| [**https://grok.com/chat/4e8f2759-da6f-4648-8322-3290d2d8a4e9**](https://grok.com/chat/4e8f2759-da6f-4648-8322-3290d2d8a4e9) | **Endpoint** | **Mô tả** | **Body (nếu có)** |
| --- | --- | --- | --- |
| POST | /api/v1/users | Tạo user mới | { "email": "...", "password": "...", "role": "...", "reference\_id": "..." } |
| GET | /api/v1/users | Lấy tất cả users | Không |
| GET | /api/v1/users/:id | Lấy user theo ID | Không |
| PUT | /api/v1/users/:id | Cập nhật user | { "email": "...", "password": "...", ... } |
| DELETE | /api/v1/users/:id | Xóa user theo ID | Không |

**a. API đầy đủ**

* **User Management**:

- Đăng ký (POST /register). <https://be-polika.onrender.com/api/v1/register> // Chỉ admin mới có thể tạo user

- Đăng nhập (POST /login) với JWT. <https://be-polika.onrender.com/api/v1/login> // Không yêu cầu auth để user có thể đăng nhập

- Cập nhật thông tin (PUT /api/users/:id). <https://be-polika.onrender.com/api/v1/users/:id> // Chỉ user đó hoặc admin mới có thể cập nhật thông tin user

- Xóa người dùng (DELETE /api/users/:id). https://be-polika.onrender.com/api/v1/users/:id

- Get toàn bộ user : <https://be-polika.onrender.com/api/v1/users> -- Chỉ có Admin mới được xem toàn bộ USER

- Get 1 user theo ID: <https://be-polika.onrender.com/api/v1/users>/:ID

* **Service Request**:
  + Tạo yêu cầu (POST /api/service-requests).
  + Lấy danh sách yêu cầu (GET /api/service-requests).
  + Cập nhật trạng thái (PUT /api/service-requests/:id).
* **Product Management**:
  + Thêm sản phẩm (POST /api/products).
  + Lấy sản phẩm (GET /api/products).
  + Cập nhật/giảm giá (PUT /api/products/:id).
* **Notification**:
  + Gửi thông báo qua email (sử dụng nodemailer từ config/mail.js).
  + Lưu thông báo trong database (notification.js).

https://github.com/mrkhangthanh/BE-POLIKA

bạn hãy đi sâu vào trong từng file trong thư mục phân tích xem tôi cần thêm những gì ?

tổng quan dự án của tôi :

- chức năng chính : khách hàng có thể tạo đơn gửi lên website và thông báo tới các thợ sử chữa. Đơn khách hàng tạo sẽ được hiển thị và thông báo với tài khoản của thợ có đơn mới để thợ nào rảnh có thể vào nhận đơn.

- ngoài ra có chức năng như chát. khách hàng có thể chát với thợ. thợ có thể chát với admin, khách hàng có thể chát với admin quản trị website.

- website còn tích hợp thêm chức năng thương mại điện tử.

ngoài ra còn có những bài viết new post các bài viết như báo điện tử

mrkhangthanh – Khang1904@14 monggo atlast

**bạn còn nhớ các tính năng dự án của tôi chứ. đây là các tính năng mà tôi đã gửi bạn**

**chức năng của website fontend và backend của tôi.**

**- đây là trang web mà tôi kết hợp cả thương mại điện tử, và có một tính năng nổi bất nhất trên trang là tạo đơn để tài khoản của thợ sửa chữa hay những tài khoản này nhận được các thông báo đơn của khách hàng tạo có thể ấn nhận đơn hoặc không.**

**Có nghĩa là tôi cần có :**

**- tài khoản admin (sau khi đăng nhập sẽ hiện trang dashboard- có tất cả các quyền. Thêm sửa xóa của tất cả các user và nhiều chức năng theo dõi khác.)**

**- tài khoản quản lý chỉ được xem mà không được sửa, xóa. Thao tác được Và không thao tác được một vài chức năng.**

**- tài khoản viết content cho phần news – post**

**- tài khoản của thợ sửa chữa – có thể xem được các đơn hàng đúng với ngành nghề của thợ đó**

**- tài khoản của khách hàng (khách hàng có thể tự đăng ký tài khoản trên trình duyệt bằng cách ấn vào nút đăng ký.**

**Tôi quên mất là tôi cần có thêm một Tài khoản đại lý. Để sau này tài khoản đại lý này có thể xem được các thông tin mà các khách hàng đã đăng ký dưới link đại lý đó, và tài khoản đại lý đó có thể liệt kê danh sách được một vài thông tin cơ bản của khách hàng này. Ngoài ra có thể xem được tổng số đơn hàng mà khách của đại lý lên đơn . Bây giờ tôi cần chỉnh sửa phần nào trong code dự án hiện tại của tôi một cách đơn giản hiệu quả để sau này tôi có thể mở rộng hơn**

**https://github.com/mrkhangthanh/BE-POLIKA vui lòng xem lại toàn bộ code hiện tại của tôi trong thư mục**

**Cần làm tiếp**

* Triển khai nhắn tin thời gian thực với socket.io.
* Thêm refresh token.
* Thêm bảo mật (rate limiting).
* Thêm thống kê cho admin.
*  Thêm xác thực cho Socket.IO.
*  Cải thiện CORS và thêm refresh token.

**Cần cải thiện**:

* **Socket.IO chưa có xác thực**: Bất kỳ client nào cũng có thể kết nối. Nên thêm middleware xác thực token.
* **CORS chưa linh hoạt**: Chỉ cho phép origin http://localhost:3000. Nên hỗ trợ nhiều origin cho production.
* **Thiếu middleware xử lý lỗi chung**: Nếu có lỗi xảy ra trong các route, server không trả về response thống nhất.
* **Thiếu xử lý lỗi khi server không khởi động được**: Nếu port bị chiếm dụng, server sẽ crash mà không có thông báo rõ ràng.

**Cần cải thiện**:

* **Thiếu API đăng ký cho khách hàng**: Bạn yêu cầu khách hàng có thể tự đăng ký tài khoản, nhưng chưa có API /register.
* **Phân quyền chưa linh hoạt**: Middleware requireRole chỉ kiểm tra một vai trò duy nhất. Nên hỗ trợ nhiều vai trò (ví dụ: cả admin và manager).
* **Thiếu API cho các tính năng khác**: Chưa có API cho quản lý đơn hàng, nhắn tin, bài viết.
* **Cập nhật user chưa đầy đủ**: Chưa xử lý cập nhật address và specialization (dành cho customer và technician).
*  **Kiểm tra trạng thái user**: Chưa kiểm tra user.status (nếu user bị inactive, vẫn cho phép truy cập).
*  **Thiếu refresh token**: Token hết hạn sau 1 giờ, nên thêm refresh token để cải thiện trải nghiệm người dùng.
*  **Chỉ hỗ trợ một vai trò**: Không hỗ trợ nhiều vai trò (ví dụ: cả admin và manager).
*  **Chưa hỗ trợ quyền chi tiết**: Chưa có cơ chế kiểm soát quyền chi tiết (ví dụ: manager chỉ được xem, không được sửa/xóa)
*  Chưa có API và logic cho quản lý đơn hàng, nhắn tin, bài viết.
*  Chưa có API đăng ký cho khách hàng.

**Thêm push notification**:

* Ngoài email, có thể gửi push notification qua Firebase để thông báo realtime cho technician.

**Điểm cần cải thiện**:

* Chưa có API để xóa user hoặc xem chi tiết user.
* Chưa có API để hủy đơn hàng (cancelOrder) hoặc hoàn thành đơn hàng (completeOrder).

**AGENT**

**4. Đề xuất mở rộng trong tương lai**

Để đảm bảo dự án dễ mở rộng, bạn có thể áp dụng các cải tiến sau:

**4.1. Thêm hệ thống hoa hồng cho đại lý**

* Thêm trường commission vào schema User để lưu tỷ lệ hoa hồng của đại lý.
* Thêm API tính toán doanh thu/hoa hồng dựa trên đơn hàng của khách hàng thuộc đại lý.  
  **Sử dụng absolute imports**: Cấu hình absolute imports để tránh lỗi liên quan đến đường dẫn tương đối (như đã đề xuất ở các phần trước).

**4.2. Tạo link giới thiệu tự động**

* Tạo một API để đại lý lấy link giới thiệu (ví dụ: GET /api/v1/agent/referral-link).
* Link này sẽ chứa ID của đại lý (ví dụ: <http://yourwebsite.com/register?referred_by=agent_id>).
*  **Frontend (FE-POLIKA)**: <https://github.com/mrkhangthanh/FE-POLIKA/tree/master/FE-POLIKA>
*  **Backend (BE-POLIKA)**: <https://github.com/mrkhangthanh/BE-POLIKA>
* Frontend sẽ tự động điền referred\_by vào form đăng ký.

**4.3. Thêm dashboard cho đại lý**

* Tạo API tổng hợp thông tin (số khách hàng, số đơn hàng, doanh thu, v.v.) để hiển thị trên dashboard của đại lý.

**4.5. Thêm logging chi tiết**

* Sử dụng thư viện như winston để log các hành động của đại lý (ví dụ: xem danh sách khách hàng, xem đơn hàng, v.v.).
*  Click "Chỉnh sửa thông tin" nên điều hướng đến /edit-profile.
*  Click "Thay đổi mật khẩu" nên điều hướng đến /change-password.
*  Click "Xem chi tiết lịch sử" nên điều hướng đến /activity-history.

**Gợi ý mở rộng**

* **Thêm API thực**: Thay dữ liệu giả lập trong activityHistory bằng dữ liệu thực từ API (ví dụ: gọi API để lấy lịch sử đơn hàng của customer hoặc công việc của technician).
* **Tạo trang /edit-profile và /change-password**:
  + Trang /edit-profile để người dùng chỉnh sửa thông tin (tên, email, số điện thoại, địa chỉ, v.v.).
  + Trang /change-password để người dùng thay đổi mật khẩu.
* **Thêm xác thực**: Đảm bảo chỉ người dùng đã đăng nhập mới truy cập được /profile.