**Azure AD Authentication Flow**

1. Overview

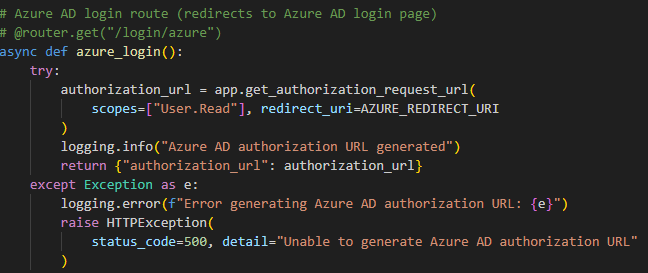
This document describes the Azure AD OAuth2 authentication flow, where the frontend URL is configured as the redirect URI. The backend processes the authorization code received from the frontend to handle token exchange, user authentication, and session creation. The flow involves key API endpoints on both the frontend and backend.

1. Authentication Flow

**Step-by-Step Process**

1. User Initiates Login

* The frontend makes a request to the backend to generate an Azure AD authorization URL.
* The backend responds with the authorization URL containing the necessary parameters (e.g., client ID, redirect URI, scopes).
* The frontend redirects the user to Azure AD for authentication.



1. Azure AD Handles Authentication

* Azure AD validates the user’s credentials and requested permissions.
* Upon successful authentication, Azure AD redirects the user to the frontend with an authorization code in the query string.

Example Redirect:

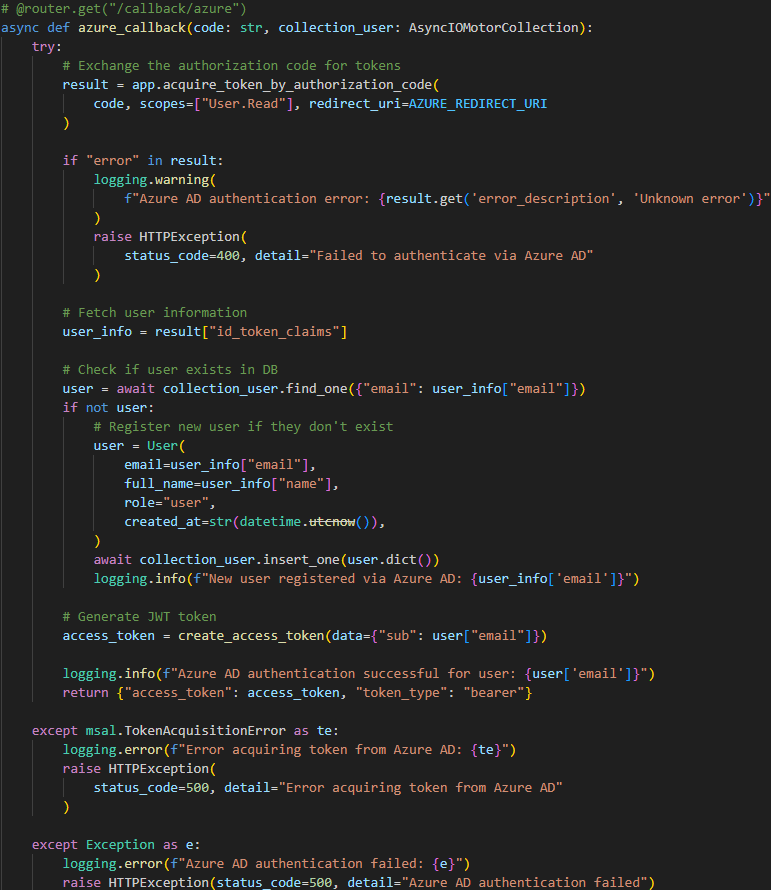
**https://frontend-url?code=AUTHORIZATION\_CODE**

1. Frontend Handles Redirect

* The frontend extracts the authorization code from the query string.
* It makes a secure request to the backend, sending the authorization code for further processing.

1. Backend Exchanges Code for Tokens

* The backend receives the authorization code and exchanges it for tokens (e.g., access token, ID token, refresh token) using Azure AD’s token endpoint.
* It extracts user information (e.g., email, name) from the ID token.



1. Backend Registers or Authenticates the User

* The backend checks whether the user exists in the database:
  + If the user exists, their details are updated if necessary.
  + If the user doesn’t exist, they are registered as a new user.
* A JWT token is generated for the user and sent back to the frontend.

1. Frontend Completes Login Process

* The frontend securely stores the JWT token (e.g., in httpOnly cookies or secure local storage).
* The user is now authenticated and can access protected resources.

1. Key API Endpoints

**Backend**

* Authorization URL Endpoint:

Handles requests from the frontend to generate the Azure AD authorization URL.

* Token Exchange Endpoint:

Receives the authorization code from the frontend, exchanges it for tokens, and handles user registration or authentication.

**Frontend**

* **Redirection to Azure AD:**

Redirects the user to Azure AD using the URL provided by the backend.

* Redirect Handling:

Extracts the authorization code from Azure AD’s response and sends it to the backend for processing.

1. Conclusion

This document describes an Azure AD authentication flow where the frontend URL is used for redirection, and the backend handles token exchange and user session management. The process ensures secure handling of user credentials and tokens while maintaining a separation of concerns between the frontend and backend.