**Step 13: Test It**

1. Register a user with role "Admin":

arduino

CopyEdit

POST /api/auth/register

{

"username": "adminuser",

"password": "adminpass",

"role": "Admin"

}S

1. Login to get a token:

bash

CopyEdit

POST /api/auth/login

{

"username": "adminuser",

"password": "adminpass"

}

1. Call the protected route:

sql

CopyEdit

GET /api/protected/admin-only

Headers:

Authorization: Bearer <your\_token\_here>

You should see:

json

CopyEdit

{ "message": "Welcome Admin! You have access to this route." }

Try changing the role to Finance or Vendor and you’ll see 403 Forbidden.

✅ **You now have:**

* authMiddleware to verify JWT
* roleMiddleware to restrict routes by user role

**🔜 Next Steps:**

Shall we now implement **Product → Phase → Task models and their APIs**, starting with Products (admin-only create/delete/view)?

Or do you want to add **file upload for tasks** first?

4o

**You said:**

What should be the GET /api/protected/admin-only Headers: Authorization: Bearer <your\_token\_here>

**ChatGPT said:**

To call the protected route /api/protected/admin-only, your request must include an **Authorization header** in this format:

makefile

CopyEdit

Authorization: Bearer <your\_token\_here>

Here's how to do it:

**✅ Example Request (Using curl)**

bash

CopyEdit

curl -X GET http://localhost:5000/api/protected/admin-only \

-H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9..."

Replace the token with the actual JWT you received after logging in.

**✅ Example Request (Using Postman or Thunder Client)**

1. **Method**: GET
2. **URL**: http://localhost:5000/api/protected/admin-only
3. **Headers**:

makefile

CopyEdit

Key: Authorization

Value: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...

**🔐 Where does <your\_token\_here> come from?**

After you POST to /api/auth/login, you’ll get a response like this:

json

CopyEdit

{

"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",

"user": {

"username": "adminuser",

"role": "Admin"

}

}

Copy that token value and use it in the Authorization header.

**Test the API**

1. **POST /api/products**  
   Create a product (Admin only)

json

CopyEdit

{

"name": "Smart Watch V3"

}

1. **GET /api/products**  
   Get all products
2. **DELETE /api/products/:id**  
   Delete a product by ID (Admin only)

Include the Authorization: Bearer <token> header for all these routes.

## ✅ API Summary

| **Endpoint** | **Method** | **Description** | **Access** |
| --- | --- | --- | --- |
| /api/phases/ | POST | Create phase under a product | Admin only |
| /api/phases/:id | DELETE | Delete phase by ID | Admin only |
| /api/phases/product/:productId | GET | Get all phases under a product | All roles |

## ✅ Behavior Summary

| **Scenario** | **Phase Status** |
| --- | --- |
| All tasks = Completed | Phase → Completed |
| Any task = Ongoing | Phase → Ongoing |

## Behavior Summary

| **Condition** | **Product Status** |
| --- | --- |
| All Phases Completed | ✅ Completed |
| Any Phase Ongoing or New Phase Added | 🔄 Ongoing |

**Part 2: Approval Workflow**

**Logic:**

* Task has needsApproval: true/false
* Finance/Vendor can trigger Ask for Approval
* Admin can Approve if asked