OllamaNet Documentation - Service Flows

Login Management Flow - Auth Service

Login Flow

User → Gateway: Login Request
Gateway → AuthController: POST /api/auth/login
AuthController → AuthService: AuthenticateAsync
AuthService → Database: Validate Credentials

alt [Valid Credentials]
- Database --> AuthService: User Found
- AuthService → JWTManager: Generate Token
- JWTManager --> AuthService: JWT Token
- AuthService → RoleManager: Get User Roles
- RoleManager --> AuthService: Role List
- AuthService → AuthService: Create Auth Response
- AuthService --> AuthController: Auth Success
- AuthController --> Gateway: 200 OK with Token
- Gateway --> User: Login Success + Token

[Invalid Credentials]
- Database --> AuthService: Invalid Credentials
- AuthService --> AuthController: Auth Failed
- AuthController --> Gateway: 401 Unauthorized
- Gateway --> User: Login Failed

Token Refresh Flow

User → Gateway: Refresh Token Request
Gateway → AuthController: POST /api/auth/refresh
AuthController → AuthService: RefreshTokenAsync
AuthService → JWTManager: Validate Refresh Token

alt [Valid Token]
- JWTManager --> AuthService: Token Valid
- AuthService → JWTManager: Generate New Tokens
- JWTManager --> AuthService: New Token Pair
- AuthService --> AuthController: Refresh Success
- AuthController --> Gateway: 200 OK with New Tokens
- Gateway --> User: New Access Token

[Invalid Token]
- JWTManager --> AuthService: Token Invalid
- AuthService --> AuthController: Refresh Failed
- AuthController --> Gateway: 401 Unauthorized
- Gateway --> User: Refresh Failed

Flow Legend
=
Green: Success Path
Red: Error Path
Blue: Token Operations
--
Includes token refresh
and role management