CLIENT SHARE COPY

KESHI ECTS

ECTS Client Documentation Pack

Client-facing documentation covering portal user workflows, architecture, technical overview, deployment, monitoring, incident handling, and recovery. Internal developer setup, source-level implementation detail, and repository-only engineering notes are intentionally excluded.

PREPARED FOR
ECTS client stakeholders

PREPARED BY
Keshi ECTS Engineering Team

PREPARED ON
March 12, 2026

AUDIENCE
Client, operations, program, IT

PACKAGE TYPE
Comprehensive external pack

INCLUDES
User guide, ops, technical overview

DISTRIBUTION
Client controlled circulation

Portal workflows | Architecture | Deployment | Monitoring | Recovery

1. Scope and Document Map

This pack is structured for client consumption. It explains what the platform does, how operational users work in the portal, how the production topology is organized, and how service continuity is managed. It is not a developer handbook.

Included in this pack

- Portal access, navigation, and end-user workflows
- Module-by-module operational coverage for Cargo, Journeys, Routes, Inventory, Alerts, Reports, Users, Settings, and Devices
- Architecture and runtime explanation at system and component level
- Deployment overview and operational topology
- Monitoring, incident handling, backup, restore, and recovery guidance
- Revision record and sign-off page for controlled sharing

Explicitly excluded

- Frontend and backend local setup instructions
- Repository structure, code ownership internals, and source-level extension notes
- Private implementation detail intended only for engineering teams
- Internal environment secrets, infrastructure credentials, and troubleshooting artifacts

How to use this document

READER	START HERE	WHAT TO FOCUS ON
Business sponsor or client lead	Platform overview, user workflows, operations checklist	Operational capability, support model, continuity planning
Operations manager	Navigation, alerts, reports, monitoring, incident response	Day-to-day platform control and escalation handling
Client IT or architecture reviewer	Architecture foundation, deployment overview, security and reporting flows	Integration posture, runtime boundaries, resilience model

Document structure aligns to client review, operations adoption, and governance sign-off.

2. Revision History and Approval Control

The revision record below makes the client pack suitable for controlled circulation, review feedback, and formal acceptance.

Revision history

VERSION	DATE	OWNER	SUMMARY
0.8	March 2, 2026	Keshi ECTS Engineering Team	Initial live-capture screenshots and workflow baseline assembled.
0.9	March 8, 2026	Keshi ECTS Engineering Team	Architecture diagrams, runtime flows, and operations content expanded.
1.0	March 10, 2026	Keshi ECTS Engineering Team	Client-safe release pack finalized, split volumes added, and distribution controls aligned.
1.1	March 12, 2026	Keshi ECTS Engineering Team	Expanded validated user workflows covering profile, alerts, journeys, inventory, maintenance, and device administration.

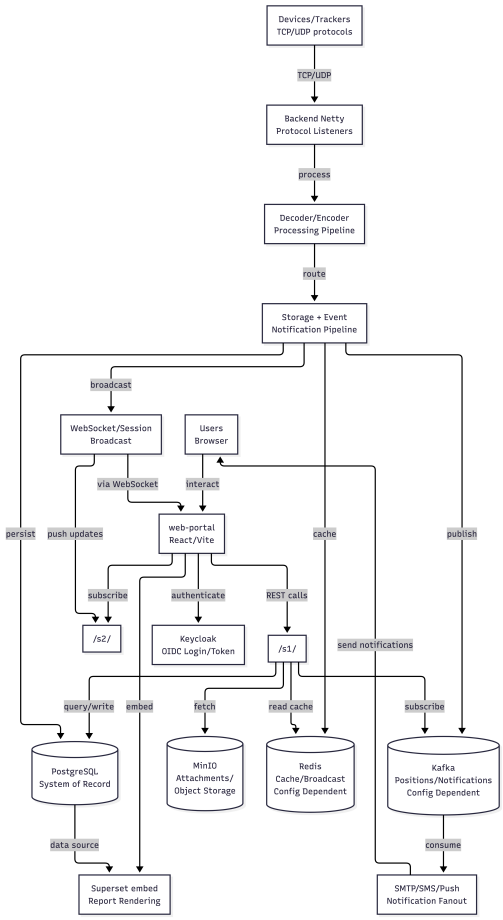
Document control

FIELD	VALUE
Current version	1.1
Classification	Client share
Primary owner	Keshi ECTS Engineering Team
Review cadence	Update after notable workflow, architecture, or operations changes
Companion volumes	User Guide, Operations and Deployment Guide, Technical Overview

This document is intended to stay synchronized with the live documentation site and the published client-share PDF volumes.

3. Platform Overview

ECTS is a logistics and control platform that combines operational workflow management, journey supervision, route governance, inventory visibility, fleet/device monitoring, alert handling, and reporting in one secured portal experience.



High-level system landscape showing client users, portal, services, data stores, and supporting platform capabilities.

Core business capabilities

- Initiate and manage cargo records and operational journeys.
- Define and govern route structures including checkpoints, authorities, and route holds.
- Track inventory position and assignment state across active operations.
- Observe and act on alerts, notifications, and device telemetry.
- Produce operational reports through embedded analytics.
- Administer users, permissions, preferences, and device assets.

Primary user groups

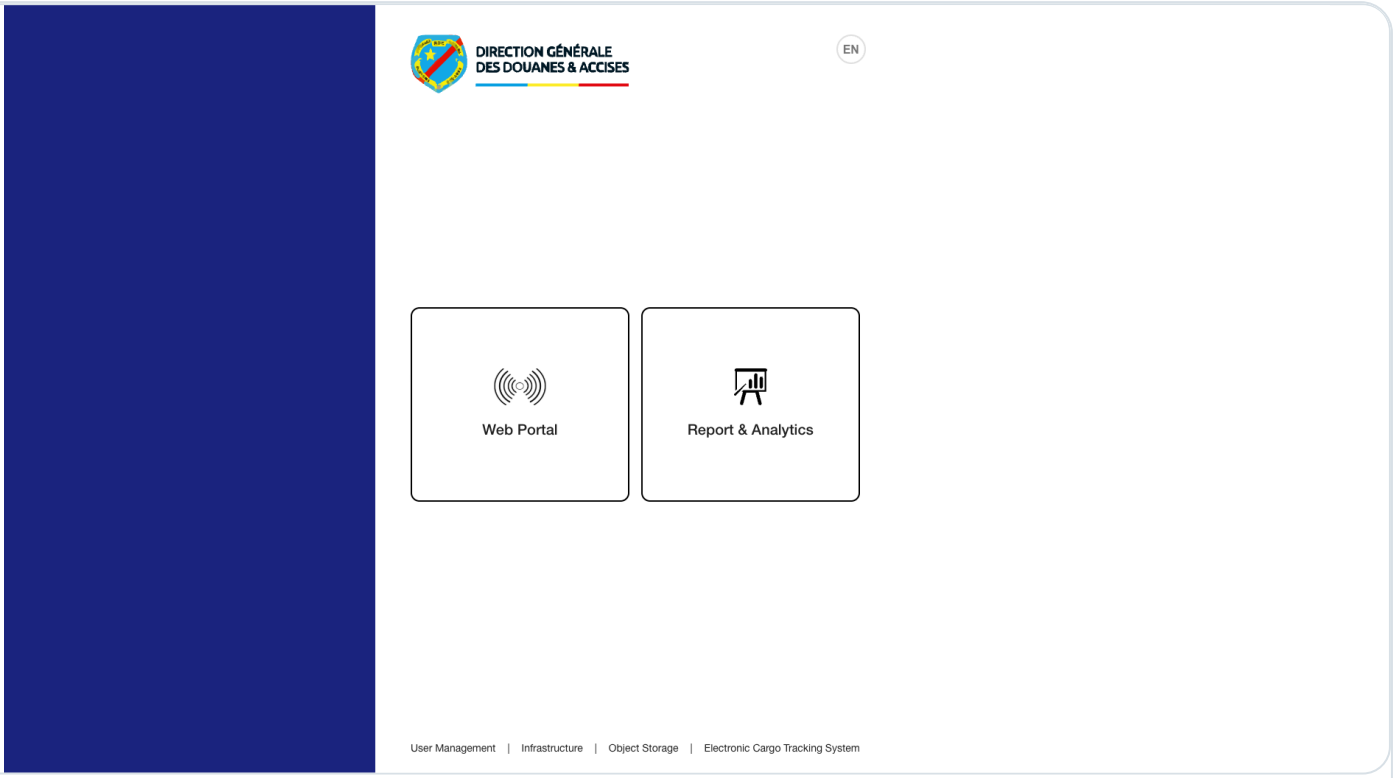
- Operations controllers and supervisors
- Security or control-room users handling alerts and incidents
- Administrators managing users, settings, and devices
- Client leads reviewing platform health and reporting outcomes

Portal module coverage

MODULE	PRIMARY PURPOSE	TYPICAL OPERATIONAL OUTCOME
Home	Map-based operational landing area	Immediate situational awareness after sign-in
Cargo and Journeys	Shipment and trip supervision	Controlled tracking of active and completed movement
Routes and Inventory	Planning and stock visibility	Governed route structure and current stock state
Alerts and Reports	Exception handling and analytics	Escalation control and business reporting
Users, Settings, Devices	Administration and fleet/device management	Managed access and operational device control

4. Portal Access and Navigation

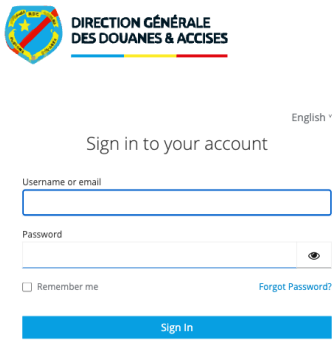
Standard access begins on the public landing page, continues through the identity provider, and ends at the home map after successful authentication. From there, users move through modules using the top navigation bar and page-level side menus.



STEP 1

Landing page entry

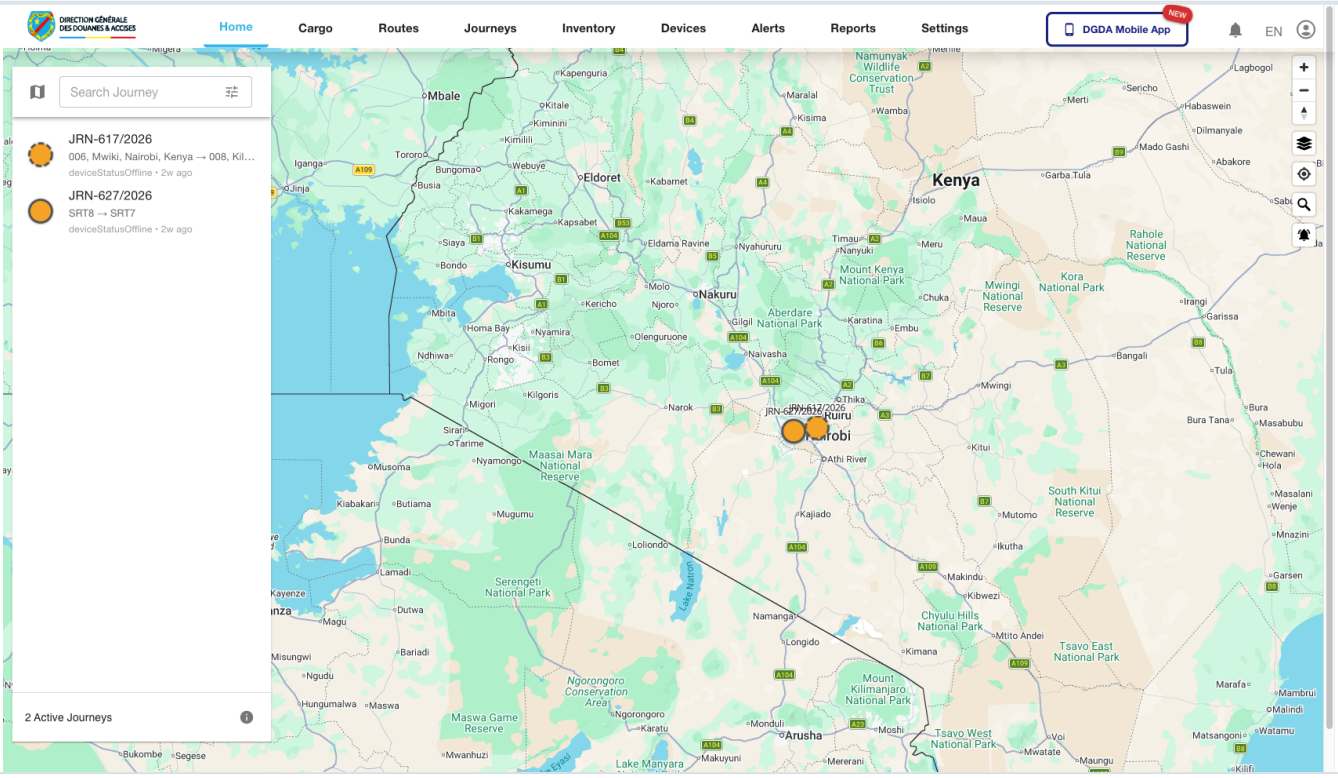
The public landing page exposes the platform entry point and reporting workspace.



STEP 2

Secure sign-in

Users authenticate through the centralized identity service before protected pages load.



STEP 3

Home map and shell

The authenticated home view exposes the operational map and full module navigation shell.

Navigation model

AREA	PURPOSE
Top navigation	Moves users between Home, Cargo, Routes, Journeys, Inventory, Alerts, Reports, Devices, and Settings.
Left navigation	Switches views inside the active module, such as lists, detail forms, dashboards, and setup pages.
Filters and search	Refine records by identifier, assignment state, route, status, or date.
Action controls	Open detail views, create records, export data, or trigger operational commands.

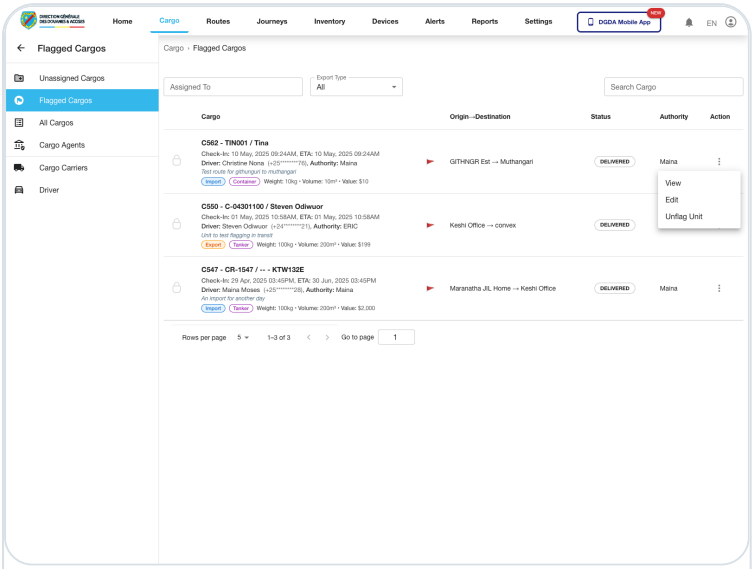
Access principles

- Protected pages require successful authentication before any operational data is displayed.
- Role-based access determines which modules and actions are available to each user.
- Operational pages are driven by live backend state and current permissions.
- Reporting pages load through a separate analytics path and may take longer than standard screens.

For training and user onboarding, this section works well as the first read before moving into module-specific flows.

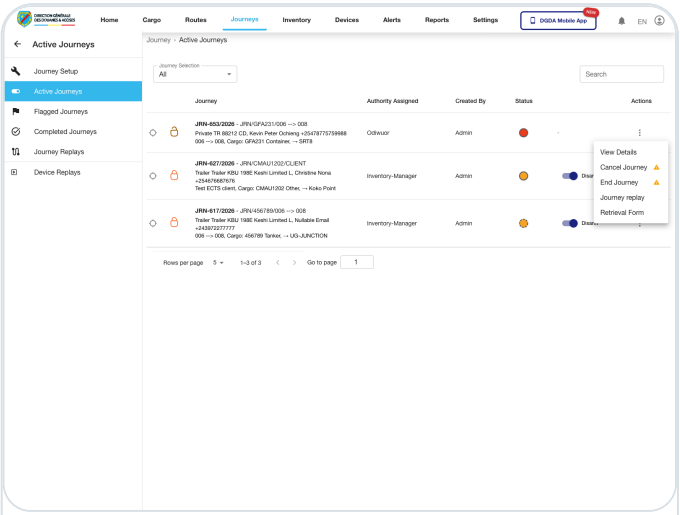
5. Cargo and Journey Workflows

Cargo and journey workflows support execution control. Users prepare cargo, investigate flagged units, maintain the carrier and driver registries, monitor active journeys, and open replay or cancellation entry points when movement needs closer inspection.



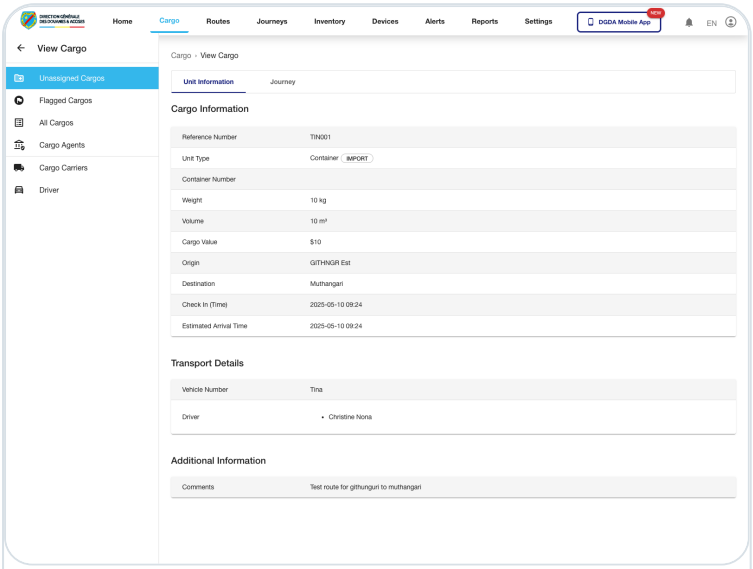
Cargo lifecycle coverage

- Review unassigned, assigned, flagged, and all cargo queues.
- Resume unfinished cargo drafts from the queue banner instead of recreating the record.
- Use the flagged queue to open detail, edit, or unflag entry points for exceptional cargo.
- Maintain the carrier and driver registries through row actions and dedicated add or edit forms.



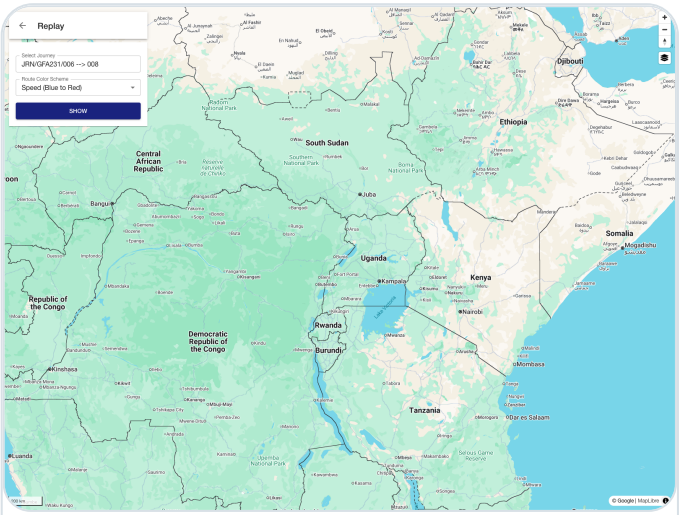
Journey supervision coverage

- Monitor active, flagged, and completed journey queues from the Journeys module.
- Open the row menu to reach detail, cancellation, completion, replay, and retrieval entry points.
- Use journey replay to re-run the movement trace in a map workspace.
- Cancellation is protected by a confirmation dialog and reason field before a change is committed.



Operational detail review

Flagged cargo opens into a full detail page where users can review cargo information, transport details, and additional context before taking further action.



Replay-oriented investigation

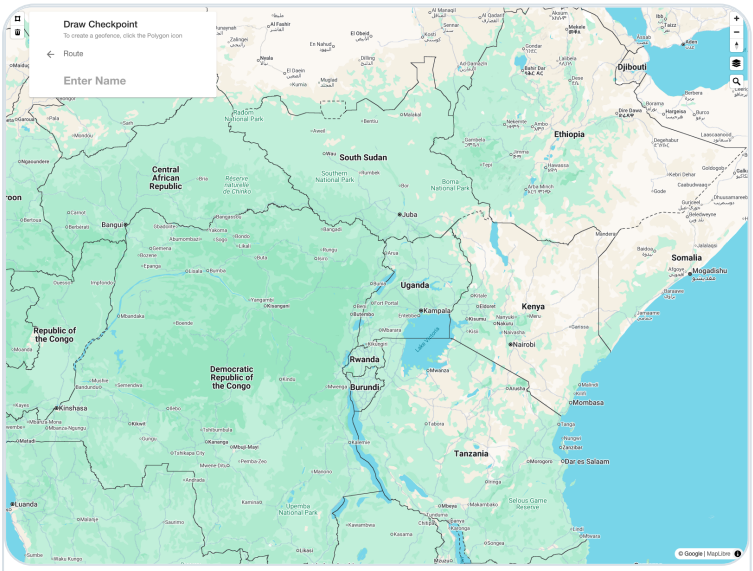
The replay workspace allows users to select a journey, choose the route color scheme, and inspect the movement trace in map form.

Typical user flow

STAGE	TYPICAL USER ACTION	EXPECTED OUTCOME
Queue review	Open the relevant cargo or journey queue and narrow it with filters.	The operator isolates the records that need attention now.
Registry validation	Check carrier and driver records before or during dispatch review.	Supporting transport records match the intended movement context.
Detail inspection	Open flagged cargo detail or journey detail/replay from row actions.	The user can validate state, investigate exceptions, or prepare follow-up action.
Controlled workflow change	Use cancel, end, unflag, or other state-change entry points where permitted.	High-impact changes remain protected by dedicated dialogs or action screens.

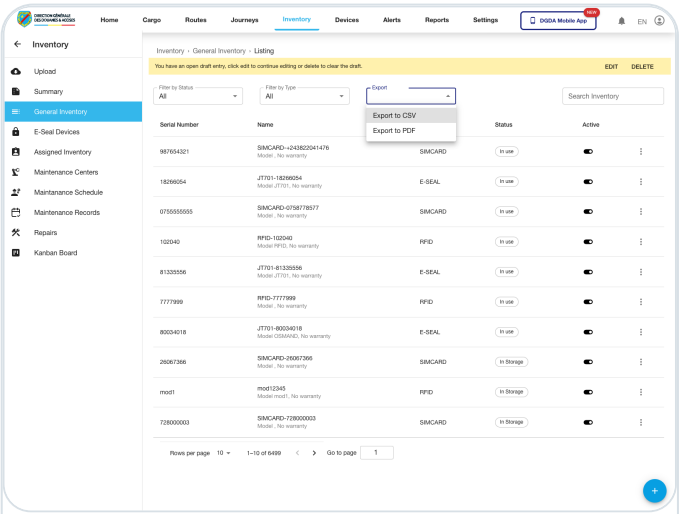
6. Routes, Inventory, Maintenance, Alerts, and Reports

These modules cover planning, control, exception handling, maintenance oversight, and analytics. Together they help users govern routes, maintain stock visibility, react to abnormal events, supervise maintenance workload, and consume formal reports.



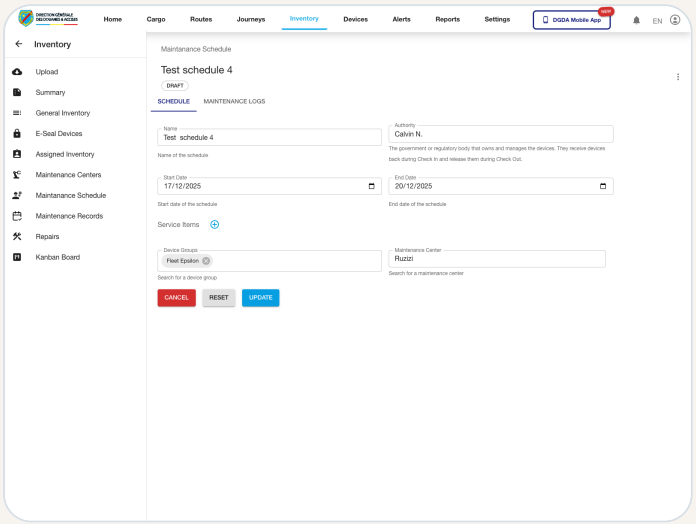
Routes and master data

- Routes rely on checkpoints, route authorities, holds, and corridors to govern movement.
- Checkpoint and corridor creation use map-based drawing workspaces.
- Corridor records expose edit and deactivate row actions from the corridor register.



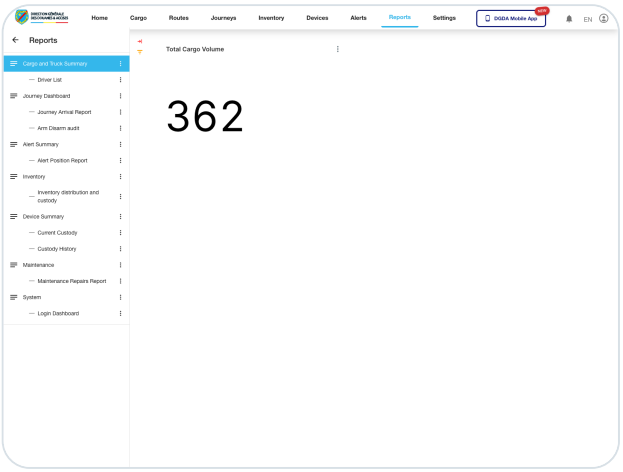
Inventory administration

- General Inventory is the main stock register with list filters and row actions.
- Exports are available as CSV or PDF.
- Item records expose dedicated detail, edit, and delete entry points.



Maintenance operations

- The Inventory module also exposes maintenance centers, schedules, records, repairs, and a kanban board.
- Maintenance center creation starts in a map-based `Draw Center` workspace with geofence drawing tools.
- Maintenance schedules expose row-level `View`, `Edit`, and `Delete` actions, and the edit page exposes schedule metadata, service items, device groups, and maintenance-center assignment.
- The kanban board gives supervisors a workflow-stage view of current workload.



Alerts and reports

- Alert queues support detail, close, and escalate entry points from the row menu.
- Alert detail pages centralize status review and top-level response controls.
- The live report catalog includes cargo, driver, journey, alert, inventory, device, maintenance, and system reporting families.
- Reports load through embedded analytics and should be allowed their normal extended load window.

Operational expectation for report pages

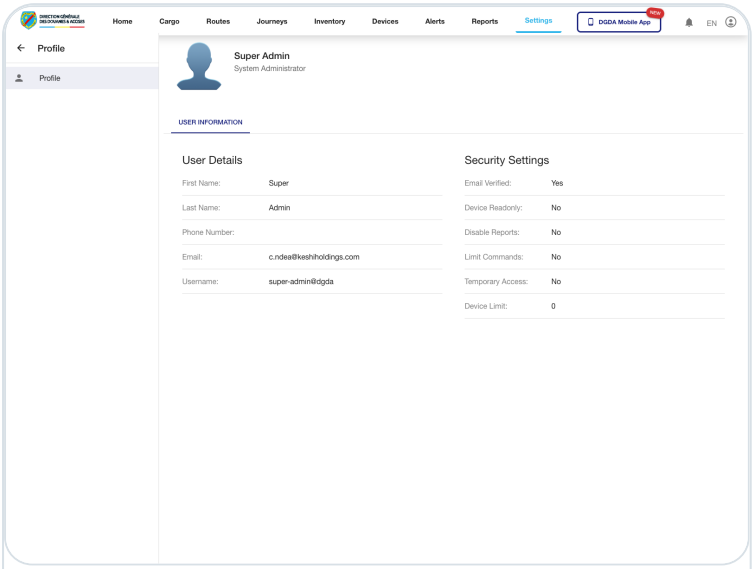
- Report pages are intentionally treated differently from normal list and form pages.
- The report catalog and selected report view may take a longer first-load window because analytics content is embedded asynchronously.
- Users should distinguish between expected loading behavior and true failure before escalating.

Where these modules matter most

- Routes: policy and execution governance
- Inventory and Maintenance: stock readiness, serviceability, and repair coordination
- Alerts: immediate response, event escalation, and controlled closure
- Reports: trend analysis, governance reporting, and stakeholder visibility

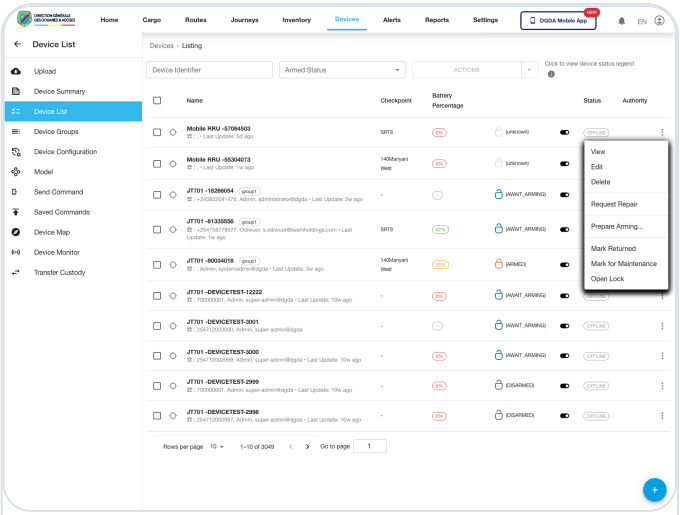
7. Administration, Settings, and Device Operations

Administrative pages support user governance and device lifecycle control. These areas are used by privileged operators to manage access, self-profile review, application preferences, and the hardware fleet.



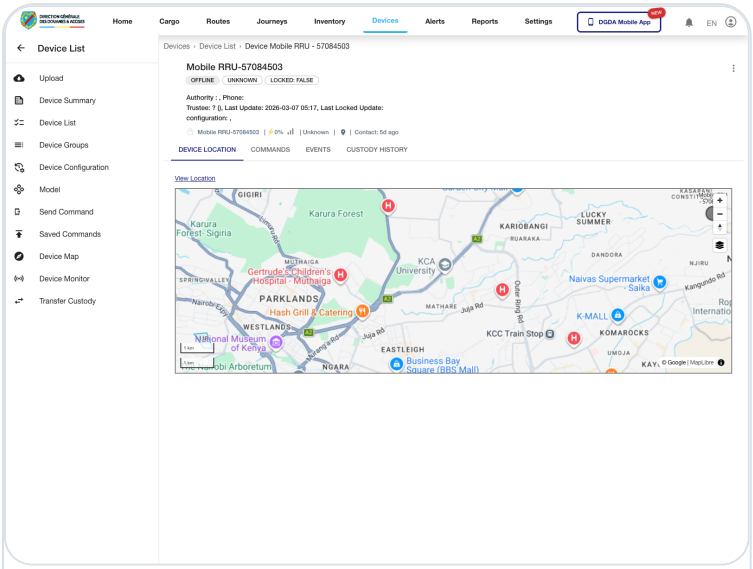
User and settings administration

- Open the account menu to review the signed-in user's own profile page.
- Search users, create accounts, and inspect user detail pages from Settings.
- Review preferences and other client-facing configuration screens from the Settings module.



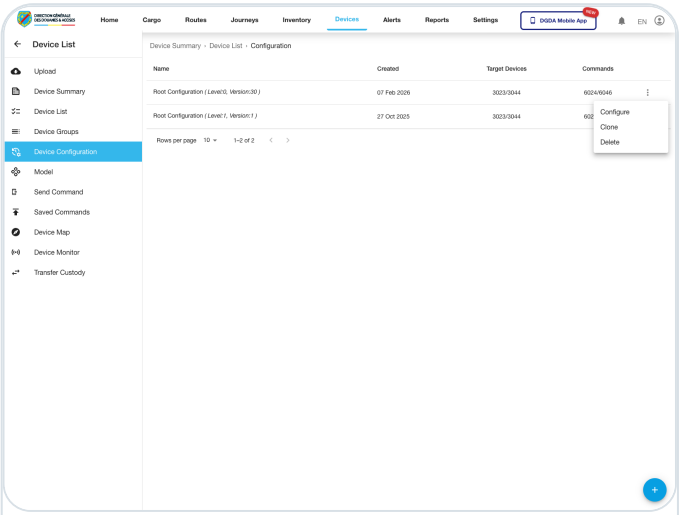
Device lifecycle management

- Device row menus expose view, edit, delete, repair, maintenance, return, arming, and lock-control entry points.
- Device detail pages expose location, command, and custody-history tabs.
- Device edit forms maintain model, configuration, and device-group assignments.
- Device configuration and model pages expose reusable action menus for ongoing administration.



Detail, command, and monitoring context

Device detail pages complement the main monitoring pages by consolidating location, command, and custody history for one selected device.



Configuration and model controls

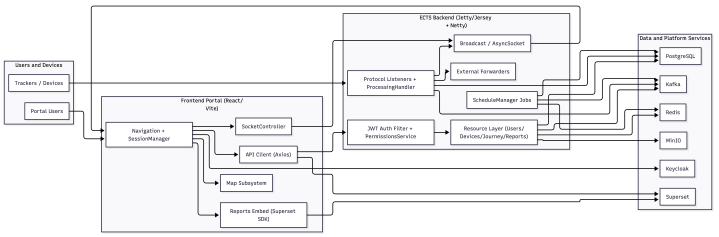
Saved configurations expose `Configure`, `Clone`, and `Delete`, while device models expose `Edit` and `Delete` and open into a dedicated model-edit form.

Typical administration outcomes

AREA	OPERATIONAL USE	EXPECTED RESULT
User administration	Create and govern user access, inspect roles, and support onboarding.	Authorized users can access the right screens and actions.
Settings	Review preference or portal-level options and allow users to inspect their own profile safely.	Consistent client operating configuration and visible user context.
Devices	Register, group, configure, inspect, monitor, and issue commands to devices.	Controlled device fleet operations and traceable changes.

8. Architecture and Technical Overview

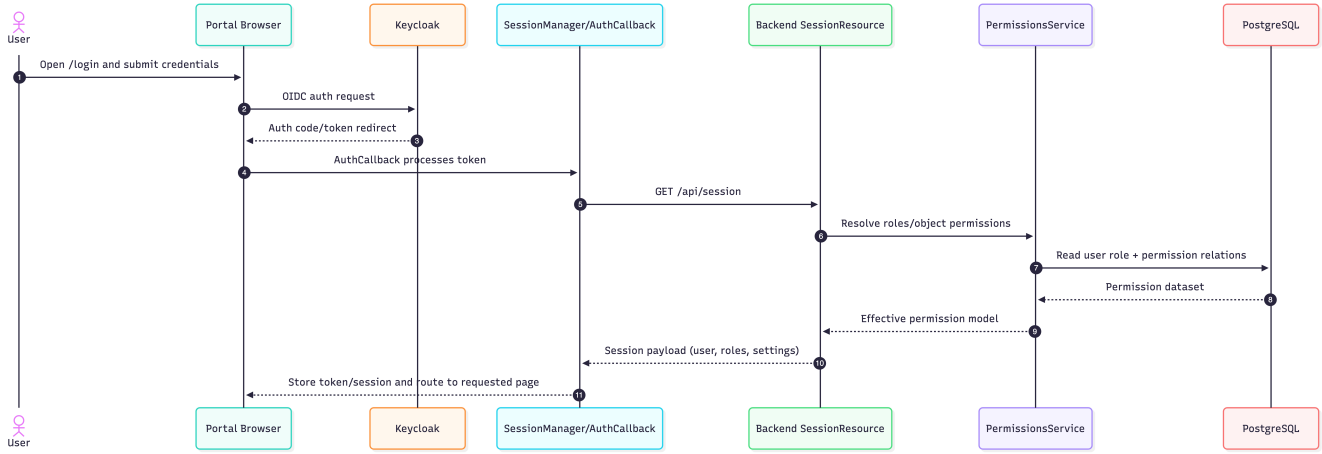
The technical model is intentionally presented at a client-safe level. It explains how the platform is structured without exposing engineering-only implementation detail.



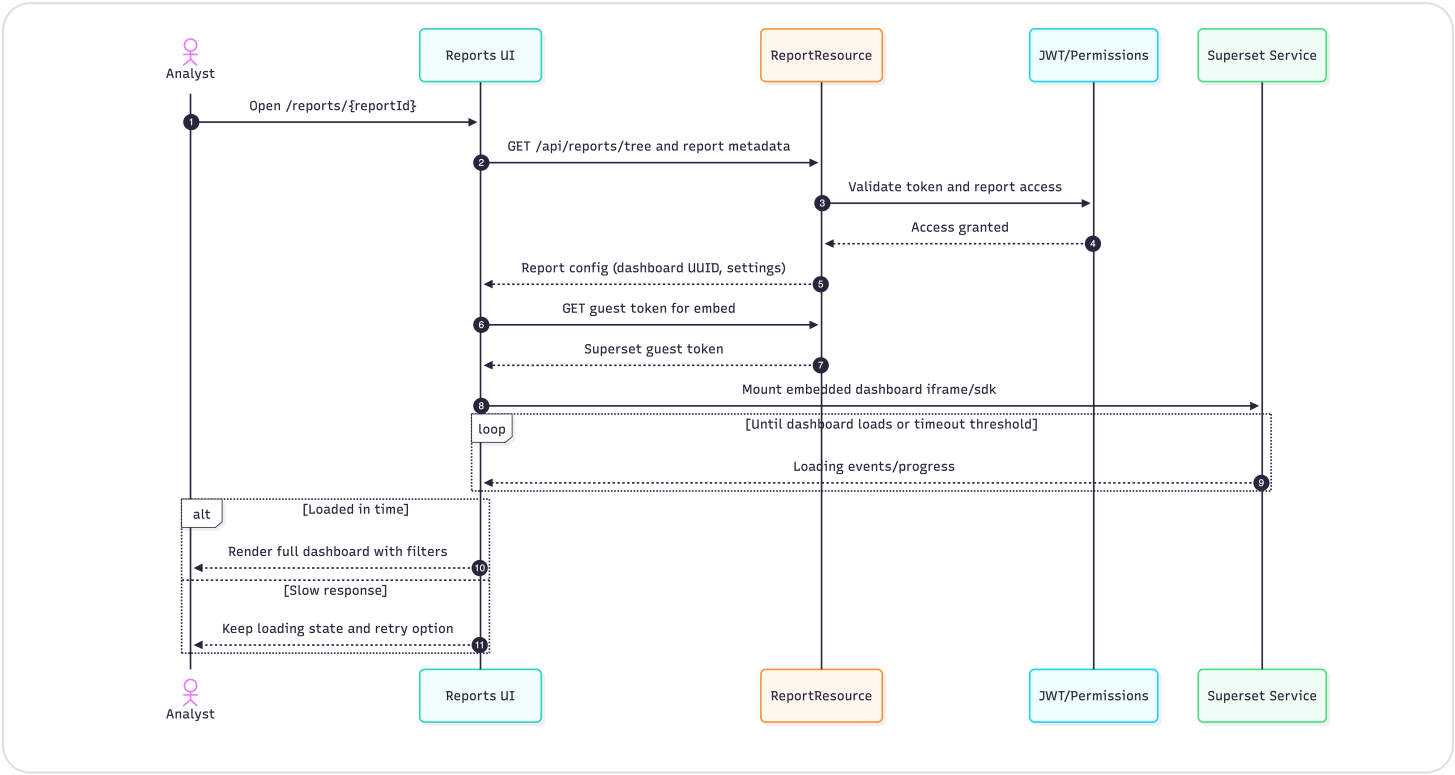
Runtime components and the main interaction boundaries across portal, services, data, and supporting infrastructure.

Architecture building blocks

- **Portal frontend:** provides the operational shell, list/detail views, map interactions, and reporting entry points.
- **Backend service layer:** enforces business logic, workflow rules, security decisions, and data access.
- **Data services:** persist transactional records, configuration, historical state, and supporting documents.
- **Identity and access:** central authentication and token-based authorization control access to protected pages and APIs.
- **Realtime and analytics:** telemetry, notifications, and reporting flows propagate operational state to end users.

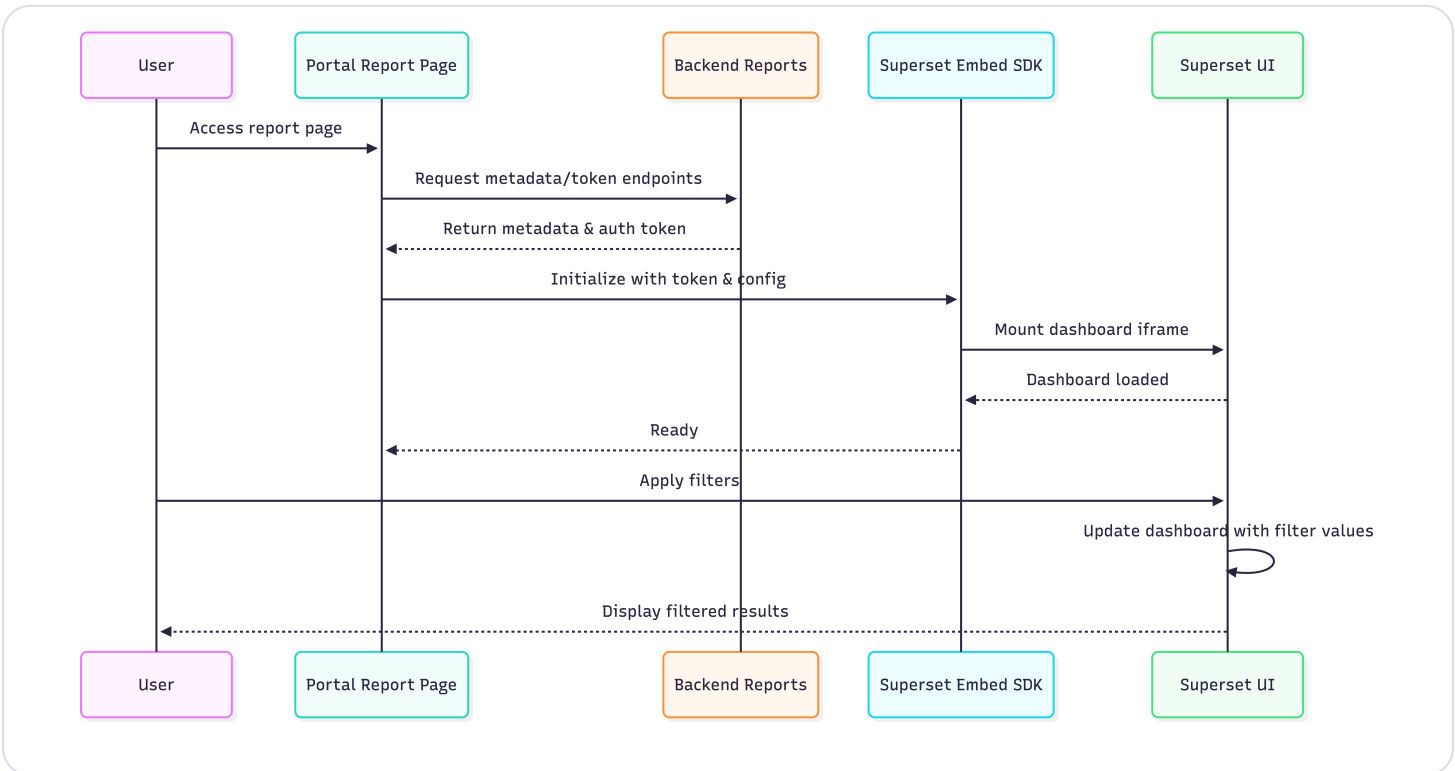


User sign-in and authenticated session establishment.



Token validation and report authorization for protected analytics access.

Realtime event and telemetry fan-out toward the portal experience.



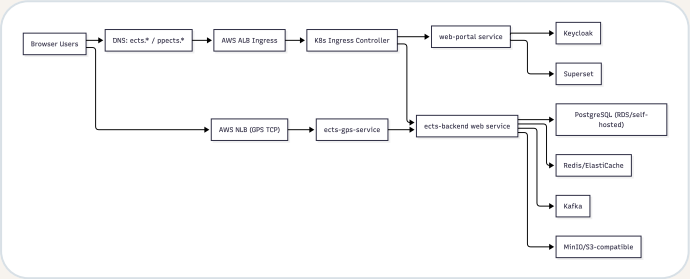
Report metadata lookup, embedded analytics path, and page rendering flow.

9. Deployment, Monitoring, and Recovery

The production operating model combines frontend delivery, backend services, data stores, identity services, and supporting observability and backup controls.

Deployment overview

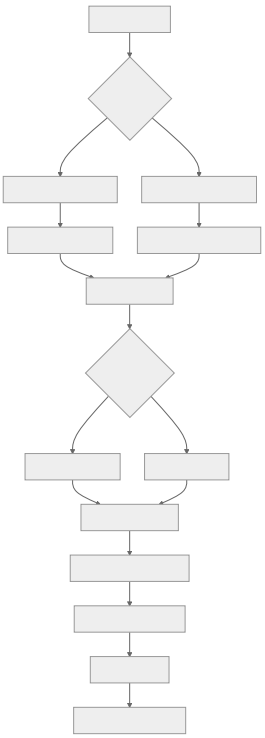
- Frontend, backend, reporting, and identity capabilities are deployed as distinct runtime components.
- Reverse proxy and access gateway layers protect public entry points and route traffic to internal services.
- Persistent data, attachments, and configuration artifacts are stored in dedicated backing services.
- Operational deployment changes are expected to follow controlled rollout and rollback procedures.



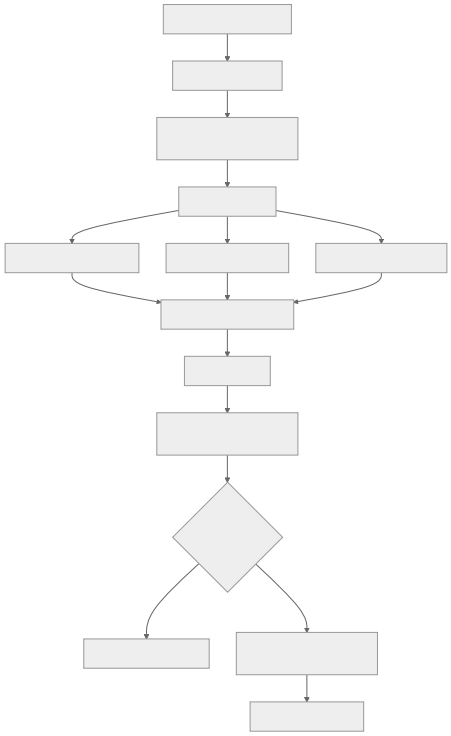
Monitoring and continuity controls

CONTROL AREA	WHAT IS WATCHED
Service health	Portal availability, API health, identity availability, and analytics access paths
Workflow success	Login completion, page load success, command execution, and report rendering
Device and telemetry	Message flow, monitoring freshness, and device command outcomes
Data protection	Backup execution, retention coverage, and restore readiness

Client stakeholders should expect formal incident escalation when authentication, core module access, device telemetry, or reporting access fails beyond the documented tolerance window.



Incident response workflow from detection through recovery verification.



Disaster recovery workflow from backup selection through restoration and closeout.

Recovery objectives

SCENARIO	RTO	RPO
Full platform outage	4 hours	30 minutes
Single service outage	1 hour	15 minutes
Report subsystem outage	2 hours	1 hour

Protected data classes

- Transactional platform data
- Telemetry-related stores
- Documents and attachments
- Configuration and identity exports

10. Client Operations Checklist and Sign-off

This closing section provides a practical readiness checklist and a formal sign-off area that can be used during handover, review, or governance approval.

Client operations checklist

CHECKPOINT	EXPECTED RESULT
Access	Landing page, login handoff, and home map load successfully.
Core workflows	Representative pages in Cargo, Journeys, Routes, Inventory, Alerts, Devices, Reports, and Settings load correctly.
Alerts and reports	Alert queues render and report pages complete after their normal asynchronous load window.
Administration	Authorized administrators can manage users and inspect device configuration pages.
Continuity	Monitoring, escalation, backup, and recovery responsibilities are understood by the client operations team.

Immediate escalation triggers

- Users cannot authenticate or protected pages fail after sign-in.
- Core module pages show blank, partial, or error state for multiple users.
- Report pages fail to load after the normal extended wait period.
- Device monitoring stops updating or command outcomes become unreliable.

Sign-off record

Client sponsor

Confirms receipt and review of the client documentation pack.

Name, signature, date

Operations owner

Confirms operational guidance, escalation paths, and continuity controls are understood.

Name, signature, date

Technical reviewer

Confirms the client-safe technical overview is sufficient for review purposes.

Name, signature, date

Supporting evidence that may be attached to this sign-off includes screenshots, client review comments, agreed action items, and approved follow-up workstreams.

Distribution and Support

This PDF is part of the public client-share documentation set published from the ECTS documentation portal. Companion volumes are available for focused audience-specific review.

Available client volumes

- Comprehensive Client Documentation Pack
- Client User Guide
- Operations and Deployment Guide
- Technical Overview

Publication and ownership

Publication: ECTS documentation portal

Prepared by: Keshi ECTS Engineering Team

Revision: 1.1, March 12, 2026