Grade Management API

Base URL

- `http://localhost:8001/api`

Auth

- Login returns a JWT token.
- For protected routes, send header: `Authorization: Bearer <token>`.
- `requireAdmin()` is used for admin-only endpoints.
- `requireUser()` is used for any logged-in user (admin or teacher).

Conventions

- Dates use `YYYY-MM-DD`.
- For PATCH/PUT/POST bodies, send `Content-Type: application/json`.
- IDs are integers unless noted otherwise.

Main

GET `/api`

- Purpose: initialize connection, quick welcome.
- Auth: none.
- Response:

```
{
  "message": "Welcome to the Grade Management System API.",
  "note": "Connection initialized! Login & check status.",
  "status": "https://localhost:8001/api/status."
}
```

GET `/api/status`

- Purpose: server + DB status.
- Auth: admin.

POST `/api/reset-database`

- Purpose: drop and recreate schema.
- Auth: admin.

POST `/api/update-database-schema`

- Purpose: apply schema updates.
- Auth: admin.

POST `/api/seed-database`

- Purpose: seed deterministic data.
- Auth: admin.

Auth

POST `/api/login`

- Purpose: login and get JWT.
- Auth: none.
- Body:

```
{
  "staff_id": "A-0001",
  "password": "password"
}
```

- Response:

```
{
  "token": "JWT_TOKEN"
}
```

Users / Staff (Admin)

`GET` `/api/users` or `/api/staff`

- Purpose: list all users.
- Auth: admin.

`GET` `/api/users/{id}`

- Purpose: get user by `user_id`.
- Auth: admin.

`GET` `/api/staff/{staff_id}`

- Purpose: get user by staff id.
- Auth: admin.

`POST` `/api/users` or `/api/staff`

- Purpose: create user.
- Auth: admin.
- Body:

```
{
  "staff_id": "T-1A",
  "password": "password",
  "first_name": "Teacher",
  "last_name": "User",
  "role_id": 2,
  "assigned_class_id": 1,
  "is_active": true
}
```

`PUT` `/api/users/{id}`

- Purpose: full update of a user.
- Auth: admin.
- Body: any fields from create (password will be re-hashed).

`DELETE` `/api/users/{id}`

- Purpose: delete user.
- Auth: admin.

Profile (Logged-in User)

`PUT` `/api/profile`

- Purpose: update own profile (admin or teacher).
- Auth: logged-in user.
- Allowed fields: `first_name`, `last_name`, `password`.
- Body:

```
{
  "first_name": "Jane",
  "last_name": "Doe",
  "password": "new-password-123"
}
```

Students (Admin)

`GET` `/api/students`

- Purpose: list students.
- Auth: admin.

`GET` `/api/students/{id}`

- Purpose: get student by `student_id`.
- Auth: admin.

`GET` `/api/students/number/{student_number}`

- Purpose: get student by student number.
- Auth: admin.

`GET` `/api/students/class/{class_id}`

- Purpose: list students in class.
- Auth: admin.

POST `/api/students`

- Purpose: add student.
- Auth: admin.
- Body:

```
{
  "student_number": "S-1A-3",
  "first_name": "Student3",
  "last_name": "Class1A",
  "class_id": 1,
  "is_active": true
}
```

PUT `/api/students/{id}`

- Purpose: update student.
- Auth: admin.
- Body: any student fields.

DELETE `/api/students/{id}`

- Purpose: soft delete (sets `is_active` to 0).
- Auth: admin.

Classroom (Admin)

GET `/api/classrooms/{id}`

- Purpose: get classroom by `class_id`.
- Auth: admin.

GET `/api/classrooms/year-grade?year=2026&grade=1`

- Purpose: list classrooms for a grade (year is validated).
- Auth: admin.
- Query params: `year`, `grade`.

GET `/api/classrooms/{id}/students`

- Purpose: list students for a classroom.
- Auth: admin.

POST `/api/classrooms`

- Purpose: add classroom.
- Auth: admin.
- Body:

```
{
  "grade_id": 1,
  "class_name": "1G"
}
```

PUT `/api/classrooms/{id}`

- Purpose: update classroom.
- Auth: admin.
- Body: `grade_id`, `class_name` (either or both).

Year (Admin)

GET `/api/years/{id}`

- Purpose: get academic year by id.
- Auth: admin.

POST `/api/years`

- Purpose: create academic year.
- Auth: admin.
- Body:

```
{
  "year_label": 2027,
  "start_date": "2026-09-01",
  "end_date": "2027-06-30",
  "is_active": true
}
```

PUT `/api/years/{id}`

- Purpose: update academic year.
- Auth: admin.
- Body: any of `year_label`, `start_date`, `end_date`, `is_active`.

Scores (Logged-in User)

GET `/api/students/{studentId}/scores/{yearLabel}`

- Purpose: get a student's scores for a year.
- Auth: logged-in user.

GET `/api/classes/{classId}/terms/{termId}/scores`

- Purpose: get class scores for a term.
- Auth: logged-in user.

POST `/api/students/{studentId}/scores/{yearLabel}/terms/{termNumber}`

- Purpose: add scores for a student + term.
- Auth: logged-in user (teacher_user_id from token).
- Body:

```
{
  "scores": [
    { "subject_id": 1, "score_value": 78 },
    { "subject_id": 2, "score_value": 84 }
  ]
}
```

PUT `/api/students/{studentId}/scores/{yearLabel}/terms/{termNumber}`

- Purpose: update scores for a student + term (upsert).
- Auth: logged-in user.
- Body: same as POST.

Reports (Logged-in User)

GET `/api/reports/student`

- Purpose: student report for a year/term.
- Auth: logged-in user.
- Query params:
  - required: `year`, `term`
  - optional: `grade`, `class`, `student`
- Example: `/api/reports/student?year=2026&term=1&grade=6&class=31&student=61`

GET `/api/reports/subject`

- Purpose: subject report average for year/term/grade/subject.
- Auth: logged-in user.
- Query params: `year`, `term`, `grade`, `subject`
- Example: `/api/reports/subject?year=2026&term=1&grade=1&subject=1`
- Response:

```
{
  "message": "Subject report generated",
  "data": {
    "subject_name": "Math",
    "average": 73.42,
    "params": {
      "year": "2026",
      "term": "1",
      "grade": "1",
      "subject": "1"
    }
  }
}
```