

VECTRO **APRON**

Product Detail and Setup Guide

A practical reference for edge deployment, camera commissioning, operations, security, and integration.

EDGE OPERATIONS EDITION | VERSION 1.0 | AUGUST 2026

Designed for airport operations, safety, IT, and field deployment teams.

Contents

Contents 2

Product Detail and Deployment Guide 3

1. Product Overview 3

2. Reference Architecture 3

3. Standard Gate Sensor Pack 4

4. Hardware and Network Requirements 5

5. Installation Procedure 6

6. Acceptance Test..... 7

7. Operating Model..... 7

8. Integration Contract 8

9. Product Path 8

10. Support and Change Control 8

Product Detail and Deployment Guide

Edge computer vision for aircraft turnaround intelligence, safety evidence, and operational learning.

Version 1.0 | August 2026

1. Product Overview

Vectro Apron is an edge-first apron intelligence platform that joins live camera operations, aircraft turnaround timelines, safety and operational alerts, governed detection review, registration verification, and retained video evidence in one role-aware application.

The platform is designed around a simple operating principle: operational systems provide schedule and allocation truth, cameras provide observable evidence, and Vectro connects both to a common flight and gate timeline without allowing uncertain AI output to become an unreviewed fact.

Available Today

- Multi-gate live view and filtered camera matrix.
- Gate-specific Front, Port, Starboard, and optional camera lanes.
- Live and retained flight context through a configurable AODB adapter.
- Per-flight turnaround Gantt with clickable event evidence.
- Protected SSD video playback with camera switching and event-offset seeking.
- Local RF-DETR object detection and tail-registration OCR.
- Safety and operational alert centres with acknowledgement, resolution, suppression, notes, and audit history.
- Detection review, correction, rejection, training-data workflow, class registry, and model inventory.
- Turnaround profiles and alert rules configurable by airline, aircraft type, gate, milestone, severity, and recipient route.
- Role-based access, MFA, account lockout, and administrator-controlled accounts.
- Offline local operation for cameras, detections, evidence, alerts, and retained history.

Commissioned Expansion Paths

- Additional gate, stand, jetbridge, ramp, or vehicle-lane cameras.
- Custom detection classes and camera-specific models.
- Network microphone and acoustic-event analytics.
- RMS, Vectro Allocate, airline/handler, and third-party operational connectors.
- Approved email, SMS, or webhook notification relays.
- Cross-site reporting and centralized fleet management.

2. Reference Architecture

SENSE	PROCESS	OPERATE	CONNECT
Three-camera gate pack Optional jetbridge + audio	Edge video, RF-DETR, OCR Tracking + retained evidence	Live views, Gantt, alerts Review + analytics	AODB, RMS, Allocate Approved APIs + webhooks

No inbound internet connection is required for normal edge operation. Cloud services are optional and must be approved by airport IT.

3. Standard Gate Sensor Pack

Front Camera

Primary coverage: lead-in line, aircraft arrival/departure, stand occupancy, pushback, personnel, cones, and GSE approach paths.

Placement priorities:

- Keep the complete stand and aircraft envelope visible.
- Avoid direct terminal reflections and persistent sky dominance.
- Preserve enough pixel density for people, cones, tugs, and vehicle classification.
- Keep the expected tail region visible when registration OCR is a requirement.

Port Camera

Primary coverage: aircraft service side, cargo/service doors, belt loaders, baggage carts, fueling equipment, personnel, and safety zones.

Placement priorities:

- Avoid placing the aircraft fuselage between the camera and required milestones.
- Include equipment staging and approach paths.
- Keep door and loader interfaces large enough for state classification.

Starboard Camera

Primary coverage: opposite aircraft service side, GPU/PCA, towbar, tug, pushback, and blind-spot completion.

Placement priorities:

- Complement rather than duplicate the Port view.
- Include the equipment position zones needed by turnaround profiles.
- Keep critical areas visible throughout expected aircraft types.

Optional Jetbridge Camera

Use a fourth fixed camera when the bridge head, cab, attachment point, or passenger-door interface cannot be reliably observed from the standard pack. Assign it a dedicated Jetbridge angle and validate extended, attached, and retracted positions.

Optional Acoustic Sensor

Use an approved ONVIF/RTSP audio source, network microphone, or audio-capable camera only after privacy and retention approval. Acoustic analytics can complement vision for alarms, impacts, engine states, and abnormal equipment noise, but requires a site-trained baseline and independent acceptance.

4. Hardware and Network Requirements

Edge Appliance

- NVIDIA Jetson-class device sized for the commissioned camera count and inference rate.
- SSD for operating system and application.
- External high-endurance evidence drive sized for retention requirements.
- Reliable power and approved shutdown procedure; UPS recommended.
- One management interface and one camera-network interface where network segmentation requires it.

Cameras

- ONVIF-capable fixed IP cameras recommended.
- H.264 or H.265 main stream; a lower-resolution substream may support matrix views.
- RTSP over TCP.
- Synchronized NTP.
- Fixed IP or DHCP reservation.
- Day/night imaging appropriate to apron lighting and weather.

Network Flows

Source	Destination	Port	Purpose
Approved operator network	Edge appliance	TCP 8088 or approved reverse-proxy port	Web application
Approved maintenance network	Edge appliance	TCP 22	Controlled SSH maintenance
Edge appliance	Cameras	TCP 554	RTSP media
Edge appliance	Cameras	TCP 80/443	Camera administration, snapshot, or ONVIF as required
Edge appliance	DNS	UDP/TCP 53	Name resolution where operational feeds use hostnames
Edge appliance	NTP	UDP 123	Time synchronization
Edge appliance	Operational feeds	TCP 443	Arrivals, departures, allocation, or approved APIs
Edge appliance	Approved relay	Site-defined	Optional notifications/webhooks

Default-deny firewall policy is recommended. The local model service and database are not published to the camera or operator networks.

5. Installation Procedure

Stage A: Bench Preparation

1. Apply the approved appliance image and deployment bundle.
2. Install model weights, OCR assets, media gateway, and application containers.
3. Configure the external evidence-drive mount by stable filesystem identifier.
4. Set secure operator, database, session, and ingestion secrets.
5. Disable self-registration and create the initial administrator through the controlled provisioning process.
6. Verify unattended startup, container health, storage health, and local web access.
7. Create and test the spare-appliance restore bundle.

Stage B: Network Commissioning

8. Record edge-appliance and camera MAC addresses.
9. Place cameras on the approved isolated network.
10. Apply fixed addresses or DHCP reservations.
11. Configure DNS, NTP, routing, and firewall flows.
12. Confirm operator access is limited to approved networks.
13. Confirm other servers on the same infrastructure cannot access the application unless explicitly authorized.

Stage C: Camera Commissioning

For each gate:

14. Mount and aim Front, Port, and Starboard cameras.
15. Add optional Jetbridge or acoustic sensors where required.
16. Set codec, resolution, frame rate, keyframe interval, exposure, and night profile.
17. Enter each RTSP endpoint in **Camera Setup** and assign gate and angle.
18. Verify Online state, snapshot, live playback, and reboot recovery.
19. Lock the camera position and document the final field of view.
20. Create regions of interest and exclusions for each required class/milestone.

Do not embed default camera credentials in production documentation or deployment bundles. Store secrets in the protected configuration system.

Stage D: Operational Data

21. Configure arrivals and departures endpoints or the approved integration adapter.
22. Map gate, airline, flight number, scheduled/estimated/actual times, aircraft type, and registration.
23. Replay a representative day into the staging environment.
24. Confirm source precedence, idempotency, timezone, and stale-data behavior.
25. Validate retained operation when the live feed is unavailable.

Stage E: Profiles, Detection, and Alerts

26. Create turnaround profiles by airline, aircraft type, and gate where operational standards differ.
27. Preview profile resolution.
28. Validate object classes per camera in day/night and representative weather.
29. Tune confidence, duration, tracking, and region thresholds.
30. Enable advisory operational alerts first.
31. Enable safety alerts only after signed onsite acceptance.

32. Configure recipient policies and approved delivery routes.

6. Acceptance Test

Platform

- Appliance restarts unattended and services recover.
- Web, API, database, media gateway, and model services are healthy.
- MFA, role restrictions, account lockout, and audit logging work.
- Evidence drive survives restart and reports healthy capacity.

Camera

- Every stream remains stable for the agreed soak period.
- Live view, camera matrix, snapshot, and protected recording playback work.
- Camera timestamps match the appliance clock.
- Day/night and difficult-lighting samples are usable.

Flight and Gantt

- Flight/gate mapping agrees with the operational source.
- A selected flight creates the correct turnaround timeline.
- Selecting an event opens the correct video and event offset.
- All overlapping camera angles are available.

Detection and Registration

- Required classes meet the agreed camera-specific quality threshold.
- Review approve/correct/reject actions persist and update analytics appropriately.
- Registration Match, Mismatch, Observed, Unreadable, and No Expected Registration behave safely.
- No unreviewed class creates a safety alert.

Resilience

- Camera loss, feed loss, internet loss, full-disk warning, model failure, and service restart are tested.
- Retained history remains available during an upstream outage.
- A checksummed USB patch and spare-appliance restoration are demonstrated.

7. Operating Model

Daily

- Confirm camera, edge, operational-feed, and storage health.
- Review new critical/high alerts.
- Check failed recordings and stale cameras.
- Review a sample of pending detections.

Weekly

- Review false alerts, missed events, and class confusion.
- Check evidence-drive health and retention.
- Confirm backup completion.

- Review camera movement or image degradation.

Monthly

- Review accounts and role assignments.
- Review model and profile performance by airline, aircraft type, gate, and lighting condition.
- Test a restore or spare-appliance synchronization.
- Approve, defer, or retire candidate classes.

8. Integration Contract

The integration layer uses a normalized flight/gate contract:

- Stable movement identifier.
- Arrival/departure flight numbers.
- Gate/stand.
- Airline and aircraft type.
- Scheduled, estimated, and actual milestones.
- Registration where available.
- Source and source-updated timestamp.

Connectors must be idempotent, observable, replayable, and explicit about source precedence. RMS or Vectro Allocate integrations are activated only after credentials, field mapping, security review, and acceptance testing.

9. Product Path

33. **Observe:** stable live and retained gate evidence.
34. **Understand:** accepted object classes, zones, tracking, and registration OCR.
35. **Time:** per-flight milestones, profiles, and event-linked Gantt.
36. **Act:** governed alerts, acknowledgement, evidence, and notification routes.
37. **Optimize:** comparative turnaround analytics and model improvement.
38. **Orchestrate:** RMS, allocation, command-centre, and multi-site integrations.

10. Support and Change Control

Every field change should include purpose, affected gates/cameras, configuration or model version, owner, test evidence, rollback method, and approval. Remote changes use approved maintenance networks. Offline sites use checksummed USB bundles applied through controlled SSH maintenance.