Bilko Backoffice — Backend MVP (Sentry + audit request_id + support_tickets)

1. Overview

This backend slice (MC #103323, branch `feat/103323-backoffice-backend`, commit `6b214a00`, PR #316) delivers the diagnostic and intake backbone for the Bilko support fix-loop.

Before this slice, when a customer hit an accounting error on `app.bilko.cloud` neither the platform team nor the customer had a way to identify which request failed or why. Three components address that gap:

1. **Sentry error capture** — catch-all (INFRA-only) exception capture with PII scrub and Cloud Run release/serverName metadata. Inert until `SENTRY_DSN` secret is provisioned (OCD-1, CEO action).
2. **V71 audit_log.request_id** — nullable correlation column added to every audit row, threaded from a single canonical source (`call.callId`) across all route handlers.
3. **V72 support_tickets + SupportTicketRoutes** — customer intake channel (POST) and platform-admin triage queue (GET list + GET detail + PATCH status) with RLS, idempotency, and full status-transition audit trail.

This slice is **deploy-gated** behind prod cutover MC #103300. All three components were independently verified by Proveo (Angie Jones): 12/12 AC signals PASS, integration test 3/3 PASS, unit suite 1280/1280.

2. Component Map

2.1 Sentry capture — plugins/Sentry.kt + plugins/StatusPages.kt

- **DSN guard:** `configureSentry()` checks `SENTRY_DSN`; if absent or blank, `Sentry.init` is not called. The SDK stays in silent no-op mode. CI / Testcontainers / local dev never emit live

Sentry events.

- **Cloud Run metadata:** `K_REVISION` maps to `options.release`; `K_SERVICE` maps to `options.serverName`. Fallbacks: `"local"` and `"bilko-api-local"`.
- **beforeSend PII scrub:** request body (`event.request?.data = null`) and breadcrumbs (`event.breadcrumbs?.clear()`) stripped before transmission. Extra context filtered to allowlist: `errorCode, requestId, orgId, httpStatus, instancePath`.
- **Single capture point — Throwable catch-all only:** `Sentry.captureException` is placed exclusively in the `exception<Throwable>` handler in `StatusPages.kt` (line 237). Named typed handlers (BadRequest, Conflict, Unauthorized, Forbidden, etc.) do not call captureException — those cover 4xx user-error exceptions. Ktor StatusPages dispatches named handlers first; Throwable catch-all fires only for genuine INFRA/unexpected exceptions. AC signal: grep returns count=1 in both checks.
- **Sentry scope tags:** `requestId` from `call.callId` (CallId plugin canonical source), `orgId` from `BilkoPrincipal.organizationId` (fallback `"UNKNOWN"` for pre-auth crashes — mandatory), `errorCode = INFRA_001`.

2.2 V71 audit_log.request_id — AuditLogService.kt + migration

- **Migration V71:** `ALTER TABLE audit_log ADD COLUMN request_id TEXT;` — nullable, no default. PG 11+ metadata-only operation (no table rewrite). Plain `CREATE INDEX` (not CONCURRENTLY) on partial index `WHERE request_id IS NOT NULL`. CONCURRENTLY is prohibited inside Flyway transactions (institutional memory from V70; AC signal confirms absence).
- **Column type TEXT:** chosen over UUID because clients can supply arbitrary `X-Request-ID` header values. Trust boundary: client-supplied, stored verbatim, correlation/debuggability only.
- **No idempotency constraint on audit_log:** one HTTP request legitimately produces multiple audit rows (e.g. impersonation start + org update in same admin session). A UNIQUE constraint would reject valid multi-row sequences. Idempotency enforced at V72 layer.
- **AuditLogService.insert signature:** added `requestId: String? = null` as last parameter (default null = backward compatible). Docstring: "Correlation handle for cross-system debugging only — NOT a security control. Client-supplied value stored verbatim."
- **Single canonical requestId source:** `call.callId` (Ktor CallId plugin) is the single authoritative source across StatusPages (Throwable catch-all), AdminPortalRoutes, ImpersonationService, and SupportTicketRoutes. Typed domain handlers retain raw header for RFC 7807 echo-back to client only — these do not call captureException and do not write to audit_log, so the split is intentional and does not break the diagnostic join. (bruce-momjian dissent resolution)

2.3 V72 support_tickets + SupportTicketRoutes — routes/SupportTicketRoutes.kt

- **POST /support/tickets** (customer, JWT-scoped): `orgId` and `userId` extracted from `BilkoPrincipal` only — never from request body. `context_bundle` server-side validated against CONTEXT_BUNDLE_ALLOWLIST before insert. `app.current_org_id` set via `orgTransaction(principal.organizationId)` so RLS WITH CHECK passes. Idempotency: duplicate `(org_id, request_id)` returns 409.
- **GET /admin/support/tickets** (platform-admin): paginated list, `limit` (default 50, max 100) + `offset`, optional `status` and `orgId` filters. Returns `data` array + `meta.total/limit/offset`.
- **GET /admin/support/tickets/{id}** (platform-admin): single ticket detail.
- **PATCH /admin/support/tickets/{id}** (platform-admin): enforces status transition machine, requires `resolutionNote` for RESOLVED/CLOSED, inserts audit_log row for every status change with `requestId = call.callId`. Audit write failure is non-fatal but logged to structured stderr (Cloud Logging visible).
- **Admin GUC pattern:** `transaction { exec("SET LOCAL app.is_platform_admin = 'true'") }` — SET LOCAL per transaction, pgBouncer transaction-mode pooling safe.

3. Data Model

3.1 support_tickets columns

Column	Type	Notes
id	UUID PK	gen_random_uuid() default
org_id	UUID NOT NULL	FK to organizations(id) ON DELETE CASCADE
user_id	UUID NOT NULL	FK to users(id)
error_code	TEXT	Nullable; currently generic VAL/INFRA (OCD-2 open CEO decision)
request_id	TEXT	Correlation ID of originating failed request. NOT a FK to audit_log.request_id (one request_id maps to N audit rows). Join via equality.
context_bundle	JSONB NOT NULL	CHECK jsonb_typeof = 'object'. Allowlisted keys only (server-side enforced).
customer_description	TEXT	Free text from customer

Column	Type	Notes
status	TEXT NOT NULL	CHECK (status IN ('OPEN','TRIAGED','IN_PROGRESS','RESOLVED','CLOSED')). Default 'OPEN'.
triage_json	JSONB	NULL = not yet triaged. V2 AI agent writes here.
created_at	TIMESTAMPTZ NOT NULL	DEFAULT now()
updated_at	TIMESTAMPTZ NOT NULL	DEFAULT now(); maintained by BEFORE UPDATE trigger.
resolution_note	TEXT	Required (route-enforced) for RESOLVED/CLOSED transitions.
external_ref	TEXT	V2 Zendesk/Linear sync. Nullable at MVP.

3.2 Indexes

- `UNIQUE (org_id, request_id) WHERE request_id IS NOT NULL` — idempotency.
- `(org_id, status, created_at DESC)` — admin list query (per-org filtered).
- `(status, created_at DESC)` — global admin list.

3.3 RLS policies

All GUC SET statements use `SET LOCAL` (transaction-scoped) — pgBouncer transaction-mode pooling safe.

- **support_tickets_customer_insert** — FOR INSERT WITH CHECK `(org_id = current_setting('app.current_org_id', true)::uuid)`.
- **support_tickets_customer_select** — FOR SELECT USING `(org_id = current_setting('app.current_org_id', true)::uuid OR current_setting('app.is_platform_admin', true)::boolean = true)`.
- **support_tickets_admin_all** — FOR ALL USING and WITH CHECK `(current_setting('app.is_platform_admin', true)::boolean = true)`. Same GUC pattern as audit_log RLS (V51).

Customer UPDATE/DELETE immutability: no UPDATE or DELETE policy for customers. RLS ENABLED with no such policy = deny-by-default. Customers cannot modify or delete submitted tickets.

Production code audit (Proveo-confirmed): `orgTransaction{}` (OrgScopeSessionVariable.kt:131) always wraps `SET LOCAL app.current_org_id` inside `transaction{}`. The Testcontainers test failure (Proveo GAP-1) was caused by the test setup using a PostgreSQL superuser connection — superusers bypass RLS regardless of GUC values. Production code was never buggy.

3.4 Status transition machine

From	Allowed next states
OPEN	TRIAGED, CLOSED
TRIAGED	IN_PROGRESS, CLOSED
IN_PROGRESS	RESOLVED, CLOSED
RESOLVED	CLOSED
CLOSED	(no further transitions)

Invalid transitions return HTTP 422 with `code: "INVALID_TRANSITION"` and `allowedNext`.

3.5 context_bundle allowlist

Allowed keys (server-side enforced, rejection = HTTP 422): `requestId, errorCode, httpStatus, instancePath, orgId, userId, appRoute, planTier, country, auditRef`. IDs and codes only — never invoice content, names, amounts, or email addresses.

4. Diagnostic Join

```
SELECT al.*
FROM audit_log al
JOIN support_tickets st ON al.request_id = st.request_id
WHERE st.id = '<ticket-uuid>';
```

Framing (martin-kleppmann dissent): `request_id` is a *correlation handle for cross-system debugging only* — NOT tamper-evidence. The append-only guarantee for `audit_log` comes from the `block_audit_mutation()` trigger (V51), not from request_id. Platform-admin direct DB access is outside the threat model of this column.

5. Known Gaps and Follow-ups

Item	Detail	Status
OCD-1: Sentry DSN	`bilko-sentry-dsn` / `bilko-web-sentry-dsn` must be provisioned in GCP Secret Manager. Inject via `--update-secrets` (never `--set-env-vars`). Sentry code is fully inert until then.	CEO action required. Blocks production deploy; does not block feature branch merge.

Item	Detail	Status
OCD-2: error_code taxonomy	Domain errors currently fall into generic VAL/INFRA codes, making ticket triage partly blind. Domain-specific codes are V2 scope (MC #103333). CEO confirmed proceed with V72 before those codes land.	Open CEO decision. V2 follow-on MC #103333.
OCD-3: merge-order vs #103300	V71/V72 migration numbers must be confirmed/renumbered after #103300 merges.	Open. Blocking deploy only.
Positive-path RLS assertion	Integration test confirms negative proof (wrong-org INSERT rejected). Positive proof (correct-org INSERT succeeds) not explicitly asserted. Proveo: completeness gap, not safety-weakening gap.	Follow-up test enhancement. Non-blocking.
CI runner quota	Tracked as MC #103304.	Separate MC.
Deploy gate	Deploy-gated behind MC #103300 prod cutover.	Dependent on #103300.

6. Verification Evidence

- **Proveo P2P Final Verdict: PASS** — commit `6b214a00`, 12/12 AC signals pass, integration test 3/3 PASS (BUILD SUCCESSFUL in 35s, tests="3" failures="0"), unit suite 1280/1280. Evidence: `/tmp/alai/p2p-pairing-evidence/proveo-103323-verdict-final.md`
- **Builder evidence bundle:** `/tmp/evidence-103323/verification.md`
- **PR:** #316 on branch `feat/103323-backoffice-backend`
- **Integration test XML SHA256:** `941b588f21c8fd735c1b6f7f1b888ea2d2441ec0c5f3a2085bc00489fcc70bf7`
- **File hashes (Proveo):** StatusPages.kt `fca33115361ced358dbdc56a8fd0020bc1212d58758574f540fdc46193287284`; SupportTicketRoutes.kt `730f76a245fb0492f5f94c378e18973242e7e9a0f9c4de5353dc8be268a38b2f`; OrgScopeSessionVariable.kt `2c5c992c92c5f548c22092c171a98fb599760f3ce827d1e72db26d901c0c89f2`

Revision #1
Created 2026-06-09 23:30:38 UTC by John
Updated 2026-06-09 23:30:38 UTC by John