8. Cơ chế xác thực & tích hợp SSO (WSO2)

8.1. Mục tiêu chương

Quy định cơ chế xác thực linh hoạt giữa:

- Local Login
- SSO qua WSO2 IS

Nhằm:

- Phục vụ dev/test
- Hỗ trợ định danh tập trung khi triển khai

8.2. Khái niệm / phạm vi áp dụng

Hai chế độ xác thực:

Chế độ	Mô tả
Local	Login nội bộ
WSO2	Login qua SSO OIDC

8.3. Quy định chính

Nguyên tắc chung

Logic xác thực nằm trong:

modules/auth

common/security

- Partner không được sửa logic xác thực
- Không thêm cơ chế login khác

Cấu hình chế độ đăng nhập

auth.type = local

auth.type = wso2

Local Login

- Xác thực username/password
- Dữ liệu ở bảng user_account
- BE sinh token

WSO2 SSO flow

1. FE redirect sang WSO2
2. User login

3. WSO2 trả access_token

FE gọi BE với:

Authorization: Bearer <token>

4. BE validate token

Quy tắc FE

- FE đọc authType từ backend
- local → hiển thị form login
- wso2 → auto redirect

Không được hardcode.

Quy tắc BE

- Tất cả API qua security filter
- Không bypass auth

Không hardcode user

8.4. Quy trình thêm FE mới vào SSO

1. Partner cung cấp:
    - Domain FE
    - Redirect URI
    - Môi trường
2. Core tạo OAuth client
3. Cấp client_id, scope

8.5. Checklist tích hợp xác thực

- Token gửi qua Authorization: Bearer
- API trả 401 nếu token sai
- Audit log ghi nhận login

Phiên bản #1
Được tạo 2026-02-23 10:22:21 UTC bởi admin_lifetex
Được cập nhật 2026-02-23 10:22:21 UTC bởi admin_lifetex