

Super-Admin Panel

Super-Admin Panel — MC #104287

Shipped: 2026-06-27

Environment: rg-qody-demo (Azure Container Apps)

Revisions: qody-api--0000046 · qody-admin--0000026

Commits: 749108b (API) · 594d9c9 (Admin frontend)

Validation: Independent code verifier · Securion security peer-review · Proveo live E2E · John live curl

Scope

Five capabilities were shipped and verified live. One capability (A-03, per-merchant Monri credential vault) is explicitly deferred and not yet built.

A-01 — Merchant Onboarding UI

Provides SUPERADMIN users with the ability to create new merchants and control their lifecycle from the admin panel.

- **Backend:** `POST /superadmin/merchants` — creates a new merchant/org record.
- **Backend:** `POST /superadmin/merchants/{id}/suspend` — suspends a merchant; guest ordering blocked at venue level.
- **Backend:** `POST /superadmin/merchants/{id}/activate` — re-activates a suspended merchant.
- **Frontend:** `MerchantsTab` — create modal + per-row suspend/activate buttons in the super-admin panel.
- A suspended venue returns 404 on the `/superadmin/impersonate/{venueId}` endpoint (see A-06).

A-02 — Per-Merchant Fee Management

Allows SUPERADMIN to configure per-venue commercial terms with enforced range guards at multiple layers.

- **Endpoint:** `PUT /superadmin/merchants/{id}/fees`
- **Bug fixed:** Frontend previously sent `PATCH` (405 Not Allowed); corrected to `PUT`.
- **Range guards (enforced at Kotlin level + DB CHECK constraint, migration V10):**
 - Platform fee: 0.3% – 0.7%
 - Monthly fee: 29 – 49 KM
- Out-of-range input: HTTP 400 with descriptive message.
- Valid input: HTTP 200.
- Proveo re-verified the 500→400 fix after the range-guard correction.

A-03 — Per-Merchant Monri Gateway Credential Vault (DEFERRED)

Not yet built. Deferred, externally blocked on:

- Monri test credentials pending (MC #104270).
- Azure Key Vault architecture decision pending.

Design intent: per-venue Monri credentials stored encrypted in Azure Key Vault; routing logic in payment service retrieves at request time. No implementation exists in the current revision.

A-04 — Cross-Merchant Transaction Search

Enables SUPERADMIN to search across all venues/merchants for specific transactions.

- **Endpoint:** `GET /superadmin/transactions?search=<query>`
- Server-side `ILIKE` match on `providerPaymentId` and `orderNumber`.
- Scope: all orgs/venues (superadmin only; RLS bypassed for this role).

A-06 — Controlled Support Impersonation

Allows SUPERADMIN to obtain a short-lived, venue-scoped session token to diagnose issues within a specific merchant's context.

- **Endpoint:** `POST /superadmin/impersonate/{venueId}`
- Returns a 30-minute MANAGER-scoped JWT (`type=impersonate`).
- Venue-scoping enforced at Postgres RLS level (not cosmetic application-layer filtering).
- Every call writes a mandatory `audit_log` row (`action=superadmin_impersonate`).
- Token issuance is **atomic** with the audit write: the transaction aborts and returns an error if the audit insert fails — no token without an audit trail.
- Returns 403 for non-SUPERADMIN callers; 404 for suspended venues.

Security Design — Impersonation

Control	Implementation	Rationale
Least privilege role	MANAGER-scoped JWT (not OWNER, not SUPERADMIN)	Limits blast radius; cannot modify org settings or fees
Short TTL	30-minute token expiry	Reduces window for token misuse or exfiltration
Mandatory audit	Atomic <code>audit_log</code> write; aborts on failure	No impersonation can occur without a traceable record
RLS venue isolation	Postgres Row-Level Security enforces venue boundary	Confirmed real by Securion peer-review (HIGH finding: audit-atomicity — fixed before ship)
SUPERADMIN gate	403 for any other role	Endpoint unreachable to merchant users or kitchen/waiter roles

Securion finding (HIGH — fixed): Initial implementation issued the token before writing the audit row. Fixed to wrap both operations in a single DB transaction; token is returned only after the commit succeeds.

A-08 — Monthly Billing Export

Provides SUPERADMIN with a per-venue revenue and fee CSV for a given calendar month.

- **Endpoint:** `GET /superadmin/billing-export?month=YYYY-MM`
- **CSV columns:** `venue_id`, `venue_name`, `org_id`, `org_name`, `currency`, `period_start`, `period_end`, `total_turnover`, `platform_fee_pct`, `fee_owed`, `monthly_fee`, `total_owed`

- **Frontend:** `BillingTab` with a month picker; exports on demand.
-

Validation Summary

Verifier	Method	Result
Independent code verifier	Static code review	PASS
Securion (Parisa Tabriz)	Security peer-review of A-06 impersonation	HIGH finding (audit atomicity) — fixed; venue-scoping confirmed RLS-real
Proveo (Angie Jones)	Live E2E: 4 PASS + A-02 range-guard 500→400 re-verify	PASS
John	Live curl against rg-qody-demo endpoints	PASS

What Is NOT in This Release

- **A-03 (Monri credential vault):** Deferred — blocked on Monri test creds (MC #104270) and Key Vault architecture.
 - Support password-reset UI, merchant onboarding billing, suspend/activate per-merchant billing — tracked separately in MC #104303.
-

Revision #1

Created 2026-06-27 22:01:40 UTC by John

Updated 2026-06-27 22:01:40 UTC by John