

EVIDENCER

Complete User and Administrator Manual

Configure, collect, review and prove KYC compliance - end to end.

Source-aligned edition | Version 2 | September 2026 | Offline manual

Contents

1. Product overview
2. Roles and access
3. Sign in and navigation
4. End-to-end KYC lifecycle
5. Technical flowcharts
6. Operational dashboard
7. Records and subjects
8. Create and deliver a KYC request
9. External applicant portal
10. Review and decisions
11. Reports and SLA
12. Field library
13. Document library
14. Classes, versions and requirements
15. Configuration approvals
16. API clients and webhooks
17. Audit and evidence
18. Platform settings
19. Security and production
20. Status model
21. Troubleshooting
22. Quick reference

1. Product overview

Evidencer is a self-hosted system for defining KYC requirements, collecting evidence securely, reviewing it with controlled decisions, and proving exactly why a subject is or is not compliant.

Configure once

Build reusable fields and document types, then assemble them into effective-dated KYC and product classes.

Collect once

Issue scoped, expiring links that expose only the outstanding information and documents for a subject.

Explain always

Each status resolves to a rule-set version, requirement result, evidence item, reviewer decision and audit event.

Core concept: a record represents one subject; an assessment represents that subject against one class and one rule-set version. One record can have several independent class statuses.

Coverage

Conditional requirements Class inheritance Duplicate prevention Evidence reuse OTP / DOB verification Chunked uploads AI extraction Maker-checker Waivers and holds SLA monitoring Status API Signed webhooks Immutable audit

2. Roles and access

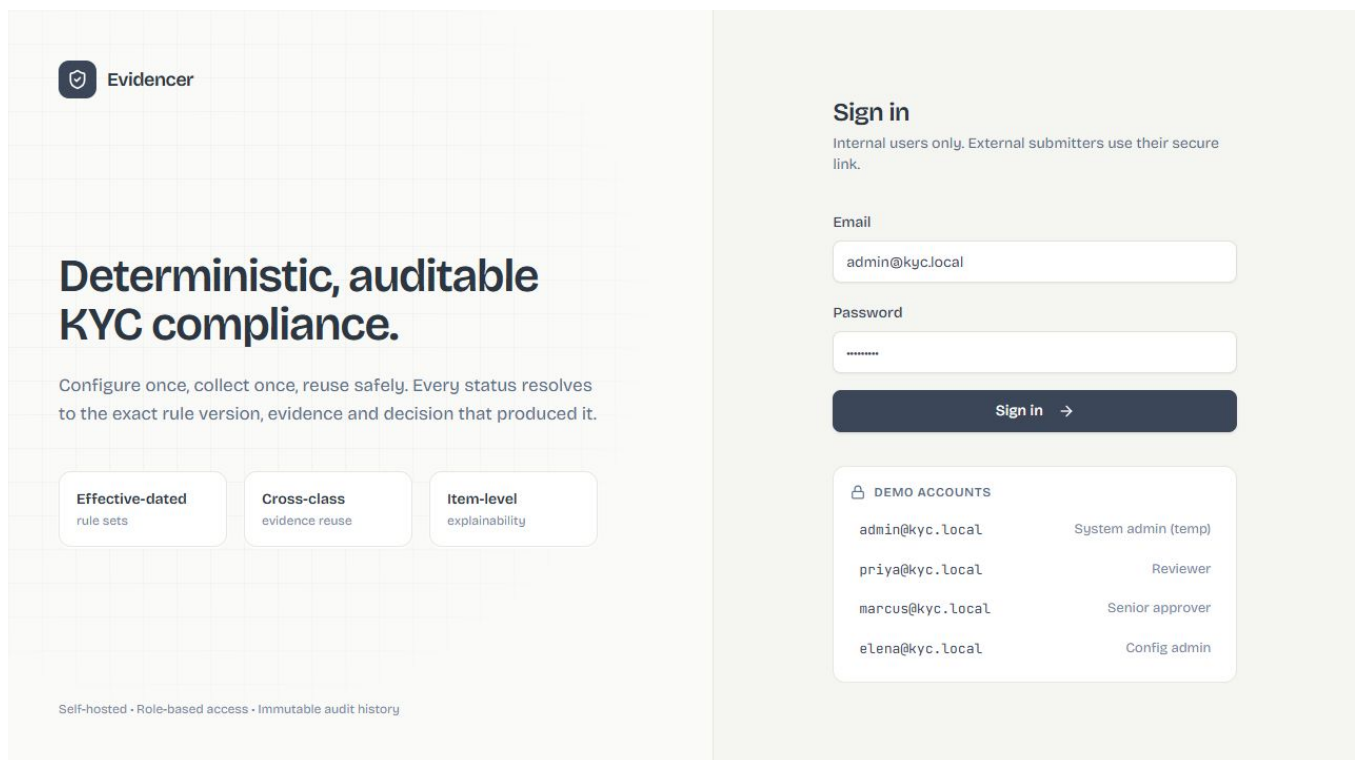
Menus control what a user sees; capabilities control what they can do; settings tabs control administration; class scope limits populations.

Role	Typical work	Key powers
System administrator	Platform ownership	All menus, settings and capabilities; cannot be reduced.
Requester / operations	Create subjects and links	Records, requests, reports; operations capability.
Reviewer	Assess submissions	Claim, approve, reject and return.
Senior approver	Escalations and dual-control	Override, waiver, hold, release/reassign.
KYC configuration admin	Rules and definitions	Fields, documents, classes, requirements, bundles.
Auditor / privacy officer	Assurance and retention	Read-only governance; privacy role also has override.

- 1 Open Settings -> Roles & access. Select or create a role.
- 2 Choose menus and settings tabs. Settings remains available so all users can reach Profile.
- 3 Assign capabilities. Operations, Review, Override, Configure, Administer and Release claims are independent.
- 4 Apply class scope. Product scope includes the parent KYC class for inherited requirements.
- 5 Optionally require approval. New fields, documents and classes enter the approval queue.
- 6 Use View as this role. The preview changes UI visibility and filtering; APIs still use your real identity.

Least privilege: configure both visibility and capabilities, then test with preview and a test account.

3. Sign in and navigation



Internal users sign in; external applicants use a secure-request link.

- 1 Enter email and password. Repeated failures trigger the configured logout.
- 2 Replace a temporary password. Use Profile & password; minimum length is eight characters.
- 3 Review new-browser alerts. They can include browser, OS, IP, time and optional approximate location.
- 4 Use left navigation and global search. Search by name, reference, email or registration number.
- 5 Use the user menu. Manage profile, theme and sign-out; use the bell for assignments, hand-offs and SLA alerts.

This wasn't me: the lockdown link signs out every session, forgets browsers and forces a password reset.

4. End-to-end KYC lifecycle

- 1 Publish a class version. Only an effective published version can assess new work.
- 2 Create a record. Primary keys are normalized; a match prevents duplication or adds the new class.
- 3 Initialize assessments. A product class also enrolls its parent and inherits requirements.
- 4 Issue a secure request. Select scope, items, expiry, mode, verification and delivery channels.
- 5 Applicant verifies and submits. Drafts can be saved; files are chunked, signature-checked, scanned, fingerprinted and optionally extracted.
- 6 Reviewer claims and decides. Dual workflows add a checker; rejected items can generate targeted rework.
- 7 Engine recalculates. Conditions, alternatives, reuse, waivers, holds and expiry are applied deterministically.
- 8 Monitor and renew. The scheduler sends renewal and SLA alerts; approved replacements supersede old evidence.

5. Technical flowcharts

These lane diagrams are configuration references. Each node names a product action or state boundary; arrows show the normal sequence and decision nodes show policy branches.

Flow A - Operator creates and delivers a KYC request

Operator	Open record -> Select classes and outstanding items -> Choose mode, verification, channels, expiry -> Create request
Evidencer	Validate scope and destination -> Generate random token and URL -> Render message template -> OTP selected? -> Generate short-lived code
Channel	Email / SMS / WhatsApp / Discord / webhook -> Deliver form link -> Deliver OTP in same selected channel set

No OTP branch: deliver the form link only. Failed delivery is logged and does not silently mark the request as received.

Flow B - Recipient verifies, updates and submits

Recipient	Open link -> Enter DOB or request/enter OTP -> Fill fields and upload documents -> Submit
Evidencer	Token active? -> Verification passes? -> Evaluate conditions and validation -> All mandatory items valid? -> Create pending-review items

Failure branches: expired/revoked/consumed token stops access; failed verification increments attempts; incomplete form remains draft or returns validation errors.

Flow C - Document upload and AI extraction

Upload service	Initialize upload -> Receive chunks -> Assemble and fingerprint -> Signature and scan clean? -> Persist local or S3/R2
Extraction	Document extraction enabled? -> Use document prompt or default -> Call active AI provider -> Map values, confidence and provenance -> Confidence above threshold?
Human control	Confirm/correct low-confidence values -> Reviewer compares document and extracted values

Extraction runs alongside the evidence record. It never silently overwrites an approved canonical value. Provider, model, confidence and evidence location are retained.

Flow D - Automatic API-derived fields

Form / record	Source field becomes complete -> All configured source values present? -> Schedule auto-fetch
Derived service	Build URL/query/JSON/form payload -> Call external API -> Success and response path found? -> Store mapped value, timestamp and provenance
Failure policy	Retry / leave missing / require manual entry -> Audit outcome and recalculate assessment

Fresh values are not fetched again until the freshness window expires unless a source value changes or an authorized user triggers Fetch now.

Flow E - Single-level review

Reviewer	Claim assessment -> Inspect each pending field/document -> Approve or reject? -> Complete decisions
Engine	Apply conditions, alternatives, reuse and waivers -> Any blocker? -> Compliant / rejected / pending / expired
Rework	Build rejected-item scope -> Issue targeted request

Flow F - Dual review / maker-checker

Maker	Claim -> Assess items and propose decisions -> Submit for checker
-------	---

Checker	Independently inspect package -> Confirm? -> Finalize -> or -> Return with reason
Controls	Enforce self-approval policy -> Audit both identities and timestamps -> Recalculate status

Flow G - Configuration approval

Maker	Create field/document/class -> Submit pending definition
Administrator	Review full definition and diff -> Approve? -> Activate -> or -> Reject with note
Governance	Record before/after and actor -> Maker corrects and resubmits

Flow H - Class version publication

Configuration	Create draft from published version -> Edit requirements, dates, conditions -> Review inheritance and alternatives -> Publish
Evidencer	Validate references and dates -> Impact analysis -> Retain old version history -> Use new version from effective date

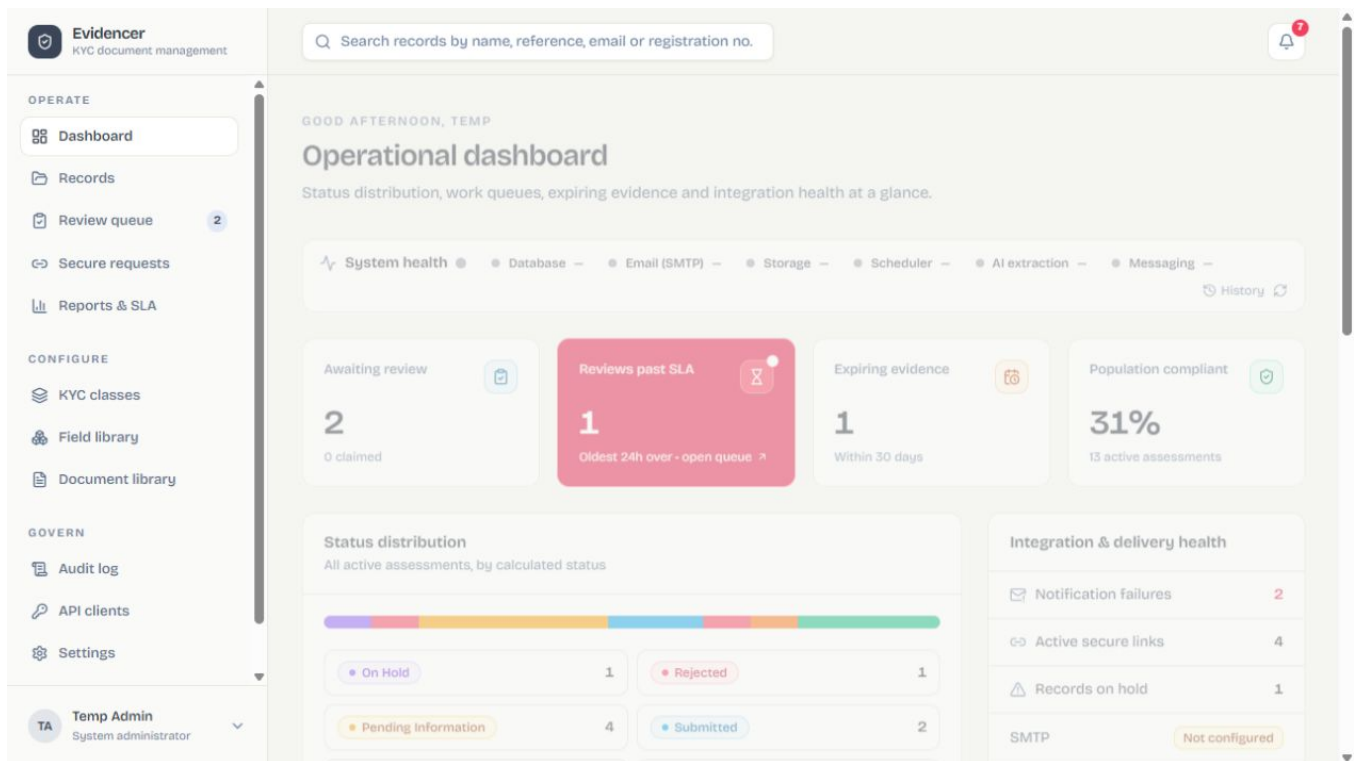
Flow I - Expiry, renewal and supersession

Scheduler	Scan evidence and SLA clocks -> Lead-day threshold reached? -> Issue scoped renewal request
Recipient / reviewer	Upload replacement -> Review replacement -> Approve
Engine	Mark older evidence superseded -> Recompute valid-until and status -> Dispatch webhooks/notifications

Flow J - Status API and outbound webhook

API client	GET KYC status with key and correlation ID -> Subject exists? -> Read status -> or -> Start KYC at source
Evidencer	Authenticate, scope and rate-limit -> Compute deterministic response -> Return allowed detail / request URL
Webhook	Create event and HMAC signature -> 2xx received? -> Record delivered -> or -> Retry and log failure

6. Operational dashboard



Queue pressure, compliance distribution, service health and approaching expiry.

Top metrics

Awaiting review, past SLA, expiring evidence and population compliant. Select a card to drill down.

Status and class

Select a status; compliance by class shows compliant assessments divided by active assessments.

Integration health

Failures, active links, holds, SMTP, AI, database, scheduler, storage and messaging.

Daily work

Open unassigned review, expiring evidence and recent audit activity directly.

7. Records and subjects

Evidencer

KYC document management

OPERATE

Dashboard

Records

Review queue

Secure requests

Reports & SLA

CONFIGURE

KYC classes

Field library

Document library

GOVERN

Audit log

API clients

Settings

Temp Admin

System administrator

Q

Search records by name, reference, email or registration no.

7

Records

Subjects identified by configurable primary keys. A record may participate in multiple classes, each with its own assessment.

+ New record

Filters

Search name, reference, primary ke

All statuses

All classes

9 record(s)

CLASS PILLS = STATUS PER CLASS:

Compliant

Expiring Soon

Submitted

Pending information

Rejected

Expired / Non-compliant

On Hold

RECORD	CLASSES	STATUS	RISK	BLOCKING ITEMS	VALID UNTIL	CREATED
Amelia Hartley KYC-000001	IND v2 IND_MOTOR v1	Expiring Soon Submitted	Low	1	30 Sept 2026	40d ago
Northwind Trading Ltd KYC-000002	CORP v1 CORP_FLEET v1	Compliant Pending Information	Medium	1	22 Jan 2027	30d ago
Daniel Okoye KYC-000003	IND v2	Submitted	Medium	9	—	12d ago
Sofia Lindqvist KYC-000004	IND v2 UBO v1	Compliant Pending Information	Low	1	08 Nov 2026	25d ago
Rahul Mehta KYC-000005	IND v2	Pending Information	High	4	06 Feb 2028	8d ago

Helix

Class pills show each class independently; the row emphasizes the most blocking result.

- 1 Select New record and an active class. It must have a published version.
- 2 Complete every primary key. These values identify the subject; display name is optional.
- 3 Create. A same-class match is blocked; a cross-class match extends the existing subject.

Evidencer User Manual

Page 10

Evidencer

KYC document management

OPERATE

Dashboard

Records

Review queue 2

Secure requests

Reports & SLA

CONFIGURE

KYC classes

Field library

Document library

GOVERN

Audit log

API clients

Settings

TA

Temp Admin

System administrator

Search records by name, reference, email or registration no.

Records

KYC-000001

Amelia Hartley

Risk Low

Created 40d ago by Tom Okafor

Decision package

Place on hold

Individual

Expiring Soon

Individual motor insurance

Submitted

Requirement checklist — Individual

Evaluated against rule set v2 (effective 2025-01-01). 0 blocking item(s).

Request missing items

Aa

Full legal name

FULL_NAME

Mandatory

Satisfied

Approved value (source: submitter)

Aa

Date of birth

DATE_OF_BIRTH

Mandatory

Satisfied

Approved value (source: submitter)

Aa

Nationality

NATIONALITY

Mandatory

Satisfied

Approved value (source: submitter)

Aa

Residential address

RES_ADDRESS

Mandatory

Satisfied

Approved value (source: submitter)

Assessment

Status

Expiring Soon

Rule-set version

v2

Assessment ID

as_001

Valid until

30 Sept 2026

SLA due

19 Aug 2026, 18:21

Claimed by

Unassigned

Next action

Renew document

Secure requests

Values, evidence, requirements, relationships, requests and decisions in one view.

Action	Result
Issue request	Creates a scoped token and delivery notification.
Place on hold	Stops affected assessments until authorized release.
Unmask sensitive value	Shows clear value and writes a sensitive-view audit event.
Fetch derived value	Runs the configured request and stores provenance.
Decision package	Exports record, rules, evidence and decisions.

Reuse: reusable approved evidence can satisfy multiple classes; class-only and non-reusable evidence cannot.

8. Create and deliver a KYC request

A KYC request is a scoped, expiring form for one existing record. Evidencer sends the form link to the recipient and, when one-time-code verification is selected, sends the secret through the same selected delivery channel or channels so the recipient can authenticate and update information.

RECORD	CLASS	SCOPE	RECIPIENT	MODE	STATUS	EXPIRES	OPENED
Marcus Delaney KYC-000009	IND_MOTOR	6 item(s)	m.delaney@example.ie	reusable none	Active	07 Oct 2026	—
Rahul Mehta KYC-000005	IND	4 item(s)	rahul.mehta@example.in	reusable otp	Active	06 Oct 2026	1d ago
Chloé Marchand KYC-000007	IND	2 item(s) rework	chloe.marchand@example.fr	single dob	Active	05 Oct 2026	—
Daniel Okoye KYC-000003	IND	9 item(s)	d.okoye@example.com	single otp	Submitted	02 Oct 2026	1d ago
Sofia				reusable		29 Sept	

The request register shows lifecycle state without routinely exposing the bearer token.

Before creating the request

Check	Why it matters
Record and class enrollment	The form is generated from the record's active assessments and effective rule versions.
Recipient address	Email, phone or Discord ID must be present in the mapped record field or entered where the request dialog permits.
Public base URL	Links in delivered messages must resolve to the externally reachable HTTPS Evidencer address.
Delivery channel	SMTP/Twilio/Discord/generic webhook must be enabled, saved and tested.
Outstanding scope	Only necessary fields and documents should be exposed; accepted items should not be collected again.

Operator procedure

- 1 Open Records and select the subject. Confirm identity, classes, assessment versions and current blocking items.
- 2 Select Issue request. Choose one or more enrolled classes. Evidencer proposes the outstanding fields and documents from applicable mandatory, conditional and rework requirements.

- 3 Review the item list. Include only what the recipient must update. A rejected-item rework request should contain the rejected field/document plus any explicitly linked correction.
- 4 Choose request mode. Single-use is consumed after a successful submission. Reusable allows draft/staged updates until expiry or revocation.
- 5 Choose verification. None relies on possession of the secret URL; Date of birth compares the entered DOB with the record; One-time code adds a short-lived secret.
- 6 Select delivery channels. Email, SMS, WhatsApp, Discord DM and/or the generic signed messaging webhook can be selected if configured. For OTP requests, the form link and the verification secret travel through the same selected channel set.
- 7 Set expiry and recipient. The default lifetime comes from Settings -> Reminders & links. Confirm the destination carefully.
- 8 Create and send. Evidencer stores the request, constructs the tokenized URL, renders the channel template and dispatches the message. The notification and audit logs record the attempt and outcome.
- 9 Monitor. Track delivery, opened, verified, draft-saved, submitted, expired or revoked states. Revoke immediately if the destination was wrong or the URL may be exposed.

What the recipient receives

Form message

Branded message containing purpose, subject/reference context, expiry, support wording and the unique secure form link. The form contains only authorized requested items.

Verification secret

For OTP, a short-lived one-time code is delivered by the same selected channel(s). Stored notification history masks the code. Date-of-birth verification sends no code.

Channel-security design: delivering link and OTP through the same channel improves usability and confirms control of that channel, but it is not independent two-factor authentication. For higher assurance, use a separately controlled channel or DOB step-up according to policy.

Form characteristics

- Token-scoped: the recipient cannot browse other records or classes.
- Dynamic: conditional requirements update as source answers change.
- Validated: field patterns, ranges and allowed values come from the field library.
- Resumable when reusable mode is selected; draft saves do not create reviewer decisions.
- Document-aware: type, maximum size, minimum/maximum count and expiry metadata are enforced.
- Secure uploads: chunks are assembled, content-signature checked, scanned and SHA-256 fingerprinted.
- Accessible status: progress separates completed, outstanding and invalid items.
- Auditable: open, verification, draft, upload, submit, expiry and revocation events are recorded.

Delivery failure and recovery

If no selected channel can deliver, the request remains visible but the recipient may not have received it. Inspect Settings connection tests and the notification log, correct the destination/configuration, then issue a fresh request or

securely convey the existing link according to policy. Demo fallback code 123456 must never be treated as a production delivery mechanism.

Secret handling: both the URL token and OTP are secrets. Do not paste them into shared tickets or logs. Revocation invalidates the URL immediately; OTPs expire and are attempt-limited.

9. External applicant portal

- 1 Open the unexpired link and verify. Revoked, expired or consumed single-use links cannot continue.
- 2 Complete fields. Help and validation come from the library; conditional items update live.
- 3 Upload documents. Follow type, size and count rules; chunk progress is visible.
- 4 Resolve extraction prompts. Low-confidence results need human confirmation and never overwrite approved values silently.
- 5 Save draft if allowed; then submit. The final action validates all current mandatory items and produces a receipt.

Upload protection

Content signatures, malware scanning, SHA-256 fingerprints and private storage apply. Removing an upload before submission removes it from the pending request.

Processing that occurs while the form is completed

AI extraction alongside the upload

When the selected document type has extraction enabled, Evidencer sends the clean uploaded file to the active AI provider after assembly and scanning. The document-specific prompt takes precedence over the global prompt. Returned values are mapped to configured metadata fields and stored with provider/model, confidence and evidence location. The upload remains the primary evidence; low-confidence or conflicting results require confirmation and reviewer comparison.

Automatic API-derived values

When a recipient completes all configured source fields for an API-derived field, Evidencer schedules the external lookup automatically. It builds the configured query, JSON or form payload, calls the service, maps the response path and stores the derived value with timestamp and provenance. Conditional requirements are recalculated when the value arrives.

Timing: the applicant may see a derived value populate after its source values are complete. A slow or failed provider must not erase their source input. The configured failure policy decides whether to retry, leave the field missing, or permit manual entry.

10. Review and decisions

Evidencer

KYC document management

Q Search records by name, reference, email or registration no.

OPERATE

Dashboard

Records

Review queue

2

Secure requests

Reports & SLA

CONFIGURE

KYC classes

Field library

Document library

GOVERN

Audit log

API clients

Settings

TA Temp Admin
System administrator

Review queue

Submitted evidence awaiting decision. Claim an assessment to move it to In Review; SLA timers are shown per item.

Team workload

0 claimed

2 unassigned

Distribute unassigned (2)

Hand a claim to a named reviewer or release it to the pool. Bars show each reviewer's decisions per day over the last two weeks. Tip: set an idle limit under Settings → Reminders to auto-release stuck claims.

Nobody holds a claim right now.

All classes

Any SLA state

Any assignment

3 in queue

RECORD	CLASS	STATUS	ITEMS TO DECIDE	RISK	SLA DUE	ASSIGNED
Chloé Marchand KYC-000007	IND v2	Rejected	0	Low	Overdue 1d ago	Claim
Amelia Hartley KYC-000001	IND_MOTOR v1	Submitted	1	Low	24h from now	Claim
Daniel Okoye KYC-000003	IND v2	Submitted	9	Medium	24h from now	Claim

Filter by class, SLA and assignment; leads can distribute unassigned work.

- 1 Open and claim. Prioritize overdue/high-risk cases and prevent competing work.
- 2 Inspect every pending item. Check preview, metadata, expiry, scan, fingerprint and extraction provenance.
- 3 Approve or reject. For rejection, choose a reason and write clear applicant remediation; keep internal notes separate.
- 4 Complete dual control when configured. Self-approval is governed by policy.

Evidencer

KYC document management

OPERATE

Dashboard

Records

Review queue2

Secure requests

Reports & SLA

CONFIGURE

KYC classes

Field library

Document library

GOVERN

Audit log

API clients

Settings

TA

Temp Admin

System administrator

Search records by name, reference, email or registration no.

7

← Review queue

KYC-000003 • INDIVIDUAL • RULE SET V2

Daniel Okoye

SubmittedSLA due 25 Sept 2026, 18:21

Claim assessment

Claim this assessment to start reviewing — claiming prevents two reviewers working the same subject at once.

Assign to a reviewer

Items awaiting decision (9)

Approve, reject or return each item individually. Bulk decisions require explicit selection.

Full legal nameFULL_NAMEMandatory

Instructions: As per passport.

SUBMITTED VALUE

Daniel Chukwuemeka Okoye

source: submitter • 20d ago

PRIOR VALUES

None — first submission

Date of birthDATE_OF_BIRTHMandatory

SUBMITTED VALUE

1979-11-02

source: submitter • 20d ago

PRIOR VALUES

None — first submission

Assessment context

Assessmentas_003

ClassIndividual (IND)

Rule setv2 • eff. 2025-01-01

WorkflowSingle approval

Risk bandMedium

Blocking9

Decided items0

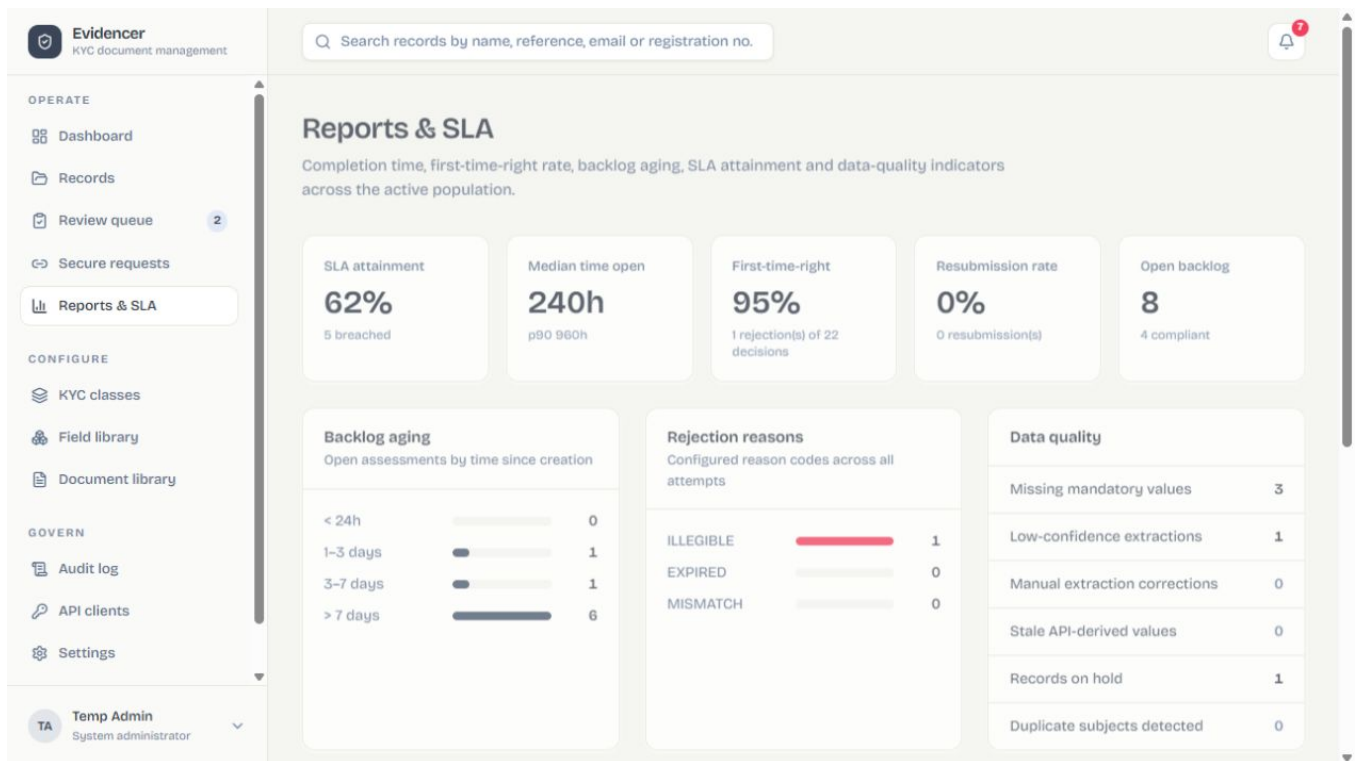
Self-approvalProhibited

Open record

Context, requirements and decisions stay together.

Control	Purpose	Capability
Waiver	Authorized exception for a missing requirement	Override
Hold	Stops progression for investigation	Override
Reassign/release	Transfers or frees a claim	Release claims
Reject/return	Invalidates item and may issue rework	Review

11. Reports and SLA



Class compliance, review timing, expiry and delivery.

Compliance

Status and class counts identify blocked populations.

SLA

Submitted, claimed, completed, approaching and breached work plus lead workload history.

Expiry

Valid-until uses document expiry or validity policy; lead days drive renewal.

Delivery

Delivered, opened, bounced and failed notifications across channels.

12. Field library

Evidencer
KYC document management

OPERATE

- Dashboard
- Records
- Review queue **2**
- Secure requests
- Reports & SLA

CONFIGURE

- KYC classes
- Field library**
- Document library

GOVERN

- Audit log
- API clients
- Settings

Temp Admin
System administrator

Search records by name, reference, email or registration no.

Field library

Reusable field definitions with data type, validation, sensitivity and introduction dates.
A field may be assigned to many classes.

Export Import + New field

Search code, name... All data types Show retired 32 definition(s)

CODE	NAME	TYPE	SENSITIVITY	USED IN	INTRODUCED	S
FULL_NAME	Full legal name Name as shown on government-issued ID.	short_text	standard	IND UBO	2024-01-01	
DATE_OF_BIRTH	Date of birth Date of birth of the natural person.	date	sensitive	IND UBO	2024-01-01	
NATIONALITY	Nationality Primary nationality.	country	standard	IND UBO	2024-01-01	
EMAIL	Email address Primary contact email.	email	standard	CORP VEND	2024-01-01	
PHONE	Telephone Mobile or landline in E164 format.	telephone	standard	IND	2024-01-01	
RES_ADDRESS	Residential address Current residential address.	address	sensitive	IND	2024-01-01	

Reusable field definitions feed every future class version that references them.

- 1 Set stable code and name. Codes are integration identifiers.
- 2 Choose type. Text, number, date, boolean, country, address, select, identifier, calculated or API-derived.
- 3 Add description/help, sensitivity and owner. Unmasking sensitive/secret values is audited.
- 4 Define validation. Length, regex/message, min/max/precision, values and uniqueness depend on type.
- 5 Set introduction/retirement dates. Retire definitions used by history instead of deleting.

API-derived fields

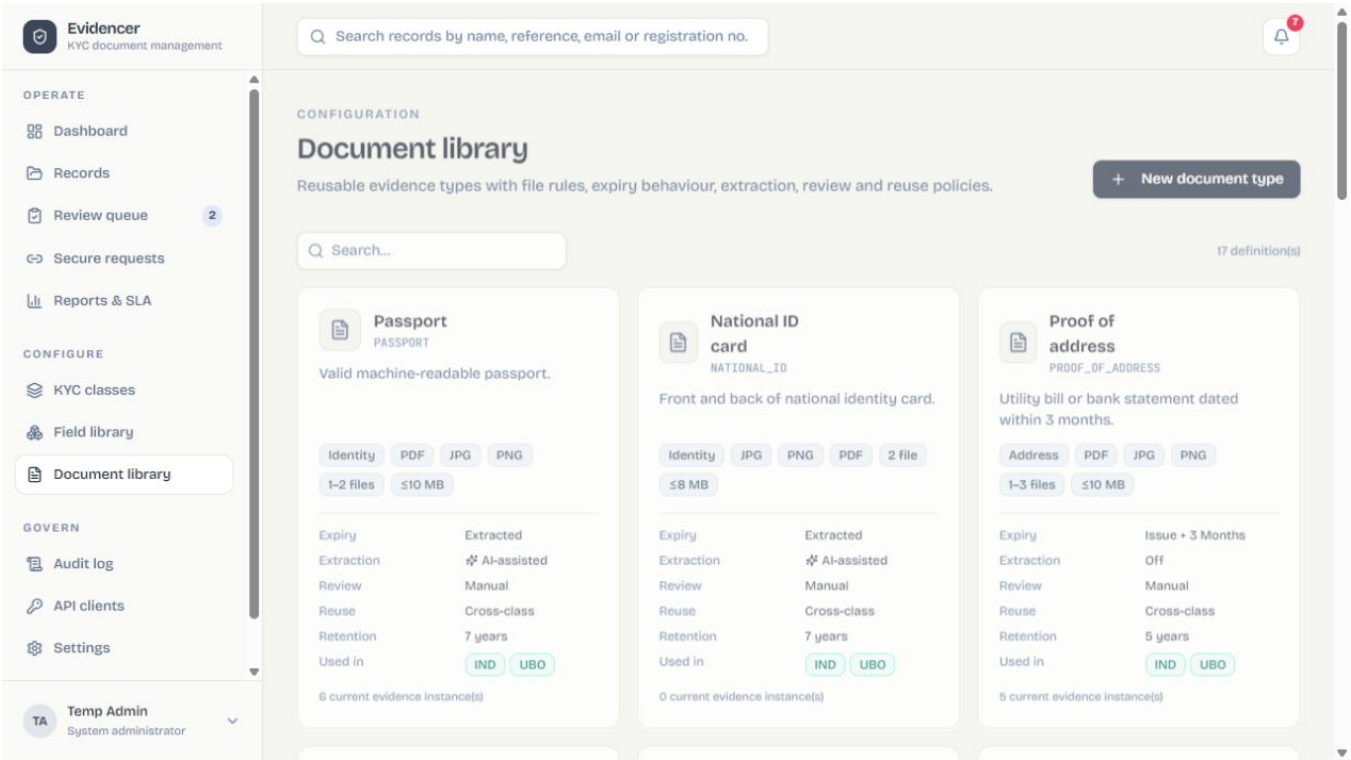
Configure service, method/URL, query/JSON/form mapping, headers/auth, response path, freshness, auto-fetch, provenance and failure behavior. Test with sample values. Secrets are never echoed.

Configure automatic derivation

- 1 Select the source fields. These are the values that must be present before automatic execution, such as country plus registration number.
- 2 Configure request construction. Choose method, URL, headers/authentication and query, JSON or form mappings. Never place secrets in visible field values.
- 3 Configure response mapping. Point the response path to the value to store and define any normalization.
- 4 Set freshness and auto-fetch. Fresh values are reused; a source-field change invalidates provenance and schedules a new fetch.
- 5 Choose failure behavior. Retry, allow manual fallback, or keep the requirement blocked.
- 6 Test with samples. Verify request rendering and response mapping before attaching the field to a published class.

Trigger rule: automatic fetch begins only when every required source value is non-empty. Results store source inputs, service, operation, response path, retrieval time and outcome so reviewers and auditors can explain the value.

13. Document library

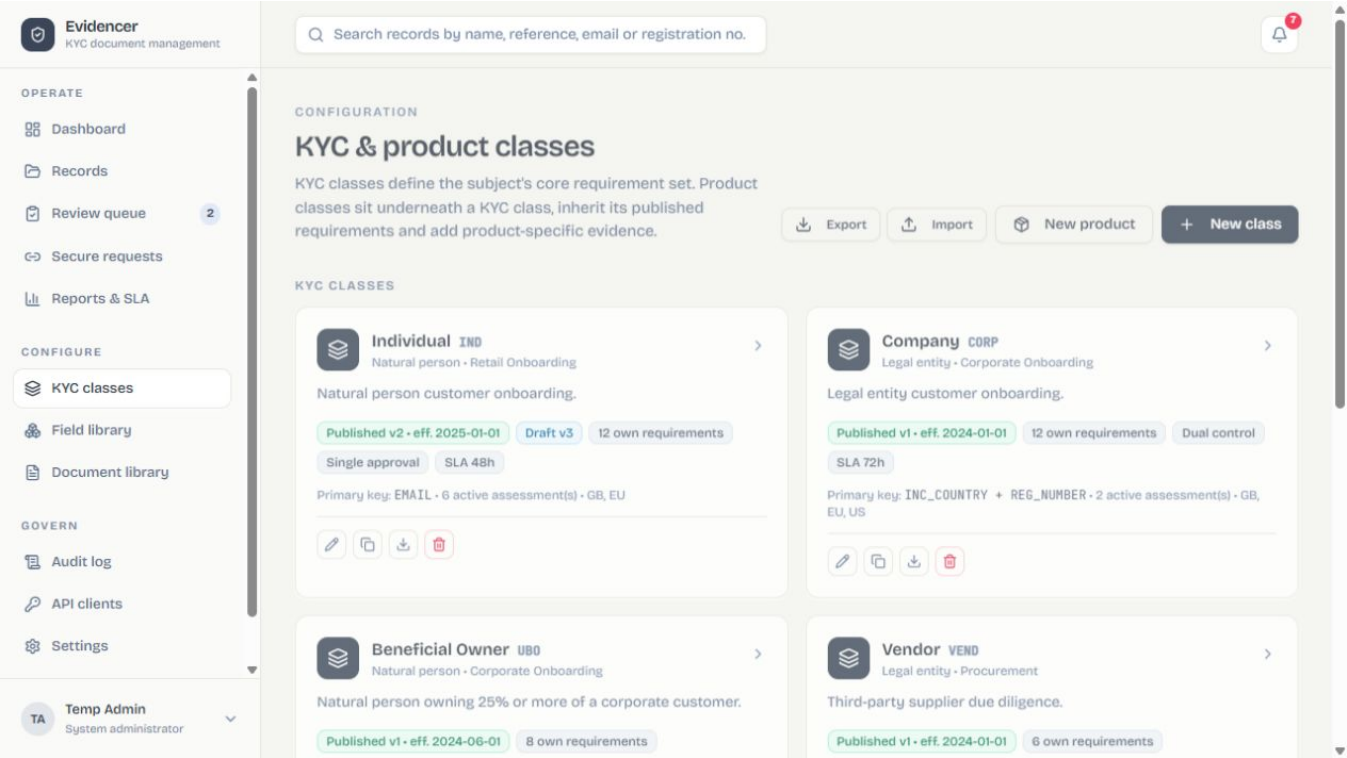


Central collection, review, reuse, expiry and retention policy.

Setting	Meaning
Types / size / count	Upload validation and multi-page/front-back rules.
Expiry	None, extracted, or calculated with validity months.
Extraction / prompt	Uses the active AI provider; a document prompt overrides the default.
Metadata fields	Maps extracted name, DOB, registration, expiry and other values.
Review / reuse	Manual or auto; reusable, class-only or non-reusable.
Retention / sensitivity	Governance, masking and downstream handling.

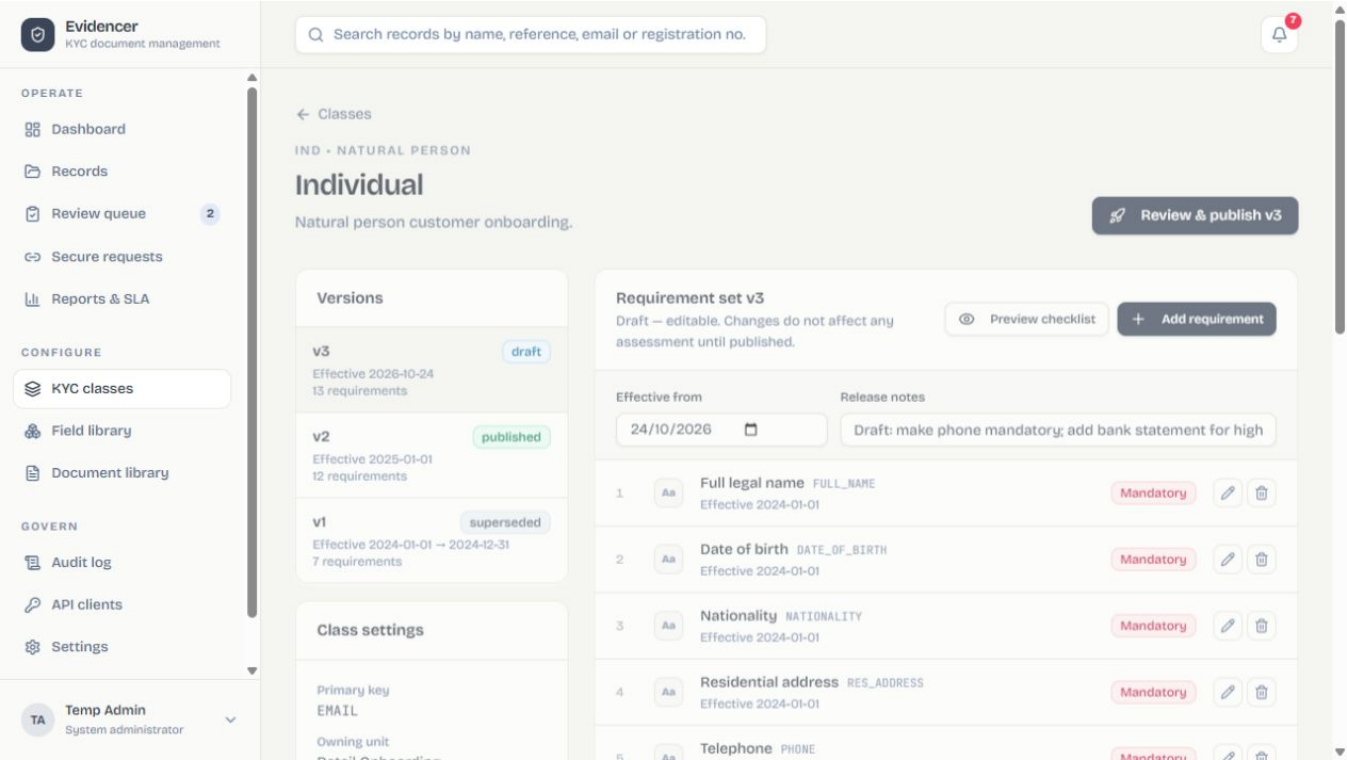
Clone similar definitions. Delete is blocked when referenced; retire instead. Changing linked metadata after approval supersedes evidence and requests a fresh upload.

14. Classes, versions and requirements



Product classes inherit a parent KYC class and add product evidence.

Define code, name, kind, subject type, primary keys, owner, jurisdiction, workflow, SLA and status. Product classes also select product and parent.



Published history is retained while the next version is edited as a draft.

- 1 Create a draft and set effective dates/notes.
- 2 Add requirements. Choose field/document, necessity, order, instructions, dates, approver and reuse.
- 3 Add conditions. For example `RISK_BAND == "High"` ; test true and false paths.
- 4 Use alternative groups. They express one-of rules such as Passport or National ID.
- 5 Review inheritance and impact. Confirm affected records and new blockers, then publish.

Never rewrite published history. Draft and publish a new effective-dated version.

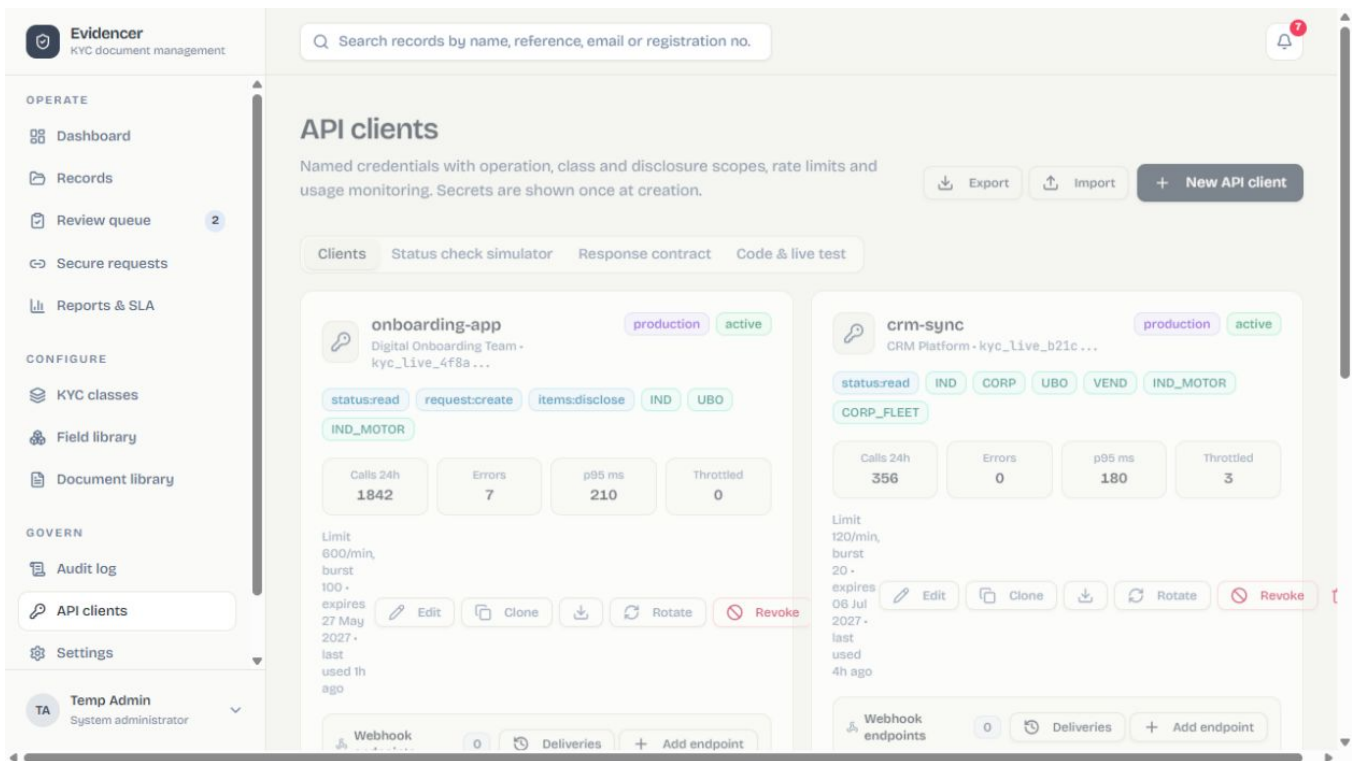
Bundles

Export selected configuration plus dependencies. Import detects conflicts and remaps identifiers; review merge/overwrite decisions.

15. Configuration approvals

- 1 Maker submits a new field, document or class. It remains unusable while pending.
- 2 Admin opens Settings -> Configuration approvals. Inspect the full definition, author and timestamps.
- 3 Compare resubmission diff. Verify corrections after rejection.
- 4 Approve or reject with a note. Approval activates; rejection provides actionable feedback.

16. API clients and webhooks



Environment, scopes, class scope, rate limits, keys and webhooks are managed per client.

- 1 Set name, owner and environment.
- 2 Grant scopes. status:read , request:create , and items:disclose are separate.
- 3 Restrict classes and rates. Set per-minute and burst limits.
- 4 Save the secret once. Store it in a secret manager; it is shown only at creation/rotation.
- 5 Use code generator and simulator. Inspect exact HTTP status/body before integrating.

```
GET /api/v1/kyc/status?classCode=IND&recipientEmail=person@example.com Authorization: Bearer kyc_live_... X-Correlation-Id: your-trace-id
```

With request:create , "start KYC at source" can create an unknown subject and return a secure URL. Item detail requires items:disclose .

Webhooks

Add multiple endpoints with independent secret, events and delivery history. Consumers verify the raw-body HMAC, reject stale/replayed messages, respond 2xx quickly and process idempotently. Test, monitor retries, rotate with overlap, then remove old endpoints.

Coordinate rotation/revocation. Old secrets cannot be recovered and callers are affected immediately.

17. Audit and evidence

Evidencer

KYC document management

Q

Search records by name, reference, email or registration no.

7

OPERATE

Dashboard

Records

Review queue2

Secure requests

Reports & SLA

CONFIGURE

KYC classes

Field library

Document library

GOVERN

Audit log

API clients

Settings

TA

Temp Admin

System administrator

Audit log

Immutable, tamper-evident history of every access, change, decision, notification and export. Searching the audit log is itself audited.

Export

Q Actor, object, correlation id...

All categories

12 event(s)

TIMESTAMP	ACTOR	ACTION	OBJECT	DETAIL	CORRELATI
24 Sept 2026, 17:21	API: onboarding-app	status.check	CORP / rec_002	Returned COMPLIANT (rule v1)	corr-8f1a2f
23 Sept 2026, 18:21	d.okoye@example.com	request.submitted	rq_003	9 items submitted; status -> SUBMITTED	corr-5a5a5a
23 Sept 2026, 15:21	d.okoye@example.com	link.opened	rq_003	OTP verified on attempt 1	corr-5a5a5a
21 Sept 2026, 18:21	Priya Natarajan	evidence.rejected	ev_018 (Proof of address)	Reason ILLEGIBLE; rework link rq_002 issued; email sent	corr-9b9b9b

Template:

Actor, action, object, time and correlation ID reconstruct each sequence.

Events cover authentication, links, submissions, decisions, configuration, derived calls, sensitive views, reminders, holds, imports and API checks. Filter then export. Correlation IDs connect browser/API activity to notifications and webhook delivery.

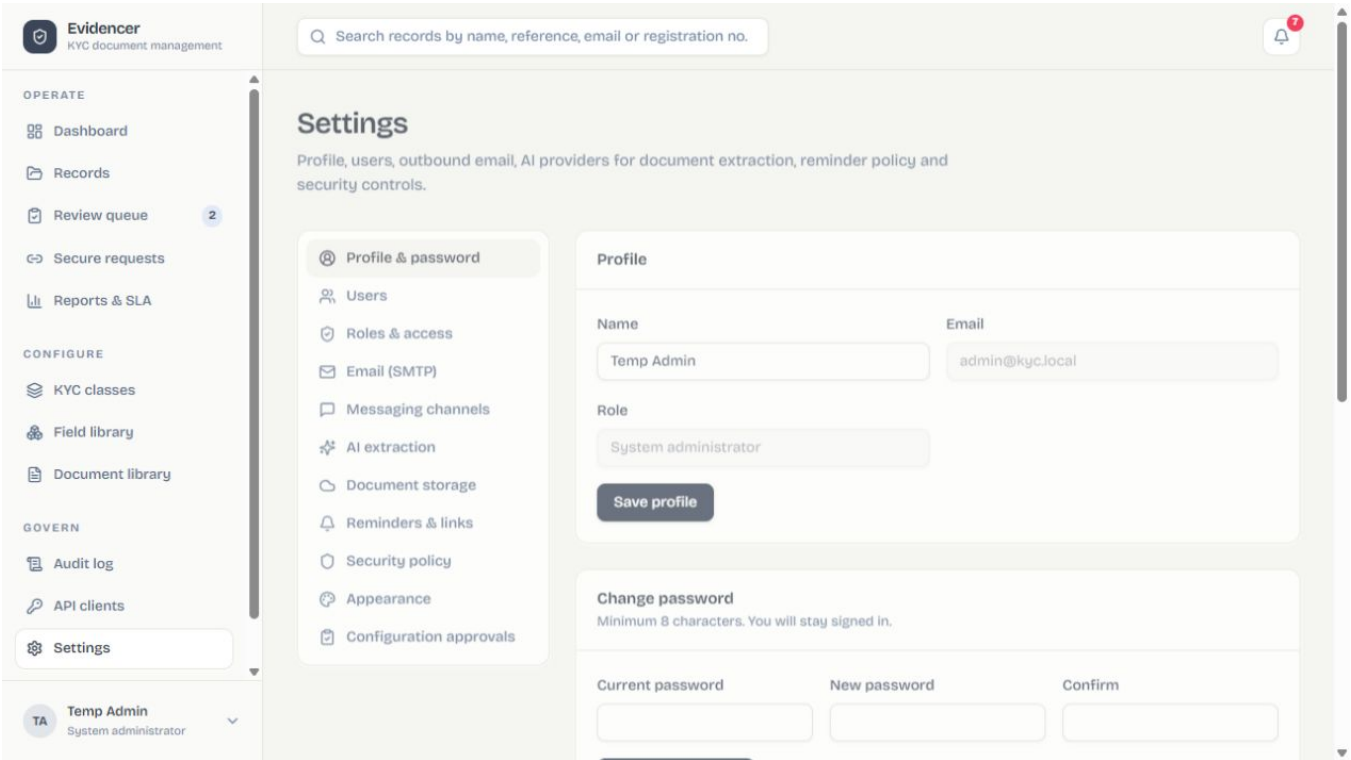
Decision package

Point-in-time proof of classes, versions, requirement results, evidence, waivers and decisions.

Notification log

Channel, recipient, template/subject and outcome; OTP values are masked and secrets excluded.

18. Platform settings



Profile is universal; admin tabs follow role access.

Tab	Purpose
Profile & password	Name, password, known browsers, alerts, quiet hours, personal theme.
Users / roles	Accounts, temporary passwords, access, class scope, preview, history and bundles.
Email (SMTP)	Host, port, credentials, encryption and sender; save then test.
Messaging	Twilio SMS/WhatsApp, Discord and HMAC webhook; map destination fields.
AI extraction	Mistral, Anthropic, OpenAI, OpenRouter or Ollama; model, URL, confidence and test.
Storage	Local, S3, R2 or compatible endpoint; bucket, region, prefix and test.
Reminders & links	Lead days, expiry window, link life, public URL, interval and SLA warning.
Security / appearance	Sessions, lockout, self-approval, locations, branding, production and palettes.

- 1 Enter values and save. Existing secrets appear only as stored placeholders.
- 2 Run the saved-connection test. Unsaved edits are not used.
- 3 Inspect health and audit. Verify success before enabling dependent workflows.

Storage changes affect new uploads only; existing files stay in place and remain accessible through the API.

19. Security and production

Sessions

Timeout limits inactivity; lockout limits guesses; users can forget browsers.

Data protection

Scanning, fingerprints, masking, write-only secrets and private object streaming.

Branding

Production workspaces can co-brand internal and applicant pages.

Backups

Back up MongoDB and uploads/bucket; test restore and secret recovery.

- 1 Pre-flight. Change demo passwords; configure TLS/public URL, delivery, storage, backup and real admins.
- 2 Open Security -> Move to production. Review impact and type the confirmation phrase.
- 3 Confirm. Demo records are removed and demo users deactivated; configuration remains.
- 4 Smoke test. Create, deliver, upload, review, query status and verify audit/webhook.

Production transition removes demo data. Back up and verify real admin access first.

20. Status model

Status	Meaning	Next action
Compliant	All applicable mandatory requirements are valid and accepted.	Monitor validity.
Expiring soon	Valid evidence is within the warning window.	Renew.
Pending information	Applicable items are missing.	Issue request.
Submitted / In review	Items await decision / are claimed.	Review within SLA.
Rejected	An applicable item was rejected.	Targeted rework or authorized waiver.
Expired	Required evidence passed validity.	Request replacement.
On hold	An authorized hold overrides progression.	Resolve and release.
Not assessed / Cancelled	No active assessment / closed without completion.	Initialize again if required.

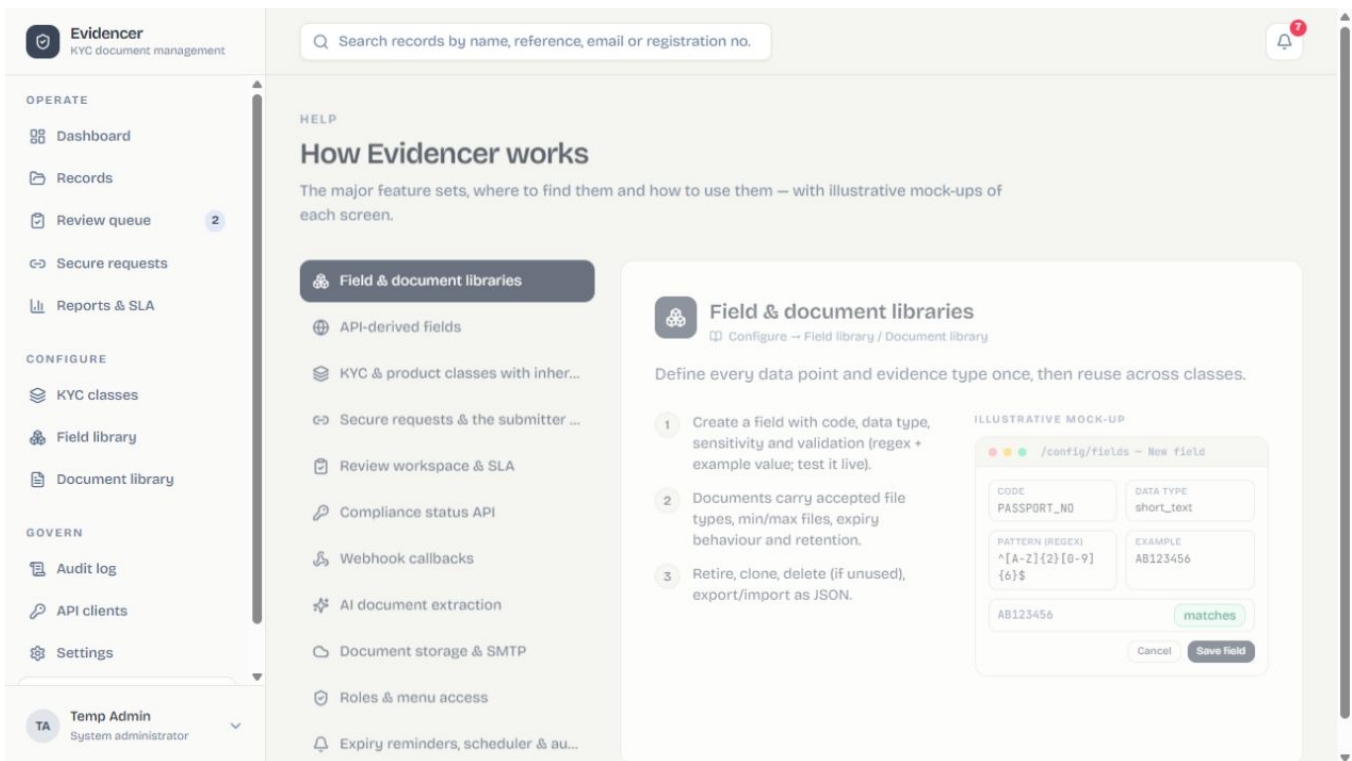
Most blocking wins: hold, rejection, missing/submitted, expiry, expiring-soon, then compliant. Optional items do not block; false conditions do not apply; one valid alternative satisfies its group; a valid waiver satisfies its target.

21. Troubleshooting

Symptom	Resolution path
Cannot sign in	Check spelling, status, lockout and temporary password; admin can reset/unlock.
Link fails	Check expired/revoked/consumed state and public base URL; create a new request.
OTP absent	Check enabled channels, mapped destination and provider status; run channel test.
Upload rejected	Check real file signature, size/count, corruption and scan. Renaming an extension does not help.
AI fails	Check active provider, saved key/URL/model and file; use connection/extraction tests.
Still blocked	Inspect assessment explanations for condition, alternative, rejection, expiry, hold and version.
Webhook fails	Check reachability, HMAC, timeout and 2xx; use test/delivery log and idempotency.
Storage fails	Check bucket, region/endpoint, policy, clock and prefix; save before retesting.
Scheduler idle	Check enabled/interval/lead boundary; run manually and inspect notification/audit.

Diagnose from evidence: system health -> audit correlation ID -> notification/webhook/test log. Change settings only after locating the boundary.

22. Quick reference



In-app guidance is concise; this manual is the detailed companion.

Operations daily

- Review health and failures.
- Match subjects with correct primary keys.
- Request only outstanding items.
- Revoke wrong/superseded links.

Reviewer daily

- Prioritize overdue/high risk.
- Claim before inspecting.
- Check file, expiry and provenance.
- Write precise remediation.

Configuration release

- Draft, never rewrite history.
- Test conditions/alternatives.
- Review inheritance/impact.
- Publish with date and notes.

Administrator weekly

- Review access and lockouts.
- Monitor delivery, webhooks, AI, storage.
- Confirm scheduler/backups.
- Rotate expiring credentials safely.

Record	Unique subject.	Assessment	Record evaluated against one class/version.
Evidence	Versioned document and decisions.	Requirement	Field/document rule.
Class	KYC population or product extension.	Waiver	Authorized exception.
Alternative group	One valid member satisfies the group.	Correlation ID	Trace key across events.

End of manual - Evidencer user and administrator guide.