

MC 106880 — PR 325 V156

RLS Grant-Gap Closure

Fix report — MC #106880 / PR 325

Date: 2026-08-10

Canonical target branch: `azdo/main` at `64edfec05b6cee2d495f1c5e0c9c3bf2d662b5a1`

Candidate: `b9b373f9ca79835729c09f0ea80a55cfe7be1ef9`

Worktree: `/Users/makinja/projects/bilko-pr325-post323-r1`

Status at this report revision: PR 325 merged no-fast-forward as

`1e98d1c29b8a817eb917d01ac4a8de8ff07a43e2` after exact-candidate local and Azure gates passed. No deployment or connection-role cutover occurred.

Scope

PR 323 made V154 and V155 immutable main history. PR 325 therefore owns exactly one new migration, V156. The repository diff contains three directly required files:

1. `apps/api/src/main/resources/db/migration/V156__rls_bilko_app_grants_and_definer_search_patterns.sql`
2. `apps/api/src/test/kotlin/no/alai/bilko/security/RlsBilkoAppGrantsV156IntegrationTest.kt`
3. `apps/api/src/test/kotlin/no/alai/bilko/migrations/V134MigrationTest.kt`

The third file is required because V156 intentionally changes `organizations`, `invoices`, and `expenses` from ACL-level permission denial to RLS-level zero visibility for `bilko_app`. The full integration gate caught the inherited test's obsolete permission-denied expectation as the sole unreviewed regression. The corrected test now requires each query to reach RLS and return zero rows under the unrelated support-agent GUC; no baseline entry was added.

No application connection setting, credential, role attribute, policy, deployment manifest, or baseline file changes in this PR.

V156 behavior

Exact 22-table privilege matrix

Table	Exact direct privileges for <code>bilko_app</code>
accounts	SELECT, INSERT, UPDATE, DELETE
bank_accounts	SELECT, INSERT, UPDATE
bank_transactions	SELECT, INSERT, UPDATE
contacts	SELECT, INSERT, UPDATE, DELETE
expense_documents	SELECT, INSERT
expenses	SELECT, INSERT, UPDATE, DELETE
inbox_items	SELECT, INSERT, UPDATE
invoice_items	SELECT, INSERT, DELETE
invoices	SELECT, INSERT, UPDATE, DELETE
logged_actions	SELECT, INSERT
offer_items	SELECT, INSERT, UPDATE
offers	SELECT, INSERT, UPDATE
transactions	SELECT, INSERT, UPDATE
travel_orders	SELECT, INSERT, UPDATE
users	SELECT, INSERT, UPDATE, DELETE
audit_log	SELECT, INSERT
impersonation_sessions	SELECT, INSERT, UPDATE
invoice_templates	SELECT, INSERT, UPDATE, DELETE
notifications	SELECT, INSERT, UPDATE
organizations	SELECT, INSERT, UPDATE, DELETE
password_reset_tokens	SELECT, INSERT, UPDATE, DELETE
user_invitations	SELECT, INSERT, UPDATE

The migration:

- fails if `bilko_app` or any target table is missing;
- requires the migration identity to be a superuser or each table's owner;
- applies only the reviewed matrix;

- reads direct ACLs with `aclexplode` and compares each table's complete privilege set exactly;
- rejects missing privileges, unexpected privileges, and `WITH GRANT OPTION` widening;
- executes transactionally, so a failed post-condition does not leave partial grants.

Exact six `SECURITY DEFINER` functions

V156 resolves and hardens these exact signatures:

- `bilko_auth.find_org_by_registration_number(text)`
- `public.purge_expired_partition(text,text)`
- `bilko_auth.find_rejected_einvoices_for_period(timestamptzt,timestamptzt)`
- `bilko_auth.mark_einvoice_report_transmission(uuid,varchar,timestamptzt,varchar)`
- `bilko_auth.find_user_by_email(text)`
- `bilko_auth.find_user_by_id(uuid)`

Before alteration it requires every exact OID to exist, remain `SECURITY DEFINER`, and be owned by the migration identity unless that identity is superuser. It rejects unexpected same-name overloads. After alteration it requires the exact catalog value `search_path=public, pg_temp` on every exact OID.

Forward-only rule

V156 has no down migration and must not be edited after application. An emergency reversal would require a new separately reviewed forward migration. This session does not apply V156 to any shared database.

Runtime proof

`RlsBilkoAppGrantsV156IntegrationTest` uses Testcontainers PostgreSQL 16 and repository migration resources. It:

1. migrates the real chain to V155;
2. proves representative reads fail at the ACL layer before V156;
3. injects an unexpected `TRIGGER` grant and proves the real V156 migration fails transactionally and names the widening;
4. removes only the test drift and runs the real V156 migration;
5. requires one successful Flyway V156 row and one `schema_version` marker `156.0.0`;
6. checks exact direct ACL sets for all 22 tables;
7. checks all six exact function OIDs, `SECURITY DEFINER`, owner resolution, and exact search path;
8. proves Org A and Org B each see only their own rows, cannot see the other tenant, and empty context fails closed on direct and subquery policy shapes.

Focused exact-patch evidence was bound to the committed candidate by matching the pre-commit and committed binary-diff object IDs:

- `/Users/makinja/system/evidence/106880/pr325-candidate-commit-2026-08-10.json`
- `/Users/makinja/system/evidence/106880/pr325-v134-v156-final-working-tree-2026-08-10.json`

Gate results bound to

`b9b373f9ca79835729c09f0ea80a55cfe7be1ef9`

- Java 21 compile + CI-mode Detekt: PASS.
- Full unit run: 1,903 tests; five existing failures; blocking exact baseline check PASS with zero unreviewed failures and no baseline growth.
- Full integration run: 2,217 tests; 76 existing failures; blocking exact baseline check PASS with zero unreviewed failures and no baseline growth. V134: 7/7 PASS. V156: 1/1 PASS. Zero skipped in both security suites.
- Gitleaks: PASS over the three-commit `azdo/main..candidate` range; three commits scanned, no leaks.
- Trivy 0.72.0: PASS on FORGE against a digest-verified `git archive` of the exact candidate with `--severity HIGH,CRITICAL --exit-code 1 --no-progress --ignorefile .trivyignore`; no `--ignore-unfixed` or suppression change.

Evidence:

- `/Users/makinja/system/evidence/106880/pr325-exact-candidate-static-unit-b9b373f9-retry1-2026-08-10.json`
- `/Users/makinja/system/evidence/106880/pr325-exact-candidate-full-integration-b9b373f9-2026-08-10.json`
- `/Users/makinja/system/evidence/106880/pr325-gitleaks-b9b373f9-2026-08-10.json`
- `/Users/makinja/system/evidence/106880/pr325-trivy-forge-b9b373f9-2026-08-10.json`

Shared-target preflight

A single `BEGIN TRANSACTION READ ONLY` catalog probe against `bilko-demo-pg/bilko` confirmed:

- `transaction_read_only=true` and `mutations=0`;
- V156 is not in Flyway or `schema_version` history;
- no failed Flyway rows;
- all 22 tables exist, have RLS enabled, and are owned by `bilko_admin`;
- all six exact function signatures exist;

- no unexpected same-name overload;
- `bilko_app` exists, cannot log in, is not superuser, and does not bypass RLS;
- latest applied shared-target migration is V153.

Evidence: `/Users/makinja/system/evidence/106880/pr325-v156-live-readonly-preflight.json`.

No Flyway migrate/repair/clean, DDL, DML, `SET ROLE`, connection-role cutover, or deployment was executed against the shared target.

Governance gate

The corrected forge is `/Users/makinja/system/prompts/forged/106880.md`; semantic validation is `/Users/makinja/system/evidence/106880/prompt-forge-corrected-semantic-validation-2026-08-10.json`. It maps D1-D10 to executable AC#1-AC#10 and preserves attributed dissent. Mehanik returned `CLEAR TO DISPATCH` before implementation resumed.

Azure and merge completion

- Non-force source push: `refs/heads/fix/106880-rls-grants` → `b9b373f9ca79835729c09f0ea80a55cfe7be1ef9`.
- Azure PR validation build 1036: `completed/succeeded`, source version `64bd26b16754594494dfbc4072c2e210e8d310e3` (the exact synthetic merge of reviewed base and candidate).
- Eight non-skipped Azure jobs succeeded: Node web quality, Kotlin compile, Kotest baseline, full integration baseline, security scans, sort contract, AI review, and Detekt.
- Blocking Build policy: `approved`, current, not expired, build 1036.
- Azure AI review for build 1036: CRITICAL none; SHOULD-FIX none; two non-blocking documentation nits.
- Independent exact-diff review: PASS, P0=0/P1=0.
- Merge: no-fast-forward commit `1e98d1c29b8a817eb917d01ac4a8de8ff07a43e2`, parents are the reviewed base and candidate.
- Merge message contains `[skip ci]`; source branch was deleted; canonical `azdo/main` equals the merge commit.
- Thirty seconds after completion, Azure had no main build with the merge SHA. No deployment was requested or executed.

Evidence:

- `/Users/makinja/system/evidence/106880/pr325-final-independent-review.json`
- `/Users/makinja/system/evidence/106880/pr325-build-1036-final.json`
- `/Users/makinja/system/evidence/106880/pr325-build-1036-ai-review-summary.json`
- `/Users/makinja/system/evidence/106880/pr325-final-premerge-gate.json`

- `/Users/makinja/system/evidence/106880/pr325-completed.json`

Explicitly excluded

The connection-role cutover remains plan-only in

`/Users/makinja/system/evidence/106880/connection-role-cutover-plan.md` and requires a separate explicit CEO decision. **Bez deploya:** no deploy, traffic change, secret/config mutation, role cutover, or shared-database migration is part of this PR session.

Revision #1

Created 2026-08-10 21:05:05 UTC by John

Updated 2026-08-10 21:05:05 UTC by John