Alohi – Authentication Flow Manual QA: Test Strategy

Context

Alohi SA (Sign.Plus, Fax.Plus, Dial.Plus) provides unified authentication across its suite — users log in once and reuse credentials.
Scope: **Signup and Login for Free & Enterprise users** (web focus).

---

1. Scope

In Scope

- **Signup:** email/password, email verification, invite-based Enterprise signup, Terms/Privacy consent.
- **Login:** verified/unverified users, lockout & rate-limits, remember-me.
- **Password reset:** request, token handling, completion.
- **Session management:** creation, refresh/expiry, logout (single & cross-app).
- **Cross-product identity reuse:** App A login grants App B access per policy.
- **Plan/role variance:** Free vs Enterprise; tenant isolation.

Out of Scope

- In-app authorization, billing, profile settings.
- Social/IdP SSO & MFA (unless enabled).
- Native mobile parity — **web only** for this exercise.

---

2. Objectives & Quality Risks

Objectives

- Validate reliability, security, and consistency across products.
- Verify cross-product identity without tenant leakage.
- Detect **P0 regressions** early with clear evidence.

Assumptions

- Shared identity service issues reusable tokens.
- Email delivery & links observable in sandbox inbox.
- Enterprise invites assign tenant roles.

Key Risks

- Token/session mismatch or logout propagation gaps.
- Tenant boundary or metadata leakage.

- Weak rate-limit/lockout (brute force exposure).
- Expired/invalid tokens accepted.
- Case/Unicode/whitespace inconsistencies causing duplicate users.
- Secrets in URLs, insecure flags, or caching of auth responses.

---

3. Test Coverage Approach

Functional (Happy Paths)

- Signup (Free & Enterprise), email verify, login, password reset, logout, cross-app SSO.
- Enterprise invite acceptance & join flow; tenant switch denial.

Exploratory Charters

- Identity propagation (App A → App B).
- Session lifecycle (idle vs absolute expiry; refresh rotation).
- Logout consistency & cache behavior.
- Tenant isolation & cross-tenant invite edges.

Edge / Negative

- Invalid inputs, spacing/case issues, Unicode names.
- Expired/tampered tokens, missing nonce/state.
- Rate-limit & lockout after N attempts; CAPTCHA if present.
- Reset for unverified/deactivated users; reset while logged in.
- Basic accessibility: focus order, error messaging, keyboard nav.

Environments & Data

- Web staging with feature flags visible.
- Seed accounts: Free (new/existing), Enterprise (invited/existing), admin inviter.
- Disposable inbox for link validation.
- Evidence: screenshots, HAR, headers (Set-Cookie, Cache-Control), response codes.

---

4. Prioritization

Method: Risk × Impact × Frequency.

Priority	Definition	Examples
P0 (Blocker)	Critical path broken	Signup/login failure, invalid tokens accepted, cross-app SSO broken, tenant leakage, logout ineffective, insecure cookies

P1 (Major)	High impact, workaround exists	Error message inconsistencies, rate-limit tuning, minor token issues
P2 (Minor)	Cosmetic/non-blocking	UI polish, rare edge formats, minor a11y defects

---

5. Representative Scenarios

ID	Area	Scenario	User	P	Expected
S1	Signup	Free signup → verify → login	Free	P0	Email verification mandatory; session cookie httpOnly, Secure, SameSite
S2	Signup	Enterprise invite (new user)	Ent	P0	One-time invite; joins correct tenant/role
S3	Signup	Invite with existing Free acct	Ent	P0	Existing ID linked; no duplicate
S4	Login	App A login → open App B	Both	P0	Cross-app SSO per policy
S5	Login	Unverified email login	Free	P1	Clear error; resend link; rate-limit enforced
S6	Reset	Request reset (verified user)	Both	P0	Token expiry enforced; password policy validated
S7	Reset	Expired/used token	Both	P0	Rejected safely; re-request offered; audit logged
S8	Session	Idle vs absolute expiry	Both	P0	Messaging clear; token rotation; no 401 loops
S9	Logout	Logout App A → access B	Both	P0	Session invalidated; cached pages blocked
S10	Lockout	N failed logins → lockout	Both	P0	Lockout duration & safe messaging; no user enumeration
S11	Input	Case/Unicode/whitespace	Both	P1	Normalized emails; consistent match
S12	Tenant	Access tenant B after join A	Ent	P0	403 denied; no metadata leak

---

6. Entry / Exit Criteria

Entry

- Stable test environment, seed data available.
- Email delivery observable; feature flags documented.
- Logging/metrics accessible.

Exit

- **100 % P0 pass**; no open Sev-1/2 defects.
- P1/P2 logged with mitigations or owners.
- Evidence attached to all executed cases.
- Known risks documented.

---

7. Reporting & Hygiene

Reporting

- Lightweight checklist + defect tickets (severity, repro, env, impact).

Evidence

- Screenshots, HAR, console logs, request/response payloads, headers, cookies, localStorage.

Security Hygiene

- No secrets in URL/query.
- Proper headers:
    - Cache-Control: no-store, Pragma: no-cache
    - Set-Cookie with HttpOnly; Secure; SameSite=Lax/Strict
    - Strict-Transport-Security (HSTS)
- No mixed-content warnings.