IP camera SH

User manual

PARTIZAN™

BE DIFFERENT

LEAD WITH IT

2026

Content

1. Product overview

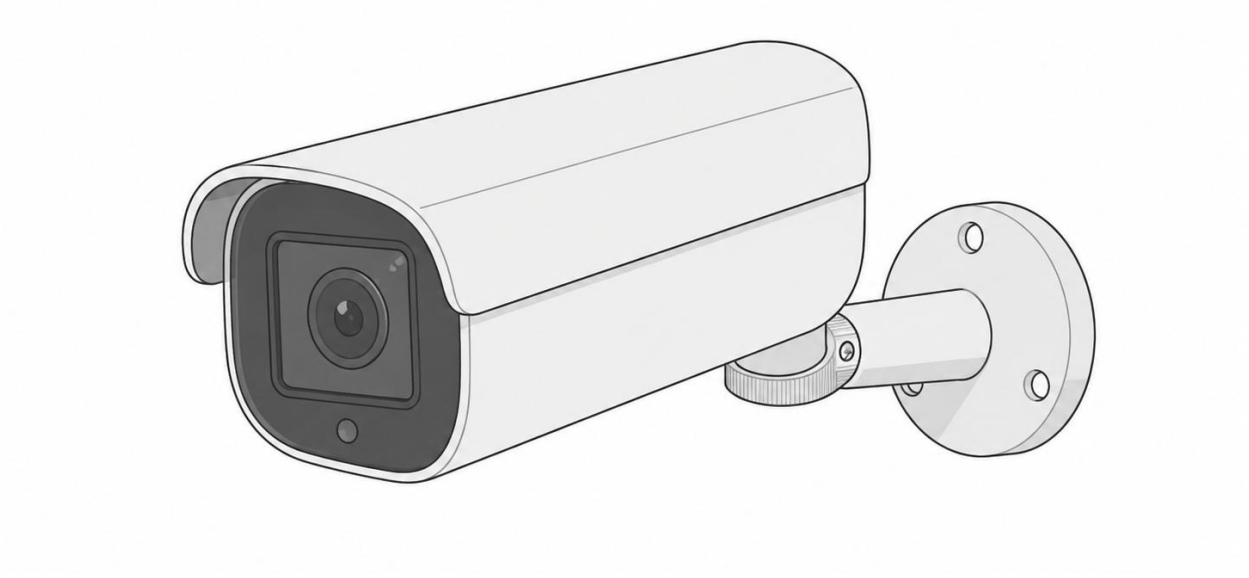

Fig. 1. Partizan IP camera cloud series

Partizan SH Series IP cameras are integrated network cameras with powerful image processing capabilities, suitable for shopping malls, supermarkets, schools, factories, warehouses, offices, residential complexes, and other public or private spaces requiring professional video surveillance.

An SH Series IP camera is a digital network monitoring camera that operates independently with a built-in web server. It can be accessed and configured directly from a standard web browser without any additional client software, supporting Internet Explorer, Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.

The camera supports multiple simultaneous users with individually configurable permission levels, and includes a comprehensive suite of built-in AI analytics — including face detection, license plate recognition, perimeter intrusion, line crossing, object detection, crowd density, queue length, and more.

Upon detecting an event (motion, sound, line crossing, intrusion, etc.), the camera can automatically record video, capture snapshots, send email notifications, push events to a remote platform, or trigger an external alarm output.

2. Login

2.1. Accessing the camera from a web browser

You can access the camera in two ways: use the Device Config Tool to search for cameras on the local network and click an IP address to open the web client directly, or open a browser and type the camera's address manually in the format: HTTP://ip:port (default port is 80, so the address is simply: http://192.168.1.168).

2.2. First-time login

When accessing the camera from a web client for the first time, you must set a new password before the login screen appears:

1. The web client prompts you to set a new password and configure password recovery options before proceeding.
2. The password must be 8–16 characters long and contain at least two combinations of: uppercase letters, lowercase letters, numbers, and special characters. The password and username cannot be the same.
3. After setting the password, you can optionally configure one or more password recovery methods:

- Security Question Configuration — select three questions and provide answers. These will be used to verify your identity if you forget the password.
- Certificate of Authorization — download and store a certificate.txt file. Use this file to recover the password if the security question method is not set up.
- Super Code (not recommended) — calculates a recovery code based on the camera's MAC address and the current time. This is an insecure method and should only be used as a last resort.

Note: Keep your recovery information in a safe place. Without it, recovering a forgotten password may not be possible.

2.3. General login

Open a web browser and enter the camera's IP address in the address bar. On first access, the camera will prompt you to create a password before you can proceed (8–16 characters, must include at least two of the following: uppercase letters, lowercase letters, numbers, and special characters).

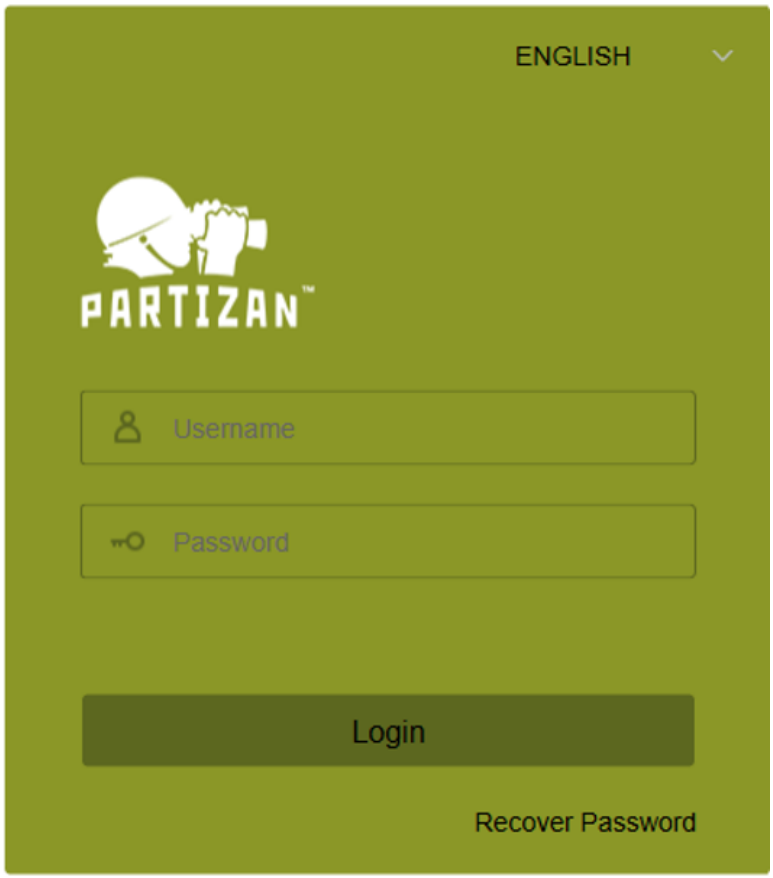

Fig. 2. Login screen — enter username and password to access the camera

1. Enter the camera's IP address in your browser's *address* bar (default: 192.168.1.168).
2. Select the interface language from the top-right dropdown if needed.
3. Enter your Username and Password, then click Login.
4. If you forget your password, click Recover Password and follow the on-screen instructions (security question, certificate, or super code).

Note: Always change the default password immediately and keep your recovery information (security questions or certificate file) in a safe place.

2.4. Recover password

If you forget the login password, click Recover Password on the login screen to open the recovery interface. Three recovery methods are available:

- Security Question — answer the security questions configured during first login to reset the password.
- Certificate of Authorization — upload the certificate.txt file downloaded during first login to authenticate and reset the password.
- Super Code — contact Partizan technical support to obtain a super code calculated from the camera's MAC address and a specific timestamp.

2.5. Password expiry

To reduce security risks from prolonged use of the same password, the system tracks when the password was last changed. When the password is considered expired, a prompt will appear asking you to change it. Enter the old password for verification, then set a new one following the same complexity requirements.

3. Live view

After logging in, the camera opens directly into the Live View screen, showing the real-time video stream along with PTZ controls (for supported models) and stream-quality switching.

Fig. 3. Live View — main stream display with PTZ control panel on the right

Control	Function
Main/ Sub / Mobile Stream	Switch between video quality/resolution profiles for the live display
PTZ Panel	Pan/tilt/zoom directional controls, zoom in/out, focus, and preset positions (PTZ-capable models)
Speed Slider	Adjusts the speed of PTZ movement
Mode	Expandable panel for additional PTZ patrol/scan modes
Toolbar icons (bottom-left)	Snapshot, digital zoom, mute, and full-screen controls

3.1. Stream switching

Switch the picture quality of the live view using the buttons at the top-left of the video area:

- MainStream — high-definition video, but requires higher bandwidth and PC performance.
- SubStream — moderate bandwidth and performance requirements, lower picture quality compared to Main Stream.
- MobileStream — lowest bandwidth and performance requirements, and lowest picture quality.

3.2. Main toolbar (top-right navigation)

The three main tabs at the top of the interface switch between the main functional screens: Live (real-time view), Playback (recorded footage), and Remote Setting (full camera configuration).

3.3. Live view controls

Control / Icon	Function
PTZ Joystick	Pan/tilt/zoom controls — directional arrows for camera movement (PTZ models only)
Speed Slider	Adjusts the speed of PTZ movement
Zoom In / Out (PTZ)	Optical zoom controls below the directional pad
Preset Points	Store and recall up to 5 camera positions (point 1–5) for quick repositioning
Mode	Expandable panel for PTZ patrol and scan modes
Stop/Play	Start or stop the live stream preview
Full Screen	Switch to full-screen view (double-click or Esc to exit)
Record	Manually record the live stream to the configured local path
Capture	Take a snapshot and save it to the configured local folder
Digital Zoom	Click and drag on the live view to zoom into a specific area
Audio / Voice Intercom	Adjust audio volume or activate two-way voice communication
Add Tag	Add a named bookmark at the current time in the recording
Light / Siren / Warning Light	Manually activate white light deterrence, siren, or warning lights (model-dependent)

3.4. Recording status indicators

The recording status icon in the live view shows the current recording and alarm state at a glance:

- No icon — SD card is functioning normally but no recording is in progress.
- Normal recording icon — the camera is recording continuously.
- SD card error icon — check the memory card; it may be missing or faulty.
- Motion alarm (recording off/on) — motion detected with or without alarm recording active.
- I/O alarm icons — external alarm input triggered (recording on or off).
- Intelligent alarm icons — AI event detected (Face/Human/Vehicle), recording on or off.

4. Playback

Click Playback in the top navigation bar to switch to the recorded footage search and playback screen. The camera stores video to the local SD card or network HDD. Select a search mode from the dropdown at the top-left of the left panel to choose the type of footage or event to search for.

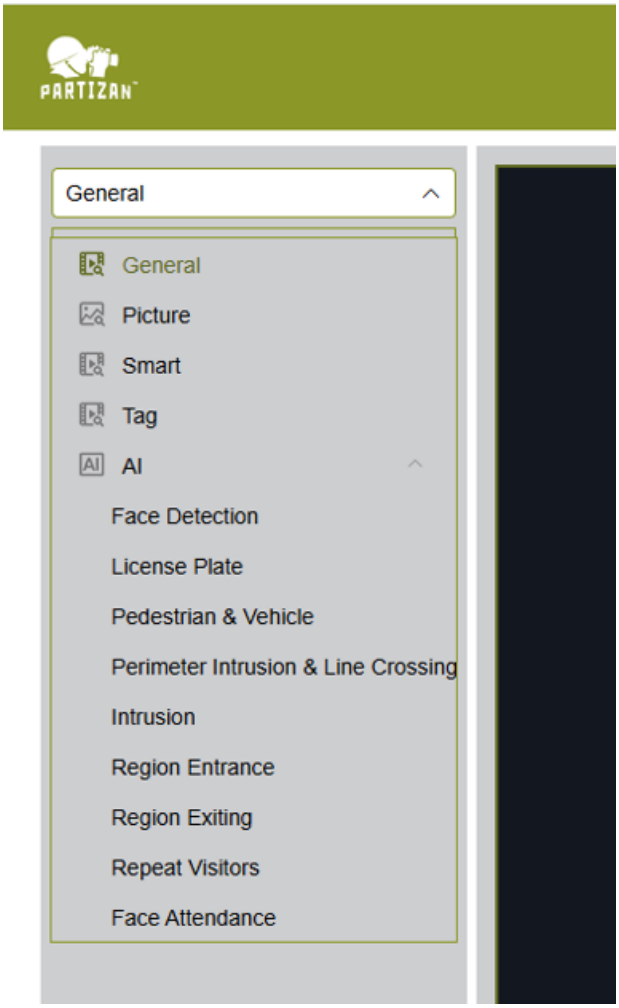

Fig. 4. Playback mode selector dropdown — General, Picture, Smart, Tag, and AI subtypes [NEW]

4.1. General playback

General Playback is selected by default and provides timeline-based search and playback of all recorded video files on the SD card.

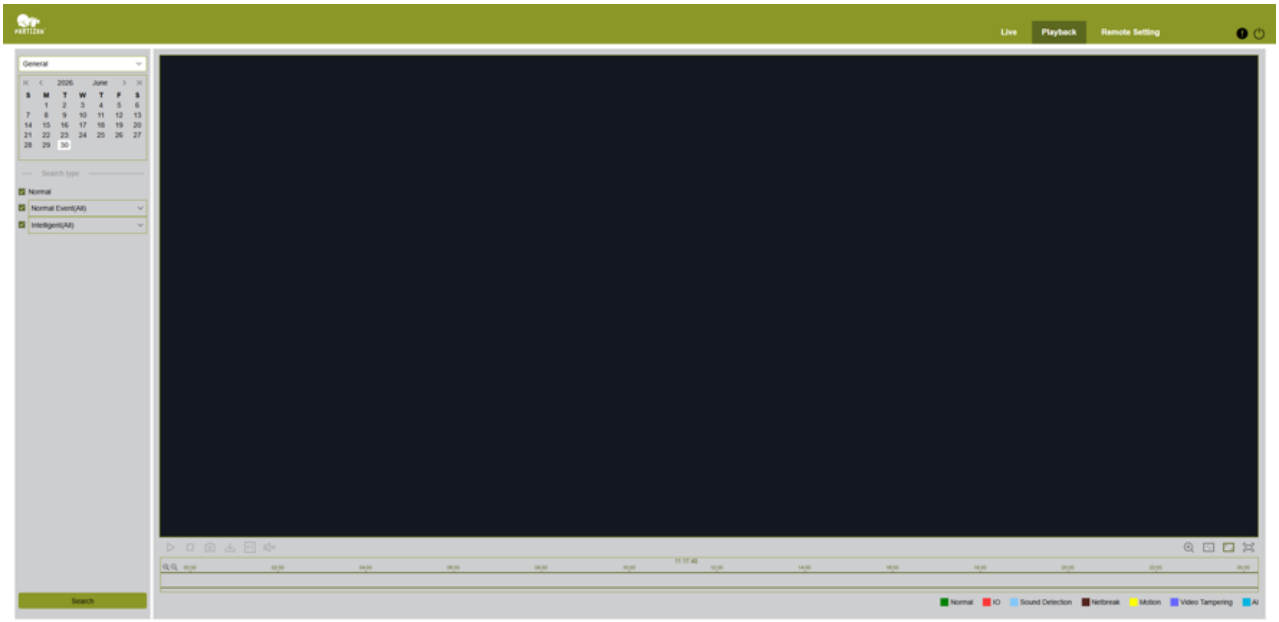

Fig. 5. General Playback — calendar, search-type filters, and timeline with color-coded event types

1. Select a date from the calendar on the left.
2. Check the desired Search Type filters: Normal, Normal Event, or Intelligent events.
3. Click Search to load recordings onto the timeline. Colors indicate event types: green = Normal, red = IO, light blue = Sound Detection, dark brown = Netbreak, yellow = Motion, purple = Video Tampering, blue = AI.
4. Click anywhere on the timeline to jump to that moment and begin playback.

Playback Control	Function
▶ / ❚❚ Play/Pause	Start or pause playback
■ Stop	Stop playback and return to the beginning
⊡ Forward by Frame	Step through the recording one frame at a time
Speed (1/8×–×16)	Rewind or fast-forward at 1/8, 1/4, 1/2, 1, ×2, ×4, ×8, or ×16 speed

Playback Control	Function
⭳ Download	Download the searched recording file to your PC (AVI or MP4 format)
Capture	Save a snapshot from the current playback frame
Audio	Toggle or adjust playback audio
Timeline Zoom	Scroll-zoom the timeline to narrow down the view (from 24 hours to minutes)

4.2. Picture search

When the auto-capture function is enabled, you can search for and browse recorded snapshots on this screen.

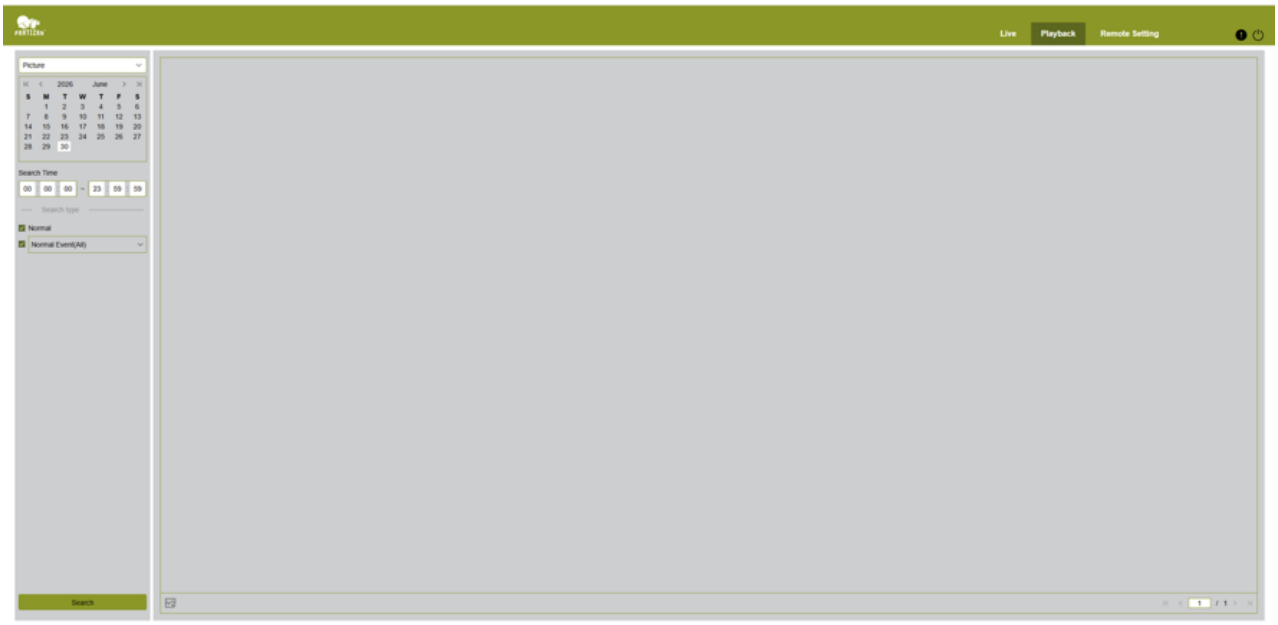

Fig. 6. Picture search — date and time range filters with thumbnail browsing

1. Switch the search mode dropdown to Picture.
2. Select the date and set a start/end time range.
3. Select the capture type (Normal Event, or All).
4. Click Search. Thumbnails of matching snapshots appear. Double-click a snapshot to play the surrounding video.

4.3. Smart search

Smart Search highlights areas of the frame containing motion or AI-detected activity, displayed as a color-coded heat grid overlay on the timeline for quick visual review.

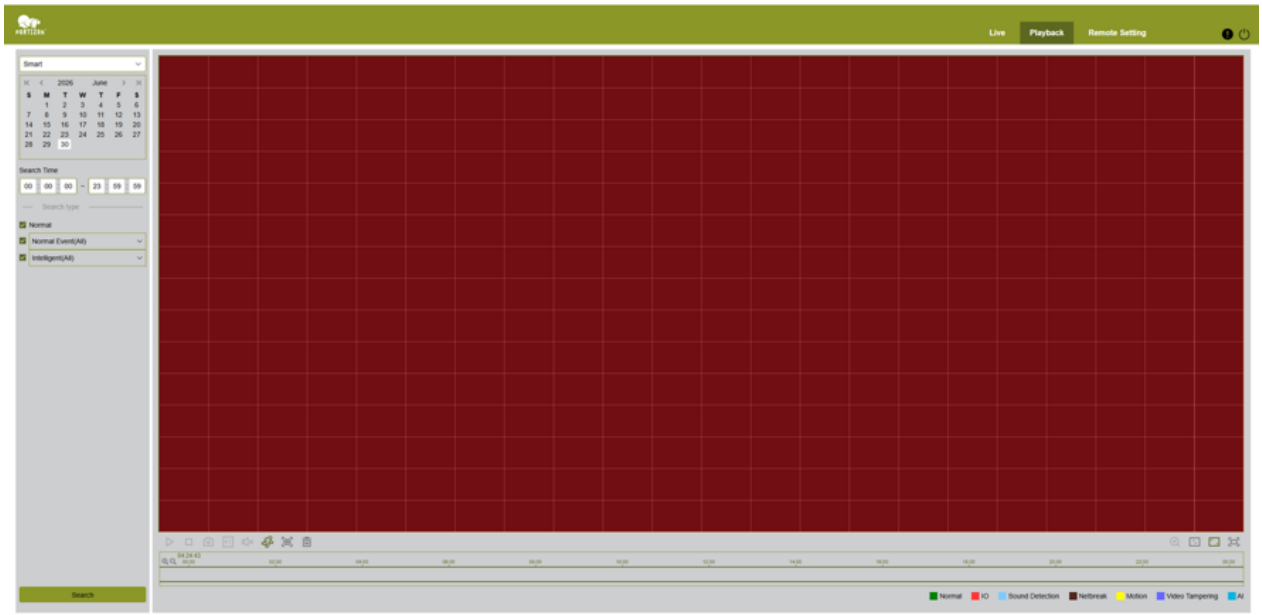

Fig. 7. Smart Search — grid overlay highlighting detected activity across the recorded period

1. Switch the search mode to Smart.
2. Set the date and search time range and search type filters.
3. Click the Smart icon in the playback toolbar to draw a detection area on the frame, or click All to use the full frame.
4. Click Search to find recordings with activity in the selected area.

4.4. Tag search

Search for manually tagged moments in the recording, identified by name and time range.

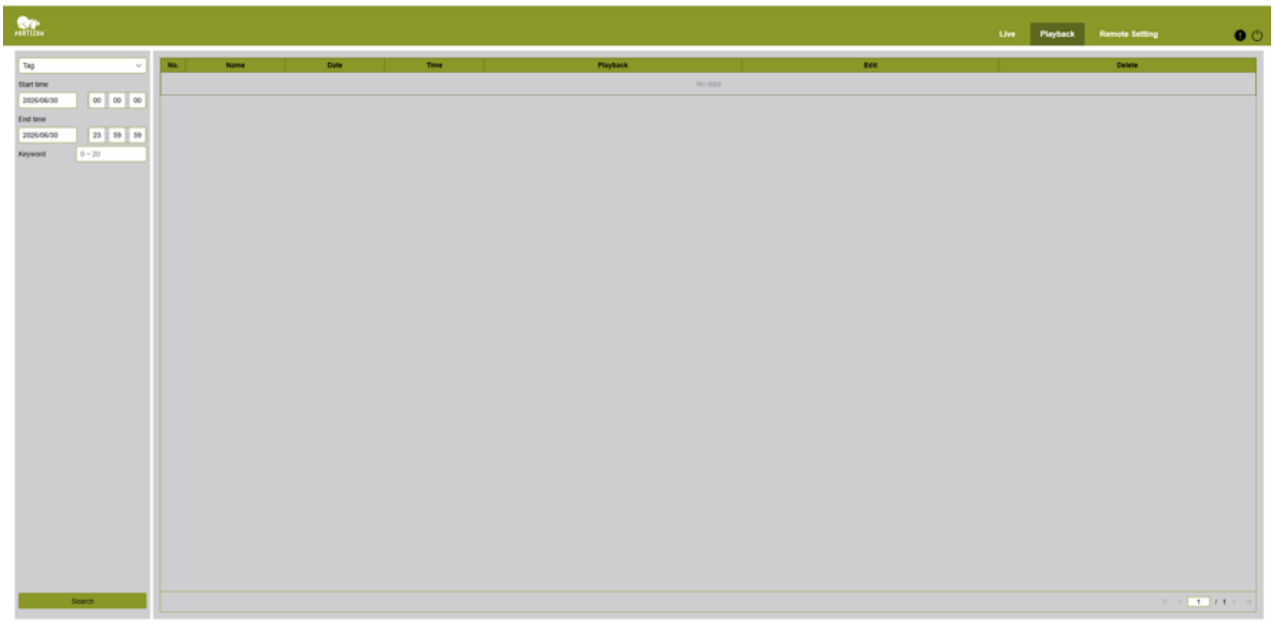

Fig. 8. Tag search — search by keyword, start time, and end time

1. Switch the search mode to Tag.
2. Set the Start Time and End Time for the search range.
3. Optionally enter a Keyword to filter tags by name.
4. Click Search. Click the play icon to jump to that moment. Click the edit icon to rename a tag.

4.5. AI search

The camera provides dedicated AI search interfaces for each type of AI analytic event it has captured.

4.5.1 Face detection

The camera performs face detection, stores face capture images to the SD card, and saves the associated metadata.

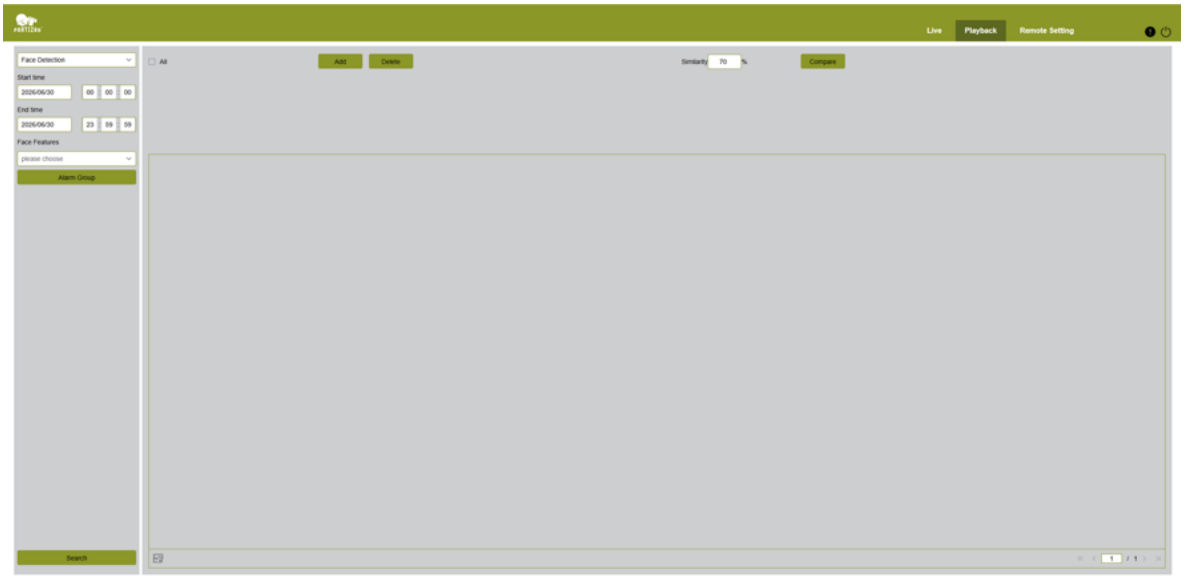

Fig. 9. Face Detection search — search by time range and face features, with similarity comparison

- Start Time / End Time — set the time range for searching captured face images.
- Face Features — when enabled, only face images captured with Face Features detection turned on are returned.
- Alarm Group — filter results by the face database group the person belongs to.
- Add — add a local or captured face image as a reference for similarity comparison.
- Similarity — set the minimum similarity threshold (0–100%) for the Compare function.
- Compare — searches for captured faces that match the reference image above the set similarity threshold.
- Double-click a result — plays the video recorded just before and after that face capture.

4.5.2 License plate

When license plate detection is enabled, captured plate images are stored with associated metadata.

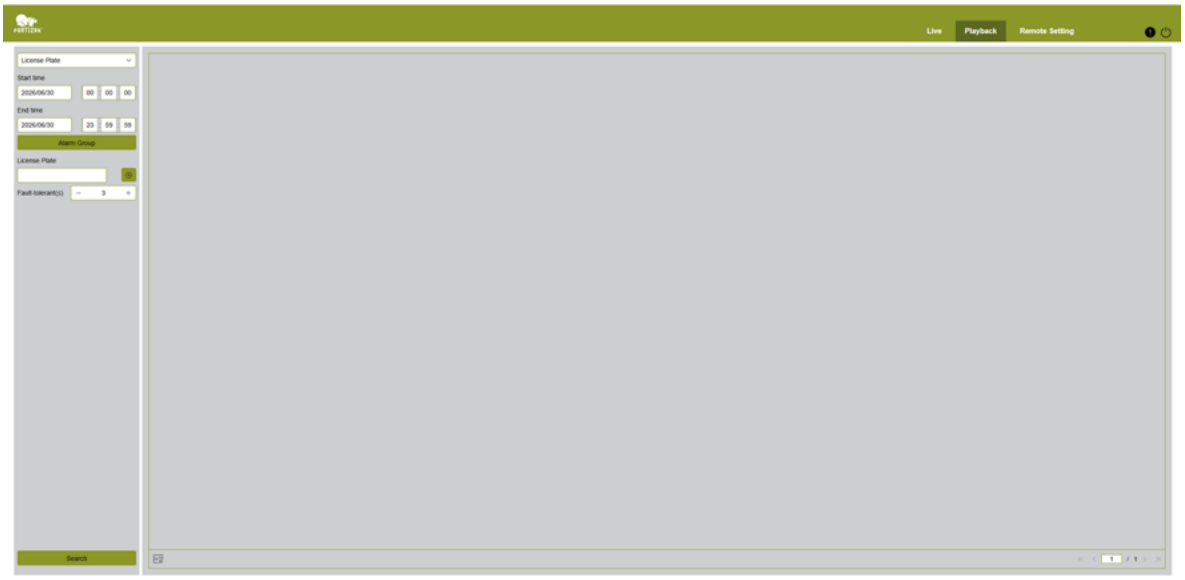

Fig. 10. License Plate search — search by plate number with fault-tolerance setting

- License Plate — enter a plate number (or partial number) to search for.
- Fault-tolerant — number of characters allowed to differ from the entered plate. For example, with fault-tolerance 3, plate B594SB will match B594XX in the database.
- Alarm Group — filter results by license plate database group.

4.5.3 Pedestrian & vehicle

The camera distinguishes humans and vehicles in the scene and allows quick retrieval by target type and time range.

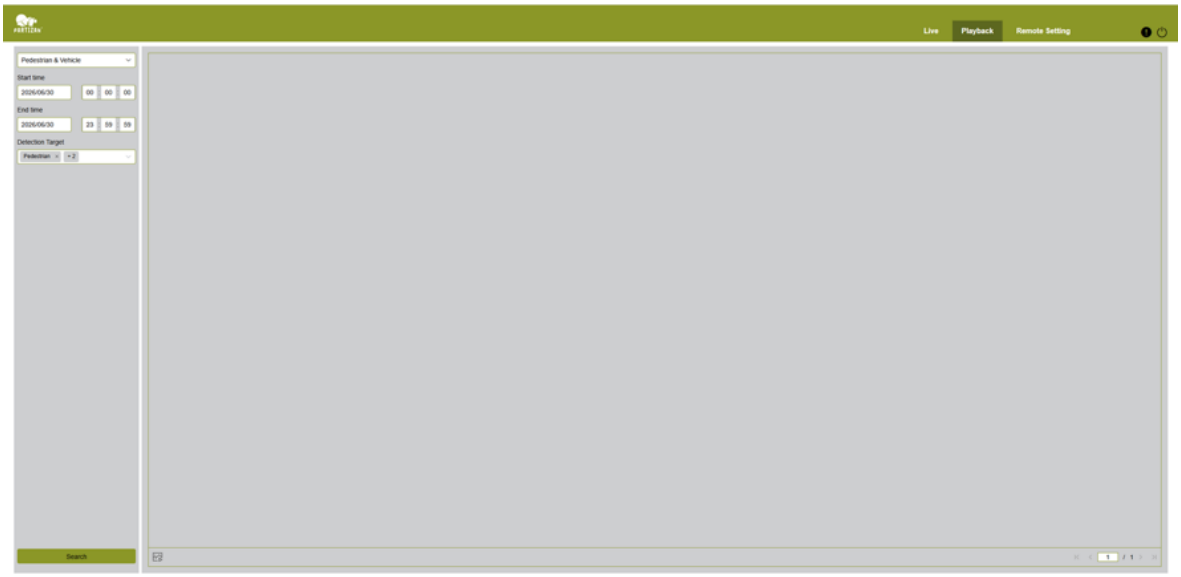

Fig. 11. Pedestrian & Vehicle search — filter by detection target type

- Detection Target — select Pedestrian, Motor Vehicle, Non-motorized Vehicle, or all types.
- Double-click a result — plays back the surrounding footage.

4.5.4 Perimeter intrusion & line crossing

Retrieves events where a target crossed a defined perimeter line or virtual border, with filtering by vigilance rule type and target.

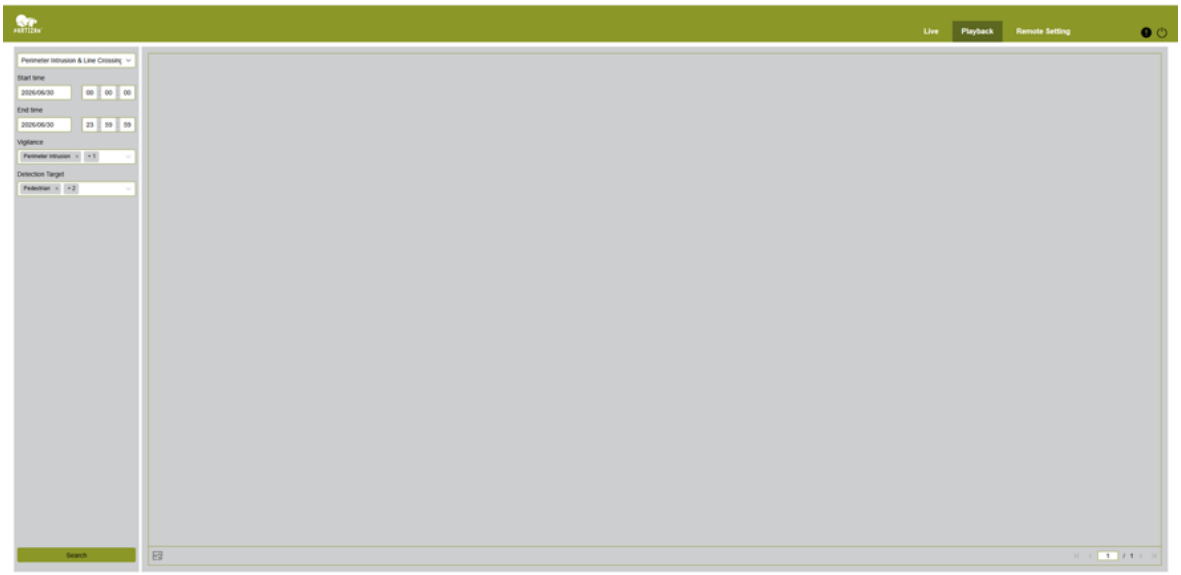

Fig. 12. Perimeter Intrusion & Line Crossing search — filter by vigilance rule and detection target

- Vigilance — select Perimeter Intrusion, Line Crossing, or both.
- Detection Target — filter by Pedestrian, Motor Vehicle, or Non-motorized Vehicle.

4.5.5 Intrusion

Retrieves events where a target entered a restricted area and stayed beyond the configured time threshold.

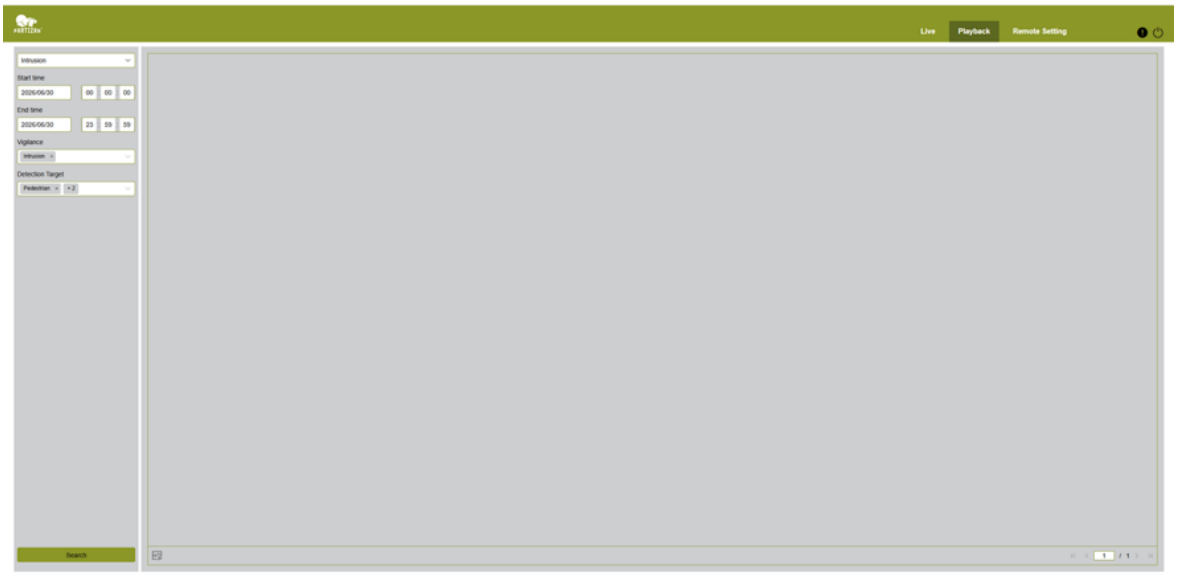

Fig. 13. Intrusion search — filter by vigilance rule and detection target

4.5.6 Region entrance

Retrieves events where a target entered the guarded area from outside.

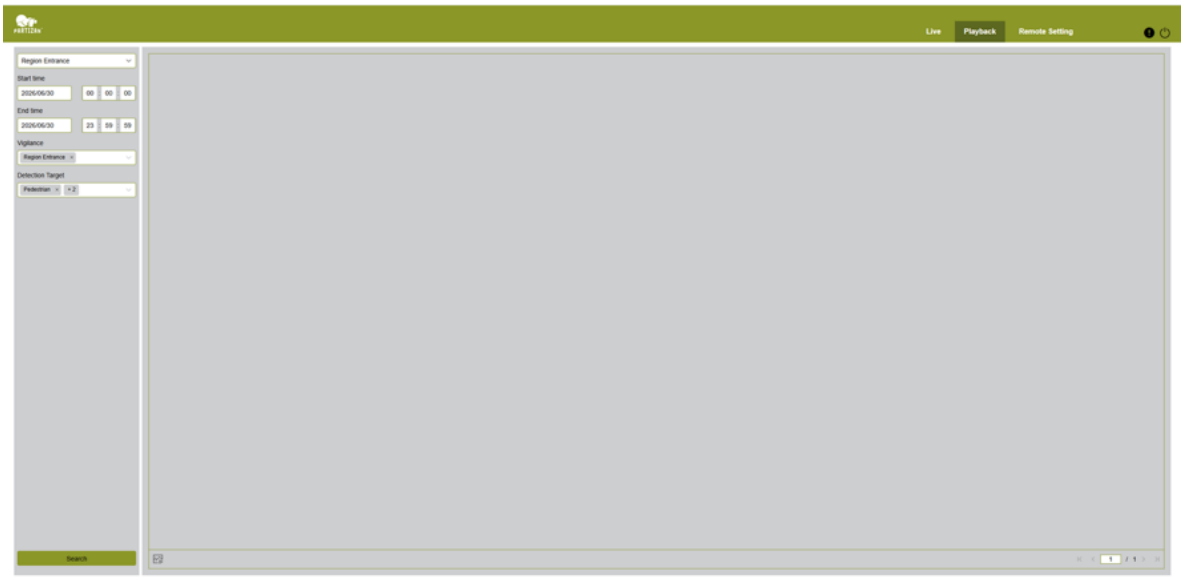

Fig. 14. Region Entrance search

4.5.7 Region exiting

Retrieves events where a target left the guarded area.

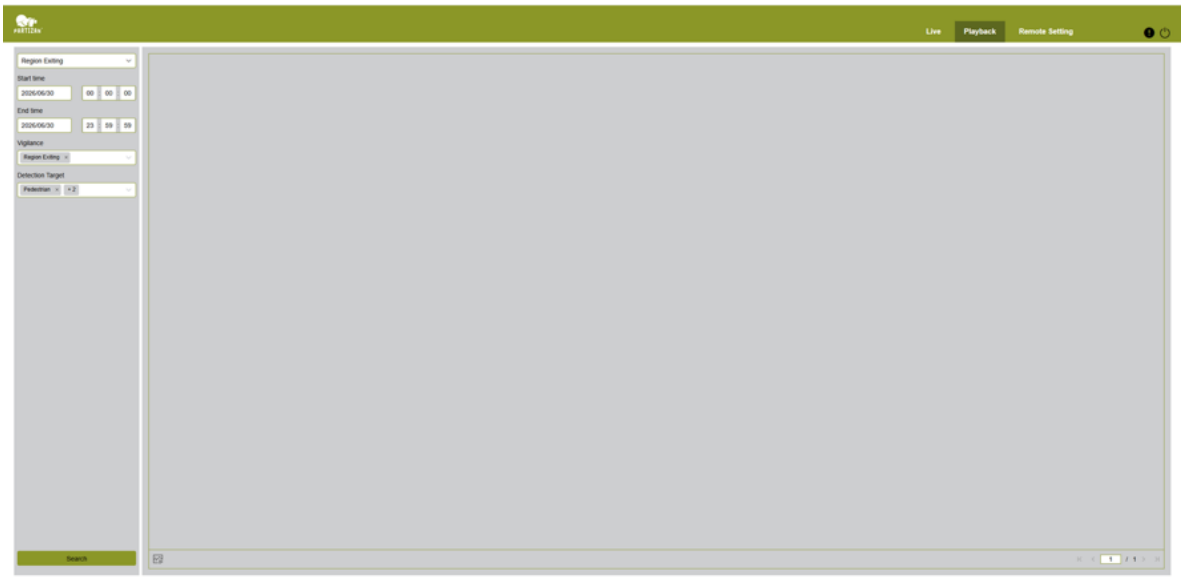

Fig. 15. Region Exiting search

4.5.8 Repeat visitors

Identifies people who appeared multiple times within a set time window, based on facial similarity matching. Useful for VIP recognition or suspicious behavior analysis.

Fig. 16. Repeat Visitors search — minimum interval, similarity threshold, and sorting options

- Minimum time interval — minimum time between two captures of the same person to count as a separate visit (seconds).
- Similarity — minimum face matching similarity (0–100%). Only effective when no Face Features filter is applied.
- Face Features — filter by facial attributes. When not set, all images in the range are searched.
- Alarm Group — search within a specific face database group.
- Minimum number of occurrences — show only people who appeared at least this many times. Click Refresh to update.
- Sort Type — sort by time or visit count, ascending or descending.

4.5.9 Face attendance

Automatically tracks when registered faces check in and out relative to configured duty hours, and generates attendance reports.

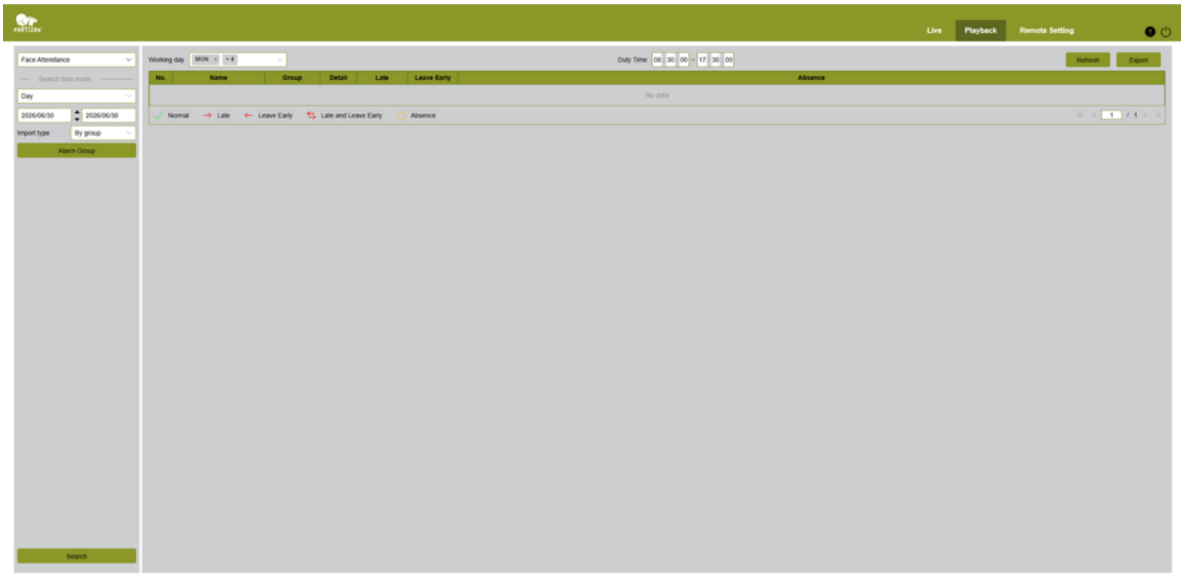

Fig. 17. Face Attendance report — working days, duty time, and attendance status legend

- Search Time Mode — Day, Week, Month, Custom, or Today.
- Import type — By Group (all people in a database group) or By Face (individual face selection).
- Working Day — set which days of the week count as working days.
- Duty Time — set the on-duty and off-duty reference times for attendance calculation.
- Export — export the attendance report to your PC.

Attendance legend: '→' = Late, '←' = Leave Early, '↔' = Late and Leave Early, '✓' = Normal, 'o' = Absence.

5. Remote setting → channel

The Remote Setting menu provides full access to camera configuration, organized into seven main categories in the left sidebar: Channel, Record, Event, AI, Network, Device, and System.

5.1. Live (on-screen display)

Configure how the camera name, date, and time are overlaid on the live video and recordings.

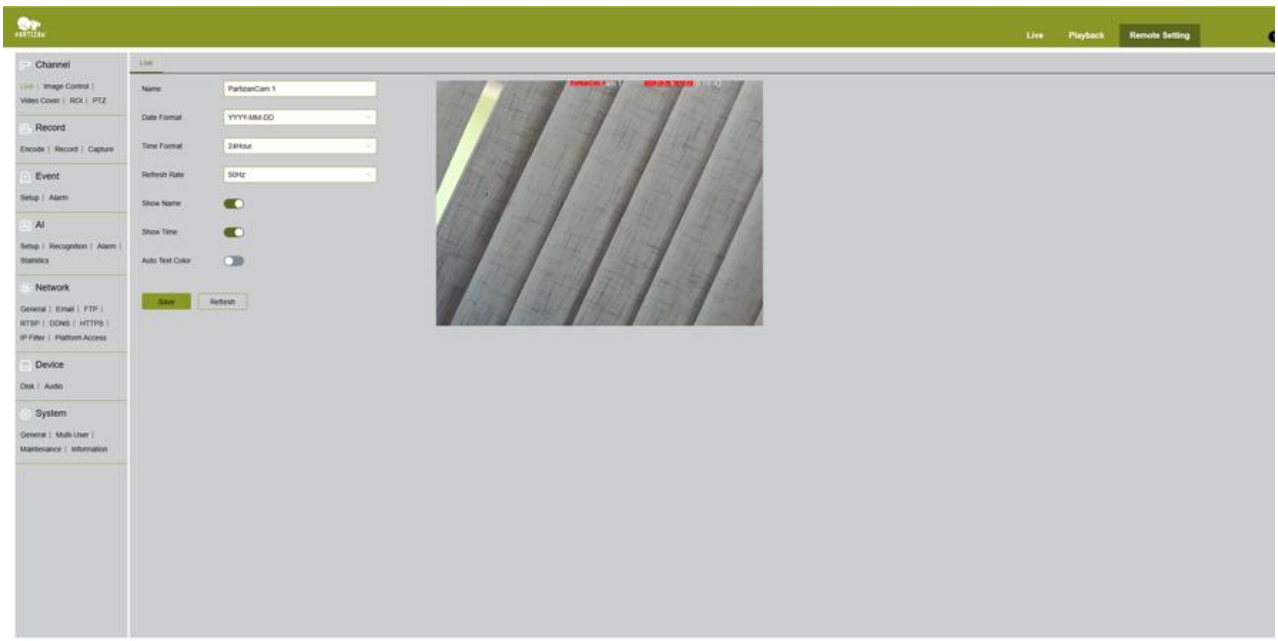

Fig. 18. Channel → Live — name, date/time format, refresh rate, and overlay toggles

Setting	Description
Name	Camera display name shown in the OSD overlay
Date Format / Time Format	Choose date layout (YYYY-MM-DD, etc.) and 12/24-hour format
Refresh Rate	Video refresh rate to match local power frequency (50Hz/60Hz)
Show Name / Show Time	Toggle the camera name and timestamp overlay on screen
Auto Text Color	Automatically adjusts overlay text color for visibility against the background

5.2. Image control

Fine-tune exposure, white balance, IR illumination, and image processing parameters.

Fig. 19. Channel → Image Control — IR-CUT, exposure, white balance, shutter, and noise reduction settings

Setting	Description
IR-CUT Mode / Sensitivity	Controls the day/night IR-cut filter switching behavior and sensitivity
IR-LED	Manual or automatic control of infrared illumination, with Low/High Beam Light sliders
Mirror	Flip the image horizontally
Exposure Compensation / White Balance / Shutter	Automatic or manual exposure and color balance controls
3D Noise Reduction	Reduces image noise in low-light conditions
Max. Zoom Ratio	Maximum optical/digital zoom level available

5.3. Video cover (privacy mask)

Define areas of the frame to be masked from view, useful for blocking out private property or sensitive areas within the camera's field of view. This page also provides PTZ preset point management.

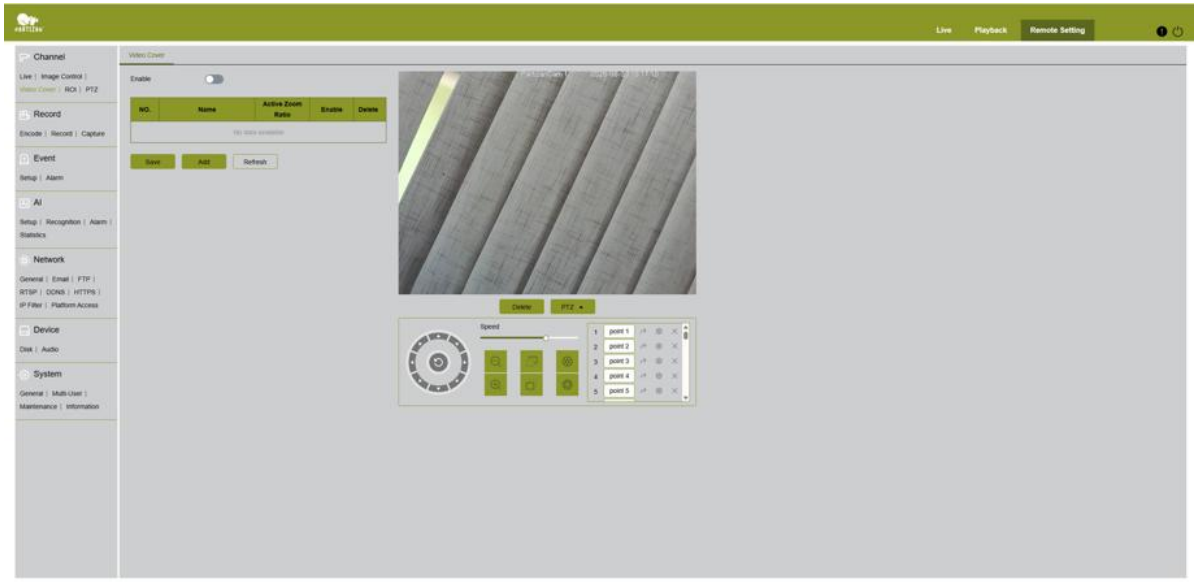

Fig. 20. Channel → Video Cover — privacy mask table and PTZ preset point list

5.4. ROI (region of interest)

Set a Region of Interest to allocate higher video quality/bitrate to a specific part of the frame, optimizing bandwidth usage while keeping important areas sharp.

Fig. 21. Channel → ROI — stream type, region selection, and ROI quality level

5.5. PTZ

Configure the PTZ communication protocol and motor behavior for cameras with mechanical pan-tilt-zoom (separate from the Video Cover preset list). A second tab, Scheduled Tasks, allows automated PTZ patrol scheduling.

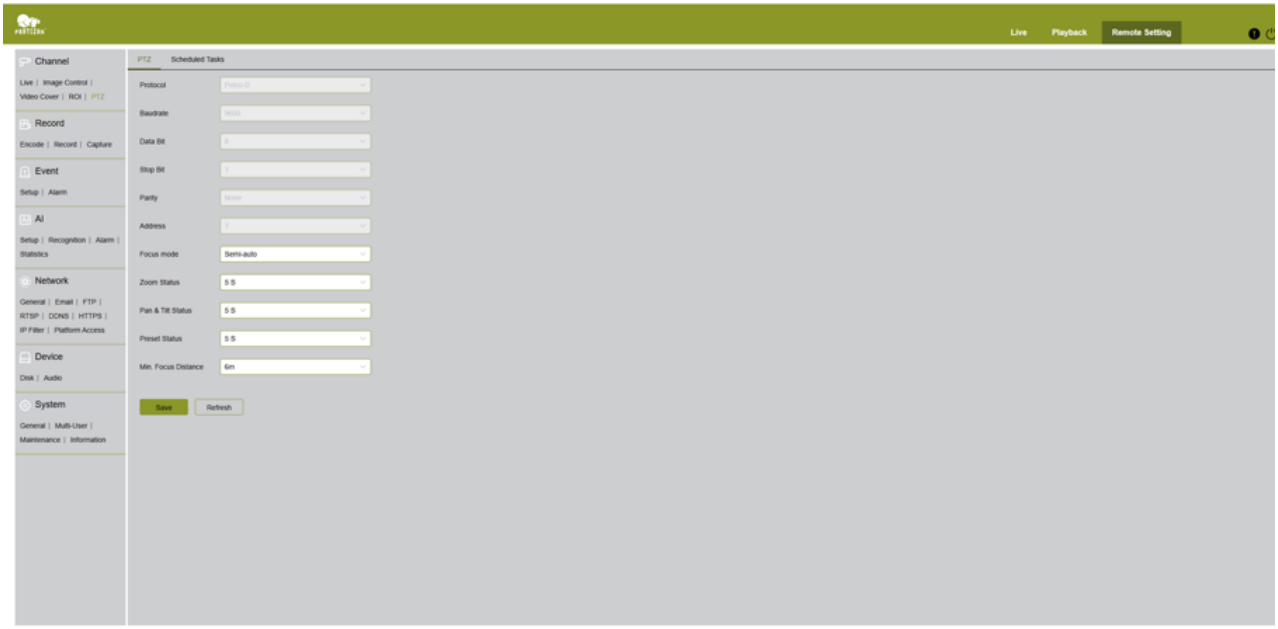

Fig. 22. Channel → PTZ — protocol, baud rate, focus mode, and zoom/pan/tilt timing

Setting	Description
Protocol / Baudrate / Data Bit / Stop Bit / Parity / Address	Serial communication parameters for external PTZ control (e.g. Pelco-D)
Focus Mode	Auto, semi-auto, or manual focus behavior
Zoom / Pan & Tilt / Preset Status	Idle timeout settings for each PTZ motor function
Min. Focus Distance	Minimum focusing distance for the lens

6. Remote setting → record

6.1. Encode

This menu allows you to configure the image quality for video recording or network transmission. Main Stream defines the quality parameters for local recording to the SD card. Sub Stream and Mobile Stream define the quality parameters for network transmission over limited-bandwidth connections and mobile access respectively.

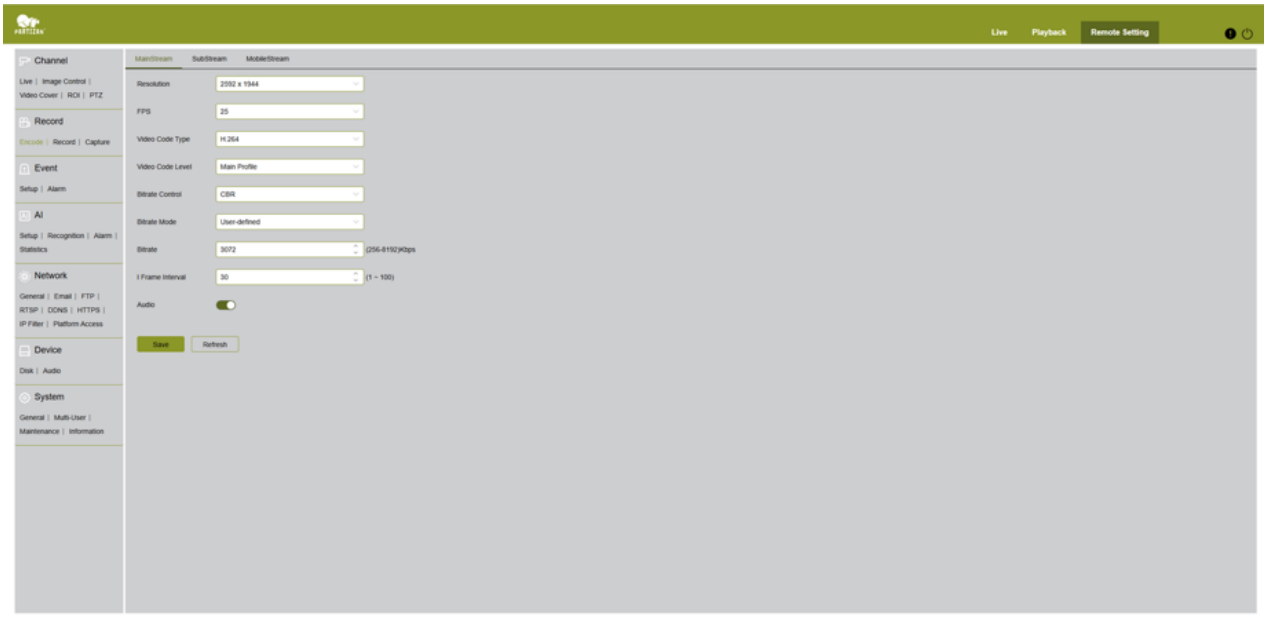

Fig. 23. Record → Encode (Main Stream) — resolution, FPS, codec, and bitrate settings

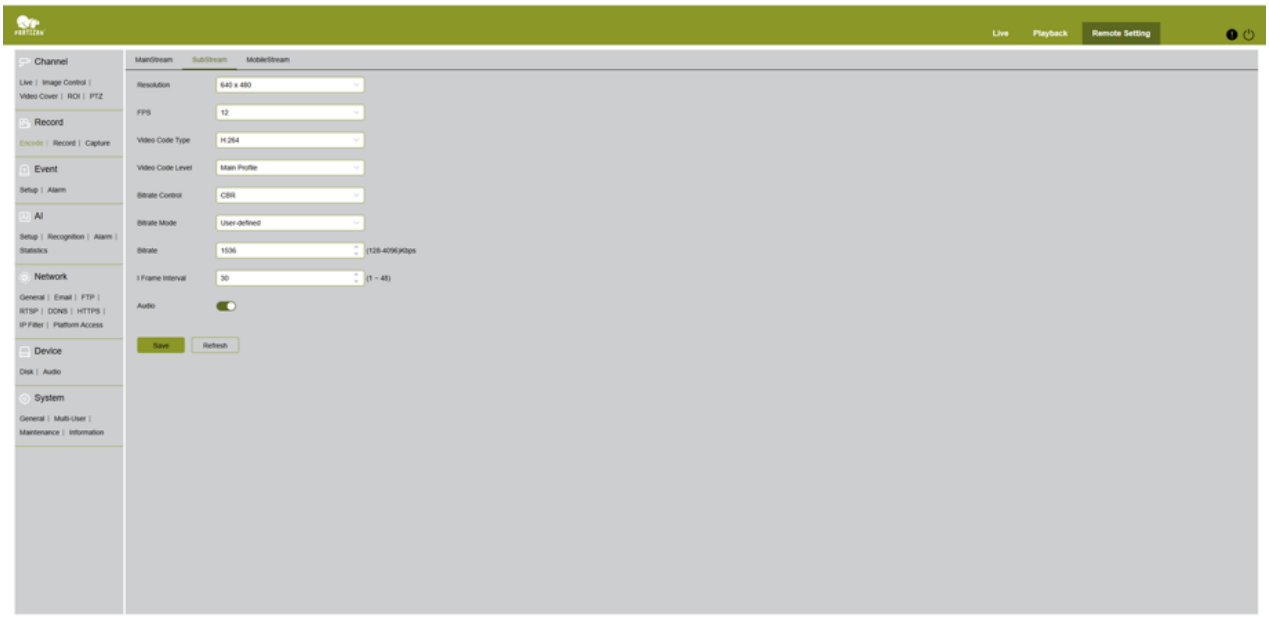

Fig. 24. Record → Encode → Sub Stream — lower resolution and bitrate for network transmission

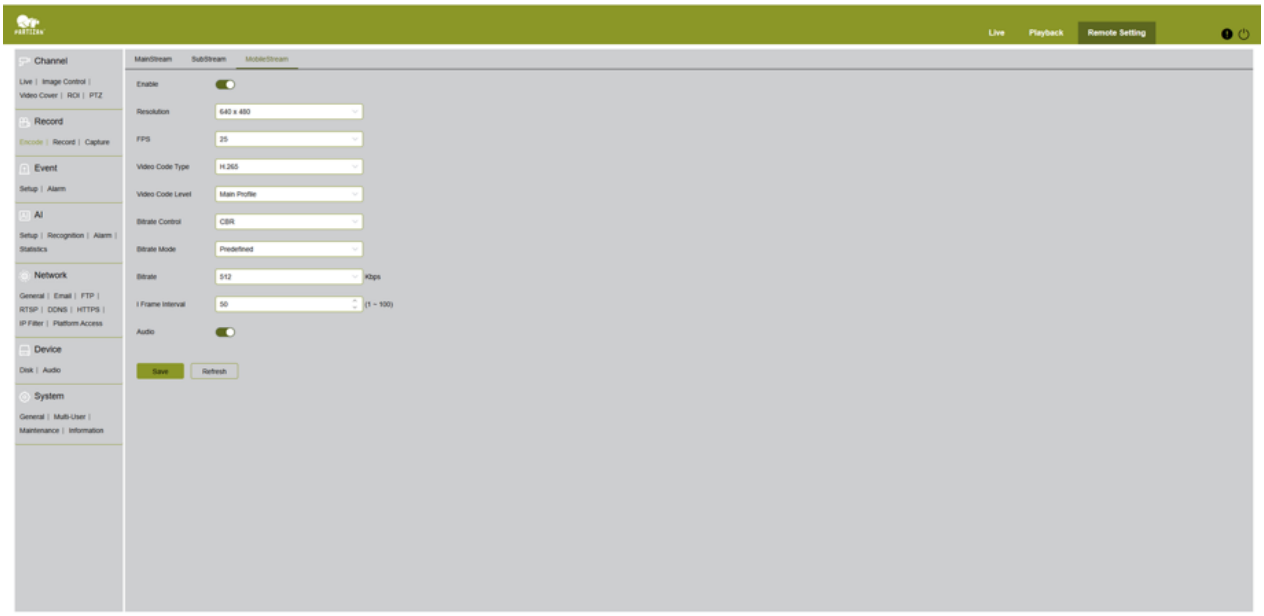

Fig. 25. Record → Encode → Mobile Stream — minimal parameters optimized for mobile devices

Parameter	Description
Resolution	Defines the resolution of the recorded image. Higher resolution requires more storage and bandwidth.
FPS	Defines the frame rate of video recording. Higher FPS produces smoother motion.
Video Code Type	Compression codec: H.264, H.265, H.264+, H.265+, or MJPEG (Sub Stream only). H.265 and H.265+ offer better compression with the same quality.
Video Code Level	Video quality level: Baseline, Main Profile, or High Profile. For H.265, only Main Profile is available.
Bitrate Control	CBR (constant bit rate) is preferred for simple scenes; VBR (variable bit rate) is more efficient for complex or changing scenes.
Bitrate Mode	User-defined: manually enter a specific bitrate. Preset: select from pre-configured bitrate levels.
Bitrate	Data transmission rate (Kbps). Higher bitrate = better image quality, but more storage and bandwidth consumption.

Parameter	Description
I Frame Interval	Sets the keyframe interval. A shorter interval improves seek performance but increases file size.
Audio	Enable to record audio along with video. Requires a connected microphone or a camera with built-in audio.

6.2. Record

6.2.1 Record parameters

This menu allows you to configure general recording parameters for the camera's local storage.

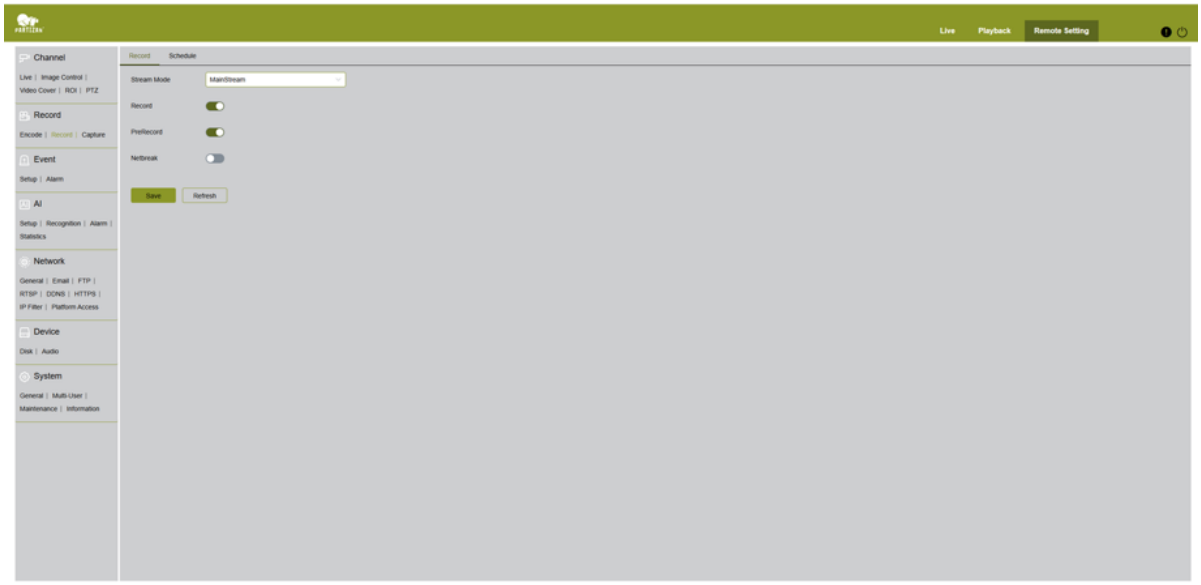

Fig. 26. Record → Record — stream mode, recording toggle, pre-record, and netbreak recovery

Setting	Description
Stream Mode	Select which video stream (Main, Sub, or Mobile) is saved to the SD card. Main Stream is selected by default.
Record	Master switch to enable or disable recording on this channel.
PreRecord	When enabled, the camera buffers a few seconds of video before an alarm event, so the lead-up to the event is included in alarm recordings. Recommended when alarm-triggered recording is the primary mode.
Netbreak	When selected, recording continues even if the network is disconnected or a network failure occurs.

6.2.2 Recording schedule

The recording schedule specifies when the camera records. Video is only recorded within the configured time windows. You can configure up to four recording windows per day using the weekly grid.

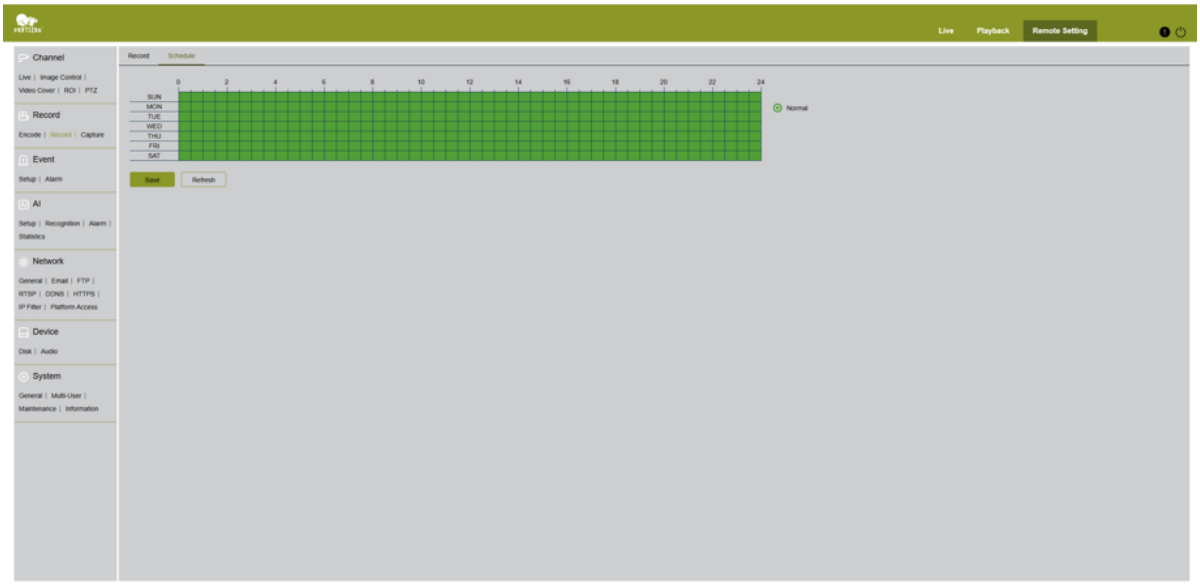

Fig. 27. Record → Schedule — weekly grid showing Normal recording (green) active 24/7 across all days

To modify the schedule, drag the mouse across the grid cells to paint time periods. Color indicates the recording type: green = Normal (continuous recording), yellow = Motion-triggered recording, red = I/O alarm-triggered recording. Uncolored cells = no recording.

6.3. Capture

6.3.1 Capture settings

Configure the intervals for automatic snapshot capture during both normal operation and alarm events.

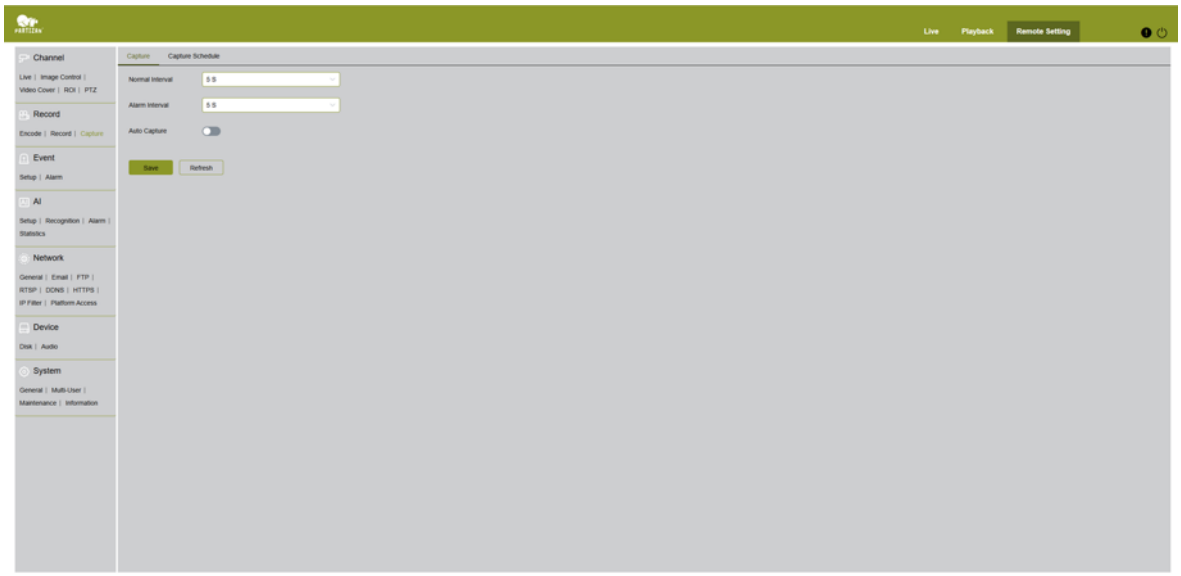

Fig. 28. Record → Capture — normal interval, alarm interval, and auto-capture toggle

Setting	Description
Normal Interval	How often the camera captures snapshots during normal continuous recording (e.g. every 5 seconds).
Alarm Interval	How often the camera captures snapshots when a motion detection, I/O alarm, or PIR alarm is triggered.
Auto Capture	When enabled, the camera automatically captures snapshots at the configured intervals without manual intervention.

6.3.2 Capture schedule

This menu specifies the time windows during which automatic image capture is performed. Capture only occurs within the scheduled periods.

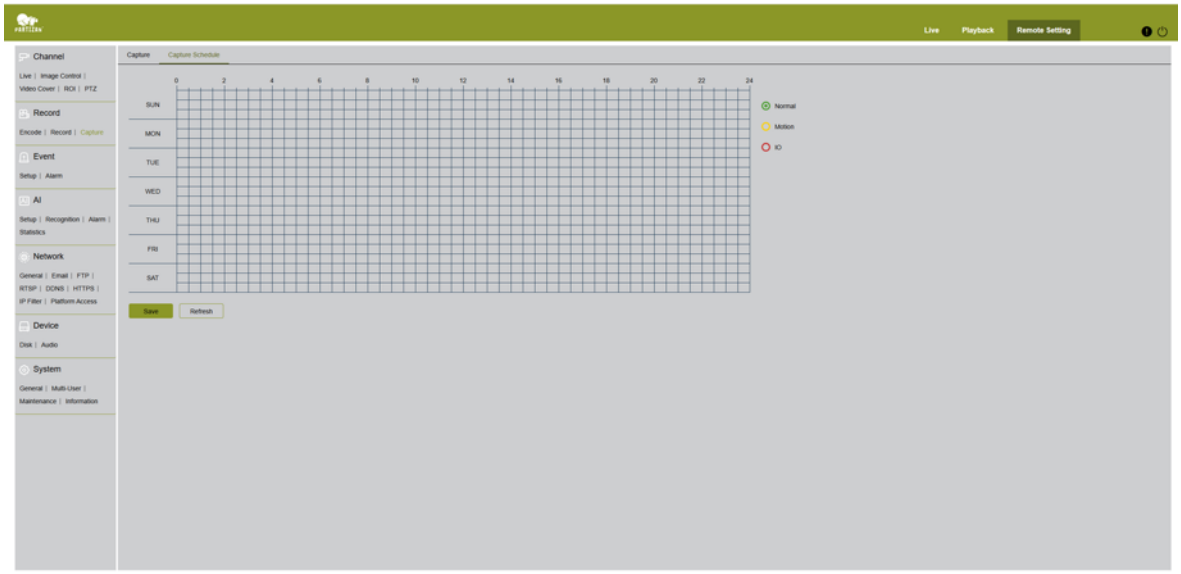

Fig. 29. Record → Capture Schedule — weekly grid with Normal (green), Motion (yellow), and IO (red) capture windows

Schedule grid colors and their meaning:

- Green — Normal capture: the camera captures images at the Normal Interval during this period.
- Yellow — Motion capture: the camera captures images at the Alarm Interval when motion is detected.
- Red — I/O alarm capture: the camera captures images at the Alarm Interval when an external alarm input is triggered.
- Purple — PIR alarm capture: captures when a PIR sensor alarm is triggered.
- Black — No capture: the camera will not capture images during this period.

7. Remote setting → event

7.1. Setup

The Setup tab configures detection sensitivity for three basic event types: Motion, Sound Detection, and Video Tampering.

7.1.1 Motion detection

This menu allows you to configure motion detection parameters. When motion is detected, a series of alarm actions will be triggered (email, FTP upload, alarm recording, etc., as configured in the Alarm tab). You can drag the left mouse button to define the detection area in the right preview window — an alarm will only be triggered when motion is detected within this area.

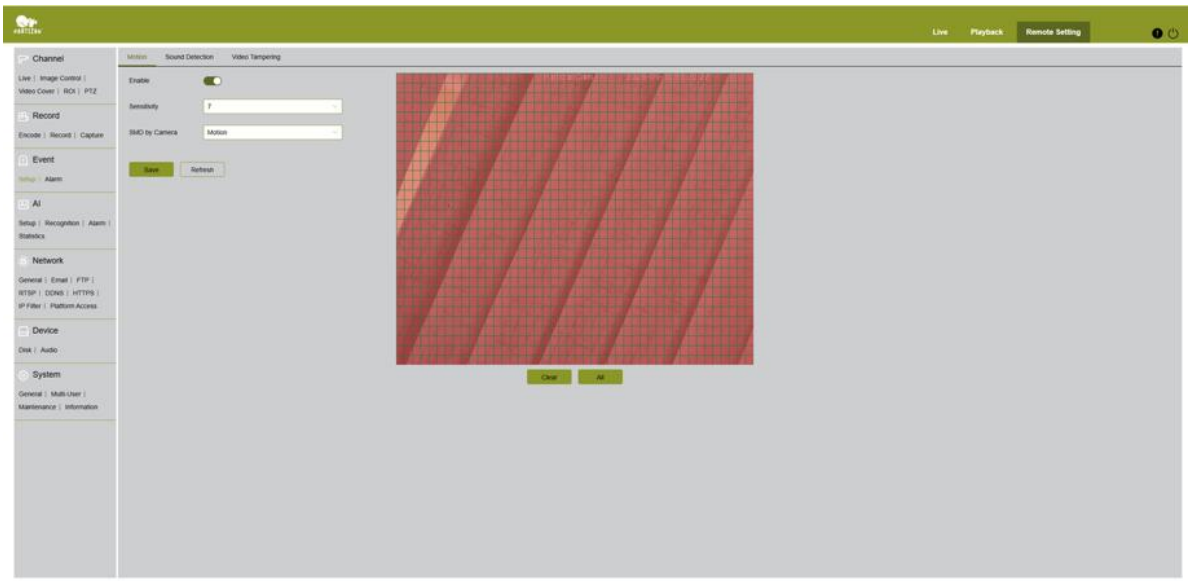

Fig. 30. Event → Setup → Motion — sensitivity, SMD target

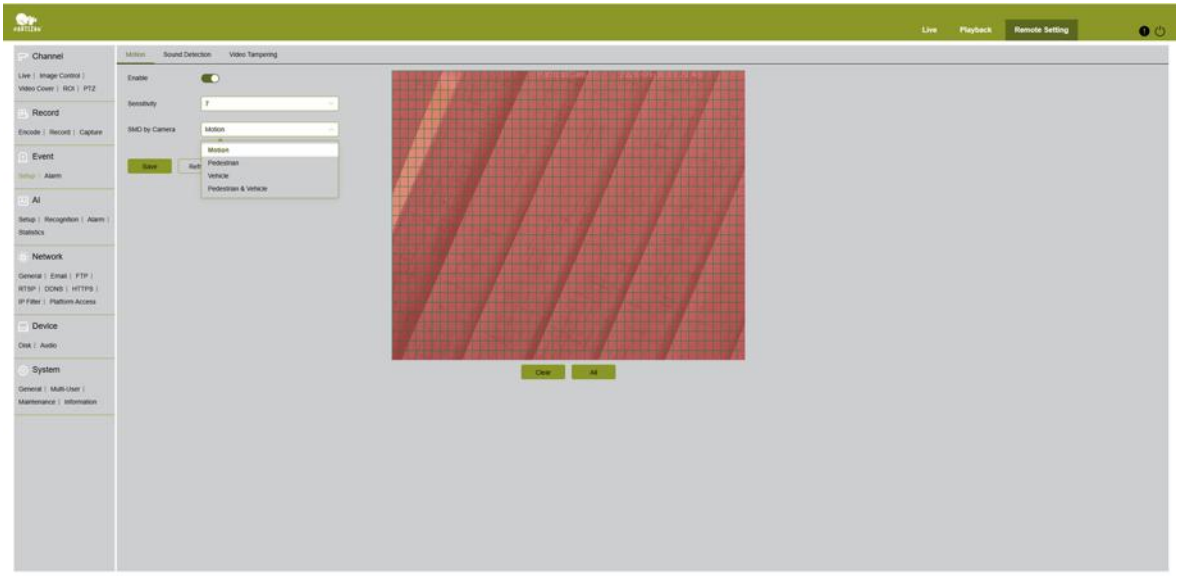

Fig. 31. Event → Setup → Motion — SMD by Camera dropdown: Motion, Pedestrian, Vehicle, Pedestrian & Vehicle

Setting	Description
Enable	Enable or disable motion detection.
Sensitivity	Set the sensitivity of motion detection. Higher values make the camera more responsive to smaller movements.
SMD by Camera	Smart Motion Detection target filter. Options: Motion (all movement), Pedestrian, Vehicle, or Pedestrian & Vehicle. When set to Pedestrian or Vehicle, only human or vehicle movement will trigger the alarm, reducing false alarms from environmental motion such as leaves or shadows.
Detection grid	Drag across the preview grid to define which zones of the frame should trigger motion detection. Clear zones are inactive; green zones are active.

7.1.2 Sound detection

Configures audio-based detection. An alarm is triggered when the camera detects that the connected audio source has changed sharply in volume and the configured threshold is exceeded.

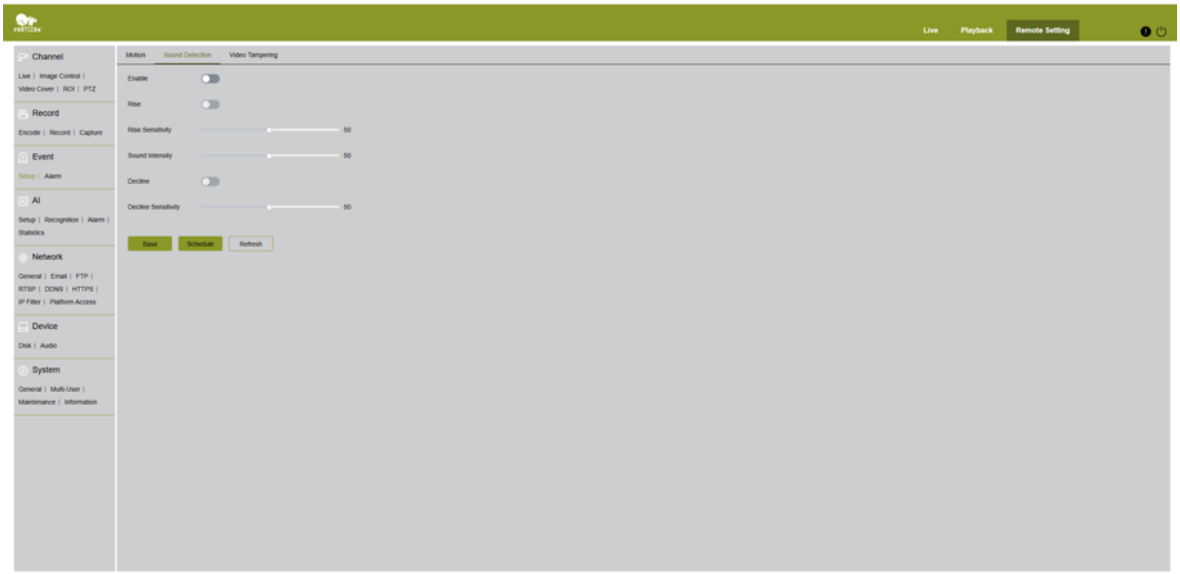

Fig. 32. Event → Setup → Sound Detection — rise/decline sensitivity and sound intensity threshold

Setting	Description
Enable	Enable or disable sound detection.
Rise	Volume rise switch. When enabled, an alarm is triggered only when the volume rises suddenly.
Rise Sensitivity	Sensitivity of volume rise detection. Higher value = easier to trigger.
Sound Intensity	Volume threshold. Larger value requires louder sound to trigger a rise alarm.
Decline	Volume decline switch. When enabled, an alarm is triggered when the volume drops suddenly.

Setting	Description
Decline Sensitivity	Sensitivity of volume decline detection. Higher value = easier to trigger.
Schedule button	Set a timetable for when sound detection is active. Alarms are only triggered within scheduled periods.

7.1.3 Video tampering

Detects physical tampering with the camera — such as the lens being covered, painted, or redirected — and triggers an alarm.

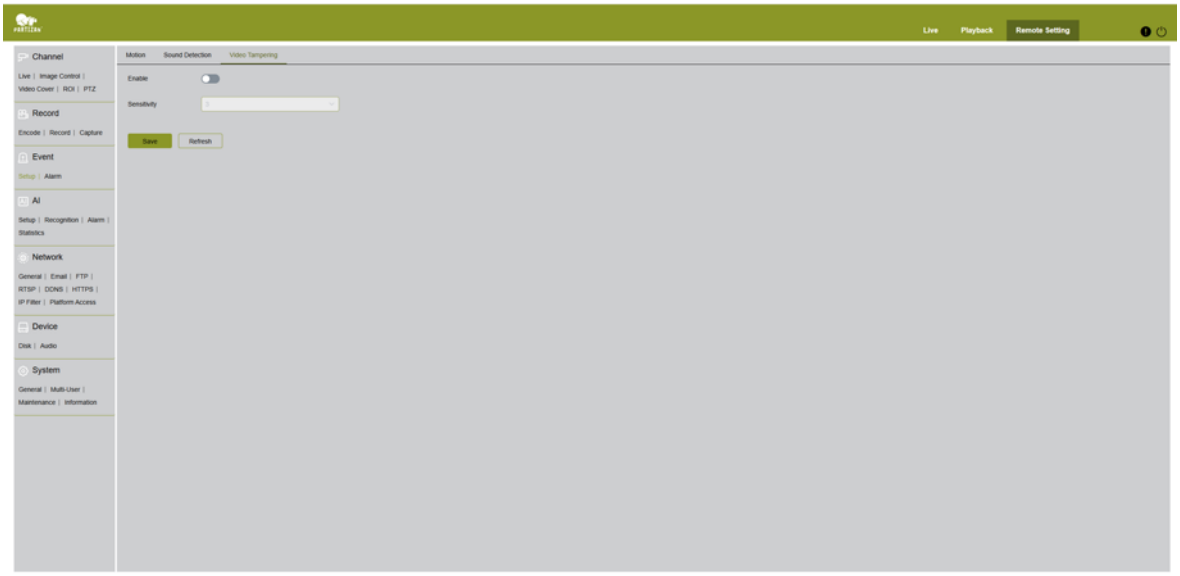

Fig. 33. Event → Setup → Video Tampering — detects camera obstruction or tampering

Setting	Description
Enable	Enable or disable video tampering detection.
Sensitivity	Detection threshold. Higher value = more sensitive to partial occlusion.

Note: Video tampering alarm is supported only on models with this capability. Check your camera's specifications.

7.2. Alarm

The Alarm tab configures the response actions for each event type: Motion, I/O (external alarm input), Sound Detection, and Video Tampering. Each event type shares the same set of response options.

7.2.1 Motion detection alarm

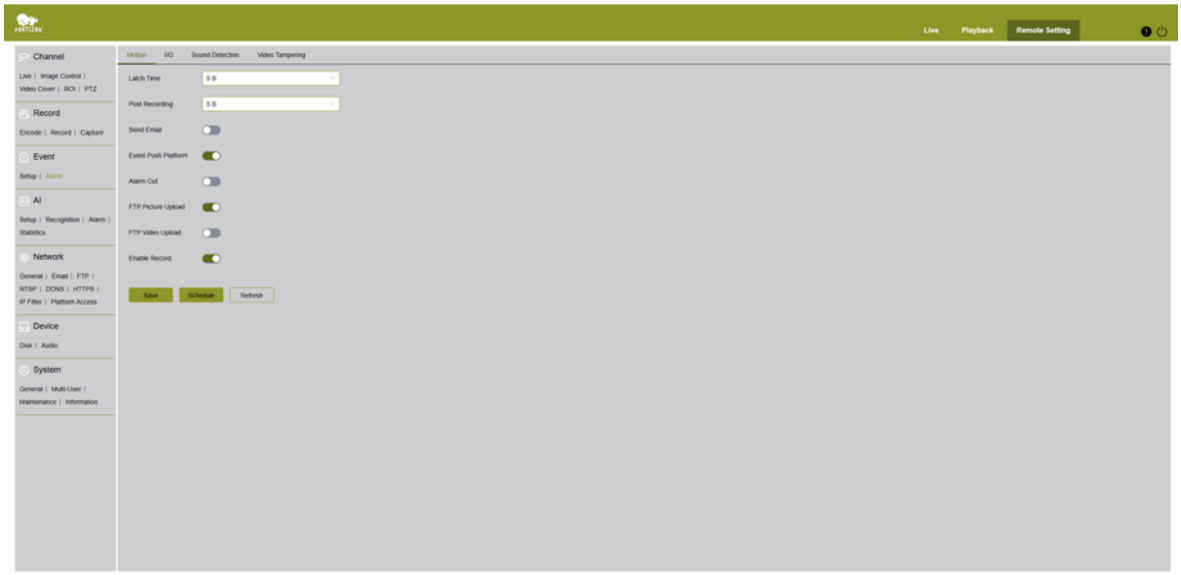

Fig. 34. Event → Alarm → Motion — response actions: email, platform push, alarm out, FTP upload, recording

Action	Description
Latch Time	Duration for which the external alarm output stays active after the alarm is detected.
Post Recording	Duration of continued recording after the alarm event ends. Options: 5s, 10s, 20s, 30s.
Send Email	The device automatically sends an email notification when motion is detected. Requires email configuration in Network → Email.
Event Push Platform	When enabled, alarm event information is pushed to the configured remote platform client in real time.

Action	Description
Alarm Out	Activates the camera's physical relay output to trigger an external alarm device (siren, light, etc.). Only available on models with I/O ports.
FTP Picture Upload	Uploads alarm snapshot images to the configured FTP server.
FTP Video Upload	Uploads alarm video clips to the configured FTP server.
Enable Record	Starts recording when the alarm is triggered. Recording duration is controlled by Post Recording setting.
Schedule button	Configures the time windows during which these alarm actions are active. Actions are only triggered within scheduled periods.

7.2.2 I/O Alarm

This alarm type is only available on camera models that have physical I/O ports and are connected to an external alarm device (door sensor, PIR, panic button, etc.). The alarm type can be configured to match the sensor's behavior — normally open (NO) or normally closed (NC).

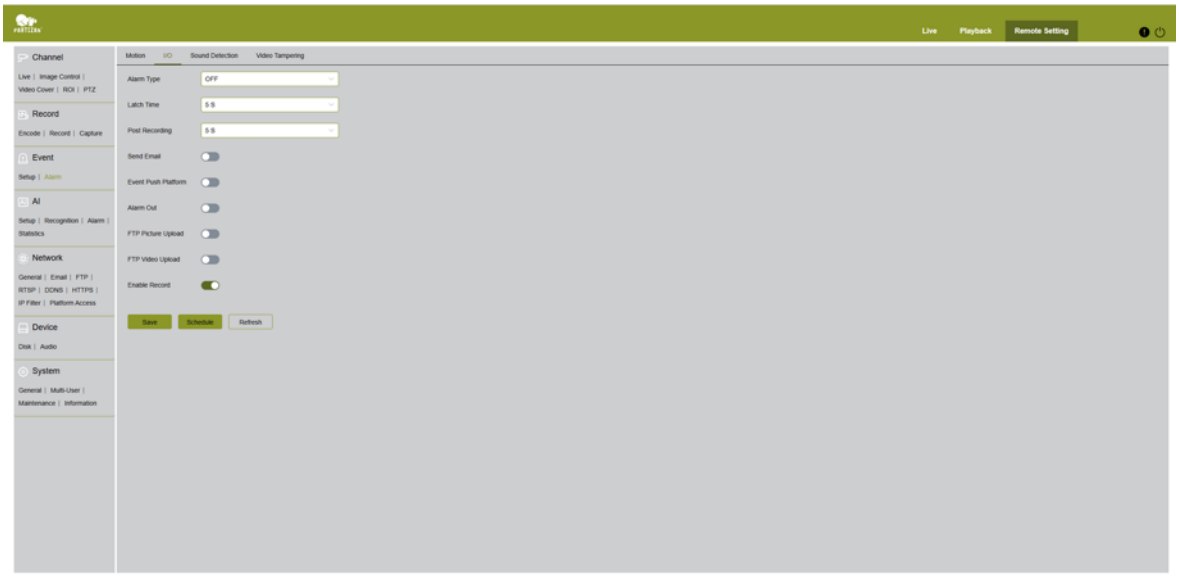

Fig. 35. Event → Alarm → I/O — alarm type (OFF/NO/NC), response action settings

All response options (Latch Time, Post Recording, Send Email, Event Push Platform, Alarm Out, FTP Picture/Video Upload, Enable Record, and Schedule) are identical to those described for Motion Detection above.

7.2.3 Sound detection alarm

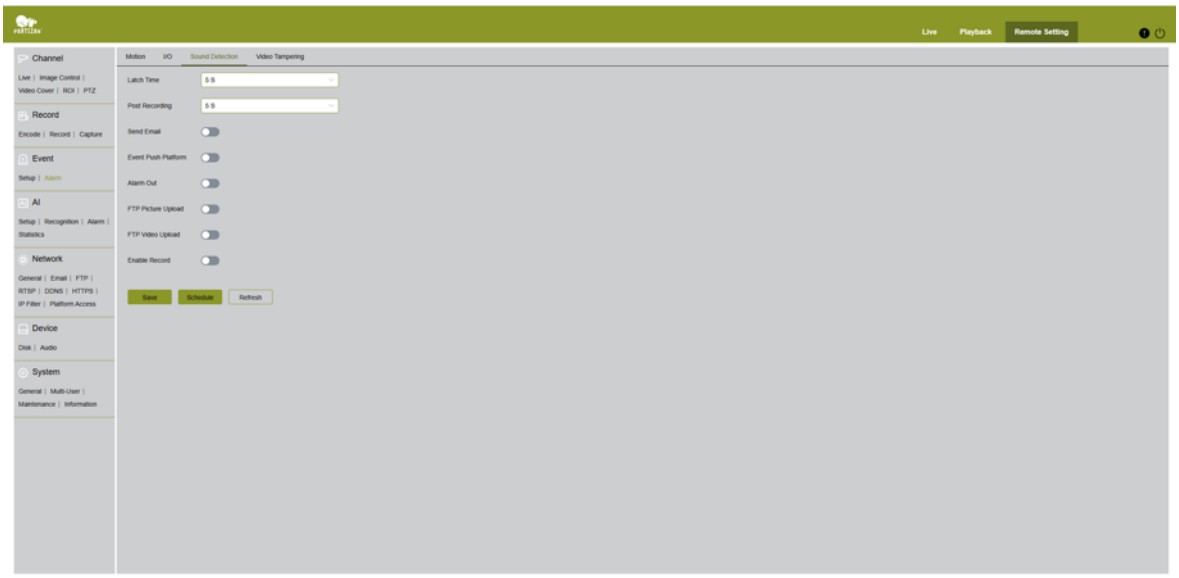

Fig. 36. Event → Alarm → Sound Detection — response actions for audio-detected events

Configures the alarm response when a sound detection event is triggered. All response actions are the same as for Motion Detection (Section 7.2.1). The Schedule button controls when these responses are active.

7.2.4 Video tampering alarm

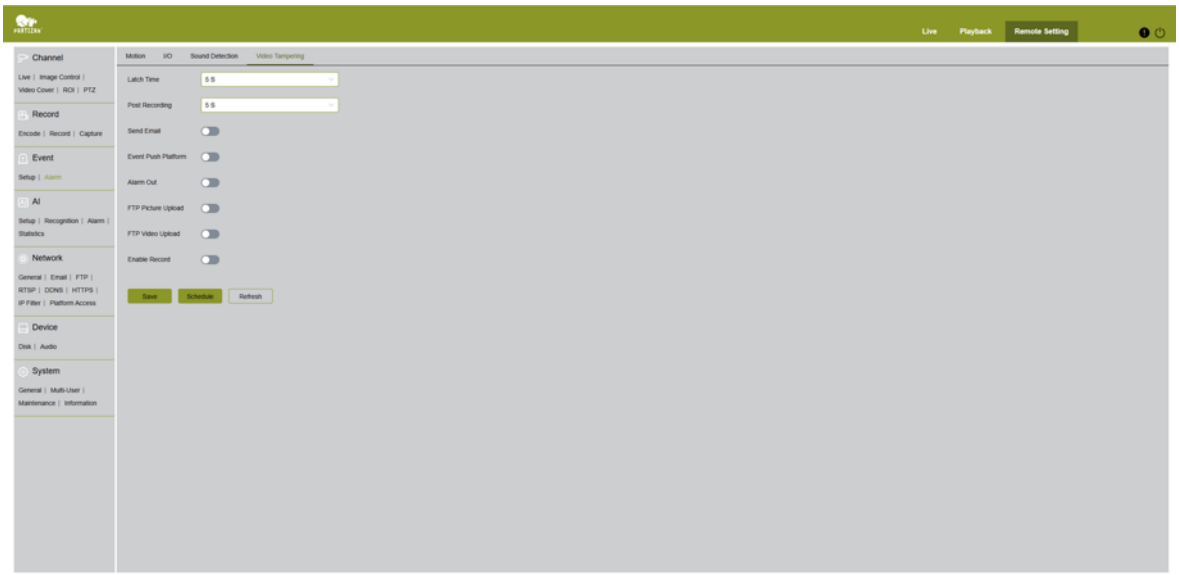

Fig. 37. Event → Alarm → Video Tampering — response actions for camera tampering events

Configures the alarm response when video tampering is detected. All response actions are the same as for Motion Detection (Section 7.2.1). The Schedule button controls when these responses are active.

8. Remote setting → ai

The AI section is the most comprehensive part of the camera's configuration. It is organized into four sub-menus: Setup (enabling and tuning each AI analytic), Recognition (database management for face and license plate matching), Alarm (response actions for each AI event type), and Statistics (reporting and spatial/temporal analysis).

To use the AI alarm functions, you must first enable the corresponding function in the Setup menu. Note that enabling multiple AI functions simultaneously consumes additional processing power. Due to hardware limitations, some functions are mutually exclusive and cannot be enabled at the same time.

8.1. AI → setup

Setup contains tabs for each supported AI analytic. Most share a similar structure: an Enable toggle, sensitivity, minimum/maximum pixel size for the detection target, a detection area drawn directly on the live preview, and rule-based configuration for line/region-based features.

8.1.1 Face detection

Face detection captures images of faces detected in the scene and stores them with metadata to the SD card. The camera can apply face feature recognition (age, gender, mask, glasses, expression) and push notifications on detection events.

Fig. 38. AI → Setup → Face Detection — snap mode, apply mode, pixel range, detection mode, and trigger mode

Setting	Description
Enable	Enable or disable face detection.
Face Features	Enables recognition of facial attributes: age, gender, mask, glasses, expression, etc. Requires Face Features to be enabled in AI → Alarm for the relevant group.
Snap Mode	Optimal Mode: pushes the single best image per detection event. RealTime Mode: pushes immediately on detection, then again when the person leaves. Interval Mode: pushes at a configurable interval and count.
Apply Mode	Frontal View: only pushes images of people facing the camera. Multi Angle: includes side-face images. Customize: define acceptable roll, pitch, and yaw angle ranges.
Min Pixel / Max Pixel	Based on 1080p resolution — filter out faces smaller or larger than the set pixel dimensions. Default: 64×64 to 640×640.
Detection Mode	Hybrid Mode: detects all faces in the frame. Motion Mode: filters out motionless faces (e.g. portraits, statues).
Trigger Mode	Rectangle: detects faces in the defined area. Line: only triggers detection when a person crosses the detection line.
Detection Area	Full Screen: detects everywhere. User-defined: detects only within the drawn polygon area.

8.1.2 Pedestrian & vehicle

Detects and classifies pedestrians (humans on foot) and vehicles (motor vehicles and non-motorized vehicles) in the scene. Generates alarm events and capture images. Useful for access control, traffic monitoring, and perimeter security.

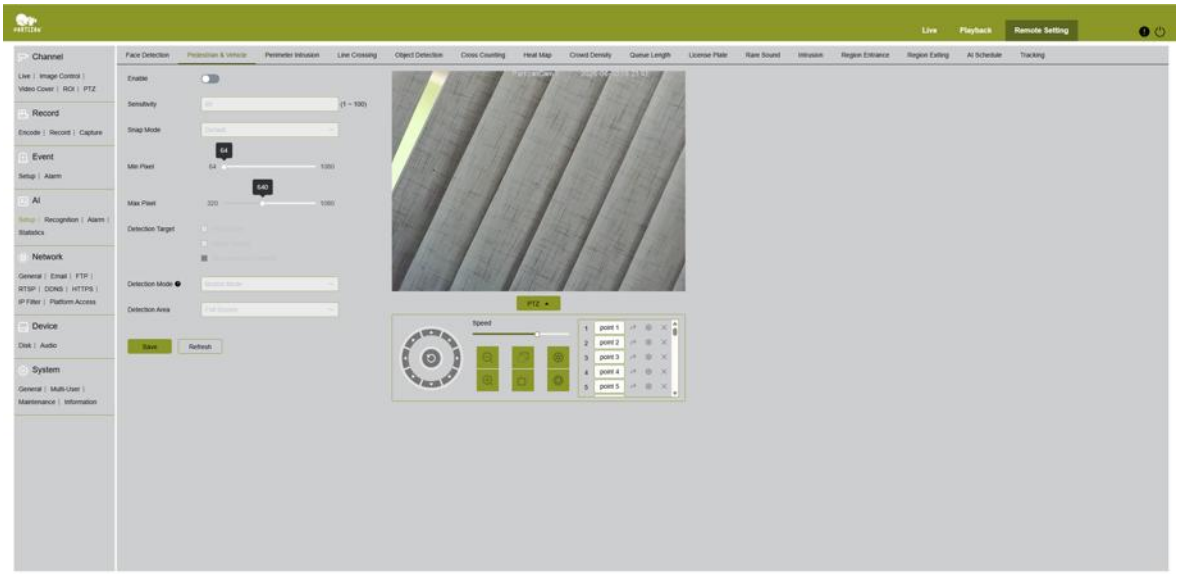

Fig. 39. AI → Setup → Pedestrian & Vehicle — sensitivity, pixel range, and detection target

Setting	Description
Sensitivity	Higher sensitivity = smaller objects can be detected, but may increase false alarms.
Snap Mode	Default: one image per detection event. RealTime Mode: immediate image + image on departure. Interval Mode: images at a configured interval.
Min Pixel / Max Pixel	Filter out pedestrian or vehicle objects that are smaller or larger than the set pixel dimensions.
Detection Target	Pedestrian, Motor Vehicle, Non-motorized Vehicle, or all.
Detection Mode	Hybrid Mode: all pedestrians/vehicles in view. Motion Mode: filters out stationary targets.
Detection Range	Full Screen or User-defined polygon area.

8.1.3 Perimeter intrusion

Detects when a specific object enters or exits a defined warning zone drawn as a line or polygon on the camera view. An alarm is triggered based on the configured crossing direction rule.

Fig. 40. AI → Setup → Perimeter Intrusion — draw a perimeter line on the preview and set rule direction (A→B)

Setting	Description
Enable	Enable or disable perimeter intrusion detection.
Sensitivity	Filters small disturbing objects. Higher sensitivity detects smaller targets.
Detection Target	Pedestrian, Motor Vehicle, or Non-motorized Vehicle — select which object types trigger the alarm.
Rule Number	Select the active rule (up to 4 independent rules supported).
Rule Enable	Each rule has its own enable switch, independently associated with the selected Rule Number.
Rule Type	A→B: alarm when object crosses from A side to B side. B→A: the reverse. A↔B: both directions.
Rule Line Setting Area	Draw and view rule lines directly on the camera preview. Use Delete / Delete All to clear rules.

8.1.4 Line crossing

Line Crossing detection triggers an alarm when a specific object crosses a predefined virtual line in the camera's field of view. Unlike Perimeter Intrusion (zone-based), Line Crossing is purely boundary-based.

Fig. 41. AI → Setup → Line Crossing — target validity, pixel range, and crossing rule

Setting	Description
Sensitivity	Related to the percentage of the target that enters the detection area. Higher sensitivity triggers on partial entry.
Target Validity	Similarity between the detection target and the configured type. 1 = 80%+ similarity, 2 = 60%+, 3 = 40%+.
Min Pixel / Max Pixel	Filter targets outside the configured pixel size range.
Detection Target	Pedestrian, Motor Vehicle, or Non-motorized Vehicle.
Rule Number / Enable / Type	Configure up to 4 crossing rules; each rule has its own enable switch and A→B / B→A / A↔B direction setting.

8.1.5 Object detection

Object Detection (also called SOD — Stationary Object Detection) triggers an alarm when an item is left behind (abandoned) or removed from the monitored scene. Useful for detecting unattended luggage, asset removal, or theft.

Fig. 42. AI → Setup → Object Detection — detects abandoned or removed objects within a defined rule area

Setting	Description
Enable	Enable or disable object detection.
Sensitivity	Filters small disturbing objects. Higher sensitivity detects smaller items.
Rule Number / Enable	Configure up to 4 independent detection rules.
Rule Type	Legacy: detects general changes. Left: triggers when an item is left behind. Lost: triggers when an item is removed.

8.1.6 Cross counting

Cross Counting (CC) records the number of specific objects crossing a defined virtual line. Useful for footfall counting at entrances, exits, or checkpoints. Supports daily reset and alarm trigger when a count threshold is exceeded.

Fig. 43. AI → Setup → Cross Counting — counts crossings by target type, with start/end time and reset option

Setting	Description
Enable	Enable or disable cross counting.
Detection Target	Motion (all objects), Pedestrian, Motor Vehicle, or Non-motorized Vehicle.
Alarm Number	Triggers an alarm when the in-count minus out-count (or vice versa) reaches this value. Range: 1–255.
Start Time / End Time	Daily time window during which cross counting is active.
Rule Type	A→B increments the in-count; B→A increments the out-count (or vice versa depending on rule direction).
Reset Count button	Clears the current displayed count manually.

8.1.7 Heat map

Heat Map tracks people activity distribution in the monitored area over time. It can generate a spatial heat map showing which areas of the frame have the most activity (red = highest, blue = lowest), or a temporal heat map showing activity levels across time.

Fig. 44. AI → Setup → Heat Map — enables spatial activity density tracking for the selected rule region

Setting	Description
Enable	Enable or disable heat map data collection.
Rule Number / Enable	One detection rule line is supported for heat map. Enable to activate data collection in the defined area.
Monitoring Area	By default, the full screen is monitored. The monitoring area defines where heat data is collected.

Note: The camera must have an SD card with available free space to store heat map data.

8.1.8 Crowd density

Crowd Density detection counts the number of people (by head detection) in a defined area and triggers an alarm when the count exceeds the configured maximum.

Fig. 45. AI → Setup → Crowd Density — user-defined detection area and maximum detection count

Setting	Description
Enable	Enable or disable crowd density detection.
Sensitivity	Higher sensitivity detects smaller/more distant heads.
Min Pixel / Max Pixel	Filter out heads smaller or larger than the configured pixel size.
Max Detection Number	Maximum number of heads in the detection area before an alarm is triggered. Range: 1–500.
Detection Area	Full Screen or User-defined polygon (3–8 vertices).

8.1.9 Queue length

Queue Length detection monitors the number of people waiting in a defined queue area and triggers an alarm when the queue is too long or the wait time exceeds a threshold. Useful for managing checkout lines, service counters, or ticket booths.

Fig. 46. AI → Setup → Queue Length — max detection number and maximum processing time

Setting	Description
Enable	Enable or disable queue length detection.
Max Detection Number	Maximum number of people in the queue area before an alarm is triggered. Range: 1–100.
Max Pro Time	Maximum duration a person is allowed to stay in the detection area (seconds). Range: 1–3600. An alarm is triggered when this is exceeded.
Detection Range	Full Screen or User-defined polygon area.

Note: Counting restarts only when a target leaves the detection area. If a target disappears suddenly (e.g., camera occlusion), counting is paused. Counting does not restart if a target reappears in the same area.

8.1.10 License plate

License plate detection captures license plates of passing vehicles and can check them against a database of registered/blocked plates. Currently, the license plate detection function is only available for European and American regions.

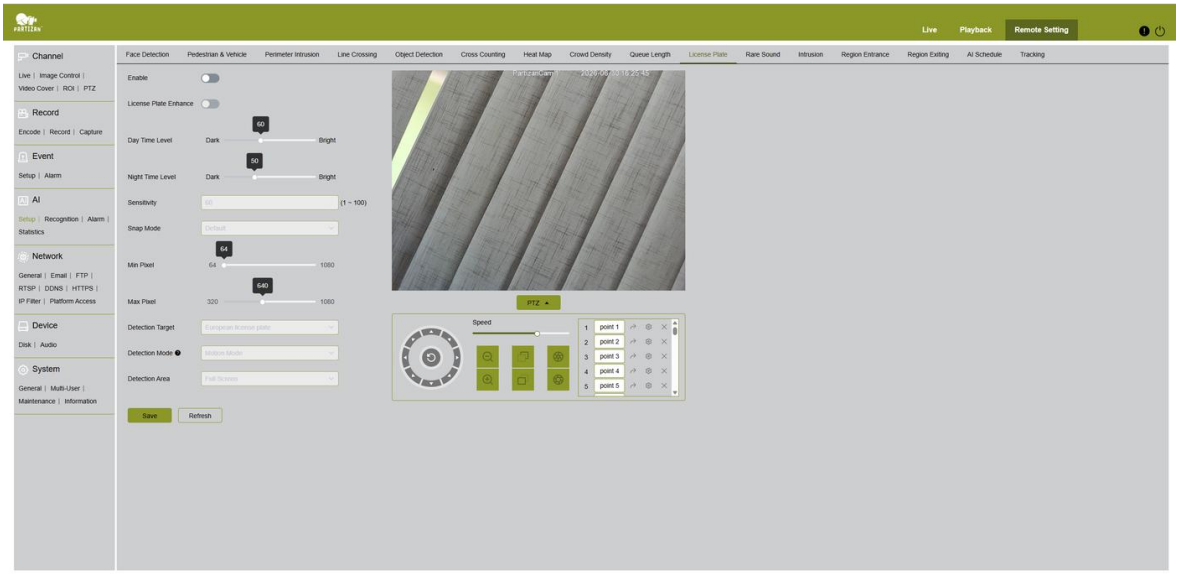

Fig. 47. AI → Setup → License Plate — day/night brightness levels, plate region (e.g. European), and detection mode

Setting	Description
Enable	Enable or disable license plate detection.
License Plate Enhance	Enables specialized image processing optimized for plate legibility. Mutually exclusive with WDR, HLC, and BLC.
Day Time Level / Night Time Level	Adjust image brightness for better plate readability in daytime and nighttime conditions.
Detection Target	European license plate or American license plate.
Detection Mode	Hybrid Mode: detects static plates in view. Motion Mode: filters out stationary vehicles, detects only moving plates.
Detection Area	Full Screen or User-defined area.

8.1.11 Rare sound

Rare Sound detection recognizes specific unusual sound events in the environment — such as a baby crying, a dog barking, or a gunshot — and triggers an alarm when detected.

Fig. 48. AI → Setup → Rare Sound — sensitivity and detection target (Crying, Dog Barking, Gunshot)

Setting	Description
Enable	Enable or disable rare sound detection.
Sensitivity	Detection sensitivity from 1 (minimum) to 100 (maximum).
Detection Target	Select which sound types to detect: Baby Crying Sound, Dog Barking, and/or Gunshot. Multiple types can be enabled simultaneously.

8.1.12 Intrusion

Intrusion detection triggers an alarm when an object enters a defined restricted area and stays there for longer than the configured time threshold. Unlike Region Entrance (which triggers immediately on entry), Intrusion allows a grace period before alarming.

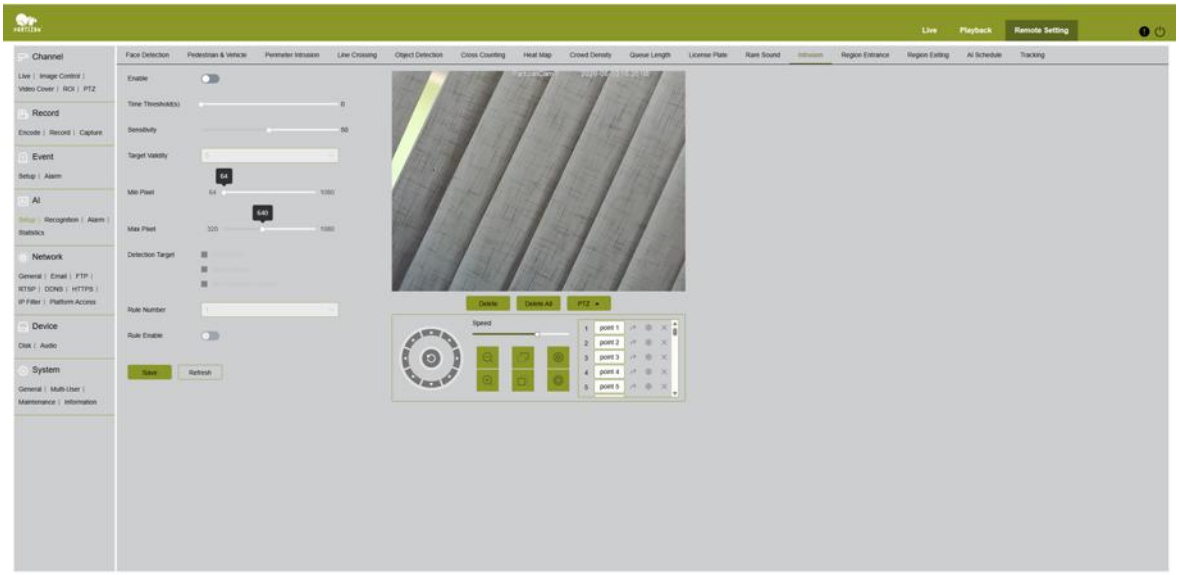

Fig. 49. AI → Setup → Intrusion — time threshold, sensitivity, target validity, and rule region

Setting	Description
Enable	Enable or disable intrusion detection.
Time Threshold (s)	Alarm is triggered only after the target has stayed in the alert area continuously for this many seconds. For example, if set to 2s, the alarm will trigger only when the target stays for 2 seconds or more.
Sensitivity	Related to the percentage of the target that enters the area. Higher sensitivity triggers on partial entry.
Target Validity	Similarity between detection target and configured type: 1 = 80%+, 2 = 60%+, 3 = 40%+.
Detection Target	Pedestrian, Motor Vehicle, or Non-motorized Vehicle.

Setting	Description
Rule Number / Enable	Up to 4 independent detection rules, each with its own enable switch.
Rule Line Setting Area	Draw the restricted zone as a polygon (3–8 vertices) directly on the camera preview.

8.1.13 Region entrance

Region Entrance detection triggers an alarm when a target enters the guarded area from outside. Targets that are already present in the area when the function is enabled are not detected. Only newly entering objects trigger alarms.

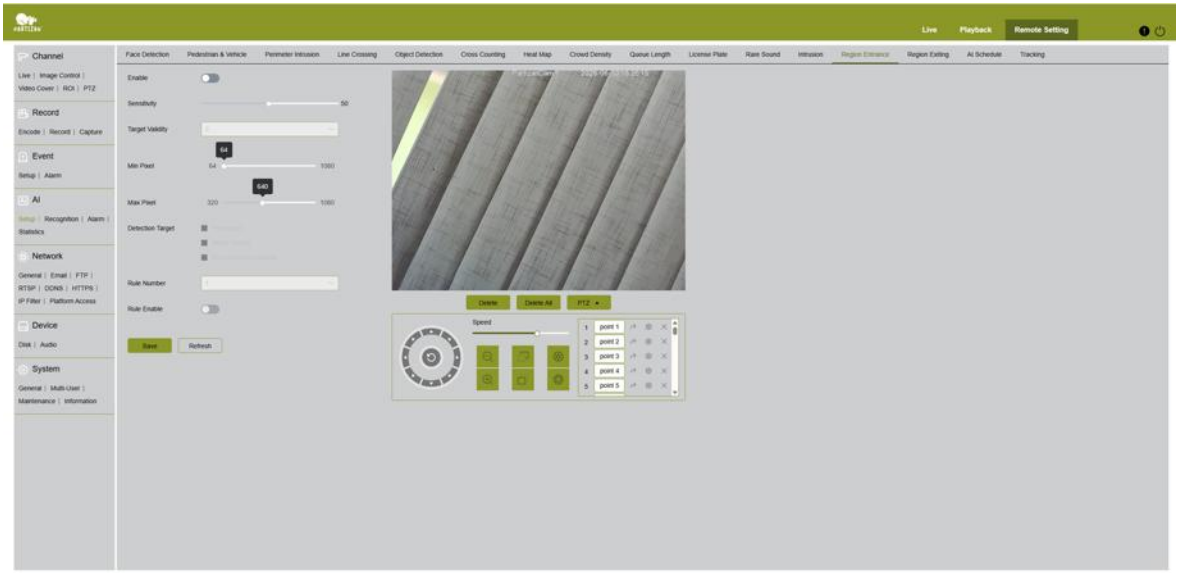

Fig. 50. AI → Setup → Region Entrance — detects targets entering a defined region

Setting	Description
Enable	Enable or disable Region Entrance detection.
Sensitivity	Higher sensitivity triggers on smaller portions of the target entering the area.
Target Validity	Similarity threshold: 1 = 80%+, 2 = 60%+, 3 = 40%+.
Detection Target	Pedestrian, Motor Vehicle, or Non-motorized Vehicle.
Rule Number / Enable	Up to 4 independent detection rules.
Rule Line Setting Area	Draw the guarded entrance zone as a polygon (3–8 vertices) on the camera preview.

8.1.14 Region exiting

Region Exiting detection triggers an alarm when a target moves from inside the guarded area to outside. Targets generated outside the area that never entered are not detected.

Fig. 51. AI → Setup → Region Exiting — sensitivity, target validity, pixel range, detection target, and rule area

Configuration is identical to Region Entrance (Section 8.1.13) — the same parameters apply: Enable, Sensitivity, Target Validity, Min/Max Pixel, Detection Target, Rule Number, and Rule Line Setting Area.

8.1.15 AI schedule

The AI Schedule function allows you to control when each AI analytic is active by defining a weekly time schedule. When enabled, all AI function switches are controlled by the schedule and cannot be manually toggled outside of it.

Fig. 52. AI → Setup → AI Schedule — weekly schedule grid for controlling AI function active periods

Setting	Description
Enable	Enable or disable the AI schedule. When enabled, AI functions are only active during scheduled periods.
Functions (mutually exclusive)	When an AI schedule is configured, the interface displays which functions are mutually exclusive to each other. Two mutually exclusive AI functions cannot be active at the same time.

Note: When setting up Face Detection schedules for the first time, the user will be prompted to review and agree to the face privacy agreement.

8.1.16 Tracking

Automatic PTZ tracking allows the camera to follow a detected target (pedestrian or vehicle) by controlling the pan-tilt-zoom motors. This function is only available on PTZ-capable camera models.

Fig. 53. AI → Setup → Tracking — tracking configuration for PTZ-capable models

8.2. AI → recognition

The Recognition sub-menu is intended for managing the Face Database and License Plate Database — the reference data used for matching detected faces and license plates against known entries. The camera supports up to 16 database groups, each with Allow List, Block List, or neutral policy.

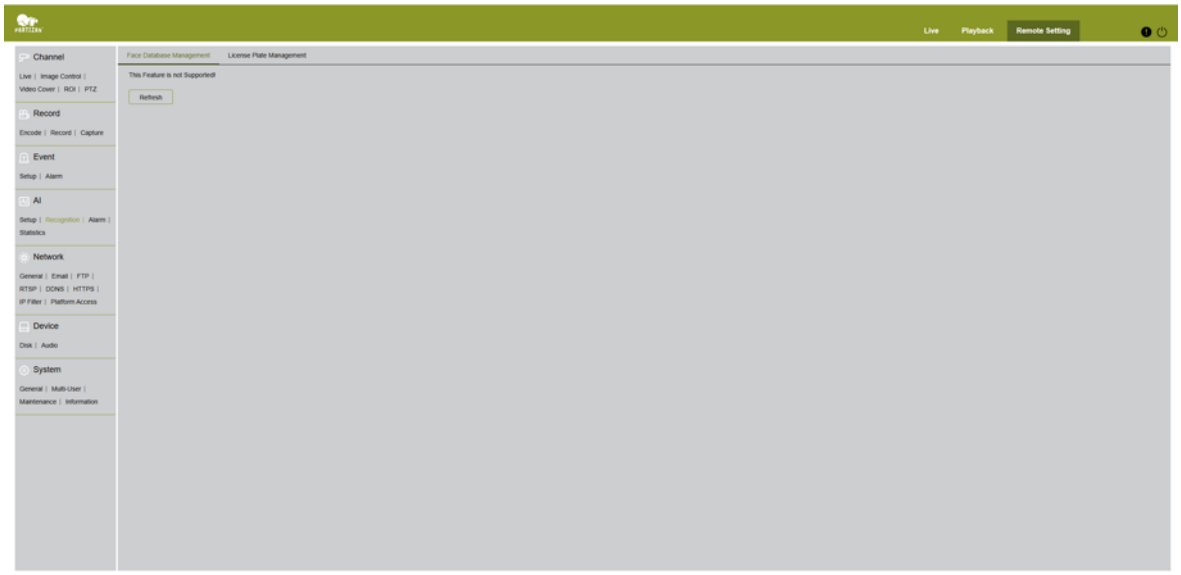

Fig. 54. AI → Recognition → Face Database Management — 'This Feature is not Supported' on this camera model

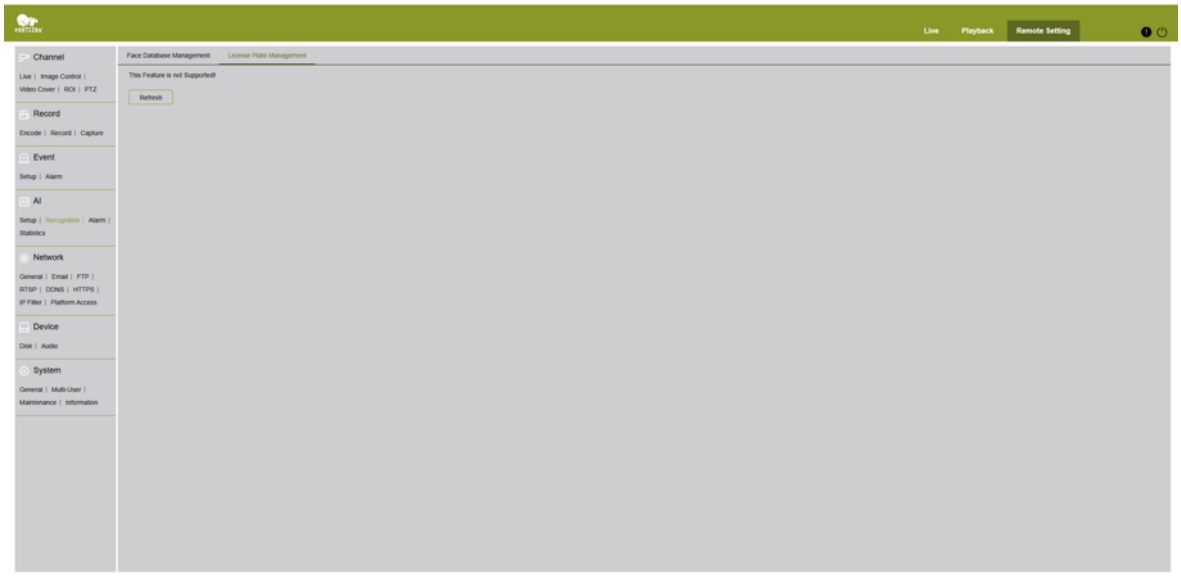

Fig. 55. AI → Recognition → License Plate Management — 'This Feature is not Supported' on this camera model

Note: On the IPS-230X-IR Starlight SH camera model used to generate this manual, both Face Database Management and License Plate Management are reported as not supported. On models where this feature is supported, the interface allows adding, editing, grouping, and exporting face/plate reference data.

8.3. AI → alarm

The Alarm sub-menu configures the camera's response actions for each AI analytic event type. There are 18 tabs, one for each supported AI function. All tabs share the same set of response actions described below — only the specific event trigger differs per tab.

AI alarm responses fall into three categories:

Category I — Direct alarm response (Face Detection, Face Features, Pedestrian & Vehicle, Perimeter Intrusion, Line Crossing, Object Detection, Cross Counting, Crowd Density, Queue Length, License Plate, Rare Sound, Intrusion, Region Entrance, Region Exiting): the camera captures an alarm image and directly triggers the configured response actions when the event is detected.

Category II — Database-matched response (Face Recognition, License Plate Recognition): the camera first matches the detected face/plate against the database, then triggers the response based on the matched group's policy.

Category III — Scheduled report (Face Attendance): the camera automatically searches face matching data at configured intervals and generates attendance reports sent by email.

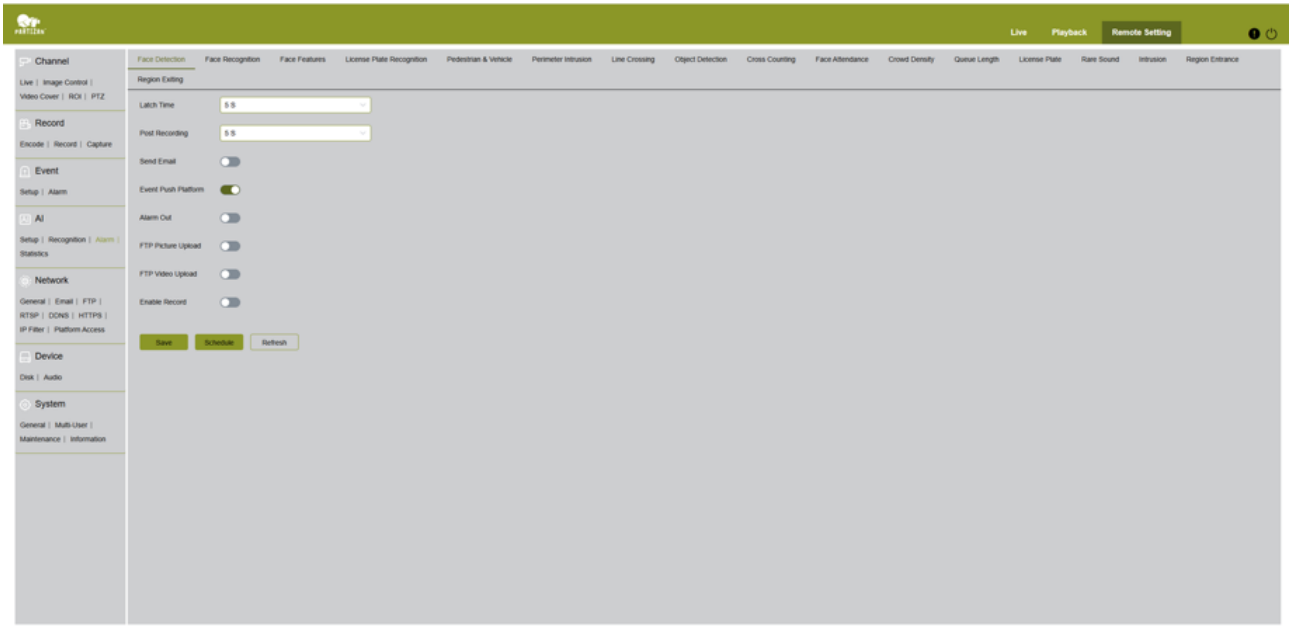

Fig. 56. AI → Alarm — response actions available for every AI event type (shown: Face Detection)

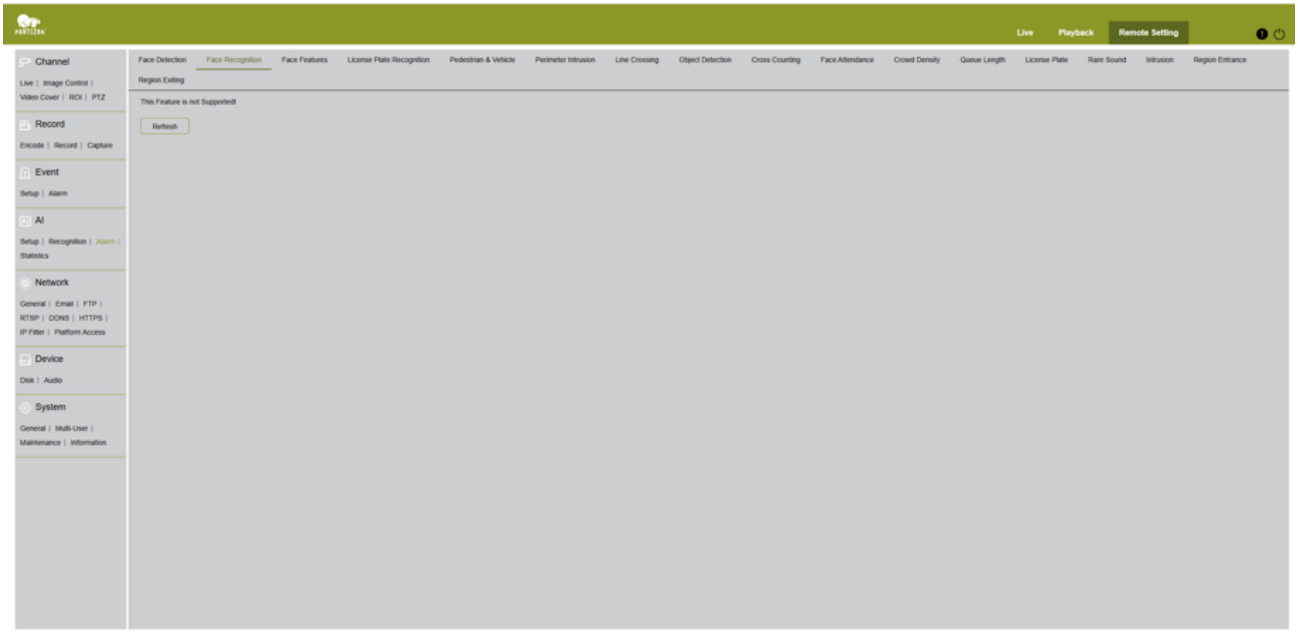

Fig. 57. AI → Alarm → Face Recognition — group-based alarm policy, similarity threshold, and response settings

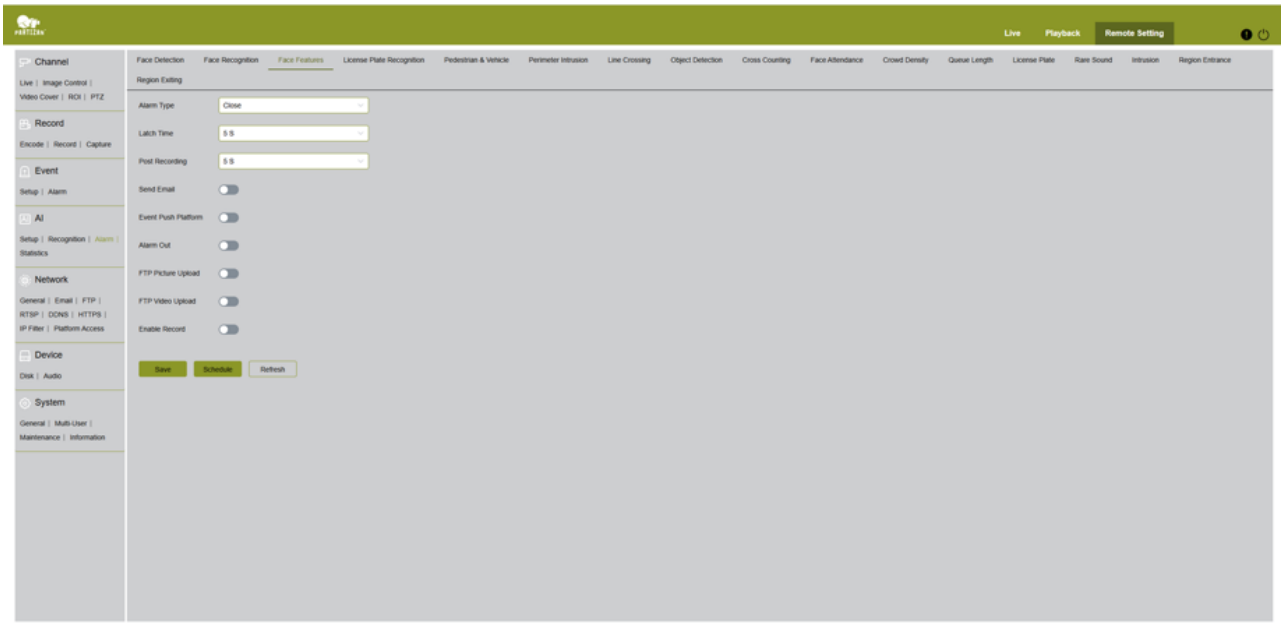

Fig. 58. AI → Alarm → Face Features — alarm type filter (No Mask / Wear Mask) for face attribute alarms

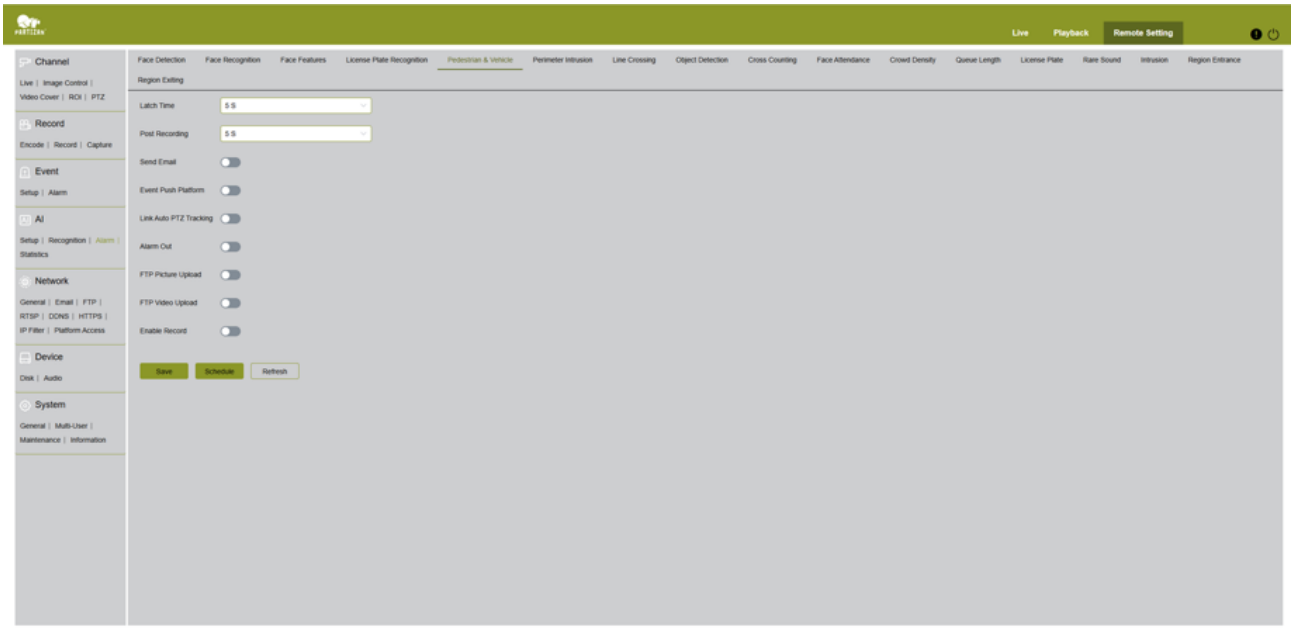

Fig. 59. AI → Alarm → License Plate Recognition — alarm response settings for plate database matches

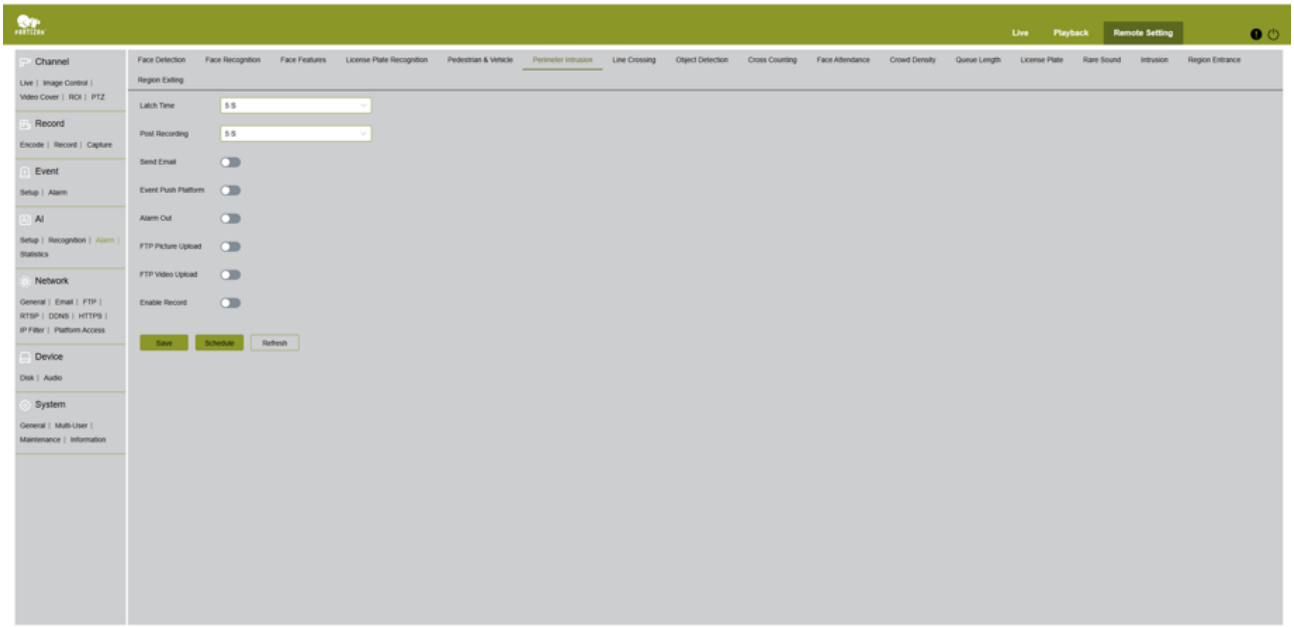

Fig. 60. AI → Alarm → Pedestrian & Vehicle — standard alarm response settings

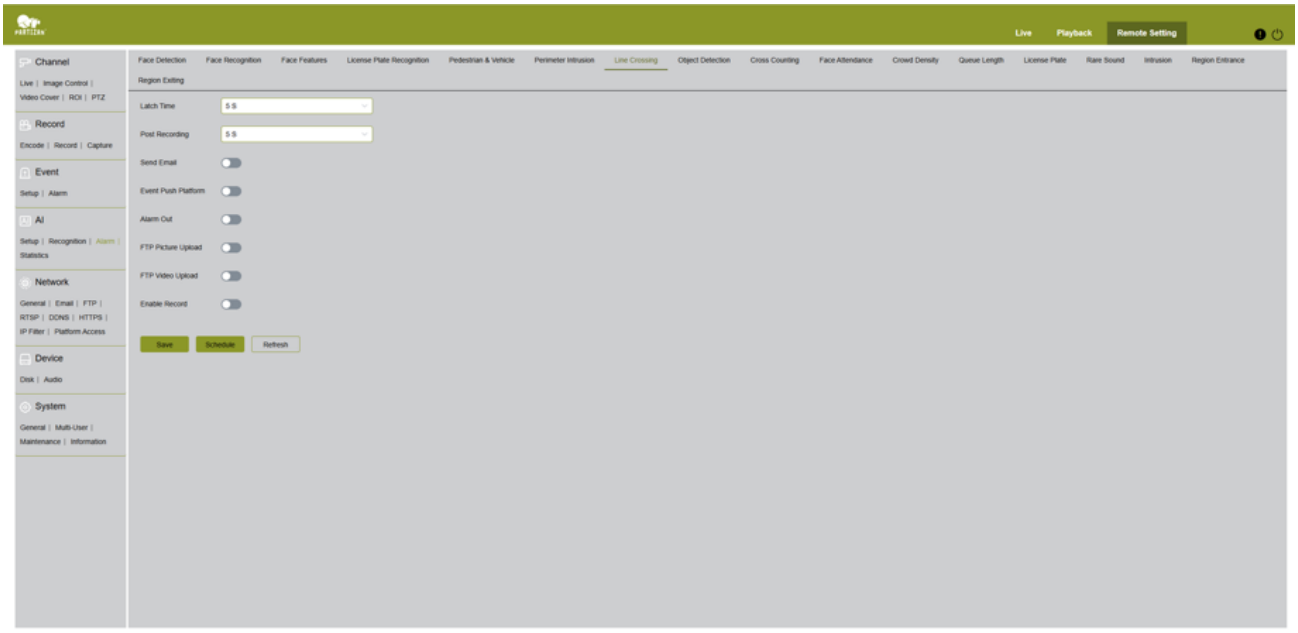

Fig. 61. AI → Alarm → Perimeter Intrusion — standard alarm response settings

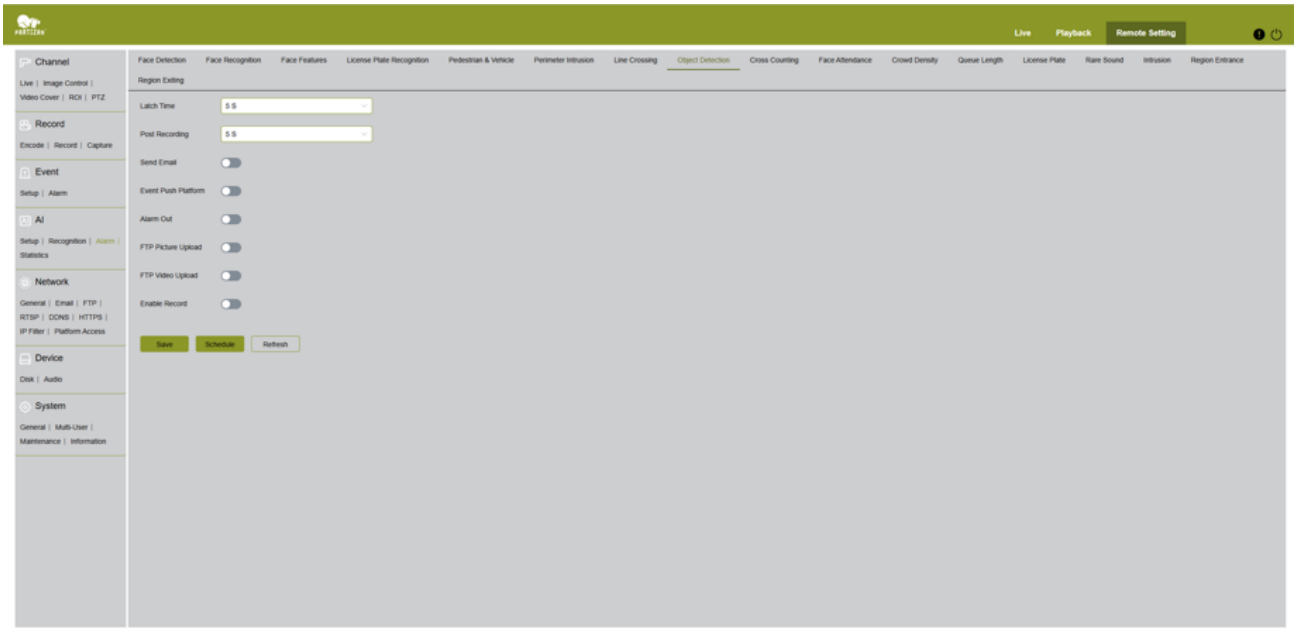

Fig. 62. AI → Alarm → Line Crossing — standard alarm response settings

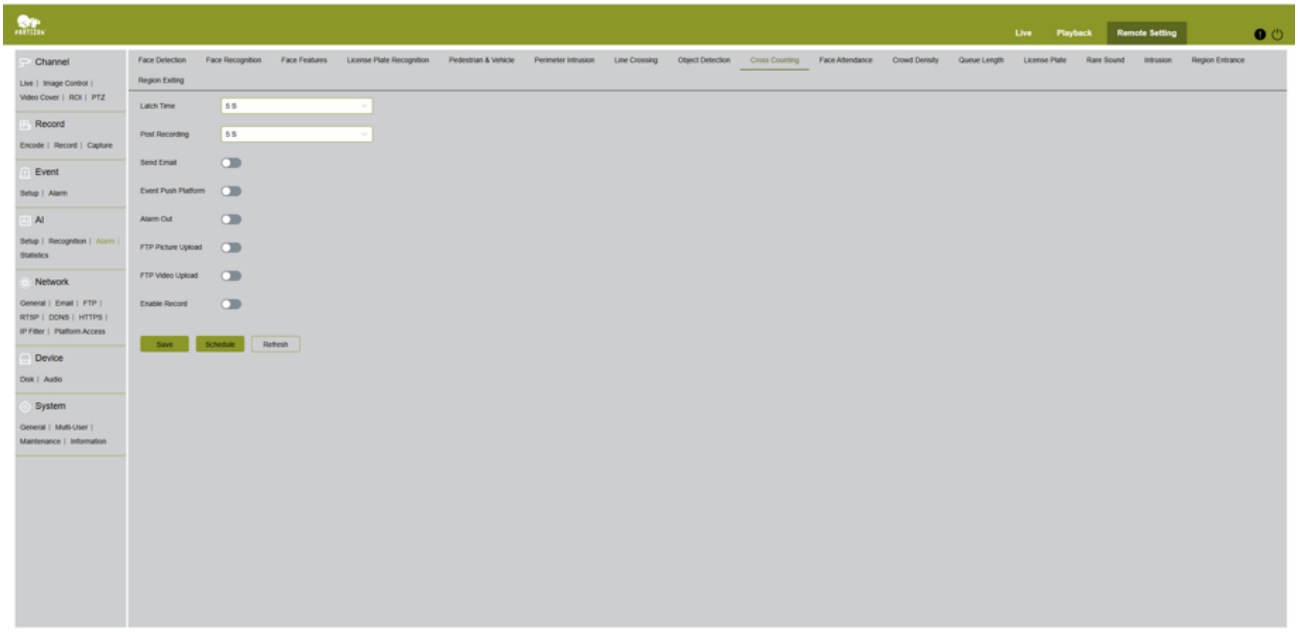

Fig. 63. AI → Alarm → Object Detection — standard alarm response settings

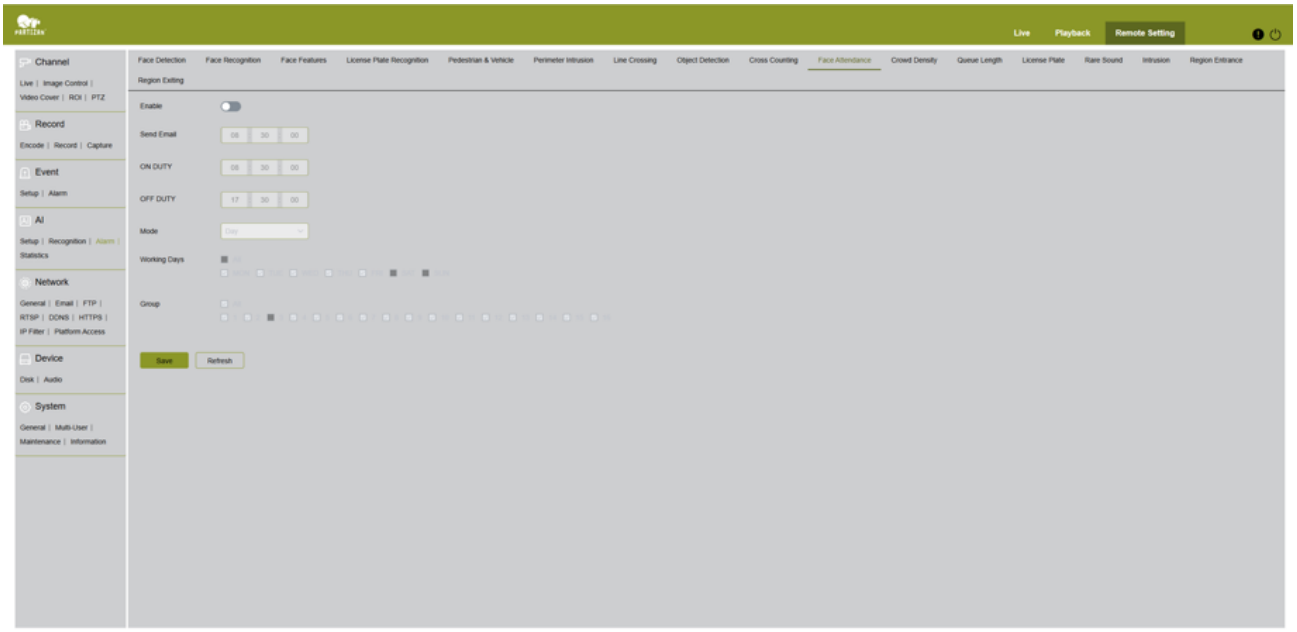

Fig. 64. AI → Alarm → Cross Counting — standard alarm response settings

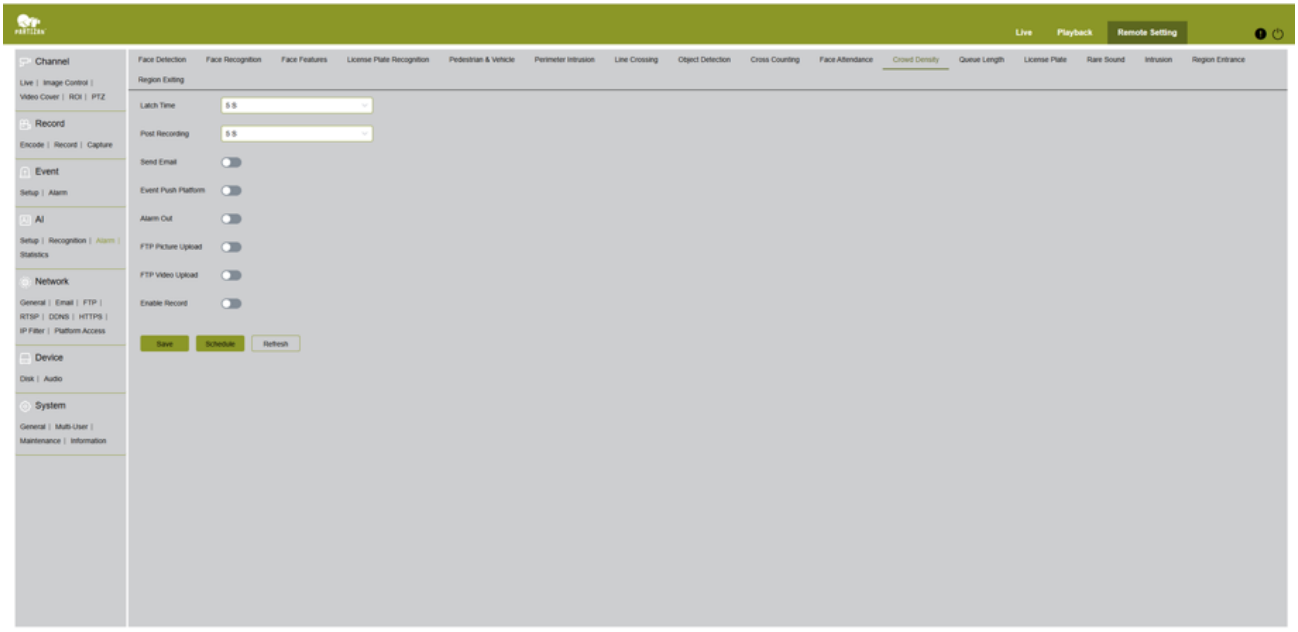

Fig. 65. AI → Alarm → Face Attendance — email schedule for automatic attendance report generation

Fig. 66. AI → Alarm → Crowd Density — standard alarm response settings

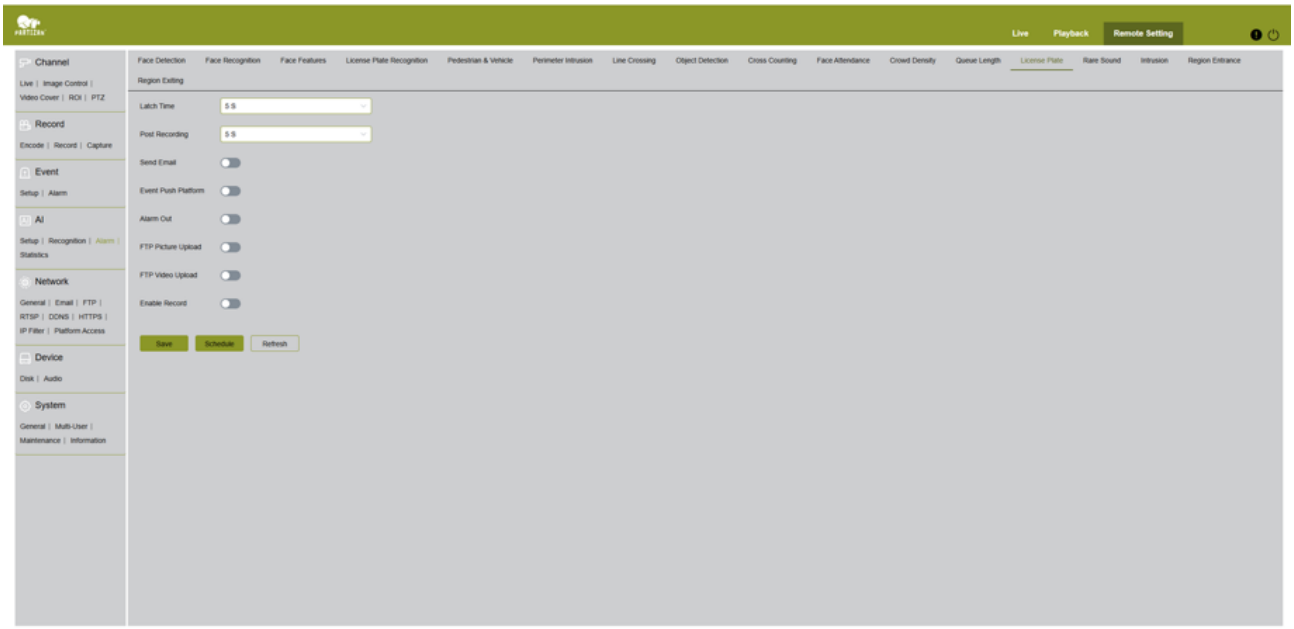

Fig. 67. AI → Alarm → Queue Length — standard alarm response settings

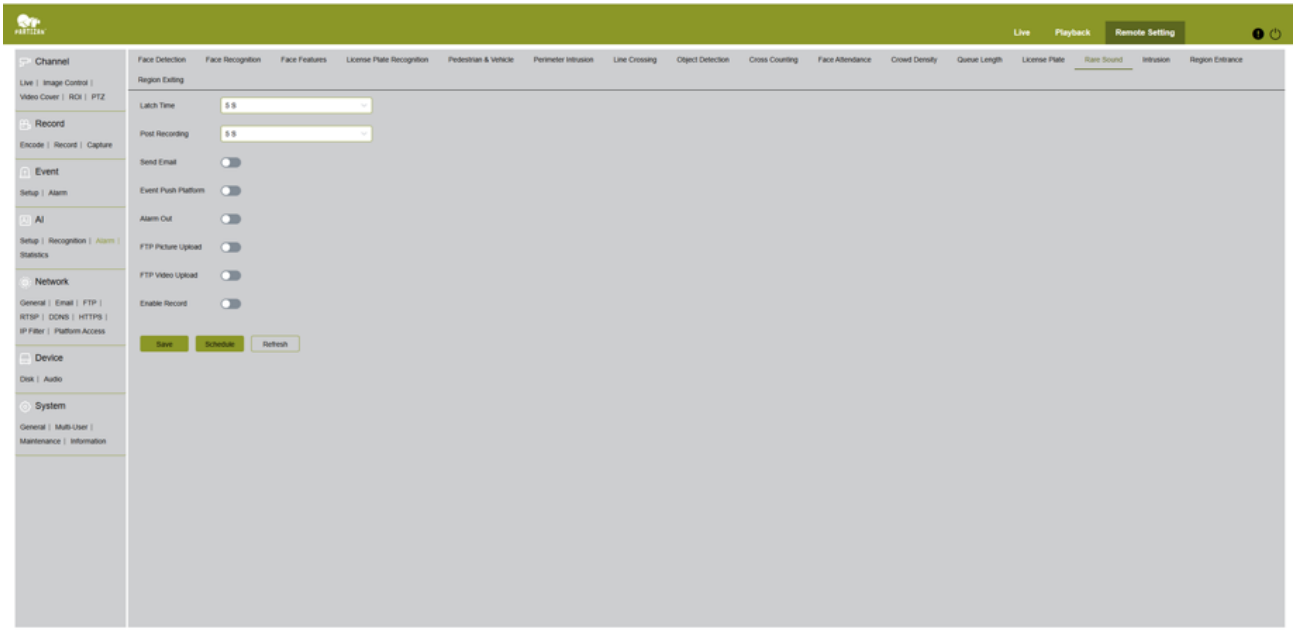

Fig. 68. AI → Alarm → License Plate — standard alarm response settings

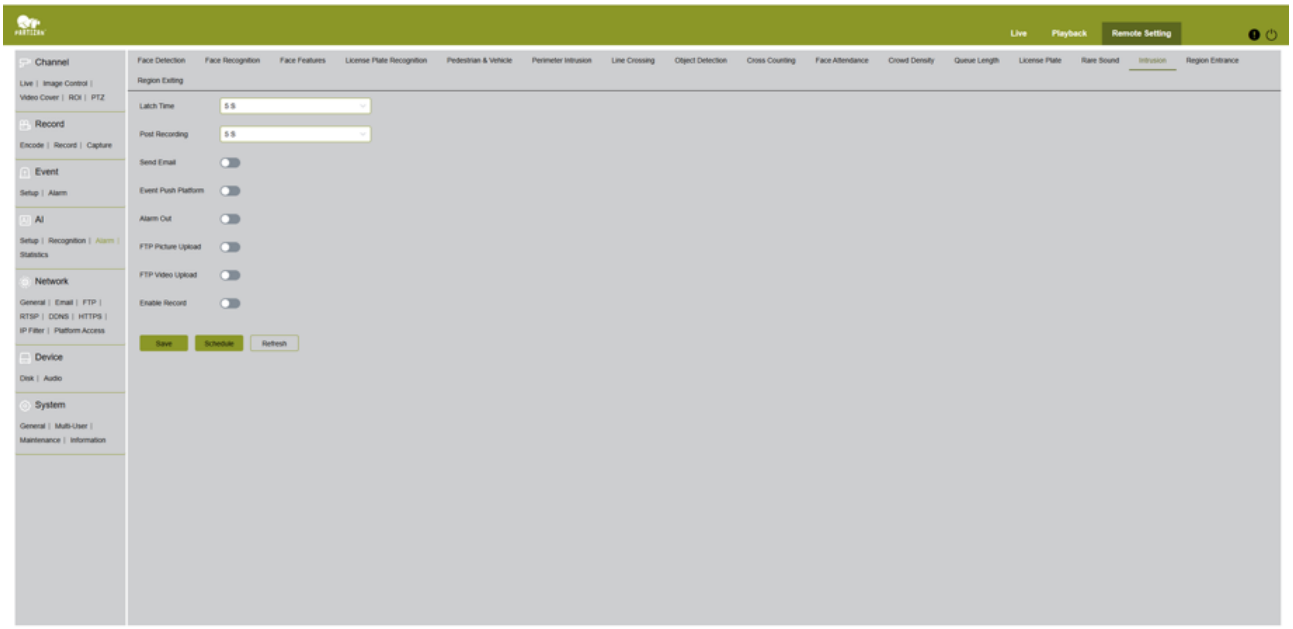

Fig. 69. AI → Alarm → Rare Sound — standard alarm response settings

Fig. 70. AI → Alarm → Intrusion — standard alarm response settings

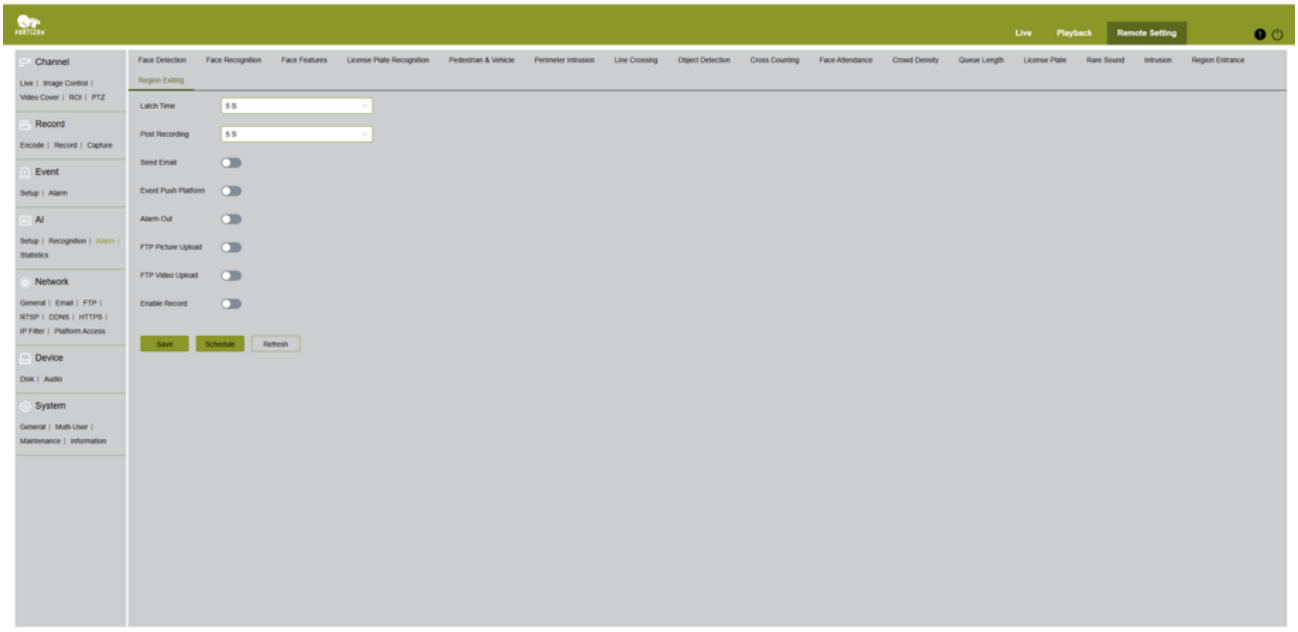

Fig. 71. AI → Alarm → Region Exiting — standard alarm response settings (last tab)

Response Action	Description
Latch Time	Duration the external alarm output (relay) remains active after the alarm event is detected. Controlled by schedule.
Post Recording	Duration of continued recording after the alarm event clears. Controlled by schedule.
Send Email	Sends an email notification when the alarm is triggered. Controlled by schedule; requires Network → Email configuration.
Event Push Platform	Pushes event data to the configured remote platform client in real time when an alarm is triggered.
Alarm Out	Activates the physical relay alarm output. Controlled by schedule. Camera must support I/O feature.
FTP Picture Upload	Uploads alarm snapshots to the configured FTP server. Controlled by schedule; FTP must be configured in advance.
FTP Video Upload	Uploads alarm video clips to the configured FTP server. Controlled by schedule; FTP must be configured in advance.

Response Action	Description
Enable Record	Enables post-event recording when the alarm is triggered. Duration is controlled by Post Recording setting.
Schedule button	Configures the time windows controlling all alarm response actions above.

8.4. AI → statistics

Statistics provides AI-driven reporting and data visualization, generating daily, weekly, monthly, quarterly, or annual reports for supported analytic types.

8.4.1 Face recognition

Retrieves face data statistics stored on the SD card according to the configured search settings. Useful for analyzing visitor patterns or attendance trends over time.

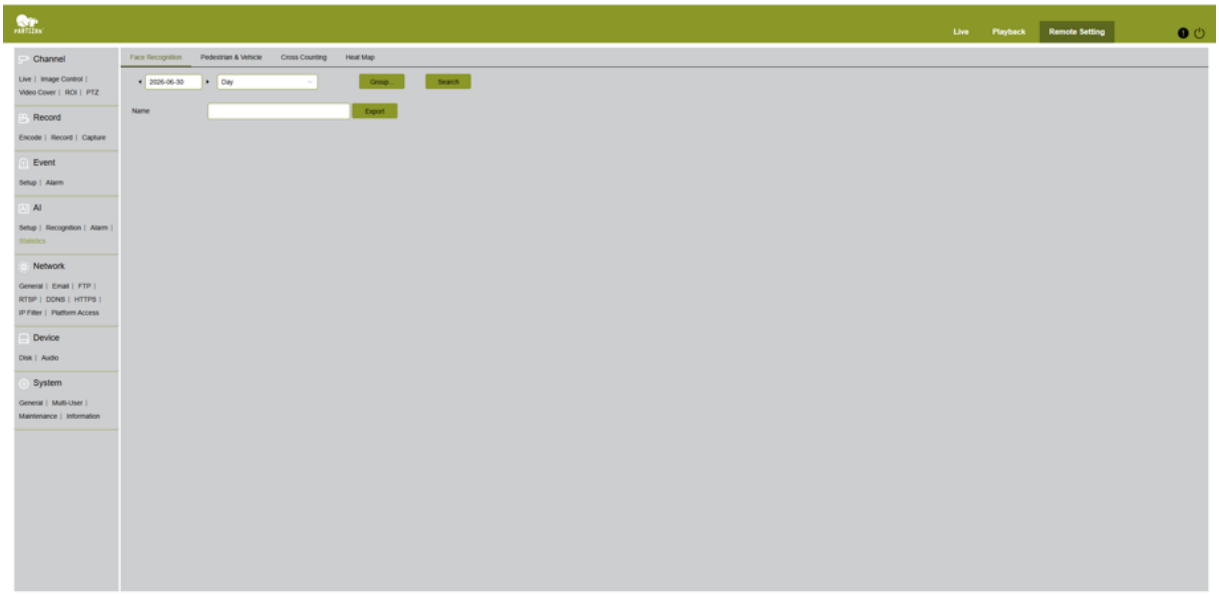

Fig. 72. AI → Statistics → Face Recognition — date range, grouping, and export

Setting / Control	Description
Time	Reference date for the selected search mode.
Search Mode	Day, Week, Month, Quarter, or Year — sets the time range for data retrieval.
Group	Filter retrieved data by database group.
Search	Initiates data retrieval according to current settings.
Export	Exports the current search results to an Excel file. Enter a filename before clicking Export.

8.4.2 Pedestrian & vehicle

Retrieves pedestrian and vehicle count statistics, including events from Perimeter Intrusion, Line Crossing, Intrusion, Region Entrance, and Region Exiting functions — all categorized by target type.

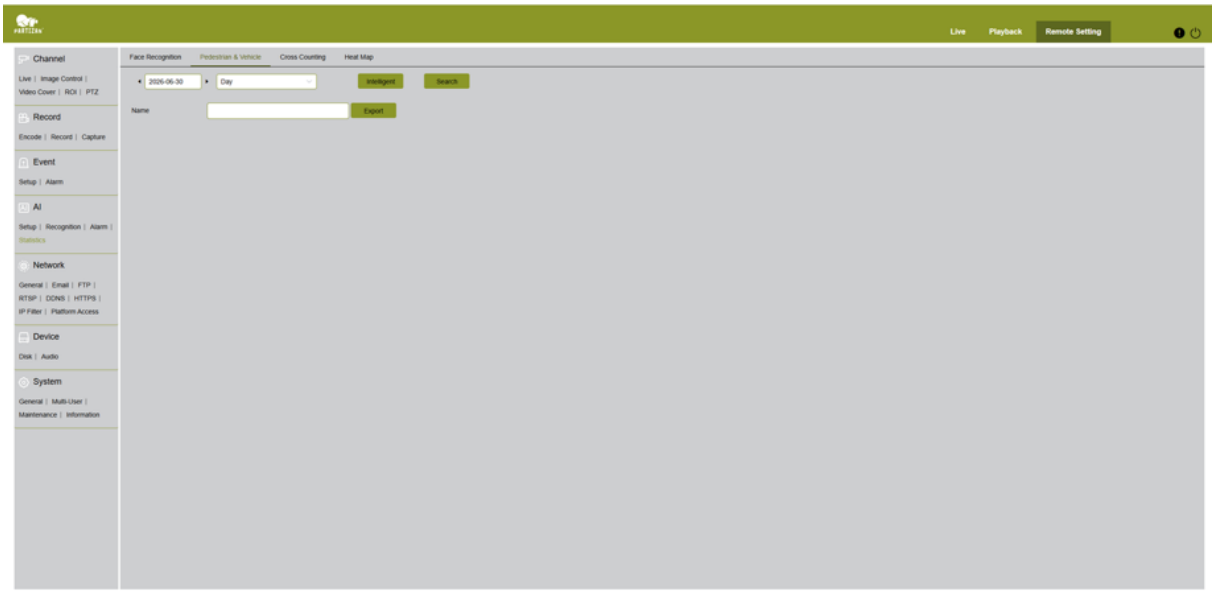

Fig. 73. AI → Statistics → Pedestrian & Vehicle — search and export pedestrian/vehicle counts

Setting / Control	Description
Time / Search Mode	Reference date and time range: Day, Week, Month, Quarter, or Year.
Intelligent	Filter by tag type: Perimeter Intrusion [Human], Perimeter Intrusion [Motor Vehicle], Line Crossing, Intrusion, Region Entrance, Region Exiting, etc.
Search / Export	Retrieve data and export results to Excel.

8.4.3 Cross counting

Generates crossing count reports in chart form (column or line), showing how many objects of a selected type crossed the detection line in a given period. Useful for footfall analysis and access monitoring.

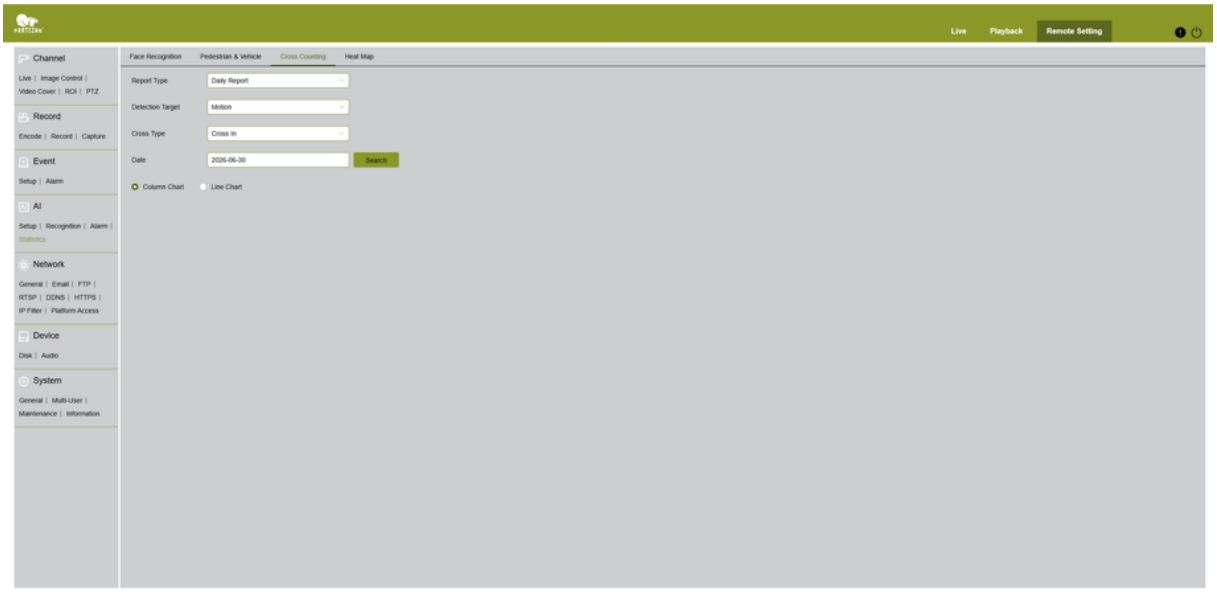

Fig. 74. AI → Statistics → Cross Counting — report type, detection target, cross type, and chart display

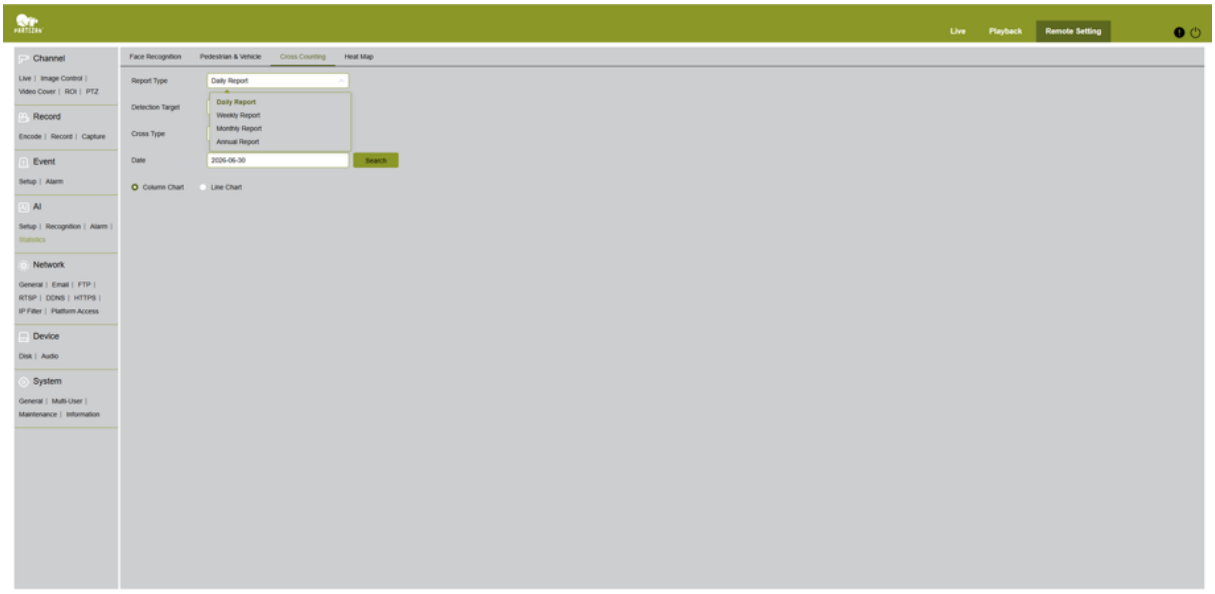

Fig. 75. AI → Statistics → Cross Counting — Report Type dropdown: Daily, Weekly, Monthly, Annual

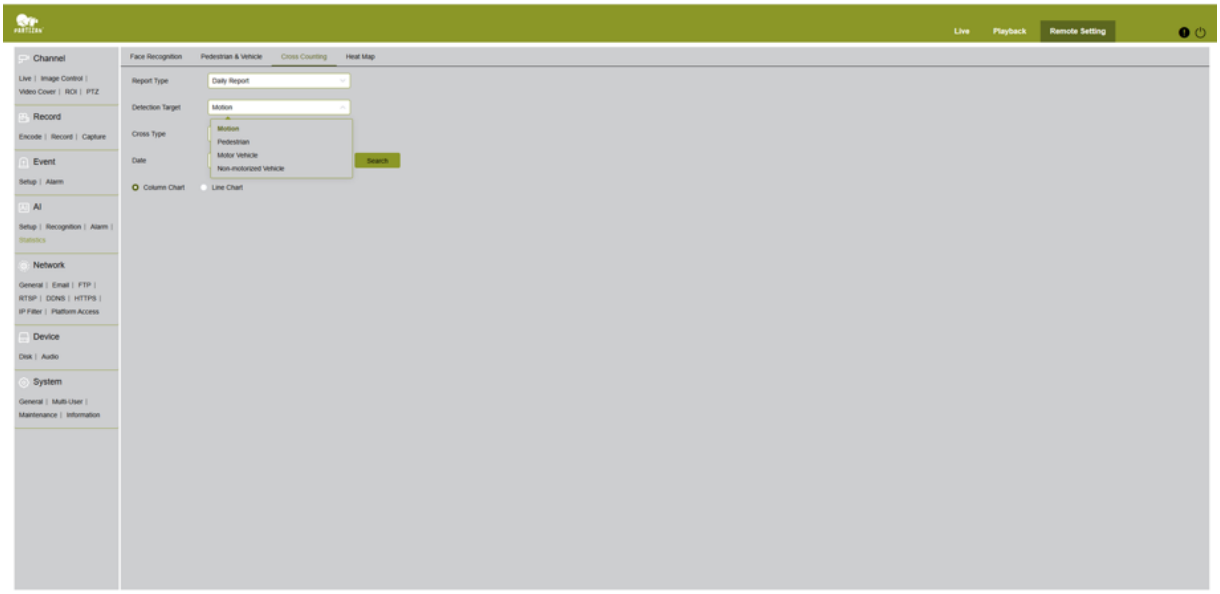

Fig. 76. AI → Statistics → Cross Counting — Detection Target dropdown: Motion, Pedestrian, Motor Vehicle, Non-motorized Vehicle

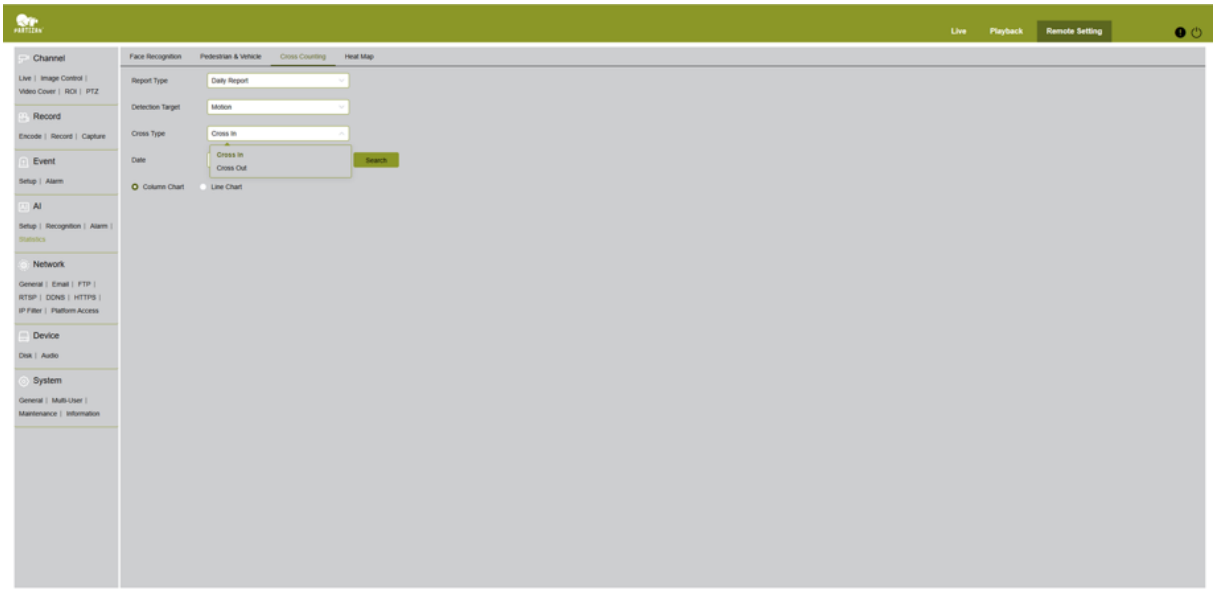

Fig. 77. AI → Statistics → Cross Counting — Cross Type dropdown: Cross In, Cross Out

Setting	Description
Report Type	Daily, Weekly, Monthly, or Annual report.
Detection Target	Motion (all objects), Pedestrian, Motor Vehicle, or Non-motorized Vehicle. Data can only be retrieved for the target type configured in the CC alarm model.
Cross Type	Cross In (entering the line's A side) or Cross Out (crossing to B side).
Date	Reference time for the selected report type.
Column Chart / Line Chart	Toggle the chart display style.
Search / Export	Retrieve data and export results to Excel.

8.4.4 Heat map

The heat map presents people distribution and activity data in two modes: spatial (which areas of the frame have the most activity) and temporal (activity intensity across different time periods).

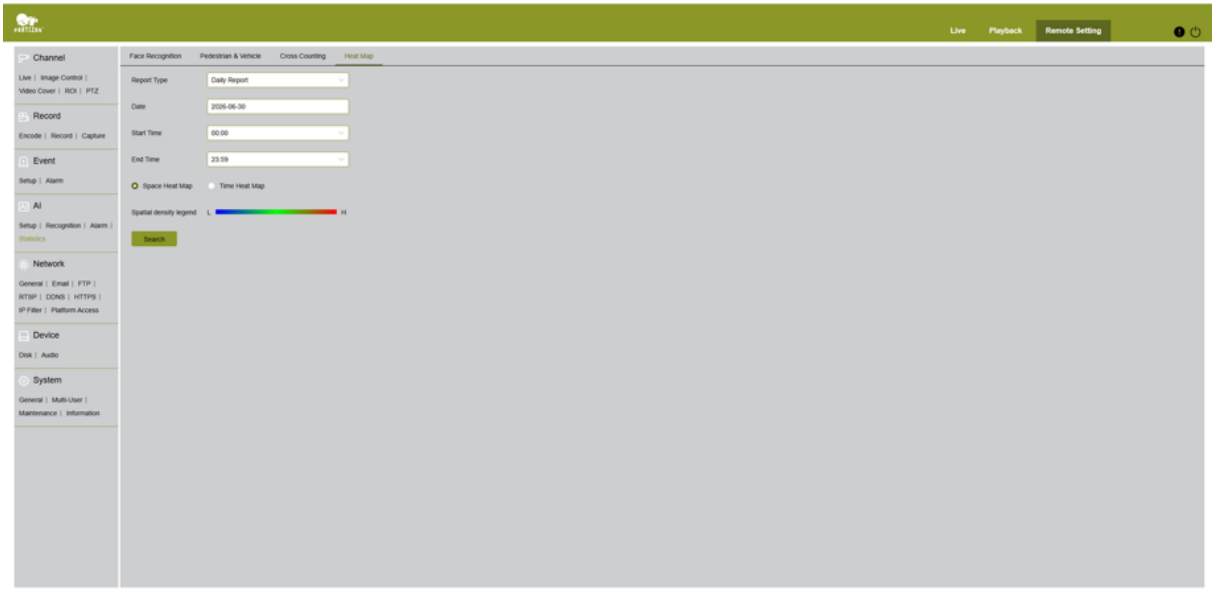

Fig. 78. AI → Statistics → Heat Map — space or time heat map with spatial density legend

Space Heat Map: Red areas indicate the highest activity density; blue areas indicate the lowest. This helps identify the most- and least-trafficked zones in the camera's view.

Time Heat Map: The Y-axis shows an activity index calculated from the number of people and duration. This helps identify peak activity periods throughout the day or week.

Setting	Description
Report Type	Daily, Weekly, Monthly, or Annual.
Date	Reference date for the selected report type.
Start Hour / End Hour	Available for Daily reports only — defines the hour range to search within.
Space Heat Map / Time Heat Map	Toggle between spatial distribution view and temporal activity view.
Search	Retrieve and display heat map data according to current settings.

9. Remote setting → network

9.1. General

Configure the camera's basic IPv4/IPv6 network settings, DNS, multicast, and video encryption. The General tab also includes sub-tabs for PPPoE, SNMP, IEEE802.1X, and Port Configuration.

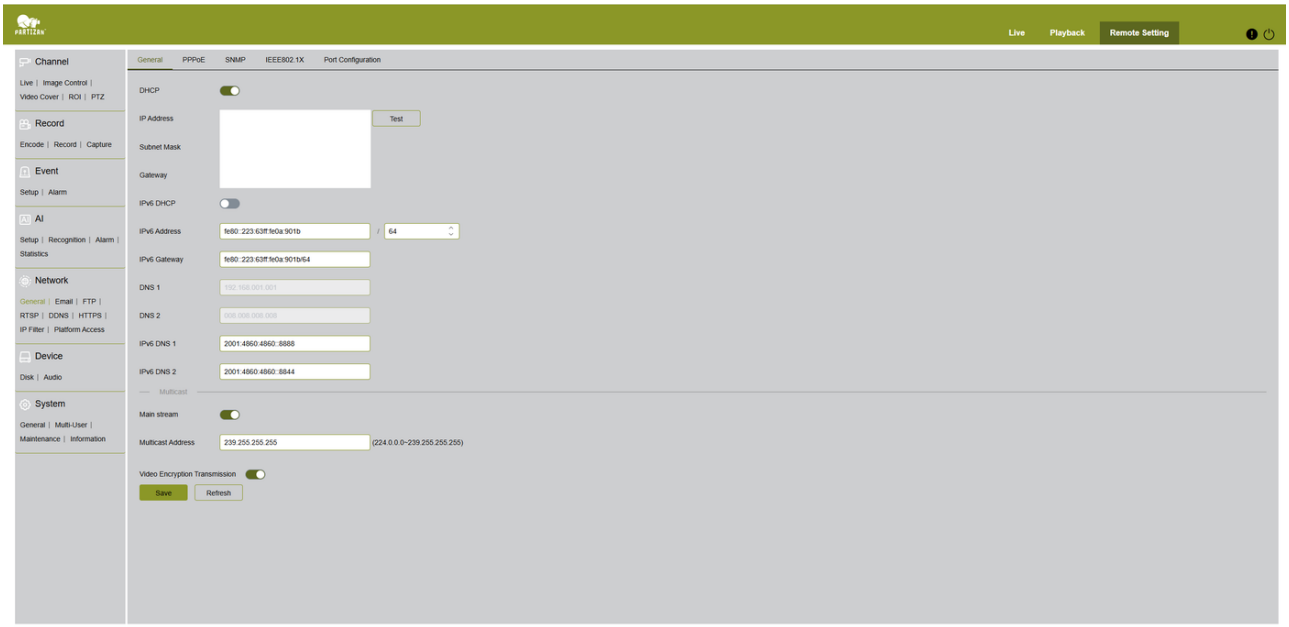

Fig. 79. Network → General — DHCP, IP/subnet/gateway (hidden), IPv6, DNS, and multicast settings

Setting	Description
DHCP	Automatically obtain an IP address from the network's DHCP server
IP Address / Subnet Mask / Gateway	Manual IPv4 network configuration (used when DHCP is off)
IPv6 DHCP / IPv6 Address / Gateway	IPv6 network configuration
DNS 1 / DNS 2	Primary and secondary DNS server addresses
Multicast	Enables multicast streaming on a configurable multicast address
Video Encryption Transmission	Encrypts the video stream in transit

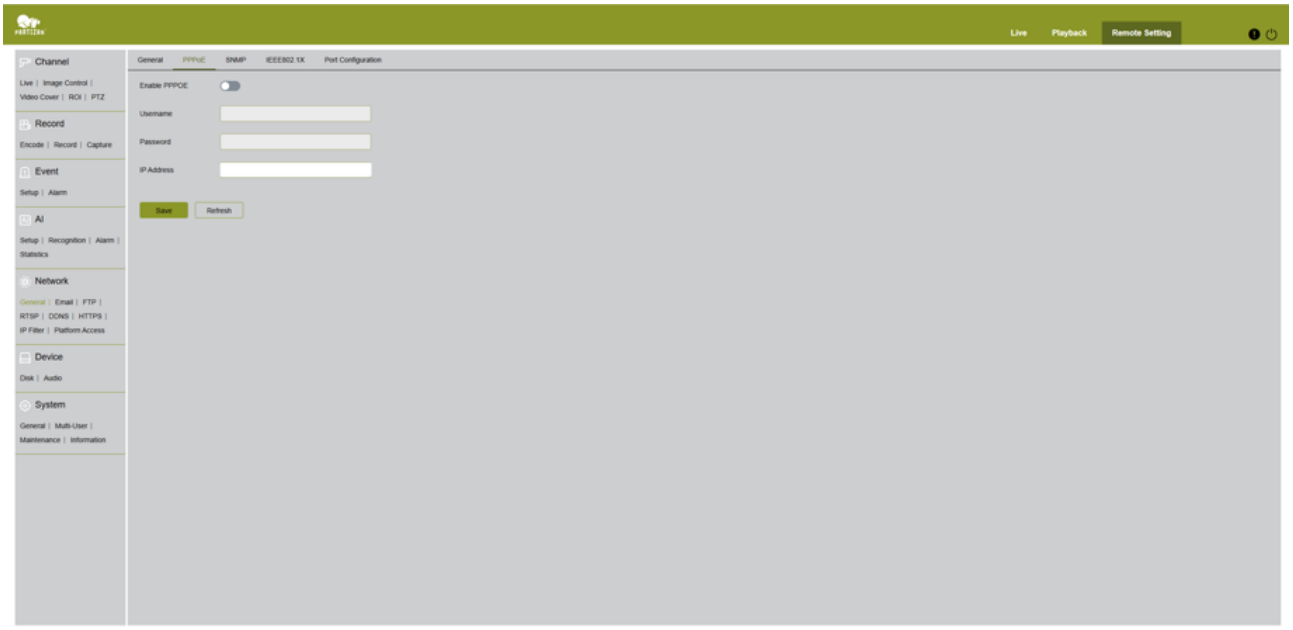

Fig. 80. Network → General → PPPoE — username, password, and assigned IP address

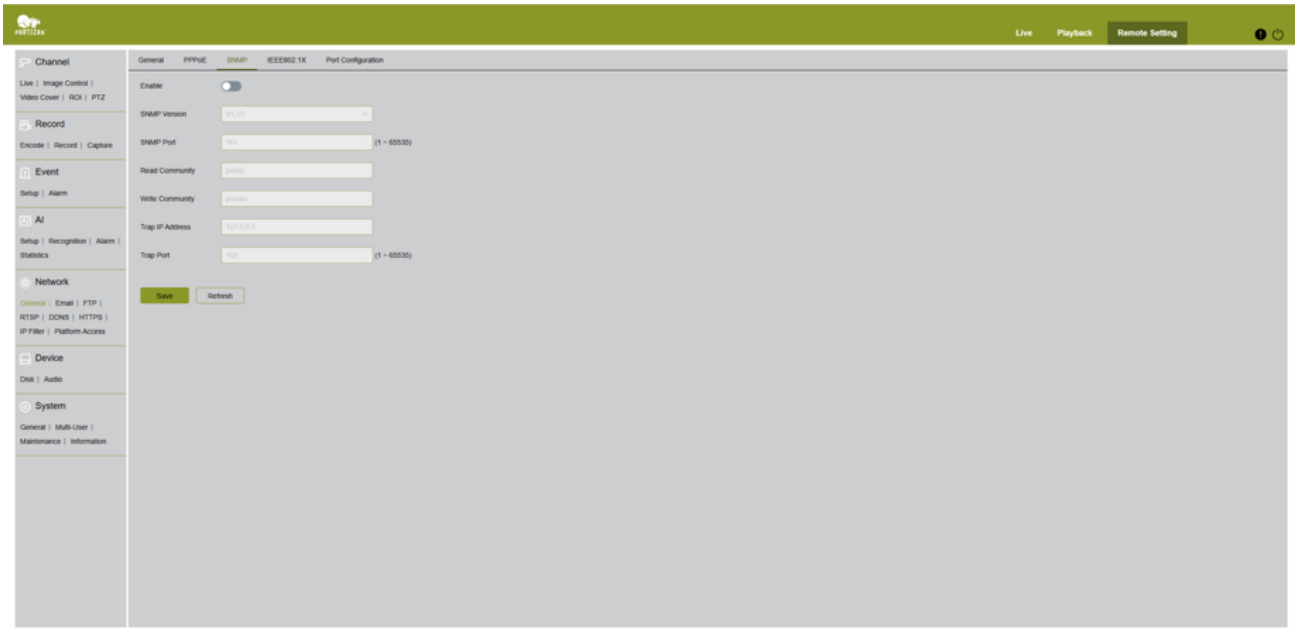

Fig. 81. Network → General → SNMP — version, port, and read/write community strings

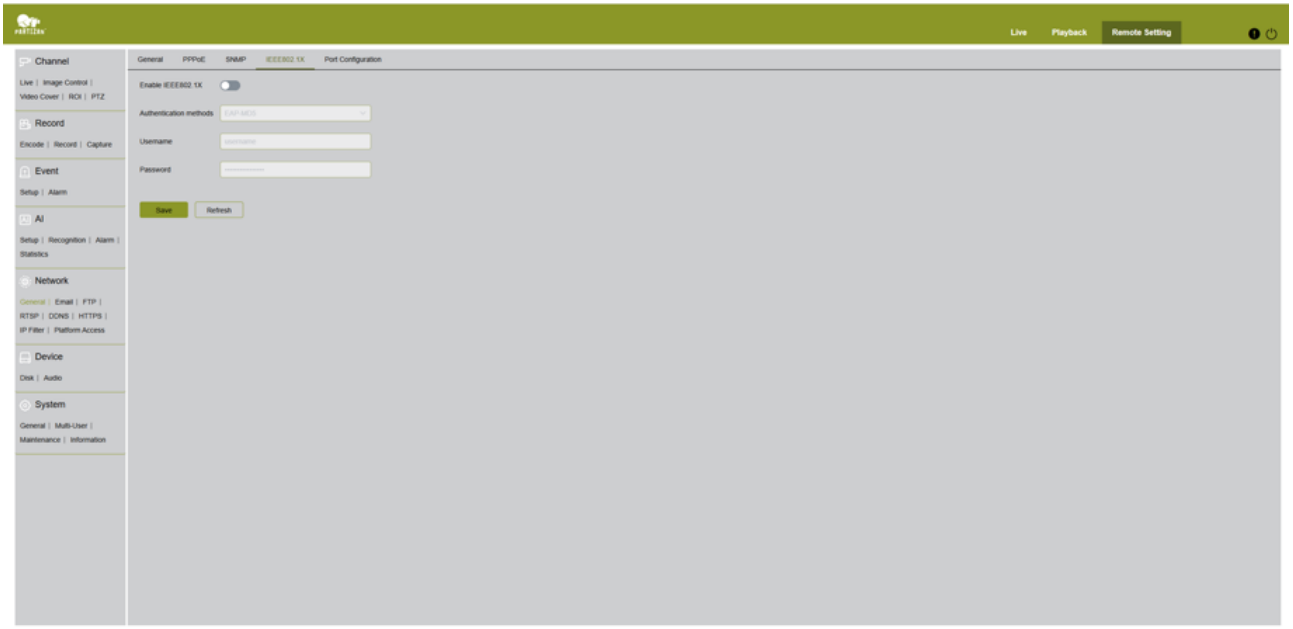

Fig. 82. Network → General → IEEE802.1X — port-based network access authentication

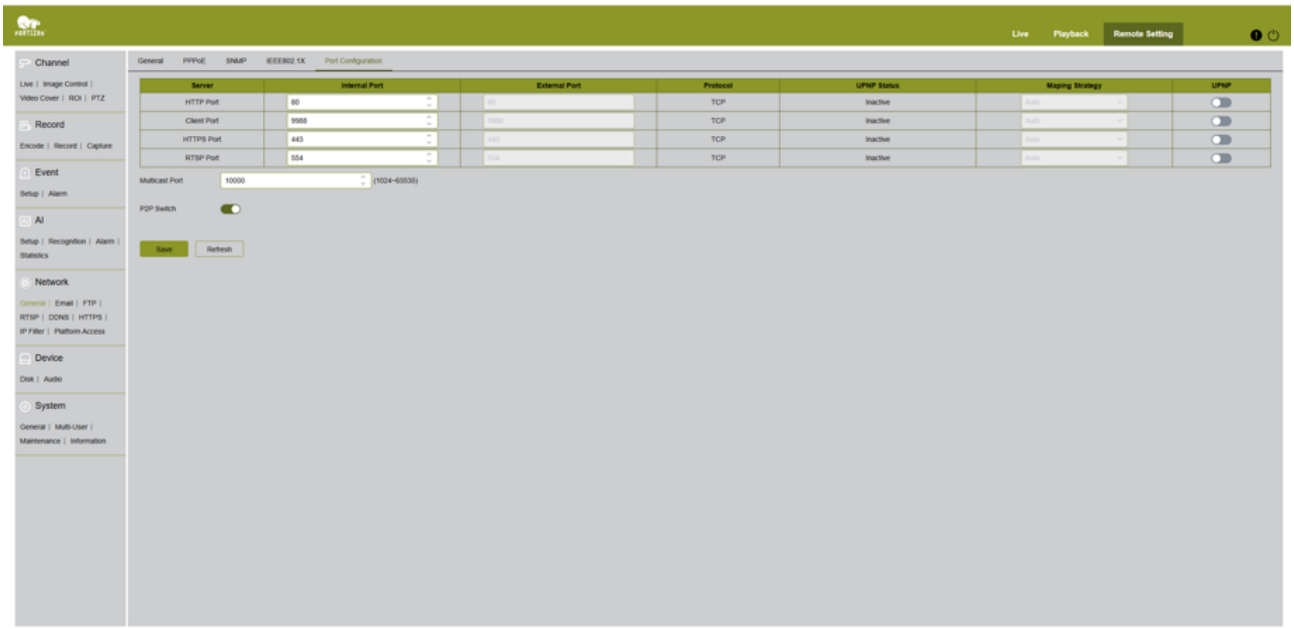

Fig. 83. Network → General → Port Configuration — HTTP/Client/HTTPS/RTSP ports, UPnP, and P2P switch

Note: The P2P Switch enables remote cloud-assisted access without manual port forwarding; disable it if you require fully local-only network access.

9.2. Email

Configure the SMTP server used to send event notification emails.

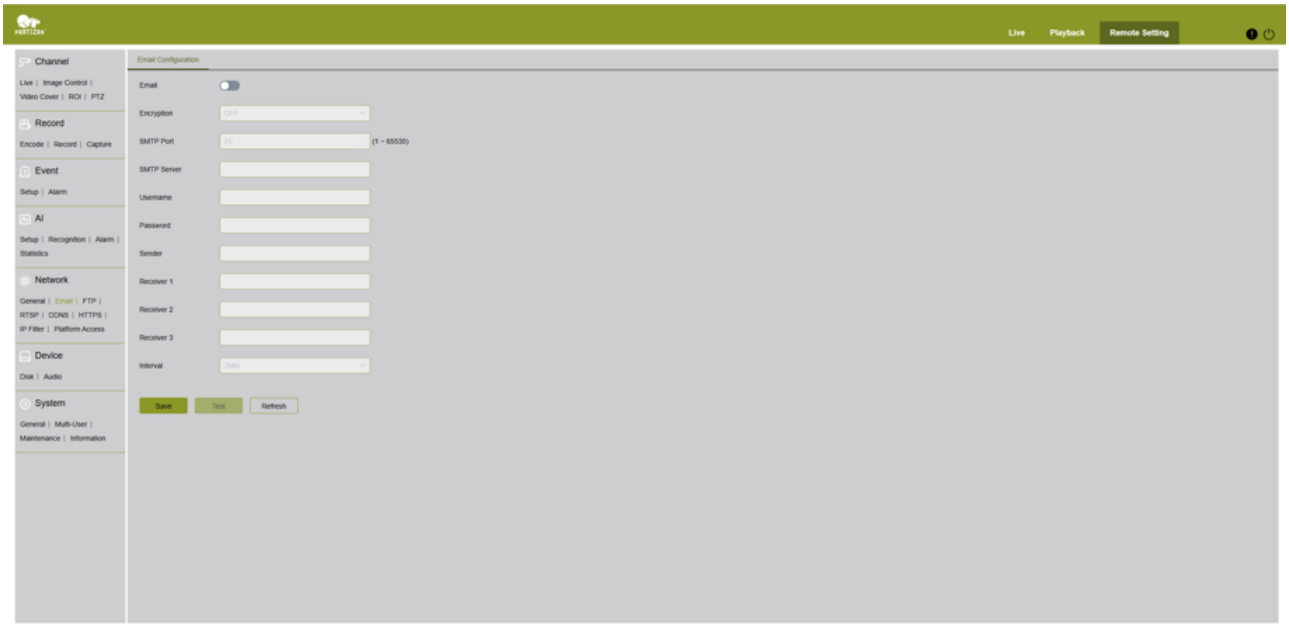

Fig. 84. Network → Email — SMTP server, encryption, sender, and up to 3 recipients

9.3. FTP

Configure an FTP server destination for uploading captured images and video clips on event triggers.

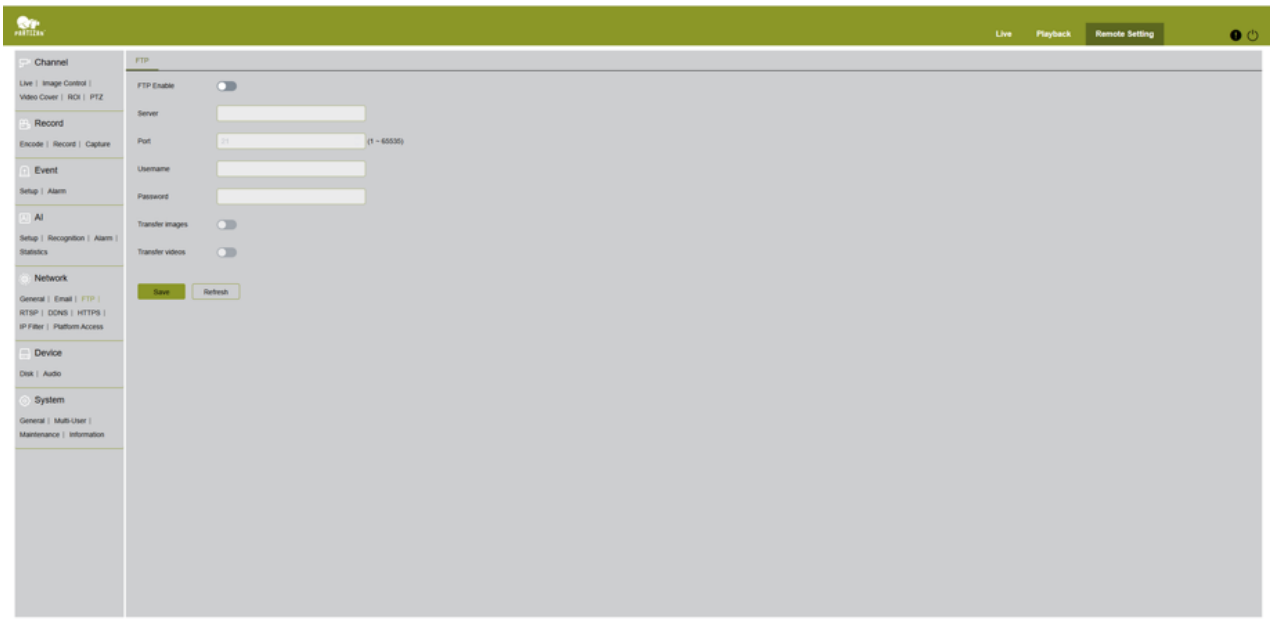

Fig. 85. Network → FTP — server, port, credentials, and transfer options

9.4. RTSP

Enable RTSP streaming for third-party NVR/VMS integration, with an optional anonymous login mode.

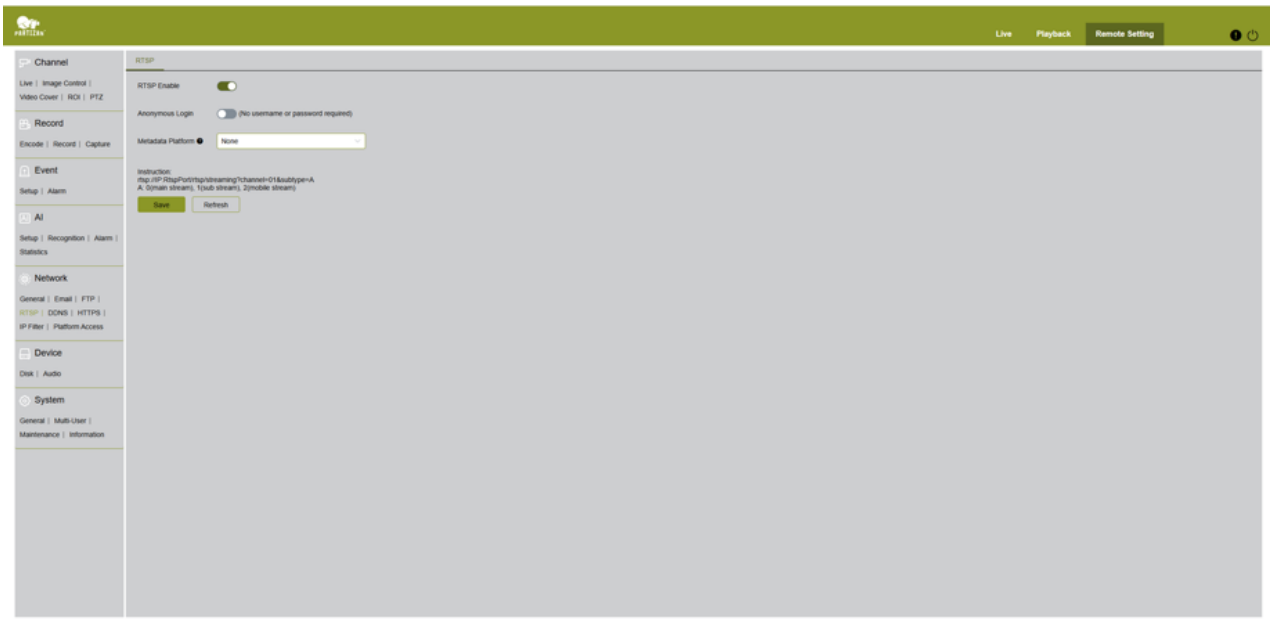

Fig. 86. Network → RTSP — enable toggle, anonymous login, and RTSP URL format instructions

Note: RTSP URL format: rtsp://IP:RtspPort/streaming?channel=01&subtype=A, where A is 0 (main stream), 1 (sub stream), or 2 (mobile stream).

9.5. DDNS

Configure a Dynamic DNS provider to maintain a consistent hostname for the camera even when its public IP address changes.

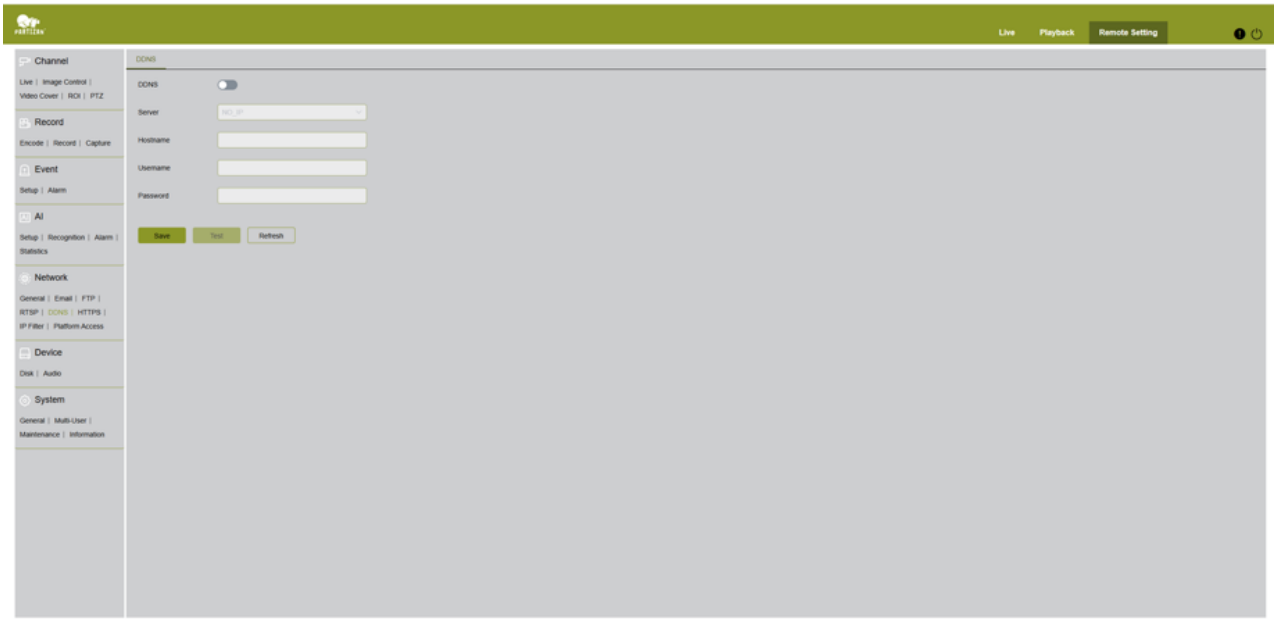

Fig. 87. Network → DDNS — provider selection, hostname, and credentials

9.6. HTTPS

Select the SSL/TLS certificate type used to secure the camera's web interface.

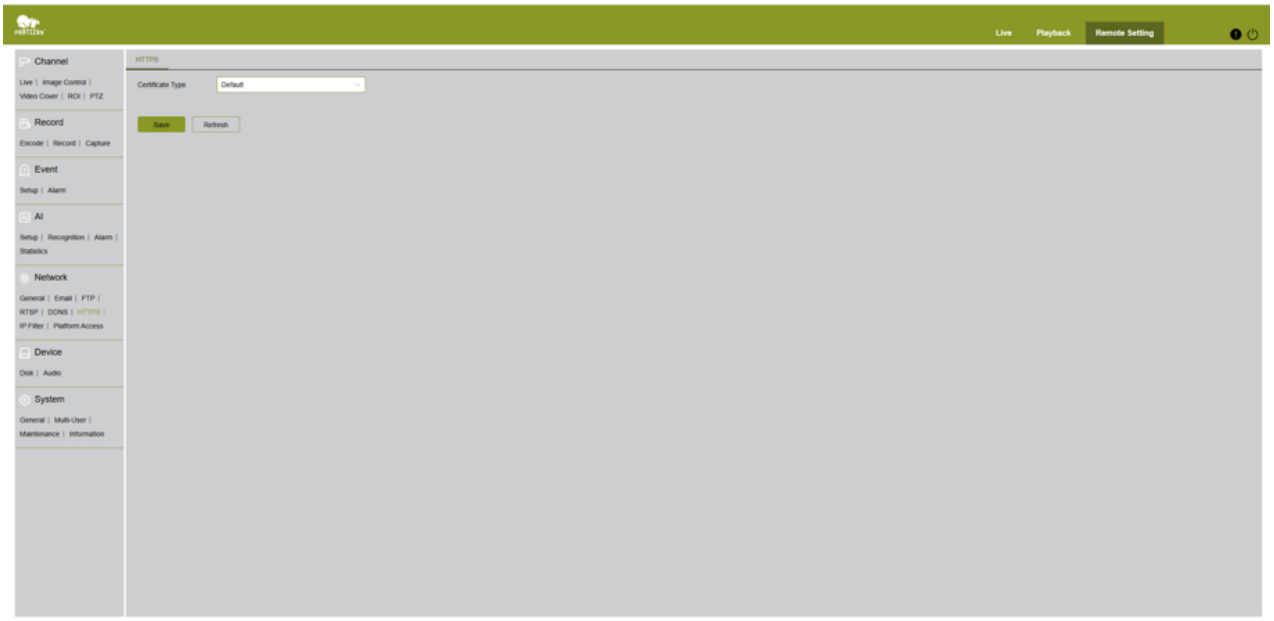

Fig. 88. Network → HTTPS — certificate type selection

9.7. IP filter

Restrict access to the camera by IP address, using either an allow list or a block list.

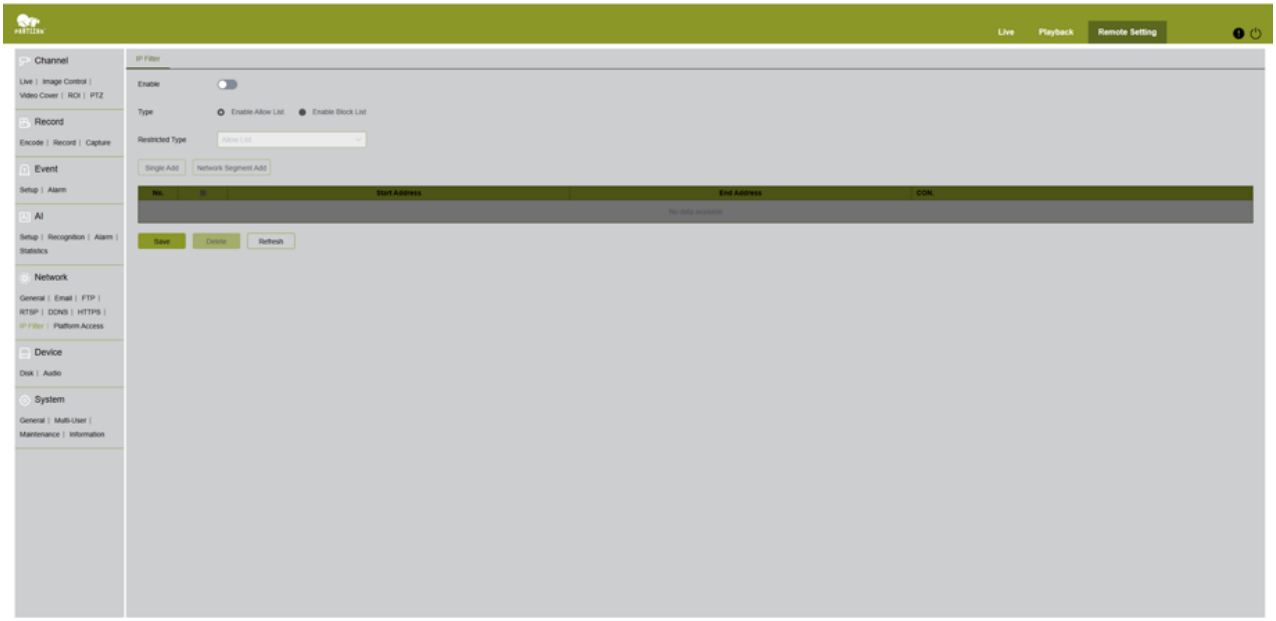

Fig. 89. Network → IP Filter — allow/block list configuration with single or range address entry

9.8. Platform access

Configure outbound integrations: RTMP live streaming to a third-party platform, and the Event Push Platform used to forward alarm events to an external server (e.g. a VMS or monitoring dashboard).

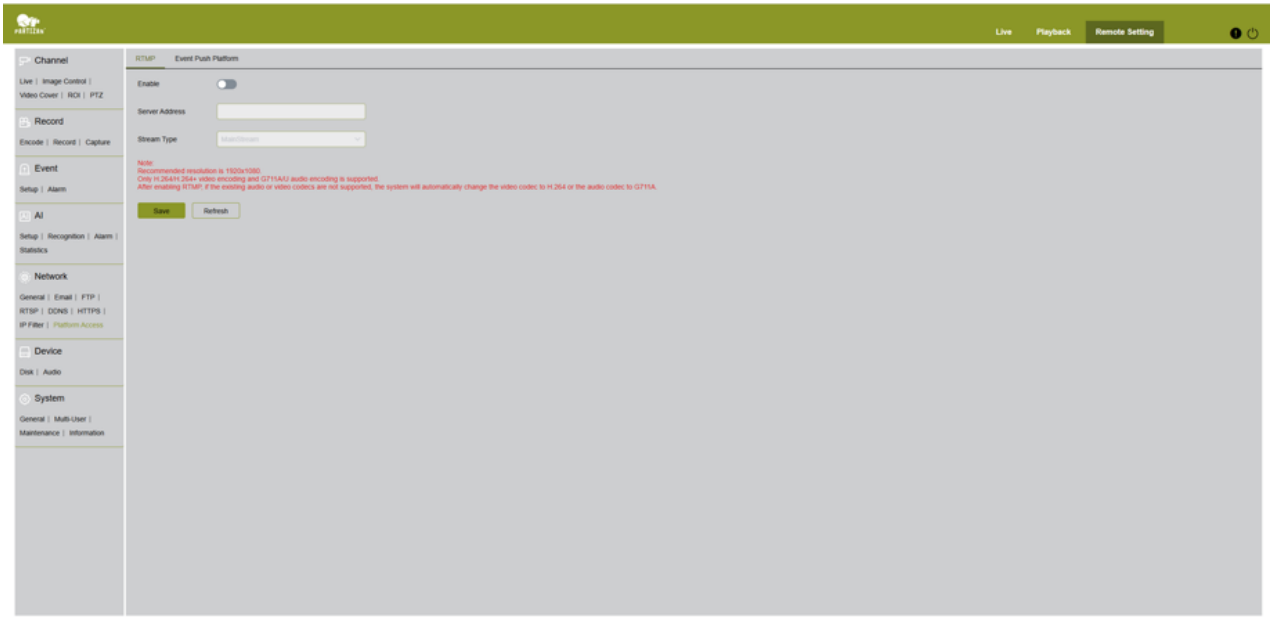

Fig. 90. Network → Platform Access → RTMP — server address and stream type for live restreaming

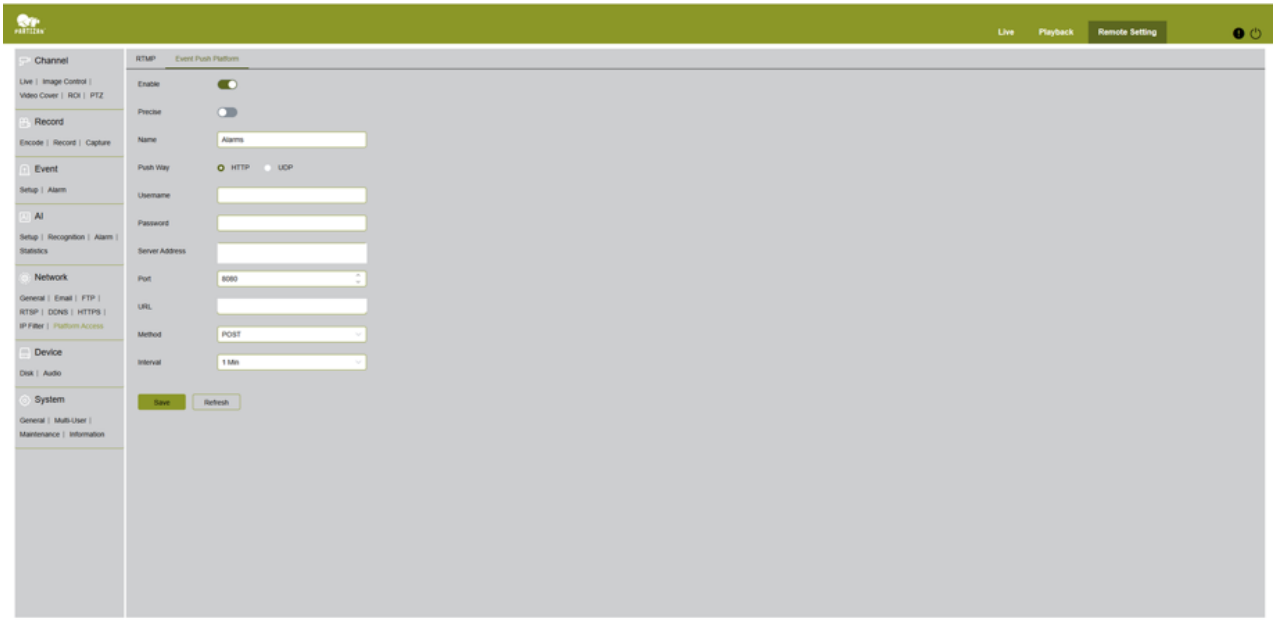

Fig. 91. Network → Platform Access → Event Push Platform — push method, credentials, and target server (hidden)

10. Remote setting → device

10.1. Disk

Manage the camera's local storage (SD card or network HDD), including overwrite policy and formatting.

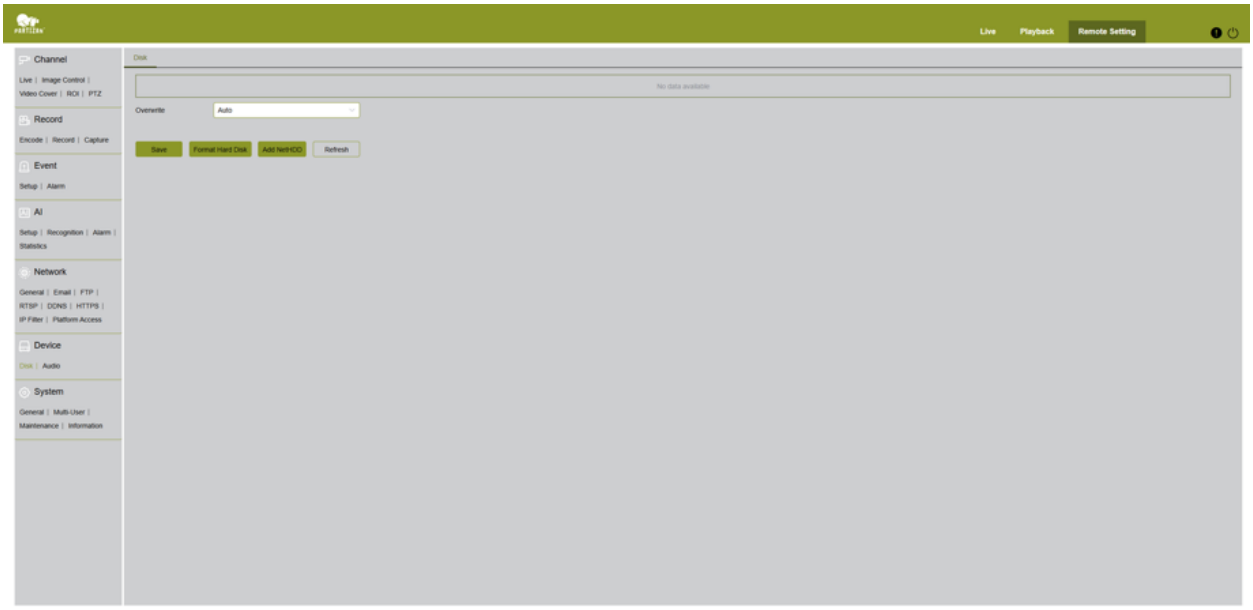

Fig. 92. Device → Disk — storage status, overwrite mode, and format/add network HDD options

10.2. Audio

Configure audio input/output volume levels and the audio codec used for two-way audio and recording.

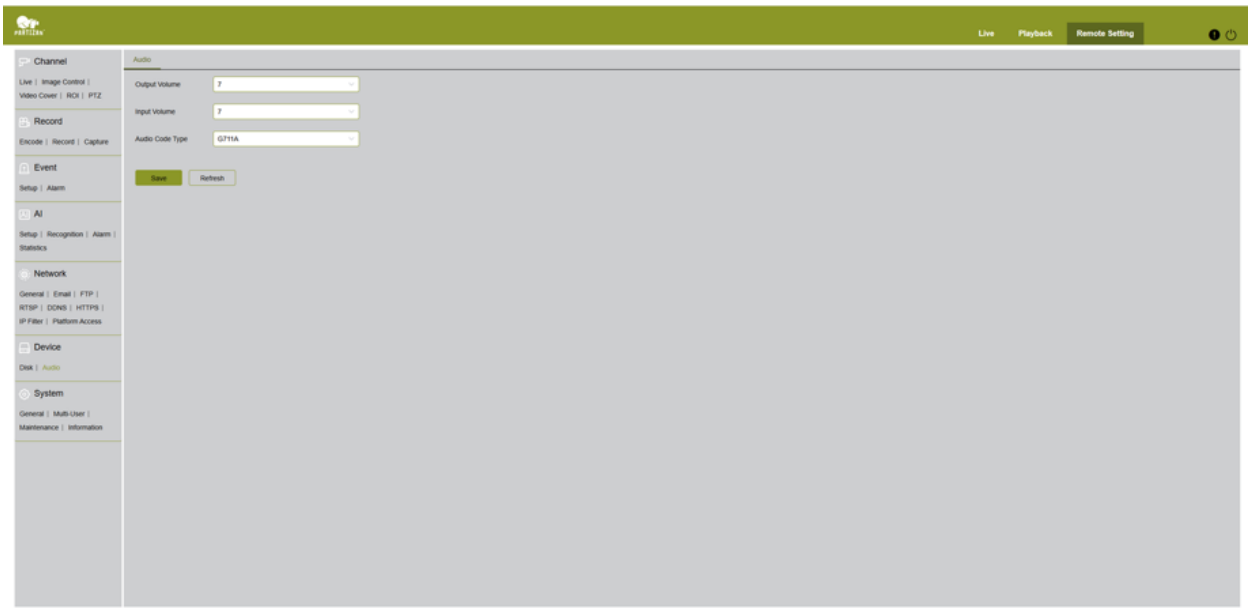

Fig. 93. Device → Audio — output/input volume and audio codec type

11. Remote setting → system

11.1. General

Configure system date, time, time zone, and daylight saving time rules.

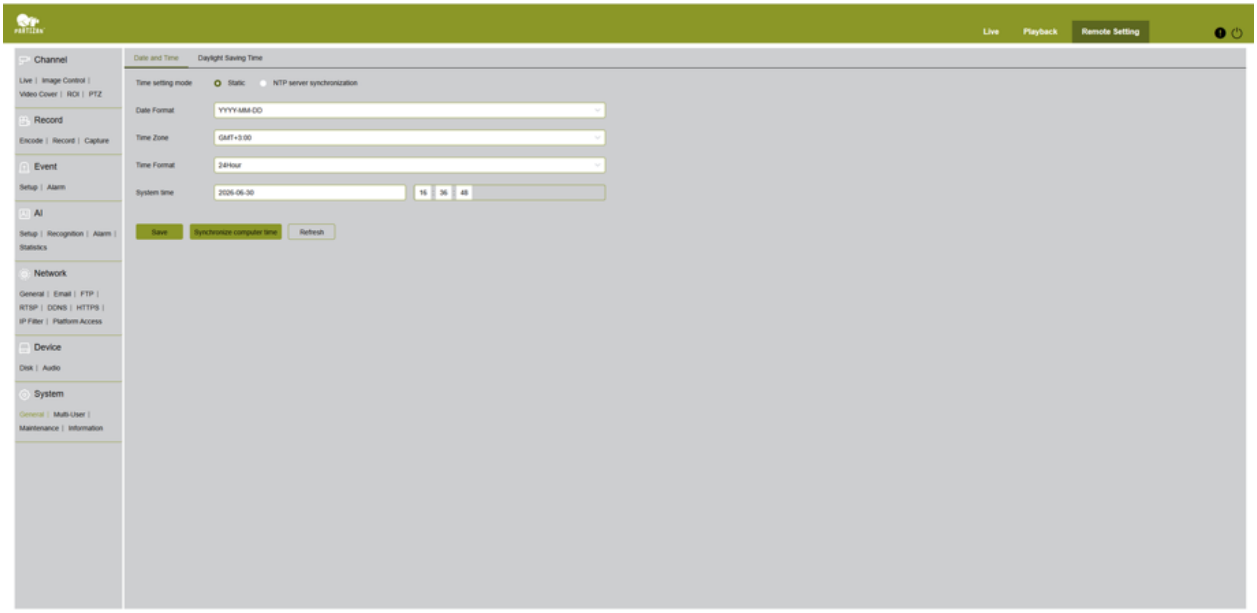

Fig. 94. System → General → Date and Time — time mode, format, time zone, and system clock

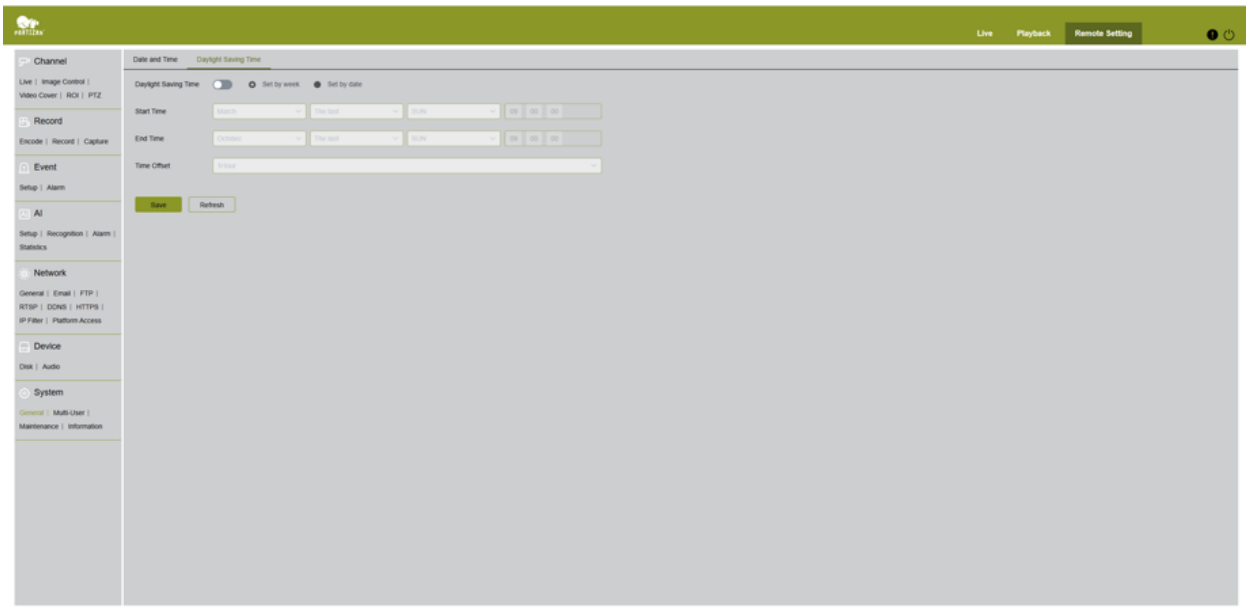

Fig. 95. System → General → Daylight Saving Time — start/end rules and time offset

11.2. Multi-user

View and manage all user accounts, their permission level (ADMIN or USER), and enable/disable status. Click the edit icon to change a password, or the gear icon to configure that user's detailed access policy.

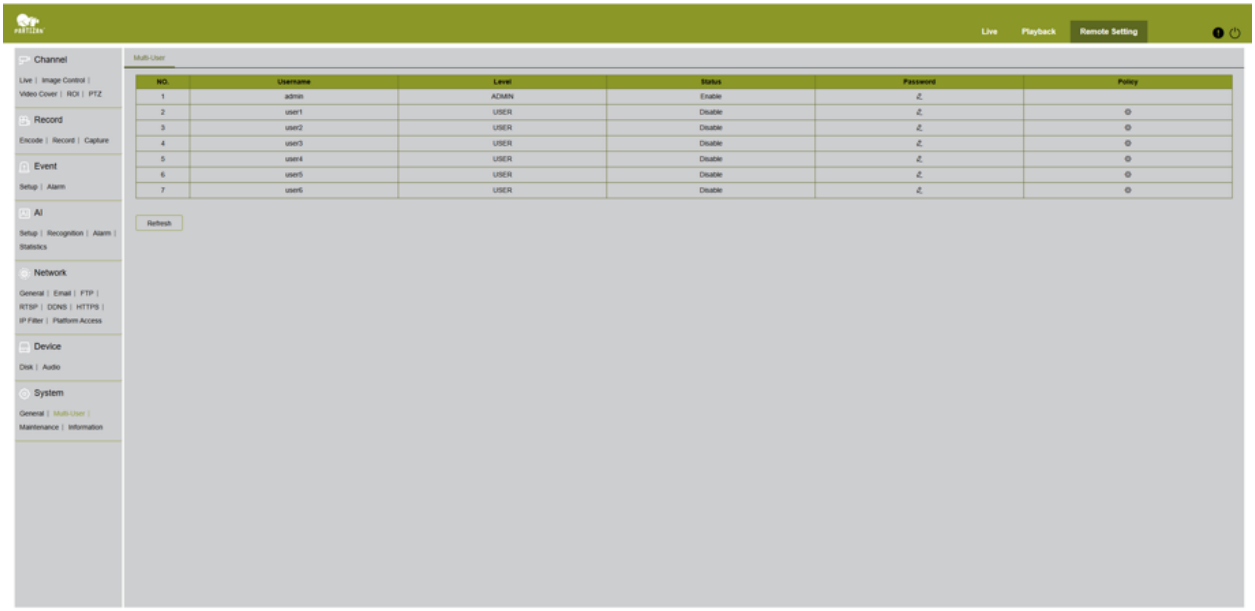

Fig. 96. System → Multi-User — user list with level, status, password, and policy controls

11.3. Maintenance

The Maintenance section provides system logs, factory reset options, firmware upgrade, configuration backup/restore, scheduled reboot, and developer diagnostic tools.

11.3.1 Log

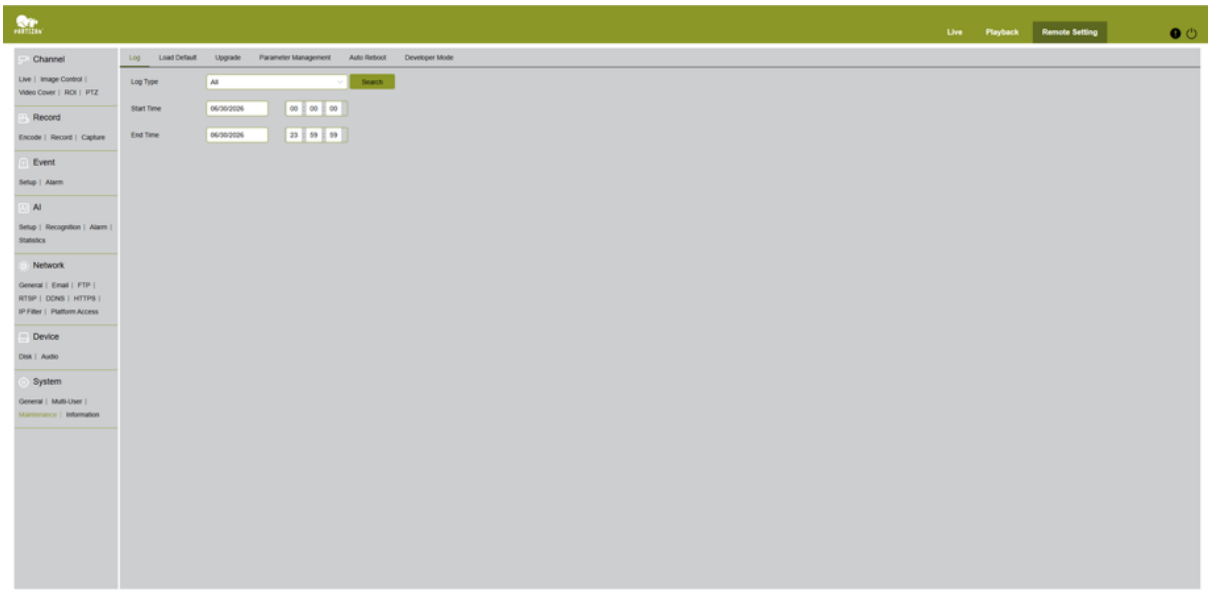

Fig. 97. System → Maintenance → Log — search system events by type and date range

11.3.2 Load default

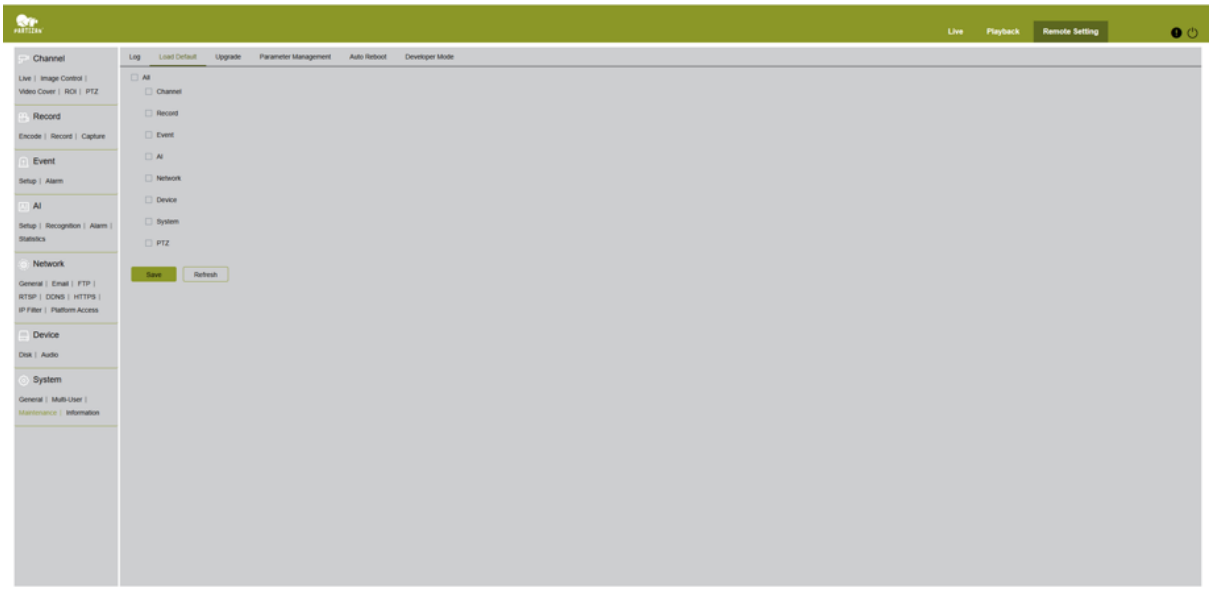

Fig. 98. System → Maintenance → Load Default — selectively restore factory defaults by module

Note: You can restore defaults selectively (e.g. only AI settings) instead of resetting the entire camera configuration.

11.3.3 Upgrade

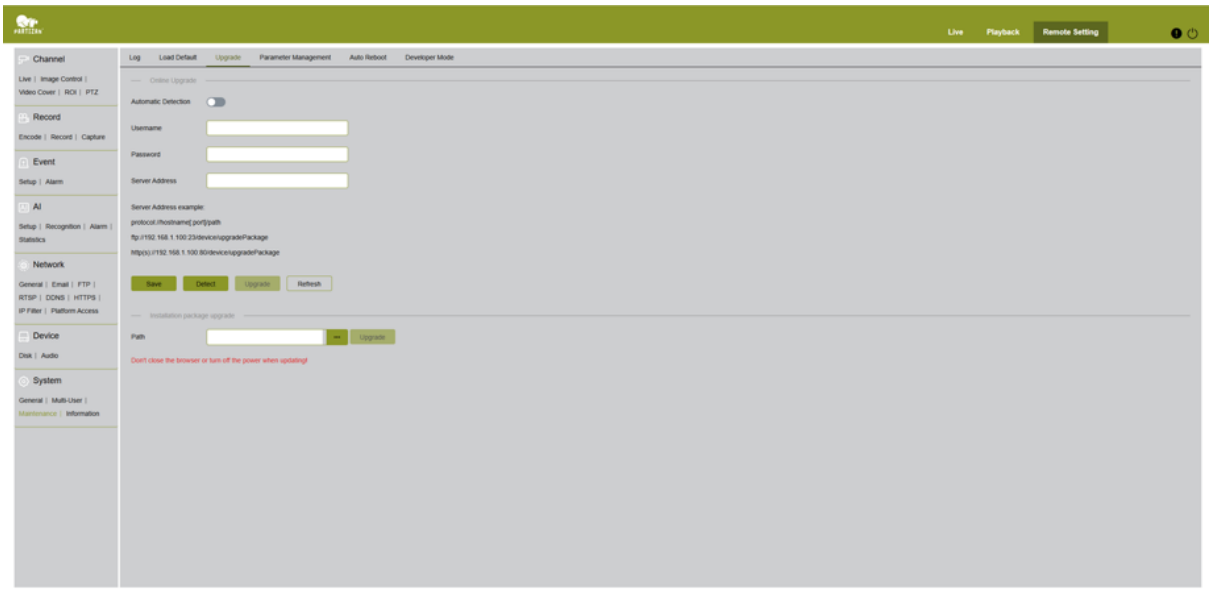

Fig. 99. System → Maintenance → Upgrade — online upgrade via server address, or manual upgrade via local file

Note: Do not power off the camera or close the browser during a firmware upgrade.

11.3.4 Parameter management

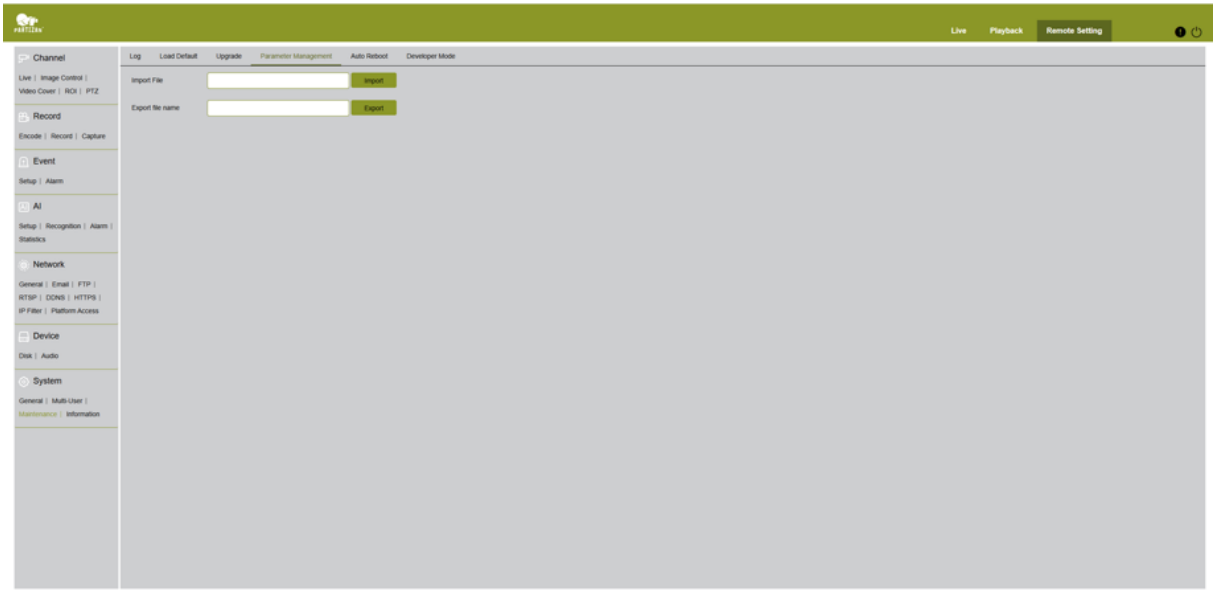

Fig. 100. System → Maintenance → Parameter Management — import or export the full camera configuration

11.3.5 Auto reboot

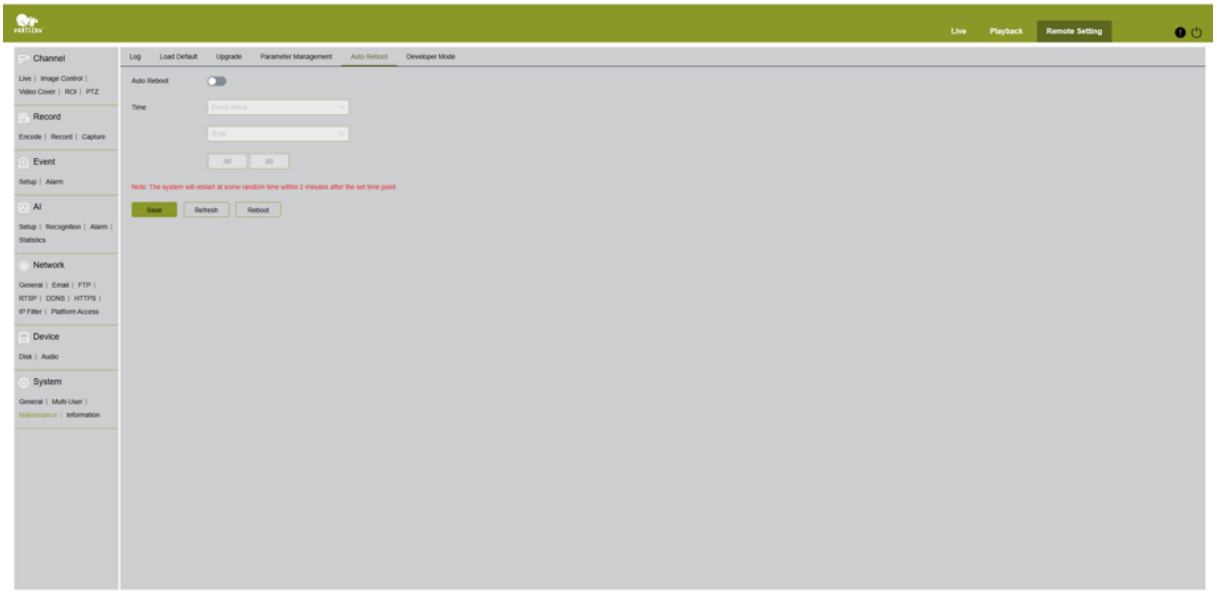

Fig. 101. System → Maintenance → Auto Reboot — scheduled reboot frequency and time

11.3.6 Developer mode

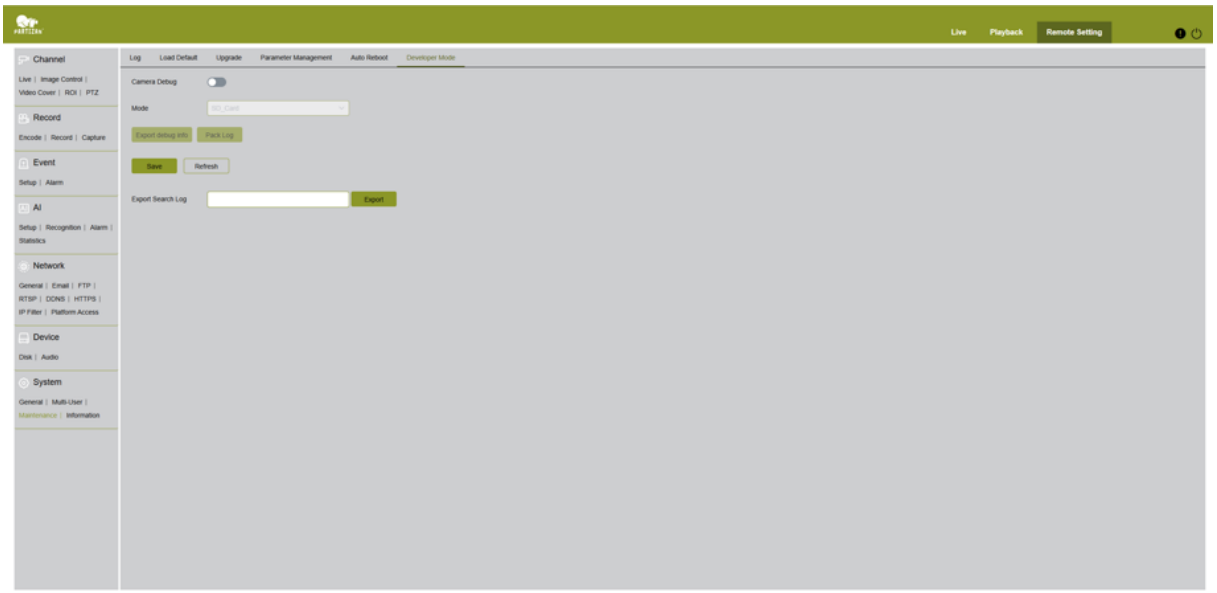

Fig. 102. System → Maintenance → Developer Mode — debug logging and log export tools for support purposes

11.4. Information

Displays read-only device identification details: Device ID, Name, Type, Hardware/Software/Web/MCU versions, MAC address, and P2P ID. A QR code is also provided here for adding the camera to a compatible mobile application via P2P, where supported.

Fig. 103. System → Information — device identification and version details (MAC, P2P ID, and QR code hidden)

12. Device connection

An SH Series IP camera can be connected to your network in one of two ways, depending on whether you are configuring it locally on a single PC or integrating it into an existing local network.

12.1. Direct connection to a PC

Use this method for initial setup or one-off configuration, connecting the camera directly to a computer with no router in between.

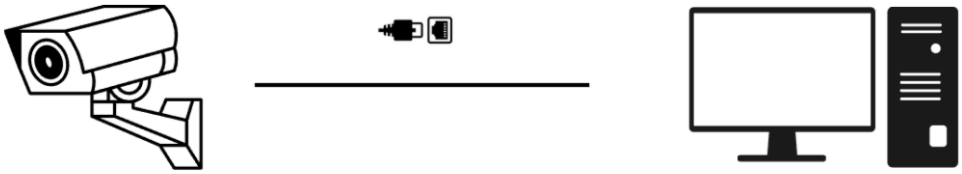

Fig. 104. Direct connection — camera connected straight to a PC via Ethernet cable

1. Connect the camera to the PC directly using an Ethernet cable and power the camera with a DC 12V adapter.
2. Set the PC's network adapter to a static IP address on the same subnet as the camera (e.g. 192.168.1.50, subnet mask 255.255.255.0).
3. Open a web browser and navigate to the camera's default IP address: 192.168.1.168.

12.2. Connection through a router or switch

Use this method when the camera and PC are both connected to the same local network, allowing access from any device on that network — and, if configured, remotely over the internet.

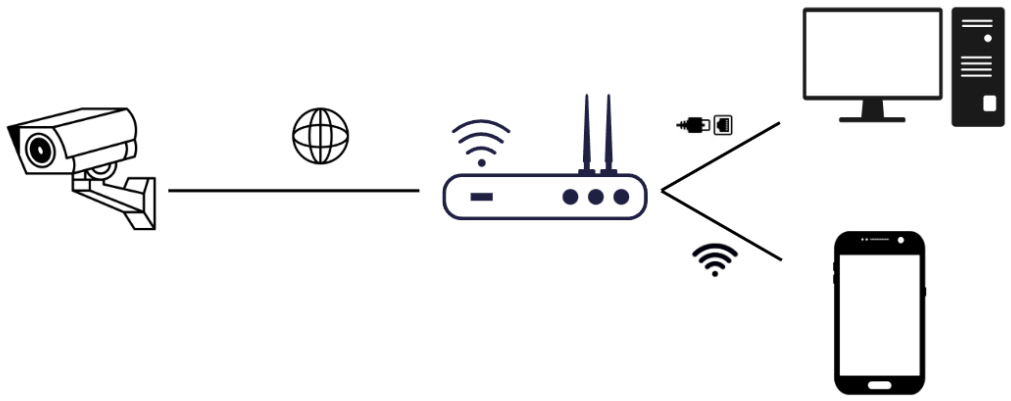

Fig. 105. Router/switch connection — camera and PC share the same LAN, with optional remote access

1. Connect the camera to a LAN port on your router or switch using an Ethernet cable.
2. Ensure the camera's gateway address matches your router's IP address (use DHCP or the Device Config Tool to assign an IP automatically).
3. From any PC on the same network, open a browser and enter the camera's IP address to access the web interface.
4. For remote access from outside the local network, configure port forwarding on the router, or use DDNS / the camera's P2P feature (see Section 9.5 and 11.4).

Note: Use the Device Config Tool (a separate desktop utility) to scan the local network and quickly locate or reconfigure the IP address of any SH Series camera — this is especially useful when the camera's current IP address is unknown.

13. Safety instructions

- **Security:** Change the default password immediately upon first login to prevent unauthorized access.
- Do not install the camera in damp, dusty, or poorly ventilated locations, or in places easily accessible to children.
- Use and store the device within its specified temperature and humidity range.
- Do not disassemble the camera or attempt unauthorized repairs.
- This product is intended for use in non-tropical climate conditions only.
- Keep your password recovery information (security question answers or certificate file) in a safe place — without it, password recovery may not be possible.

Note: The content of this manual is for reference only and may differ slightly from the actual product or firmware version. Features and menu layout may vary depending on the specific camera model.

Contacts:

WhatsApp: +420 777 054 888

Email: support@partizan.global
Telegram: https://t.me/PartizanSupport_bot