

AG RUNBOOK — Phase 7.1

Admin User Provisioning (Invite-Only)

Purpose:

This runbook defines a safe, ordered, and auditable procedure for implementing invite-only admin user provisioning in a multi-tenant SaaS system.

Global Constraints:

- Do not modify existing authentication flows
- Do not add public signup
- Do not allow admins to set passwords
- Do not weaken tenant isolation
- Do not refactor audit logging

Step 1 — Prisma Schema Changes:

- Add `UserStatus` enum (PENDING, ACTIVE, DISABLED)
- Update `User` model with status and nullable `passwordHash`
- Add `UserInvite` model with hashed token and expiration

Step 2 — Admin API: Create User & Invite:

- POST `/api/admin/users`
- Create PENDING user
- Assign roles
- Generate hashed invite token
- Store invite with 24h expiry
- Log `USER.CREATE` audit event

Step 3 — User Activation:

- POST `/api/auth/activate`
- Validate invite token
- Set password
- Activate user
- Mark invite as used

Step 4 — Login Guard:

- Block login for PENDING and DISABLED users
- Allow only ACTIVE users

Step 5 — Audit Taxonomy:

- Ensure `USER.CREATE` action exists

Outcome:

Secure, auditable, invite-only user provisioning with full tenant isolation.