ADMTPRO 需求规格、架构与实施方案（汇总）

> 说明：以下内容为“默认方案 + 最佳实践”整理的完整规格文档，已包含新增功能：密码到期提醒与“忘记密码”流程。

---

1. 项目概述

- 项目名称：ADMTPRO
- 架构：BS 架构、前后端分离、单体应用
- 运行环境：Docker Compose
- 开发语言：后端 Python 3.12；前端 TypeScript
- 框架：Flask

---

2. 角色与权限划分

- 普通用户
  - 默认入口登录
  - 仅查看自身信息：姓名/邮箱/手机号
  - 可自助修改密码
  - 可通过“忘记密码”短信流程重置密码
- 管理员
  - 独立入口登录
  - 管理用户与 OU（CRUD）
  - 重置用户密码
  - OTP 二次验证登录
- 审计员（补充）
  - 仅可查看审计日志

---

3. 核心功能清单

3.1 权限与登录

- 普通用户默认入口登录
- 管理员独立入口登录
- 管理员需 OTP 二次验证

3.2 用户功能

- 普通用户查看自身信息：姓名/邮箱/手机号

- 普通用户自助修改密码（需旧密码 + 短信验证码）
- “忘记密码”流程：短信验证后修改密码

3.3 管理员功能

- 用户管理：增删改查、启用/禁用、重置密码
- OU 管理：增删改查、移动用户

3.4 二次验证

- 普通用户忘记密码/改密短信验证码（阿里云短信）
- 管理员 OTP 二次验证登录

3.5 日志审计

- 所有 DDL 操作必须记录
- 审计支持筛选与导出

3.6 密码到期提醒（新增）

- 读取 AD 到期时间或策略计算
- 提前 7/3/1 天提醒
- 站内通知 + 可选短信

---

4. 需求补充（默认开启）

- 搜索与过滤（按 OU、状态、邮箱、部门、岗位）
- 配置中心（LDAP/短信/OTP/日志/提醒阈值）
- 系统健康检查（AD/短信通道）
- 只读降级（AD 不可用时）

---

5. 模块设计

- 认证与会话
- AD 适配层（LDAP/LDAPS）
- 用户管理
- OU 管理
- 密码管理（改密/忘记密码/重置）
- 短信服务
- 审计日志

- 配置中心
- 健康检查
- 通知与到期提醒

---

6. 架构分层与依赖关系

6.1 分层

- 表现层：前端 TypeScript SPA
- API 层：Flask REST API
- 服务层：用户/OU/密码/审计/通知
- 适配层：AD/短信/OTP
- 数据层：PostgreSQL

6.2 依赖关系

- 认证 → AD 适配 → 审计
- 用户/OU 管理 → AD 适配 → 审计
- 密码管理 → AD 适配 + 短信 → 审计
- 到期提醒 → AD 适配 + 通知 → 审计
- 配置中心 → 全局读取

---

7. 关键流程（文字版）

- 普通用户登录 → AD 认证 → 会话
- 管理员登录 → OTP → 会话
- 自助改密 → 短信验证 → AD 改密 → 审计
- 忘记密码 → 短信验证 → AD 改密 → 审计
- 管理员重置密码 → AD 重置 → 审计
- 用户/OU CRUD → AD 更新 → 审计
- 到期提醒任务 → 查询即将到期 → 通知 → 审计

---

8. 数据模型（逻辑层）

- User
  - dn, sAMAccountName, displayName, mail, mobile
  - department, title, enabled, ou
- OU
  - dn, name, parentDn, description

- AuditLog
  - actor, actorRole, action, targetDn
  - before/after, ip, ua, createdAt
- OTP
  - userId, secret, enabled, lastVerifiedAt
- SmsCode
  - userId, phone, code, expiresAt, status

---

9. API 接口清单（REST）

- 认证
  - POST /api/auth/login
  - POST /api/auth/otp/verify
  - POST /api/auth/logout
- 用户自助
  - GET /api/me
  - POST /api/me/password
  - POST /api/me/forgot-password
- 用户管理
  - GET /api/users
  - POST /api/users
  - PUT /api/users/:id
  - PATCH /api/users/:id/status
  - POST /api/users/:id/reset-password
  - DELETE /api/users/:id
- OU 管理
  - GET /api/ous
  - POST /api/ous
  - PUT /api/ous/:id
  - DELETE /api/ous/:id
  - POST /api/ous/:id/move-user
- 审计
  - GET /api/audit
  - GET /api/audit/:id
  - POST /api/audit/export
- 配置与健康
  - GET /api/config
  - PUT /api/config
  - GET /api/health

---

10. 权限矩阵（简版）

- 普通用户：查看自己/改密/忘记密码
- 管理员：用户/OU 管理、重置密码、审计查看
- 审计员：只读审计

---

11. AD 属性映射建议

- sAMAccountName / userPrincipalName / distinguishedName
- displayName, mail, mobile
- department, title
- userAccountControl（启用/禁用）

---

12. 字段校验（摘要）

- username：3—64
- password：8—128（遵循 AD 策略）
- otpCode / smsCode：6 位数字
- mail/mobile：格式校验
- ouDn/name：必填

---

13. 错误响应规范

- 通用字段：code, message, details, requestId
- 示例错误码：
  - AUTH_INVALID, AUTH_OTP_INVALID
  - PERMISSION_DENIED, AD_UNAVAILABLE
  - OBJECT_NOT_FOUND, OBJECT_CONFLICT
  - VALIDATION_ERROR, RATE_LIMITED

---

14. 审计字段与事件枚举

14.1 审计字段

- actor, actorRole, action, targetDn
- before, after, ip, ua, result, requestId, createdAt

14.2 事件枚举

- AUTH_LOGIN, AUTH_LOGOUT
- USER_CREATE, USER_UPDATE, USER_DISABLE, USER_ENABLE
- USER_DELETE, USER_MOVE_OU
- PASSWORD_CHANGE_SELF, PASSWORD_RESET_ADMIN
- PASSWORD_RESET_FORGOT
- OU_CREATE, OU_UPDATE, OU_DELETE
- OTP_BIND, OTP_UNBIND
- SMS_SEND, SMS_VERIFY
- PASSWORD_EXPIRY_NOTIFY

---

15. 安全基线

- HTTPS + HSTS
- LDAPS + 证书校验
- 管理员入口独立 + 可选 IP 白名单
- 登录失败锁定 + 限流
- CSRF 防护
- 审计日志不可篡改

---

16. 部署拓扑与 Docker Compose

- Nginx 反向代理 + HTTPS
- Flask API
- PostgreSQL 审计/配置/验证码
- Redis（可选）

---

17. 运行参数（示例）

- LDAP_URL, LDAP_BIND_DN, LDAP_BIND_PASSWORD, LDAP_BASE_DN, LDAP_CA_CERT
- ALIYUN_ACCESS_KEY_ID, ALIYUN_ACCESS_KEY_SECRET
- ALIYUN_SMS_SIGN_NAME, ALIYUN_SMS_TEMPLATE_RESET, ALIYUN_SMS_TEMPLATE_NOTIFY
- OTP_ISSUER, OTP_WINDOW
- DB_URL, AUDIT_RETENTION_DAYS
- SESSION_TTL, LOGIN_MAX_FAILS, LOGIN_LOCK_MINUTES
- SMS_CODE_TTL, SMS_SEND_INTERVAL

18. 测试与验收（摘要）

- 登录：普通/管理员/OTP
- 权限：普通用户不可管理
- 密码：改密/忘记密码/重置
- 用户/OU：CRUD 与移动
- 审计：DDL 全记录
- 到期提醒：7/3/1 天触发

---

19. 实施蓝图（Sprint 拆解）

- Sprint 1：AD 联通与登录
- Sprint 2：用户/OU 管理
- Sprint 3：改密/忘记密码/OTP/短信
- Sprint 4：审计/配置/提醒
- Sprint 5：安全与稳定

---

20. D1–D20 日计划

- D1：确认 AD 权限与证书、短信模板、OTP 规则
- D2：AD 连接验证与配置清单
- D3：登录流程设计
- D4：登录联调与审计落库
- D5：阶段评审
- D6：用户查询/分页/过滤
- D7：用户 CRUD 与启用/禁用
- D8：OU CRUD 与移动用户
- D9：管理台基础页面
- D10：阶段评审
- D11：自助改密
- D12：忘记密码流程
- D13：短信服务与限频
- D14：管理员 OTP 绑定/验证
- D15：阶段评审
- D16：审计查询/导出
- D17：配置中心
- D18：密码到期提醒
- D19：健康检查/限流/只读降级
- D20：最终验收与交付

21. 实施准备清单

- AD 网络可达 + 636 端口
- 服务账号最小权限
- CA 证书与 HTTPS 证书
- 阿里云短信账号/模板
- OTP 绑定流程说明
- PostgreSQL 实例与备份策略
- 默认 OU 与禁用 OU
- 密码到期提醒阈值

---

22. 前端页面与文案（摘要）

- 登录页：普通用户入口 + 管理员入口按钮 + 忘记密码
- 忘记密码页：账号 → 短信验证码 → 新密码
- 个人中心：展示自身信息 + 修改密码
- 管理台：用户管理、OU 管理、审计日志、系统设置

---

23. 用例清单（摘要）

- 普通用户登录
- 管理员登录 + OTP
- 查看个人信息
- 自助改密
- 忘记密码
- 管理员重置密码
- 用户 CRUD
- OU CRUD
- 移动用户 OU
- 审计日志查询
- 密码到期提醒

---

24. 非功能需求

- 安全：强制 HTTPS + LDAPS
- 可用：只读降级
- 审计：可追溯、不可篡改

- 兼容：Chrome/Edge 最新版