MONITOREAL

Monitoreal User Guide

Version 2.5.1

Operation and administration of the web interface

For operators, installers and administrators

Verified interface: SPARTAN 2.5.1

This guide documents the inspected release build.

Contents

Select a chapter title to jump to its instructions.

01 About this guide 3
02 Getting started 4
03 Finding your way around 5
04 Everyday monitoring 7
05 Finding detections 8
06 Playing and exporting recordings 10
07 Managing archive storage 11
08 Adding and managing cameras 13
09 Configuring capture and detection 15
10 Configuring recording and bulk changes 17
11 Creating rules 19
12 Defining detection zones 21
13 Building scenarios 23
14 Connecting alerts and integrations 27
15 Relays and audio actions 31
16 Scheduling system behavior 33
17 Network and system administration 35
18 Backups and maintenance 36
19 Accounts and permissions 38
20 Mobile access and licenses 39
21 Troubleshooting and practical checks 41
22 Reference and further help 43

Related topics are linked within the text. The footer returns to Contents.

01 About this guide

This guide explains how to operate and configure the Monitoreal web interface: connect cameras, review live views and recorded evidence, tune detection, create rules and scenarios, deliver notifications, and maintain the appliance. Start with Getting started if you are installing a system. For an existing installation, begin with Everyday monitoring or Finding detections.

Version scope. This edition targets Monitoreal 2.5.1. The inspected SPARTAN appliance reported **2.5.1**, a latest production build, published by Monitoreal Limited on 3rd September 2026. The interface instructions and screenshots reflect that build. Check your own version under Settings > System before following an installation-specific procedure.

The guide distinguishes controls inspected on the appliance from operations that require a live test at your site. Recording playback and a short video download were verified. Firmware changes, archive deletion, restoration, physical outputs and delivery to external services were not exercised. A separate Coverage and verification report identifies the remaining limits.

How to use the instructions

Bold labels reproduce the English interface. A path such as **Settings > Network** means open Settings in the top navigation and select Network. Numbered steps describe a task; reference tables explain individual controls. Examples are suggested configurations, not factory defaults. Existing device values and initial values in a new form are not proof of a factory default.

Some controls depend on your role, the selected camera, connected hardware, configuration or license. If a control is missing or disabled, first check those dependencies. An administrator can review the permissions described in Accounts and permissions. Do not assume that another user's screen will contain the same controls.

Screenshots show the application only. Sensitive values and camera imagery have been obscured where necessary. A blurred image is a privacy treatment of an actual device capture, not an illustration of a different interface. Camera names, device counts and example values are specific to the inspected installation.

Terms used throughout the guide

Term	Meaning
Appliance	The Monitoreal unit running the web interface and processing camera imagery.
Capture source	The stream, substream or snapshot feed used for object detection. This is separate from the recording stream.
Detection	An object or motion result produced from camera imagery. Not every stored detection necessarily becomes a notification.
Rule	A camera-specific definition of an object event, its timing, profile and associated actions.
Scenario	A camera-specific combination of conditions, including relationships between objects, with notification and action outputs.
Profile or system mode	Armed or Disarmed. A rule's Profile and a scenario's System mode determine the modes in which they apply.
Zone	An inclusive or exclusive region used to restrict detection relevance. It is not a privacy mask.

Term	Meaning
Bounding box	The rectangle surrounding a detected object. Zones and proximity conditions use this box.
OD	Object detection. The interface uses this abbreviation in accuracy and doublecheck settings.
Notifier	A configured destination or service for outgoing alerts.

02 Getting started

Prepare the installation

You need a powered Monitoreal appliance, a network path to each camera, a computer with a browser, and the appliance and camera credentials. For an initial wired setup, connect the appliance to the local network using Ethernet and follow the quick-start instructions supplied with your hardware for power and discovery. The example unit is a SPARTAN; physical buttons and display behavior on other models are outside this guide's verified scope.

Obtain the appliance's IP address from your network administrator, the router's device list or the applicable Monitoreal discovery instructions. The inspected interface uses an HTTP address on the local network. Enter the address assigned to your own appliance; do not copy an address from an example or screenshot.

1. Open the appliance address in your browser from a network that can reach it.
2. Sign in with the credentials provided for your account. Follow any required password-change prompt.
3. Open **Settings > Profile** to review your account details and change your password when required. See Accounts and permissions.
4. Open **Settings > System**. Record the model and complete Software version, including any suffix.
5. Check **Timezone** and **Datetime format**. Correct time is essential when comparing recordings, detections and external alerts.
6. Review **Settings > Network** and confirm that the appliance can reach both its cameras and any required external services.

Use your organization's credential policy. Camera credentials and Monitoreal user credentials serve different systems; changing one does not establish that the other has changed. This guide intentionally does not publish an unverified default password for 2.5.1.

Connect and commission a camera

1. Open **Cameras > Add camera**. Use **Camera search** for a discoverable ONVIF camera, or **Add camera manually** when you have its source URLs.
2. Confirm that the camera appears with the expected name and image. Open **Details** and verify its identity and available feeds.
3. Open **Change settings** and choose the appropriate **Capture source**. Review detection settings before changing them.
4. Set **Recording**, **Recording stream** and **Record when the system is** according to the recording policy. These are independent choices from detection capture.
5. Configure a zone and a simple rule for the area and object of interest. Add notification delivery only after the detection behavior is appropriate.

6. Arrange a controlled site test. Check the live view, a detection result and a recording from the same time. Then verify the intended alert destination with the responsible recipient.

A successful live image does not by itself prove that recording, rules or notification delivery work. Check each stage. Do not enable a relay or speaker action while equipment is connected unless the site is prepared for it to operate.

A practical commissioning record

Record the camera name and purpose, its network address, capture and recording sources, recording mode, relevant zones, active rules/scenarios, notifier destinations and the person responsible for maintenance. Keep passwords and tokens in an approved credential store rather than in the commissioning record. Record the installed software version alongside test results so future changes can be compared accurately.

03 Finding your way around

The top navigation groups the system into four work areas. **Live stream** is the daily monitoring view. **Archive** contains stored detections, recorded video and storage management. **Cameras** contains camera configuration, rules and scenarios. **Settings** contains appliance, service and account configuration.

Navigation	Use it for
Live stream	Camera tiles, individual live views, full-screen monitoring and Recent events.
Archive > Detections	Search notifications or stored detection images; inspect event imagery and associated video.
Archive > Video	Select a camera and date, navigate the recording timeline and download video.
Archive > Archive actions	Copy the archive to a connected drive, clear archives and set retention.
Cameras	Add and manage cameras; configure recording, detection, zones, Rules and Scenarios.
Settings > Alerts	Outgoing notifications, integrations and GMS access.
Settings > System	Version, health information, clock, updates, backups, logs and maintenance.
Settings > Network	Ethernet and Wi-Fi configuration.
Settings > Relays	Relay discovery, state and available hardware settings.
Settings > Schedule	Timed arming, disarming and relay triggers.
Settings > Audio	Audio devices, speaker configuration and audio files.
Settings > Mobile app	Mobile account connection and listed mobile sessions.
Settings > Licenses	Check a license ID and synchronize the displayed license list.
Settings > Profile	Your account details and password.
Settings > Users	Local users, roles, permissions and mobile invitation links.
Settings > Logout	End the web session for the named user.

Breadcrumbs beneath the navigation identify the current area and, where relevant, the camera, rule or zone. Use **Home**, **Cameras** or **Back** to move up a level. The Armed/Disarmed control is visible in several areas; it is an operating control, not simply a page filter.

Understand Armed and Disarmed before switching

Armed and Disarmed are two selectable system modes. They are not universal synonyms for “record everything” and “stop everything.” Each rule has a **Profile**; each scenario has a **System mode**; each camera has a recording-mode selection. Those settings determine what continues in each mode.

Configuration	Practical effect
Rule Profile = Armed	Its configured alert/action behavior is associated with Armed operation.
Rule Profile = Disarmed	Its configured behavior is associated with Disarmed operation.
Rule Profile = Armed & Disarmed	The rule applies in either mode.
Scenario System mode = All	The scenario is eligible in both system modes, subject to its schedule and conditions.
Recording = enabled, Record when = Armed & Disarmed	Recording is configured for both modes. Switching to Disarmed is not a recording stop command.
Save snapshots when the rule profile is inactive	Controls storage of relevant detections outside that rule's active profile; it does not make the profile active.

Before changing mode, review schedules and any rules or scenarios that operate relays, speakers or external systems. To switch manually, select the required **Armed** or **Disarmed** position and check the displayed state. See Scheduling for automatic changes.

04 Everyday monitoring

Work with live camera tiles

Open **Live stream**. Camera tiles identify the camera and its ID, show the current imagery and provide a **LIVE** control and a camera-settings gear. A **REC** badge identifies a recording indication. Status dots and images must be interpreted together: a tile can retain an old image when a camera is off or unavailable. Check the image timestamp and camera state rather than treating any visible image as proof of a current connection.

1. Locate the required camera by its name and ID.
2. Select its **LIVE** control to open the individual live view.
3. Allow the stream to connect. If the interface reports a connection error, return to the camera configuration and check the source and network path.
4. Use the view's close/collapse control to return to the tiles. The camera-settings gear opens **Camera settings** directly from monitoring.

The live **Cameras** menu lists cameras with selection controls. The full-screen view has its own **Cameras (n)** menu. Use these selectors to choose the cameras relevant to your current monitoring layout. Check the displayed layout after reopening the page.

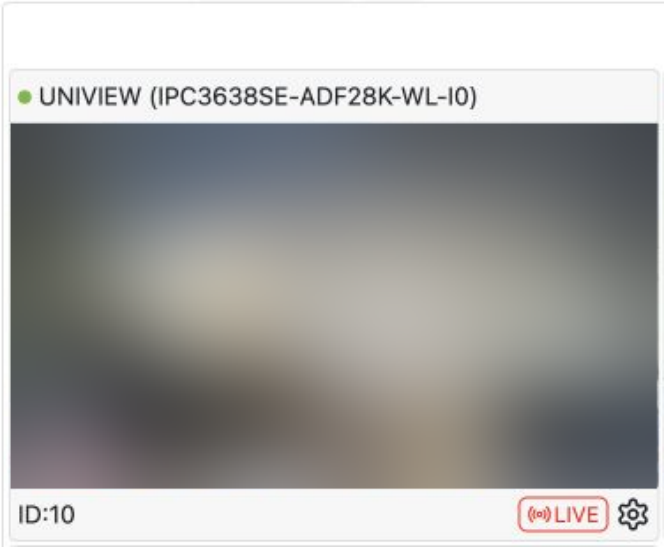


Figure 1. A live camera tile with its camera ID, LIVE control and settings gear. Camera imagery is obscured for privacy.

Use full-screen monitoring

Select the full-screen icon beside the live Cameras menu. The interface displays **Fullscreen mode**, a camera selector and **Esc**. Choose the cameras in **Cameras (n)** as needed. Use **Esc** to return. Full-screen display changes the viewing layout; it is not a recording or arming command.

If live video is unreliable, check another camera and a recent archive clip to separate a camera connection problem from a player problem. Do not reboot the appliance as the first response to a single failed stream.

Review Recent events

The feed contains object events and system messages. Depending on the event, a card can provide **Play**, **Download**, **Details**, and a seen/unseen control. Names such as “detected,” “disappeared,”

“number changed,” “still present,” “Moving … detected” and “Moving … stopped” describe different event transitions. They are not interchangeable alerts.

Open **Filter by** to narrow the feed by time range, event type, seen status and cameras. Event choices include **Detected**, **Disappeared**, **Motion detected**, **Motion stopped**, **Unknown event detected**, **Unknown event stopped**, **Scenario satisfied** and **Scenario cleared**. Choose **All**, **Seen** or **Unseen**, then **Apply**. Use **Reset** to remove the filter.

A check-mark control changes seen status. **Mark n as seen** applies a bulk acknowledgement to the indicated count. Use it only when that is your intended review action. Seen status is an acknowledgement aid; it is not a deletion, notification-disable command or proof that someone investigated the event. Opening an event image sequence marks that event seen during verification. See Finding detections for detailed evidence review.

05 Finding detections

Choose the right archive view

Open **Archive > Detections**. **Filter by** offers **Notifications** and **All**. Notifications is the event-oriented view, including event type and seen status. All is the stored-detection view, with object filtering and image browsing. A result can exist in one view without appearing in the other, because storage and alert eligibility are distinct settings.

1. Select **Notifications** or **All** according to what you are investigating.
2. Select a time range. Use a preset or enter From and To values, then confirm with **OK**.
3. Choose **Camera**. In Notifications, selecting a camera makes its **Rule** filter available where applicable.
4. Select the remaining event, object or seen-status filters.
5. Select **Apply**. Check that the result period and camera match the incident.
6. Use **Reset** before starting a substantially different search.

Filter	Availability and purpose
Event type	Notifications: All, Detected, Disappeared, Motion detected, Motion stopped, Unknown event detected, Unknown event stopped, Scenario satisfied and Scenario cleared.
Seen status	Notifications: All, Seen or Unseen. Useful for reviewing unacknowledged events.
Camera	Both views. Select All or a camera available to your account.
Rule	Notifications. Depends on the selected camera; avoid confusing two rules for the same object.
Object	All. Select All or an available object class, including Unknown event.
Time range	From/To controls plus Last 5 min, Last 15 min, Last 30 min, Last hour, Today and Yesterday. The picker displays its timezone.

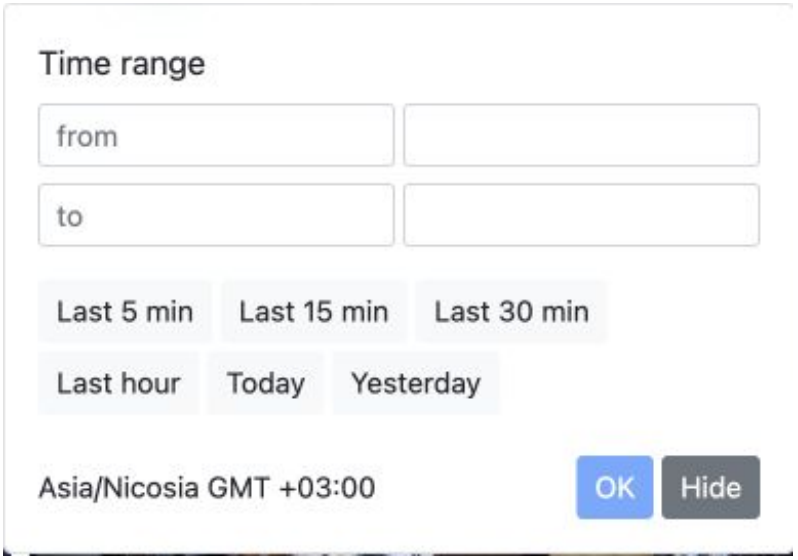


Figure 2. The detection archive time-range picker offers exact intervals and quick presets.

Interpret event cards

Read the camera name, event wording, count and timestamp together. A disappearance event's “Last seen at” time describes the object's last detection; it need not be the time you open the event. A loitering-delay label explains why an alert follows sustained presence. A number-change event reports a count transition within the rule's logic.

Select **View all** in the archive, or **Details** in Recent events, when available to review an event's image sequence. Use the previous/next arrows, or the indicated left/right keyboard controls, to inspect the sequence. **Close (Esc)** returns to the results. The sequence counter indicates your position within the available images.

The image sequence displays bounding boxes, object labels and confidence values. A confidence value expresses a detection score, not a guarantee of correctness. Compare the image with the configured object class and zone. Shadows, small objects, obstructions and poor illumination can affect results.

Play and download event video

1. Find the required event card and check its camera and time.
2. Select **Play** to inspect the associated clip, where available.
3. Close playback and select **Download** to save the event video through the browser.
4. Open the downloaded file and confirm that it contains the required event before sharing or retaining it as evidence.

An approximately 22-second MP4 downloaded successfully during verification. That is an observed sample, not a guaranteed event-clip duration. The presence of event imagery does not guarantee that the corresponding video was recorded or retained. If a clip is unavailable, check the camera's recording configuration, mode at the event time, storage availability and retention settings.

Browse all stored detections

In **All**, use **Object** and **Camera** with the time range, then Apply. The results show **Detection time from** and **to** and navigation controls for successive groups. Select a thumbnail to open its image viewer. The viewer shows the image time, detected object information and sequence navigation. Do not treat the displayed group size as a universal archive limit.

For recorded footage use **Archive > Video**. For whole-archive storage operations use **Archive actions**. Avoid substituting Clear archive for selective housekeeping; its scope is much broader.

06 Playing and exporting recordings

Find a recording

Open **Archive > Video**, or use a camera's **View recordings** shortcut on Cameras. The video archive combines a camera/date selection, a player and a timeline. Recording availability and object-event markers help you find a useful period, but playback depends on footage actually being present.

1. Select the camera.
2. Open the calendar and choose an available date. Dates marked **Not available** cannot be selected for footage in that view.
3. Confirm the date with **OK**.
4. Locate a period marked as available on the timeline. Select a segment to load its video.
5. Check the selected segment's start and end times, then use the player controls to review it.

A roughly five-minute recording segment is a set standard within the video archive storage format. An empty interval can reflect no recording, a camera or network interruption, recording limited to a different mode, or footage removed by retention.



Figure 3. Recording timeline detail: time labels, available footage and the object-event legend.

Use player and timeline controls

Control	Use
Play/pause and progress bar	Start or pause the loaded recording and move within it.
Previous/next segment	Move between available recording segments.
Audio control	Control browser playback audio. This is separate from the system's configured speaker actions.
Speed menu	The player offers 0.5, Normal, 1.5 and 2 playback speed.
Scissors	Open the loaded clip's cropping tool. Two handles define the wanted section From and To.
Download	Save the loaded clip or the selected cropped interval, according to the active tool.
Picture in picture and full screen	Change the player's presentation where the browser supports it.
Timeline zoom selection	Draw a range on the timeline to inspect a shorter period.
Previous zoom and reset	Return to an earlier timeline view or the full displayed range.

Control	Use
Timeline range selection	Define a start/end interval across recordings, then load that selection.

The colored object bars on the timeline help identify activity; the legend identifies the classes shown. They are not an assurance that every person or vehicle in the footage was detected. Review video when the distinction matters.

Download a short portion of a loaded clip

1. Load and pause the desired clip.
2. Select the **scissors** control. The cropping tool displays start and end handles and their times.
3. Move the handles to bracket the required action, leaving enough context before and after it.
4. Use the cropping tool's **Download** control.
5. Close the cropping tool when finished and verify the saved file's duration and content.

Test this export at your site before relying on it for a deadline and contact Monitoreal in case of any malfunction. Do not assume that moving the handles edits or deletes the original archive; the mentioned workflow is a download selection.



Figure 4. Cropping controls: the left and right handles set the interval; the download icon saves the selected portion.

Select a longer interval from the timeline

Use the timeline's range-selection control, then drag the start and end boundaries. Read the resulting **Time from** and **Time to** values. Use the selection's play/load control to assemble that interval in the player, then review it before downloading.

For longer exports, choose the smallest interval that preserves the incident and relevant context. Allow the browser to finish its download and verify the result. Browser and storage constraints still apply.

Keep an untouched copy of any downloaded original used for an investigation. Record the camera, time range, timezone and appliance version alongside it. A downloaded clip is separate from a settings backup and from copying the archive to a drive.

07 Managing archive storage

Open **Archive > Archive actions**. This page contains **Manage archive** and **Retention settings**. Access can be restricted by the **Archive Actions** permission.

Set a retention period

Retention limit (days) specifies how long video archives, detections and events should remain before automatic cleanup. Enter the required number of days and select **Save**. Leave the field blank to retain data until storage becomes full. The form exposes a whole-day numeric field with a minimum of 0; use the documented blank state when you want no day-based limit.

The page states that cleanup runs hourly and deletes data two hours before the limit to avoid overflow between cycles. If storage fills first, data may be deleted earlier than the configured retention period. A setting of, for example, 30 days is therefore not a guarantee that 30 days will remain available.

Before reducing retention: export any material that must be preserved. A shorter limit can make existing data eligible for deletion. Check disk usage under Settings > System and review actual archive availability after commissioning a retention policy.

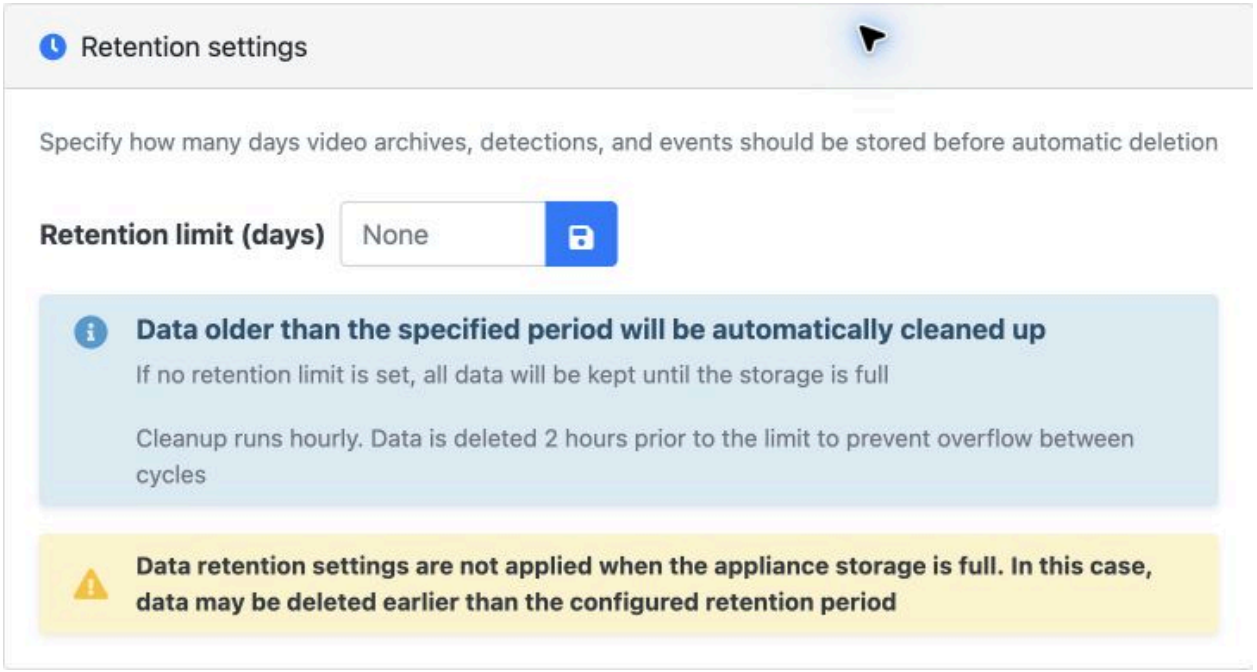


Figure 5. Archive actions and the retention warnings shown by the device.

Copy the archive to a drive

Connect a suitable drive and select **Copy archive to drive**. Follow the detected-drive workflow and verify the resulting copy before disconnecting the drive.

Clear the archive

Clear archive is destructive. Its confirmation states that both Snapshot and Video archives will be completely erased from all disks and cannot be restored through that action.

1. Export and verify everything that must be retained.
2. Obtain the required operational authorization for the site.
3. Open Archive > Archive actions and select Clear archive.
4. Read the scope in the confirmation. Select **Cancel** if you do not intend to erase all of it. Select **OK** only when permanent deletion is intended.

08 Adding and managing cameras

Discover an ONVIF camera

ONVIF discovery is the established camera-search workflow. The camera must be reachable from the appliance and have compatible discovery/access enabled. Some cameras require a separate ONVIF user. Obtain the correct credentials from the camera administrator.

1. Open **Cameras > Add camera > Camera search**.
2. Enter **Username** and **Password** for the camera's ONVIF access.
3. Use the optional IP-address field to target a specific camera when appropriate.
4. Select **Start searching** and review the result before proceeding with any addition.
5. Repeat for cameras using different credentials. Confirm each added camera's identity, source and image.

The form includes **Search Monitoreal cameras**. That option is associated with discovery of Monitoreal branded cameras; it should not be treated as a credential bypass for arbitrary cameras.

Add a camera by URL

Use **Cameras > Add camera > Add camera manually** when discovery is unsuitable or when you need a particular source. Obtain URLs from the camera or video-server documentation rather than guessing a path.

1. Enter a useful **Camera name**, such as “Loading bay entrance.”
2. Enter **Stream URL(RTSP)** for the main video source.
3. Enter **Substream URL** and **Snapshot URL** when those feeds are available and required.
4. Enter the camera's **Username** and **Password**.
5. Select **Save**, then verify the camera image and Details. Choose the intended capture and recording sources separately.

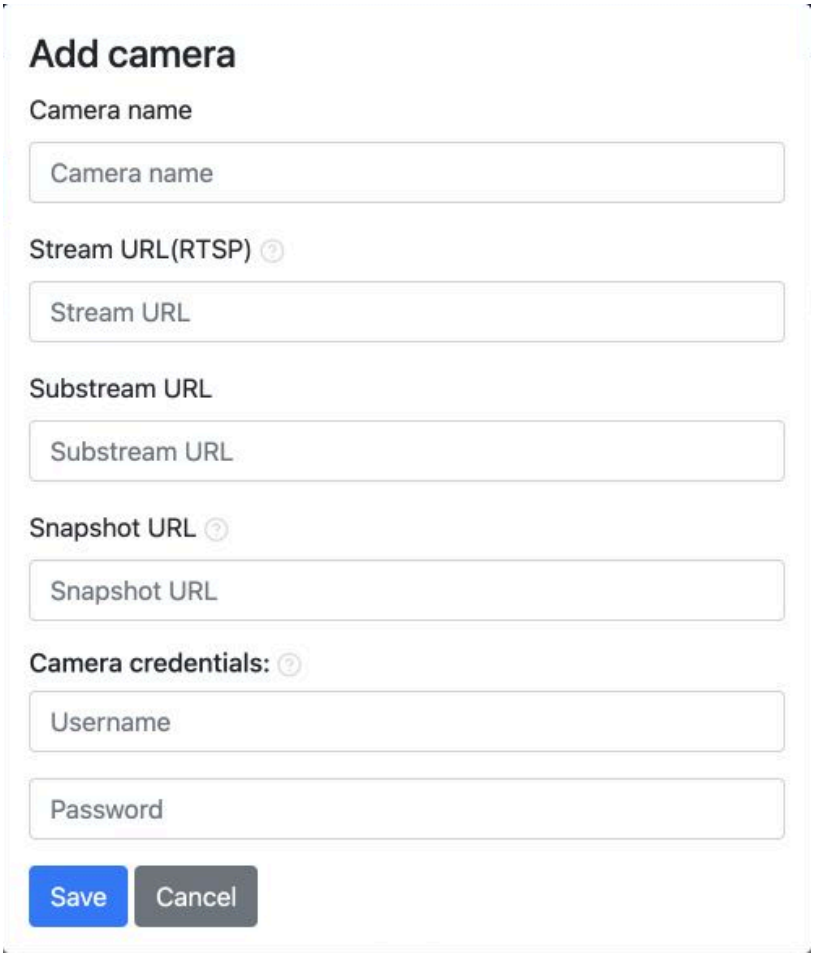


Figure 6. The manual camera form keeps stream URLs and camera credentials separate.

Field	Purpose and dependency
Camera name	A recognizable name used in monitoring, archives and configuration. Avoid ambiguous names across similar views.
Stream URL(RTSP)	The main streaming endpoint. RTSP is the protocol used to request the camera's video stream.
Substream URL	A secondary video endpoint, often configured separately in the camera. It must exist before you can select it.
Snapshot URL	An endpoint that supplies a still image. Required for a usable snapshot capture configuration.
Username / Password	Credentials for the source camera or video server, not the Monitoreal web account.

A camera connected to an NVR's isolated camera network may not be reachable from the ordinary office network. Ask the installer to provide a routed path or the appropriate NVR channel source. Do not expose a camera to the public internet merely to make discovery work.

Read camera status and details

The Cameras page shows names, addresses, IDs, image previews, enabled state, available resolution and recording indicators. A megapixel meter reports the current aggregate resolution against the device's available budget. The set cumulative limit is 48 MP; that is appliance-specific, not a universal entitlement.

Details displays the Stream, Substream and Snapshot URLs, IP address, MAC address, manufacturer, model and image dimensions where available. URL copy controls are provided. Treat copied URLs as sensitive: they can reveal network structure and may include access information. Check the receiving document before sharing them.

The card's controls include **Change settings**, **Edit zone**, **View recordings**, **Reboot camera** and **Delete camera**. Use the gear for detection configuration, the zone control for camera-wide regions and View recordings for evidence review.

Disable, reboot or remove a camera

The **Off/On** control changes the camera's enabled state in Monitoreal. It is different from hiding a tile, disabling one rule or choosing a recording mode. Treat it as an operational change and confirm the effect at your site before using it during monitored hours.

Reboot camera can interrupt that camera's video and detection. **Delete camera** removes a configured camera and can affect dependent rules, scenarios and actions. It also removes all detections and video recordings related to that camera. Before removal, preserve the source details and document dependencies; export any required evidence. Re-adding a camera will recover its former configuration or archive association.

09 Configuring capture and detection

Open a camera's **Change settings** button on Cameras, or its settings gear on Live stream. Review the existing values before changing them. Use **Save** to apply the form or **Cancel** to discard a draft.

Choose capture and recording sources independently

Capture source offers **Stream**, **Substream** and **Snapshot**. It selects the imagery used for analysis. **Recording stream**, on the camera's Settings tab, selects the feed saved as video. A lower-resolution analysis source can reduce processing demand, but may make distant or small objects harder to identify. A higher-resolution recording can preserve detail even if analysis uses a substream, provided the feeds and device capacity support that setup.

A source option is only useful when its URL and camera service work. The inspected camera's recording selector disabled **Substream - Not configured** when no substream existed. Configure the camera's own resolution, encoding and image parameters in the camera interface when they are not exposed in Monitoreal.

Understand the camera settings

Setting	Purpose and practical effect
Camera name	Changes the label used to identify this camera. Use a stable, location-based name.
Speaker	Associates an available speaker with the camera, or Not selected. Explicit audio actions also select a device; check the action's destination.
Automatically Sync Date & Time	The help text says the camera is synchronized to appliance time when it comes online. Incorrect appliance time can therefore propagate.
Automatically restart camera session	The help describes an attempt to restart an unexpectedly offline camera. Compatibility and recovery success were not exercised.

Setting	Purpose and practical effect
Capture source	Stream, Substream or Snapshot for analysis. Ensure the chosen feed exists and remains reachable.
Motion threshold	Adjusts the moving-object size that triggers processing. Observed slider: 10–90 in steps of 5. Lower values admit smaller motion; excessive sensitivity can increase processing load.
Camera priority	Observed range 1–10 in steps of 1. Help identifies 1 as highest priority and states that priority also affects interface order. Use it when some views matter more under load.
OD minimal accuracy	Observed slider: 25–90 in steps of 5. Results below the chosen confidence threshold are ignored by the relevant detection logic.
OD alerts doublecheck	Uses two separate algorithms to validate alerts and reduce false alarms. The live help says it is not applied to images stored or shown in the web interface.
Alerts	Controls camera alert output. Do not use it as a substitute for disabling recording or verifying every associated automation. See the qualification below.
Error reports	The help says connection-error notifications are sent immediately when enabled. Delivery still depends on configured destinations and service availability.

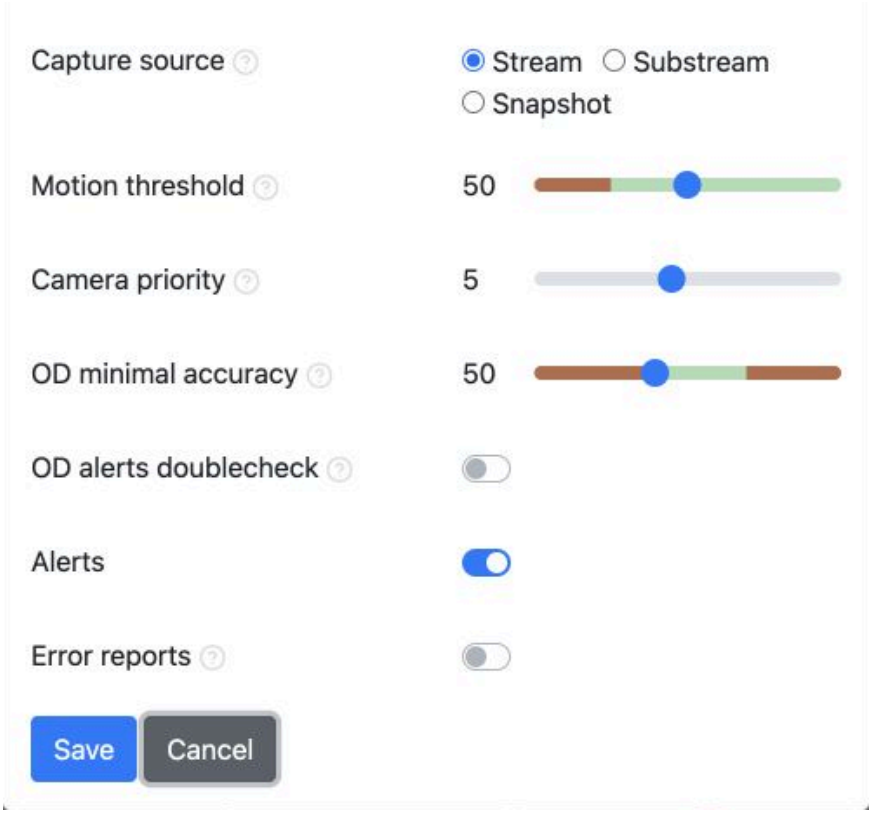


Figure 7. Capture source and camera detection controls. These are inspected values, not factory defaults.

Tune accuracy and motion separately

OD minimal accuracy asks how confident the classifier must be about the object's identity. Raising it can suppress uncertain false positives, but can also miss valid objects in difficult light, at a distance or

partly hidden. Lowering it accepts more uncertain classifications. A threshold of 70 is not a promise that 70% of alerts are correct.

Motion threshold controls which movement is large enough to draw processing attention. It is not another confidence threshold. Lowering it can help with smaller moving objects, but foliage, weather, reflections or image noise may then create more work. The camera help warns that values below 30 can overload the system, delay processing and reduce accuracy. That warning is not a recommendation to use 30 in every scene.

1. Save or record your current settings and define the actual problem: missed objects, wrong classifications or irrelevant movement.
2. Check camera aim, focus, lighting and object size before changing software thresholds.
3. Use a zone to remove irrelevant areas where appropriate.
4. Change one relevant setting by a small amount.
5. Compare detections and recorded footage across representative day/night conditions.
6. Keep the setting only if the observed improvement is worth the missed-event or processing tradeoff.

For example, a doorway rule that mistakes a shadow for a person may benefit from a higher accuracy threshold. A distant person that never enters analysis may require better framing or motion sensitivity. Increasing confidence cannot recover an object that is too small or never reaches the analysis stage.

10 Configuring recording and bulk changes

Record in the modes you intend

On **Cameras**, open the camera's **Settings** tab. The recording controls sit on the card rather than inside the Change settings dialog.

1. Enable **Recording** when you want video stored.
2. Choose **Recording stream**: Main Stream or a configured Substream.
3. Set **Record when the system is** to **Armed**, **Disarmed** or **Armed & Disarmed**.
4. Check the recording indication and open View recordings after an appropriate interval to confirm that footage is being retained.

Choose Main Stream when its detail is needed and storage/network capacity permit. A lower-bitrate substream can reduce storage use, but may not preserve enough detail for later identification. Configure the underlying stream in the camera itself.

A recording mode is a condition, not a calendar. To change system mode by time, use Settings > Schedule. To make a detection rule active only at certain times, use the rule's own time/day controls. These mechanisms serve different purposes.

Apply common settings to several cameras

The **Cameras settings** button opens a bulk form with a camera selector and shared settings. Choose the target cameras carefully. **Apply recording settings** reveals Recording, recording-stream and mode options. The form also includes speaker and detection settings. **Apply** remains unavailable when the required selection is incomplete.

1. Record the existing settings for every target camera.

2. Select only the intended cameras in Cameras settings.
3. Enable Apply recording settings only when the recording configuration is part of the change.
4. Review every displayed field, including capture source, thresholds, priority, Alerts and Error reports.
5. Apply the change, then inspect representative target cameras and their recordings/detections.

Bulk initial values must not be read as a summary of every selected camera's current settings. Cameras can differ in source availability and scene conditions. A uniform threshold is convenient but may perform poorly across unlike views.

Understand the global menus

The **Recording** menu offers **Enable on all cameras** and **Disable on all cameras**. These actions have system-wide recording consequences; verify their scope before use.

The **Rules** menu provides **Add rule** for a camera selection and bulk snapshot-storage choices for all rule profiles or active profiles only. The underlying rule form is described in Creating rules. A storage change can reduce the evidence available outside active profiles even when alert behavior is unchanged. Review retention and investigation needs before using it.

11 Creating rules

A rule belongs to a camera and defines which object event matters, when the rule applies and what outputs are associated with it. Use a rule for a straightforward object-presence, count, moving-object or unknown-motion requirement. Use a scenario when the requirement involves combinations or relationships between objects.

Create a detection rule

1. Open **Cameras**, locate the camera and select **Rules**.
2. Select **+ Add rule**. For a bulk addition, use the top Rules menu and choose the target cameras in the form.
3. Enter an optional **Rule name** that describes the purpose, such as “Person at loading entrance.”
4. Choose **Object category**, then select the required **Object** or objects. Use All select or Clear all carefully in the object selector.
5. Set **Density control**, the time range and **Days of the week**.
6. Configure the applicable accuracy, moving-object, loitering and event choices.
7. Set **Profile** and the inactive-profile snapshot option.
8. Select **Save**. Check that the rule is enabled in the list, then configure its zone and any relay/audio actions as needed.

Do not assume that the new rule's initial selections are suitable. The inspected draft enabled several event types and selected Armed; those observations are not a promise of factory defaults for every installation.

Select an object class

Object category	Objects shown in the inspected rule selector
Humans and Animals	Person, Bird, Cat(dog), Dog(cat), Horse, Sheep, Cow, Elephant, Bear.
Vehicles and Luggage	Bicycle, Car, Motorcycle, Airplane, Bus, Train, Truck, Boat, Backpack, Handbag, Suitcase.
Other objects	Umbrella, Bottle, Wine glass, Cup, Unknown event.

The labels **Cat(dog)** and **Dog(cat)** reproduce the interface. Do not silently rename them when matching a rule to the UI. The available list is not evidence of guaranteed detection performance for every class in every scene. PPE requirements appear in scenarios and have a separate licensing dependency; they are not listed as ordinary object choices here.

Rule field reference

Setting	How to use it
Rule name	Optional descriptive label. If omitted, the list can identify a rule using its object and ID.
Object category / Object	Select the class or classes that this rule evaluates. Category changes affect the available object choices.

Setting	How to use it
Density control	Sets the object-count requirement. The inspected numeric control exposed 1–15. Use 1 for a single-object requirement; validate multi-object behavior in the actual scene.
Start time / End time	Limit the rule's daily time interval. Existing unrestricted rules displayed 24h. Overnight boundary behavior for these particular fields was not tested; do not infer it from scenario scheduling.
Days of the week	Select the days on which the rule applies. Review all seven selections.
Only detect moving objects	Available for the vehicle/luggage category in the inspected form. Changes the event choices to moving/stopped events.
OD minimal accuracy	An optional rule-specific confidence setting. Observed slider 25–90, step 5. Use an override when this rule needs a different threshold; test interaction with camera settings.
Loitering delay	Require sustained presence before the relevant detection alert. Helps ignore brief passers-by, but delays notification of a real event.
Loitering reminder	Repeat a presence reminder while the condition remains relevant. Observed field range 1–86400 seconds; inspected initial value 60 seconds.
Alert on object detection	Request an event when the object is detected under the rule's conditions.
Alert on object disappearance	Request an event when the object disappears. Review the last-seen timestamp in the resulting event.
Alert on object number changes	Request a count-change event where this option is available.
Profile	Armed, Disarmed or Armed & Disarmed. Controls mode eligibility, separately from the rule's time/day choices.
Save snapshots when the rule profile is inactive	Preserve detections outside the rule's active profile. Disabling it can save storage without changing the profile's notification eligibility, according to live help.

Create an Unknown event rule

Select **Other objects > Unknown event** to work with motion that is not handled as an ordinary recognized object event. The form changes: count, accuracy and reminder controls available for standard objects are not all shown, and two specific controls appear.

Exclude known object classes ignores motion overlapping recognized classes, even when no rule targets those classes, according to the live help. Use it to focus on motion outside the known-object results. **Display motion boxes on snapshots** overlays the relevant motion regions so a reviewer can see what prompted the event.

Keep the distinction clear: Unknown event is not a newly identified object category and does not tell you what caused the motion. Review the imagery. Test in wind, rain and changing illumination before enabling high-volume external notification delivery.

Manage an existing rule

The Rules list provides an enable checkbox/switch, rule identification, schedule/profile information and icons for audio actions, zones, relay actions, edit and delete. Use the pencil to change the rule. Disabling a rule is different from deleting it, changing its profile or stopping the camera.

Before deleting a rule, record its conditions, zones and actions. Treat deletion as permanent unless your version explicitly offers recovery. Icons without text deserve particular care: identify the pencil, trash or zone symbol before selecting it; do not assume their order.

Example configurations

People at a doorway after hours. Use Person, a doorway inclusion zone, a count requirement of 1 and an Armed profile. Use a short, validated loitering delay only if brief passers-by should be ignored. Schedule the system to arm after closing, or use the rule's time/day interval. First confirm detection with notifications only, then consider an output action.

A moving vehicle in a service lane. Use the relevant vehicle class and Only detect moving objects. Restrict the lane with a zone and select the moving/stopped event choices required by the operating procedure. Test both a vehicle entering and one remaining stationary.

An unexplained movement investigation. Use Unknown event and Display motion boxes on snapshots. Decide whether Exclude known object classes should be enabled. Review results before enabling a remote recipient, because environmental motion can produce substantial activity.

12 Defining detection zones

Zones let you focus a camera or rule on a meaningful part of the image. **Inclusive** zones identify areas of interest. **Exclusive** zones exclude areas from the relevant zone decision. The feature does not conceal pixels in recordings or guarantee that imagery outside a zone is never stored. Use separate privacy controls when a scene must not be captured.

Choose the correct scope

Open a camera's **Edit zone** for camera-level zones. Open the zone icon within a particular rule for rule-level zones; the breadcrumb and heading include the rule's object/name. Check this scope before editing.

The live help states that camera zones apply to rules by default, rule zones take precedence over camera zones, and exclusive zones prevail over inclusive zones at the same scope. It specifically notes that a rule-level inclusion can prevail over a camera-level exclusion. A camera exclusion should therefore not be treated as an unconditional privacy boundary.

Draw a rectangle

1. Open the appropriate zone page and select **Refresh preview** if the reference image needs updating.
2. Select **Add zone**, then **Rectangle**.
3. Adjust the on-image handles to cover the intended area. Use the rotation handle where needed.
4. Enter a meaningful name and choose **inclusive** or **exclusive**.
5. Check **Active** and select the disk/save icon for the zone. Use the X/cancel control to discard an unsaved zone.
6. Verify the saved shape and test representative object positions near its boundaries.

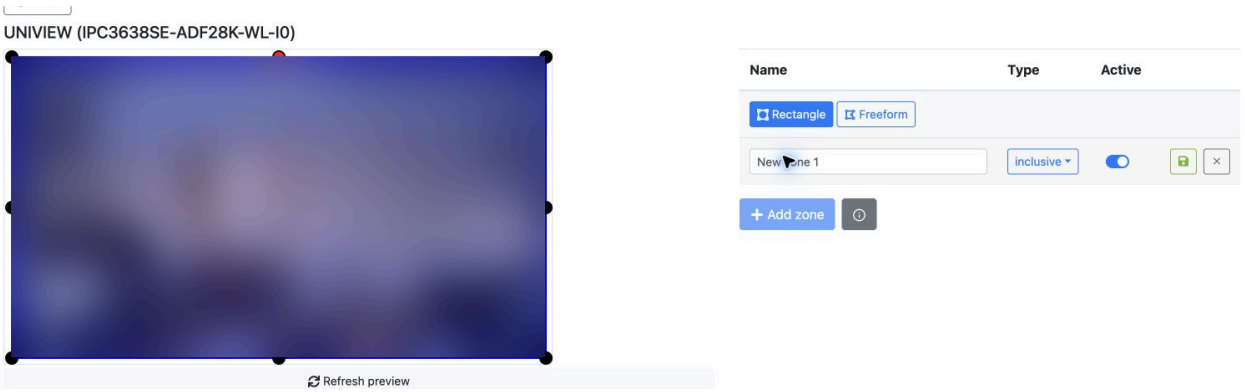


Figure 8. A rectangle zone draft. Check the camera/rule scope and save control before applying changes.

Draw a freeform zone

Select **Freeform** in a new zone draft. Click the camera preview to place the first node, then add points around the required shape. Complete the shape by clicking the initial node, highlighted in green or blue. The on-screen instructions say a completed zone can be moved by dragging and rotated using the red node. Give it a name, type and Active state, then save it.

Use a simple shape that follows the actual region of interest. Very tight boundaries can exclude a valid object when its bounding box shifts from frame to frame. Test the approach path and the far end of the zone, not only a stationary object in its center.

Choose how a box intersects a zone

React to intersections by offers **edge of bounding box** and **center of bounding box**. Edge-based evaluation can react when part of a detected box reaches the zone; center-based evaluation waits for its center to enter. The inspected pages selected center, but an existing selection is not a verified factory default.

For a doorway, center-based evaluation may reduce alerts from people walking just outside the boundary. For a narrow approach area, edge-based evaluation may react earlier. Tune the shape and intersection method together and use recorded examples to understand borderline cases.

Display zone on results adds zone visualization to results for review. It does not turn the zone into a mask. The exact persistence and propagation of these page-level options were not altered during verification.

Edit or remove a zone

Use the saved zone's edit control, adjust the shape or fields and save. Use its delete control only when removal is intended. The inspected interface exposed unlabeled icon buttons, and a zone removal applied immediately during the review. Do not assume a confirmation will appear. Preserve a screenshot or configuration backup before modifying operational zones.

When a rule-level zone is removed, review what camera-level coverage will apply afterward. A rule that falls back to a broader region may generate different events. Check all dependent rules/scenarios when changing shared camera zones.

13 Building scenarios

Scenarios combine object conditions and relationships that would be difficult to express as a single ordinary rule. They are configured per camera under **Cameras > Scenarios**. The inspected editor used three steps: **1 Setup**, **2 When** and **3 Then**. A scenario has its own enabled state, schedule, mode and outputs; it is not merely a label grouping existing rules.

Create a scenario

1. Open the required camera's Scenarios tab and select **+ Add Scenario**.
2. Enter a **Scenario name** that describes the situation.
3. In Setup, choose **System mode** and the time/day schedule.
4. In When, choose a template or construct the conditions, including any zones, counts, timing, proximity or PPE requirements.
5. In Then, select notification events and configure any relay/audio actions.
6. Review all three steps and any validation messages before selecting **Save**.
7. Check the scenario's enable control in the list and commission it with realistic staged events.

Use **Back**, **Next** or the numbered steps to review the configuration. **Cancel** leaves a draft unsaved. Existing scenarios have **Edit** and **Delete** controls. Deletion and live activation were not tested; preserve the configuration before removing it.

Setup defines when evaluation matters

System mode offers Armed, Disarmed and All. **All day (24h)** and **Every day** simplify an unrestricted schedule. Clear All day to enter **From** and **To**. The editor explicitly says that an end time earlier than the start creates an overnight window. Clear Every day to select individual weekdays.

This is a scenario eligibility schedule; it does not switch the appliance between Armed and Disarmed. Use Settings > Schedule for system-mode changes. A scenario limited to Armed from 20:00 to 06:00 still depends on the system actually being Armed.

When defines the condition groups

Each top-level condition has a letter, a **There is** or **There is no** choice and an object class. Presence conditions can use **count ≥**. Add another group with **+ Add condition**. With multiple groups, **All** requires all groups and **Any** accepts any qualifying group; the editor displays a sentence describing the selected match mode.

Within a group, **+ Add subcondition** adds an **And** relationship to another object. The editor offers presence/absence, target object, a radius multiplier and a duration in seconds. The radius is based on the longer side of the source object's bounding box, multiplied by 0.5×, 1×, 1.5×, 1.7×, 2× or 3×. The help says the relationship fires when that region touches the target object's bounding box. This is image-space geometry, not a measured distance in meters.

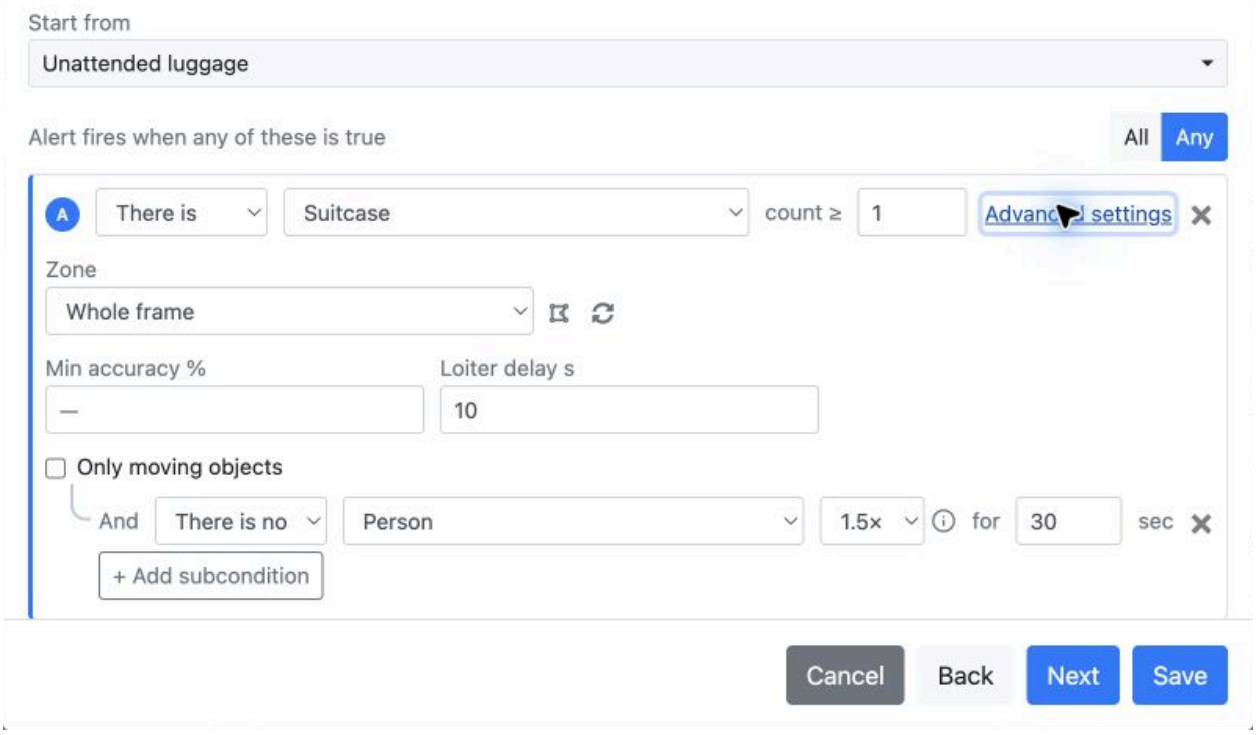


Figure 9. Advanced condition settings and an object-proximity subcondition.

For example, “Suitcase present AND no Person within 1.5× for 30 seconds” expresses a different situation from “Suitcase present AND Person present somewhere in the frame.” Choose the relationship according to the real operating requirement, and test with changing perspective and partial occlusion.

Advanced condition settings

Setting	Purpose and verified form behavior
Zone	Whole frame or an available zone. Restricts the condition to the selected region.
Add / draw zone	Opens zone creation from the condition workflow. Check the scope and save the zone deliberately.
Refresh zones	Refreshes the available zone list after zone work.
Min accuracy %	A condition-specific confidence field. Inspected HTML bounds were 0–100; no server-side acceptance test was performed.
Loiter delay s	A condition-specific sustained-presence delay. The field exposed a minimum of 0; no upper limit was shown in the inspected control.
Only moving objects	Restricts the condition to moving objects where offered. It was enabled in the tailgating template's vehicle conditions.
count ≥	A minimum count control with a visible lower bound of 1. No universal maximum was established.
Subcondition duration	The “for … sec” interval in the relationship. The inspected field had a minimum of 0; validate timing in a staged test.

The form's numeric attributes document its visible constraints, not an assurance that every value is accepted or performs usefully. Do not assume the camera, rule and scenario accuracy controls have

identical ranges or precedence. Where several thresholds interact, validate the resulting detections with the complete configuration.

PPE requirements (Licenced content)

For a Person condition, **+ Add PPE requirement** exposes **Wearing** or **Not wearing**, **Helmet** or **Vest**, and **Min accuracy %**. The PPE violation template creates alternative Person conditions for a missing helmet or missing vest. Published release information identifies PPE as licensed functionality. Seeing the editor does not prove that the current appliance is entitled to execute PPE detection.

Confirm the license and stage representative tests before deployment. Small equipment, occlusion, camera angle and clothing color can affect classification. A PPE detection alert should support a site procedure; it is not a certification that every person complied or that every violation was captured.

Then defines notifications and actions

Notification provides **On conditions satisfied**, **On conditions closure** and **On conditions satisfied continuously every** with a seconds interval. Choose an initial notification, a clearing notification, repeated reminders, or the appropriate combination. The continuous reminder draft showed 60 seconds; this is not a universal factory default.

Under **Relay & audio actions**, use **+ Relay** or **+ Audio**. Each action selects the event phase: conditions satisfied or closure. Complete the relay/channel/action/mode/timing or audio device/file/timing fields. An incomplete action produced a validation message requiring every Then action to be finished before saving.

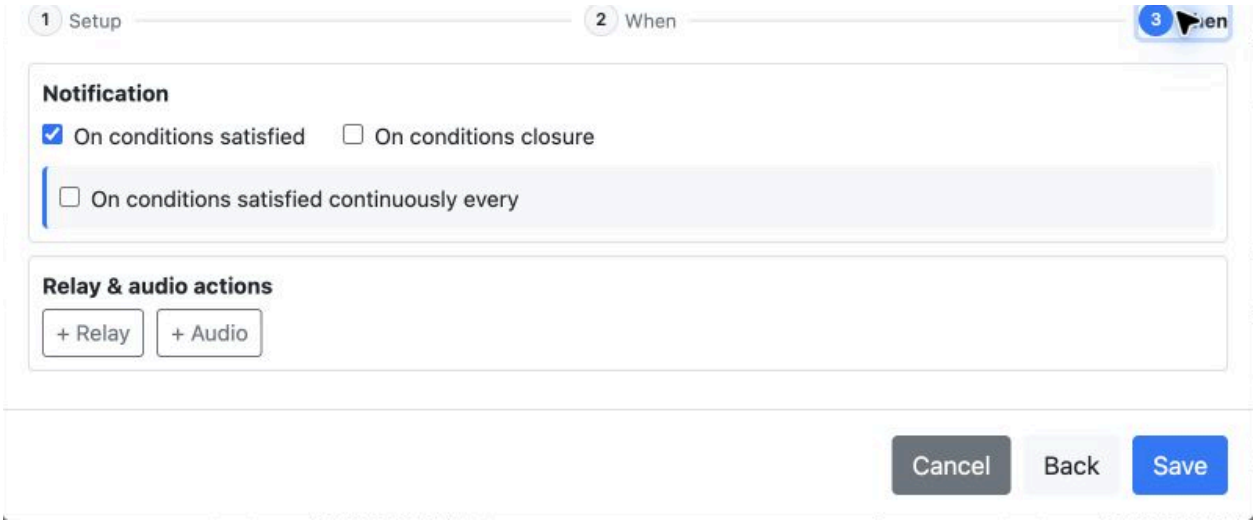


Figure 10. Scenario notification phases and the Relay & audio actions area.

A clearing event is useful when an operator must know that a condition has ended. Repeated notifications may be useful for an unresolved situation, but can overwhelm recipients. Coordinate the interval with the response procedure and the receiving service's capacity.

Start from a template

Templates are editable starting points. Changing a template can rewrite **Setup, When and Then**, while keeping relay and audio actions, according to the confirmation. Review retained actions carefully so that a different condition does not unexpectedly operate old equipment.

Template	Inspected starting logic
Custom scenario	Begin with an empty object condition and build the requirement yourself.
Unattended luggage	Alternative Suitcase, Backpack and Handbag groups, with no Person nearby for a period. The inspected draft used a 1.5× relationship, 30-second absence and a 10-second loiter delay on the object condition.
Tailgating at barrier	Alternative moving Car or Truck groups with a Person proximity subcondition. The inspected relationship used 1.5× for 2 seconds. The name does not imply access-control credential validation.
Loitering near vehicle (night)	Alternative Car or Truck groups with a Person within 3× for 30 seconds. Setup showed Armed, every day, 20:00–06:00.
PPE violation	Alternative Person conditions with Not wearing Helmet or Not wearing Vest. Requires the relevant licensed capability.

These values are template observations from the inspected build, not recommended universal settings. Review every advanced field after loading a template. No live scenario was created or triggered during verification.

14 Connecting alerts and integrations

Open **Settings > Alerts** to configure outgoing services. The page lists GMS access and the supported notifier types. Service sections and individual entries can have active controls; a visible entry or enabled switch is not proof that a remote recipient received anything.

Plan the delivery chain

An outgoing notification depends on more than credentials. Check the camera's Alerts setting, the rule/scenario being enabled and eligible for the current mode/time, the selected event type, notifier activation, network access, service authentication and any license requirement. Review both the event archive and the receiving system during commissioning.

1. Obtain the exact destination and authentication information from the service administrator.
2. Open the appropriate service section and select **Add new**.
3. Complete the required fields and review any report-type or permission choices.
4. Save the entry, then check its active state.
5. Arrange an authorized test event and verify receipt and content at the destination.
6. Record the owner of the integration and how to revoke or rotate its credentials.

No external delivery test was sent during this review. The tables below describe the forms available on the appliance, not a certification of each third-party service. Payload schemas, remote API permissions and acceptance behavior must be agreed with the receiving service; do not invent them from field names.

Telegram

The Telegram form contains **Bot token**, **Use proxy** (Yes/No), **Admin permissions** (Enabled/Disabled), **Authenticated users**, Save and Close. Obtain a token for the intended bot and keep it private. Use proxy only when your network/service setup requires it; selecting Yes did not reveal additional proxy-address fields in the inspected form.

Admin permissions affect the bot's control capability. Grant them only to a bot and authenticated users trusted for system administration. The old manual describes authentication through the bot and interactive commands, but current command behavior and the complete command list were not tested. Consult the bot's current help and Monitoreal documentation rather than assuming older commands are unchanged.

After saving, review Authenticated users and the notifier's active state. A token alone does not establish that every intended person has authenticated or that administrative commands will be allowed. Do not include bot tokens in screenshots, tickets or the user guide.

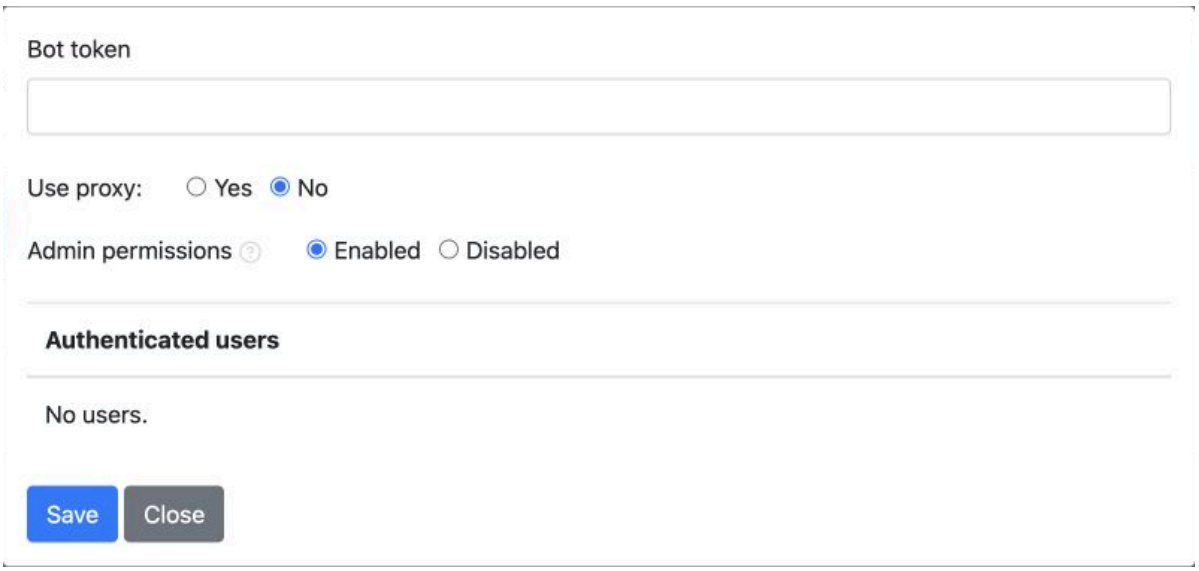


Figure 11. The Telegram configuration form includes separate proxy and administrative-permission choices.

Slack

The Slack form contains **Bot token** and **App token**, with Authenticated users, Save and Close. The placeholders distinguish a bot token beginning with xoxb from an app-level token beginning with xapp. Obtain both from the intended Slack application and workspace administrator.

The older manual's Slack setup is useful background, but third-party application setup and required scopes can change. Verify the current Slack configuration and Monitoreal integration instructions before provisioning tokens. Save the notifier, authenticate the intended users through the supported flow and test receipt in the intended workspace. Slack delivery and user authentication were not exercised in this review.

Email

Email uses SMTP, the service that sends mail. Enter **Name of sender/site** if you want a recognizable source label, then the SMTP **Server**, **Port**, **User/from address** and optional **Password**. **Security** offers **None** and **Automatic**. Use the mail administrator's documented security and port combination; do not copy a generic port because it appears common.

The established manual describes Automatic as using SSL/TLS or STARTTLS and None as an unencrypted connection. That connection behavior was not tested on this build. **Send to addresses** identifies recipients. The legacy instructions use comma-separated addresses; verify acceptance of your complete recipient list during setup.

Enable **Reply-to different address** to enter a separate reply-to name and address. This redirects human replies; it does not change the SMTP server. The page warns that mail providers can block large volumes of messages. Tune detection and reminder frequency before enabling a busy camera's mail delivery.

Webhooks and extended reports

A webhook sends an event to a configured URL. **Webhooks** exposes **Payload URL**, **Method** (GET or POST) and an optional **Token**. Choose the method and authentication required by the receiver. The form does not by itself define a complete integration contract or prove that the receiver accepted an event.

WebhooksExt adds a licensed report selector. The detected-event choices shown were **Snapshot**, **Detections report** and **Video report**. For a disappeared event, choose **Send detections report** or **Do**

not send. Richer reports can require more data and processing than a simple notification; verify the resulting content and delivery time at the destination.

Several monitoring-center forms use the same report controls and mark them **Licensed Extension**. Check the actual license and the receiving service's expected report. The Alerts page's license indication and the separate Licenses page describe different views; an empty Partner Portal list does not, by itself, prove that every alert extension is unavailable.

Monitoring and alarm-system forms

All the following are under Settings > Alerts. Select the named section, use Add new, enter the service-provided values, save and verify its active state. Review existing entries using their edit control. Deletion removes the destination and was not tested.

Integration	Fields and dependencies shown
Sentinel	Sender/site, SMTP server/port, User/from address, optional password, security, recipients and optional reply-to; licensed detected/disappeared report choices.
Immix	The same SMTP and licensed report structure. Coordinate recipient identity and report type with the monitoring center.
Scanalitix	SMTP/report configuration plus Site-ID. Use the identifier assigned by the receiving service.
Securithor	Payload URL, optional Partition number, optional Account number, optional Token.
SecurithorExt	Securithor fields plus licensed detected/disappeared report choices.
Praxis	Payload URL and optional Token.
Patriot	Payload URL, Account number, Username and Password.
SBN	Payload URL, account number and credentials, plus licensed report choices.
Manitou	Host and Port. Obtain the receiving endpoint and network requirements from the operator.
Eyemax	IP Address, Port, Username and Password.
Ksenia	Camera, Object, Object detected/Object disappeared, Sent to, Payload URL, optional Token, GET/POST/PUT and Body. Several fields depend on the preceding selections.

For Ksenia, select the camera first, then its available object/event and destination mapping. The initial form disabled Object until a camera was chosen and disabled the request fields until prerequisite selections were made. A complete destination mapping and live alarm-panel delivery were not tested. Do not treat a sample URL or existing site's account number as a reusable template.

FTP media delivery

The **FTP** section combines an email/report configuration with **FTP destinations (media upload)**. It is more than a standalone file-server address. Complete the sender/SMTP and report fields where the service workflow requires them, then configure the media destination.

FTP field	Purpose
Server entry	Configure the destination host/server, Port, User/from address and Password shown in the form.
Remote path	Destination directory. The inspected draft used /. Confirm write permission and the intended folder.
Protocol	FTP or FTPS. The inspected draft selected FTPS; match the server's supported secure configuration.
Add FTP server	Adds another destination configuration to the form. Multi-destination delivery behavior was not tested.
File name template	The inspected template was {deviceName}-{channel}-{date}-{time}.{ext}. These tokens describe how uploaded files are named. Additional tokens were not established.
Retries per cycle (X)	The draft showed 5. Controls retry configuration; the exact cycle/failover behavior was not exercised.
Retry delay seconds (Y)	The draft showed 30. Sets the configured delay between retry attempts.

The FTP port draft showed 21. That value is not a recommendation for every server. Confirm protocol, certificate/security requirements, folder permissions and filename uniqueness with the server administrator. Test both normal upload and a controlled outage before relying on delivery for evidence preservation.

GMS access and license extension

The GMS access section displays an existing organization/access relationship and a **Remove access** control. It concerns external management access rather than a simple email recipient. Confirm the responsible organization before changing it.

Extend license appears on Alerts. Licensing and entitlement changes were not performed. Use Settings > Licenses to inspect the supported license-ID workflow, and contact the responsible partner or Monitoreal for entitlement details. This guide contains no pricing or product-concept material.

15 Relays and audio actions

Relay actions can operate physical equipment; audio actions can play sound through connected devices. Configure them only after detection logic works and the site is prepared for the output. An alert-only test does not prove an output is wired correctly or safe to operate.

Inspect relay hardware

Open **Settings > Relays**. The example device listed a relay with three output channels and three input controls. Do not generalize that channel count to every supported relay model.

Relay search starts discovery; **Refresh** repeats it.

The relay menu exposed Network mode, Wi-Fi/Ethernet status, a firmware version, Update firmware and Delete. Network and firmware operations can disconnect the relay; perform them within a maintenance window.

The live help explains a four-digit PIN when not already set, and warns that linking a relay to another appliance disconnects its previous association without deleting the old entry. It also describes deleting the old entry before discovery when moving the relay back. Follow the exact model's setup instructions and preserve the existing assignment before pairing or moving hardware.

Input behavior, pull-up configuration, channel naming, live network changes and firmware update progress were not accessible on the offline relay. Ask the installer to document the actual wired inputs, their electrical mode and the outputs they can trigger.

Add a relay

1. Power and connect the relay according to its model’s installation instructions. Make sure the appliance can reach it on the network.

2. Open **Settings > Relays** and select **Relay search**. Wait for discovery to finish. If **No new relays found** appears, check power and network connectivity, then select **Refresh**.

3. When a relay is offered for addition, follow its pairing prompt. The page help specifies a four-digit PIN: if no PIN has been set, the four digits entered during addition become the PIN. Keep the PIN securely.

4. After pairing, check the relay card. A green status dot identifies the online relay in the example below; the offline relay has a red dot and disabled controls.

Moving a relay. Pairing it with another appliance disconnects its previous association but leaves the old entry. The page help says to delete that old entry before discovery when moving the relay back. Plan the move before breaking an existing connection.

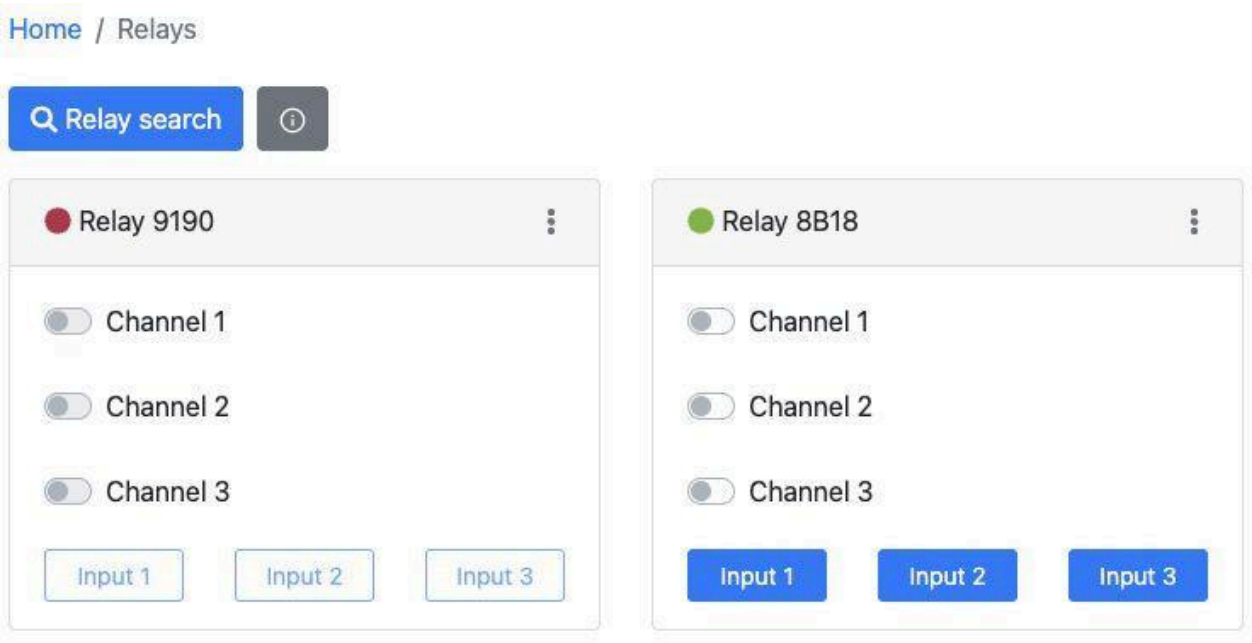


Figure 15A. Relay discovery and status. The online example has three outputs and three input buttons; channel counts depend on the hardware.

Pairing check. Discovery found no unpaired relay during this review, so the final addition prompt and successful pairing were not tested.

Identify outputs and manage the connection

Name the relay and its outputs

Point to the relay name and select the pencil icon. Enter a useful location name, such as **Gate cabinet**, then select the disk icon to save; the **×** cancels. To rename an output, point to its **Channel** label, select its pencil icon, edit **Channel name**, and select **Save**. Use names that identify the connected equipment.

The channel editor also contains **Duration sec**, accepting whole seconds from **0 to 99999**. The inspected channel showed **0**. The interface does not explain zero's meaning or how this value interacts with other relay action durations; confirm those details before changing it.

Physical outputs. The switches beside the channel names are output controls. Use them only when the connected equipment is safe to operate. Changing a label does not require toggling its output.

Configure the relay network

Open the **three-dot menu** on the relay card. **Network mode** offers **Wifi** and **Ethernet**. Switching modes can interrupt relay communication. The inspected relay used Ethernet; **Wifi Offline** was disabled, so its Wi-Fi setup form could not be checked safely.

Select the **Eth** entry to open **Ethernet configuration**. Choose **DHCP** for an automatically assigned address, or **Static** to edit **IP address** and **Mask**. Select **Save** to apply or **Cancel** to discard. Record the current values and agree any static address with the network administrator first.

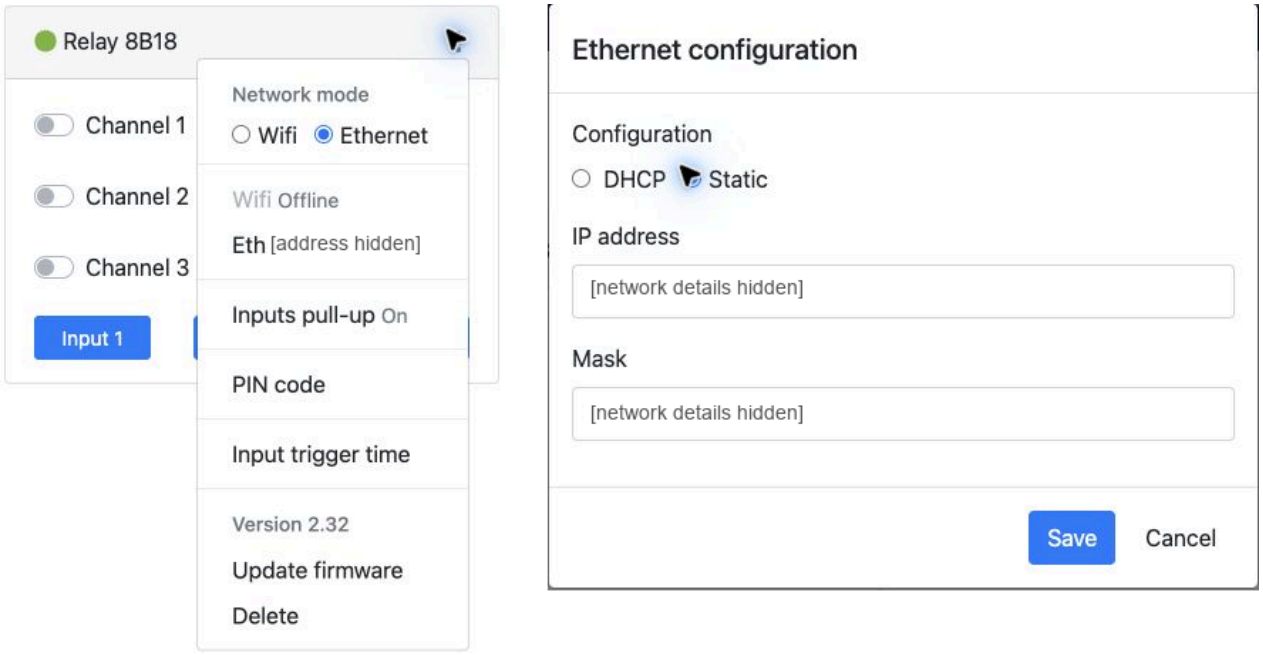


Figure 15B. Online relay menu and the Ethernet dialog with Static selected as an unsaved example. Network details are concealed.

PIN and maintenance. PIN code opens the PIN editor. The page help says the connected appliance can change it without the previous PIN. **Version** identifies the relay firmware. **Update firmware** and **Delete** are also available; plan a maintenance window before using operations that may interrupt or remove the relay connection.

Configure relay inputs

An input reads an external contact or signal. Its rules run an action when the input changes to the selected state. Open **Input 1**, **Input 2** or **Input 3** to see its **Current input value** and configure its rules.

Match the pull-up setting to the wiring

Open the relay's three-dot menu and select **Inputs pull-up**. In **Inputs pull-up configuration**, use **Show more** to read both wiring modes. Choose the required mode, then **Save**, or use **Cancel** to leave it unchanged.

On — dry contacts. The help identifies the +5 V DC pull-up as enabled by default. A switch or contact connected between an input and GND produces **Low** when closed and **High** when open. No external voltage source is needed for a dry contact.

Off — externally powered inputs. The pull-up help describes applying up to **30 V DC** to produce **High**, with no voltage producing **Low**. This is a different electrical mode. The input-rule help separately warns against exceeding **5 V**. Confirm the exact relay model and wiring mode with the installer before applying voltage; do not treat 30 V as a limit that applies in every mode.

Create an input rule

1. Open the required **Input** button and select **Add rule**.

2. Choose **Low** or **High** under **Input State**, then choose the **Action**. The available actions are **Armed**, **Disarmed**, **Do snapshots** and **Trigger output**.

3. For **Armed** or **Disarmed**, enter **Delay sec** from **0 to 255**. For example, Low → Armed with a delay of 0 requests arming when the contact closes. Confirm that this matches the site's intended operation.

4. Select **Save** to apply the rules, or **Close** to discard edits. Use the trash icon beside a row to remove that rule, then save the revised list.

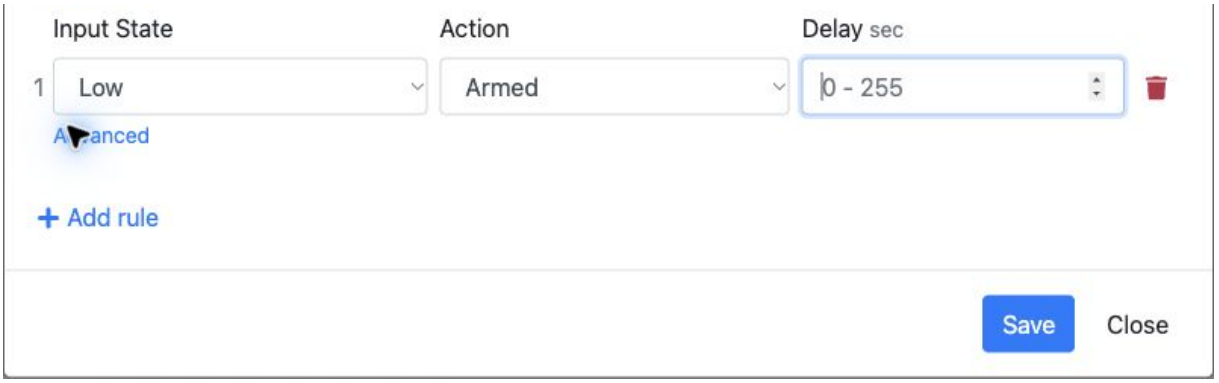


Figure 15C. Detail of an unsaved input rule: Low → Armed. Enter the required delay before saving.

Set input thresholds and timing

Use an input to trigger an output

In the input rule, select **Trigger output**, then choose **Output** and **Channel action**. The inspected relay offers **Channel 1–3** and **Turn on**, **Turn off** or **Strobe**. Set **Delay sec** and **Duration sec**, each accepting **0–255** whole seconds, then save only when the connected equipment is ready.

Do snapshots is also available as an input action. Selecting it removed the delay field and did not expose a camera selector in the inspected form. Which cameras contribute snapshots was not verified.

Use a custom input range

Select **Advanced** beneath a rule to replace the Low/High selector with two percentage fields, each accepting **0–100**. These define the input range for the rule. Select **Hide** to return to the basic selector. Use a custom range only when the sensor's measured values and intended trigger range are known.

The basic ranges shown in the interface are **Low: 0–20%** and **High: 21–100%**. With the inspected pull-up setting, the help also lists Low as 0–360 Ω / 0–1.3 V and High as 380 Ω to open circuit / 1.4–5 V. These are the interface's stated ranges, not a substitute for the relay's electrical specifications.

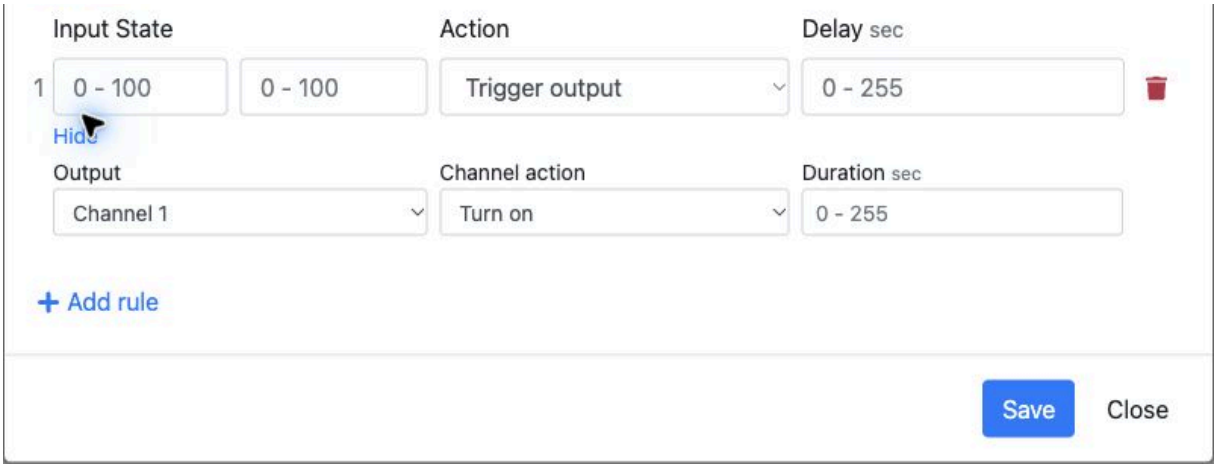


Figure 15D. Advanced input range and Trigger output fields. This draft was inspected and closed without saving or activating an output.

Retain arm and disarm commands during an outage

In the relay menu, open **Input trigger time**. Despite its name, the help defines this as how long an Arm/Disarm command received while disconnected is stored in relay memory for later delivery to the appliance. Enter **0–99999 seconds** and select **Save**, or **Cancel** to discard.

The inspected value was **3600 seconds** (one hour), not a verified factory default. A longer interval allows an older command to be delivered after reconnection. The meaning of zero was not explained in the interface.

Attach a relay action to a rule

1. Open the camera's Rules tab and identify the intended rule.
2. Select its relay-action icon.
3. Choose **Object detected** or **Object disappeared**.
4. Select **Create action** and enter **Name**, **Relay** and **Channel**.
5. Choose **Turn on**, **Turn off** or **Strobe**, then the mode and timing.
6. Save only after checking the wiring, recipient/confirmation path and intended physical consequence.

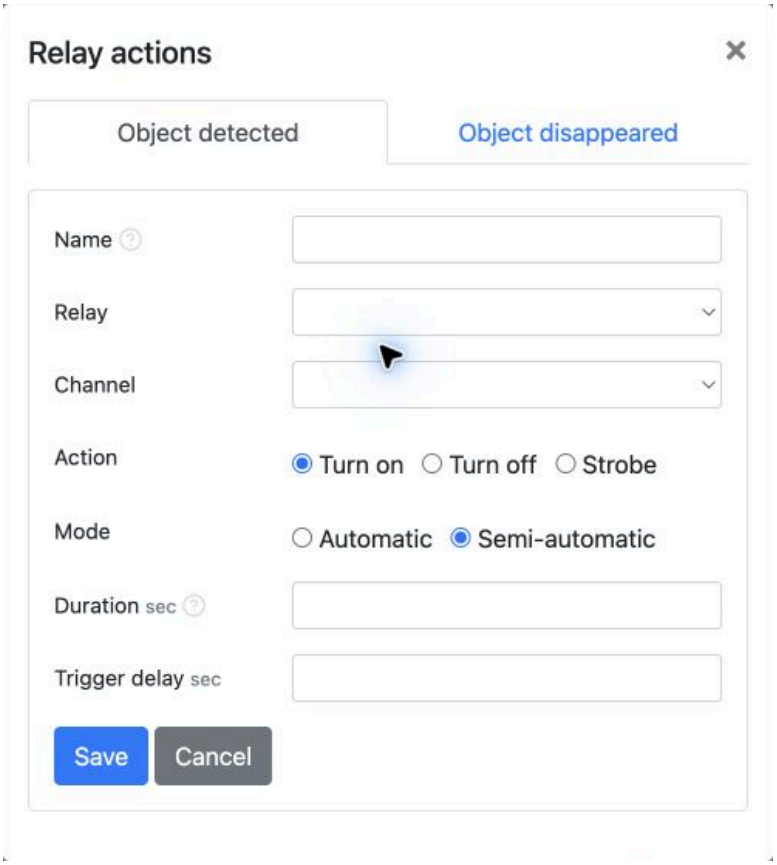


Figure 12. Relay actions select a target, event phase, operating mode and timing.

Setting	Meaning and verification limit
Name	A useful description of the device/action, such as “Entrance warning lamp.”
Relay / Channel	The physical output to operate. An offline relay may not populate selectable channels.
Turn on / Turn off	The requested channel state. Check the connected circuit's behavior; “off” is not universally the safe equipment state.
Strobe	The established workflow repeatedly switches the output. Switching rate and hardware behavior were not tested.
Automatic	The established direct-execution mode when the triggering condition occurs. Physical execution was not tested.

Setting	Meaning and verification limit
Semi-automatic	The legacy guide describes confirmation through Telegram before execution. The current confirmation path and timeout were not tested. Do not assume it provides a safety interlock.
Duration, sec	How long the action is requested to remain effective. The form allows it to be blank; blank/zero semantics and restoration behavior require a controlled test.
Trigger delay, sec	Delay before the output action. Verify whether the condition must remain true and how overlapping triggers behave; those details were not established.

Multiple actions are supported by the current action-list/editor workflow; coordinate their delays and validate the intended sequence.

Configure audio devices and files

Open **Settings > Audio**. **My devices** lists configured destinations; the example list included an IP speaker and **Audio jack 3.5mm**. **Other devices > Search** provides device discovery, and **Add speaker** opens fields for **Name**, **IP address**, **Port** and **User**. The port placeholder showed 5060. Use the speaker's documented settings; do not assume that every network speaker uses them.

Configured speakers have Edit and Delete controls. Removing a device can invalidate actions that target it. Bluetooth discovery/pairing and network-speaker audio were not tested. Use the hardware-specific guide for electrical connections, pairing and volume controls that are not present in the inspected page.

The **Audio files** panel provides Browse, Upload, a playback destination selector and play/delete controls for stored files. The displayed maximum file size was **2.4 MB**. Listed formats were aac, aif, flac, iff, m4a, m4b, mid, midi, mp3, mpa, mpc, oga, ogg, opus, ra, ram, snd, wav and wma. A listed extension does not establish that every encoding variant will play correctly; verify the actual file.

1. Select **Browse** and choose an appropriate audio file within the displayed limit.
2. Select **Upload**.
3. Choose the intended playback device.
4. When the site is ready for sound, use the play control and verify audibility and content.
5. Stop playback if necessary using the displayed stop control. Do not test through an occupied site without warning the responsible operator.

Attach an audio action

Open the rule's audio-action icon, choose Object detected or Object disappeared, then Create action. Enter **Name**, select **Device** and **Audio file**, and set **Trigger delay sec**. Save when ready. The inspected new action showed a delay of 0 seconds; this is an initial form value, not a universal requirement.

In a scenario, use **Then > + Audio** and select conditions satisfied or closure. Ensure that the chosen file remains installed and the device is available. A speaker selected in Camera settings does not replace checking the explicit destination in an audio action.

16 Scheduling system behavior

Open **Settings > Schedule**. The page is titled **Armed/Disarmed Schedule** and includes a calendar, a legend and the schedule-rule list. **Add rule** opens **Periodic**, **One-time** and **Relay Trigger** tabs. These schedule rules are separate from camera detection rules.

Create a periodic mode change

1. Select Add rule and open Periodic.
2. Enter **Name**, such as “Weekday closing.”
3. Choose **Action**: Armed or Disarmed.
4. Enter **Time**.
5. Select the required recurrence using Days of week, Date range or Days of month, and the applicable Months.
6. Save, then review the calendar and rule list for the intended occurrences.

The form offers weekday buttons, start/end day values in Date range, day-of-month selections from 1 to 31 and month selections from January to December. Review the displayed calendar, especially around month boundaries, rather than assuming how a missing day such as the 31st is handled. Precedence between conflicting schedules was not tested.

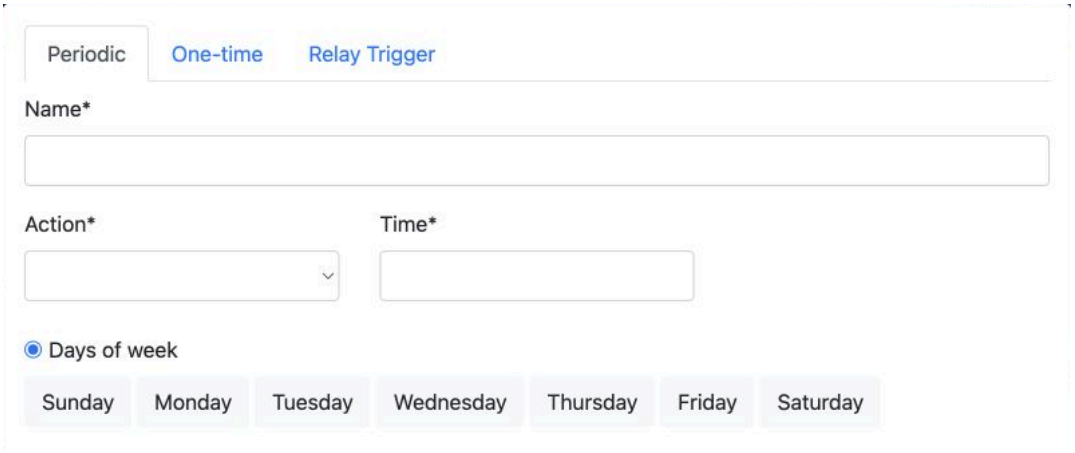


Figure 13. The upper section of the periodic schedule editor. Further recurrence and month controls appear below.

A nightly arm/disarm pattern generally needs two actions: one that arms at closing and another that disarms at opening. Changing system mode can affect many camera rules, scenarios and recording policies at once. Review those dependencies before enabling a schedule.

Create a one-time change

Open **One-time**, enter Name, choose Armed or Disarmed, set Time and select Date. The current form expresses one selected action at a date/time.

After saving, check the scheduled occurrence in the calendar. For a temporary closure that needs both arming and later disarming, create and verify the required individual actions rather than assuming an automatic reversal.

Schedule a relay trigger

Open **Relay Trigger** and select Name, Time, Relay and the recurrence controls. A usable target depends on connected relay hardware and its available channels/actions.

Treat a scheduled relay operation like any other physical action. Confirm the connected circuit, timing, intended state and recovery behavior. Check timezone and overlapping schedules before enabling it. Scheduled outputs must not be used as an unverified substitute for the equipment's required control system.

Maintain schedules

Review the calendar after editing a rule and after changing the appliance timezone. The inspected page contained no saved schedule rules, so saved-rule edit/delete behavior and holiday/exception precedence were not exercised. Preserve a record of the intended weekly pattern and verify the next scheduled transitions after changes.

Use three separate questions when troubleshooting timing: Is the system mode correct? Is the camera rule or scenario eligible now? Is recording configured for that mode? A correct schedule cannot compensate for the wrong rule profile or recording selection.

17 Network and system administration

Understand network interfaces

Open **Settings > Network**. Each interface card shows Configuration, IP address, Mask, Gateway, DNS, MAC and Primary gateway, along with its connection status. The example SPARTAN had two Ethernet interfaces and one Wi-Fi interface; other hardware can differ.

DHCP obtains network settings from the network's address service. **Static** uses values you enter. An incorrect IP address, mask, gateway or DNS can disconnect the interface, break camera access or prevent external alerts. Preserve the old values and an independent way to regain access before applying changes.

Field	Purpose
IP address	The appliance's address on this interface. It must be valid and unique on the network.
Mask	Defines the local subnet. Do not infer subnet membership solely from the first three address numbers.
Gateway	The router used to reach destinations outside the local subnet.
DNS	Resolves service hostnames to addresses. Incorrect DNS can break external services even when local cameras still work.
Primary gateway	Identifies the preferred gateway selection in the form. Confirm the intended route when using multiple interfaces.
MAC	Hardware interface identifier, useful for a DHCP reservation. It is not an IP address.

Change Ethernet configuration

1. Record the interface name and all current values.
2. Select **Network settings** for that interface.
3. Choose DHCP or Static. Static enables the address fields.
4. Enter administrator-approved IP address, Mask, Gateway and DNS, and review Primary gateway.
5. Select **Apply** only when ready for a possible connection change.
6. Reopen the appliance at the new address if necessary and verify cameras, DNS-dependent services and remote access.

The form was inspected in both DHCP and Static modes without applying changes. A router-side DHCP reservation can provide a stable address while leaving the appliance in DHCP, when supported by your network policy. Do not assign a static address that conflicts with another device or the DHCP pool.

Connect Wi-Fi

Select **WiFi networks** on the wireless card. Refresh the scan if needed, choose the required network and enter its WLAN password. The connection form includes DHCP/Static, IP address, Mask, Gateway, DNS, Primary gateway and **Connect**. Review the network and route choices before connecting.

Wi-Fi discovery and the connection form were inspected, but no connection was established. Do not change the only working network path while relying on it for remote administration. A camera network attached to one interface and an office network attached to another need deliberate routing; merely plugging both in does not prove the appliance can reach every camera.

Check health and version

Open **Settings > System**. System info shows **Model**, **Serial number**, **Software version**, **Uptime**, **CPU load**, **CPU temperature**, **RAM** and **Disk usage**. Use trends and symptoms rather than a single number to diagnose a problem. The review did not establish hardware-specific temperature or load alarm thresholds.

Record the full version, not just 2.5.1 (if applicable). The **Release notes** link opens Monitoreal's published change history. **Check for update** checks availability; installing an update is a separate operational decision. Plan maintenance before firmware work because recording, detection and access can be interrupted.

Set time, language and update behavior

Setting	Available choices and effect
Timezone	Regional timezone list. Choose the site's intended zone and verify archive/event times afterward.
Datetime format	Six formats were shown: year-month-day 24h; day.month.year 24h; year-month-day 12h; day/month/year 12h; month.day.year 12h; month/day/year 12h.
Language	English, Deutsch, Ελληνικά, Русский, Português, Español, Français, Italiano, Türkçe and Українська. This guide uses the English labels.
Autoupdate	When enabled, offers Anytime (default) or During these hours only: with from/to fields. Save applies the chosen settings.
NTP Server Address	Address of the time source in NTP Time Synchronization. Sync Time is disabled when empty. The page also displays System Time in UTC.

Use a trusted, reachable NTP source and confirm the result before relying on timestamps. Changing time can affect event interpretation and schedules; it was not executed on the running installation. A camera's burned-in timestamp may use its own clock/timezone even when the web interface shows appliance-local time. Compare both when investigating an apparent offset.

Restrict automatic updates to an agreed maintenance window when uninterrupted operation is important.

18 Backups and maintenance

Download a settings backup

1. Open **Settings > System > Download settings**.
2. Optionally enter **Password** and **Confirm password**.
3. Select **Download** and store the resulting file securely.
4. Record the appliance model, complete software version, date and reason for the backup. Keep the password in an approved credential store.

The password and confirmation fields were inspected without exporting the site's configuration. A settings backup is not a copy of recorded video.

Restore settings deliberately

Open **Upload settings**, enter the backup password if used, select **Choose file / Browse** and choose the intended backup. Review its source and compatibility before selecting **Upload**. Restoration can replace operating configuration and alter detection/actions. Preserve a current backup and plan a maintenance window first.

Do not assume that a backup from another model or software version will restore every setting safely. After a supported restoration, verify accounts, network access, camera sources, recording, zones, rules/scenarios, notifiers, hardware associations and schedules as a fresh commissioning check.

Logs and service status

Download logs provides diagnostic material for support. Logs can contain network, device or account information; review and transfer them using the support channel approved for your site. **View system status** opens the service-status page. The inspected page listed services including engine, pi_panel, celery, notifier, tools, audio and recorder with status/creation information.

Use this view to provide evidence to support, not to infer that every internal service can be restarted safely. Unlabeled service controls were not used. Record the symptom, affected camera/time, complete software version and relevant status before restarting anything; a restart can remove useful transient evidence.

If necessary, fill out a ticket using the official Monitoreal Support Form to request assistance or use the official Monitoreal Recovery Tool to provide remote access to a member of Monitoreal team

Restart, Recover and Factory reset

Operation	Consequence and appropriate use
Restart	Restarts the appliance. Expect a period without normal recording, detection or access. Use within an approved maintenance window.
Recover	Its confirmation says services stop and restart; if launch fails, the appliance attempts to update program firmware to the latest version and launch again. It is not a harmless refresh.
Factory reset	Its confirmation says all data is erased, settings return to defaults and accounts disconnect from the device. Use only when that complete reset is intended.

For Recover or Factory reset, read the displayed warning and choose **Cancel** unless you are ready for the stated consequences. **Do not** remove power or network connectivity during a firmware operation. If the web interface is unreachable, obtain the current model-specific recovery instructions from Monitoreal support rather than applying legacy button sequences from another model.

A useful maintenance routine

Review disk usage and actual oldest available footage, camera availability, recent error reports, notifier health, license status and the next scheduled mode changes. After any firmware or camera update, repeat a small set of site tests: live view, a representative detection, recorded playback and authorized notification delivery.

19 Accounts and permissions

Manage your profile

Open **Settings > Profile**. The profile page shows Username, Email, First name and Last name. **Edit** opens those fields with Save and Cancel. **Change password** opens **Current password**, **New password** and **Confirm password**. Enter matching new values and save when ready.

Use a unique account for each person where practical. The example user was the Owner and had Administrator rights; that does not establish the rights of other users. Do not change another person's credentials merely to troubleshoot their permissions.

Add or edit a user

Open **Settings > Users**. The Users list shows account identities, roles and linked/mobile invitation state. To create an account, select **Add user**, enter required Username, Password and Role, and optionally First name, Last name and Email. Select Save when the role and access scope are correct.

Existing users have edit and delete controls where your role permits them. Check ownership and dependencies before deletion; removing a user can remove their ability to monitor or manage the site. User creation, deletion and password changes were not performed during verification.

Understand roles before assigning them

The Roles list includes **Administrator**, **Editor**, **Viewer** and custom roles. Administrator opened as a read-only permission view. Editor and Viewer opened editable permission forms. Therefore, a role name alone is not a reliable statement of current access: inspect its actual checkboxes and resource selections.

Add custom role (not recommended) opens a role-name form. The interface's wording is reproduced here. Use existing roles when they meet your needs, or have an administrator design and test a custom role deliberately.

Some permissions have a resource selector such as **All cameras**, **All relays** or **All audio devices**. An enabled permission can still be limited to selected resources. Review both the permission and its scope. Test the result using the intended user account before handing it over.

Permission reference

Group	Controls shown in the inspected role editor
Peripheral	Discover and Add cameras; Delete cameras; Add relays; Delete relays; Add Audio and Bluetooth devices; Delete Audio and Bluetooth devices.
Cameras	View cameras with resource scope; Access live stream; Change camera settings, enable or disable camera; Enable or disable video recording; Access snapshot archive; Access the video archive; Archive Actions.
Zones	View zones; Add zones; Delete zones; Change zones.
Rules	View rules; Add rules; Delete rules; Change rules.
Scenarios	View scenarios; Add scenarios; Delete scenarios; Change scenarios.
Relay	View relays with scope; Modify relay or input settings; Switch relay channels.

Group	Controls shown in the inspected role editor
Relay actions	View, Add, Delete and Change relay actions.
Audio	View audio files; Add audio files; Delete audio files.
Audio and Bluetooth	Access settings with audio-device scope.
Audio actions	View, Add, Delete and Change audio actions.
Schedule	View, Add, Delete and Change schedule entries.
Arm/disarm	View modes; Switch between modes.
Feed	Access feed.
Settings	Manage alerts; Perform system recovery or factory reset; Restart system; View system status; Create backup; Restore backup; Update system; Access logs; Modify system settings; Configure network; View licenses and Manage licenses.
Roles	View, Add, Delete and Modify roles.
Users	View, Add, Delete and Modify user details; View mobile invite links and Manage those links.

The layout uses parent/child permissions. Do not assume that a child checkbox grants useful access when its parent or resource scope is unavailable. No restricted-role session was used to verify every enforcement boundary. In particular, “notification-only” access should be commissioned by testing the intended feed and camera restrictions, rather than inferred solely from a role name.

Use least privilege in practical terms

For a monitoring operator, start from the required live views, event feed and archives, then add mode switching only if their job requires it. For an installer, add camera/rule/zone management for the relevant resources. Reserve user/role changes, network changes, firmware, reset and archive deletion for responsible administrators.

These are role-design **examples**, **not descriptions** of the current Editor or Viewer preset. The reviewed Viewer configuration included permissions that may surprise a reader expecting a strict read-only role. Always inspect the saved configuration. Review access when staff leave, devices are reassigned or a monitoring provider changes.

20 Mobile access and licenses

Connect a profile to the mobile app

Open **Settings > Mobile app**. Before connection, the page displays **Connect to the mobile app**, **Login** and a message to sign in to link the profile to a mobile account. Use the intended account and verify its identity before completing the flow.

Login can reuse an existing authenticated browser account and the system will record a new mobile-connection event. This demonstrates that Login can have an immediate account-linking effect; it is not merely a preview of a sign-in form. Check shared-browser sessions before connecting a profile.

After connection, the page shows the linked account and **Mobile devices**, including a device name, IP/session information, **Terminate session** and **Refresh**. Refresh updates the displayed list. Terminate session can interrupt that mobile device's access; select it only when revocation is intended.

Use the current Monitoreal mobile guide for the app's own navigation. This chapter documents the appliance-side connection and session controls.

Manage mobile invitations

Settings > Users exposes invitation-link controls for eligible users. Existing rows can show an invitation link, a linked account or **Link expired**. The permissions include viewing and managing mobile invite links. Regenerating a link can affect a pending invitation; coordinate with the recipient rather than repeatedly regenerating it.

Treat invitation URLs as access material. Share them only with the intended person and do not include them in public screenshots or tickets. Invitation creation, regeneration, acceptance and expiry duration were not tested, so this guide does not claim a fixed validity period.

Check a license ID

Open **Settings > Licenses**. **Activate a license by ID** accepts an ID received from the Partner Portal. The page says the check shows what it covers and how the device would change before activation.

1. Obtain the intended license ID from the responsible partner or administrator.
2. Enter it in **License ID** and select **Check**.
3. Review coverage and proposed changes before any activation step.
4. After authorized activation, verify the enabled features and use **Sync** under Licenses on this device when appropriate.

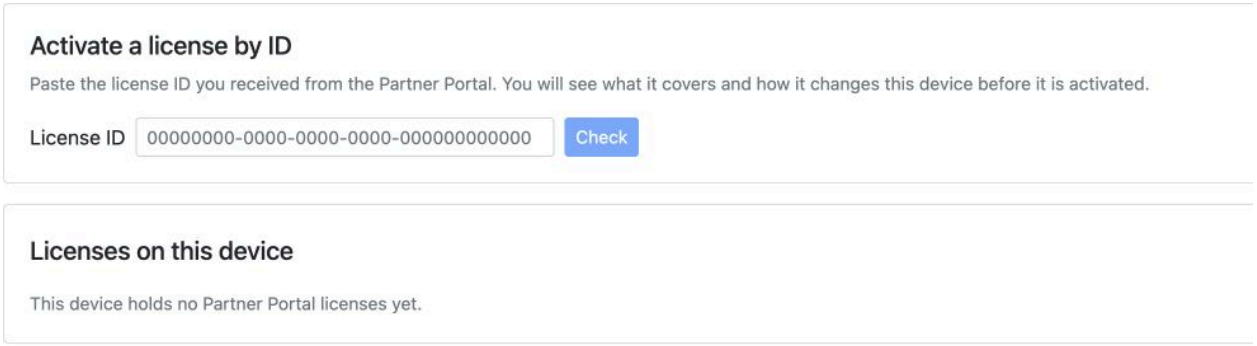


Figure 14. The license page checks an ID before the activation decision.

21 Troubleshooting and practical checks

Start by identifying what failed: access, camera capture, detection, event creation, recording, playback, delivery or a physical action. Work along that chain. Changing many settings at once makes it difficult to determine what fixed the problem.

Access and camera problems

Symptom	Checks to make before disruptive action
Web interface will not open	Confirm appliance power, network link and current address. Check whether the computer can reach that network and whether the IP changed. Verify the intended protocol/address with the administrator.
Camera is missing or offline	Confirm its power/network path, enabled state and credentials. Check ONVIF access for discovery and the source URL for manual feeds. A stale thumbnail is not evidence of a live connection.
Camera discovery finds nothing	Check that discovery is enabled and reachable, and whether a separate ONVIF user is required. Use the optional camera IP or a documented manual source when appropriate.
A substream cannot be selected	Check whether the camera exposes it and whether Substream URL is configured. The interface can explicitly mark it Not configured.
Live view reports an error	Try another camera and a recent archive clip, then check the source and network. Preserve the error/time for support rather than immediately restarting every device.
New camera exceeds capacity	Review the displayed megapixel budget and actual source resolution. Capacity is model/license-specific. Do not apply the inspected unit's 48 MP figure to another appliance.

Detection and event problems

Symptom	Checks and tradeoffs
Relevant object is missed	Inspect the actual footage, image quality, object size, capture source, motion threshold, confidence threshold and zone intersection method. Review rule/scenario eligibility and timing.
Too many false classifications	Improve framing/lighting, restrict irrelevant regions and consider increasing the appropriate confidence threshold. Verify that true events remain detectable.
Wind or shadows cause activity	Review zones, motion threshold and Unknown event settings. Lower motion thresholds can increase processing and environmental detections.
Alert arrives later than expected	Check loitering delay, proximity duration, action trigger delay and external delivery. Do not assume all delay is a network issue.
Repeated alerts	Check loitering reminders, scenario continuous notifications, count-change events, overlapping rules and duplicate notifier destinations.
Events appear while Disarmed	Check rules with Disarmed or Armed & Disarmed profiles, scenarios with All, and inactive-profile snapshot storage. Disarmed does not universally stop storage or every rule.

Symptom	Checks and tradeoffs
A zone seems ineffective	Confirm camera versus rule scope, active state, inclusive/exclusive precedence and center/edge evaluation. It is not a visual privacy mask.
A scenario never satisfies	Check All versus Any, absence/presence choices, object counts, source/target relationship, zone, schedule, mode and required license. Test each condition before combining them.

Recording and archive problems

Symptom	Checks
Detection image exists but no video	Confirm Recording, the selected recording stream, recording mode at that time, camera availability and retention. Detection storage and recording are separate.
Date is unavailable	Check the chosen camera, date/timezone and whether footage was ever recorded or has been removed.
Old footage disappeared early	Check storage capacity. The retention page explicitly allows earlier deletion when storage is full.
Download is incomplete or wrong	Recheck camera and time range, allow completion and play the saved file. Try a shorter interval to isolate the problem.
Video time differs from the camera overlay	Compare appliance timezone/UTC, camera clock and any burned-in timestamp. Do not silently shift an incident time without documenting the difference.
No compatible archive-copy drive	Check supported drive/filesystem requirements with Monitoreal. The available review did not establish those requirements or full copy scope.

Notification and action problems

Symptom	Checks
Event exists but no message arrives	Verify camera Alerts, eligible rule/scenario event choices, active notifier, recipient authentication, credentials, network/DNS and license. Check the receiving service's logs or rejection reason.
Email is rejected or delayed	Confirm the exact SMTP/security/port combination and provider limits. Reduce unnecessary repeats and verify recipients.
Webhook or monitoring-center event fails	Confirm endpoint, method, token/account/site fields, expected payload/report and receiving-system acceptance. A saved form is not a delivery test.
Relay action cannot choose a channel	Confirm that the relay is online and associated with this appliance. The reviewed offline relay left target selection incomplete.
Relay does not operate	Verify the event phase, target, mode/confirmation dependency and timing, then use the installer's safe hardware test procedure. Do not bypass required confirmation simply to make it operate.
Audio does not play	Check output device availability, selected file, size/format compatibility, timing and hardware volume/power. Warn occupants before a playback test.
Permission is missing	Inspect the actual role checkboxes, parent permissions and resource scope. Do not rely on the name Viewer or Editor alone.

Prepare a useful support request

Provide the appliance model and complete software version, the affected function, camera/rule/scenario identifiers, incident time and timezone, expected versus observed behavior, and the last relevant configuration change. Include a sanitized screenshot or short clip when appropriate. Download logs through Settings > System when support requests them.

Do not send passwords, bot tokens, invitation links or unrestricted configuration files through a public channel. Ask support which diagnostic files are needed and how to transfer them. If a maintenance action is proposed, confirm its effect on recording and access before proceeding.

22 Reference and further help

Before leaving a configured site

1. Verify the full software version and record the timezone.
2. Check every required camera's current image and intended capture source.
3. Confirm recording in each intended system mode and play a new archive clip.
4. Test representative objects and boundary positions for the configured zones.
5. Verify enabled rules/scenarios, timing, profiles and duplicate coverage.
6. Perform authorized notification tests with the intended recipients.
7. Have the responsible installer test physical outputs and their return/stop behavior.
8. Verify the next scheduled mode changes and the permissions of each operational account.
9. Check retention against actual capacity, then preserve a current settings backup.
10. Hand over the configuration record, recovery contacts and known limitations.

This is a recommended commissioning sequence. It does not imply that these live operational tests were all performed while preparing this guide.

Useful links

Monitoreal support · Documentation center · Software release notes · Monitoreal website

Use the documentation for your exact hardware and installed build. External service interfaces and licensing workflows may change independently of the appliance software.