

Account Lockout (Brute-Force zaštita) — A12

Bilko — Account Lockout (Brute-Force zaštita) — A12 / MC #104687

Status: implementirano 2026-07-03, commit `13b3a729` na `feat/task-104687` (Wave 1 — čeka merge u dev) **Vlasnik:** CodeCraft backend · Proveo PASS (nezavisna verifikacija svih 5 AC)

Ponašanje

- Nakon **5 uzastopnih neuspješnih** email/password login pokušaja, nalog se zaključava **15 minuta**.
- **6. pokušaj vraća HTTP 423** (`BILKO-AUTH-005`) **čak i s tačnom šifrom** — provjera zaključanosti ide PRIJE verifikacije šifre.
- Uspješan login **resetuje brojač** na 0 (legitimni korisnici s povremenim tipfelerima se ne zaključavaju).
- Istekli `locked_until` se auto-čisti prije provjere šifre (cooldown se sam otključa).
- **Admin unlock:** `PUT /api/v1/users/{id}/unlock` (permisija `users:manage`, org-scoped — cross-org pokušaj vraća 404).
- **Entra-only korisnici** (`passwordHash = NULL`, V66) nikad ne dotiču lockout logiku; Entra SSO put (`markEntraLogin`) ne konsultuje lockout.

Implementacija

Sloj	Šta
------	-----

Migracija	V108__account_lockout.sql — users.failed_login_attempts INT NOT NULL DEFAULT 0, users.locked_until TIMESTAMPTZ NULL (aditivno) + drop/recreate 3 bilko_auth.* SECURITY DEFINER lookup funkcije (RETURNS TABLE promjena; OWNER/GRANT identični V31/V66 originalima — diffano)
Servis	AuthService.kt — lock-check prije verifyPassword; brojač = jedan atomski parametrizovani UPDATE (nema izgubljenih inkremenata pod konkurencijom); adminUnlock(orgId, userId)
HTTP	LockedException → BILKO-AUTH-005 (423) u StatusPages.kt ; ruta unlock u UserManagementRoutes.kt; dokumentovano u ERROR-CODES.md + openapi.yaml
Testovi	AuthServiceLockoutTest.kt — 5 scenarija (6. pokušaj s tačnom šifrom → 423; reset na uspjeh; cooldown expiry; admin unlock; cross-org 404). Izvršeno 5/5 + regresija AuthServiceTest 31/31, skipped=0 (XML ground truth)

Bitno: javna login ruta je 410

POST /api/v1/auth/login vraća **410 Gone** platformski (WP4/MC #103144 — Bilko je Entra-only, password login penzionisan). Lockout je time defense-in-depth: javna brute-force površina je ZATVORENA (Proveo live probe: 7×410 na api.bilko.cloud), a lockout se automatski primjenjuje ako se ruta ikad reaktivira. Odluka: rutu NE reaktivirati radi live-423 demonstracije.

Poznati follow-up

- bilko_auth.find_user_by_email / find_user_by_id i dalje nemaju SET search_path = public, pg_temp (naslijeđeno iz V31, nije uvedeno ovim taskom) — hardening ticket.

Evidence

- /Users/makinja/system/evidence/104687/build-report-20260703.md
- /Users/makinja/system/evidence/104687/proveo-verdict-20260703.md
- P2P mesh: mesh-thr-357b1180 (builder) → mesh-thr-516f2df0 / mesh-msg-ba98cc59 (Proveo PASS)

Ops napomene (otkriveno tokom taska)

- Gitleaks pre-commit** je gađao ../../.gitleaks.toml — rušio SVAKI commit iz nested .claude/worktrees/* (fail-closed "Secrets detected" bez skena). Fixano u .husky/pre-commit (commit 13b3a729): config je tracked na repo root-u → --show-

`toplevel/.gitleaks.toml`.

2. **Testcontainers silent-skip:** `~/.testcontainers.properties` je pokazivao na legacy `docker.raw.sock` koji Ryuk ne može bind-mountati na aktuelnom Docker Desktopu → SVI integration testovi tiho SKIPPED uz "BUILD SUCCESSFUL". Fix: `unix:///var/run/docker.sock` + `ryuk.disabled=true`. **Lekcija: uvijek čitati `tests=` / `skipped=` iz testsuite XML-a, ne vjerovati zelenom buildu.**
-

Revision #1

Created 2026-07-02 22:46:14 UTC by John

Updated 2026-07-02 22:46:15 UTC by John