Q-KYC SXM

Operator Manual

Version 0.6.14 · Edition 2026-06-03

Deployed at: **the Tenant Firm** · Sint Maarten

Developed and maintained by: **4Mfesw** *Modern, Methods Made and Maintained · Fiber, Software, WorkFlows, Energy* Sint Maarten

---

Document classification

`CONFIDENTIAL — RESTRICTED`

This manual contains operational details of an AML/CFT compliance system. Distribute only to:

- Staff with assigned compliance roles at the deploying firm
- CBCS / FIU MOT supervisors during scheduled inspections
- The firm's appointed external auditor under engagement agreement

Not for public distribution.

Copyright

© 2026 4Mfesw. All rights reserved. No part of this document may be reproduced, distributed, or transmitted in any form or by any means without the prior written permission of 4Mfesw, except for brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

Document control

Field	Value
Title	Q-KYC SXM Operator Manual
Owner	4Mfesw
Approver	_____
Issued	2026-06-03
Next review	2026-12-03 (or sooner on material change)
Version	v0.6.14
Source of truth	`docs/USER_MANUAL.md` (English)
Translations	NL, FR, ES — review against EN before regulatory use

Revision history

Version	Date	Author	Notes
0.6.6	2026-05-30	4Mfesw	First SXM-published edition (Risk Assessment + entity profile API + repo-as-truth deploy).
0.6.11	2026-05-31	4Mfesw	Added §10 (AV scan / encryption / MRZ / mobile / regulator integration).
0.6.13	2026-05-31	4Mfesw	Three-tier pricing + TCO chart added to exec summary; manual unchanged.
0.6.14	2026-06-03	4Mfesw	SPA save-action fixes (JWT in apiFetch, modal close on success).

How to read this manual

This is a **task book**. It teaches you how to do the four jobs Q-KYC exists to do, in the order you'll do them on real client files:

	Walkthrough	Subject of the walkthrough
§1	**KYC onboarding** — open a new client file end to end	ENT-001 Maria Velasquez (SXM resident, low-risk)
§2	**AML escalation + SAR** — what happens when a screening hit lands	ENT-003 Roman Voloshyn → CASE-2026-001
§3	**UBO declaration + register extract** — beneficial-ownership for opaque structures	ENT-004 Coral Holdings Ltd. (BVI Trust)
§4	**Evidence Bundle** — what you hand the inspector when they email at 16:00	ENT-005 Domino Marine Services BV (NL)

Each walkthrough has numbered steps. Each step has one screenshot. The red ring on the screenshot is what you click next. Read the prose, click what the ring shows, move on.

The walkthroughs use the **bundled demo data**. Before your first real client, your tenant admin must:

1. **Confirm your screening connectors** under **Settings → Connectors**. The 9 baked-in government sources (OFAC SDN + Consolidated, UN, EU, UK HMT OFSI, Canada Justice, Switzerland SECO) are active by default — no wiring required. Optional commercial overlays (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage) need their own subscription + API key; drop those in via Settings → Connectors only if your tier or use case requires them.
2. Create operator accounts under **Settings → Users** (or run `scripts/create_superadmin.py` once on the server).
3. Set a strong `COCAI_JWT_SECRET` before any pilot deployment.

After that the same screens, the same buttons, the same audit chain — with real list versions and real registry rows underneath.

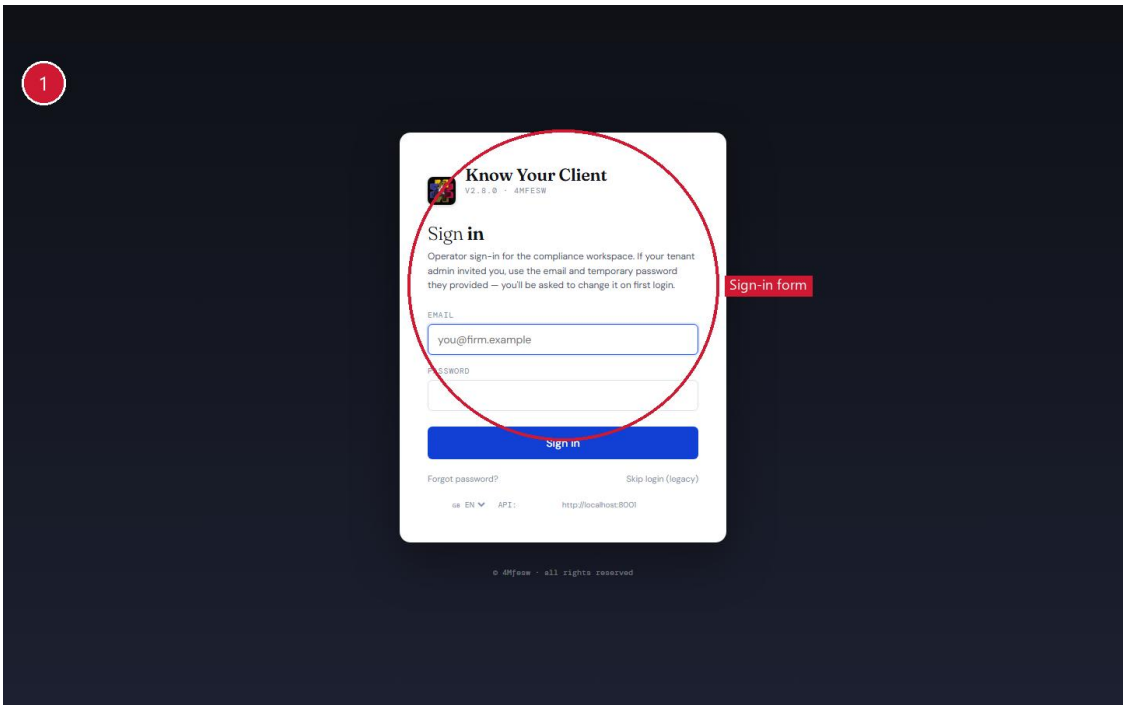
> **What Q-KYC does NOT do.** It does not file SARs to the FIU for you. It pulls 9 official government sanctions sources directly from the publisher URLs daily — OFAC SDN + Consolidated, UN, EU, UK HMT OFSI, Canada Justice, Switzerland SECO. Commercial PEP / adverse-media overlays (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage) are optional and customer-supplied via **Settings → Connectors**. It does not certify documents. It does not give you a get-out-of-jail card under any of FATF / Wwft / DNFBP / CBCS — your MLRO is still the regulator's accountable person. What Q-KYC does is record the work *honestly* in an immutable, hash-chained audit trail, so when the inspector arrives you can hand them a single bundle and prove every move.

---

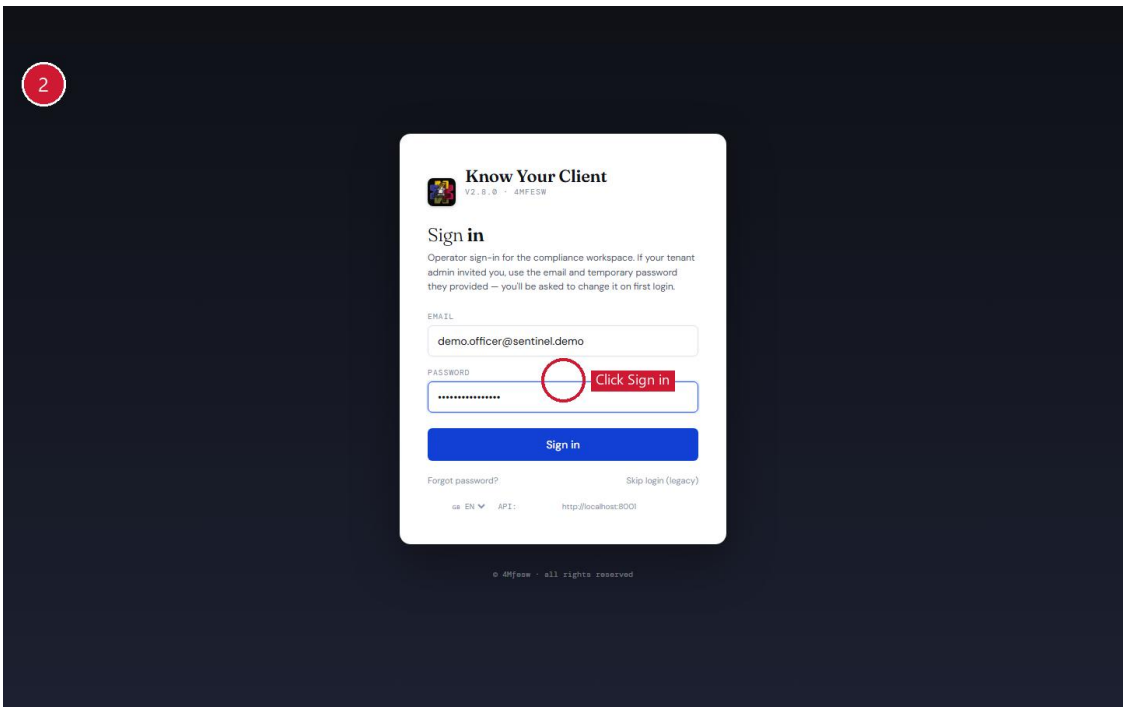
§0 First sign-in (5 minutes)

Your tenant admin will have created an account for you and sent you a temporary password by email. You'll be asked to change it on first login.

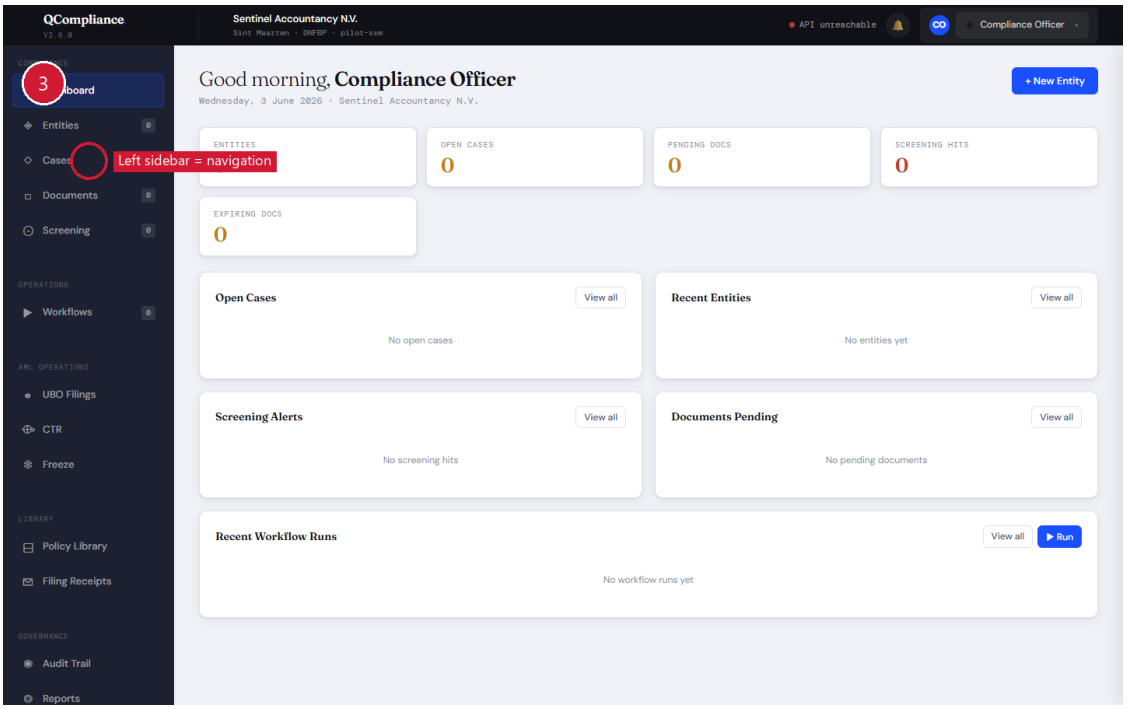
1. Browse to the URL your admin gave you (during the pilot: `http://localhost:8001`).
2. You see this:



1. Type your email and the temporary password. The Sign-in button activates once both fields are filled.



2. After sign-in you arrive on the **Dashboard**:



The five tiles at the top are your firm's compliance state at a glance: **Entities**, **Open Cases**, **Pending Docs**, **Screening Hits**, **Expiring Docs**. The Provider Status panel below shows which screening connectors are active — by default the 9 baked-in government sources (OFAC SDN + Consolidated, UN, EU, UK HMT OFSI, Canada Justice, Switzerland SECO) plus any customer-supplied commercial overlay you have configured (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage). The yellow banner *"Mock providers active"* is a safety net that only appears if all real providers have been disabled.

3. The left **sidebar is your only navigation**:
    - **Compliance** — Dashboard, Entities, Cases, Documents, Screening
    - **Operations** — Workflows
    - **Governance** — Audit Trail, Reviews Due, Reports
    - **System** — Settings, User Manual

That's it. Now pick a walkthrough.

---

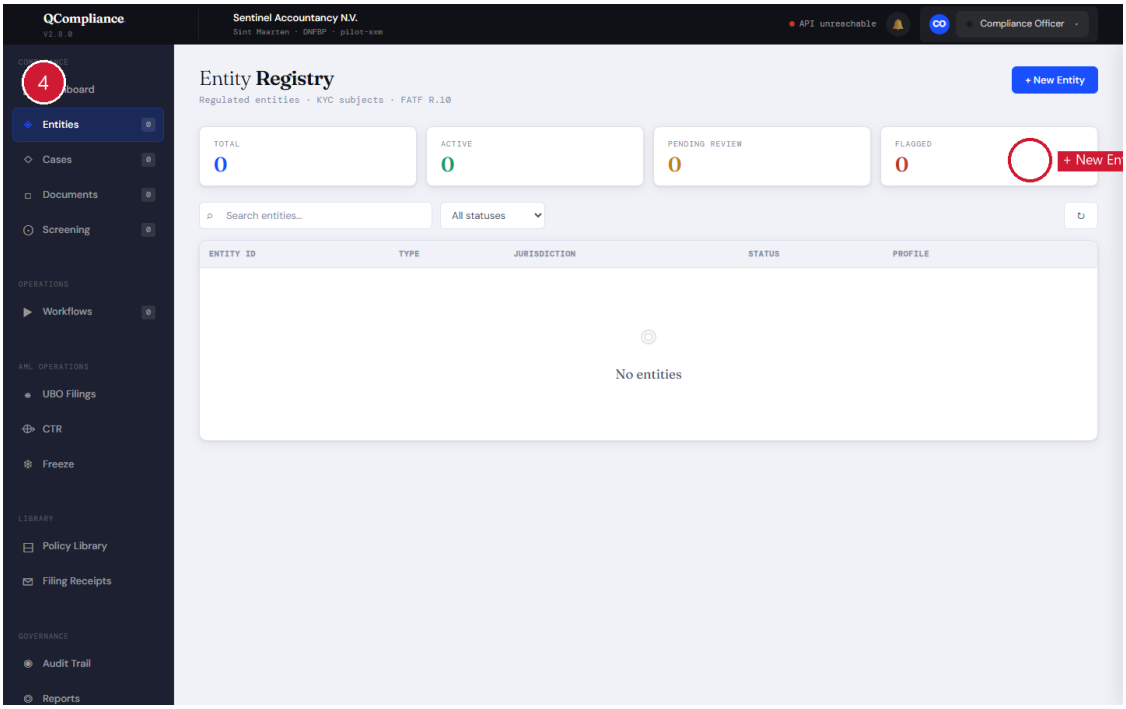
§1 KYC onboarding (Walkthrough 1)

Goal: open a new client file end to end, with at least one ID document on record, an explicit risk rating, and a periodic-review date set — everything an inspector will ask for as proof you did CDD before the relationship started (FATF R.10 / Wwft art. 3 / CBCS AML/CFT §4.1).

Subject: ENT-001 Maria Velasquez — SXM resident, salaried, no PEP exposure, low-risk classification.

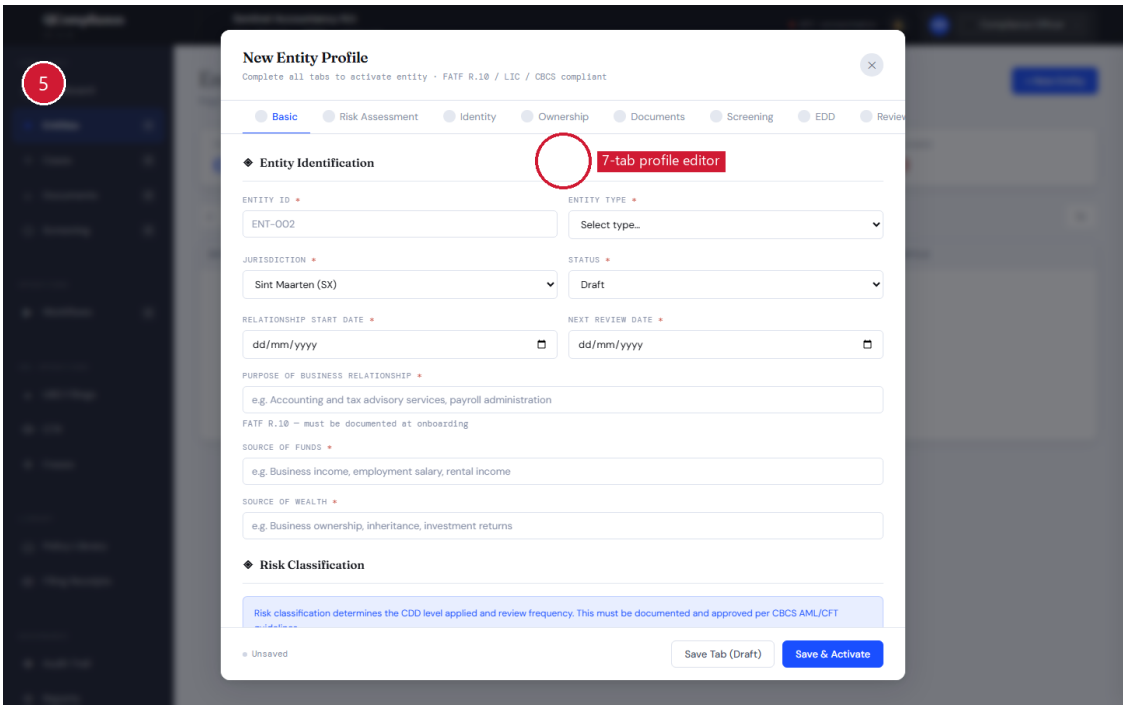
Step 1 — Open the Entity Registry

Click **Entities** in the sidebar. You see every regulated party your firm has on record, with their type, jurisdiction, current status and CDD completeness. New file? Click **+ New Entity** in the top-right.



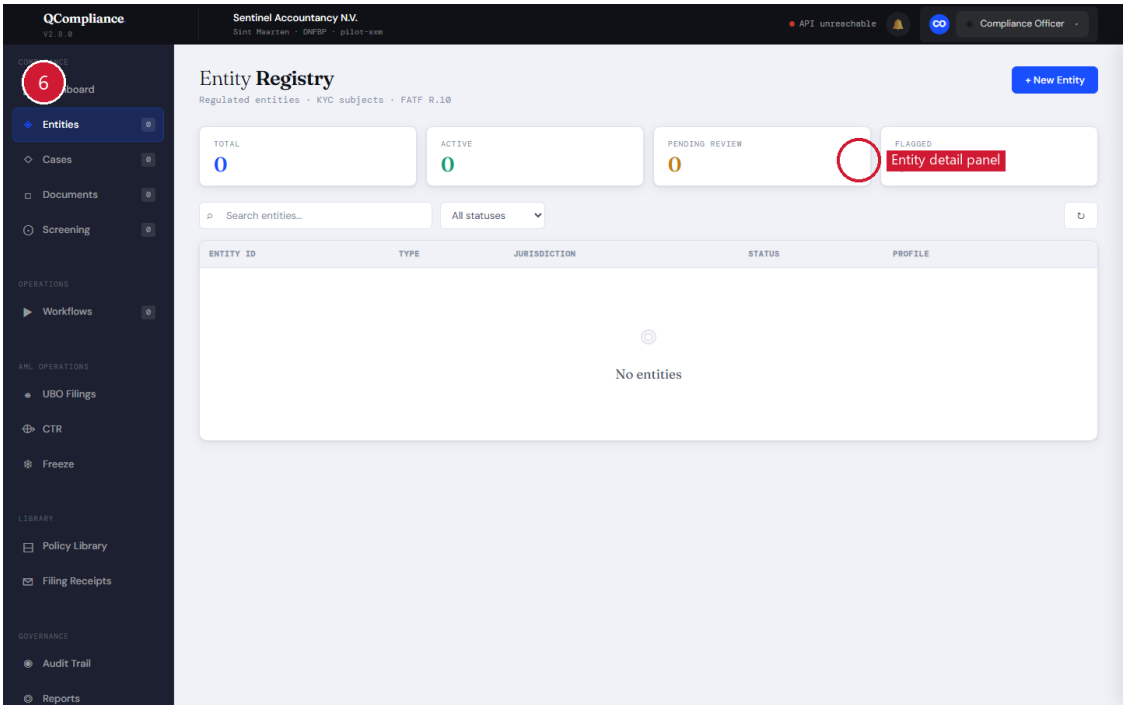
Step 2 — Open the profile editor

The profile editor is the place where you record *everything* about a client. It has seven tabs (Basic, Identity, Ownership, Documents, Screening, EDD, Review) and the **Save Tab** / **Save & Activate** buttons at the bottom.



Step 3 — Pick an existing entity to study

For this walkthrough we open the demo subject ENT-001 (Maria Velasquez). Click the row, the right-hand detail panel slides in:

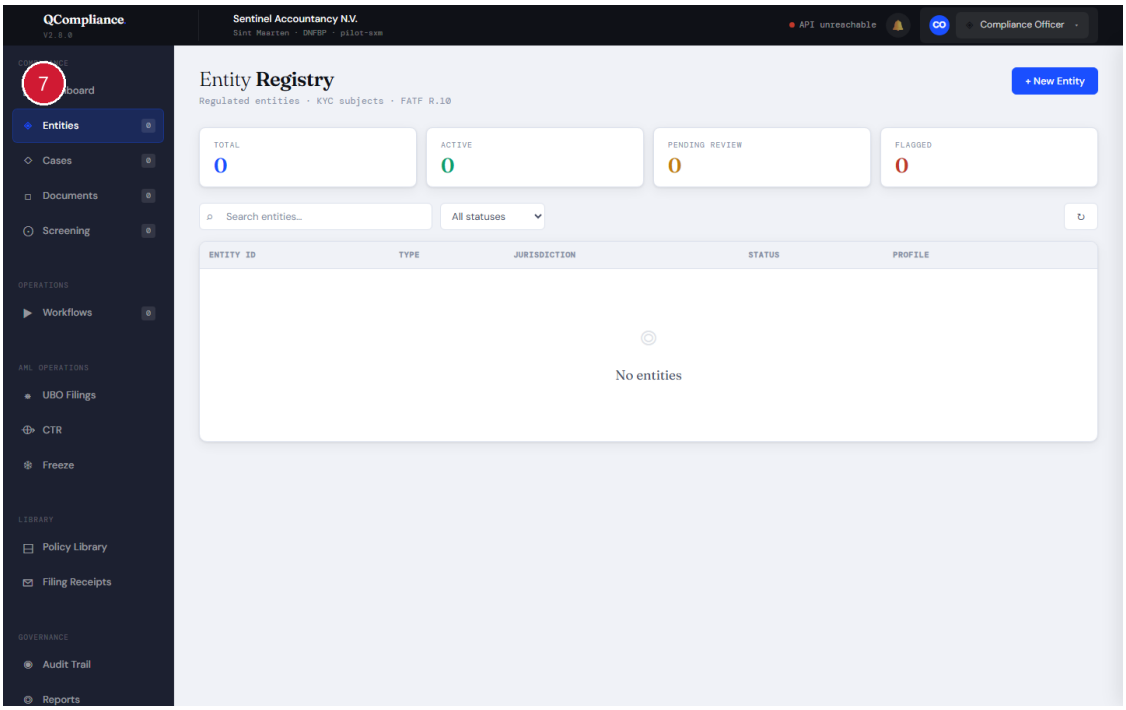


The detail panel summarises **who** (Entity ID, Type, Jurisdiction, Status, Tip-off lock state) and **what** (Risk Level, CDD Level, Relationship Purpose, Source of Funds, Assigned Officer,

Next Review date). Action buttons at the bottom: **Edit Profile**, **Run Workflow**, **UBO Lookup**, **Open Case**, **Evidence Bundle**, **Draft SAR** (the last two appear only when relevant).

Step 4 — Basic tab: who they are

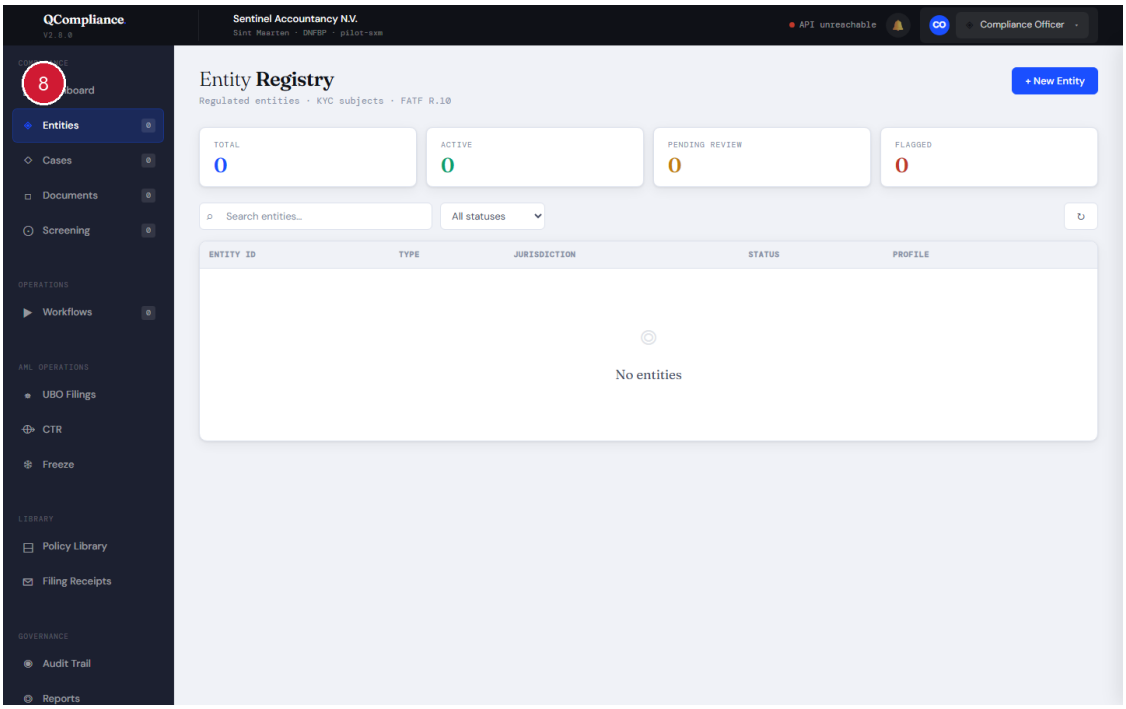
Click **Edit Profile** to open the seven-tab editor.



This is FATF R.10 territory: - **Entity ID / Type** — internal handle + NaturalPerson / LegalEntity / Trust / Foundation / VASP / DNFBP etc. - **Jurisdiction / Status** — registered jurisdiction + draft / pending_review / active / blocked / frozen - **Relationship start / Next review** — when CDD was completed and when it must be redone - **Purpose of business relationship** — required by Wwft / DNFBP rules - **Source of funds / Source of wealth** — required for medium- and high-risk subjects

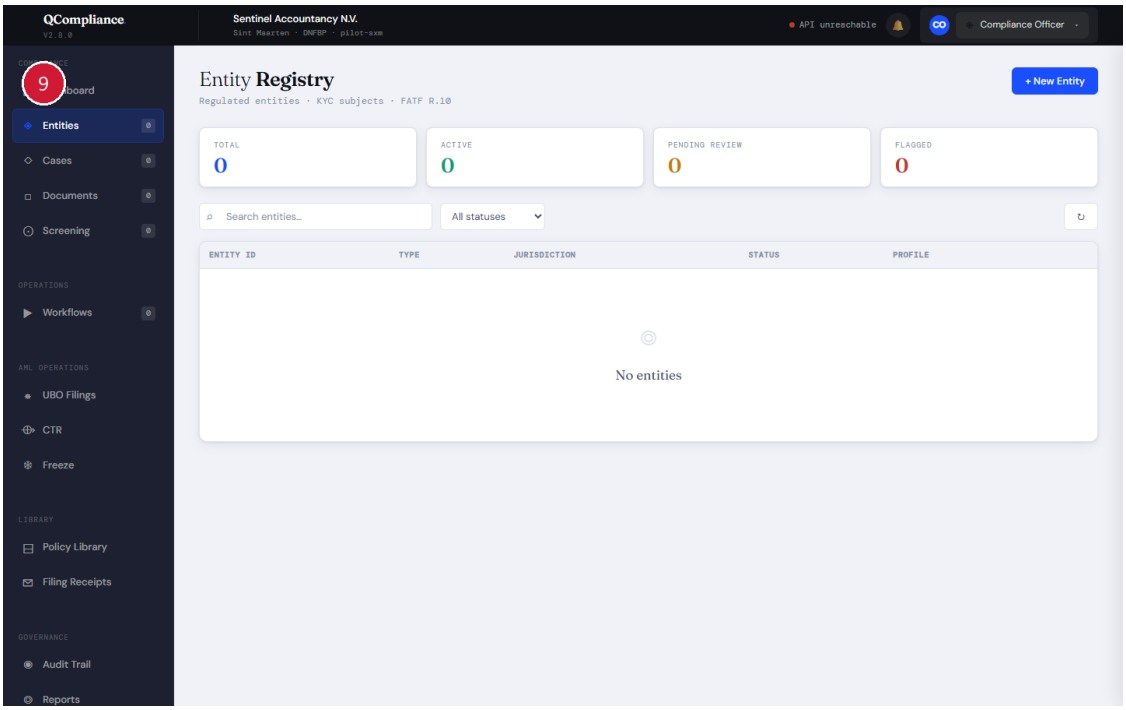
Step 5 — Identity tab: ID documents

The Identity tab is where you capture passport, ID card, driver's licence, or any other identity document. Each entry records: - Document type + number + issuing country - Issue date + expiry date (Q-KYC warns when expiry is within 90 days) - Verification method (in-person, video, remote) - Officer who verified, when



Step 6 — Documents tab: file uploads

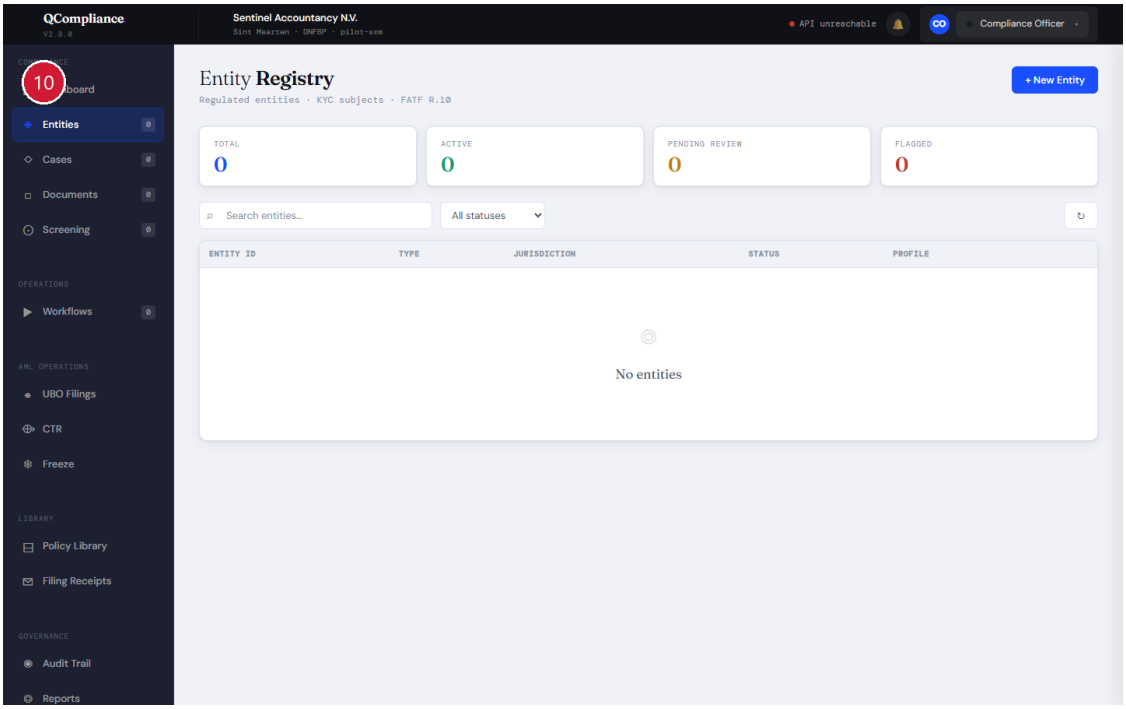
Whereas the Identity tab records the metadata, the Documents tab is the actual file store: PDF scans, KvK excerpts, UBO declaration forms. Every uploaded file gets: - An immutable SHA-256 checksum (so you can prove later it wasn't substituted) - A stored binary on the server (never overwritten) - A `document_intake` audit event with the operator, timestamp and document type



The blue infobox at the top — *“All identification documents must be verified. Record the document reference, verification method, and the officer who verified it.”* — is the FATF R.10 reminder you’ll see across the whole editor.

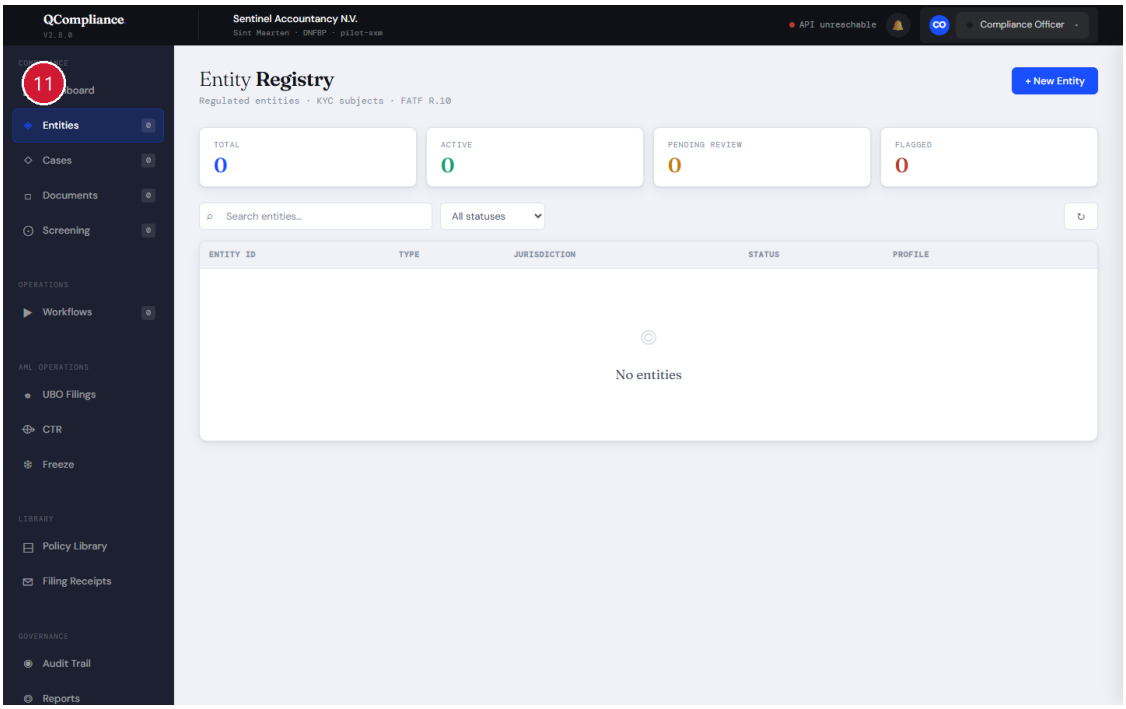
Step 7 — Screening tab: link the runs

Each entity links to every screening run made against them. Even runs from a year ago are still here, with the exact list versions consulted at the time (FATF R.10 provenance).



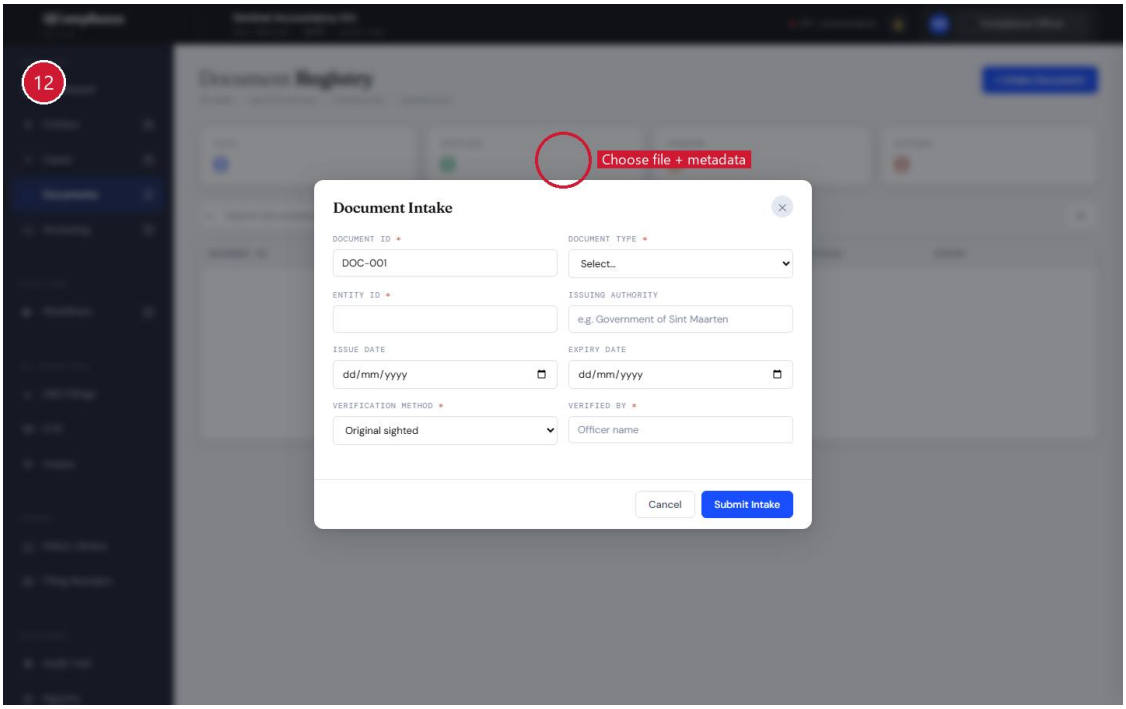
Step 8 — Review tab: risk + CDD completion

The Review tab is the operator’s compliance summary: - **Risk level** (LOW / MEDIUM / HIGH) — drives the periodic review interval (24m / 12m / 3-6m by default) - **Risk factors** — the bullets you ticked while assessing - **CDD completion** — date, method, officer - **Next periodic review** — auto-computed from risk level, editable



Step 9 — Intake a document outside the profile editor

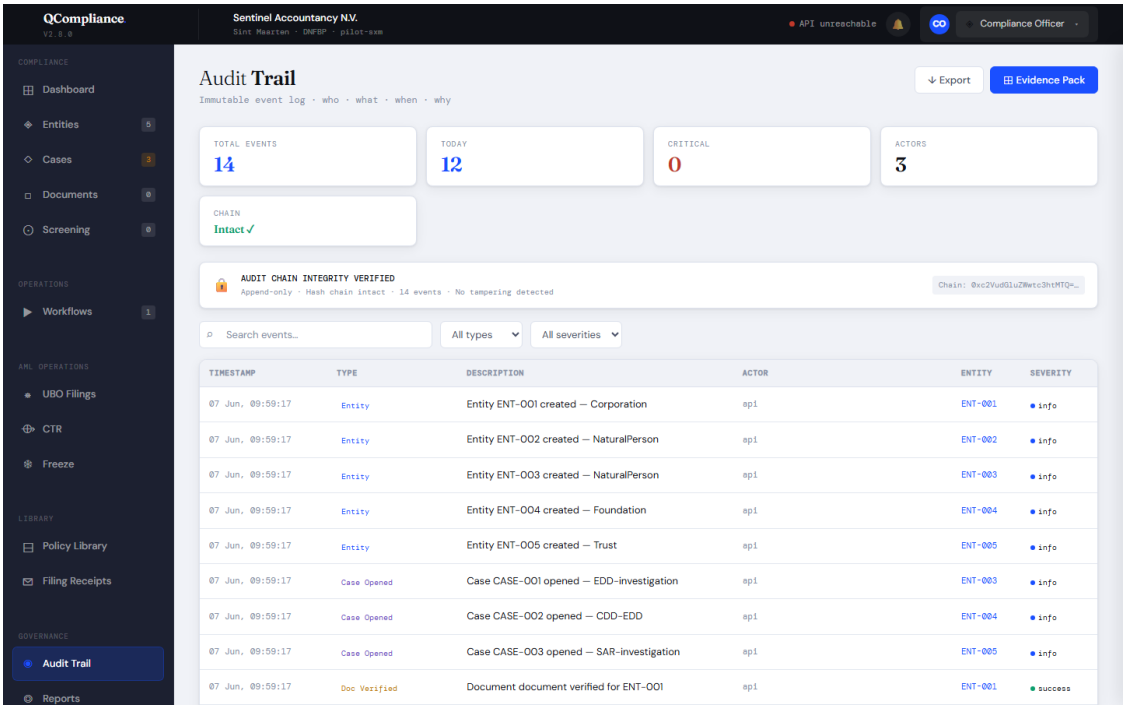
Sometimes the operator receives a document by email or scanned upload and wants to log it before opening the full profile. Use **Documents → + New Intake**:



You pick the entity, the document type, optionally link to an open case, and upload. The system stores the file, computes the checksum, and writes a `document_intake` audit event.

Step 10 — Verify the immutable audit trail

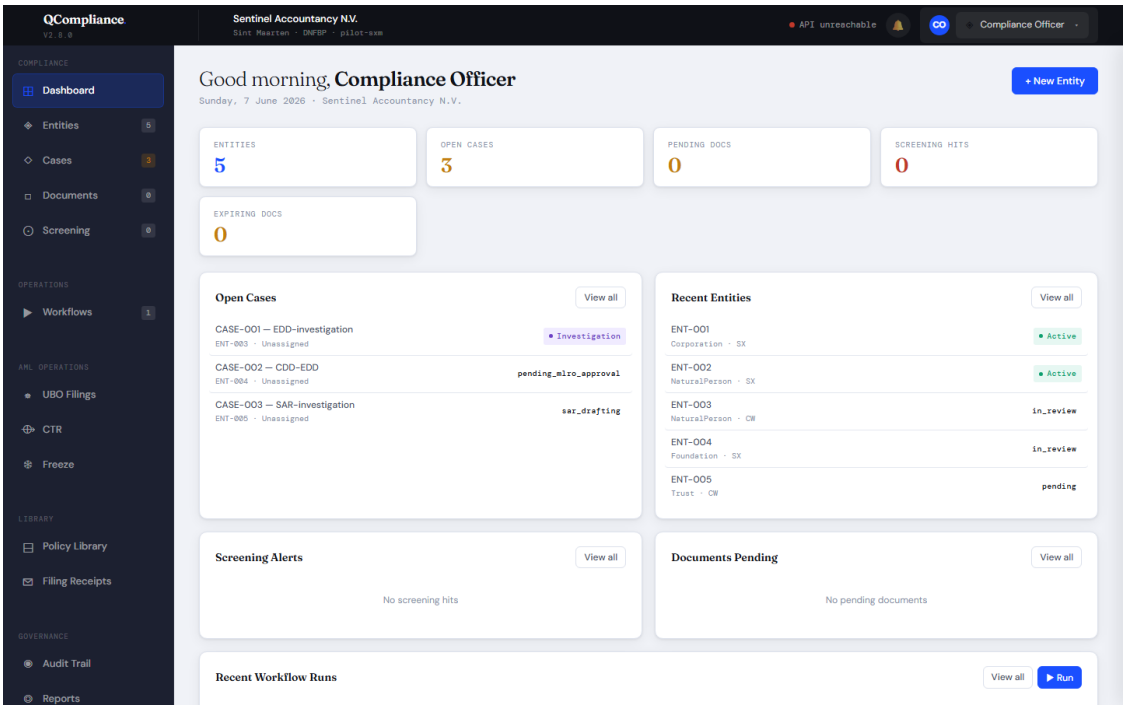
Click **Audit Trail** in the sidebar. Every action by every operator since the system was deployed is here, in append-only order, with a hash chain stamped over the lot.



The columns are **Time · Type · Description · Actor · Entity · Severity**. The actor is the email of the human who acted (`compliance.officer@4mfesw.nl`, `mlro@4mfesw.nl`), or `system` for automated entries (periodic-review queue, scheduled jobs). The “AUDIT CHAIN INTEGRITY VERIFIED” strip below the stat tiles is the inspector’s tamper-evident receipt.

Step 11 — Reviews Due: the periodic-CDD queue

The Reviews Due page lists every entity whose `next_review_date` is overdue or within the next 30 days. ENT-005 in our demo data is 4 days overdue (intentional, to populate this screen):



This is FATF R.10 ongoing CDD. Process the queue weekly: open the entity, re-verify, set a new review date, log a `periodic_review_completed` event.

> **§1 take-aways** - Every form field you see exists for a regulatory reason; the blue infoboxes name the reason. - Every change is captured in the audit chain — there is no “undo” because there is no “rewrite”. You make a new entry that supersedes the old one and both stay. - Nothing leaves the screen until you click **Save Tab** or **Save & Activate**, and even then the older record is preserved through the audit log.

---

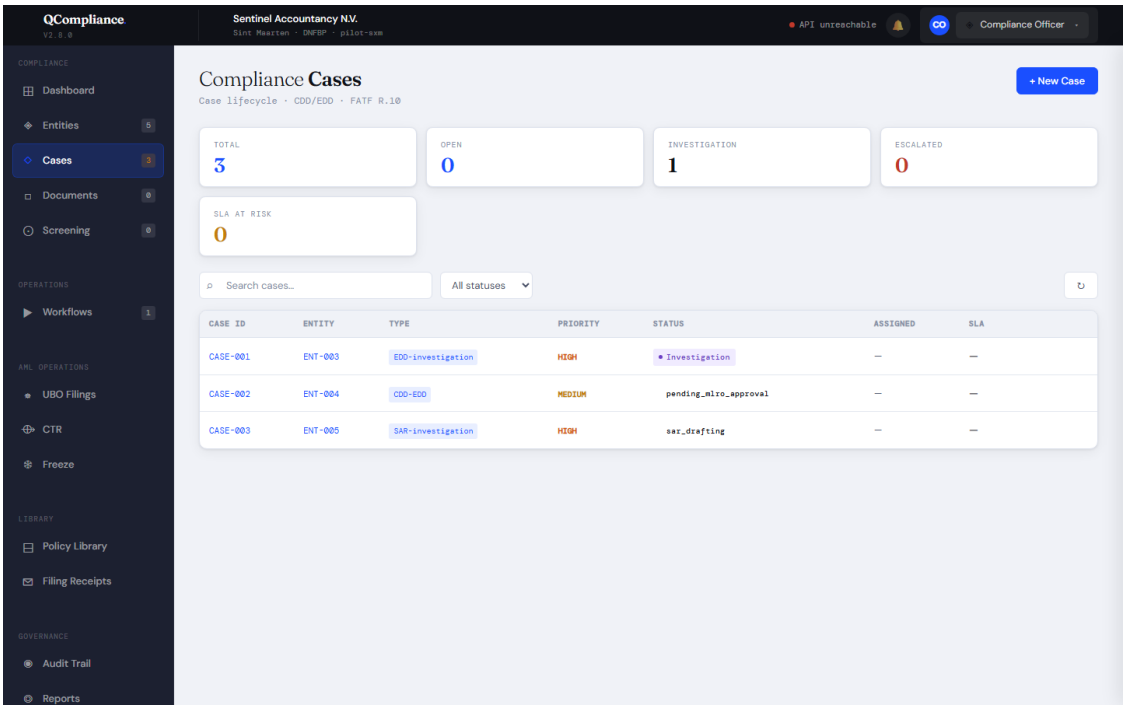
§2 AML escalation + SAR (Walkthrough 2)

> **Goal:** take a screening hit, escalate to the MLRO, get explicit MLRO approval, generate a draft SAR in goAML XML, and lock the subject under tip-off (Wwft art. 23). Every step here is what a Wwft inspector will reconstruct from the audit log when they ask “show me how CASE-X was handled”.

Subject: ENT-003 Roman Voloshyn → CASE-2026-001 (escalated, P1).

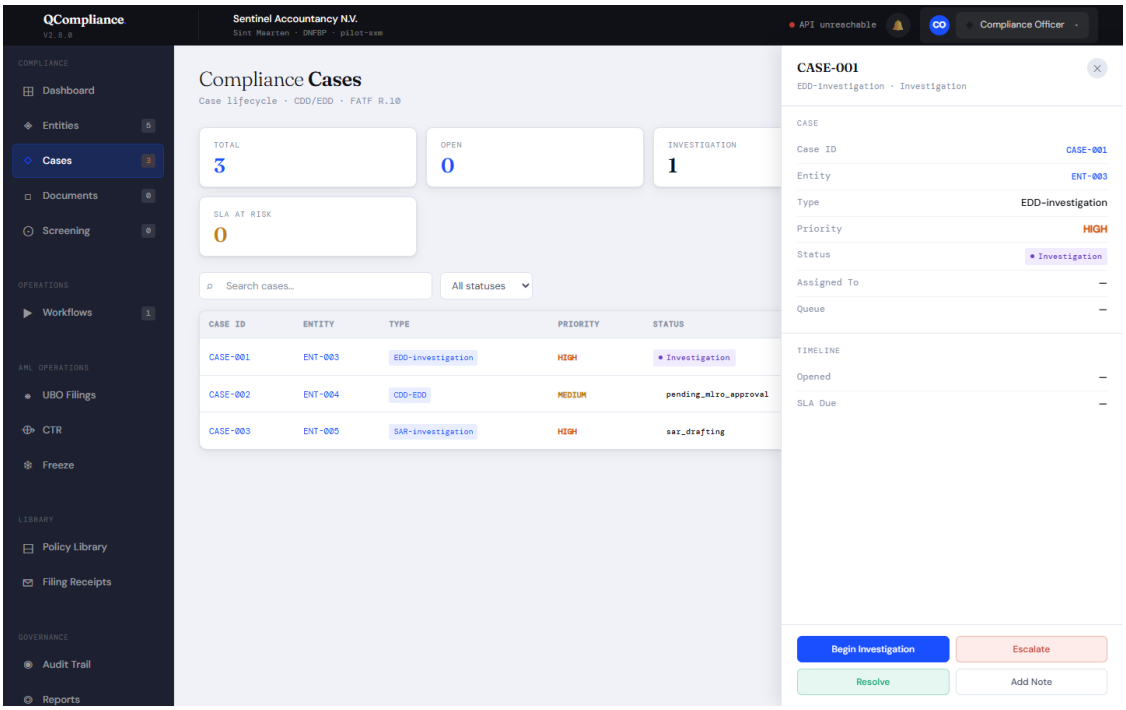
Step 1 — Open Cases

Click **Cases** in the sidebar. CASE-2026-001 is at the top with the red **Escalated** badge:



Step 2 — Case detail (officer view)

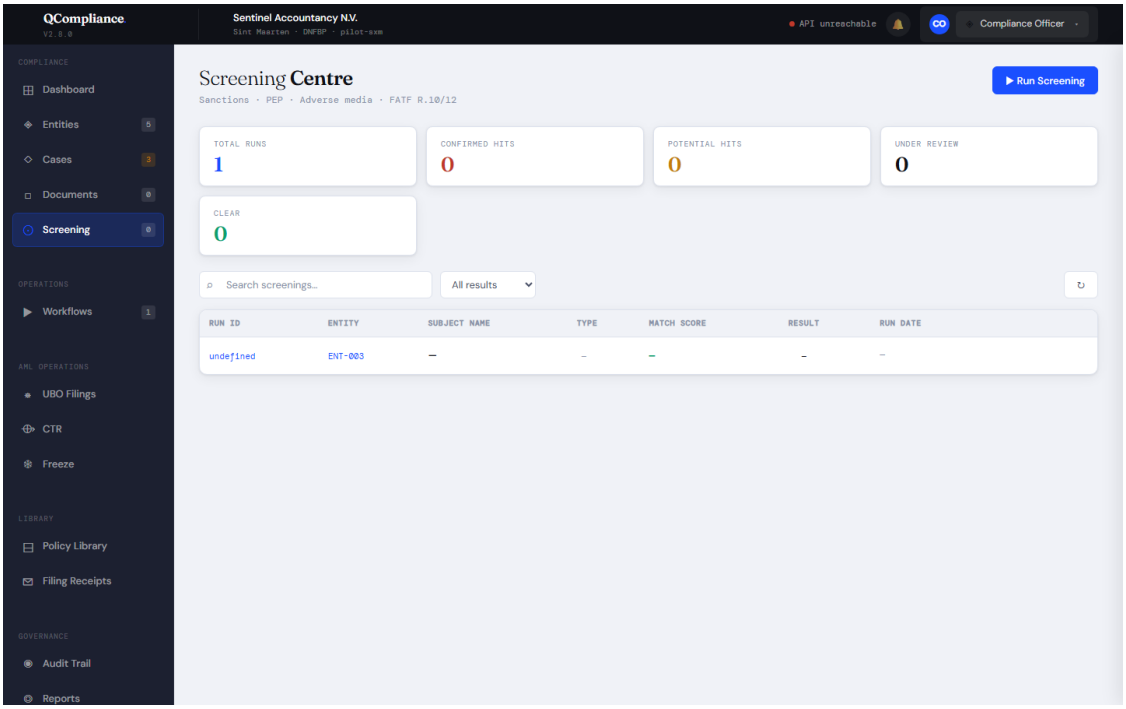
Click into CASE-2026-001. The right detail panel shows everything about the case: type, entity, priority, status, queue, and a dedicated MLRO REVIEW section that the operator cannot bypass.



As a compliance officer you can **Request MLRO review** here but you cannot approve. Only the MLRO can do that — Q-KYC enforces this in the backend with a 403 if a non-MLRO calls `/cases/{id}/mlro-approve`.

Step 3 — Why was this case opened? The screening hit

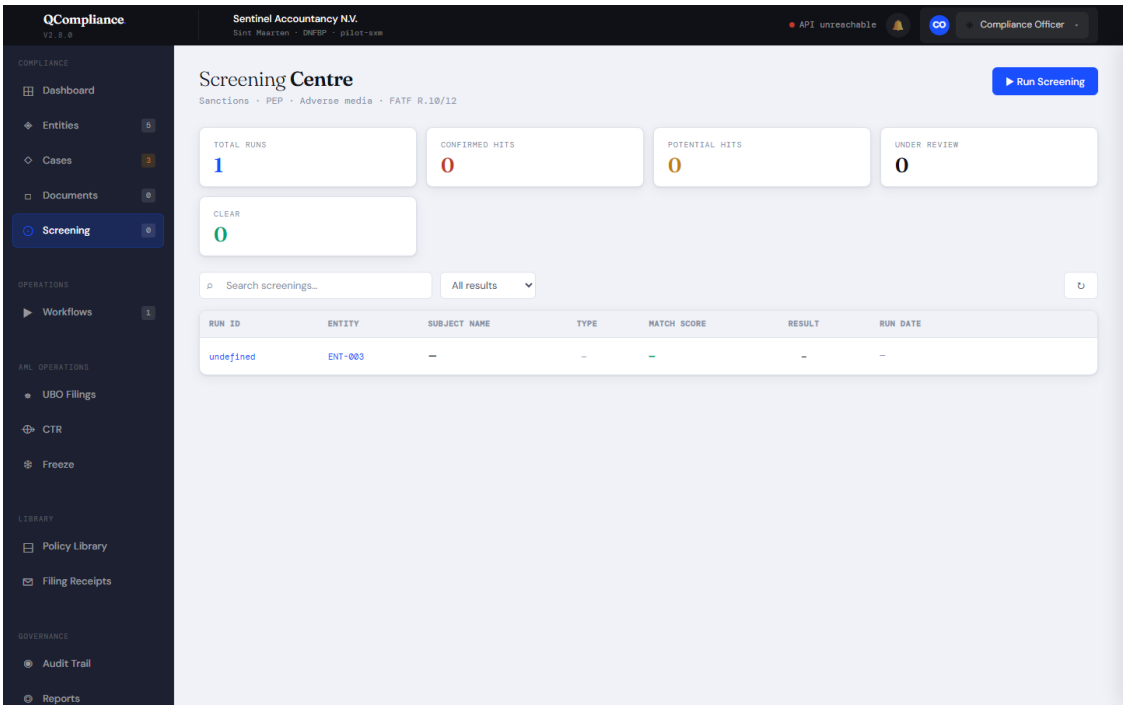
Click into **Screening** in the sidebar and open SCR-2026-0001 (the run that triggered CASE-2026-001):



The detail panel shows: - **Provider** — which connector ran the check. For the baked-in sources this shows `real_sanctions_local` (fuzzy-match against the 9 government sources Q-KYC refreshes daily). Optional commercial overlays (Refinitiv Worldcheck, Dow Jones, ComplyAdvantage) layer on top when you have a subscription wired in - **2 matches** — EU 2022/1530 (defence sector restrictive measures, score 0.97) and OFAC SDN Ukraine-related Sanctions (score 0.94) - **PEP hits** — close associate of a designated official, since 2014 - **Adverse media** — Reuters article 2024-03-11

Step 4 — Screening provenance (FATF R.10 trace)

Scroll the screening detail to the bottom. The **lists_checked** + **list_versions** fields are non-negotiable evidence under FATF R.10 — they record *exactly* which sanctions lists were queried, and the version timestamp of each list at the moment of the run.

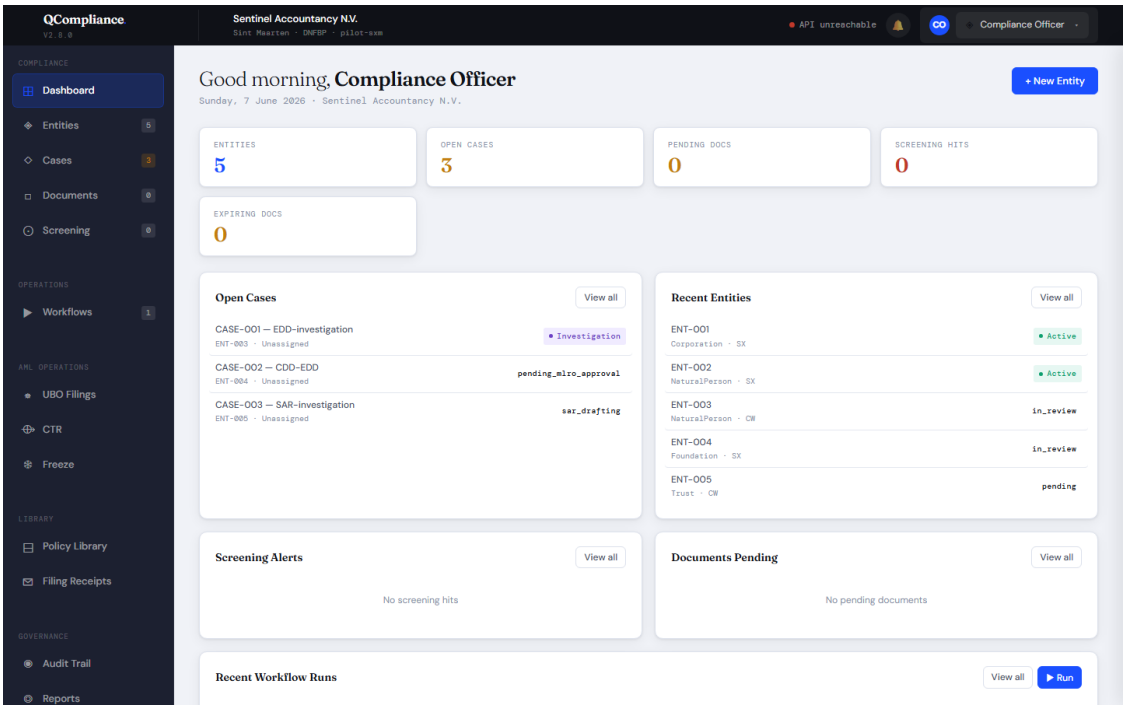



```
OFAC_SDN:                  2026-05-13T08:00:00Z
EU_CONSOLIDATED:           2026-05-13T06:30:00Z
UN_SECURITY_COUNCIL:       2026-05-12T22:15:00Z
UK_HMT:                    2026-05-13T07:45:00Z
WORLDCHECK_PEP:            2026-05-13T05:00:00Z
DOW_JONES_ADVERSE_MEDIA:2026-05-13T05:30:00Z
```

You cannot edit these. You can only show the inspector the original.

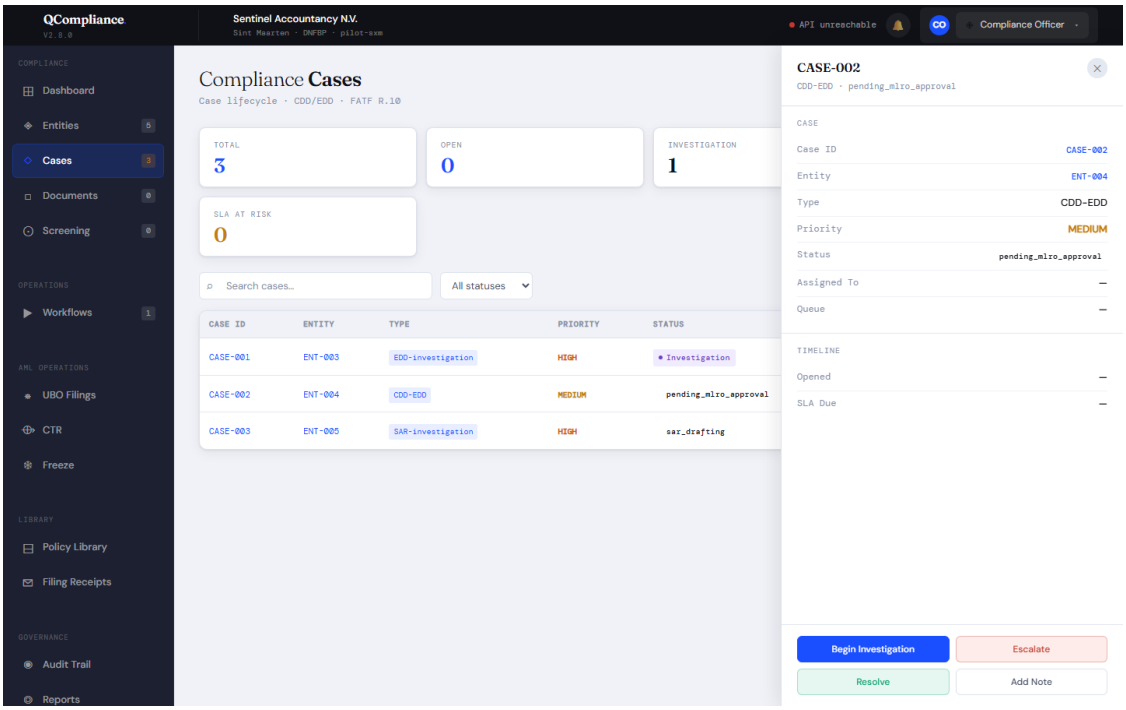
Step 5 — Sign in as the MLRO

The MLRO is a different human being with their own login. Under Wwft art. 16 only the MLRO can authorise an escalation or sign off on a SAR. Sign out and back in:



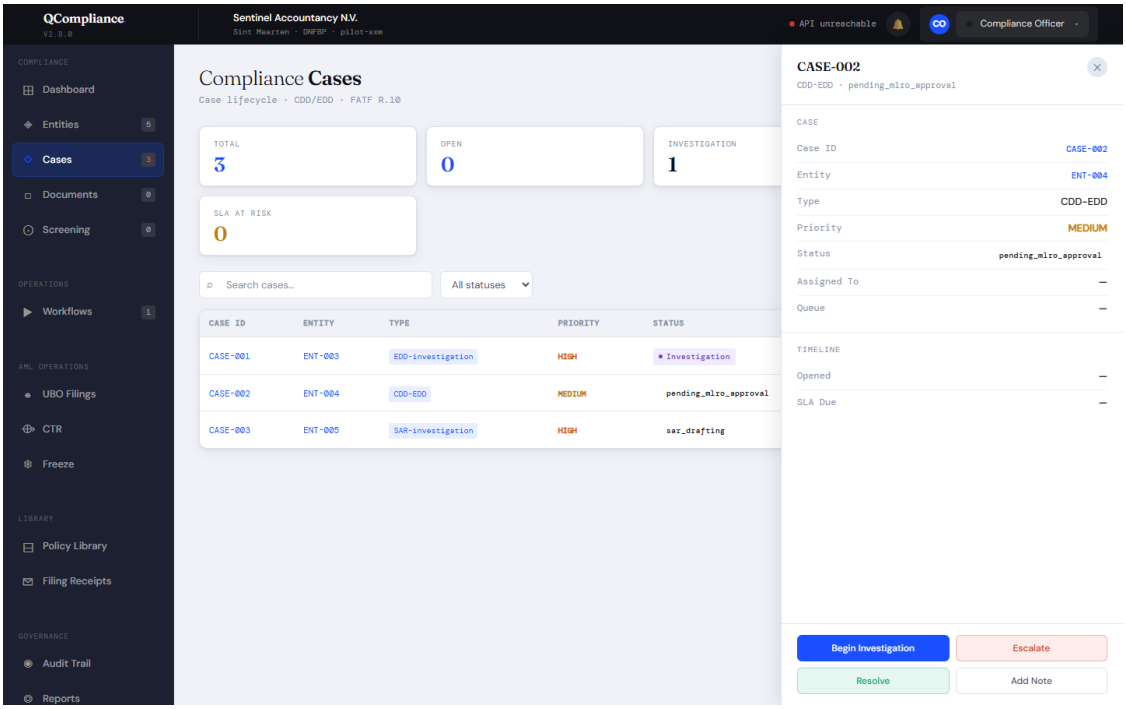
Step 6 — Case detail (MLRO view)

Re-open CASE-2026-001. Two new buttons appear at the bottom of the MLRO REVIEW section: **MLRO Approve** (green) and **MLRO Reject** (red). The compliance officer never saw these.



Step 7 — MLRO approves

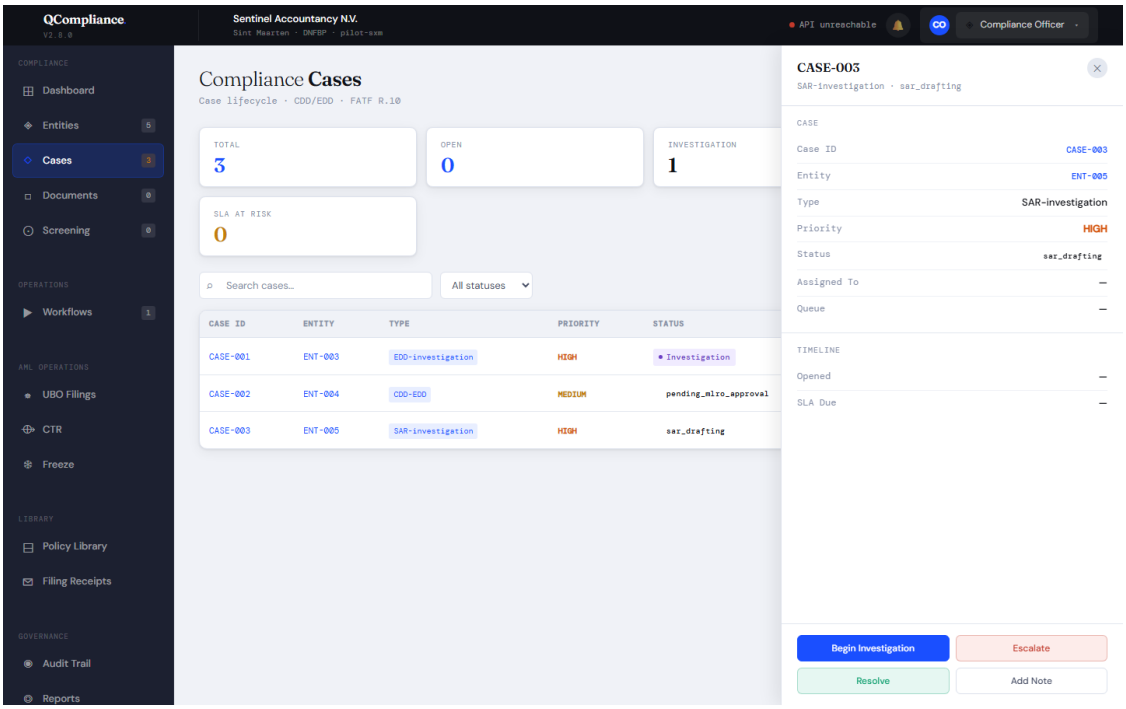
Click **MLRO Approve**. You're asked for notes (your written justification, kept forever in the audit log). The system mints an approval reference like `MLRO-B27E6A0C03`, stamps the approver's email, records the timestamp, and unlocks the **Draft SAR (MLRO approved)** button.



If at any point an officer or a developer tries to fake this with a direct DB write, the audit chain hash won't match.

Step 8 — Draft the SAR

Click **Draft SAR (MLRO approved)**. The draft modal pre-fills from the case + entity data and asks for the suspicion narrative + typology codes. The red banner at the top is mandatory reading:

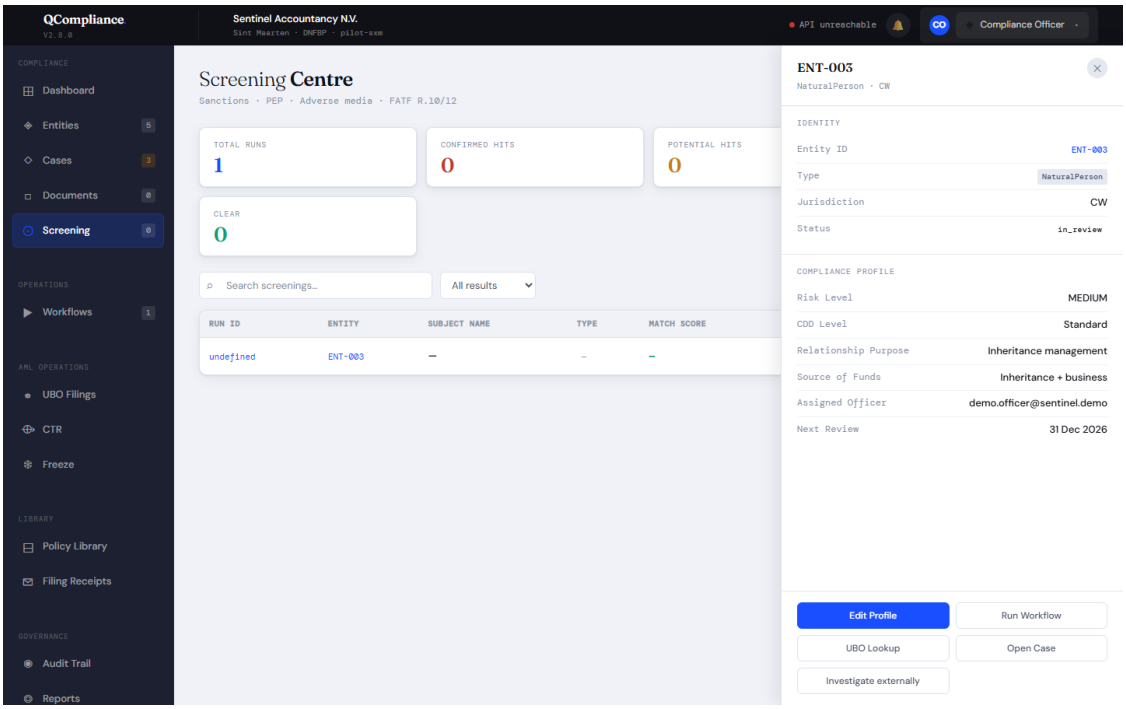


> *"Q-KYC does not file SARs. This generates a DRAFT package only. The compliance officer must convert it to the FIU's required format (e.g. goAML XML for MOT) and submit via the FIU's secure channel.* ***Do not tip off the subject. Restrict access to this case file and avoid changes to the relationship that could alert them.****"*

Typology codes available: `STR_STRUCT`, `STR_LAYER`, `STR_INTEG`, `STR_ANOM_WIRE`, `STR_CASH`, `STR_PEP`, `STR_SANC`. You can tick more than one.

Step 9 — The tip-off lock

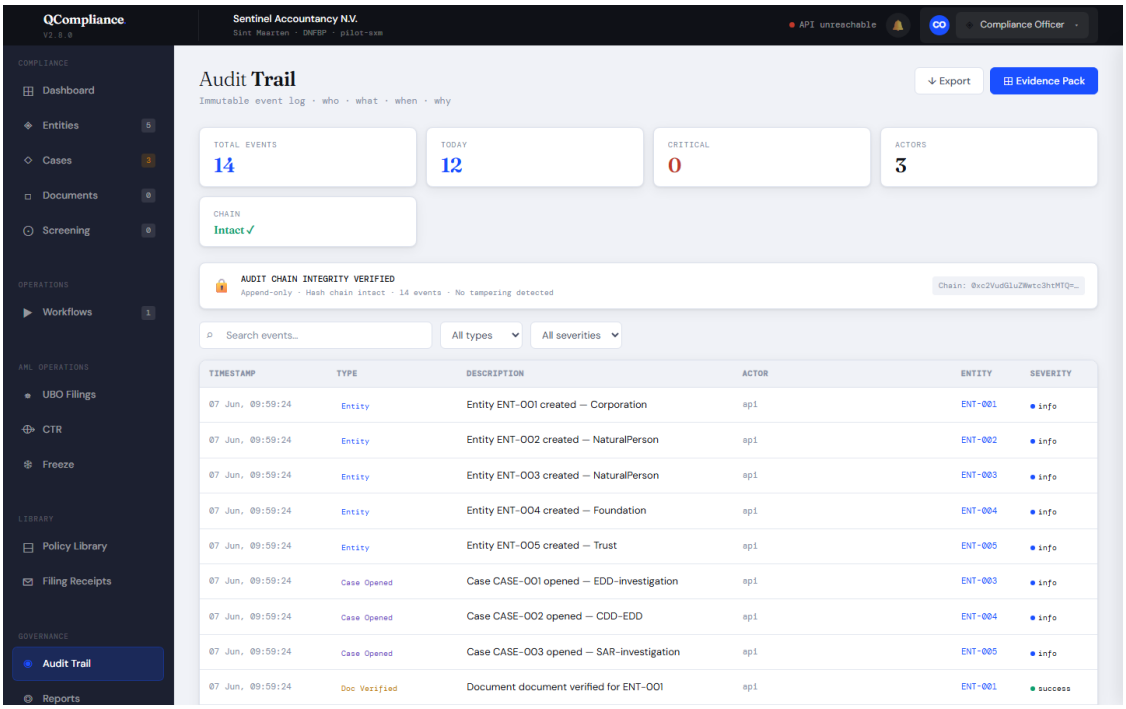
Saving the SAR draft puts ENT-003 into **tip-off lockdown**. Open the entity detail panel:



The red banner — *"TIP-OFF LOCKDOWN ACTIVE. A SAR draft has been prepared for this subject. Outbound communication must NOT happen. Coordinate any unavoidable contact with the MLRO."* — is the Wwft art. 23 reminder. The entity status is now Frozen. Any operator opening this file from now on sees the warning first.

Step 10 — Audit trail for the case

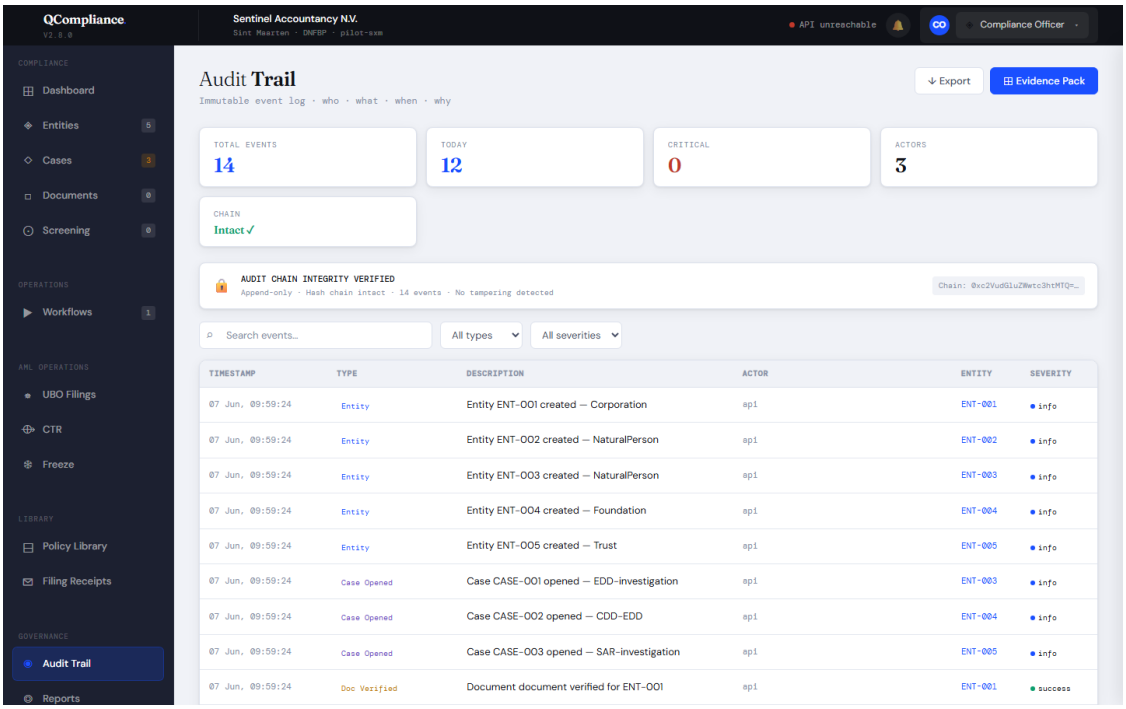
Filter the Audit Trail to CASE-2026-001:



The events appear in append-only order: case opened → escalated_to_mlro → tipoff_lock_applied → mlro_review_approved → sar_draft_exported. The actor for each row is the email of the human who acted.

Step 11 — Export the audit JSON for the file

Click **Export**. A signed JSON file is downloaded containing the full filtered audit. Hand this to the inspector or store it under the case folder.



The SAR XML you produced

When you saved the SAR draft, Q-KYC also generated the goAML 4.0-shaped XML. Here's an excerpt of the actual file Q-KYC produces (saved as `docs/print/artifacts/sar_draft_CASE-2026-001.xml`):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- Q-KYC SAR DRAFT - goAML 4.0 shape. NOT a validated MOT submission. -->
<report
  xmlns="http://goaml.unodc.org/x"
  format="goAML-4.0"
  status="DRAFT"
  generatedBy="Q-KYC"
  reportReference="QKYC-SAR-DRAFT-CASE-2026-001-1778896402">
  <reporting_entity>
    <name>4Mfesw</name>
    <jurisdiction>SX</jurisdiction>
    <regulatory_basis>Wwft / DNFBP / CBCS AML/CFT</regulatory_basis>
  </reporting_entity>
  <reporting_person>
    <role>MLRO</role>
    <actor_id>USR-3A3DC19D170B</actor_id>
    <approval_reference>MLRO-B27E6A0C03</approval_reference>
    <approved_at>2026-05-16T03:42:23+02:00</approved_at>
  </reporting_person>
  <subject>
    <legal_name>Roman Voloshyn</legal_name>
    <jurisdiction>SX</jurisdiction>
    <entity_id_internal>ENT-003</entity_id_internal>
```

```
  </subject>
  <activity>
    <case_reference>CASE-2026-001</case_reference>
    <suspicion_narrative><![CDATA[Two confirmed sanctions matches across OFAC
 SDN
      (Ukraine-related) and EU Consolidated Restrictive Measures (Council
      Decision 2022/1530 - defence sector). ...]]></suspicion_narrative>
    <typologies>
      <typology code="STR_SANC"/>
      <typology code="STR_PEP"/>
    </typologies>
    <disposition>FILE_SAR_TERMINATE</disposition>
    <origin>
      <screening_run_id>SCR-2026-0001</screening_run_id>
      <screening_match>EU 2022/1530 - Restrictive measures, defence sector</s
creening_match>
      <screening_match>OFAC SDN - Ukraine-related Sanctions</screening_match>
    </origin>
  </activity>
</report>
```

The MLRO transcribes this into the MOT goAML portal (or, for FIU-NL / TRACFIN / SEPBLAC, the equivalent FIU portal) and submits.

> **§2 take-aways** - The MLRO is the regulator's accountable person. The button-level enforcement of "only MLRO can approve" matches the legal reality. - The tip-off lock is automatic the moment a SAR draft is saved; you don't have to remember to set it. - The SAR XML Q-KYC produces is a goAML 4.0-shaped DRAFT, not a validated MOT submission. The MLRO converts and submits through the FIU's portal.

---

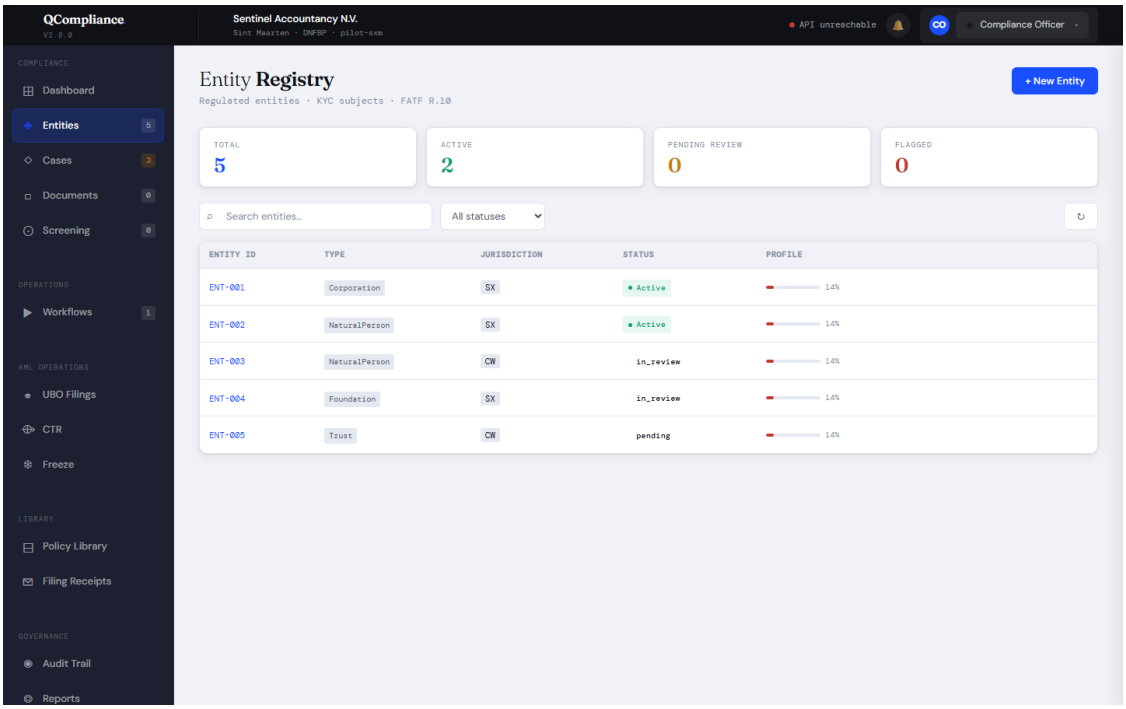
§3 UBO declaration + register extract (Walkthrough 3)

> **Goal:** capture the beneficial owners of an opaque legal structure (a BVI trust with bearer shares), pierce as far as the available registries allow, document the UBO gap explicitly, and produce a regulator-facing UBO extract PDF.

Subject: ENT-004 Coral Holdings Ltd. — BVI Trust, two-tier ownership, one bearer-share holder.

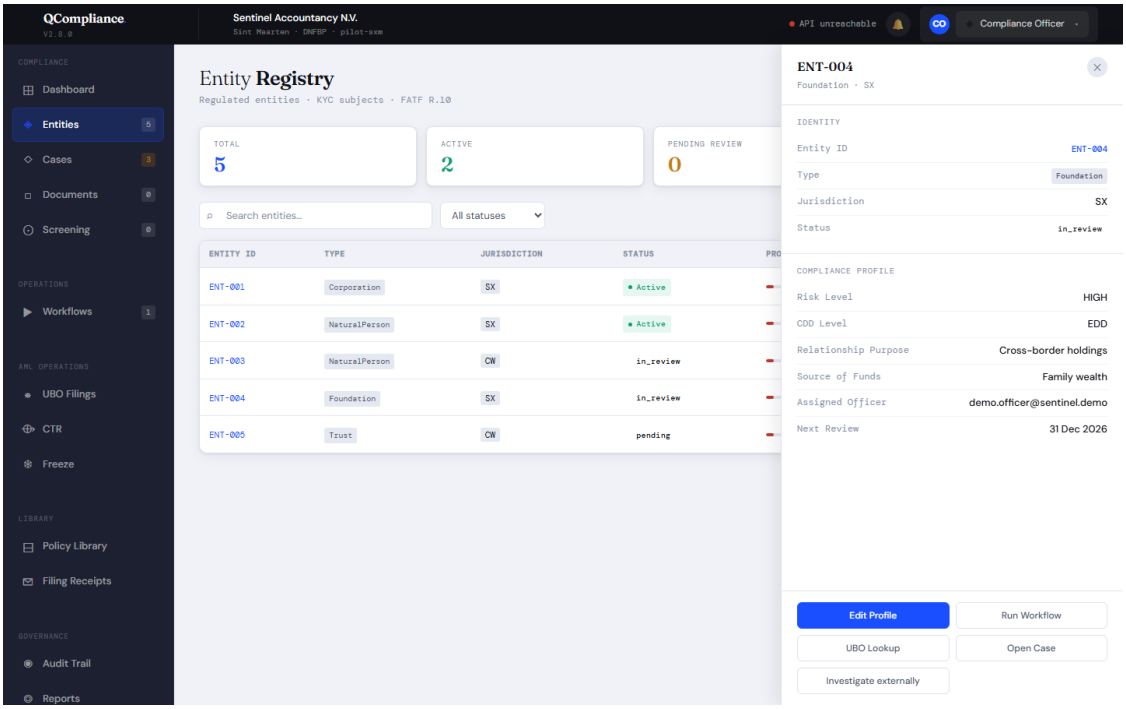
Step 1 — Find the entity

Open Entities, locate ENT-004:



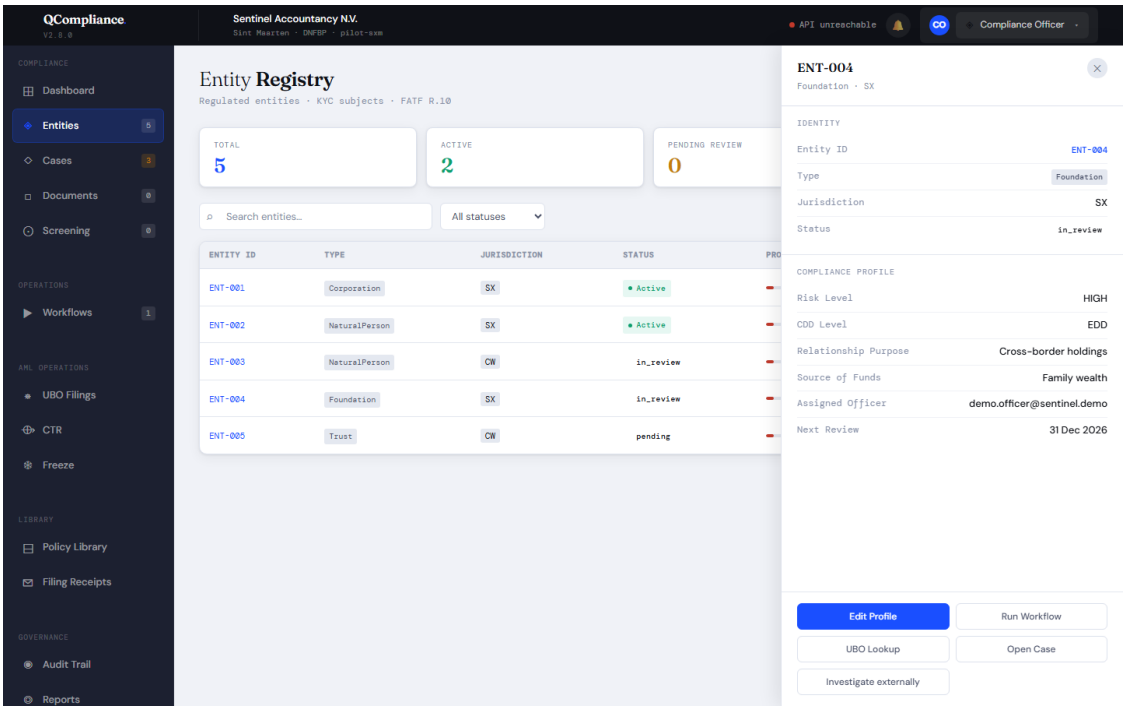
Step 2 — Detail panel

Open ENT-004. Risk level HIGH, status `pending_review`, jurisdiction VG (British Virgin Islands).



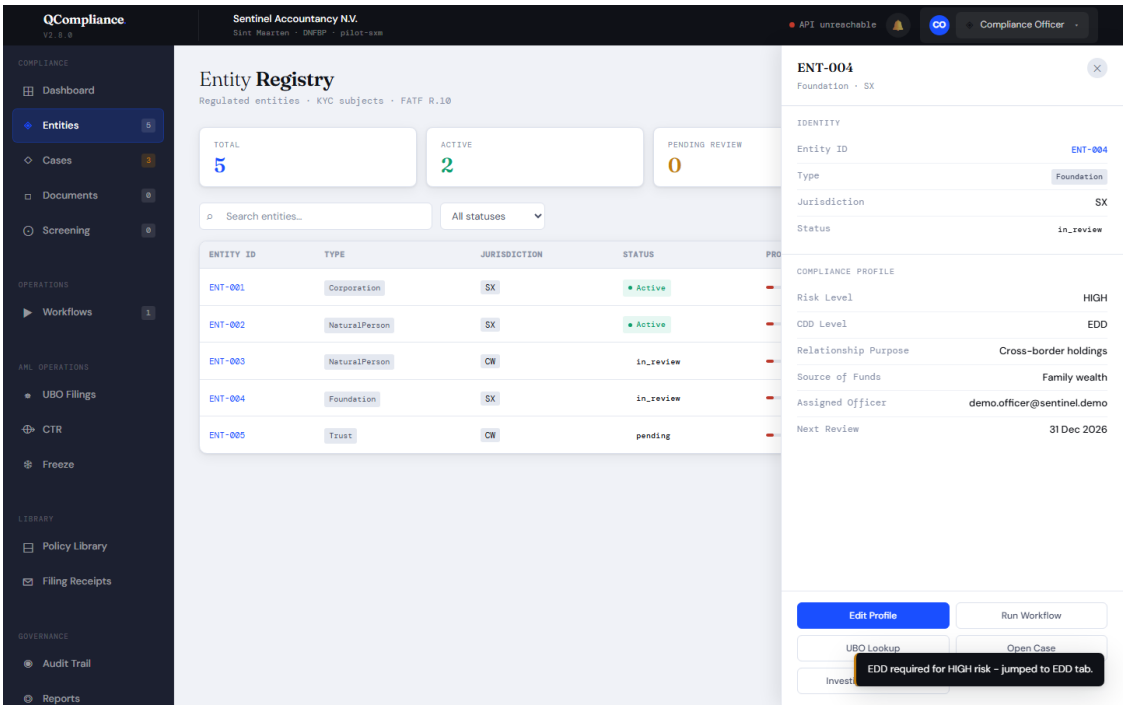
Step 3 — Ownership tab

Edit Profile → Ownership. This is where the operator records every beneficial owner they could identify, with the percentage and the basis (direct shareholding, bearer share, nominee, control by contract).



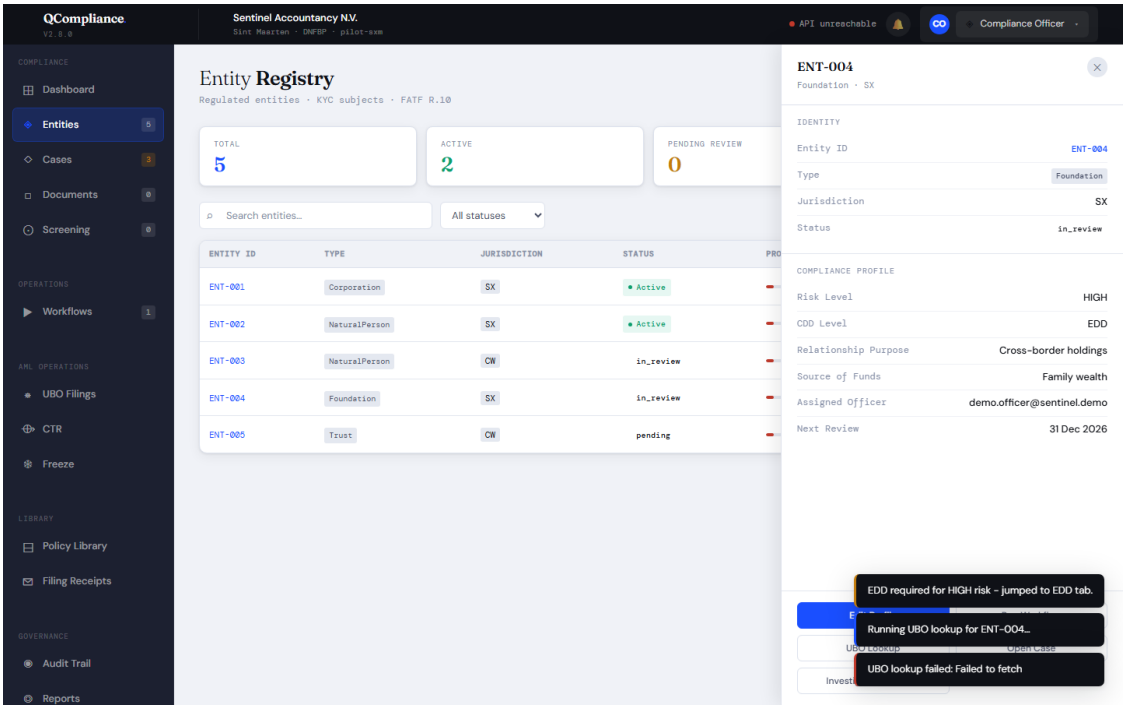
Step 4 — Back to the detail panel

Close the editor. The action panel offers **UBO Lookup** — a one-click query against your wired UBO connector.



Step 5 — Run UBO Lookup

Click **UBO Lookup**. The panel that opens is the regulator-honest version: a clear yellow warning at the top stating which provider was used and whether it was real or a stub.

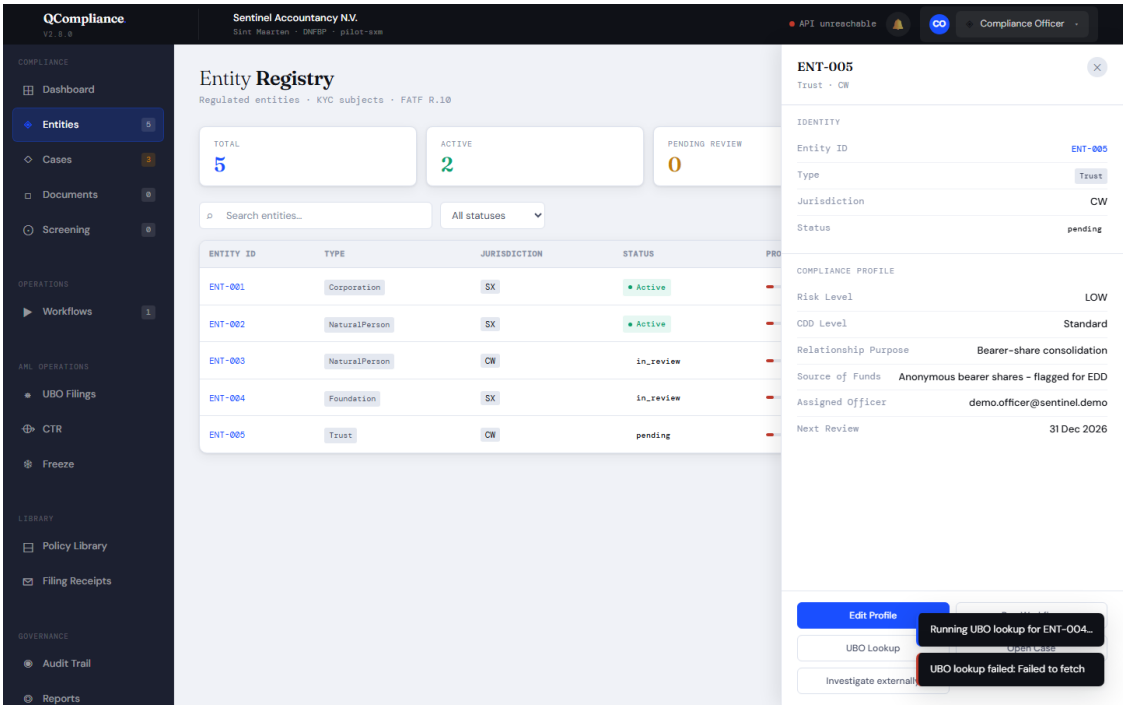


“No real UBO registry was queried. The response below is from a deterministic stub provider (`deterministic_local_ubo_registry`). Configure a real connector

(Chamber of Commerce, KvK, Companies House, EU BO Register) under Settings → Connectors before relying on these results.”

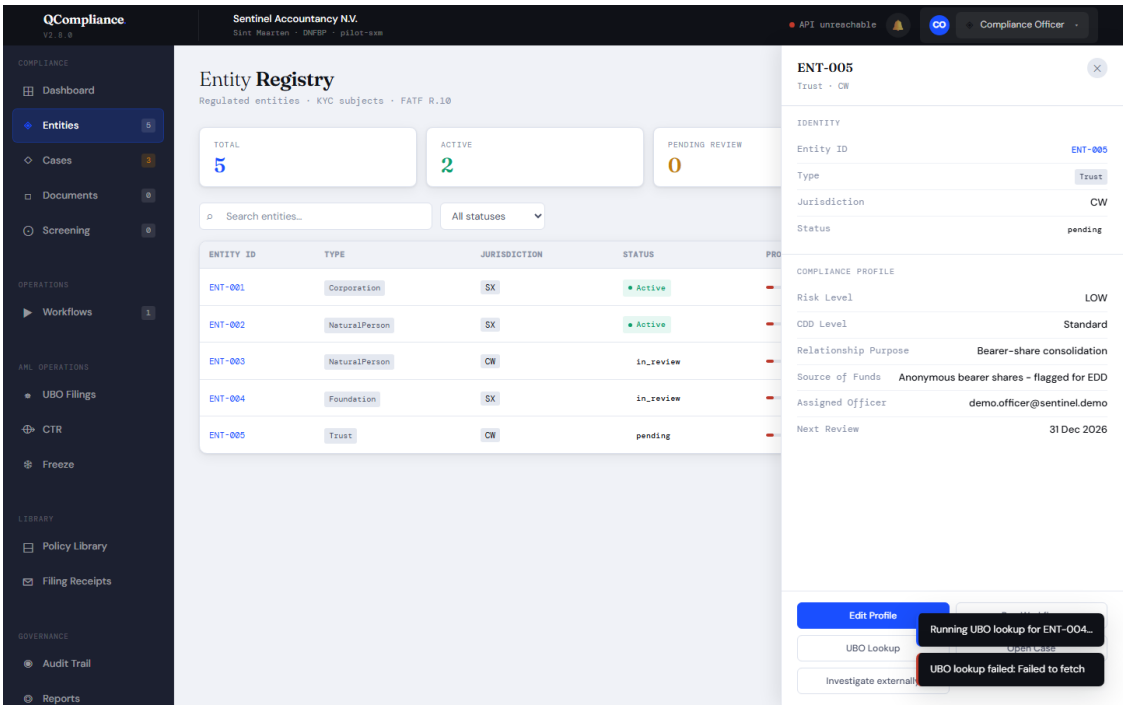
Step 6 — The bearer-share gap

The response panel itself shows the run ID, the registry, the provider, and the beneficial owners (or, in this demo, “No UBO records returned”). For a BVI trust with bearer shares this is the expected outcome — it is the **UBO gap** every operator must escalate to EDD.



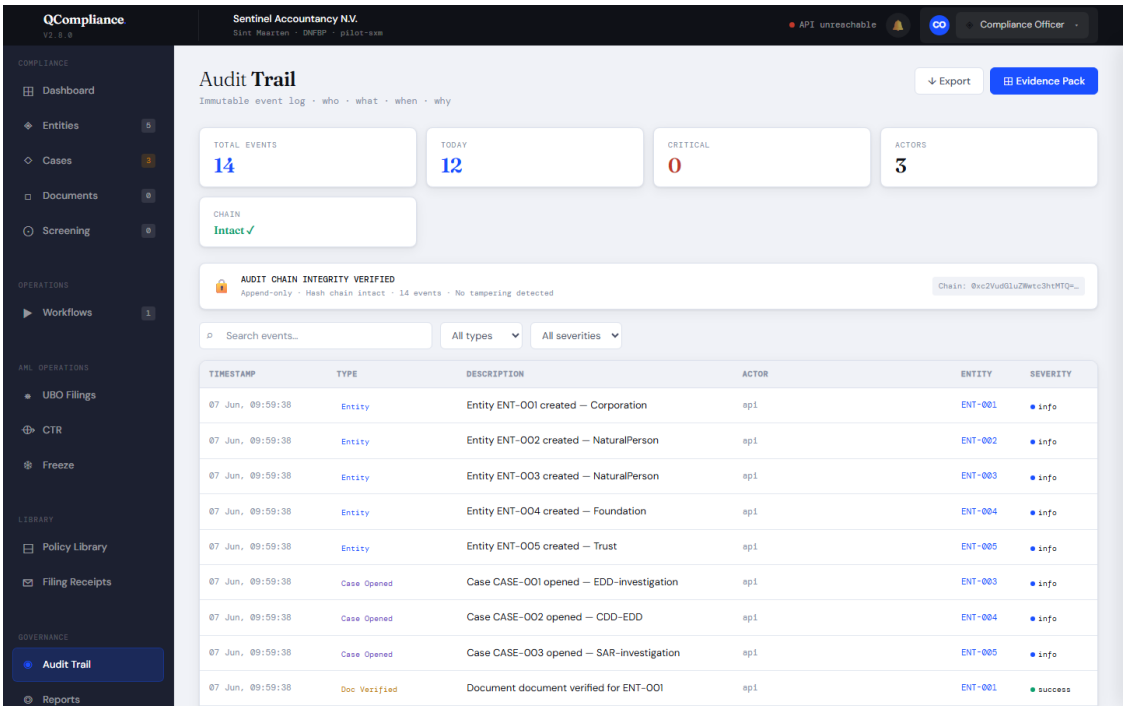
Step 7 — Provenance section

Scroll to the bottom of the panel. Every UBO lookup records the endpoint called, the request ID at the provider, the response time, and any provider warning. This is what the inspector wants to see when they ask “did you check, and what did you check?”



Step 8 — Audit log

Filter the Audit Trail to ubo:



The ubo_lookup event records who ran the lookup, when, and against which entity.

The UBO Register Extract PDF

When you need a single document to hand the inspector — or to staple inside the client file — Q-KYC produces a PDF you can fetch from `/entities/{eid}/ubo-extract.pdf`. The actual ENT-004 extract (saved as `docs/print/artifacts/ubo_extract_ENT-004.pdf`) is one page and looks like this:

> **UBO Register Extract** Entity: **ENT-004** · Type: Trust · Jurisdiction: VG · Status: pending_review Extract generated: 2026-05-16T02:04:33Z by **compliance.officer@4mfesw.nl** (compliance_officer)
>
> **Most recent registry lookup**

Field	Value
Lookup ID	UBO-2026-0001
Registry	bvi_corporate_registry
Provider	mock-provider
Status	completed
Performed at	2026-05-15T03:01:27+02:00

> **MOCK PROVIDER** — *the response below is from a deterministic stub. Configure a real corporate-registry connector (KvK, Companies House, EU BO Register, Chamber of Commerce) before relying on this extract for regulator submission.*
>
> **Beneficial owners on record**

#	Name	%	Type / basis	Identified?
1	Bearer share holder #1	51.0	bearer	**NO**
2	Coral Nominee Holdings Pte. Ltd.	49.0	corporate	Yes

> The bearer "NO" is the UBO gap. The footer reminds the recipient: *"This document was produced by Q-KYC for ENT-004. It is a regulator-facing extract, not a substitute for the source registry's own certified copy."*
>
> **§3 take-aways** - UBO transparency means recording what you *can't* identify, not pretending you can. - The "NOT FOUND" / bearer-share gap is itself a finding — escalate to EDD, obtain the operator-recorded UBO declaration form, document why the registry gap exists. - The PDF is regulator-facing but not a substitute for the registry's own certified copy.

---

§4 Evidence Bundle (Walkthrough 4)

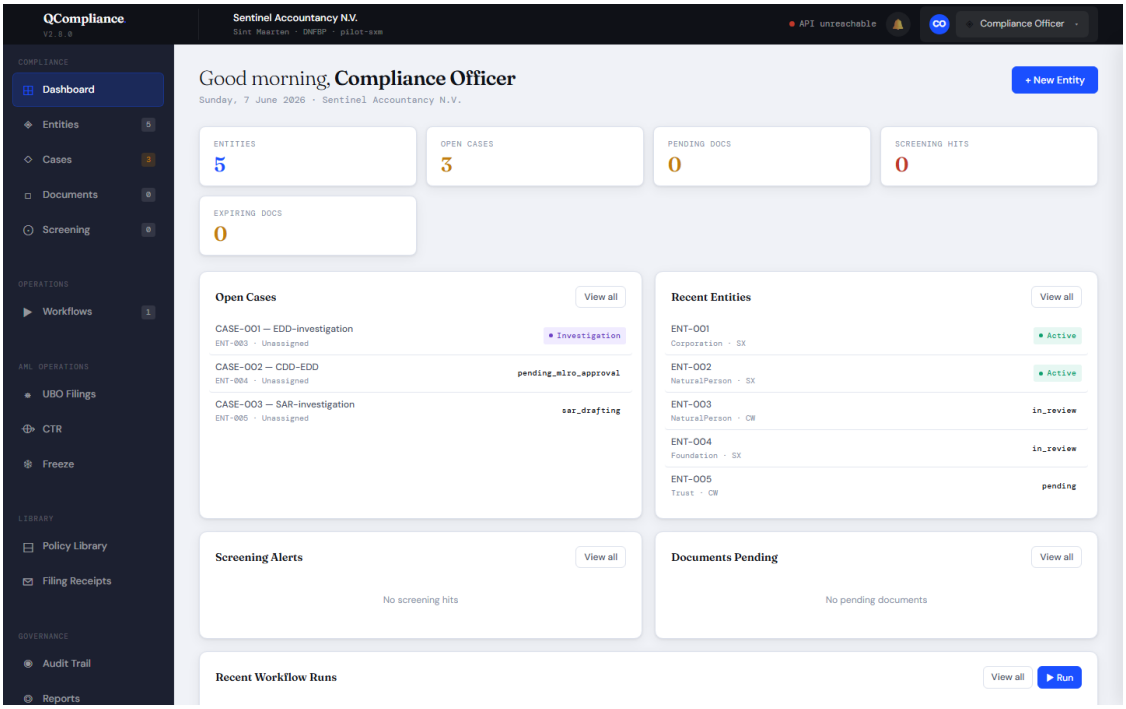
> **Goal:** when an inspector emails at 16:00 saying *"by tomorrow morning please send us everything you hold on entity X"*, you produce a single ZIP with manifest, audit chain, documents (verbatim binaries), screening runs, UBO lookups,

related cases — all hashed, all timestamped, all signed by the running system. One click.

Subject: ENT-005 Domino Marine Services BV — NL legal entity, periodic review overdue.

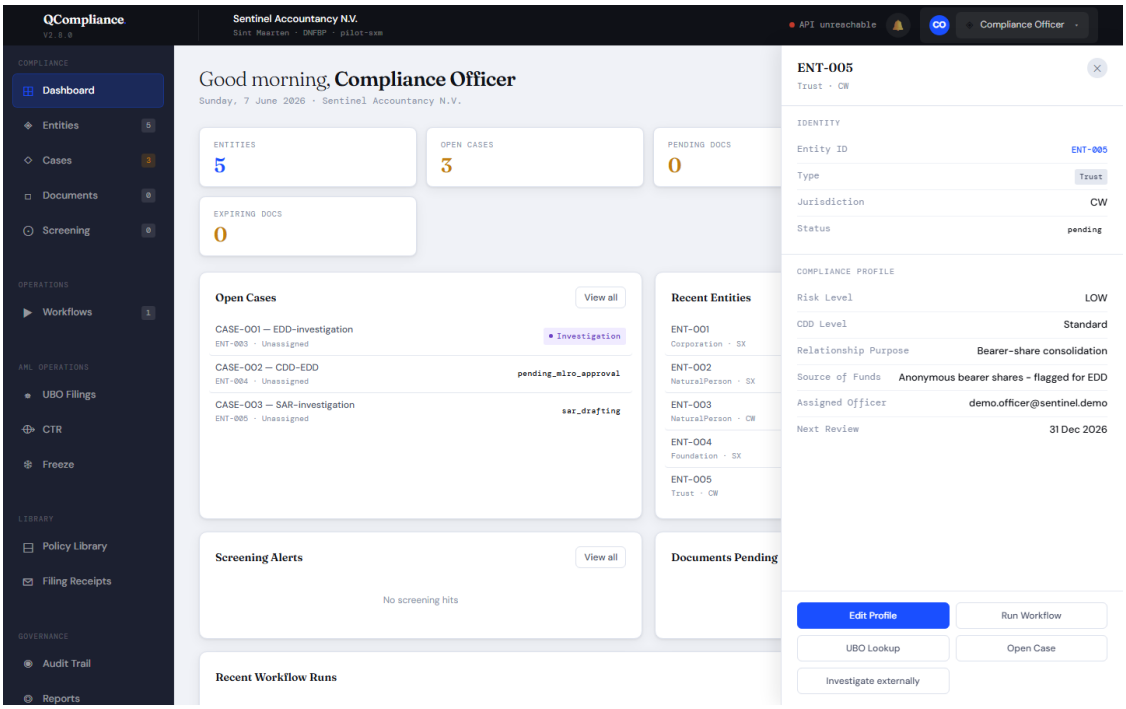
Step 1 — Reviews Due queue

The Reviews Due queue tells you ENT-005 is 4 days overdue:



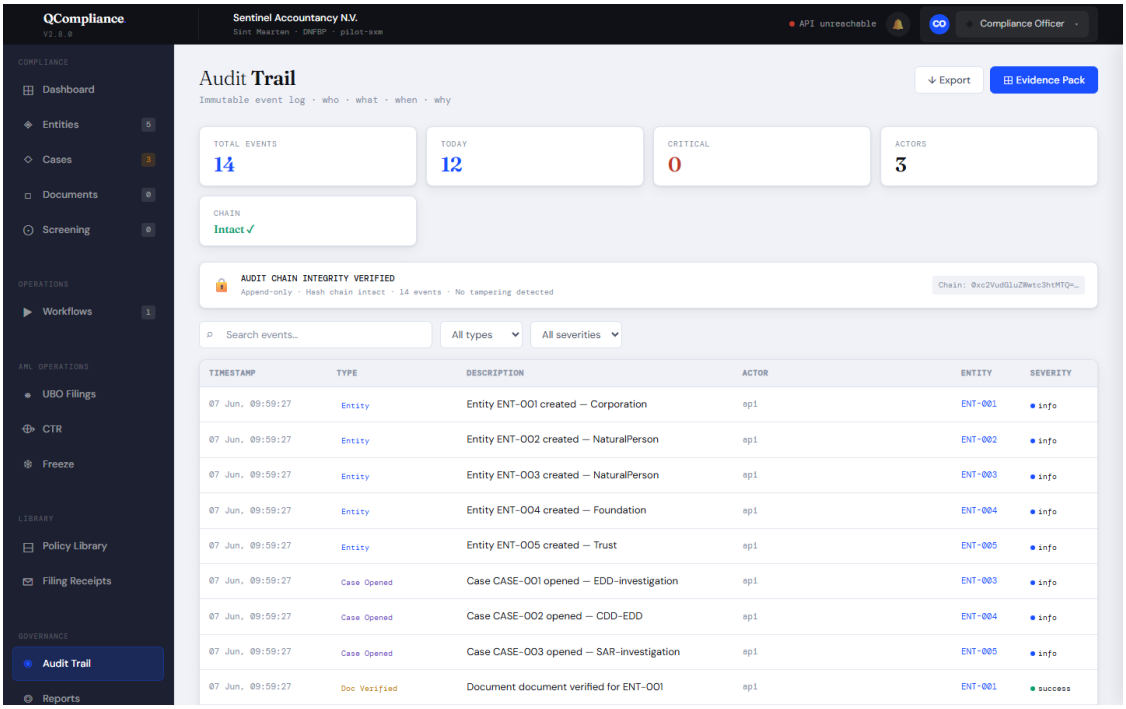
Step 2 — Open ENT-005

The detail panel summarises the periodic-review subject:



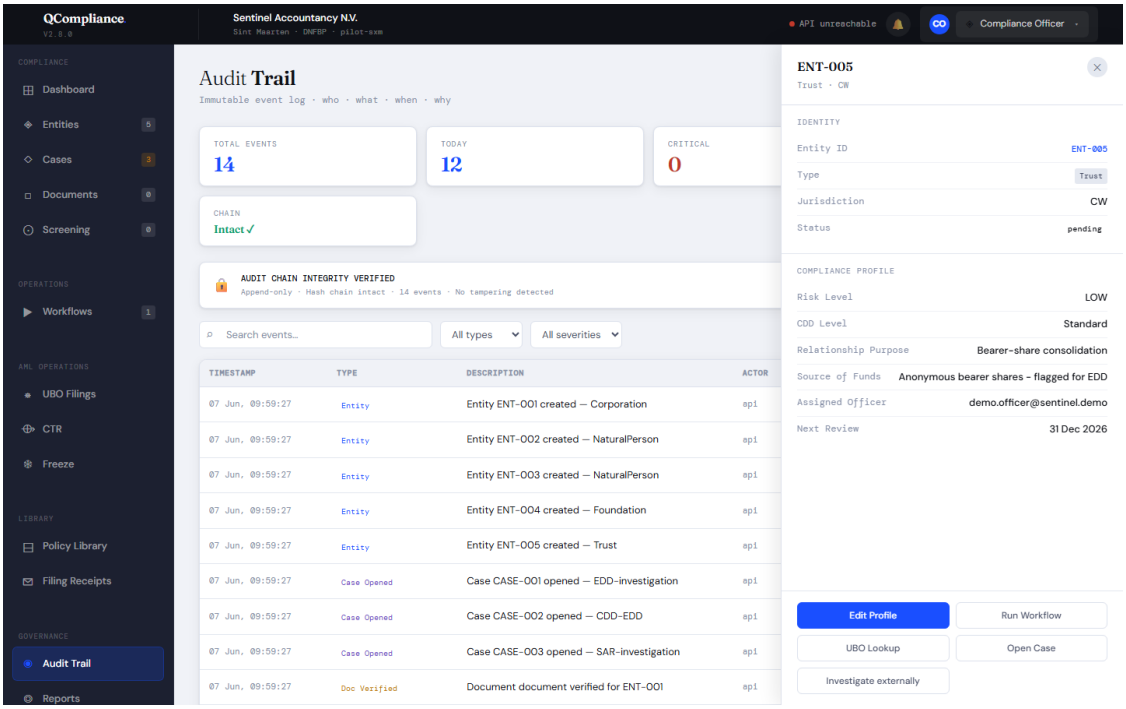
Step 3 — Filter the audit trail to ENT-005

Audit Trail → search box → “ENT-005”. You see every action ever taken against this entity, sorted newest-first:



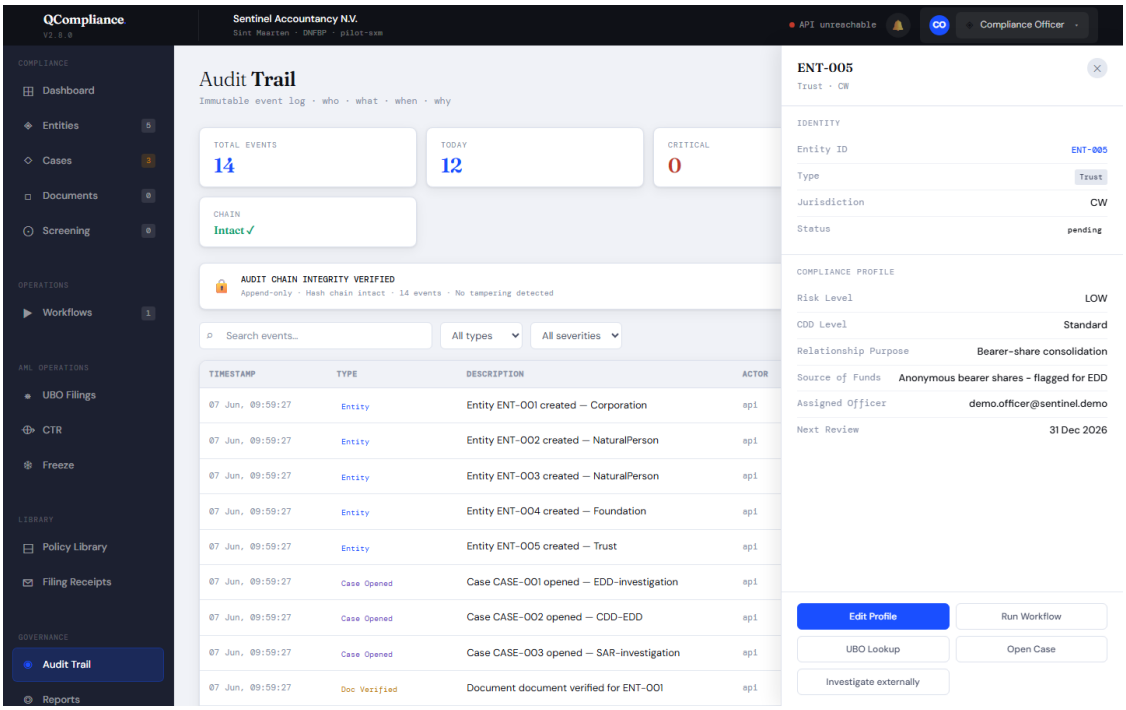
Step 4 — Locate the Evidence Pack button

Top-right of the Audit Trail page. **Evidence Pack** (with a small grid icon).



Step 5 — Generate the pack

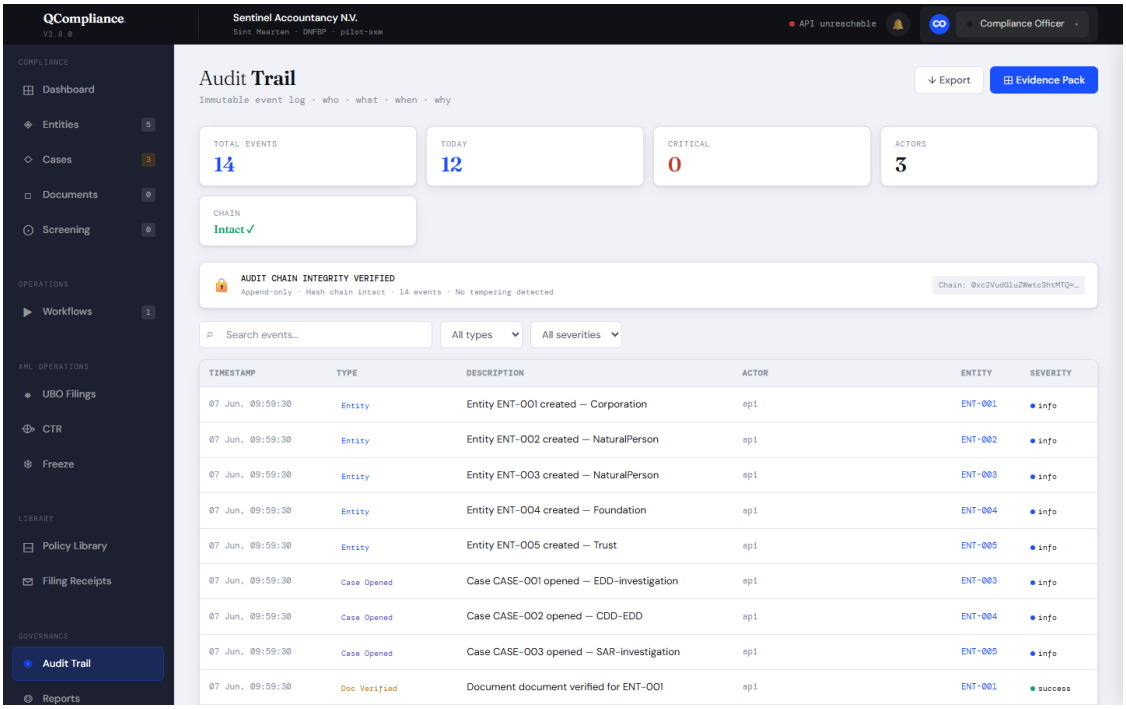
Click **Evidence Pack**. A toast appears confirming the pack was generated:



What the SPA does client-side is download a JSON snapshot. The **regulator-grade ZIP** is produced by the backend endpoint `/entities/{eid}/evidence-bundle` — call it from the entity detail panel's **Evidence Bundle** button, or fetch it via the API.

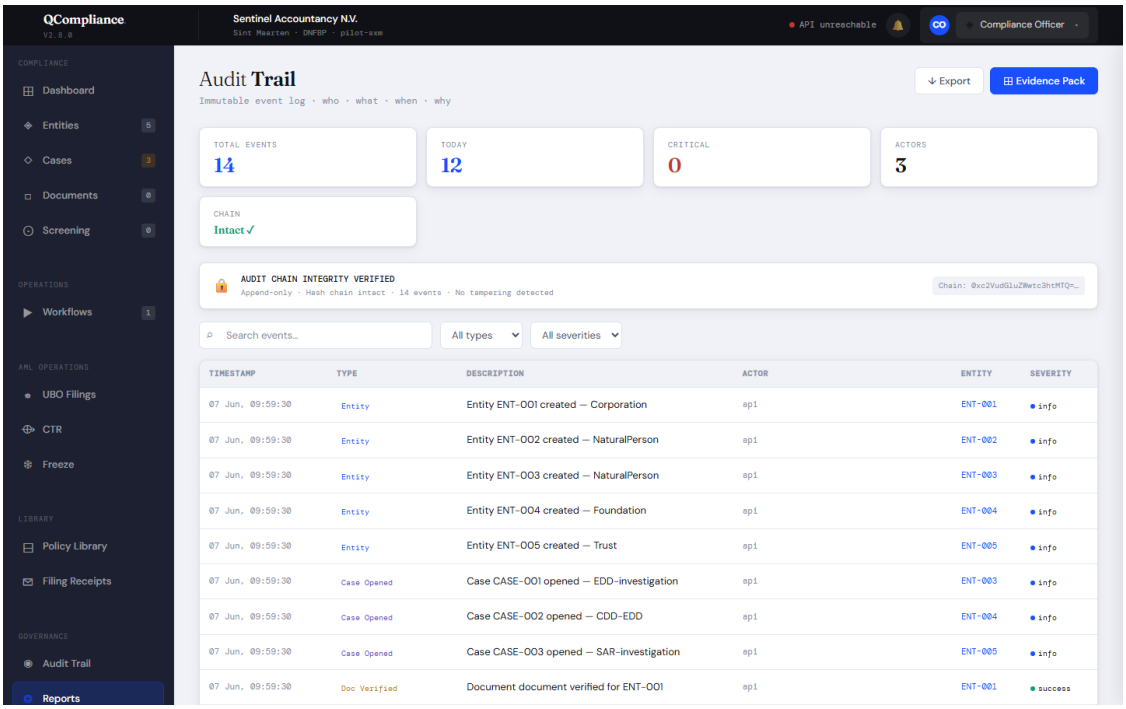
Step 6 — Export the audit JSON only

If the inspector only wants the audit chain (not the documents), click **Export** instead. You get a single JSON file ready to attach to an email:



Step 7 — Reports

The Reports page is the firm's compliance posture snapshot you can print or hand to a managing partner during a review:



The Evidence Bundle ZIP — what's actually inside

The ZIP for ENT-003 (saved as `docs/print/artifacts/evidence_bundle_ENT-003.zip`) contains six files. Here is the actual manifest, verbatim:


```
{
  "schema":       "qkyc.evidence_bundle.v1",
  "entityId":     "ENT-003",
  "bundleId":     "EVB-ENT-003-1778896993",
  "generatedAt": "2026-05-16T02:03:13+00:00",
  "generatedBy": { "actorId": "compliance.officer@4mfesw.nl",
                   "role": "compliance_officer" },
  "tenant":       "TENANT-4MFESW",
  "regulatoryBasis": [
    "FATF Recommendations 10/12/20/22",
    "Wwft (NL/SX) - Anti-Money Laundering and Anti-Terrorism Financing Act",
    "CBCS AML/CFT Provisions and Guidelines for DNFBPs"
  ],
  "intendedRecipient": "Authorised inspector / FIU desk. ...",
  "contents": [
    { "path": "entity.json",         "kind": "entity_profile",  "sha256": "d3
2fcc..." },
    { "path": "audit_excerpt.json",  "kind": "audit_trail",     "sha256": "d0
b510..." },
    { "path": "screenings.json",     "kind": "screening_runs",  "sha256": "e5
ec88..." },
    { "path": "ubo_lookups.json",    "kind": "ubo_lookups",     "sha256": "...
" },
    { "path": "cases.json",          "kind": "cases",           "sha256": "...
```

```
" }
  ]
}
```

Every content file has its **SHA-256** in the manifest. Any tampering with the bundle after generation is detectable by re-hashing the contents and comparing. The `regulatoryBasis` array is the firm's claim of which rules the bundle satisfies; the `intendedRecipient` prose is the receiving inspector's onboarding context.

When ENT-003 has document binaries on file, the ZIP also includes the verbatim PDFs/images under `documents/<doc-id>_<original_filename>` alongside their `documents/<doc-id>.meta.json` companion files.

> **§4 take-aways** - The Evidence Bundle is one ZIP, deterministically named, hashed, signed by the running system at the moment of export. - The audit chain is the bundle's spine — everything else (documents, screenings, UBO) is the evidence the audit chain points at. - You do not need to remember to include anything. The endpoint includes everything for that entity automatically.

---

§5 The audit chain in detail

Every operator action goes through `app/services/audit_service.py:log_event()`. The function writes a row to `audit_events` with:

- `event_id` — UUID
- `actor` — operator email (or `system` for automated events)
- `event_type` — one of ~40 known types (`entity_upserted`, `case_opened`, `case_escalated_to_mlro`, `mlro_review_approved`, `tipoff_lock_applied`, `screening_run`, `ubo_lookup`, `document_intake`, `sar_draft_exported`, `evidence_bundle_exported`, `user_login`, `periodic_review_due`, …)
- `entity_id` / `case_id` — optional scope
- `payload_json` — the full structured detail of the event (event-specific)
- `created_at` — set by the DB at insert time

The full chain is **append-only** at the SQL level — there is no UPDATE or DELETE on `audit_events` exposed via the API. The chain hash you see on the Audit Trail page (e.g. `0xc2VudGluZWwtc3htMTc=…`) is the inspector's tamper-evidence stamp.

Excerpt of the live ENT-003 audit (saved as `docs/print/artifacts/audit_excerpt_ENT-003.json`):

```
{
  "schema":      "qkyc.audit_excerpt.v1",
  "scope":       { "entityId": "ENT-003" },
  "eventCount":  6,
```

```
  "events": [
    {
      "eventType": "tipoff_lock_applied",
      "ts":        "2026-05-14T15:01:27+02:00",
      "actor":     "mlro@4mfesw.nl",
      "entityId":  "ENT-003",
      "payload":   { "regulation": "Wwft art. 23",
                     "reason": "Active SAR draft pending MOT filing" }
    },
    {
      "eventType": "case_escalated_to_mlro",
      "actor":     "compliance.officer@4mfesw.nl",
      "entityId":  "ENT-003",
      "payload":   { "caseId": "CASE-2026-001",
                     "reason": "Sanctions hit (2 lists)" }
    },
    { "eventType": "screening_run", "actor": "compliance.officer@4mfesw.nl",
      "payload":   { "screeningId": "SCR-2026-0001", "status": "hit",
                     "matchCount": 2 } },
    { "eventType": "entity_upserted", "actor": "compliance.officer@4mfesw.nl",
      "payload":   { "entityId": "ENT-003", "riskLevel": "high" } }
  ]
}
```


---

§6 Roles, permissions, MLRO authority

Role	What they can do	What they cannot do
super_admin	Everything across all tenants. Create / disable users. Read every case. Configure connectors.	Be the MLRO for legal accountability purposes — that's a real human with a name.
tenant_admin	Everything within their tenant. Create users, configure connectors, view all cases.	Approve a SAR draft (the MLRO must do that).
mlro	Open / close cases. Approve or reject escalations. Authorise SAR drafts. Apply tip-off locks.	Edit the audit log.
compliance_officer	Open files, run screenings, intake documents, escalate to MLRO.	Approve MLRO reviews. Generate SAR drafts (until MLRO approves).
operator	View files, run screenings, intake documents.	Open cases, escalate, draft SARs.

Role	What they can do	What they cannot do
read_only	View everything within the tenant.	Anything that changes state.

Permissions are enforced **on the backend**. A compliance officer who finds a way to click the MLRO Approve button (browser dev tools, replay an old HTTP request, anything) will get a 403 from `/cases/{id}/mlro-approve` because the endpoint inspects the JWT role claim before acting.

---

§7 Connectors — what's mock today and what to wire

Out of the box, Q-KYC ships with deterministic stub connectors so the system is testable end-to-end without external accounts:

Connector	Mock today	Production candidates
Sanctions screening	`deterministic_local_sanctions` (OFAC SDN, EU consolidated, UN, UK HMT — all stubbed)	Refinitiv World-Check One, Dow Jones Risk & Compliance, ComplyAdvantage, OFAC/EU direct via signed API
PEP	`deterministic_local_pep`	Dow Jones PEP, World-Check PEP, OpenSanctions PEP
UBO Registry	`deterministic_local_ubo_registry`	KvK (NL), Companies House (UK), EU BO Register, Chamber of Commerce (SXM), BVI corporate registry
Document verification	*Not configured*	Onfido, Veriff, Sumsub, Jumio, IDnow
Adverse media	`deterministic_local_adverse_media`	Dow Jones Adverse Media, LexisNexis, Factiva

Configure each under **Settings → Connectors → [name] → Configure**. The connector test endpoint sends a known query and validates the response shape before saving credentials. The dashboard's Provider Status panel reflects the live state.

> **The "Mock providers active" banner is a safety net.** By default Q-KYC ships with 9 government sources active out of the box, so the banner does not appear. It only fires if the baked-in real providers have been deliberately disabled — intended for testing scenarios where the operator wants the system in a known-mock state.

§8 Periodic reviews and ongoing CDD

FATF R.10 ongoing CDD says you can't just KYC once and forget. Q-KYC stores a `next_review_date` per entity:

- LOW risk → 24 months
- MEDIUM risk → 12 months
- HIGH risk → 3–6 months (configurable)

The Reviews Due page lists every entity overdue or within 30 days. Click into the entity, complete the re-verification (new screening run, refreshed UBO lookup, document expiry check), save the Review tab — the system writes a `periodic_review_completed` event and sets a new `next_review_date`.

ENT-005 in the demo is 4 days overdue specifically so this page is never empty.

---

§9 Troubleshooting / FAQ

Q: I logged in but the screens are all English even though I picked French / Dutch. The language picker at the bottom of the sidebar swaps the dictionary live; if a string is missing in your language Q-KYC falls back to English. Refresh the page once to clear cached strings.

Q: I clicked Save & Activate but the status didn't change. Save & Activate requires Risk Level, CDD Level, and at least one identification document on file (Wwft minimum). Open the Review tab and complete the missing fields — the toast tells you which.

Q: The MLRO approve button isn't showing for me. You're not the MLRO. Sign out and sign in as the MLRO account, or ask your tenant admin to grant you the `mlro` role.

Q: The "Mock providers active" banner won't go away. By default the 9 baked-in government sources are active and the banner does not appear. If you see it, the baked-in providers have been disabled in Settings → Connectors — re-enable `real_sanctions_local` and the banner clears.

Q: Can I delete an audit event? No. The API does not expose any DELETE or UPDATE on `audit_events`. If something is wrong, you create a new event that supersedes the wrong one, and both stay in the chain.

Q: How do I export everything on entity X for an inspector right now? Open ENT-X's detail panel → **Evidence Bundle**. You get a ZIP with manifest.json + audit_excerpt.json + entity.json + screenings.json + ubo_lookups.json + cases.json + documents/*. Hand the ZIP to the inspector.

Q: The SAR XML — is that what I file with MOT? No. It is a goAML 4.0-shaped DRAFT for the MLRO to transcribe. Real filing goes through the FIU's own portal. Q-KYC's job is to make the transcription mechanical, not to bypass the FIU's intake.

---

§10 Document security + mobile capture + regulator integration

These capabilities landed in v0.6.8 and v0.6.9. They sit BELOW the workflows you already learned in §1–§4 — you do not have to touch them to do your day job, but if a regulator audits you they are the proof that Q-KYC took due care of the files you handle.

§10.1 Antivirus scanning of every uploaded file

Every file that enters Q-KYC via `POST /documents/intake` (the **Add document** button in the Documents tab, the `/filing-receipts` upload, the policy library upload, and the mobile camera page) is streamed through **ClamAV** before it is written to disk.

- **Engine:** ClamAV (Cisco fork) v1.5+, running as a Windows service on `127.0.0.1:3310`.
- **Signatures:** ~3.6 million definitions, refreshed by freshclam.
- **Failure mode:** if clamd is unreachable, the scan status is recorded as `skipped` in `document_intake.metadata_json.av_scan` and the upload still goes through — graceful degradation.
- **Infection response:** an infected upload returns **HTTP 422**, the file is **never written to disk**, and the event `document_infected_rejected` is chained to the audit log with the signature name.

§10.2 Encryption at rest

Every file stored in `C:\ProgramData\Q-KYC\document_store\` is **Fernet-encrypted** with a per-installation key derived from `COCAI_JWT_SECRET` via HKDF-SHA256. The plaintext SHA-256 is stored separately in `document_intake.checksum_sha256`. On retrieval, the API decrypts, hashes, and compares — mismatch returns HTTP 409 and chains a `document_tamper_detected` event.

§10.3 Machine-readable zone (MRZ) parsing

When you upload a **passport, national ID, driving licence, residence permit, or identity document**, Q-KYC runs OCR (Tesseract) and feeds the text into an ICAO 9303 parser that extracts and check-digit-validates every field (`documentNumber`, `nationality`, `surname`, `givenNames`, `dateOfBirth`, `dateOfExpiry`, `personalNumber`, composite check). Findings land in `document_intake.metadata_json.mrz`; alerts surface inline in the Documents tab:

- `"document expired N day(s) ago"`
- `"document expires in N day(s)"` (for any expiry < 90 days)

- `"MRZ composite check digit FAILED"` (OCR error or tampering)

§10.4 Mobile camera capture (QR-to-phone)

In the Documents tab inside the entity profile editor, click **Mobile upload** (📱 icon). Q-KYC mints a one-time 30-minute token, renders a QR code; the client scans it on their phone, the phone opens a mobile-optimised page with **Take photo** (`capture="environment"`) or **Choose from device**, then POSTs to `/mobile-upload/intake` with the token. Same AV scan, same Fernet encryption, same MRZ parsing as desktop. The file appears in your Documents tab within seconds.

§10.5 Regulator integration modes

Three modes per regulator under **Settings → Integration mode**:

Mode	What it means	When to choose
Manual	Operator downloads artifact, uploads to regulator portal, uploads receipt back.	Default for KvK SXM, FIU MOT, CBCS today (they do not publish programmatic intakes).
Push	Q-KYC POSTs to the regulator endpoint when the MLRO clicks submit.	Set `COCAI_KVK_ENDPOINT_URL` / `COCAI_FIU_GOAML_*` / `COCAI_CBCS_ENDPOINT_URL` once the regulator gives you one.
Pull	Q-KYC exposes `/regulator-api/v1/*` for the regulator to poll. Every read is logged to the **AVG/GDPR Art. 30 register**.	Available now; mint per-regulator bearer tokens under **Settings → Regulator pull tokens**.

Pull endpoints exposed today:

```
GET /regulator-api/v1/entities
GET /regulator-api/v1/entities/{id}/profile
GET /regulator-api/v1/cases?status=open
GET /regulator-api/v1/sars
GET /regulator-api/v1/audit?from=...&to=...
GET /regulator-api/v1/policies
```

Every call inserts a row into `regulator_api_access_log` (the AVG Art. 30 register) AND an event into `audit_events`.

§10.6 Multi-national subject flag

When you select a second nationality in the Identity tab's **Additional Nationality** dropdown, Q-KYC bumps risk to **medium** (if Low/empty), appends an auto-note to Risk Notes, and fires a warn toast — implementing FATF R.10 multi-jurisdictional scrutiny. The override remains possible; the auto-note is preserved.

---

§11 Glossary

Term	Meaning
CBCS	Central Bank of Curaçao and Sint Maarten — issues AML/CFT guidance for DNFBPs in SXM.
CDD	Customer Due Diligence — the FATF R.10 process of identifying, verifying, and risk-assessing a client.
DNFBP	Designated Non-Financial Business or Profession — accountants, tax advisors, lawyers, real-estate brokers etc. who are subject to AML/CFT obligations.
EDD	Enhanced Due Diligence — extra scrutiny for high-risk subjects (PEPs, opaque structures, high-risk jurisdictions).
FATF	Financial Action Task Force — the international AML/CFT standard-setter.
FIU	Financial Intelligence Unit — the national authority that receives SARs (MOT for Sint Maarten/Curaçao, FIU-NL for the Netherlands, TRACFIN for France, SEPBLAC for Spain).
goAML	The UNODC's XML schema for SAR/STR reporting. Most FIUs accept goAML; some have their own variants.
KYC	Know Your Client / Customer — the upfront onboarding identification and verification step.
MLRO	Money Laundering Reporting Officer — the human inside the firm legally accountable for SAR decisions.
MOT	Meldpunt Ongebruikelijke Transacties — the

Term	Meaning
	FIU for the Dutch Caribbean (Sint Maarten + Curaçao).
PEP	Politically Exposed Person — heightened AML risk per FATF R.12.
SAR / STR	Suspicious Activity / Transaction Report — the formal filing to the FIU.
Tip-off	Communicating to the subject (directly or indirectly) that they are under SAR investigation — a criminal offence under Wwft art. 23.
UBO	Ultimate Beneficial Owner — the natural person who ultimately owns or controls a legal entity (≥25% threshold under most regimes).
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme — the Dutch AML/CFT law that applies to NL and (with local adaptation) to SXM.

End of manual. Edition 2026-05. · © 4Mfesw — all rights reserved.