



# Installation & Operations Handbook

Case Files Professional  
GIB and Commercial editions  
Version 2.0.0-batch.18

This handbook covers both the GIB and Commercial clean installers. Application code is shared; agency identities, databases, accounts, licenses, uploads and integrations remain separate. Original Case Files and ATLAS archives were references, not production data imports.

The build has local automated and disposable-site verification. Production use still needs the deployment acceptance record on the actual host, real provider sandbox checks and desktop/mobile browser review. No production LicenseHub release is published by these clean installers.

# 1. Installation and first sign-in

Use a separate HTTPS test domain or subdomain and a new empty database. Do not overwrite the original production system. Upload the selected edition's complete files, keeping the folder structure intact.

The host needs 64-bit PHP 8.3 or newer, PDO MySQL, cURL, OpenSSL, Fileinfo, mbstring, ZIP, DOM/XML, XMLWriter, GD, iconv and ctype. Use MySQL 8 or MariaDB 10.6 or newer. Configuration and private storage must be writable by the hosting account, with restricted permissions.

Apache must enforce the supplied .htaccess rules. On Nginx or other servers, deny direct web access to app, config, database, storage, vendor, tests, docs and cron, plus SQL, configuration, log and encrypted files. Before acceptance, request known protected paths and confirm 403/404 responses without file contents.

1. Configure the Case Files Professional product, customer, license and one-time activation code in <https://licenses.casefilespro.com>.
2. Open <https://your-test-domain/install/index.php>. Enter the actual serving domain without a scheme or folder, product key and activation code. The installation folder is detected. Public verification keys are retrieved automatically; there is no public-key input.
3. Choose Manual Database or cPanel provisioning. Manual mode requires an empty database and a user with schema/CRUD privileges. Use full cPanel-prefixed names where applicable. cPanel mode uses your HTTPS host, account and API token; the token is not retained after provisioning.
4. Enter agency information, timezone and the first administrator. Use a password of at least 12 characters. There are no default login accounts.
5. Select the actual PHP CLI binary. The installer attempts a single scheduler registration, preserves unrelated jobs and verifies the resulting listing. If blocked, use its exact manual command.
6. Sign in. Confirm the edition, agency and version. Configure SMTP and verify a test message before relying on password reset.

If cPanel fails before schema/activation, follow the installer recovery message and switch to manual credentials without deleting recovery journals. A nonempty database is rejected. Do not delete unknown database contents or install/recovery files merely to retry.

## 2. Agency setup, accounts and scheduling

Set agency name, contact details, timezone and logo in Agency Setup. Print & Report Branding controls the header, signature, signer/title and license line. Commercial has no GIB identity assets. GIB defaults can be replaced with configured branding. Approved reports retain their saved branding context.

Create staff/client accounts in Users & Permissions. Set role and active status carefully. Employee/Vendor ID and lifecycle dates support verification; an inactive user requires a separation date. Changing account security invalidates existing account sessions.

| Role          | Normal access                                                                            |
|---------------|------------------------------------------------------------------------------------------|
| Administrator | Agency/system administration and management across cases.                                |
| Case Manager  | Assigned case management, assignments, report review/release, closure and reopening.     |
| Investigator  | Assigned writable case reports, evidence, tasks, notes and own timesheets.               |
| Accounting    | Assigned financial records and approved time; payroll management.                        |
| Client        | Assigned case overview, released reports/documents, permitted invoices and deliverables. |

Assignment controls case access. A role does not automatically expose every case. Accounting does not gain internal investigation evidence. Client assignment does not expose drafts or internal notes. Public delivery-link visitors have only that link's permitted content; they are not authenticated client identities.

Agency Setup can enable authenticator enrollment. Users enroll in My Account and save their single-use recovery codes. This option does not automatically mandate enrollment for every account. Administrators can reset a lost enrollment using account controls.

Scheduler / Cron shows actual registration separately from execution heartbeat. After manual installation, use Check / Install Cron through local crontab or configured cPanel access. One frequent dispatcher manages due jobs. Registration alone does not prove execution; verify recent timestamps and job outcomes. Keep the application and CLI paths correct after moving hosts.

### 3. Cases, assignment and reopened efforts

Managers create a case with its type, title, priority, deadline, instructions and required fields. Case-type definitions are saved with the case. Annual numbering starts at YEAR-1000 and is allocated atomically; existing numbers stay locked. Deadlines and schedules use the agency timezone.

Assign the active manager, investigators, client and accounting staff who need the case. Review assignments after staffing changes. Removing assignment removes access on subsequent requests, including inherited history access.

Use the case's folder tabs for Overview, Subjects, Activity, Reports, Evidence, Timesheets, AI and Billing. Additional links organize vehicles, documents, legal/claim/IME records, diagrams, client videos, tasks, assignments, notifications and closure.

Prior efforts are read-only when reached through a later assigned effort. A reopened case creates a suffix such as -01 or -02 and retains the closed original. Reusable people, vehicles, internal reference documents and appropriate legal/claim/contact references are copied independently. Operational reports, evidence, timesheets, tasks, notes, IME appointments and histories are not duplicated. Investigators must be assigned anew; active non-investigator assignments carry forward. Enter a new deadline explicitly and review copied references before using them.

Closed and cancelled efforts stay locked. Closure requires reviewed reports, evidence integrity/disposition, resolved tasks/time/expenses, financial gates and checklist attestations. Save incomplete checklist progress while reviewing. Cancellation requires an explanation and resolution/voiding of unfinished time entries; it cancels unfinished tasks and applicable queued case messages.

## 4. People, documents, legal records and evidence

Subjects & People records claimant/subject/witness/contact details and protected photos. Vehicles can be entered manually or decoded from NHTSA VIN data. A partial decode needs human review. Optional provider vehicle images are representative reference images, not verified photographs or ownership evidence.

Case Documents default to internal visibility. Management releases specific documents for clients. Keep private working material internal. All attachment downloads follow role and case authorization; private upload paths must never be publicly served.

Legal, claims, IME and counsel/contact records require source/document references. Investigators can draft on writable assigned cases; management review locks the source. Use amendments for corrections and preserve prior reviewed content. Outstanding IME appointments/reports can block closure. Appointment-to-task drafts require review; later record changes do not silently alter the saved task.

Evidence records identify the item, type, custodian, location and collection time. Digital evidence needs a preserved file. Record every custody transfer with responsible person, location, time and authority/reason. Management records retention or final disposition. The application checks the keyed custody chain and preserved file integrity; it does not replace physical handling procedures or source documentation.

For client reports, explicitly attach reviewed case-record snapshots and reviewed diagram revisions. Internal working notes are excluded. Later changes to a source do not silently rewrite a saved report snapshot.

## 5. Reports, print/PDF/Word and AI

1. Create a report on the correct writable effort. Choose the actual investigation date and enter factual scope, findings and chronology.
2. For surveillance, enter the daily summary and video duration. A summary can include up to four photographs; each chronological activity entry supports up to two. Management-only first-date sections remain with the primary report/revision chain.
3. Review photographs, captions, selected case-record and diagram snapshots, subject/client references and agency branding.
4. Save, submit, obtain management approval, then release the client version. Approval does not itself make a draft public. Clients receive released reports only.
5. Preview the full or supported surveillance summary. Combine selected dates only from the same case and report profile. Check the final print, PDF and native Word files before delivery.
6. Revise approved/released work through a new draft. Review and release the correction explicitly. Previously saved snapshots remain preserved.

Exports share saved report data and original-style hierarchy, metadata, chronology, paired photos, closing/signature and disclaimers. Public exports exclude internal SIU analysis. PDF uses bundled fonts; Word uses requested platform fonts. Pagination can differ between Word, PDF and browser print. Your actual letterhead, long text and real photos require target-host review.

Agency AI is disabled until explicitly enabled with the agency credential and chosen model. Improve Writing sends only the entered field text after consent; Check Report sends the entered report sections. Case/person documents are not attached automatically. Review the plain-text suggestion, Accept or Discard. Source changes invalidate stale suggestions. Resolve pending suggestions before saving. Requests/results are retained in encrypted case-scoped history. Account availability, model permissions and fees are provider-dependent.

## 6. Tasks, calendar and notifications

Create tasks with assigned investigator, title, location, start/end, instructions and priority. Review agency-local dates. Set email/SMS notification choices explicitly. Appointment tasks preserve their own schedule after creation.

The task calendar and downloadable ICS event contain authorized schedule details. Importing an ICS into a calendar can disclose that event to the calendar service; it does not invite anyone or automatically send a message.

Configure SMTP and optional Twilio through Agency Setup. SMS recipients need an enabled account and international-format number. The dispatcher checks current assignment, activity and task/invoice state before dispatch. Initial case assignment SMS is deduplicated per effort/investigator when enabled.

Accepted SMTP/Twilio submission is not proof of recipient delivery. Review provider and recipient logs. An uncertain delivery must be reconciled before retrying; do not duplicate notifications to force a result. Restore cancels historical pending/uncertain outbound work and pauses dispatch until reconciliation.

## 7. Timesheets, payroll and metrics

Enter separate actual field/travel hours to two decimals, work date, mileage, meals, tolls, parking, other expenses, activity and work notes. Attach a receipt where available. Expense-only records have zero hours. Optional start/end and unpaid breaks must match the declared hours. Active daily records cannot duplicate the same person/case/date, and combined daily hours across cases cannot exceed 24.

Save Draft or Save & Submit for Approval. Management approves or disapproves with a correction reason. Correct and resubmit. Managers may correct nonapproved records while retaining ownership/history. Approved records require an audited correction draft; invoice reservations must be reconciled before amendment. Superseded and voided records do not add to active totals.

Approved Work Summary provides authorized person/date-filtered print/PDF/Word and financial CSV. Investigators see their own entries; accounting sees approved assigned-case entries. Metrics use approved manual measurements and show observation, video/usable-footage, task timeliness and optional review-score denominators. These are recorded-work measures, not automatic quality judgments.

Payroll & Payments has Pay Rates, Approved Work Estimate and Payment Ledger folders. Administrators, Case Managers and Accounting manage agency-wide pay rates and payment ledger records; approved-work estimates remain case-scoped. Pay rates are separate from client billing rates. Set linked personnel type Employee or Vendor where appropriate. Estimates use approved work in the viewer's case scope. Employee net is gross plus reimbursement less manually entered withholding/deductions. Vendor 1099 records use gross paid only and exclude those extra amounts.

Record only payments actually made, with period, paid date, method and reference. This does not transfer money or file tax forms. Incorrect records are voided with a reason and remain in history; voided amounts are excluded from totals. Investigators can view their own payment records but cannot post, void or change rates.

## 8. Invoices, payments and budgets

Assign the billed client and set its bill-to profile before issuing. Create a draft invoice from the case. Add service lines or approved work; review rates, mileage, expenses, taxes, discounts, notes and due date. Importing approved work reserves the entry against duplicate billing. Field/travel hours use exact decimal totals rather than rounded whole minutes.

Issue the invoice after review. Issued client/agency identity is frozen. Send an invoice notice only when intended. Clients can view their issued invoices and enabled hosted payment methods. Application return URLs do not prove payment: signed events and provider verification drive ledger posting.

Stripe and Authorize.Net are configurable and disabled by default. Use provider sandbox credentials and the webhook URLs shown in Payments & Billing before live activation. Do not enter card numbers in Case Files Professional. Verify captured/duplicate events, partial payments, outages, refunds and settlement with real sandbox accounts.

Uncertain attempts/refunds must be reconciled using provider records. They can block more payments or credits. Do not reset database rows to bypass financial protection. Administrator refunds depend on provider eligibility. Record supported manual payments with a reference and review receipts/outstanding balances.

Case budgets distinguish approved and pending cost estimates. Closure requires outstanding financial work to be resolved and exceeded-budget overrides to be documented where applicable. After restore, reconcile external customer and payroll payments before resuming new postings.

## 9. Final videos and client access

Management uploads a final MP4 (up to 128 MB; host limits also apply), previews it and releases it with a reason. Export H.264 video with AAC audio for broad browser support. Local protected mirrors support playback/range requests; configured Case Cloud transfers are verified separately.

Create a link for the active assigned client, with expiry, optional separate password, download and notes choices. Attach only a released report from that case and an issued invoice for that client. Copy the unique URL and send it through your chosen channel; the system does not automatically send the copied URL. Send a delivery password separately.

Test in a separate browser: password, playback/seek, permitted downloads, related PDFs and notes. A visitor note is shared with the case team and does not establish authenticated client identity. Viewer grants last 30 minutes; reopen the original link afterward.

Revoke a link or withdraw the video to stop new access. Expiry, client assignment/account status and related record state are checked on each request. Already downloaded copies and in-flight transfers cannot be recalled. Actual codecs and desktop/mobile playback require browser acceptance.

## 10. Case Cloud, maps and public verification

Case Cloud uses agency-owned Dropbox credentials and a scoped authorization flow. Verify a real upload/download/hash/delete test before relying on off-server copies. Pending transfers retain private local mirrors. Reconnect the original account before managing its existing remote archives.

Google Maps uses separate browser Embed and server Geocoding keys, exact referrer/IP restrictions and agency policy URLs. Send only the requested location/directions input after consent. Provider results do not silently change source records. A server key stays encrypted; an Embed key is visible in its iframe URL by design. Optional vehicle reference images require a licensed provider account and human match review.

Personnel & Verification is administrator-controlled and opt-in. A profile does not create a login. Publish only reviewed public display name, role, portrait, ID, surname match and lifecycle dates. The public lookup uses ID plus exact normalized surname, CAPTCHA and rate limits. A published profile does not reveal case assignments or authenticate the person currently presenting it.

Keep provider credentials out of reports, screenshots and support messages. Configure optional integrations only after their domain/account tests pass. VideoPro remains reserved for a later phase.

## 11. Backups, restore and recovery

Database backups protect records only; full backups protect application/local files and records together. Normal policy is daily database/newest four and full every 14 days/newest two. Protected pre-restore/pre-update sets are separate and retained. Archives use authenticated encryption in the application's .cfpb format; ATLAS tar/gzip files are not compatible.

Use Protection & Schedule for prerequisites and cron status. Archives & Restore filters type, protection and ID/date/version/destination. File presence/size is distinct from Verify Integrity, which authenticates the archive and entry hashes without restoring records. Older-version archives can be verified/downloaded, but in-place restore requires the exact installed version and same installation/domain/edition/keys.

Capture can be cancelled at a safe checkpoint before a complete copy is retained. Retained-copy/cloud finalization and restore/update replacement cannot be cancelled. Original-session monitoring reconnects without restarting a worker. Expired unfinished 2 MB chunk uploads are cleaned; finalized imports are preserved. Import verification does not itself restore records. The total encrypted import limit is 8 GB and requires staging/decryption space.

Regular archive deletion requires DELETE, administrator password and a reason. It removes managed local/cloud copies using the original account; partial failures remain visible. Protected safety sets cannot be deleted here. Missing-copy detection records availability, not a proven deleter. Stopped empty attempts may be dismissed while their signed history remains. Audit supports paging/date filters and current/all-matching print/PDF/Word, bounded to 5,000 matching events.

Restore requires RESTORE and the administrator password. A verified protected full safety snapshot precedes replacement. Success invalidates sessions and pauses outbound/financial posting until password-confirmed reconciliation. Database audit returns to the chosen snapshot's point in time. Reconcile real payments, payroll, refunds and messages separately.

If interrupted, retain maintenance, journals and safety material. SSH recovery refuses a live worker and decides rollback/completion using commit markers. A broken updated bootstrap uses that operation's preserved recovery runtime. Store the private recovery bundle securely outside the server, separately from archives. Cold host recovery, cron recreation and grant/permission restoration need a rehearsed hosting procedure.

# 12. Updates, troubleshooting and acceptance

Update Center offers entitled LicenseHub releases, manual cumulative upload and history/recovery. Administrators approve updates with UPDATE and their password. Manual updates require the published release SHA-256 and current entitlement. Clean-install ZIPs are not cumulative updates and do not need a clean-install SHA.

Updates validate product/version/edition/runtime, files and additive migrations, create a full safety snapshot and verify the new application. Failed pre-commit work rolls back files/schema. Uncertain recovery remains locked; a committed update is not silently downgraded. Successful updates invalidate sessions and retain protected safety archives. Pending deployment reports retry without undoing a verified commit.

| Symptom                     | First checks                                                                                             |
|-----------------------------|----------------------------------------------------------------------------------------------------------|
| Installation database error | Empty DB, full prefixed names, host/port, user grants and installer recovery message.                    |
| License lock                | Actual domain/HTTPS, original entitlement, network/TLS and LicenseHub state; use Refresh License Status. |
| Case unavailable            | Active account, role and current assignment; related history is read-only.                               |
| Changed-record warning      | Reload, review the latest record and reapply intended edits; do not overwrite silently.                  |
| Missing email/SMS           | Agency settings, recipient preferences, dispatcher heartbeat and provider logs.                          |
| Export/image issue          | Saved report revision, actual branding/media integrity, fonts and host PHP limits.                       |
| Backup missing/failing      | Private disk capacity, original cloud account, archive verification and activity result.                 |
| Recovery lock               | Preserve journals/safety material and use the documented operation-specific recovery command.            |

Complete DEPLOYMENT-ACCEPTANCE.md on the actual staging host. It covers installation/licensing, copied-domain/revocation behavior, directory protection, five-role scope, cron execution, desktop/mobile review, real exports/video, sandbox integrations, backup/restore rehearsal and recovery. Record evidence, operator/date and unresolved items. Local checks alone do not establish production acceptance.

Detailed setup references remain in docs: INSTALLER-CRON-FIX, CASE-CLOUD-SETUP, OUTPUT-AI-SETUP, TIMESHEETS-PAYROLL-SETUP, PAYMENTS-SETUP, CLIENT-VIDEO-SETUP, PERSONNEL-CASE-RECORDS-SETUP, INTEGRATIONS-SETUP, BACKUP-RESTORE-SETUP and UPDATE-SETUP. Use Help & Guides in the application for role-appropriate quick guidance and the staff handbook download.