**SOBERNESS SERVER-SIDE DOCUMENTATION**

**Authentication APIs**

**Sign Up (Create a new user account)**

* URL: /signup
* Method: POST
* Request Body:
  + email (string, required): The email address of the user.
  + password (string, required): The password for the user account.
* Responses:
  + 201 Created: User account created successfully.
  + 400 Bad Request: User already exists.
  + 500 Internal Server Error: Signup failed.

**Login**

**Authenticate a user and generate a JSON Web Token (JWT).**

* URL: /login
* Method: POST
* Request Body:
  + email (string, required): The email address of the user.
  + password (string, required): The password for the user account.
* Responses:
  + 200 OK: Login successful. Returns a JWT in the response body.
  + 401 Unauthorized: Invalid password.
  + 404 Not Found: User not found.
  + 500 Internal Server Error: Login failed.

**Reset Password**

**Reset a user's password and send the new password via email.**

* URL: /reset-password
* Method: POST
* Request Body:
  + email (string, required): The email address of the user.
* Responses:
  + 200 OK: Password reset email sent successfully.
  + 404 Not Found: User not found.
  + 500 Internal Server Error: Password reset failed.

**Protected Routes**

**These routes require a valid JSON Web Token (JWT) in the Authorization header for authentication**.

Protected Route

Access a protected route that requires authentication.

* URL: /protected-route
* Method: GET
* Headers:
  + Authorization (string, required): The JWT token received during login.
* Responses:
  + 200 OK: Access to the protected route granted.
  + 401 Unauthorized: Invalid or missing token.