User and technical guide

FleetTime Local and FleetTime Network

Version 2.10.0 / Testing edition

Connected fleet, equipment and driver records

Practical workflows / Actual software screenshots / Recovery guidance

2 November 2026 | DesignWorks

Contents

Choose your edition setup first. Click a heading or a PDF bookmark to jump to a task.

Introduction 6

Install FleetTime Local 7

Install FleetTime Network 9

Update an existing installation 11

Use and remove demonstration data 12

Fleet Dashboard / Fleet Asset Card 13

Workshop / Equipment Card 14

Drivers & Licences / Driver Card 15

Settings & Administration / Maintenance Costs 16

Settings & Administration / Bulk Uploads 17

Settings & Administration / Users and Access 18

Choose your FleetTime edition 19

First-time user: start here 20

Fleet Dashboard / Overview 21

Fleet Dashboard / Fleet Library 23

Fleet Dashboard / Fleet Planner 26

Fleet Dashboard / Insurance Audit 28

Fleet Dashboard / Inspections & Certificates 30

Fleet Dashboard / Defects, Services & Repairs 33

Fleet Dashboard / Fleet Analysis 35

Fleet Dashboard / Document Library 37

Workshop / Overview 38

Workshop / Workshop Planner 40

Workshop / Weekly Site Diary 41

Workshop / Equipment Locations 42

Workshop / Import Equipment 44

Workshop / Inspections & Certificates 46

Workshop / Document Library 47

Drivers & Licences / Overview 48

Drivers & Licences / Driver Register 49

Drivers & Licences / Points & Risk 50

Drivers & Licences / Driver CPC 51

Drivers & Licences / Document Library 52

Working Time / Overview 53

Working Time / Reference Averages 54

Working Time / Weekly Returns & Imports 56

Working Time / Document Library 58

Tachographs / Overview 59

Tachographs / Download monitor 60

Tachographs / Infringements 61

Tachographs / Reports 62

Accidents & Incidents / Overview 63

Accidents & Incidents / Analysis & Map 65

Accidents & Incidents / Expanded Map 66

Accidents & Incidents / Insurance Documents 67

Accidents & Incidents / Document Library 68

Fines / Overview 69

Fines / Analysis & Map 70

Fines / Import Fines 72

Fines / Document Library 73

Fuel / Overview 74

Fuel / Purchase Locations 75

Fuel / Imports & Accounts 76

Fuel / Review Rules 77

Fuel / Document Library 78

Reporting / Overview 79

Documents / Overview 82

Settings & Administration / Overview 84

Settings & Administration / Working-Time Rules 86

Settings & Administration / RAM Mileage Integration 87

Settings & Administration / Field View Integration 90

Settings & Administration / Backup & Restore 92

Settings & Administration / Privacy & GDPR 94

Technical & support / Architecture and persistence 96

Technical & support / Locations, files and identifiers 97

Technical & support / Document storage, limits and validation 98

Technical & support / Accounts, permissions and sessions 99

Technical & support / Encryption scope and portability 100

Technical & support / Network: shared-folder deployment 101

Technical & support / Network: HTTPS service deployment 102

Technical & support / Backup format, verification and capacity 104

Technical & support / Recovery and upgrade runbook 105

Technical & support / Manual cold copy and disaster planning 106

Technical & support / Install, repair, update and uninstall 107

Technical & support / Exports, maps and integration boundaries 108

Technical & support / Diagnostics: symptom to next action 109

Technical & support / Support tickets and feature suggestions 110

About DesignWorks 111

Introduction

A practical guide to FleetTime Local and FleetTime Network

What FleetTime does

FleetTime brings vehicle and trailer compliance dates, maintenance, workshop equipment, working time, driver licence and CPC records, incidents, fines, fuel analysis and supporting documents into connected records. Use divisions to focus the view, then open a record to review its details and evidence. Application permissions control access to sections; a division filter is not a security boundary.

How to use this guide

Start with your edition installation and first-time setup. Add divisions and drivers before importing related data. Each task chapter starts on a clean page and explains the named controls, the saved result and important limits. Screenshots show fictional data from the native 2.10.0 testing build; records, dates and permissions on your screen can differ.

Responsibility and scope

FleetTime helps organise recorded information and highlight due dates. A green status applies to the named check and the data available. It does not certify a vehicle, driver, lifting item or operator as legally compliant. Confirm the applicable rules, jurisdiction and evidence with your competent transport or safety adviser.

Install FleetTime Local

Choose where this Windows user keeps the local workspace

Before installation

Create and verify a complete backup if upgrading. Close FleetTime. Extract the release ZIP completely, then run FleetTime-Local-Setup-2.10.0.exe from the extracted Local folder. Windows may warn because this testing release is unsigned. Check the source and supplied checksum through your normal IT procedure.

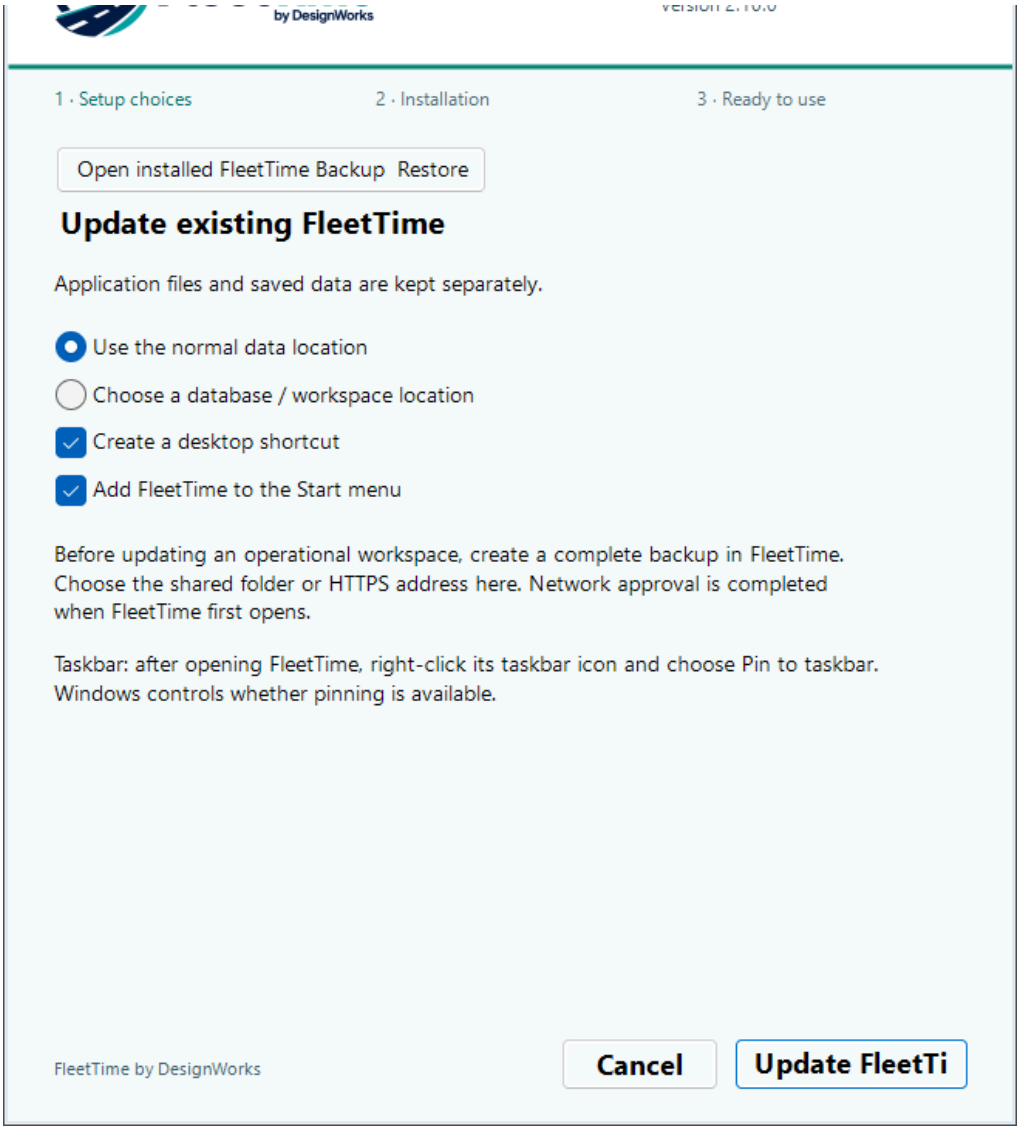
Choose setup and storage

For an existing installation, keep the existing workspace / connection. For a new workspace, type a full local folder path in the installer or use Browse, then Check location. For example, D:\FleetTime Data. FleetTime stores its Data subfolder beneath that selected workspace. Use a private local folder outside live cloud-sync folders. A backup destination is a separate choice.

Finish and sign in

Choose whether to create Desktop and Start menu shortcuts. Wait for Installed, then choose Open FleetTime if required. Create the first administrator for this workspace and store its recovery key securely. The main software opens maximised after sign-in. A Local copy uses Windows-user protection; use encrypted complete backup and recovery to move to another Windows account or machine.

Install FleetTime Local - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Install FleetTime Network

Choose a shared Windows folder or an HTTPS FleetTime server

Choose the connection type

Run FleetTime-Network-Setup-2.10.0.exe after extracting the ZIP. Keep the existing connection on an update. During a new setup, choose Shared Windows folder or HTTPS server, type the path/address and Check location. Shared examples are \\SERVER\Transport\FleetTime or R:\AIMS\7.0 Plant & Transport\FleetTime DB. A mapped drive must exist for the Windows user running FleetTime; a UNC path is generally easier to identify consistently.

Shared Windows folder

Use a reliable share with the required read, write, create and replace permissions. The shared-folder protocol keeps versioned snapshots with locking; it does not place Local SQLite onto a share. The first administrator creates the workspace encryption passphrase. Keep it securely for recovery. Other Windows accounts/computers request approval and give their pairing code to the administrator, who verifies it under Users & Access. After approval, the authorised Windows account caches its key using Windows protection and signs in with its own FleetTime credentials.

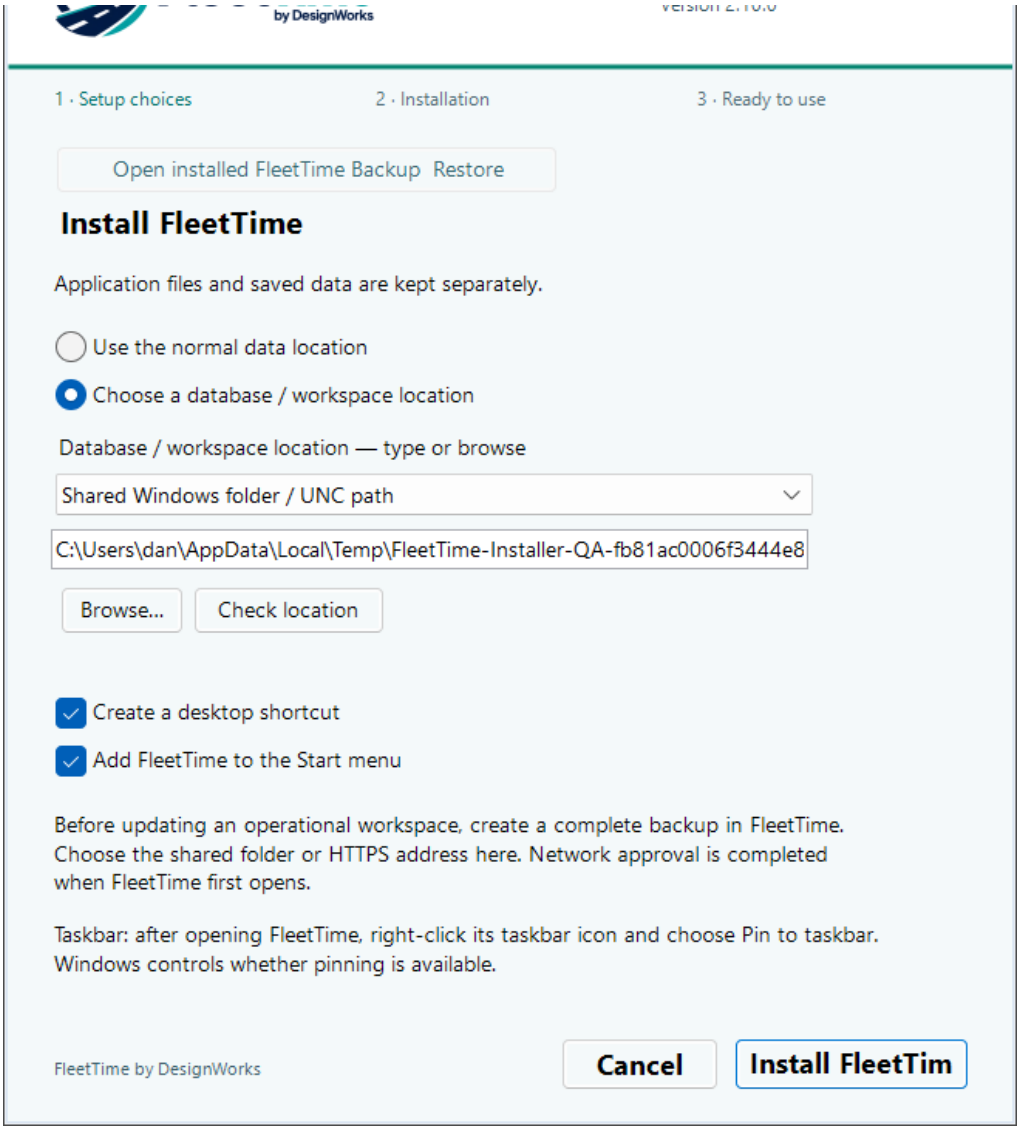
HTTPS server

Your IT administrator installs/configures the supplied FleetTime server tools, private data folder, HTTPS certificate, firewall and service identity. Enter the base HTTPS address in Network setup. The first administrator uses Administrator: connect with server setup key to bootstrap the connection. Later computers request approval; the administrator verifies the pairing code under Users & Access. Computer approval permits a connection; each person still needs an active user account and the appropriate section permissions.

Verify before use

Open the same known record from two authorised clients, test a controlled edit and reload the other client. Stale saves should be rejected rather than overwriting newer work. Test backup and recovery separately. Update the server and clients together under administrator control. Internet/server acceptance, certificates and site permissions need testing on your actual deployment.

Install FleetTime Network - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Update an existing installation

Update the same edition without uninstalling it

Back up first

Use Backup & Restore, create a complete encrypted backup and verify recovery into a separate empty location. Include every uploaded original. Keep the manifest and all split parts together and confirm cloud synchronisation has completed. The installer can open the installed backup page; sign in if asked, complete backup, then close FleetTime before returning.

Run the new installer

Close the installed software on each computer. Run the new installer for the same edition and retain the existing workspace / connection. Installation replaces application files separately from operational data and accounts. It does not merge workspaces. Never choose a new workspace solely to bypass a failed login or a damaged file.

Update notifications

Help > Check for updates checks the DesignWorks release service. A background check is also attempted at most daily after sign-in. This testing release has no live published signed update yet, so the service can report unavailable. Future downloadable updates require a matching SHA-256 hash, a Windows-verified code signature, a trusted code-signing certificate and the publisher thumbprint specified by the release feed. No downloaded installer runs automatically.

After updating

Open About FleetTime and confirm 2.10.0 and the expected edition. Verify the known records, an attachment preview and user permissions. For Network, coordinate server/client updates and reopen clients after the server upgrade. Microsoft Store distribution and its update mechanism remain separate release work.

Use and remove demonstration data

Explore every section in an empty training workspace

Load the demo

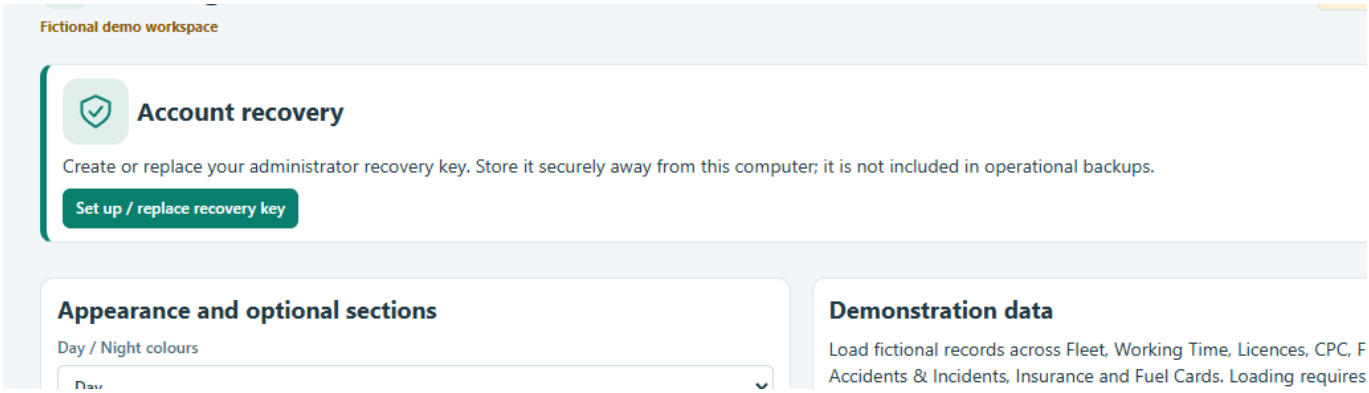
As administrator, open Settings & Administration > Overview > Demonstration data. Choose Load demo data and confirm only in an empty workspace. The demo covers vehicles/trailers, plant, varied weekly hours, licence/CPC checks, fines, fuel, incidents/insurance, evidence, inspections and maintenance costs. Fictional inspection findings demonstrate A/B/C/unknown cases and keep source evidence separate from operational availability.

Explore the records

Use Fleet Asset Card, Equipment Card and Driver Card to see mixed miles/km, operating hours, dated readings, due-date tiles and monthly maintenance costs. Some dates are overdue, some current and others unknown. Open the matching record for evidence and original data. Demo results are deliberately varied and do not represent customer information or genuine provider certificates.

Remove everything in demo mode

Choose Remove demo data in Configuration or Leave demo. This clears all operational records and uploaded originals added while in demo mode, including your own test edits/files. Accounts and system settings are retained. Keep a backup if anything is needed. After clearing, the empty workspace can load the demo again. Separately exported files, backups and screenshots are not deleted.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Fleet Asset Card

Find and update one vehicle or trailer quickly

Find the asset

Choose a division, use the Fleet asset selector or type a registration, asset ID, description or serial in Live search. Select a suggested record; typing alone does not change a saved record. Trailer records retain their asset/Ministry/VIN identifiers even where no road registration is used.

Review the top section

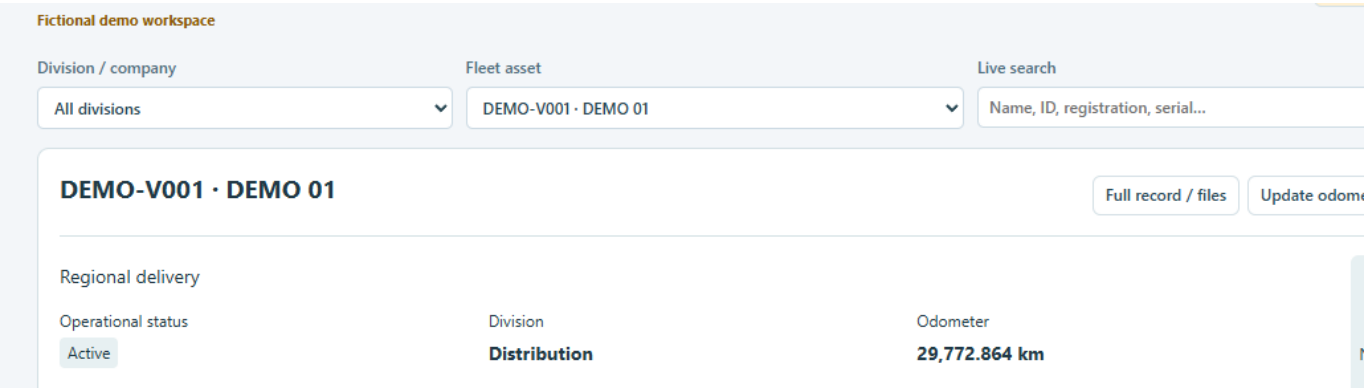
Identity, current operational status, meter reading and its unit/date/source appear together, with the main photo on the right if selected. Last received / updated is the time FleetTime saved or imported the reading; it is not necessarily the tracker observation time. Review missing or stale dates before using the value.

Read the checks

MOT, tax, service, PMI, airport passes, calibration, LOLER and other applicable measures display due dates and countdowns. Applicability and evidence matter; no blanket trailer ADR requirement is inferred. Service considers the saved date and distance trigger separately, and the earliest applicable trigger needs attention.

Update deliberately

Update odometer saves a dated reading with source/history. Use the explicit conversion action to convert both the current distance and service threshold; do not relabel miles as km. Update status requires a reason. Full record / files opens the connected editing, evidence and work history without creating a second asset.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Equipment Card

Review equipment, meters and maintenance in the same compact layout

Find the equipment

Choose a division and an equipment record or use Live search. The card shows its identity, location/status, current meter and main image where selected. Full record / files opens the same workshop asset and its evidence.

Choose its meter

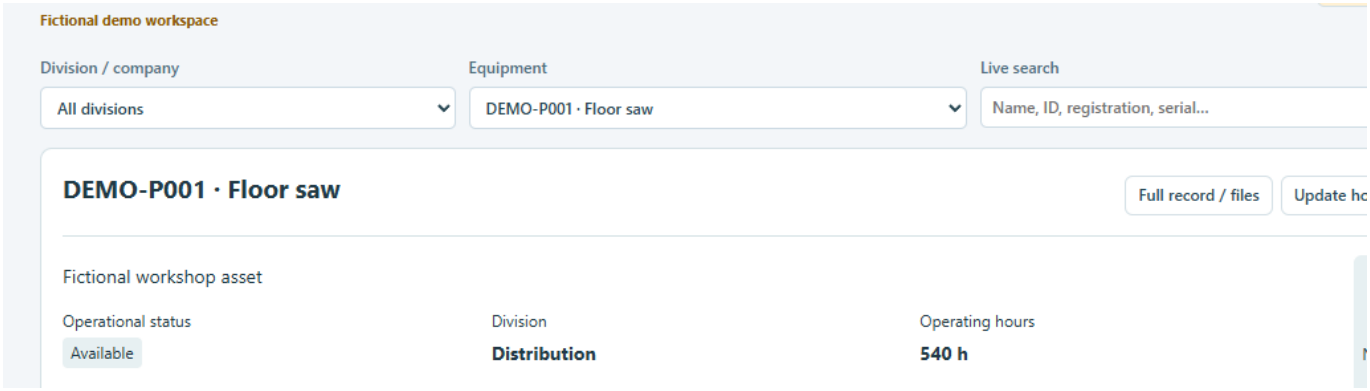
Update operating hours opens Meter display. Choose Operating hours, Distance, Hours and distance, or No meter. Enter the relevant reading dates and source. Changing the display mode retains historical readings. A lower/older reading or a different recorded distance unit requires a reviewed correction rather than silent replacement.

Review maintenance and inspections

Check date-based servicing/inspection and any recorded hours-based trigger. Saved provider inspection findings, certificates and uploaded evidence remain separate from VOR release decisions. A provider Active status or a next-due date alone does not prove a clean inspection or current safe availability.

Use costs if enabled

The January-December cost panel uses recorded work costs and supports year/month drilldown. Use Record job costs for an existing work item. Return to the original workshop workflow to enter or complete maintenance and add evidence.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Driver Card

Review licence and CPC check status for one driver

Find one person

Use division, Driver selection or Live search. The card uses the common driver record. Phone, email, monitoring purpose and photograph come from that record; add each person once. Licence-only drivers are excluded from working-time and CPC monitoring.

Last checked and next due

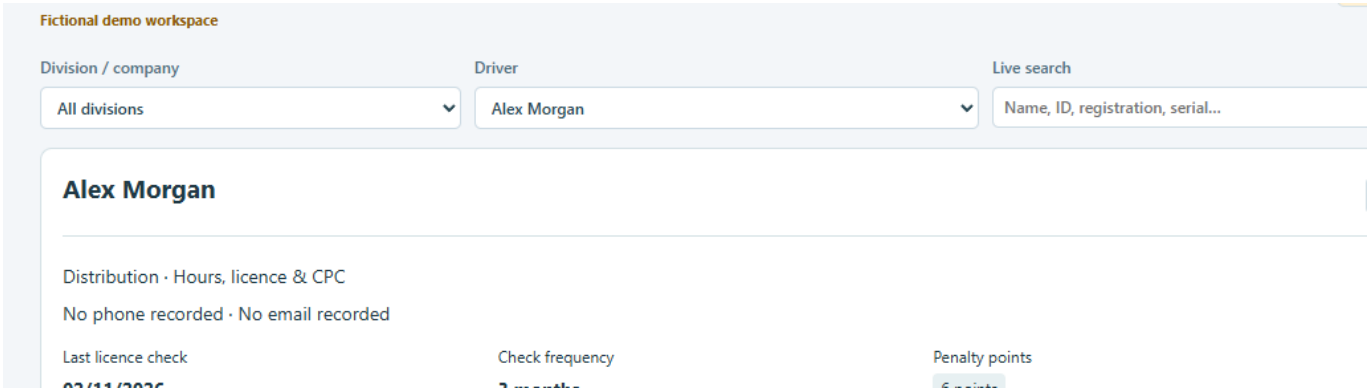
Last licence check is the latest recorded check/source-check date. Next check uses the configured frequency and any earlier imported next-check deadline. High-points thresholds and review frequency are configurable policy settings; the common default is 12 months, or 3 months at 6 or more points. They are company monitoring policy, not a universal DVLA check interval.

Expiry versus verification

Licence, CPC and ADR expiry tiles show recorded due dates. Last CPC verified is a distinct manual verification date. Record CPC verification only after the user has performed that verification; uploading a file does not complete a licence or CPC check. FleetTime does not automatically retrieve DVLA check results.

Open the full record

Full driver record / files opens the common driver/licence record, entitlements, revision number, check history and supporting originals. Missing or foreign-licence eligibility information requires manual review.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Maintenance Costs

Record actual costs without treating missing values as zero

Enable the feature

An authorised user enables maintenance cost tracking in Settings & Administration > Overview. The setting exposes cost panels and reporting; it does not change job completion or operational status. Fleet and workshop permissions still apply.

Enter the amounts

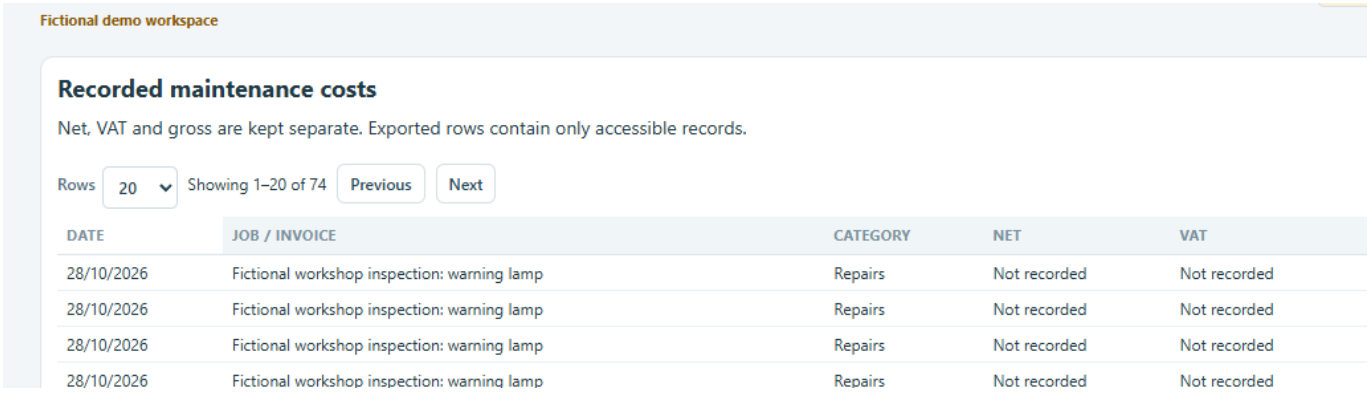
Choose an existing job and Record job costs. Record its cost date, parts, labour, other costs, VAT, cost centre and invoice reference. Blank means unknown. Enter 0 only when a cost is genuinely zero. Net requires all three net components; gross requires known net and VAT. Attach the invoice through the original job/evidence workflow.

Interpret the charts

January-December panels group actual recorded costs by cost date and distinguish estimates and missing costs. Future months remain unreported. Select a month to inspect the underlying work records. Comparisons use equally long elapsed periods rather than comparing a partial current month against a full previous month.

Export and review

Reporting adds cost details and labelled monthly calendar context to selected fleet/workshop sections. These operational costs are not a tax ledger or proof of invoice payment. Review completeness, currency and the selected scope before sharing a report.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Bulk Uploads

Choose the right importer from one place

Choose a record type

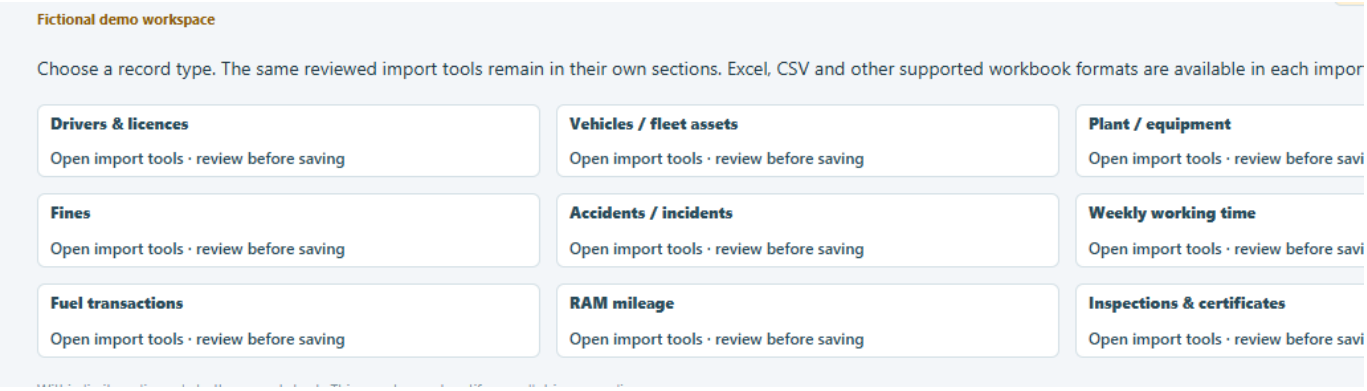
Open Bulk Uploads and select Drivers & licences, Vehicles, Plant/equipment, Fines, Incidents, Weekly working time, Fuel, RAM mileage or Inspections. These are the same reviewed importers available within each operational section. Available choices depend on permissions.

Review before saving

Choose the source file and worksheet, inspect recognised headings and mapping, check dates/units/identifiers and resolve unmatched or duplicate records. Supported formats are shown by the chosen importer; workbook support does not imply every attachment form accepts every spreadsheet type.

Check the result

Save the reviewed rows, then open a known record in the operational register. Compare an amount, identifier and date with the source. A loaded file or completed progress bar alone does not prove that every row was imported. Keep original evidence securely.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Users and Access

Manage people and computer connections separately

Manage user accounts

Open Users & Access to see the account list, active state and permissions. Create a user or choose Edit existing account. Give each person a unique username, a temporary password and only the section/action tick boxes required. The user changes a temporary password before normal work.

Review access

View, edit, delete and export are separate capabilities. Sensitive driver details, original documents, backups, restore, configuration and user administration have separate grants. Test the result with a standard account. A hidden menu is not the only protection: native operations also enforce permissions.

Approve a computer

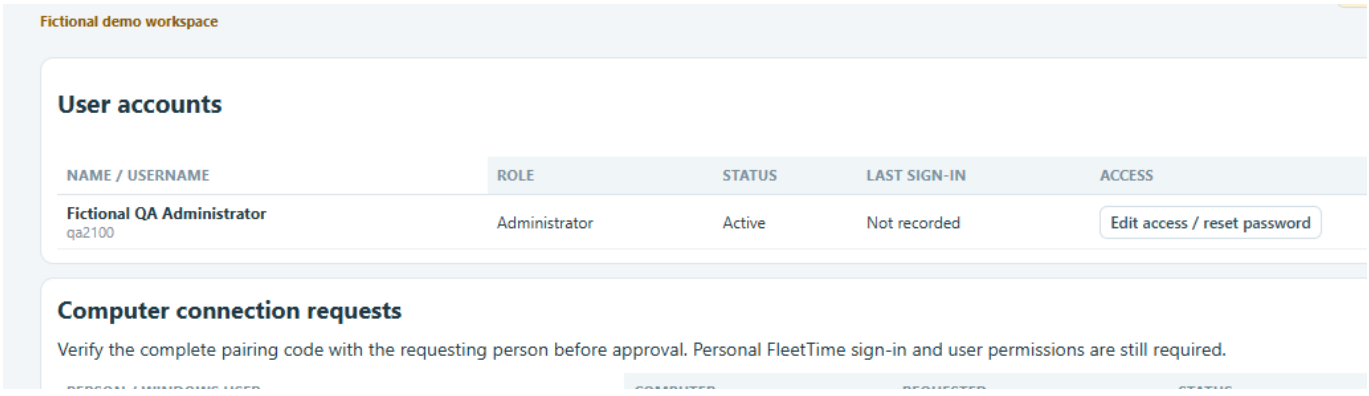
A shared-folder or HTTPS connection request appears separately from user accounts. Ask the requester to give you the full pairing code and verify it against the request. Approve only the expected Windows account/computer. After connection approval, the person still signs in and receives their user permissions.

Revoke or recover

Deactivate an account to prevent further sign-in, or revoke the computer connection when it is no longer authorised. Retain administrator recovery keys and the shared encryption/backup secrets securely and separately. Application permission revocation cannot erase files or keys already copied outside the application; use appropriate Windows/server access controls.

Session warning

After inactivity, FleetTime displays Are you still there? with a 60-second countdown before the 20-minute session lock. Choose Stay signed in to continue, or Sign out now. This is not an automatic save: save changes regularly before leaving your computer.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Choose your FleetTime edition

FleetTime Local and FleetTime Network use the connected operational sections; their working-data connection is the main difference.

FleetTime Local

For one independent working computer/Windows account. Local keeps protected records and managed originals on the selected local drive. It avoids a shared-service dependency, but needs individual access and independent complete backups. Separate working copies do not automatically merge.

FleetTime Network

For authorised computers sharing one supported workspace. Choose a supported shared-folder snapshot or administered HTTPS service, with individual access and revision checks. Network also has a separate this-computer mode. IT must establish permissions, keys, connectivity and recovery arrangements.

Shared folder or HTTPS service

Shared-folder mode uses protected snapshots, exclusive locks and revision checks, rather than SQLite opened across SMB. An HTTPS service owns its local data disk; clients connect through the configured endpoint. Use native Settings > Data connection. Sidebar Settings & Administration configures application behaviour.

Cloud backup and moving computers

Dropbox, OneDrive and similar services can hold complete backup sets. Ordinary sync is not a supported live database connection and does not merge records. Use the reviewed complete-backup/recovery or migration procedure and verify the destination before selecting it.

First-time user: start here

Use a training workspace and follow each task in order. Do not assume a successful click proves the record was saved.

Set up divisions and drivers first

As administrator, enter your divisions/defaults in Settings & Administration, then add/import the driver register before uploading working time, licence checks, incidents or fines. Create asset records with consistent identifiers before importing related work or mileage.

Start safely

Ask an administrator for an approved training workspace with fictional records. Check edition and location. Do not experiment with deletion, restore, erasure or fresh-workspace choices on operational data.

Find your page

Click the parent menu, then the named child. Set division, dates and filters before interpreting a result. Follow the task steps, then check the saved result.

Terms

Division is the operating group used to filter records; it is not a security permission. An asset ID is the permanent internal identity, separate from registration/VIN/serial. VOR means unavailable for use, requiring a reason and a release review. Import reads source information; export creates another file. A report is not a complete backup.

If something is missing

Clear search, check division/dates and confirm edition/workspace. Ask an administrator to check missing/disabled actions. Do not create duplicate people/assets because a first search was empty.

Fleet Dashboard / Overview

Review current fleet status and open the records needing action.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Select all divisions for a fleet-wide review, or choose the division you manage. Check any status, type and search filters.

Step 3

Read the summary labels and totals. Select a due-work or VOR box to focus its supporting records; use View to choose the boxes you need.

Step 4

Open the relevant asset and confirm its registration or permanent asset ID before editing.

Step 5

Click Log defect / service / repair to start work against the correct saved asset, or open the existing work record to update it.

06

Return to Overview and check that the saved work, due dates and availability agree.

Check it worked

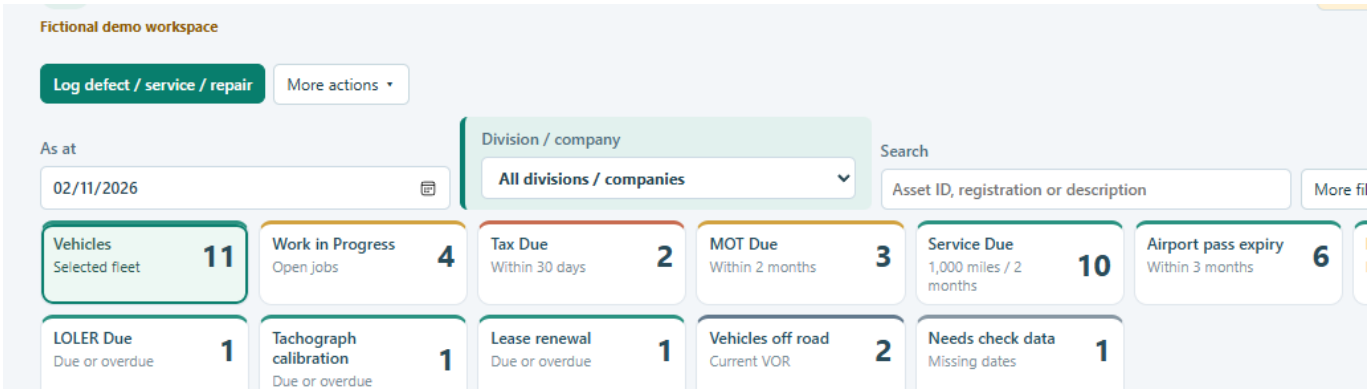
An actionable list of fleet exceptions supported by saved asset and work records.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Changing a filter changes the view, not the underlying asset. A VOR decision needs an explicit reason and a controlled release after work.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Fleet Library

Create, identify and review a fleet asset through its card.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Fleet Library. If its child list is closed, click the parent name once to open it.

Step 2

Search before adding an asset. Use the existing card if the registration or permanent asset ID already exists.

Step 3

Choose Add fleet asset. Select the actual type: car, van, rigid HGV, tractor unit or the appropriate trailer type. Enter a unique permanent asset ID and the applicable registration, Ministry identifier or VIN.

Step 4

Record the division, status and available operating information. Complete the conditional HGV/trailer fields only where relevant; select refrigeration or lifting fitment when present.

Step 5

Save, then reopen the asset card. Add its picture, evidence, mileage and work through the relevant controls. Check that each file belongs to this asset.

06

To connect assets, expand Linked assets, select a saved asset, choose Tows, Carries or Associated with, and enter dates and a reason. Review overlap warnings before saving.

07

When an assignment ends, record its end rather than deleting the past. Review the reciprocal link from the other asset.

Check it worked

One asset card connects identity, mileage, work, documents and dated relationships.

If it did not work

Unexpected Fleet Library results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Asset identity and conditional fields

For HGVs and trailers, use reliable specifications for weight, axles, brakes and coupling details. Changing the type retains previously recorded technical values for review. A recorded towing relationship does not calculate technical compatibility.

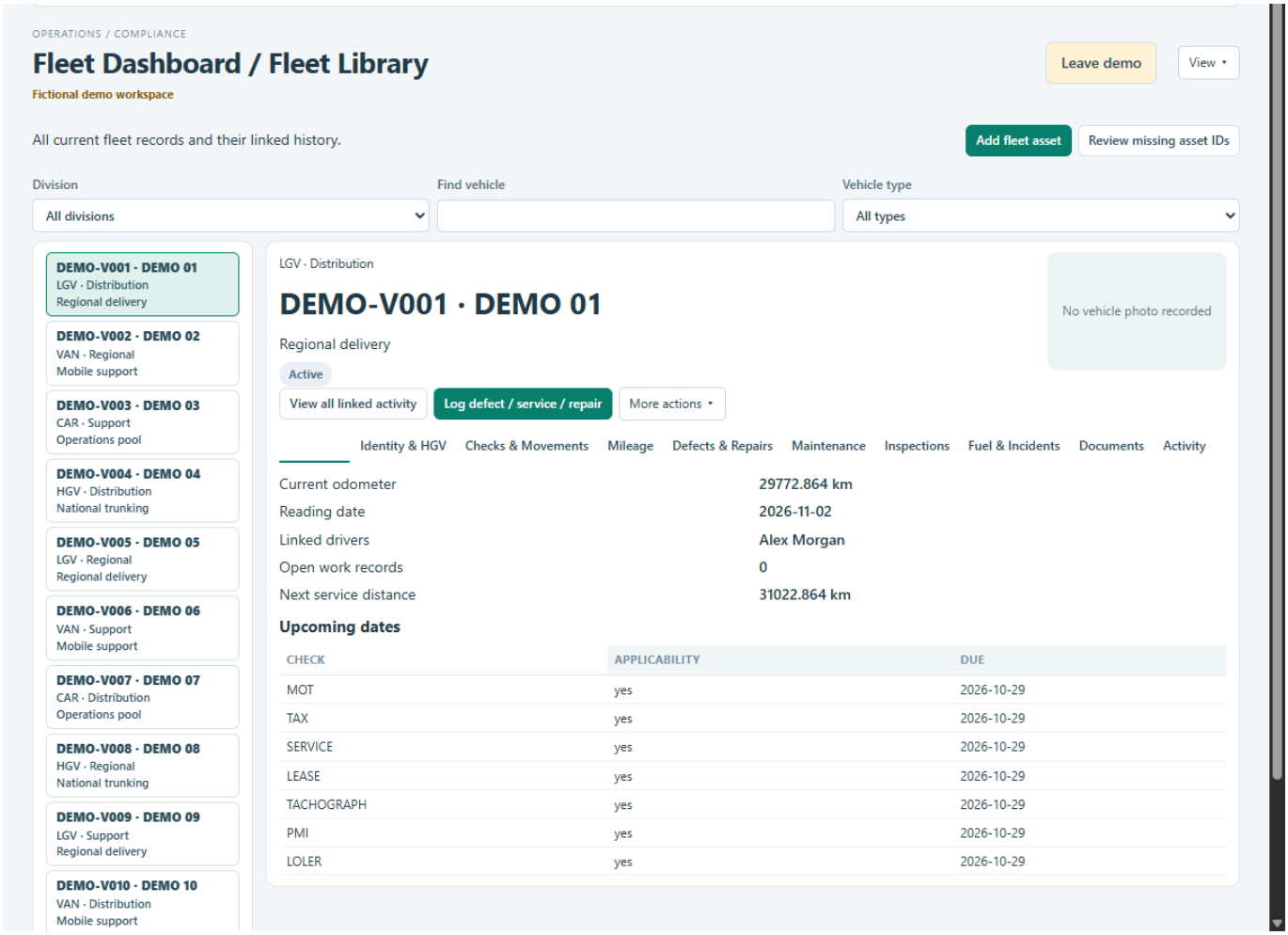
Worked example

Create trailer TR-061 with its actual Ministry identifier or VIN. Link tractor TRA-014 using a dated Tows relationship. Log a trailer brake defect against TR-061; the tractor does not inherit that defect or its VOR status.

Check / boundary

A saved permanent asset ID is not reassigned. A trailer need not have an invented road registration. Links do not transfer defects, VOR or maintenance requirements.

Fleet Dashboard / Fleet Library - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Closer view of the page controls



Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Fleet Dashboard / Fleet Planner

Turn saved planned work and confirmed test requirements into a calendar.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Fleet Planner. If its child list is closed, click the parent name once to open it.

Step 2

Choose the division, asset type and planning period. Include the relevant cars, vans, tractors and trailers.

Step 3

Use the maintenance summary boxes to focus a work category. Read registrations/asset identities down the left and dated events across the calendar.

Step 4

Select an event to open its linked work or requirement. Check the asset, task, booking date, due date and status.

Step 5

Update the source record when dates or completion change. Return to the planner to check the revised position.

06

Review gaps, overlapping bookings, overdue requirements and unavailable assets before issuing the operational plan.

Check it worked

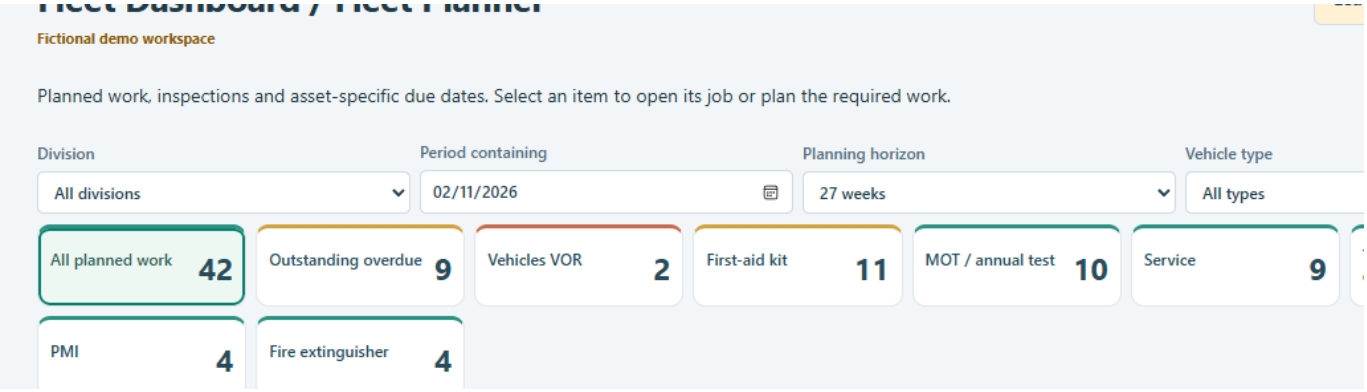
Calendar events lead back to their source records and can be reconciled with completed work.

If it did not work

Unexpected Fleet Planner results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Confirmed provider requirements and manually entered maintenance dates are separate sources. The planner does not choose a legally appropriate inspection interval for the operator.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Insurance Audit

Compare an insurer-provided list with the fleet register and retain a reproducible snapshot.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Insurance Audit. If its child list is closed, click the parent name once to open it.

Step 2

Obtain the insurer schedule and keep the original. Open Insurance Audit, select the division and schedule effective date, and review whether off-hired assets should be included. VOR assets are included by default.

Step 3

Read the supported spreadsheet/CSV, choose the worksheet and map the registration or asset identifier columns.

Step 4

Validate and inspect matches, fleet assets missing from the insurer list, insurer-only rows, duplicates and ambiguous identifiers.

Step 5

Resolve incorrect mappings or source values before saving the comparison. Add follow-up notes for genuine exceptions.

06

Save the snapshot. Open a sample match and exception, then export PDF/XLSX/ODS or Print if a review copy is required.

07

Use Accidents & Incidents > Insurance Documents to retain the current certificate and policy evidence.

Check it worked

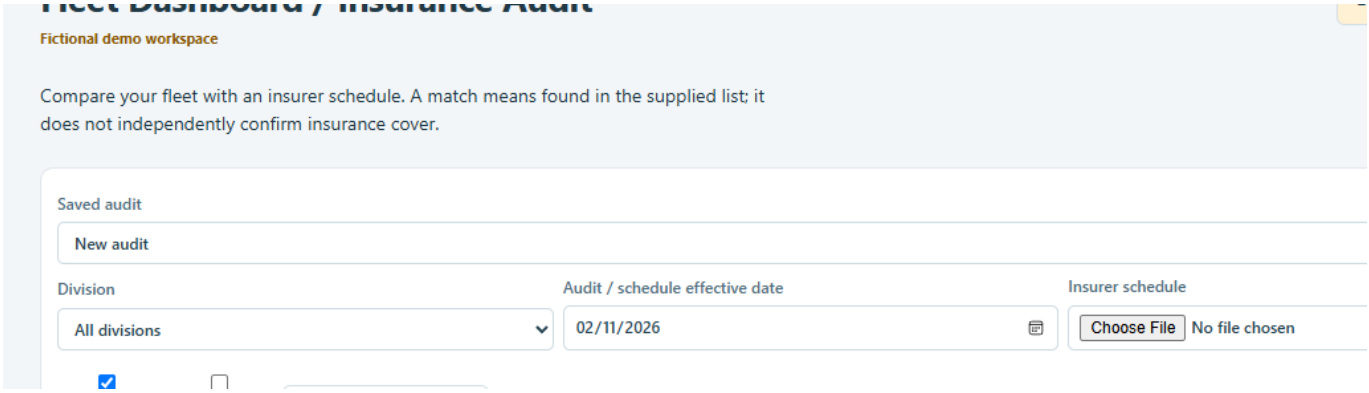
A saved comparison retains the source name, worksheet, row references, mapping, effective date, reviewer and fingerprint.

If it did not work

Unexpected Insurance Audit results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

A list match is not independent proof of insurance cover. Historical eligibility uses recorded added-to-fleet dates and current status; it does not reconstruct every historical status change.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Inspections & Certificates

Import a provider list, link its items and review certificates and deadlines.

Before you start

Have the relevant untouched source file and reliable asset/driver identifiers ready.

01

In the left menu, open Fleet Dashboard, then choose Inspections & Certificates. If its child list is closed, click the parent name once to open it.

02

Download the provider export and preserve it. Choose the provider profile, select CSV/XLSX/ODS, then review worksheet, column mapping and date format.

03

Review each proposed match using plant/asset number, serial/VIN and previously reviewed provider identities. Keep conflicting, inactive or ambiguous rows in review.

04

Missing-asset creation is off by default. If needed, enable it deliberately and supply the correct fleet/equipment type, permanent asset ID and division for each new record. Otherwise leave the row for review or explicitly skip it.

05

Commit the reviewed batch. Check the retained original source, imported item, report reference and asset link.

06

Download certificates through the provider website. Use Add PDF or Import PDF certificates / ZIP; review the report matches rather than accepting filenames as proof.

07

Open an inspection, check the certificate and source dates, then confirm the reminder requirement only when the evidence supports it. Compare manually held maintenance dates separately.

08

Use View inspection / issue from the asset card to read original codes, source rows, history and shared report evidence.

Check it worked

Provider items link to fleet or workshop records, with source provenance and reviewed deadlines.

If it did not work

Unexpected Inspections & Certificates results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Provider settings

Provider settings holds the portal, file/API preference, browser preference and reminder lead times. API requested records an intention only. Chrome is the recommended portal browser; Windows default/manual use remains available.

Certificate limits

Each PDF remains limited to 12 MiB. The certificate ZIP intake permits 128 MiB, up to 1,000 entries and up to 2 GB expanded PDFs. Review CRC/path/size failures. If stopped, inspect the result because files already saved remain saved.

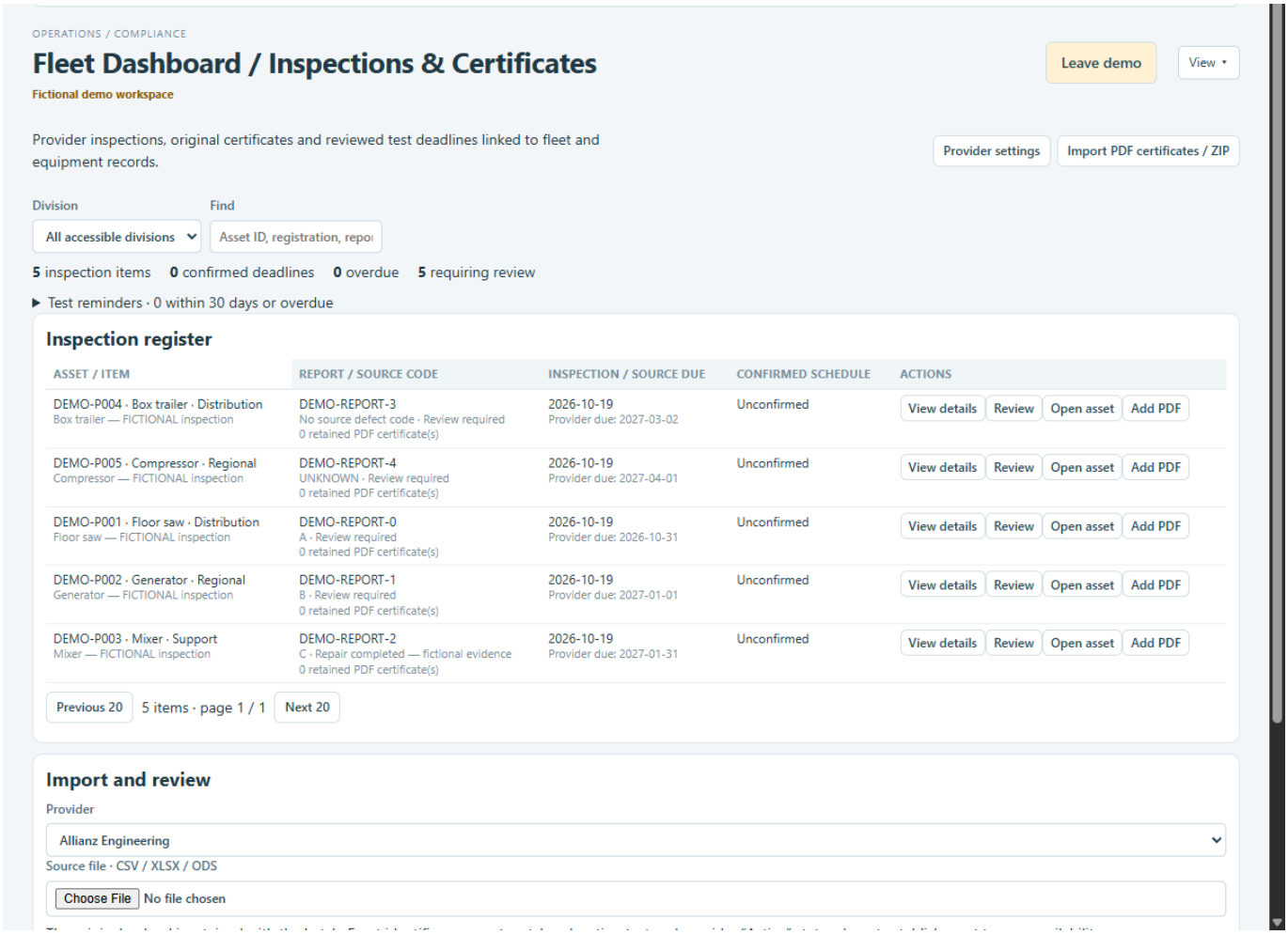
Deadline workflow

Source deadline > compare with certificate > resolve contradictions > confirm requirement > planner/reminder/report. Existing manual service fields are not silently overwritten. Reminders are in-app, with no background email service implied.

Check / boundary

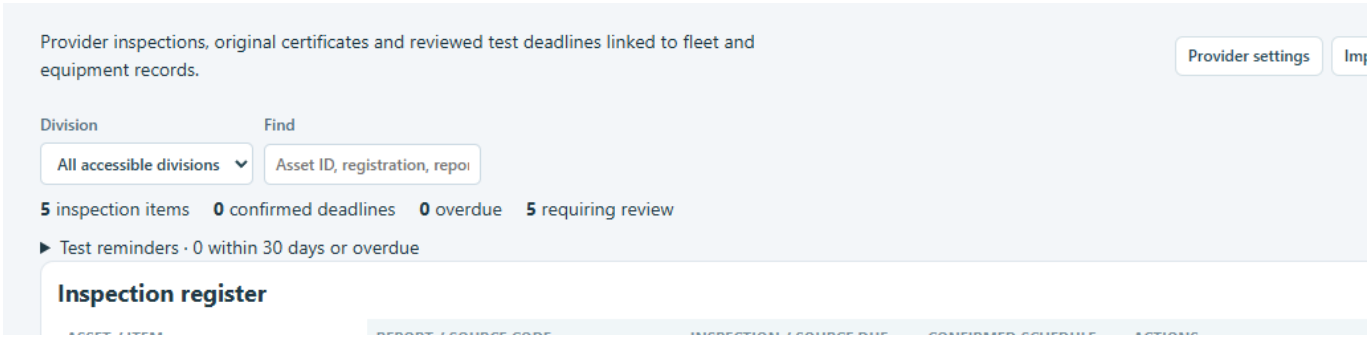
No provider API or automatic portal certificate fetching is connected in 2.10.0. A report can cover several assets and its certificate is stored once. Imported Active/repair status does not release VOR.

Fleet Dashboard / Inspections & Certificates - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Closer view of the page controls



Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Fleet Dashboard / Defects, Services & Repairs

Record and complete fleet work with evidence and an explicit availability decision.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Defects, Services & Repairs. If its child list is closed, click the parent name once to open it.

Step 2

Find the asset and check for an existing open record describing the same issue.

Step 3

Click Add defect / service / repair. Select the saved asset and work type, then enter a short title, factual description, dates and responsible party where provided.

Step 4

Record work status. If the asset is unavailable, choose VOR and enter why it cannot be used.

Step 5

Attach relevant defect photos and documents. Check the filenames and asset identity before saving.

06

Reopen the saved work to verify description, status and evidence. Check its appearance in the asset history and planner.

07

After completion, record the outcome, date and evidence. Review the outstanding defect and asset availability through the organisation's release process.

Check it worked

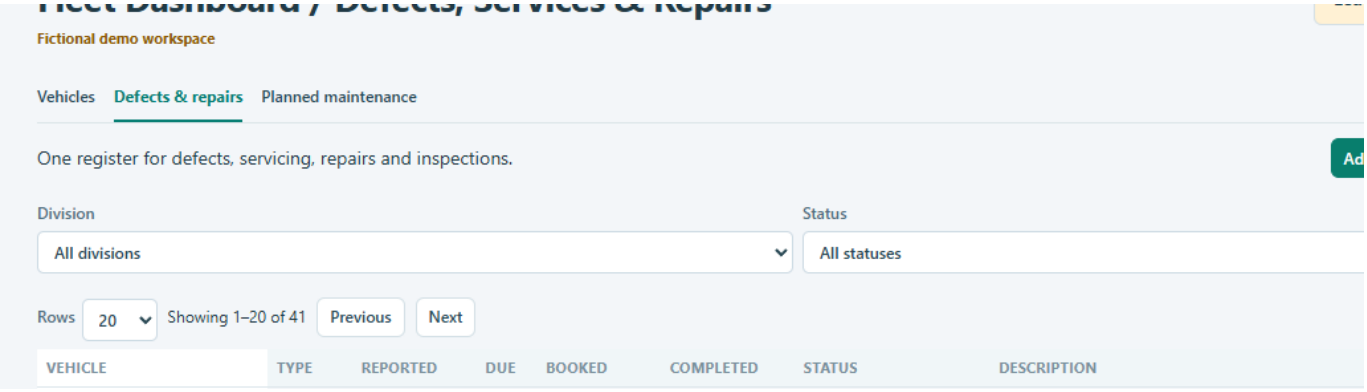
The original issue, planned action and completion can be followed from the same asset history.

If it did not work

Unexpected Defects, Services & Repairs results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Do not mark a repair complete solely because a file was uploaded. A completed job and a release from VOR are separate decisions.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Fleet Analysis

Review defect and repair patterns before preparing management reporting.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Fleet Analysis. If its child list is closed, click the parent name once to open it.

Step 2

Set the division and analysis period. Keep comparable periods consistent.

Step 3

Review defect counts, repairs and the monthly view. Distinguish open work from completed work.

Step 4

Open the contributing records for the assets or categories with repeated issues.

Step 5

Check descriptions, dates, mileage and completion evidence before deciding whether an apparent repeat is a recurring fault.

06

Export the scoped analysis or add Fleet to Reporting > Overview. Retain the supporting records for the conclusions.

Check it worked

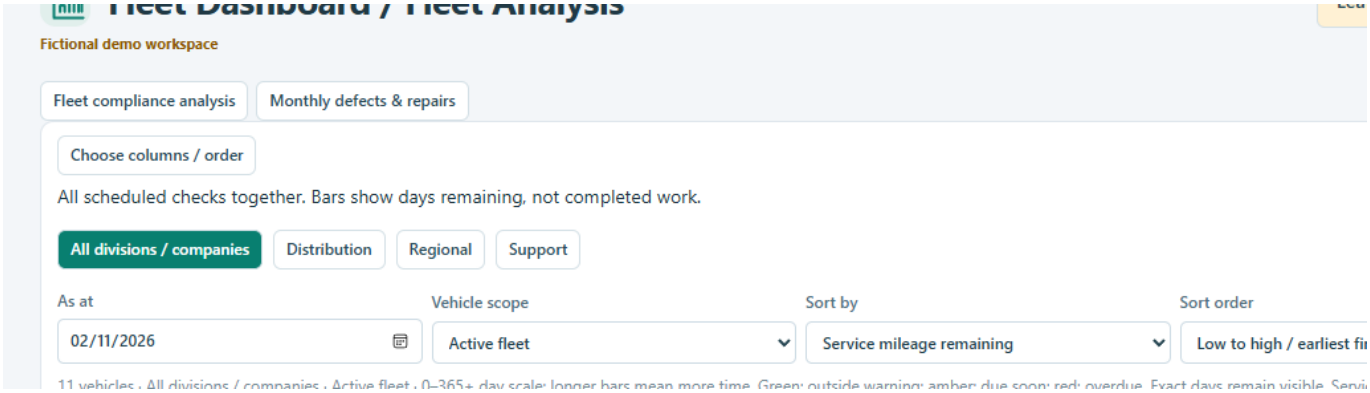
A trend can be traced to dated work records and a defined fleet scope.

If it did not work

Unexpected Fleet Analysis results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

A falling count may reflect missing entries or a different population. Check coverage before describing an improvement.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fleet Dashboard / Document Library

Find the original files linked to fleet assets, work and inspection records.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Fleet Dashboard, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Fleet Dashboard > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Fleet Dashboard record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Fleet Dashboard result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

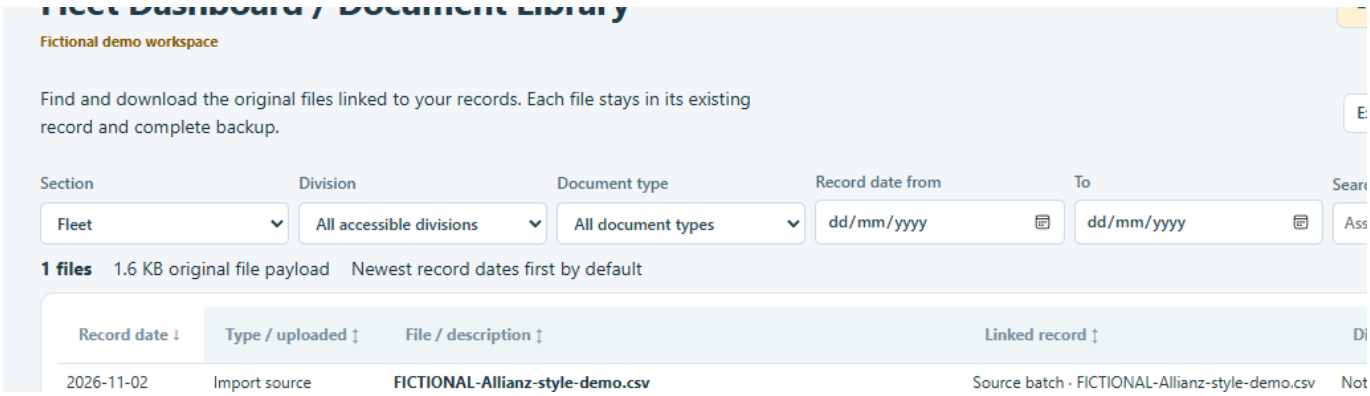
Open the downloaded Fleet Dashboard file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Fleet Dashboard catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Overview

Review workshop equipment and log its maintenance or repair.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Workshop, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Filter by division, equipment type and status. Search the permanent asset ID or serial number.

Step 3

Open the correct equipment record and review existing work before creating another job.

Step 4

Use the equipment work form to enter a defect, service or repair, with description, relevant dates and responsibility.

Step 5

Choose VOR when the equipment is unavailable and state the reason. Add photographs and supporting documents.

06

Save, reopen the record and check work history. After repair, record the outcome and review availability through the normal release process.

Check it worked

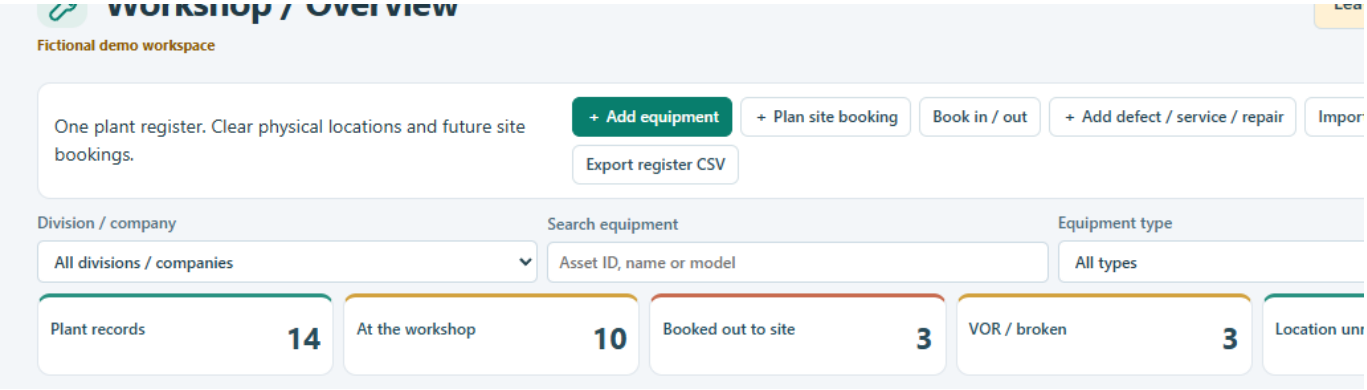
Equipment status and its work history explain what is unavailable and why.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Fleet and workshop records can be related, but each retains its own identity and availability decision.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Workshop Planner

Schedule and review equipment work and confirmed inspection requirements.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Workshop, then choose Workshop Planner. If its child list is closed, click the parent name once to open it.

Step 2

Choose the division and planning dates.

Step 3

Locate the equipment and check planned work and confirmed provider deadlines.

Step 4

Open the item requiring attention to inspect its source record.

Step 5

Change dates or completion in the source work/requirement record and save.

06

Return to the planner and check overdue items, VOR conflicts and revised dates.

Check it worked

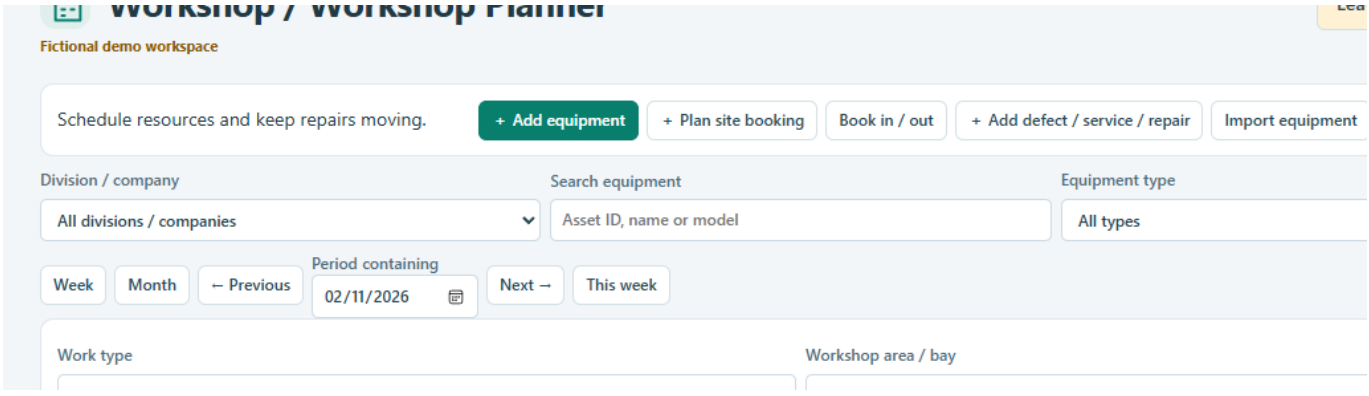
The plan reflects saved work and reviewed requirements.

If it did not work

Unexpected Workshop Planner results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

An imported date requiring review is not a confirmed maintenance instruction until reviewed.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Weekly Site Diary

Review and maintain the weekly placement/use information for plant.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Workshop, then choose Weekly Site Diary. If its child list is closed, click the parent name once to open it.

Step 2

Choose the relevant week and division.

Step 3

Identify each item by its asset ID and check its recorded site/location.

Step 4

Record or correct the available diary information using the page controls. Keep the actual week and equipment identity intact.

Step 5

Review missing information and confirm changes against the source operational information.

06

Save and revisit the week to check the entry against the equipment record.

Check it worked

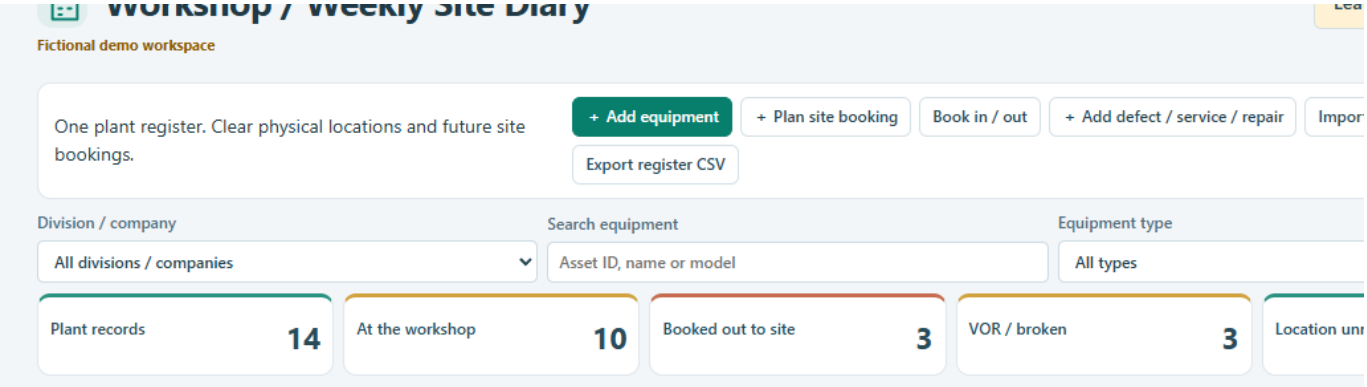
A dated diary can be reconciled with the item's recorded location and operational evidence.

If it did not work

Unexpected Weekly Site Diary results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Diary information is entered/imported evidence, not live GPS tracking.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Equipment Locations

Find equipment through linked list and map views.

Before you start

Have the relevant saved location information ready.

Step 1

In the left menu, open Workshop, then choose Equipment Locations. If its child list is closed, click the parent name once to open it.

Step 2

Select the division and status, then review location/postcode coverage.

Step 3

Select an equipment row to focus its saved map location. Use the optional hover-highlighting control when that interaction is helpful.

Step 4

Read the equipment identity and location label together. Open the underlying equipment record before correcting a location.

Step 5

For missing points, check usable coordinates/postcode on the record. Keep unknown positions unplotted rather than guessing.

06

If map services are disabled or unavailable, use the location list and coverage information. Review the map again after authorised configuration or corrected data.

Check it worked

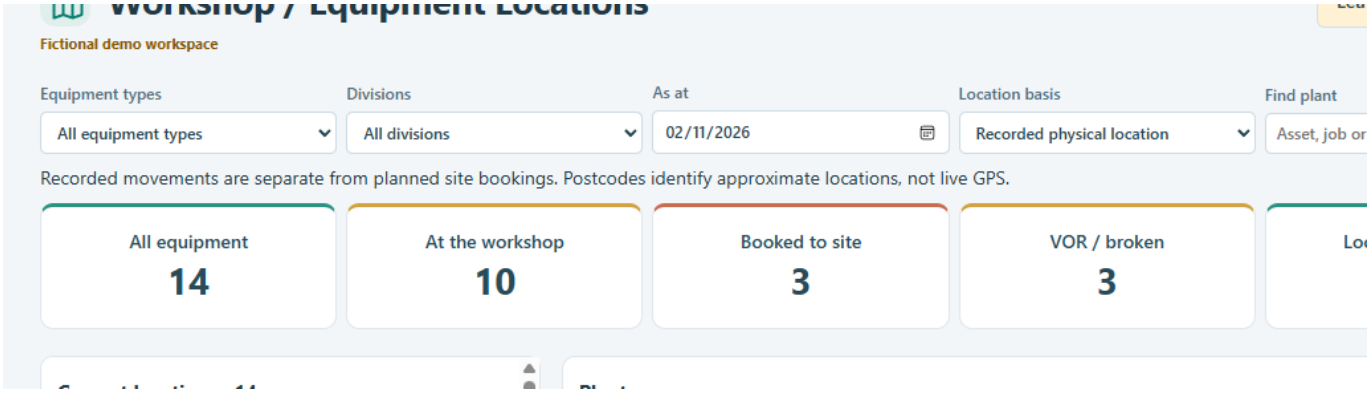
The list and map refer to the same selected equipment and explain missing coverage.

If it did not work

Unexpected Equipment Locations results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Screenshot: map controls in the offline demonstration state; street tiles are not loaded. Online maps are optional and may involve external services. A recorded location is not a live vehicle tracker.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Import Equipment

Bring supported equipment rows into the existing register without creating avoidable duplicates.

Before you start

Have the relevant untouched source file and reliable asset/driver identifiers ready.

Step 1

In the left menu, open Workshop, then choose Import Equipment. If its child list is closed, click the parent name once to open it.

Step 2

Keep the untouched source file. Open Import Equipment and use the offered template/format.

Step 3

Review headings, units and identifiers. Match existing equipment by reliable asset/serial identity.

Step 4

On Import Equipment, click Check file and inspect the preview for duplicates, rejected rows and uncertain identities. Correct the source or mapping before continuing.

Step 5

Click Import reviewed only after the Import Equipment preview is correct. Read the result, then reconcile the imported records with the original source.

06

Compare counts with the source and open representative equipment records to verify division, identity and dates.

Check it worked

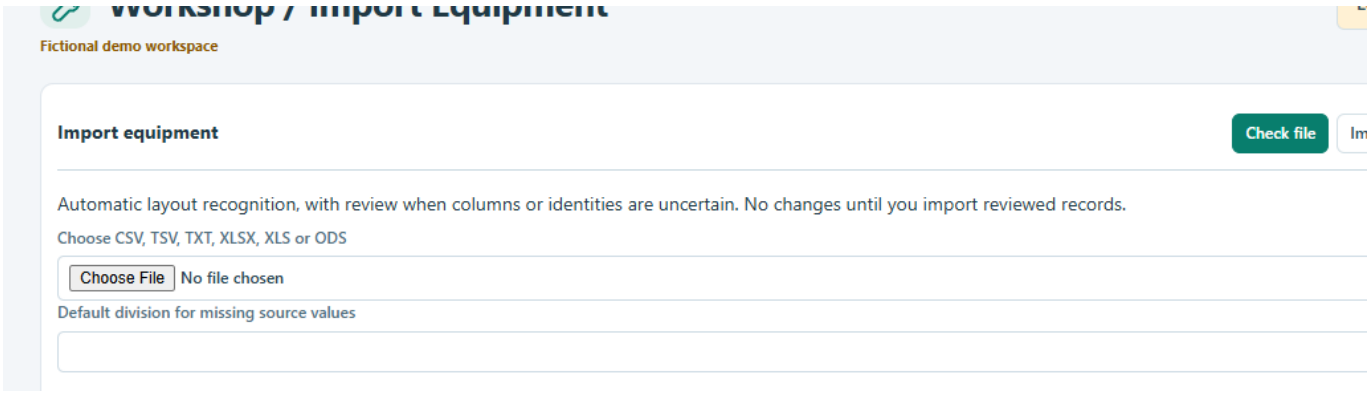
Imported equipment is reconciled with the source and the existing register.

If it did not work

Unexpected Import Equipment results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

For testing-company lists use Inspections & Certificates, which retains report evidence and review states. Do not use a generic equipment import as a substitute for inspection review.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Inspections & Certificates

Review the same provider evidence from the equipment side.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Workshop, then choose Inspections & Certificates. If its child list is closed, click the parent name once to open it.

Step 2

Open Workshop > Inspections & Certificates and select the division/provider scope.

Step 3

Use the import, matching and missing-asset review procedure in Fleet Dashboard > Inspections & Certificates.

Step 4

For every equipment item, confirm the asset ID/serial and its original provider issue code.

Step 5

Attach or match the report certificate and confirm the relevant deadline after checking the evidence.

06

Reopen the equipment card and Workshop Planner to verify the saved links and requirements.

Check it worked

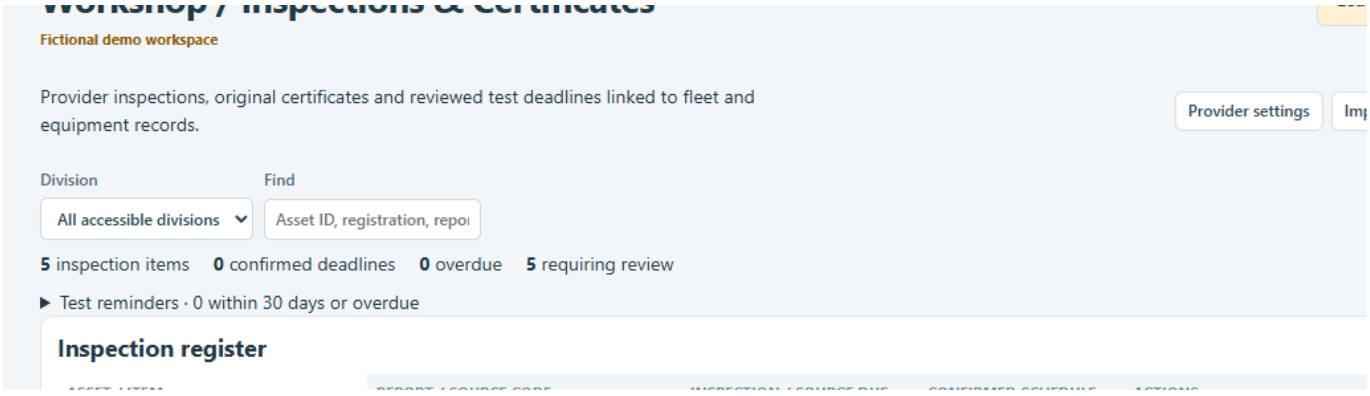
Workshop equipment uses the same retained report/source evidence as the provider workflow.

If it did not work

Unexpected Inspections & Certificates results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

A test item located on a vehicle or trailer is not automatically that host asset. Keep both identities distinct.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Workshop / Document Library

Find the original files linked to workshop equipment, its jobs and provider reports.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Workshop, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Workshop > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Workshop record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Workshop result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

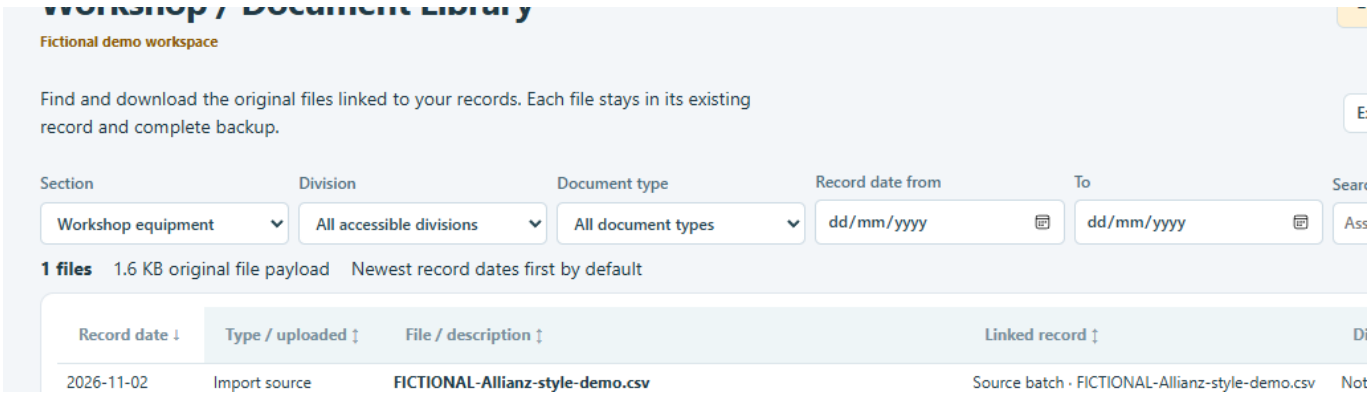
Open the downloaded Workshop file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Workshop catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Overview

Review recorded licence details and upcoming checks.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Drivers & Licences, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Select division, issuing country and any due/expiry filters.

Step 3

Read the compact summary boxes and select an exception to show contributing drivers.

Step 4

Open the existing driver record and verify identity before changing entitlements, points or dates.

Step 5

Record the actual check, its date and outcome, and the next review information where provided. Upload supporting evidence against the driver.

06

Save and check the register again, including the next due date and missing fields.

Check it worked

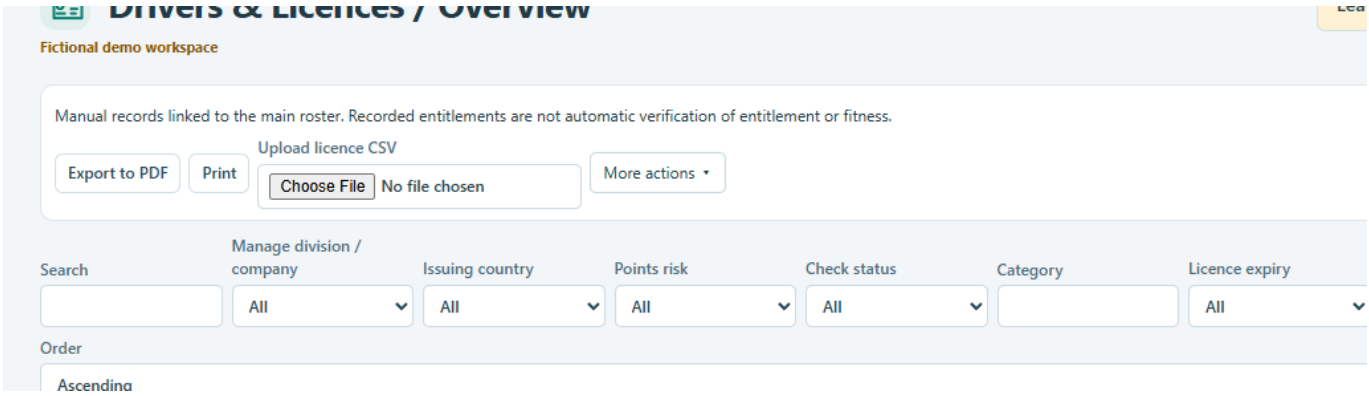
The overview becomes a traceable list of required licence-check actions.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

FleetTime logs checks and evidence; it does not automatically verify entitlement with DVLA or another issuing authority.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Driver Register

Find the common driver record and review or edit its saved information.

Create a new person

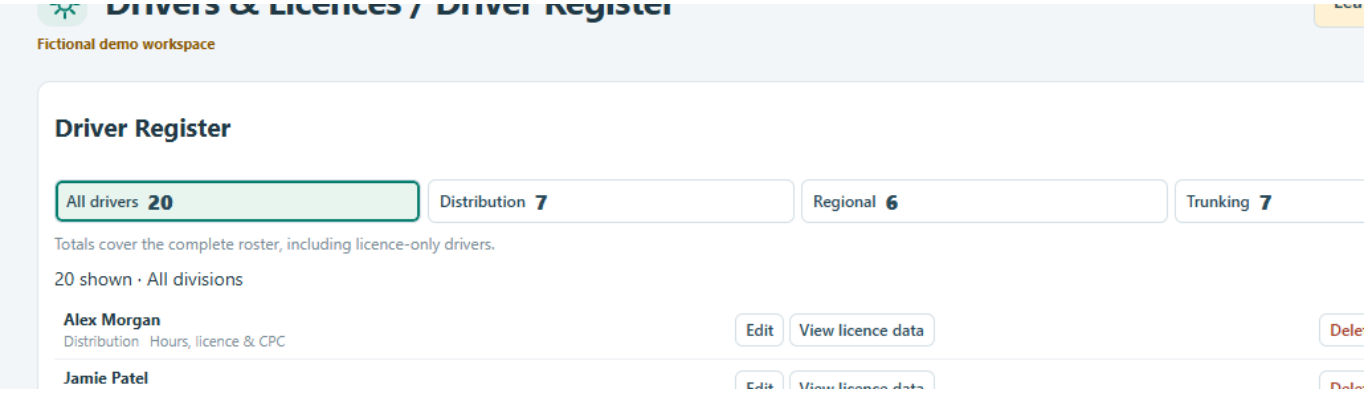
Open Drivers & Licences > Driver Register > Add driver. Enter name and division, optional phone/email and a unique roster reference where used. Choose Hours, licence and CPC or Licence only, then Save driver. Driver editing permission is required.

Edit without duplication

Find the existing person using division/search and choose Edit. Confirm the identity before changing details. Changing monitoring purpose retains the historical records; licence-only records are excluded from working time and CPC monitoring.

Verify the saved record

Reopen the person, check the name/division/contact details and open their Driver Card or licence record. Resolve duplicate warnings rather than adding the same person under a slightly different name.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Points & Risk

Prioritise drivers whose recorded information needs attention.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Drivers & Licences, then choose Points & Risk. If its child list is closed, click the parent name once to open it.

Step 2

Set the division and read the ranked list.

Step 3

Inspect the recorded points and reasons behind the displayed risk indicator.

Step 4

Open the underlying driver/check to establish whether information is current, missing or incorrect.

Step 5

Correct factual errors at source and save evidence for the review.

06

Use the organisation's checking process for follow-up, then revisit the list and report outstanding high-risk items.

Check it worked

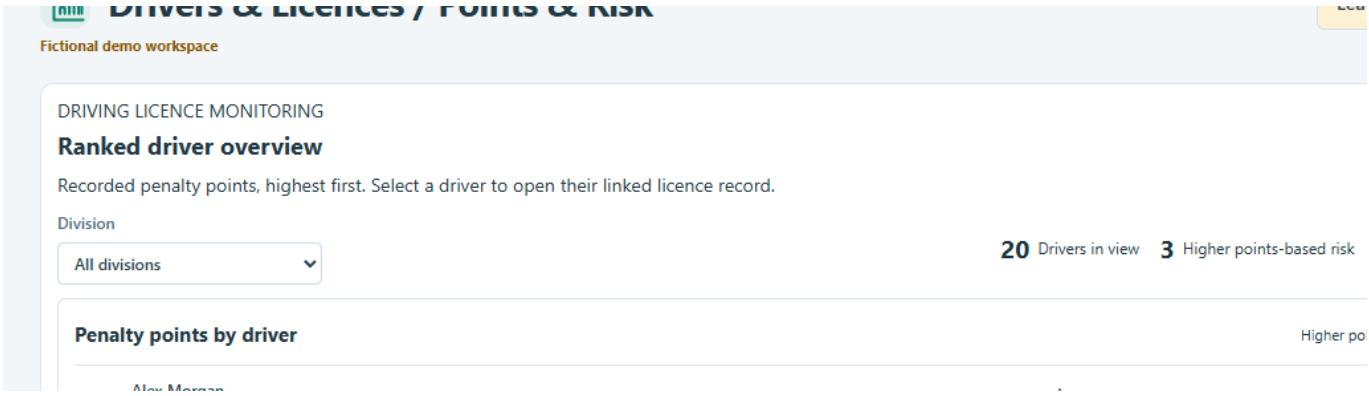
Risk review is supported by identifiable source records rather than colour alone.

If it did not work

Unexpected Points & Risk results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

The displayed risk score is an operational prioritisation tool, not a decision that someone is legally entitled or fit to drive.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Driver CPC

Maintain qualification information and monitor incomplete/expiring records.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Drivers & Licences, then choose Driver CPC. If its child list is closed, click the parent name once to open it.

Step 2

Choose the division and the relevant expiry/incomplete filter.

Step 3

Select the existing driver and check whether CPC monitoring applies.

Step 4

Enter the qualification details and dates from reliable evidence. Add the relevant copy against that driver.

Step 5

Save and reopen to confirm the evidence and date fields.

06

Review the updated due list and arrange the required training/check through your organisation.

Check it worked

The qualification register distinguishes recorded evidence from missing or due information.

If it did not work

Unexpected Driver CPC results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

A licence-only driver is excluded from this monitoring. An empty qualification field is not treated as a pass.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Drivers & Licences / Document Library

Find the original files linked to drivers and their licence/CPC evidence.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Drivers & Licences, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Drivers & Licences > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Drivers & Licences record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Drivers & Licences result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

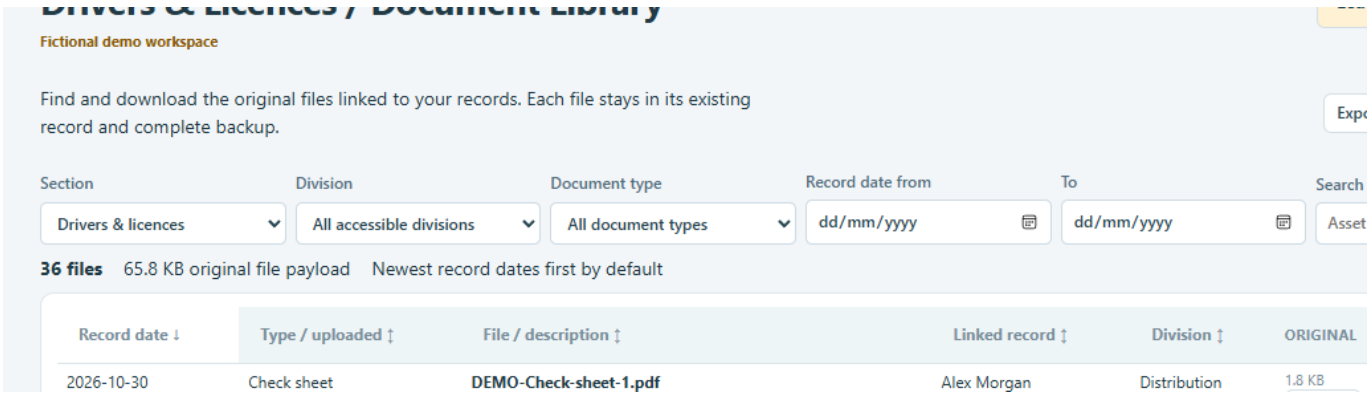
Open the downloaded Drivers & Licences file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Drivers & Licences catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Working Time / Overview

Review submitted weekly totals and outstanding data.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Working Time, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Select the division and the relevant week/reference scope.

Step 3

Read the totals and coverage indicators. Identify drivers with missing returns before interpreting an average.

Step 4

In the compact weekly grid, use names down the left and weeks across the right. Review each status label as well as its colour.

Step 5

Open the driver/week requiring review; enter or correct information in Weekly Returns & Imports.

06

Return to Overview to confirm the change and retain the outstanding submission list for follow-up.

Check it worked

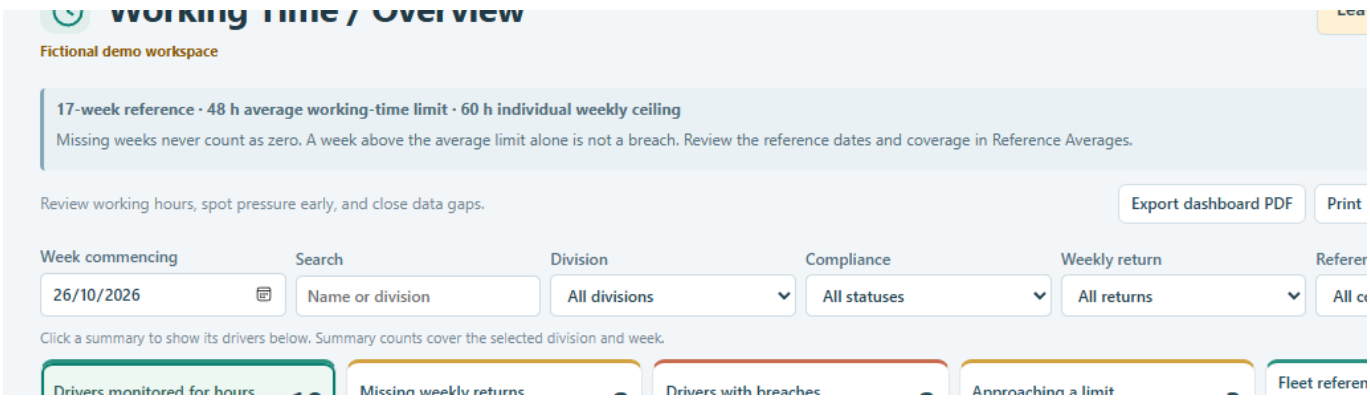
The review separates a submitted zero-hour week from a week that has not been supplied.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Weekly limits and reference-average limits are different measures. Follow the configured rule set; colour is not a complete compliance assessment.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Working Time / Reference Averages

Read high-to-low driver averages and inspect incomplete coverage.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Working Time, then choose Reference Averages. If its child list is closed, click the parent name once to open it.

Step 2

Choose the division and reference period. Check Working-Time Rules if the period/threshold is unexpected.

Step 3

Read the ranked average bars, numeric hours and status together. The dashed marker represents the configured average limit.

Step 4

Treat grey/hatched values as provisional: these use submitted weeks and do not represent complete coverage.

Step 5

Use the weekly totals to locate gaps or unusually high weeks, then open the relevant driver for supporting checks.

06

Correct missing/incorrect source returns and recalculate the review. Record persistent missing-data patterns in the management report.

Check it worked

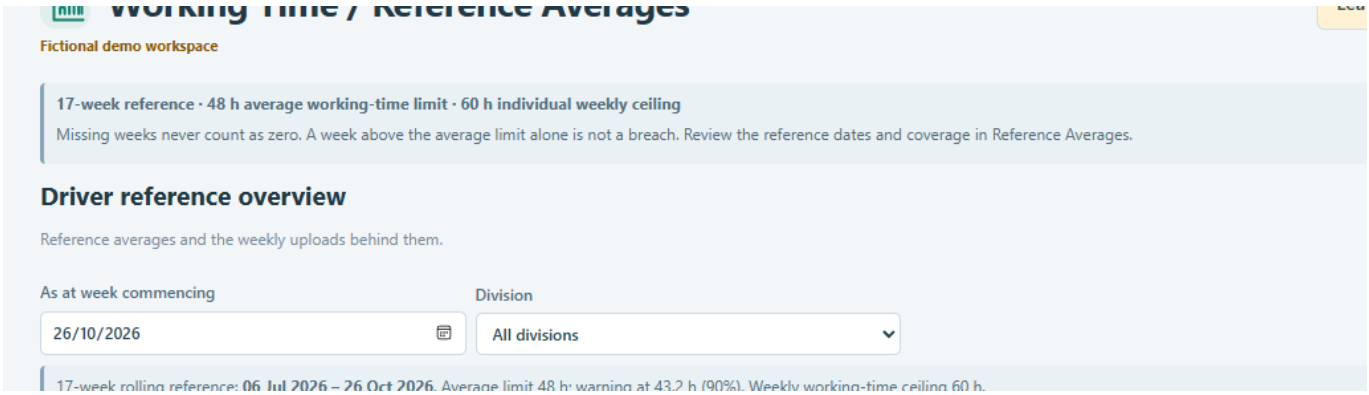
A ranked review shows both the observed average and whether it is supported by complete weekly data.

If it did not work

Unexpected Reference Averages results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Do not enter fabricated hours to remove an incomplete warning. Future, missing and genuine zero weeks have different meanings.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Working Time / Weekly Returns & Imports

Enter a single return or validate a supported bulk template.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Working Time, then choose Weekly Returns & Imports. If its child list is closed, click the parent name once to open it.

Step 2

Select the existing driver and the correct week. Check division and units.

Step 3

Choose detailed entry when component times are available, or total entry for an already calculated net working-time total.

Step 4

Keep work, breaks and qualifying availability categories separate. Record leave/absence using its controls rather than inventing worked hours.

Step 5

For bulk import, use the matching template, review headings and driver/week matches, then inspect duplicates and rejected rows.

06

Click Save return after reviewing the driver/week and values. Reconcile any imported counts and check Working Time > Overview and Reference Averages.

Check it worked

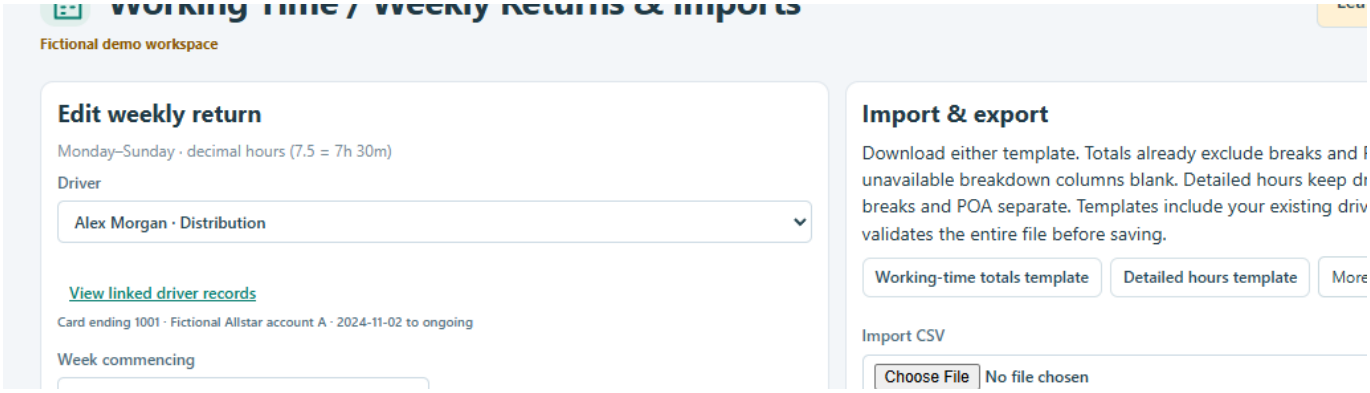
The correct driver/week receives the intended data and unresolved gaps remain visible.

If it did not work

Unexpected Weekly Returns & Imports results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

An absent return is not zero. Retain the source information used to produce totals.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Working Time / Document Library

Find the original files linked to working-time supporting records.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Working Time, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Working Time > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Working Time record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Working Time result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

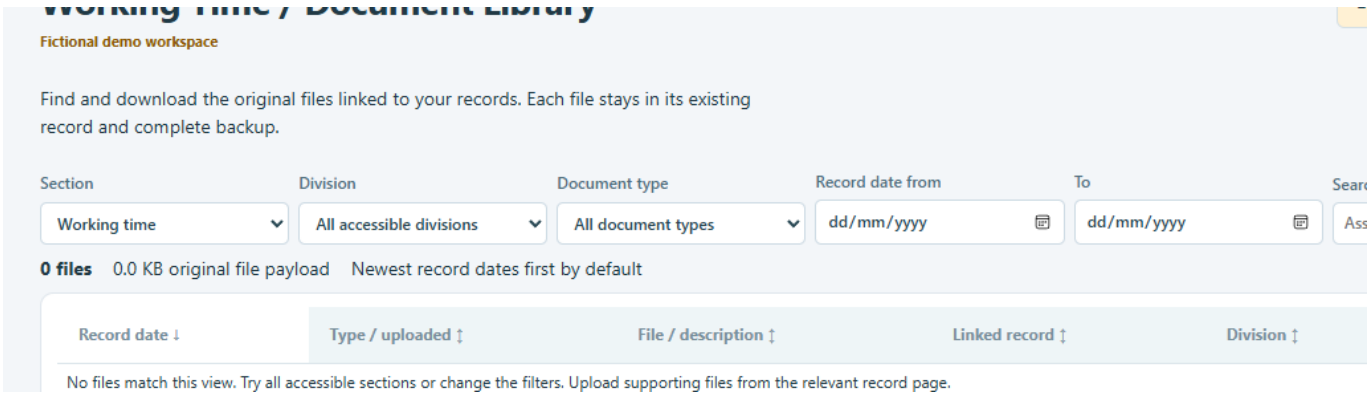
Open the downloaded Working Time file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Working Time catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Tachographs / Overview

Review the integration readiness and its current limitations.

Before you start

This optional section must be enabled by an administrator. It is a readiness screen, not a working tachograph analysis service.

Step 1

In the left menu, open Tachographs, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Ask an administrator whether Tachographs is enabled; it is disabled by default.

Step 3

Open Overview and read the readiness message.

Step 4

Continue using the provider's verified operational process and retain sample exports for future validated integration.

Check it worked

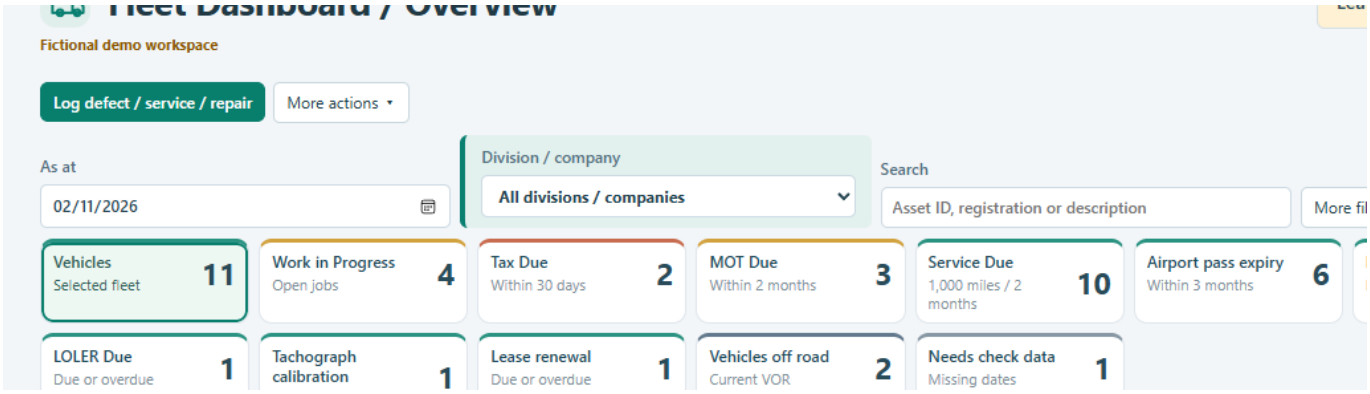
The visible section is understood as preparation, not a connected analysis service.

If it did not work

Do not enter invented download dates or infringement totals to populate a readiness screen. Continue with the verified provider process described in this section.

Check / boundary

Novadata Excel imports, raw card parsing, download-deadline calculations and infringement analysis are not operational in 2.10.0.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Tachographs / Download monitor

Understand the boundary of the download-monitor screen.

Before you start

This optional section must be enabled by an administrator. It is a readiness screen, not a working tachograph analysis service.

Step 1

In the left menu, open Tachographs, then choose Download monitor. If its child list is closed, click the parent name once to open it.

Step 2

Open Download monitor after reading the section Overview.

Step 3

Check the readiness statement; do not interpret the page as a live card/vehicle download register.

Step 4

Use the provider's verified download records to chase operational submissions until a validated monitor is supplied.

Check it worked

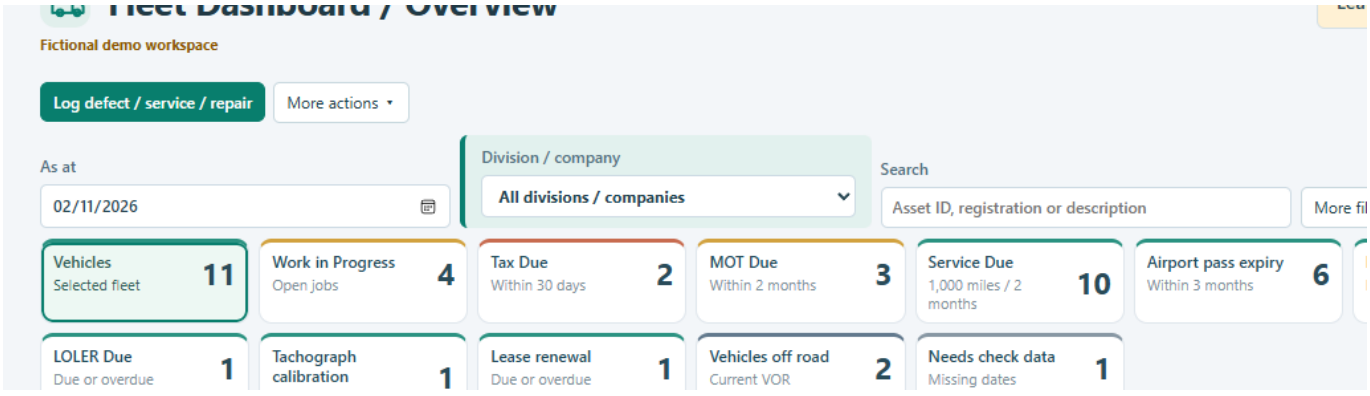
Download checks remain with the established provider process.

If it did not work

Do not enter invented download dates or infringement totals to populate a readiness screen. Continue with the verified provider process described in this section.

Check / boundary

A visible readiness page does not calculate which driver or vehicle has missed a deadline.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Tachographs / Infringements

Understand the boundary of the infringement screen.

Before you start

This optional section must be enabled by an administrator. It is a readiness screen, not a working tachograph analysis service.

Step 1

In the left menu, open Tachographs, then choose Infringements. If its child list is closed, click the parent name once to open it.

Step 2

Open Infringements and read its stated availability.

Step 3

Use the provider's verified analysis report for current infringement review.

Step 4

Retain a suitable synthetic export sample for adapter validation rather than assuming the screen has imported provider findings.

Check it worked

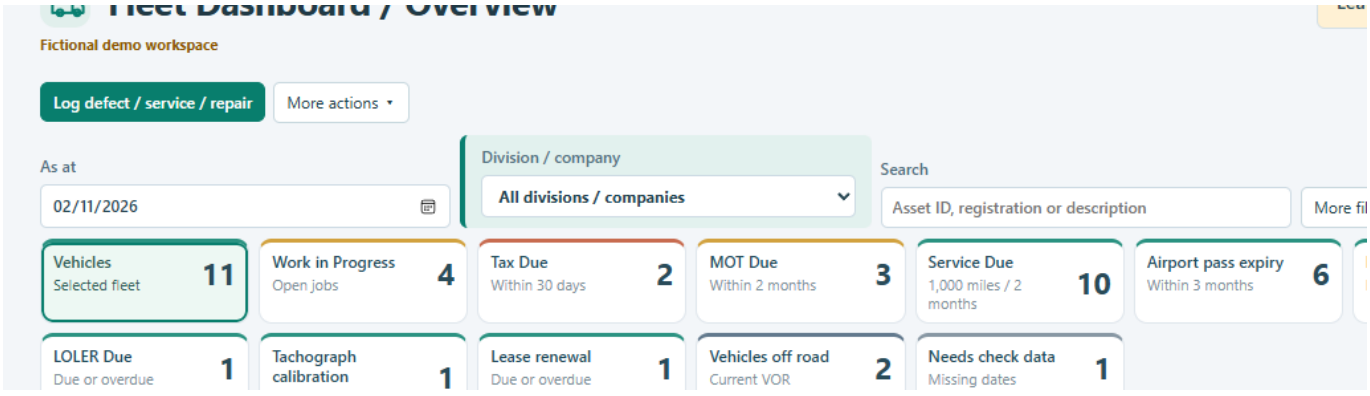
Provider findings are not confused with an unimplemented analysis feature.

If it did not work

Do not enter invented download dates or infringement totals to populate a readiness screen. Continue with the verified provider process described in this section.

Check / boundary

No operational infringement import or validated analysis is supplied here.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Tachographs / Reports

Check reporting readiness for the optional integration.

Before you start

This optional section must be enabled by an administrator. It is a readiness screen, not a working tachograph analysis service.

Step 1

In the left menu, open Tachographs, then choose Reports. If its child list is closed, click the parent name once to open it.

Step 2

Open Reports and inspect its current status.

Step 3

Use current provider reports for operational tachograph statistics.

Step 4

Before a future release is adopted, verify its data import, driver identity links and report totals against source samples.

Check it worked

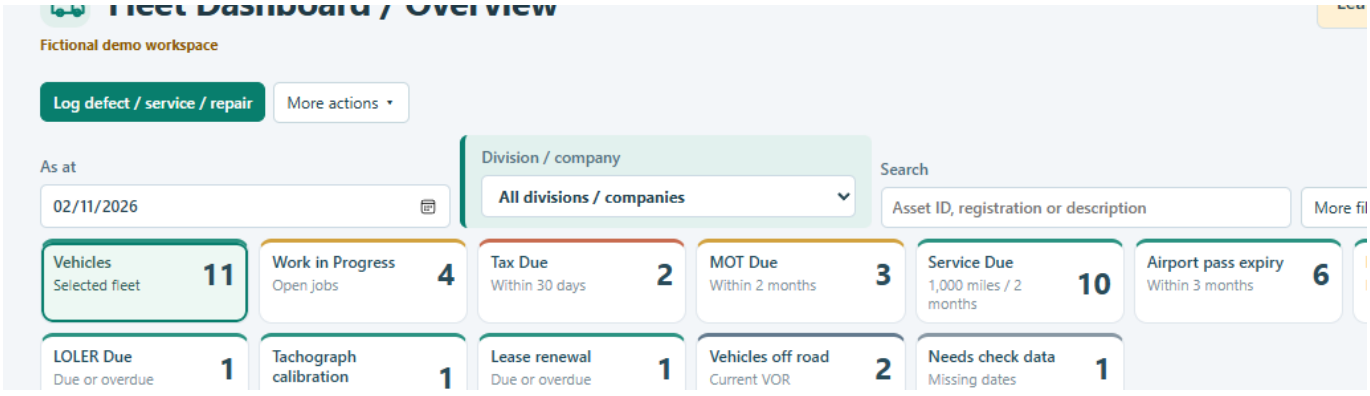
A future report will require source reconciliation before use.

If it did not work

Do not enter invented download dates or infringement totals to populate a readiness screen. Continue with the verified provider process described in this section.

Check / boundary

Do not present this readiness view as evidence of operational download-compliance or infringement statistics.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Accidents & Incidents / Overview

Create and maintain an incident case.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Accidents & Incidents, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Set the division and period. Search for an existing case before recording another event.

Step 3

Choose Record incident. Select the saved asset and driver, then enter event date/time, type, location and factual description.

Step 4

Record the available injury, claim, repair and status information. Attach appropriate photos/documents to this case.

Step 5

Save and reopen the case. Check reference, asset/driver, evidence and status.

06

Update claim and repairs as information develops. Before export, set dates/division/register filters and check the selected scope.

07

Use Export PDF or Print and inspect the full output. Evidence filenames do not imply every attached original is embedded.

Check it worked

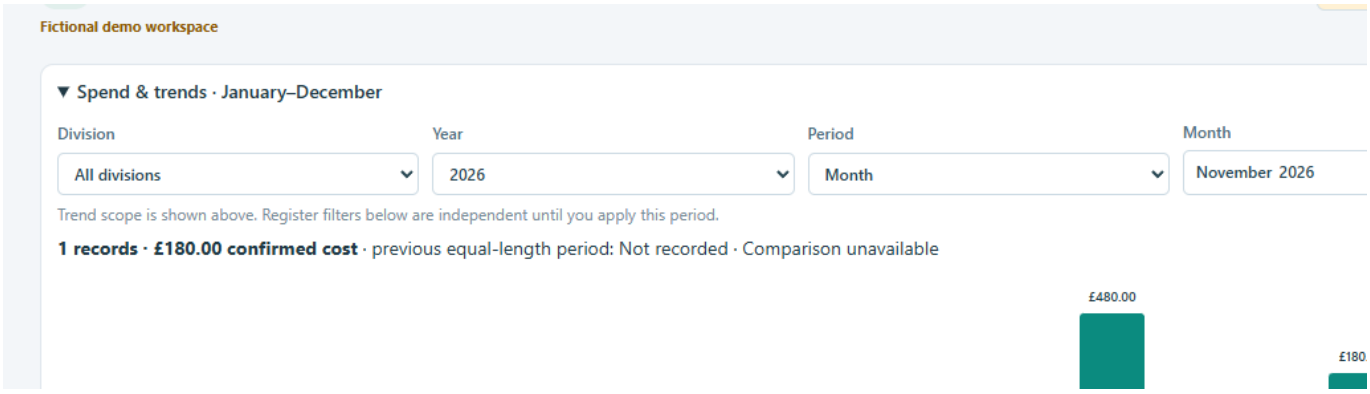
The case can be followed from occurrence to closure using its reference and linked evidence.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Do not record unverified attribution as a confirmed fact.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Accidents & Incidents / Analysis & Map

Compare incident types, periods and recorded locations.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Accidents & Incidents, then choose Analysis & Map. If its child list is closed, click the parent name once to open it.

Step 2

Choose the period, division and case filters.

Step 3

Review the graphical totals and contributing cases.

Step 4

Select a map/list item and read its case details; enable optional hover highlighting when helpful.

Step 5

Check unplotted cases separately and correct usable location data at source.

06

Export or include the incident section in Reporting, retaining scope and coverage notes.

Check it worked

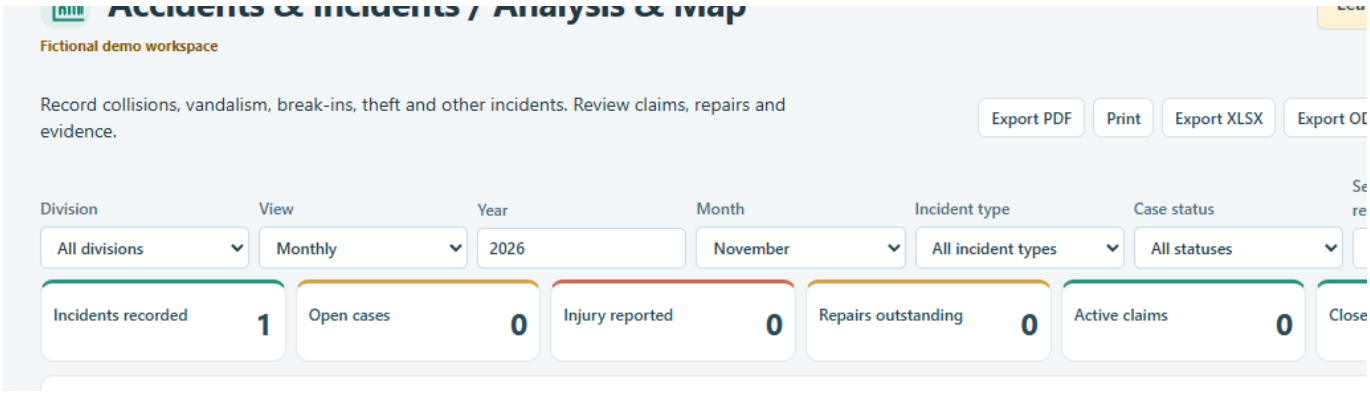
Location patterns are supported by case records and known map coverage.

If it did not work

Unexpected Analysis & Map results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Screenshot: map controls in the offline demonstration state; street tiles are not loaded. Map services are optional. Missing coordinates do not remove an incident from the register.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Accidents & Incidents / Expanded Map

Inspect the saved incident locations using the larger map view.

Before you start

Have the relevant saved location information ready.

Step 1

In the left menu, open Accidents & Incidents, then choose Expanded Map. If its child list is closed, click the parent name once to open it.

Step 2

Apply the same division/date scope as the analysis you are reviewing.

Step 3

Select the case/location and check the reference and asset/driver context.

Step 4

Open the underlying case to inspect evidence or correct location information.

Step 5

Return to the map to confirm the saved correction.

06

Use a fixed export for sharing; interactive map controls do not survive in PDF or presentation slides.

Check it worked

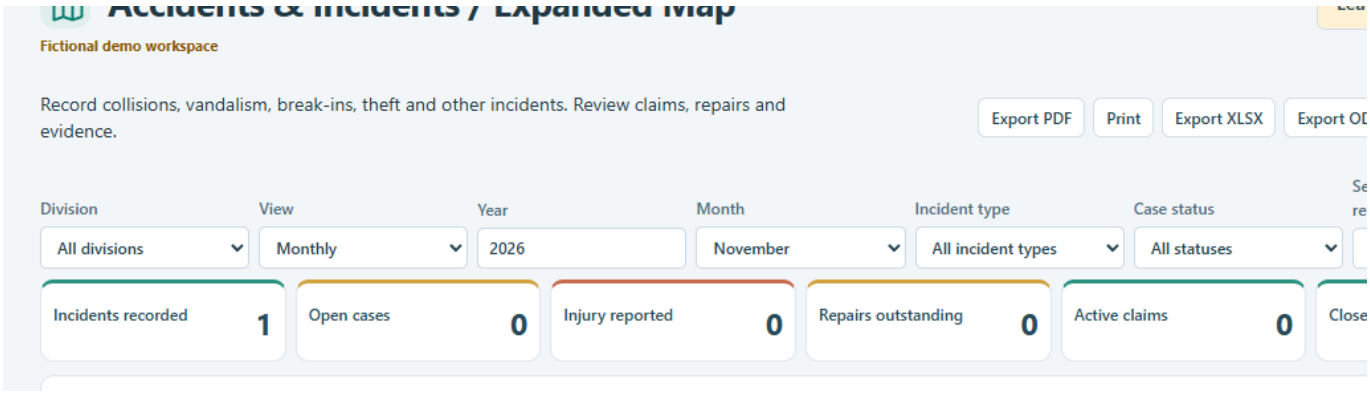
The expanded view helps examine recorded clusters while preserving a route to the case.

If it did not work

Unexpected Expanded Map results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Screenshot: map controls in the offline demonstration state; street tiles are not loaded. A point is a recorded location, not independent proof of liability.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Accidents & Incidents / Insurance Documents

Keep current policy/certificate copies accessible.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Accidents & Incidents, then choose Insurance Documents. If its child list is closed, click the parent name once to open it.

Step 2

Open Insurance Documents and locate the policy already covering the relevant scope.

Step 3

Add or update the policy information using the page controls, keeping provider/reference, applicable dates and scope clear.

Step 4

Upload the current certificate and supporting documents to the policy record.

Step 5

Save, reopen and download a copy to verify the original is readable.

06

Use the policy record or Document Library for later retrieval. Compare fleet coverage through Fleet Dashboard > Insurance Audit.

Check it worked

Insurance evidence is retained with its policy rather than scattered across unrelated cases.

If it did not work

Unexpected Insurance Documents results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

An uploaded certificate or audit match alone does not validate every asset's eligibility or policy condition.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Accidents & Incidents / Document Library

Find the original files linked to incident cases and accessible insurance evidence.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Accidents & Incidents, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Accidents & Incidents > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Accidents & Incidents record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Accidents & Incidents result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

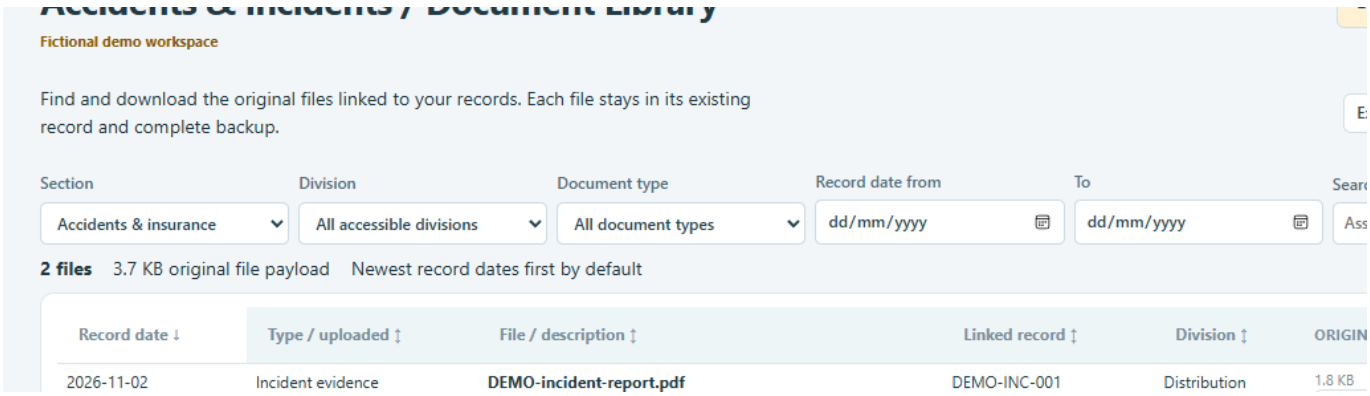
Open the downloaded Accidents & Incidents file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Accidents & Incidents catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fines / Overview

Maintain the fines register and supporting case information.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fines, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Set the division and dates, then search the reference before adding a fine.

Step 3

Use the fine entry controls to select the saved asset and driver and enter date, reference, amount, type, location and status as available.

Step 4

Attach the relevant notice/evidence and save.

Step 5

Reopen the fine to verify its reference, associations, amount and case state.

06

Update outcomes as they are confirmed, then reconcile the scoped totals before export.

Check it worked

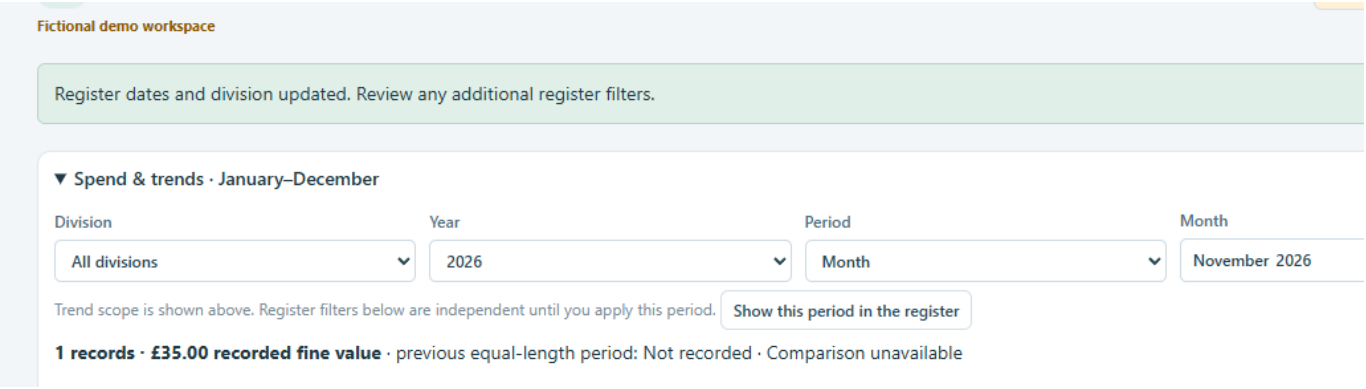
The fine remains traceable to its source notice and recorded outcome.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Verify driver attribution; a default vehicle/card association is not proof of responsibility.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fines / Analysis & Map

Investigate repeated fines alongside monthly comparison and location.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fines, then choose Analysis & Map. If its child list is closed, click the parent name once to open it.

Step 2

Choose the division and date range.

Step 3

Select a clickable summary box to review the fine records behind it.

Step 4

Use highest-repeat information and the monthly comparison to identify repeated drivers, assets or locations.

Step 5

Inspect the map and underlying fine. Review names, references, amounts and location text together, including records without usable coordinates.

06

Keep an action against the evidence and include the scoped trend in the management report.

Check it worked

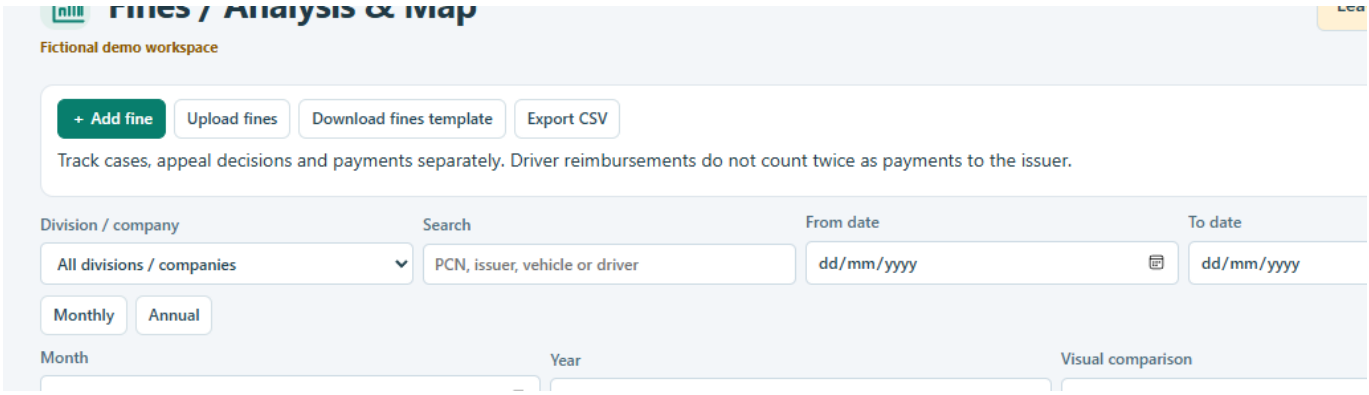
A repeat trend can be traced back to the contributing notices and locations.

If it did not work

Unexpected Analysis & Map results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Screenshot: map controls in the offline demonstration state; street tiles are not loaded. The map is part of the review where usable location information and map settings permit it. Exports contain static graphics, not an interactive map.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fines / Import Fines

Validate a supported fines file before updating the register.

Before you start

Have the relevant untouched source file and reliable asset/driver identifiers ready.

Step 1

In the left menu, open Fines, then choose Import Fines. If its child list is closed, click the parent name once to open it.

Step 2

Keep the source export and choose the offered import format/template.

Step 3

Check headings, date format, amount units and fine references.

Step 4

On Import Fines, click Check file and inspect the preview for duplicates, rejected rows and uncertain identities. Correct the source or mapping before continuing.

Step 5

Click Import reviewed only after the Import Fines preview is correct. Read the result, then reconcile the imported records with the original source.

06

Reconcile counts/amounts with the source and open a sample imported fine.

Check it worked

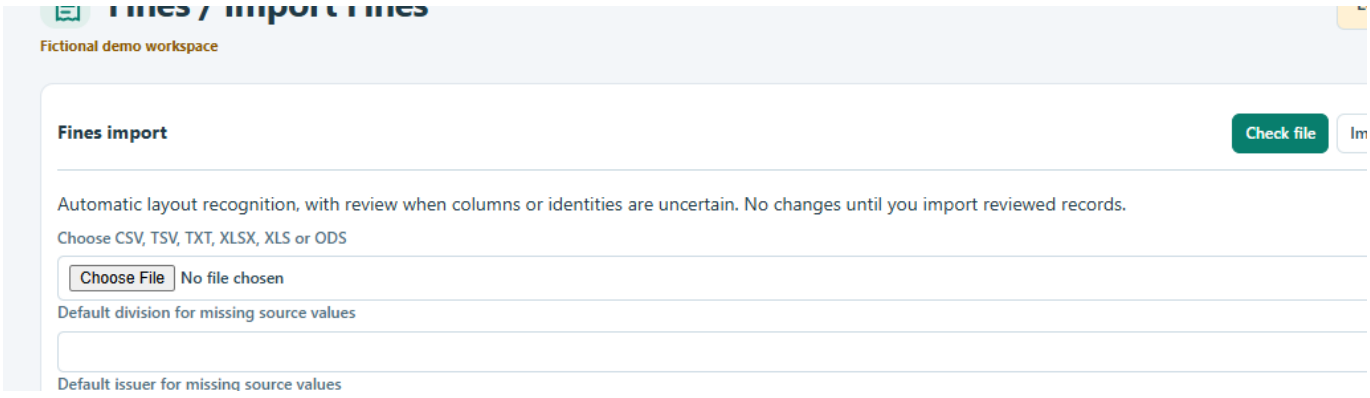
The import result is reconciled and uncertain cases are not disguised as valid matches.

If it did not work

Unexpected Import Fines results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

An import provider label does not imply a live data connection.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fines / Document Library

Find the original files linked to fine notices and supporting evidence.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Fines, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Fines > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Fines record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Fines result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

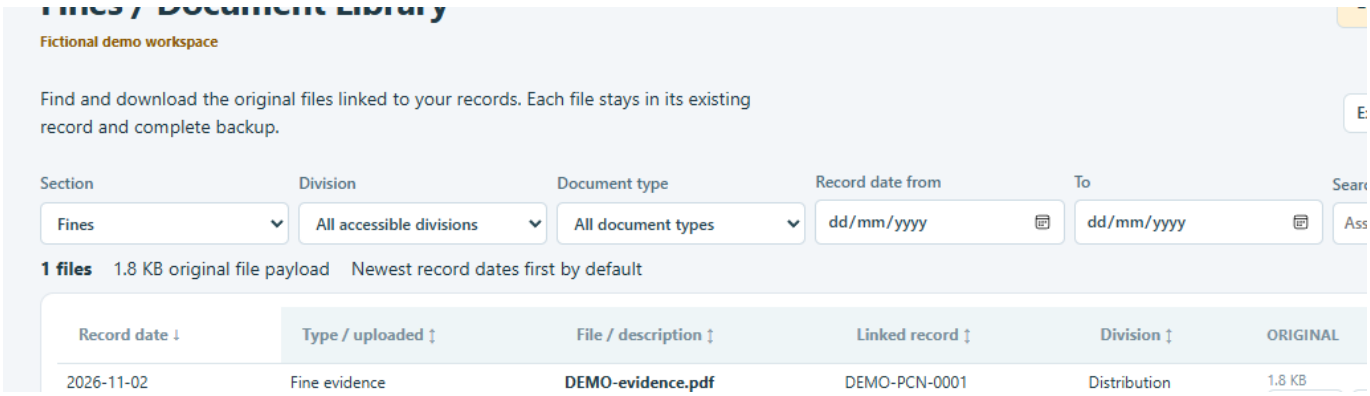
Open the downloaded Fines file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Fines catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fuel / Overview

Review purchases and investigate flagged transactions.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fuel, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Set the reporting dates and division. If empty, check filters before importing again.

Step 3

Inspect purchase totals and exceptions. Open a transaction and read its reason, product, amount and source details.

Step 4

Check the account/card, asset and driver association. Investigate reassigned/shared cards rather than assuming a named driver made the purchase.

Step 5

Compare source values and Review Rules before recording the review decision.

06

Export the scoped results or select Fuel in Reporting. Retain useful product, date, cost and location detail.

Check it worked

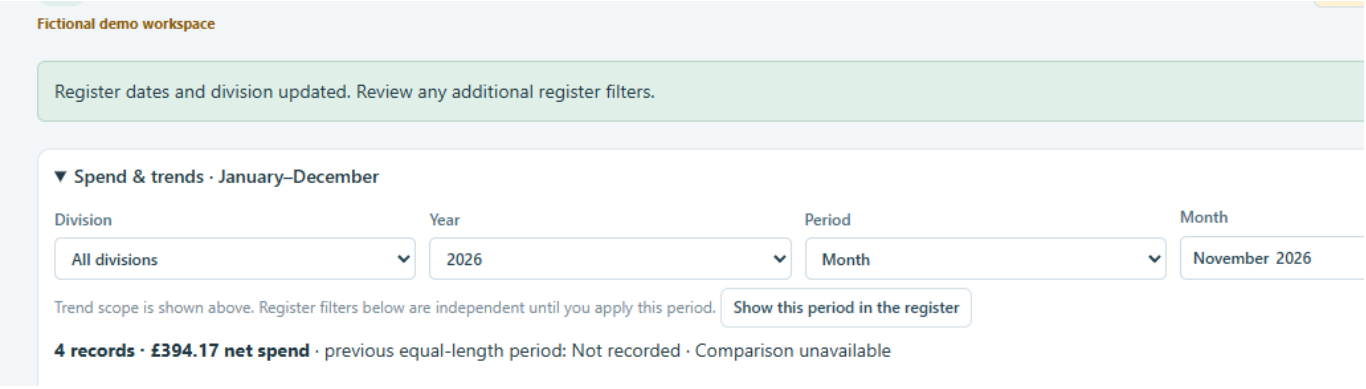
Exceptions are explained by actual transactions and known associations.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

A flag identifies a review condition. It does not establish fraud or personal responsibility.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fuel / Purchase Locations

Review where purchases were recorded and identify location-data gaps.

Before you start

Have the relevant saved location information ready.

Step 1

In the left menu, open Fuel, then choose Purchase Locations. If its child list is closed, click the parent name once to open it.

Step 2

Use the required dates/division.

Step 3

Select a transaction/location and compare it with its account, card and asset context.

Step 4

Use selection/optional hover highlighting to move between the list and map.

Step 5

Check unplotted purchases and the source location values separately.

06

Correct reliable source information and rerun the scoped review.

Check it worked

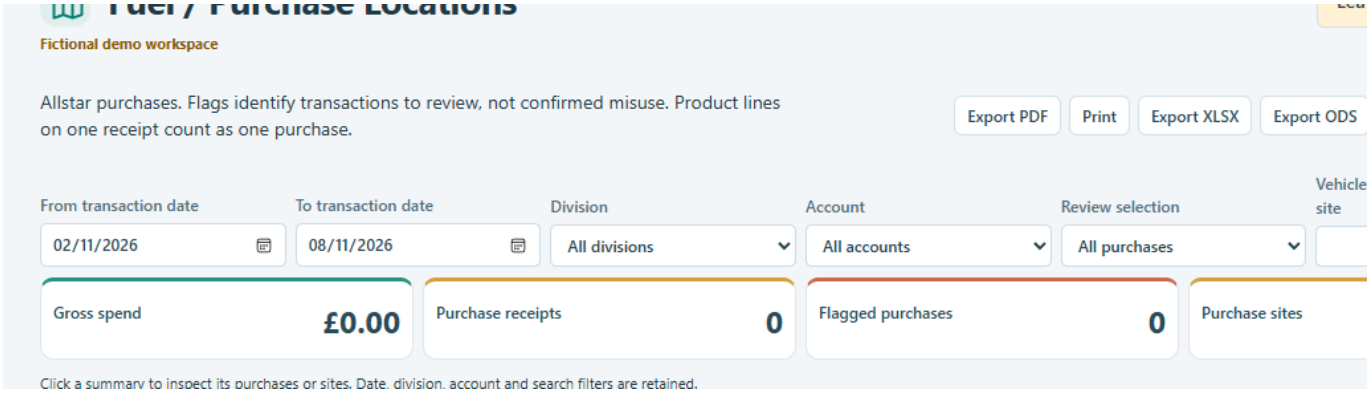
Map findings remain connected to purchases, with incomplete location coverage visible.

If it did not work

Unexpected Purchase Locations results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Screenshot: map controls in the offline demonstration state; street tiles are not loaded. Recorded transaction locations are not live GPS tracking.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fuel / Imports & Accounts

Load supported fuel exports and maintain the associated accounts/cards.

Before you start

Have the relevant untouched source file and reliable asset/driver identifiers ready.

Step 1

In the left menu, open Fuel, then choose Imports & Accounts. If its child list is closed, click the parent name once to open it.

Step 2

Keep the original provider file and choose the matching supported import format.

Step 3

Review account/card identity, headings, dates, product units and purchase values.

Step 4

Match existing assets/drivers where available. Review rejected, duplicate or unmatched rows before committing.

Step 5

Apply the reviewed import, compare its counts/totals with the source, and open sample purchases.

06

Maintain account/card associations deliberately when cards or vehicles change. Recheck resulting transaction context in Overview.

Check it worked

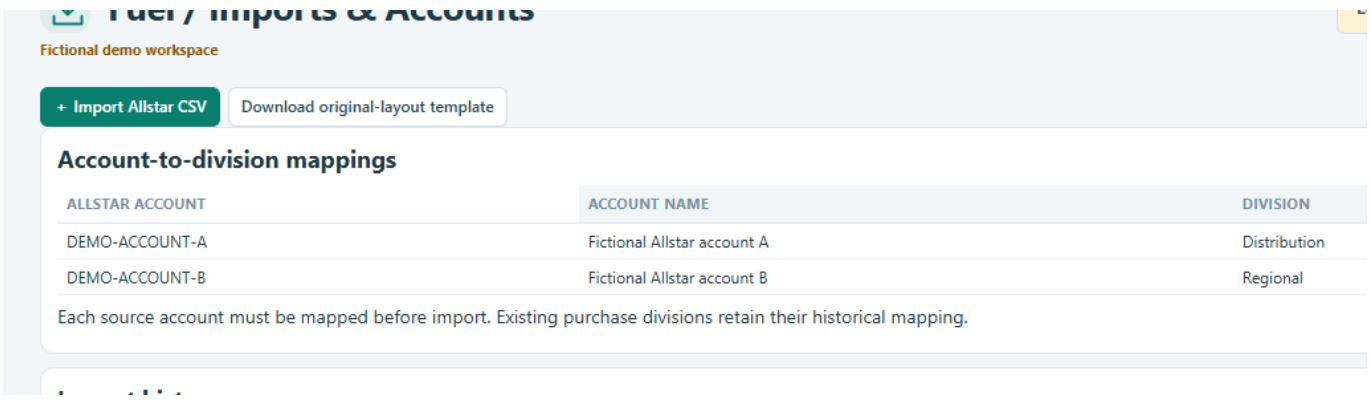
The imported purchases and saved account relationships can be reconciled with the provider source.

If it did not work

Unexpected Imports & Accounts results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Do not create duplicate drivers merely to resolve a fuel import.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fuel / Review Rules

Choose the review conditions used to flag fuel transactions.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Fuel, then choose Review Rules. If its child list is closed, click the parent name once to open it.

Step 2

Open Review Rules with an authorised account.

Step 3

Read the available rule descriptions and existing thresholds.

Step 4

Change only rules appropriate to the intended review and source data.

Step 5

Save, then inspect representative transactions in Overview to understand the effects.

06

Explain the selected rule basis in management reviews; investigate flagged data before assigning an outcome.

Check it worked

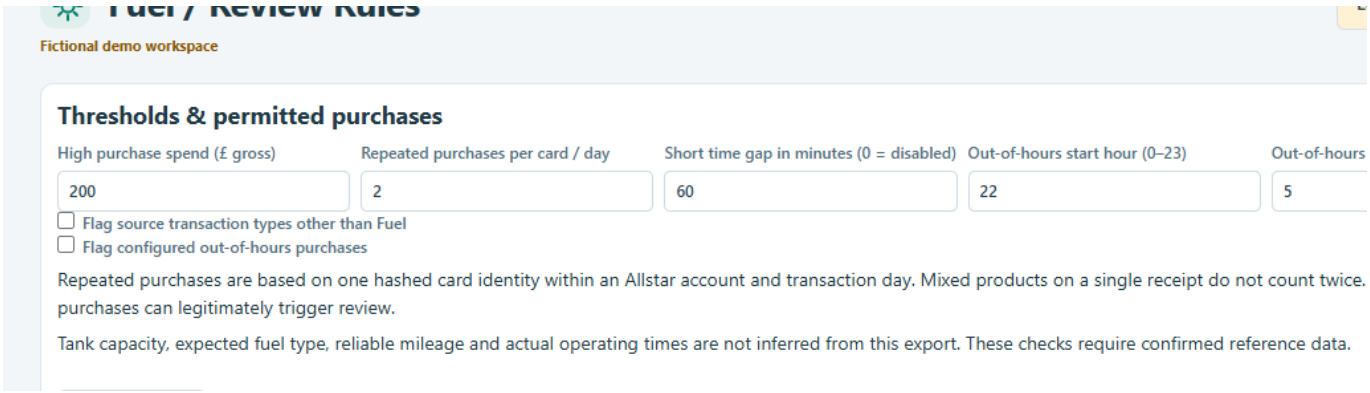
Review flags have an understood configuration and traceable transaction evidence.

If it did not work

Unexpected Review Rules results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Changing thresholds changes the review population; it does not change the provider's original transaction values.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Fuel / Document Library

Find the original files linked to fuel-section evidence.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Fuel, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

On Fuel > Document Library, choose the required division, record date and document type. Clear any old search text before beginning a different search.

Step 3

Search the Fuel record identity, filename or description. Use Previous / Next 20 or the available page-size control to inspect more rows.

Step 4

For the selected Fuel result, choose Open record to verify the owner. Use Preview for a supported PDF/image or Download for the original.

Step 5

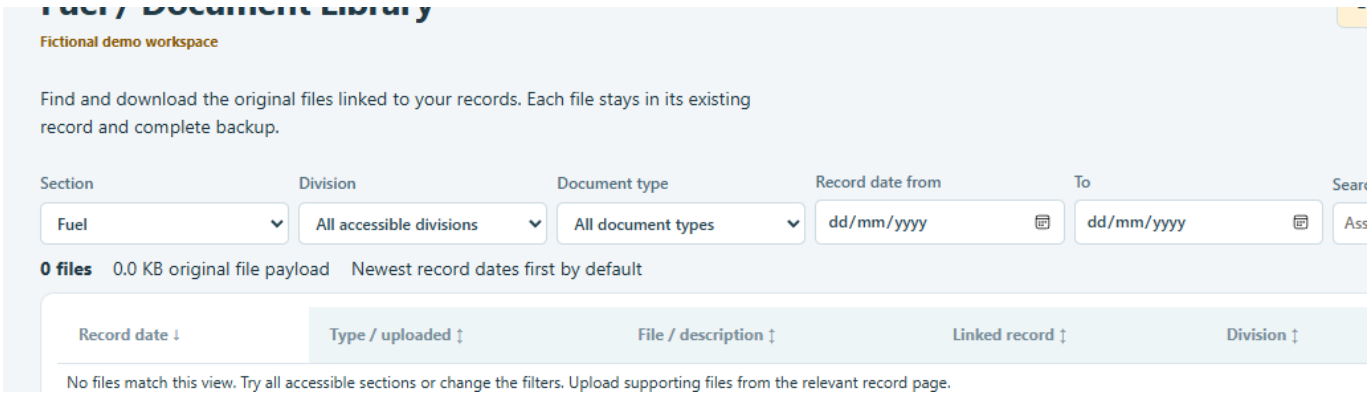
Open the downloaded Fuel file and check its content. To upload or correct evidence, return to its owning record rather than creating another library entry.

Check it worked

The same stored original is accessible through the Fuel catalogue.

If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Reporting / Overview

Generate a branded graphical report for the intended audience.

Before you start

Have the relevant report dates, division and intended audience ready.

Step 1

In the left menu, open Reporting, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Set From, To and Division. Last calendar month is a shortcut; check the resulting dates before continuing.

Step 3

Choose Complete report for all offered sections, or Choose sections and tick only the required report elements.

Step 4

Review company branding and choose the company logo through the available controls. Keep Full supporting records selected when detailed evidence is required; it is enabled by default in 2.10.0.

Step 5

Click Update report preview. Inspect the scope, totals, graphical summaries, missing data and supporting detail before choosing an export format.

06

Choose the format and follow generation progress/completion messages. Open the finished file before distribution.

07

Reconcile totals, dates and division with the screen; inspect charts, labels, maps/coverage and supporting detail in the recipient's office program.

Check it worked

A report combines graphical explanation with the records needed to support it.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Working-time reporting

Keep reference averages high-to-low with incomplete bars labelled. Include missing weekly returns and repeated gaps rather than treating them as zero. Read weekly totals against weekly thresholds and averages against their configured reference threshold.

Repeat-event reporting

For repeated fines/incidents include the contributing driver/asset, date, reference, amount/type and location information where recorded. A map complements the detailed records; unplotted events still require review.

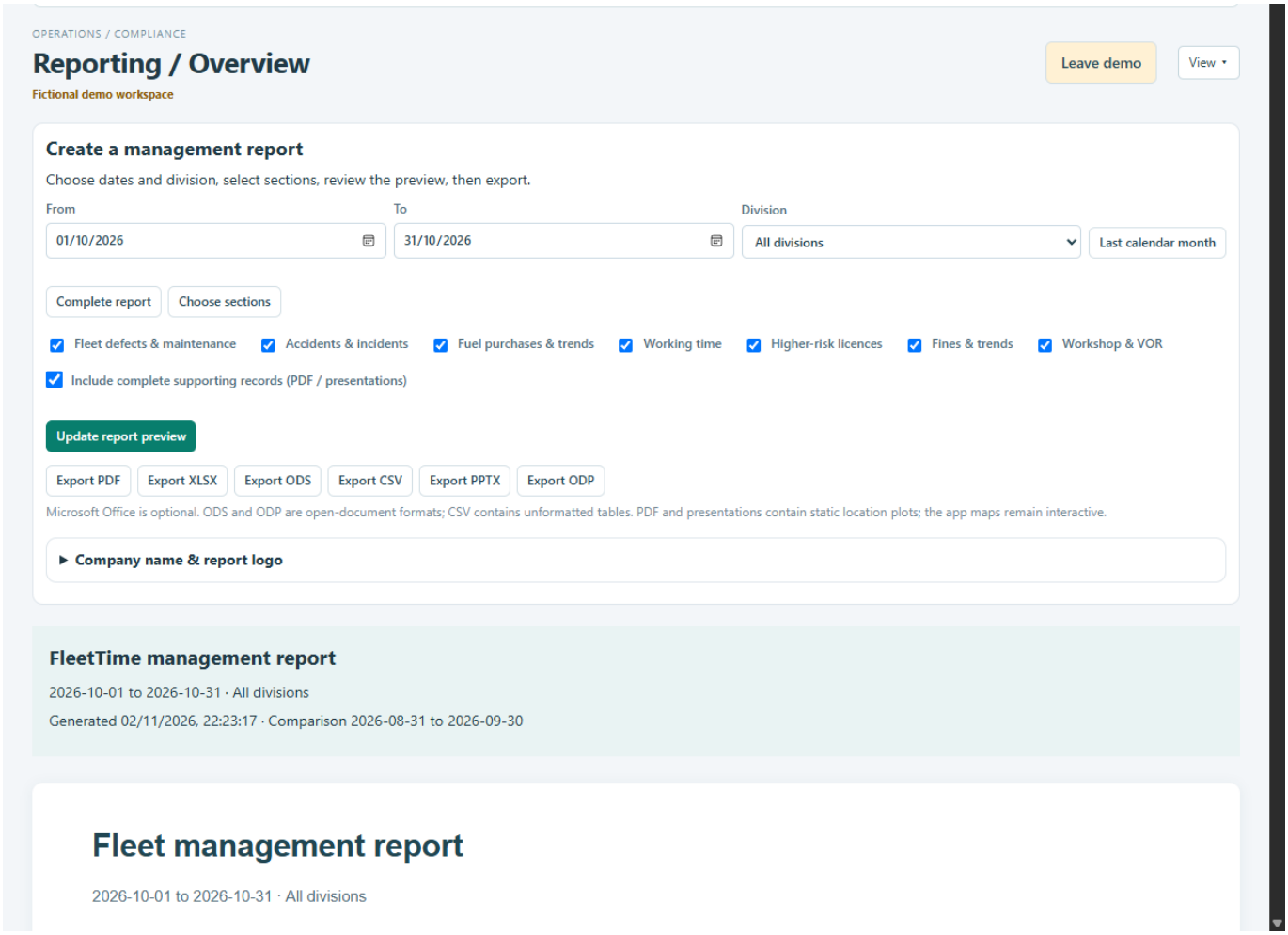
Read the finished presentation

Inspect each slide for a clear headline, chart labels, date/division scope and readable supporting detail. Verify the logo and any map coverage note. A successful file save does not guarantee that another office suite renders every element identically.

Check / boundary

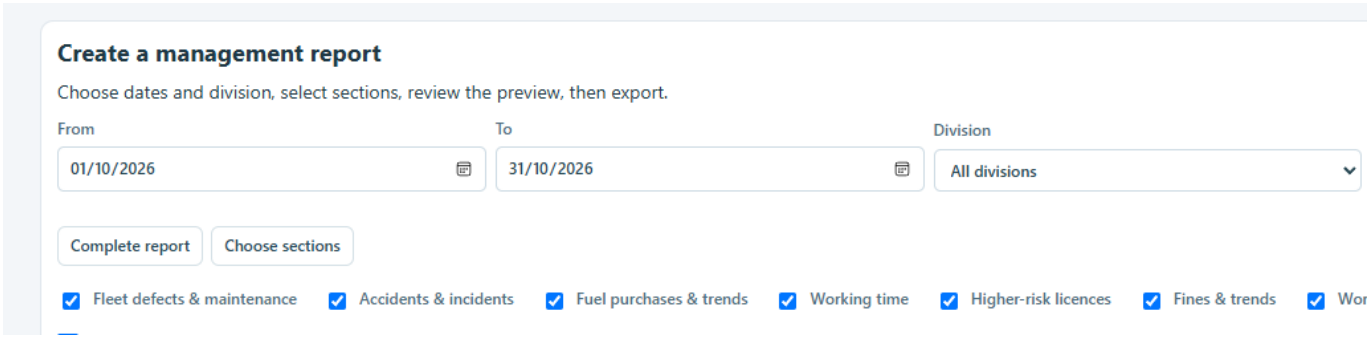
Use PDF for fixed pages; PPTX/ODP for presentations; XLSX/ODS for spreadsheet work and CSV where offered. Office alternatives still need a receiving-program layout check. Exported maps are static; files are not a complete data backup.

Reporting / Overview - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Closer view of the page controls



Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Documents / Overview

Search the all-accessible catalogue of originals held by FleetTime.

Central document search

Open Documents > Overview to search permitted documents across driver, vehicle/trailer, equipment, fines, incidents and other source records. Use owner, filename, reference, division and date/type filters; open a preview or the linked source record. Search covers indexed metadata; no automatic full-text OCR is promised.

Before you start

Have the relevant owning record and original-file access ready.

Step 1

In the left menu, open Reporting, then choose Document Library. If its child list is closed, click the parent name once to open it.

Step 2

Choose section, division, document type and document/record dates as appropriate.

Step 3

Search by registration, asset ID, driver, filename, description or other available identity. Use 20/50/100-row paging and the sticky headings for large results.

Step 4

Use Open record to confirm the owning asset, case, policy or import batch.

Step 5

Preview supported PDF/images or choose Download to obtain the original. Preparation progress is displayed when requested.

06

For shared inspection evidence check all represented assets/sections. If access is refused, request the appropriate business access rather than duplicating the file elsewhere.

07

Use the catalogue export only where your section export permissions allow it; retain full backups through Backup & Restore.

Check it worked

One original can be found through multiple relevant record routes without duplicate storage.

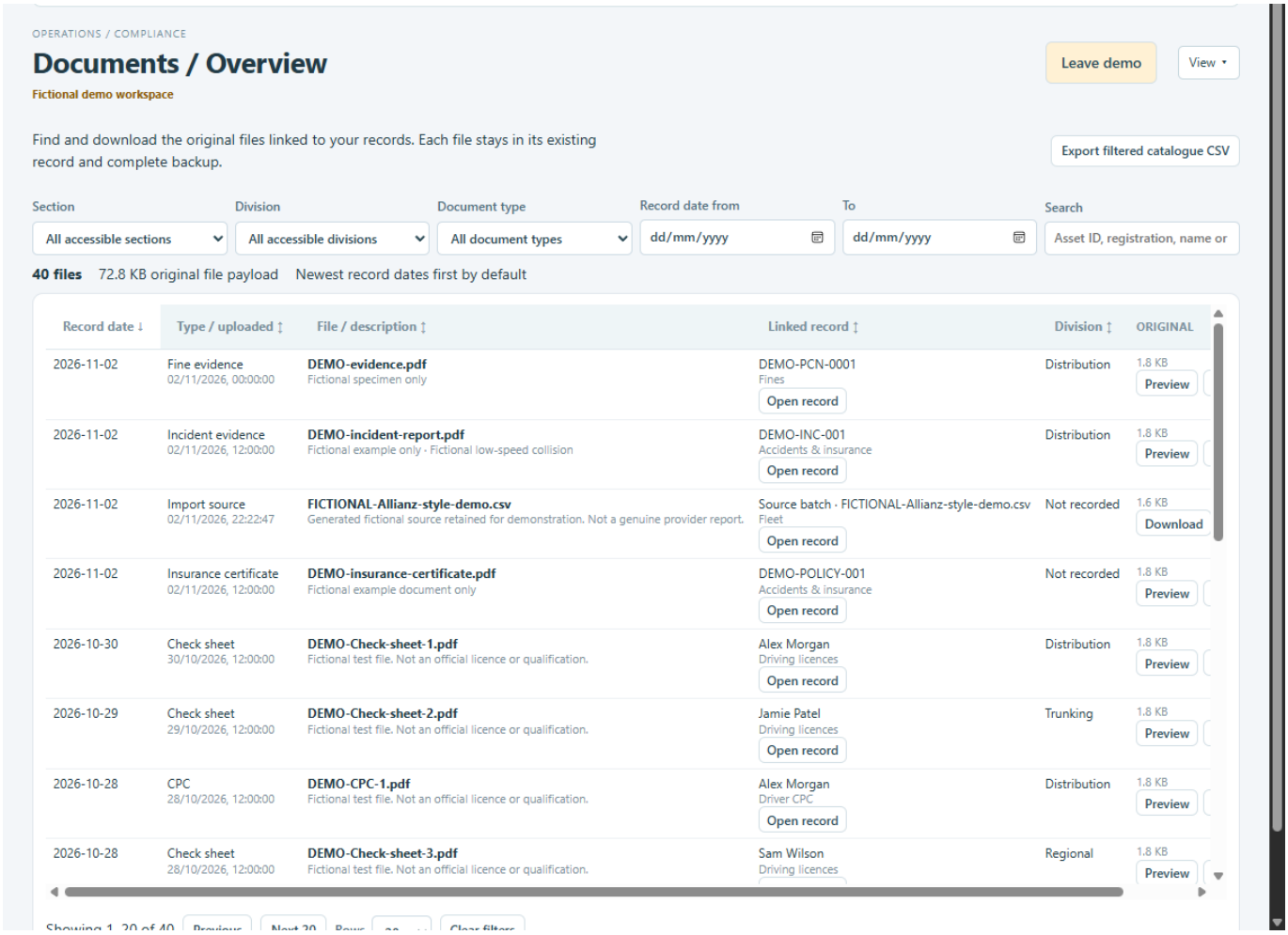
If it did not work

If the catalogue is empty, clear the search and check dates/division, then check whether a document was uploaded to the owning record. If a shared original is refused, ask the administrator to review access to every represented section.

Check / boundary

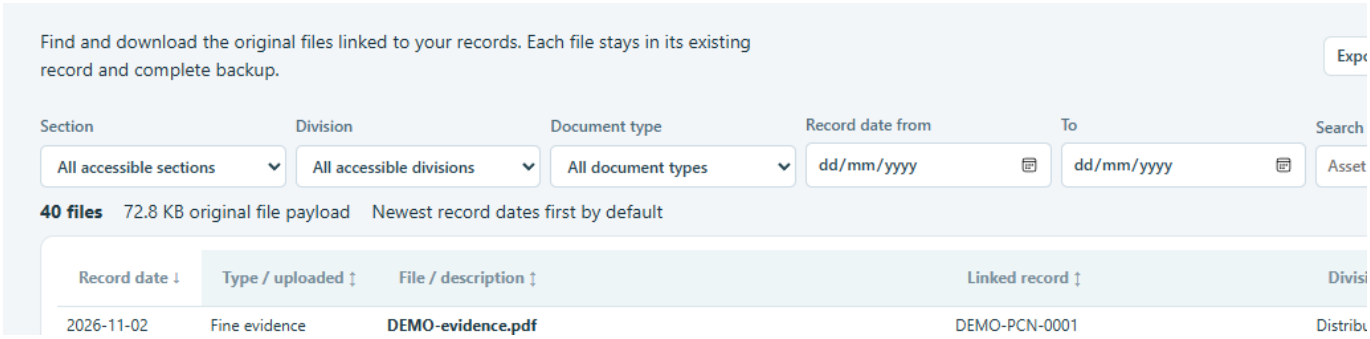
The library is permission-scoped. Mixed-section originals require access to all represented sections, and catalogue export checks export rights. Spreadsheet sources are downloadable evidence, not executable previews.

Documents / Overview - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Closer view of the page controls



Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Settings & Administration / Overview

Configure the tools and display used by this workspace.

New configuration tasks

Use Bulk Uploads for central import access, Users & Access for account and computer approvals, and the maintenance-cost switch to expose optional cost charts. Demo load/remove remains in Overview. Back up before trying destructive test actions.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Settings & Administration, then choose Overview. If its child list is closed, click the parent name once to open it.

Step 2

Open the page with configuration access and review existing options.

Step 3

Choose the required optional tools and display options, then save.

Step 4

Verify the resulting menu visibility using the intended user account. A hidden optional menu is different from deleted data.

Step 5

Open the relevant integration/provider settings to review file/API and browser preferences.

06

For users/access administration, create individual accounts and grant only the tasks required. Check view/edit/export/document and administrative capabilities before operational use.

Check it worked

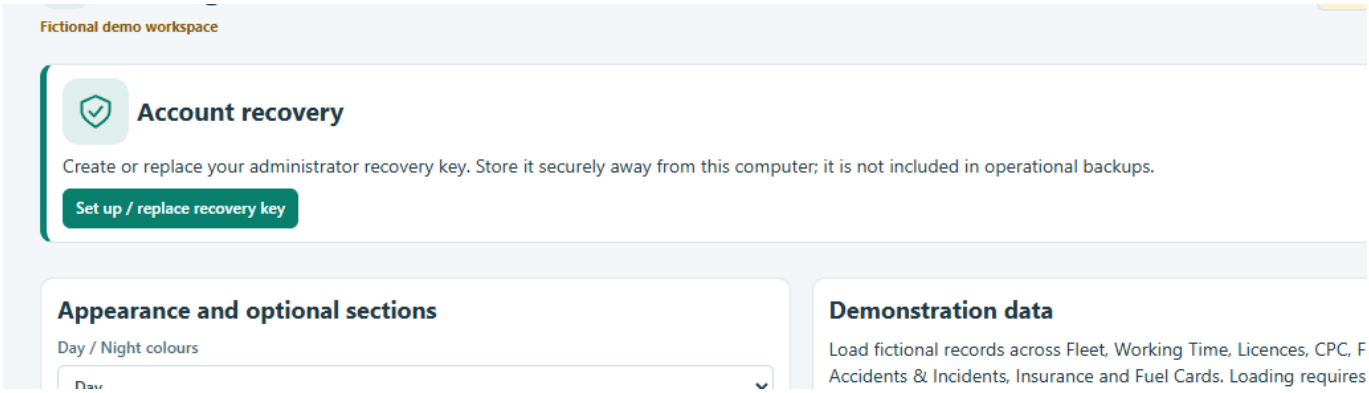
Optional visibility and user permissions match the intended operation.

If it did not work

Unexpected Overview results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Tachographs is readiness-only in this release. API requested is not connected. Network data connection is a native Settings > Data connection command, separate from this sidebar configuration.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Working-Time Rules

Maintain the reference periods and thresholds used by the working-time views.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Settings & Administration, then choose Working-Time Rules. If its child list is closed, click the parent name once to open it.

Step 2

Review the intended monitoring policy before changing any rules.

Step 3

Open Working-Time Rules and check the existing reference period and threshold settings.

Step 4

Enter the approved configuration and save.

Step 5

Revisit Overview and Reference Averages using known returns to check the period and indicators.

06

Explain rule changes in operational reviews and retain the basis for the organisation's chosen monitoring arrangements.

Check it worked

Weekly totals and reference averages use an understood configuration.

If it did not work

Unexpected Working-Time Rules results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Software configuration is not a substitute for determining which rules apply to an operation.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / RAM Mileage Integration

Review odometer readings downloaded from the RAM Tracking portal, or use the reviewed browser-collection route.

Simple three-step route

Enable RAM in Configuration, then open RAM Mileage Integration. 1 Get readings: use Open RAM browser & collect, sign in to RAM and complete MFA yourself; or choose an exported file from our optional RAM Mileage Reader extension. 2 Check readings: review registration/asset matching, dates, units, old/lower readings and rejected rows. 3 Save reviewed mileage, then reopen an asset to verify. The optional extension is included under RAM Mileage Reader 0.2.2 with Chrome/Edge Load unpacked instructions; publication in browser stores is deferred. Live portal collection still needs acceptance testing against your RAM account.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Settings & Administration, then choose RAM Mileage Integration. If its child list is closed, click the parent name once to open it.

Step 2

Choose mileage file and the correct Source layout. For a RAM Tracking portal export, select the layout currently labelled RAM desktop / browser export. Preserve the original file.

Step 3

Select the worksheet. For Other mileage spreadsheet, map distinct registration, mileage and date columns and choose miles or km.

Step 4

Click Check readings. Compare current versus incoming absolute odometer readings, identities, dates and units. Resolve rejected lower/older/duplicate readings before continuing.

Step 5

Read the acknowledgement and tick I have reviewed the mileage changes only when satisfied. Click Save reviewed mileage, wait for Mileage saved to the selected workspace, then open the asset mileage history.

06

The button currently labelled Open RAM browser & collect opens the RAM Tracking portal collection route. Sign in normally and review the collected readings before saving. Live acceptance against the customer's RAM Tracking portal account is still required; this screenshot does not demonstrate a live connection.

Check it worked

Imported readings remain associated with the correct asset and dates.

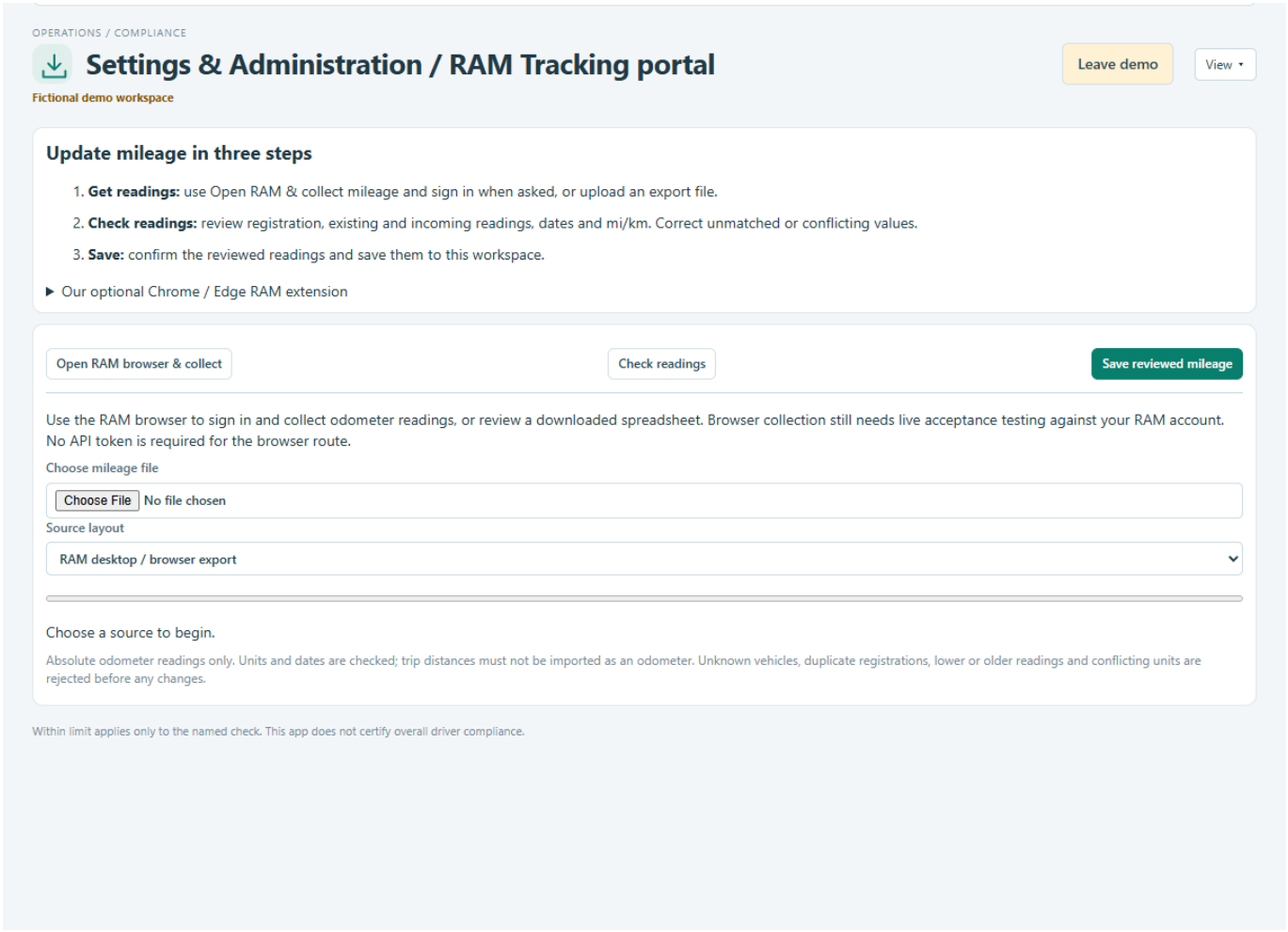
If it did not work

Unexpected RAM Mileage Integration results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

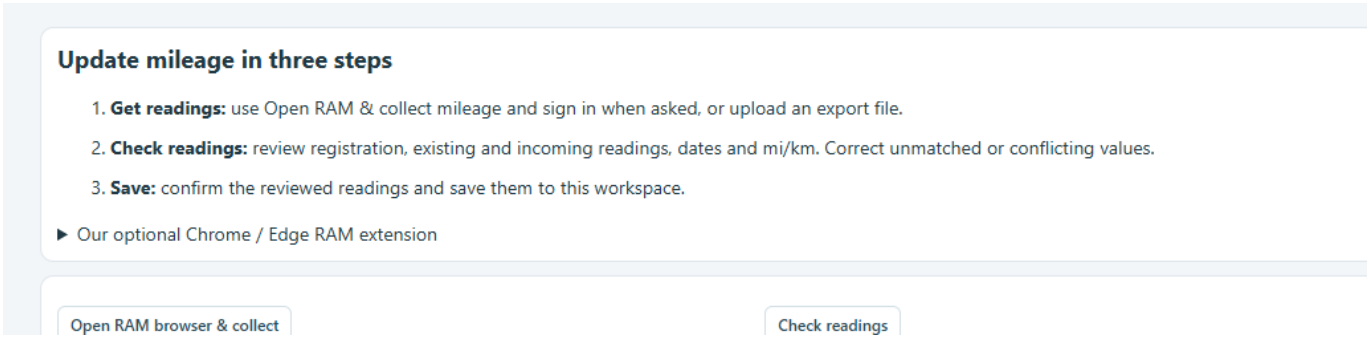
RAM Tracking portal is the provider name used in this guide. The menu and button labels above match the current software screenshot. Absolute odometer readings are required; trip distances are not odometer readings. No browser credentials or customer account were used in this capture.

Settings & Administration / RAM Mileage Integration - screen reference



The named page, captured from FleetTime 2.10.0 with fictional records. Use this view to locate the controls described on the preceding page.

Closer view of the page controls



Screens are within their task chapter, not in a separate duplicate screenshot appendix. Full-size images can be enlarged in the in-program guide. Provider connections and genuine customer records are not shown.

Settings & Administration / Field View Integration

Retrieve or inspect source data without automatically creating operational records.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Settings & Administration, then choose Field View Integration. If its child list is closed, click the parent name once to open it.

Step 2

For API discovery, an authorised administrator obtains the appropriate Field View token through the provider process. Enter it on the authorised PC and choose Save protected token. Never send the token in a ticket.

Step 3

Choose Test connection / business units, then Load projects. Projects are paged 100 at a time; change Project results start row for the next page.

Step 4

Enter the correct Project ID, choose Load form templates, and take the relevant template link IDs from the response.

Step 5

Set Form template link IDs and Modified from / Modified through, keeping the answer range shorter than three months. Choose Retrieve form answers and wait for the result.

06

Review returned source fields and use Download retrieved JSON if needed. Applying answers to working hours or creating defects is disabled until real question IDs, units, statuses and identity mapping are validated.

07

Without an API token, use Choose Field View export in Manual file review to inspect a supported CSV/TSV/TXT/XLSX/XLS/ODS export. This does not apply its records to FleetTime.

Check it worked

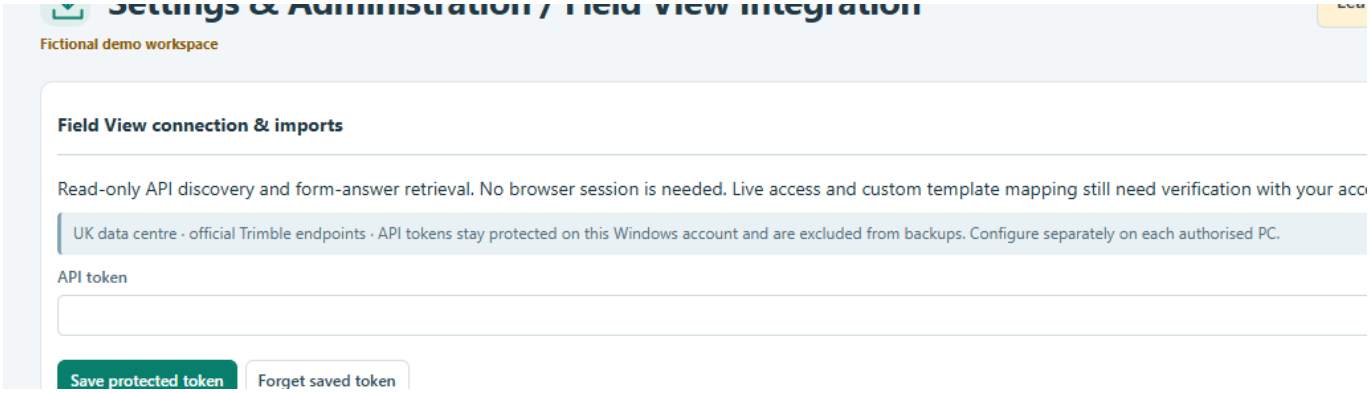
Users understand what has been inspected and what has actually been imported.

If it did not work

Unexpected Field View Integration results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

The packaged interface supports read-only API discovery/retrieval and file review. Live provider access still needs account-specific acceptance. Tokens stay protected on the Windows account and are excluded from backups.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Backup & Restore

Create and verify a complete backup, or recover a separate working copy.

Before you start

Have the relevant complete backup set, separate passphrase and destination space ready.

Step 1

In the left menu, open Settings & Administration, then choose Backup & Restore. If its child list is closed, click the parent name once to open it.

Step 2

Check the active edition/location and decide whether it is an earlier embedded workspace or managed format 13. Use the reviewed upgrade flow for a separate managed copy; do not convert files by hand.

Step 3

Choose a private backup destination. For cloud folders, select a locally installed sync folder and remember that FleetTime verifies local files only.

Step 4

Create an encrypted complete backup and retain its passphrase separately. Managed backup parts default to 2 GB decimal; 400 MB parts remain an option.

Step 5

Wait for packing and verification to complete. Keep the .ftbackup.json manifest and every numbered part together; no individual part is a complete backup.

06

For recovery, select the complete set and a separate destination. Follow progress until validation completes, then review records, originals and privacy decisions.

07

Switch to a verified recovered/upgraded copy only after review. Keep the original and earlier installer until the new copy is operationally accepted.

Check it worked

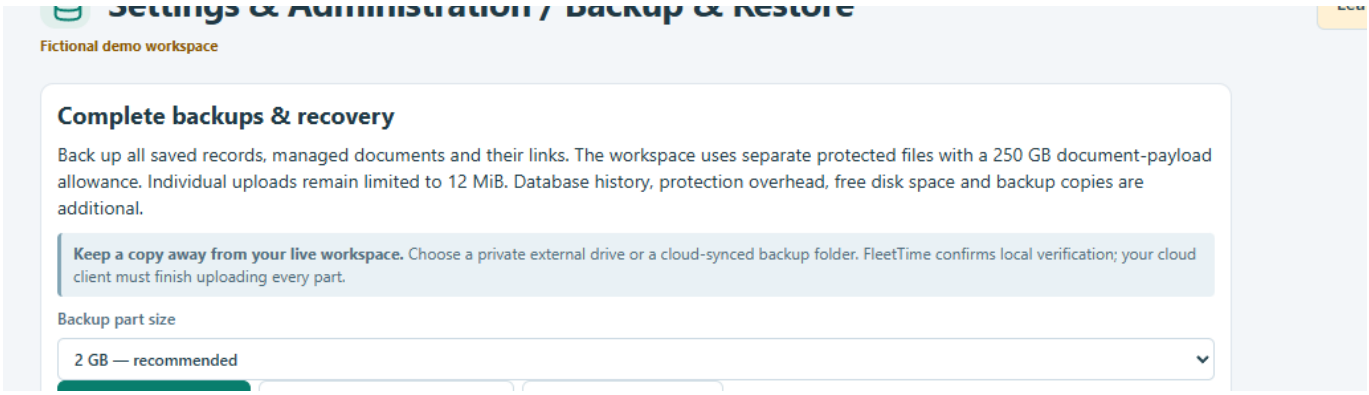
A complete verified set can create a separate recoverable copy while the original remains intact.

If it did not work

Unexpected Backup & Restore results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

Account recovery keys do not unlock backup passphrases. Do not place live databases in Dropbox/OneDrive sync folders. The administrator reference explains formats, capacity and cold-copy precautions.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Settings & Administration / Privacy & GDPR

Use the software's privacy administration tools as part of an organisation-controlled process.

Before you start

Have the relevant record identity, source information and permission for the task ready.

Step 1

In the left menu, open Settings & Administration, then choose Privacy & GDPR. If its child list is closed, click the parent name once to open it.

Step 2

Maintain the organisation's staff notice, individual accounts and access permissions.

Step 3

Record requests in the privacy request register and review access/export drafts before disclosure.

Step 4

For retention or erasure, inspect the preview and any holds. Investigate records and supporting evidence before authorising a destructive decision.

Step 5

Repeat review if the source changed. The structured driver erasure confirmation is ERASE DRIVER; use only through the authorised procedure.

06

Include external exports, aliases, free text and backups in the organisation's review. After recovery reconcile later erasure/retention decisions before use.

Check it worked

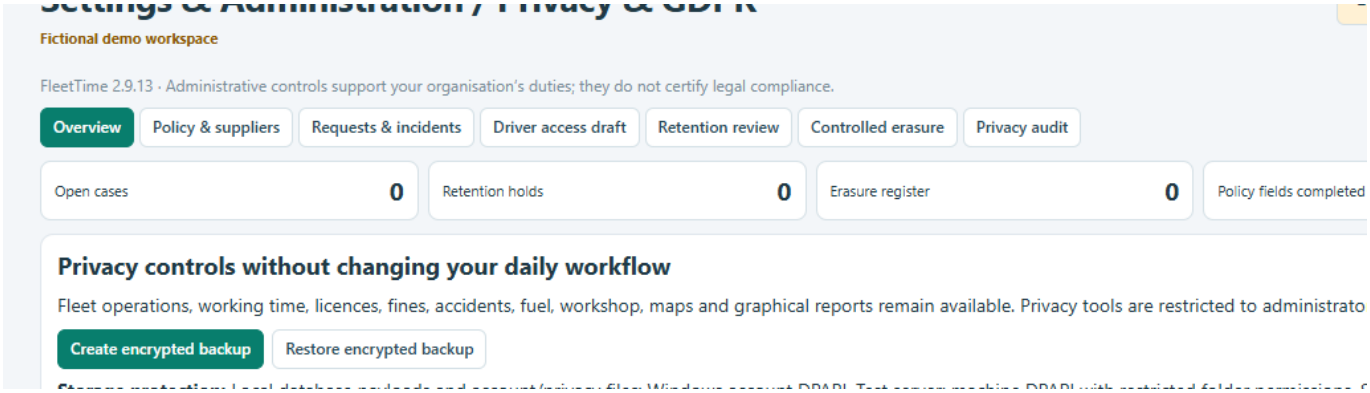
Privacy actions are reviewed and recorded alongside the organisation's own procedures.

If it did not work

Unexpected Privacy & GDPR results: clear search, check division/dates and confirm the workspace. For unavailable actions, ask the administrator to check permissions/configuration.

Check / boundary

These are operational software controls, not certification of GDPR compliance. The supplied privacy guide/company worksheet and the organisation's responsible advisers determine policy.



Screen detail from the named 2.10.0 page, using fictional records. The full screenshot can be enlarged in the in-program guide.

Technical & support / Architecture and persistence

Technical reference for administrators supporting the supplied 2.9.13 package. This describes implementation behaviour; it is not a production-deployment certification.

Client execution model

FleetTime is a Windows desktop application with a C# Windows Forms host and an embedded Microsoft Edge WebView2 interface. Local HTML, CSS and JavaScript modules provide the interface; a native host bridge performs protected data access, authentication, document operations and export/save integration. A normal external browser is not the FleetTime desktop runtime.

Trust boundary

The host maps bundled assets to https://fleettime.local. Native navigation and message handlers restrict the accepted origin. The user interface must not be treated as the sole permission boundary: AccessBridge/AccessPolicy and server access handlers validate the user and allowed changes. UI visibility and authorisation are separate concerns.

Logical data model

Operational information is a versioned JSON workspace containing drivers, working-time rows, rules and section-specific records. Fleet assets, workshop equipment, incidents, fines, fuel, provider batches, reports and documents use saved identities/references. The model is not a separate relational table for each visible register. Imports must preserve these identities rather than infer a new person from a similar name.

Local/server database

Store uses Windows winsqlite3.dll to maintain fleettime.db. The workspace table holds the current protected workspace; history retains earlier snapshots; revision provides an optimistic concurrency value. Writes use BEGIN IMMEDIATE, a protected payload and COMMIT, with rollback on failure. synchronous=FULL and secure_delete are requested. This is application-managed persistence, not a public SQL integration interface.

History is not backup

Ordinary saves retain up to 20 previous workspace snapshots in the database. Privacy purge writes remove history and run VACUUM. History on the same disk is not an independent recovery copy, and retained snapshots/pending files consume additional physical capacity.

Shared-folder difference

Network shared-folder mode uses an encrypted snapshot file and a Windows file lock. It deliberately does not open a shared SQLite database across SMB. The HTTPS service owns its SQLite data on the server, with clients using authenticated requests.

Technical & support / Locations, files and identifiers

Determine the actual active location before touching files. Historical identifier strings are retained for compatibility and must not be renamed to look newer.

Find the running copy

Use Help > About FleetTime to record edition, version, application folder, Windows user and installation status. A pinned taskbar item can still launch a portable/package copy. Use File > Open local data folder only with the relevant permission; in Network mode it is not proof that the active server data is held in that local folder.

Selected workspace

workspace-location.txt can redirect the edition's default location to a separately verified recovered/upgraded workspace. WorkspaceChoice expects verified markers and the Data/fleettime.db layout. If the selected folder is unavailable or marked incomplete, it fails rather than silently creating a new blank replacement.

Default paths are fallbacks

Local defaults to %LOCALAPPDATA%/FleetTime298TestLocal/Data; Network defaults to %LOCALAPPDATA%/FleetTime298TestNetwork/Data. A server setup starts with %PROGRAMDATA%/FleetTime298TestServer/Data unless configured otherwise. Actual selections may differ. The retained 298Test strings are internal compatibility names, not an instruction to delete the folders.

Protection and sidecars

Keep the whole data/security context for a cold-copy procedure: the database or shared snapshot, managed document folder and storage.key, protection marker, applicable account files, privacy register and shared key. The account directory for earlier workspaces can differ from the data directory; managed activation relocates/preserves it deliberately. Inspect the active configuration rather than copying only files from an assumed default.

Incomplete candidates

RECOVERY-INCOMPLETE.txt deliberately blocks a failed/interrupted recovery candidate. managed-storage-ready.json and recovery-success.json identify completed workflow stages. Do not delete an incomplete marker manually or manufacture a success file to bypass validation. Retry recovery into another new destination.

Quick reference

fleettime.db - Local/server protected workspace and history; ManagedDocuments.v2 - Protected original-file blobs plus storage.key; FleetTime.workspace.ftdb - Network shared snapshot, not SQLite; FleetTime.gdpr-key - Passphrase-wrapped shared protection key; FleetTime.accounts.json - Protected individual account configuration; FleetTime.privacy.ftprivacy - Protected privacy decision register; connection.json - Network connection options; protected saved server key; workspace-location.txt - Selection of a verified workspace copy

Technical & support / Document storage, limits and validation

Managed format separates record metadata from original bytes. A database-only copy is incomplete.

Managed references

Schema 13/documentStorageVersion 2 keeps document metadata with a storage reference: blob ID, original length, SHA-256 digest and a short content header. The document data field is empty. Protected .ftdoc files are immutable blobs beneath ManagedDocuments.v2. New writes are staged/verified before the reference is committed; lease markers distinguish pending uploads.

Protection format

ProtectedDocumentFile uses the FTDOC02 header, 256 KiB chunks and a random per-file nonce. Chunk context includes nonce and index; HMAC-SHA512 derives encryption/authentication material. AES-CBC plus HMAC-SHA256 authenticates protected content before releasing plaintext. This documents the supplied implementation; it is not an independent cryptographic audit.

File validation

Allowed type, filename and content-header checks apply. Common originals are PDF/JPEG/PNG. Incident evidence can additionally accept MP4/WebM through that workflow. Retained inspection sources have their own CSV/XLSX/ODS checks. A supported import-source type does not make that format a universal attachment type in every form.

Capacity interpretation

The managed current-original payload ceiling is 250,000,000,000 bytes, with up to 100,000 current document references. The per-original limit is 12,582,912 bytes (12 MiB). Physical disk use also includes protection overhead, database snapshots, retained/pending files, backups and recovery candidates. Earlier embedded-document workspaces keep their earlier limits until a reviewed upgrade.

Space checks

The software estimates space for archive/workspace preparation and adds a reserve. These checks do not guarantee that the drive stays free during another process's writes. Keep headroom and use a destination capable of files of the selected part size. The Windows path check rejects excessively long destinations; choose a short direct folder when it reports this.

Support investigation

If a file fails to open, record its document/owner identity, filename, time and exact error. Check whether the original blob and storage key are present in the complete workspace. Recover a verified set into a separate destination if required. Never regenerate storage.key or edit a blob/reference to make validation pass.

Quick reference

Current attachment payload - 250 GB decimal; Current document references - 100,000; One original file - 12 MiB; Default archive part - 2 GB decimal; Optional smaller part - 400 MB decimal; Streamed archive safeguard - 300 GB decimal archive stream ceiling

Technical & support / Accounts, permissions and sessions

Application accounts are separate from the operational workspace import. Restoring records must not grant someone administrator rights.

Individual users

AccessService stores protected account settings with active/admin flags, permissions, revision and password state. Section permissions distinguish view/edit/delete/export, with additional capabilities for sensitive data, documents, backup, restore, configuration and users. The supplied model is capability-based; do not assume that choosing a division filter provides a division-level security boundary.

Password storage

Account password hashes use PBKDF2-HMAC-SHA256 with 210,000 iterations and per-account salt. Backup/shared-folder passphrase derivation is a separate process. Passwords are not stored as plain text in the account file. Give every operator an individual account and avoid routine use of a shared administrator login.

Sessions and failure handling

The service maintains in-memory tokens tied to account revision. Current() checks active status and a 20-minute inactivity condition when validating a request. Account changes/password changes invalidate sessions through revision or explicit removal. Five failed sign-in/recovery attempts trigger a five-minute block in the account store. These implementation values are not an assurance of a desktop timer firing at an exact wall-clock second.

Temporary passwords

Administrator resets/new accounts can require password change. Native Require() refuses normal work while MustChange is set. If access appears restricted immediately after a reset, complete the password-change procedure rather than altering records or removing account files.

Administrator recovery

The administrator recovery key is distinct from the password, server connection key and backup passphrase. Successful recovery replaces the password, rotates the recovery key and revokes earlier sessions. Store the new key through the organisation's approved secret-storage process. Deleting account files to trigger first setup is not a supported repair.

Diagnose denied operations

Check exact edition/workspace, account active status, temporary-password state and required capability. For shared evidence, check access to every represented section. Confirm with a non-administrator test account. Do not solve a normal task by granting unrestricted administration to all users.

Computer connections

Computer approval is a separate gate from account permissions. The first HTTPS administrator can bootstrap using the server setup key. Shared-folder administrators retain the encryption recovery passphrase. Subsequent users request approval instead of sharing those secrets. Locally cached shared keys/connection tokens are protected for the Windows user; server/shared revocation is checked on subsequent access.

Technical & support / Encryption scope and portability

A copied protected file is not necessarily readable under a different Windows account or machine.

Local protection

Local protected workspace/account material uses Windows DPAPI CurrentUser. Copying fleettime.db to a different Windows account is therefore not a portable migration. Preserve the original context until an encrypted complete backup has been restored and verified under the destination account.

Shared-folder protection

The shared workspace uses a random key wrapped in FleetTime.gdpr-key by a 12-to-256-character passphrase. PasswordKey uses PBKDF2-HMAC-SHA256, 600,000 iterations and a random 32-byte salt; protected content uses separate encryption and authentication key material. Keep the original wrapped key; do not create a replacement when it is missing.

Server context

Server protection includes machine-scope DPAPI handling and restrictive data-folder access checks. A folder writable by an interactive administrator does not establish that a separate Windows service identity can use its keys and files. Establish the actual service-account protection behaviour in a controlled deployment before relying on it.

Backup secrets

Portable encrypted backup protection is passphrase-based. There is no master publisher code in this build that recovers a lost backup passphrase. An application administrator recovery key restores account access, not cryptographic access to an unrelated encrypted archive.

Migration method

Use the reviewed copy/backup/recovery workflow to move between storage contexts. Keep source application, data, identity and configuration unchanged until the destination has passed record and document checks. Do not bulk-decrypt or hand-edit protected files as a routine support action.

Technical & support / Network: shared-folder deployment

Use this mode only on a reliable Windows-compatible share supporting exclusive locks and atomic replacement.

Connection procedure

Use the Network installer typed path, or Settings > Data connection, Shared Windows folder. Test the full UNC or mapped path and verify the expected workspace. The first administrator creates/unlocks the shared encryption key and retains its recovery passphrase. Other Windows accounts/computers request administrator approval using the verified pairing code in Users & Access, then sign in individually. No local fallback or record merge is performed.

Storage protocol

FolderStore uses FleetTime.workspace.ftdb with a magic header, stable folder ID, revision GUID, payload length and SHA-256 integrity value. Reads/commits hold FleetTime.workspace.lock using FileShare.None; contention waits up to the configured interval (10 seconds by default). Commit writes a durable temporary file and replaces the snapshot atomically, retaining .previous where applicable.

Concurrency

A client saves against the revision it loaded. If another client committed first, saving fails instead of silently overwriting newer work. Capture the unsaved information, then File > Reload saved data and re-enter/review the change. Do not repeatedly force the stale save or delete the lock file while clients are running.

Permissions and identity

Users need the operations required by the application, including creation and atomic replacement; a read-only share is insufficient for writers. The saved folderId detects a different workspace substituted at the same path. Follow the deliberate reselect/test procedure for an intentional replacement; do not edit folderId to suppress the check.

Unavailable share

A missing folder, missing expected snapshot, hash failure or inability to obtain the lock blocks access. Local data is not selected as a fallback. Check drive availability, network, permissions, share behaviour and concurrent saves before recovery. Ordinary cloud-sync folders do not implement this shared live protocol.

Technical & support / Network: HTTPS service deployment

The Network client connects to a FleetTime service. It does not connect directly to a website-hosted SQLite file.

Server prerequisites

Use a Windows server/dedicated machine with a direct local data disk, known service identity, trusted server certificate and private key access, reachable DNS/port, adequate storage and a backup/recovery plan. Run server setup on the machine that owns the disk. The setup form does not automatically arrange firewall rules, certificate trust or service installation.

Configuration

Server setup holds DataDirectory, Prefix, CertificateThumbprint and Key in the selected configuration. A typical client endpoint is https://fleettime-server:8443/. Production requires HTTPS; plain HTTP is accepted only for loopback testing. Preserve the configured key/address/certificate when updating. Do not publish keys in screenshots or support attachments.

Authentication layers

The bearer connection key (at least 24 characters) identifies authorised client access to the service; it is not an individual login. Access endpoints also use individual application sign-in/session tokens. First administrator creation uses a separate one-time code from the service host. Client connection keys are saved using Windows CurrentUser DPAPI.

Protocol compatibility

The service health response exposes API/protocol/document-storage compatibility. Internal strings such as FleetTime298TestServer and GDPR-test-1 remain compatibility identifiers. Managed clients use managed-files-2 and the service document-storage protocol 2; the health workspaceVersion field is not the same as JSON schema 13. Use matched supplied clients/server rather than changing headers to bypass checks.

Request and save model

Access routes under /v1/access perform permission-scoped reads, writes, document staging/read and administration. Writes use ETag/If-Match revision checks. The server validates the source and committed document inventory. This internal API is not an advertised general integration API for provider imports.

Acceptance on the real host

Test service start/restart under the real service identity, certificate private-key use, client trust, DNS/firewall reachability, account setup, two-user conflict handling, original-file access, backup and separate recovery. An interactive test or localhost health reply does not replace this acceptance.

Relocation caution

Stop clients/service and preserve the original directory/configuration. For managed workspaces use the reviewed whole-workspace upgrade/backup workflow. Do not assume a generic database-location copy dialog transfers ManagedDocuments.v2 and every protection dependency. Validate the complete destination before changing production selection.

Quick reference

401 / 403 - Connection key, individual sign-in and capabilities; 412 / revision conflict - Reload saved data and re-enter the change; 426 / incompatible client - Use a matched client/server release; 400 / 413 - Rejected values, payload size and supported format; Timeout / connection failure - Address, TLS trust, service, firewall and network

Technical & support / Backup format, verification and capacity

A complete backup includes operational metadata and every referenced original. Spreadsheet/PDF reports and metadata-only JSON are not equivalent.

Managed complete archive

ManagedBackupV2 takes a frozen metadata snapshot and immutable document references, then streams a ZIP64 archive containing workspace.json, inventory.json, optional privacy.json and document entries. It validates original lengths and SHA-256 values while writing. The manifest is published after part verification; an incomplete write is not a successful backup.

Manifest and parts

StreamingBackupParts formatVersion 2 stores set identity, encryption state/salt, archive byte count/digest and ordered part inventory/authentication. Part names, indexes, lengths and checksums are validated on open. Default plaintext part size is 2,000,000,000 bytes; the smaller offered value is 400,000,000. Keep every generated part with its manifest and select the manifest in recovery.

Encryption and limits

Encrypted and readable managed sets use the same complete-file workflow. Prefer encryption for portable personal records. The streamed archive safeguard is 300,000,000,000 bytes and is separate from the 250 GB current attachment-payload ceiling. Current metadata has its own bounded serializer/backup allowance; large attachment capacity does not imply unlimited record metadata.

Legacy distinction

Earlier embedded workspaces/backup formats retain their older code paths and limits. Existing 400 MB-part sets remain supported. A 1,100 MB message can therefore refer to an earlier encrypted/embedded archive path, not the new managed capacity. Establish storage/backup format before diagnosing a cap; do not edit constants or filename extensions to convert it.

Operational backup procedure

Pause avoidable edits, confirm the active source, choose an independent private destination and create the complete encrypted set. Record completion time, set name, source edition/version, document count and the separate secret-storage reference. Verify local success, then confirm every part has reached any cloud/remote destination. Schedule a separate recovery exercise.

Physical planning example

At 200 GB of current originals, the live managed folder needs additional room for database/history, pending/retained originals and protection overhead. A backup and a separate recovery candidate can require roughly another full payload each, depending on compression and overhead. Do not size a disk at exactly the configured payload ceiling or assume JPEG/PDF data compresses substantially.

Validation evidence

The supplied package records an approximately 4.61 GB generated-payload round trip with every file digest/link checked. Metadata boundary tests covered 100,000 references and 250 GB logical payload. A full physical 250 GB workload was not benchmarked. Test time/memory figures from one machine are not customer performance guarantees.

Technical & support / Recovery and upgrade runbook

Protect the source first. Recovery prepares a separate candidate, validates it and leaves a deliberate review step before operational use.

1. Triage

Record edition/version, active location and failure symptom. Stop unnecessary writes. Preserve the complete source and backup set; do not repeatedly reinstall with a fresh workspace or delete databases/keys. Distinguish missing application, unavailable location, authentication failure and damaged data.

2. Gather the complete input

For a managed set gather manifest plus every part and the correct passphrase. Fully download cloud placeholders first. Confirm destination availability/free space and use a short direct local parent folder. Keep backup passphrase separate from the incident report.

3. Prepare the separate copy

Run FleetTime Recovery or the in-app Recover a separate copy command. Select the complete input and a new destination. Progress covers checking parts, recovering originals and validating records. The software rejects unsafe/duplicate entries, inventory mismatches, damaged content and incomplete candidates.

4. Understand account handling

A reviewed in-app upgrade/recovery can preserve existing accounts and current privacy decisions where available. Standalone backup recovery deliberately omits accounts/connection secrets and may require an authorised administrator to initialise access. Never assume an operational-data backup includes reusable passwords or server connection configuration.

5. Review before switching

Check representative drivers, assets, open VOR/work, recent transactions, original downloads and last known changes. Reconcile the current privacy/erasure register and external decisions, including ones made after the backup. Review access before permitting operational work. A recovered copy cannot discover a later decision held only on another lost machine.

6. Activate deliberately

For a verified local candidate use File > Open verified workspace copy. Managed schema 13 requires compatible clients; older clients cannot be used to write it. Keep the previous application and original workspace as the rollback route. Data written after a copy/switch is not automatically merged back.

If cancelled or failed

Keep the failure message and source intact. Do not remove RECOVERY-INCOMPLETE.txt to open the candidate. Correct the cause, choose a new candidate destination and repeat. If stopping a certificate batch import, distinguish its retained saved files from a complete-backup recovery transaction.

Technical & support / Manual cold copy and disaster planning

A cold copy is an administrator operation requiring the full storage/protection context, not a normal user file move.

Quiesce all writers

Close all clients using the workspace and stop the server service when applicable. Confirm that the application/service is no longer writing. Do not delete SQLite journal/WAL/SHM files to obtain a copy; recover/close consistently first.

Copy the complete unit

Copy the whole selected data root and all applicable protection/account/privacy dependencies. In managed format include ManagedDocuments.v2 and storage.key. For shared folders include the wrapped shared key and snapshot context. Preserve configuration and the secret-storage references through the organisation's private process.

Understand portability

A file-system copy of DPAPI-protected data remains bound to its Windows/machine context. It is not a guaranteed migration to a replacement computer. A verified encrypted complete backup provides the supported portable recovery path for operational data.

Prove recovery

Use an isolated destination. Open with the intended context, check database integrity through supported tools, sample original downloads, record counts, latest timestamps and permissions. Then create a new complete encrypted backup from the accepted copy. Do not overwrite the only original with an unreviewed candidate.

Define ownership

Set a backup owner, frequency, retention, offline/off-site copy, recovery exercise frequency and acceptable data-loss/recovery-time targets. FleetTime does not establish those business targets or prove cloud sync completed. Preserve evidence of each recovery exercise.

Technical & support / Install, repair, update and uninstall

Program registration and workspace data are separate. A missing uninstall entry is an installation issue to investigate, not evidence that records should be discarded.

Normal installation

Run the edition-specific installer for a normal registered copy. Choose Desktop and Start menu shortcuts independently. Keep Use the existing workspace / connection for a normal update. Setup stages/verifies application files, Windows registration and shortcut targets before reporting Installed.

Portable copies

Start FleetTime.cmd and Start FleetTime Network.cmd run package copies and do not create an uninstall entry. About FleetTime identifies package/portable use and the actual application folder. A taskbar pin may target such a copy even after a separate installed copy exists.

Registration

The standard per-user installation location is %LOCALAPPDATA%/Programs/FleetTime Local or FleetTime Network. Uninstall registration is under HKCU/Software/Microsoft/Windows/CurrentVersion/Uninstall/FleetTimeLocal or FleetTimeNetwork. Do not hand-create registry values as a routine fix; use the same-edition repair installer and inspect its result.

Diagnostics

Private stage logs are retained under %LOCALAPPDATA%/FleetTime/InstallerLogs. They contain stage/path/error information and can expose usernames or installation locations. Review before attaching to a ticket. Record whether setup reached Installed, actual running copy, Windows Installed apps entry and exact failure time.

Antivirus or endpoint protection software

If installation disappears or a write is denied, inspect quarantine/history and the operating system/application event information with authorised IT. Confirm the installer source and package identity. Do not assume antivirus caused every access error, and do not disable protection or create broad exclusions as a troubleshooting shortcut. A confirmed detection needs the exact file/hash/product/error for review.

Repair and rollback

Keep a complete backup, close the running copy and rerun the correct installer retaining the workspace. Failed installation uses rollback/read-back safeguards, but cannot prevent later quarantine, disk damage or system rollback. Recheck registration, the uninstaller and actual launch target after repair.

Uninstall

Save/verify a complete backup before uninstall. Program files and installed shortcuts/registration are removed; retained operational records, originals and connection settings remain separate. Retained data still needs protection and the organisation's retention procedure. Pinning remains a Windows user action. Signing and Microsoft Store acceptance are separate release work.

Technical & support / Exports, maps and integration boundaries

A report describes the selected records. It is not a complete system archive or an assurance that source information is correct.

Export pipeline

A section builds the selected data, detail and graphical output; native WebView2 print/PDF operations create fixed pages where used. Management reports support PDF, PPTX, ODP, XLSX, ODS and CSV according to the offered action. Record report dates, division, included sections and detail choices during support diagnosis.

Receiving programs

PPTX/ODP support presentation use and XLSX/ODS support spreadsheet use without requiring Microsoft Office for every recipient. Validate in the actual receiving program. Fonts, chart rendering, pagination and printer settings can differ. A file existing on disk does not prove the output includes the intended selection.

Map dependency

Usable saved locations, enabled map settings and available services determine coverage. Static PDF/presentation maps cannot retain interactive pan/zoom/hover behaviour. Review unplotted rows separately and retain a location/coverage note. Disabled online maps should not be described as lost incident records.

Provider import boundary

Inspection CSV/XLSX/ODS imports retain source fingerprints, mappings, rows, provider reports and review history. Creating missing assets is optional and explicitly reviewed. PDF/ZIP certificate matching is a separate evidence step. A source report ID identifies a report, not an asset.

Unavailable integrations

Provider API requested and browser preference do not create a working API or logged-in browser scraper. Novadata data imports, raw tachograph parsing and operational download/infringement calculations are not implemented in this release. Commercial licensing, time-limited trial enforcement and Microsoft signing are also separate work, not a hidden master-key feature.

Technical & support / Diagnostics: symptom to next action

Use this sequence before escalating. Keep the original state and avoid repeated imports or destructive resets.

Wrong or empty workspace

Record About FleetTime identity. Check the selected edition, location/connection and date/division filters. Confirm that the expected source exists. If the selected folder is unavailable, reconnect it or recover separately; do not choose a fresh workspace just to dismiss the error.

Records changed / save conflict

Capture the unsaved values safely. Choose File > Reload saved data, noting that unsaved form entries are discarded, then re-enter the intended change against the latest revision. If the connection failed during save, reload to establish whether it committed before retrying.

Cannot sign in / permission denied

Check correct workspace and account, active state and temporary-password requirement. Observe any temporary lockout delay. Use authorised administrator recovery where needed. Keep account recovery and data recovery separate.

Cannot open an original

Check owning record, document capability, all represented sections and complete storage/key presence. Record the error and affected filename/record ID. Use complete-backup recovery for damage; metadata-only restore cannot recreate missing blobs.

Backup/recovery refused

Check format, complete manifest/parts, local cloud availability, correct passphrase, free space and path length. Mixed parts or a checksum failure must be corrected by obtaining an intact set. Renaming/dropping files to defeat validation is not a repair.

Export incomplete or oddly formatted

Check selected dates/division/filters, report sections and Full supporting records. Reconcile source counts, inspect map coverage, then open the output in the receiving program. Supply a synthetic/redacted example rather than a live licence scan.

Installer missing or quarantined

Check actual running copy and Installed apps, then installer logs and antivirus or endpoint protection software history. Record evidence without disabling security. Use same-edition repair after the cause has been established.

Quick reference

Edition/version, time and exact action - Passwords / recovery keys; Expected versus actual result - Server bearer tokens / cookies; Redacted error and relevant stage log - Live driver scans or private client data; Safe reproduction and source counts - Unreviewed database or backup uploads

Technical & support / Support tickets and feature suggestions

Software support: support@design-works.org.uk. General project/sales enquiries: hello@design-works.org.uk.

Before opening a ticket

Use Help > About FleetTime to obtain edition/version and the running application folder. Note which parent/child page you were using, the exact action, expected result, actual message and whether other users are affected. Keep a safe example and check the symptom guide first.

Raise a support ticket

Open the Support area from the DesignWorks website and sign in to your client account when requested. Choose the new-ticket action, enter a clear subject and description, choose the available relevant category, and attach reviewed evidence. Read the privacy/terms acknowledgements yourself before submission. Keep the ticket reference shown after submission.

Follow the conversation

Use the portal ticket list and open the same ticket to read status/replies and provide requested details. Avoid creating multiple tickets for one incident. Portal updates are the supported tracking route; email notification is a prompt to check the ticket. Automatic reply-by-email ingestion has not been configured in the current support setup.

Attachments and privacy

Attach redacted screenshots or a synthetic example, and a reviewed installer log when relevant. Never send passwords, recovery/backup passphrases, API keys or browser session data. The web portal has its own displayed upload limit; it is separate from FleetTime's 12 MiB original-file limit. For larger/private datasets ask support to agree a suitable transfer route first.

Suggest a feature

FleetTime continues to receive improvements and new features. Users are welcome to suggest ideas through Support. State the task you are trying to complete, current difficulty/workaround, expected benefit and affected section/edition. A sketch or synthetic example helps. Suggestions are reviewed; submission is not a promise of implementation or release date.

Guide-based help

The current website help popup provides searchable guide answers and a route to support, rather than a conversational AI service. After this manual is approved, its versioned content is intended to become the reference for popup answers and support articles. Do not describe the revised content as embedded until that update has actually been made.

Support launch state

At this manual review, the redesigned public portal, legal links, account-isolation checks and notification delivery acceptance remain launch checks. This section describes the intended supported process. Before publishing the manual, verify the final public Support route and the visible ticket/category labels against the launched site.

About DesignWorks

Transport experience and practical IT delivery

Experience behind FleetTime

The developer brings 20 years of transport-industry experience and currently works as a Head in a national company across IT and Transport. More than 25 years of IT experience spans low-level design, high-level hardware and marketing projects. FleetTime draws on that operational and technical background to make recorded fleet and driver information easier to manage.

DesignWorks

DesignWorks has been delivering digital solutions for more than 20 years, bringing practical design, technology and business needs together. Product support and feature suggestions: https://www.design-works.org.uk/support/. Software support: support@design-works.org.uk. General enquiries: hello@design-works.org.uk.

Rules and official guidance

Use the current DVSA goods-vehicle drivers hours guidance and its working-time annex: https://www.gov.uk/guidance/drivers-hours-goods-vehicles and https://www.gov.uk/guidance/drivers-hours-goods-vehicles/annex-2-working-time-rules. Company check frequencies, risk ratings and reminders are configurable monitoring policy. FleetTime does not claim DVLA/DVSA approval or replace the official guidance, actual checks or competent professional judgement.