# Enable Microsoft Entra ID SSO for Open WebUI

To enable Microsoft Entra ID SSO, you'll need to:

1. Register an application in Microsoft Entra ID

2. Configure the application in Open WebUI

Here are the steps:

First, register your application in Microsoft Entra ID:

- Go to the Azure Portal (https://portal.azure.com)

- Navigate to Microsoft Entra ID

- Go to 'App registrations' and click 'New registration'

- Name your application (e.g., 'Open WebUI')

- Select 'Single tenant' for supported account types

- Add a redirect URI: https://your-domain/oauth/microsoft/callback

- Click 'Register'

- Note down the Application (client) ID and Directory (tenant) ID

- Go to 'Certificates & secrets' and create a new client secret

- Note down the client secret value

Next, configure Open WebUI with the Microsoft Entra ID credentials.

You'll need to set these environment variables:

## Environment Variables:

* MICROSOFT\_CLIENT\_ID="your-client-id"
* MICROSOFT\_CLIENT\_SECRET="your-client-secret"
* MICROSOFT\_CLIENT\_TENANT\_ID="your-tenant-id"
* MICROSOFT\_REDIRECT\_URI="https://your-domain/oauth/microsoft/callback"
* MICROSOFT\_OAUTH\_SCOPE="openid email profile"
* ENABLE\_OAUTH\_SIGNUP=true

Open Web Ui Frontend is running on - http://localhost:5173

Open Web Ui Backend is running on - <http://localhost:8080>

I see you are in the "Token configuration" section of your Microsoft Entra ID app registration, ready to add optional claims. This is exactly where you need to be to ensure the necessary user information is sent to Open WebUI. **To solve the "email or password incorrect" erro**r, you need to add claims that provide the user's email address and potentially their name to the tokens issued by Microsoft Entra ID

1. **Select Token type:** Choose **"ID"**. The ID token is primarily used for authentication and carries basic profile information about the user. The Open WebUI backend will use information from the ID token to identify and authenticate the user.
2. **Add Claims:** After selecting "ID", a list of available optional claims will appear. Select the following claims by checking the boxes next to them:

* **email**: This is the most important claim needed by Open WebUI to identify the user.
* **given\_name**: Recommended for the user's first name.
* **family\_name**: Recommended for the user's last name.

**3. Add Claim:** After selecting the desired claims, click the **"Add"** button at the bottom of the dialog.

**4.Save Configuration:** Once you've added the claims, make sure to **save** the Token configuration in the Azure portal (there's usually a "Save" button at the top or bottom of the "Token configuration" page).

# Fixing Redirect URL Mismatch in Open WebUI

If you navigate to http://localhost:3000 and the backend redirects your browser to http://localhost:3000/auth#token=..., but your Open WebUI frontend is not running on port 3000, this indicates a redirect URL mismatch.

## Issue

The backend is attempting to redirect the user to http://localhost:3000, which is incorrect. Based on earlier errors, the actual frontend is running on http://localhost:5173.

## Solution

To resolve this issue, you need to explicitly define the correct frontend URL in your .env file using the `WEBUI\_URL` environment variable.

### Add the following line to your .env file:

* WEBUI\_URL="http://localhost:5173"

Additionally, you should **configure a Logout redirect URI in your Microsoft Entra ID App Registration**:

1. Go to the Azure Portal (portal.azure.com).
2. Navigate to Microsoft Entra ID -> App registrations -> Your Open WebUI application.
3. In the left menu, click on "Authentication".
4. Under "Platform configurations", select your "Web" platform.
5. Under "Logout redirect URIs", add the URL where you want Microsoft Entra ID to redirect the user after they are logged out of Microsoft. A common practice is to redirect back to your Open WebUI login page. Using your frontend URL:

<https://localhost:5173/auth>

6. Add and Confirm the OPENID\_PROVIDER\_URL in your .env file is correct and matches the format https://login.microsoftonline.com/<YOUR\_TENANT\_ID>/v2.0/.well-known/openid-configuration.

Eg;-

MICROSOFT\_CLIENT\_ID="a9a49955-16ce-4088-b15a-8dbd9b791db8"

MICROSOFT\_CLIENT\_SECRET=".ob8Q~0Mf~ljiwUJnyuEkTxIVvNLc\_zGluU6kcim"

MICROSOFT\_CLIENT\_TENANT\_ID="204d80f2-f55b-417f-9b65-13572d18a2b1"

MICROSOFT\_REDIRECT\_URI="http://localhost:8080/oauth/microsoft/callback"

MICROSOFT\_OAUTH\_SCOPE="openid email profile"

OAUTH\_USERNAME\_CLAIM="sub"

OAUTH\_EMAIL\_CLAIM="sub"

ENABLE\_OAUTH\_SIGNUP=true

WEBUI\_URL="http://localhost:5173"

OPENID\_PROVIDER\_URL="https://login.microsoftonline.com/204d80f2-f55b-417f-9b65-13572d18a2b1/v2.0/.well-known/openid-configuration"