

# Bilko — Support agent rola + RLS temelj (Faza A, MC #106050/#106051)

## Support agent rola + RLS (Support MVP Faza A)

**MC:** #106050 (A1) + #106051 (A2), parent #106049 · **Autor:** Bruce Momjian · **Red-zone verify:** Parisa Tabriz (Securion) PASS · **Grana:** azdo `feat/106051-support-agent-rbac` (c4c8b4f4, NIJE main dok se A4/B ne ožiče)

## Šta

DB temelj za support osoblje: nova rola `support_agent` koja vidi tikete SVIH klijenata ali NIŠTA finansijsko.

- **V133** — permission catalog: `support_agent` dobija TAČNO `support_ticket:read` + `support_ticket:reply` (colon-format po V67 CHECK-u). NULA finance/accounting/payroll ključeva. Idempotentno.
- **V134** — RLS + grants: cross-org SELECT na `support_tickets` gejtovan NOVIM GUC-om `app.is_support_agent` (NAMJERNO NE reciklira `app.is_platform_admin` — to bi tiho dalo supportu sve što platform-admin tabele daju). Column-scoped UPDATE grant (status, resolution\_note, triage\_json, external\_ref, updated\_at — org\_id/context\_bundle isključeni na GRANT nivou). Usput zakrpio pre-existing gap: support\_tickets (V73) nikad nije imao eksplicitan bilko\_app GRANT (nevidljivo u prod jer bilko\_admin BYPASSRLS).
- **Rola = pravi users.role login**, ne service-account (bilko-support-triage je mašinski, bez per-human atribucije).

## Sigurnost (Parisa adversarial verify, 6/6 drži)

1. Finance leak: nema — `is_support_agent` se ne pojavljuje ni u jednoj finance/audit policy kroz 134 migracije; support konekcija na te tabele vezana istim org\_isolation policy-ma. 2. GUC scope: `is_support_agent` samo u V134, samo na support\_tickets policy-ma. 3. Cross-org: samo support\_tickets otvoren, ništa drugo. 4. Permission over-grant: resolve() = exact-equality lookup, bez wildcard/prefix; mehanički ne može vratiti više od 2 ključa. 5. Column-scoped grant potvrđen. 6. RLS nigdje globalno ugašen; nema GUC-injection primitiva. Evidence: `~/system/evidence/106051/parisa-adversarial-verify.md`.

## ?? Bitno za sljedeću fazu (A4/B)

Aplikacijski sloj JOŠ ne ožičuje rolu — RLS politike su trenutno nedostižan **dead code** (siguran failure mode; rute i dalje idu preko `app.is_platform_admin`). A4 (`requireSupportAgent()` guard) + B (rute koje SET LOCAL `app.is_support_agent`) su prvi kod koji stvarno pali novi GUC → **traže vlastiti adversarial pass**, ne voze na ovom verдикtu (Parisa flag).

---

Revision #2

Created 2026-07-20 07:30:12 UTC by John

Updated 2026-08-10 07:37:48 UTC by John