Login with optional 2FA

User → **Web/App Client**: Submit email + password

Web/App Client → **Auth API**: POST /login

Auth API → **User DB**: fetch user; verify hash; status?

alt [inactive/invalid]

Auth API → **Web/App Client**: 401/403

[valid credentials]

opt [2FA enabled?]

Auth API → **OTP Service**: generate + deliver code

OTP Service → **User**: OTP via SMS/Email

User → **Web/App Client**: Enter OTP

Web/App Client → **Auth API**: POST /login/otp (code)

Auth API → **OTP Service**: verify code

alt [OTP invalid]

Auth API → **Web/App Client**: 401

Auth API → **Auth API**: issue Access + Refresh (short/long TTL)

Note: Set tokens via HttpOnly+Secure cookies SameSite=Strict; rotate refresh

Auth API → **Web/App Client**: 200 (session established)