USER DOCUMENTATION-SSO System with Kong API Gateway

This SSO implementation provides authentication through **Google Workspace SAML**, with all requests routed through **Kong API Gateway**. All requests must be sent through Kong at:

`http://localhost:8000`

Authentication Flow

These endpoints control the user login and logout process.

1. Initiate Authentication

`GET /auth`

Description: Initiates the SAML authentication flow with Google Workspace. This is the primary entry point for logging in. Kong and the backend services handle the redirects to and from Google. Upon successful authentication, the user is redirected back to the page they were originally trying to access.

Example:
To log in, direct the user's browser to:
`http://localhost:8000/auth`

2. Logout

`GET /custom-logout`

Description: Logs the user out by invalidating the backend session and clearing authentication cookies from the browser.

Request Parameters:

- `redirect_to` (optional): The full URL to redirect the user to after logout is complete. Defaults to the root of the application (`http://localhost:8000`).

Example:
`http://localhost:8000/custom-logout?redirect_to=http://localhost:8000/app2`

Response: Redirects the user to the specified `redirect_to` URL and clears authentication cookies.

Protected API Endpoints

1. User Information

`GET /api/userinfo`

Description: Returns the claims and details for the currently authenticated user. This is the standard way for a frontend application to verify if a user is logged in and get their identity.

Response Body (200 OK):

```
{
  "sub": "user@example.com",
  "email": "user@example.com",
  "name": "User Name",
  "authenticated": true
}
```

Error Response (401 Unauthorized):

```
{
  "error": "Not authenticated"
}
```

Frontend Applications & Protected Routes

These frontend routes require a valid `access_token` cookie. If a user is not authenticated, Kong will automatically redirect them through the `/auth` flow and return them to their originally requested page upon success.

Main Application

- `GET /` - The public home page.
- `GET /profile` - **Protected route**. Displays the user's profile.
- `GET /dashboard` - **Protected route**. Displays the main application dashboard.

Second Application

- `GET /app2` - The public entry point for the second application.
- `GET /app2/dashboard` - **Protected route**. Displays the second app's dashboard.
- `GET /app2/settings` - **Protected route**. Displays the second app's settings page.