Hands-on authorization review

RentDesk isolated application code + Fusion storefront public boundary
Deep Audit / Pro service sample. Performed 14 September 2026.

Result

No authorization bypass was confirmed in the scoped checks. Twenty-one isolated API assertions passed, including four real bcrypt sign-ins. Five browser-operated screenshots corroborate selected results. Three live storefront API requests were refused with HTTP 401, and the admin entry opened a sign-in gate.

This is a bounded result, not a production security clearance. RentDesk authorization code ran unchanged against an isolated database through an explicit framework adapter. The deployed Next request pipeline, real customer identities, external report email, walkthrough and later re-audit were not exercised.

What was exercised

Area	Observed result
Access control	Anonymous receipt and write requests refused.
Two-identity IDOR	A/B own receipts readable; reciprocal foreign IDs returned 404.
Write authorization	Owner and granted manager writes persisted; cross-account and ungranted writes refused.
RBAC / privilege	Viewer writes, manager owner operations and owner-role invitation refused.
Data export	Owner export excluded foreign rows; viewer export returned 403.
Live admin boundary	Admin/CRM reads and empty admin POST returned 401.

Scope and isolation

Owned source: RentDesk revision **51b055772ee4**. Synthetic accounts A and B, plus viewer and restricted manager roles, used .invalid email addresses and real application-created session cookies. Only isolated records were changed. No production sign-in, provider call, customer data, charge or outbound email was used.

Findings and interpretation

F01 - Tenant isolation held for the sampled read and write paths. Owner A read receipt 101 and Owner B read receipt 201. Swapping the IDs returned 404 in both directions. Cross-account building mutations returned a refusal. The persisted state still contained the original foreign-account and restricted-building labels. Evidence: api-checks.json and screenshots 01, 02 and 05.

F02 - Role and property grants were enforced server-side. The viewer was refused a write; the restricted manager could change building 101 but not building 102, and could not rename the account. An owner could not invite another owner through the manager/viewer invitation action. These calls used the actual RentDesk actions and getViewer database/session resolution. Evidence: api-checks.json and screenshots 03 and 04.

F03 - Live anonymous admin access was refused. GET /api/admin/stats, GET /api/crm/contacts and POST /api/admin/blog-posts with an empty JSON body each returned 401. The browser entry /admin redirected to fusiondataco.app/admin and showed a sign-in gate. No authenticated admin authorization claim is made. Evidence: live-storefront-api.json and screenshot 06.

Additional correct behavior: the first fixture used an active plan without a subscription expiry, and the app refused writes. The fixture was corrected to a current trial before the authorization matrix. This was an entitlement guard working correctly, not an application defect.

F04 - Public sign-in displays a development-mode label. Screenshot 06 shows the Clerk form at fusiondataco.app/admin labelled Development mode. This is a directly observed deployment/configuration concern, not proof of an authorization bypass. Verify the intended production Clerk instance and configuration.

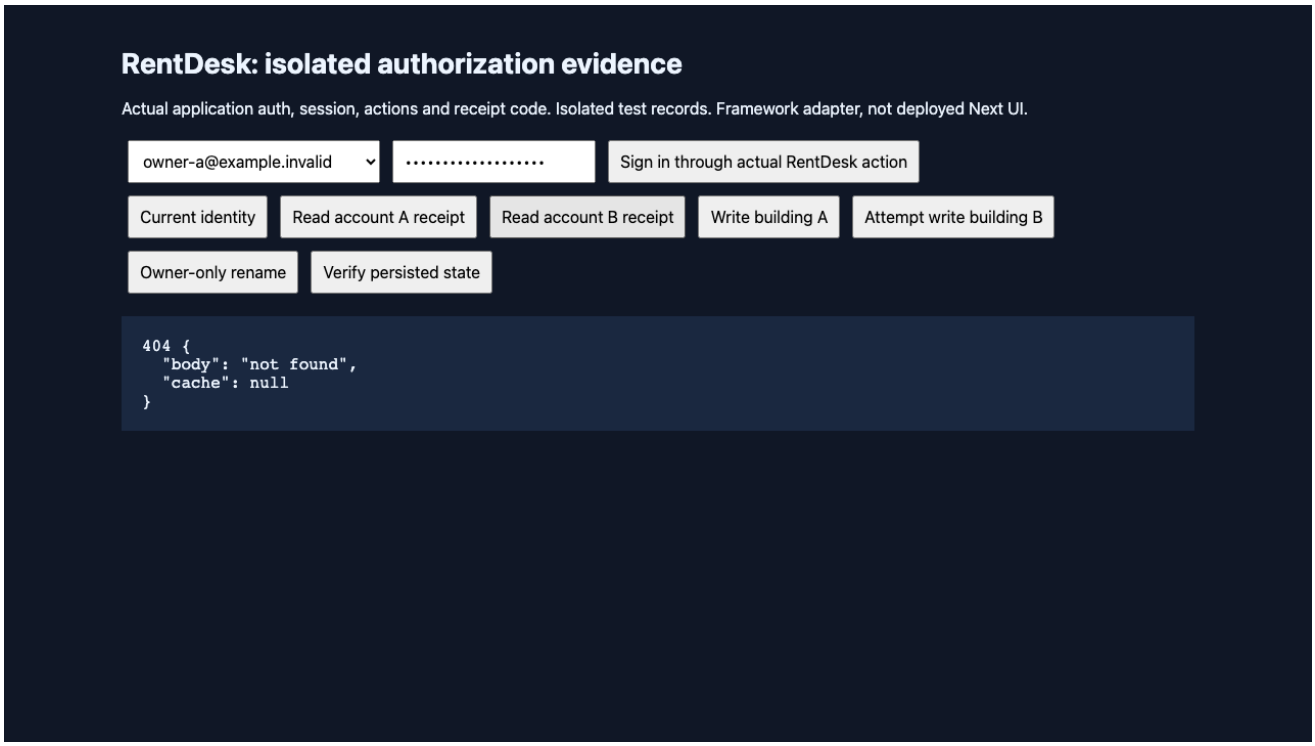
Prioritized follow-up plan

P1 - Verify identity deployment and the real Next request boundary. Resolve or explain the public Clerk Development mode label, then repeat the two-identity matrix on an isolated deployment using native pages and Server Action transport. Include cross-origin requests, middleware redirects and session expiry/revocation. Exit condition: the same tenant/role outcomes hold without the cookie/cache/navigation adapter. No code fix is prescribed without a reproduced failure.

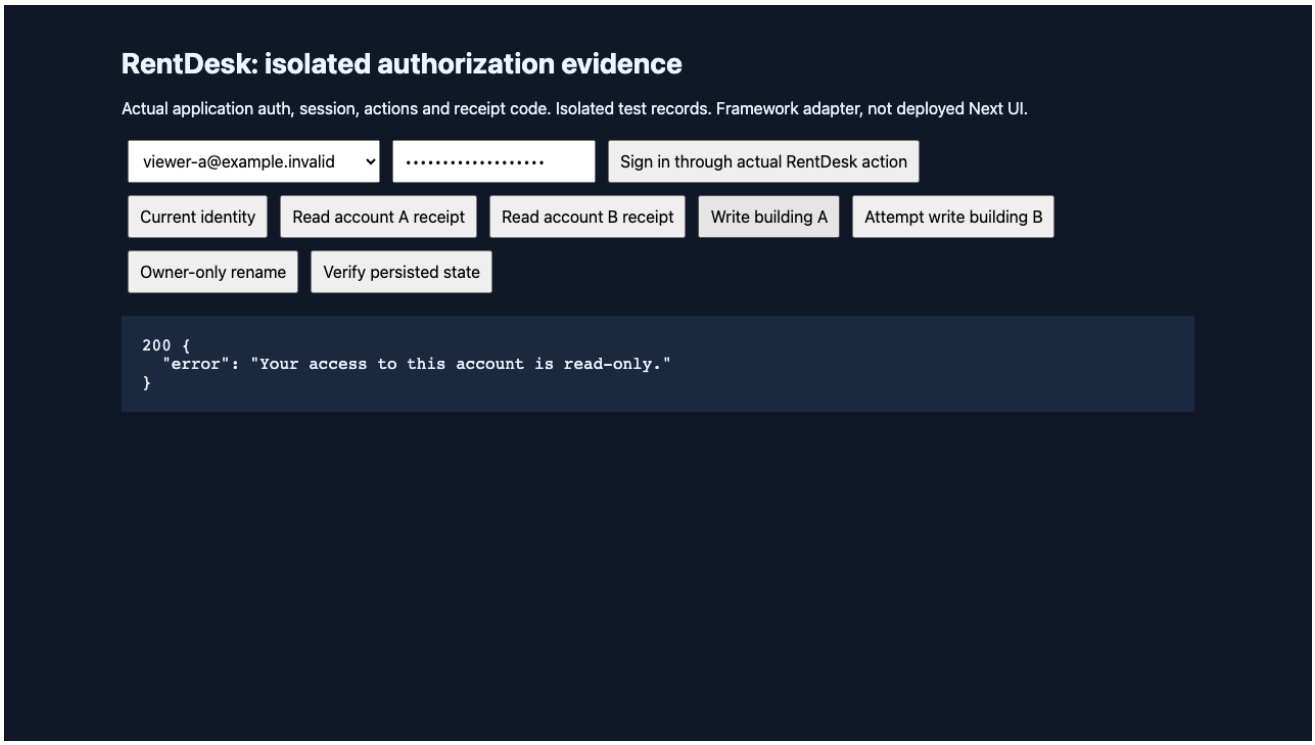
P1 - Extend the object coverage. Test lease, tenant, rent, note and receipt mutation paths with the same two identities and a restricted manager. Exit condition: reciprocal foreign IDs and denied buildings remain inaccessible and unchanged. The current sample proves only the named paths, not every resource.

P2 - Complete the service-specific steps with authentic records. Retain buyer-confirmed scope, actual check evidence and the prioritized plan; record the real accepted report delivery. For Pro, perform the 30 minute walkthrough and re-audit after changes. Neither a file hash nor this sample stands in for a call, email receipt or customer service completion.

Browser evidence: access and role refusal

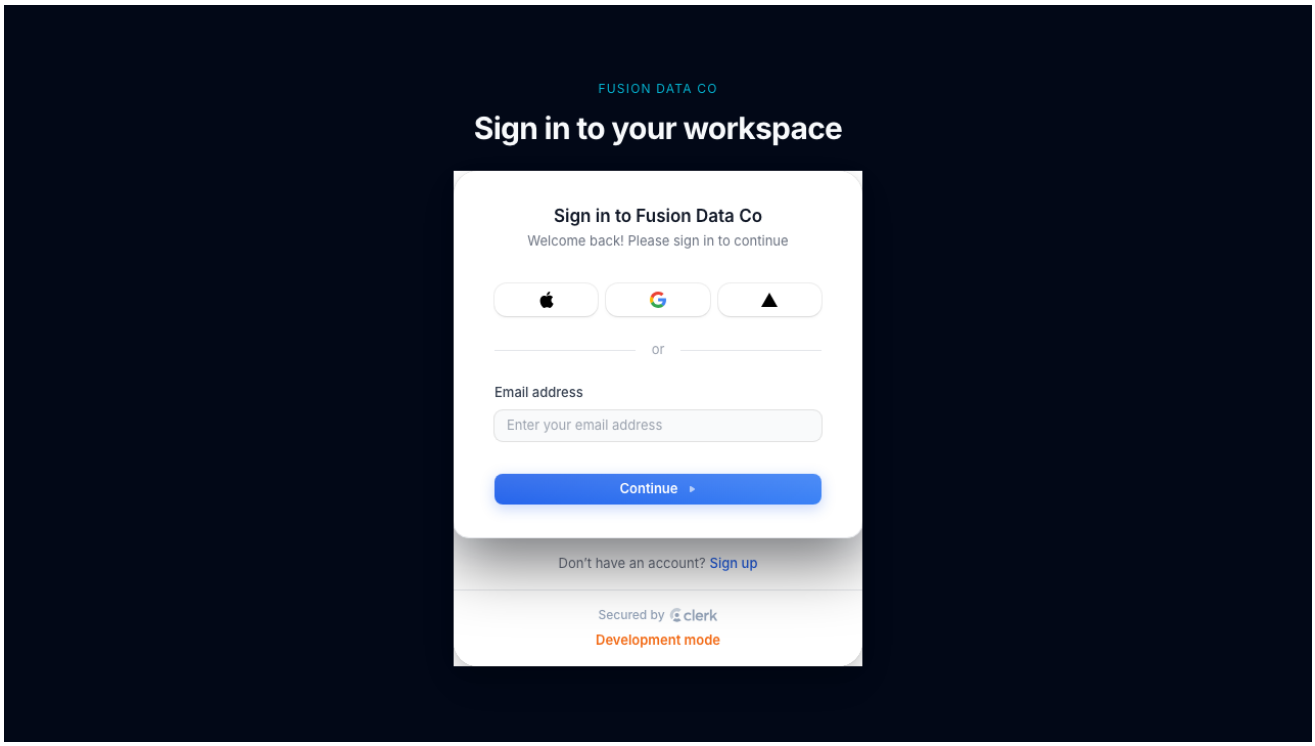


01. Owner A, signed in through the real RentDesk action, attempts the other account receipt. The actual receipt handler returns 404.



03. Viewer identity calls the actual building-write action. The error is the application action result; the adapter HTTP 200 is not a successful write.

Live boundary and reproducibility



06. Browser entry from fusiondataco.com/admin reaches the Fusion sign-in gate. No production credentials were entered.

Reproduce the isolated run: start isolated-rentdesk.cjs from this evidence directory with existing Audit and RentDesk dependencies, then run check-api.py and check-browser.py. The adapter binds only 127.0.0.1:4318. Stop it after use. It mints only synthetic sessions against PGlite.

Transport substitutions: PGlite replaces Neon; a request-local cookie/header bridge replaces Next request context; redirect becomes an evidence response; cache revalidation is a no-op. Outbound fetch and mail are forbidden. Authentication, bcrypt, HMAC, session database lookup, role/property guards and selected action/route code are the real application source.

Evidence index: api-checks.json (21 assertions and observed results), isolated-http.jsonl (request/results, no passwords or cookies), browser-operations.json (actual browser operations), live-storefront-api.json (three live denials), source-manifest.json (revision and SHA-256 of tested files), screenshots 01-06. The machine-readable evidence belongs with this report.

Residual limits: no claim of full deployment penetration testing, SSO/Clerk coverage, CSRF coverage, session-revocation coverage, a customer sale, accepted external email, completed call or completed re-audit. There were no confirmed vulnerabilities to retest. The listed follow-ups are coverage work, not invented defects.