Bilko Auth Migration Runbook + Admin Guide

Scope

This runbook covers: (1) how an operator bootstraps the first admin after legacy auth is retired, (2) how an admin creates and invites users, (3) how to assign and change roles, (4) the full user lifecycle via Entra, (5) migration notes from the WP1–WP4 branch stack. For architecture detail see Bilko Authentication — Entra External ID (CIAM).

1. Bootstrapping the First Admin (Break-Glass)

After legacy `/auth/register` is retired (HTTP 410), there is no HTTP endpoint for creating the first user. Use the Gradle break-glass task:

```
# Set environment variables (never commit these):
export BOOTSTRAP_ADMIN_EMAIL="admin@yourorg.com"
export BOOTSTRAP_ADMIN_PASSWORD="<strong-temporary-password>"

# Run from the api project root:
cd apps/api
./gradlew :apps:api:bootStrapAdmin
```

What this does: calls `AuthService.register()` directly (bypasses HTTP routing), creates an organisation + owner user. No HTTP endpoint is exposed — zero backdoor surface. The temporary password should be rotated immediately via Entra SSPR after the admin first signs in.

Full runbook file: `apps/api/docs/runbooks/BREAK-GLASS-BOOTSTRAP.md` (on branch `feat/rbac-wp4-retire-legacy-auth`).

2. Creating / Inviting Users (Admin Flow)

User creation is now admin-gated. Self-serve registration is retired.

Via API

```
POST /api/v1/admin/users
Authorization: Bearer <admin-or-owner-access-token>

{
  "email": "newuser@example.com",
  "fullName": "Full Name",
  "role": "viewer"        // viewer | accountant | admin | owner
}
```

Response: `HTTP 201 Created` — returns the new user object including their UUID. The user receives an invite; they sign in via Entra (JIT provisioning links their Entra identity on first sign-in).

Permission required

`users:manage` — held by `admin` and `owner` roles.

Via Web Admin UI

1. Sign in as admin or owner
2. Navigate to **Settings > Users** (`/admin/users`)
3. Click **Invite User**
4. Enter email, full name, and select role
5. Submit — user receives invite email (Entra CIAM invitation flow)

Viewers and accountants see a redirect to the dashboard if they navigate to `/admin/users`.

3. Assigning / Changing Roles

Via API

```
PUT /api/v1/users/:id/role
Authorization: Bearer <admin-or-owner-access-token>

{
  "role": "accountant"    // viewer | accountant | admin | owner
}
```

Constraints enforced:

- Caller must have `users:manage` permission (admin+)
- A user **cannot change their own role** (self-escalation blocked — HTTP 403)
- The `owner` role cannot be changed via this endpoint (owner is protected in `SettingsService.changeUserRole()`)
- Invalid role values return HTTP 400

Via Web Admin UI

1. Navigate to **Settings > Users**
2. Find the user row
3. Click the role dropdown (visible to admin/owner only)
4. Select the new role — saved immediately via `PUT /users/:id/role`

4. User Lifecycle

1. **Admin creates user** via `POST /admin/users` (role = viewer by default, or specified role)
2. **User receives Entra invite** (email from `bilkociam.onmicrosoft.com`)
3. **First sign-in**: user clicks Entra sign-in on Bilko web login → authenticates in Entra CIAM → Bilko backend calls `createSessionFromEntraIdToken()`:
   - Looks up `entra_external_identities` by `oid` → not found (first login)
   - Email-match lookup → finds pre-created user → inserts `entra_external_identities` row (JIT link) → audit event `entra_jit_link`
   - Bilko session returned; user is logged in as viewer
4. **Admin promotes role** if needed via `PUT /users/:id/role`
5. **Subsequent logins**: Entra → backend finds `entra_external_identities` by `oid` → direct session, no email-match step
6. **Sign-out**: MSAL calls Entra logout endpoint → Entra session invalidated → Bilko session cookie cleared → next visit redirects to Entra login

5. What Changed — Migration Notes (WP1–WP4)

Area	Before (pre-WP1)	After (WP1–WP4)
Backend auth enforcement	`requireRole("admin")` inline in 51+ route handlers	`requirePermission("invoice:create")` via extension fn; 0 residual requireRole in routes
Permission data	No tables; hardcoded numeric hierarchy in RbacHelper	V67: `permissions` table (52 keys), `role_permissions` seed; V68: provisioning function
User provisioning	Self-serve `POST /auth/register`	Admin invite (`POST /admin/users`) + JIT Entra link on first sign-in; `UserProvisioningService`
Web login	Email/password form + "Sign in with Microsoft" coexisting	Entra-only CTA; no email/password form; register page shows "contact your admin"
Legacy endpoints	Active: /auth/login, /auth/register, /auth/forgot-password, /auth/reset-password	HTTP 410 Gone + ENDPOINT_RETIRED body
Password reset	Email-based reset-password flow (V57 table)	Redirect to Entra SSPR portal (self-service via Microsoft account)
RBAC admin UI	No UI; role changes required direct DB query	Web: Settings > Users page with role dropdown (admin/owner only)

6. Branch Stack (WP1–WP4 Stacked PRs)

WP	Branch	Latest commit	Key files
WP1 — RBAC catalog	`feat/rbac-wp1-permissions-catalog`	890168d (last route commit)	V67 migration, PermissionService, BilkoPrincipal, RbacHelper, 17 route files migrated
WP2 — Provisioning	`feat/rbac-wp2-user-provisioning`	a9fa67c	V68 migration, UserProvisioningService, UserManagementRoutes
WP3 — Web UI	`feat/rbac-wp3-web-entra-ui`	3c1c019	login/page.tsx (Entra CTA), register/page.tsx (retired), admin/users/page.tsx, lib/permissions.ts

WP	Branch	Latest commit	Key files
WP4 — Retire legacy	`feat/rbac-wp4-retire-legacy-auth`	3ac1388	AuthRoutes.kt (5 x 410), api.ts (removed methods), auth-store.ts, 13 new web tests

These branches are stacked and NOT yet merged to main. Production cutover requires a consolidated merge PR after CEO/Securion sign-off.

7. Rollback Procedure

If the consolidated deploy to main needs to be rolled back:

1. **Feature flag path** (if `FEATURE_ENTRA_AUTH_ENABLED` env var is present): set to `false` to re-enable the password auth provider path (AuthProvider interface, D5 in MC #103075)
2. **Hard rollback**: revert to the pre-WP1 commit; Flyway handles down-migration if reversible V67/V68 down scripts were authored (check migration files)
3. **password_hash**: column was made nullable in V66 but existing rows retain their hash values — password-based login can be re-enabled without data loss during the rollback window
4. **Password reset tokens table (V57)**: NOT dropped. Must not be dropped until the rollback window closes (minimum 30 days post-production cutover). See D8 plan in MC #103075
5. **Entra disable**: if Entra must be disabled urgently, also disable users in Bilko DB to enforce immediate revocation (7-day refresh window caveat — OC#4)

8. Database Schema Reference

Table	Key columns	Notes
`users`	`id`, `organization_id`, `email`, `password_hash` (nullable), `role` (CHECK owner|admin|accountant|viewer), `two_factor_*`	V66: password_hash nullable; V67: role CHECK added
`entra_external_identities`	`issuer`, `subject` (= oid), `user_id`, `last_login_at`	V64: created; UNIQUE(issuer,subject), UNIQUE(user_id,issuer); RLS: V66
`permissions`	`permission_key` (PK, CHECK format)	V67: 52 keys; global catalog, no RLS, GRANT SELECT bilko_app
`role_permissions`	`role`, `permission_key`	V67: exhaustive flat seed; V68: users:manage + users:invite added

Evidence Files

- WP1 verification: `/tmp/evidence-103141/wp1-verification.md`, proveo-verdict.json
- WP2 verification: `/tmp/evidence-103142/wp2-verification.md`, proveo-wp2-verdict.json
- WP3 Proveo: `/tmp/evidence-103143/proveo-wp3-validation.md`
- WP4 verification: `/tmp/evidence-103144/wp4-verification.md`
- WP5 E2E: `/tmp/evidence-103145/wp5-e2e.md`, verification.json
- Phase 0 config: `/tmp/evidence-103076/phase0-config.md`

Revision #2
Created 2026-06-08 07:42:16 UTC by John
Updated 2026-07-12 20:03:29 UTC by John