

User Authentication API Guide

This document provides a basic guide for integrating and using the User Authentication API.

Base URL

```
https://api.example.com/v1/auth
```

Endpoints

1. Register User

POST /register

Create a new user account.

```
POST /register
Content-Type: application/json
{
  "username": "johndoe",
  "email": "john@example.com",
  "password": "yourPassword123"
}
```

2. Login User

POST /login

Authenticate an existing user and receive a token.

```
POST /login
Content-Type: application/json
{
  "email": "john@example.com",
  "password": "yourPassword123"
}
```

3. Get Profile

GET /profile

Retrieve authenticated user's profile. *Requires Bearer token.*

```
GET /profile
Authorization: Bearer <token>
```

4. Logout

POST /logout

Invalidate the current session token.

```
POST /logout
Authorization: Bearer <token>
```

Response Example

```
{
  "status": "success",
  "message": "Authenticated successfully.",
  "data": {
    "token": "eyJhbGciOiJIUzI1..."
  }
}
```

Errors

- **400 Bad Request:** Invalid input.
- **401 Unauthorized:** Authentication failed.
- **404 Not Found:** Resource does not exist.

Notes

- All endpoints require HTTPS.
- Use the received token in the Authorization header for protected routes.