Bilko Signup Jurisdiction Fix — MC #103501

Bilko Signup Jurisdiction Fix — MC #103501

Status: Branch-verified only. Merge, stage deploy, and production deploy are PENDING as of 2026-06-12.

Branch: `fix/103501-oauth-jurisdiction` | **PR:** #356 | **Commits:** `418a35f0`, `9e05e5c6`

Mesh record: `mesh-thr-6a18851a-476c-4aff-a6c9-92665d35fb3f`

---

1. Root Cause

The PostgreSQL function `bilko_auth.provision_user_with_org` had the org's `country` column hardcoded to `'BA'`. During a Google or Entra OAuth signup, the Ktor backend called this function without passing any jurisdiction context. As a result, a user who signed up on **bilko.cloud** (Croatia) received an organisation record with `country='BA'` (Bosnia), even though the frontend MarketContext.tsx correctly pinned that domain to Croatia (HR, 25% PDV).

This created a silent jurisdiction mismatch: the backend would apply BA fiscal rules (17% PDV) while the UI presented HR rules (25% PDV). The bug only surfaced for OAuth signups; email/password signups were not affected by the same code path.

2. Domain ? Jurisdiction Resolution Table

The new `JurisdictionResolver.kt` provides the canonical mapping. The same mapping is mirrored in `apps/web onboarding/page.tsx` (region-confirm step) and was already in `MarketContext.tsx`.

Domain (request Host)	Country	Base Currency	Language
`bilko.cloud`	HR	EUR	hr
`bilko.io`	RS	RSD	sr
`bilko.company`	BA	BAM	bs
Unknown / fallback	BA	BAM	bs

Notes:

- Host normalization: trailing dots are stripped, value is uppercased before comparison, so `bilko.cloud.` and `BILKO.CLOUD` both resolve correctly.
- A `?country=` query parameter overrides the host-derived jurisdiction. This is intended for internal tooling and testing only.

3. Fix Summary

3.1 New file: `JurisdictionResolver.kt`

Encapsulates all domain → (country, baseCurrency, language) logic. Called from `AuthRoutes.kt` using `call.request.host()` before any provisioning occurs. The resolver is the single source of truth for host-to-jurisdiction mapping in the backend.

3.2 Changed: `AuthRoutes.kt`

Derives jurisdiction via `JurisdictionResolver` at the start of the Entra JIT provisioning path and threads the resolved `country` and `baseCurrency` values through to the database provisioning call.

3.3 New Flyway migration: V80

Gives `bilko_auth.provision_user_with_org` a new 6-argument overload that accepts `country` and `base_currency` as explicit parameters. The original 4-argument signature is preserved for backward compatibility with existing callers (defaults to BA/BAM). The migration also corrects language derivation, which was previously hardcoded to `'bs'` regardless of the org's country; the new logic derives HR→`hr`, RS→`sr`, else→`bs`. `SECURITY DEFINER` and RLS are preserved unchanged.

3.4 Changed: `apps/web onboarding/page.tsx`

Adds a region-confirm step during onboarding that persists `org.country` explicitly. This provides a user-visible confirmation of the resolved jurisdiction and allows a deliberate override before the account is fully committed.

3.5 Security fix included in PR #356

During Proveo round-1 review, a bypass was identified: `PUT /settings` lacked an owner-only guard on the `country` field, meaning an admin-role user could silently change the org's jurisdiction via that endpoint. The guard was added in the same PR, restricting `country` writes to the org owner on **both** `PUT /settings` and `PUT /organization`.

4. Verification Evidence

Proveo verification — two rounds

Round	Result	Findings
Round 1	PARTIAL	Test-harness blocker; /settings owner-guard security gap; trailing-dot edge case not handled
Round 2	PASS	All three findings resolved and re-verified

JUnit test results (branch, Testcontainers PostgreSQL)

Test class	Result	Key assertion
`JurisdictionResolverTest`	18/18 PASS	All domain mappings, trailing-dot normalization, uppercase Host, unknown-host fallback, ?country= override
`UserProvisioningWp2Test`	9/9 PASS	T9 reads the org row from a real Testcontainers PostgreSQL instance and asserts `country='HR'`, `base_currency='EUR'` for a bilko.cloud signup
`SettingsRoutesHttpIntegrationTest`	23/23 PASS	Admin-role user receives HTTP 403 on both `PUT /settings` (country field) and `PUT /organization` (country field)

Mesh record: `mesh-thr-6a18851a-476c-4aff-a6c9-92665d35fb3f`

5. Backfill Plan (DOC-ONLY — requires CEO sign-off)

Scope: Organisations that were provisioned via OAuth signup through the *bilko.cloud* or *bilko.io* domain but have `country='BA'` in the database.

Reference file: `docs/runbooks/jurisdiction-backfill-plan.md` in the Bilko repo.

This plan is documentation only. No automated or manual data mutation must be executed without explicit written sign-off from Alem Basic (CEO).

Identification query (read-only)

```
-- Identify potentially mismatched orgs (read-only diagnostic)
SELECT o.id, o.name, o.country, o.created_at, u.email
FROM organizations o
JOIN users u ON u.org_id = o.id AND u.role = 'OWNER'
WHERE o.country = 'BA'
  AND o.created_at >= '2024-01-01'  -- adjust to known start of OAuth signup availability
ORDER BY o.created_at DESC;
```

Backfill procedure (requires CEO sign-off before execution)

1. Run the identification query in a read-only transaction and export results for CEO review.
2. For each org, determine the correct jurisdiction by cross-referencing the user's signup domain from audit logs (if available) or by manual confirmation with the org owner.
3. Update via a Flyway-managed migration (versioned, reversible) — do not use ad-hoc SQL in production.
4. Re-verify affected org invoices: any invoices already issued with wrong tax rates may require credit notes and re-issue depending on the jurisdiction's accounting law. Involve a local accountant for HR and RS cases.
5. Notify affected org owners of the correction.

Risk

Any org that has already issued invoices under the wrong jurisdiction has a fiscal compliance exposure. The data fix alone does not resolve the accounting liability — that requires domain-

specific legal/accounting review per country.

6. Residual Items

Follow-on MC #103505 (non-blocker)

`baseCurrency` currently lacks a parallel owner-only guard on the settings/organization update endpoints. This means an admin-role user could change the base currency. Tracked as a separate non-blocking follow-on.

7. Pending Deploy Status

As of 2026-06-12, the following have NOT been completed:

- Merge of PR #356 (`fix/103501-oauth-jurisdiction`) to `main`
- Stage auto-deploy (triggered by merge to main)
- Semver tag `vX.Y.Z` to trigger `bilko-main-deploy` (prod + demo via `cloudbuild.yaml`)
- Live post-deploy E2E verification:
  - Confirm migration V80 present in `flyway_schema_history` on the production database
  - A real signup flow on `bilko.cloud` yields `organizations.country='HR'`
  - A real signup flow on `bilko.io` yields `organizations.country='RS'`

Do not mark this fix as production-live until these post-deploy checks pass and evidence is recorded.

Documented by Skillforge (ALAI Knowledge & Training) — 2026-06-12. Source of truth for MC #103501 jurisdiction fix. For backfill execution, obtain CEO sign-off first.

Revision #1
Created 2026-06-12 13:55:40 UTC by John
Updated 2026-06-12 13:55:40 UTC by John