Q-KYC SXM

Operator-handleiding

Versie 0.6.14 · Editie 2026-06-03

Geïmplementeerd bij: **the Tenant Firm** · Sint Maarten

Ontwikkeld en onderhouden door: **4Mfesw** *Modern, Methods Made and Maintained · Fiber, Software, WorkFlows, Energy* Sint Maarten

---

Documentclassificatie

`VERTROUWELIJK — BEPERKT`

Deze handleiding bevat operationele details van een AML/CFT-systeem. Uitsluitend verspreiden onder:

- Personeel met toegewezen compliance-rollen binnen de implementerende firma
- CBCS / FIU MOT-toezichthouders tijdens geplande inspecties
- De door de firma aangestelde externe auditor onder opdrachtovereenkomst

Niet voor openbare verspreiding.

Auteursrecht

© 2026 4Mfesw. Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen of openbaar gemaakt in enige vorm of op enige wijze zonder voorafgaande schriftelijke toestemming van 4Mfesw, met uitzondering van korte citaten in kritische besprekingen en bepaalde andere niet-commerciële vormen van gebruik toegestaan door het auteursrecht.

Documentbeheer

Veld	Waarde
Titel	Q-KYC SXM Operator-handleiding
Eigenaar	4Mfesw
Goedkeurder	_____
Uitgegeven	2026-06-03
Volgende review	2026-12-03 (of eerder bij materiële wijziging)
Versie	v0.6.14
Bron van waarheid	`docs/USER_MANUAL.md` (Engels)
Vertalingen	NL, FR, ES — verifieer tegen de Engelse

Veld	Waarde
	editie vóór toezichthoudergebruik

Hoe deze handleiding te lezen

Dit is een **taakboek**. Het leert u de vier taken die Q-KYC bestaat om uit te voeren, in de volgorde waarin u ze op echte klantdossiers zult uitvoeren:

	Doorlopen	Onderwerp van het doorlopen
§1	**KYC-onboarding** — open een nieuw klantdossier van begin tot eind	ENT-001 Maria Velasquez (inwoner SXM, laag risico)
§2	**AML-escalatie + SAR** — wat gebeurt er bij een screening-hit	ENT-003 Roman Voloshyn → CASE-2026-001
§3	**UBO-verklaring + registeruittreksel** — uiteindelijk-belanghebbenden bij ondoorzichtige structuren	ENT-004 Coral Holdings Ltd. (BVI Trust)
§4	**Bewijspakket** — wat u de inspecteur overhandigt wanneer hij om 16:00 mailt	ENT-005 Domino Marine Services BV (NL)

Elke doorlopen heeft genummerde stappen. Elke stap heeft één schermafbeelding. De rode cirkel op de schermafbeelding is wat u vervolgens aanklikt. Lees de tekst, klik wat de cirkel toont, ga verder.

De doorlopen gebruiken de **meegeleverde demonstratiegegevens**. Vóór uw eerste echte klant moet uw tenant-beheerder:

1. **Bevestig uw screening-connectoren** onder **Instellingen → Connectoren**. De 9 ingebouwde overheidsbronnen (OFAC SDN + Consolidated, VN, EU, UK HMT OFSI, Canada Justice, Zwitserland SECO) zijn standaard actief — geen configuratie vereist. Optionele commerciële overlays (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage) hebben hun eigen abonnement + API-sleutel nodig; voeg die toe via Instellingen → Connectoren alleen als uw tier of use-case dat vereist.
2. Operator-accounts aanmaken onder **Instellingen → Gebruikers** (of `scripts/create_superadmin.py` één keer op de server uitvoeren).
3. Een sterk `COCAI_JWT_SECRET` instellen vóór elke pilot-uitrol.

Daarna dezelfde schermen, dezelfde knoppen, dezelfde audit-keten — maar met echte lijstversies en echte registerrijen eronder.

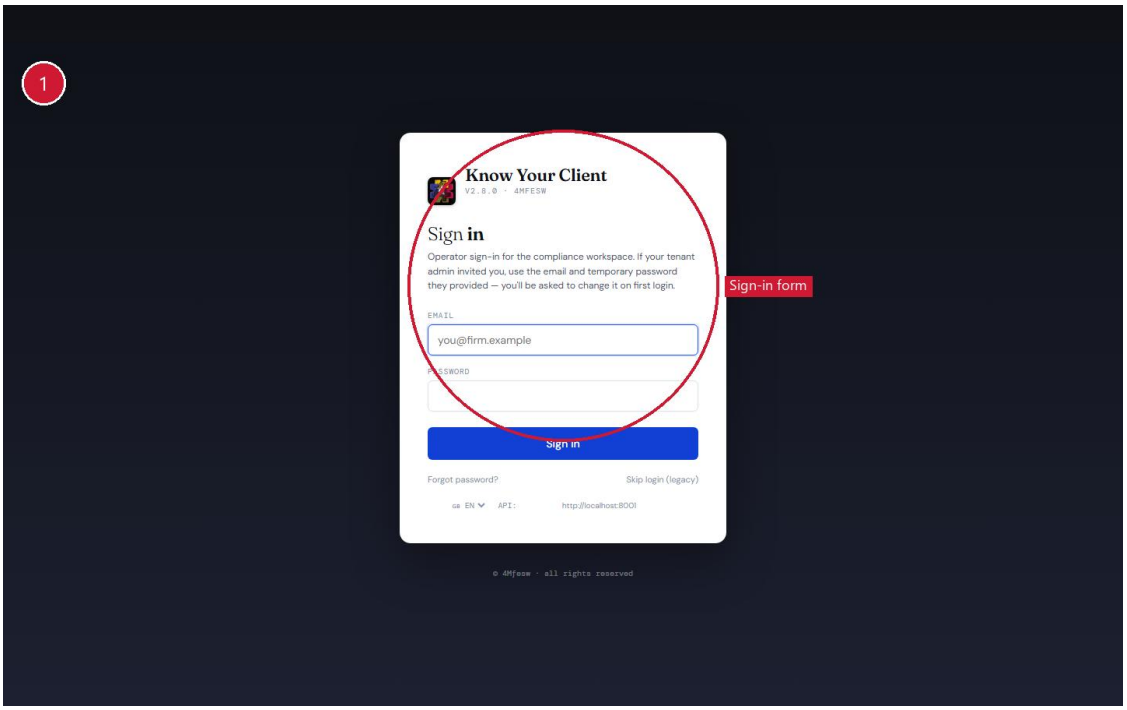
> **Wat Q-KYC NIET doet.** Het dient geen SAR's bij de FIU voor u in. Het haalt 9 officiële overheidsbronnen voor sancties dagelijks rechtstreeks op van de publicatie-URL's — OFAC SDN + Consolidated, VN, EU, UK HMT OFSI, Canada Justice, Zwitserland SECO. Commerciële PEP- / adverse-media-overlays (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage) zijn optioneel en door de klant aan te leveren via **Instellingen → Connectoren**. Het certificeert geen documenten. Het geeft u geen vrijbrief onder FATF / Wwft / DNFBP / CBCS — uw MLRO blijft de verantwoordelijke persoon voor de toezichthouder. Wat Q-KYC wél doet is het werk *eerlijk* vastleggen in een onveranderlijke, hash-geketende audit-trail, zodat wanneer de inspecteur komt u één bundel kunt overhandigen en elke handeling kunt aantonen.

---

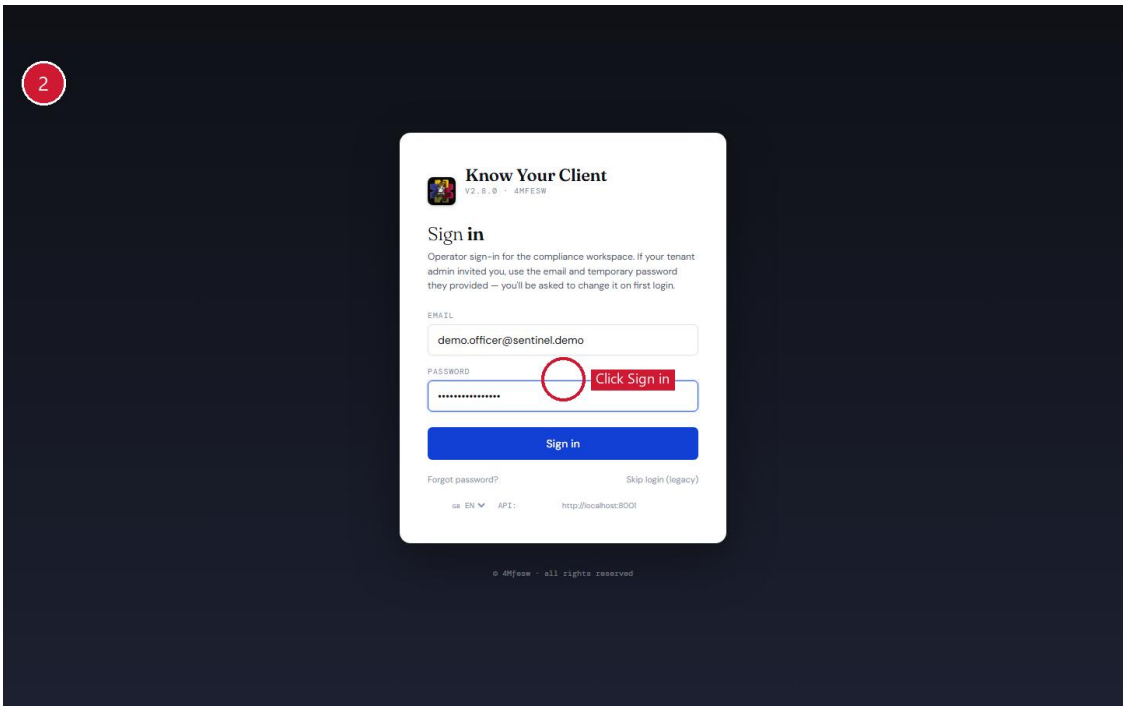
§0 Eerste aanmelding (5 minuten)

Uw tenant-beheerder zal een account voor u hebben aangemaakt en een tijdelijk wachtwoord per e-mail hebben gestuurd. U wordt gevraagd dit bij de eerste aanmelding te wijzigen.

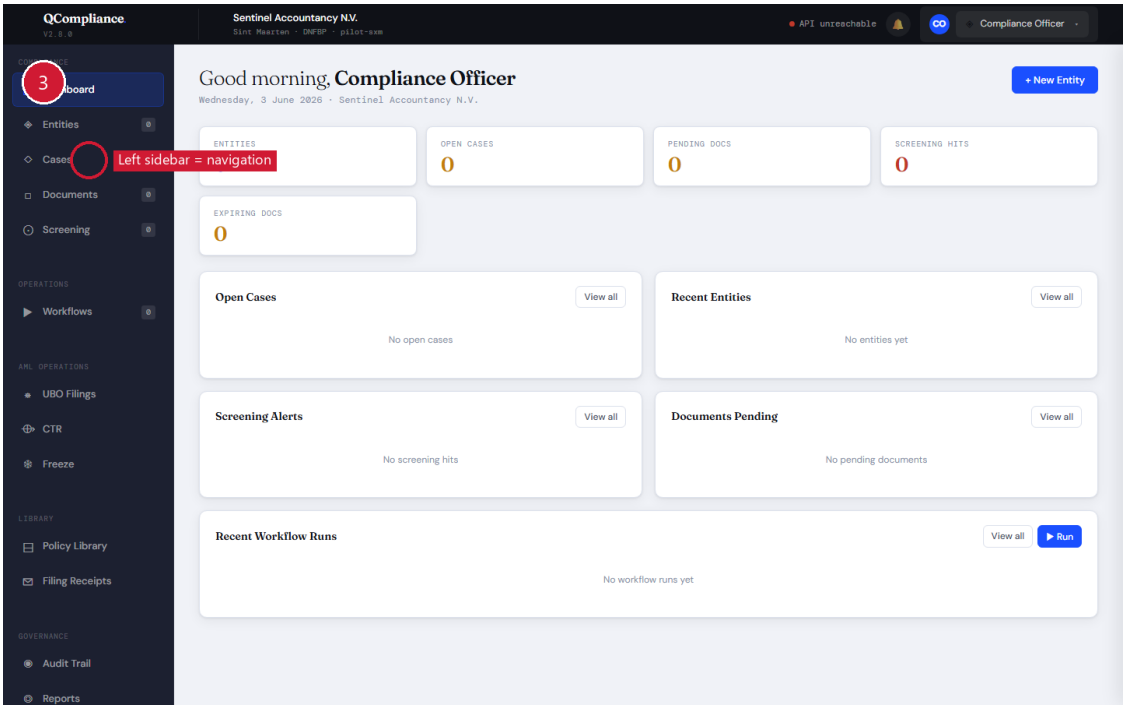
1. Open de URL die uw beheerder u gaf (tijdens de pilot: `http://localhost:8001`).
2. U ziet dit:



3. Typ uw e-mailadres en het tijdelijke wachtwoord. De Aanmelden-knop wordt actief zodra beide velden zijn ingevuld.



1. Na aanmelding komt u op het **Dashboard**:



De vijf tegels bovenaan tonen de compliance-toestand van uw firma in één oogopslag: **Entiteiten**, **Open dossiers**, **Documenten in behandeling**, **Screening-**

treffers, **Verlopende documenten**. Het Provider-statuspaneel daaronder toont welke screening-connectoren actief zijn — standaard de 9 ingebouwde overheidsbronnen (OFAC SDN + Consolidated, VN, EU, UK HMT OFSI, Canada Justice, Zwitserland SECO) plus eventuele door de klant aangeleverde commerciële overlays (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage). De gele banner *"Mock-providers actief"* is een vangnet dat alleen verschijnt als alle echte providers zijn uitgeschakeld.

2. De linker **zijbalk is uw enige navigatie**:
    - **Compliance** — Dashboard, Entiteiten, Dossiers, Documenten, Screening
    - **Operatie** — Werkprocessen
    - **Bestuur** — Audit-spoor, Herzieningen, Rapporten
    - **Systeem** — Instellingen, Gebruikershandleiding

Dat is het. Kies nu een doorlopen.

---

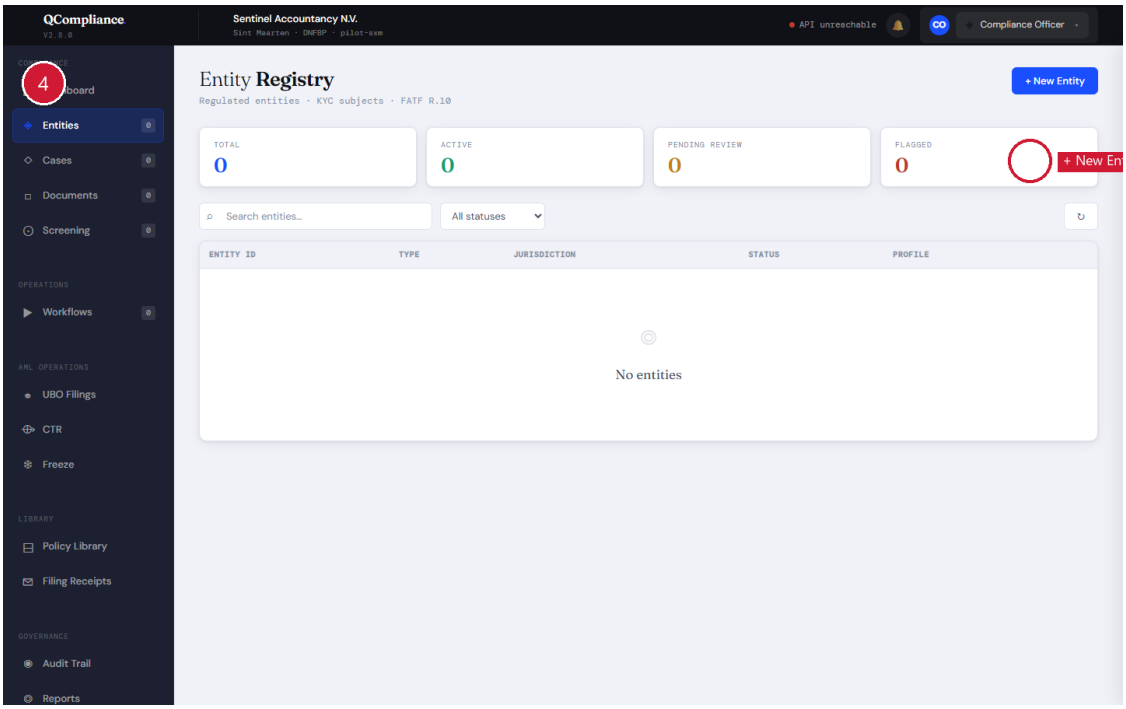
§1 KYC-onboarding (Doorlopen 1)

Doel: open een nieuw klantdossier van begin tot eind, met ten minste één identiteitsdocument geregistreerd, een expliciete risico-classificatie, en een periodieke-herzieningsdatum gezet — alles wat een inspecteur als bewijs zal vragen dat u CDD heeft gedaan vóór aanvang van de relatie (FATF R.10 / Wwft art. 3 / CBCS AML/CFT §4.1).

Onderwerp: ENT-001 Maria Velasquez — inwoner SXM, in loondienst, geen PEP-blootstelling, laagrisico-classificatie.

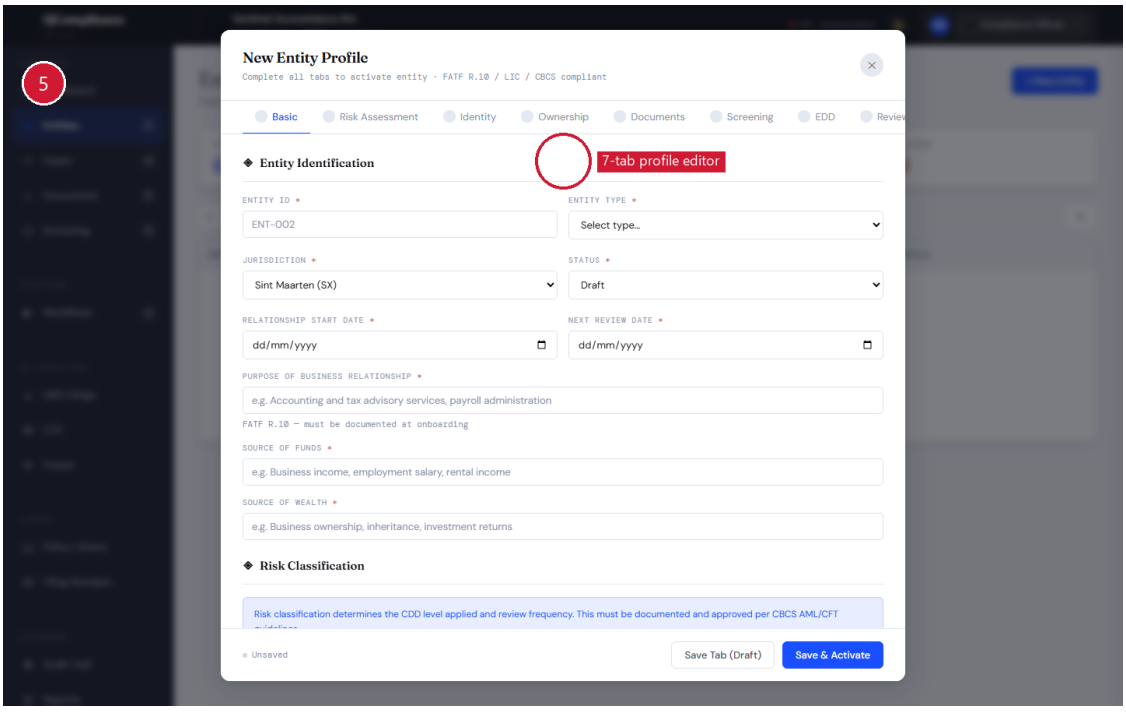
Stap 1 — Open het Entiteitenregister

Klik **Entiteiten** in de zijbalk. U ziet elke gereguleerde partij die uw firma in dossier heeft, met type, jurisdictie, huidige status en CDD-volledigheid. Nieuw dossier? Klik **+ Nieuwe entiteit** rechtsboven.



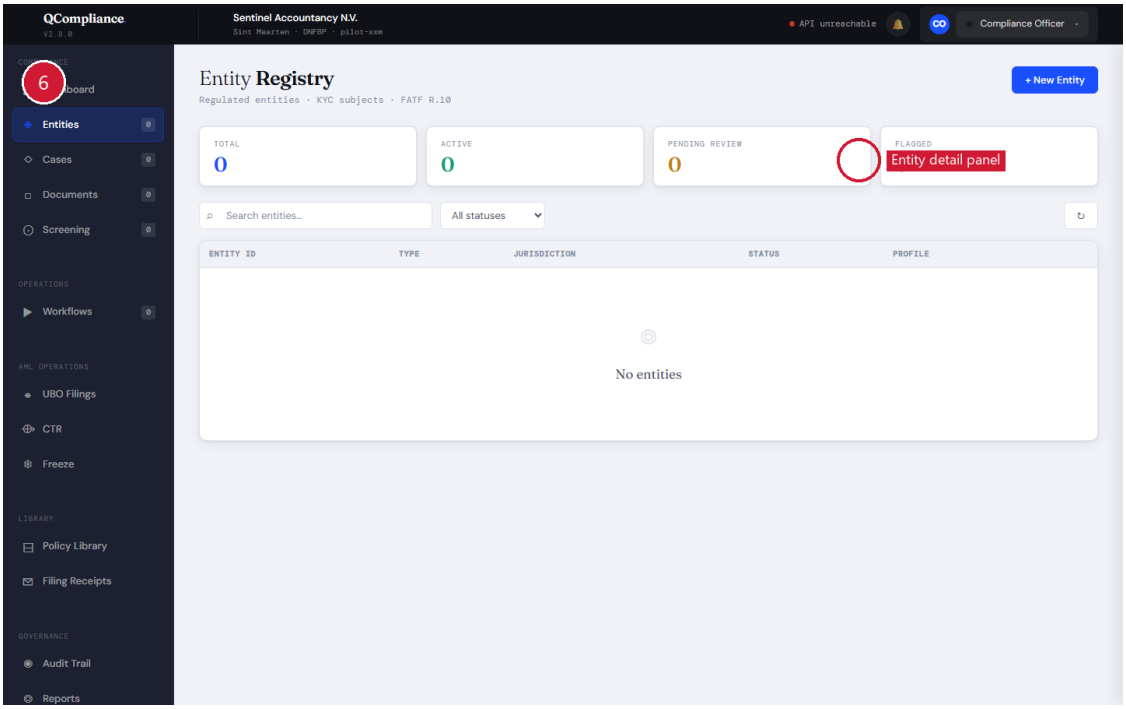
Stap 2 — Open de profieleditor

De profieleditor is de plek waar u *alles* over een klant vastlegt. Zeven tabbladen (Basis, Identiteit, Eigendom, Documenten, Screening, EDD, Herziening) en de **Tabblad opslaan** / **Opslaan & activeren** knoppen onderaan.



Stap 3 — Kies een bestaande entiteit om te bestuderen

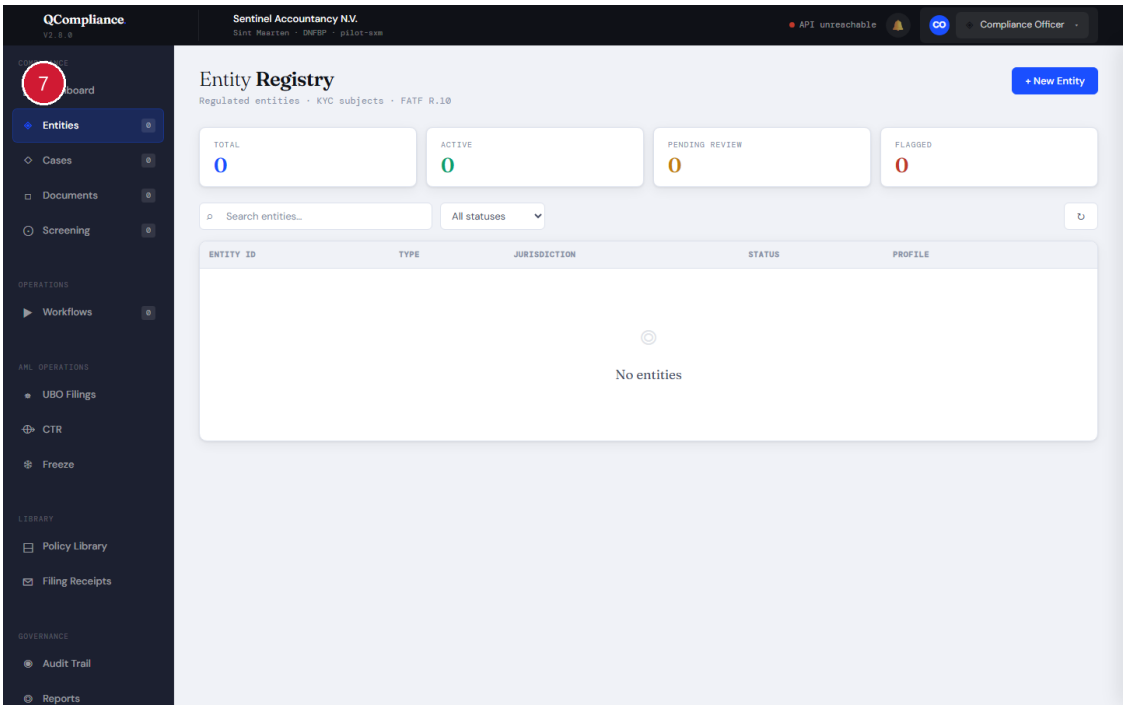
Voor deze doorlopen openen we het demo-onderwerp ENT-001 (Maria Velasquez). Klik op de regel, het rechter detailpaneel schuift in:



Het detailpaneel vat samen **wie** (Entity ID, Type, Jurisdictie, Status, Tipoff-vergrendelingsstatus) en **wat** (Risiconiveau, CDD-niveau, Doel relatie, Bron van middelen, Toegewezen functionaris, Volgende herzieningsdatum). Actieknoppen onderaan: **Profiel bewerken**, **Werkproces uitvoeren**, **UBO-opzoeking**, **Dossier openen**, **Bewijspakket**, **SAR opstellen** (de laatste twee verschijnen alleen wanneer van toepassing).

Stap 4 — Tabblad Basis: wie zij zijn

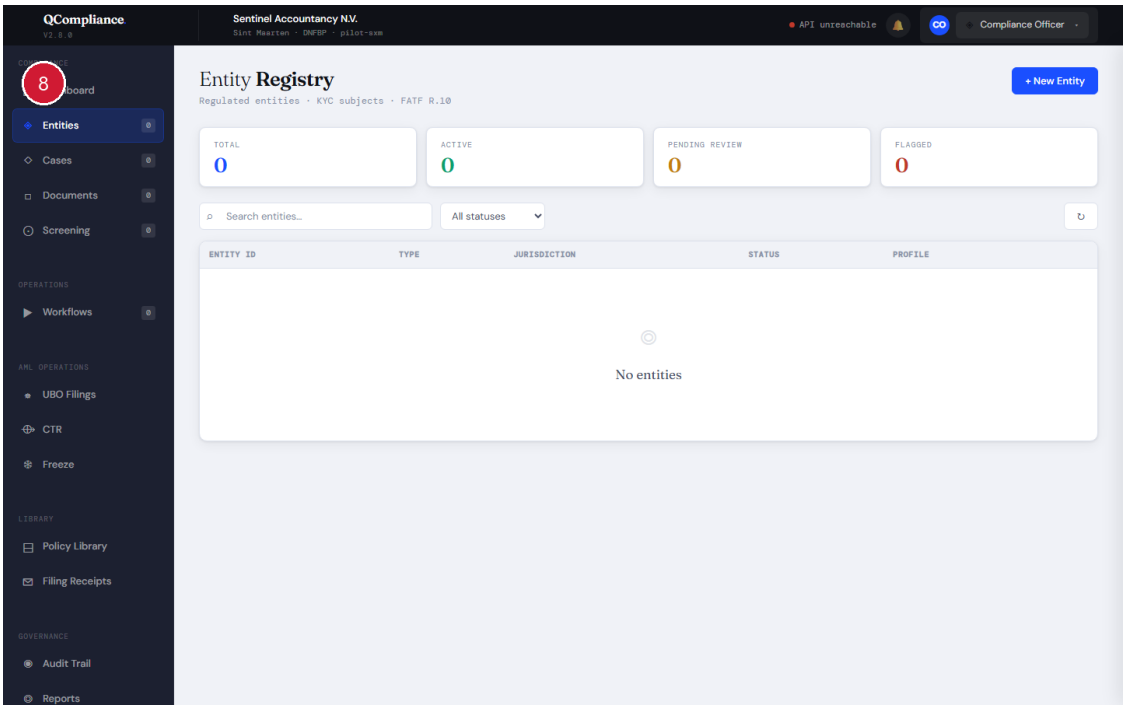
Klik **Profiel bewerken** om de zeven-tabs-editor te openen.



Dit is FATF R.10-gebied: - **Entity ID / Type** — interne handle + NaturalPerson / LegalEntity / Trust / Foundation / VASP / DNFBP enz. - **Jurisdictie / Status** — geregistreerde jurisdictie + draft / pending_review / active / blocked / frozen - **Relatie-startdatum / Volgende herziening** — wanneer CDD voltooid werd en wanneer het opnieuw moet - **Doel van de zakelijke relatie** — vereist door Wwft / DNFBP-regels - **Bron van middelen / Bron van vermogen** — vereist voor middel- en hoogrisico-onderwerpen

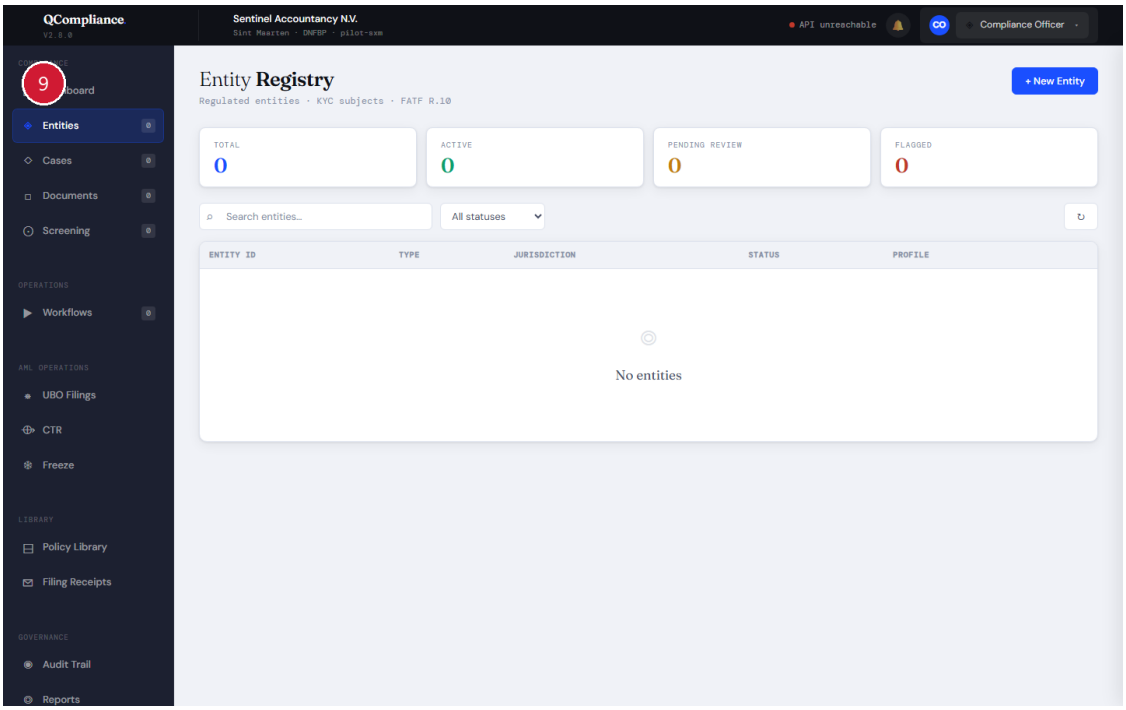
Stap 5 — Tabblad Identiteit: identiteitsdocumenten

Het tabblad Identiteit is waar u paspoort, ID-kaart, rijbewijs of elk ander identiteitsdocument vastlegt. Elke vermelding registreert: - Documenttype + nummer + uitgevend land - Uitgiftedatum + vervaldatum (Q-KYC waarschuwt wanneer vervaldatum binnen 90 dagen is) - Verificatiemethode (persoonlijk, video, op afstand) - Functionaris die heeft geverifieerd, wanneer



Stap 6 — Tabblad Documenten: bestandsuploads

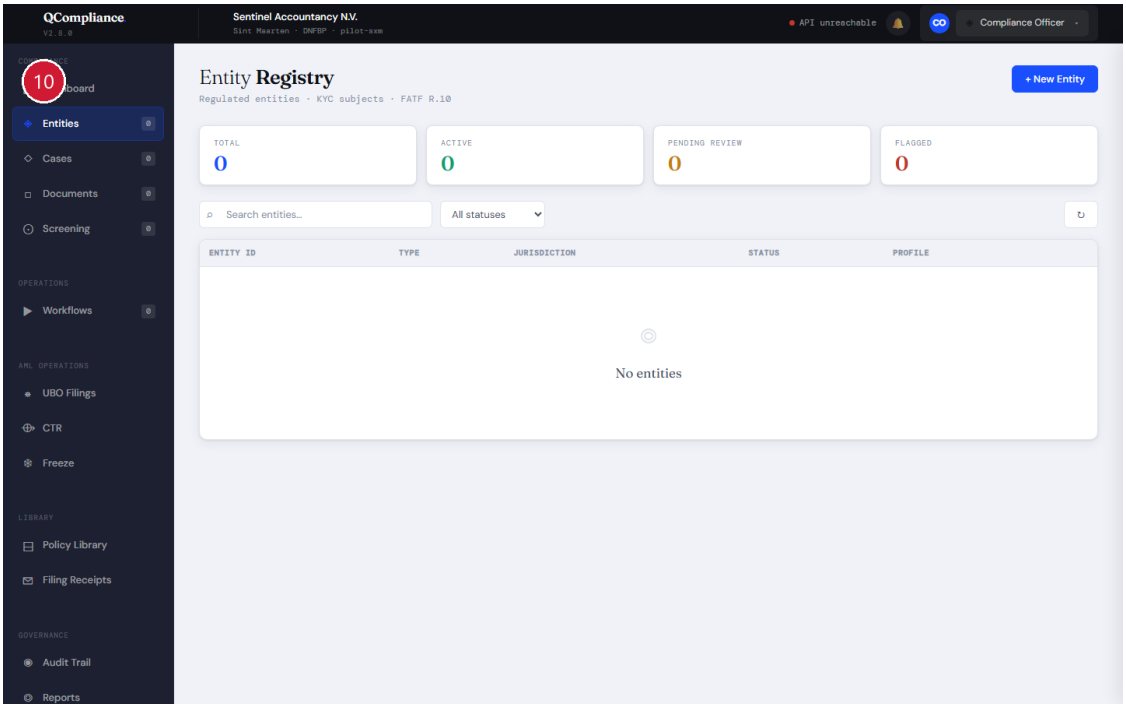
Waar het tabblad Identiteit de metadata vastlegt, is het tabblad Documenten de werkelijke bestandsopslag: pdf-scans, KvK-uittreksels, UBO-verklaringsformulieren. Elk geüpload bestand krijgt: - Een onveranderlijke SHA-256-checksum (zodat u later kunt aantonen dat het niet werd vervangen) - Een opgeslagen binair op de server (nooit overschreven) - Een `document_intake` audit-gebeurtenis met de operator, tijdstempel en documenttype



De blauwe infobox bovenaan — *“Alle identiteitsdocumenten moeten worden geverifieerd. Leg de documentreferentie, verificatiemethode en de functionaris die heeft geverifieerd vast.”* — is de FATF R.10-herinnering die u in de hele editor zult zien.

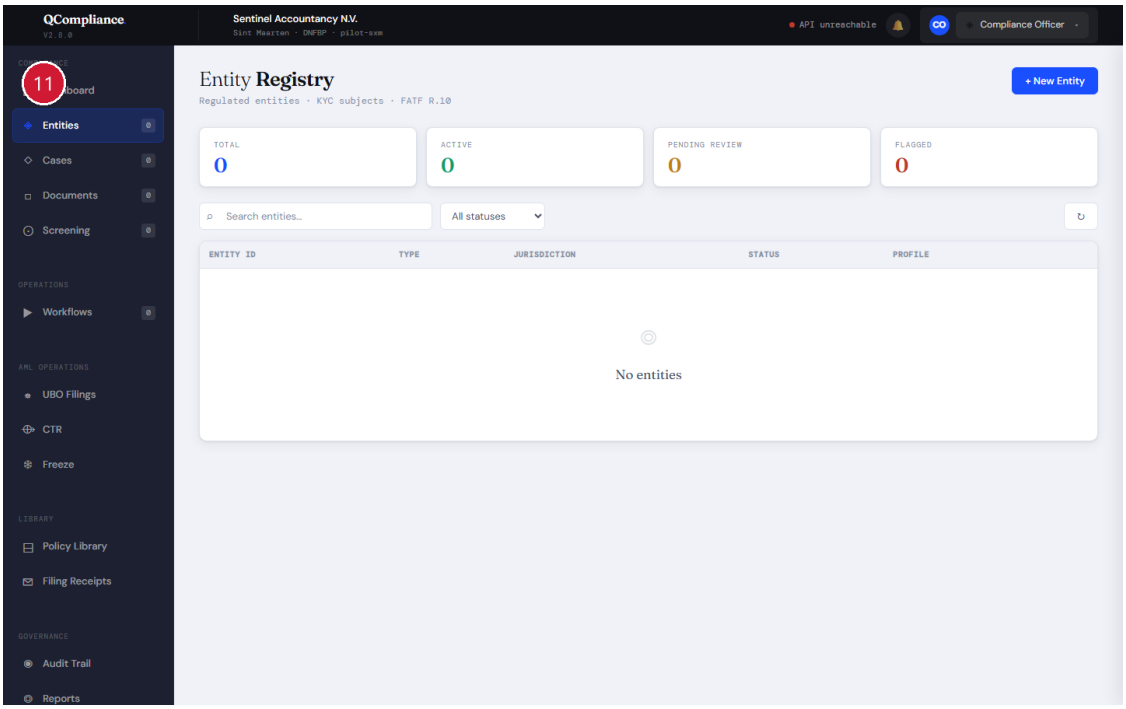
Stap 7 — Tabblad Screening: koppel de runs

Elke entiteit linkt naar elke screening-run die tegen hen is uitgevoerd. Zelfs runs van een jaar geleden staan hier nog, met de exacte lijstversies die op dat moment werden geraadpleegd (FATF R.10-herleidbaarheid).



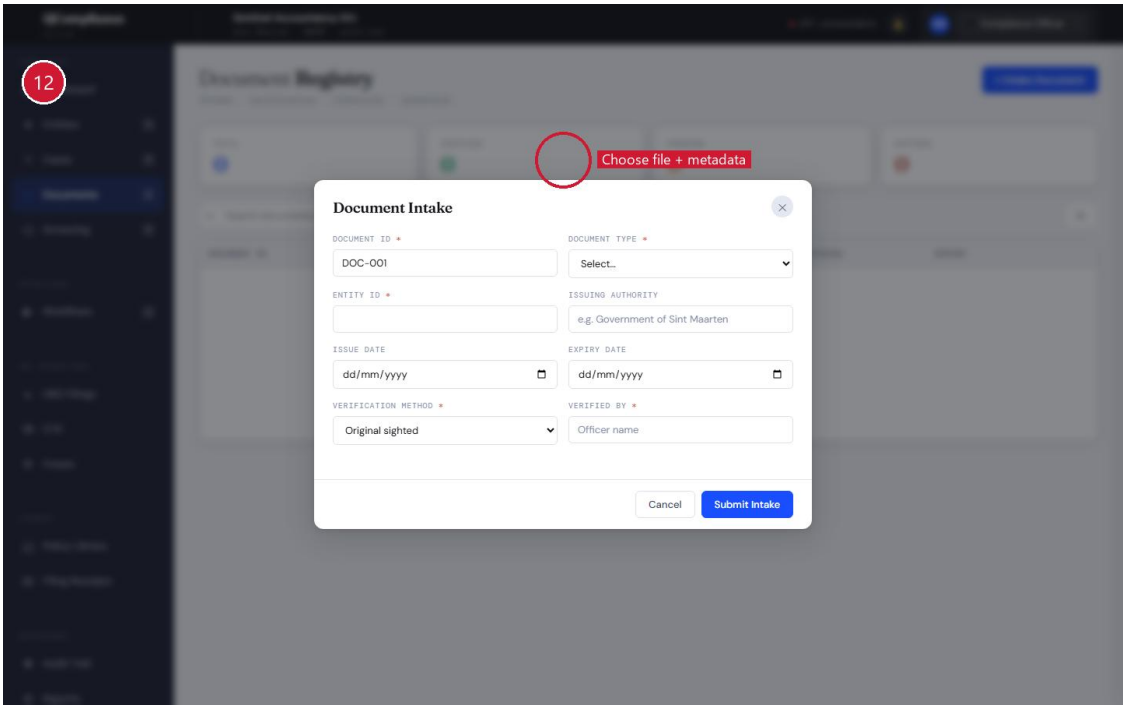
Stap 8 — Tabblad Herziening: risico + CDD-voltooiing

Het tabblad Herziening is de compliance-samenvatting van de operator: - **Risiconiveau** (LAAG / MIDDEL / HOOG) — stuurt het periodieke herzieningsinterval (24m / 12m / 3–6m standaard) - **Risicofactoren** — de bullets die u afvinkte tijdens beoordeling - **CDD-voltooiing** — datum, methode, functionaris - **Volgende periodieke herziening** — automatisch berekend uit risiconiveau, bewerkbaar



Stap 9 — Document intaken buiten de profieleditor

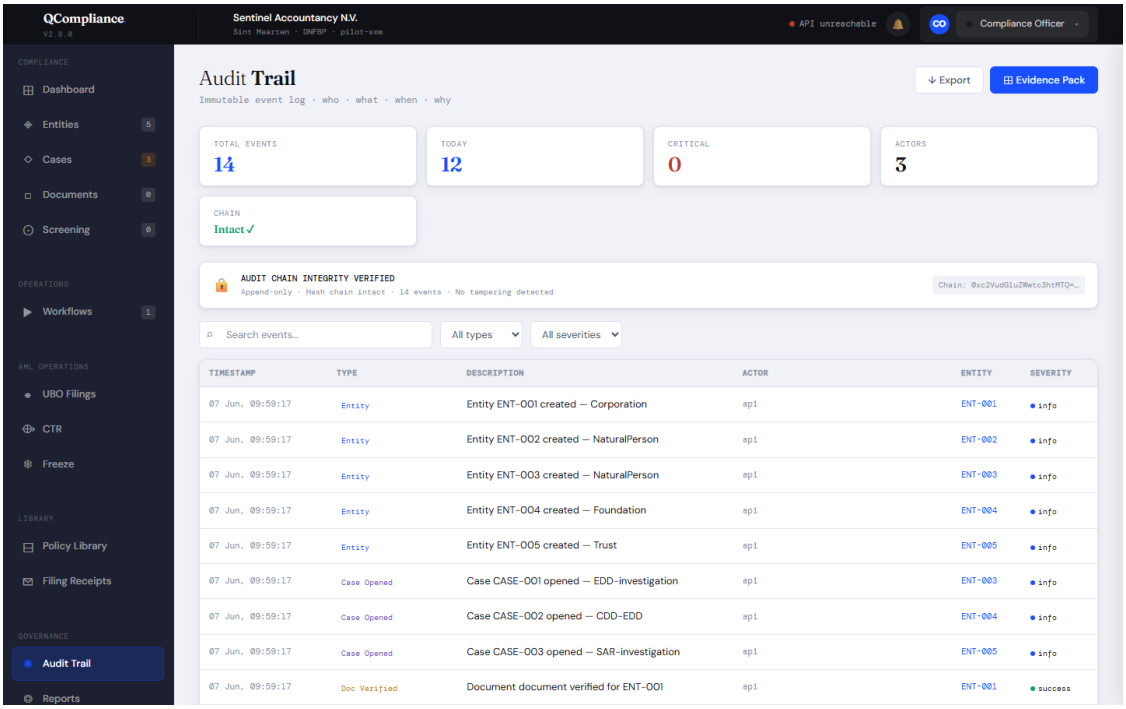
Soms ontvangt de operator een document per e-mail of gescande upload en wil dit registreren vóór hij het volledige profiel opent. Gebruik **Documenten → + Nieuwe intake**:



U kiest de entiteit, het documenttype, eventueel link aan een open dossier, en uploadt. Het systeem slaat het bestand op, berekent de checksum en schrijft een `document_intake` audit-gebeurtenis.

Stap 10 — Verifieer het onveranderlijke audit-spoor

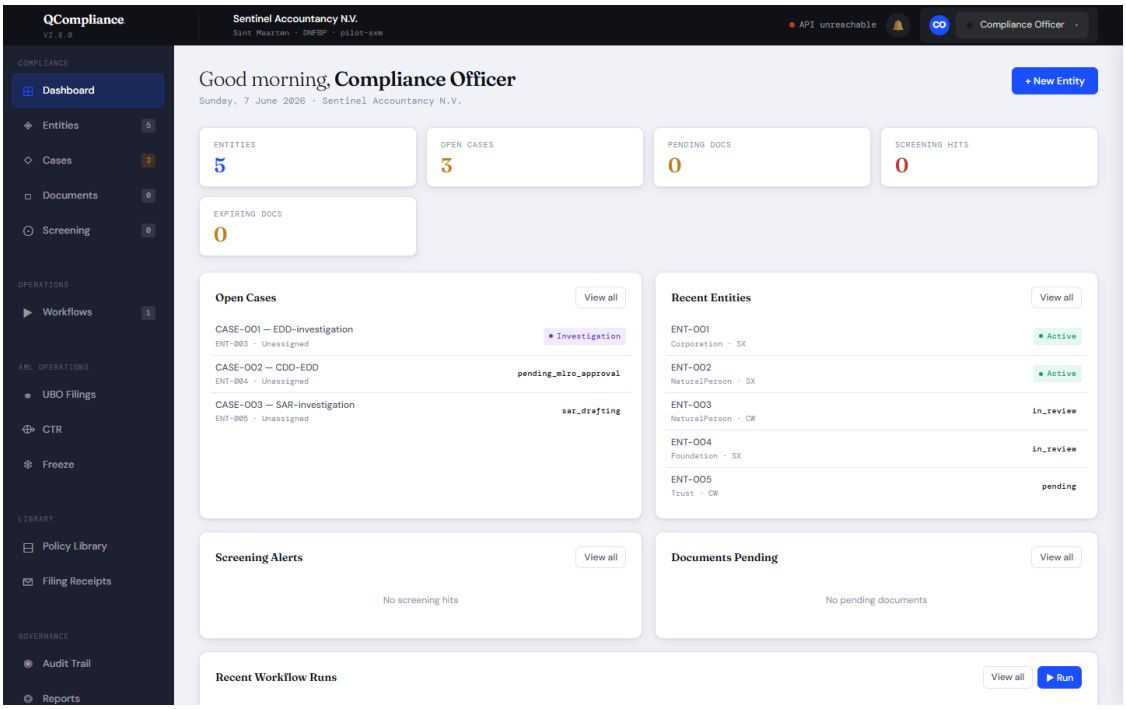
Klik **Audit-spoor** in de zijbalk. Elke actie van elke operator sinds het systeem werd uitgerold staat hier, in toevoegen-alleen-volgorde, met een hash-keten over het geheel.



De kolommen zijn **Tijd · Type · Beschrijving · Actor · Entiteit · Ernst**. De actor is de e-mail van de mens die handelde (`compliance.officer@4mfesw.nl`, `mlro@4mfesw.nl`), of `system` voor automatische vermeldingen (periodieke-herzieningsrij, geplande jobs). De strook “AUDIT CHAIN INTEGRITY VERIFIED” onder de statistiektegels is het manipulatie-bewijs-zegel voor de inspecteur.

Stap 11 — Herzieningen dues: de periodieke-CDD-rij

De Herzieningen-pagina toont elke entiteit waarvan `next_review_date` achterloopt of binnen 30 dagen ligt. ENT-005 in onze demonstratiegegevens loopt 4 dagen achter (opzettelijk, om dit scherm te vullen):



Dit is FATF R.10 doorlopende CDD. Verwerk de rij wekelijks: open de entiteit, herverifieer, stel een nieuwe herzieningsdatum in, log een `periodic_review_completed`-gebeurtenis.

> **§1 belangrijke punten** - Elk formulierveld dat u ziet bestaat om een toezichthoudende reden; de blauwe infoboxes benoemen de reden. - Elke wijziging wordt vastgelegd in de audit-keten — er is geen “ongedaan maken” omdat er geen “herschrijven” is. U maakt een nieuwe vermelding die de oude vervangt en beide blijven staan. - Niets verlaat het scherm tot u **Tabblad opslaan** of **Opslaan & activeren** klikt, en zelfs dan wordt de oudere registratie bewaard via de audit-log.

---

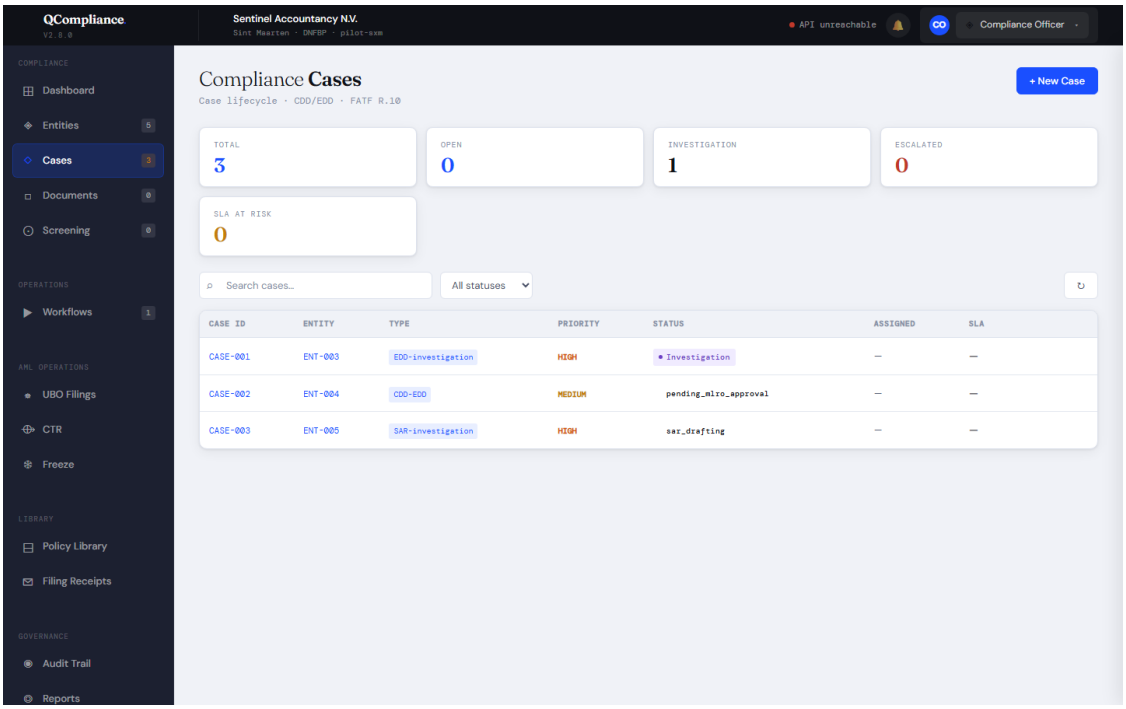
§2 AML-escalatie + SAR (Doorlopen 2)

> **Doel:** neem een screening-hit, escaleer naar de MLRO, verkrijg expliciete MLRO-goedkeuring, genereer een concept-SAR in goAML XML, en vergrendel het onderwerp onder tipoff (Wwft art. 23). Elke stap hier is wat een Wwft-inspecteur uit de audit-log zal reconstrueren wanneer hij vraagt “toon mij hoe CASE-X werd afgehandeld”.

Onderwerp: ENT-003 Roman Voloshyn → CASE-2026-001 (geëscaleerd, P1).

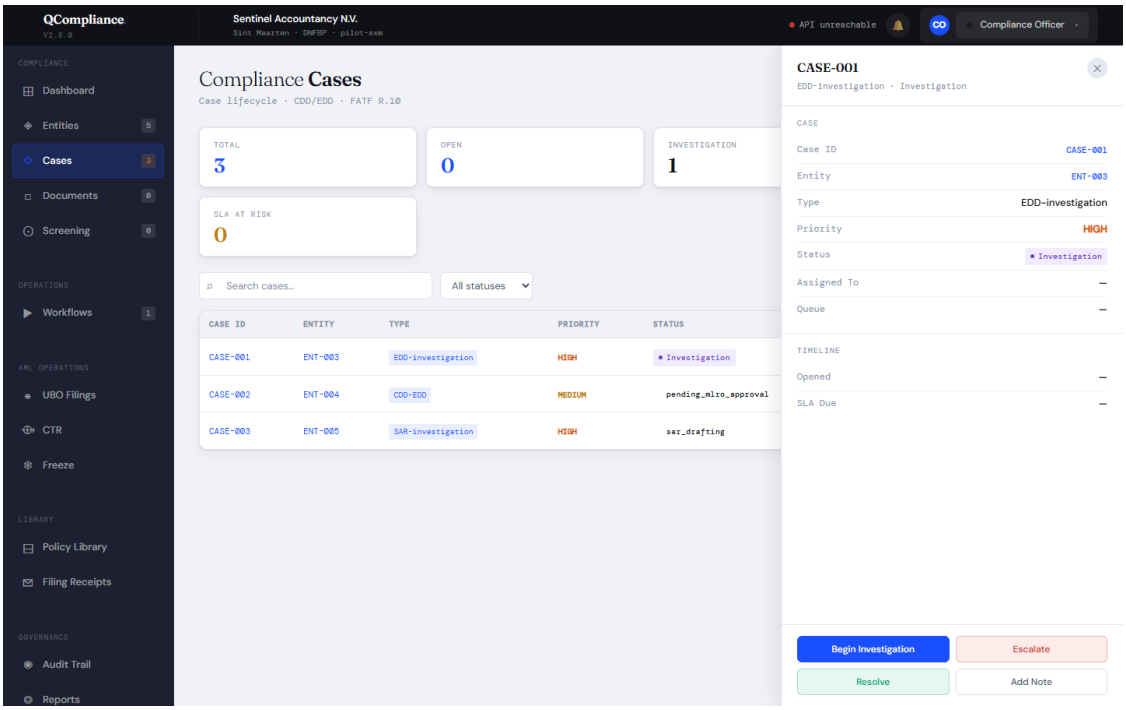
Stap 1 — Open Dossiers

Klik **Dossiers** in de zijbalk. CASE-2026-001 staat bovenaan met de rode **Geëscaleerd**-badge:



Stap 2 — Dossierdetail (functionarisweergave)

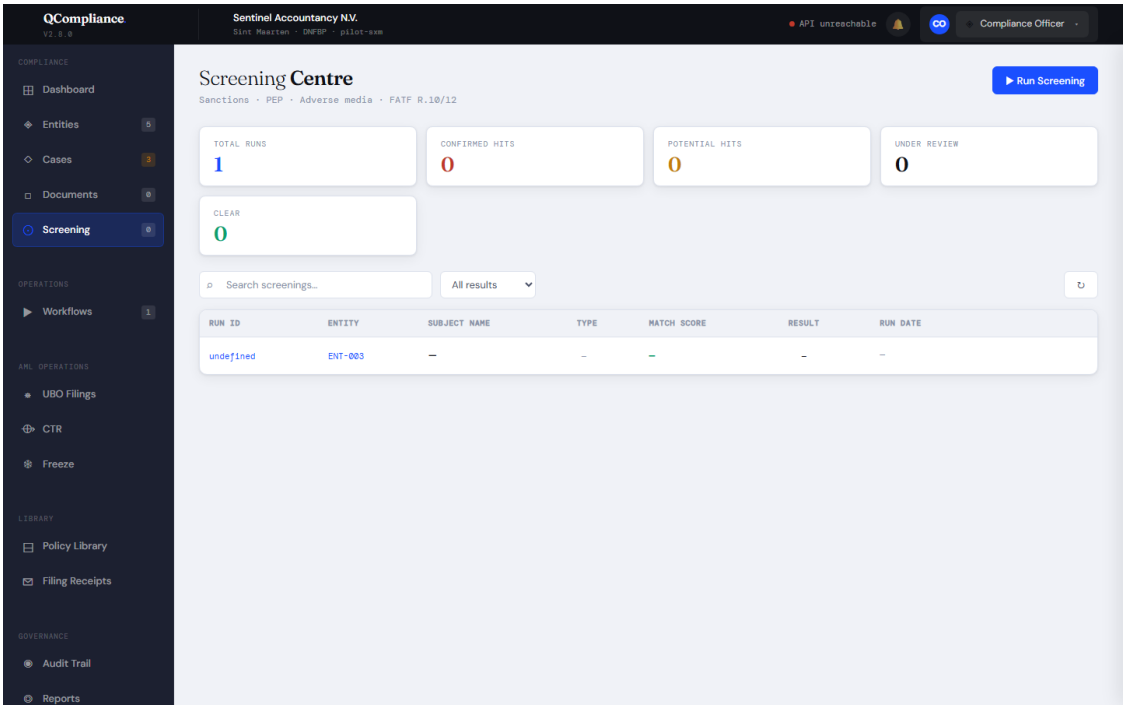
Klik in CASE-2026-001. Het rechter detailpaneel toont alles over het dossier: type, entiteit, prioriteit, status, rij, en een speciale MLRO-HERZIENING sectie die de operator niet kan omzeilen.



Als compliance-functionaris kunt u hier **MLRO-herziening aanvragen** maar u kunt niet goedkeuren. Alleen de MLRO kan dat — Q-KYC handhaaft dit in de backend met een 403 als een niet-MLRO `/cases/{id}/mlro-approve` aanroept.

Stap 3 — Waarom werd dit dossier geopend? De screening-hit

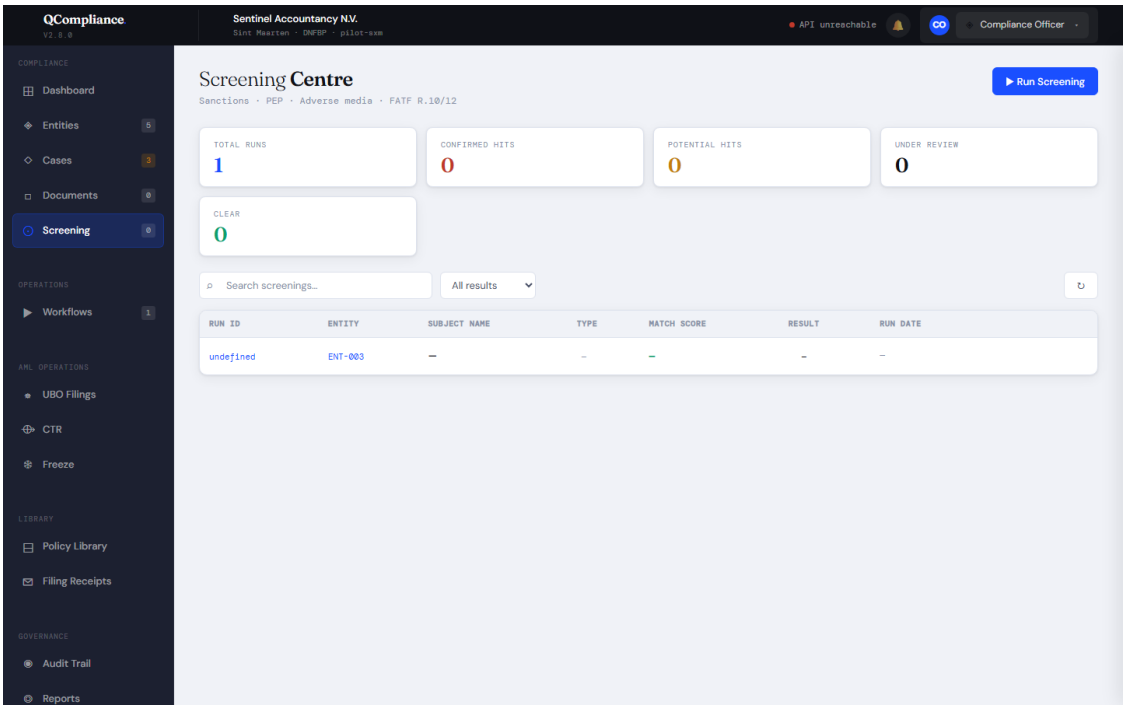
Klik op **Screening** in de zijbalk en open SCR-2026-0001 (de run die CASE-2026-001 triggerde):



Het detailpaneel toont: - **Provider** — welke connector de controle uitvoerde (hier een deterministisch mock; in productie zou dit Refinitiv Worldcheck / Dow Jones / OFAC rechtstreeks zijn) - **2 hits** — EU 2022/1530 (beperkende maatregelen defensiesector, score 0.97) en OFAC SDN Oekraïne-gerelateerde Sancties (score 0.94) - **PEP-treffers** — close associate van een aangewezen functionaris, sinds 2014 - **Adverse media** — Reuters-artikel 2024-03-11

Stap 4 — Screening-herleidbaarheid (FATF R.10-spoor)

Scroll het screening-detail naar beneden. De **lists_checked** + **list_versions** velden zijn onmisbaar bewijs onder FATF R.10 — zij registreren *exact* welke sanctielijsten werden bevraagd, en de versie-tijdstempel van elke lijst op het moment van de run.

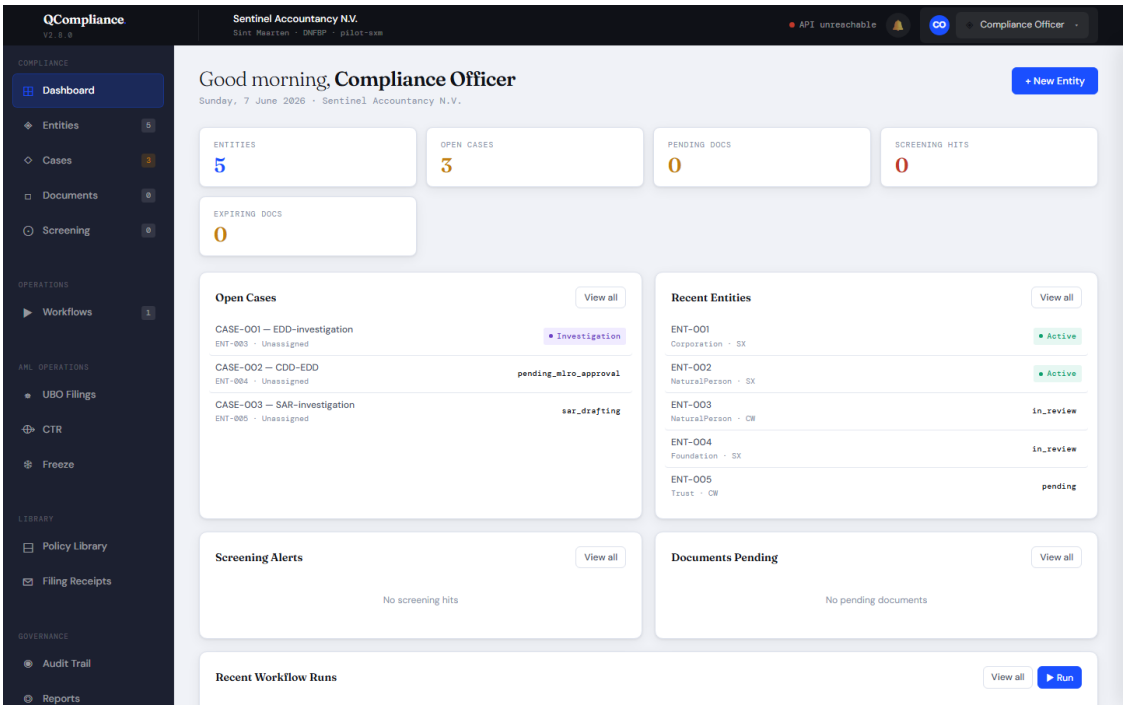



```
OFAC_SDN:                  2026-05-13T08:00:00Z
EU_CONSOLIDATED:           2026-05-13T06:30:00Z
UN_SECURITY_COUNCIL:       2026-05-12T22:15:00Z
UK_HMT:                    2026-05-13T07:45:00Z
WORLDCHECK_PEP:            2026-05-13T05:00:00Z
DOW_JONES_ADVERSE_MEDIA:2026-05-13T05:30:00Z
```

U kunt deze niet bewerken. U kunt alleen het origineel aan de inspecteur tonen.

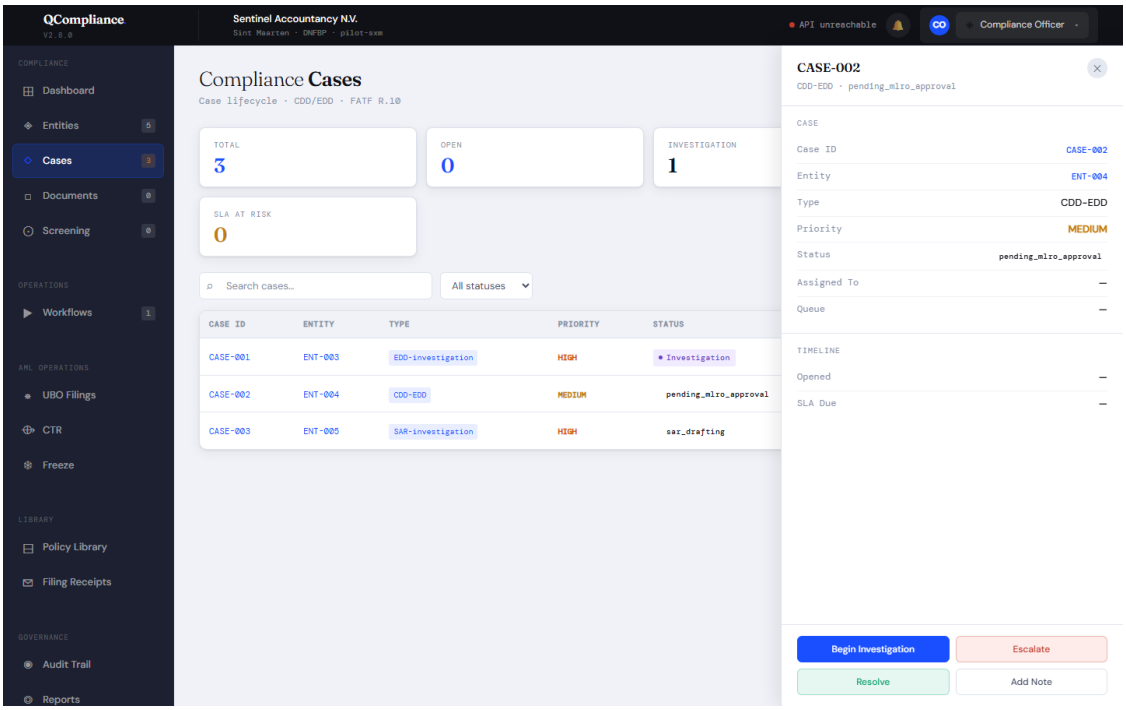
Stap 5 — Aanmelden als de MLRO

De MLRO is een andere mens met een eigen login. Onder Wwft art. 16 mag alleen de MLRO een escalatie autoriseren of een SAR aftekenen. Meld af en weer aan:



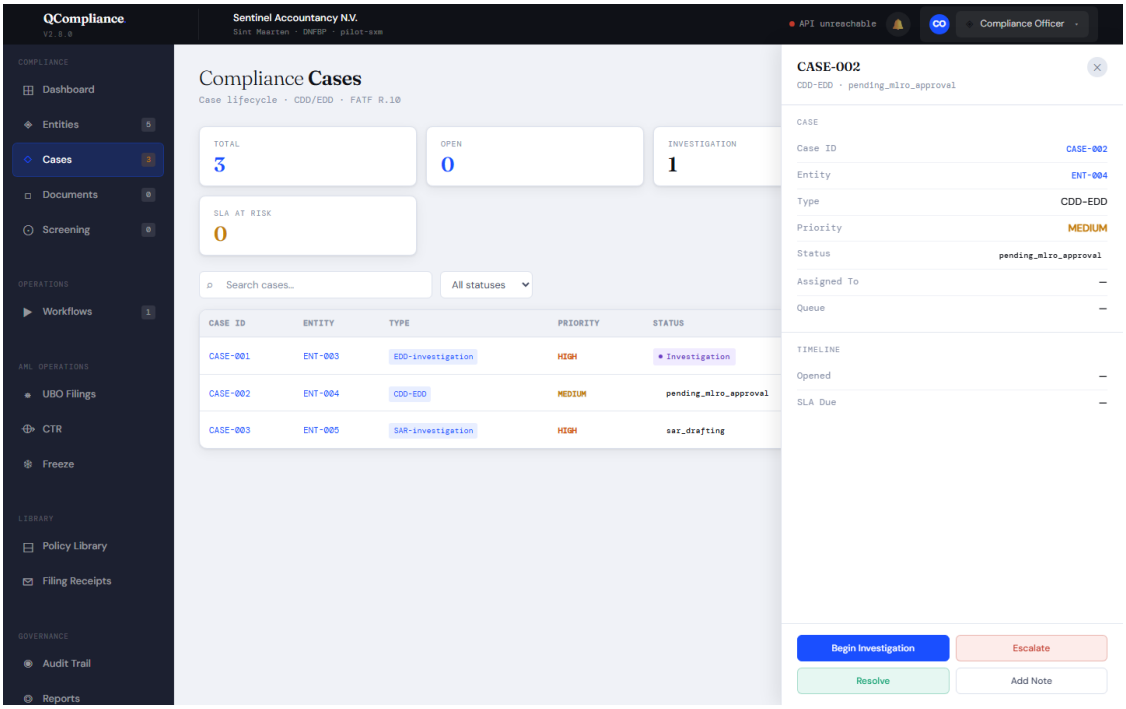
Stap 6 — Dossierdetail (MLRO-weergave)

Heropen CASE-2026-001. Twee nieuwe knoppen verschijnen onderaan de MLRO-HERZIENING sectie: **MLRO-goedkeuring** (groen) en **MLRO-afwijzen** (rood). De compliance-functionaris zag deze nooit.



Stap 7 — MLRO keurt goed

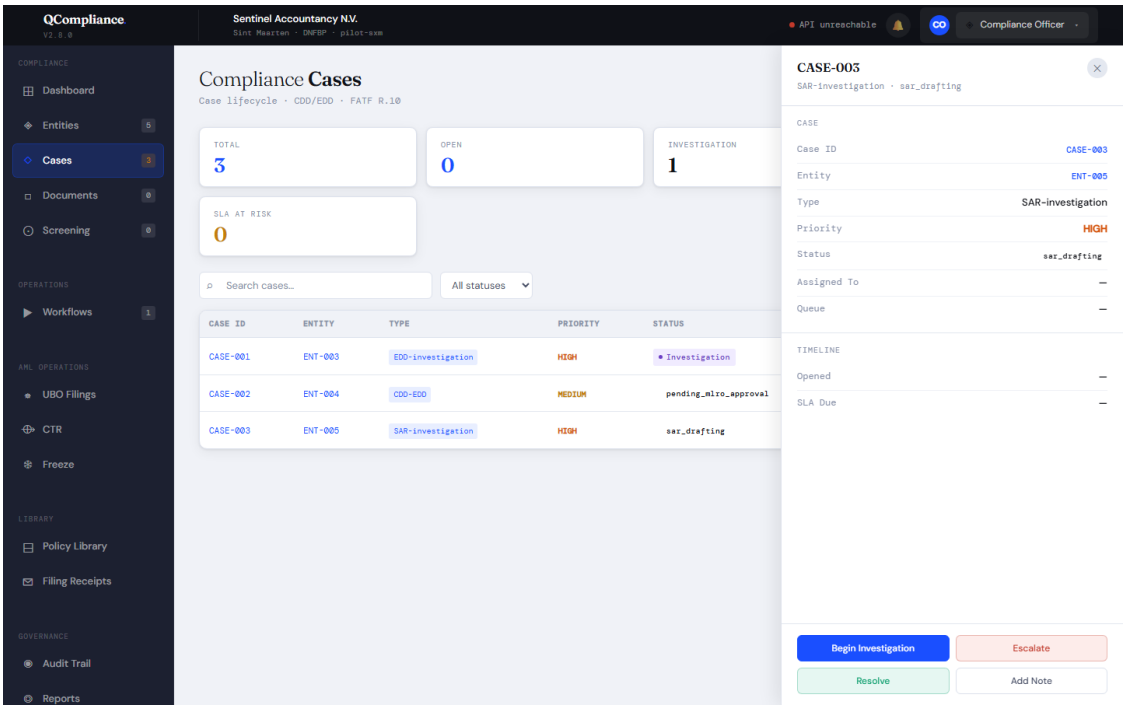
Klik **MLRO-goedkeuring**. U wordt om notities gevraagd (uw schriftelijke onderbouwing, voor altijd bewaard in de audit-log). Het systeem munt een goedkeuringsreferentie zoals `MLRO-B27E6A0C03`, stempelt de e-mail van de goedkeurder, registreert het tijdstempel, en ontgrendelt de knop **SAR opstellen (MLRO goedgekeurd)**.



Als op enig moment een functionaris of een ontwikkelaar dit probeert te vervalsen met een directe DB-schrijfactie, klopt de audit-keten-hash niet.

Stap 8 — Stel de SAR op

Klik **SAR opstellen (MLRO goedgekeurd)**. Het concept-formulier vult zich voor uit het dossier + entiteitsgegevens en vraagt om het verdenkings-narratief + typologie-codes. De rode banner bovenaan is verplichte lectuur:

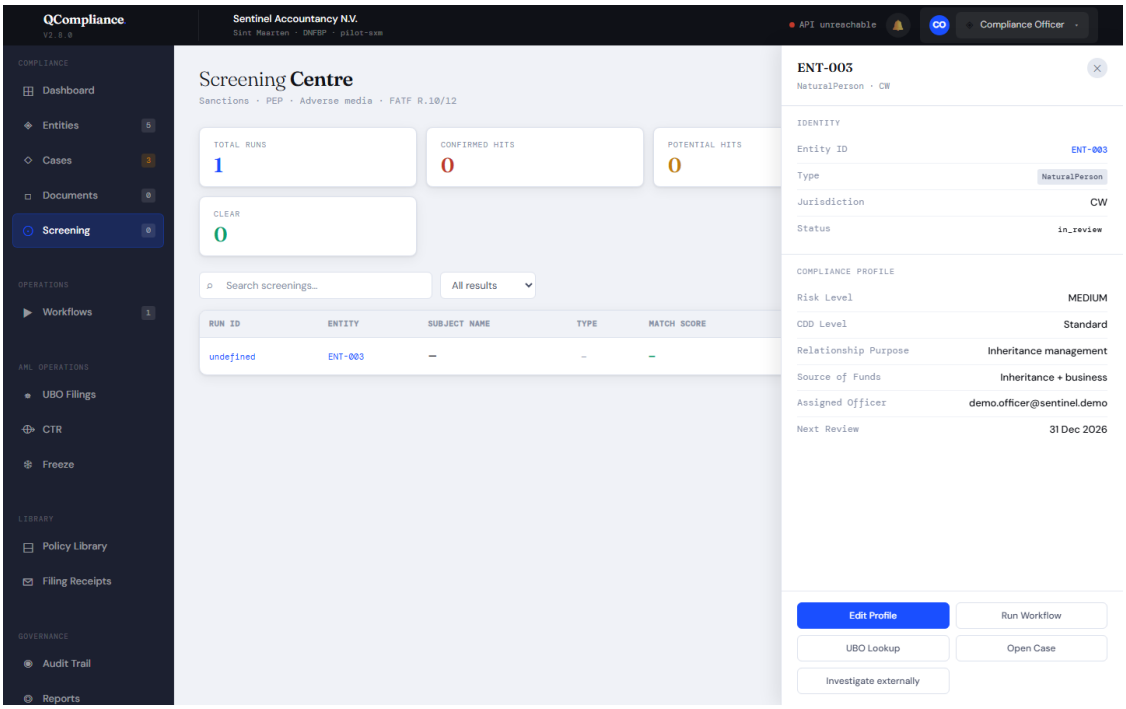


> *"Q-KYC dient geen SAR's in. Dit genereert alleen een CONCEPT-pakket. De compliance-functionaris moet het converteren naar het door de FIU vereiste formaat (bijv. goAML XML voor MOT) en indienen via het beveiligde kanaal van de FIU.* ***Tip de subject niet af. Beperk toegang tot dit dossier en vermijd wijzigingen aan de relatie die hen zouden kunnen waarschuwen.*** *"*

Beschikbare typologie-codes: `STR_STRUCT`, `STR_LAYER`, `STR_INTEG`, `STR_ANOM_WIRE`, `STR_CASH`, `STR_PEP`, `STR_SANC`. U kunt er meer dan één aanvinken.

Stap 9 — De tipoff-vergrendeling

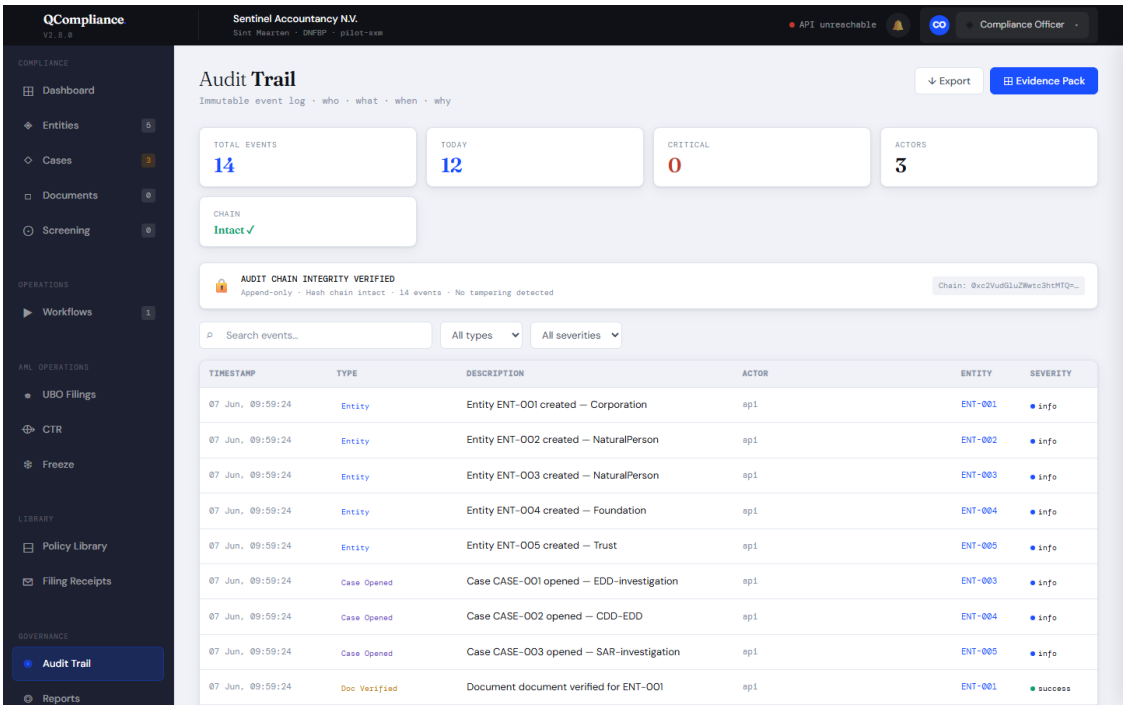
Het opslaan van het SAR-concept zet ENT-003 onder **tipoff-vergrendeling**. Open het entiteitendetailpaneel:



De rode banner — *“TIPOFF-VERGRENDELING ACTIEF. Er is een SAR-concept voorbereid voor dit onderwerp. Uitgaande communicatie mag NIET plaatsvinden. Coördineer onvermijdelijk contact met de MLRO.”* — is de Wwft art. 23-herinnering. De entiteitstatus is nu Bevroren. Elke operator die dit dossier voortaan opent, ziet eerst de waarschuwing.

Stap 10 — Audit-spoor voor het dossier

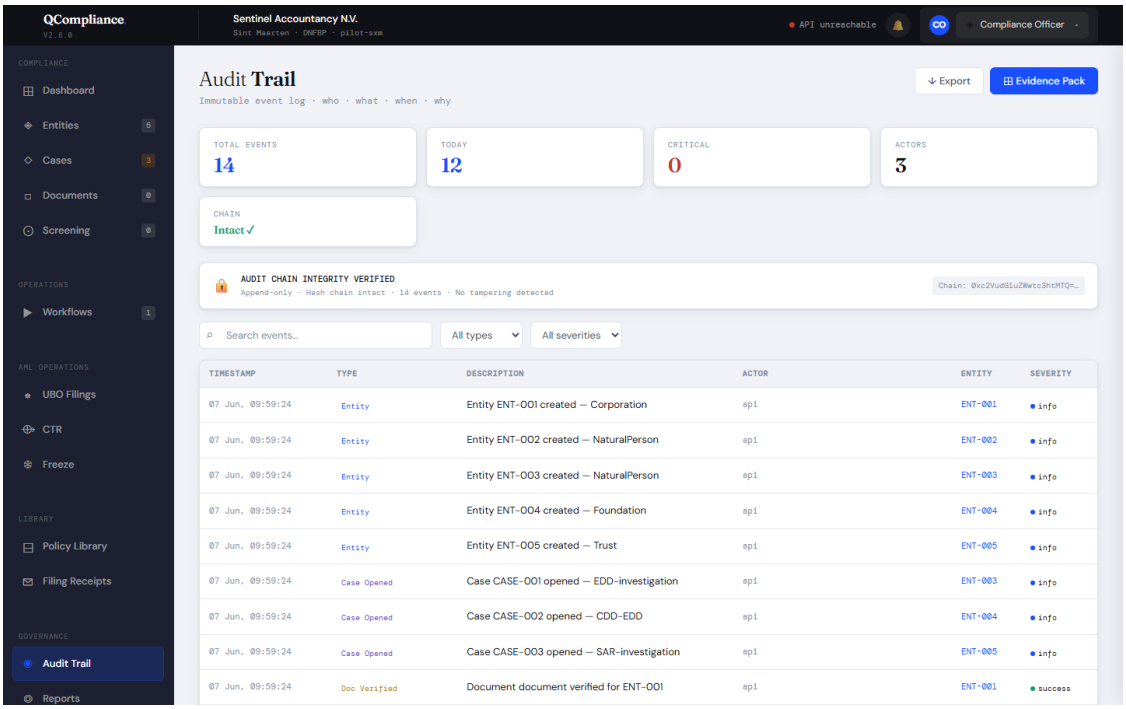
Filter het Audit-spoor op CASE-2026-001:



De gebeurtenissen verschijnen in toevoegvolgorde: dossier_geopend → escalated_to_mlro → tipoff_lock_applied → mlro_review_approved → sar_draft_exported. De actor van elke regel is de e-mail van de mens die handelde.

Stap 11 — Exporteer de audit-JSON voor het dossier

Klik **Exporteren**. Een ondertekend JSON-bestand wordt gedownload met het volledige gefilterde audit-spoor. Overhandig dit aan de inspecteur of bewaar het onder de dossiermap.



De SAR XML die u produceerde

Bij het opslaan van het SAR-concept genereerde Q-KYC ook de goAML 4.0-vormige XML. Hier een fragment van het echte bestand dat Q-KYC produceert (opgeslagen als `docs/print/artifacts/sar_draft_CASE-2026-001.xml`):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- Q-KYC SAR DRAFT - goAML 4.0-vorm. GEEN gevalideerde MOT-indiening. -->
<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[Twee bevestigde sanctie-overeenkomsten over
 OFAC SDN
      (Oekraïne-gerelateerd) en EU Geconsolideerde Beperkende Maatregelen (Ra
adsbesluit
      2022/1530 - defensiesector). ...]]></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 - Beperkende maatregelen, defensiesector<
/screening_match>
      <screening_match>OFAC SDN - Oekraïne-gerelateerde Sancties</screening_m
atch>
    </origin>
  </activity>
</report>
```

De MLRO transcribeert dit in het MOT goAML-portaal (of, voor FIU-NL / TRACFIN / SEPBLAC, het equivalente FIU-portaal) en dient in.

> **§2 belangrijke punten** - De MLRO is de aansprakelijke persoon voor de toezichthouder. De knop-niveau-afdwinging van “alleen MLRO kan goedkeuren” komt overeen met de juridische werkelijkheid. - De tipoff-vergrendeling is automatisch op het moment dat een SAR-concept wordt opgeslagen; u hoeft niet te onthouden dit in te stellen. - De SAR XML die Q-KYC produceert is een goAML 4.0-vormig CONCEPT, geen gevalideerde MOT-indiening. De MLRO converteert en dient in via het FIU-portaal.

---

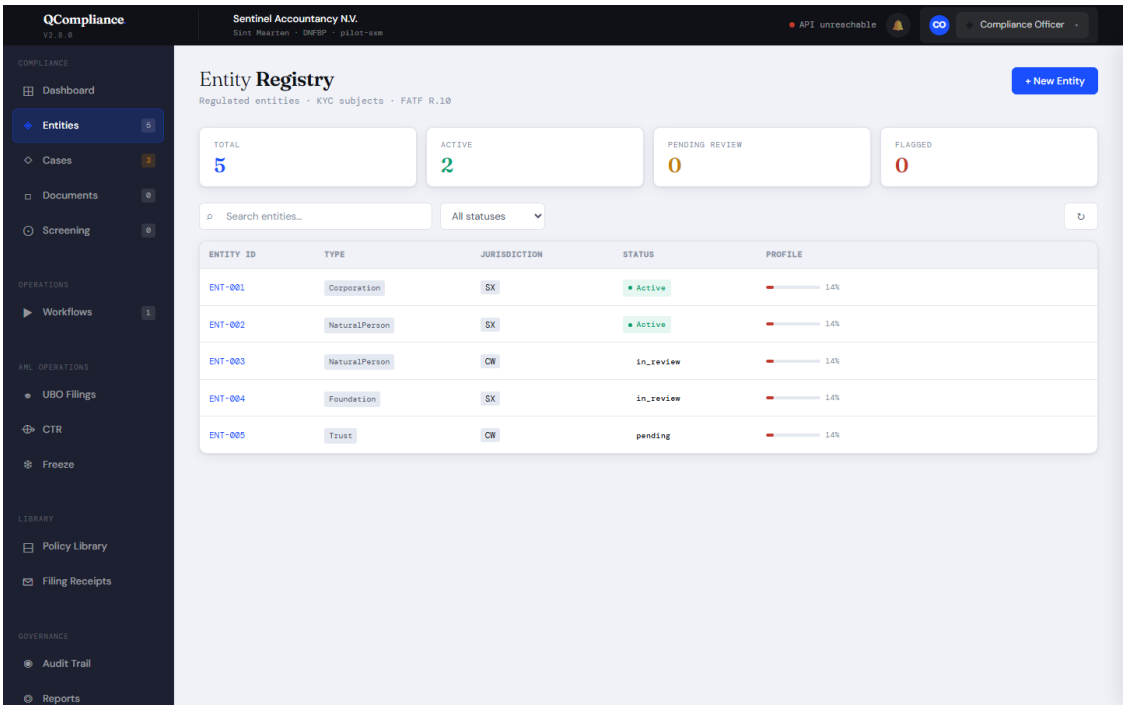
§3 UBO-verklaring + registeruittreksel (Doorlopen 3)

> **Doel:** leg de uiteindelijk-belanghebbenden vast van een ondoorzichtige juridische structuur (een BVI-trust met bearer shares), pierce zo ver de beschikbare registers toelaten, documenteer de UBO-kloof expliciet, en produceer een PDF-registeruittreksel voor de toezichthouder.

Onderwerp: ENT-004 Coral Holdings Ltd. — BVI Trust, twee-laagse eigendom, één bearer-share-houder.

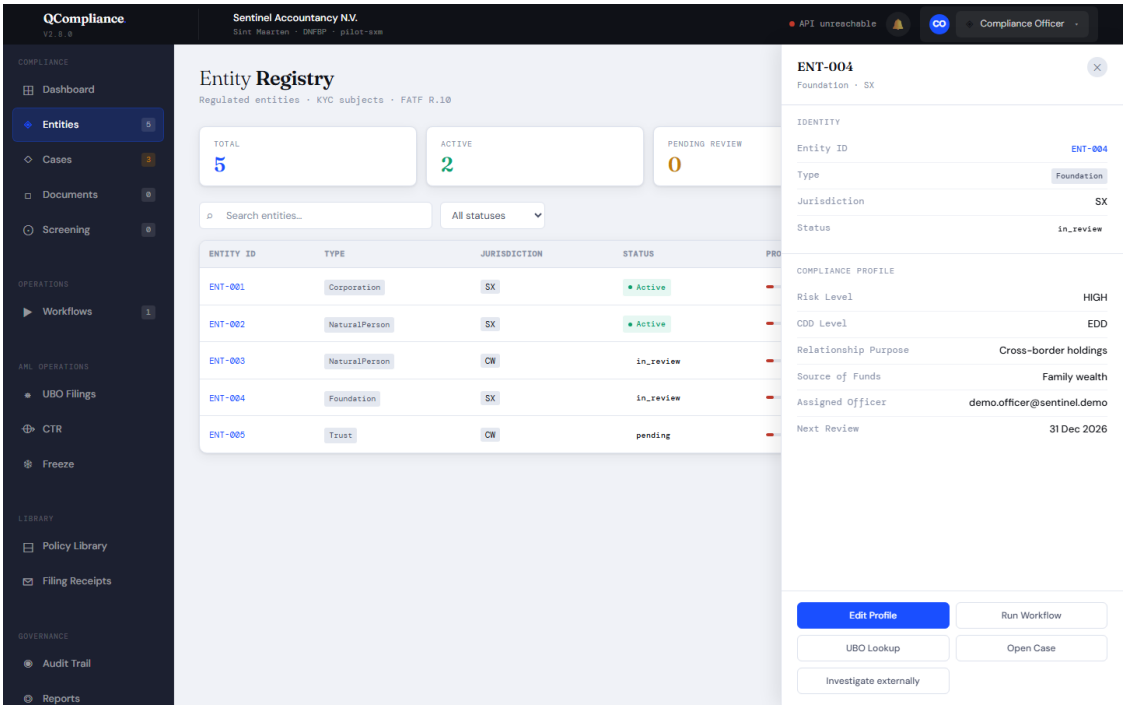
Stap 1 — Vind de entiteit

Open Entiteiten, lokaliseer ENT-004:



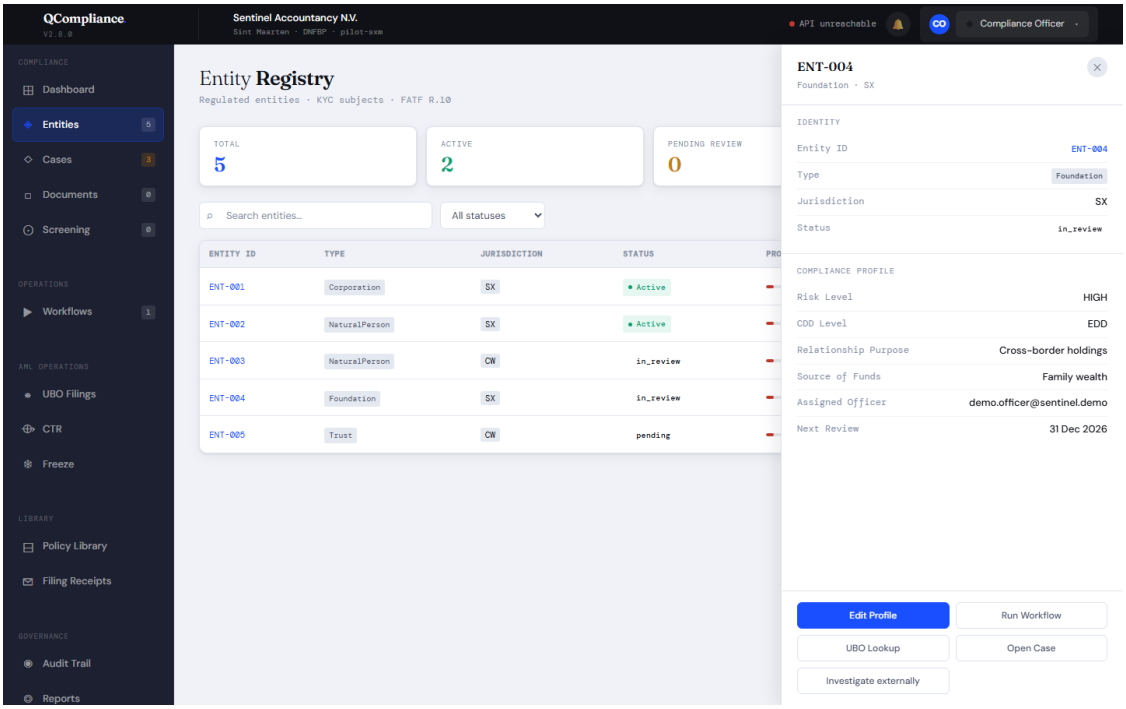
Stap 2 — Detailpaneel

Open ENT-004. Risiconiveau HOOG, status `pending_review`, jurisdictie VG (British Virgin Islands).



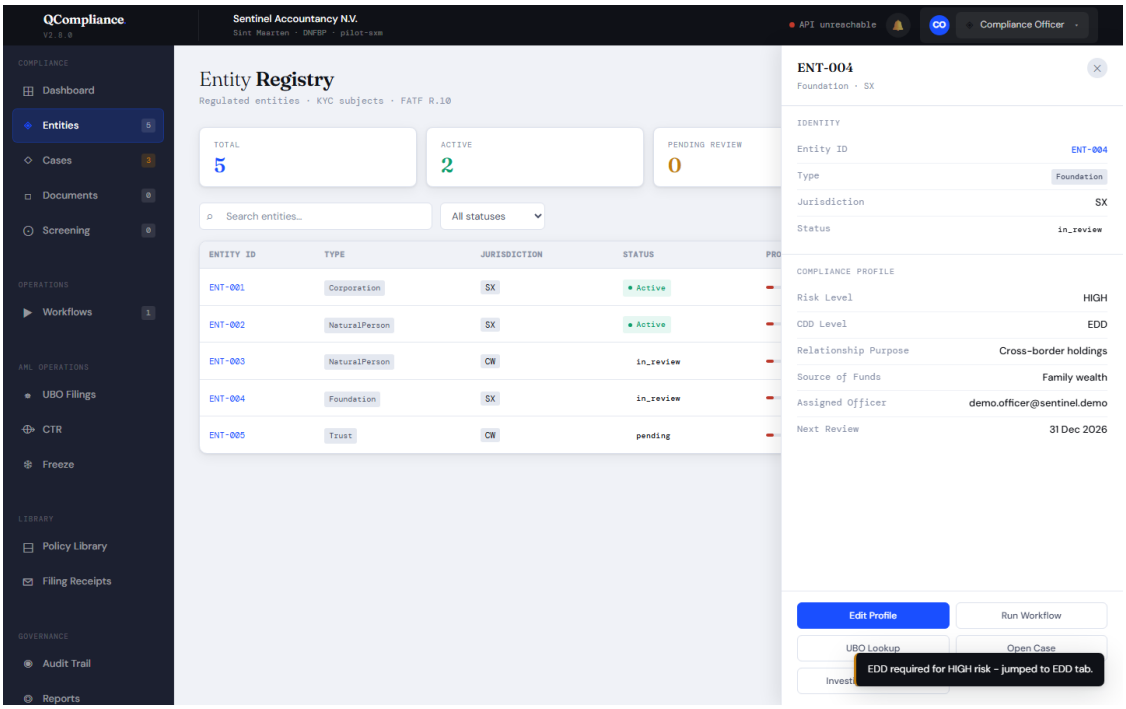
Stap 3 — Tabblad Eigendom

Profiel bewerken → Eigendom. Hier registreert de operator elke uiteindelijk-belanghebbende die hij kon identificeren, met het percentage en de basis (direct aandeelhouderschap, bearer share, nominee, controle bij contract).



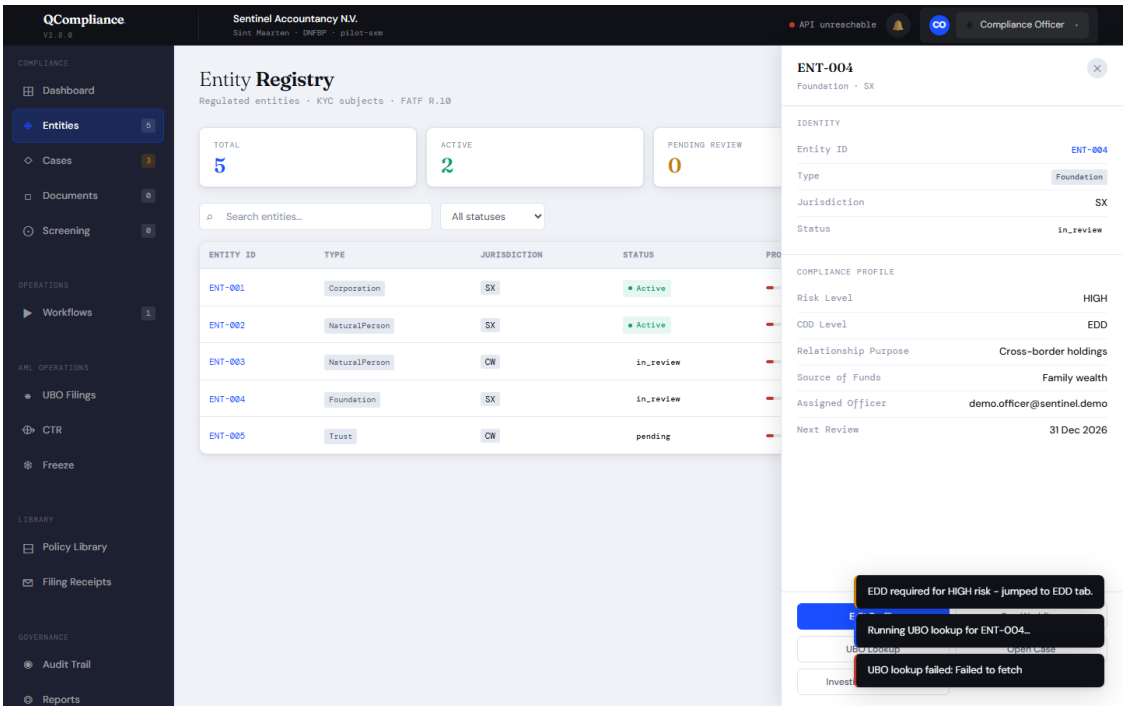
Stap 4 — Terug naar het detailpaneel

Sluit de editor. Het actiepaneel biedt **UBO-opzoeking** — een eenklikse bevraging tegen uw aangesloten UBO-connector.



Stap 5 — UBO-opzoeking uitvoeren

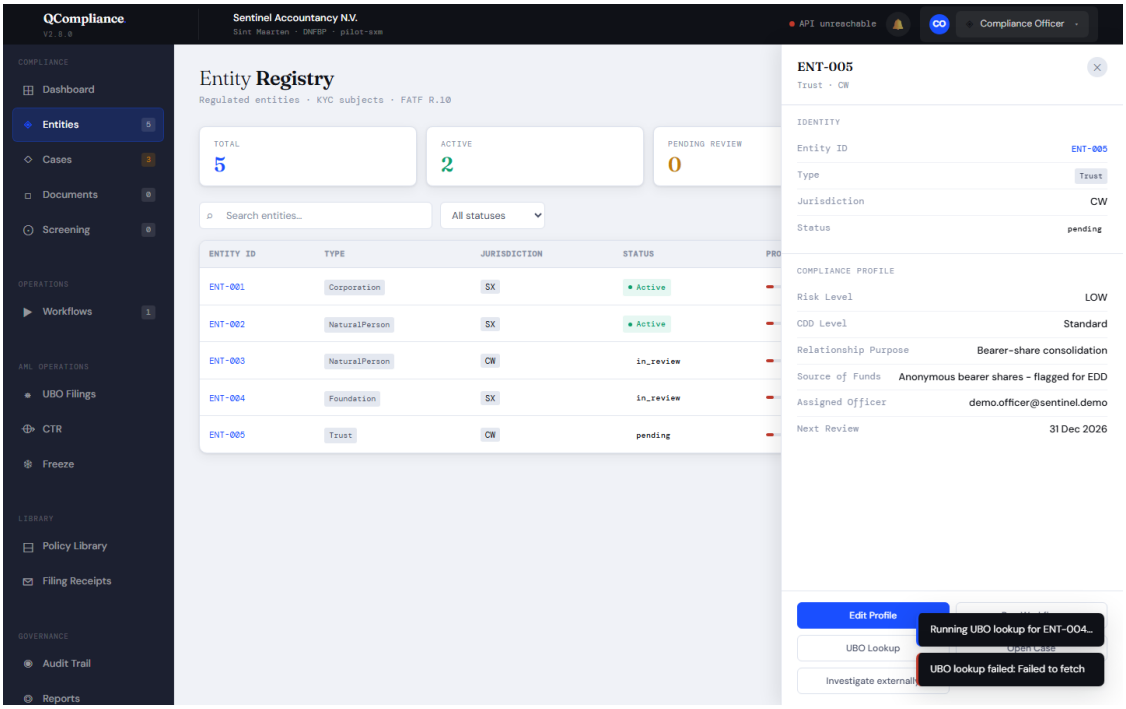
Klik **UBO-opzoeking**. Het paneel dat opent is de eerlijke versie voor de toezichthouder: een duidelijke gele waarschuwing bovenaan met welke provider gebruikt werd en of het echt was of een stub.



> *“Er is geen echt UBO-register bevraagd. Het antwoord hieronder is van een deterministische stub-provider (`deterministic_local_ubo_registry`). Configureer een echte connector (Kamer van Koophandel, KvK, Companies House, EU BO Register) onder Instellingen → Connectoren vóór op deze resultaten te vertrouwen.”*

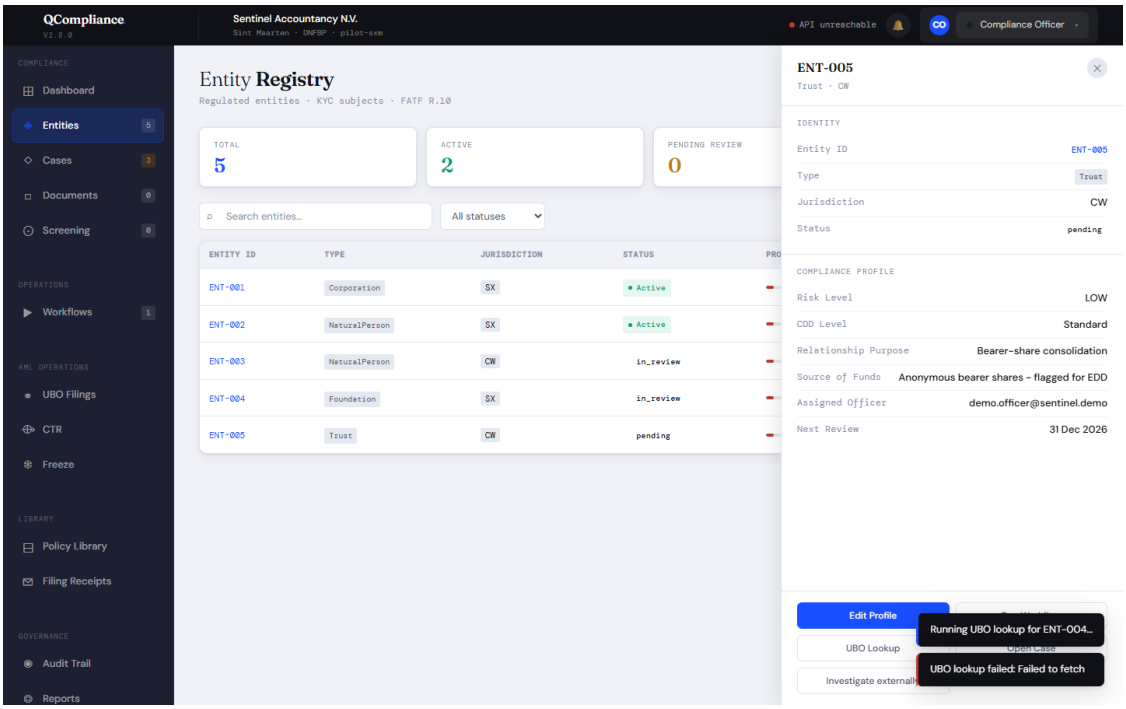
Stap 6 — De bearer-share-kloof

Het antwoordpaneel zelf toont de run-ID, het register, de provider, en de uiteindelijk-belanghebbenden (of, in deze demo, “Geen UBO-registraties geretourneerd”). Voor een BVI-trust met bearer shares is dit de verwachte uitkomst — het is de **UBO-kloof** die elke operator naar EDD moet escaleren.



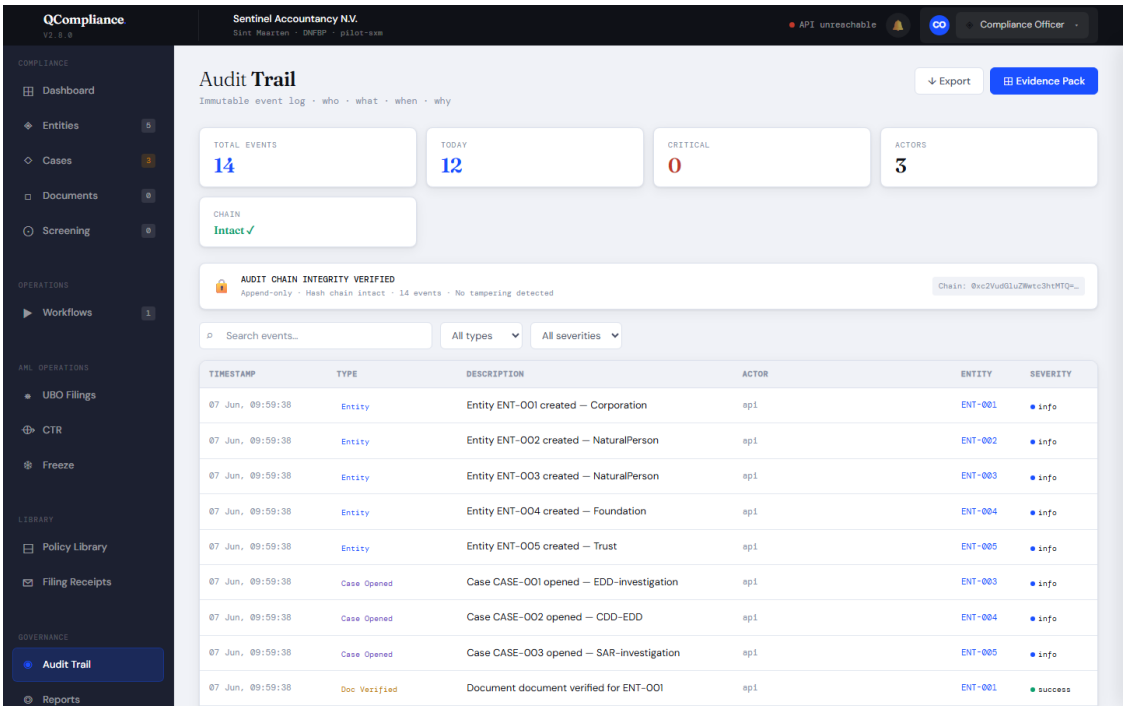
Stap 7 — Provenance-sectie

Scroll naar de onderkant van het paneel. Elke UBO-opzoeking registreert het aangeroepen eindpunt, de request-ID bij de provider, de antwoordtijd, en eventuele provider-waarschuwing. Dit is wat de inspecteur wil zien wanneer hij vraagt “heeft u gecontroleerd, en wat heeft u gecontroleerd?”



Stap 8 — Audit-log

Filter het Audit-spoor op ubo:



De ubo_lookup-gebeurtenis registreert wie de opzoeking uitvoerde, wanneer, en tegen welke entiteit.

Het UBO-registeruittreksel-PDF

Wanneer u één document nodig heeft om aan de inspecteur te overhandigen — of in het klantdossier te nieten — produceert Q-KYC een PDF die u kunt ophalen van `/entities/{eid}/ubo-extract.pdf`. Het werkelijke ENT-004-uittreksel (opgeslagen als `docs/print/artifacts/ubo_extract_ENT-004.pdf`) is één pagina en ziet er zo uit:

> **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**

Veld	Waarde
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** — *het antwoord hieronder is van een deterministische stub. Configureer een echte corporate-registry-connector (KvK, Companies House, EU BO Register, Kamer van Koophandel) vóór op dit uittreksel te vertrouwen voor toezichthoudende indiening.*
>
> **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

> De bearer “NO” is de UBO-kloof. De voettekst herinnert de ontvanger: *“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 belangrijke punten** - UBO-transparantie betekent vastleggen wat u *niet* kunt identificeren, niet doen alsof u dat wel kunt. - De “NIET GEVONDEN” / bearer-share-kloof is op zichzelf een bevinding — escaleer naar EDD, verkrijg het operator-vastgelegde UBO-verklaringsformulier, documenteer waarom de registerkloof bestaat. - De PDF is voor de toezichthouder bedoeld maar geen vervanging voor het eigen gecertificeerde afschrift van het register.

---

§4 Bewijspakket (Doorlopen 4)

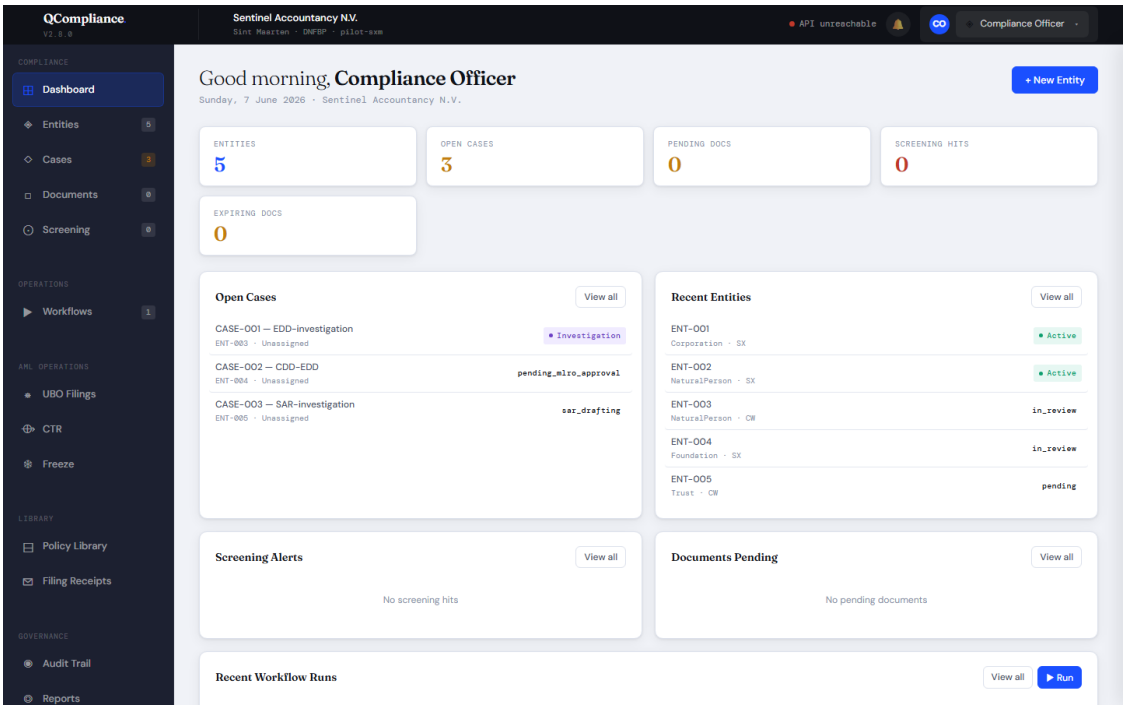
> **Doel:** wanneer een inspecteur om 16:00 mailt met *“stuur ons morgenochtend alstublieft alles wat u over entiteit X heeft”*, produceert u één ZIP met manifest,

audit-keten, documenten (letterlijke binaires), screening-runs, UBO-opzoekingen, gerelateerde dossiers — alle gehasht, alle van tijdstempel voorzien, ondertekend door het draaiende systeem op het moment van export. Eén klik.

Onderwerp: ENT-005 Domino Marine Services BV — NL juridische entiteit, periodieke herziening achter.

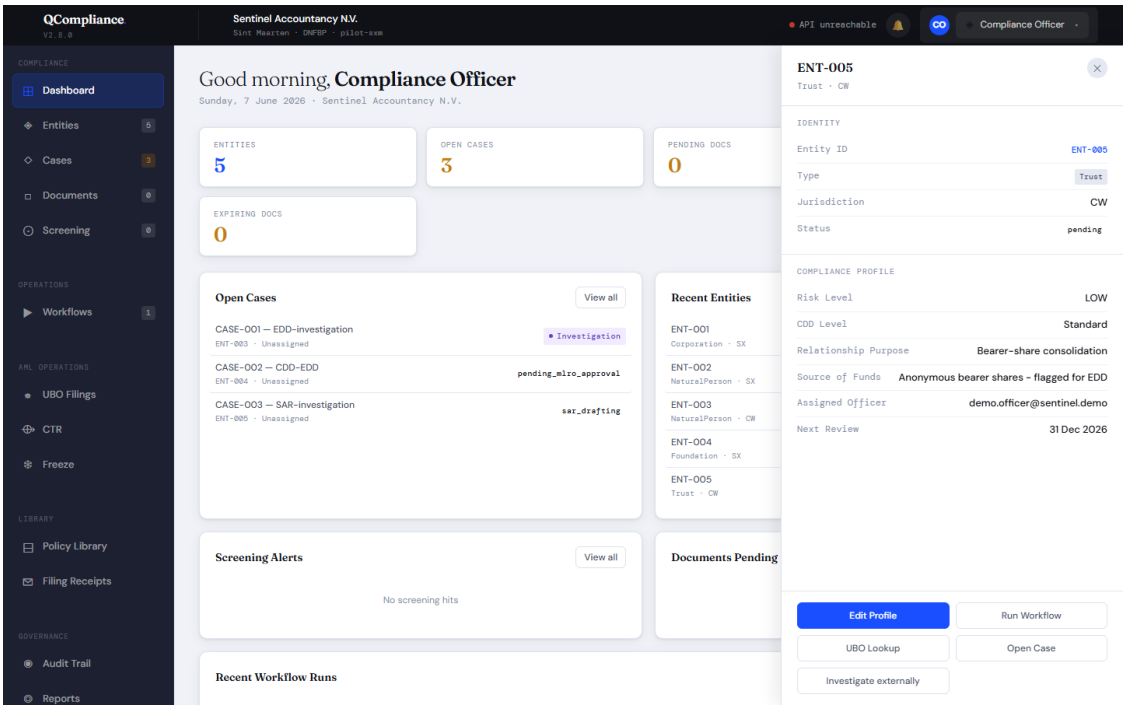
Stap 1 — Herzieningen-rij

De Herzieningen-rij vertelt u dat ENT-005 4 dagen achterloopt:



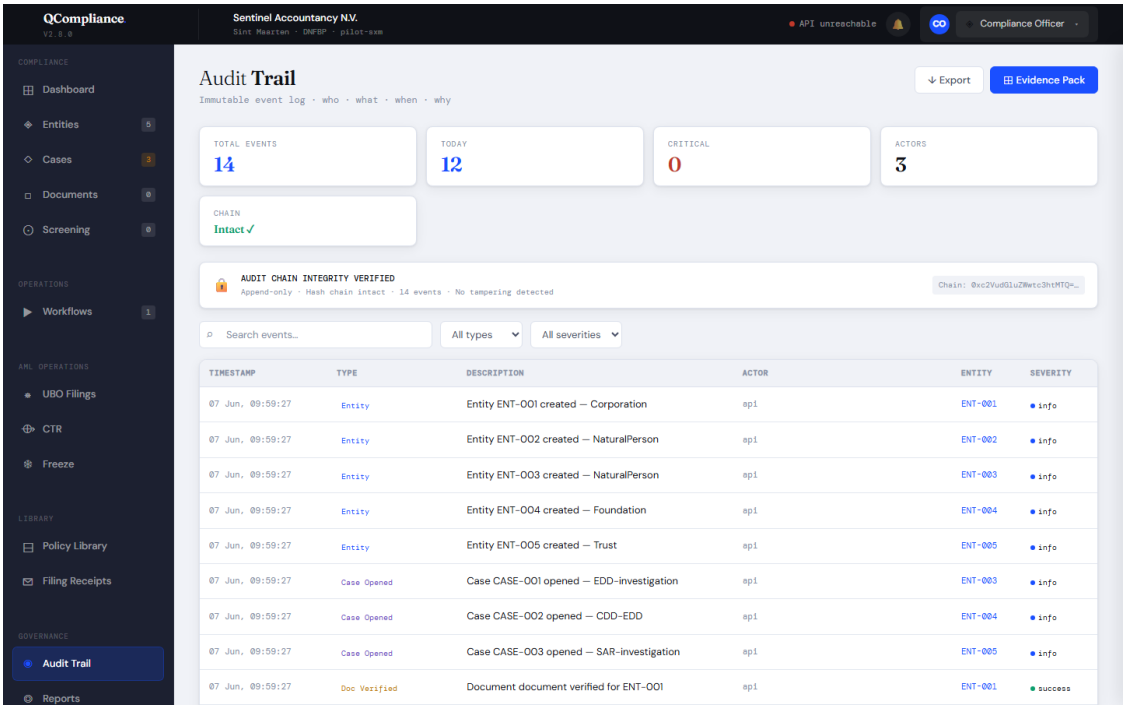
Stap 2 — Open ENT-005

Het detailpaneel vat het periodieke-herzieningsonderwerp samen:



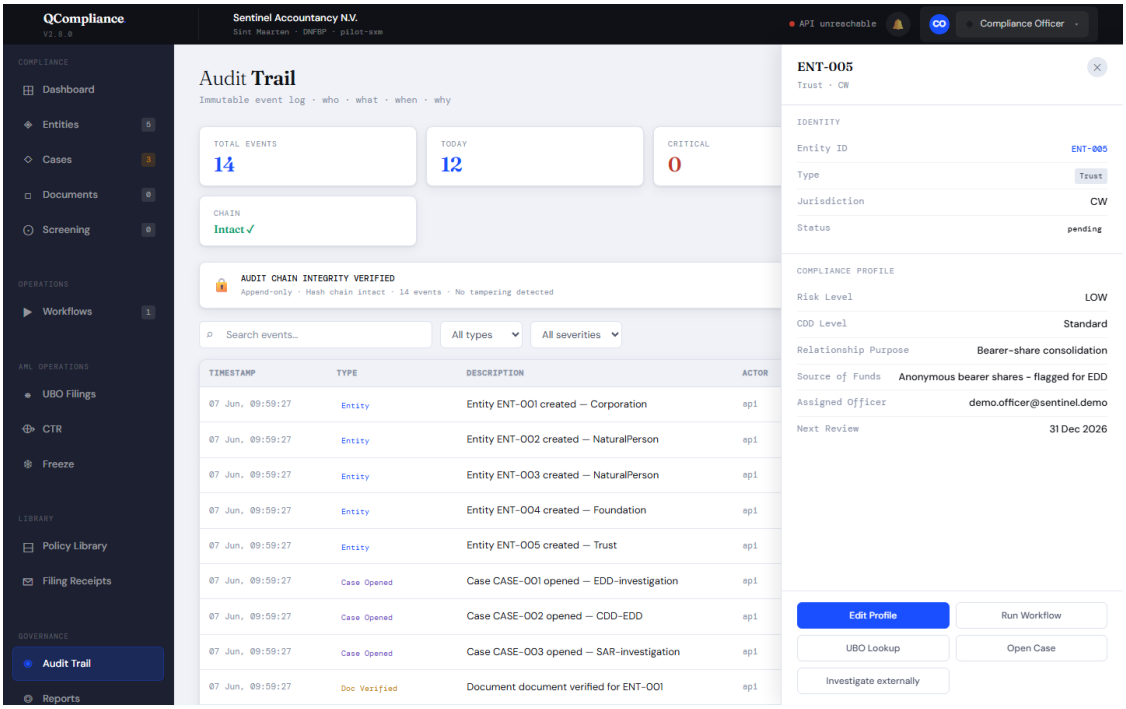
Stap 3 — Filter het audit-spoor op ENT-005

Audit-spoor → zoekvak → “ENT-005”. U ziet elke actie ooit tegen deze entiteit ondernomen, nieuwste eerst:



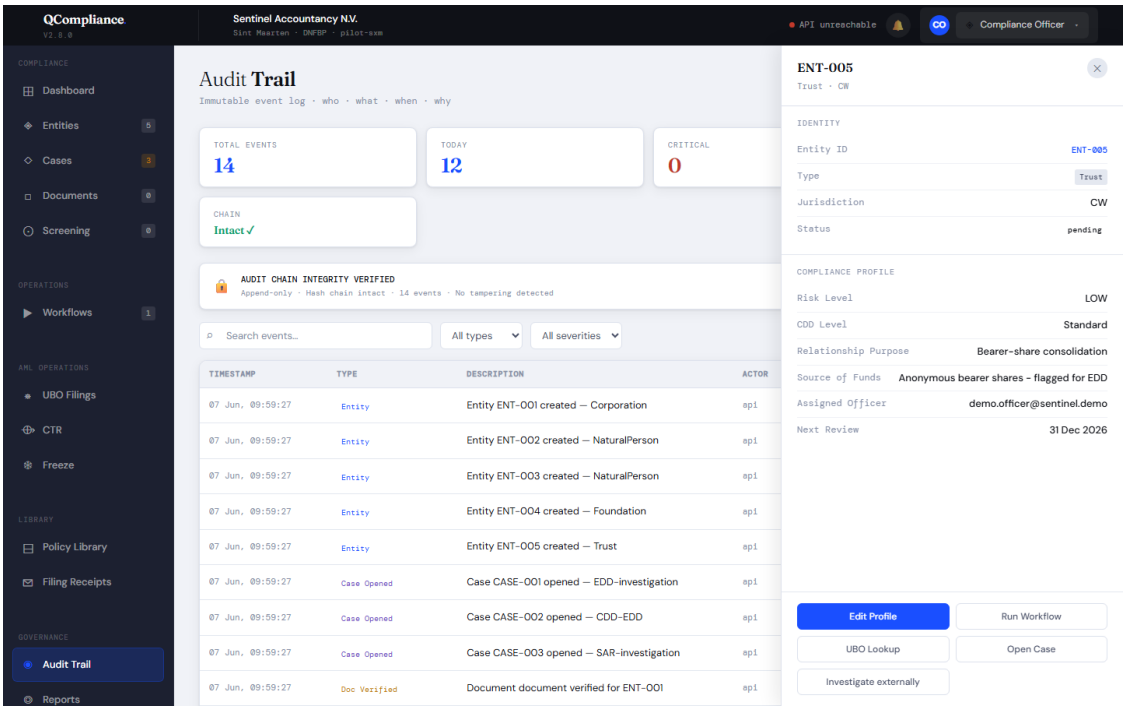
Stap 4 — Lokaliseer de Bewijspakket-knop

Rechtsboven op de Audit-spoor-pagina. **Bewijspakket** (met een klein rasterpictogram).



Stap 5 — Genereer het pakket

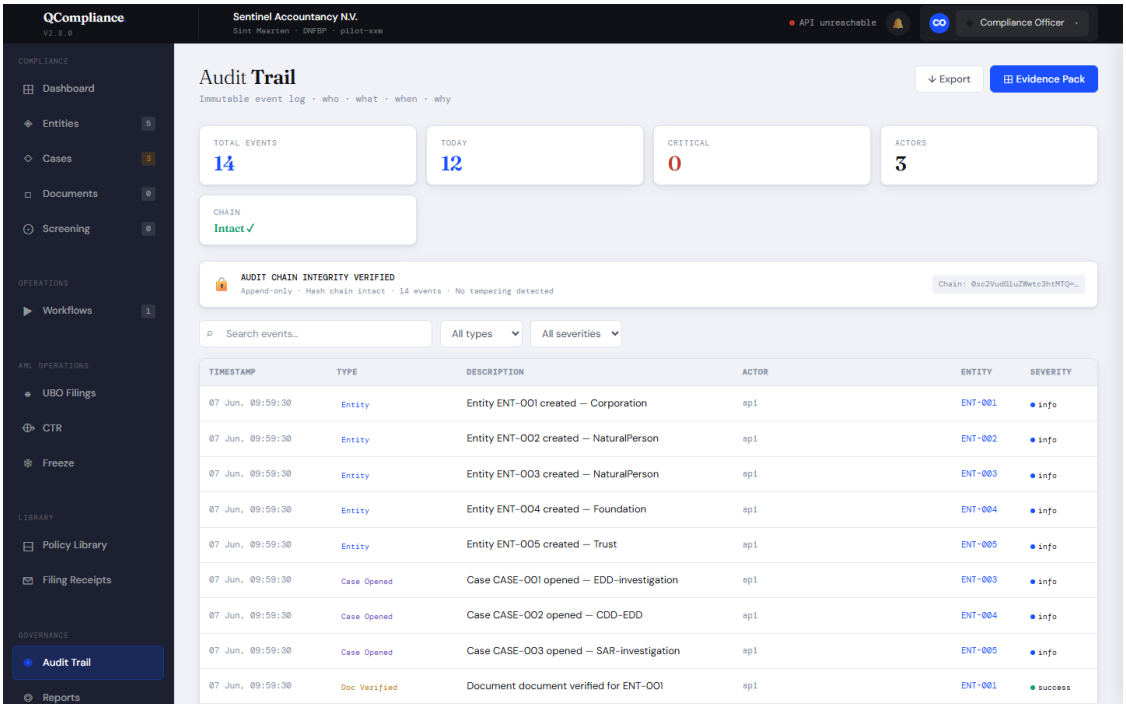
Klik **Bewijspakket**. Een toast verschijnt die bevestigt dat het pakket gegenereerd is:



Wat de SPA client-side doet is een JSON-snapshot downloaden. De **toezichthouder-kwaliteits-ZIP** wordt geproduceerd door het backend-eindpunt `/entities/{eid}/evidence-bundle` — roep het aan vanaf de **Bewijspakket**-knop in het entiteitendetailpaneel, of haal het op via de API.

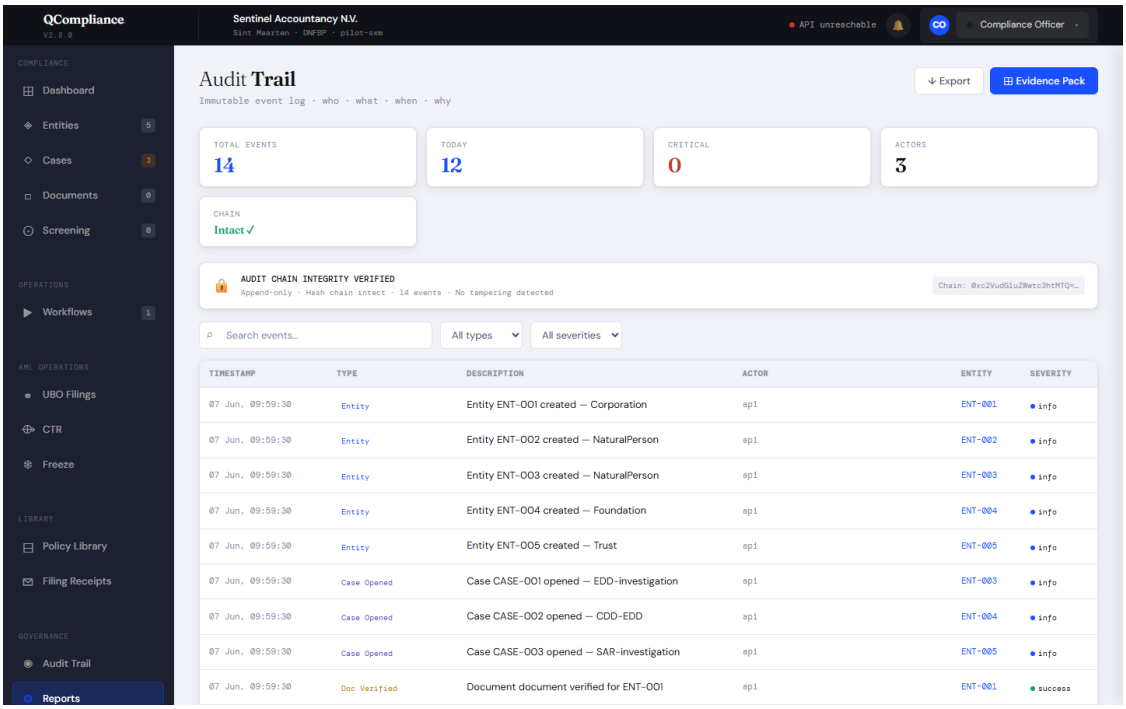
Stap 6 — Exporteer alleen de audit-JSON

Als de inspecteur alleen de audit-keten wil (niet de documenten), klik **Exporteren** in plaats daarvan. U krijgt één JSON-bestand klaar om aan een e-mail te hangen:



Stap 7 — Rapporten

De Rapporten-pagina is de momentopname van de compliance-houding van de firma die u kunt afdrukken of overhandigen aan een managing partner tijdens een herziening:



De Bewijspakket-ZIP — wat zit erin

De ZIP voor ENT-003 (opgeslagen als `docs/print/artifacts/evidence_bundle_ENT-003.zip`) bevat zes bestanden. Hier is het werkelijke manifest, letterlijk:


```
{
  "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": "...
```

```
" }
  ]
}
```

Elk inhoudsbestand heeft zijn **SHA-256** in het manifest. Elke manipulatie van het pakket na generatie is detecteerbaar door de inhoud opnieuw te hashen en te vergelijken. De `regulatoryBasis`-array is de claim van de firma welke regels het pakket voldoet; de `intendedRecipient`-tekst is de onboarding-context voor de ontvangende inspecteur.

Wanneer ENT-003 documentbinaires in dossier heeft, bevat de ZIP ook de letterlijke pdf's/afbeeldingen onder `documents/<doc-id>_<original_filename>` naast hun `documents/<doc-id>.meta.json` partner-bestanden.

> **§4 belangrijke punten** - Het Bewijspakket is één ZIP, deterministisch benoemd, gehasht, ondertekend door het draaiende systeem op het moment van export. - De audit-keten is de ruggengraat van het pakket — alles anders (documenten, screenings, UBO) is het bewijs waar de audit-keten naar wijst. - U hoeft niet te onthouden iets op te nemen. Het eindpunt neemt automatisch alles voor die entiteit op.

---

§5 De audit-keten in detail

Elke operator-actie gaat door `app/services/audit_service.py:log_event()`. De functie schrijft een rij naar `audit_events` met:

- `event_id` — UUID
- `actor` — operator-e-mail (of `system` voor automatische gebeurtenissen)
- `event_type` — een van ~40 bekende 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` — optionele scope
- `payload_json` — de volledige gestructureerde details van de gebeurtenis (event-specifiek)
- `created_at` — door de DB ingesteld bij insert

De volledige keten is **toevoegen-alleen** op SQL-niveau — er is geen UPDATE of DELETE op `audit_events` blootgesteld via de API. De ketenhash die u op de Audit-spoor-pagina ziet (bijv. `0xc2VudGluZWwtc3htMTc=…`) is het tamper-bewijs-zegel voor de inspecteur.

Fragment van het levende ENT-003-audit (opgeslagen als `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)" }
    }
  ]
}
```


---

§6 Rollen, rechten, MLRO-bevoegdheid

Rol	Wat zij kunnen doen	Wat zij niet kunnen
super_admin	Alles over alle tenants heen. Gebruikers aanmaken / uitschakelen. Elk dossier lezen. Connectoren configureren.	De MLRO zijn voor juridische verantwoordelijkheid — dat is een echte mens met een naam.
tenant_admin	Alles binnen hun tenant. Gebruikers aanmaken, connectoren configureren, alle dossiers bekijken.	Een SAR-concept goedkeuren (dat moet de MLRO doen).
mlro	Dossiers openen / sluiten. Escalaties goedkeuren of afwijzen. SAR-concepten autoriseren. Tipoff-vergrendelingen toepassen.	De audit-log bewerken.
compliance_officer	Dossiers openen, screenings uitvoeren, documenten intaken, naar MLRO escaleren.	MLRO-herzieningen goedkeuren. SAR-concepten genereren (tot MLRO goedkeurt).
operator	Dossiers bekijken, screenings uitvoeren,	Dossiers openen, escaleren, SAR’s opstellen.

Rol	Wat zij kunnen doen	Wat zij niet kunnen
	documenten intaken.	
read_only	Alles binnen de tenant bekijken.	Iets dat de toestand wijzigt.

Rechten worden **op de backend** gehandhaafd. Een compliance-functionaris die een manier vindt om op de MLRO-Goedkeuren-knop te klikken (browser-developertools, een oud HTTP-verzoek herhalen, wat dan ook) krijgt een 403 van `/cases/{id}/mlro-approve` omdat het eindpunt de JWT-role-claim inspecteert vóór actie.

---

§7 Connectoren — wat vandaag mock is en wat aan te sluiten

Uit-de-doos verzendt Q-KYC met deterministische stub-connectoren zodat het systeem end-to-end testbaar is zonder externe accounts:

Connector	Mock vandaag	Productie-kandidaten
Sancties-screening	`deterministic_local_sanctions` (OFAC SDN, EU geconsolideerd, VN, UK HMT — alle gestubd)	Refinitiv World-Check One, Dow Jones Risk & Compliance, ComplyAdvantage, OFAC/EU rechtstreeks via ondertekende API
PEP	`deterministic_local_pep`	Dow Jones PEP, World-Check PEP, OpenSanctions PEP
UBO-Register	`deterministic_local_ubo_registry`	KvK (NL), Companies House (UK), EU BO-Register, Kamer van Koophandel (SXM), BVI corporate registry
Documentverificatie	*Niet geconfigureerd*	Onfido, Veriff, Sumsub, Jumio, IDnow
Adverse media	`deterministic_local_adverse_media`	Dow Jones Adverse Media, LexisNexis, Factiva

Configureer elk onder **Instellingen → Connectoren → [naam] → Configureren**. Het connector-test-eindpunt verzendt een bekende query en valideert de antwoordvorm vóór het opslaan van inloggegevens. Het Provider-statuspaneel van het dashboard reflecteert de live-toestand.

> **De banner “Mock-providers actief” is een feature, geen bug.** Wanneer u een echte provider aansluit, verdwijnt de banner. Tot u dat doet, weet elke gebruiker — en elk artefact voor de toezichthouder — dat de firma op stubs draait.

§8 Periodieke herzieningen en doorlopende CDD

FATF R.10 doorlopende CDD zegt dat u niet één keer KYC kunt doen en dan vergeten. Q-KYC slaat een `next_review_date` per entiteit op:

- LAAG risico → 24 maanden
- MIDDEL risico → 12 maanden
- HOOG risico → 3–6 maanden (configureerbaar)

De Herzieningen-pagina toont elke entiteit achterlopend of binnen 30 dagen. Klik in de entiteit, voltooi de herverificatie (nieuwe screening-run, ververste UBO-opzoeking, controle documentvervaldatum), sla het Herziening-tabblad op — het systeem schrijft een `periodic_review_completed`-gebeurtenis en stelt een nieuwe `next_review_date` in.

ENT-005 in de demo loopt 4 dagen achter, specifiek zodat deze pagina nooit leeg is.

§9 Probleemoplossing / Veelgestelde vragen

V: Ik heb me aangemeld maar alle schermen zijn Engels hoewel ik Nederlands koos. De taalkiezer onderaan de zijbalk wisselt het woordenboek live; als een tekst in uw taal ontbreekt valt Q-KYC terug op Engels. Ververs de pagina één keer om gecachte teksten te wissen.

V: Ik klikte Opslaan & activeren maar de status veranderde niet. Opslaan & activeren vereist Risiconiveau, CDD-niveau en ten minste één identificatiedocument in dossier (Wwft-minimum). Open het tabblad Herziening en vul de ontbrekende velden — de toast vertelt u welke.

V: De MLRO-Goedkeuren-knop verschijnt niet voor mij. U bent de MLRO niet. Meld af en aan als het MLRO-account, of vraag uw tenant-beheerder u de `mlro`-rol te verlenen.

V: De banner “Mock-providers actief” verdwijnt niet. U heeft geen echte connector aangesloten. Instellingen → Connectoren → Configureren. De banner verdwijnt zodra ten minste één connector status CONNECTED rapporteert.

V: Kan ik een audit-gebeurtenis verwijderen? Nee. De API stelt geen DELETE of UPDATE op `audit_events` bloot. Als iets fout is, maakt u een nieuwe gebeurtenis die de foute vervangt, en beide blijven in de keten.

V: Hoe exporteer ik alles over entiteit X voor een inspecteur nu meteen? Open het detailpaneel van ENT-X → **Bewijspakket**. U krijgt een ZIP met manifest.json + audit_excerpt.json + entity.json + screenings.json + ubo_lookups.json + cases.json + documents/*. Overhandig de ZIP aan de inspecteur.

V: De SAR XML — is dat wat ik bij MOT indien? Nee. Het is een goAML 4.0-vormig CONCEPT voor de MLRO om over te schrijven. Echte indiening loopt via het eigen portaal van de FIU. De taak van Q-KYC is de overschrijving mechanisch te maken, niet de FIU-inname te omzeilen.

---

§10 Documentbeveiliging + mobiele opname + regelgeverskoppeling

Deze functionaliteit landde in v0.6.8 en v0.6.9. Ze zitten ONDER de workflows die u al kent uit §1–§4 — u hoeft er niet aan te raken om uw dagelijks werk te doen, maar als een toezichthouder u auditeert zijn ze het bewijs dat Q-KYC zorgvuldig is omgegaan met de bestanden die u beheert.

§10.1 Antivirus-scan op elk geüpload bestand

Elk bestand dat Q-KYC binnenkomt via `POST /documents/intake` (de **Document toevoegen**-knop in het Documenten-tabblad, de `/filing-receipts`-upload, de policy-library-upload en de mobiele camerapagina) wordt via **ClamAV** gestreamd voordat het naar schijf wordt geschreven.

- **Engine:** ClamAV (Cisco-fork) v1.5+, draait als Windows-dienst op `127.0.0.1:3310`.
- **Signaturen:** ~3,6 miljoen definities, dagelijks ververst door freshclam.
- **Faalmodus:** als clamd onbereikbaar is wordt de scanstatus opgeslagen als `skipped` in `document_intake.metadata_json.av_scan` en gaat de upload toch door — graceful degradation.
- **Reactie bij infectie:** een geïnfecteerde upload geeft **HTTP 422**, het bestand wordt **nooit naar schijf geschreven**, en het event `document_infected_rejected` wordt aan de audit-keten toegevoegd met de signatuurnaam.

§10.2 Versleuteling in rust

Elk bestand opgeslagen in `C:\ProgramData\Q-KYC\document_store\` is **Fernet-versleuteld** met een per-installatie sleutel afgeleid van `COCAI_JWT_SECRET` via HKDF-SHA256. De plaintext SHA-256 wordt apart opgeslagen in `document_intake.checksum_sha256`. Bij ophalen ontsleutelt de API, hasht de plaintext en vergelijkt — mismatch geeft HTTP 409 en logt een `document_tamper_detected`-event.

§10.3 Machine-readable-zone (MRZ)-parser

Bij upload van een **paspoort, nationale identiteitskaart, rijbewijs, verblijfsvergunning of ander identiteitsdocument** voert Q-KYC OCR uit (Tesseract) en geeft de tekst aan een ICAO 9303-parser die elk veld check-digit-valideert (`documentNumber`, `nationality`, `surname`, `givenNames`, `dateOfBirth`, `dateOfExpiry`, `personalNumber`, composite check). Bevindingen landen in `document_intake.metadata_json.mrz`; meldingen verschijnen inline in het Documenten-tabblad:

- `"document expired N day(s) ago"`
- `"document expires in N day(s)"` (bij vervaldatum < 90 dagen)
- `"MRZ composite check digit FAILED"` (OCR-fout of manipulatie)

§10.4 Mobiele camera-opname (QR-naar-telefoon)

In het Documenten-tabblad binnen de profieleditor klikt u op **Mobile upload** (-icoon). Q-KYC genereert een eenmalige 30-minuten-token, toont een QR-code; de cliënt scant deze op zijn telefoon, de telefoon opent een mobiel-geoptimaliseerde pagina met **Foto maken** (`capture="environment"`) of **Kies van apparaat**, en POSTt naar `/mobile-upload/intake` met de token. Zelfde AV-scan, zelfde Fernet-versleuteling, zelfde MRZ-parsing als desktop. Het bestand verschijnt binnen seconden in uw Documenten-tabblad.

§10.5 Integratiemodi per toezichthouder

Drie modi per toezichthouder onder **Settings → Integration mode**:

Modus	Wat het betekent	Wanneer te kiezen
Handmatig	Operator downloadt artefact, uploadt naar toezichthouder-portaal, uploadt ontvangstbewijs terug.	Standaard voor KvK SXM, FIU MOT, CBCS vandaag (zij publiceren geen programmatische intake).
Push	Q-KYC POSTt naar het endpoint van de toezichthouder zodra de MLRO op verzenden klikt.	Stel `COCAI_KVK_ENDPOINT_URL` / `COCAI_FIU_GOAML_*` / `COCAI_CBCS_ENDPOINT_URL` in zodra de toezichthouder er een uitgeeft.
Pull	Q-KYC stelt `/regulator-api/v1/*` beschikbaar voor de toezichthouder om op eigen schema op te halen. Elke read wordt vastgelegd in het **AVG Art. 30-register**.	Nu beschikbaar; genereer bearer-tokens per toezichthouder onder **Settings → Regulator pull tokens**.

Pull-endpoints vandaag beschikbaar:

```
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
```

Elke call voegt één rij toe aan `regulator_api_access_log` (het AVG Art. 30-register) EN één event aan `audit_events`.

§10.6 Multi-nationaliteit-vlag

Wanneer u een tweede nationaliteit kiest in het Identiteits-tabblad bij **Additional Nationality** verhoogt Q-KYC het risiconiveau automatisch naar **medium** (als het Low/leeg was), voegt een auto-notitie toe aan Risk Notes, en geeft een warn-toast — implementeert FATF R.10 multi-jurisdictionele scrutinie. De override blijft mogelijk; de auto-notitie blijft staan.

---

§11 Verklarende woordenlijst

Term	Betekenis
CBCS	Centrale Bank van Curaçao en Sint Maarten — geeft AML/CFT-richtlijnen uit voor DNFBPs in SXM.
CDD	Customer Due Diligence — het FATF R.10-proces van identificeren, verifiëren en risico-beoordelen van een klant.
DNFBP	Designated Non-Financial Business or Profession — accountants, belastingadviseurs, advocaten, makelaars enz. die onder AML/CFT-verplichtingen vallen.
EDD	Enhanced Due Diligence — extra toezicht voor hoogrisico-onderwerpen (PEPs, ondoorzichtige structuren, hoogrisico-jurisdicties).
FATF	Financial Action Task Force — de internationale AML/CFT-standaard-zetter.
FIU	Financial Intelligence Unit — de nationale autoriteit die SAR’s ontvangt (MOT voor Sint Maarten/Curaçao, FIU-NL voor Nederland, TRACFIN voor Frankrijk, SEPBLAC voor Spanje).
goAML	Het XML-schema van UNODC voor SAR/STR-rapportage. De meeste FIU’s accepteren goAML; sommige hebben hun eigen varianten.
KYC	Know Your Client / Customer — de upfront

Term	Betekenis
	onboarding-identificatie en verificatie.
MLRO	Money Laundering Reporting Officer — de mens binnen de firma juridisch verantwoordelijk voor SAR-beslissingen.
MOT	Meldpunt Ongebruikelijke Transacties — de FIU voor het Nederlandse Caribisch gebied (Sint Maarten + Curaçao).
PEP	Politically Exposed Person — verhoogd AML-risico volgens FATF R.12.
SAR / STR	Suspicious Activity / Transaction Report — de formele indiening bij de FIU.
Tipoff	Communicatie aan het subject (direct of indirect) dat zij onder SAR-onderzoek staan — een strafbaar feit onder Wwft art. 23.
UBO	Ultimate Beneficial Owner — de natuurlijke persoon die uiteindelijk een juridische entiteit bezit of beheerst (≥25%-drempel onder de meeste regimes).
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme — de Nederlandse AML/CFT-wet die geldt voor NL en (met lokale aanpassing) voor SXM.

Einde van handleiding. Editie 2026-05. · © 4Mfesw — alle rechten voorbehouden.