

Bilko — Support ticket reply + GUC aktivacija (Faza B, MC #106054-106057)

Support ticket reply + GUC aktivacija (Faza B)

MC: #106054 (B1) #106055 (B2) #106056 (B3) #106057 (B4) + #106071 (gap-fix), parent #106049 · **Build:** Momjian (B1+gap) + CodeCraft (B2-B4) · **Red-zone verify:** Parisa Tabriz GUC-execution adversarial PASS · **Grana:** azdo `feat/106051-support-agent-rbac` (5c06350a, NIJE main)

Šta

Support agent sada može ODGOVORITI korisniku na tiket (async), i tu se PRVI put aktivira `app.is_support_agent` prekidač (dosad dead-code).

- **B1** (V136): `support_ticket_messages` thread tabela (agent↔customer poruke) + RLS (agent cross-org kroz `app.is_support_agent`, customer samo svoj tiket) + uski grants. Append-only.
- **B2** `POST /admin/support/tickets/{id}/messages` — agent reply. **PRVI kod koji izvršava** `SET LOCAL app.is_support_agent='true'` — unutar vlastite transakcije, tek nakon `requireSupportAgent()` guarda, mirror `OrgScopeSessionVariable` pattern. Upis poruke + `NotificationService` (korisnik dobije obavijest) + `audit_log`.
- **B3**: `GET /support/tickets/{id}/messages` — customer strana, postojeći JWT, NE pali GUC; app-layer org+ticket WHERE filter (defense-in-depth uz RLS) → cross-tenant = 404.
- **B4**: `GET /admin/support/tickets` scope za `support_agent` (cross-org) + `platform_admin` backward-compat. Zaseban guard/sealed-class, ne dira detail/PATCH.
- **#106071 gap-fix**: generički invite putevi (`POST /admin/invitations`, `POST /admin/users`, `PUT /users/:id/role`) sada REJECT-uju `role=support_agent` — samo dedicated platform-admin support-invite (A3) ga smije dodijeliti.

? Sigurnost (Parisa GUC-execution adversarial, sve drži)

1. **Pool leakage: nema** — Database.kt isAutoCommit=false (SET LOCAL transaction-scoped); svaki request svježa Exposed transakcija; pool-test (Hikari pool=1, druga tx čita NULL, 3×) + Parisa nezavisno potvrdila handler shape.
2. **Ekskluzivnost:** B4 sealed-class exhaustive `when` = compile-time garancija da se nikad ne postave oba prekidača; grep — nijedan drugi fajl ne referencira `is_support_agent`.
3. **#106071 stbapno zatvoren** na 5c06350a (3 call-site exact-match reject, ne tiketiran).
4. **B3** ne pali GUC, app-layer filter daje pravi 404.
5. **B4** detail/PATCH byte-for-byte nepromijenjeni. Evidence:

`~/system/evidence/106055/parisa-b-guc-adversarial-verify.md`.

Otvoreni tech-debt (van scope-a, evidentiran)

#106070 StatusPages 403-body · #106072 org-name unique · #106075 V73 ::uuid 500 · Jackson-vs-kotlinx serialization mehanizam (D1 docs presuda).

Ostaje

C (Vizu support konzola UI) → D (docs) → E (Angie E2E uživo).

Revision #2

Created 2026-07-20 08:49:10 UTC by John

Updated 2026-08-10 07:37:49 UTC by John