

ILLUSTRATED PRODUCT PROPOSAL

# Sentinel SiteGuard

## Company camera monitoring and building access tied to accountable records.

Prepared for organisations assessing Sentinel SiteGuard. This is a product overview and proposed implementation approach, not a signed offer or statement of completed deployment.

Sentinel SiteGuard is the facility-security product. It is separate from the national identity system, Sentinel Assure workspaces and Sentinel SkyWatch. Collection permits are a review register, not an ERP or weighbridge integration.

31 October 2026

Generated cover illustration. Product-specific scope and commissioning apply.

# Executive overview

Camera monitoring, restricted-area alerts, staff and visitor access, and collection authorizations for company facilities.



Generated illustrative scenario; not a customer deployment.

## Intended team

Company security managers, control rooms and front-desk teams

## Operational outcome

Camera events and access decisions with records that can be reviewed.

## Implementation boundary

Company camera monitoring and building access tied to accountable records. Requirements depend on the chosen host, inputs, permissions and agreed integration scope.

## Decision context

The organisation retains responsibility for authorised use, staff decisions, source data and commissioning. Illustrative scenarios are examples, not customer testimonials.

# Users and responsibilities

Clear ownership supports accountable operation.



Generated illustrative scenario; not a customer deployment.

### Security manager

Configure areas and detection policies, register doors/lifts/floors and manage current-assignment permissions.

### Front desk

Register visitors and manage bookings, card issuance and badge returns within assigned permissions.

### Guard / operator

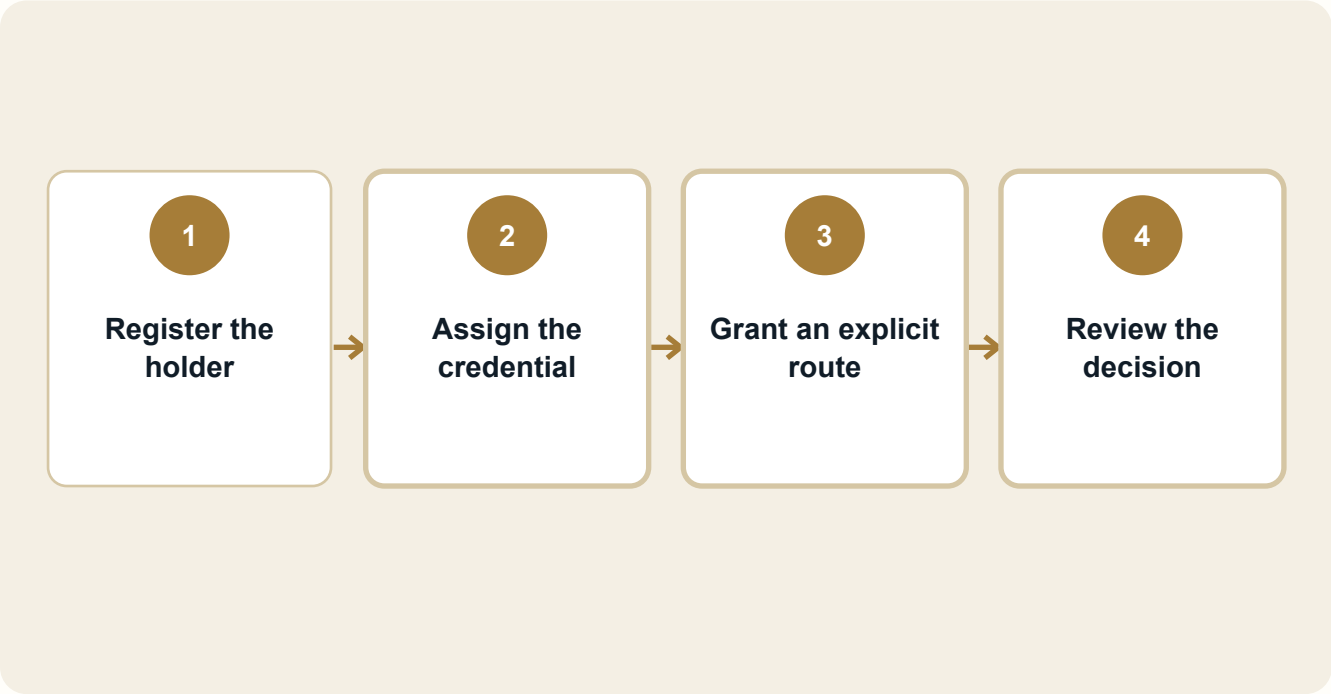
Review camera alerts and check signed credentials at registered points.

### Integration gateway

Use a scoped API key and commissioned vendor driver for mapped controller operations.

# Operational workflow

The product follows its own recorded workflow.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

### Stage 1

Register areas, cameras and permitted entry points.

### Stage 2

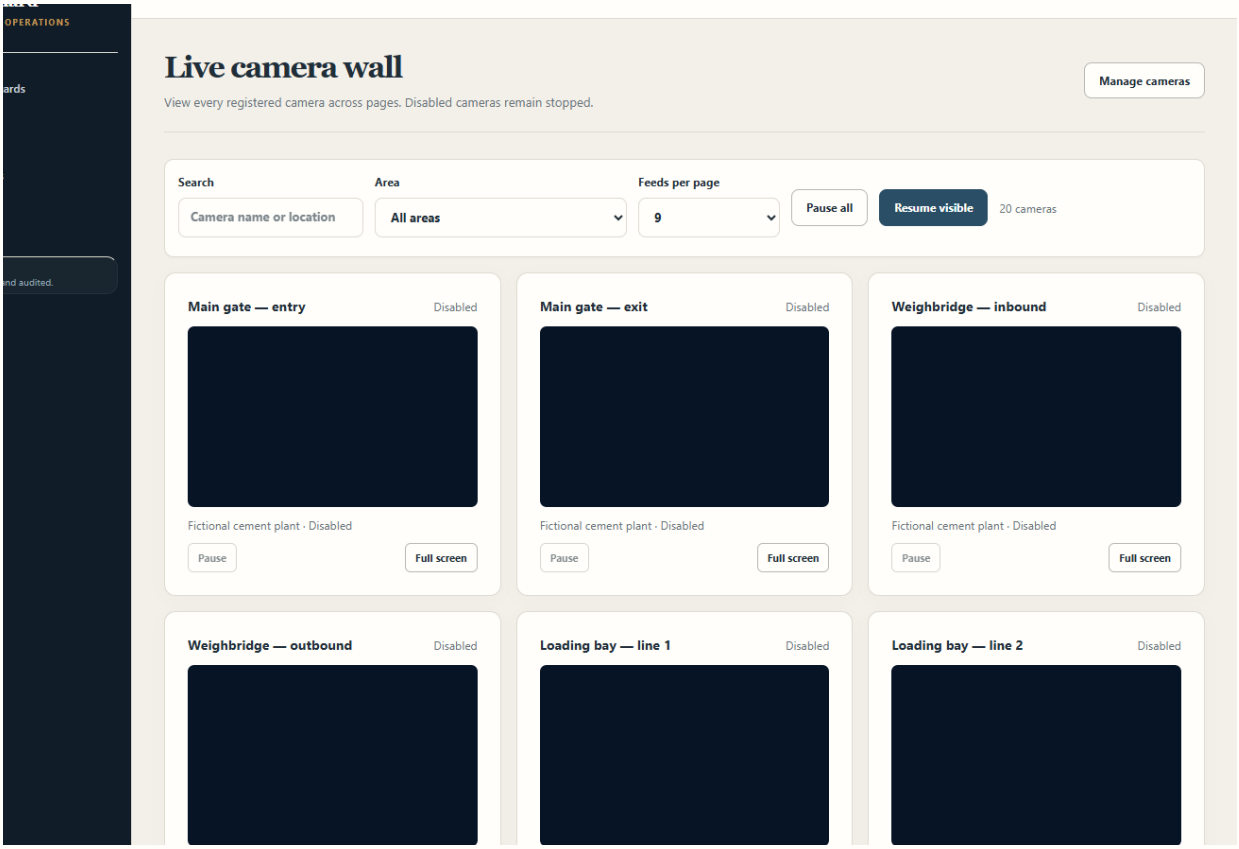
Configure monitoring rules and issue approved access or collection permits.

### Stage 3

Review alerts and credentials, verify the person or vehicle, and record the outcome.

# Site control room

Group cameras by area, review alerts and inspect detection readiness. Configure supported people and vehicle policies for the assigned coverage.




Current interface; source connections are inactive in this test capture.

## Operating approach

Schedules, thresholds and recipients should reflect the operational responsibilities. Monitoring state remains separate from the areaâ€™s physical-access policy.

## What the team reviews

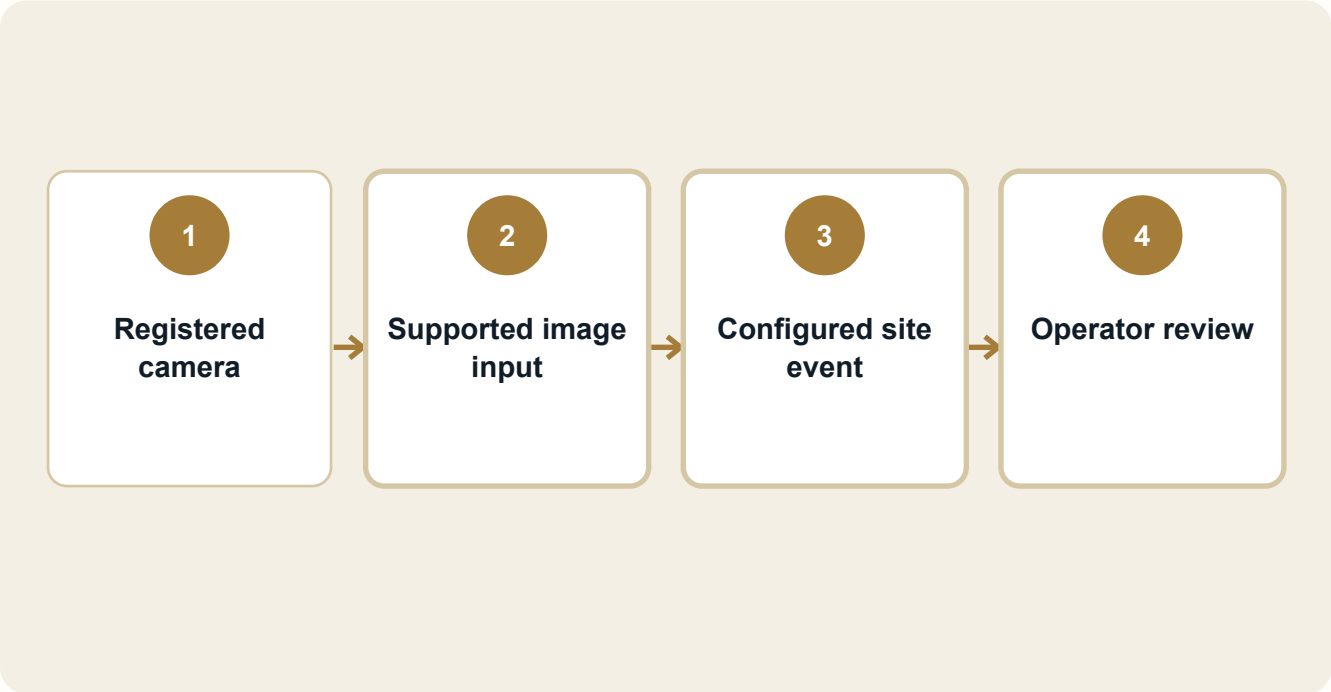
- Assign cameras to the correct areas.
- Review source images with the event.
- Separate camera monitoring from entry policy.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Camera monitoring

Supported feeds and uploads support configured object detection and operator review. The camera wall supports reviewing several feeds.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Operating approach

Image quality, placement and processing resources determine useful coverage. Model output does not establish intent or independently confirm identity.

## What the team reviews

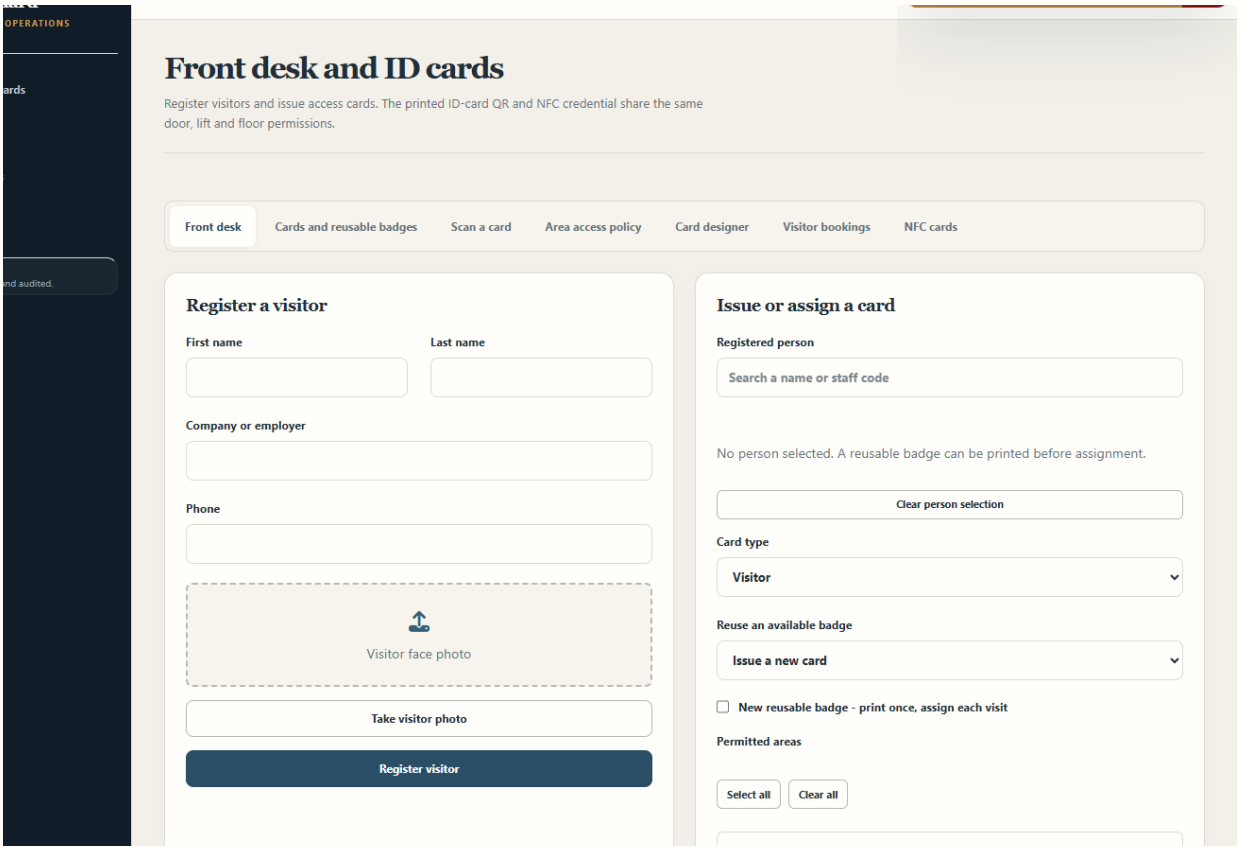
- Validate the actual stream and capture quality.
- Test day/night scenes and difficult conditions.
- Keep an operator responsible for decisions.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Visitors and reusable badges

The front desk registers permitted visitors, coordinates bookings and assigns or returns visitor badges.




Current application interface captured from the configured test system.

## Operating approach

A reusable badge keeps its signed credential. The live assignment determines its current holder, dates and areas. Staff cards remain personal.

## What the team reviews

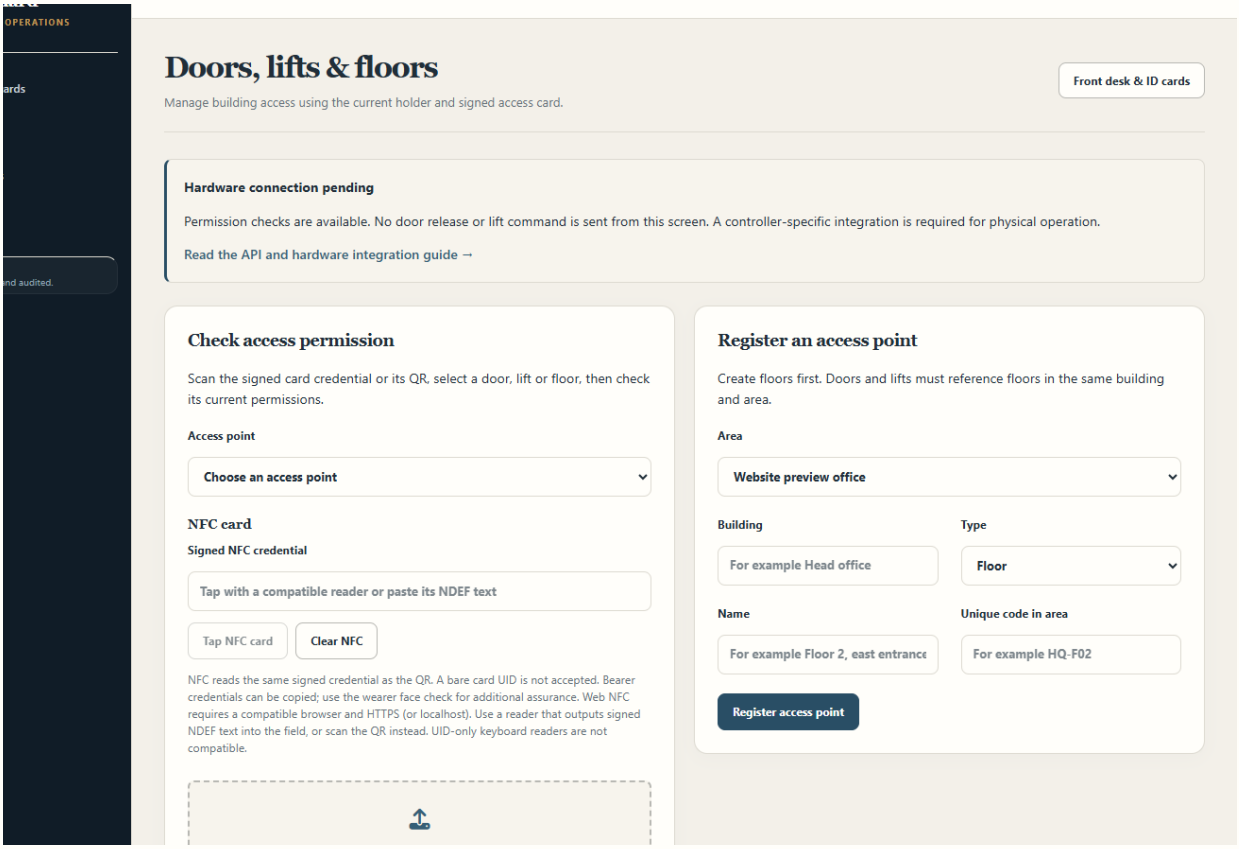
- Check approval, induction and visit state.
- Compare the wearer with the registered holder.
- Return, revoke or expire access promptly.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Doors, lifts and floors

Register floors, doors linked to floors and lifts with served destinations. Grant explicit points to the current card assignment.




Current application interface captured from the configured test system.

## Operating approach

The printed ID-card QR and NFC copy share the same signed credential and permission record. A door needs its floor; a lift needs its requested served destination.

## What the team reviews

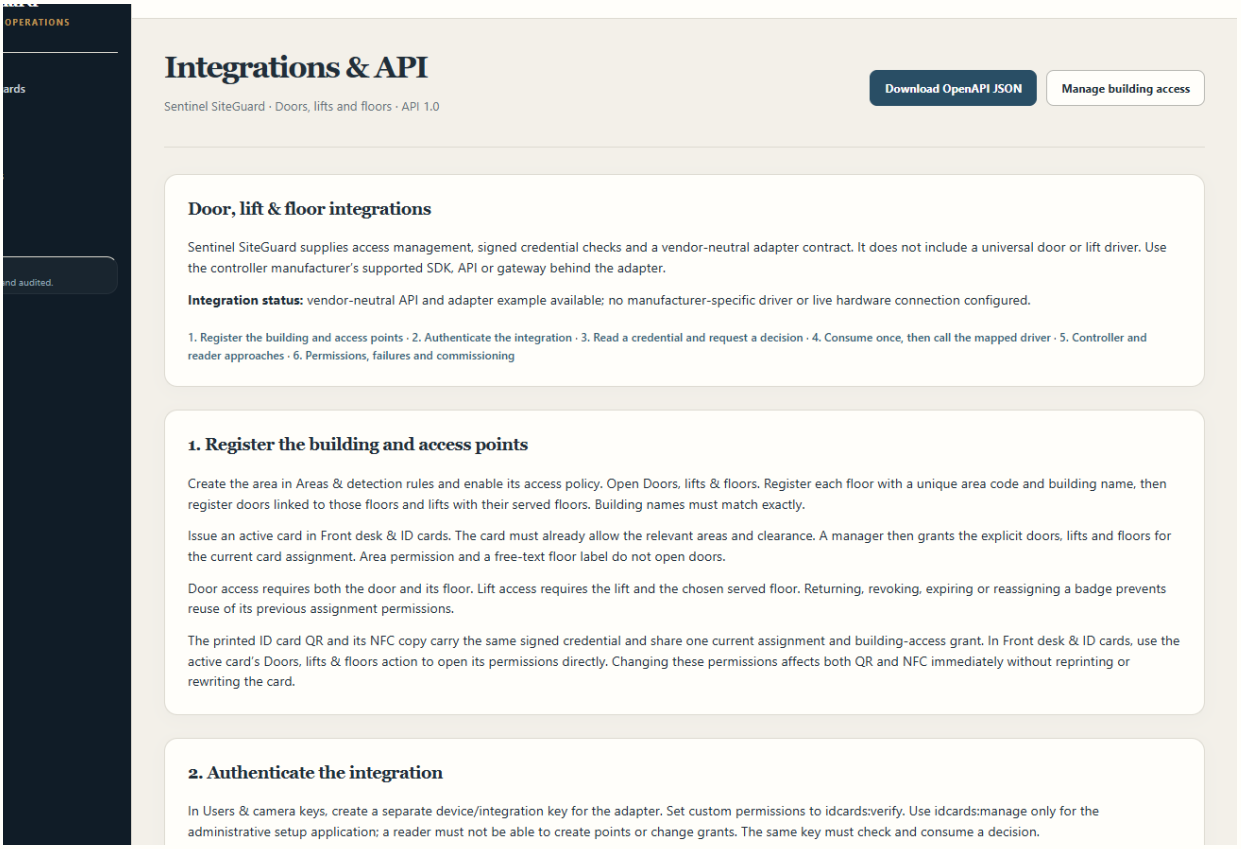
- A text floor label grants no physical entry.
- Reassignment does not inherit old grants.
- Changes affect both QR and NFC immediately.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Hardware integration API

The API checks a credential and issues a short-lived decision. The same integration key consumes it once before a trusted adapter calls the mapped vendor driver.




Current application interface captured from the configured test system.

## Operating approach

The in-app guide includes API examples, OpenAPI and failure behavior. Manufacturer-specific hardware drivers require separate setup and commissioning.

## What the team reviews

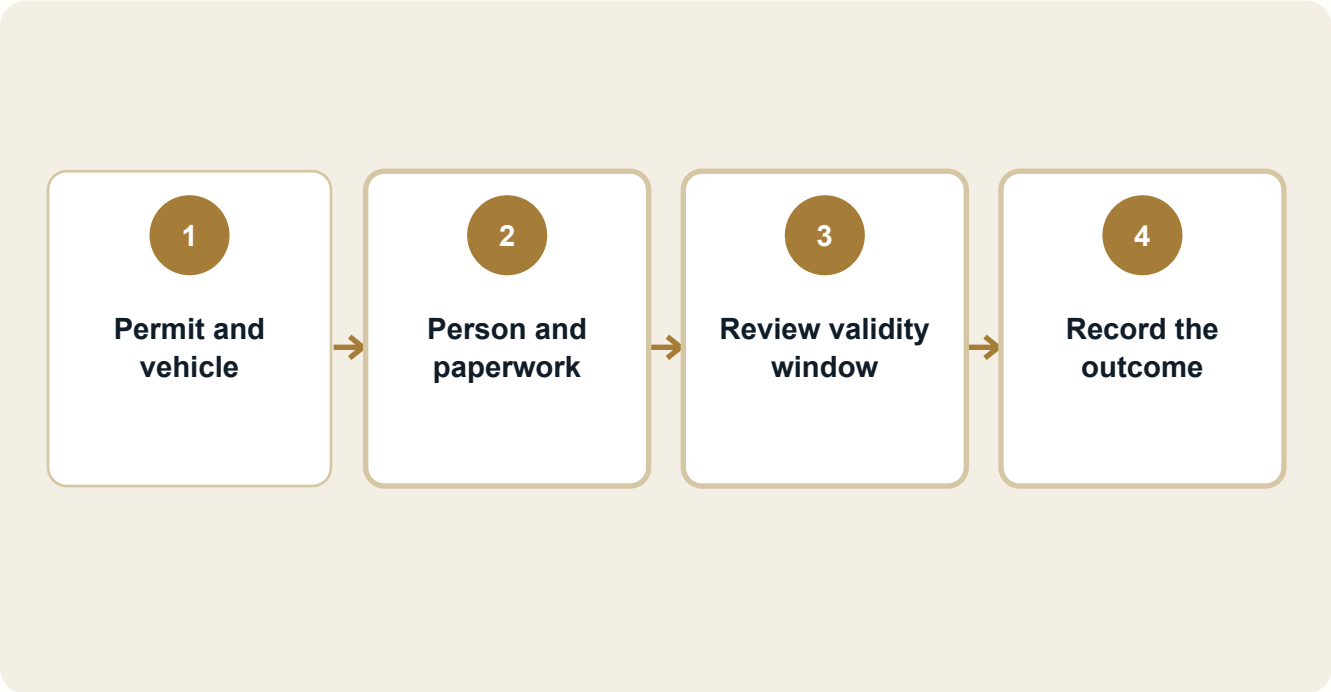
- Use a dedicated scoped integration key.
- Map only the approved door or lift floor.
- Deny on stale, failed or ambiguous responses.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Collection review and auditing

Collection permits link plates, dispatch references and a bounded validity window for supervisor review.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Operating approach

A matching permit informs review without proving the truck, driver or load is correct. Access history records permission checks rather than independently confirmed physical entry.

## What the team reviews

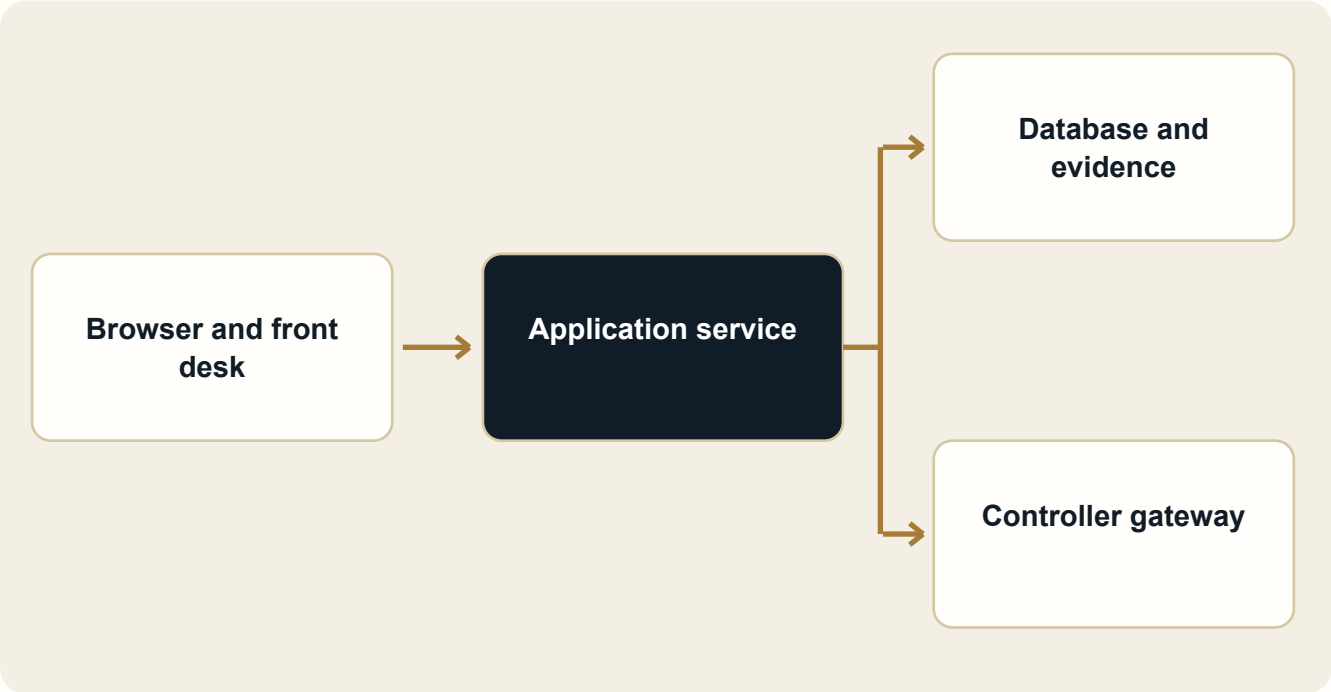
- Verify vehicle, driver and paperwork.
- Separate manager and guard responsibilities.
- Use controller telemetry for physical confirmation.

## Acceptance evidence

Demonstrate this workflow using representative permitted inputs. Record the expected result, actual result, responsible reviewer and any remaining conditions before production approval.

# Architecture and information flow

Components and responsibilities for this product.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

### Browser and front desk

Monitoring, visitors and current-assignment management.

### Application service

Card, booking, area, clearance, point and floor decisions.

### Database and evidence

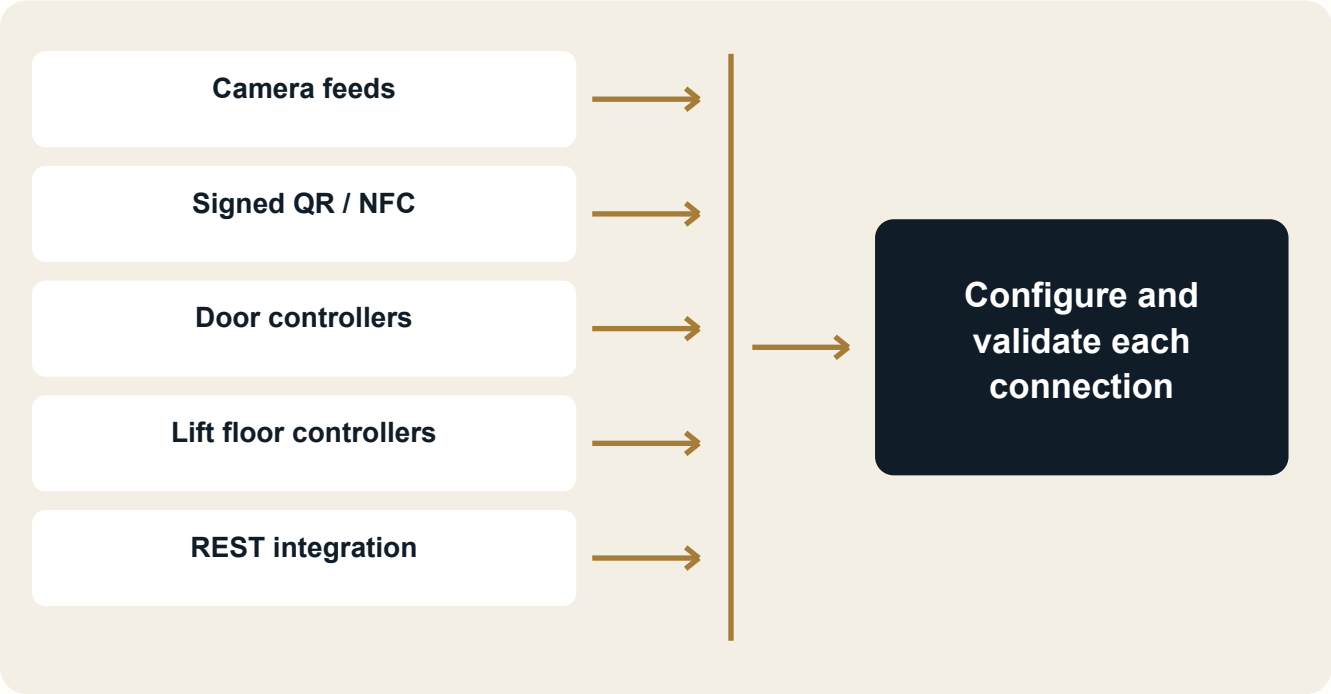
MongoDB and protected configured evidence storage.

### Controller gateway

Single-use decisions and an administrator-mapped vendor driver.

# Integrations and commissioning

Each connection requires authorised configuration.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Camera feeds

Supported configured camera source or ingestion connection. Validate image quality, source identity and monitoring rules.

## Signed QR / NFC

Installation-issued signed text and a compatible reader. A bare UID or generic card serial is not an authenticated application credential.

## Door controllers

Manufacturer API, SDK or supported gateway behind the adapter. No universal driver or vendor certification is claimed.

## Lift floor controllers

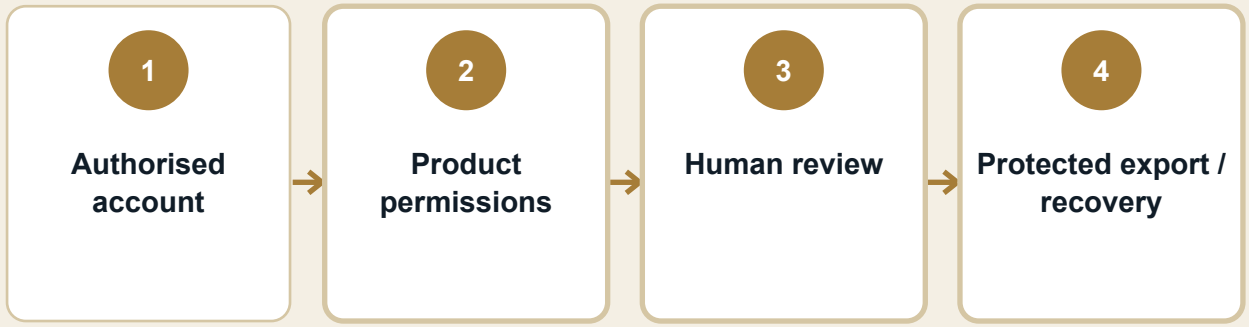
Commissioned floor-output/command integration with explicit destination mapping. Preserve emergency egress and certified safety functions.

## REST integration

Scoped X-API-Key, HTTPS and the OpenAPI contract. Successful decisions expire in five seconds and require one consumption by the same key.

# Security and access boundaries

Security depends on the product controls and the operating environment.




Permissions and review belong to this product's deployment.

Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

### Live card lifecycle

Active holder, assignment, area clearance, booking and access window checks.

### Explicit point grants

Door, lift and floor permissions in addition to the area.

### Integration credentials

Separate scoped keys with network restrictions and expiry.

### Replay control

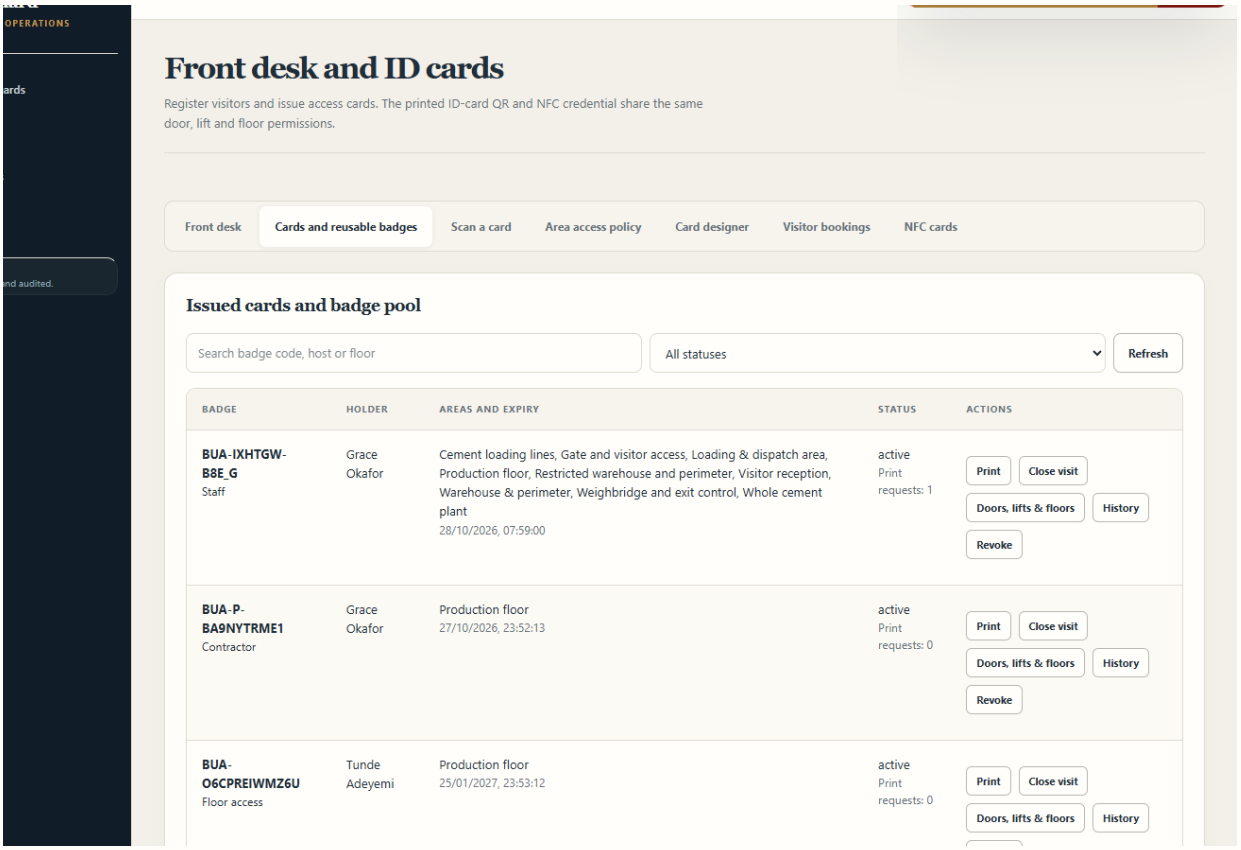
Atomic single-use consumption of a short-lived decision.

### Hardware boundary

The adapter denies new release requests on error and preserves controller emergency behavior.

# Reports and information handling

Reports should retain source context and operating limits.




Current application interface captured from the configured test system.

## Product outputs

- Source-linked camera and detection review.
- Visitor bookings, badge assignments and rollcall workflows.
- Collection-permit status and supervisor review context.
- Timestamped permission decisions with reason, separate from attendance.

## Handling responsibilities

Agree who may read, export, share and retain each output. Protect reports and media according to their sensitivity. Review the source records and filters before relying on totals or conclusions.

# Illustrative workflows 1

Examples explain use; they do not claim real customer results.



Generated illustrative scenario; not a customer deployment.

## A visitor may use reception only

A visitor has an approved appointment at reception. An ungranted destination remains blocked.

- Register/check in the visitor and assign a badge.
- Grant the reception door and its floor.
- Check the same QR/NFC credential at each requested point.

Conditions: Booking state, card validity, area clearance and point grants must all permit the request.

## A lift serves restricted floors

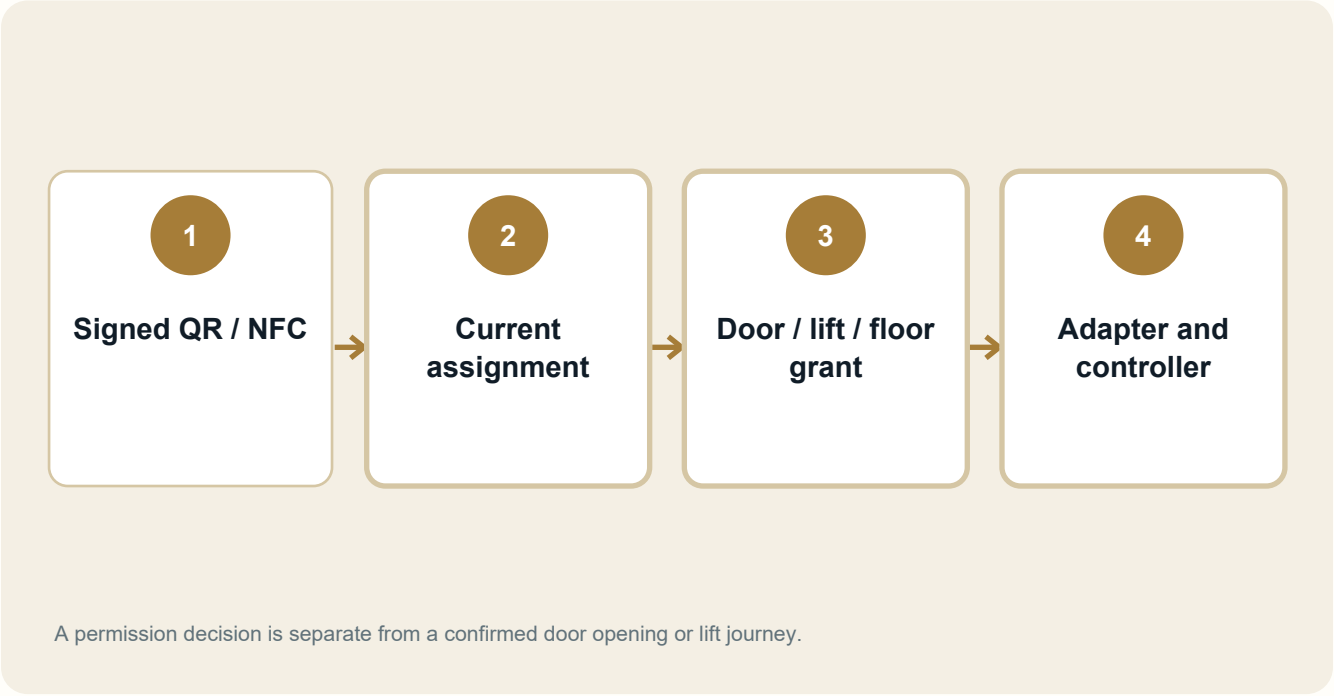
An employee needs Floor 2 but not the executive floor. Lift permission does not enable every floor.

- Grant Lift A and Floor 2.
- Send the requested destination with the signed credential.
- Consume the decision and call the mapped vendor floor command.

Conditions: A commissioned driver and correct controller mappings are required.

# Illustrative workflows 2

Examples explain use; they do not claim real customer results.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## A returned badge changes hands

The front desk reuses a physical visitor badge. The previous visitorâ€™s permissions do not carry over.

- Close the previous assignment.
- Assign the badge to the new visitor.
- Grant the new route for the new assignment.

Conditions: The desk must complete return and reassignment; readers must request live decisions.

## A truck arrives for collection

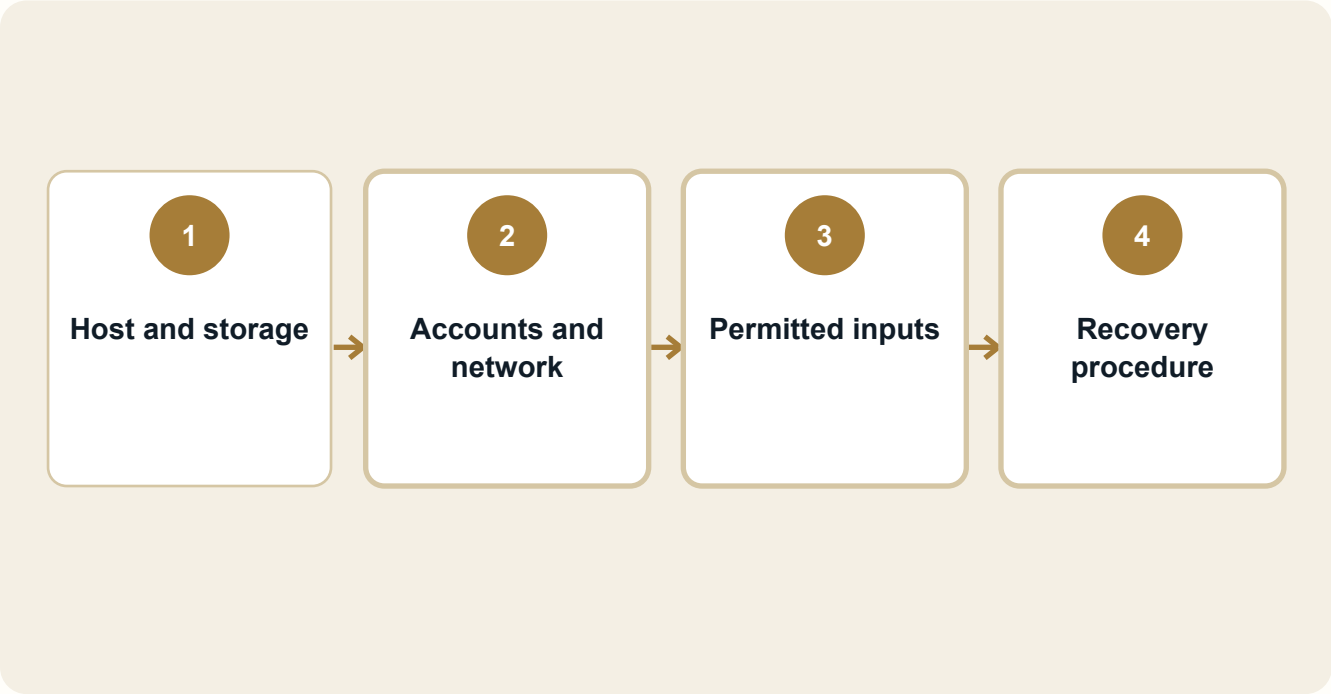
An operator reviews a vehicle at the loading area. The local permit record supports accountable review.

- Review the plate candidate and permit.
- Confirm the truck, driver and paperwork.
- Close or revoke the permit after collection.

Conditions: ERP, weighbridge and physical load checks require separate arrangements.

# Deployment prerequisites

The deployment plan must name the actual infrastructure and inputs.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Requirements

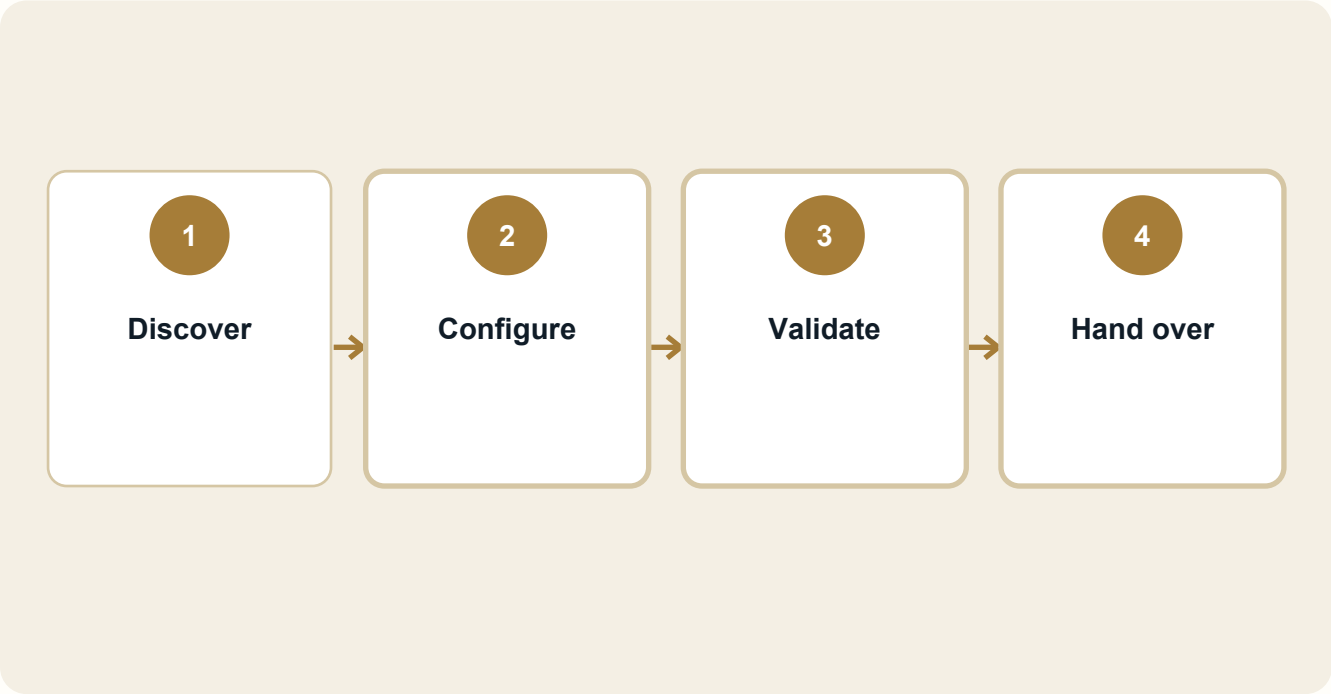
- Supported Node.js host, MongoDB and protected evidence storage.
- Trusted HTTPS and the intended browser/reader devices.
- Configured cameras and representative commissioning footage.
- Registered areas, buildings, floors, doors and lift destinations.
- Manufacturer-supported controller interfaces and commissioned drivers for physical operation.

## Capacity and dependencies

Confirm load, data size, retention, input quality, network behavior and backup needs through representative tests. The product overview does not guarantee throughput or availability.

# Pilot and implementation plan

A proposed sequence to agree with the customer.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Discovery

Confirm the intended users, workflows, source systems, integrations and acceptance criteria.

## Configuration

Prepare accounts, permissions, infrastructure and the required inputs. Keep any external adapters within the agreed scope.

## Pilot

Exercise normal and failure cases with representative authorised data. Record defects and unresolved dependencies.

## Handover

Train the responsible staff, review acceptance evidence and agree the support, maintenance and recovery process.

# Acceptance and validation

Production approval requires evidence from the intended deployment.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Acceptance checks

- Area permission alone does not permit door or lift access.
- A door also requires its enabled floor.
- A lift rejects ungranted or unserved floors.
- Expired, revoked, returned and reassigned badges cannot reuse old permissions.
- Wrong-key, stale and repeated decision consumption fails.
- The controller does not operate after a denied or ambiguous response.
- ID-card QR and NFC produce the same current-assignment outcome.

## Sign-off record

For each check retain the owner, date, test inputs, expected result and observed result. Resolve critical failures before treating the workflow as commissioned.

# Training and handover

Training should follow the roles that will use the installed product.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Administration

Accounts, permissions, source/device configuration and ongoing access reviews.

## Daily operation

The product workflow, source review, exception handling and escalation.

## Technical handover

Integration responsibilities, protected credentials, backup/restore and host monitoring.

## Completion evidence

Record attendance, operating procedures, responsible contacts and any remaining configuration requirements.

# Operations and support

Maintain the installation and the human review process.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Operational checklist

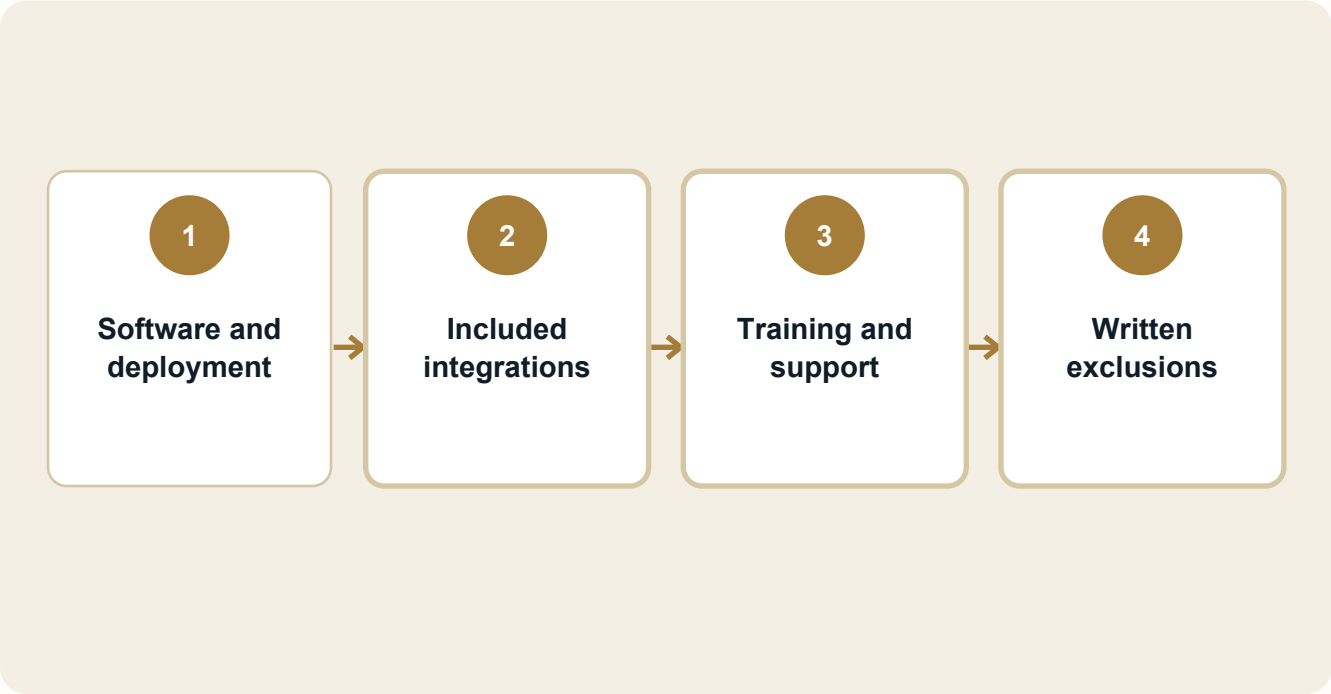
- Review card grants, point mappings and visitor checkout.
- Monitor camera health, alert delivery and storage.
- Rotate keys and test network/device restrictions.
- Exercise controller failures, emergency procedures and recovery with the responsible specialists.

## Support agreement

Agree working hours, response targets, escalation contacts, defect/change handling, update responsibilities and any on-site requirements in the commercial agreement. No service-level guarantee is made here.

# Commercial scope

A product-specific written quotation defines the offer.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Software and deployment

State the product, permitted deployment, user/usage scope and installation responsibilities.

## Integration and hardware

List each included source, device, adapter, third-party licence and specialist service. Identify customer-provided hardware and excluded work.

## Training and support

Specify training sessions, handover deliverables, support coverage and renewal arrangements.

## Costs and changes

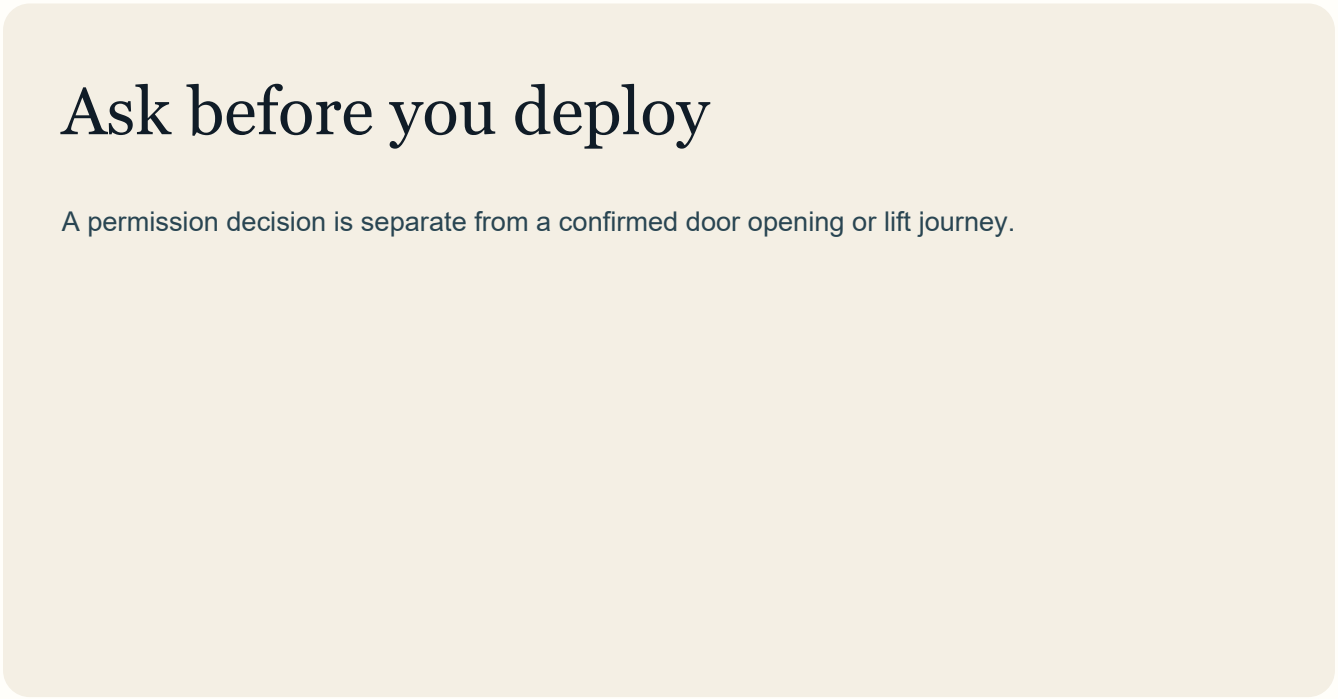
Confirm currency, taxes, payment milestones, travel and infrastructure costs in the quotation. New requirements need written change approval.

# Questions and scope boundaries

The product remains separate from the other portfolio applications.

## Ask before you deploy

A permission decision is separate from a confirmed door opening or lift journey.



Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

### Can one ID card work at doors and lifts?

Yes, with explicit permissions for its current assignment. QR and NFC share those permissions.

### Does every controller work automatically?

No. A manufacturer-supported API, SDK or gateway and commissioning are required.

### Can a raw NFC UID open a door?

The built-in flow uses signed QR/NDEF text. Other secure-card protocols require explicit integration.

### Does a successful check unlock hardware?

A trusted adapter must consume the decision and call the configured mapped driver.

### Does decision history prove attendance?

No. Physical confirmation needs controller contacts or other authorised telemetry.

### Are permits an ERP integration?

The permit register supports supervisor review. ERP, weighbridge and load validation require separate work.

# Next steps and proposal review

A focused discussion before implementation.




Workflow illustration · A permission decision is separate from a confirmed door opening or lift journey.

## Demonstration

Review Sentinel SiteGuard using your intended workflow and representative authorised inputs.

## Scope workshop

Agree the users, infrastructure, sources, integrations and operating responsibilities.

## Written proposal

Confirm deliverables, acceptance evidence, exclusions, training and commercial terms.

## Source basis

Product descriptions reflect the local Sentinel SiteGuard application README and relevant implementation documentation reviewed on 31 October 2026. Optional services and model/hardware performance require validation.

## Enquiries

Use the website support form and select Sentinel SiteGuard for a demonstration or quotation.