

Staff Password Reset

Overview

QODY supports two complementary password-reset mechanisms for venue staff. **Part A** is manager/owner-initiated (admin UI, no email required). **Part B** is self-service via email token. Both paths were verified live on `rg-qody-demo` on 2026-06-28 (qody-api--0000047, qody-admin--0000027, qody-staff-kitchen--0000012; commit `e4c035e`).

Part A — Manager/Owner-Initiated Reset

Endpoint

```
POST /admin/staff/{id}/reset-password
```

Authorization

- Requires `OWNER` or `MANAGER` role.
- **Guard:** a MANAGER cannot reset an OWNER or another MANAGER (returns 403). Only an OWNER can reset any staff member. This prevents privilege escalation and account logout.

Behaviour

1. Generates a cryptographically random one-time temporary password.
2. Sets the staff account password to this temporary value (argon2id hash stored).
3. Returns the plaintext temporary password **once** in the response body — it is never stored in plaintext and cannot be retrieved again.
4. Displays the temporary password in the StaffView modal in the admin UI.
5. The action is written to the audit log.

Dependencies

No external dependency. Works in demo and production environments regardless of SMTP configuration.

Part B — Self-Service Forgot/Reset Flow

Step 1: Request a reset link

POST /auth/forgot-password

Body: { "email": "staff@example.com", "venueSlug": "my-restaurant" }

- Unauthenticated endpoint.
- Always returns a generic `200 OK` regardless of whether the email exists (anti-enumeration).
- Rate-limited: 3 requests per 15 minutes per email + IP combination.
- Token generation and email dispatch run async (fire-and-forget) so response timing does not leak account existence.

Step 2: Apply the reset token

POST /auth/reset-password

Body: { "token": "<token>", "newPassword": "<password>" }

Response codes:

Status	Meaning
<code>200 ok</code>	Password updated successfully.
<code>400 invalid</code>	Token not found or does not match stored hash.
<code>400 expired</code>	Token is older than 1 hour.
<code>400 used</code>	Token has already been consumed.
<code>400 weak</code>	New password does not meet minimum requirements.

Entry points

- "Zaboravljena lozinka?" link on the admin login screen and the kitchen login screen.
- `/reset-password?token=<token>` page (linked from the email).

Token Security

Property	Value
Entropy	256-bit SecureRandom token
Storage	Only the SHA-256 hash is stored (UNIQUE index) — plaintext never persisted
Single-use	Atomic CAS: <code>UPDATE ... WHERE used_at IS NULL</code> prevents TOCTOU double-use
TTL	1 hour
Password hashing	argon2id
Password length	8-1024 characters (upper bound guards against DoS via hashing large inputs)
Scope	Token is bound to a specific <code>staff_id</code> — cross-venue reset is not possible
Unauthenticated datasource	Forgot/reset routes use the admin bypass datasource (no session required)

Database migration

V21 adds the `password_reset_tokens` table with `token_hash` (UNIQUE), `staff_id` (FK), `expires_at`, and `used_at` columns.

Email Delivery

Part B uses the existing `EmailService`. In the current demo environment, no SMTP credentials are configured — the service performs a graceful no-op and the reset link is not delivered by email. Part A (manager-initiated) works fully in demo.

“ **Production note:** configure an SMTP or Resend secret to enable Part B email delivery. Without it, self-service resets are non-functional for end users.

Validation Chain

1. **verifier(code)** — internal code review
 2. **Securion peer-review** — APPROVE-WITH-FIXES; issues found and fixed: timing-oracle, TOCTOU double-use, argon2 DoS guard, UNIQUE index on token hash, MANAGER-to-OWNER reset guard
 3. **FlowForge** — deployed to `rg-qody-demo`
 4. **Proveo** — browser E2E tests, all flows PASS
 5. **John live curl** — all flows verified PASS on 2026-06-28
-

Related

- MC task: #104424
 - Live revisions: qody-api--0000047 | qody-admin--0000027 | qody-staff-kitchen--0000012
 - Commit: `e4c035e`
 - Production SMTP config: set `SMTP_HOST`, `SMTP_USER`, `SMTP_PASSWORD` (or `RESEND_API_KEY`) environment variables on qody-api container app.
-

Revision #1

Created 2026-06-28 07:21:14 UTC by John

Updated 2026-06-28 07:21:14 UTC by John