OAuth 2.0 Authentication API Documentation

Overview

This API uses OAuth 2.0 for authentication and authorization, allowing secure access to protected resources.

Base URL

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

Authorization Endpoint

```
GET /oauth/authorize
```

Parameters

Parameter	Type	Description	Required
response_type	string	Must be `code`.	Yes
client_id	string	Client identifier.	Yes
redirect_uri	string	Registered redirect URI.	Yes
scope	string	Requested scopes (space-separated).	No
state	string	CSRF token for validation.	No

Token Endpoint

```
POST /oauth/token
```

Parameters (x-www-form-urlencoded)

Parameter	Type	Description	Required
grant_type	string	Should be `authorization_code`.	Yes
code	string	Authorization code received from /authorize.	Yes
redirect_uri	string	Registered redirect URI.	Yes
client_id	string	Client identifier.	Yes
client_secret	string	Client secret.	Yes

Token Response

```
{
  "access_token": "string",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "string",
  "scope": "read write"
}
```

Scopes

- `read` : Read access to resources
- `write` : Write access to resources

Error Response

```
{
  "error": "invalid_request",
  "error_description": "Missing parameter: code"
}
```

Example Flow

1. Redirect user to `/oauth/authorize` with required parameters.
2. User authorizes the application.
3. Receive authorization `code` at the registered `redirect_uri` .
4. Exchange code for tokens via `/oauth/token` .
5. Use `access_token` to authenticate requests to protected APIs.