ClearPath RD

clearpathrd.com

Admin Dashboard Specification

Version 1.0 — February 2026 — Confidential

What this document covers

- Architecture — where /admin lives, how it is protected, middleware stack
- Role model — admin vs support permissions matrix across all 20 actions
- Navigation structure — sidebar, route map, and breadcrumb conventions
- 8 screen specifications — each with route, access roles, columns, actions, filters, and notes
- Destructive action confirmation pattern — modal confirmation for irreversible actions
- Audit log requirements — what gets logged, where, and how long it is retained
- Platform metrics dashboard — 8 KPI cards with data sources
- Implementation checklist

1. Architecture

1.1 Location and Route Prefix

The admin dashboard is built into the ClearPath Next.js app under the /admin route prefix. It is not a separate service or subdomain. All admin routes are protected at the middleware level before any page component renders.

Property	Specification
Base route	/admin
File location	app/(admin)/ route group in the Next.js App Router
Layout file	app/(admin)/layout.tsx — wraps all admin pages with the admin shell (sidebar, header, role check)
Middleware	middleware.ts checks: (1) user is authenticated via Supabase Auth session, (2) users.role IN (admin, support). Unauthenticated → redirect to /login. Authenticated non-admin → redirect to /dashboard with a 403 toast.
Server-side role check	Every admin API endpoint (/api/v1/admin/*) independently verifies role = admin or support via the Supabase JWT. Middleware is defence-in-depth, not the primary control.

1.2 Admin Shell Layout

All admin pages share a consistent shell:

- Left sidebar (fixed, 240px): ClearPath RD logo, nav links for each section, current user name and role badge at the bottom, "Back to app" link
- Top header bar: page title, breadcrumb, and a global search input (searches users and orders by email or ID)
- Main content area: page-specific content
- No mobile layout required for MVP — admin is desktop-only

1.3 API Endpoints

Admin pages call /api/v1/admin/* endpoints on the Fastify API. All admin endpoints require role IN (admin, support) unless otherwise noted. Endpoints that perform mutations (refunds, cancellations, state changes) require role = admin specifically.

2. Role Model

2.1 Role Definitions

Role	Description
admin	Full access to all admin screens and all actions. Can promote other users to support or admin. This role should be held by at most 2–3 people at MVP.
support	Read access to all admin screens. Can perform a limited set of non-destructive actions (flag user, edit contractor listing). Cannot issue refunds, cancel sessions, enter results, supersede certificates, or promote users.
user (default)	No access to /admin. Redirected to /dashboard.

2.2 Permission Matrix

All 20 admin actions and which roles can perform them:

Action	admin	support
View user list and profiles	✓	✓
Search users by email / name	✓	✓
Edit user name, phone	✓	✗
Promote user to support or admin role	✓	✗
Flag user for review	✓	✓
View order list and detail	✓	✓
Issue refund	✓	✗
Resubmit order to lab	✓	✗
View session list and detail	✓	✓
Cancel session	✓	✗
Manually advance session state	✓	✗
Enter result on behalf of user	✓	✗
Supersede certificate	✓	✗
View certificate detail	✓	✓
View contractor listings	✓	✓
Add contractor listing	✓	✗
Edit contractor listing	✓	✓
Delete contractor listing	✓	✗
View email log	✓	✓
View platform metrics	✓	✓

3. Navigation Structure

3.1 Sidebar Links

Nav label	Route	Access
Overview	`/admin`	admin, support
Users	`/admin/users`	admin, support
Orders	`/admin/orders`	admin, support
Sessions	`/admin/sessions`	admin, support
Results & Certs	`/admin/results`	admin, support
Contractors	`/admin/contractors`	admin, support
Email Log	`/admin/email-log`	admin, support
Metrics	`/admin/metrics`	admin, support

3.2 Detail Page Routes

Each list screen has a corresponding detail page at /:id. Detail pages show the full record and expose action buttons appropriate to the viewer's role.

Detail route	Shows
`/admin/users/:id`	Full user profile, all homes, all orders, all sessions, email log for this user
`/admin/orders/:id`	Order detail, payment status, Stripe payment intent link, session(s), lab submission status
`/admin/sessions/:id`	Session detail, full status history, email log for this session, result (if entered), certificate (if issued)
`/admin/results/:sessionId`	Result entry form or result display + certificate detail + supersede action
`/admin/contractors/:id`	Contractor detail and edit form

4. Screen Specifications

> *Convention: all list screens are paginated (20 rows per page). All list screens support a global text search. Actions marked [admin only] are hidden entirely from support users — not just disabled.*

4.1 Overview Dashboard

Overview Dashboard

Route: `/admin` Access: **admin** **support**

Landing page for the admin section. Shows high-level KPI summary cards and recent activity feed.

Columns / fields	Actions	Filters / search	Notes
• 8 KPI metric cards (see Section 6) • Recent orders (last 10, with status badges) • Recent sessions with status changes (last 10) • Flagged users requiring review	• Click any card → navigates to the relevant list screen • Click any row in recent activity → navigates to detail page	• No filters on overview — it is a summary page	• Metrics are computed on page load (no real-time updates for MVP) • Cache metrics for 5 minutes to avoid hammering the database on every admin page load

4.2 Users

User Management

Route: `/admin/users` Access: **admin** **support**

Paginated list of all registered users. Supports search and filtering by role and flag status.

Columns / fields	Actions	Filters / search	Notes
• Name (first + last) • Email • Role badge (user / support / admin) • Registered date • Order count • Flagged indicator	• View profile → /admin/users/:id • Flag / unflag user (both roles) • Edit name, phone [admin only] • Promote to support or admin [admin only]	• Search by name or email • Filter by role • Filter by flagged = true • Sort by registered date (default: newest first)	• Flagged users appear with an amber indicator in the list • Promoting a user to admin requires a second confirmation modal: "This will give full admin access. Are you sure?" • Role changes are audit-logged

4.3 Orders

Order Management

Route: `/admin/orders` Access: **admin** **support**

Paginated list of all kit orders. Primary tool for investigating payment issues and triggering refunds or lab resubmissions.

Columns / fields	Actions	Filters / search	Notes
• Order ID (short) • User name + email • Product SKU • Amount (CAD) • Tax (CAD) • Payment status badge • Paid date • Lab submission status	• View order detail → /admin/orders/:id • Issue full refund [admin only] • Issue partial refund [admin only] • Resubmit to lab [admin only] — if initial submission failed	• Search by order ID or user email • Filter by payment_status (pending / paid / failed / refunded) • Filter by lab submission status • Date range picker for paid_at • Sort by paid_at (default: newest first)	• Resubmit to lab is only shown if lab_submission_status = failed • Refund action opens a modal with amount input and reason field — reason is stored in audit log • Link to Stripe dashboard for the payment intent is shown on the detail page

4.4 Sessions

Session Management

Route: `/admin/sessions` Access: **admin** **support**

Paginated list of all test sessions across all users. Used to investigate stuck sessions, manually advance state when the user cannot, and cancel sessions after a refund.

Columns / fields	Actions	Filters / search	Notes
• Session ID (short) • User name • Kit type badge • Kit serial • Status badge • Activated date • Expected completion date • Days overdue (if applicable)	• View session detail → /admin/sessions/:id • Cancel session [admin only] — with reason • Mark as retrieved [admin only] — if user cannot self-serve • Mark as mailed [admin only] — if user cannot self-serve • Enter result → navigates to /admin/results/:sessionId [admin only]	• Search by session ID, user email, or kit serial • Filter by status • Filter by kit type • Filter by overdue (expected_completion_date < today AND status NOT IN completed/expired/cancelled) • Sort by expected_completion_date (default)	• Overdue sessions (past expected completion date with no result) should be highlighted with an amber row background • State-advancing actions (mark retrieved, mark mailed) are only shown when the session is in the correct preceding status • Cancel requires a reason string — stored in audit log and on the session record

4.5 Results & Certificates

Results & Certificate Management

Route: `/admin/results` Access: **admin** **support**

Used to enter results on behalf of users (lab email received, user unable to self-serve) and to manage certificate supersession after lab errors.

Columns / fields	Actions	Filters / search	Notes
• Session ID • User name • Kit serial • Result value (Bq/m³) if entered • Zone badge if entered • Certificate status badge • Certificate number if issued	• Enter result for session [admin only] — opens result entry form • Supersede certificate [admin only] — requires reason string • View certificate → /admin/results/:sessionId (certificate detail, download link, verify link) • Download certificate PDF	• Search by session ID, user email, kit serial, or certificate number • Filter by result entered = yes/no • Filter by certificate status (pending / valid / expired / superseded / failed)	• Result entry form: value_bqm3 input, recorded_at date picker, lab_reference text field (optional) • After result entry, certificate generation fires automatically — admin can refresh to see certificate status • Supersede requires a plain-text reason — logged to audit log

			and stored on the certificate record • If certificate generation failed (status = failed), show a "Retry generation" button [admin only]

4.6 Contractor Directory

Contractor Directory Management

Route: `/admin/contractors` Access: **admin** **support**

Manage the contractor listings shown to users after elevated-result certificates. Support can edit existing listings; only admin can add or delete.

Columns / fields	Actions	Filters / search	Notes
• Company name • Contact name • Province(s) served • Services offered badges • C-NRPP number • Status badge (active / inactive / pending_review) • Featured flag	• Add contractor [admin only] — opens creation form • Edit contractor (both roles) — opens edit form • Set featured / unfeatured [admin only] • Set status active / inactive [admin only] • Delete contractor [admin only] — with confirmation modal	• Search by company name, contact name, or C-NRPP number • Filter by province • Filter by status • Filter by featured = true	• Featured contractors appear first in the public directory, above the fold • C-NRPP number must be entered for the listing to have status = active • Deletion is soft-delete (status = deleted) — records are not removed from the database

4.7 Email Log

Email Log

Route: `/admin/email-log` Access: **admin** **support**

Read-only view of all emails sent or queued by the system. Used to investigate delivery failures, confirm emails were sent, and check bounce rates.

Columns / fields	Actions	Filters / search	Notes
• Recipient email • Email type badge • Status badge (queued / sent / delivered / bounced / failed) • Scheduled at • Sent at • Resend message ID • Session ID (link)	• Resend via Resend dashboard link (opens Resend dashboard in new tab) — no direct resend action in ClearPath for MVP • View associated session → /admin/sessions/:id	• Search by recipient email or session ID • Filter by email_type • Filter by status • Date range picker for sent_at • Filter by bounced = true	• Bounced emails are highlighted with a red row background • Users with 3+ consecutive bounces are flagged automatically by the system — their user record shows a bounced indicator • No resend action in ClearPath admin for MVP — admin uses Resend dashboard to investigate and resend if needed

4.8 Metrics

Platform Metrics

Route: `/admin/metrics` Access: **admin** **support**

High-level KPI dashboard showing platform health, revenue, and test outcome distribution.

Columns / fields	Actions	Filters / search	Notes
• 8 KPI cards (same as overview, with more detail) • Results by zone: bar chart or table breakdown • Revenue trend: monthly totals for last 6 months (table, not chart, for MVP) • Top provinces by order volume	• Export metrics as CSV [admin only] — calls GET /api/v1/admin/metrics?format=csv	• Date range selector (default: current month) • Compare to previous period toggle	• Metrics are calculated server-side via the GET /api/v1/admin/metrics endpoint • For MVP, no real-time updates — data is fresh on each page load • The results by zone breakdown is the most important metric for validating the product's market (what proportion of homes have elevated readings)

5. UI Patterns

5.1 Destructive Action Confirmation

Any action that cannot be undone must be confirmed via a modal dialog before executing. This applies to: refunds, session cancellation, certificate supersession, contractor deletion, and user role promotion to admin.

Property	Specification
Modal title	Describes the action clearly. e.g. "Cancel session CPR-2026-000142?"
Modal body	One sentence explaining what will happen. e.g. "This will cancel the test session and all associated queued emails. This cannot be undone."
Reason field	Required for: session cancellation, certificate supersession, refunds. Optional for others. Stored in audit log.
Confirm button	Red background for destructive actions. Label matches the action verb: "Cancel session", "Issue refund", "Supersede certificate".
Cancel button	Secondary style. Closes modal with no action taken.
Keyboard behaviour	Escape closes the modal. Enter does not confirm (prevents accidental confirmation).

5.2 Status Badges

Consistent colour-coded badges are used throughout the admin UI. Badge colours match the user-facing app for consistency.

Status	Badge colour
paid / valid / active / delivered	Green badge
pending / queued / ordered	Grey badge
failed / cancelled / expired / bounced	Red badge
action_required / superseded / flagged	Amber badge
refunded / partially_refunded	Purple badge
support (role)	Navy badge
admin (role)	Teal badge

5.3 Pagination

All list screens use cursor-based pagination (not offset). 20 rows per page. The API returns a nextCursor token. The frontend passes cursor= as a query parameter to fetch the next page. Previous page is not supported (users navigate forward only) — upgrade to bidirectional pagination in v2.

6. Platform Metrics — KPI Cards

Eight metric cards appear on both the Overview and Metrics screens. Each card shows a number, a label, the data source, and the measurement period.

Total users `users.count` All time	**Active sessions** `test_sessions WHERE status=active` Live count	**Completed this month** `results WHERE recorded_at >= month_start` Rolling month	**Revenue this month** `kit_orders WHERE paid_at >= month_start` CAD, excl. tax
Results by zone `results GROUP BY zone` All time	**Certificates issued** `certificates WHERE status=valid` All time	**Contractor leads** `contractor_leads COUNT` This month	**Email bounce rate** `email_log bounced/sent` Rolling 30 days

6.1 Metrics API Endpoint

GET /api/v1/admin/metrics returns all eight metrics in a single response. The endpoint accepts optional start_date and end_date query parameters for date-range filtering (used by the Metrics screen). The Overview screen always uses the current month.

```
// Response shape
{
  "totalUsers": 142,
  "activeSessions": 38,
  "completedThisMonth": 14,
  "revenueThisMonthCad": 1649.86,
  "resultsByZone": {
    "below_guideline": 89,
    "caution": 23,
    "action_required": 11,
    "urgent_action": 2
  },
  "certificatesIssued": 125,
  "contractorLeadsThisMonth": 8,
  "emailBounceRate": 0.012
}
```

7. Audit Log

Every admin action that mutates data must be logged. The audit log is the authoritative record of who did what and when. It is separate from the application logs and is queryable by admins.

7.1 What Gets Logged

Action	Fields logged
Refund issued	admin_id, order_id, amount_cad, reason, timestamp
Session cancelled	admin_id, session_id, reason, previous_status, timestamp
Session state advanced	admin_id, session_id, from_status, to_status, timestamp
Result entered by admin	admin_id, session_id, value_bqm3, lab_reference, timestamp
Certificate superseded	admin_id, certificate_id, reason, timestamp
User role changed	admin_id, target_user_id, from_role, to_role, timestamp
User flagged / unflagged	admin_id, target_user_id, action (flagged/unflagged), timestamp
Contractor created / updated / deleted	admin_id, contractor_id, action, changed_fields, timestamp
Lab order resubmitted	admin_id, order_id, timestamp

7.2 Storage

For MVP, audit log entries are stored in a dedicated audit_log table in the PostgreSQL database. Schema: id (UUID), admin_id (FK users), action (string), entity_type (string), entity_id (UUID), payload (JSONB), created_at (timestamptz).

The audit log table is append-only. No admin can delete audit log records — the API has no DELETE endpoint for audit_log. Retention: indefinite for MVP.

7.3 Viewing the Audit Log

For MVP, the audit log is not exposed as a dedicated admin screen. It is visible inline on detail pages: the user detail page shows all audit entries for that user, the order detail page shows all entries for that order, and so on. A dedicated /admin/audit-log screen can be added in v2.

8. Implementation Checklist

Auth and middleware

- Implement middleware.ts: check Supabase Auth session + role check for /admin routes
- Add admin and support values to UserRole enum in Prisma schema (already in schema)
- Implement role check in all /api/v1/admin/* Fastify route handlers
- Create initial admin user: set role = admin on a user record via Supabase Table Editor before the admin UI exists

Layout and navigation

- Implement app/(admin)/layout.tsx with sidebar and top header
- Implement sidebar nav with all 8 links
- Implement role-based action visibility (hide [admin only] actions from support users)
- Implement global search in header (search users and orders by email/ID)

Screen implementation order (suggested)

- 1. Metrics — read-only, good first screen to build (validates API connectivity)
- 2. Users — read-heavy, confirms auth and role display
- 3. Orders — needed early for manual order investigation during soft launch
- 4. Sessions — needed for manual state advancement if users get stuck
- 5. Results & Certificates — needed for admin result entry (lab email path)
- 6. Email Log — needed for delivery issue investigation
- 7. Contractors — needed before elevated-result certificates start appearing
- 8. Overview Dashboard — can be assembled from components already built

Patterns

- Implement reusable ConfirmModal component for all destructive actions
- Implement StatusBadge component with all status/colour mappings
- Implement PaginatedTable component with cursor-based pagination
- Implement AuditLogger utility in src/services/audit.ts

End-to-end tests

- Confirm support user cannot see [admin only] action buttons
- Confirm non-admin user is redirected away from /admin
- Confirm refund flow: issue refund → Stripe refund created → session cancelled → audit log entry created
- Confirm result entry by admin: enter result → certificate generated → certificate_ready email sent
- Confirm certificate supersession flow

— *End of Admin Dashboard Specification* —

ClearPath RD | clearpathrd.com | Version 1.0 | February 2026