Using Authentication Token

After Sign up / Sign in, a new token is generated. Token will be expired in 2 weeks Token information are stored in HEADER in response and should be passed as HEADERS for each request

Token Header Format

The headers follow the RFC 6750 Bearer Token format: Authentication headers example:

```
"access-token": "wwwww",
"client":      "xxxxx",
"expiry":      "yyyyy",
"uid":        "zzzzz"
```

The authentication headers consists of the following params:

param	description
access-token	This serves as the user's password for each request. A hashed version of this value is stored in the database for later comparison. This value should be changed on each request.
client	This enables the use of multiple simultaneous sessions on different clients. (For example, a user may want to be authenticated on both their phone and their laptop at the same time.)
expiry	The date at which the current session will expire. This can be used by clients to invalidate expired tokens without the need for an API request.
uid	A unique value that is used to identify the user. This is necessary because searching the DB for users by their access token will make the API susceptible to timing attacks.

The authentication headers required for each request will be available in the response from the previous request.