

AutoDBA Web – API Contract

1. Overview

This document defines the REST API interface used in the AutoDBA Web MVP. It includes all endpoints related to authentication, database connection, and audit execution. All protected endpoints require a valid JWT token in the Authorization header.

2. Authentication Endpoints

POST /signup

- Description: Create a new user account.

- Request Body:

```
{  
  "email": "user@example.com",  
  "password": "securePassword"  
}
```

- Response: 201 Created or 409 Conflict (email already registered)

POST /login

- Description: Authenticate a user and return a JWT.

- Request Body:

```
{  
  "email": "user@example.com",  
  "password": "securePassword"  
}
```

- Response: 200 OK with JSON { token: "<JWT>" }, or 401 Unauthorized

3. Database Connection Endpoint

POST /connect-db

- Description: Validate the provided MySQL database credentials.

- Headers: Authorization: Bearer <token>

- Request Body:

```
{  
  "host": "hostname",  
  "port": 3306,  
  "database": "dbname",  
  "user": "dbuser",  
  "password": "dbpass"  
}
```

- Response:

- 200 OK with connection metadata (e.g. table list)

- 403 Forbidden / 500 Internal Error on failure

4. Audit Execution Endpoint

POST /audit

- Description: Run all audit modules and return the results.

- Headers: Authorization: Bearer <token>

- Request Body: {}

- Response:

```
{  
  "schema": { ... },  
  "indexes": { ... },  
  "constraints": { ... }
```

}

- Status Codes:

- 200 OK (success)
- 207 Multi-Status (some modules failed)
- 500 Internal Server Error (fatal error)

5. Authorization

- All protected routes require a JWT token.

- Header format:

Authorization: Bearer <JWT>

- JWT includes user ID and expiration timestamp.

- Backend uses middleware `verifyToken.js` to authenticate requests.

6. Error Handling

Error Codes Used:

- 400 Bad Request: Missing or malformed input
- 401 Unauthorized: Invalid or missing token
- 403 Forbidden: Access denied (e.g. DB connection failure)
- 404 Not Found: Resource not found
- 409 Conflict: Duplicate signup email
- 500 Internal Server Error: Unexpected server-side error
- 207 Multi-Status: Some audit modules failed but others succeeded