Sentinel ID

PLATFORM PROPOSAL

Sentinel ID

Identity, investigation and emergency response

Connect person records and investigative leads to cases, evidence and field operations.

SentinelSecureID.com

Product overview and illustrative case studies
26 October 2026

INSIDE THIS PROPOSAL

A guide to the platform and pilot

Explore the capabilities, camera deployment choices and practical scenarios, then use the acceptance worksheet to plan a pilot.

03 A connected operational record

04 People and identity history

05 Biometric investigation

06 Complaints, cases and evidence

07 Officer safety and emergency response

08 Dispatch and communications

09 Android phones and tablets

10 Vehicles, cameras and guarded sites

11 Events and investigation

12 Account security and accountability

13 Deployment and integrations

14 A common picture for each team

15 When contact details change

16 Choose the view before the device

17 Connect the source to the workflow

18 A perimeter event becomes a reviewed lead

19 Follow a plate read back to its source

20 Design coverage around the site

21 Turn the capture plan into a storage estimate

22 From a patrol check to a dispatch

23 Connect the installation without hiding dependencies

24 Make success observable

25 Plan for up to 10 billion people

26 Understand what the projection includes

27 Approved access to a private workspace

28 An outbound connection from the private server

29 Sessions, temporary access and team approvals

30 Preserving responsibility and recovery options

31 A site, its cameras and its operating rules

32 Additional examples, independent validation

33 Officer safety and field continuity

34 Identity history and camera observations

35 Partner access and device review

36 Recovery and remote cameras

37 Video review and shared cases

38 Identity checks and inconsistencies

39 A pilot with explicit success criteria

40 Your workflow, demonstrated

EXECUTIVE OVERVIEW

A connected operational record

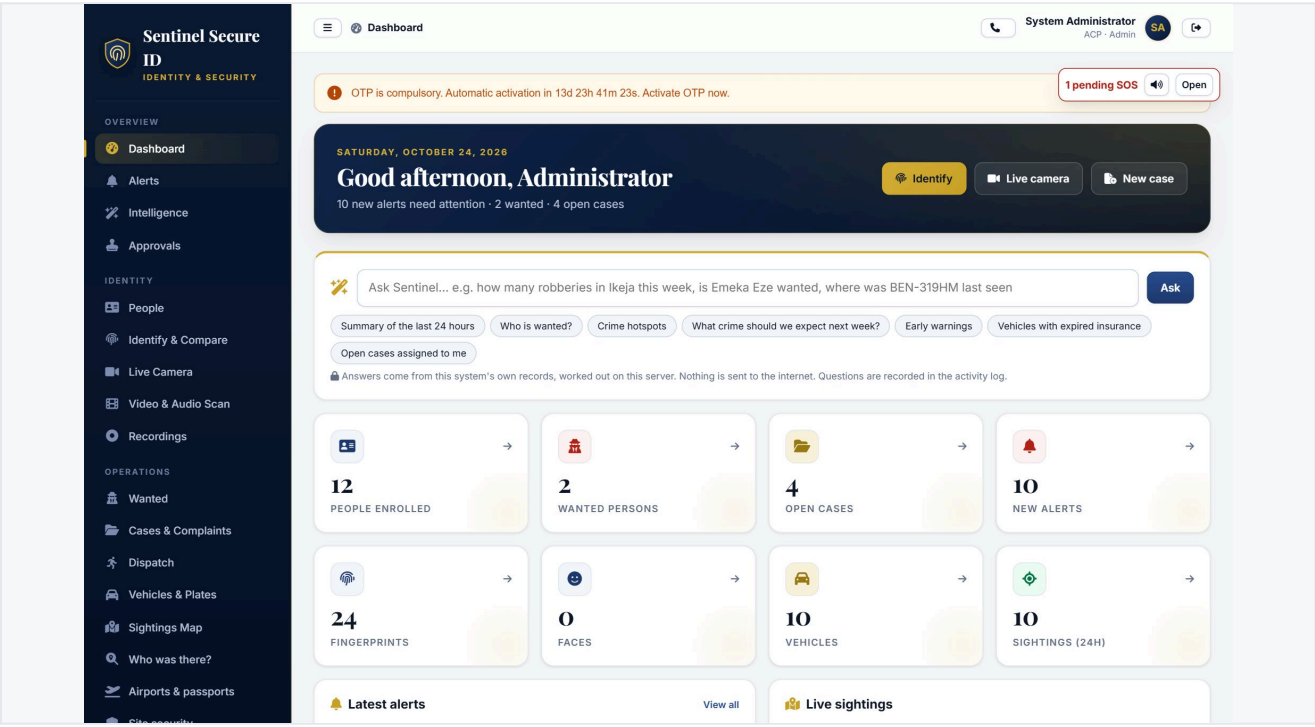
A control-room workspace, an approved Android field app and scoped partner APIs support the agency’s operating workflow.

People and investigation

- Identity and contact history retain context as details change.
- Biometric candidates link to registered records for human review.
- Cases connect assignments, attachments and recorded observations.

Field response and accountability

- SOS reports stay pending until acknowledged.
- Dispatch links the incident to selected responders and their acceptance.
- Permissions, approvals, audit and evidence controls record responsibility.



Current demonstration workspace. All displayed records are fictional test data.

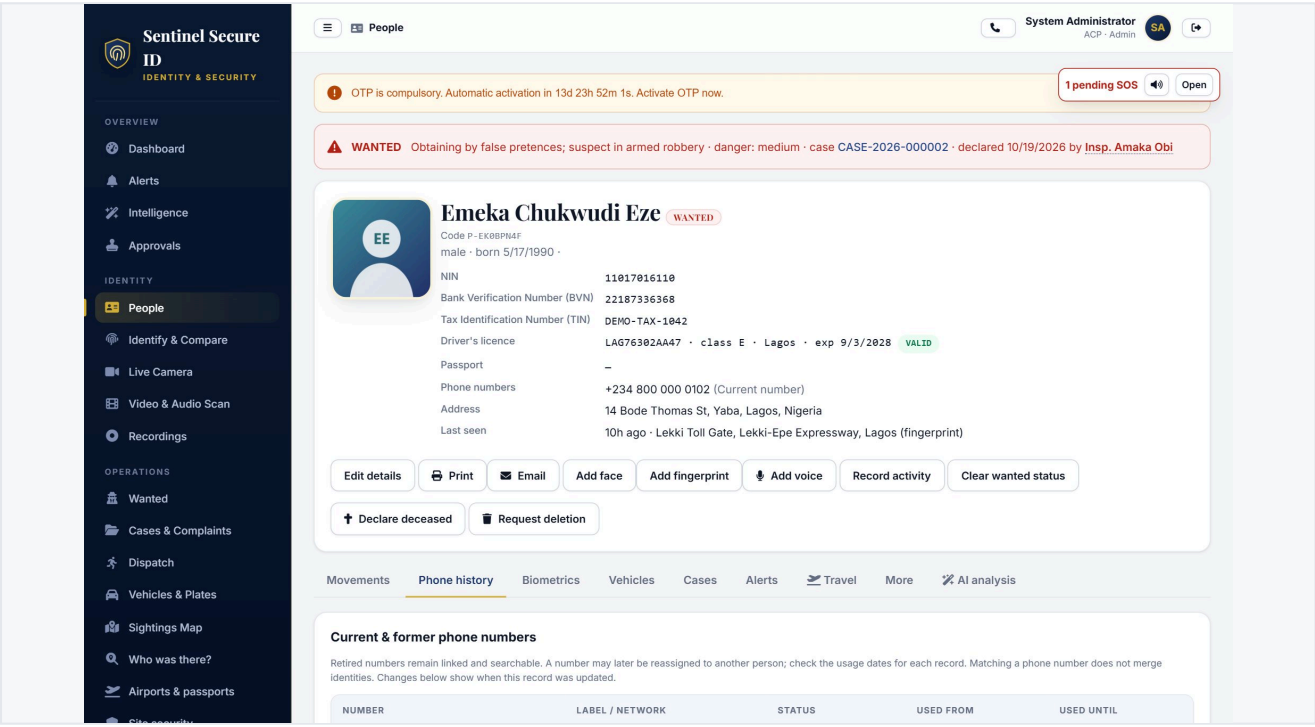
This proposal describes implemented software workflows. External services, hardware integration, recognition performance and production capacity require deployment-specific validation.

PLATFORM CAPABILITIES

People and identity history

Keep identifiers and changing contact details in one person profile.

- National ID, Bank ID and TAX ID labels adapt to the organisation and country.
- Record multiple bank accounts and phone numbers, including active and retired numbers.
- Retain dated phone changes and number reassignment history instead of treating a phone number as permanent identity.
- Connect wanted status, watchlists, vehicles, cases and recorded sightings. Sensitive identifiers follow access permissions.



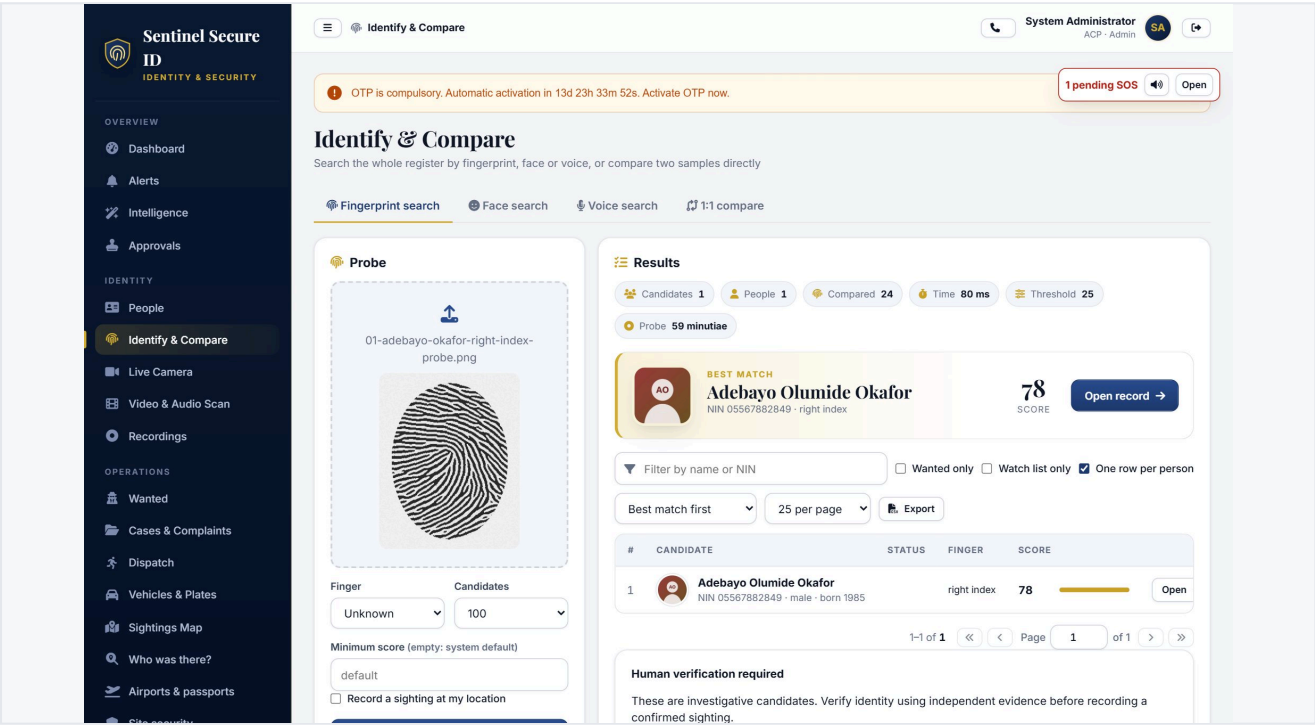
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Biometric investigation

Search registered records and review candidate matches in context.

- Fingerprint identification and verification, plus comparison of two submitted prints.
- Face search from photographs, supported cameras and uploaded video. Voice enrolment, comparison and audio investigation.
- Candidate review, configurable thresholds and manual decisions support responsible interpretation.
- Capture quality, liveness and independent performance evaluation depend on configured services and representative validation. A candidate match is an investigative lead.



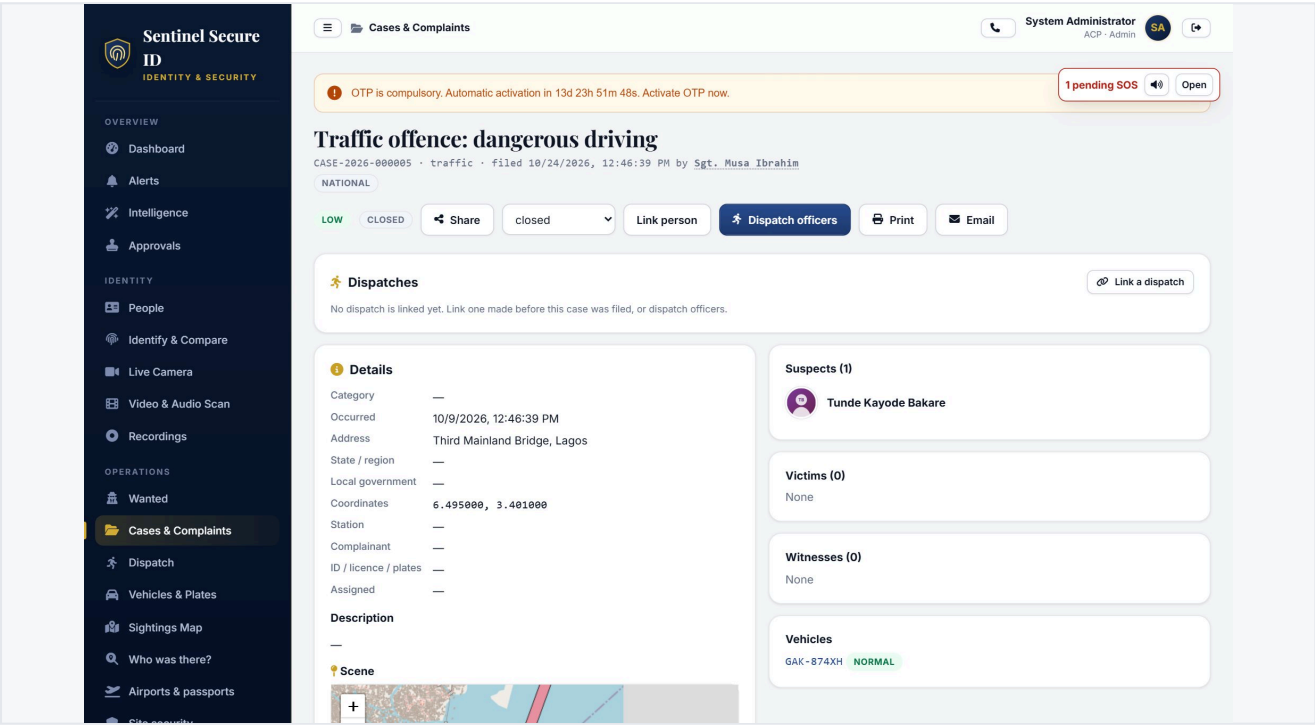
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Complaints, cases and evidence

Carry a complaint through assignment, investigation and review.

- Register complaints and connect people, vehicles, locations and evidence. Names or ID details can create and link people during registration under the existing flow.
- Review proposed links, missing biometrics and possible duplicate people through the special approvals workflow.
- Assign or reassign investigators, follow tasks and activity, and report overdue or inactive cases. Reminders prompt officers to record updates.
- Unit / Station and agency permissions govern case approvals. Evidence originals, custody history, legal holds and configured signed dockets support review.



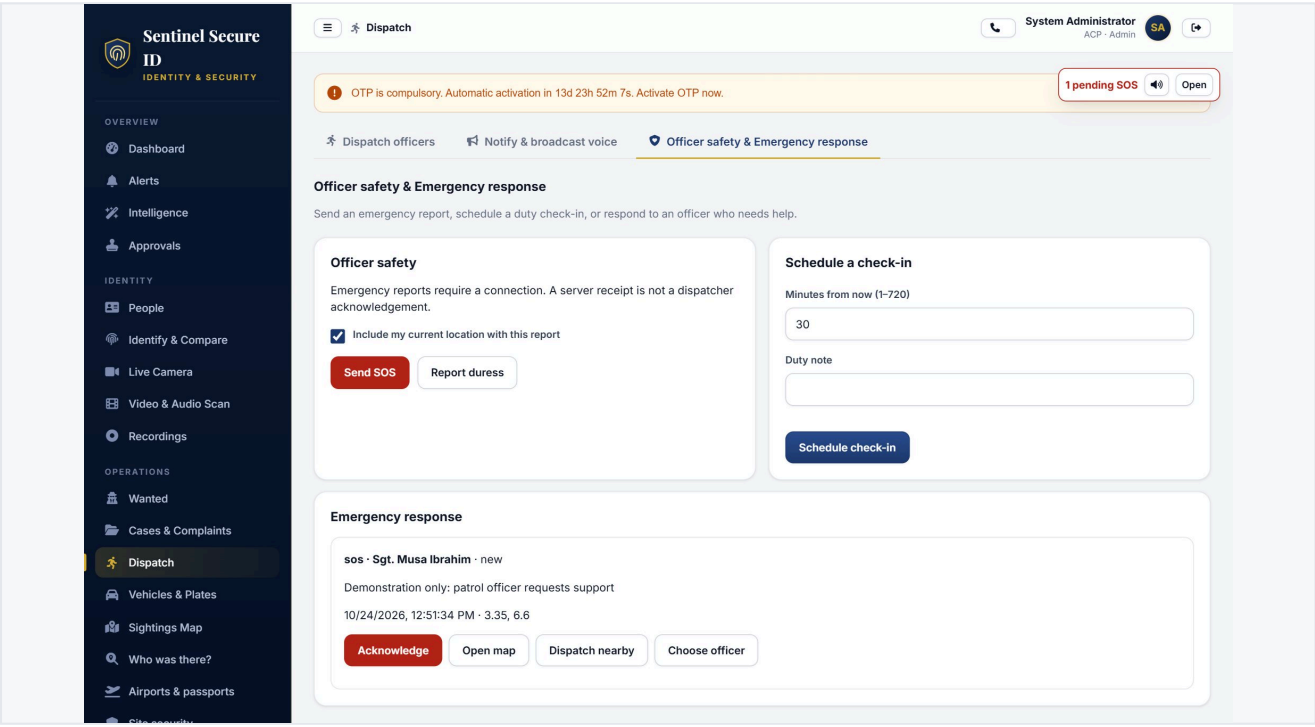
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Officer safety and emergency response

Keep a pending emergency visible until control acknowledges it.

- The field app sends SOS with an optional location. GPS failure still allows a report without coordinates.
- A small floating badge starts minimized. A new pending emergency plays an alarm, with an enable-sound control if the browser blocks playback.
- Open available coordinates on a map, find nearby officers or choose a specific officer. Dispatches await the officer's acceptance.
- Control can call back after a dropped or missed one-to-one call, including a call originally made to headquarters.



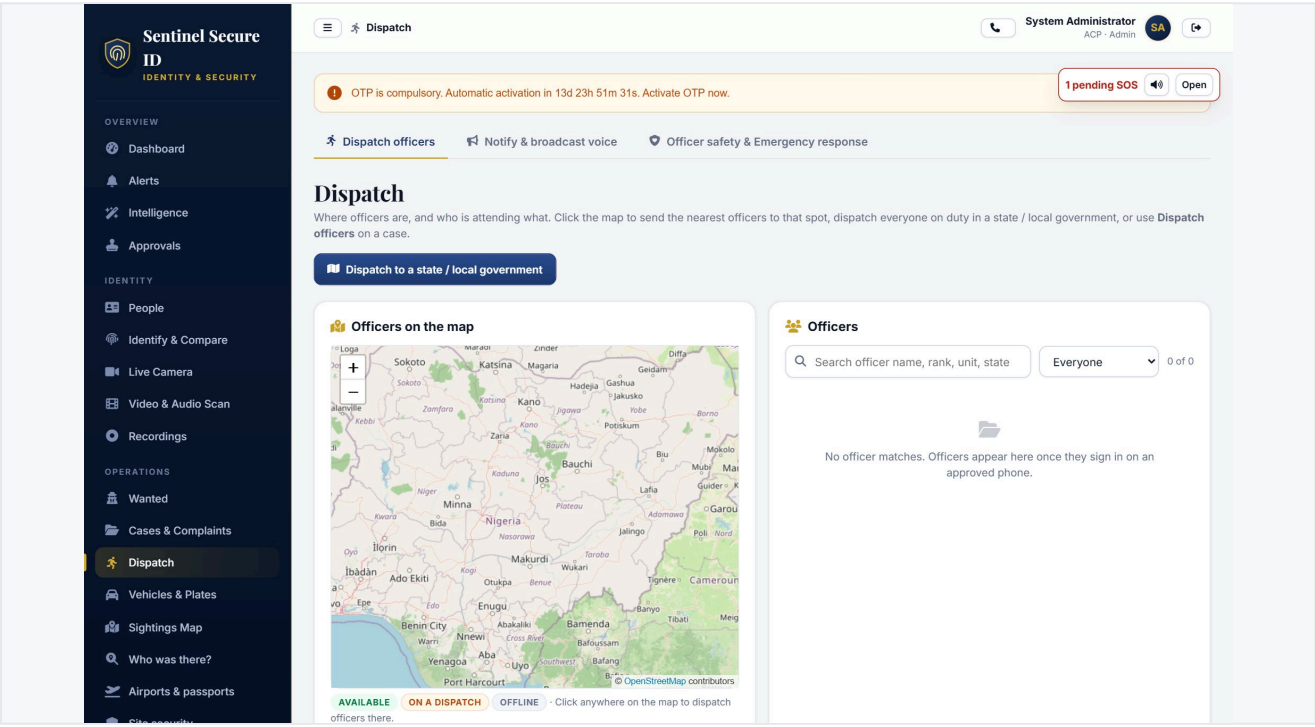
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Dispatch and communications

Coordinate field activity and retain a record of the response.

- Send officers to a case, emergency, map point or duty area. Track acceptance, arrival and completion.
- Officer location and duty information follow the relevant permissions. Position age matters when selecting responders.
- Direct voice calls, headquarters calls, broadcasts and targeted notices connect control and approved devices.
- Calls across mobile networks may require a configured relay service. Notifications depend on network access and device permissions.



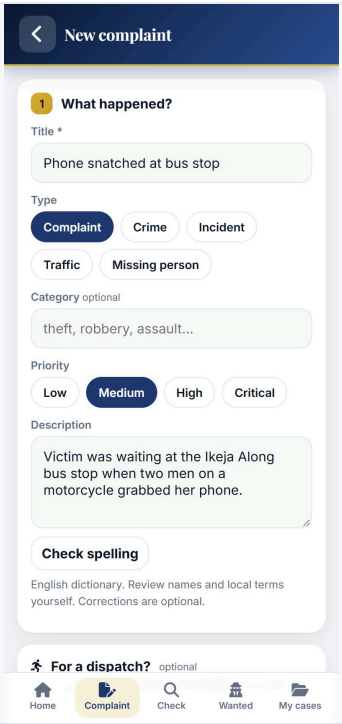
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Android phones and tablets

Support field work on an approved Android device.

- Approved Android phones and tablets support the Field workflow, responsive screens and portrait or landscape capture.
- Device-owner biometrics or PIN can unlock protected local access. The built-in phone sensor does not export public identity-search fingerprints.
- Offline access follows cached authorisation and expiry rules. Encrypted drafts and a retry queue preserve supported work until connectivity returns.
- In-app conversations support replies, with SOS, dispatch, voice and requested live video subject to permissions and connectivity. Location reporting suppresses unchanged coordinates and GPS jitter.



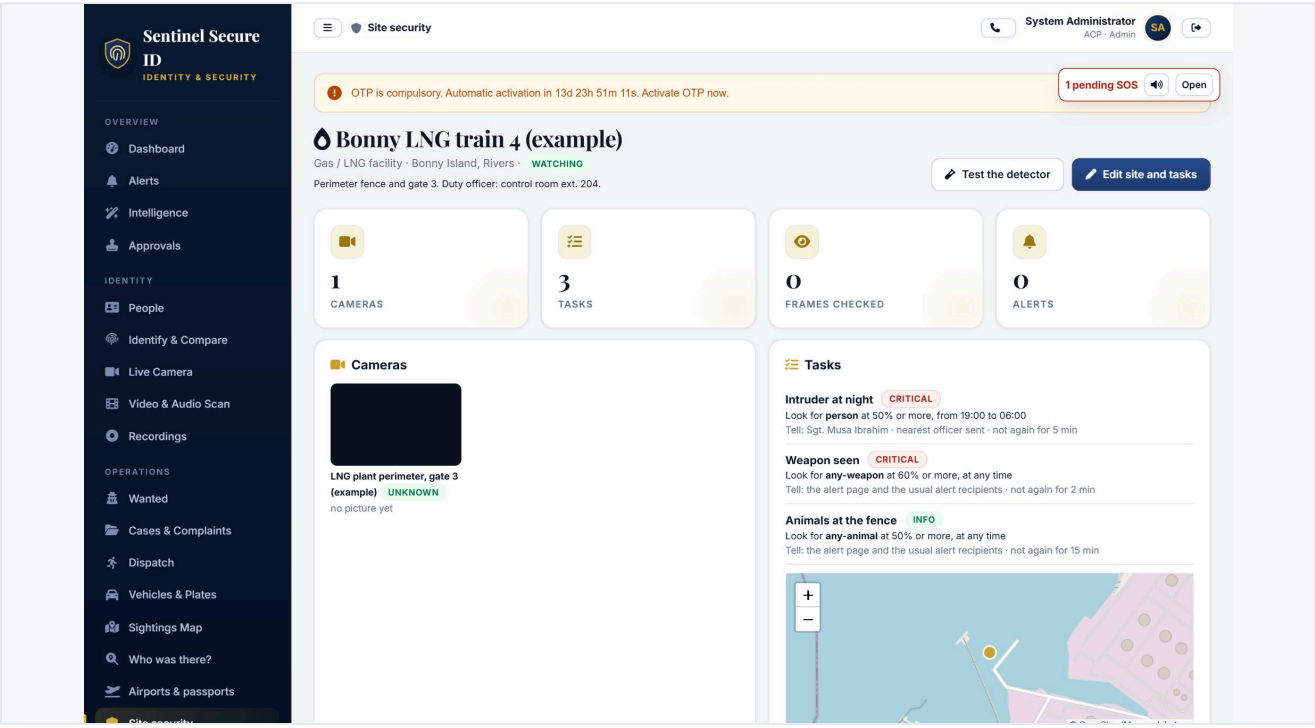
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Vehicles, cameras and guarded sites

Connect observations to the people and vehicles in the register.

- Connect image-push cameras, ANPR devices and supported NVR or RTSP sources. RTMP and SRT publishing use the configured media relay and registered camera credentials.
- A site opens with its previews stopped. Start or stop each camera individually while configured background detection runs independently.
- Face and plate observations can raise watchlist alerts when detection, matching and suitable capture are configured. Site rules can notify officers or request dispatch.
- Custom detector training can add new examples and continue from existing training. Validate held-out and full-frame results before activation. A configured label alone does not prove detection accuracy.



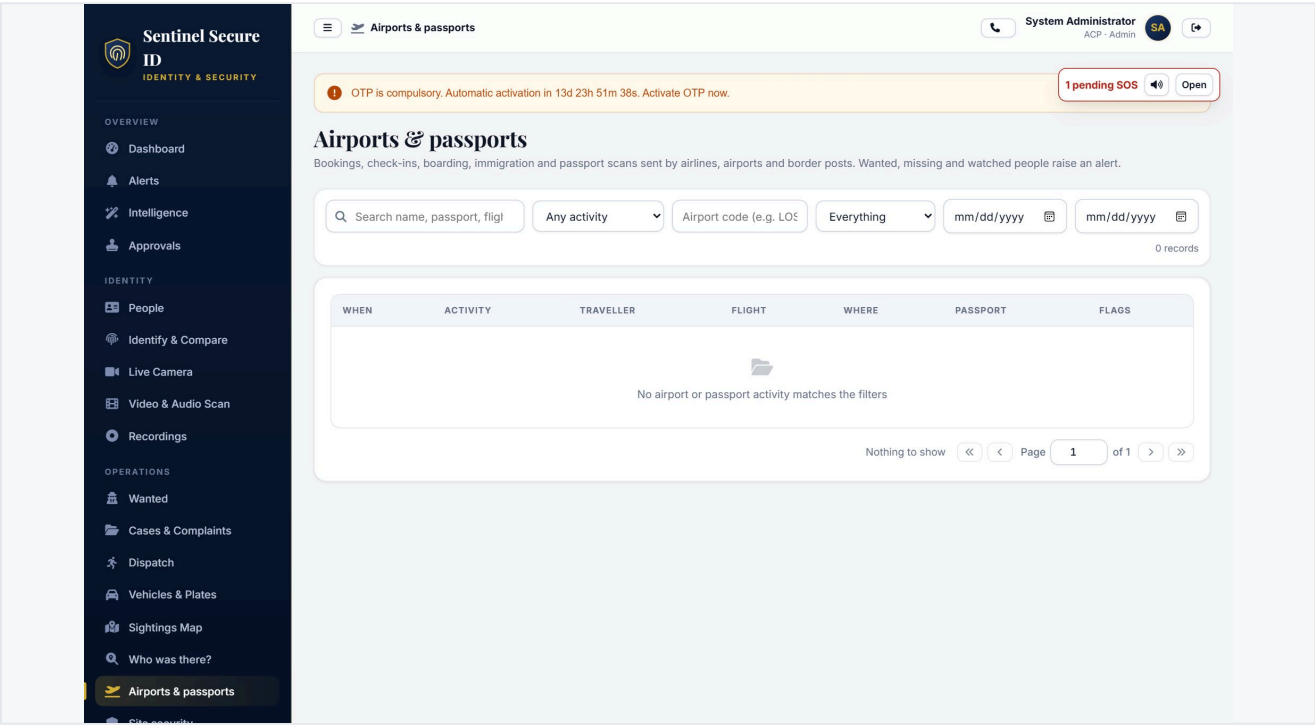
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Events and investigation

Follow connected records and incoming partner events.

- Built-in local analysis presents wanted-record results, hotspots, warnings and person context in compact tables and charts with supported drill-down.
- Case reports highlight overdue work and inactive cases. Authorised staff can reassign cases and send reminders to responsible officers.
- Relevant pages provide permission-controlled reports and exports. Backend search, pagination and on-demand tab loading avoid downloading entire registers.
- Analytics reflect recorded data and configured rules. Forecasts and biometric candidates require human review and are not proof of an offence.



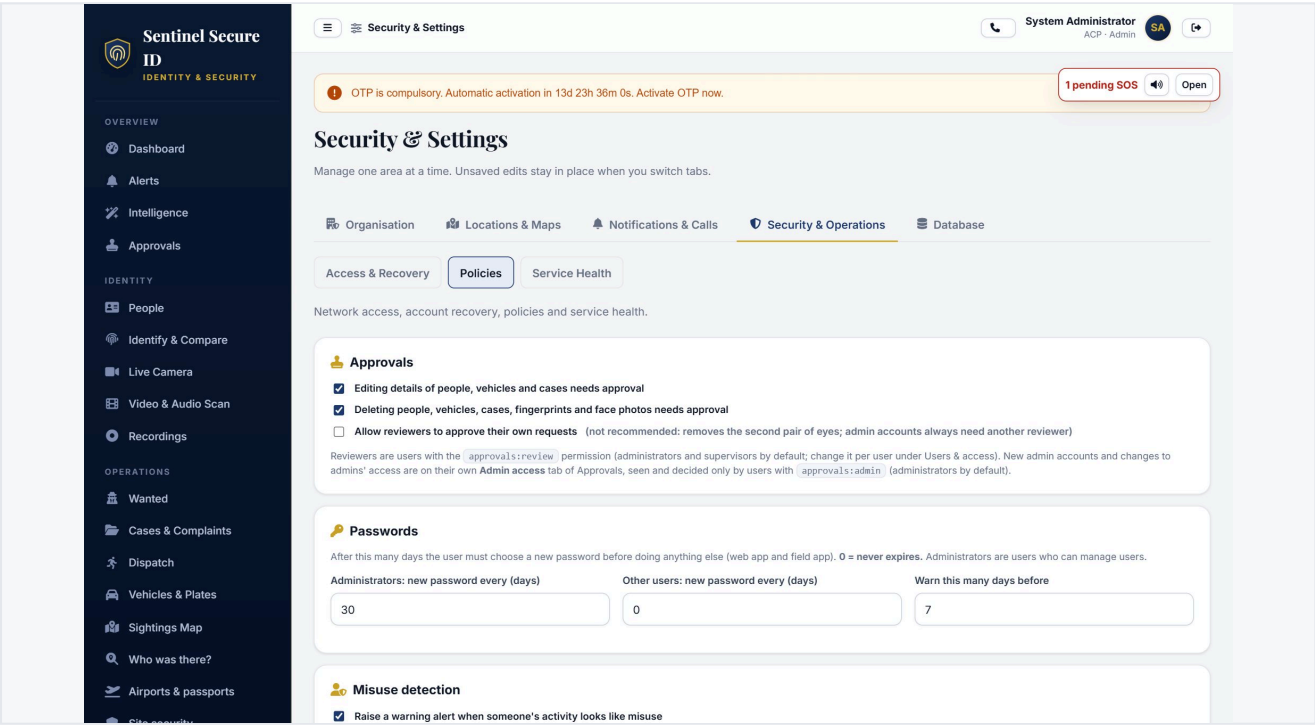
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Account security and accountability

Protect access to the system and keep sensitive changes under review.

- Approved devices and a separate gateway help control web access. The Field app and partner APIs use their own access rules.
- Each account has one active login. Authenticator codes, recovery options and temporary permissions help administrators manage access.
- Unit and agency permissions govern case approvals. Identity changes and biometric removal have their own review process.
- Evidence checks, controlled downloads, activity records and encrypted backup tools support responsible handling of data.



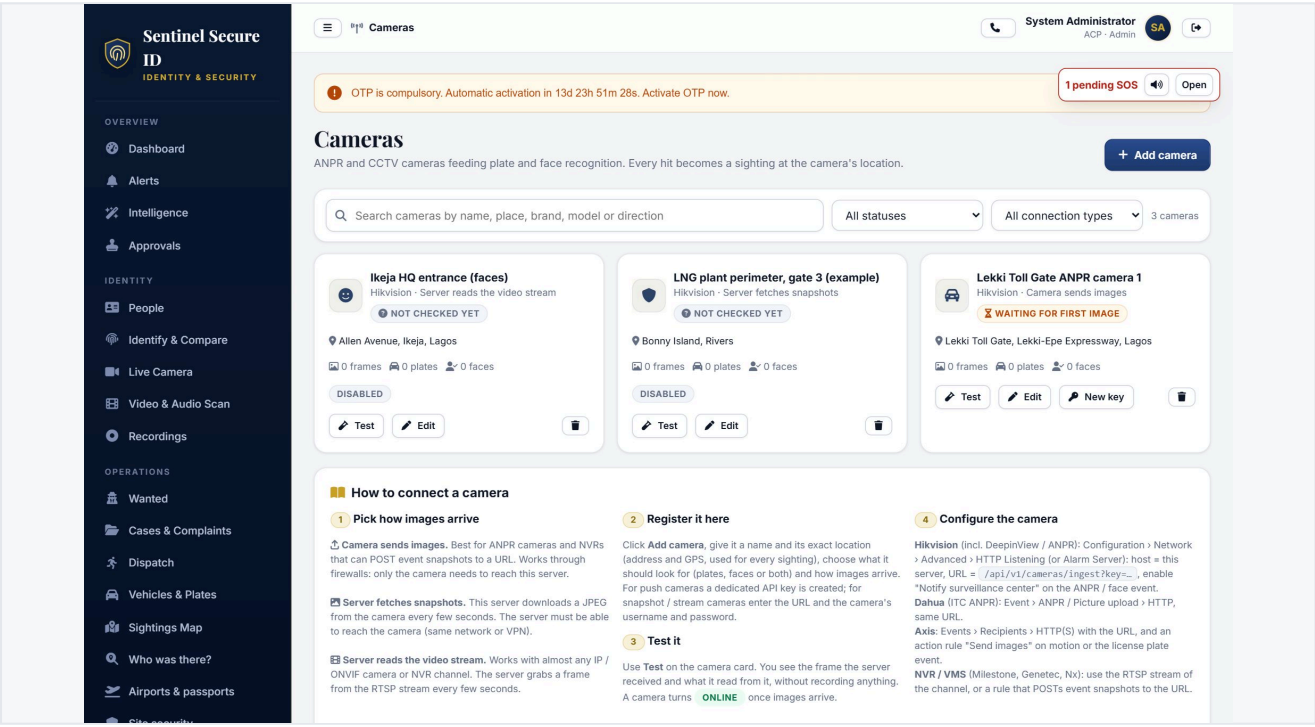
Demonstration interface. Configuration and access permissions affect the available workflow.

PLATFORM CAPABILITIES

Deployment and integrations

Plan capacity and external services around the agency’s needs.

- Deploy on infrastructure controlled by the organisation and use permission-scoped APIs for authorised integrations.
- Backend search and pagination keep large record selectors from downloading the complete register.
- External audit archives, fingerprint quality tools, capture assurance, device attestation and National/Bank/TAX ID verification are configurable integrations.
- Provider contracts, credentials, certificates and production testing are required where applicable. Capacity, availability and recognition accuracy must be measured for the intended deployment.



Demonstration interface. Configuration and access permissions affect the available workflow.

OPERATING MODEL

A common picture for each team

Each team works from connected records, with the access and responsibilities appropriate to its role.

Team	Daily work	Control to agree
Control and dispatch	Review pending SOS, camera events and officer availability; coordinate a response.	Define acknowledgement, escalation and shift handover responsibilities.
Field officers	Check authorised records, capture complaints and photos, receive assignments and report progress.	Approve the device, set location permissions and rehearse poor-connectivity procedures.
Investigators	Review identity histories, candidate matches, evidence and linked cases.	Use source records, preserve context and document the basis of decisions.
Supervisors	Review assignments, approvals and operational reports.	Agree who may approve sensitive changes and close an investigation.
Administrators	Manage roles, devices, connections, account controls and configuration.	Restrict privileged access and retain administrative audit records.
Authorised partners	Supply permitted events or records through scoped connections.	Agree the data-sharing scope, credential owner and revocation procedure.

This is a proposed operating model. Actual roles, permissions and approval routes are configured with the organisation.

IDENTITY CONTINUITY

When contact details change

A phone number is a contact point with a history. It is not a permanent identity.

01 / First assignment

Record the person, number and relevant dates. Keep other identifiers and the source of the information.

02 / Number replaced

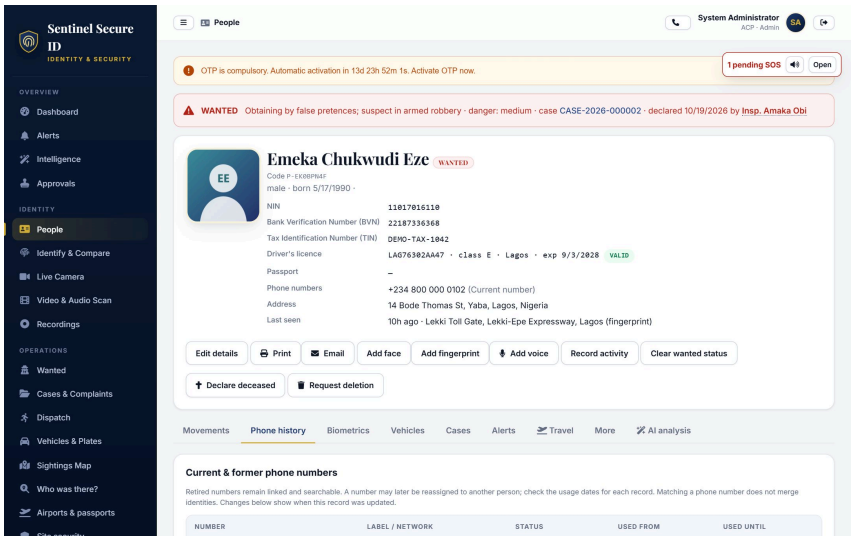
Retain the earlier number in the history and record the replacement. Do not erase the context of an older case.

03 / Number reassigned

Record that another person uses the number later. Review assignment dates before linking a search result to a person.

04 / Investigator review

Compare dates, source records, identifiers and case context. A matching number alone does not establish identity.



Demonstration person profile and identity history.

Person profile

Multiple current and retired phone numbers, bank accounts, Bank ID and TAX ID details remain connected to the person record.

Local terminology

Set National ID, Bank ID and TAX ID labels under Organisation & country to match the deployment.

CAMERA HARDWARE GUIDE

Choose the view before the device

Common camera categories serve different locations. Select exact devices after a site survey and integration test.



Bullet

Gates, driveways and focused perimeter views.



Dome

Indoor corridors, reception and shops.



PTZ

Wider observation with device-dependent pan, tilt and zoom.



ANPR

Plate capture with suitable position, shutter and illumination.



Solar / 4G

Remote locations with an engineered power and data budget.



Body-worn

Field footage through an agreed capture or upload workflow.

Camera types for different deployment needs. Body-worn and PTZ functions depend on the selected device and integration.

Check image quality, supported image or stream output, authentication, connectivity and mounting conditions before procurement.

CAMERA CONNECTION OPTIONS

Connect the source to the workflow

Use a connection method the selected camera or gateway can actually provide.

Method	How it works	Verify during the pilot
Camera sends images	An approved camera or gateway uploads captures using its dedicated camera key.	Confirm server reachability, image format, timing, registered camera location and credential rotation.
Server fetches snapshots	The server retrieves a supported camera image endpoint.	Confirm network routing, authentication, capture frequency and how an unavailable camera is reported.
Supported stream	An available stream supplies frames through the configured integration.	Test the actual codec, transport, bandwidth, sampling and recovery after an interruption.
Field phone sharing	Headquarters requests a remote camera view from an approved field device.	Verify officer consent, network behaviour, device permissions and how sharing ends.

Image-push onboarding

Register

Create and approve the camera record, site and location.

Configure

Use the server connection instructions and the dedicated revocable key.

Send a test

Confirm the received image, source association, time and location.

Exercise the response

Test a configured event, operator review and dispatch.

The dedicated image-upload service does not require a source-IP allowlist. The camera still needs an approved connection and valid credentials. Production connections should use HTTPS and protected secrets.

ILLUSTRATIVE CAMERA RESPONSE

A perimeter event becomes a reviewed lead

The camera captures the scene. The operator checks the context. The responder receives the assignment.



Example scenario: perimeter crossing and vehicle detection.

01 / Capture and alert

An approved source supplies an image. A configured site rule raises an event with the source location and captured scene.

02 / Review

Control checks the image, time, location and site context before deciding what action is justified.

03 / Dispatch

Select a nearby or specific officer. Send instructions and follow acceptance and progress.

04 / Preserve

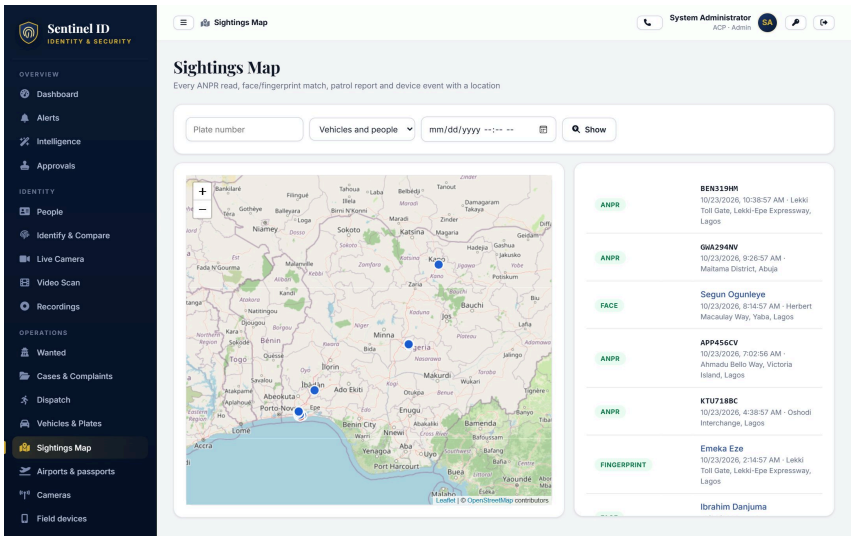
Connect relevant captures and observations to a case, preserving source context and handling history.

Detection results support human review. A highlighted object, plate read or biometric candidate does not by itself establish a crime or identify an offender.

ILLUSTRATIVE VEHICLE RESPONSE

Follow a plate read back to its source

A flagged vehicle sighting is useful when the operator can examine the image and the record behind the alert.



Demonstration sightings map. Events are fictional.

Flag and scope

An authorised user records a vehicle lookout linked to the relevant investigation.

Observe

A connected camera supplies a readable capture and source location.

Review the candidate

Check the plate characters against the image, confirm the flag is current and review the source time.

Coordinate

Issue a dispatch where appropriate, follow acceptance and record what the responding officer finds.

Capture conditions matter

Lane geometry, plate size in the image, vehicle speed, focus, lighting, reflections and weather all affect recognition. Validate daytime and nighttime captures at the actual site.

This is an illustrative workflow, not a promise of an arrest, an identification rate or a response time. Licensing and insurance checks require authorised records or a configured partner connection.

CAMERA DEPLOYMENT PLANNING

Design coverage around the site

A useful camera installation begins with the observation needed and the response available.

Survey topic	Decisions to record
Purpose and area	Define the gate, road lane, fence line or public area; specify the event an operator needs to review.
Capture geometry	Test height, angle, distance, plate or subject size, occlusion and coverage at the relevant times.
Lighting and weather	Test glare, headlights, low light, rain and the selected illumination method.
Power	Record load and operating schedule. Size mains backup or solar panel and battery for the location and autonomy target.
Connectivity	Measure upload capacity and latency. Confirm routing, mobile coverage and recovery after a connection loss.
Physical installation	Agree mounting, enclosure, tamper exposure, service access and maintenance responsibility.
Data and access	Agree capture frequency, permitted uses, retention, operator permissions and who can export material.
Response	Name the team receiving alerts, acknowledgement procedure and available dispatch coverage.

Minimum pilot kit to agree

Camera and mount; suitable power supply; network connection or gateway; server capacity; protected connection credentials; operator access; and a maintenance plan. Solar and cellular components are site-specific options.

Illustrated camera types do not establish support for every device. Prove compatibility with the intended model, firmware and connection method before purchasing a fleet.

CAPACITY PLANNING EXAMPLE

Turn the capture plan into a storage estimate

Estimate the data workload from measured images and the agreed retention period. The numbers below are an example, not a platform capacity claim.

Daily image storage = cameras × images per day × average image size

Example assumption	Value
Image-push cameras	24
Capture interval	One image every 30 seconds per camera
Images per camera per day	2,880
Average stored image size	200 kB, using decimal units
Total images per day	69,120
Raw image storage per day	13.824 GB
Raw image storage for 30 days	414.72 GB

Add to the raw estimate

- Database records and indexes.
- Audit records, attachments and retained clips.
- Redundancy, backups and growth allowance.

Measure separately

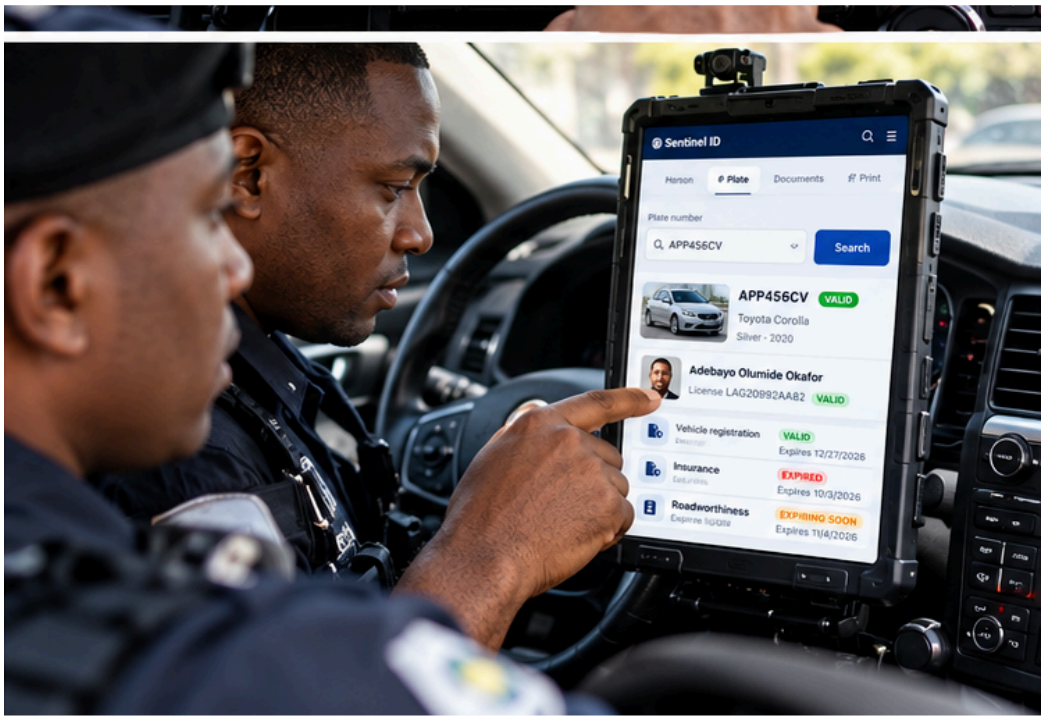
- Stream bandwidth and video retention.
- Processing cost at the actual capture rate.
- Search latency and operator review workload.

Motion-triggered capture, compression and actual image size change the result. Retaining full video can dominate storage. Benchmark the proposed deployment rather than extrapolating from this example.

FIELD OPERATIONS IN CONTEXT

From a patrol check to a dispatch

Phones, tablets and control-room screens support different stages of the same operational record.



Example scenario: checking a vehicle record during patrol.

Before the assignment

Approve the device and user access. Confirm sign-in, app lock, location and notification settings.

During the patrol

Search permitted person or vehicle records, capture a complaint, attach a photo and record a location where available.

When control dispatches

Review instructions, accept the assignment and report progress. The dispatcher follows the response and can call back after a dropped call.

When coverage drops

Use supported offline complaint capture. Live calls, fresh searches and new server events need connectivity.

The phone’s built-in biometric sensor unlocks the app. It does not export fingerprints for searching other people’s identity records. Identity capture needs a supported scanner or input workflow.

DEPLOYMENT BLUEPRINT

Connect the installation without hiding dependencies

Separate the record system, capture sources and external services so every dependency has an owner.

Capture and field

Approved cameras / supported scanners / Android phones and tablets / authorised partner sources

↓ controlled connections ↓

Sentinel ID

Identity register / cases and evidence / sightings and alerts / dispatch and communications / access and audit

↓ organisation-controlled storage and services ↓

Operational infrastructure

Application hosting / database and files / backup and restore / monitoring / keys and certificates

Configure external services explicitly

External audit archives, fingerprint quality, capture assurance, device attestation, National ID, Bank ID and TAX ID verification, and release-signer verification require the relevant configuration. Maps, notifications and voice relay requirements depend on the deployment.

Organisation responsibilities

Assign access owners, approve data sources, set retention and arrange hardware, networking and provider authority.

Pilot responsibilities

Verify compatibility, record expected behaviour, exercise failures and document acceptance results.

This is a conceptual deployment view. The final network topology and infrastructure sizing follow a technical survey. The platform does not grant access to third-party databases.

PILOT ACCEPTANCE WORKSHEET

Make success observable

Agree the targets before the pilot, then record evidence against each one. Suggested checks are below; thresholds are set with the organisation.

Workflow	Demonstration or test	Evidence to retain
Identity history	Replace and reassign a phone number across dated person records.	Earlier history remains visible; the later assignment is distinct.
Fingerprint / face review	Run representative captures, including difficult and non-matching samples.	Candidate quality, review decisions and measured errors; no assumed accuracy.
Camera integration	Send and fetch supported images using the intended devices.	Correct source association, usable image and tested access revocation.
Site detection	Use agreed test events under day and night conditions.	Source images, alerts, misses and operator review workload.
SOS and callback	Send an emergency, acknowledge it, assign a responder and exercise a dropped call.	Notification, map handling, acceptance and successful callback where connectivity permits.
Offline field capture	Save a complaint offline, reconnect and repeat a lost-response submission.	Usable local draft, later sync and duplicate prevention.
Access and recovery	Revoke a device, test permissions and restore a separate recovery copy.	Denied access where expected and documented restore results.

Record device and camera models, firmware, configuration, network conditions and test data alongside the results. Resolve failed checks and operational dependencies before acceptance.

SCALING AND CAPACITY PLANNING

Plan for up to 10 billion people

The website capacity planner ranges from one million to ten billion people, with separate fingerprint-template and face-record controls.

People × enrolled fingers per person = fingerprint templates

Planning example	People	Templates at 10 fingers	Faces at 1 per person
Initial operating scale	1 million	10 million	1 million
Large register scenario	400 million	4 billion	400 million
Maximum planner scenario	10 billion	100 billion	10 billion

Separate population from records

A person can have several biometric samples or enrolment versions. The people slider derives an initial gallery using the selected fingers-per-person setting; independent record sliders allow a different capture plan.

Separate records from activity

A register's stored population does not tell you its concurrent query rate, image-ingestion volume, operator workload or recovery requirement. Size each role against its own workload.

Search roles

Gallery partitions, candidate retrieval, exact comparisons and result coordination.

Camera roles

Capture frequency, ingestion bursts, event review and device connectivity.

Data roles

Database indexes, event history, evidence, retention and backup copies.

Operational roles

Web and field access, permissions, monitoring and recovery procedures.

Ten billion is the selectable planning range. It is not evidence of a deployed population or a benchmarked system capacity. Final sizing and response targets require representative testing on the proposed installation.

Interactive planner: SentinelSecureID.com/scale#calculator

SCALING ASSUMPTIONS

Understand what the projection includes

The planner makes its arithmetic visible. Replace the assumptions with target-hardware measurements during engineering and acceptance.

Model input	Illustrative assumption
Fingerprint matcher memory	1.7 kB per template; 340 GB usable gallery memory on a nominal 512 GB server.
Fingerprint candidate index	525 bytes per template, before additional index replication and operational overhead.
Search copies	Two matcher copies and two face-search copies in the resource estimate.
Comparison arithmetic	64-core search role; 100,000 to 200,000 fingerprint comparisons per second per core as a planning range.
Face gallery	One billion descriptors per modelled shard; actual descriptor and index overhead must be measured.
Database estimate	420 bytes per fingerprint record and 1,100 bytes per face record, held in three copies; not total database storage.
Resource multiplier	Standard, twice or five times the search resources; the multiplier changes the arithmetic projection.

Additional resources

Camera ingestion, event and plate storage, full media files, backup capacity, network infrastructure and operating headroom need their own sizing plan.

Additional validation

Measure shortlist recall, real contention, concurrency, tail latency, warm-up, outages and recovery. Daily search projections assume continuous work and do not establish service capacity.

The platform’s practical capacity, availability and recognition performance are determined by the configured implementation and measured results. This proposal does not state that a ten-billion-person deployment has been delivered or validated.

SECURITY / CONTROLLED CONNECTIONS

Approved access to a private workspace

Approve the devices used for web access. Field devices and partner systems follow their own access rules.

Approved devices for web access

- Web access can require the Sentinel access client on an approved device. The server checks the installation before allowing a connection, including for privileged accounts.
- The client opens the workspace through a local connection and stops after an hour without activity. A copied program folder does not give another device approval.
- The Android Field app uses its own device approval. Partner systems connect through permission-controlled APIs, with IP restrictions when enabled. Neither needs the desktop access client.

The random local browser address is the installed client tunnel. The configured destination remains visible in the client. It does not route unrelated internet browsing.

Operational acceptance

- Approve and revoke a test installation, then verify its requests at the server.
- Test account verification, replay rejection, idle stop and restarting the client.
- Validate target operating-system packages and distribution requirements before rollout.

SECURITY / GATEWAY ARCHITECTURE

An outbound connection from the private server

A separate public gateway carries pages and APIs without publishing the private application address.

Connection	Purpose and control
Installed client to gateway	Approved access for web users, checked by the application server.
Private agent to gateway	The private server starts a secure connection to the gateway.
Field and partner APIs	Approved devices or API keys with limited permissions. IP restrictions apply when enabled.
Private agent to application	Requests reach the private application, where account and record permissions still apply.

- Staff and authorised partner systems connect through a secure public gateway. It carries pages, API requests, file transfers and live communications.
- The private application server starts the connection to the gateway. This allows the application and database to stay on the organisation’s private network.
- The gateway supports a separate access point for the service. Production planning covers network security, reliable connectivity and enough capacity for the expected traffic.

The gateway protects access when the network keeps the application and database private. Capacity depends on the traffic being carried, especially continuous video.

SECURITY / ACCOUNTS AND REVIEW

Sessions, temporary access and team approvals

Limit both who can act and how long that authority remains valid.

Account security and temporary access

- Each account has one active login. Signing in on another device signs out the earlier session. Password and security changes also end earlier sessions.
- Web users receive a 14-day deadline to set up an authenticator app. They can manage their password, authenticator and single-use recovery codes from their profile.
- Administrators can grant extra permissions for a set number of days. Attempt limits and account lockout help prevent repeated password or code guesses. The Android Field app follows its own device security controls.

Case and identity approvals

- Every officer belongs to a unit or station. Approval permissions can limit case reviewers to their own unit or agency. Self-approval follows the organisation’s policy.
- A separate review queue handles suggested links between cases and people, missing biometrics, new person records and possible duplicates.
- Removing a biometric requires the relevant permission and approval. The system checks the reviewer’s authority and records the decision before applying the change.

SECURITY / EVIDENCE AND ASSURANCE

Preserving responsibility and recovery options

Keep track of evidence, review access and prepare for recovery.

Evidence and confidential records

- Evidence records include checks for file changes and a history of who handled each item. Digital signatures and legal holds are available when set up for the organisation.
- Permissions govern access to personal details, biometrics, reports and downloads. Operational reports let authorised staff choose dates and open supporting records from available charts.
- Temporary scans and processing files are kept separately for cleanup. Clearing them leaves registered biometrics and protected evidence intact.

Activity records and recovery

- Activity records help administrators review actions and investigate unusual use. Integrity checks help identify changes to the audit trail. An external archive can be connected where required.
- Encrypted backups, archive checks and restore exercises support recovery. Signing and backup keys need their own protected storage.
- Device revocation, secure connections and release checks support day-to-day security. External identity checks and device verification work only after the required services have been connected.

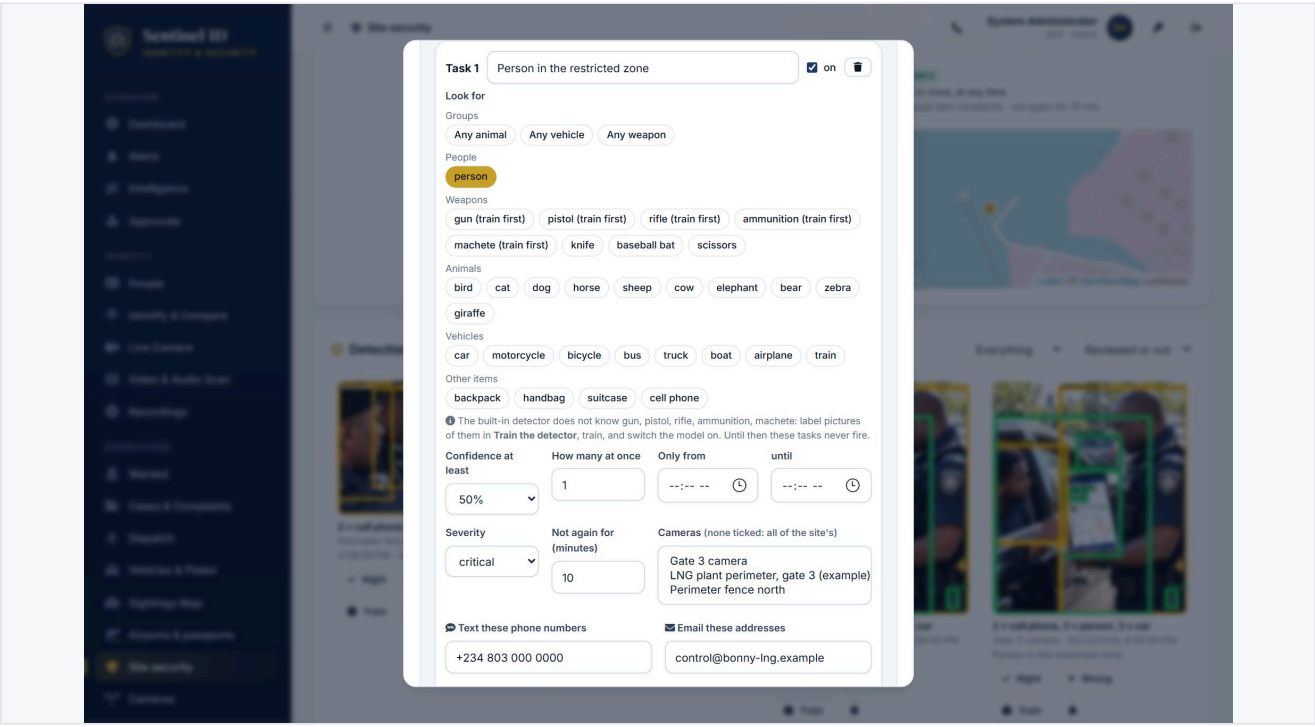
External archives and identity checks need an authorised provider. Protect recovery keys and test backup restoration before relying on it.

SITE SECURITY / COVERAGE AND RESPONSE

A site, its cameras and its operating rules

Use the existing Site security workspace to register coverage and connect detections to response.

- Record the site location and type, attach cameras and set the operating period.
- Check camera placement, useful image detail, lighting and network reachability at the site.
- Configure supported rules and response recipients. Background analysis requires connected cameras and working detection workers.
- Open a small, searchable camera page and preview only the cameras needed. Start and stop previews individually.
- Review observations, site detections and watchlist leads before taking operational action.



Demonstration site configuration. Site setup does not certify coverage or recognition accuracy.

AI TRAINING / CONTINUED IMPROVEMENT

Additional examples, independent validation

Extend existing labelled data and evaluate a candidate before changing live detection.

Dataset and continuation

- Collect authorised pictures with provenance. Label object boxes and include background-only scenes.
- Add examples to an existing dataset or continue training from an earlier model.
- Keep independent validation and full-frame test pictures outside training.

Evaluation and activation

- Review per-label precision and recall, misses, duplicate detections and false alarms on full frames.
- Review the test results before activation. A failed training run leaves the previous model in place.
- Test the model at the site and add examples where it struggles.

Test each detector with the cameras and conditions where it will be used. Review false alarms and missed detections before approving it for live monitoring.

ILLUSTRATIVE CASE STUDIES

Officer safety and field continuity

These scenarios explain workflows. They are not verified customer deployments or measured results.

ILLUSTRATIVE SCENARIO / OFFICER SAFETY

An officer loses the connection during an SOS

An officer sends an SOS during patrol. A voice call to headquarters drops before the details are complete.

1. Control receives the minimized pending-emergency badge and a new-alert sound. The emergency remains pending until acknowledged.
2. The dispatcher opens the reported map location, checks the age of nearby officer positions and sends a nearby responder or chooses a specific officer.
3. Control uses Call back to reach the originating officer directly. The responder accepts the dispatch and reports progress.

Practical value: A visible acknowledgement step and a linked response record help control follow up.

Conditions: The map needs reported coordinates. Voice reconnection depends on connectivity, permissions and a suitable relay configuration.

ILLUSTRATIVE SCENARIO / FIELD OPERATIONS

A complaint starts where there is no signal

An officer takes a complaint on an approved Android tablet in an area with unreliable data coverage.

1. The officer records the description and statement, reviews spelling suggestions and saves an encrypted local draft.
2. When connectivity returns, the app retries synchronisation. An idempotency reference helps prevent duplicate complaints after a lost response.
3. The case enters the agency’s normal assignment, evidence and review workflow.

Practical value: Field capture can continue while the network is unavailable.

Conditions: Server searches, live calls and external checks require connectivity. Device approval and storage must be correctly configured.

ILLUSTRATIVE CASE STUDIES

Identity history and camera observations

Agency procedures and supporting evidence determine the appropriate action.

ILLUSTRATIVE SCENARIO / IDENTITY HISTORY

A phone number belongs to a different person later

An investigator searches a number that a witness stopped using last year. Another person now uses the same number.

1. The register retains the earlier person's dated phone history and records the later assignment separately.
2. The investigator compares the relevant dates, registered identifiers and case context.
3. Any update follows the applicable permissions and approval policy, while the change history remains available.

Practical value: The record preserves context when a number changes hands.

Conditions: A shared or reassigned number is not proof that two people are the same person. Information remains subject to authorised verification.

ILLUSTRATIVE SCENARIO / CAMERA OPERATIONS

A camera reports a vehicle on a lookout

An agency flags a vehicle associated with an open investigation. A connected camera sends a readable plate image.

1. The camera submits the image using its dedicated key and registered location.
2. The system records the sighting and raises the configured alert when the recognised plate matches a flagged record.
3. An authorised operator reviews the source image, checks the record and issues a dispatch where appropriate.

Practical value: A camera observation can become a reviewed investigative lead with a location and time.

Conditions: Plate recognition depends on image quality, supported formats and deployment validation. This scenario does not claim an arrest or guaranteed match.

ILLUSTRATIVE CASE STUDIES

Partner access and device review

Illustrative workflows, not verified customer results. The stated dependencies apply.

ILLUSTRATIVE SCENARIO / PARTNER INTEGRATION

A travel watch receives an authorised partner event

An agency places a travel watch on a registered person. An authorised airline or border integration supplies an event.

1. A scoped partner credential submits the supported event and its reference identifiers.
2. The system records the event and evaluates the configured watch conditions.
3. An authorised reviewer checks the alert and supporting records before taking action under the agency's procedures.

Practical value: Partner events appear alongside other recorded activity for a permitted investigation.

Conditions: This requires an actual partner connection, data-sharing authority and matching identifiers. It is not evidence of a live airline or border deployment.

ILLUSTRATIVE SCENARIO / ACCESS CONTROL

An unfamiliar device attempts to sign in

An administrator sees a sign-in attempt from an Android installation that has not been approved.

1. The installation enters the configured device approval and key-enrolment process.
2. An authorised administrator reviews the request and can refuse or revoke the device, investigate the account and rotate credentials.
3. Web authenticator policy, session controls and audit records support the follow-up.

Practical value: Device review gives administrators an explicit control over field access.

Conditions: Effective protection also requires secure device configuration, account hygiene and timely administrative review.

ILLUSTRATIVE CASE STUDIES

Recovery and remote cameras

Illustrative workflows, not verified customer results. The stated dependencies apply.

ILLUSTRATIVE SCENARIO / CONTINUITY

A restore drill checks recovery readiness

The agency wants to confirm that an encrypted archive can restore a working copy before it relies on the backup process.

1. An authorised operator creates an encrypted archive using the provisioned backup key.
2. The team verifies it and restores into a separate, isolated recovery database and storage location.
3. Operators compare the restored records and attachments and record the drill result against the recovery procedure.

Practical value: A completed drill provides evidence about that archive and recovery procedure.

Conditions: Protected keys, sufficient storage and an isolated recovery target are essential. This is not an uptime or recovery-time guarantee.

ILLUSTRATIVE SCENARIO / CAMERA CONNECTION

A remote camera sends an image to control

A remote site has a camera that can upload images but cannot accept an inbound connection from the control room.

1. An administrator registers the camera location and supplies its dedicated upload key and server connection details.
2. The camera submits supported images over a reachable network connection. Source-IP allowlisting is not required for this image-upload service.
3. The operator reviews recorded observations and configured alerts. The administrator can rotate or revoke the key.

Practical value: Outbound image upload offers a connection path for supported remote cameras.

Conditions: The camera must support the required image request, reach the server and protect its credential. Network coverage and camera compatibility need testing.

ILLUSTRATIVE CASE STUDIES

Video review and shared cases

Illustrative workflows, not verified customer results. The stated dependencies apply.

ILLUSTRATIVE SCENARIO / VIDEO INVESTIGATION

Investigators review a submitted video

An authorised investigator has approved CCTV footage relevant to an open case.

1. The investigator submits a supported recording for video analysis.
2. The system extracts candidate observations and compares supported biometric information with the registered records.
3. The investigator reviews candidate matches, source frames and relevant timestamps before linking any finding to the case.

Practical value: The workflow helps organise review of recorded footage.

Conditions: Quality, visibility and representative recognition evaluation matter. A candidate does not establish identity or guilt.

ILLUSTRATIVE SCENARIO / AGENCY COOPERATION

Two agencies review an authorised shared case

A case owner needs a second agency to review permitted information without opening the entire case register.

1. An authorised owner selects the receiving agency through a live backend search.
2. Sharing rules and the receiving user’s permissions determine the available case information and actions.
3. The teams record their notes and follow the normal evidence, assignment and approval processes.

Practical value: Explicit case sharing supports cooperation with a defined access boundary.

Conditions: Agency agreements, user permissions and evidence-handling procedures must be established. Sharing a case does not grant access to unrelated records.

ILLUSTRATIVE CASE STUDIES

Identity checks and inconsistencies

Illustrative workflows, not verified customer results. The stated dependencies apply.

ILLUSTRATIVE SCENARIO / IDENTITY INVESTIGATION

A claimed identity needs further checking

An officer has a permitted reason to verify a person's claimed identity using an external fingerprint sample.

1. The officer uses a compatible scanner integration or an approved imported sample. The phone's built-in sensor only unlocks the app.
2. The system returns candidate records under the configured search threshold and review policy.
3. The officer checks independent identifiers and follows the required human verification and escalation procedure.

Practical value: The search provides leads for an authorised identity review.

Conditions: A suitable sample, hardware integration and evaluated recognition performance are required. No automatic detention or verified identification is implied.

ILLUSTRATIVE SCENARIO / IDENTITY REVIEW

Activity appears against a recorded deceased identity

A new recorded event refers to an identity marked deceased in the register.

1. The configured workflow flags the inconsistency for authorised review.
2. An investigator checks the original event, identifiers and provenance of the deceased-status entry.
3. Any correction or escalation follows the agency's evidence and approval procedures.

Practical value: The inconsistency becomes visible alongside the identity record.

Conditions: Incorrect source records and reused identifiers can produce misleading leads. An alert is not proof of fraud.

DELIVERY AND ACCEPTANCE

A pilot with explicit success criteria

Start with a bounded operating scenario and record the results before extending coverage.

01 / Scope and authority

Agree participating teams, data-sharing authority, capture sources and permitted uses. Identify external provider contracts and retention requirements.

02 / Representative demonstration

Use approved test records and actual target devices, cameras and scanners. Exercise SOS, callback, number reassignment, offline capture and case review.

03 / Operational and security testing

Measure task completion, search latency, false matches and review workload. Test connectivity loss, device revocation, audit continuity and backup restoration.

04 / Acceptance and expansion

Record results against agreed criteria. Resolve outstanding provider, hardware and infrastructure dependencies before production acceptance.

Readiness items to agree

- HTTPS, protected keys and the controlled Android signing identity.
- External verifiers and audit archives only where authorised and configured.
- Map, notification and voice relay providers where the network requires them.
- Capacity and recognition benchmarks using representative data.

NEXT DISCUSSION

Your workflow, demonstrated

Bring a small set of approved scenarios and the devices the team intends to use.

For the demonstration

- Choose an investigation and a field-response workflow.
- Identify the records, scanners, cameras and Android devices involved.
- Define what a successful result looks like and how it will be measured.
- List the partner systems and approvals that would be needed.

Sentinel ID

SentinelSecureID.com

Demonstrations, proposals and support requests:
SentinelSecureID.com/support

Built-in phone biometrics unlock the Android app and do not supply identity-search fingerprints. Identity verifiers require a configured and authorised provider. No blanket certification, capacity guarantee or comparative superiority is asserted.