

IP camera cloud

User Manual



BE **DIFFERENT**

LEAD WITH IT

Contents

1. Product overview	4
2. Interface overview	5
3. Installation and startup	6
3.1. General options	6
3.2. Scheme 2 — PoE switch + Partizan cloud access	7
3.3. Default network settings	8
4. Network settings	9
4.1. Searching for and configuring cameras with the Partizan software	9
4.2. Adding a device manually (+ Add button)	10
4.3. My devices panel	11
4.4. Changing the IP address via the Partizan app	12
5. Live view	13
6. Archive playback	14
7. Cloud account and remote access	15
7.1. Step 1 — entering the login and password	15
7.2. Mobile app — scan the QR code to add the camera	16
7.3. Downloading the Partizan software	17
8. Camera settings	18
8.1. Time settings	19
8.2. Storage management	20
8.3. Recording settings	21
8.4. User management	22
8.5. Video parameters	24
8.6. Stream parameters	25
8.7. Overlay settings	26
8.8. Privacy mask	28

9. Alarms	29
9.1. Motion detection	29
9.2. Audio detection	31
9.3. Video tampering	32
9.4. Email notification settings	33
10. Maintenance	37
10.1. Event log	37
10.2. Service — reboot and restore default settings	38
10.3. Firmware upgrade	39
Contacts:	40

1. Product overview

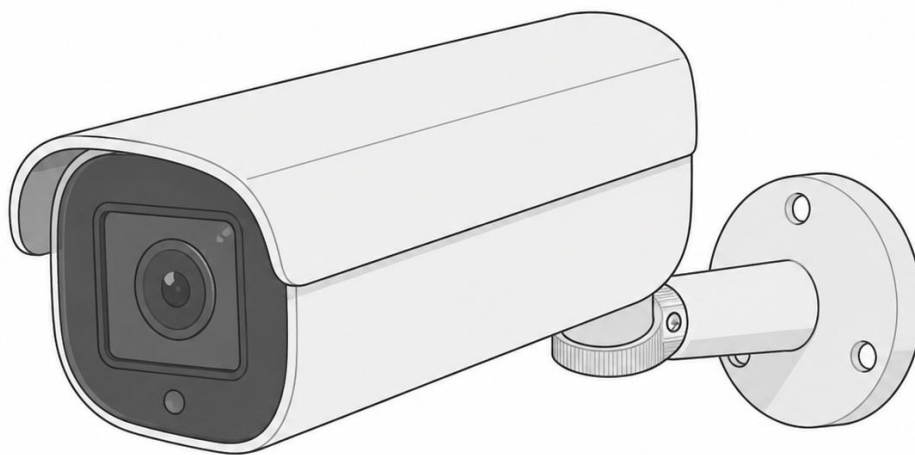


Fig. 1. IP cameras of the Cloud series

The Cloud series IP cameras are a range of professional network cameras designed for reliable round-the-clock video surveillance in residential, commercial, and industrial premises.

Built on Partizan's own Partizan Cloud platform, Cloud series cameras provide seamless remote access from anywhere in the world — with no need for port forwarding or complex network configuration. Simply connect the camera to the internet, scan the QR code in the Partizan mobile app, and the live stream becomes instantly available on any device.

The lineup covers a wide range of installation scenarios: compact dome and bullet cameras for indoor use, weatherproof outdoor models with IR night vision up to 30 metres, and high-resolution 4K devices for sites that require maximum detail. All models support Power over Ethernet (PoE) for simplified cabling and are compatible with the Partizan software on Windows, macOS, and Linux.

Key features of the Cloud series: motion detection with configurable zones and email alerts, scheduled or event-triggered recording to an internal SD card or cloud storage, H.264/H.265 video compression for efficient bandwidth and storage use, and full remote configuration without the need for physical access to the device.

Whether you need to secure a single office or manage a video surveillance system across multiple sites, Cloud series cameras integrate into the Partizan ecosystem — including VMS software, NVRs, and the Partizan mobile app — providing a single platform for monitoring, playback, and device management.

2. Interface overview

The table below describes the available ports and connectors. Port availability may vary by model.

Interface	Function
RJ-45	Connect an Ethernet cable to a network switch or router. Power over Ethernet — powers the camera through the network cable (PoE models only)
Audio input (RCA / 3.5 mm)	Receives an audio signal from an external microphone or receiver
I/O port	Input/output — function depends on the model
Power (DC 12V)	DC 12V power input

3. Installation and startup

3.1. General options

Use this method to connect the camera directly to your router and access it by IP address from the same network.

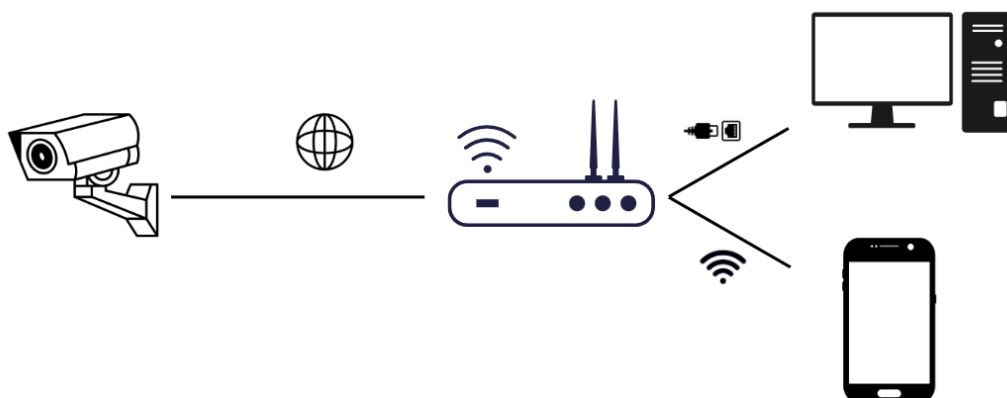


Fig. 2. Direct IP connection: camera → router → PC / mobile app

1. Connect the camera to the local network with an Ethernet cable via the LAN port.
2. Power the camera with a DC 12V adapter, or connect it to a PoE switch (PoE cameras only).
3. Open the Partizan software on your PC, click Search to find the camera, and add it.
4. On your mobile device, open the Partizan app and add the camera by its IP address or by scanning the QR code.
5. The camera can also be added by MAC address: in the Partizan mobile app, choose the option to add a device by MAC address and enter the address printed on the camera body or on the box.

3.2. Scheme 2 — PoE switch + Partizan cloud access

Use this method for multiple PoE-powered cameras. Cloud access allows remote monitoring from anywhere.

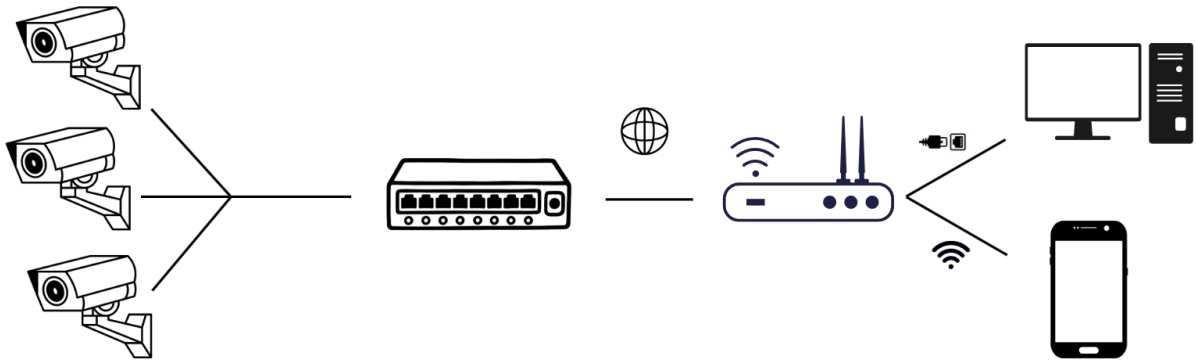


Fig. 3. PoE switch + cloud: cameras → PoE switch → router → internet → Partizan cloud

1. Connect each camera to the PoE switch with an Ethernet cable (data and power over a single cable).
2. Connect the PoE switch to the router via Ethernet.
3. Make sure the router has internet access for the cloud connection.
4. In the Partizan software, sign in to your Partizan cloud account for remote access to the cameras.

3.3. Default network settings

Parameter	Default value
IP address	192.168.1.10
Username	admin
Password	admin

Note: Change the default password immediately after your first login. Go to Device settings > Users > User management.

4. Network settings

4.1. Searching for and configuring cameras with the Partizan software

Download the Partizan software from <https://apps.partizan.global/> and install it on your PC.

1. Launch the Partizan software.
2. Click Search in the left sidebar to scan the local network for Partizan devices.

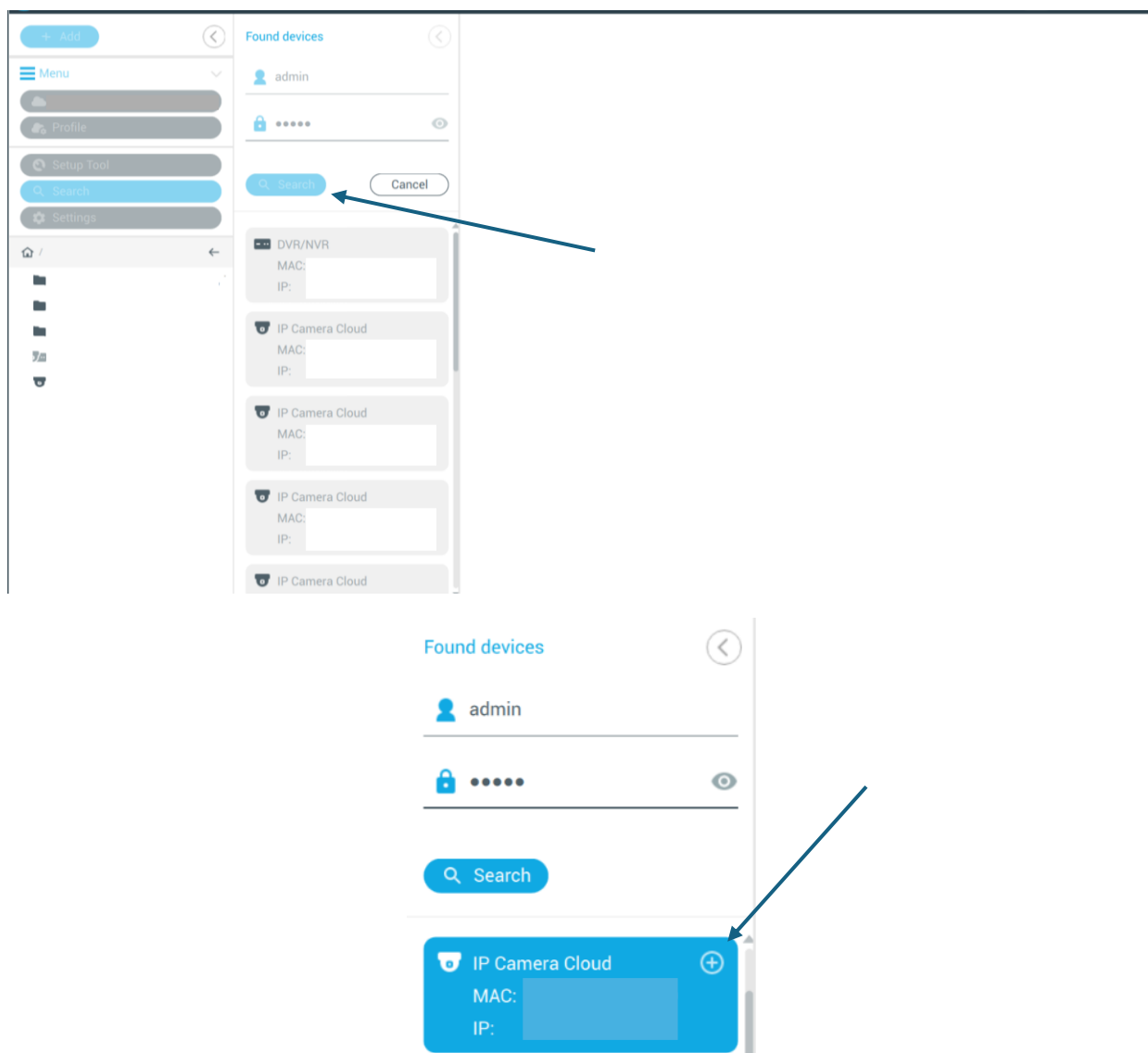


Fig. 4. Search panel — discovered devices appear in the list on the right

3. Select your camera from the list of discovered devices and click Add to add it to My devices.

4.2. Adding a device manually (+ Add button)

Click the blue + Add button in the top-left corner to add a device manually by IP, MAC address, or Partizan ID.

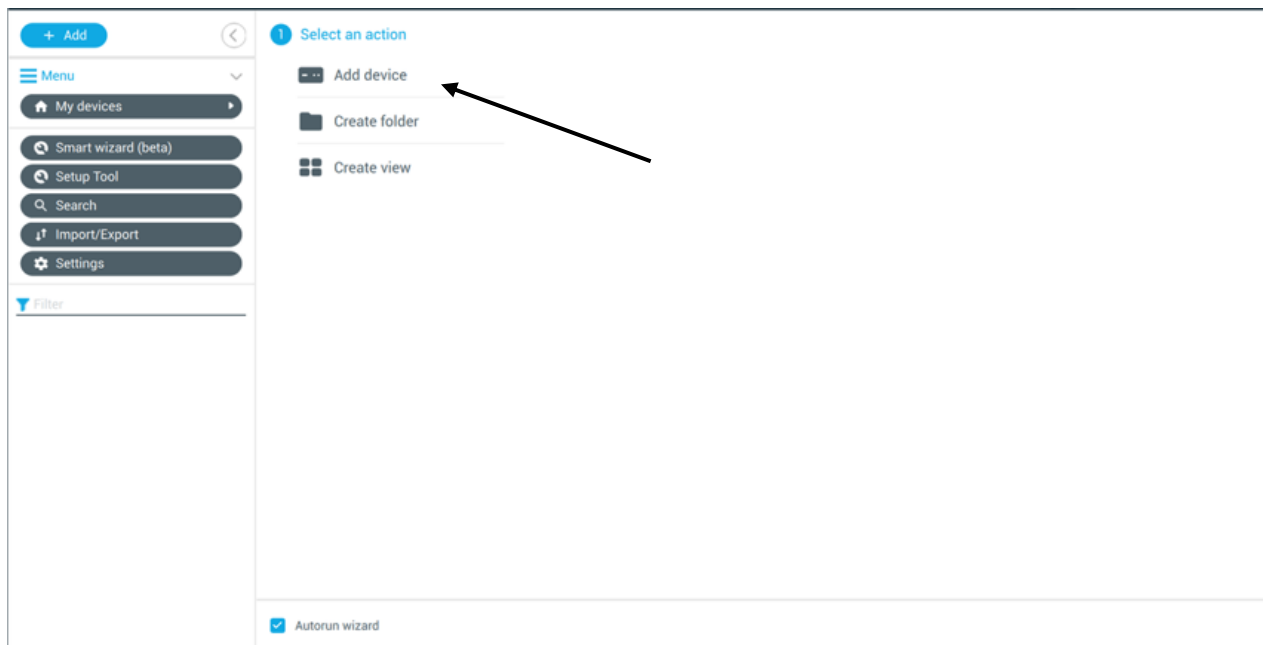


Fig. 5. + Add action panel — add a device, create a folder, or create a multi-camera view

4.3. My devices panel

Once added, cameras appear under My devices. Click any camera to open its live stream.

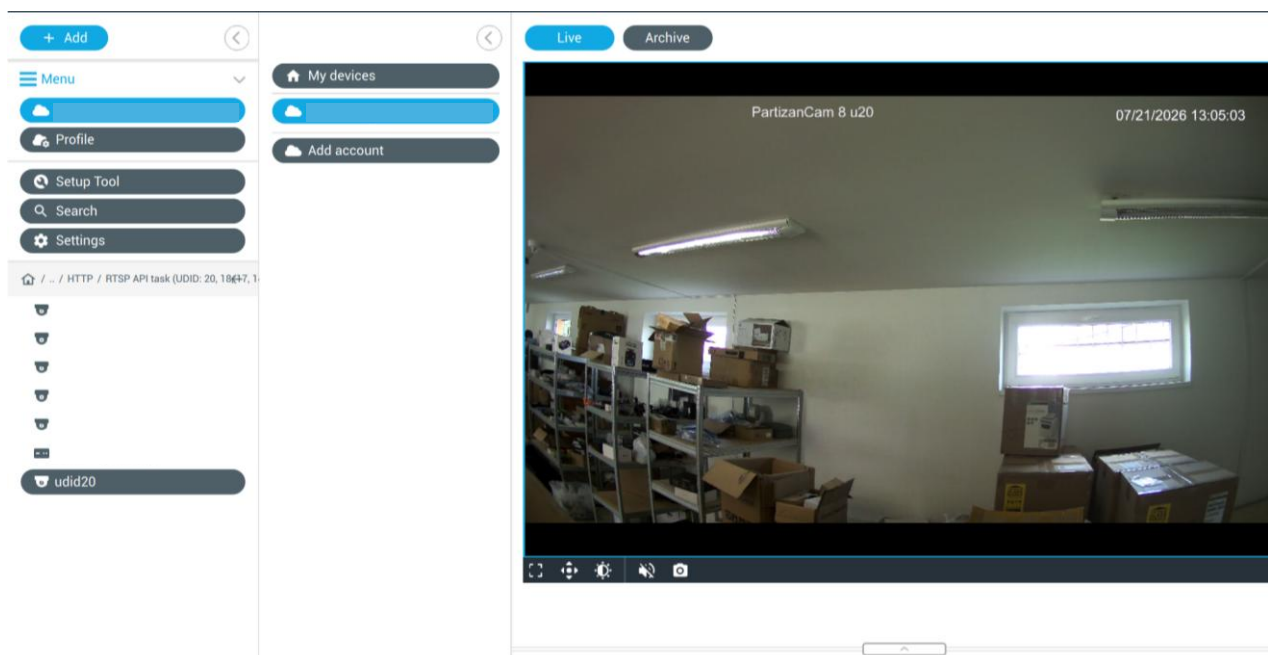
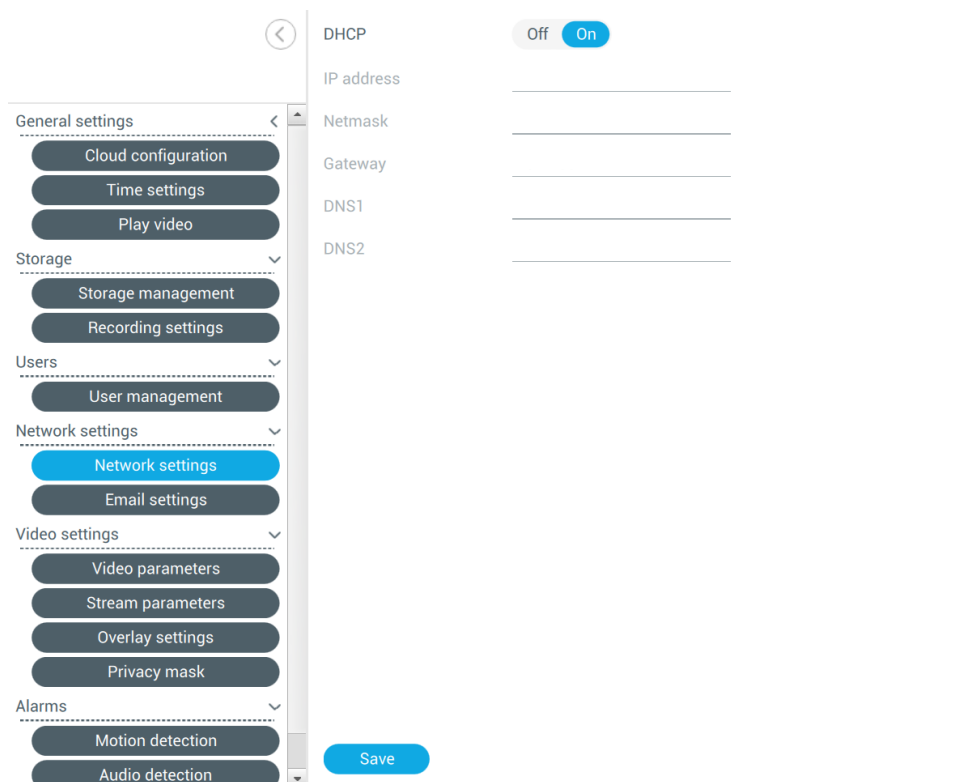


Fig. 6. My devices panel with a device list and the Add account option

4.4. Changing the IP address via the Partizan app

1. In the Partizan app, open the connection to the camera by entering its current IP address (default: 192.168.1.10).
2. Enter the login admin and password admin (if the default values have not been changed).
3. Go to Device settings > Network settings to change the IP address.



< DHCP Off On

IP address

Netmask

Gateway

DNS1

DNS2

General settings <

Cloud configuration

Time settings

Play video

Storage

Storage management

Recording settings

Users

User management

Network settings

Network settings

Email settings

Video settings

Video parameters

Stream parameters

Overlay settings

Privacy mask

Alarms

Motion detection

Audio detection

Save

Fig. 7. Network settings — DHCP, IP address, gateway, and DNS configuration

4. Turn off DHCP and enter all required details.
5. Click the “Save” button at the bottom of the screen.

5. Live view

Click any camera in the device list to open its live video stream. Use the Live and Archive tabs at the top to switch modes.

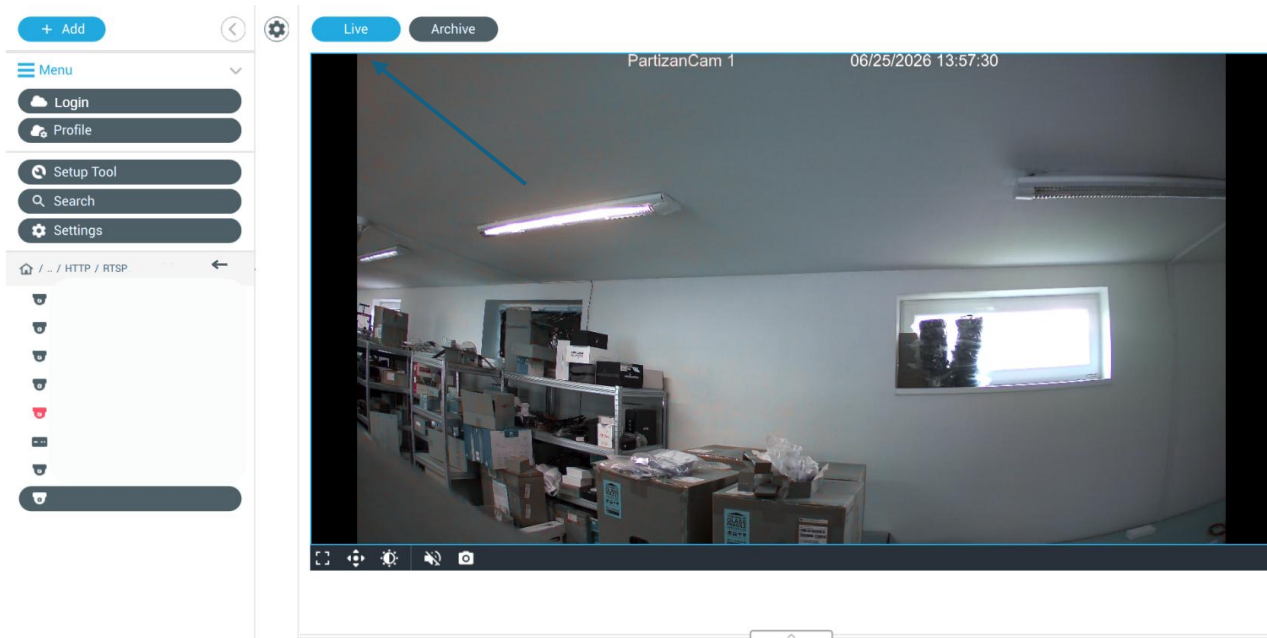


Fig. 8. Live view — real-time stream with camera name and timestamp overlay

Function	Description
 Full screen	Expands the video to full screen. Press Esc to exit full screen mode.
 PTZ / Move	Opens the pan-tilt-zoom controls, if the camera supports these functions.
 Brightness	Adjusts the image brightness and contrast settings.
 Mute	Turns the sound on or off for cameras with microphones.
 Snapshot	Takes a screenshot and saves it to the configured snapshot folder.

Note: To switch between cameras, simply click another device in the left panel. The stream updates immediately.

6. Archive playback

Click the Archive tab to switch from live view to playing back recorded footage.

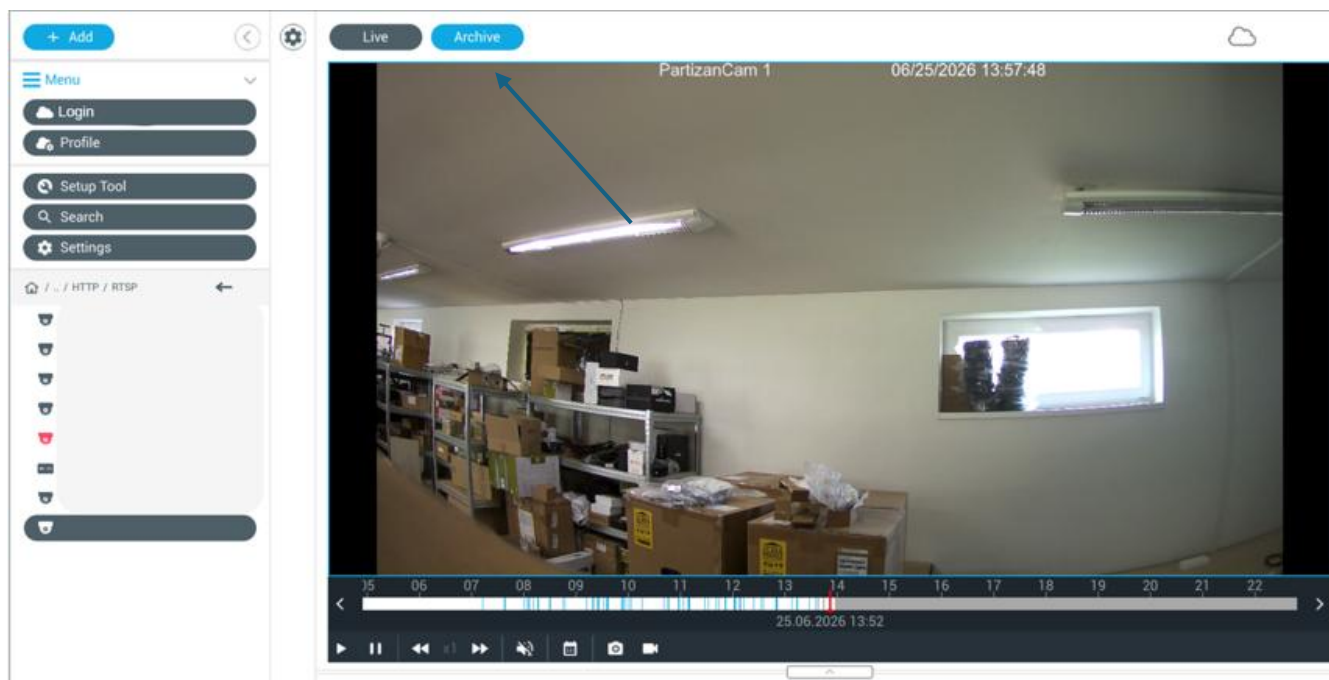


Fig. 9. Archive view — the timeline bar shows a 24-hour period; blue marks indicate recorded segments, white marks indicate the current playback position, and grey marks indicate no recording

Function	Description
► / Play/Pause	Starts or pauses playback.
◀◀ / ▶▶ Speed	Changes the playback speed. The x1 label shows the current speed.
📅 Calendar	Jump to a specific date and time in the archive.
📷 Snapshot	Save a screenshot of the current archive frame.
📂 Download	Export a video clip from the archive to your computer.

Note: Click anywhere on the timeline to jump to that moment. Drag the red cursor left or right to scrub through the footage.

7. Cloud account and remote access

7.1. Step 1 — entering the login and password

Click “Add account” in the left sidebar to connect your Partizan cloud account and get remote access to cameras registered in the cloud.

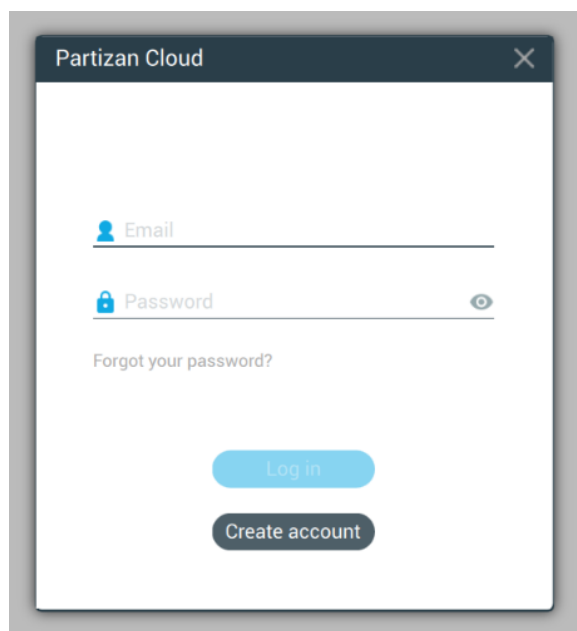


Fig. 10. User account

7.2. Mobile app — scan the QR code to add the camera

Every Partizan Cloud camera has a unique QR code on the Cloud configuration screen. Scan it with the Partizan mobile app (sequence: add device → scan QR code) to add the camera instantly, without having to enter the IP address manually.

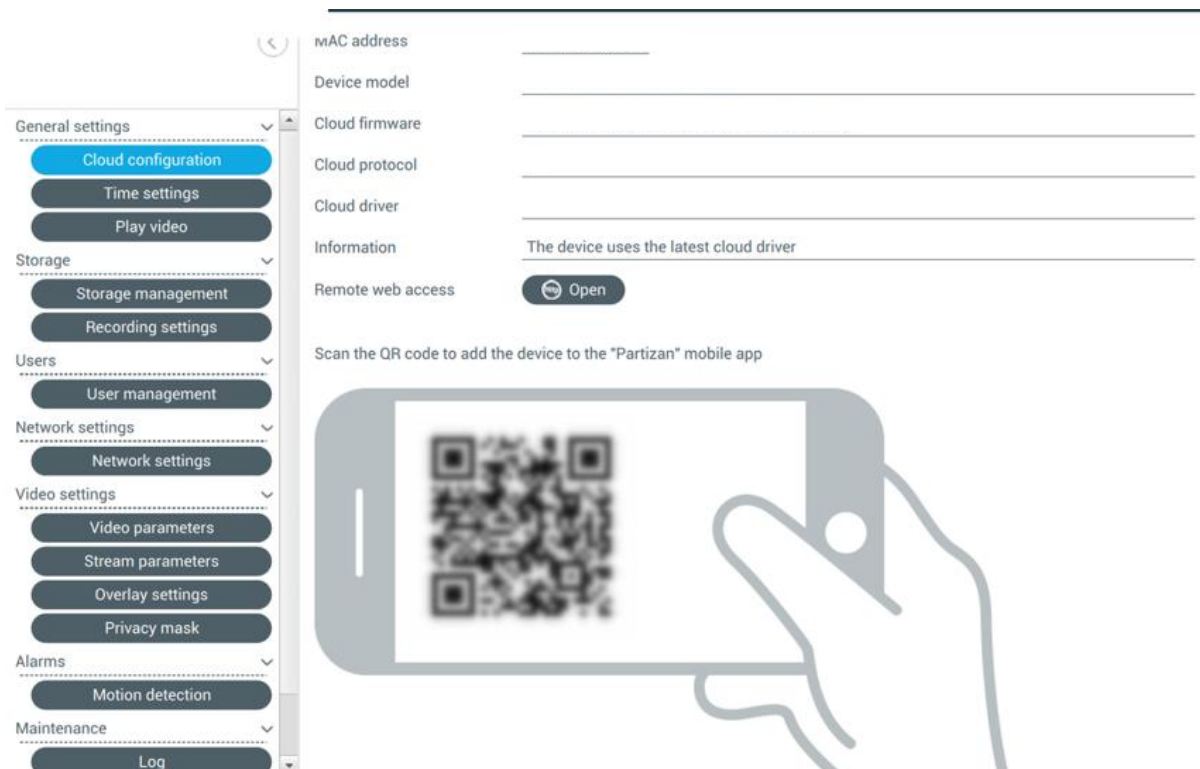


Fig. 11. Cloud configuration — device information and QR code for the mobile app

1. Open the Partizan mobile app (available on Google Play, the App Store, and Huawei AppGallery).
2. Sign in to your Partizan cloud account.
3. In the Partizan mobile app, tap "+", choose "Add device", and scan the QR code.

7.3. Downloading the Partizan software

Platform	Resource
PC (Windows 64-bit / macOS Intel & Apple Silicon / Ubuntu 24.04)	https://my.partizancloud.com/login
Android, iOS	https://my.partizancloud.com/login

8. Camera settings

Click any camera in the device list, then click the gear icon ⚙️ to open the configuration panel. The camera is identified by its MAC address at the top.

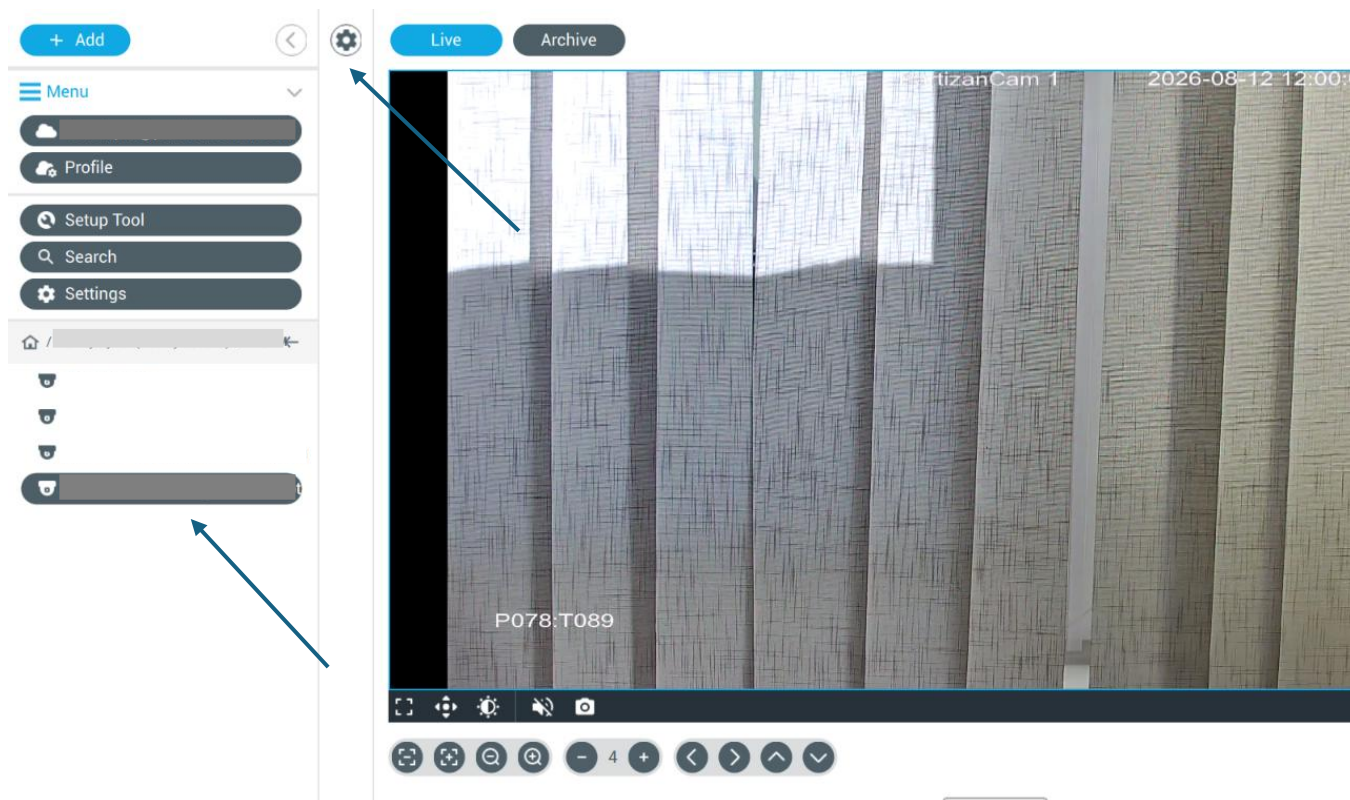


Fig. 12. Camera settings panel — all configuration categories in the sidebar on the left of the screen

8.1. Time settings

Set the camera clock, time zone, and NTP synchronisation.

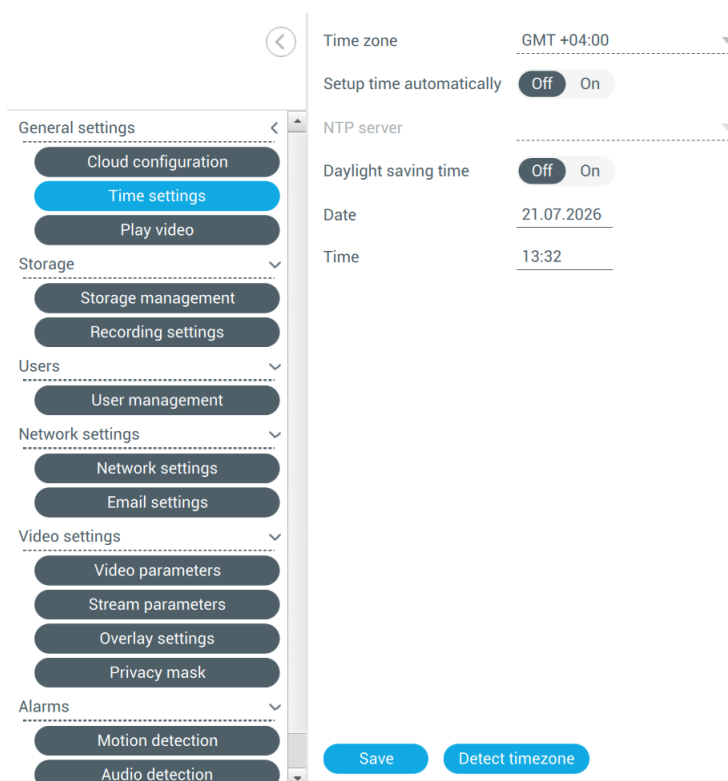


Fig. 13. Time settings — time zone, automatic NTP synchronisation, and daylight saving time

Setting	Description
Time zone	Select the local time zone for the camera.
Setup time automatically	When enabled, the device automatically synchronises its clock via NTP.
NTP server	NTP server address (default: pool.ntp.org).
Daylight saving time	Enable this to automatically adjust for seasonal time changes.
Detect timezone (at the bottom of the screen)	Automatically applies your computer's time zone to the camera.

8.2. Storage management

View and manage the camera's internal storage (SD card).

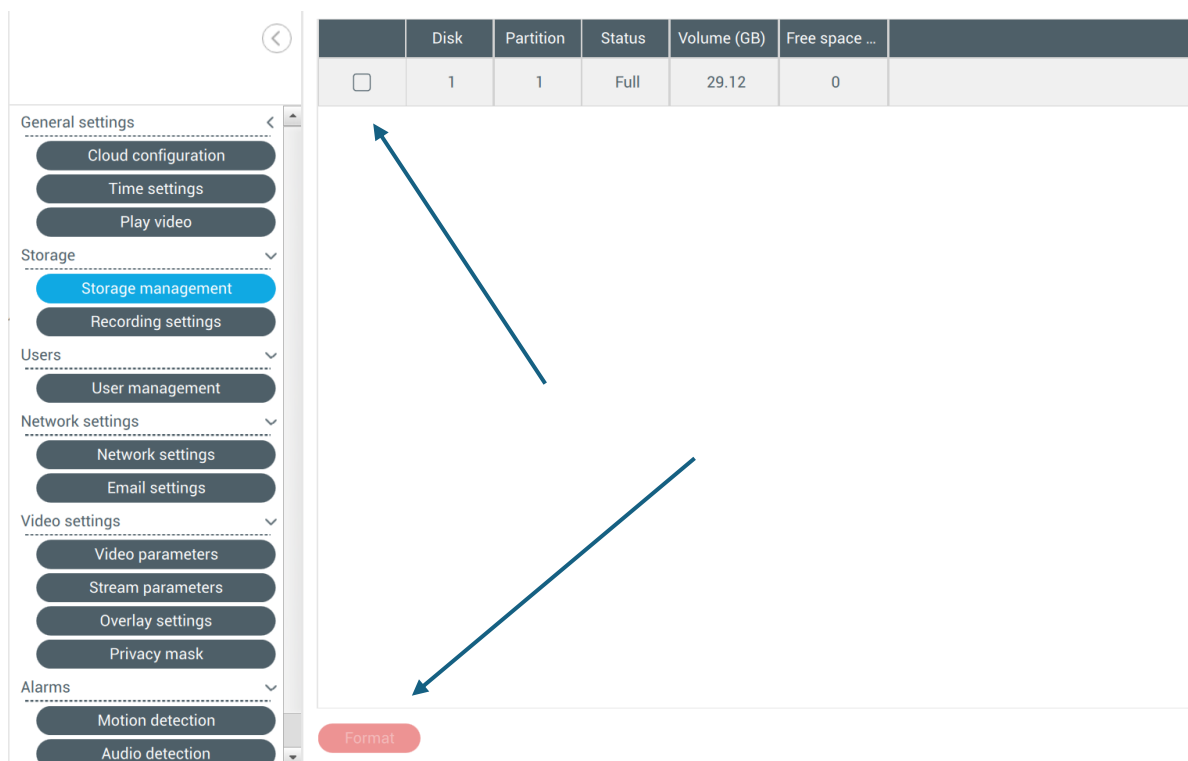


Fig. 14. Storage management — disk status, volume, and free space

To format the SD card, tick the checkbox next to the required card and click the “Format” button.

Note: If the storage shows Status: Full and Free space: 0, click Format to clear the storage before configuring recording.

8.3. Recording settings

Configure the recording schedule, mode, and camera channel.

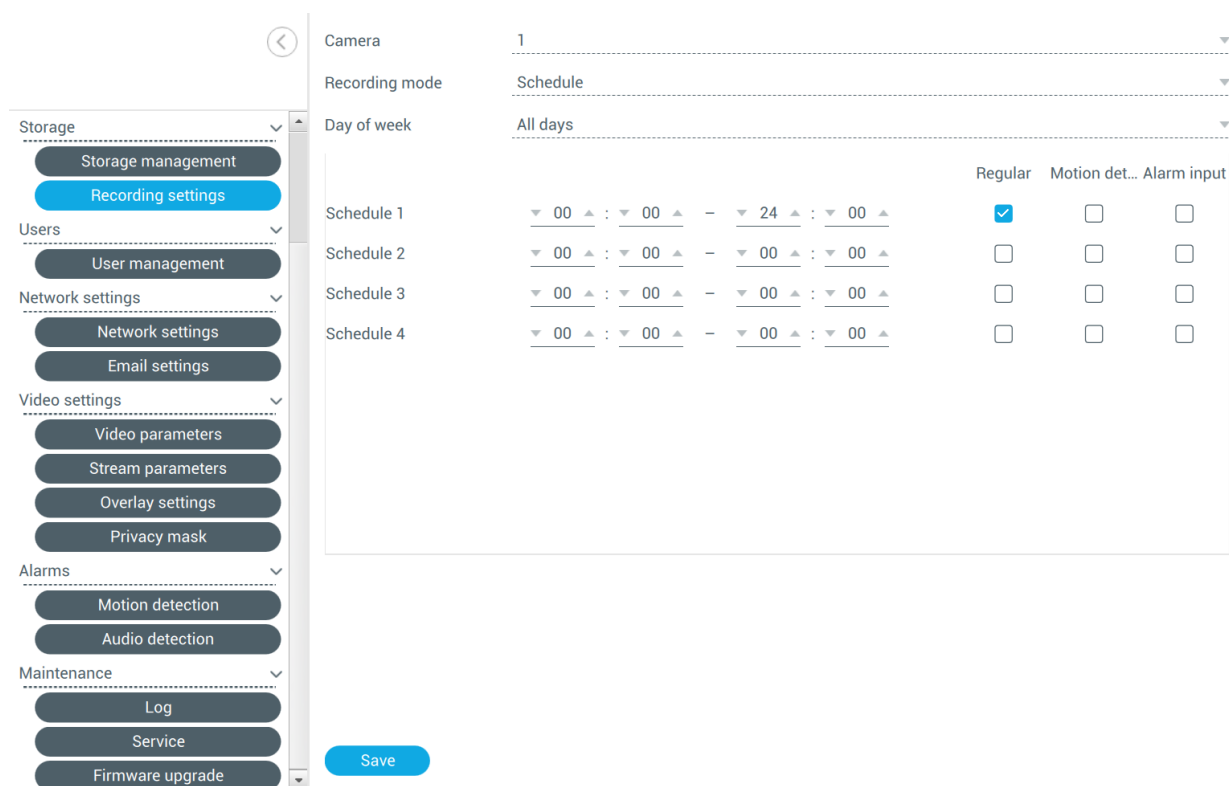


Fig. 15. Recording settings — schedule, recording mode, and day of week

Setting	Description
Camera	Select which camera channel to configure.
Recording mode	Schedule, Continuous, or Motion-triggered.
Day of week	Apply the schedule to all days or to specific days.
Schedule 1–4	Define up to 4 time slots with a recording type (Regular / Motion / Alarm).

8.4. User management

Add or edit user accounts and configure access rights for each user.

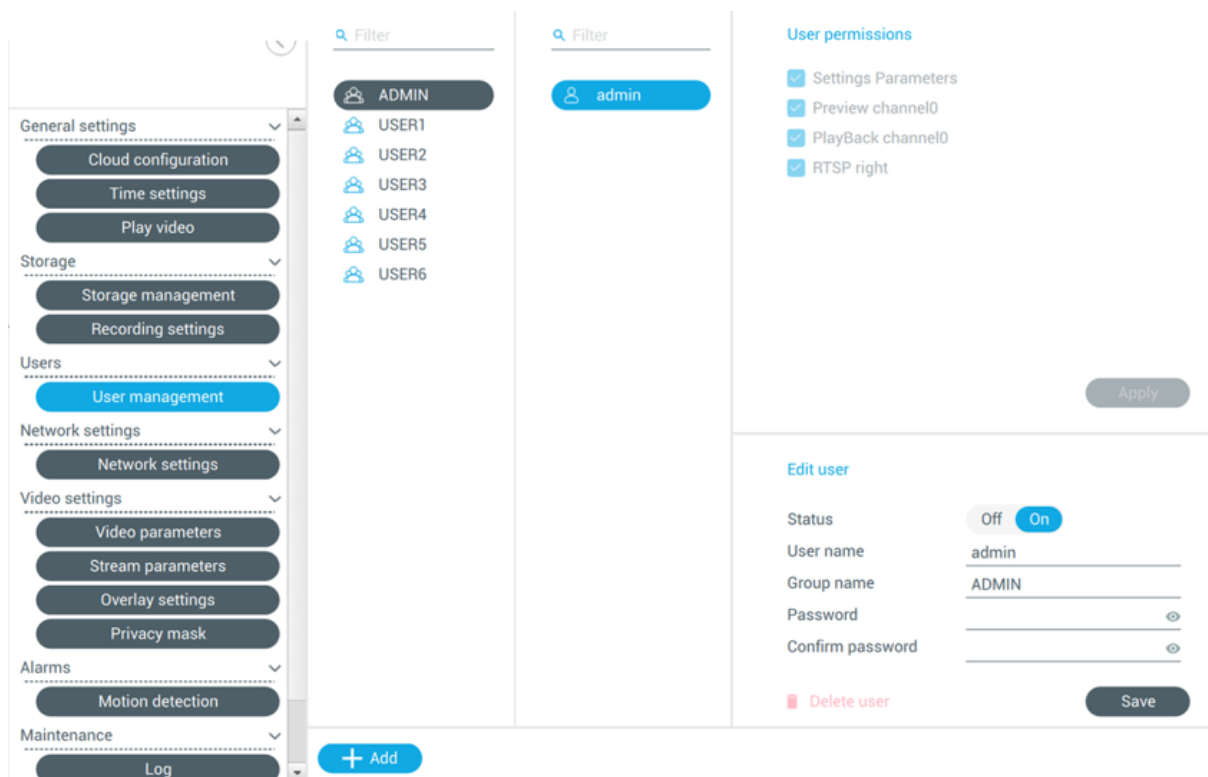


Fig. 16. User management — user list, permissions, and the user edit panel

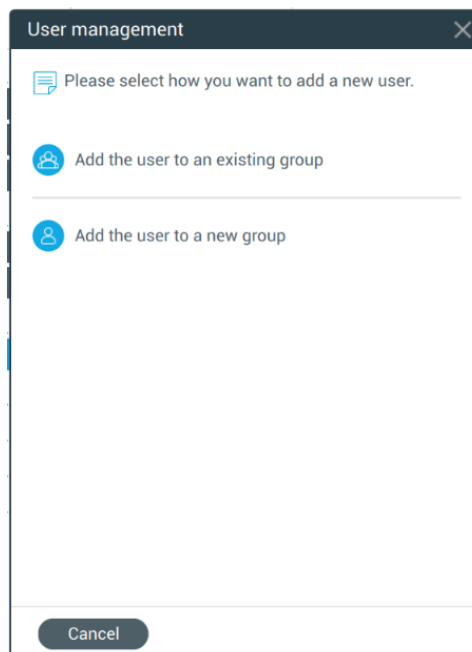


Fig. 17. User adding options

Setting	Description
Username	The login for this user account.
Group name	ADMIN or USER — sets the default level of permissions.
Password	Set or change the user's password. Use the eye icon to reveal it.
Permissions	Settings Parameters, Preview, Playback, RTSP access. The number of permissions available to users depends on the camera's capabilities.
Add	Lets you add a new user to an existing permission group, or create a new group with its own access rights.

8.5. Video parameters

Configure day/night mode, mirror image, 180-degree rotation, and the IR filter.

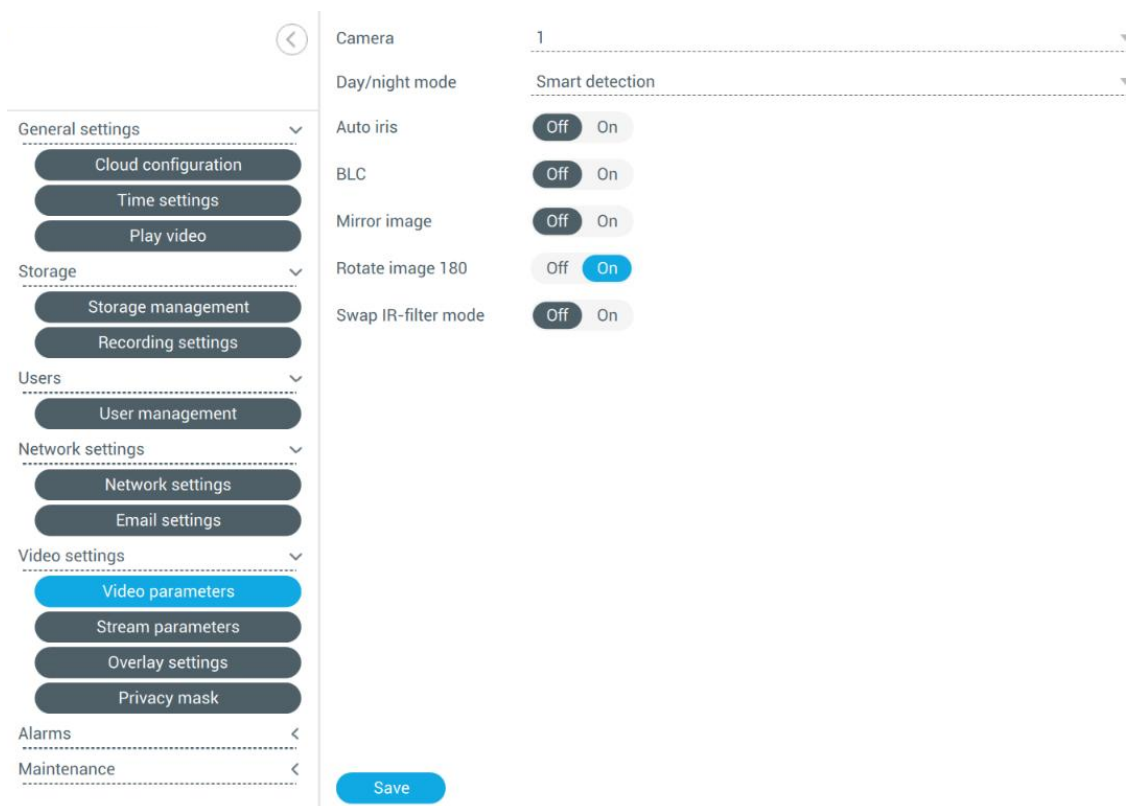


Fig. 17. Video parameters — day/night mode, BLC, mirror image, 180-degree rotation, IR filter

Setting	Description
Camera	Select the camera channel for which you want to configure the video parameters (relevant for multi-channel devices).
Day/night mode	Determines when the camera switches between colour (day) and black-and-white IR (night) mode: Auto, Day only, Night only, or Schedule.
BLC	Back Light Compensation — improves the visibility of objects against a bright light source behind them, such as a window.
Mirror image	Mirrors the image horizontally. Used depending on how the camera is mounted.
Rotate image 180	Flips the image by 180° — used when the camera is mounted upside down, for example on a ceiling.
Swap IR-filter mode	Controls the mechanical IR filter: automatically removes or returns the filter depending on the light level, for accurate colour rendering by day and a clear image at night.

8.6. Stream parameters

Set the resolution, frame rate, codec, and bitrate for the main, sub, and mobile streams.

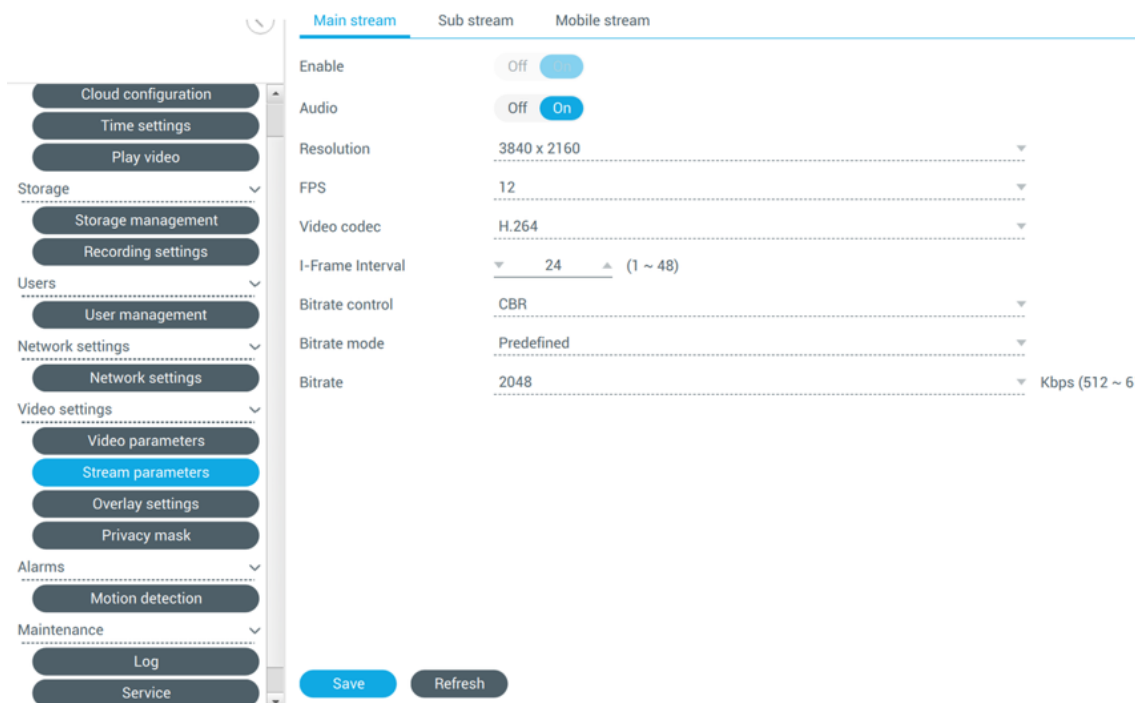


Fig. 18. Stream parameters — resolution, FPS, codec, bitrate

Setting	Description
Resolution	The video resolution (e.g. 3840×2160 for 4K), which can be changed as needed.
Audio	Enables or disables audio transmission in the stream (if a built-in or connected microphone is available).
FPS	Frames per second — higher values give smoother video but require more storage space.
Video codec	H.264 (default) or H.265 for better compression.
Bitrate control	CBR (constant) or VBR (variable) bitrate.
Bitrate	The data transmission rate, in Kbps.
I-Frame Interval	The interval between reference frames (I-frames) in the video stream. A lower value improves archive-seeking accuracy but increases the bitrate; a higher value saves bandwidth and storage space.

8.7. Overlay settings

Configure the on-screen display — camera name, timestamp, date format, and text colour.

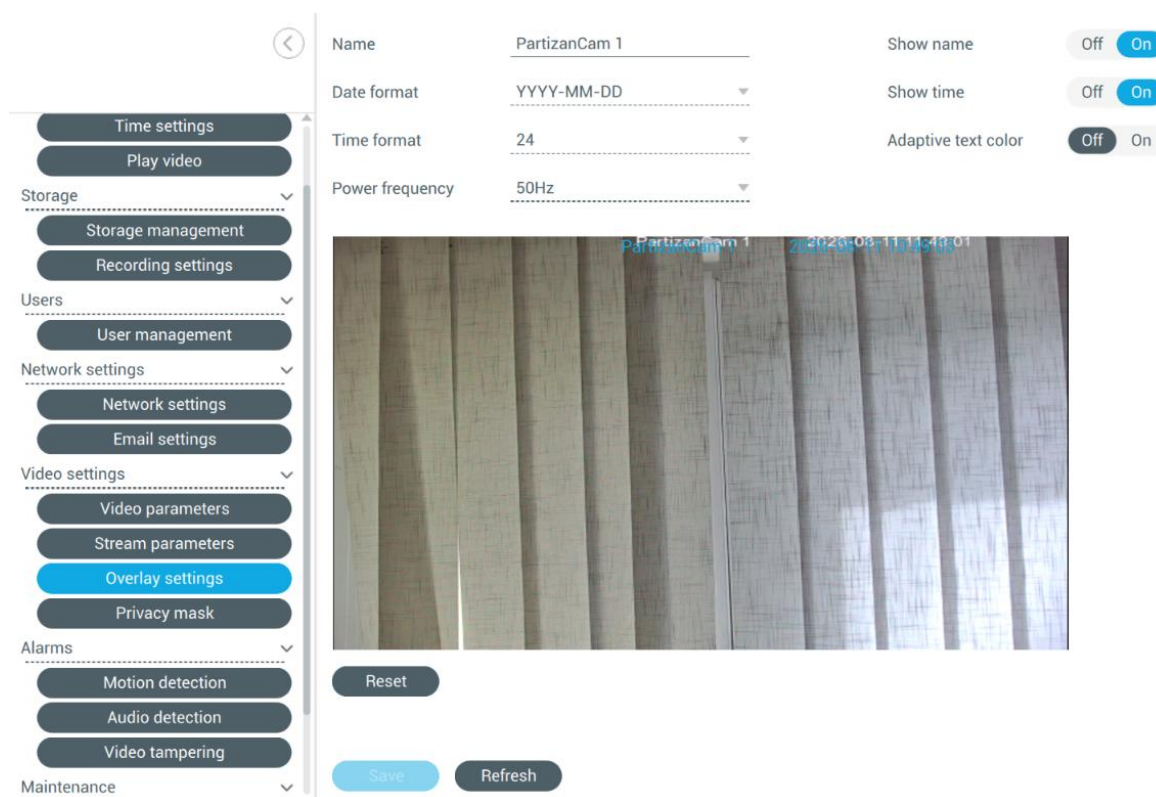


Fig. 19. Overlay settings — camera name, date/time format, flicker reduction, adaptive text colour

Setting	Description
Name	The text overlaid on the video image (e.g. the camera or location name). Displayed in the corner of the frame.
Date format	The date display format on the video image (e.g. DD-MM-YYYY or MM-DD-YYYY).
Time format	The time display format — 12-hour or 24-hour.
Power frequency (Hz)	The mains power frequency (50 Hz or 60 Hz) — affects flicker suppression from artificial lighting.
Flicker reduction	Suppresses image flicker from artificial lighting by matching the sensor's exposure to the mains frequency.
Show name	Turns the display of the camera name on the video image on or off.

Show time	Turns the display of the timestamp on the video image on or off.
Adaptive text color	Automatically changes the overlay text colour depending on the background brightness for better readability.
Reset	Resets all overlay settings to their default values.

8.8. Privacy mask

Enable the privacy mask to block certain areas of the camera view from being displayed. Click the “On” button to start configuring it.

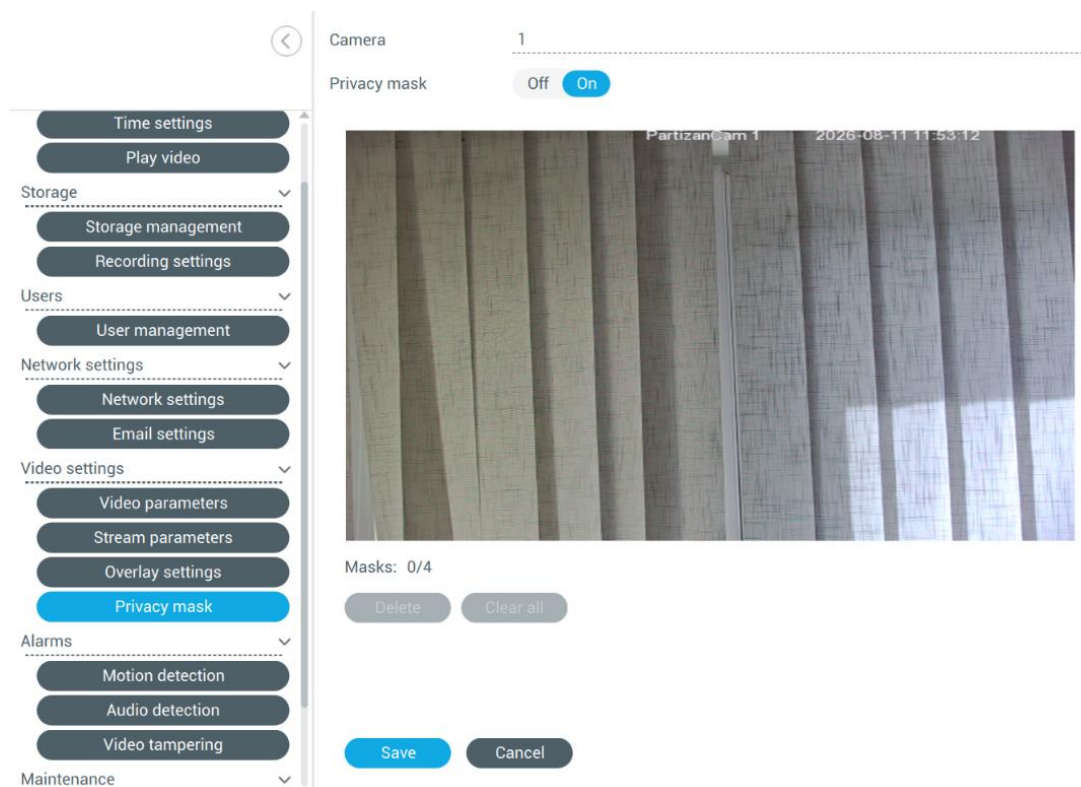


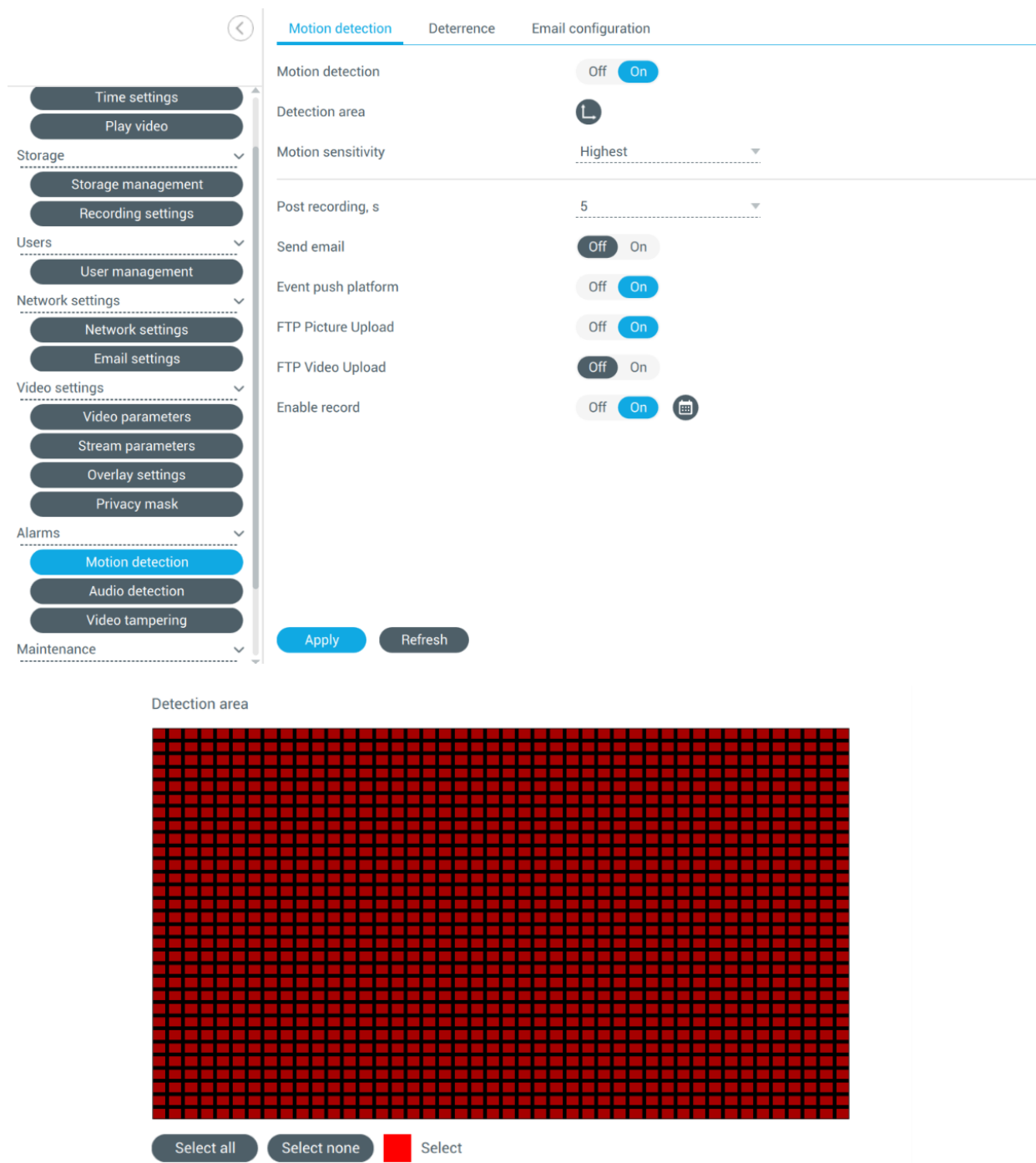
Fig. 20. Privacy mask — turn on/off for each camera channel

Setting	Description
Camera	Select the camera channel for which you want to configure the privacy mask.
Privacy mask	First enable the feature with the toggle, then draw one or more zones on the camera image to hide them from viewing and recording.
Delete	Deletes the selected mask zone.
Clear all	Deletes all created mask zones at once.

9. Alarms

9.1. Motion detection

Configure how the camera detects and responds to motion events. Click the “On” button to start configuring it.



The screenshot displays the 'Motion detection' configuration page. On the left, a sidebar menu lists various settings categories, with 'Alarms' expanded to show 'Motion detection', 'Audio detection', and 'Video tampering'. The main content area has three tabs: 'Motion detection' (selected), 'Deterrence', and 'Email configuration'. Under the 'Motion detection' tab, the following settings are visible:

- Motion detection:** A toggle switch set to 'On'.
- Detection area:** A red grid icon representing the detection area.
- Motion sensitivity:** A dropdown menu set to 'Highest'.
- Post recording, s:** A dropdown menu set to '5'.
- Send email:** A toggle switch set to 'On'.
- Event push platform:** A toggle switch set to 'On'.
- FTP Picture Upload:** A toggle switch set to 'On'.
- FTP Video Upload:** A toggle switch set to 'On'.
- Enable record:** A toggle switch set to 'On'.

At the bottom of the page, there is a large red grid representing the 'Detection area'. Below the grid are three buttons: 'Select all', 'Select none', and a red square icon labeled 'Select'.

Fig. 21. Motion detection — detection area, sensitivity, recording trigger, and email notifications

Setting	Description
Detection area	On/Off — enables detection. Click the zone-selection icon to draw the detection area.
Motion sensitivity	Lowest / Low / Medium / High / Highest — controls the alarm threshold.
Post recording, s	When set, this defines how long the camera keeps recording (in seconds) after motion detection has stopped detecting motion — i.e. how many seconds of recording continue AFTER the event.
Send email	When enabled, an email notification is sent on motion. Requires the email server to be configured.
FTP Picture/Video Upload	Automatically sends a photo or a short video clip of the event to the specified FTP server.
Select all	Highlights the entire detection area in red. The selected zone is marked in red.
Select none	Clears the selection from the entire detection area (deselects the selected zone).

Note: High sensitivity may cause false alarms due to changes in lighting or shadows. Start with Medium and adjust as needed.

9.2. Audio detection

Configure how the camera detects and responds to audio events. Click the “On” button to start configuring it.

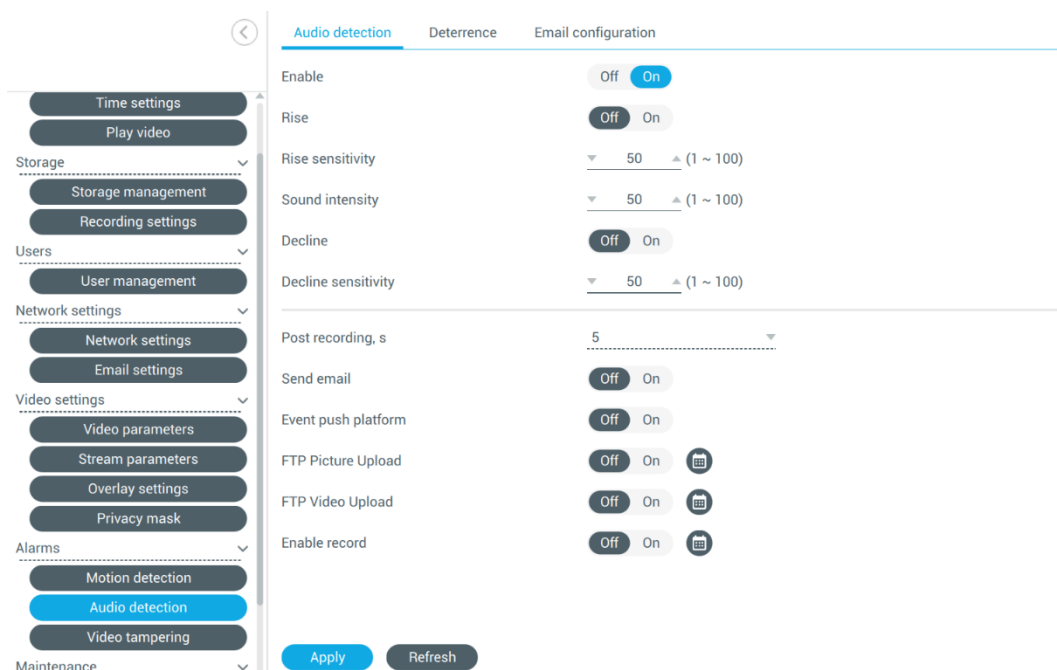


Fig. 23. Audio detection

Setting	Description
Rise	Detects a sudden increase in sound level (e.g. a shout or a bang).
Rise sensitivity	The sensitivity threshold for triggering on a rise in volume: the lower the value, the smaller the change in sound needed to trigger the alarm.
Sound intensity	The overall microphone sensitivity threshold for detecting sound activity.
Decline	Detects a sudden drop in sound level (e.g. sudden silence).
Decline sensitivity	The sensitivity threshold for triggering on a drop in volume.
Post recording, s	How long recording continues after the audio event ends.
Send email	Sends a notification (e.g. by email) when audio detection is triggered.
FTP Picture/Video Upload	Automatically sends a photo or a short video clip of the event to the specified FTP server.

9.3. Video tampering

Click the “On” button to start configuring it.

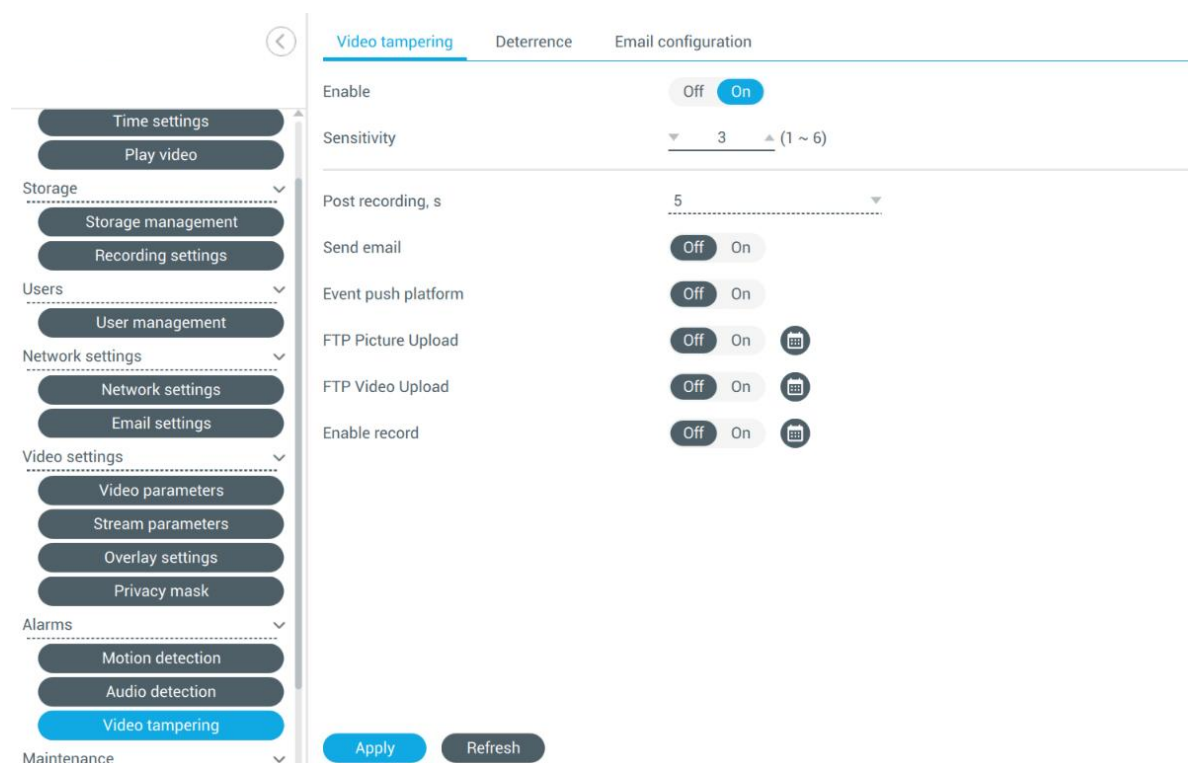
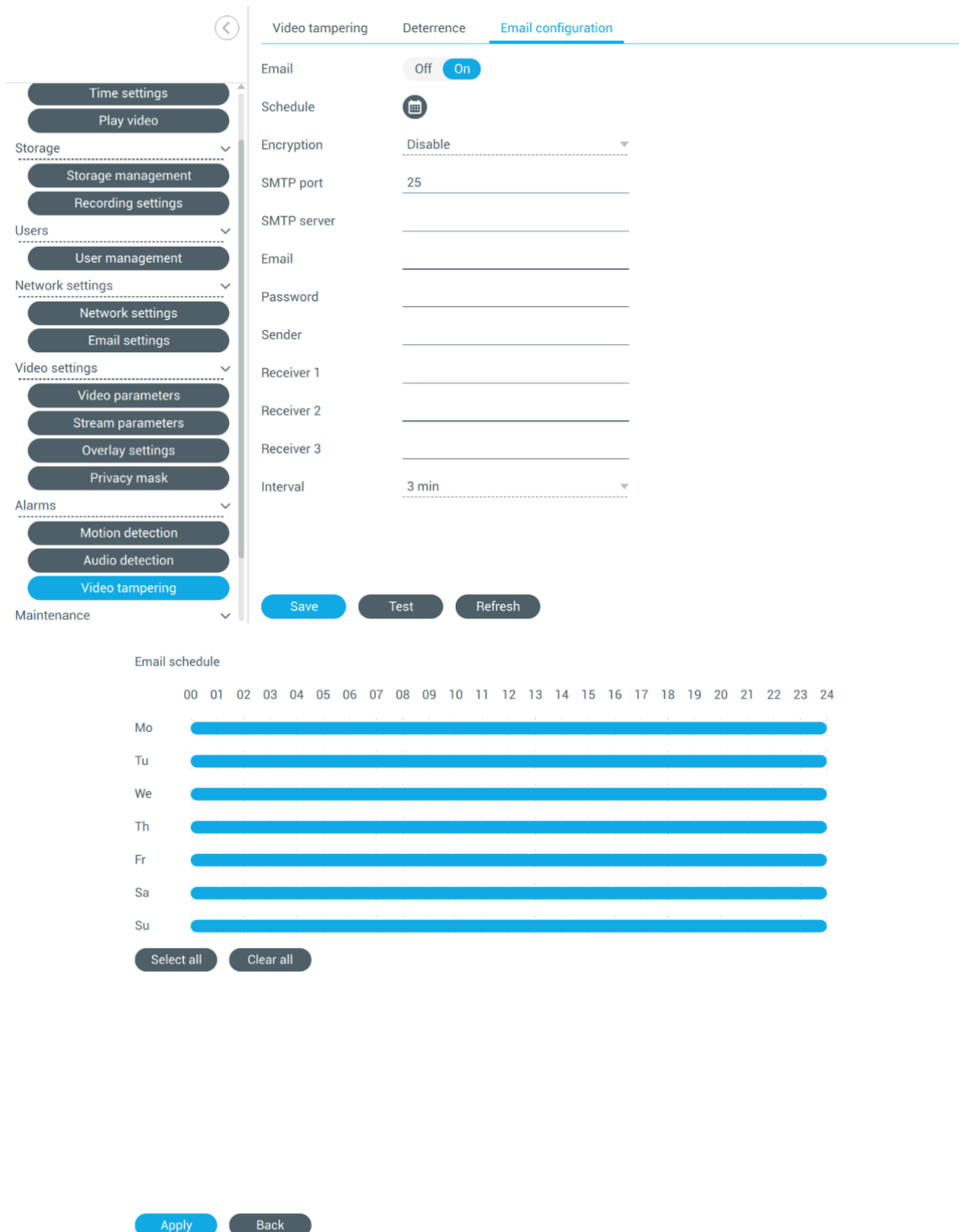


Fig. 24. Video tampering

Setting	Description
Sensitivity	The sensitivity threshold for detecting tampering with the camera: lens covering, a change in viewing angle, or defocusing.
Post recording, s	How long recording continues after the event ends.
Send email	Sends a notification about a detected tampering attempt.
FTP Picture/Video Upload	Automatically sends a photo or a short video clip of the event to the specified FTP server.

9.4. Email notification settings

A separate email notification setup is available for each type of alarm. Click the “On” button to start configuring it.



The screenshot shows the 'Email configuration' tab selected in the settings menu. The left sidebar contains a list of settings categories: Time settings, Play video, Storage, Users, Network settings, Video settings, Alarms, and Maintenance. The 'Alarms' category is expanded, showing 'Motion detection', 'Audio detection', and 'Video tampering' (which is selected). The main content area displays the email configuration settings for the selected alarm type. The settings include: Email (On), Schedule (calendar icon), Encryption (Disable), SMTP port (25), SMTP server, Email, Password, Sender, Receiver 1, Receiver 2, Receiver 3, and Interval (3 min). Below the settings are 'Save', 'Test', and 'Refresh' buttons. At the bottom, there is an 'Email schedule' section with a 24-hour timeline (00 to 24) and a grid for selecting email notification times for each day of the week (Mo, Tu, We, Th, Fr, Sa, Su). The 'Select all' and 'Clear all' buttons are located below the grid. At the very bottom, there are 'Apply' and 'Back' buttons.

Fig. 25. Email settings

Setting	Description
Schedule	The time slots during which emails may be sent for this specific type of alarm. Click the calendar icon to open the schedule grid and fill it in by marking the required time slots.
Encryption	The type of encryption for the connection to the mail server. Four values are available: Disable — no encryption, SSL, TLS, Auto — the device chooses automatically. The value must match your email provider's requirements and be consistent with the port number.
SMTP port	The mail server port for outgoing emails. Only digits are accepted, the valid range is 1–65535, and the default value is 25. The most common combinations are: 465 for SSL, 587 for TLS, 25 with no encryption. Port 25 is often blocked by internet providers for external mail services.
SMTP server	The SMTP server address of your email provider, e.g. smtp.gmail.com. Enter only the hostname — without the smtp:// prefix and without a port number.
Email	The email address the device uses to authenticate with the SMTP server.
Password	The password for the specified mailbox. If a password is already saved on the device, the field shows eight placeholder dots — this means a password is set; the device simply does not return it. Leave the field blank to keep the existing password. Enter a value only when you want to change it. Mailboxes with two-step verification (Gmail, Outlook, and similar) require a separate app password rather than the regular account password.
Sender	The address that will be shown as the email sender. The device itself allows this field to be left blank, but most mail servers reject emails where the sender does not match the authentication address, so it's best to enter the same address as in the Email field. The value is normalised in the process — the “@” and “.” characters are stripped out.
Receiver 1-3	Up to three addresses to which notifications will be sent. You don't have to fill in all three — empty fields are simply not used — but at least one address must be provided if the Email toggle is enabled, otherwise the device will refuse to save.
Interval	The minimum time between two emails about the same type of event: 1, 3, 5, or 10 minutes, with a default of 3. This protects against a flood of emails when an alarm is triggered repeatedly. Events that occur within this interval after a sent email are not duplicated in separate emails.

Note: Be sure to save the settings when you're done. You can send a test email to check the connection.

Motion detection

Deterrence

Email configuration

Email

Off On

Schedule



Encryption

TLS

SMTP port

587

SMTP server

smtp.gmail.com

Email

myname@gmail.com

Password

••••••••••••••••

Sender

myname@gmail.com

Receiver 1

receiver@gmail.com

Receiver 2

Receiver 3

Interval

1 min

Save

Test

Refresh

Fig. 26. Example of completed email notification settings

Where to get an app password:

1. Enable two-step verification on your Google account — without it, app passwords are unavailable.
2. Open <https://myaccount.google.com/apppasswords>.
3. Create a new password, giving it any name, e.g. "Partizan".
4. Copy the 16 characters and enter them in the Password field.

Procedure:

1. Fill in the fields as described in the table.
2. Fill in the schedule.
3. Click Save.
4. Click Test and wait for the result — the check is performed by the device, so the response may arrive with a slight delay. You should receive an email containing the MAC address of the selected device and the message “this is the email test”.

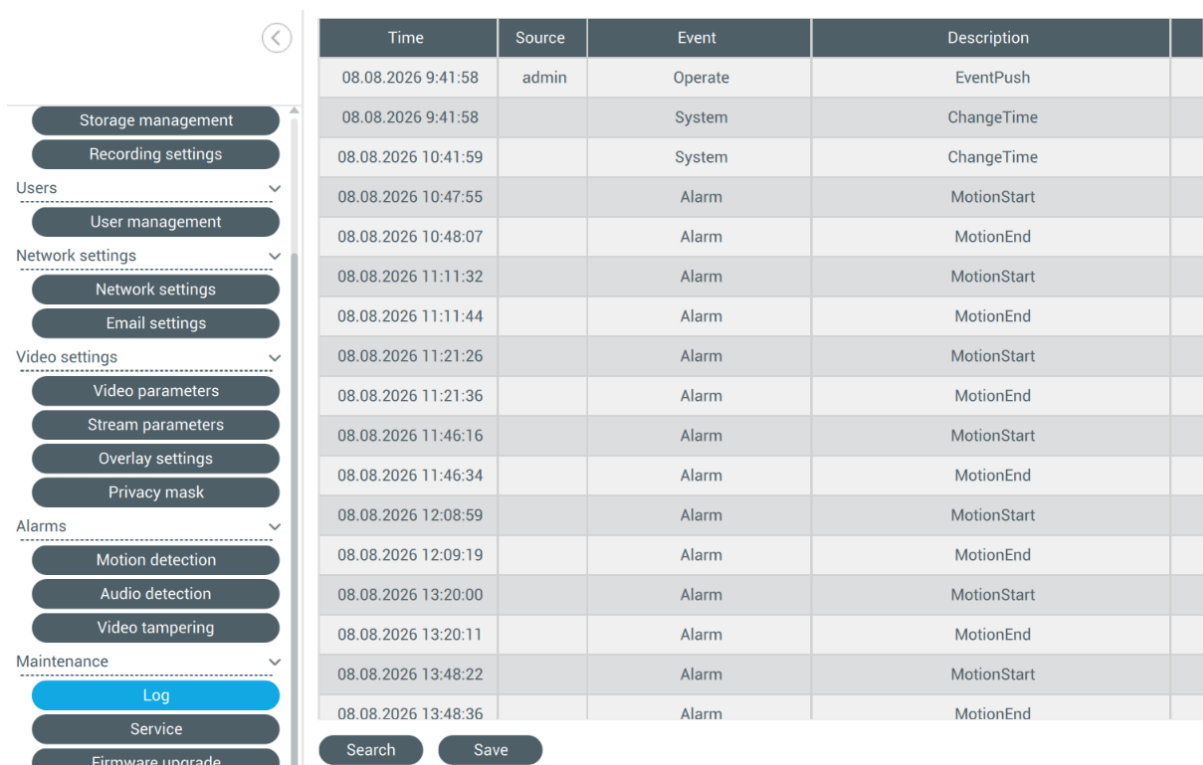
Common errors:

- A regular account password was entered. Gmail will reject it — an app password is required.
- There is no App passwords section. This means two-step verification is disabled — enable it and try again.
- Port 25 was selected. Gmail does not work on this port, and many providers block it as well.
- The port does not match the encryption type. 587 works only with TLS, 465 only with SSL.

10. Maintenance

10.1. Event log

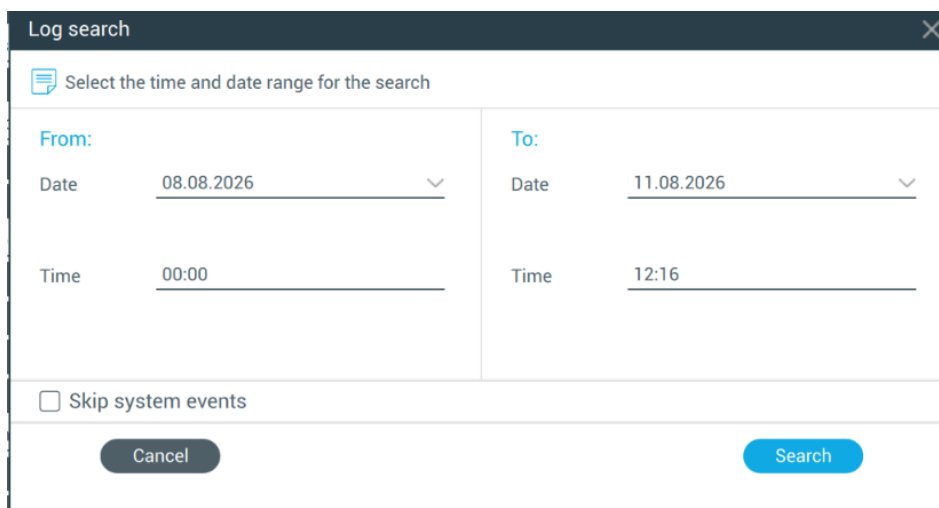
The log screen shows a list of all camera events with timestamps — motion start/end, alarms, and system events.



The screenshot shows the Event Log interface. On the left is a sidebar with navigation options: Storage management, Recording settings, Users (User management), Network settings (Network settings, Email settings), Video settings (Video parameters, Stream parameters, Overlay settings, Privacy mask), Alarms (Motion detection, Audio detection, Video tampering), and Maintenance (Log, Service, Firmware upgrade). The 'Log' option is highlighted. The main area displays a table of events with columns: Time, Source, Event, and Description.

Time	Source	Event	Description
08.08.2026 9:41:58	admin	Operate	EventPush
08.08.2026 9:41:58		System	ChangeTime
08.08.2026 10:41:59		System	ChangeTime
08.08.2026 10:47:55		Alarm	MotionStart
08.08.2026 10:48:07		Alarm	MotionEnd
08.08.2026 11:11:32		Alarm	MotionStart
08.08.2026 11:11:44		Alarm	MotionEnd
08.08.2026 11:21:26		Alarm	MotionStart
08.08.2026 11:21:36		Alarm	MotionEnd
08.08.2026 11:46:16		Alarm	MotionStart
08.08.2026 11:46:34		Alarm	MotionEnd
08.08.2026 12:08:59		Alarm	MotionStart
08.08.2026 12:09:19		Alarm	MotionEnd
08.08.2026 13:20:00		Alarm	MotionStart
08.08.2026 13:20:11		Alarm	MotionEnd
08.08.2026 13:48:22		Alarm	MotionStart
08.08.2026 13:48:36		Alarm	MotionEnd

At the bottom of the table are 'Search' and 'Save' buttons.



The screenshot shows the 'Log search' dialog box. It has a title bar with a close button. Below the title bar is a section with a magnifying glass icon and the text 'Select the time and date range for the search'. There are two columns for date and time selection. The 'From' column has 'Date' set to '08.08.2026' and 'Time' set to '00:00'. The 'To' column has 'Date' set to '11.08.2026' and 'Time' set to '12:16'. Below these fields is a checkbox labeled 'Skip system events'. At the bottom are 'Cancel' and 'Search' buttons.

Fig. 27. Event log — list of motion and alarm events with timestamps

Use the search function to filter events for a specific time period: enter the start date and time on the left, the end date and time on the right, then click the “Search” button. The results list shows: event time, source (camera), event type, and status.

10.2. Service — reboot and restore default settings

Use the Service screen to reboot the camera or restore the factory default settings.

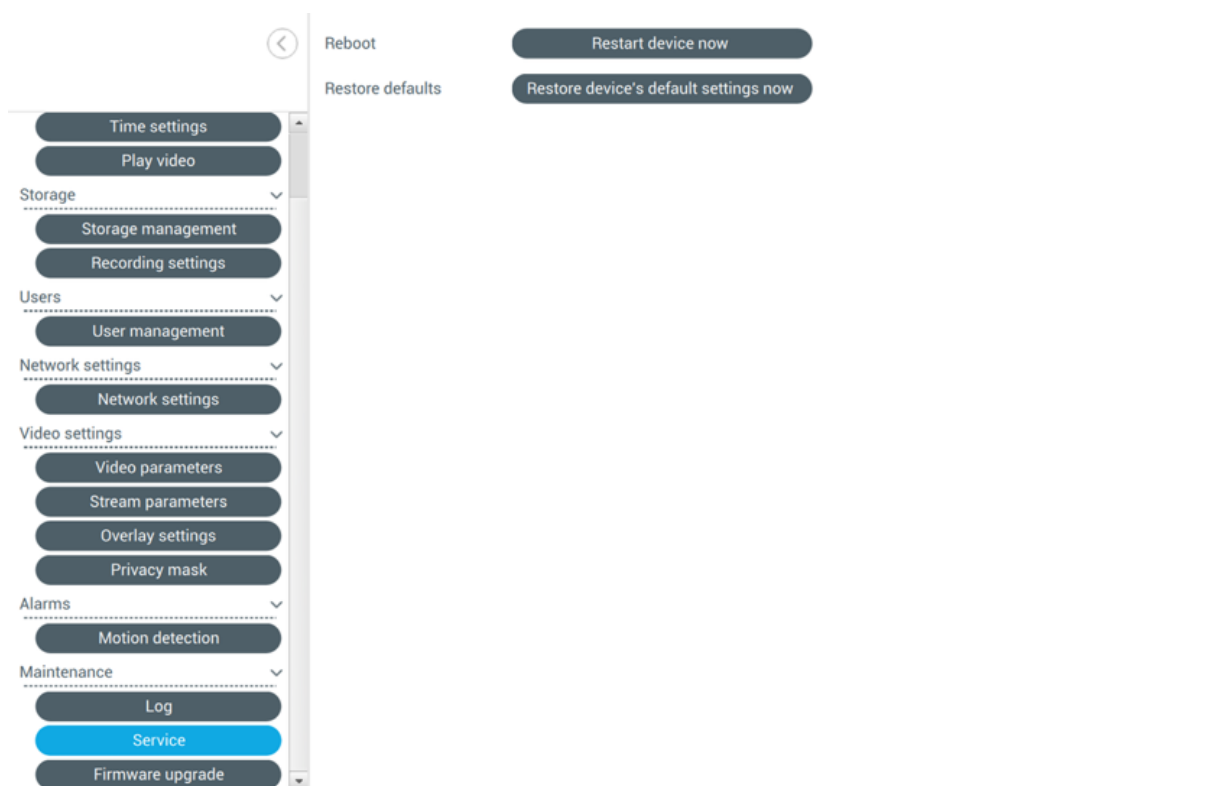


Fig. 28. Service — reboot the device and restore default settings

Reboot — restarts the camera while keeping all current settings. Restore defaults — resets the camera to its factory settings (see the note below).

Note: Restoring the default settings will remove all custom settings, including the network configuration and user accounts.

10.3. Firmware upgrade

Keep your camera up to date by updating its firmware directly from the Partizan software.

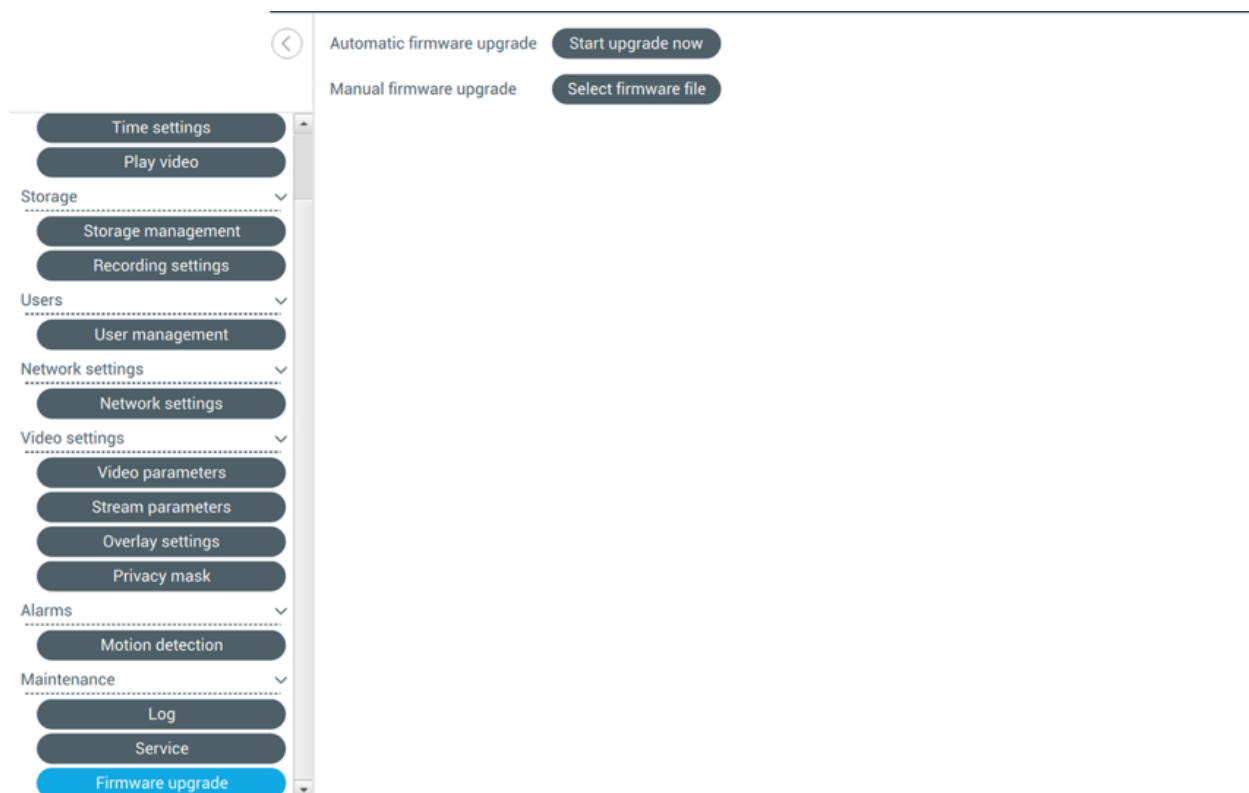


Fig. 29. Firmware upgrade — automatic (cloud) or manual (local file)

Method	Description
Automatic firmware upgrade	Click Start upgrade now — the camera automatically downloads and installs the latest firmware from the Partizan cloud.
Manual firmware upgrade	Click Select firmware file — choose a locally downloaded firmware file to install. Only Partizan firmware files in .pbi format are supported.

Note: Do not turn off the camera while the firmware is updating. The process may take a few minutes.

Contacts:

WhatsApp: +420 777 054 888

Email: support@partizan.global

Telegram: https://t.me/PartizanSupport_bot