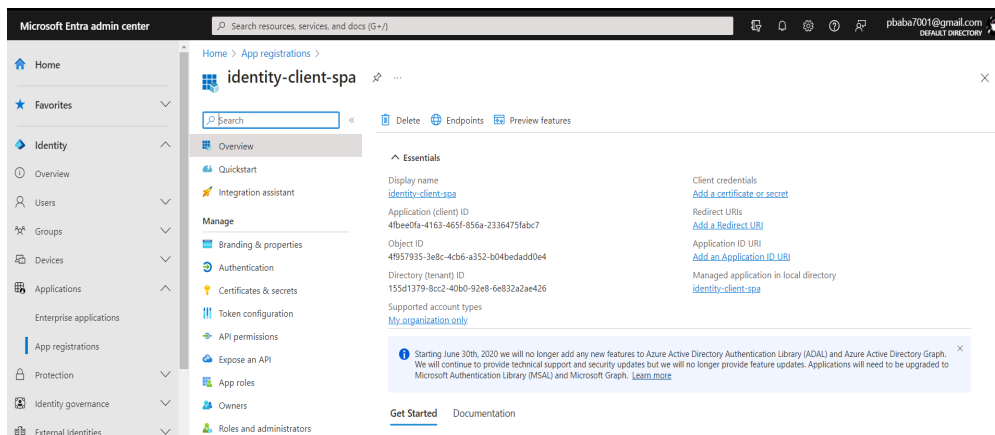
Navigate to "Azure Active Directory" > "App registrations".



## ★ Click on "New registration" and fill in the required details (e.g., Name, Supported account types).



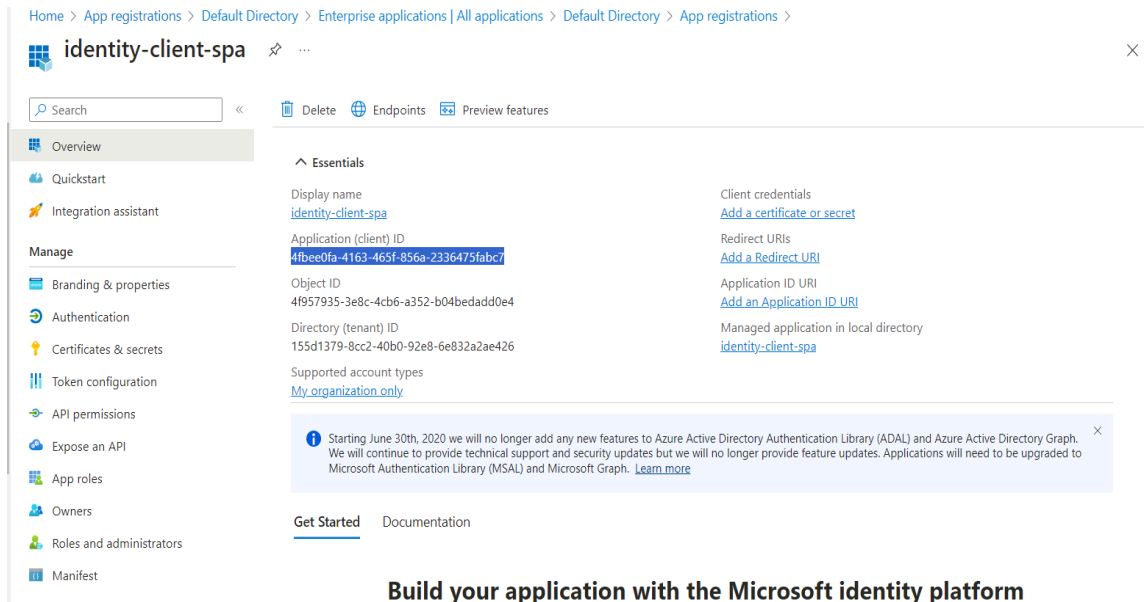
## ★ Note down the "Application (client) ID" and "Directory (tenant) ID" upon registration.



## ★ Create a client's secret

Secret used by a client (application) to authenticate with the Authorization Server; it should be known to only the client and the Authorization Server and must be sufficiently random to not be guessable.

*In the App Registration settings, go to "**Certificates & Secrets**" Create a new client secret and note down the generated **secret value**.*



Home > App registrations > Default Directory > Enterprise applications | All applications > Default Directory > App registrations > identity-client-spa

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Essentials

Display name  
identity-client-spa

Application (client) ID  
4fbee0fa-4163-465f-856a-2336475fabcd

Object ID  
4f957935-3e8c-4cb6-a352-b04bedadd0e4

Directory (tenant) ID  
155d1379-8cc2-40b0-92e8-6e832a2ae426

Supported account types  
My organization only

Client credentials  
Add a certificate or secret

Redirect URIs  
Add a Redirect URI

Application ID URI  
Add an Application ID URI

Managed application in local directory  
identity-client-spa

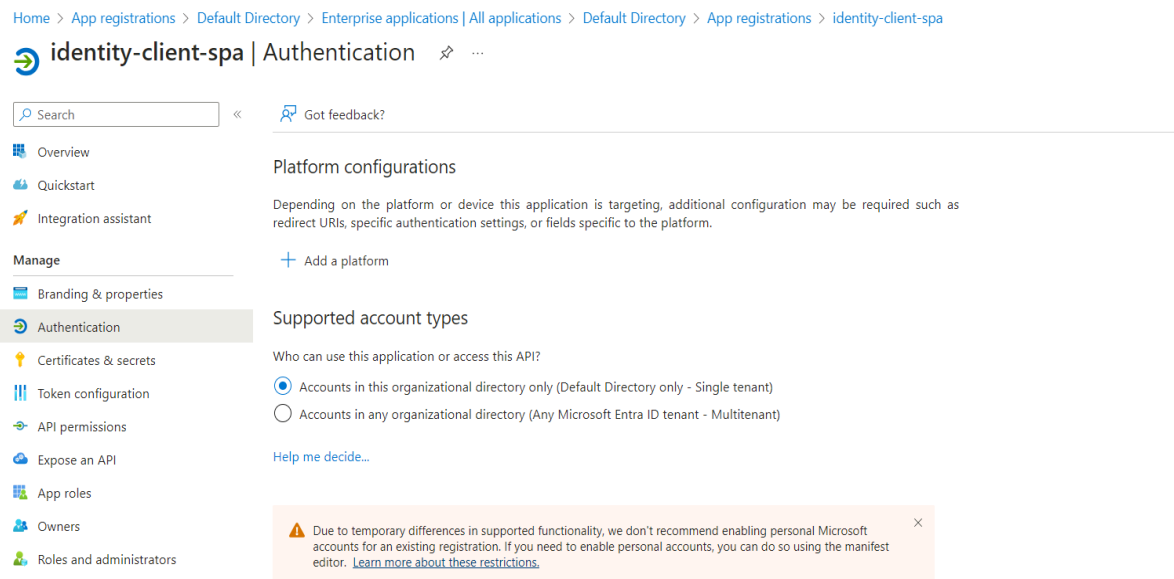
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Get Started Documentation

Build your application with the Microsoft identity platform

## ★ Configure Authentication Redirect URIs

*Under App Registration in the Azure portal, navigate to "Authentication."*



Home > App registrations > Default Directory > Enterprise applications | All applications > Default Directory > App registrations > identity-client-spa

identity-client-spa | Authentication

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

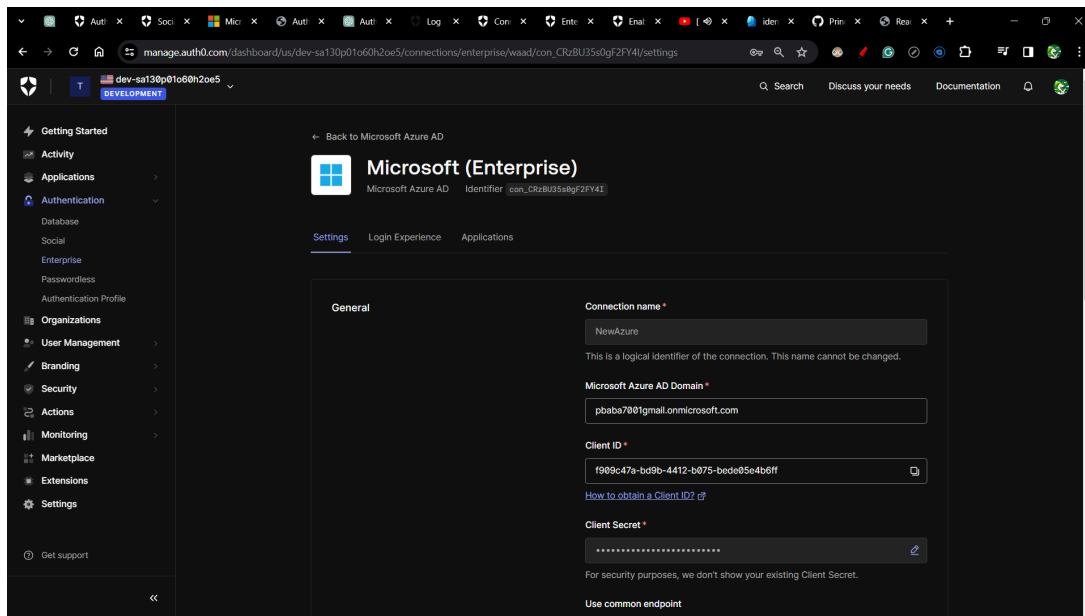
[Help me decide...](#)

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts, you can do so using the manifest editor. [Learn more about these restrictions.](#)

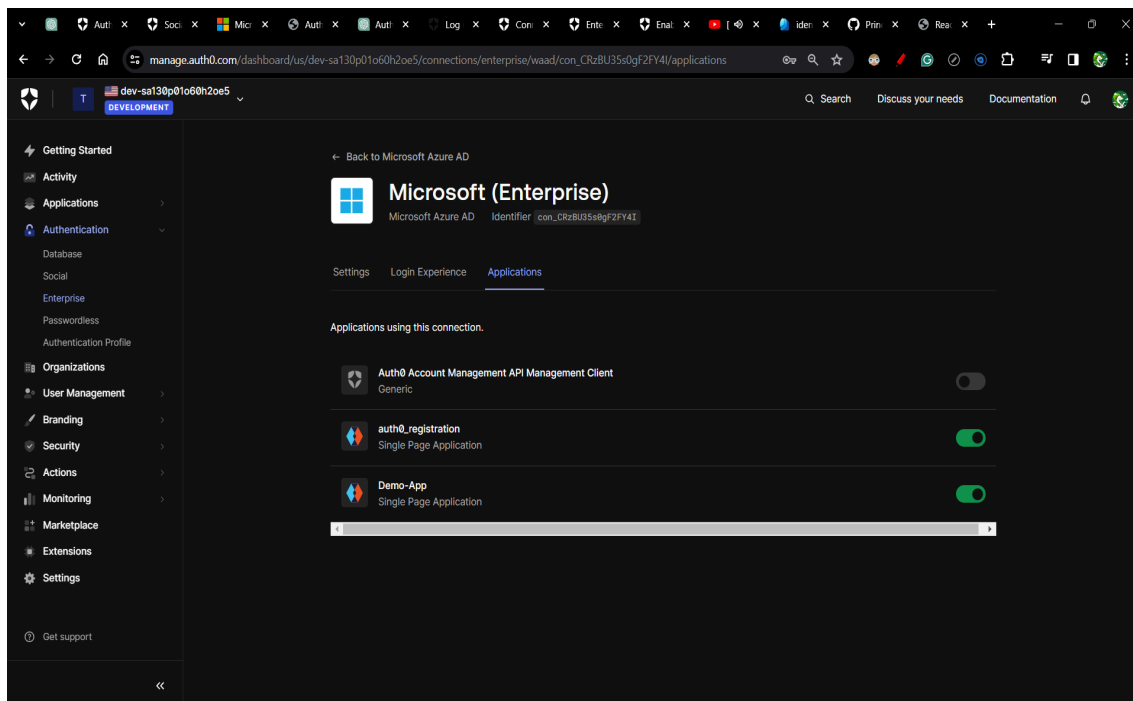
## ★ Configure Microsoft Identity in Auth0

Create and configure an Azure AD Enterprise Connection in Auth0. Make sure you have the Application (client) ID and the Client secret generated when you set up your app in the Microsoft Azure portal.

Navigate to **Auth0 Dashboard > Authentication > Enterprise**, and locate **Microsoft Azure AD**.

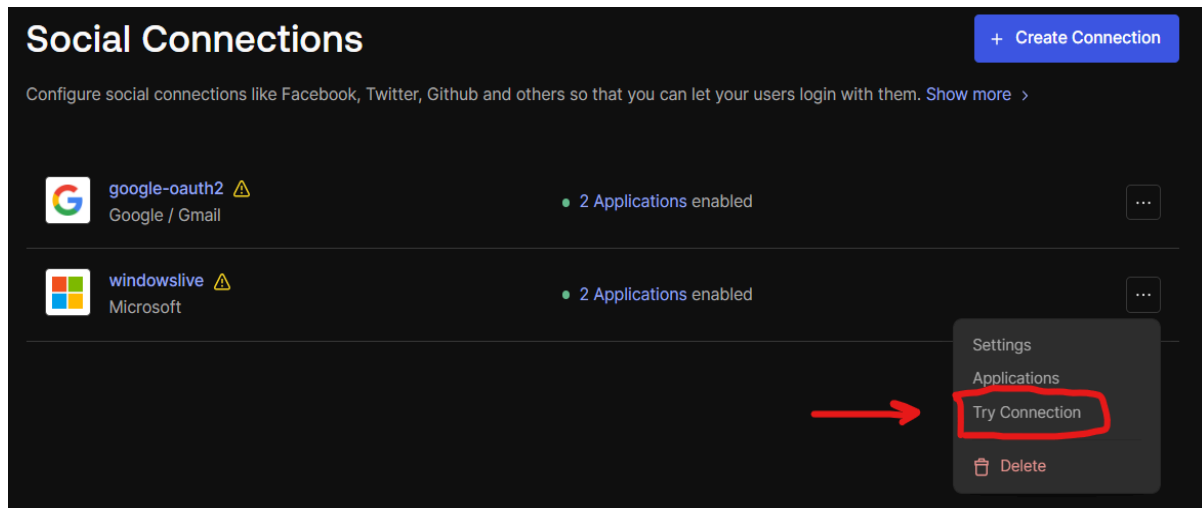


## Enable Connection

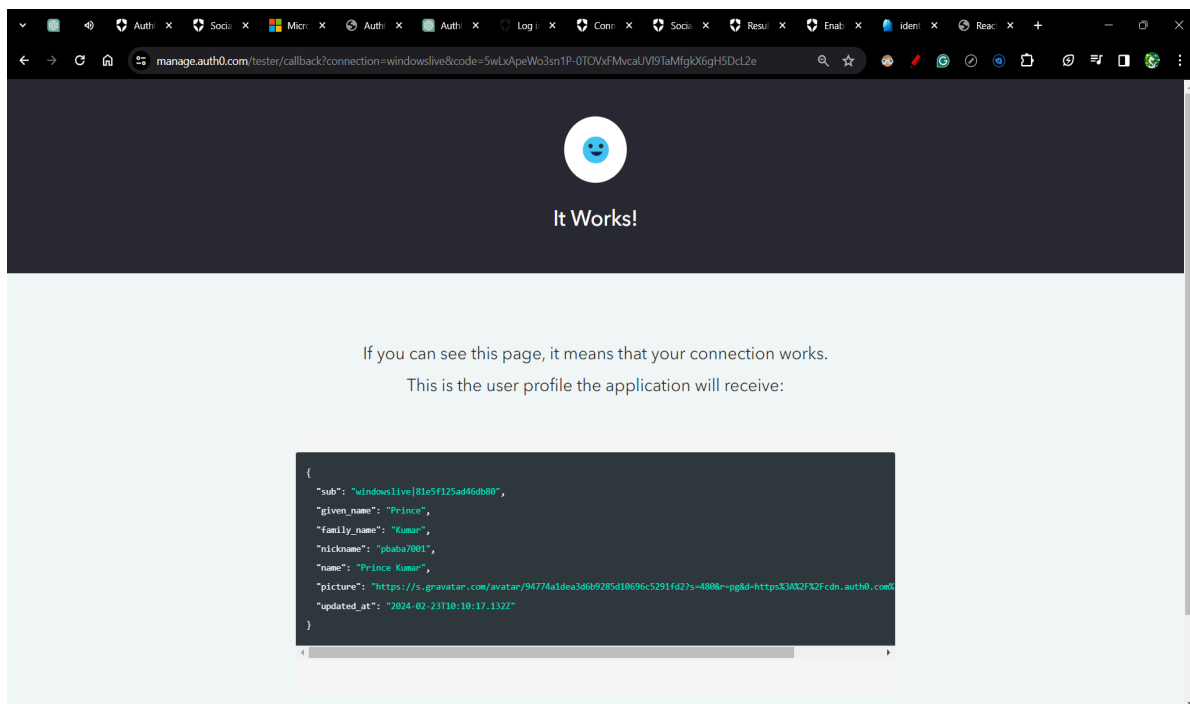


## 4. Test

Click on "Try Connection"



If it displays '**It works**' then your integration process has been completed **successfully**.



If the message "It works" is visible on the screen, it indicates that the integration process has been completed successfully. Users are then automatically redirected to the homepage, confirming that the system is functioning as intended.



**Integrating Auth0 with Microsoft Identity requires several steps to establish a smooth and secure authentication process. Below is a comprehensive guide outlining the necessary actions:**

**1. Create an Auth0 Account and Application:**

Sign up for an Auth0 account if you haven't already.

Within the Auth0 Dashboard, initiate the creation of a new application.

Make note of the Client ID and Client Secret provided by Auth0 for the designated application.

**2. Set Up Microsoft Identity in the Azure Portal:**

Access the Azure portal (<https://portal.azure.com/>) and log in.

Navigate to "Azure Active Directory" > "App registrations."

Generate a new app registration specific to your application.

Record the Application (client) ID, and Directory (tenant) ID, and generate a Client Secret.

**3. Configure Authentication Redirect URIs:**

Within the Azure portal, under your app registration, proceed to "Authentication."

Specify the Redirect URIs where Microsoft Identity will forward authentication responses. Ensure alignment with the callback URLs configured in Auth0.

**4. Configure Microsoft Identity in Auth0:**

Within the Auth0 Dashboard, access "Connections" > "Social" > "Microsoft."

Activate the Microsoft connection.

Input the Application (client) ID, Directory (tenant) ID, and Client Secret acquired from the Azure portal.

**5. Test the Connection:**

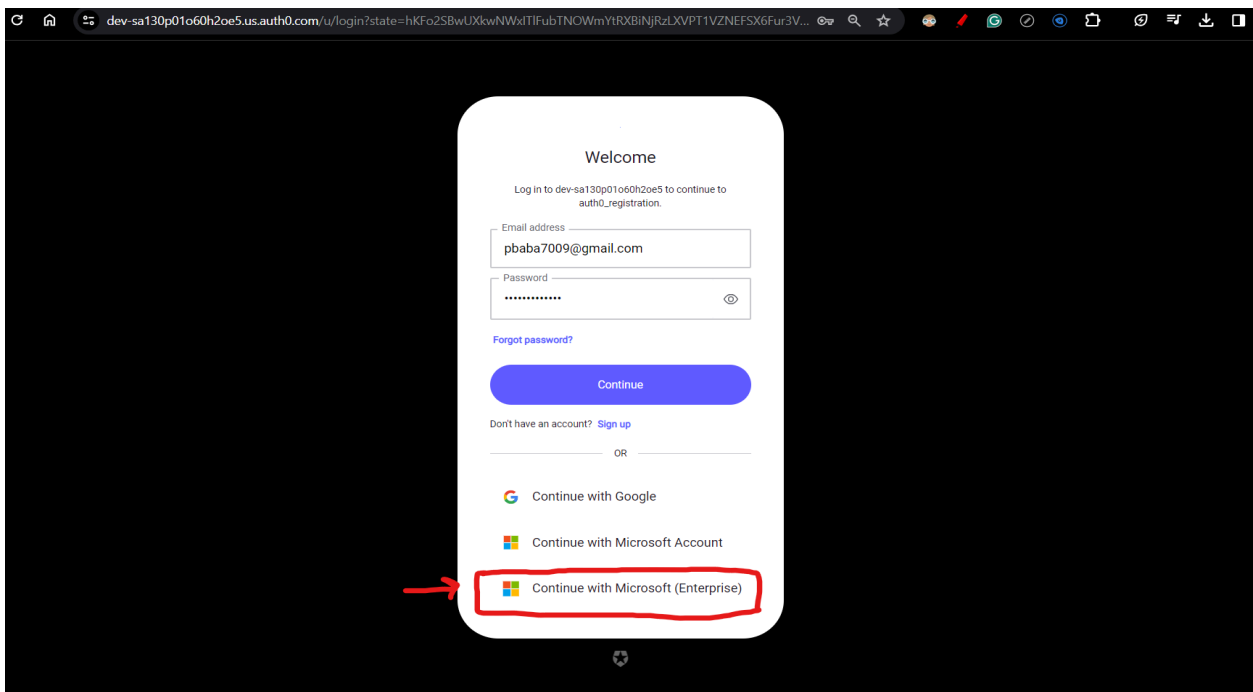
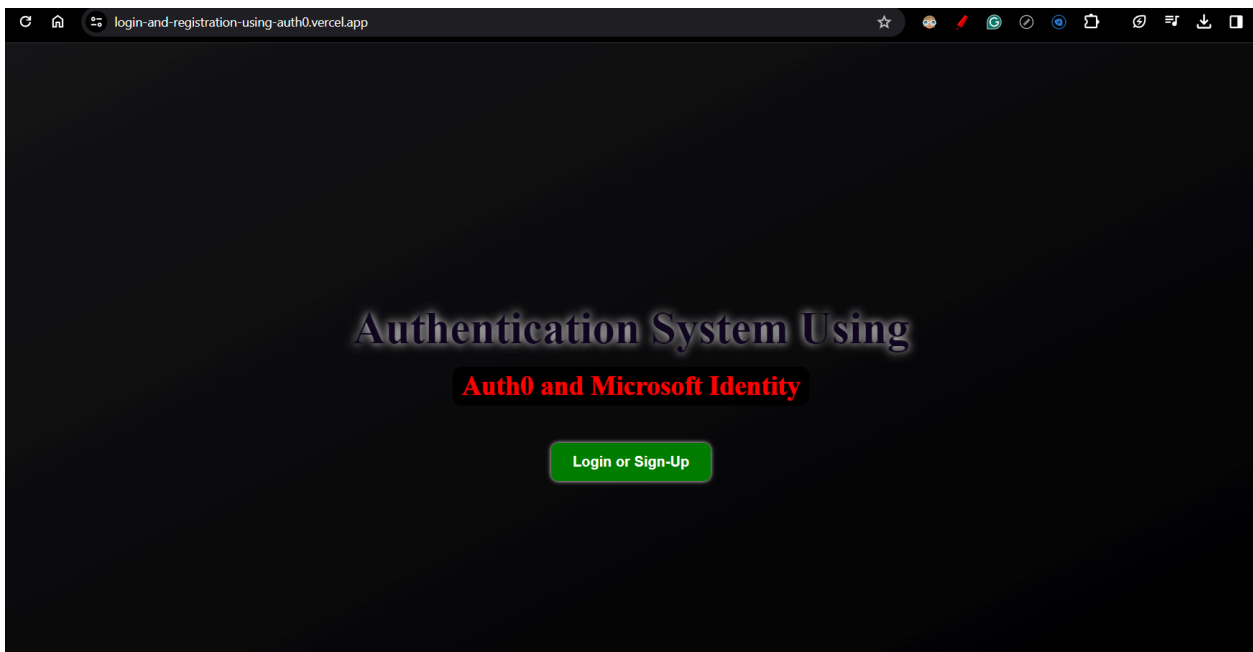
Utilize the Auth0 Dashboard to execute a test of the Microsoft connection to confirm successful integration.

Verify the accurate processing of authentication requests initiated by Auth0 through Microsoft Identity.

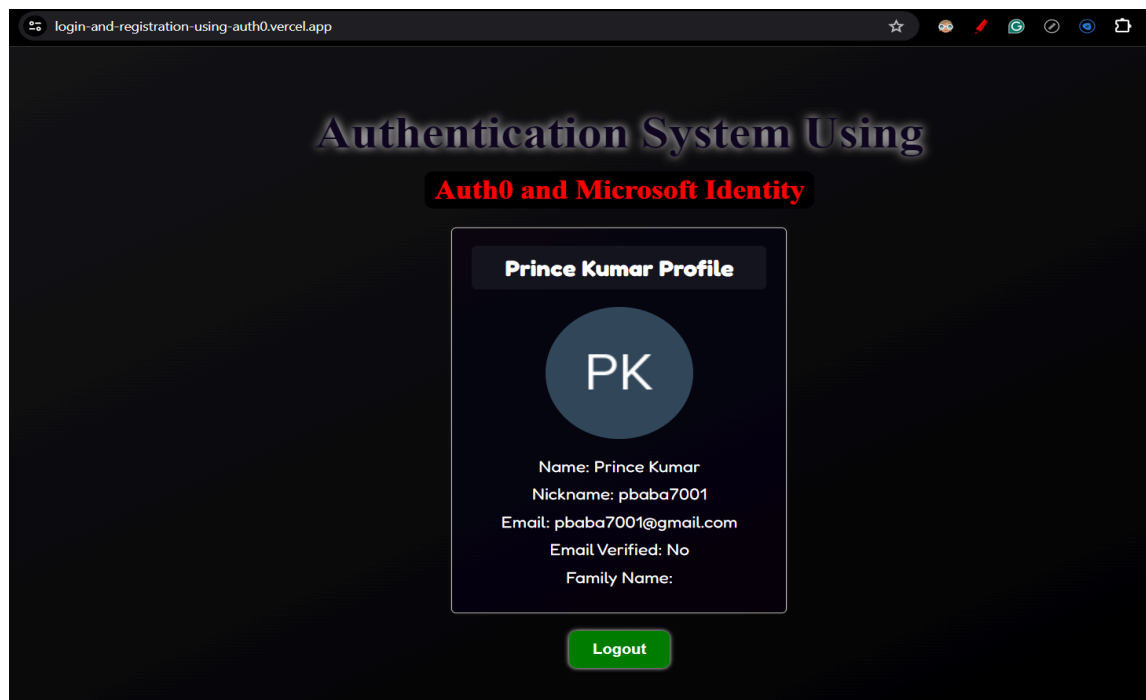
## 4. User Guide: Login and Registration Feature

### Logging In Steps:

1. Access the [login page](#) of the web application.
2. Click on the **"Login with Microsoft"** button.
3. You will be redirected to the Microsoft login page.
4. Enter your Microsoft credentials (email and password) and proceed with the authentication process.



5. Upon **successful authentication**, you will be redirected back to the web application and logged in automatically.



## 5. Code Setup

- Install SDK  
`npm install @auth0/auth0-react`
- Configure the Auth0Provider component

```
1  import React from 'react';
2  import { createRoot } from 'react-dom/client';
3  import { Auth0Provider } from '@auth0/auth0-react';
4  import App from './App';
5
6  const root = createRoot(document.getElementById('root'));
7
8  root.render(
9    <Auth0Provider
10      domain="dev-sa130p01o60h2oe5.us.auth0.com"
11      clientId="CHuoqSS2aRRBbGymav7Gf8IAVRV4Waa"
12      authorizationParams={{
13        redirect_uri: window.location.origin
14      }}
15    >
16      <App />
17    </Auth0Provider>,
18  );
```

# **Conclusion**

In conclusion, setting up Auth0 and Microsoft Identity for our web application's authentication is a major achievement. This ensures a secure and user-friendly authentication process. By using Auth0 as the main authentication provider and Microsoft Identity as the identity provider, we've created a straightforward authentication process that enhances security.

Our documentation provides developers with a useful guide, and the user guide simplifies navigation for end-users. During the live demo, we showcased the successful collaboration between Auth0 and Microsoft Identity. In summary, Auth0 and Microsoft Identity create a dependable authentication solution, laying the groundwork for a secure and user-friendly web application experience.

## **References:**

- Auth official Docs(<https://auth0.com/docs>)
- Microsoft Identity [Docs](#)