AI Video Analytics

User Guide

Configuring analytics, working with alarms and automating responses

Version 2.8.17

7 October 2026

Contents

1. About This Guide
2. Getting Started
- Signing in
- Language
- Layout

3. Cameras
4. Analytics: Common Concepts
- Adding an analysis to a camera
- Analysis status
- Drawing regions
- Classes
- Sensitivity
- Frame rate
- Schedules
- Analyses managed from a VMS

5. Analysis Types
- PPE
- Traffic
- Object Detection
- Helmetless Biker
- Fire & Smoke
- Heatmap
- Custom models

6. Face Recognition
- Person lists
- People
- Camera configuration
- Live matches and archive search
- Face recognition settings

7. Plate Recognition (ANPR)
- Adding a camera
- Plate lists
- Licence plates
- Parking lots and sessions
- Working with plate passes

8. Alarms
- Live alarms
- Searching alarms
- Exporting

9. Dashboard
10. Analysis Scheduling
11. Event Manager
- Starting from a template
- Blocks

Run history

1. About This Guide

This guide is for operators and supervisors who use AI Video Analytics every day: adding cameras, configuring video analytics, watching and reviewing alarms, building dashboards and automating what happens when an alarm is raised.

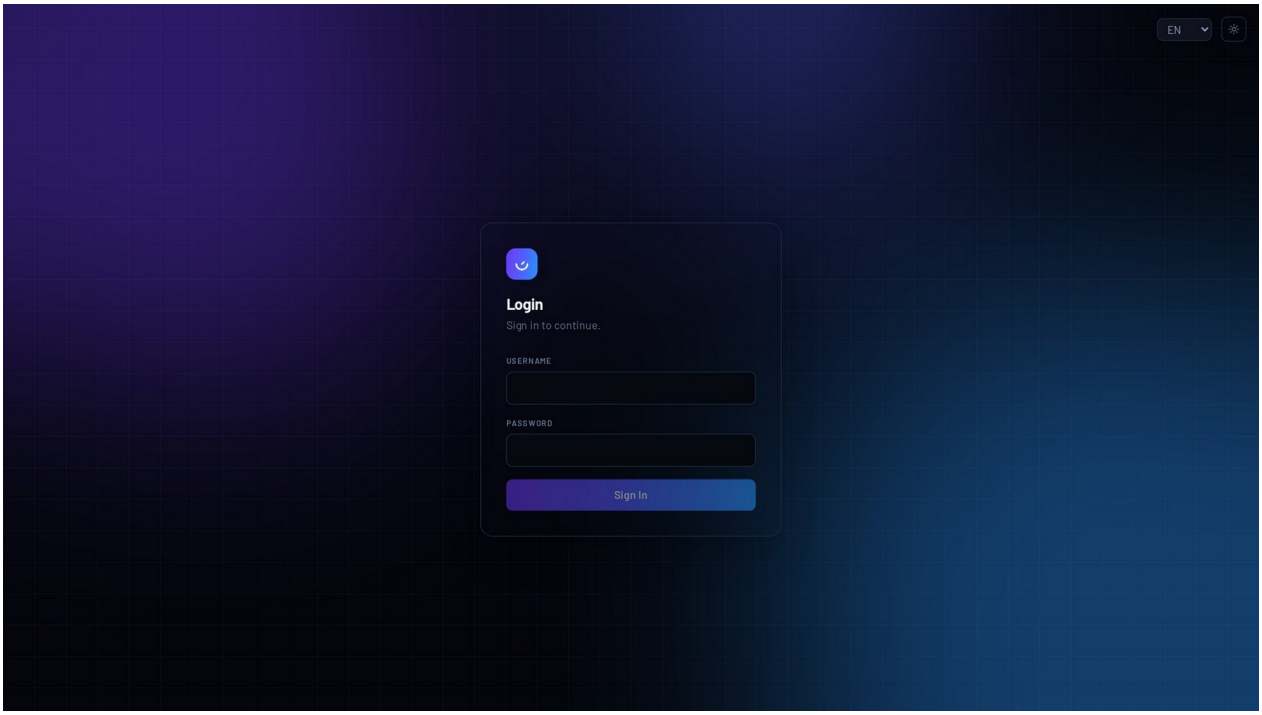
Installing and maintaining the server is covered in the **Installation and Administration Guide**. Connecting video management systems (VMS) and other external systems is covered in the **Integration Guide**.

> **Note:** What you see depends on your role. Menu items, buttons and pages you have no permission for are hidden or shown read-only. Ask your administrator if something described here is missing.

2. Getting Started

Signing in

Open the web console address given by your administrator and sign in with your user name and password. If your organisation uses directory sign-in, use your corporate account.



The sign-in page

On first sign-in, or after an administrator has reset your password, you are asked to choose a new password before anything else. The screen lists the password rules in force.

Language

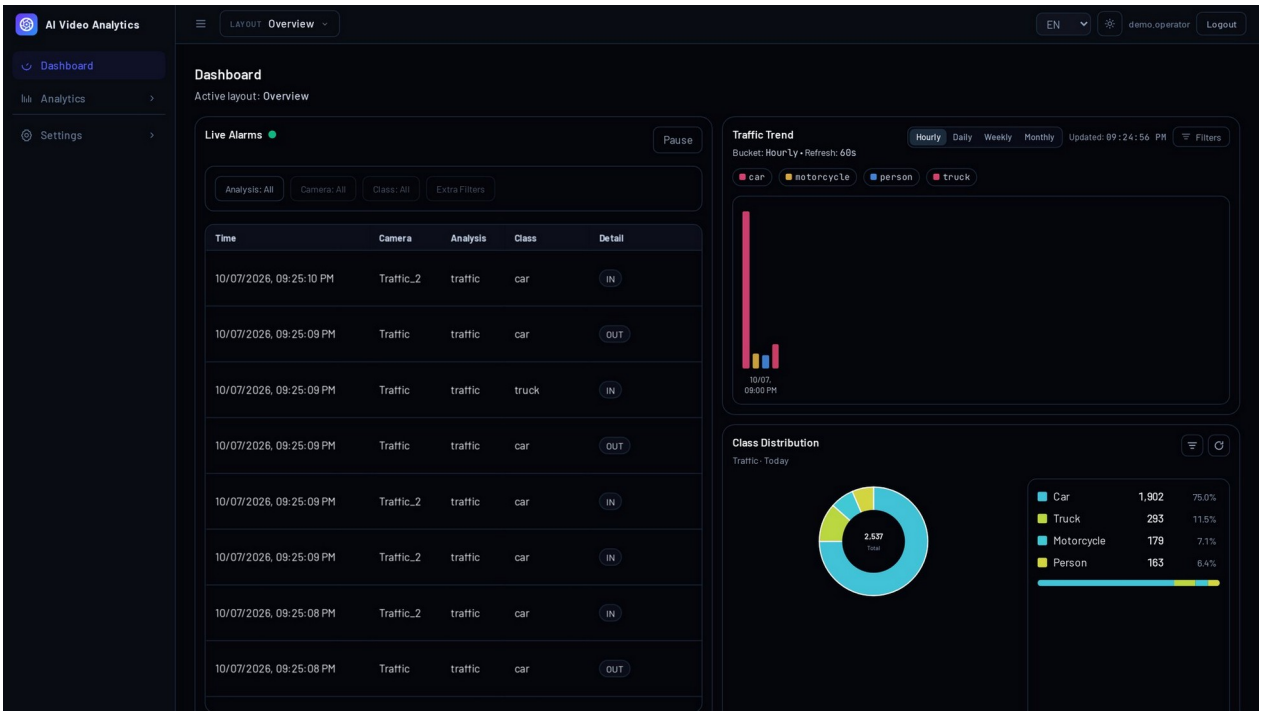
Use the language menu at the top of the screen to switch between English, Turkish, Spanish, Arabic and Traditional Chinese. Arabic uses a right-to-left layout.

Layout

- **Dashboard** — your own arrangement of live alarm lists, charts and camera views.
- **Analytics** — one page per analysis type, plus Face Recognition.

- **Settings** — cameras, schedules, automation flows, integrations and system settings.

An analysis type appears in the Analytics menu only after its AI engine has been activated by an administrator.



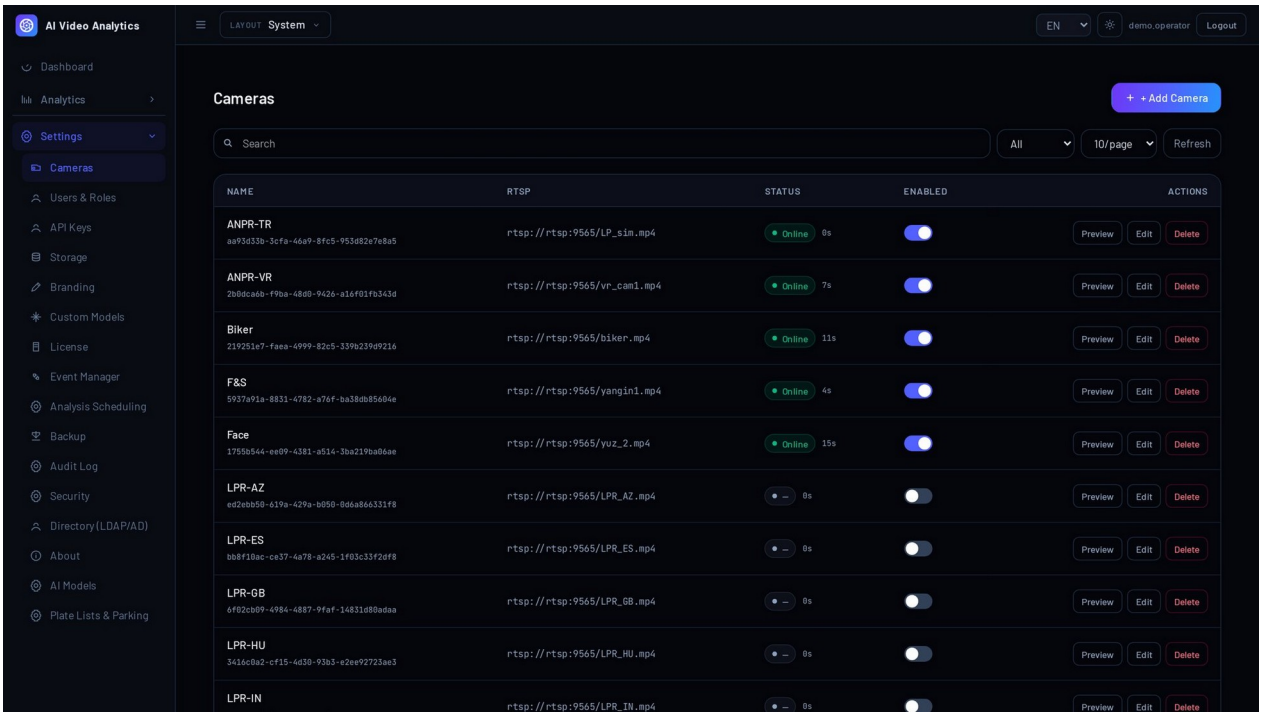
A dashboard with the live alarm panel, a traffic trend and a class distribution

3. Cameras

Settings → **Cameras** lists the video sources. To add a camera:

1. Select **+ Add Camera**.
2. Enter a **Camera Name** that operators will recognise.
3. Enter the **RTSP URL** of the camera stream, including user name and password if the camera requires them, for example `rtsp://user:password@192.0.2.10:554/stream1`.
4. Leave **Enabled** switched on and save.

Camera passwords are stored encrypted and are never shown again in the console or written to logs.



Settings → Cameras

A camera keeps receiving video as long as it is enabled, independently of which analyses run on it. One camera can run several analysis types at the same time.

> **Tip:** Use the camera's main stream only if you need the detail. A sub-stream at 1080p or below is usually enough for analytics and reduces server load.

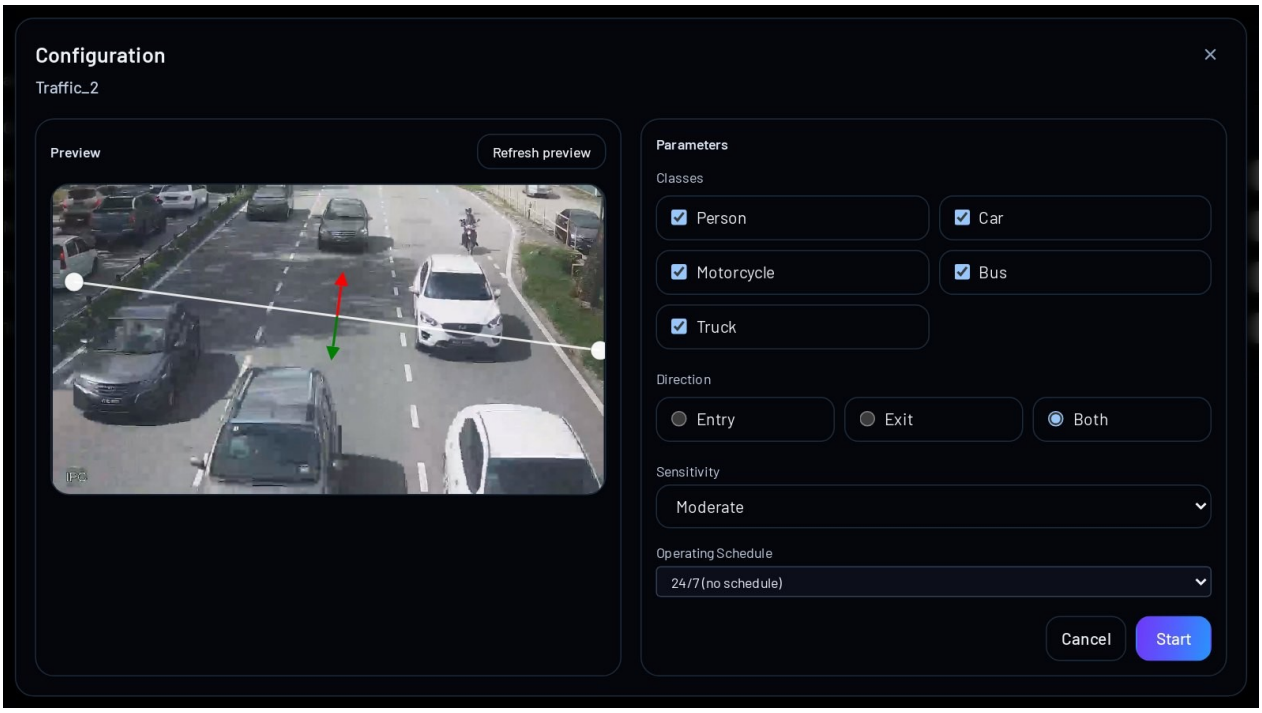
4. Analytics: Common Concepts

All analysis types are configured the same way.

Adding an analysis to a camera

1. Open the analysis page from the **Analytics** menu.
2. Select **+ Add new analysis** and choose a camera. Only cameras that do not yet have this analysis are offered.
3. Draw the region(s), choose the classes and sensitivity, and save.
4. Select **Start**.

The page lists every camera that has this analysis, with its state. **Stop** pauses the analysis; its configuration is kept.



Configuring a traffic analysis: the counting line on the camera picture, classes, direction, sensitivity and schedule

Analysis status

Each camera on an analysis page shows whether the analysis is **Active** (running) or only **Saved** (configured but stopped).

If an analysis is switched on but the analysis server could not start it, the camera shows a **Not running** badge with the reason — for example that the GPU is fully used by other analyses. Such an analysis is retried automatically every two minutes and starts by itself as soon as capacity frees up; you do not need to press **Start** again. A system notification is also shown. Stop another analysis or add GPU capacity if it does not start.

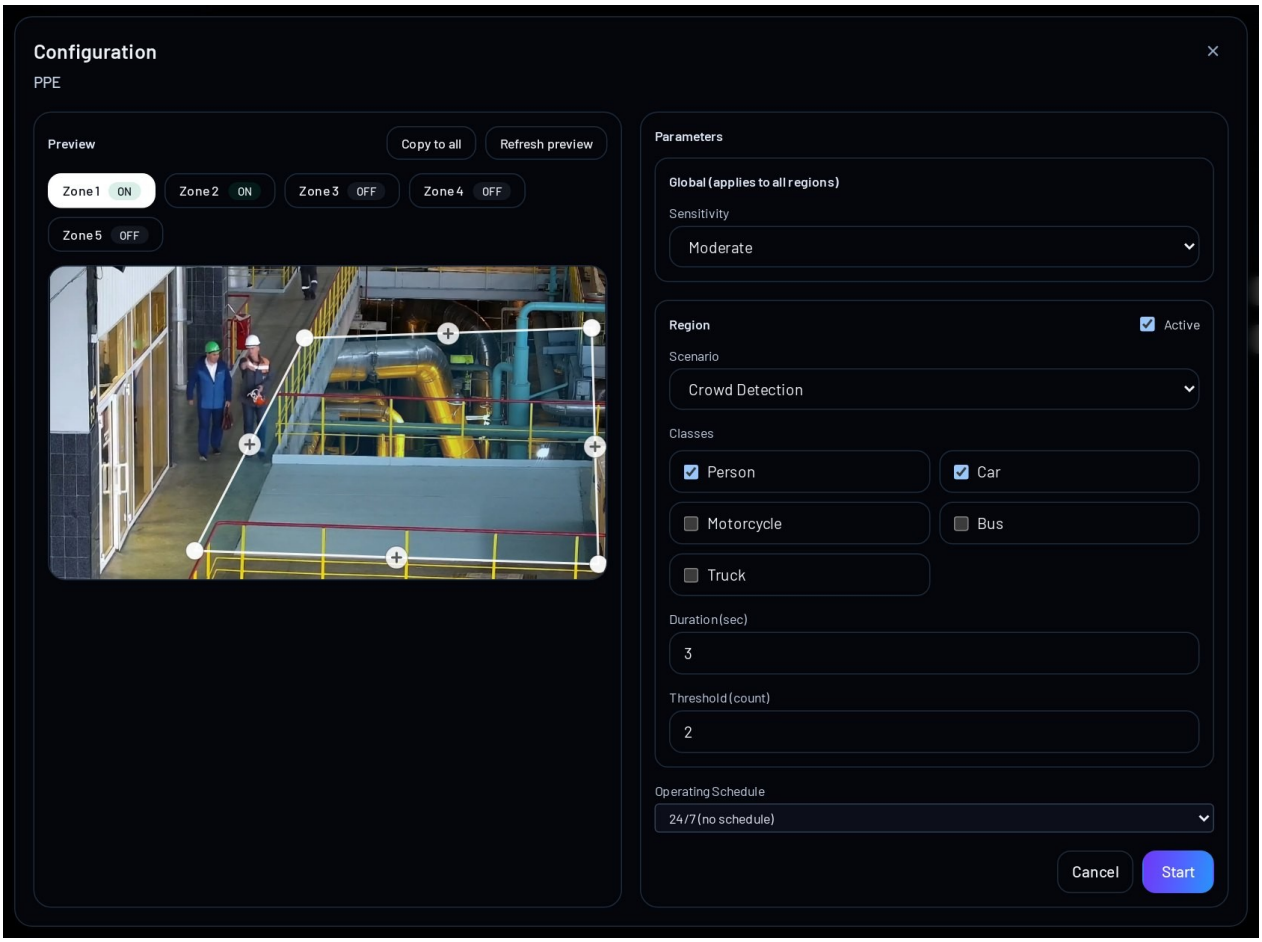
Drawing regions

Regions limit the analysis to the part of the picture that matters. The camera's current picture is shown as the background.

- Drag a corner point to move it.
- Select the **+** on an edge to add a point.
- Right-click a point to remove it (a region needs at least three points).

For analyses that count or detect direction, you draw a **line** instead; the arrows show the direction that is counted.

Regions are stored relative to the picture size, so they stay correct if the camera's resolution changes.



Object Detection: several regions per camera, each with its own scenario, classes, duration and threshold

Classes

Choose which object classes the analysis should react to. Only the classes that make sense for the analysis type are offered.

Sensitivity

Each analysis has five sensitivity levels. The level sets how certain the AI model must be about a detection before it counts:

Level	Required certainty	Effect
Maximum	80 %	Fewest false alarms; borderline detections are ignored
High	70 %	
Good	60 %	
Moderate	50 %	Default
Low	40 %	Reacts to less certain detections; more false alarms

Start with the default and adjust per camera: raise the level if you get false alarms, lower it if real events are missed.

Frame rate

The number of frames analysed per second is fixed per analysis type for predictable server load: one frame per second for fire and smoke, eight for face recognition, and up to fifteen for the others.

Schedules

An analysis can run only at certain times of the week. Choose a schedule on the analysis page; schedules themselves are created under **Settings → Analysis Scheduling** (see **Analysis Scheduling**). Pressing **Start** or **Stop** by hand overrides the schedule for the rest of that day.

Analyses managed from a VMS

If your administrator has handed an analysis type over to the VMS (see the **Integration Guide**), its pages are locked for cameras linked to that VMS. The page says so and names where the settings are changed.

5. Analysis Types

PPE

Detects people inside the drawn region and checks for a helmet and a high-visibility vest. Select which violations raise an alarm — **no helmet**, **no vest** or both. A person who has already caused an alarm does not cause another one for a short time.

Traffic

Counts and reports vehicles and people crossing a line in a chosen direction. Draw the line across the lane and set its direction with the arrows. Use it to detect wrong-way movement or to count flows.

Object Detection

Up to five regions per camera, each with its own **scenario**:

Scenario	Raises an alarm when
Entry Detection	An object of a selected class appears in the region
Empty Region Detection	The region stays empty of the selected class for the set time
Outside Region Detection	An object of the selected class is outside the region for the set time
Crowd Detection	The number of objects in the region exceeds the threshold
Occupancy Tracking	Records how long the region is occupied and vacant (for dashboards)
Abandoned Object	A bag, suitcase or backpack stays in the region for the set time

For **Abandoned Object** the classes are fixed to handbag, suitcase and backpack.

Helmetless Biker

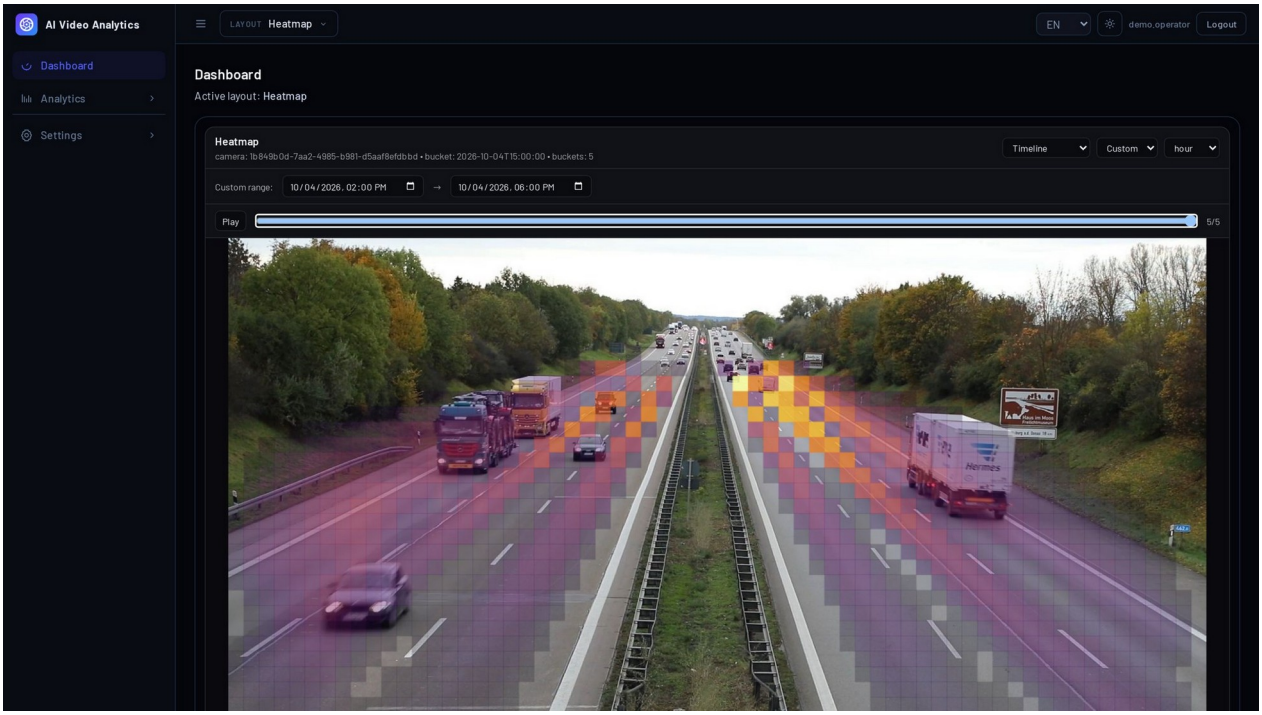
Detects two-wheeler riders without a helmet inside the region.

Fire & Smoke

Detects flames and smoke. A cool-down time prevents a continuing fire from raising a new alarm on every frame.

Heatmap

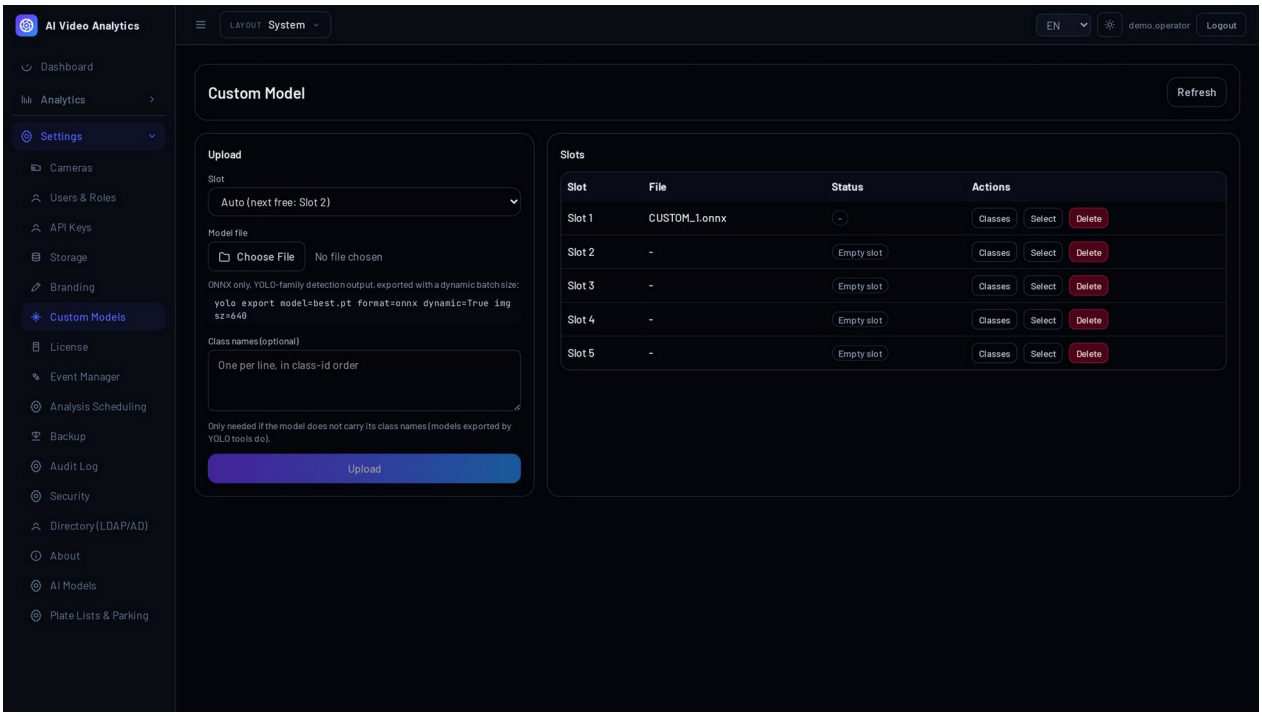
Builds an hourly heatmap of where people move in the picture. It raises no alarms; view the result on the dashboard.



The heatmap widget on the dashboard

Custom models

Your own detection models can be used in up to five custom slots. An administrator uploads the model file under **Settings** → **Custom Models**; the classes are read from the model.



Settings → Custom Models: upload form and the five slots with their status

Models are uploaded in **ONNX** format, with YOLO-family detection output. If the model does not carry its class names, enter them in the upload form. After upload the slot shows whether the model is ready or, if it was rejected, why.

Each custom analysis can run in one of two modes:

- **Detection** — alarm when a selected class appears inside a region,
- **Counting** — count objects crossing a line in the chosen direction(s).

6. Face Recognition

Face recognition matches faces seen by a camera against lists of people you maintain. It works differently from the other analyses and has its own menu.

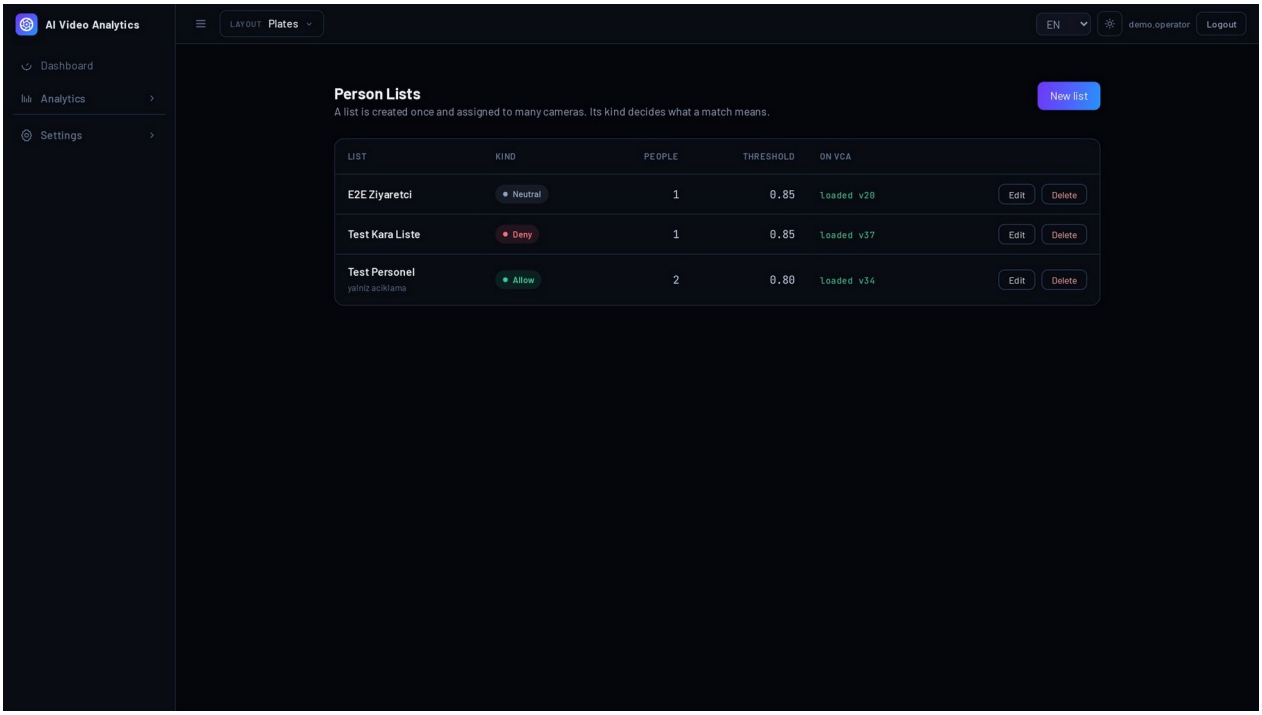
> **Important:** Face images and face descriptors are biometric data. Process them only on a lawful basis, record consent where it is required, and switch on only the functions you actually need. Every access to face images is recorded.

Person lists

Face Recognition → Person Lists. A list is created once and assigned to any number of cameras. Its **kind** decides what a match means:

Kind	A match
Deny	Raises an alarm and is sent to integrations
Allow	Writes an access record; no alarm
Neutral	Is archived only; no alarm and no access record

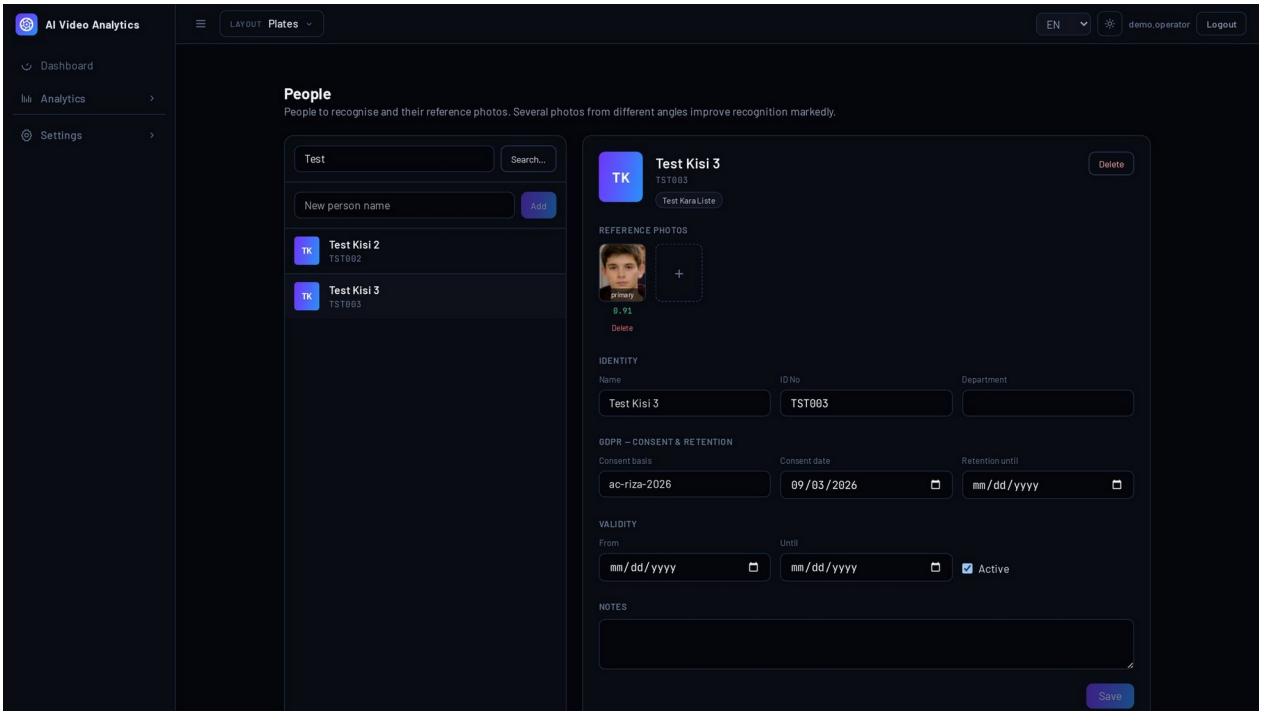
People



Face Recognition → Person Lists

Face Recognition → People. Add the people to recognise, with one or more reference photos. Several photos from different angles improve recognition markedly. Record the **consent basis** and **consent date** where your policy requires them.

The person card also holds an ID number, a department, a validity period (a person outside it is not matched) and notes. A photo whose quality is below the reference threshold is marked, because it weakens recognition.



A person card with reference photos, identity, consent and validity

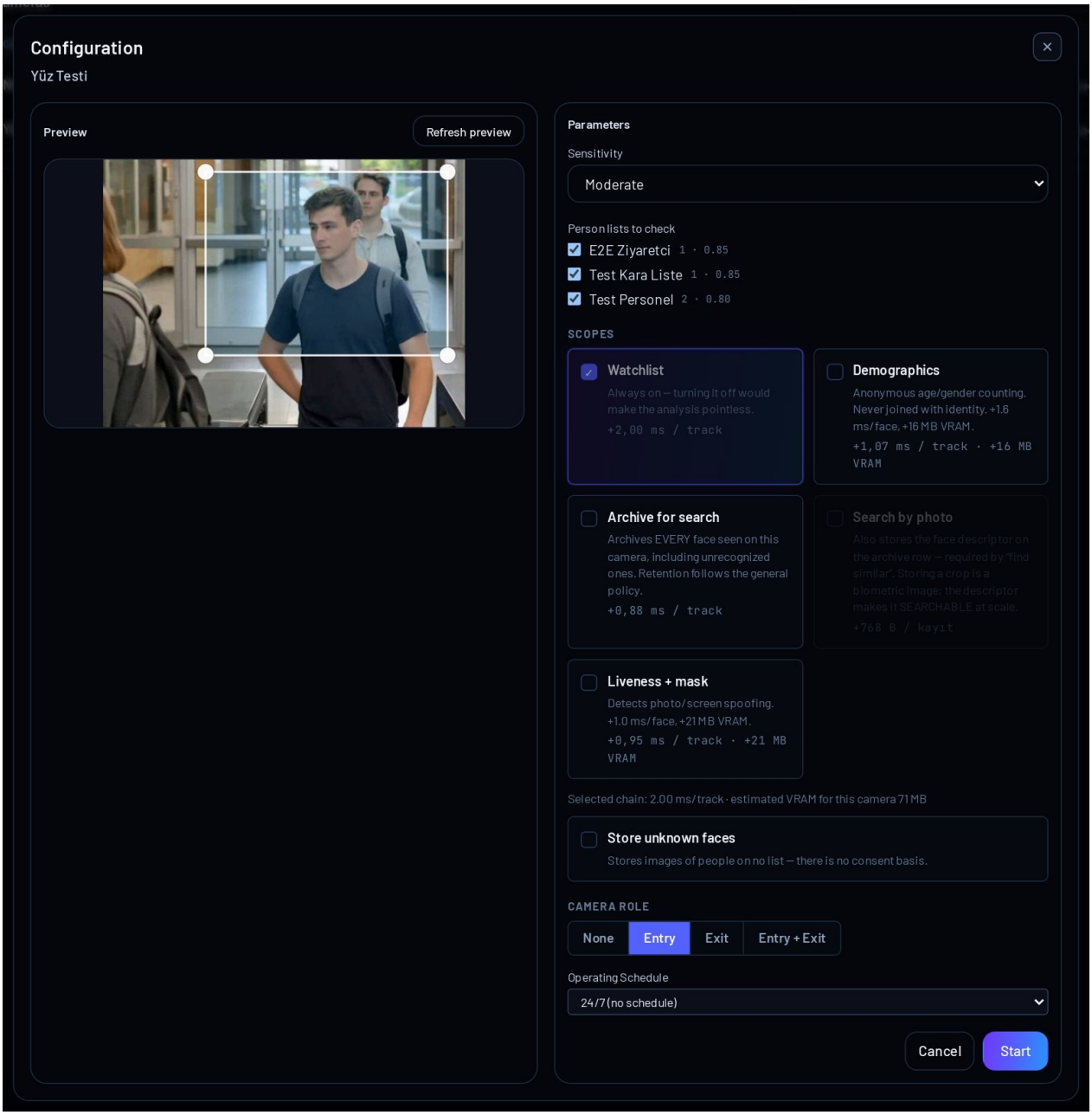
Camera configuration

On the Face Recognition analysis page, choose for each camera which lists it uses and which functions are switched on. Functions that are off do not load their AI model at all.

Function	Purpose	Default
Watchlist matching	Match against the assigned lists (always on)	On
Access log	Entry and exit records, from the camera's entry/exit role	Off
Demographics	Anonymous age and gender counting, never linked to identity	Off
Archive search	Archive every face seen, including unrecognised ones	Off
Anti-spoofing	Detect photos or screens held up to the camera	Off
Collect unknown faces	Store images of people on no list	Off
Store descriptor	Allow "find similar" searches on the archive	Off

Switch on **Archive search**, **Collect unknown faces** and **Store descriptor** only with a clear legal basis: they store biometric data of people who are not on any list, and the descriptor makes it searchable at scale.

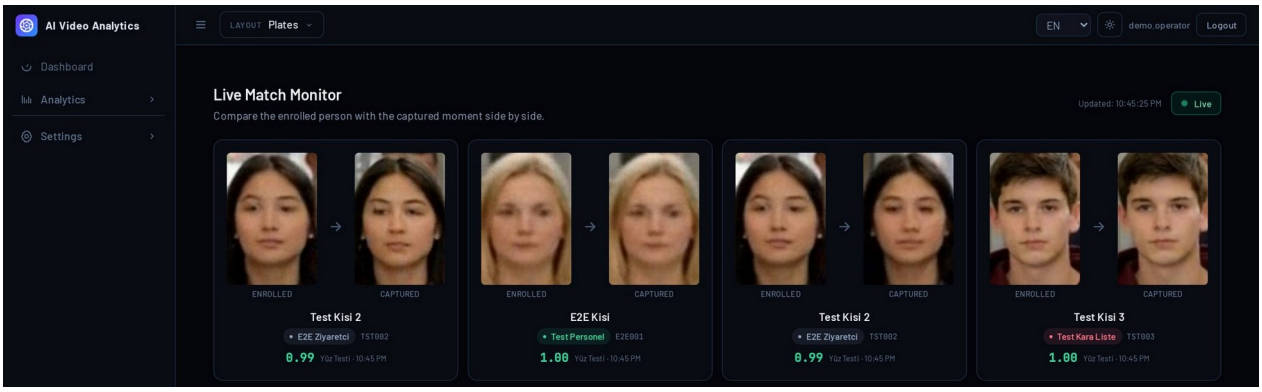
The **camera role** (entry, exit, or entry and exit) feeds the access log and the **Currently Inside** widget. The detection area limits face detection to part of the picture.



Face recognition camera settings: lists, functions, camera role and detection area

Live matches and archive search

- **Live Matches** (**Face Recognition** → **Live Matches**) opens the Live Match Monitor: it shows the enrolled photo and the captured moment side by side, with the list, the score and the camera. The same view is available as a dashboard widget.
- **Archive Search** searches archived face records by time, camera and attributes, and — if descriptors are stored — by a photo.



Live Match Monitor: enrolled photo and captured moment side by side

Seeing face images requires a separate permission. Without it, alarm thumbnails of face matches show a lock symbol.

Face recognition settings

Face Recognition → Settings holds the settings that apply to all face cameras:

- **Quality gates** — the minimum frame quality for a live match (a higher value waits for a better frame), the time after which a match is attempted anyway, and the minimum quality of reference photos.
- **Retention** — face images and records follow the general retention settings under **Settings → Storage**.
- **Audit** — list and person changes, photo views and identity exports are always recorded. This cannot be switched off.

7. Plate Recognition (ANPR)

Plate recognition reads the licence plates of passing vehicles, checks them against your plate lists and, for car parks, keeps track of which vehicles are inside. It has its own page, **Analytics → Parking (ANPR)**, and its own settings page, **Settings → Plate Lists & Parking**.

Every vehicle that passes is recorded **once**, with the plate text, a crop of the plate, a picture of the vehicle and its colour. Only a plate on an **alert list** raises an alarm; all other passes are archived and can be searched, but they do not fill the live alarm panel.

> **Note:** Licence plates are personal data in many jurisdictions. Keep alert lists to what you need and set retention under **Settings → Storage** accordingly.

Adding a camera

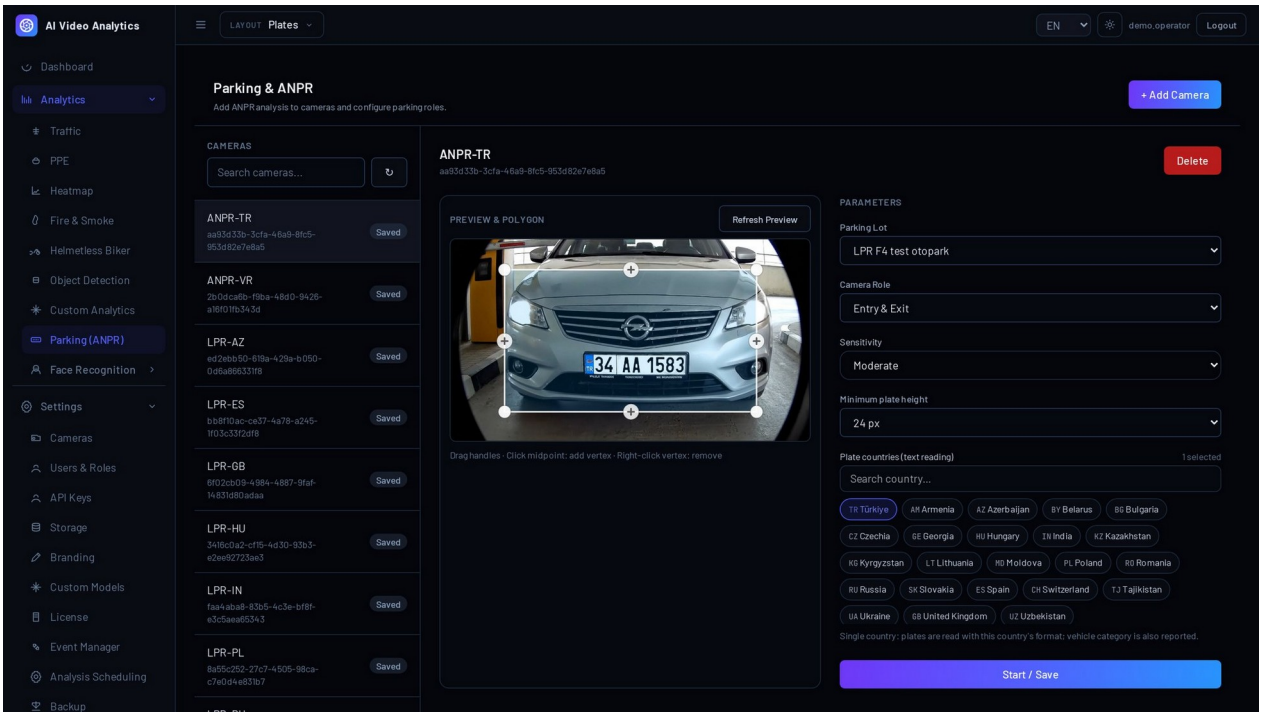
1. Open **Analytics → Parking (ANPR)** and select **+ Add Camera**.
2. Choose the camera and select **Add & Configure**.
3. Draw the region where plates should be read. Keep it tight around the lane: plates outside it are ignored.
4. Set the parameters and select **Start / Save**.

Setting	Meaning
Parking Lot	The car park this camera belongs to, or none for plain plate reading
Camera Role	**Entry**, **Exit** or **Entry & Exit** — decides whether a pass opens or closes a parking session
Sensitivity	The same five levels as other analyses

Setting	Meaning
Minimum plate height	Plates smaller than this in the picture (16, 24 or 32 pixels) are not read; raise it to ignore distant vehicles
Plate countries	The countries whose plate formats are read

With **one country** selected, plates are read in that country's format and the vehicle category is reported as well. With **several countries**, each plate's country is detected first and then read; the vehicle category is not reported. Select only the countries you expect — fewer countries mean fewer misreadings.

Supported countries: Turkey, Russia, United Kingdom, Spain, Poland, Romania, Czechia, Slovakia, Hungary, Bulgaria, Lithuania, Switzerland, Ukraine, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, Azerbaijan, Armenia, Georgia, Moldova and India.



Configuring plate recognition: region, parking lot, camera role, minimum plate height and countries

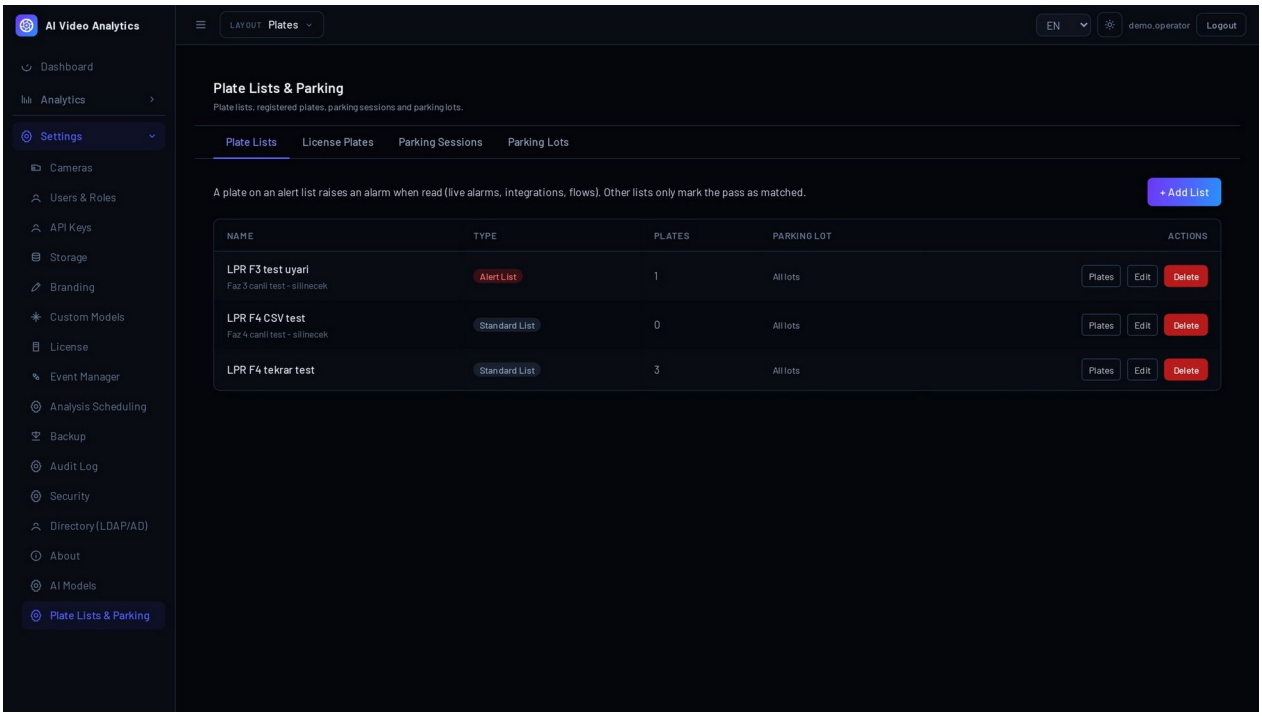
A plate whose text does not fit the selected country's format is still archived, but it is not matched against lists and does not open or close a parking session. This prevents a misread plate from raising a wrong alarm or closing someone else's session.

Plate lists

Settings → Plate Lists & Parking → Plate Lists. A list groups plates for a purpose — staff, visitors, banned vehicles.

- An **Alert List** raises an alarm whenever one of its plates is read. The alarm appears in the live alarm panel and can be sent on by Event Manager flows and webhooks.
- A **Standard List** only marks the pass as matched (for example, a known staff vehicle).
- A list can be tied to one parking lot; it then matches only on that lot's cameras.

Deleting a list also deletes the plates in it.

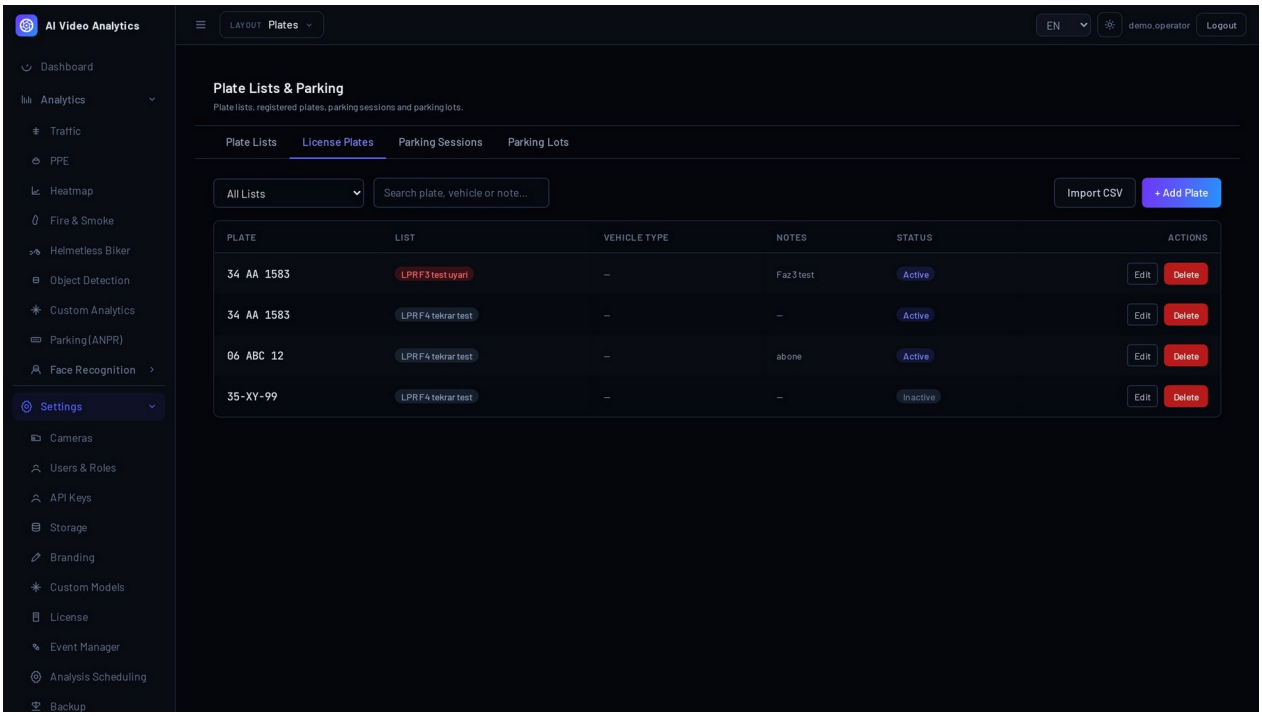


Settings → Plate Lists & Parking

Licence plates

License Plates holds the plates of every list, with vehicle type, notes and an active flag. When plates are matched, spaces and dashes are ignored and the letters O/0, I/1 and B/8 are treated as the same, so `34 ABC 123` and `34ABC123` are one plate.

Import CSV adds many plates at once. The file has the columns `plate_text` (required), `vehicle_type`, `notes` and `active`, separated by commas or semicolons; up to 20,000 rows and 2 MB. A plate already in the list is updated, not duplicated; rows that cannot be read are listed with the reason.

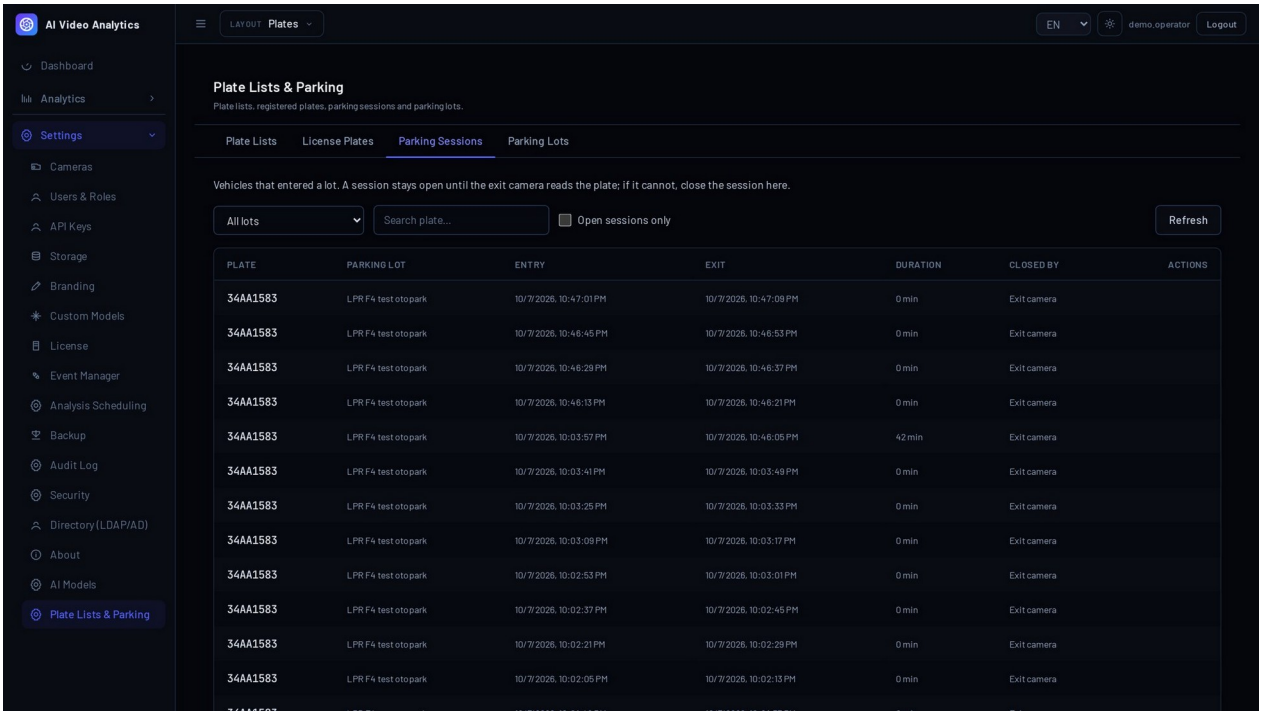


License Plates

Parking lots and sessions

Parking Lots defines each car park with its capacity. Assign entry and exit cameras to a lot on the camera's ANPR settings.

A vehicle read by an entry camera opens a **parking session**; the same plate read by an exit camera closes it and records the duration. **Parking Sessions** lists them; **Open sessions only** shows who is inside now. If an exit was missed, select **Close session** — the session is recorded as closed by an operator.



Parking Sessions

A lot that is still used by cameras or lists cannot be deleted; remove those links first.

Working with plate passes

Five dashboard widgets cover plate recognition:

Widget	Shows
Live Plate Passes	The latest vehicle large, with plate and vehicle pictures; recent passes below
Alert List Matches	Only plates on an alert list, from the last 24 hours
Plate Search	The pass history and parking sessions of one plate; part of a plate is enough
Plate Pass Statistics	Entries, exits and detections per hour, vehicles inside now and average stay
Parking Occupancy	Occupied and free spaces per lot

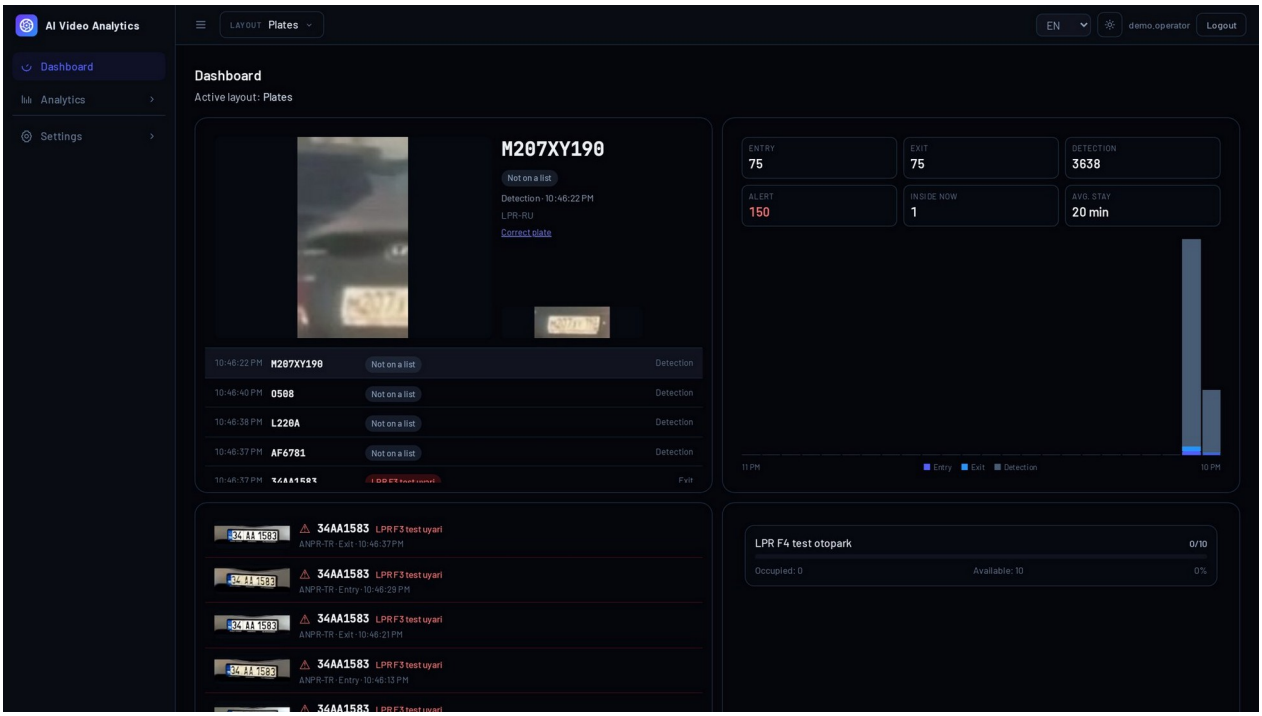


Plate recognition widgets on the dashboard

If the camera could not read a plate, or read it wrongly, select **Enter plate** or **Correct plate** on the pass. The corrected text is matched against the lists again and the original reading is kept as evidence. A correction never raises an alarm or opens a session after the fact; if the corrected plate is on an alert list, this is shown on the pass.

Passes whose plate could not be read at all are hidden by default, because the same vehicle often also produces a separate pass with its plate. Switch on **Show unread plates** in the widget settings to see them.

8. Alarms

Live alarms

Alarms appear on the dashboard as they happen, in the **Live Alarm Panel**. Select an alarm to open its details: time, camera, analysis, class, a detail specific to the analysis (for example the direction or scenario) and the evidence image.

Searching alarms

The **Alarm Search** widget filters alarms by analysis type, camera, class and date range. Results are paged; use **Load more** to continue.

Exporting

From **Alarm Search**, **Export** creates a file in the background — you can close the window while it is prepared, and download it from the same place when it is ready:

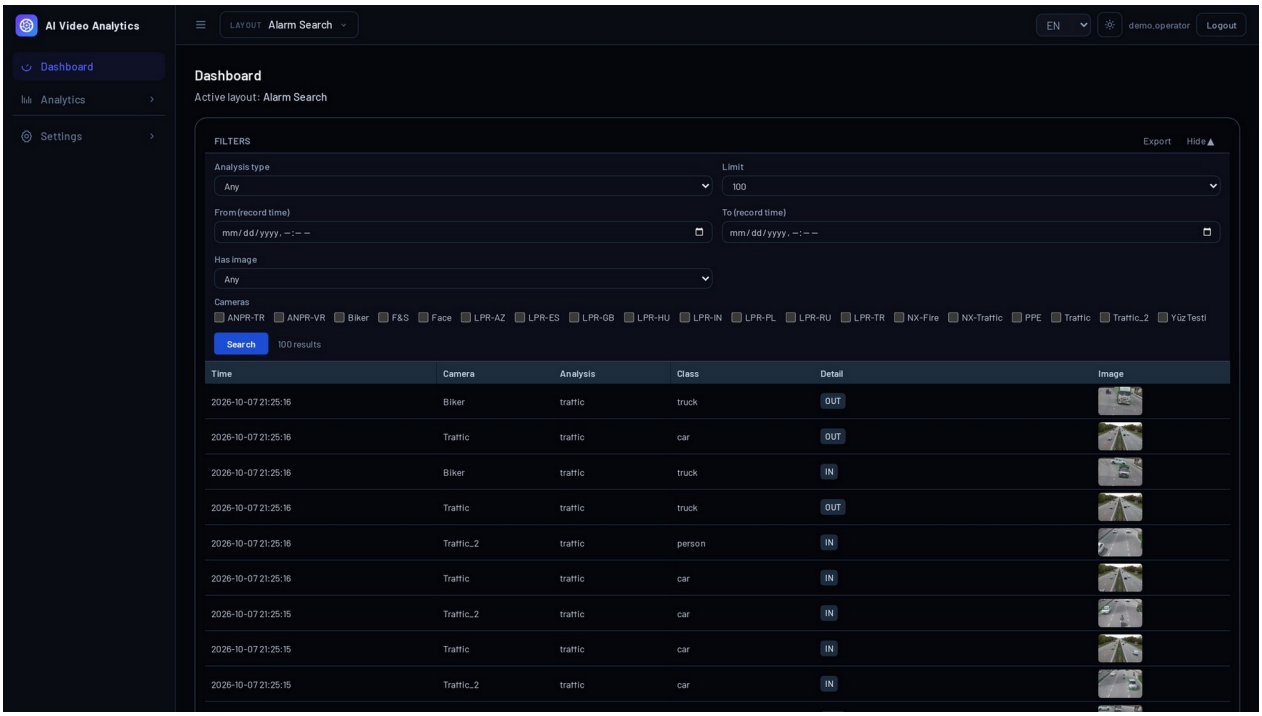
Export	Content
Alarm list (CSV)	One row per alarm, with the current filters
Summary (CSV)	Grouped counts
Executive summary (PDF)	Tables and a chart

The exported file always contains exactly the alarms that match the filters on screen. Exporting needs its own permission. The names of recognised persons are included only if you are allowed to see face identities.

9. Dashboard

Select **Edit** at the top of the dashboard, then **+ Add Widget** to add widgets; drag them to move or resize. Changes apply when you select **Save & Exit**. A layout can be kept private or shared with a role, so that everyone in that role sees the same dashboard.

Widget	Shows
Live Alarm Panel	The newest alarms as they arrive
Alarm Search	Search, filter and export alarms
Alarm Summary Cards	Alarm totals at a glance
Analysis Distribution (Pie)	Alarms split by camera, analysis type or class
Time Series (Trend)	Alarm counts over time
Heatmap	The heatmap of a camera, as a rolling view or a timeline
Occupancy & Vacancy	Occupancy and vacancy times per Object Detection region
Server Resources	CPU, memory, disk and GPU usage
Live Matches	Recent face matches: person, list, score and camera
List Health	People with low-quality or missing reference photos
Unknown Faces	Faces not on any list; add one directly to a list
Demographics	Gender distribution by age band, without identity
Currently Inside	Live occupancy from entry and exit cameras
Passage Log	Entry, exit and duration per person
Archive Status / Face Search	Face archive status and search
Live Plate Passes, Alert List Matches, Plate Search, Plate Pass Statistics, Parking Occupancy	Plate recognition (see **Plate Recognition**)



Alarm Search with filters, results and evidence thumbnails

10. Analysis Scheduling

Settings → Analysis Scheduling creates reusable weekly schedules: select days and time windows, including windows that run past midnight. Assign a schedule to an analysis on the analysis page. Outside its windows the analysis is fully stopped.

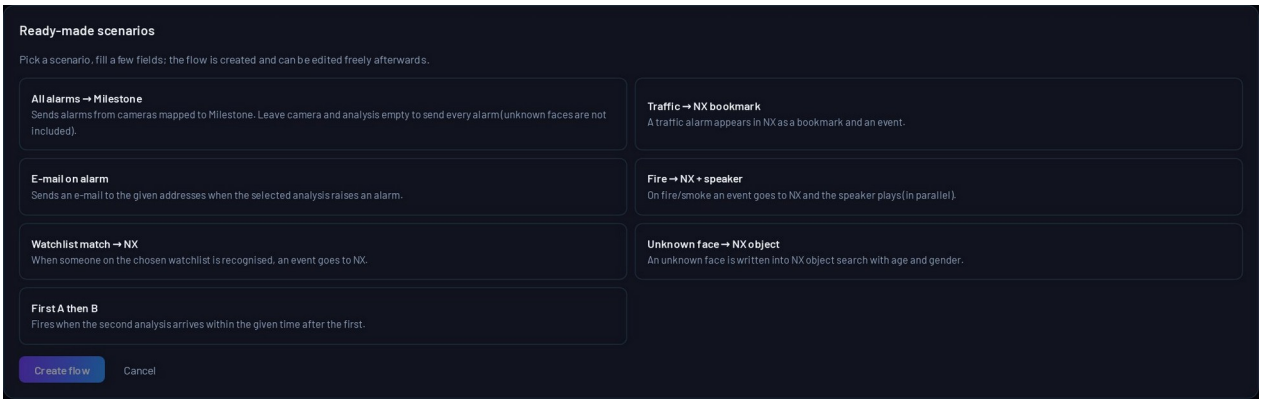
A schedule is re-checked every minute, so an analysis catches up by itself after a server restart. Starting or stopping an analysis by hand overrides its schedule for the rest of the day; the schedule takes over again the next day.

11. Event Manager

Settings → Event Manager decides what happens when an alarm is raised — beyond showing it in the console, which always happens. A **flow** is a chain of blocks drawn on a canvas.

Starting from a template

Select **From a template**, pick one of the ready-made scenarios, fill in the few fields it asks for and select **Create flow**. To build a flow from scratch, select **+ New Flow** and drag blocks onto the canvas.



Ready-made scenarios

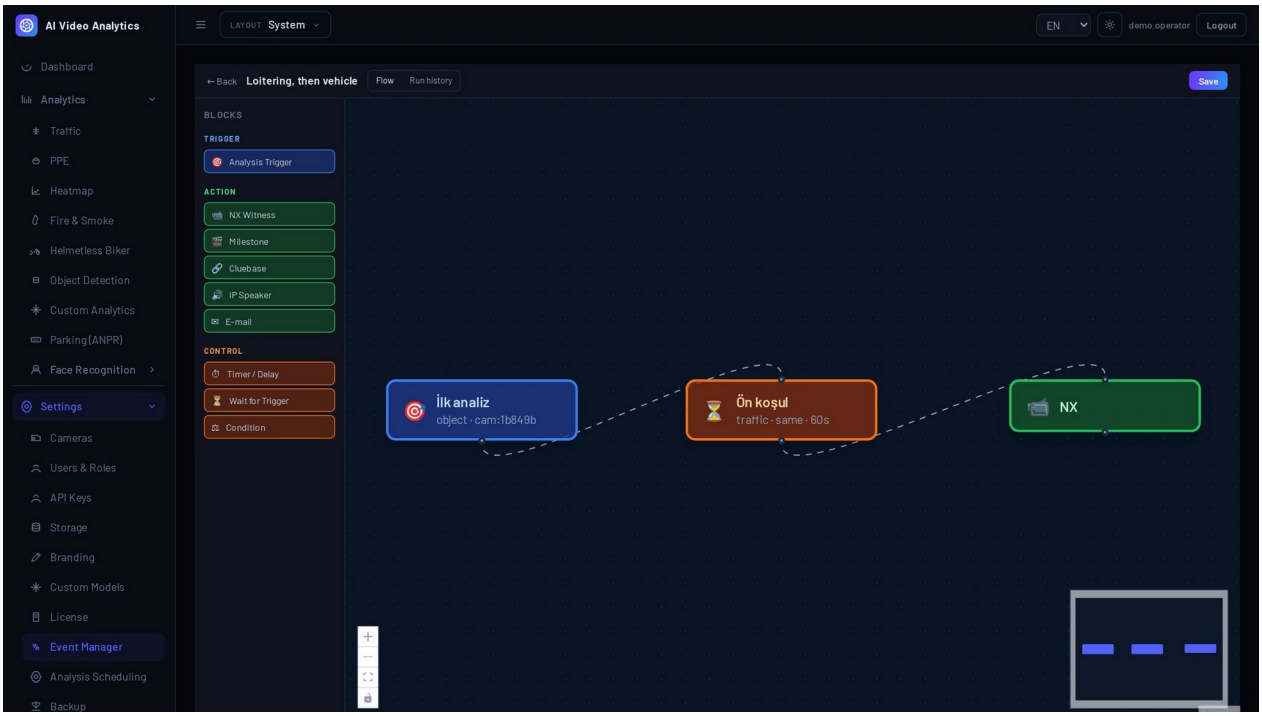
Template	What it does
Traffic → NX bookmark	A traffic alarm appears in the VMS as a bookmark and an event
Fire → NX + speaker	On fire or smoke, an event goes to the VMS and an IP speaker plays, in parallel
Watchlist match → NX	When someone on the chosen list is recognised, an event goes to the VMS
Unknown face → NX object	An unknown face is written into the VMS object search with age and gender
First A then B	Fires when a second analysis alarm follows the first within a set time
E-mail on alarm	Sends an e-mail to the given addresses

Blocks

Group	Block	Purpose
Trigger	Analysis Trigger	Starts the flow on an alarm of the selected analysis, cameras, classes or regions
Control	Condition	Continues on the **then** or **else** path depending on rules (for example class, confidence, time of week)
Control	Timer / Delay	Waits before continuing
Control	Wait for Trigger	Waits for a second alarm within a time window — on the same camera, a specific camera or any camera
Action	NX Witness	Sends an event, bookmark or analytics object to the VMS
Action	Milestone	Sends the alarm to Milestone XProtect
Action	Cluebase	Sends the alarm to Cluebase
Action	IP Speaker	Plays an announcement on a network speaker
Action	E-mail	Sends an e-mail
Action	UX Alarm	Kept for compatibility; alarms always appear in the console, so it has no extra effect

Messages can include details of the alarm with placeholders such as `{camera_name}`, `{analysis_type}`, `{class_name}`, `{confidence}`, `{zone_id}` and `{timestamp}`. The same placeholders work in every action.

Invalid settings are shown next to the block when you save; a flow is not saved until they are fixed.



A "First A then B" flow: an object alarm, then a traffic alarm on the same camera within 60 seconds, then an action

Run history

Run history shows every execution of a flow and the result of each step. If a step fails — for example because an e-mail server is unreachable — the reason is shown there; connection details and passwords are removed from the message.