

Backend → GUI Coverage Audit (Maritime Onboarding System)

Last updated: August 2025
Owner: Shipdocs — Middelweg 211, 1911 EE Uitgeest, Netherlands

Executive Summary

This audit verifies whether all backend services (API endpoints, services) have corresponding, accessible web GUIs. The system has strong coverage for core admin, manager, and operational features; however, several compliance and operations capabilities lack GUIs and require direct API/CLI usage.

- Overall GUI Coverage: High for Admin/Manager features (Managers, System Settings, Templates, Audit, Security, Performance)
 - Highest-priority gaps (P1):
 - Access Reports (GDPR Article 15): No UI for creation/download
 - User Data Export + Status/Download (GDPR Portability): No profile UI
 - Account Deletion (GDPR Article 17): No self-service UI
 - Admin Feature Flags: No toggle/rollout management UI
 - Incident Center (events/webhooks): No admin UI
-

Methodology

- Mapped 128 API endpoints to React routes/components
 - Reviewed AdminDashboard tabs and nested components
 - Verified client services calling admin privacy/security/performance endpoints
 - Cross-checked with E2E admin flows where relevant
-

Coverage Matrix (Highlights)

- Admin Dashboard
 - Managers: CRUD (present)
 - Templates: list/create/edit/preview/delete (present)
 - Performance: metrics, export (present)
 - Security: events & metrics, export (present)
 - Audit Log: filter/paginate (present)
 - System Settings: categorized settings UI (present)
 - Content Management: rich training content editor (present)
 - Manager Dashboard
 - Crew CRUD, bulk actions, emails, approvals (present)
 - Crew Profile
 - MFA management (present)
 - Data privacy actions (missing)
-

Missing GUIs (Details)

1. GDPR Access Report (API: GET /api/privacy/access-report)

- Current: API only. No UI for users/admins to request access reports, filter, and download.
- Impact: Manual/API requests slow compliance workflows; users cannot self-serve.
- Priority: P1
- Effort: 1–2 days
- Proposal: Add Profile → Privacy tab and Admin → Compliance tab with report form (user/company, date range, format) and results grid + CSV download.

2. User Data Export: Request/Status/Download

- APIs: POST /pages/api/user/export-data, GET /pages/api/user/export-status/[id], GET /pages/api/user/download-export/[id]
- Current: API only. No profile UI to request/check/download exports.
- Impact: Users cannot perform GDPR data portability via web.
- Priority: P1
- Effort: 1.5–2.5 days
- Proposal: Profile → Privacy tab section “My Data Export” with Request button, recent jobs list (status, links), download button.

3. Account Deletion (API: DELETE /api/privacy/delete-account)

- Current: API only. No self-service UI with password/MFA verification.
- Impact: GDPR erasure requires support/API calls; higher admin burden.
- Priority: P1
- Effort: 1–1.5 days
- Proposal: Profile → Privacy tab “Delete Account” flow with confirmation, verification code (password/TOTP), warnings, and success receipt.

4. Feature Flags Admin (API: /api/admin/feature-flags)

- Current: Client-side environment featureFlags.js exists; no admin UI to toggle or scope flags.
- Impact: Slows controlled rollouts; tracing/rollback less safe.
- Priority: P1
- Effort: 1.5–2.5 days
- Proposal: Admin → Settings or a new “Feature Flags” tab to list flags, toggle per environment, add notes, and audit changes.

5. Incident Center (APIs: /api/incidents/index|[id]|stats|webhook)

- Current: No incident overview UI, no webhook test utility.
- Impact: Limited visibility/triage; operations rely on logs/API.
- Priority: P1
- Effort: 2–3 days
- Proposal: Admin → Incidents center listing active/resolved incidents, drill-down details, filters, status changes, webhook test tool.

6. Maintenance/Cron & Admin Tools

- APIs: /api/cron/*, /api/admin/cleanup-tokens, run/test notification migrations
- Current: No guarded admin panel for manual triggers.
- Impact: Direct calls are risky and inconvenient.
- Priority: P2
- Effort: 1.5–2 days
- Proposal: Admin → Maintenance tab with protected actions, confirmations, and minimal output.

7. Configuration Keys Explorer/Editor

- APIs: /api/config/[key], /api/config/batch (SystemSettings covers many but not generic keys)
- Impact: Non-modeled keys require manual calls.
- Priority: P2

- Effort: 2 days
- Proposal: Admin → Advanced Config explorer (read-only and editable keys, search, masking, audit).

8. Content Import/Export UI

- Client service supports export/import, but no visible buttons/flows.
- Impact: Slower migrations/backups of content.
- Priority: P2
- Effort: 1.5–2 days
- Proposal: Content Management page: “Export selected phases” + “Import from file” with validation and progress.

9. Backup Management & Retention UI

- Current: Backups/retention controlled via cron/config; no UI overview.
- Impact: Ops tasks are opaque; auditing is harder.
- Priority: P2
- Effort: 2–3 days
- Proposal: Admin → Data Management dashboard with backup schedule, manual trigger, last results, retention settings (with RLS policy notes).

10. Health/Uptime Aggregation Page

- APIs: /api/health/* (auth, email, storage, database)
- Impact: Diagnosis requires multiple calls.
- Priority: P3
- Effort: 1 day
- Proposal: Admin → Health page aggregating checks with color-coded status.

11. Roles/Permission Templates UI

- Current: Manager permissions set in forms; no centralized role templates.
- Impact: Harder to standardize and audit.
- Priority: P3
- Effort: 2–3 days
- Proposal: Admin → Roles & Permissions templates; assign templates to users.

Recommended Roadmap

- Sprint 1 (P1): Access Report UI, Data Export UI, Account Deletion UI
 - Sprint 2 (P1): Feature Flags Admin, Incident Center
 - Sprint 3 (P2): Maintenance/Cron tools, Config Explorer, Content Import/Export
 - Sprint 4 (P2/P3): Backup/Retention UI, Health/Uptime page, Role Templates
-

Acceptance Criteria (Samples)

- Access Report UI: Admin and users can generate reports; CSV/JSON export; RLS/authorization enforced; audit logged.
 - Data Export UI: Request flow with deduping of pending jobs; list shows status; download link works; expiration noted; audit logged.
 - Account Deletion UI: Explicit confirmation, verification (password/TOTP), last-admin protection; returns certificate; audit logged.
 - Feature Flags UI: List/toggle flags with change log; optional environment scoping; permission-gated.
 - Incident Center: List with filters; detail view; acknowledge/resolve actions; webhook test.
-

Notes

- This report reflects the current repository state and E2E/admin module flows
 - No external certification claims are included; security follows industry best practices
-

Contact

Shipdocs

Middelweg 211, 1911 EE Uitgeest, Netherlands

Email: info@shipdocs.app

DPO/Security: M. Splinter
