Q-KYC SXM

Manuel d’utilisation

Version 0.6.14 · Édition 2026-06-03

Déployé chez : **the Tenant Firm** · Sint Maarten

Développé et maintenu par : **4Mfesw** *Modern, Methods Made and Maintained · Fiber, Software, WorkFlows, Energy* Sint Maarten

---

Classification du document

`CONFIDENTIEL — RESTREINT`

Ce manuel contient des détails opérationnels d’un système de conformité LCB-FT. Diffuser uniquement à :

- Le personnel ayant des rôles de conformité assignés dans le cabinet déployant
- Les superviseurs CBCS / SRC MOT lors d’inspections programmées
- L’auditeur externe désigné par le cabinet sous accord de mission

Non destiné à la diffusion publique.

Droits d’auteur

© 2026 4Mfesw. Tous droits réservés. Aucune partie de ce document ne peut être reproduite, distribuée ou transmise sous quelque forme ou par quelque moyen que ce soit sans l’autorisation écrite préalable de 4Mfesw, à l’exception de brèves citations dans des analyses critiques et certains autres usages non commerciaux autorisés par le droit d’auteur.

Contrôle documentaire

Champ	Valeur
Titre	Q-KYC SXM Manuel d’utilisation
Propriétaire	4Mfesw
Approbateur	_____
Émis	2026-06-03
Prochaine révision	2026-12-03 (ou plus tôt si modification substantielle)
Version	v0.6.14
Source de vérité	`docs/USER_MANUAL.md` (anglais)

Champ	Valeur
Traductions	NL, FR, ES — vérifier contre la version anglaise avant usage régulateur

Comment lire ce manuel

Ce manuel est un **livre de tâches**. Il vous apprend les quatre travaux que Q-KYC existe pour faire, dans l'ordre où vous les ferez sur de vrais dossiers clients :

	Parcours	Sujet du parcours
§1	**Onboarding KYC** — ouvrir un nouveau dossier client de bout en bout	ENT-001 Maria Velasquez (résidente SXM, faible risque)
§2	**Escalade LCB-FT + DOS** — ce qui se passe lors d'un signal de criblage	ENT-003 Roman Voloshyn → CASE-2026-001
§3	**Déclaration UBO + extrait de registre** — bénéficiaires effectifs des structures opaques	ENT-004 Coral Holdings Ltd. (Trust BVI)
§4	**Dossier de preuve** — ce que vous remettez à l'inspecteur lorsqu'il écrit à 16h00	ENT-005 Domino Marine Services BV (NL)

Chaque parcours a des étapes numérotées. Chaque étape a une capture d'écran. L'anneau rouge sur la capture est ce que vous cliquez ensuite. Lisez le texte, cliquez ce que l'anneau montre, passez à la suivante.

Les parcours utilisent les **données de démonstration livrées**. Avant votre premier vrai client, votre administrateur de tenant doit :

1. Câbler les vrais connecteurs criblage / PEP / UBO sous **Paramètres → Connecteurs**. Le bandeau jaune *« Fournisseurs mock actifs — connectez des fournisseurs externes avant l'usage en production »* vous signale tant que vous êtes sur des stubs.
2. Créer des comptes opérateurs sous **Paramètres → Utilisateurs** (ou exécuter `scripts/create_superadmin.py` une fois sur le serveur).
3. Définir un `COCAI_JWT_SECRET` fort avant tout déploiement pilote.

Après cela : mêmes écrans, mêmes boutons, même chaîne d'audit — avec de vraies versions de listes et de vraies lignes de registre en dessous.

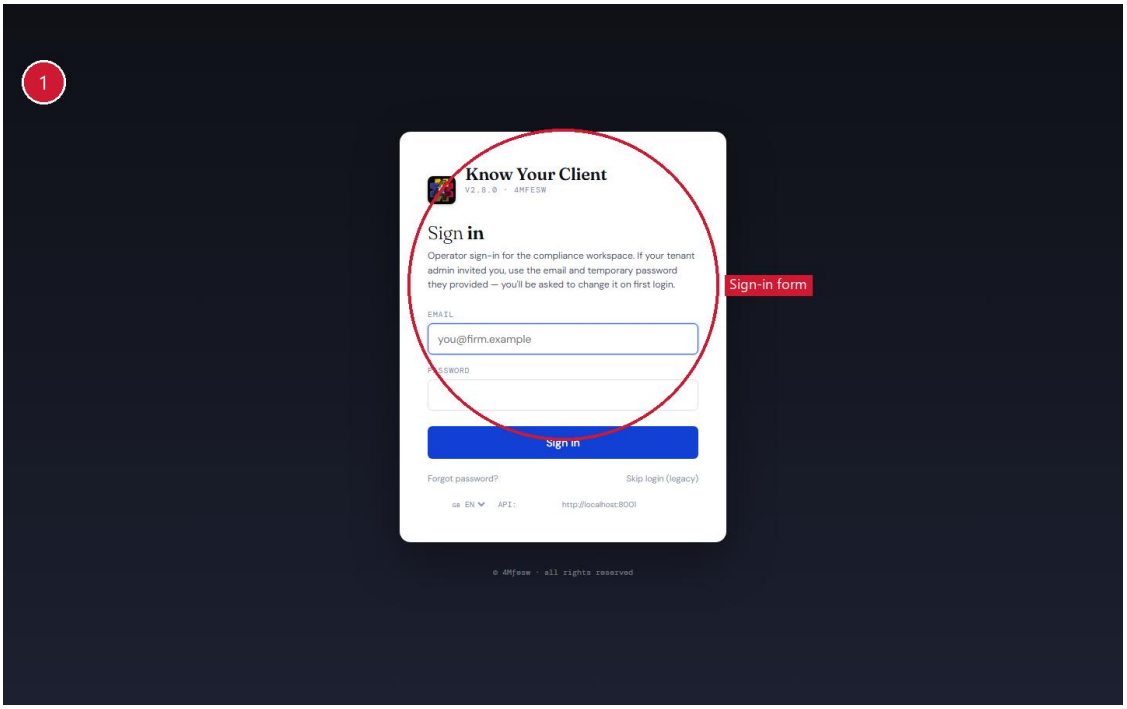
Ce que Q-KYC NE fait PAS. Il ne dépose pas de DOS auprès du SRC pour vous. Il récupère quotidiennement 9 sources gouvernementales officielles de sanctions directement depuis les URL des éditeurs — OFAC SDN + Consolidated, ONU, UE, UK HMT OFSI, Justice Canada, SECO Suisse. Les surcouches commerciales PEP / médias défavorables (OpenSanctions, Refinitiv, Dow Jones, ComplyAdvantage) sont optionnelles et fournies par le client via **Paramètres → Connecteurs**. Il ne certifie pas les documents. Il ne vous donne aucune dispense au titre de GAFI / Wwft / EPNFD / CBCS — votre MLRO reste la personne responsable devant le régulateur. Ce que Q-KYC fait, c'est consigner le travail *honnêtement* dans une piste d'audit immuable et chaînée par hash, pour que lorsque l'inspecteur arrive, vous puissiez lui remettre un seul dossier et prouver chaque geste.

---

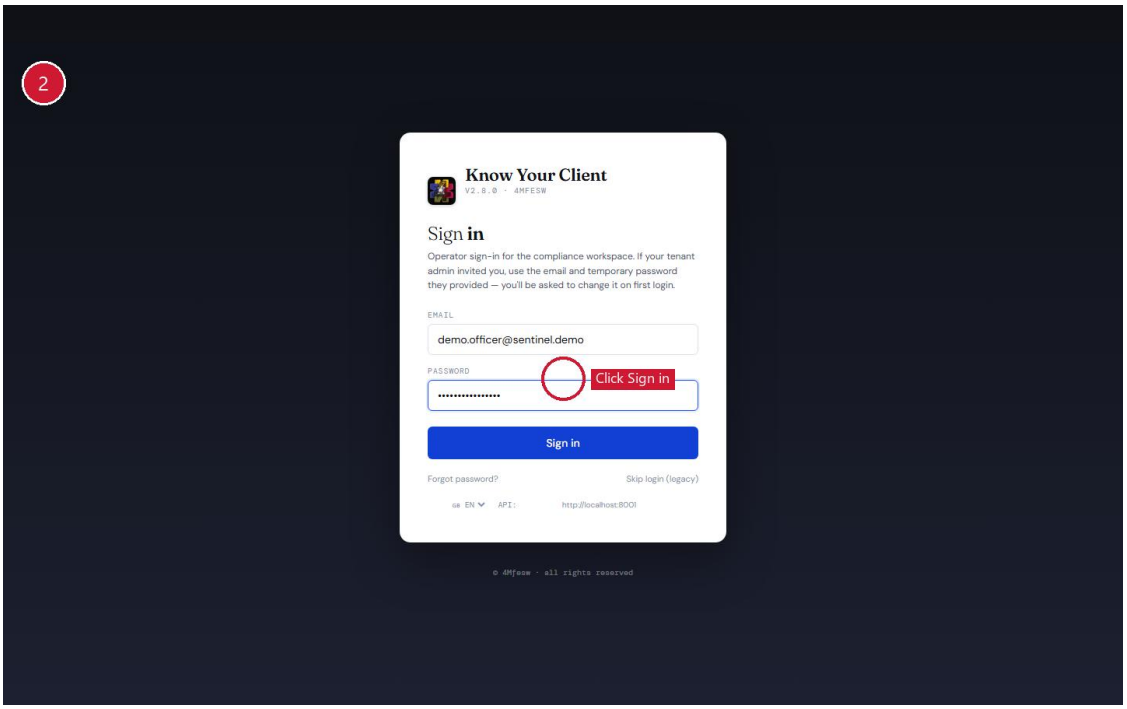
§0 Première connexion (5 minutes)

Votre administrateur de tenant aura créé un compte pour vous et envoyé un mot de passe temporaire par e-mail. Vous serez invité à le changer lors de la première connexion.

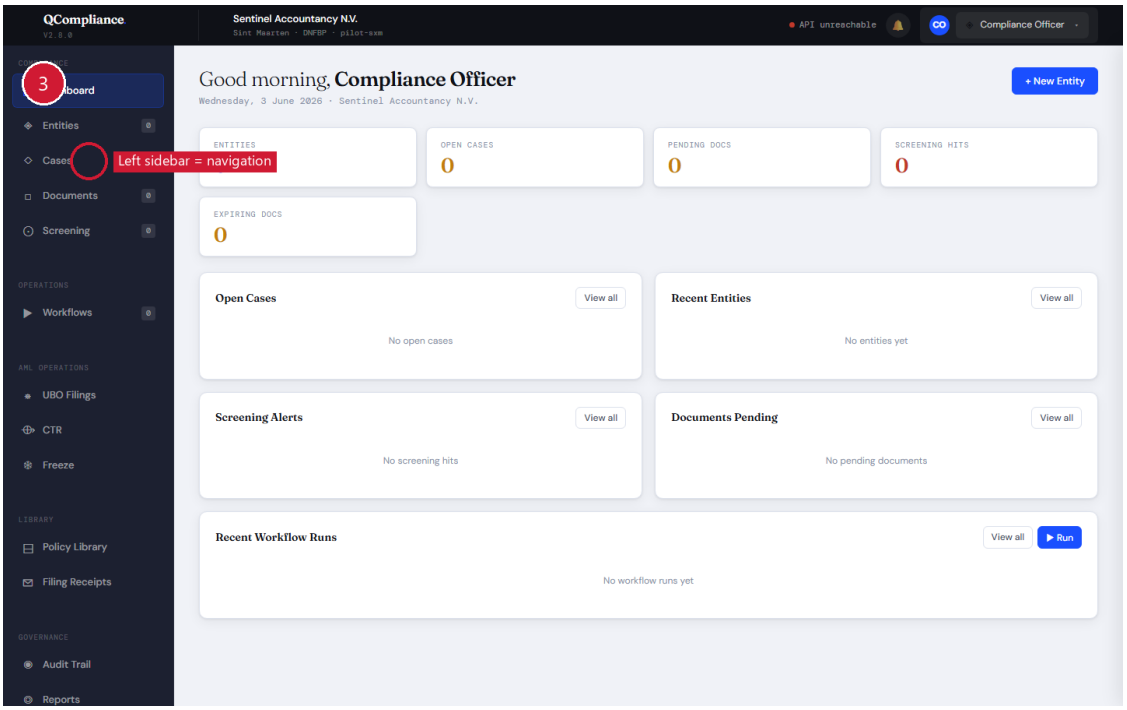
1. Ouvrez l'URL fournie par votre administrateur (pendant le pilote : `http://localhost:8001`).
2. Vous voyez ceci :



3. Saisissez votre e-mail et le mot de passe temporaire. Le bouton Se connecter s'active dès que les deux champs sont remplis.



1. Après connexion vous arrivez sur le **Tableau de bord** :



Les cinq tuiles en haut résument l'état de conformité de votre cabinet d'un coup d'œil : **Entités**, **Dossiers ouverts**, **Documents en attente**, **Correspondances de criblage**, **Documents expirants**. Le bandeau jaune *« Fournisseurs mock actifs — connectez des fournisseurs externes avant l'usage en production »* reste visible jusqu'à ce que votre administrateur connecte les vrais fournisseurs criblage / PEP /

UBO sous **Paramètres → Connecteurs**. Le panneau État des fournisseurs en dessous nomme exactement quelles fentes de connecteur sont mock, réelles ou pas encore configurées.

2. La **barre latérale gauche est votre seule navigation** :
    - **Conformité** — Tableau de bord, Entités, Dossiers, Documents, Filtrage
    - **Opérations** — Processus
    - **Gouvernance** — Piste d'audit, Révisions dues, Rapports
    - **Système** — Paramètres, Manuel utilisateur

C'est tout. Choisissez maintenant un parcours.

---

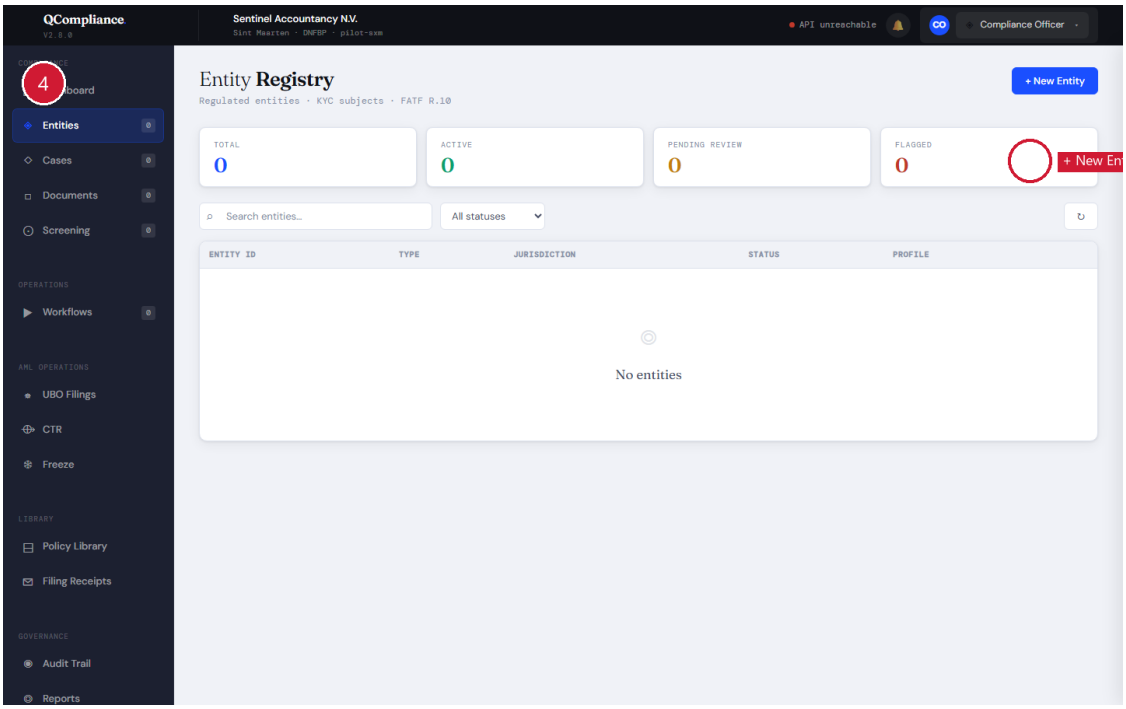
§1 Onboarding KYC (Parcours 1)

Objectif : ouvrir un nouveau dossier client de bout en bout, avec au moins un document d'identité au dossier, une notation de risque explicite, et une date de révision périodique fixée — tout ce qu'un inspecteur demandera comme preuve que vous avez effectué la CDD avant le début de la relation (GAFI R.10 / Wwft art. 3 / CBCS LCB-FT §4.1).

Sujet : ENT-001 Maria Velasquez — résidente SXM, salariée, aucune exposition PEP, classification faible risque.

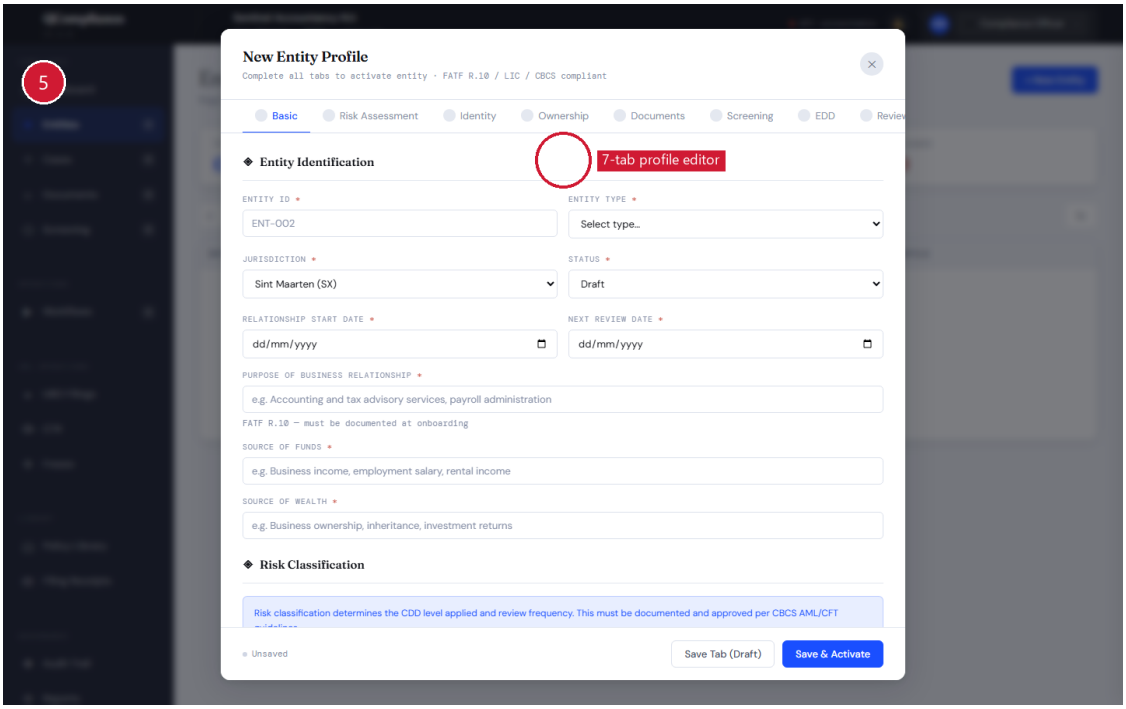
Étape 1 — Ouvrir le Registre des Entités

Cliquez **Entités** dans la barre latérale. Vous voyez chaque partie régulée dont votre cabinet a le dossier, avec son type, sa juridiction, son statut actuel et la complétude CDD. Nouveau dossier ? Cliquez **+ Nouvelle entité** en haut à droite.



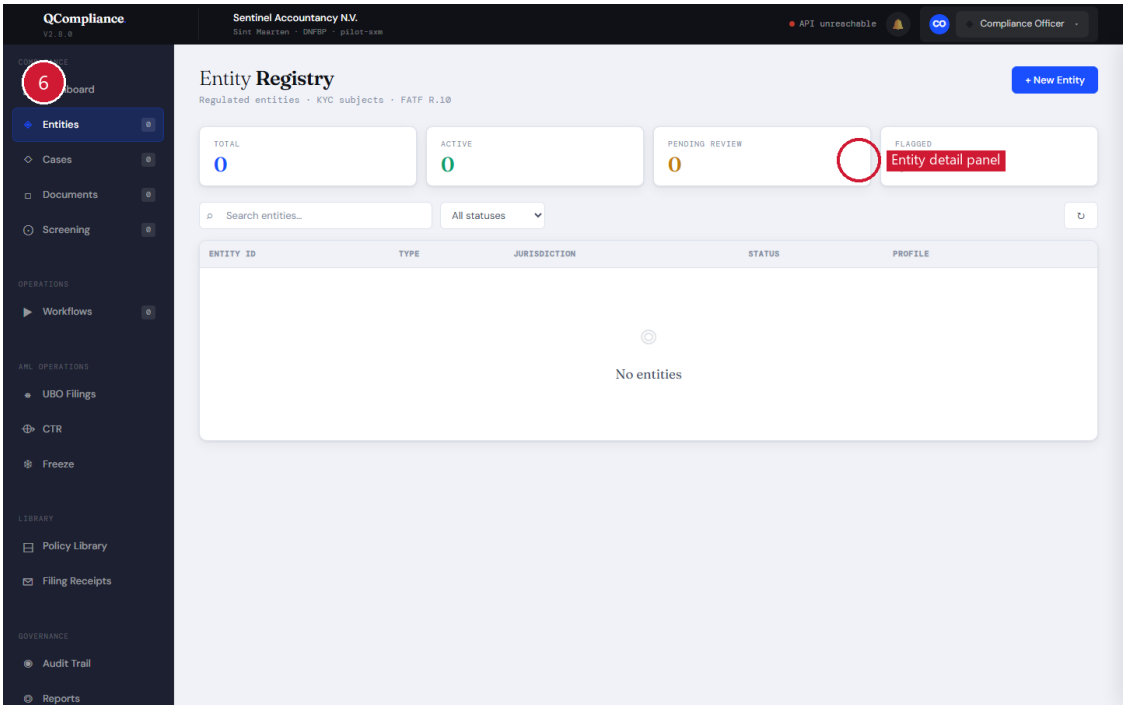
Étape 2 — Ouvrir l'éditeur de profil

L'éditeur de profil est l'endroit où vous consignez *tout* sur un client. Sept onglets (Basique, Identité, Propriété, Documents, Filtrage, EDD, Révision) et les boutons **Enregistrer onglet** / **Enregistrer & activer** en bas.



Étape 3 — Choisir une entité existante à étudier

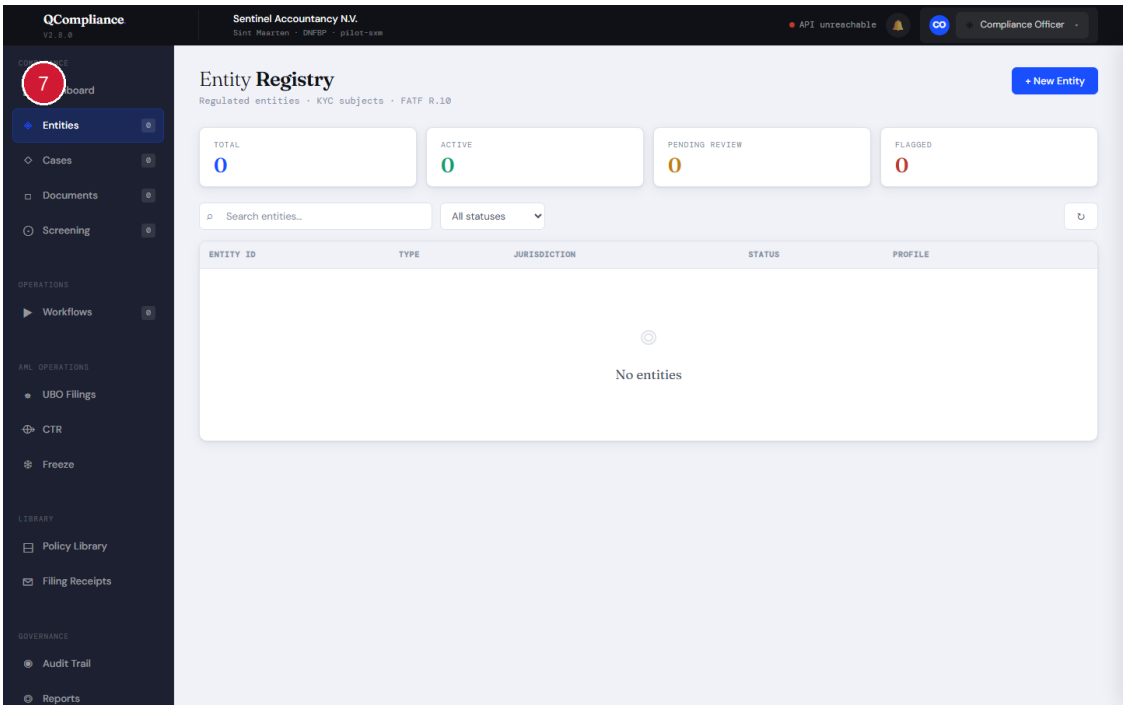
Pour ce parcours nous ouvrons le sujet de démo ENT-001 (Maria Velasquez). Cliquez la ligne, le panneau de détail droit glisse à l'intérieur :



Le panneau de détail résume **qui** (Entity ID, Type, Juridiction, Statut, État de verrouillage tipoff) et **quoi** (Niveau de risque, Niveau CDD, Objet de la relation, Origine des fonds, Agent assigné, Prochaine date de révision). Boutons d'action en bas : **Modifier le profil**, **Exécuter le processus**, **Recherche UBO**, **Ouvrir un dossier**, **Dossier de preuve**, **Rédiger DOS** (les deux derniers n'apparaissent que lorsque pertinents).

Étape 4 — Onglet Basique : qui ils sont

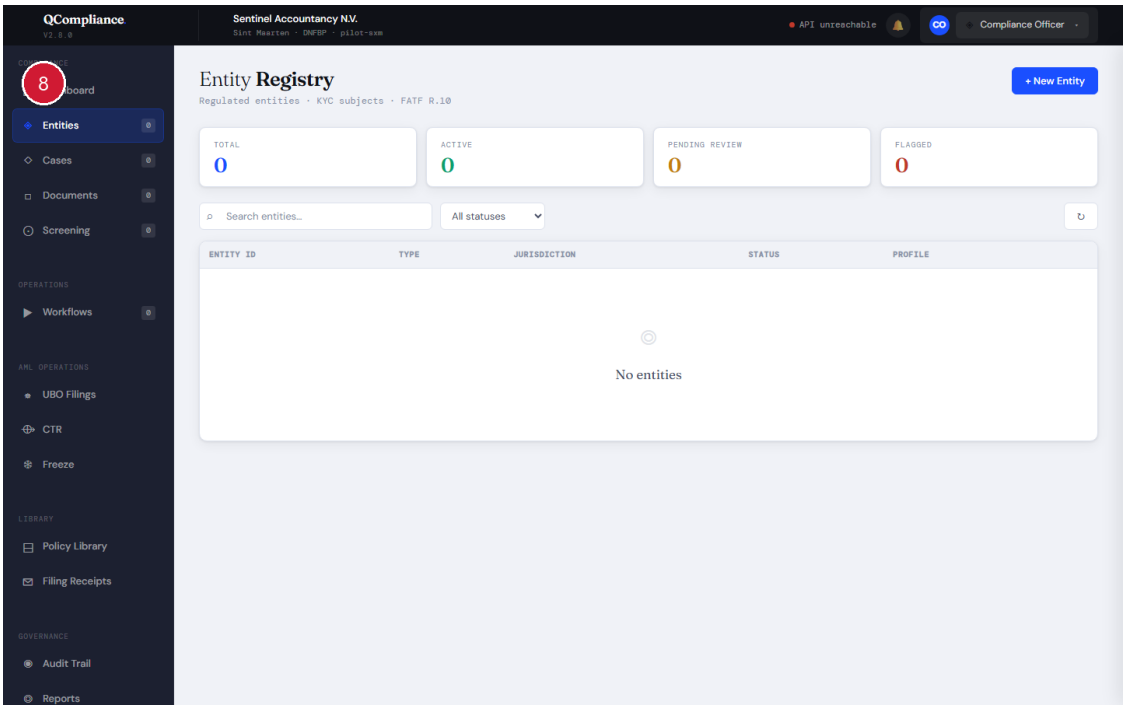
Cliquez **Modifier le profil** pour ouvrir l'éditeur à sept onglets.



C’est le territoire de GAFI R.10 : - **Entity ID / Type** — handle interne + NaturalPerson / LegalEntity / Trust / Foundation / VASP / DNFBP, etc. - **Juridiction / Statut** — juridiction enregistrée + draft / pending_review / active / blocked / frozen - **Début relation / Prochaine révision** — quand la CDD fut achevée et quand elle doit être refaite - **Objet de la relation d’affaires** — exigé par les règles Wwft / DNFBP - **Origine des fonds / Origine du patrimoine** — exigé pour les sujets à risque moyen et élevé

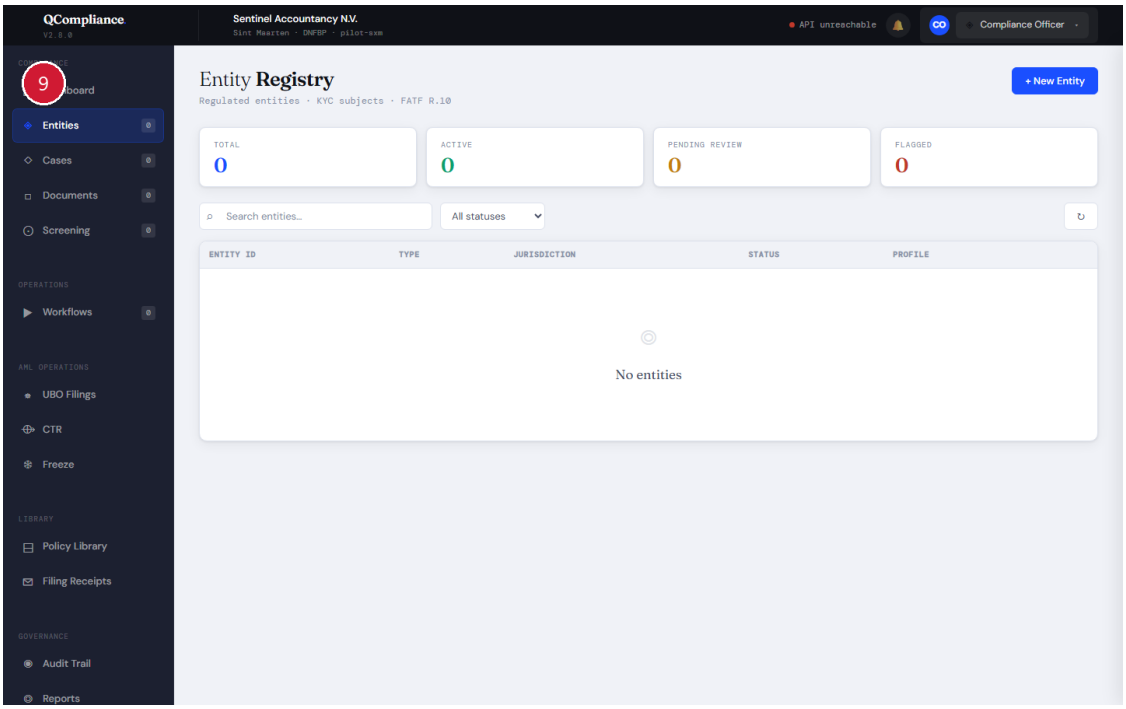
Étape 5 — Onglet Identité : documents d’identité

L’onglet Identité est l’endroit où vous capturez passeport, carte d’identité, permis de conduire, ou tout autre document d’identité. Chaque entrée enregistre : - Type de document + numéro + pays d’émission - Date d’émission + date d’expiration (Q-KYC alerte lorsque l’expiration est dans les 90 jours) - Méthode de vérification (en personne, vidéo, à distance) - Agent qui a vérifié, quand



Étape 6 — Onglet Documents : téléversements de fichiers

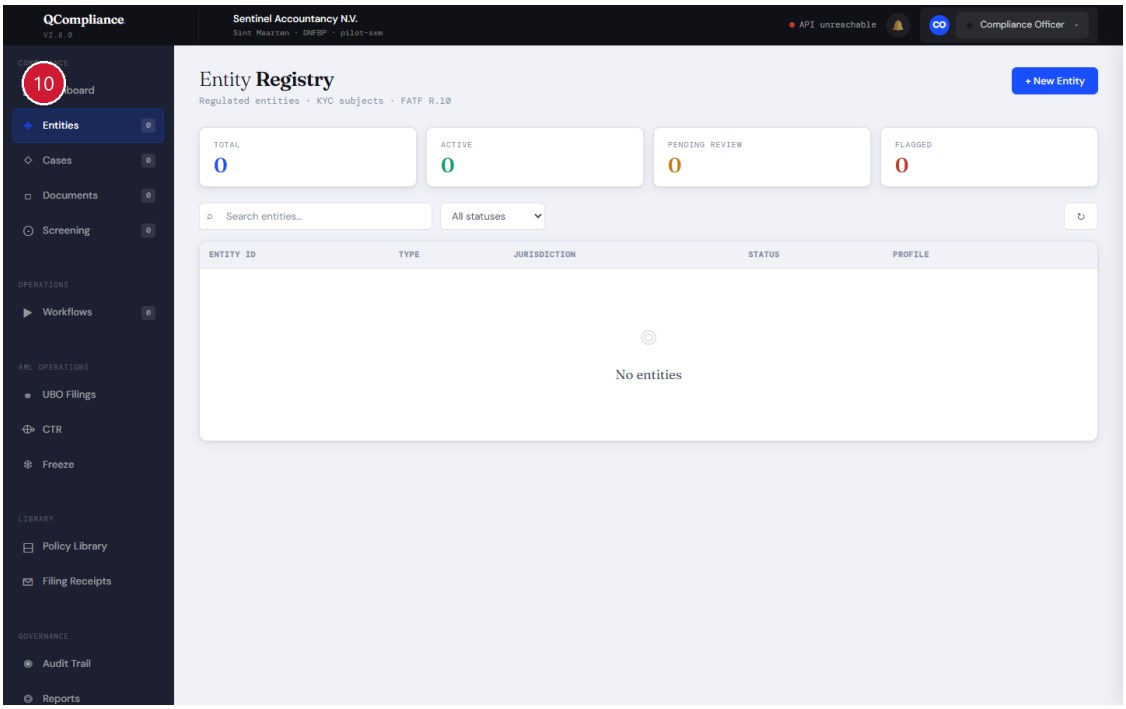
Là où l'onglet Identité enregistre les métadonnées, l'onglet Documents est le vrai stockage de fichiers : PDF scannés, extraits KvK, formulaires de déclaration UBO. Chaque fichier téléversé reçoit : - Une somme de contrôle SHA-256 immuable (pour pouvoir prouver plus tard qu'il n'a pas été remplacé) - Un binaire stocké sur le serveur (jamais écrasé) - Un événement d'audit `document_intake` avec l'opérateur, l'horodatage et le type de document



L'infobulle bleue en haut — *« Tous les documents d'identité doivent être vérifiés. Consignez la référence du document, la méthode de vérification, et l'agent qui a vérifié. »* — est le rappel GAFI R.10 que vous verrez dans tout l'éditeur.

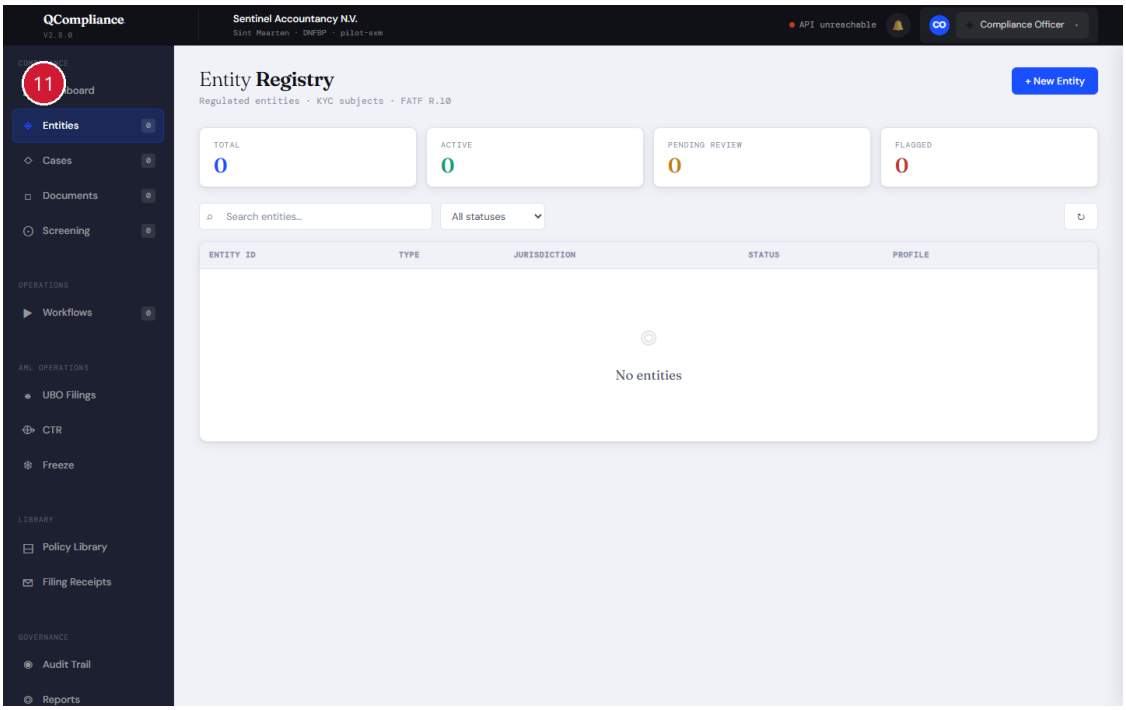
Étape 7 — Onglet Filtrage : lier les exécutions

Chaque entité est reliée à chaque exécution de criblage faite contre elle. Même des exécutions d'il y a un an sont encore là, avec les versions exactes de listes consultées à l'époque (traçabilité GAFI R.10).



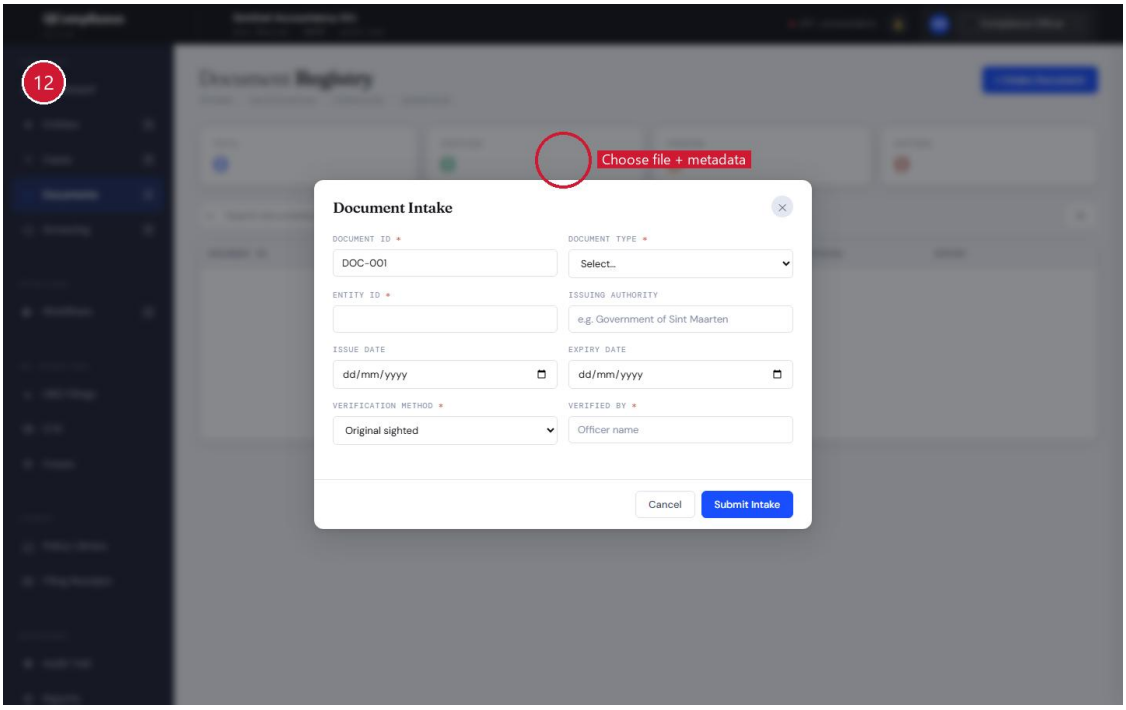
Étape 8 — Onglet Révision : risque + achèvement CDD

L'onglet Révision est le résumé conformité de l'opérateur : - **Niveau de risque** (FAIBLE / MOYEN / ÉLEVÉ) — pilote l'intervalle de révision périodique (24m / 12m / 3–6m par défaut) - **Facteurs de risque** — les puces cochées lors de l'évaluation - **Achèvement CDD** — date, méthode, agent - **Prochaine révision périodique** — calculée automatiquement à partir du niveau de risque, modifiable



Étape 9 — Réceptionner un document hors de l’éditeur de profil

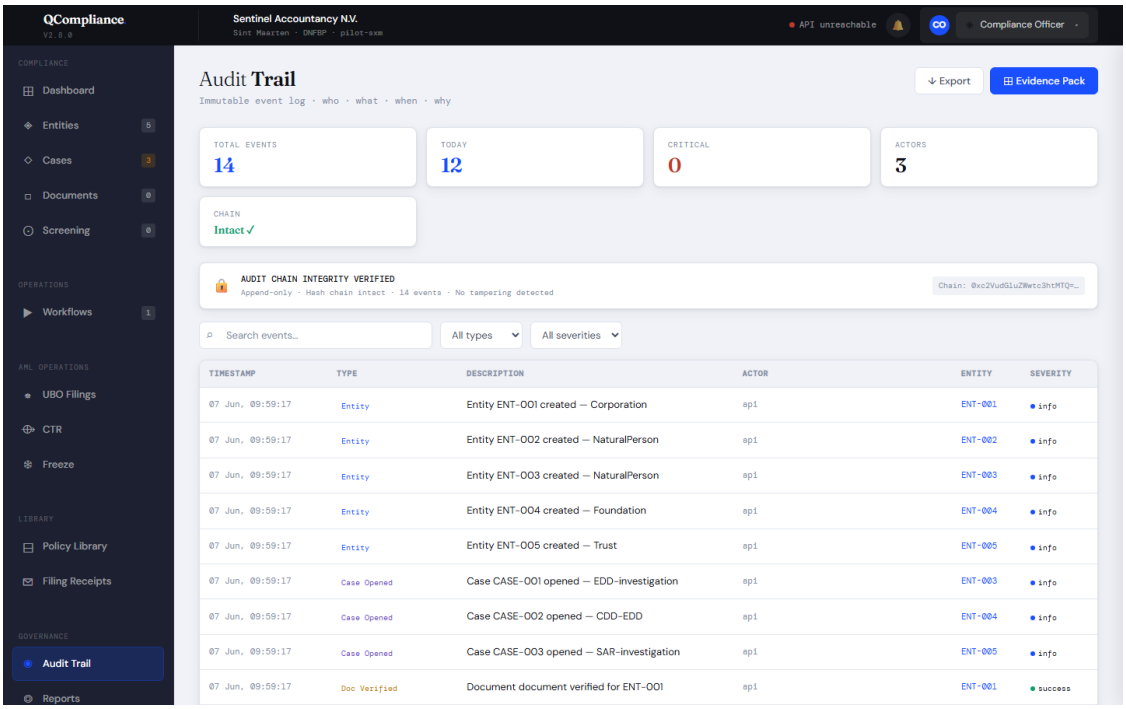
Parfois l’opérateur reçoit un document par e-mail ou téléversement scanné et veut l’enregistrer avant d’ouvrir le profil complet. Utilisez **Documents → + Nouvelle réception** :



Vous choisissez l’entité, le type de document, optionnellement lié à un dossier ouvert, et téléversez. Le système stocke le fichier, calcule la somme de contrôle et écrit un événement d’audit `document_intake`.

Étape 10 — Vérifier la piste d’audit immuable

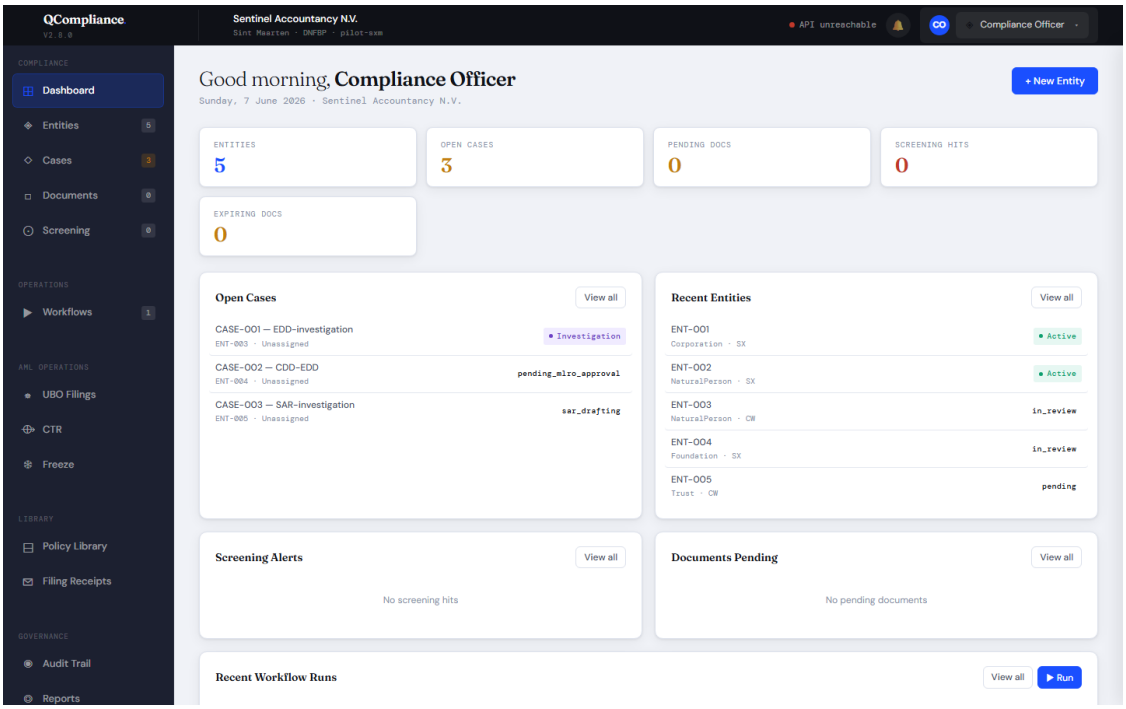
Cliquez **Piste d’audit** dans la barre latérale. Chaque action de chaque opérateur depuis le déploiement du système est ici, en ordre append-only, avec une chaîne de hash sur l’ensemble.



Les colonnes sont **Heure · Type · Description · Acteur · Entité · Sévérité**. L'acteur est l'e-mail de l'humain qui a agi (`compliance.officer@4mfesw.nl`, `mlro@4mfesw.nl`), ou `system` pour les entrées automatiques (file de révision périodique, tâches planifiées). La bande « AUDIT CHAIN INTEGRITY VERIFIED » sous les tuiles de statistiques est le cachet d'anti-falsification pour l'inspecteur.

Étape 11 — Révisions dues : la file CDD périodique

La page Révisions dues liste chaque entité dont la `next_review_date` est en retard ou dans les 30 prochains jours. ENT-005 dans nos données de démo est en retard de 4 jours (intentionnel, pour peupler cet écran) :



C’est la CDD continue GAFI R.10. Traitez la file chaque semaine : ouvrez l’entité, re-vérifiez, fixez une nouvelle date de révision, journalisez un événement `periodic_review_completed`.

> **§1 points-clés** - Chaque champ de formulaire que vous voyez existe pour une raison réglementaire ; les infobulles bleues nomment la raison. - Chaque changement est capturé dans la chaîne d’audit — il n’y a pas d’« annuler » parce qu’il n’y a pas de « réécrire ». Vous créez une nouvelle entrée qui remplace l’ancienne et les deux restent. - Rien ne quitte l’écran tant que vous ne cliquez pas **Enregistrer onglet** ou **Enregistrer & activer**, et même alors l’enregistrement plus ancien est conservé via la piste d’audit.

---

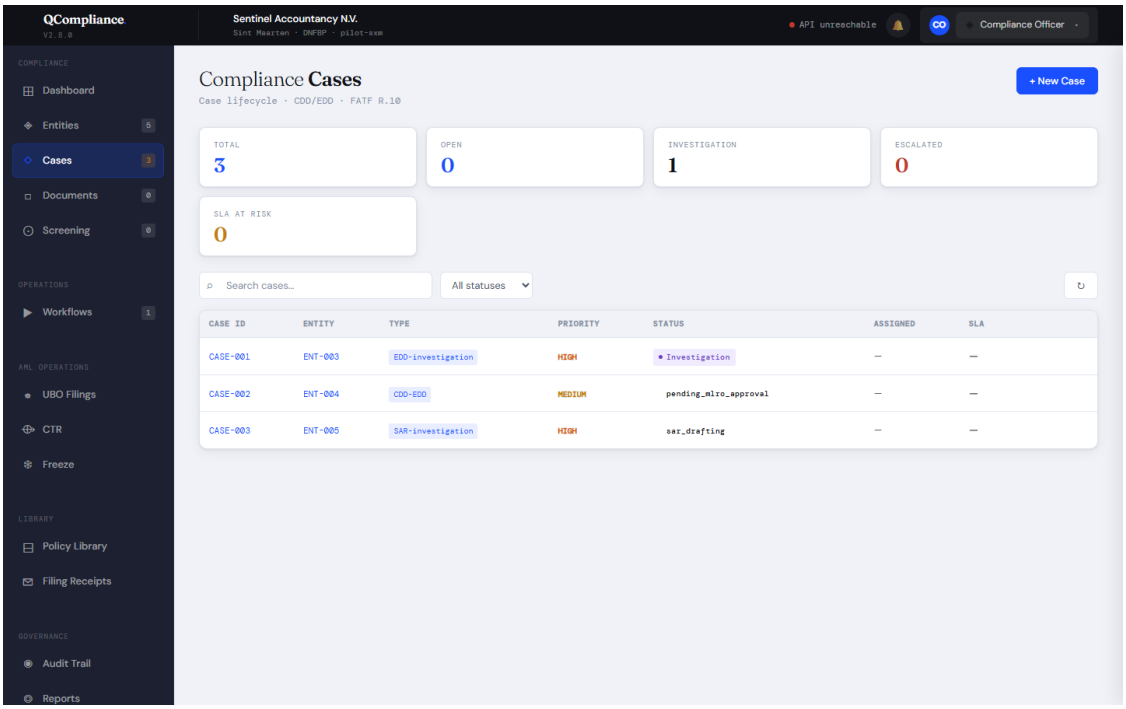
§2 Escalade LCB-FT + DOS (Parcours 2)

> **Objectif :** prendre un signal de criblage, escalader au MLRO, obtenir l’approbation explicite du MLRO, générer un brouillon de DOS au format goAML XML, et verrouiller le sujet sous tipoff (Wwft art. 23). Chaque étape ici est ce qu’un inspecteur Wwft reconstruira depuis la piste d’audit lorsqu’il demandera « montrez-moi comment CASE-X a été traité ».

Sujet : ENT-003 Roman Voloshyn → CASE-2026-001 (escaladé, P1).

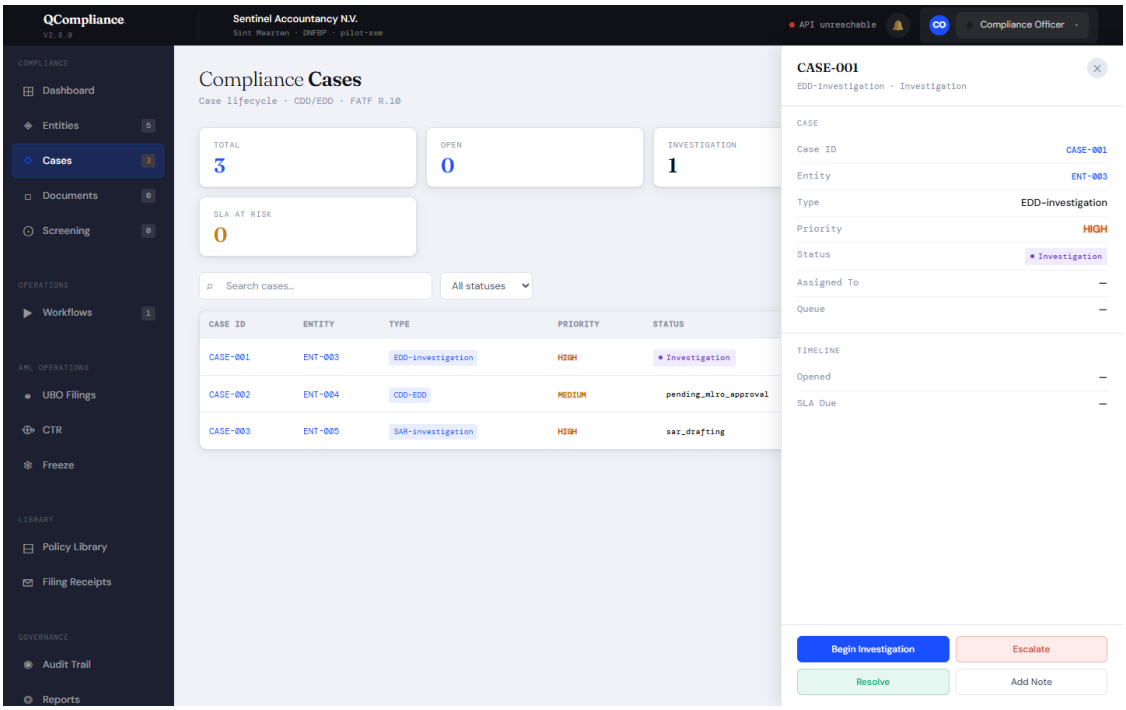
Étape 1 — Ouvrir les Dossiers

Cliquez **Dossiers** dans la barre latérale. CASE-2026-001 est en haut avec le badge rouge **Escaladé** :



Étape 2 — Détail du dossier (vue agent)

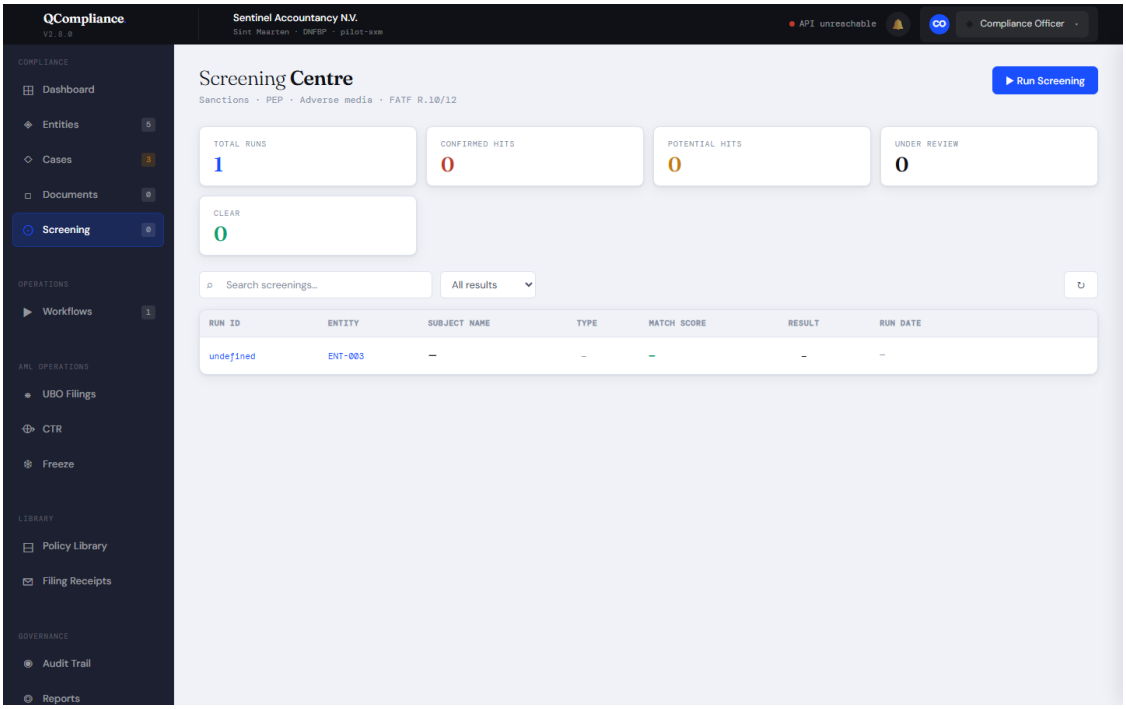
Cliquez dans CASE-2026-001. Le panneau de détail droit montre tout sur le dossier : type, entité, priorité, statut, file, et une section dédiée RÉVISION MLRO que l'opérateur ne peut contourner.



En tant qu'agent de conformité, vous pouvez **Demander une révision MLRO** ici mais vous ne pouvez pas approuver. Seul le MLRO le peut — Q-KYC l'impose dans le backend avec un 403 si un non-MLRO appelle `/cases/{id}/mlro-approve`.

Étape 3 — Pourquoi ce dossier a-t-il été ouvert ? Le signal de criblage

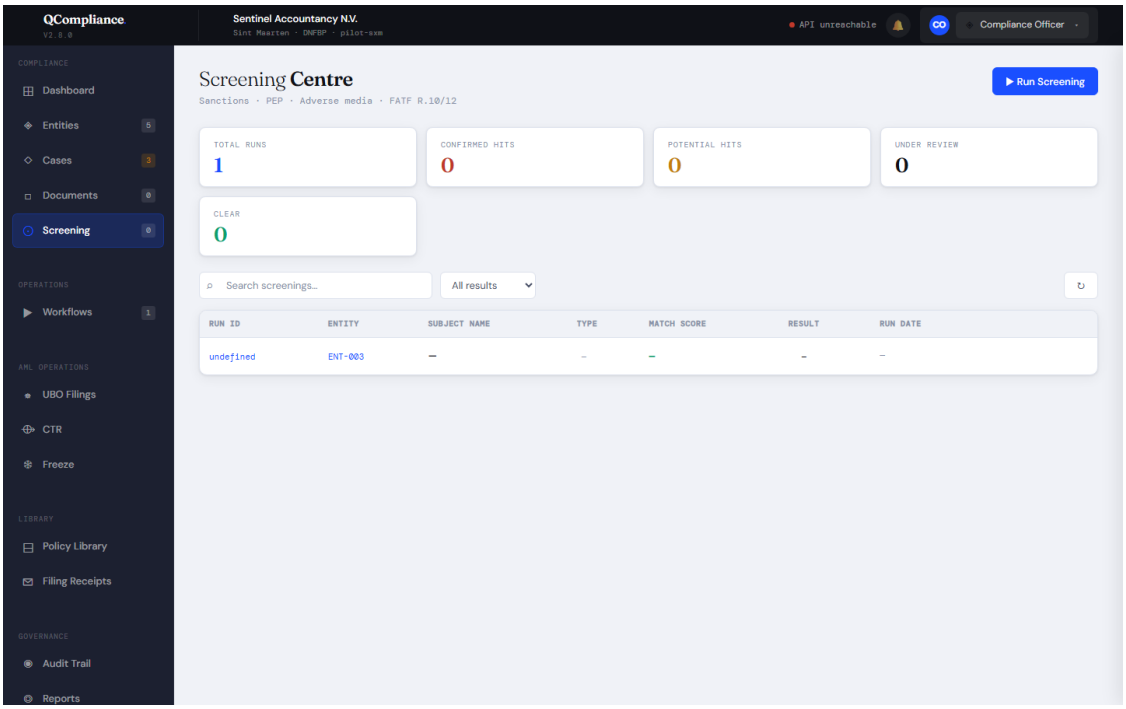
Cliquez **Filtrage** dans la barre latérale et ouvrez SCR-2026-0001 (l'exécution qui a déclenché CASE-2026-001) :



Le panneau de détail montre : - **Fournisseur** — quel connecteur a effectué la vérification. Pour les sources intégrées, affiche `real_sanctions_local` (recherche floue contre les 9 sources gouvernementales que Q-KYC rafraîchit quotidiennement). Les surcouches commerciales optionnelles (Refinitiv Worldcheck, Dow Jones, ComplyAdvantage) se superposent lorsque vous avez un abonnement câblé - **2 correspondances** — UE 2022/1530 (mesures restrictives secteur défense, score 0,97) et OFAC SDN Sanctions liées à l'Ukraine (score 0,94) - **Correspondances PEP** — associé proche d'un fonctionnaire désigné, depuis 2014 - **Adverse media** — article Reuters 2024-03-11

Étape 4 — Traçabilité du criblage (trace GAFI R.10)

Faites défiler le détail du criblage jusqu'au bas. Les champs **lists_checked** + **list_versions** sont des preuves non-négociables sous GAFI R.10 — ils enregistrent *exactement* quelles listes de sanctions ont été interrogées, et l'horodatage de version de chaque liste au moment de l'exécution.

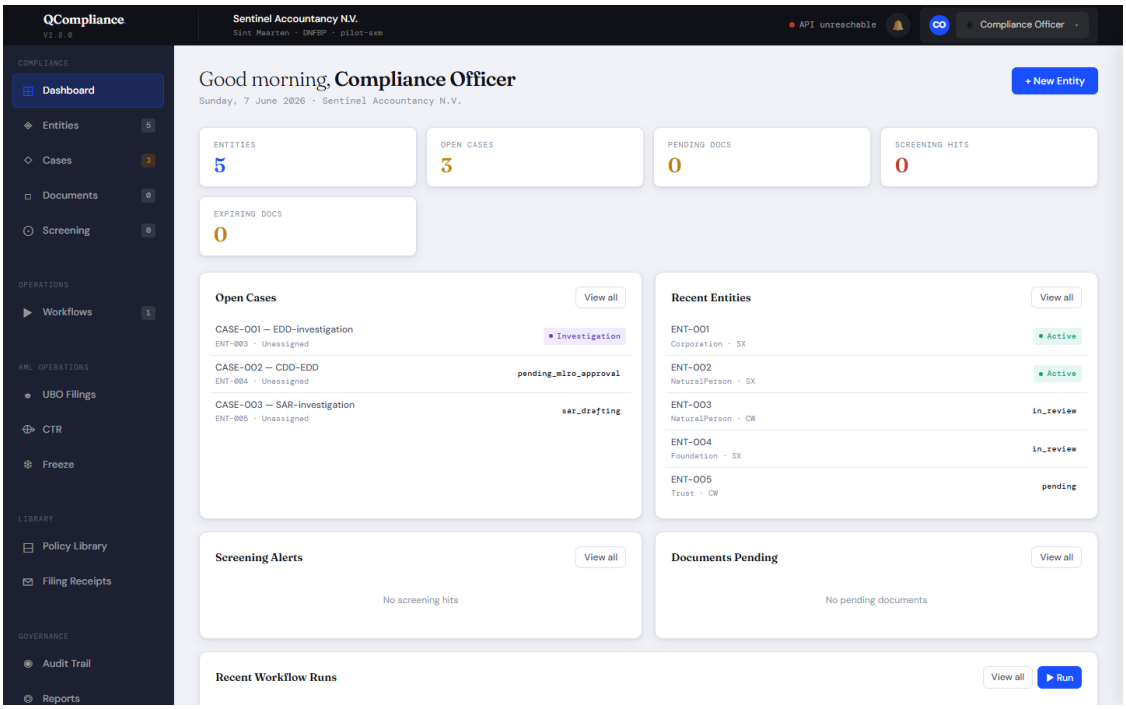



```
OFAC_SDN:                    2026-05-13T08:00:00Z
EU_CONSOLIDATED:             2026-05-13T06:30:00Z
UN_SECURITY_COUNCIL:         2026-05-12T22:15:00Z
UK_HMT:                      2026-05-13T07:45:00Z
WORLDCHECK_PEP:              2026-05-13T05:00:00Z
DOW_JONES_ADVERSE_MEDIA:2026-05-13T05:30:00Z
```

Vous ne pouvez pas les modifier. Vous ne pouvez que montrer l'original à l'inspecteur.

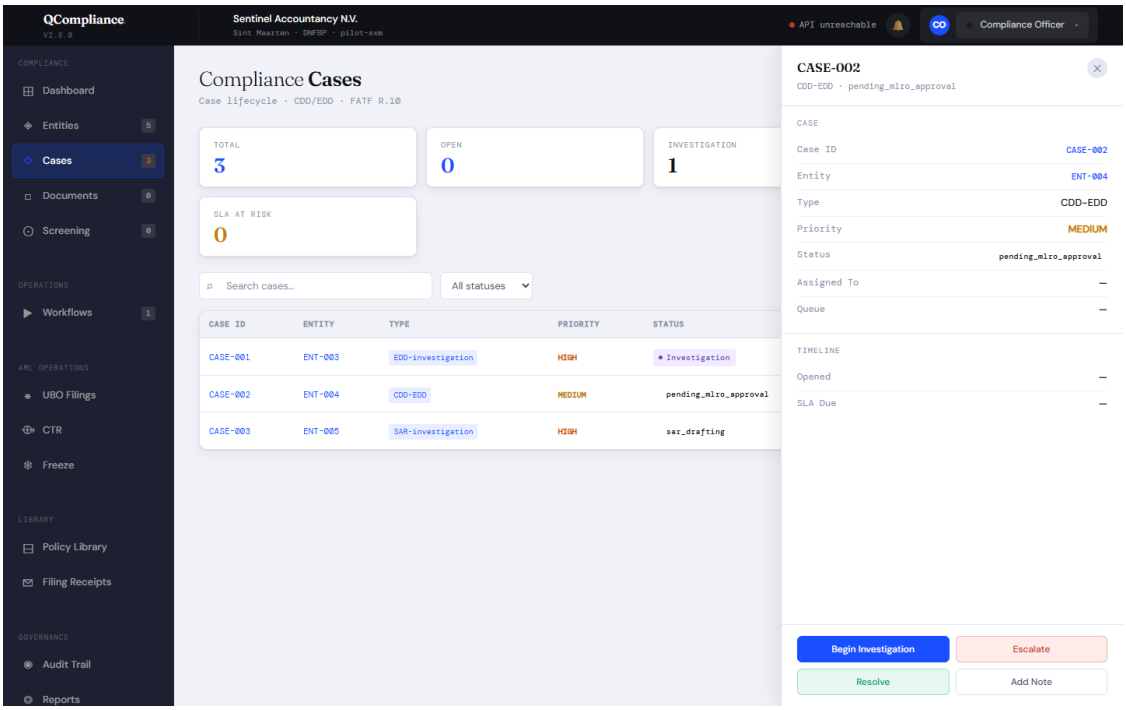
Étape 5 — Se connecter en tant que MLRO

Le MLRO est un autre humain avec sa propre connexion. Sous Wwft art. 16, seul le MLRO peut autoriser une escalade ou signer une DOS. Déconnectez-vous et reconnectez-vous :



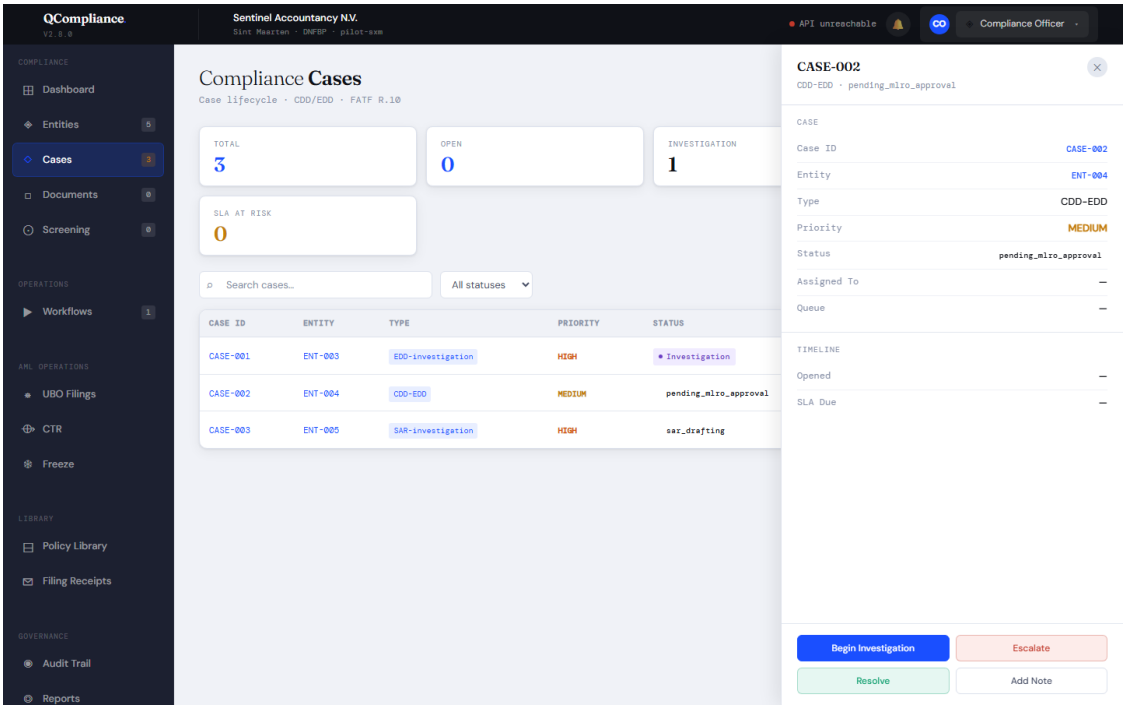
Étape 6 — Détail du dossier (vue MLRO)

Ré-ouvrez CASE-2026-001. Deux nouveaux boutons apparaissent en bas de la section RÉVISION MLRO : **MLRO Approuver** (vert) et **MLRO Rejeter** (rouge). L'agent de conformité ne les a jamais vus.



Étape 7 — Le MLRO approuve

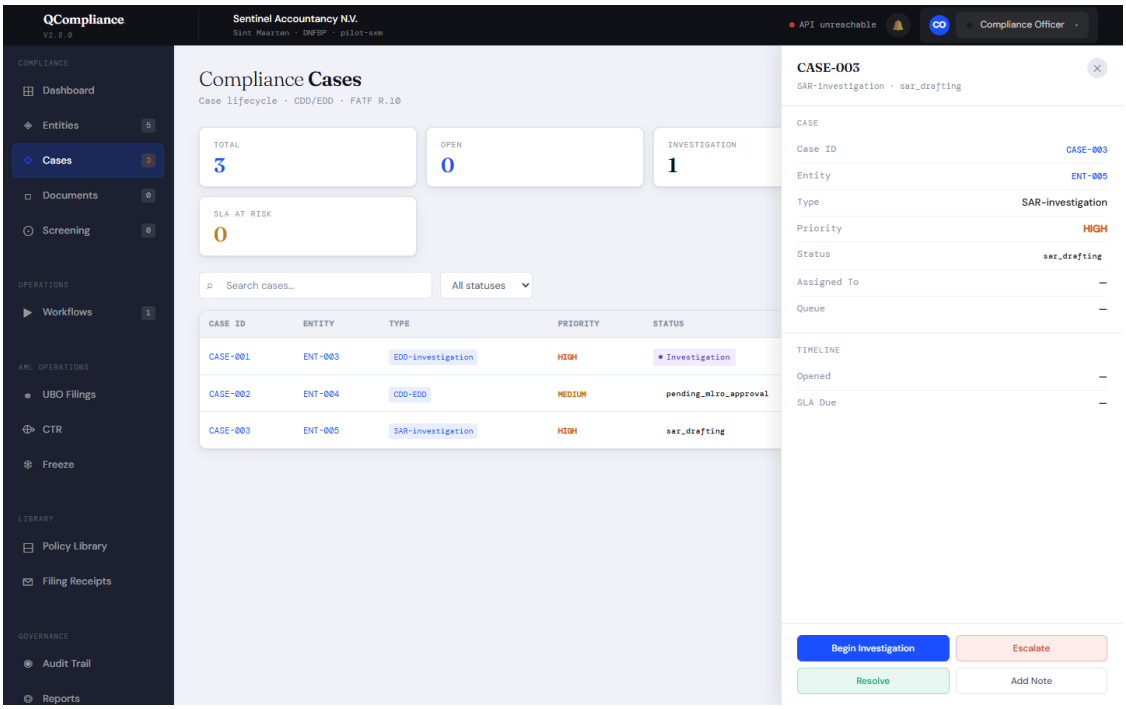
Cliquez **MLRO Approuver**. On vous demande des notes (votre justification écrite, conservée à jamais dans la piste d'audit). Le système forge une référence d'approbation comme `MLRO-B27E6A0C03`, estampille l'e-mail de l'approbateur, enregistre l'horodatage, et déverrouille le bouton **Rédiger DOS (MLRO approuvé)**.



Si à un moment quelconque un agent ou un développeur tente de falsifier ceci par une écriture directe en base, le hash de la chaîne d'audit ne correspondra plus.

Étape 8 — Rédiger la DOS

Cliquez **Rédiger DOS (MLRO approuvé)**. Le formulaire de brouillon se pré-remplit depuis les données du dossier + entité et demande le récit de suspicion + codes de typologie. Le bandeau rouge en haut est une lecture obligatoire :

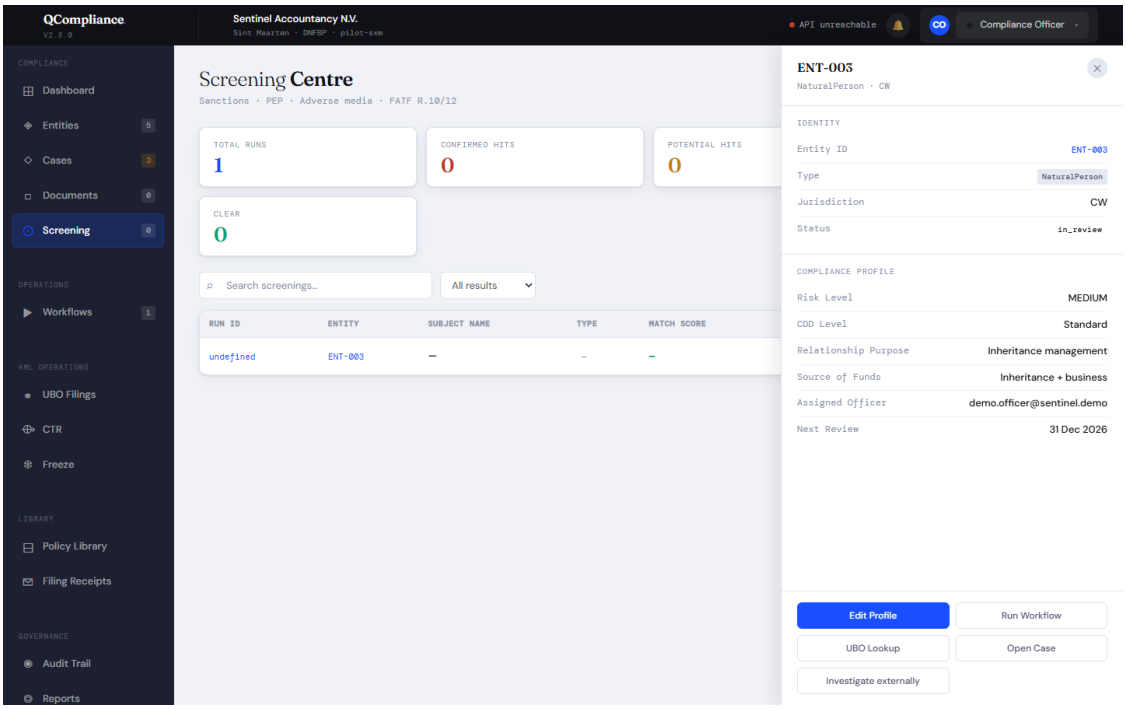


> *« Q-KYC ne dépose pas de DOS. Ceci génère un paquet de BROUILLON seulement. L'agent de conformité doit le convertir au format requis du SRC (par ex. goAML XML pour MOT) et le soumettre via le canal sécurisé du SRC.* ***Ne signalez pas le sujet. Restreignez l'accès à ce dossier et évitez les changements dans la relation qui pourraient l'alerter.*** *»*

Codes de typologie disponibles : `STR_STRUCT`, `STR_LAYER`, `STR_INTEG`, `STR_ANOM_WIRE`, `STR_CASH`, `STR_PEP`, `STR_SANC`. Vous pouvez en cocher plus d'un.

Étape 9 — Le verrou tipoff

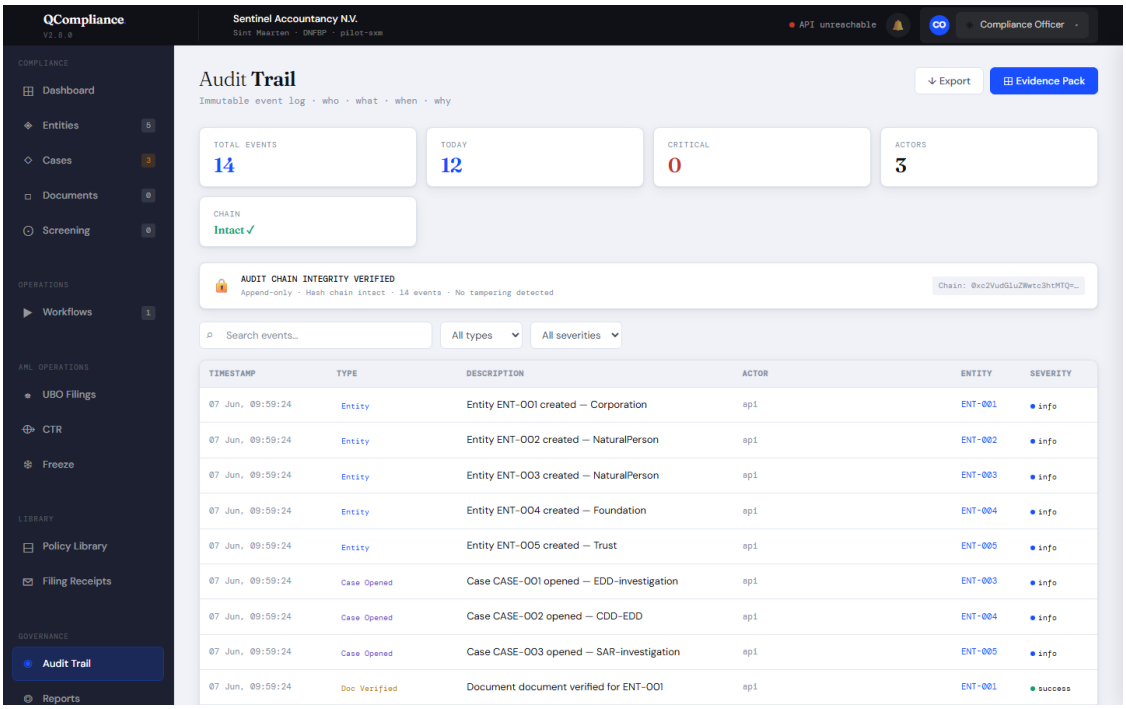
Enregistrer le brouillon de DOS met ENT-003 sous **verrouillage tipoff**. Ouvrez le panneau de détail de l'entité :



Le bandeau rouge — « *VERROUILLAGE TIPOFF ACTIF. Un brouillon de DOS a été préparé pour ce sujet. Aucune communication sortante ne doit avoir lieu. Coordonnez tout contact inévitable avec le MLRO.* » — est le rappel Wwft art. 23. Le statut de l'entité est maintenant `Gelé`. Tout opérateur ouvrant ce dossier désormais voit d'abord l'avertissement.

Étape 10 — Piste d'audit pour le dossier

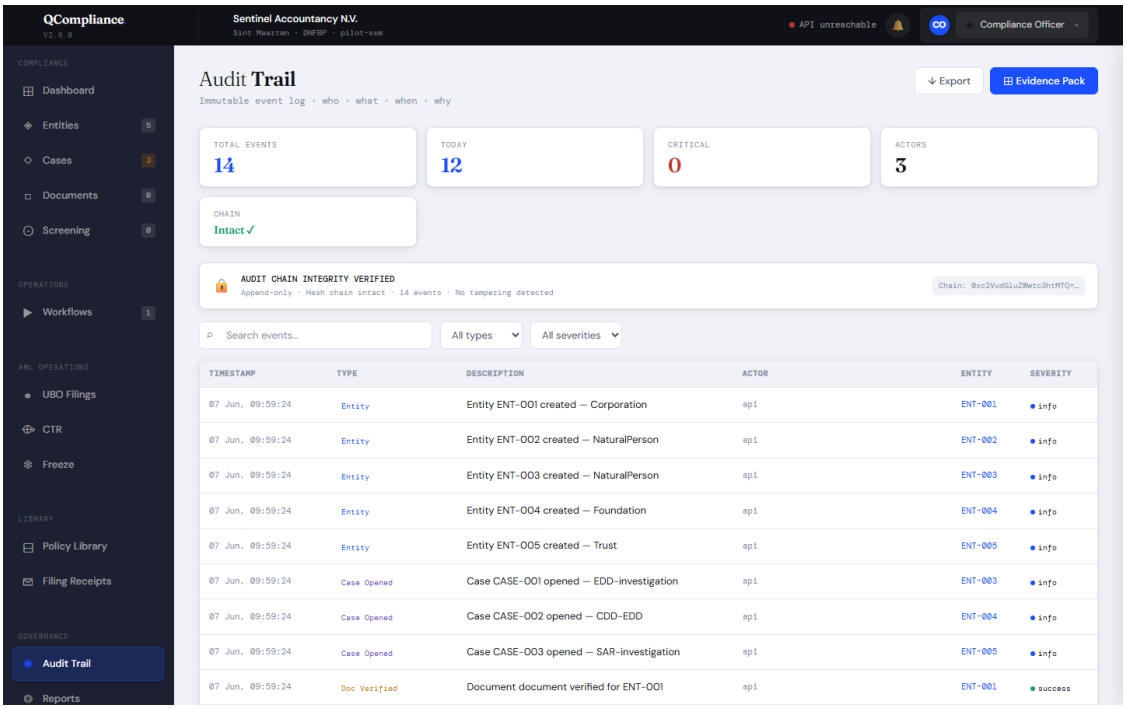
Filtrez la Piste d'audit sur CASE-2026-001 :



Les événements apparaissent en ordre d'ajout : dossier_ouvert → escalated_to_mlro → tipoff_lock_applied → mlro_review_approved → sar_draft_exported. L'acteur de chaque ligne est l'e-mail de l'humain qui a agi.

Étape 11 — Exporter le JSON d'audit pour le dossier

Cliquez **Exporter**. Un fichier JSON signé est téléchargé contenant la piste d'audit filtrée complète. Remettez-le à l'inspecteur ou stockez-le sous le dossier du cas.



La DOS XML que vous avez produite

Lors de l'enregistrement du brouillon de DOS, Q-KYC a aussi généré le XML de forme goAML 4.0. Voici un extrait du vrai fichier que Q-KYC produit (sauvegardé sous `docs/print/artifacts/sar_draft_CASE-2026-001.xml`) :

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- Q-KYC SAR DRAFT - forme goAML 4.0. PAS une soumission MOT validée. -->
<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[Deux correspondances de sanctions confirmee
s sur OFAC SDN
      (liees Ukraine) et Mesures Restrictives Consolidees UE (Decision du Con
seil
      2022/1530 - secteur defense). ...]]></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>UE 2022/1530 - Mesures restrictives, secteur defense</
screening_match>
      <screening_match>OFAC SDN - Sanctions liees a l'Ukraine</screening_matc
h>
    </origin>
  </activity>
</report>
```

Le MLRO transcrit ceci dans le portail goAML du MOT (ou, pour FIU-NL / TRACFIN / SEPBLAC, le portail SRC équivalent) et soumet.

> **§2 points-clés** - Le MLRO est la personne responsable devant le régulateur. L'imposition au niveau du bouton de « seul le MLRO peut approuver » correspond à la réalité juridique. - Le verrou tipoff est automatique dès l'enregistrement d'un brouillon de DOS ; vous n'avez pas à vous rappeler de l'activer. - Le XML de DOS que Q-KYC produit est un BROUILLON de forme goAML 4.0, pas une soumission MOT validée. Le MLRO convertit et soumet via le portail SRC.

---

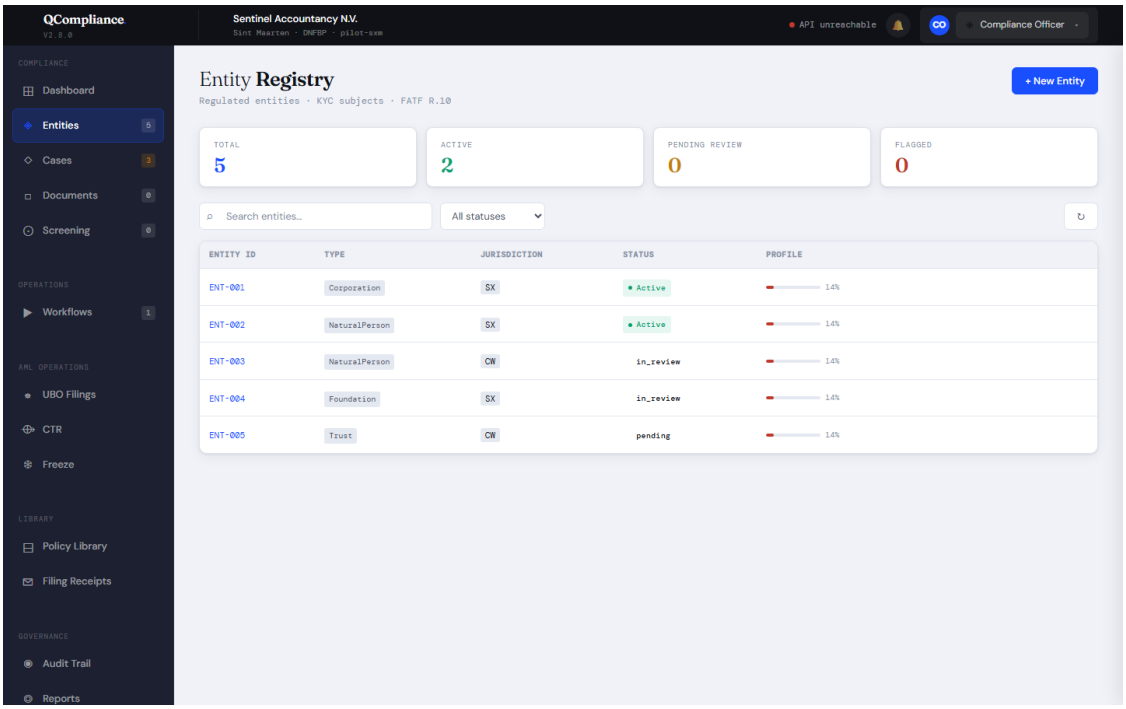
§3 Déclaration UBO + extrait de registre (Parcours 3)

> **Objectif :** capturer les bénéficiaires effectifs d'une structure juridique opaque (un trust BVI à parts au porteur), percer aussi loin que les registres disponibles le permettent, documenter explicitement la lacune UBO, et produire un PDF d'extrait UBO destiné au régulateur.

Sujet : ENT-004 Coral Holdings Ltd. — Trust BVI, propriété à deux niveaux, un porteur de parts au porteur.

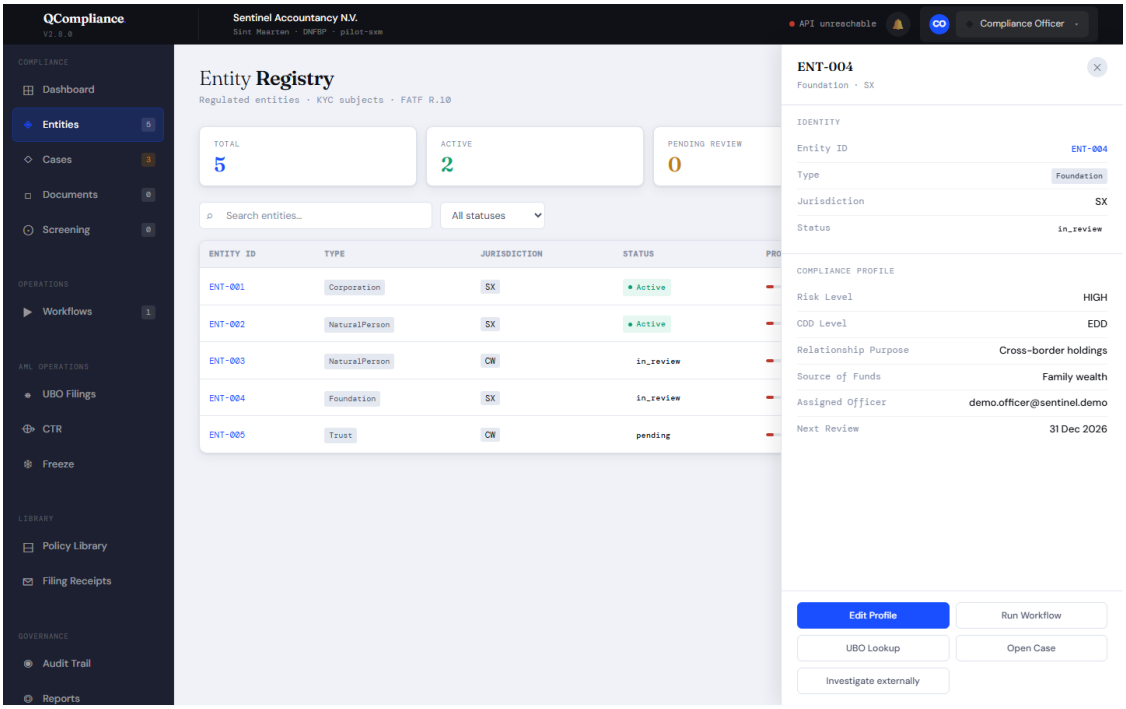
Étape 1 — Trouver l'entité

Ouvrez Entités, repérez ENT-004 :



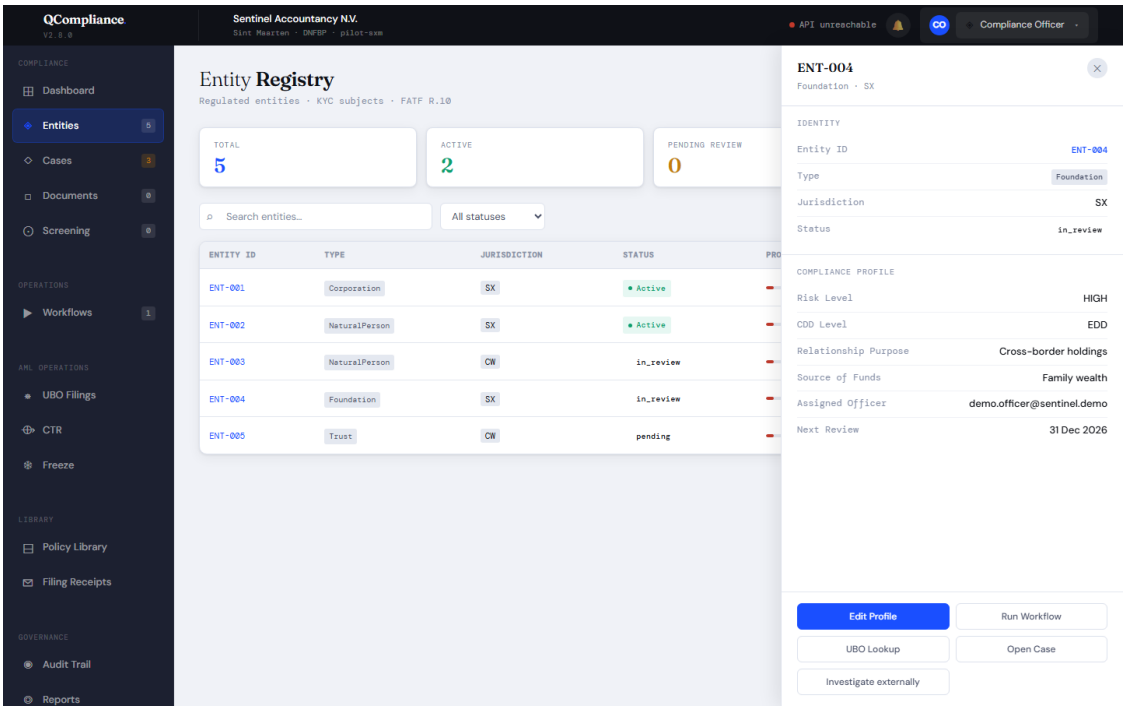
Étape 2 — Panneau de détail

Ouvrez ENT-004. Niveau de risque ÉLEVÉ, statut `pending_review`, juridiction VG (Îles Vierges britanniques).



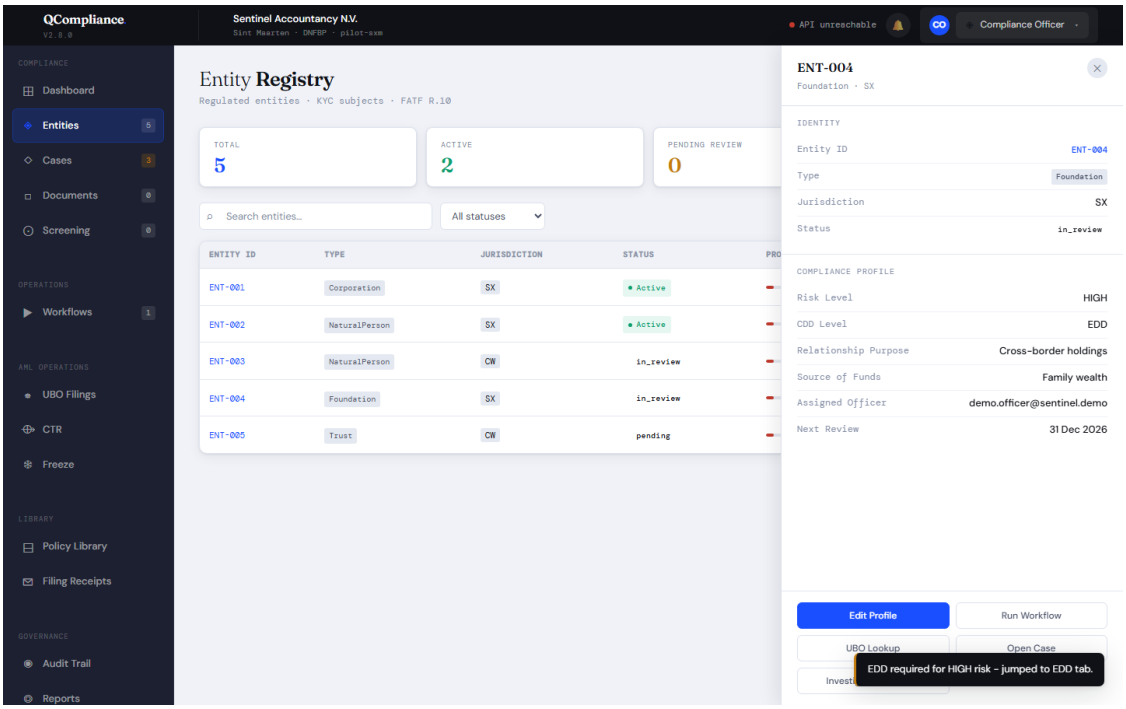
Étape 3 — Onglet Propriété

Modifier le profil → Propriété. Ici l'opérateur consigne chaque bénéficiaire effectif qu'il a pu identifier, avec le pourcentage et la base (actionnariat direct, part au porteur, prête-nom, contrôle par contrat).



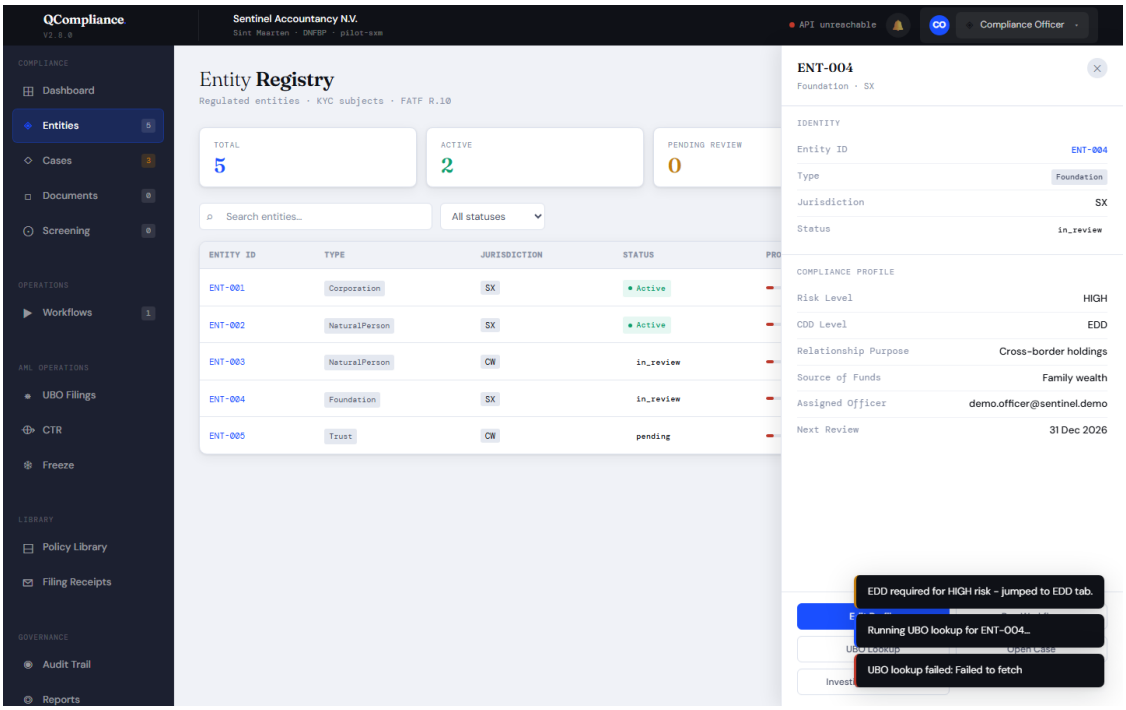
Étape 4 — Retour au panneau de détail

Fermez l'éditeur. Le panneau d'action propose **Recherche UBO** — une interrogation en un clic contre votre connecteur UBO câblé.



Étape 5 — Lancer la Recherche UBO

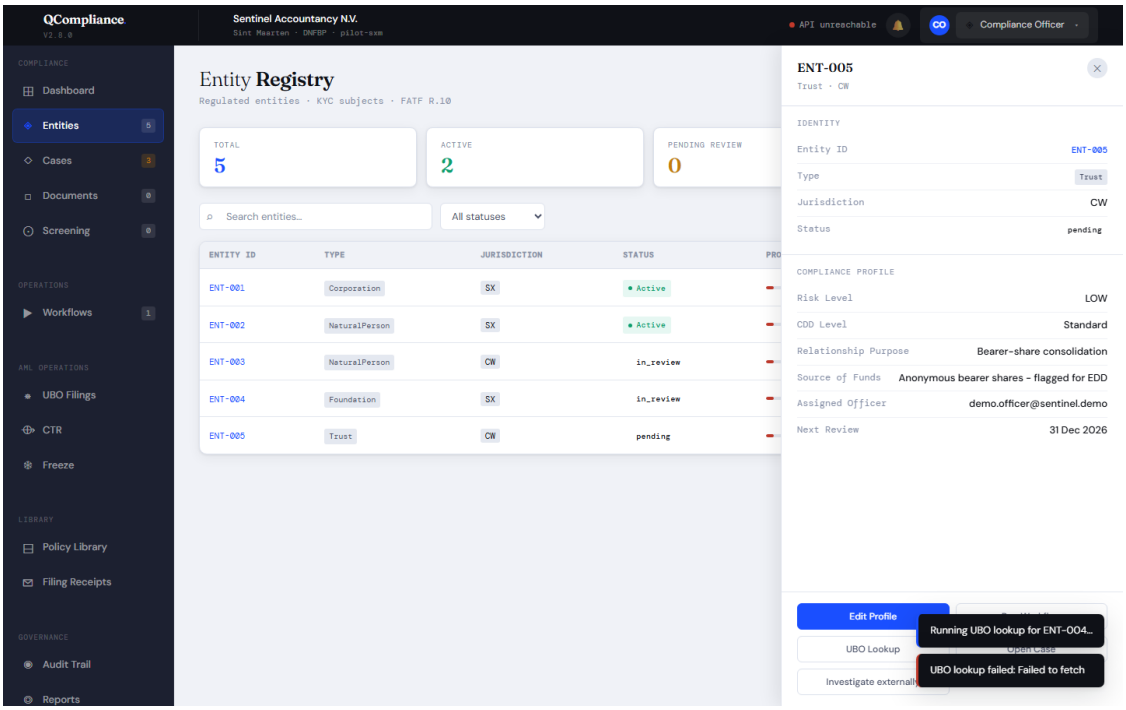
Cliquez **Recherche UBO**. Le panneau qui s'ouvre est la version honnête envers le régulateur : un avertissement jaune clair en haut indiquant quel fournisseur a été utilisé et si c'était réel ou un stub.



> *« Aucun registre UBO réel n'a été interrogé. La réponse ci-dessous provient d'un fournisseur stub déterministe (`deterministic_local_ubo_registry`). Configurez un connecteur réel (Chambre de commerce, KvK, Companies House, EU BO Register) sous Paramètres → Connecteurs avant de vous fier à ces résultats. »*

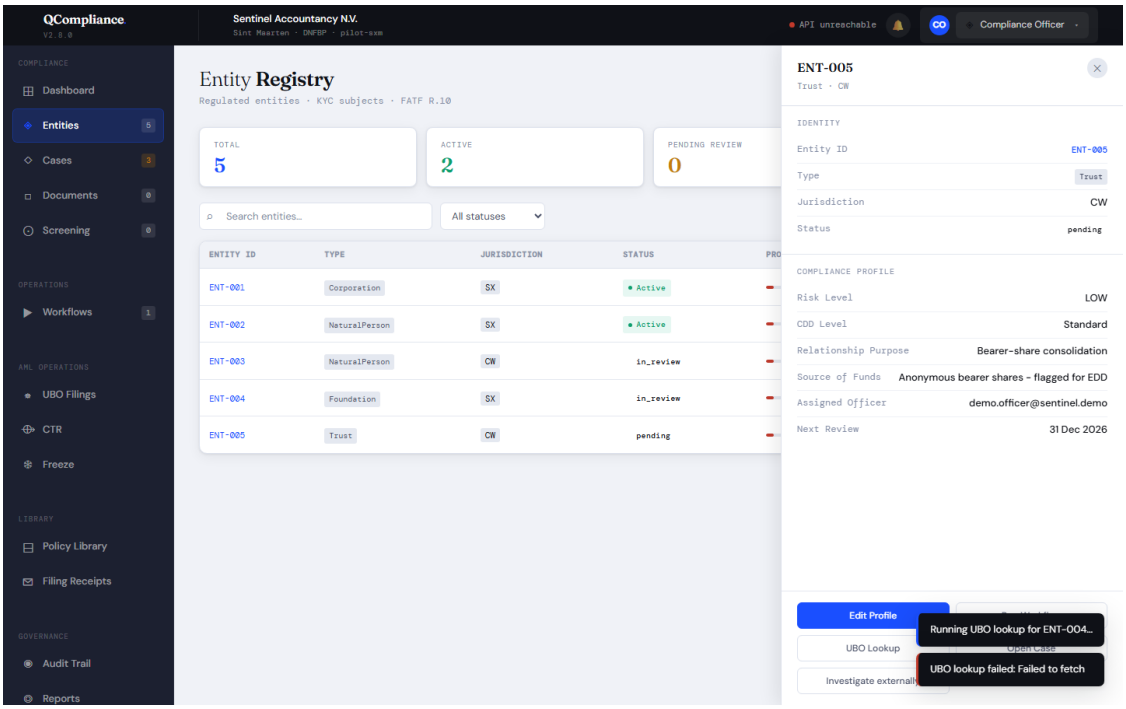
Étape 6 — La lacune des parts au porteur

Le panneau de réponse lui-même montre l'ID d'exécution, le registre, le fournisseur, et les bénéficiaires effectifs (ou, dans cette démo, « Aucun enregistrement UBO retourné »). Pour un trust BVI à parts au porteur c'est le résultat attendu — c'est la **lacune UBO** que chaque opérateur doit escalader en EDD.



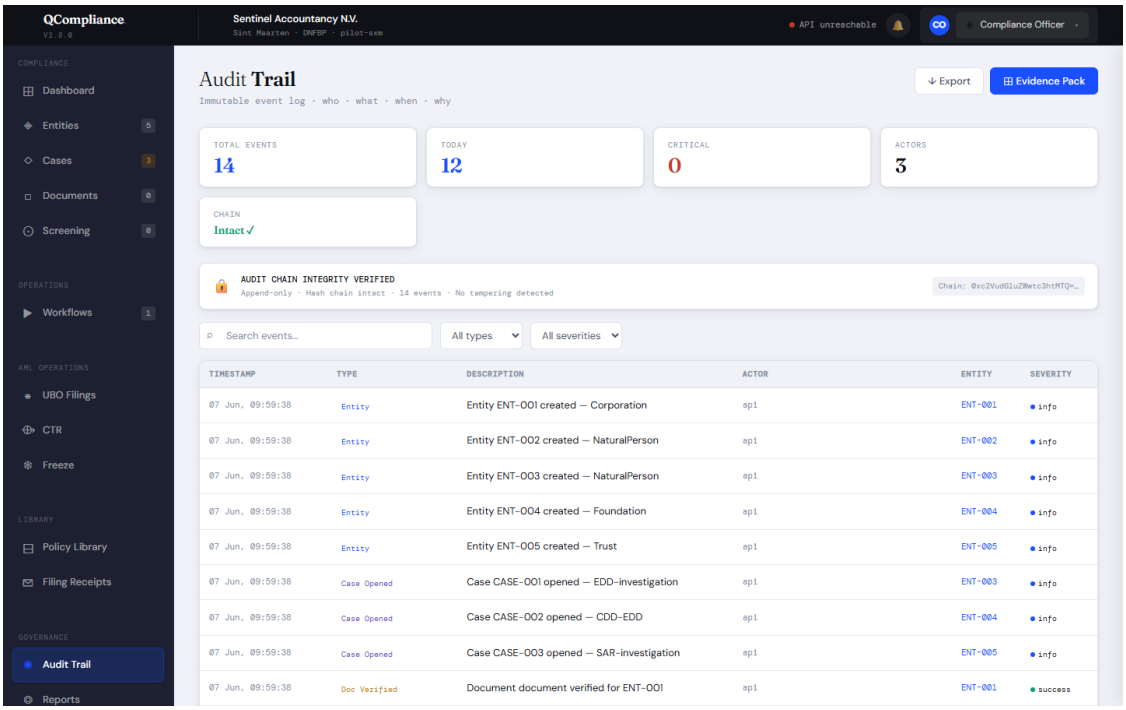
Étape 7 — Section provenance

Faites défiler jusqu'au bas du panneau. Chaque recherche UBO enregistre le point d'accès appelé, l'ID de requête chez le fournisseur, le temps de réponse, et tout avertissement du fournisseur. C'est ce que l'inspecteur veut voir quand il demande « avez-vous vérifié, et qu'avez-vous vérifié ? »



Étape 8 — Journal d'audit

Filtrez la Piste d'audit sur ubo :



L'événement ubo_lookup enregistre qui a effectué la recherche, quand, et contre quelle entité.

L’extrait UBO PDF

Lorsque vous avez besoin d’un document unique à remettre à l’inspecteur — ou à agrafer dans le dossier client — Q-KYC produit un PDF récupérable depuis `/entities/{eid}/ubo-extract.pdf`. Le vrai extrait ENT-004 (sauvegardé sous `docs/print/artifacts/ubo_extract_ENT-004.pdf`) tient sur une page et ressemble à ceci :

> **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**

Champ	Valeur
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** — *la réponse ci-dessous provient d’un stub déterministe. Configurez un vrai connecteur de registre des entreprises (KvK, Companies House, EU BO Register, Chambre de commerce) avant de vous fier à cet extrait pour une soumission au régulateur.*
>
> **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

> Le « NO » du porteur est la lacune UBO. Le pied de page rappelle au destinataire : *« 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 points-clés** - La transparence UBO signifie consigner ce que vous *ne pouvez pas* identifier, pas faire semblant que vous le pouvez. - La lacune « NON TROUVÉ » / parts au porteur est elle-même une constatation — escaladez en EDD, obtenez le formulaire de déclaration UBO consigné par l’opérateur, documentez pourquoi la lacune du registre existe. - Le PDF est destiné au régulateur mais ne se substitue pas à la copie certifiée du registre lui-même.

---

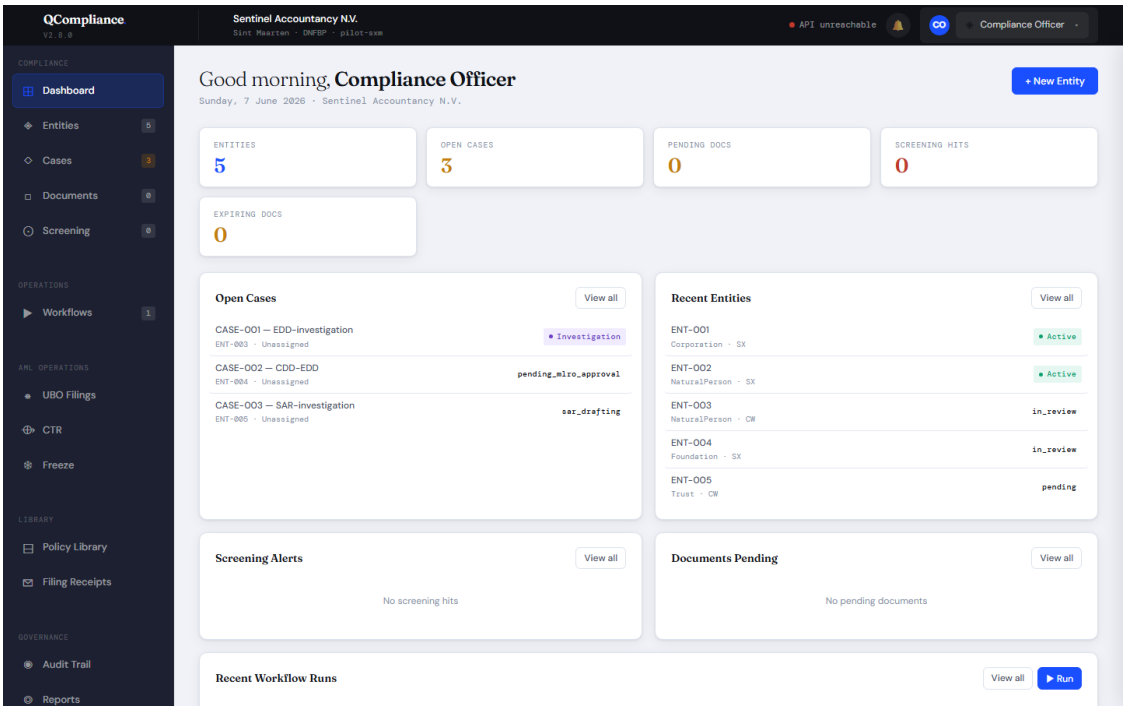
§4 Dossier de preuve (Parcours 4)

> **Objectif :** lorsqu'un inspecteur écrit à 16h00 disant *« veuillez nous envoyer demain matin tout ce que vous détenez sur l'entité X »*, vous produisez une seule archive ZIP avec manifeste, chaîne d'audit, documents (binaires verbatim), exécutions de criblage, recherches UBO, dossiers liés — toutes hashées, toutes horodatées, toutes signées par le système en marche au moment de l'export. Un clic.

Sujet : ENT-005 Domino Marine Services BV — entité juridique NL, révision périodique en retard.

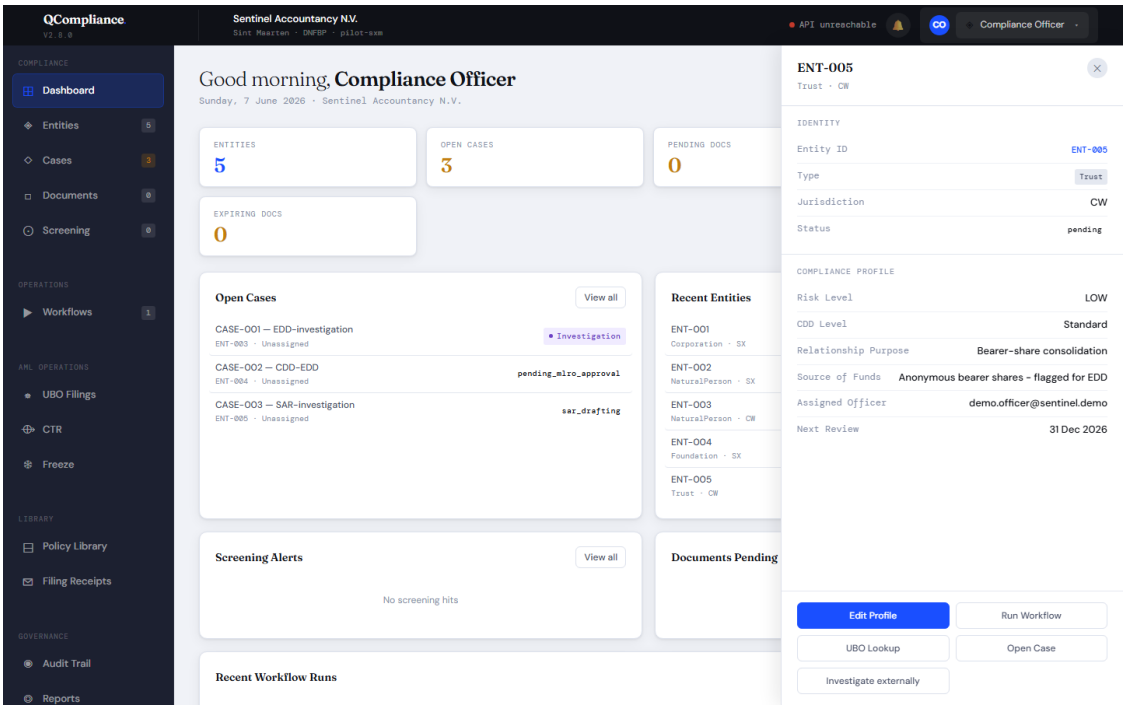
Étape 1 — File des révisions dues

La file des révisions dues vous dit que ENT-005 est en retard de 4 jours :



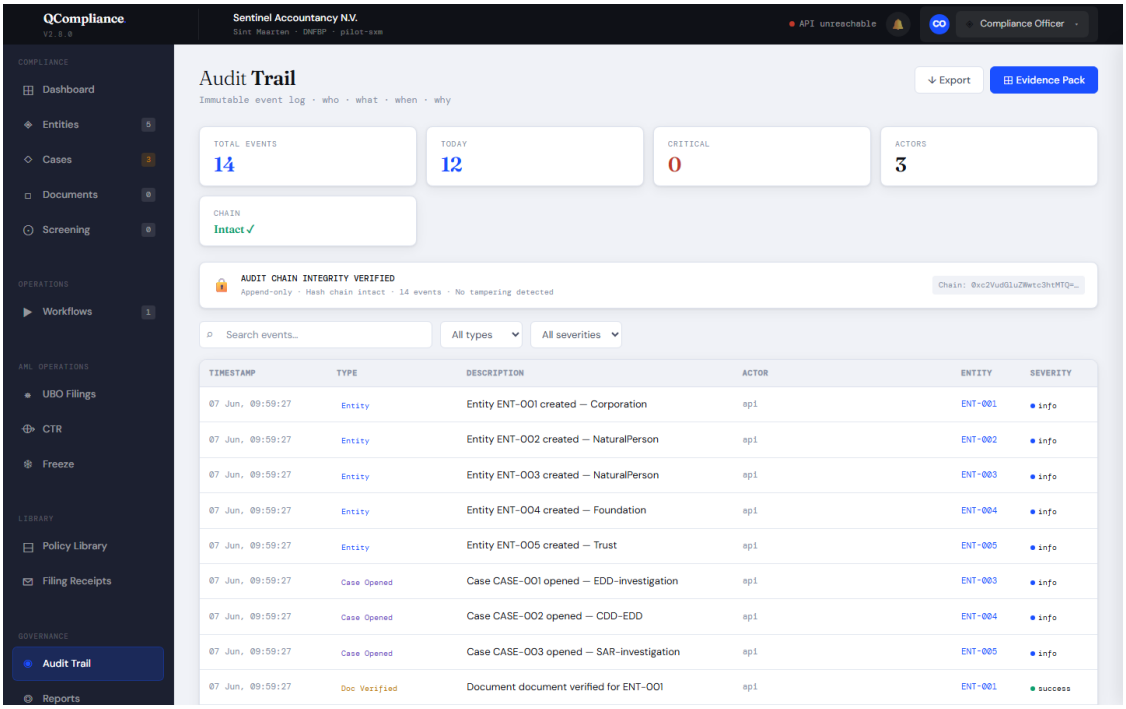
Étape 2 — Ouvrir ENT-005

Le panneau de détail résume le sujet de révision périodique :



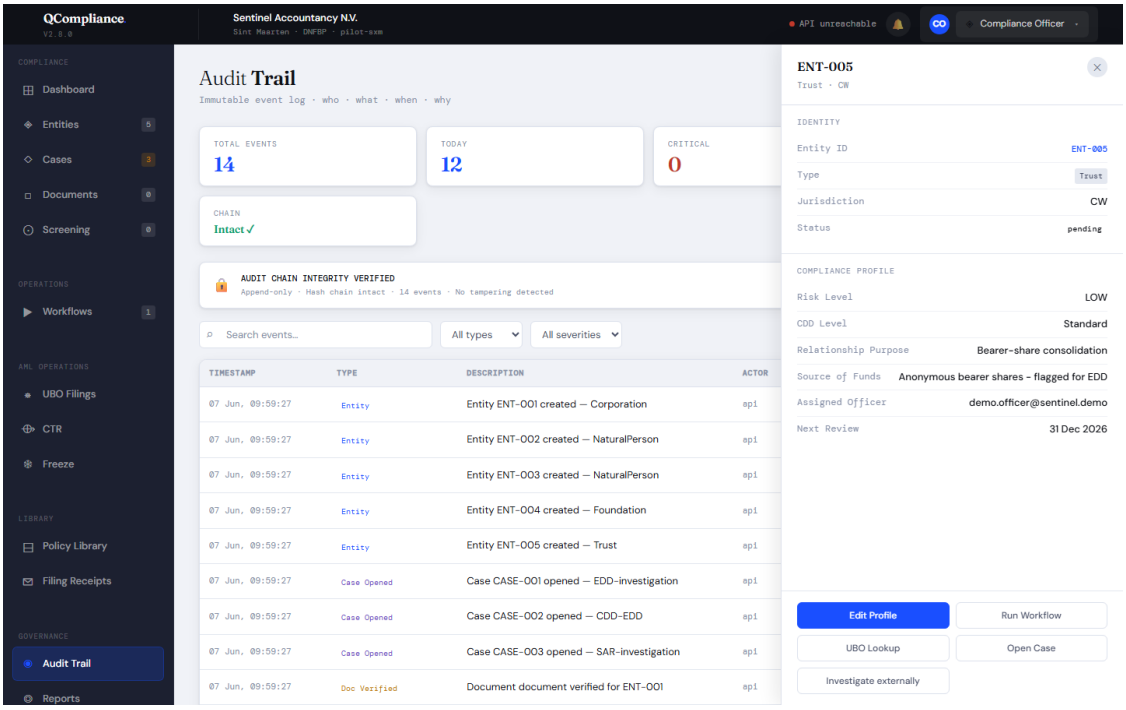
Étape 3 — Filtrer la piste d'audit sur ENT-005

Piste d'audit → boîte de recherche → « ENT-005 ». Vous voyez chaque action jamais entreprise contre cette entité, triée du plus récent au plus ancien :



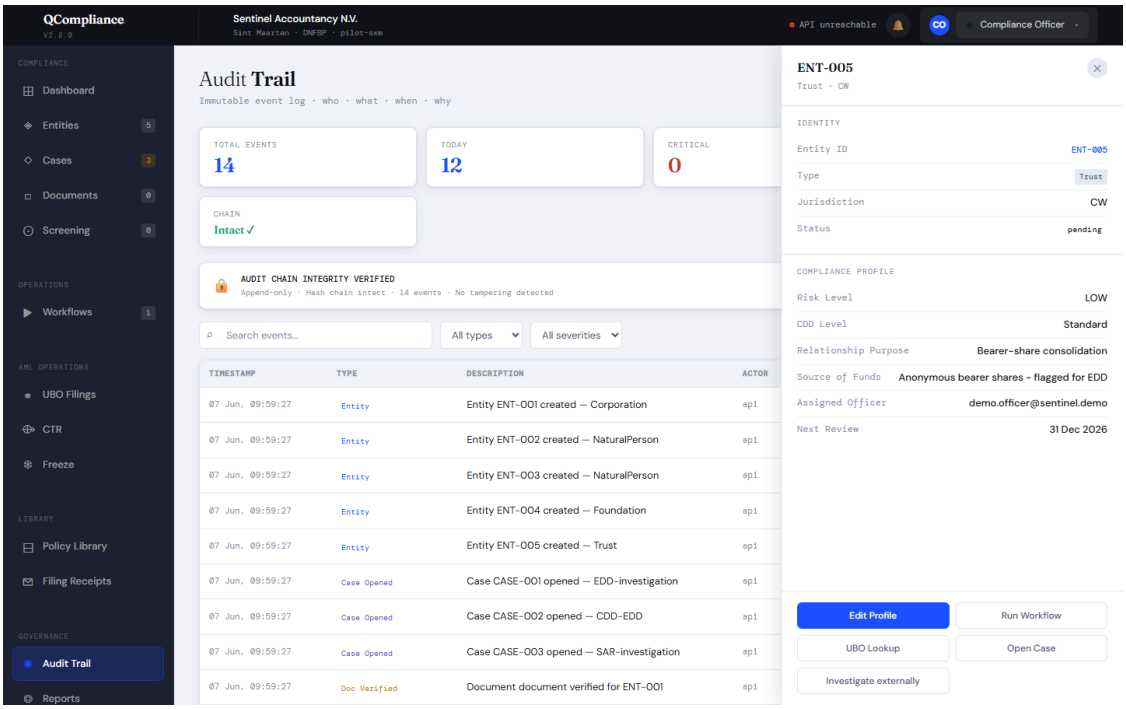
Étape 4 — Repérer le bouton Dossier de preuve

En haut à droite de la page Piste d’audit. **Dossier de preuve** (avec une petite icône de grille).



Étape 5 — Générer le dossier

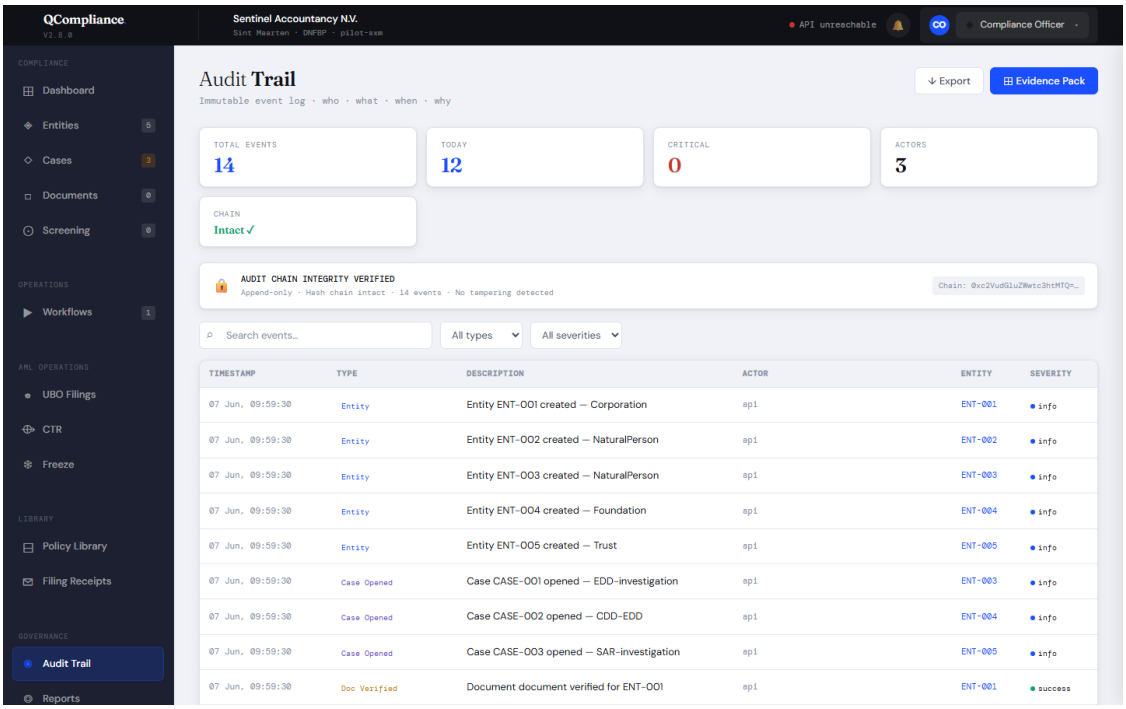
Cliquez **Dossier de preuve**. Une notification apparaît confirmant que le dossier a été généré :



Ce que le SPA fait côté client est télécharger un instantané JSON. Le **ZIP de qualité régulateur** est produit par le point d'accès backend `/entities/{eid}/evidence-bundle` — appelez-le depuis le bouton **Dossier de preuve** du panneau de détail de l'entité, ou récupérez-le via l'API.

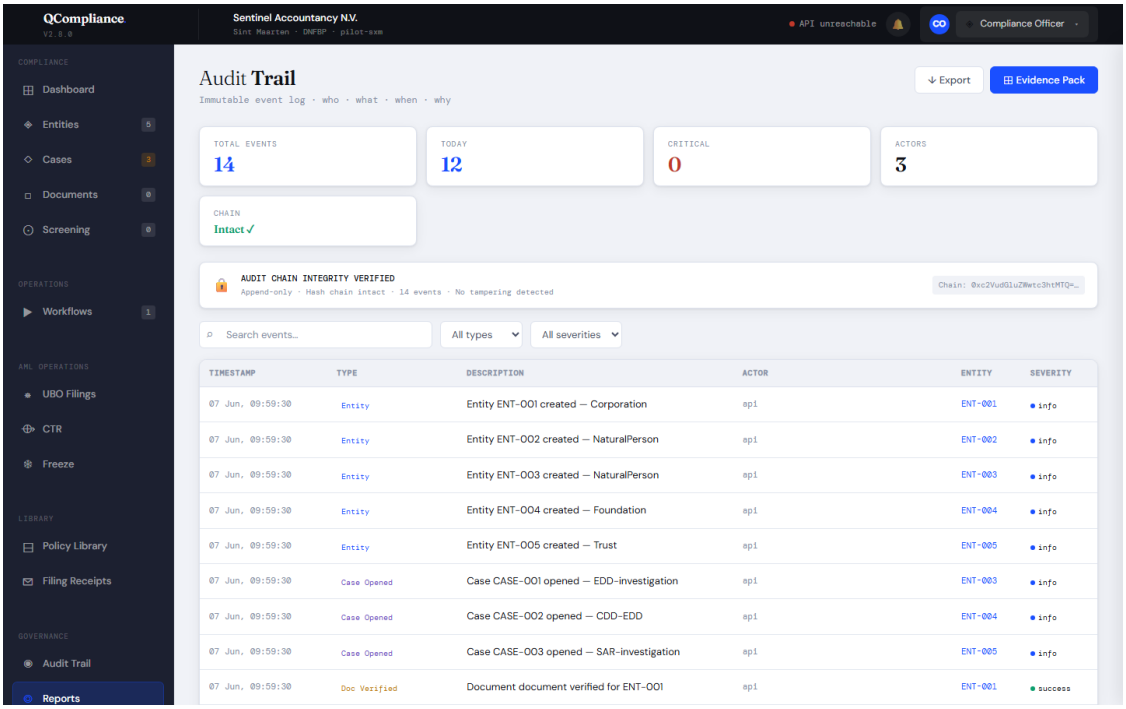
Étape 6 — Exporter le JSON d'audit seul

Si l'inspecteur ne veut que la chaîne d'audit (pas les documents), cliquez **Exporter** à la place. Vous obtenez un seul fichier JSON prêt à joindre à un e-mail :



Étape 7 — Rapports

La page Rapports est l'instantané de la posture de conformité du cabinet que vous pouvez imprimer ou remettre à un associé gérant lors d'une révision :



Le ZIP du Dossier de preuve — ce qu'il contient

Le ZIP pour ENT-003 (sauvegardé sous `docs/print/artifacts/evidence_bundle_ENT-003.zip`) contient six fichiers. Voici le vrai manifeste, 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": "...
" }
  ]
}
```


Chaque fichier de contenu a son **SHA-256** dans le manifeste. Toute manipulation du dossier après génération est détectable en re-hashant les contenus et en comparant. Le tableau `regulatoryBasis` est la prétention du cabinet à quelles règles le dossier satisfait ; le texte `intendedRecipient` est le contexte d'embarquement pour l'inspecteur receveur.

Lorsque ENT-003 possède des binaires de documents en dossier, le ZIP inclut aussi les PDF/images verbatim sous `documents/<doc-id>_<original_filename>` à côté de leurs fichiers `documents/<doc-id>.meta.json` compagnons.

> **§4 points-clés** - Le Dossier de preuve est un seul ZIP, nommé de manière déterministe, hashé, signé par le système en marche au moment de l'export. - La chaîne d'audit est la colonne vertébrale du dossier — tout le reste (documents, criblages, UBO) est la preuve que la chaîne d'audit pointe. - Vous n'avez pas à vous souvenir d'inclure quoi que ce soit. Le point d'accès inclut tout pour cette entité automatiquement.

§5 La chaîne d'audit en détail

Chaque action d'opérateur passe par `app/services/audit_service.py:log_event()`. La fonction écrit une ligne dans `audit_events` avec :

- `event_id` — UUID
- `actor` — e-mail de l'opérateur (ou `system` pour les événements automatisés)
- `event_type` — l'un d'environ 40 types connus (`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` — portée optionnelle
- `payload_json` — le détail structuré complet de l'événement (spécifique à l'événement)
- `created_at` — défini par la base au moment de l'insertion

La chaîne complète est **append-only** au niveau SQL — il n'y a pas d'UPDATE ni DELETE sur `audit_events` exposé via l'API. Le hash de chaîne que vous voyez sur la page Piste d'audit (par ex. `0xc2VudGluZWwtc3htMTc=…`) est le cachet d'anti-falsification pour l'inspecteur.

Extrait de l'audit ENT-003 vivant (sauvegardé sous `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 Rôles, droits, autorité MLRO

Rôle	Ce qu'ils peuvent faire	Ce qu'ils ne peuvent pas faire
super_admin	Tout, sur tous les tenants. Créer / désactiver des utilisateurs. Lire chaque dossier. Configurer les connecteurs.	Être le MLRO au sens de la responsabilité juridique — c'est un humain réel avec un nom.
tenant_admin	Tout dans leur tenant. Créer des utilisateurs, configurer les connecteurs, voir tous les dossiers.	Approuver un brouillon de DOS (le MLRO doit le faire).
mlro	Ouvrir / fermer des dossiers. Approuver ou rejeter les escalades. Autoriser les brouillons de DOS. Appliquer les verrous tipoff.	Modifier la piste d'audit.
compliance_officer	Ouvrir des dossiers, exécuter des criblages, réceptionner des documents, escalader au MLRO.	Approuver les révisions MLRO. Générer des brouillons de DOS (jusqu'à approbation MLRO).
operator	Voir les dossiers, exécuter des criblages, réceptionner des documents.	Ouvrir des dossiers, escalader, rédiger des DOS.
read_only	Tout voir dans le tenant.	Tout ce qui change l'état.

Les droits sont appliqués **côté backend**. Un agent de conformité qui trouve un moyen de cliquer sur le bouton MLRO Approuver (outils développeur du navigateur, rejouer une vieille requête HTTP, quoi que ce soit) obtiendra un 403 de `/cases/{id}/mlro-approve` parce que le point d'accès inspecte la revendication de rôle du JWT avant d'agir.

§7 Connecteurs — ce qui est mock aujourd'hui et ce qu'il faut câbler

Prêt à l'emploi, Q-KYC livre des connecteurs stub déterministes pour que le système soit testable de bout en bout sans comptes externes :

Connecteur	Mock aujourd'hui	Candidats production
Criblage sanctions	`deterministic_local_sanc`	Refinitiv World-Check One,

Connecteur	Mock aujourd'hui	Candidats production
	`tions` (OFAC SDN, UE consolidé, ONU, UK HMT — tous stubés)	Dow Jones Risk & Compliance, ComplyAdvantage, OFAC/UE direct via API signée
PEP	`deterministic_local_pep`	Dow Jones PEP, World-Check PEP, OpenSanctions PEP
Registre UBO	`deterministic_local_ubo_registry`	KvK (NL), Companies House (UK), EU BO Register, Chambre de commerce (SXM), BVI corporate registry
Vérification de documents	*Non configuré*	Onfido, Veriff, Sumsub, Jumio, IDnow
Adverse media	`deterministic_local_adverse_media`	Dow Jones Adverse Media, LexisNexis, Factiva

Configurez chacun sous **Paramètres → Connecteurs → [nom] → Configurer**. Le point d'accès de test du connecteur envoie une requête connue et valide la forme de réponse avant de sauvegarder les identifiants. Le panneau État des fournisseurs du tableau de bord reflète l'état en direct.

> **Le bandeau « Fournisseurs mock actifs » est une fonctionnalité, pas un bug.** Quand vous connectez un vrai fournisseur, le bandeau disparaît. Jusque-là, chaque utilisateur — et chaque artefact destiné au régulateur — sait que le cabinet est sur des stubs.

---

§8 Révisions périodiques et CDD continue

La CDD continue GAFI R.10 dit qu'on ne peut pas KYC une fois et puis oublier. Q-KYC stocke une `next_review_date` par entité :

- Risque FAIBLE → 24 mois
- Risque MOYEN → 12 mois
- Risque ÉLEVÉ → 3–6 mois (configurable)

La page Révisions dues liste chaque entité en retard ou dans les 30 jours. Cliquez dans l'entité, terminez la re-vérification (nouvelle exécution de criblage, recherche UBO rafraîchie, contrôle d'expiration de documents), enregistrez l'onglet Révision — le système écrit un événement `periodic_review_completed` et fixe une nouvelle `next_review_date`.

ENT-005 dans la démo est en retard de 4 jours, spécifiquement pour que cette page ne soit jamais vide.

---

§9 Dépannage / FAQ

Q : Je me suis connecté mais tous les écrans sont en anglais alors que j'ai choisi le français. Le sélecteur de langue en bas de la barre latérale échange le dictionnaire en direct ; si une chaîne manque dans votre langue, Q-KYC retombe sur l'anglais. Rafraîchissez la page une fois pour vider les chaînes en cache.

Q : J'ai cliqué Enregistrer & activer mais le statut n'a pas changé. Enregistrer & activer exige le Niveau de risque, le Niveau CDD, et au moins un document d'identification au dossier (minimum Wwft). Ouvrez l'onglet Révision et complétez les champs manquants — la notification vous dit lesquels.

Q : Le bouton MLRO Approuver n'apparaît pas pour moi. Vous n'êtes pas le MLRO. Déconnectez-vous et reconnectez-vous avec le compte MLRO, ou demandez à votre administrateur de tenant de vous accorder le rôle `mlro`.

Q : Le bandeau « Fournisseurs mock actifs » ne disparaît pas. Vous n'avez câblé aucun vrai connecteur. Paramètres → Connecteurs → Configurer. Le bandeau disparaît dès qu'au moins un connecteur rapporte le statut CONNECTED.

Q : Puis-je supprimer un événement d'audit ? Non. L'API n'expose aucun DELETE ou UPDATE sur `audit_events`. Si quelque chose ne va pas, vous créez un nouvel événement qui remplace l'erroné, et les deux restent dans la chaîne.

Q : Comment exporter tout sur l'entité X pour un inspecteur tout de suite ? Ouvrez le panneau de détail de ENT-X → **Dossier de preuve**. Vous obtenez un ZIP avec manifest.json + audit_excerpt.json + entity.json + screenings.json + ubo_lookups.json + cases.json + documents/*. Remettez le ZIP à l'inspecteur.

Q : Le XML de DOS — c'est ce que je dépose auprès du MOT ? Non. C'est un BROUILLON de forme goAML 4.0 que le MLRO doit transcrire. Le dépôt réel passe par le portail propre du SRC. Le travail de Q-KYC est de rendre la transcription mécanique, pas de contourner l'admission du SRC.

---

§10 Sécurité documentaire + capture mobile + intégration régulateur

Ces capacités ont été livrées en v0.6.8 et v0.6.9. Elles se trouvent SOUS les parcours que vous avez déjà appris en §1–§4 — vous n'avez pas à y toucher pour faire votre travail quotidien, mais si un régulateur vous audite elles sont la preuve que Q-KYC a pris dûment soin des fichiers que vous traitez.

§10.1 Analyse antivirus de chaque fichier téléversé

Chaque fichier qui entre dans Q-KYC via `POST /documents/intake` (le bouton **Ajouter un document** dans l'onglet Documents, l'envoi `/filing-receipts`, l'envoi vers la policy library, et la page caméra mobile) est diffusé à travers **ClamAV** avant d'être écrit sur disque.

- **Moteur :** ClamAV (fork Cisco) v1.5+, fonctionnant comme service Windows sur `127.0.0.1:3310`.
- **Signatures :** ~3,6 millions de définitions, rafraîchies quotidiennement par freshclam.
- **Mode d'échec :** si clamd est injoignable, le statut de l'analyse est enregistré comme `skipped` dans `document_intake.metadata_json.av_scan` et l'envoi passe quand même — graceful degradation.
- **Réponse à l'infection :** un envoi infecté retourne **HTTP 422**, le fichier n'est **jamais écrit sur disque**, et l'événement `document_infected_rejected` est chaîné dans le journal d'audit avec le nom de signature.

§10.2 Chiffrement au repos

Chaque fichier stocké dans `C:\ProgramData\Q-KYC\document_store\` est **chiffré Fernet** avec une clé par-installation dérivée de `COCAI_JWT_SECRET` via HKDF-SHA256. Le SHA-256 du clair est stocké séparément dans `document_intake.checksum_sha256`. Au retrait, l'API déchiffre, hash et compare — un mismatch retourne HTTP 409 et chaîne un événement `document_tamper_detected`.

§10.3 Analyse de la zone lisible en machine (MRZ)

Lors du téléversement d'un **passeport, carte d'identité nationale, permis de conduire, titre de séjour ou document d'identité**, Q-KYC exécute l'OCR (Tesseract) et alimente le texte dans un analyseur ICAO 9303 qui extrait et valide-par-chiffre-de-contrôle chaque champ (`documentNumber`, `nationality`, `surname`, `givenNames`, `dateOfBirth`, `dateOfExpiry`, `personalNumber`, contrôle composite). Les résultats vont dans `document_intake.metadata_json.mrz` ; les alertes apparaissent en ligne dans l'onglet Documents :

- `"document expired N day(s) ago"`
- `"document expires in N day(s)"` (pour expiration < 90 jours)
- `"MRZ composite check digit FAILED"` (erreur OCR ou falsification)

§10.4 Capture caméra mobile (QR-vers-téléphone)

Dans l'onglet Documents à l'intérieur de l'éditeur de profil, cliquez sur **Mobile upload** (icône ). Q-KYC frappe un jeton unique à 30 minutes, affiche un QR code ; le client le scanne avec son téléphone, le téléphone ouvre une page optimisée mobile avec **Prendre une photo** (`capture="environment"`) ou **Choisir depuis l'appareil**, puis POST sur

`/mobile-upload/intake` avec le jeton. Même analyse AV, même chiffrement Fernet, même analyse MRZ que sur ordinateur. Le fichier apparaît dans votre onglet Documents en quelques secondes.

§10.5 Modes d'intégration par régulateur

Trois modes par régulateur sous **Settings → Integration mode** :

Mode	Ce que cela signifie	Quand choisir
Manuel	L'opérateur télécharge l'artefact, l'envoie via le portail web du régulateur, puis ré-envoie le reçu dans `/filing-receipts`.	Par défaut pour KvK SXM, FIU MOT, CBCS aujourd'hui (aucun ne publie d'admission programmatique).
Push	Q-KYC POST l'artefact à l'endpoint du régulateur dès que le MLRO clique sur envoyer.	Configurez `COCAI_KVK_ENDPOINT_URL` / `COCAI_FIU_GOAML_*` / `COCAI_CBCS_ENDPOINT_URL` dès qu'un régulateur en publie un.
Pull	Q-KYC expose `/regulator-api/v1/*` que le régulateur consulte à son propre rythme. Chaque lecture est journalisée dans le **registre Art. 30 RGPD**.	Disponible aujourd'hui ; frappez des jetons bearer par régulateur sous **Settings → Regulator pull tokens**.

Endpoints pull exposés aujourd'hui :

```
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
```

Chaque appel insère une ligne dans `regulator_api_access_log` (le registre Art. 30 RGPD) ET un événement dans `audit_events`.

§10.6 Indicateur multi-national

Lorsque vous sélectionnez une seconde nationalité dans la liste **Additional Nationality** de l'onglet Identité, Q-KYC élève le niveau de risque à **medium** (s'il était Low/vide), ajoute une auto-note à Risk Notes, et déclenche un warn-toast — implémentant la vigilance multi-juridictionnelle GAFI R.10. La surchage manuelle reste possible ; l'auto-note demeure visible.

§11 Glossaire

Terme	Signification
CBCS	Centrale Bank van Curaçao en Sint Maarten — publie des orientations LCB-FT pour les EPNFD à SXM.
CDD	Customer Due Diligence — le processus GAFI R.10 d'identification, vérification et évaluation du risque client.
DNFBP / EPNFD	Designated Non-Financial Business or Profession / Entreprise et Profession Non Financière Désignée — experts-comptables, conseillers fiscaux, avocats, agents immobiliers, etc. soumis aux obligations LCB-FT.
EDD	Enhanced Due Diligence / Vigilance renforcée — examen supplémentaire pour les sujets à haut risque (PPE, structures opaques, juridictions à haut risque).
FATF / GAFI	Financial Action Task Force / Groupe d'action financière — l'instance internationale de normalisation LCB-FT.
FIU / SRC	Financial Intelligence Unit / Service de renseignement financier — l'autorité nationale qui reçoit les DOS (MOT pour Sint Maarten/Curaçao, FIU-NL pour les Pays-Bas, TRACFIN pour la France, SEPBLAC pour l'Espagne).
goAML	Le schéma XML de l'ONUDC pour la déclaration DOS/STR. La plupart des SRC acceptent goAML ; certains ont leurs propres variantes.
KYC	Know Your Client / Connaissance Client — l'étape d'identification et de vérification d'embarquement initial.
MLRO	Money Laundering Reporting Officer / Responsable de la déclaration de soupçon — l'humain au sein du cabinet juridiquement responsable des décisions de DOS.

Terme	Signification
MOT	Meldpunt Ongebruikelijke Transacties — le SRC des Caraïbes néerlandaises (Sint Maarten + Curaçao).
PEP / PPE	Politically Exposed Person / Personne Politiquement Exposée — risque LCB-FT élevé selon GAFI R.12.
SAR / STR / DOS	Suspicious Activity / Transaction Report / Déclaration d'opération suspecte — la déclaration formelle au SRC.
Tipoff	Communication au sujet (directe ou indirecte) qu'il est sous enquête DOS — un délit pénal sous Wwft art. 23.
UBO / BE	Ultimate Beneficial Owner / Bénéficiaire Effectif — la personne physique qui possède ou contrôle ultimement une entité juridique (seuil ≥25 % sous la plupart des régimes).
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme — la loi LCB-FT néerlandaise qui s'applique aux Pays-Bas et (avec adaptation locale) à SXM.

Fin du manuel. Édition 2026-05. · © 4Mfesw — tous droits réservés.