**Caso de Uso — Login e Autenticação**

**1) Identificação**

* **ID:** UC-SEG-001
* **Nome:** Login e Autenticação
* **Objetivo:** Autenticar o cliente e emitir **tokens de sessão** para acessar os endpoints do sistema.

**2) Atores**

* **Primário:** Cliente (app/web).
* **Sistemas externos:** API de Autenticação (interno do projeto).

**3) Pré-condições**

* API de Autenticação e banco disponíveis.
* Cliente **cadastrado** (UC-CLI-001) e **ativo**.
* Senha previamente definida.

**4) Disparador**

* Cliente envia **credenciais** (login + senha).

**5) Regras de Negócio e Validações (MVP)**

* **Campos obrigatórios:**
  + login (pode ser **email** ou **cpf**)
  + senha
* **Formato:**
  + Se login for email → formato válido.
  + Se login for CPF → dígito verificador válido.
* **Status do cliente:** **Ativo** para autenticar; **Inativo/Bloqueado** → negar.
* **Credenciais inválidas:** mensagem genérica (não revelar se login existe).
* **Política de senha (MVP):** mínimo **8** caracteres (recomendado ≥ 12).
* **Proteção a força bruta:**
  + Contador de tentativas falhas por **login** e por **IP**.
  + Após **5** falhas consecutivas → **bloqueio temporário de 15 min**.
  + Responder **429** se ultrapassar limiar por IP.
* **Tokens:**
  + **Access Token (JWT)**: exp=15m, aud="fd-bank-api", sub=userId, clienteId, scope: "self".
  + **Refresh Token**: exp=7d, **rotativo** (gera novo a cada refresh).
  + Armazenar hash do refresh token (não o token puro).
  + **Revogação** na troca (reuse detection → invalida sessão).
* **Sessões múltiplas:** permitidas por dispositivo (MVP); suportar revogação global.
* **Auditoria:** registrar sucesso/fracasso de login, CorrelationId (se houver), IP, user agent (normalizado), timestamps.

**Futuro (não MVP):** MFA/2FA, verificação de e-mail, check de senhas vazadas, captcha adaptativo.

**6) Fluxo Principal (Feliz)**

1. Cliente envia login (email/CPF) e senha.
2. Sistema valida presença/formatos (email/CPF).
3. Sistema busca o cliente e verifica **Status = Ativo**.
4. Sistema verifica senha (hash seguro).
5. Sistema gera **Access Token** e **Refresh Token (rotativo)**; persiste/atualiza sessão.
6. Sistema registra **audit trail** (sucesso).
7. Sistema retorna **200 OK** com tokens e dados mínimos do cliente.

**7) Fluxos Alternativos / Exceções**

* **A1 — Campos obrigatórios ausentes:**  
  2a. **400 Bad Request** CAMPOS\_OBRIGATORIOS (login/senha).
* **A2 — Formato inválido (email/CPF):**  
  2b. **422 Unprocessable Entity** LOGIN\_INVALIDO.
* **A3 — Credenciais inválidas:**  
  4a. **401 Unauthorized** CREDENCIAIS\_INVALIDAS.  
  4b. Incrementar contador de falhas.
* **A4 — Usuário bloqueado/inativo (login):**  
  3a. **423 Locked** USUARIO\_BLOQUEADO **ou** **403 Forbidden** USUARIO\_INATIVO.
* **A5 — Limite de tentativas/Rate limit:**  
  4c. **429 Too Many Requests** MUITAS\_TENTATIVAS.
* **A6 — Erro interno:**  
  5a. **500 Internal Server Error** ERRO\_AUTENTICACAO.

**8) Pós-condições**

* Sessão criada/atualizada (refresh armazenado com hash, expiração, device).
* Auditoria de login registrada (sucesso/fracasso).

**9) Dados Persistidos (rascunho)**

* **Usuario/Cliente:** Id, ClienteId, Email, CPF, Status, SenhaHash, SenhaAlg (argon2id/bcrypt), TentativasFalhas, UltimaFalhaEm, UltimoLoginEm.
* **Sessao:** Id, UsuarioId, RefreshTokenHash, ExpiraEm, DeviceInfo, Ip, Revogado (bool), CriadoEm, AtualizadoEm.
* **AuditoriaLogin:** Id, UsuarioId?, Resultado (Sucesso/Fracasso), Motivo (inválida/bloqueado/rate-limit), Ip, UserAgent, CorrelationId, CriadoEm.

**10) Interface/Contrato de API (MVP)**

**Login**

* **Endpoint:** POST /api/auth/login
* **Headers recomendados:** X-Correlation-Id: "<uuid>"
* **Request:**

{

"login": "ana.souza@example.com",

"senha": "minhaSenhaSegura!"

}

Também aceitar: "login": "12345678909" (CPF normalizado)

* **Response 200:**

{

"tokenType": "Bearer",

"accessToken": "<jwt>",

"expiresIn": 900,

"refreshToken": "<refresh>",

"usuario": {

"id": "f5b9a6a3-8e3f-4a61-9f2e-2a1b3c4d5e6f",

"clienteId": "b3c3a6b1-7a2c-4c49-8b6f-0d3c4a9d2e10",

"nome": "Ana Souza",

"email": "ana.souza@example.com"

}

}

**Refresh**

* **Endpoint:** POST /api/auth/refresh
* **Request:**

{

"refreshToken": "<refresh>"

}

* **Response 200 (rotativo):**

{

"tokenType": "Bearer",

"accessToken": "<novo\_jwt>",

"expiresIn": 900,

"refreshToken": "<novo\_refresh>"

}

Se houver **reuso** de refresh revogado → invalidar sessões e responder **401** REFRESH\_REUTILIZADO.

**Logout (revogar sessão atual)**

* **Endpoint:** POST /api/auth/logout
* **Headers:** Authorization: Bearer <accessToken>

**Logout de todas as sessões**

* **Endpoint:** POST /api/auth/logout-all
* **Headers:** Authorization: Bearer <accessToken>
* **Erros comuns:** 400, 401, 403/423, 429, 500.

**11) Critérios de Aceitação (Given–When–Then)**

1. **Login válido**
   * Given cliente ativo, login e senha corretos
   * When POST /api/auth/login
   * Then **200** com accessToken (15m) e refreshToken (7d).
2. **Credenciais inválidas**
   * Given senha incorreta
   * When login
   * Then **401 CREDENCIAIS\_INVALIDAS** e tentativa falha contabilizada.
3. **Bloqueio por tentativas**
   * Given 5 falhas consecutivas
   * When nova tentativa em < 15 min
   * Then **423 USUARIO\_BLOQUEADO** (ou **429 MUITAS\_TENTATIVAS** por IP).
4. **Refresh rotativo**
   * Given refresh válido
   * When POST /api/auth/refresh
   * Then **200** com **novo** access/refresh e o antigo é revogado.
5. **Reuso de refresh**
   * Given refresh já trocado
   * When tentar reutilizar
   * Then **401 REFRESH\_REUTILIZADO** e sessões correlatas revogadas.

**12) Observações de Segurança e Privacidade**

* **Hash de senha:** **Argon2id** (recomendado) ou **bcrypt (cost ≥ 12)**; **sal** único; comparação **tempo constante**.
* **Tokens:** assinar JWT com chave segura; incluir jti; validar aud/iss/exp.
* **Armazenamento dos tokens no cliente:**
  + **Web:** preferir **HttpOnly Secure Cookie** para refresh; access em memória.
  + **Mobile:** Keystore/Keychain.
* **Respostas de erro genéricas** (não indicar se login existe).
* **TLS obrigatório**; Cache-Control: no-store nas respostas.
* **Logs mínimos** (mascarar email/CPF/IP parcialmente).

**13) Métricas & Logs (MVP)**

* Taxa de sucesso de login; taxa de 401/423/429; tempo médio de autenticação; dispositivos/UA mais comuns.
* Alarmes para picos de falha por IP/login (possível ataque).

**14) TODOs / Futuro**

* **[TODO-SEG-LOGIN-01]** **MFA/2FA** (TOTP, push, SMS — definir canal).
* **[TODO-SEG-LOGIN-02]** Política de senha mais forte (mín. 12, blacklist de senhas vazadas).
* **[TODO-SEG-LOGIN-03]** **Captcha adaptativo** após múltiplas falhas.
* **[TODO-SEG-LOGIN-04]** Notificação de novo dispositivo/local.
* **[TODO-SEG-LOGIN-05]** Expansão de sessão baseada em risco (geo-velocity, device fingerprint).
* **[TODO-SEG-LOGIN-06]** Recuperação/Redefinição de senha (fluxo dedicado).