Sentry Firefly

Configuration Guide

Version 2026R1

05.02.2026

Contents

Copyright, trademarks, and disclaimer

Trademarks

Sentry is a trademark or registered trademarks of IntelexVision. All other trademarks mentioned in this guide are the property of their respective holders. This product may make use of third-party software for which specific terms and conditions may apply.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

Disclaimer

This document is intended for general Information purposes only and due care has been taken in its preparation. Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

IntelexVision may make changes without prior notice.

This product may make use of third-party software for which specific terms and conditions may apply.

1 Introduction

1.1 Scope

This document provides instructions for configuring **Sentry Firefly** using ***WebSettings*** UI, which can be accessed via any common web browsers such as Chrome, Firefox or Edge. This allows users to configure **Sentry Firefly** system installed locally. It is assumed **Sentry Firefly** was successfully installed.

The scope of this guide is limited to the configuration phase and does not include information about the installation of the system.

1.2 Audience

The following roles are the intended audience for this guide:

- **System Administrators:** Responsible for managing the infrastructure and ensuring the software is installed correctly within the organization's IT environment.
- **IT Support Engineers:** Tasked with resolving technical issues during installation and initial setup.
- **Solution Architects:** Overseeing the installation to ensure alignment with the organization's architecture and project requirements.
- **Technical Implementation Specialists:** Handling the detailed implementation of the software for specific use cases.
- **Product Specialists:** Verifying the successful setup and ensuring that the installed component meets the business needs.

2 Pre-requisites

2.1 Technical Knowledge

- **Operating System Proficiency.** Familiarity with Windows-based systems, including navigating the interface, using command-line tools (e.g., PowerShell), and managing system settings.
- **Networking Basics.** Understanding of IP addressing, ports, firewalls, and network protocols commonly used in enterprise environments.
- **Web Interfaces** and b**rowser-based Configuration Tools**. Understanding how to navigate, manage, and customize settings within web-based platforms.
- **Video Surveillance Systems knowledge**. Understanding how security cameras, recording devices, and monitoring software work together to provide surveillance and protection.
- **Troubleshooting Readiness.** Knowledge of basic troubleshooting steps, such as interpreting log files or checking service statuses.

2.2 System Access

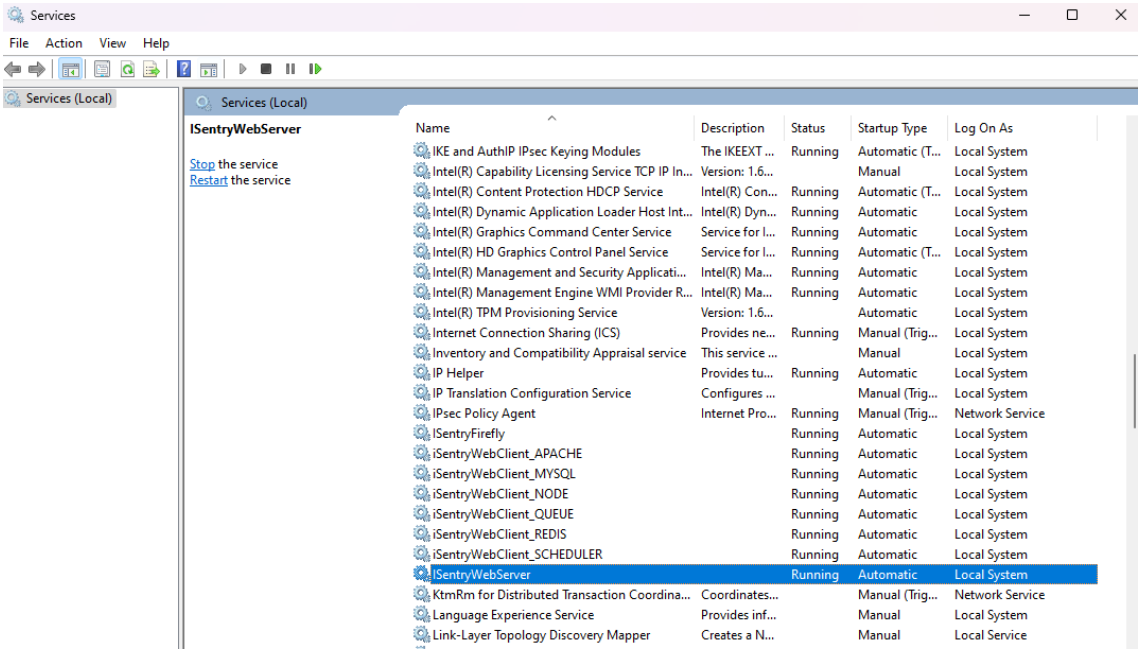
- **Administrator Privileges.** Access to a user account with administrator rights on the target Windows machine.
- **Network Permissions.** Make sure you have the required permissions to install software and adjust network settings, such as setting up firewall exceptions.

2.3 Preparatory Tasks

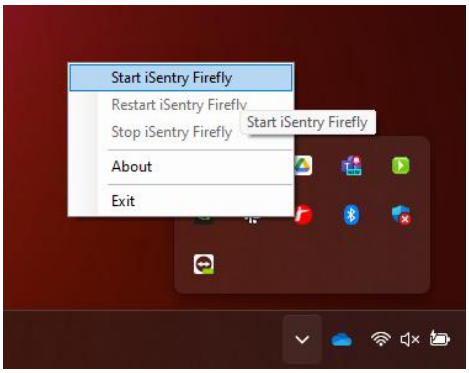
- **Review Documentation.** Familiarize yourself with this guide and any other documentation.
- **Backup Policies.** Make sure there's a backup plan ready for any existing software or data that could be impacted during installation.
- **Dependencies Check.** Verify that all required software components or services (e.g., runtime environments, frameworks) are pre-installed or accessible.

3 Pre-requisites

Check the **iSentryWebServer** service is running (on windows):



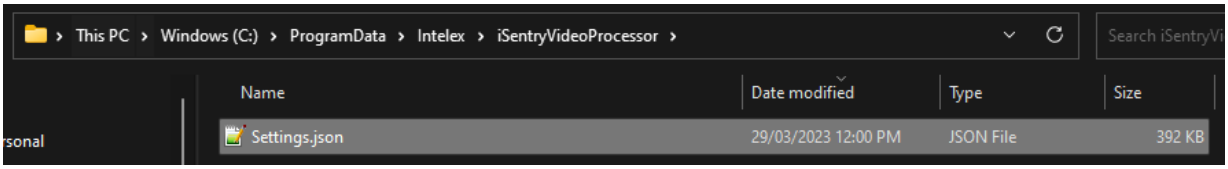
If is not present double check your **Sentry Firefly** icon tray and start **Sentry Firefly**.



3.1 Settings file

After a new installation a template file **Settings.json** will be created on the server:

[isentry_folder]/iSentryVideoProcessor/Settings.json



This file is a JSON formatted file which contains the human readable settings for **Sentry Firefly** to run.

> **INFORMATION**
>
> Some experimental or limited features are only available by manually editing this file but be aware that manipulating or altering this file other than the options mentioned in this manual will cause the system to fail.

3.1.1 Downtime

The user can alter the Downtime key to configure a VP: Scheduled daily restart, for doing so follow these examples and prepare yours accordingly.

- Every 100 hours uptime

```
"Downtime": {
   "Enabled": true,
   "DurationBasedDowntime": 100
},
```

- Every Sunday at midnight

```
"Downtime": {
   "Enabled": true,
   "WeekSchedule": [
      "DayOfWeek": 0,
      "Hour": 0,
      "Minute": 0
   ]
},
```

- Every Second Wednesday at 12:30pm

```
    "Downtime": {
       "Enabled": true,
       "WeekSchedule": [
          "DayOfWeek": 3,
          "Interval": 2,
          "Hour": 12,
          "Minute": 30
       ]
},
```

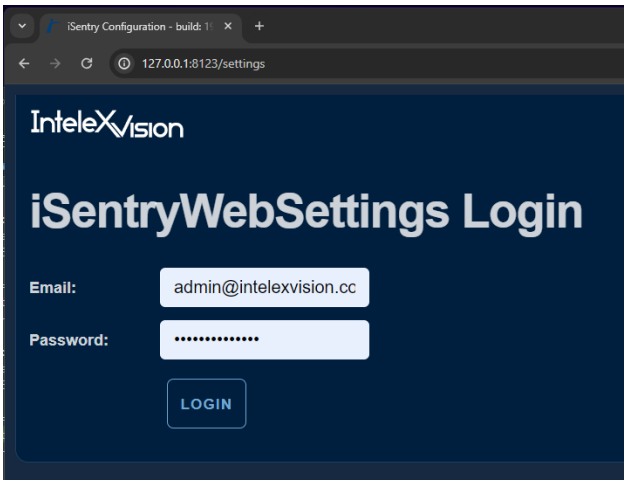
3.2 Integrators management

One of the **most important configurations is the authentication of integrators** who will be receiving alerts from **Sentry Firefly**. To do this please read this section carefully.

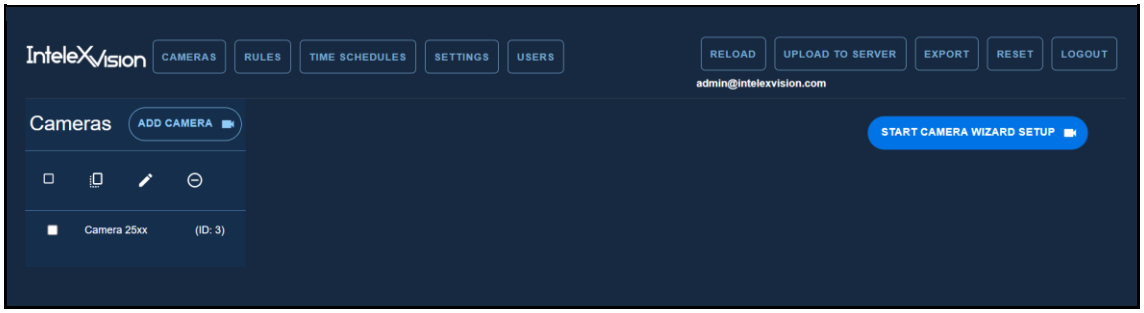
4 WebSettings Interface

Access via web browser to the <URL>:<port>/settings knowing that the port is 8123. In a Linux server you must enter <URL>:<port>/settings**?ServerID=1.**

You will be presented with the login menu:



After you login, the main menu contains in the top bar the logo followed by ten buttons described in the table below and the list of **Cameras** in the left side panel, this is the default view:



Button	Descriptions
Cameras	Switch to **Camera** Menu. This menu is used for configuring all the settings for cameras in the server.
Rules	Switch to **Rules** Sub-menu. This menu is used for configuring classification rules and their associated alert/dismissal actions.
Time Schedules	It brings the menu for building personalised schedules for different moments. Cameras might be more active or have improved image quality at certain times of day.
Settings	It opens the menu for managing the main settings of the server.

Users	Manage the users that can log into the websettings website.
Reload	Load the latest settings for Settings.json file stored in the server.
Upload to Server	Save the latest changes users have made with the Web Settings tool to Settings.json stored in the server.
Export	Download a copy of the latest Settings.json stored in the server to the user's local hard drive.
Reset	Reset all settings on the Web Settings tool to Default State. Note: This reset will delete all user's custom cameras, time zones and rule settings. A set of default configurations will be loaded instead.
Logout	Ends the current user session.

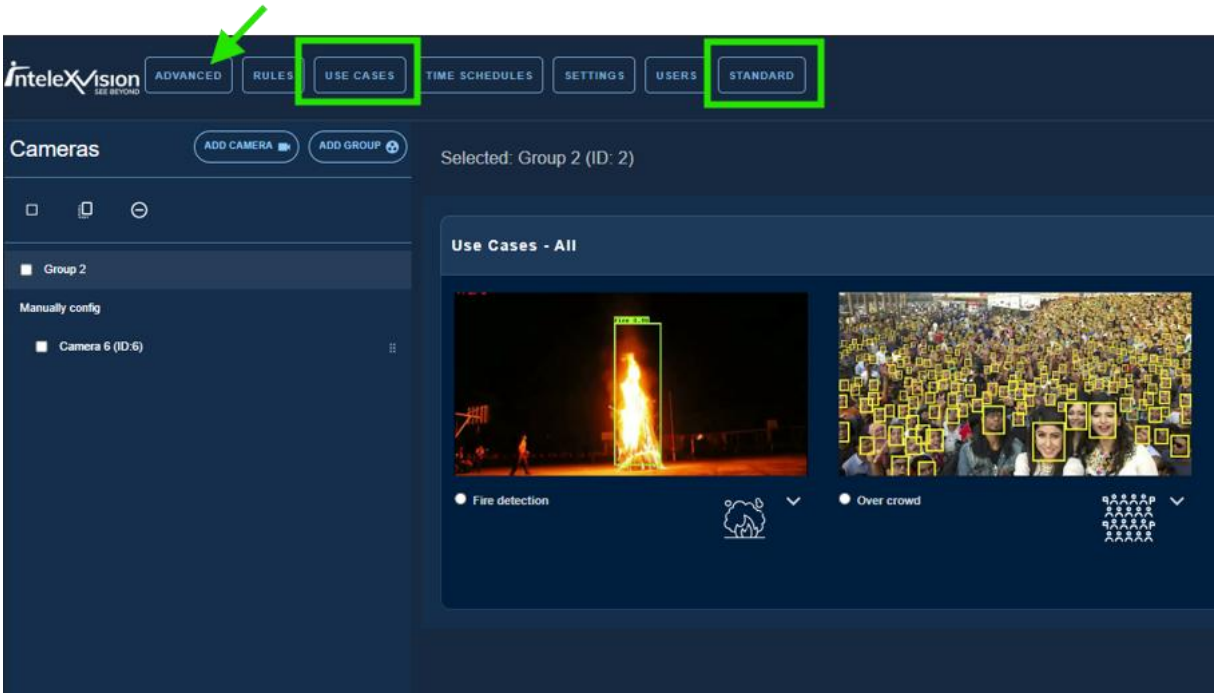
4.1 Standard Camera

The user can configure cameras at scale. Using a template use-case-oriented the user can propagate the behaviour of the use case to multiple cameras that belong to the same group.

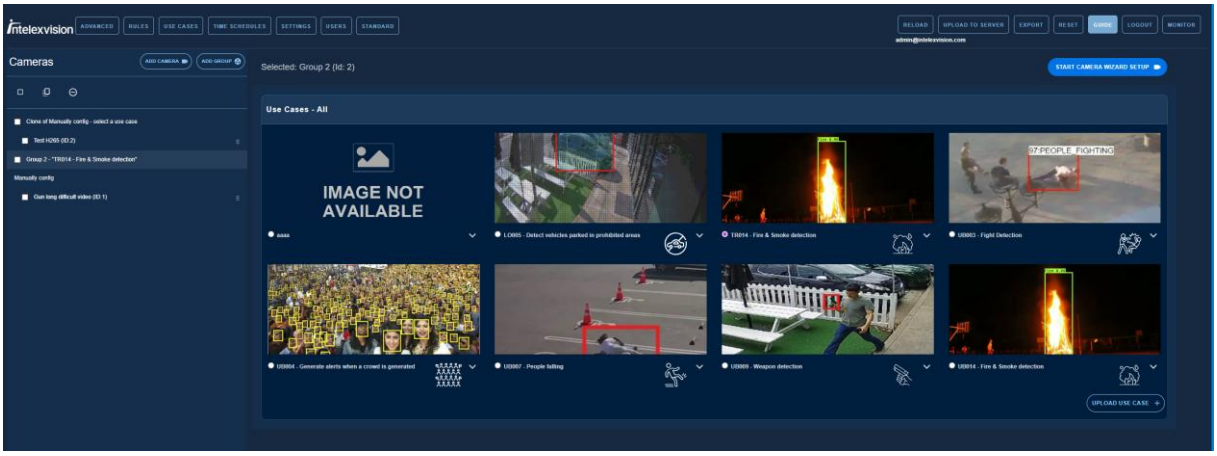
Enabling this setting falls into Experimental mode:

When doing so, the Cameras menu will be become Advanced and Use Cases and Standard will show up.

When you click in Standard you will be able to add cameras to groups, and these groups will have a predefined behaviour as described by the use case they cover. Below we have Fire Detection and Over Crowd:

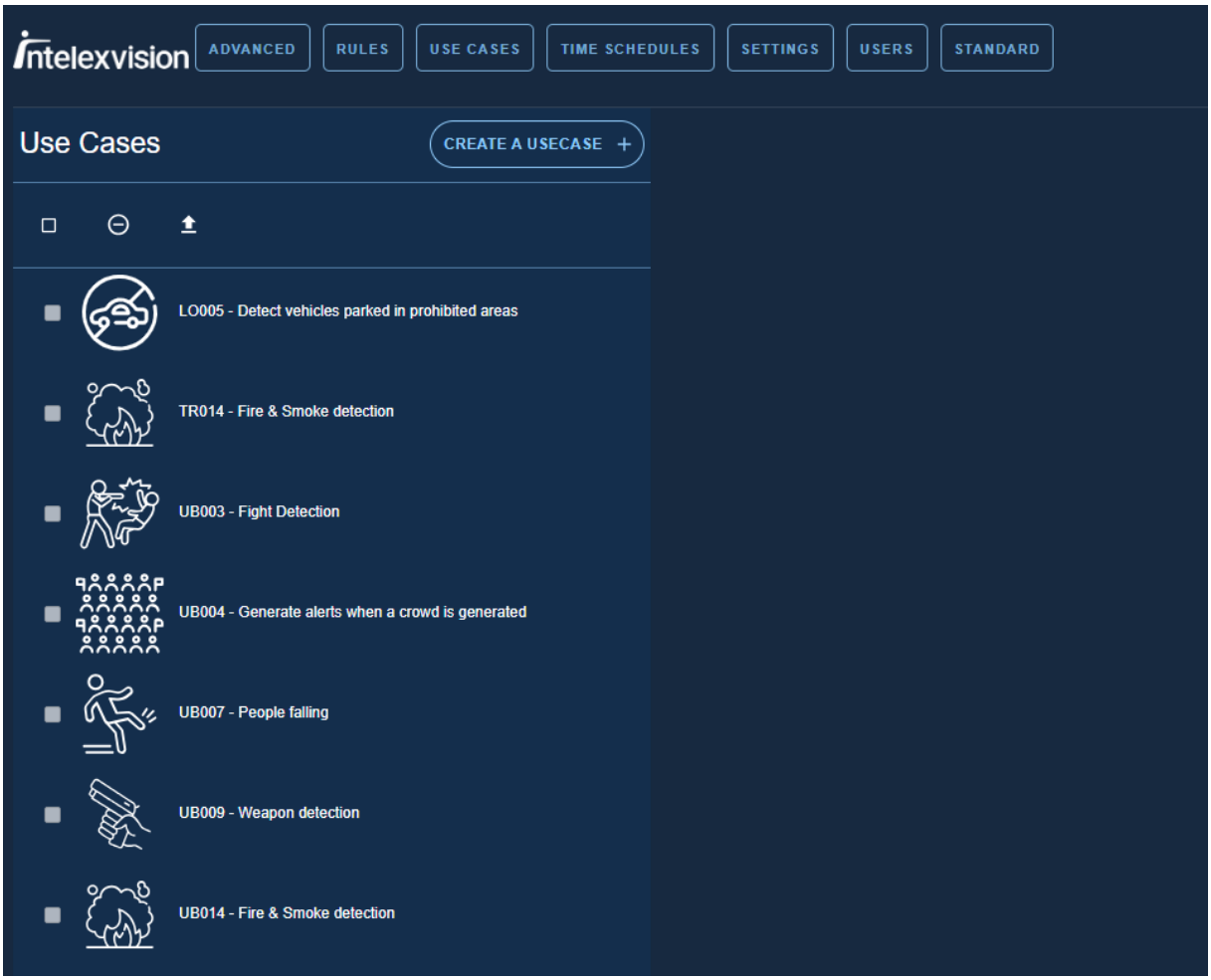


The group will follow the behaviour of the selected use case, as will the cameras within it. In the example bellow the Group 1 has the behaviour of TR014 - Fire & Smoke detection (TREX Fire and Smoke), so cameras added in it will inherit its behaviour.



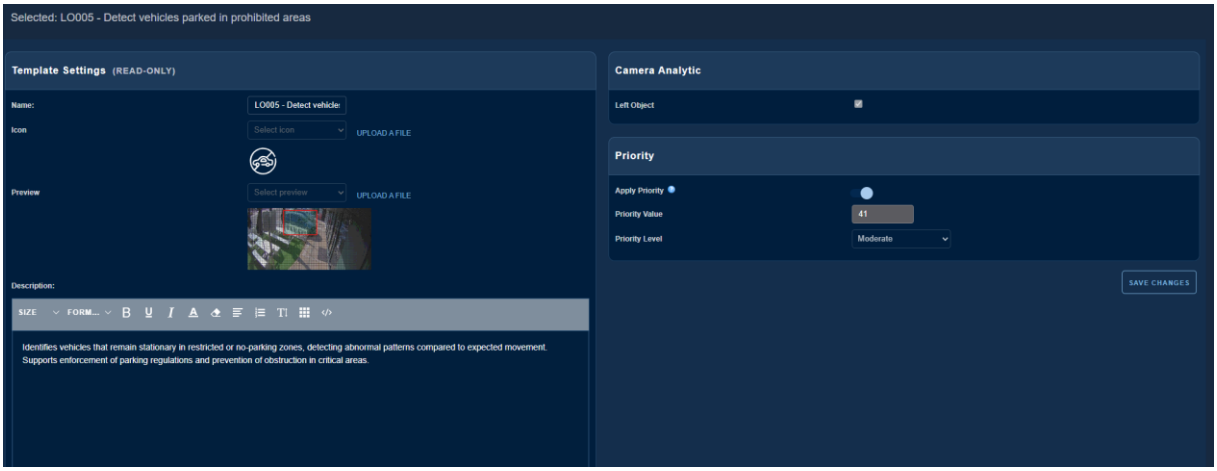
Camera specific configuration will not be overridden by the use-case-oriented settings such as masks, wire position and ROIs. This option is only available if experimental features are turned on, which is NOT the case by default.

If the user clicks in Use Cases a list of built-in use cases will show up:



The user can create or upload Use Cases using this menu. Follow a naming convention for a good practice such as Analytic followed by a number and a short description, for example UB015 – Fire & Smoke detection.

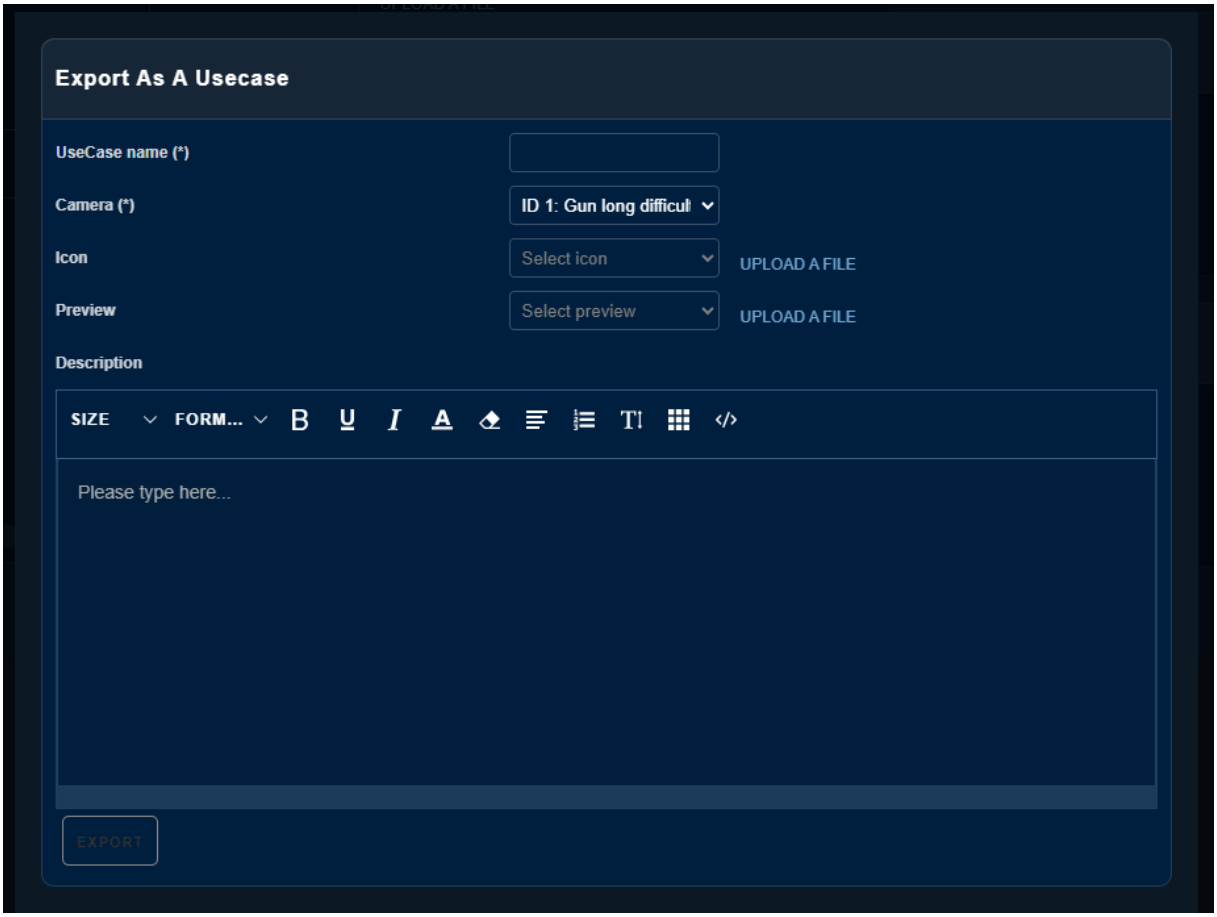
When you click in one Use Case you will be presented with the following screen:



It contains the name, the icon, the preview of an image showing what that camera looks like, a text area for entering a text description and in the right-hand side the Camera Analytic that the camera has (Left Object in the example) followed but the priority of the rule that the camera has in case there is any.

4.1.1 Creating Use case

When clicking in create use case the following screen is displayed:

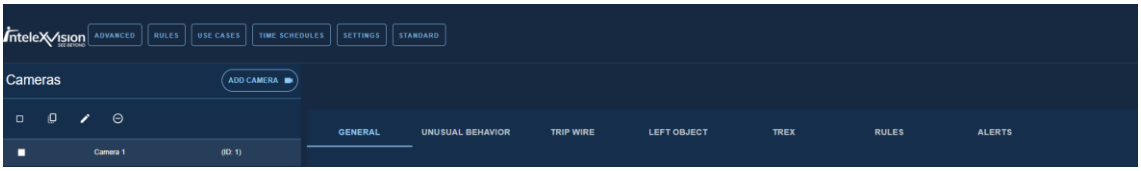


The user can enter a descriptive name, enter de camera from which the use case will be based on, inheriting the common things such as rules and analytics but not the camera dependant attributes such as masks or regions.

Once you are done you click export and a save dialog will ask you where to save your UseCase file (a Json file), which can be uploaded later.

4.2 Advanced Cameras

At least one camera should be added first. When you click one **Camera** the centre panel shows 7 tabs (note it can be more if selected such as Flow when selected):



General (default view)
Unusual Behaviour
Trip Wire

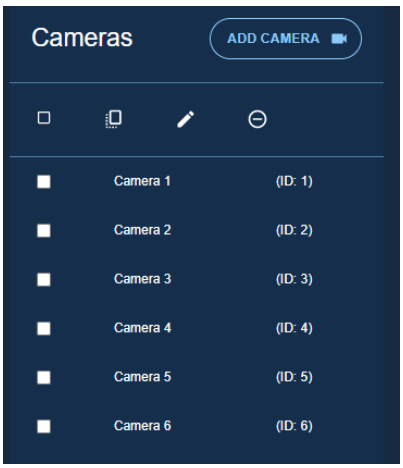
Left Object
TRex
Rules
Alerts

We will go through all the options in detail in the following sections.

Please note that some of these sub-menus can be enabled/disabled from Settings as shown in the image below (i.e. in the image below Tamper (BETA) is disabled):

4.2.1 Add/Remove Camera

This is the list of the cameras:



Users can Add/Remove new customised cameras using **Add** or **Remove buttons.**

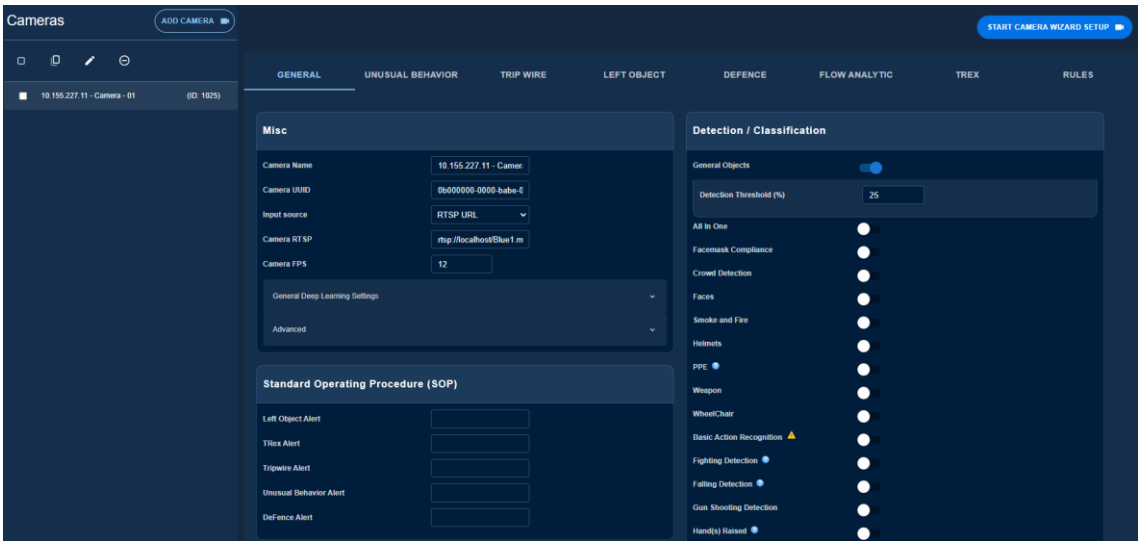
Add Camera	ADD CAMERA
Remove	

Other interesting options are Bulk and Clone, it will help you in a scenario with a high number of cameras, the user can use them to edit in bulk or clone one or many cameras at once.

Bulk Edit		Can be used to edit multiple selected cameras at once.
Clones		For creating a duplicated version of a selected camera.

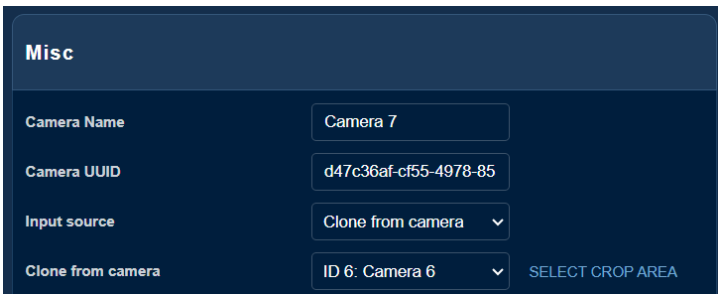
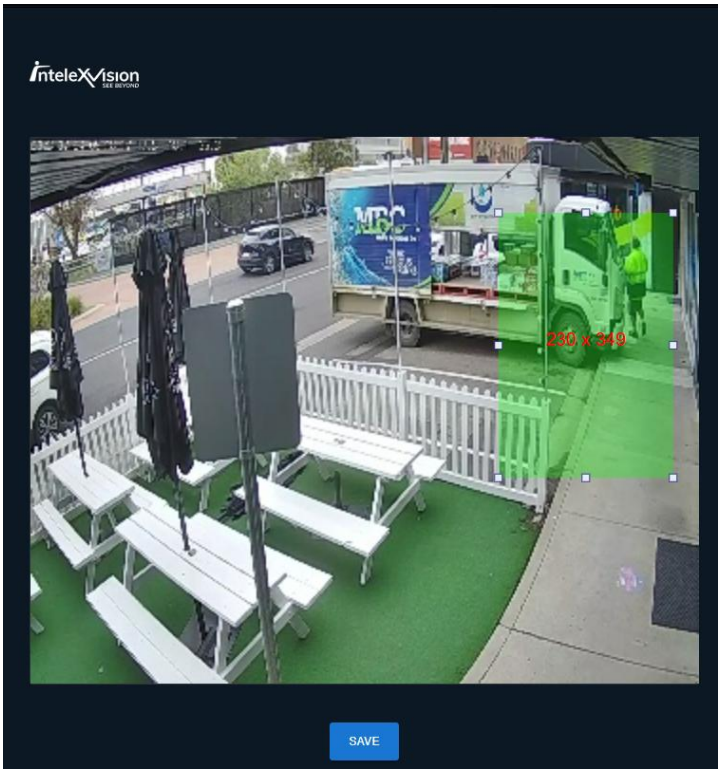
4.2.2 General (Camera Settings)

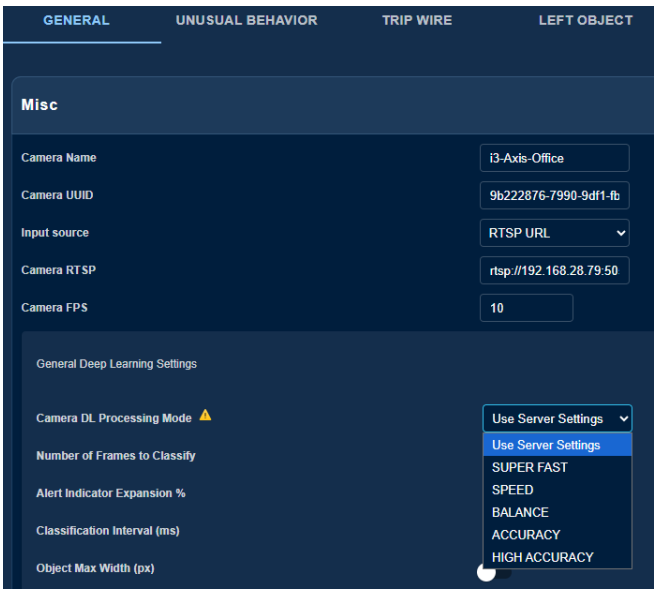
This submenu contains general camera configuration, including:



4.2.2.1 Misc (General Deep Learning settings and Advanced menu):

Misc	Default	Description
Camera Name	-	Camera name customised by users.
Camera UUID	-	The value provided here will be used for third-party integration. For example in Sitasys it will be deviceid/siteid depending on the use case (more info :Sitasys deviceId)
Input source	RTSP URL	Use this setting to clone a camera feed.

		  Cloned cameras do not decode the video stream. ⚠ Hint: some browsers do not display properly the cropping UI, please zoom out/in on your browser to bring back the cropping UI.
RTSP	-	Link to a real-time streaming of the camera view.
Camera FPS	12	Average frame rate (fps) of cameras.
Misc → General Deep Learning Settings	**Default**	**Description**
Camera DL Processing Mode ⚠When your hardware can handle.	Inherit Server Settings	This DL mode is only for full-time per camera analytics such as TW DL counting, fight detection, gun detection.

		
Number of Frames to Classify	3	The number of frames in which object classification is performed per alert.
Alert Indicator Expansion %	5	Expands the bounding box of the alert indicator causing the event. Check the case study section for more details.
Classification Interval (ms)	500	Duration (ms) between frames that the system uses to perform object classification on.
Object Max Width (px)	Disabled	Maximum width (pixel) of bounding box.
Object Min Width (px)	Disabled	Minimum width (pixel) of bounding box
Object Max Height (px)	Disabled	Maximum height (pixel) of bounding box
Object Max Height (px)	Disabled	Minimum height (pixel) of bounding box

Misc->Advanced	Default	Description
Camera group	0	Camera group: customised by users. (Must be a number)
Minimum Alert Duration (s)	2	Minimum time (seconds) between two alerts of the same analytic type.

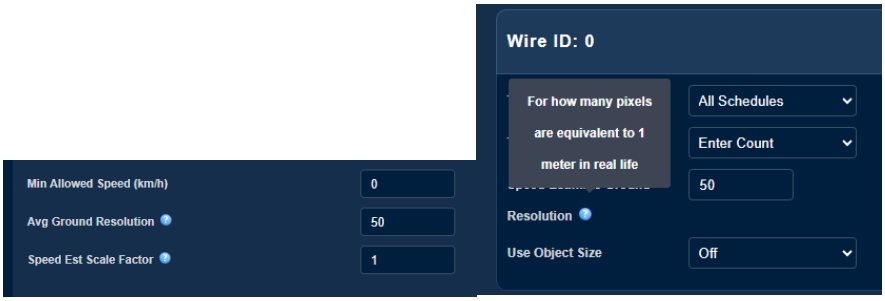
GPU decode	OFF	Enable/Disable GPU Decoder.
Disable Loss of Signal Alerts	OFF	When a signal is lost with the camera, enable or disable the alert about this.
Video Codec	H.264	Support codecs: H.264, H.265, MJPEG, VP8, VP9
Colour Processing	ON	Enable/disable processing video in colour.
Output Alert Video*	OFF	Enable/disable outputting alert video. See directory **[isentry_folder]/iSentryVideoProcessor/AlertOutput**
Output Alert Metadata	OFF	Enable/disable outputting metadata of video. Base64 embedded in .idat file in **[isentry_folder]/iSentryVideoProcessor/AlertOutput**
Image Quality	Standard	Standard/High/Lossless (important if you want to visualize in the alert images crisp text such as numbers for plate recognition).
Overlay Detected Object	OFF	Enable/Disable drawing detected objects by the DL on the output image.
Overlay Nearby Objects Only	OFF	Enables/Disables drawing a box around detected objects **close** to the Alert Indicators (Alert Indicators are a square depicting where the alert just happened, in the picture below is a TW Alert Indicator). If it's ON, it only shows **red boxes around** objects if the Render Detected option is ON like in the image below:  If it's OFF, it shows **red and yellow** detection boxes like in the image below:

		
Show DL Detection Object Probability	ON	Enable visualizing the percentage of confidence in the prediction from the DL model.
NVR Compatibility Mode	OFF	
Frames Process Ratio	1	Process one every nth frame with n is input value.
Enable TCP Connection	ON	Using TCP is highly recommended as this protocol will guarantee video packet transmission. However, in some cases, such as congested or high delay networks, using UDP may deliver more videos to Sentry at the cost of higher video corruptions. Use UDP only if there is no other choice and you are aware of the downsides.
Max Input Frame Gap (ms)	5000	It sets the maximum time in ms for the gap between frames. Above this value a frame gap log is saved to disk in "Cam_1_Connection_Error.txt".
Enter/Exit Estimate ([1])	OFF	Estimate object enter/exit speed. When is on you can use for TREX enter/exit or TW DL counting (enter/exit).
Max Allowed Speed (km/h)	0	Max Allowed Speed
Min Allowed Speed (km/h)	0	Min Allowed Speed
Avg Ground Resolution	0	For how many pixels are equivalent to 1 metre in real life
Speed Est Scale Factor	1.0	Default value is 1.0. Adjust the value to compensate for ground resolution estimation error.

4.2.2.2 ([1]) Setting Up Enter/Exit speed alert

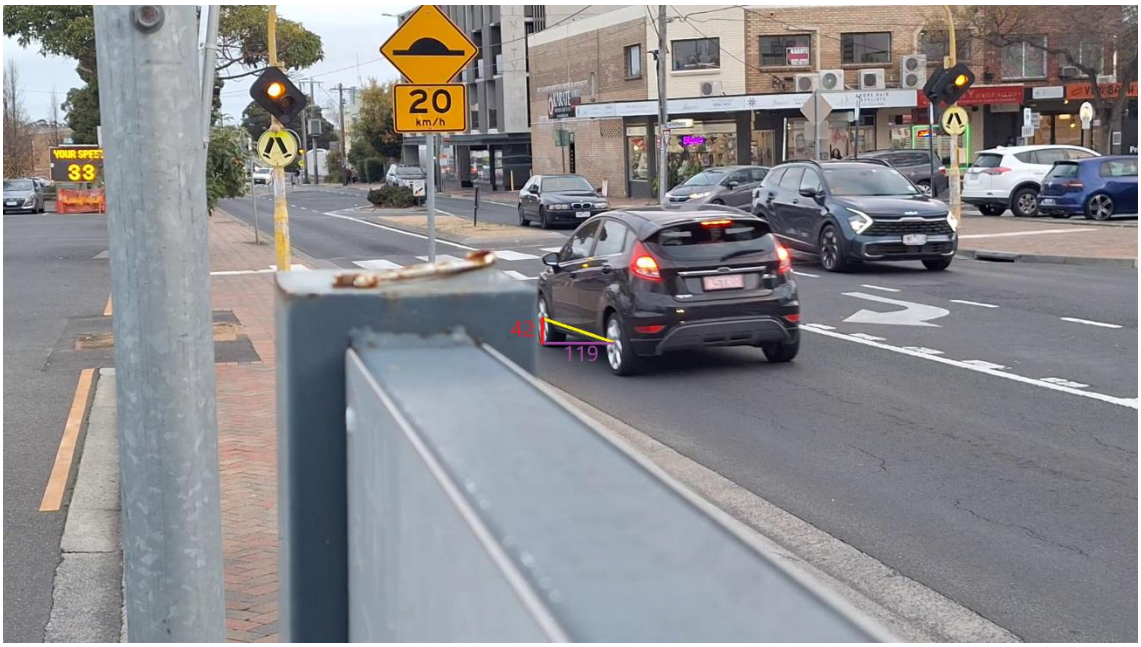
To raise alerts on too fast or too slow vehicles in a certain scene, one can set up enter exit alerting with speed estimation turned on, available in the General/Misc Advanced:

Standard Enter/Exit count settings are required to set up speed estimation alerting. It is important to understand that the speed estimation accuracy is not very high and **should only be used as a guide only**. **The estimated error ranges around +/- 10Km/h, if set up properly**. **The maximum speed that can be estimated accurately is 40Km/h**. The key to achieve a good result is to set the **accurate average ground resolution for Trex or TW DL counting:**

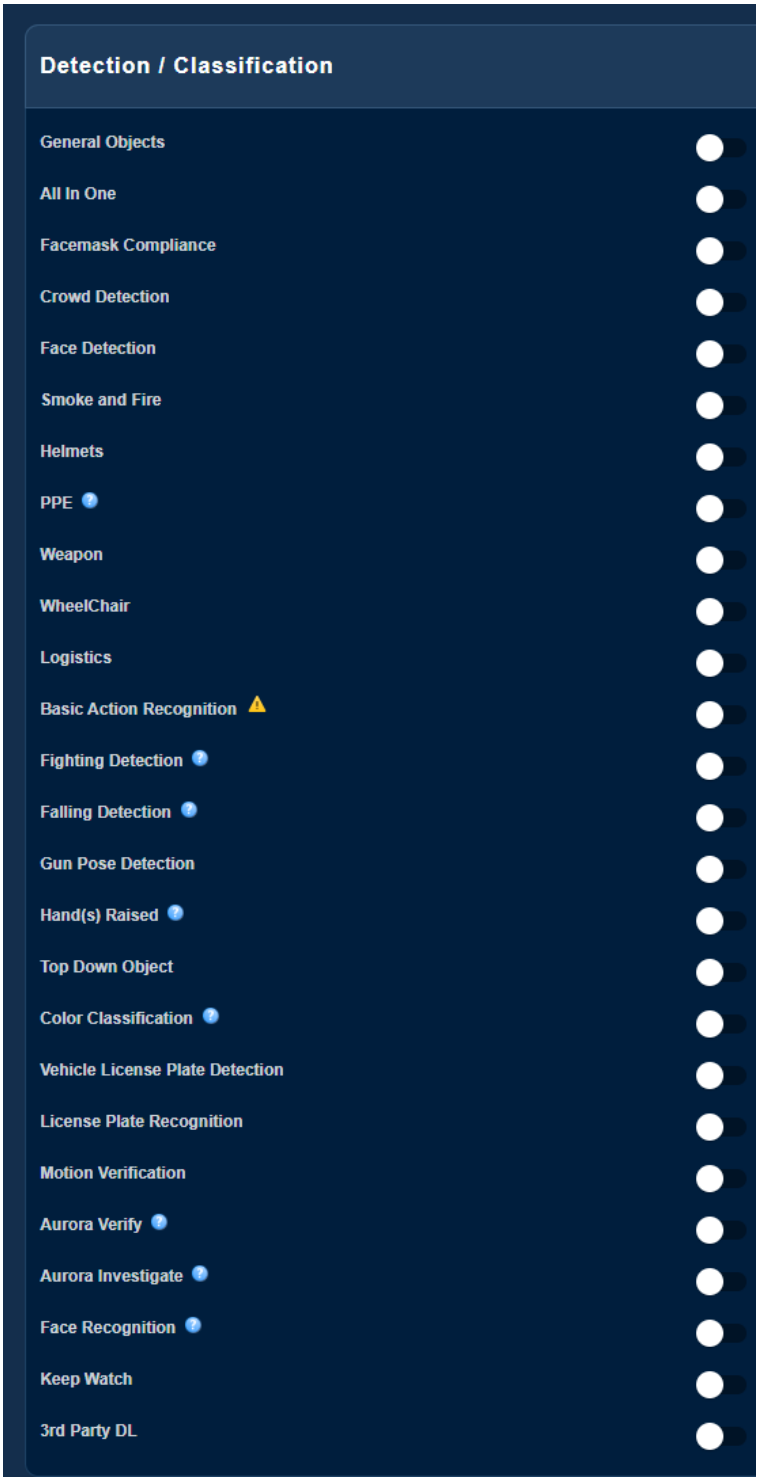


There are several ways to set this value including:

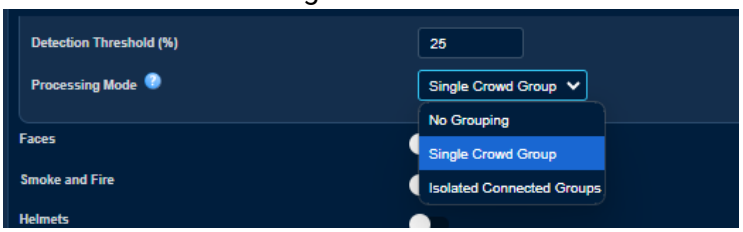
1. Real life measurements: At the interested area use a tape measure on the road/path to measure how many pixels in the colour background images in folder in the ***C:\Program Data\Intelex\iSentryVideoProcessor\images (take colour image)*** folder is equivalent to 1 metre in real life.
2. Estimate measurements: like the above method but instead of physically being on site, one can use known images of reference objects to estimate the distance (there is always a distortion when the camera is forming an angle with the objects). For example, the wheelbase (distance between axis) of a Ford Fiesta is ~2.5m. In the image below we calculate the hypotenuse is ~126 pixels (yellow segment) so you can calculate that 126pix/2.5m = ~50pix/metre. This is the value to use in the **average ground resolution**. It is advisable to calibrate these settings several times with real world verification to compare and improve the accuracy of the output.

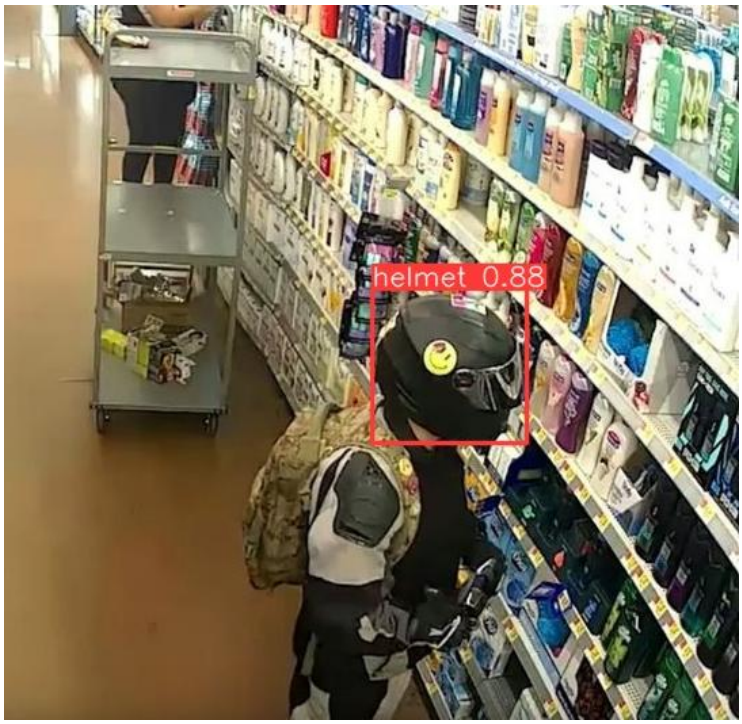
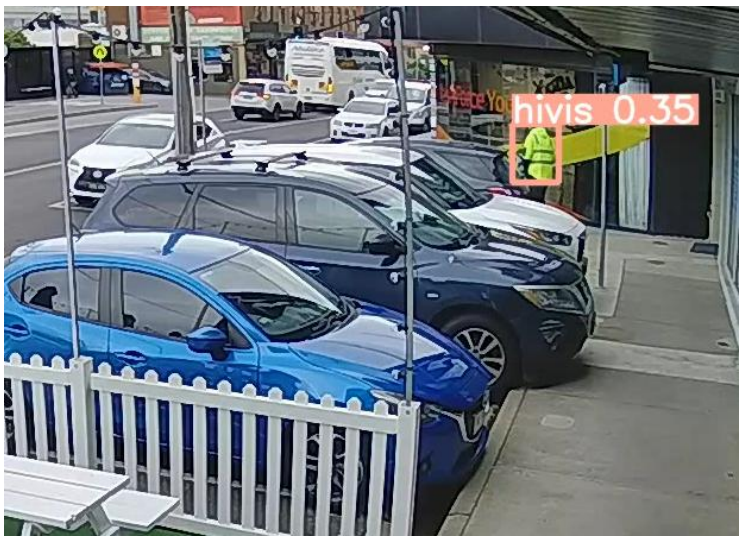

20
km/h
33
42
119

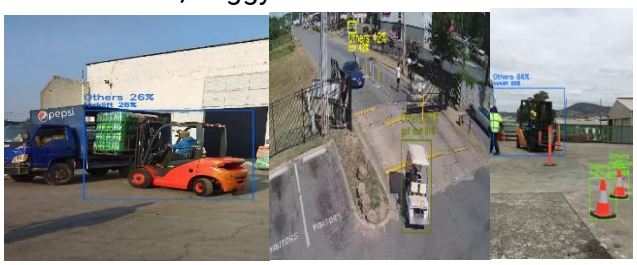
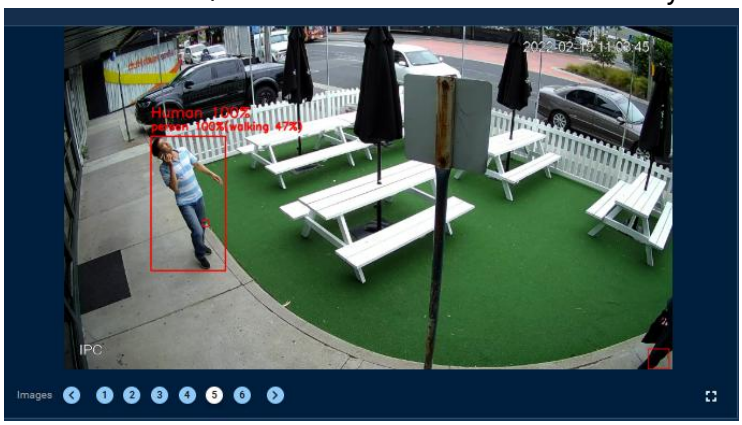
4.2.2.3 Detection / Classification:

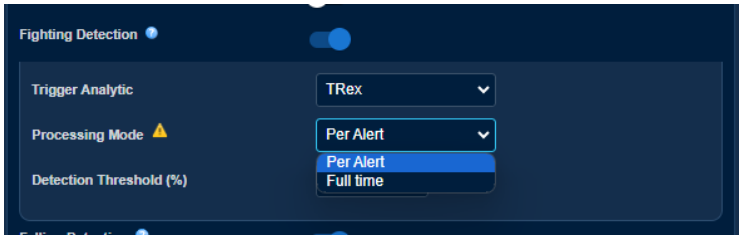


Settings	Default	Description
General Objects	OFF	Detect and classify general object types, such as person, dog, cat, car, truck, bicycle, etc.
All In One	OFF	Detect and classify general objects such as backpack, handbag, cell phone, etc.

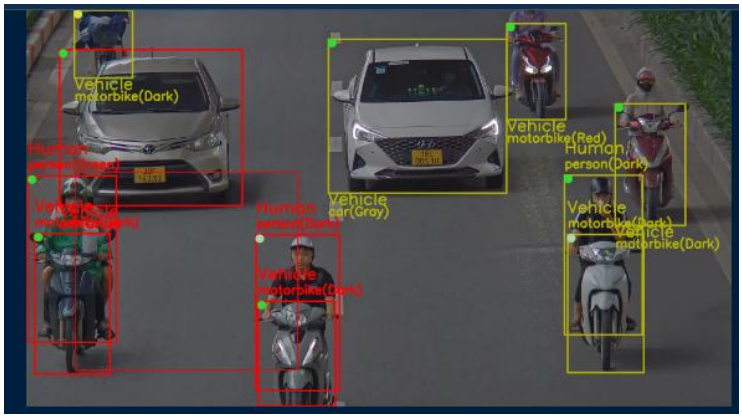
Facemask Compliance	OFF	Detect personal facemask. The detected objects will be: • no mask • partial mask • facemask compliance
Crowd Detection	OFF	When there are many people. Crowd can detect single person, crowd as a big group or groups of crowds. Combine with Rules to get the most out of it.  • No grouping: object type will be person, so with the rules we can count how many objects type “people” are present. • Single crowd group: object type will be ONE “crowd” with key count: n (n number of people), so with the rule one can say a crowd > n | n = 20 for example. • Isolated Connected groups: object type will be SEVERAL “crowd” with key count: n (n number of people). You can use Rules to trigger for crowds in different locations in the scene.
Face Detection	OFF	Detects human faces
Smoke and Fire	OFF	Detects fire and smoke. Need to be clearly visible 

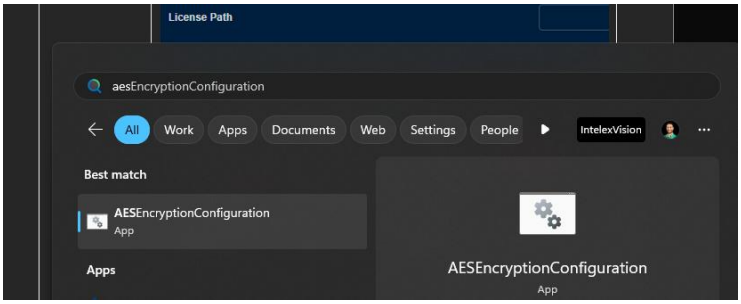
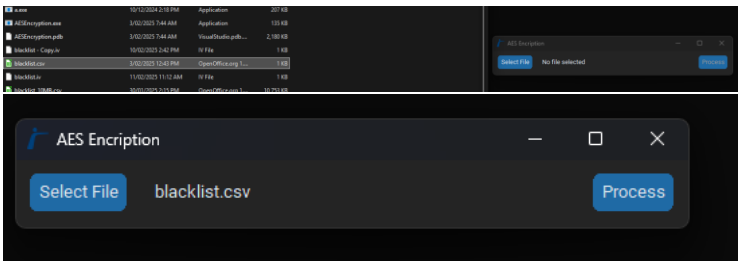
Helmets	OFF	Detects motorbike/bicycle helmets. Combine this with person/people detection and create rules to get the most of it. You need a good view of the subject. 
PPE	OFF	Detects personal protection equipment such as hi vis vest, glasses, safety helmets etc. Needs general objects to work. You can enable compliance or detection. Compliance will detect negative objects such as no_hivis or no_hardhat for you to apply rules. 
Weapon	OFF	Detects weapons such as guns, rifles and shotguns. Preferred a low mount and low angle view.

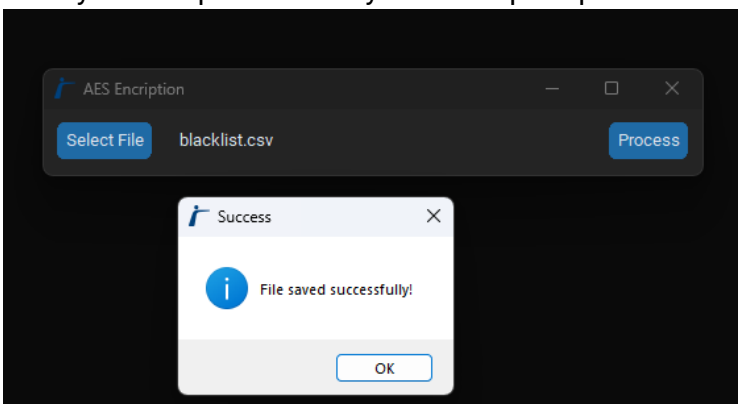
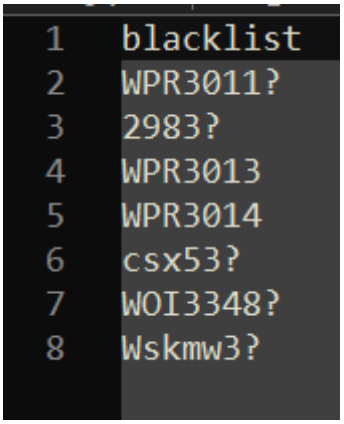
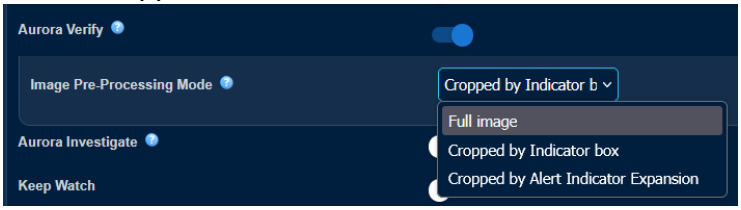
		
Wheelchair	OFF	Detect wheelchairs. Need good unobstructed view of the wheelchair(s)
Logistics	OFF	detect forklift, buggy cart and traffic cone. 
Basic Action Recognition	OFF	Detects people action: Standing, Walking, Sitting, Lying Down, Standing Up, Sitting Down, Fall Down. Require General Object Detection enabled. Preferred low mount and low angle view. Currently only available on Nvidia-enabled servers/PCs. Needs 9-10 frames to classify. 
Fighting Detection	OFF	Resource intensive. Use at you own discretion.

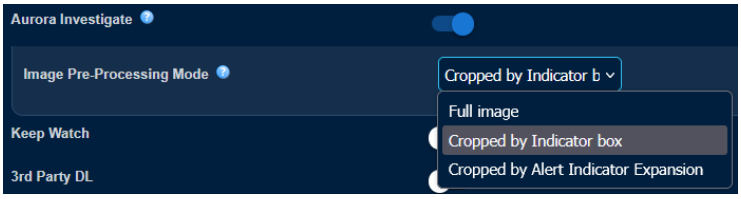
		 This detection mode can be alert-driven or fulltime (continuous mode frame by frame which is resource intensive). This detection mode can be alert-driven or fulltime (Only TREX and you can apply masking). 
Falling Detection	OFF	Resource intensive. Use at you own discretion.  User can decide which analytic triggers the detection. This detection mode can be alert-driven or fulltime (Only TREX and you can apply masking).

		
Gun Pose Detection	OFF	⚠ (Experimental) Alert Base mode or Full Time mode. If Full time mode, alert type is Action and Trex/Flow Analytic is required with suitable processing interval.  Threshold options are special in this detector: 25%: there is something like a weapon, but it could be phone or another object that the person is holding. Use this for difficult scene (such as far away, fast movement and/or need high security and accept more false positives 50%: something is more concerning, and we think the operator should be aware of this. The chance of false positive is lower but still exists. This is the recommended balance to close range, good quality set up 70%: we will raise and alert if something quite concerning detected. At this point, false positives are still possible but should be a lot less. Someone holding a phone/gun up and point it to someone, it will likely alert. But someone just look at the phone while walking, generally Sentry will not be triggering. However, this mode will miss true alerts if the person is showing the gun (not pointing the gun with the intention/action to shoot). It will also miss the gun if the gun only appears for a very short duration (due to occlusion or running for example). ⚠ Full time mode: might be the case when FF produces a lot of TREX alerts. If the user is ONLY interested in gun pose detections it is highly recommended to setup a rule to dismiss “TREX no gun”.
Hand(s) Raised	OFF	Detects hand raised from people. Require General Object Detection enabled. **Require** low mount and low angle view. Currently only available on Nvidia-enabled servers/PCs

Top Down Object	OFF	Detects objects when the camera is placed up in a tower and points to objects in the floor. 
Colour Classification	OFF	Classify the colour of detected objects. It needs General Objects model to be enabled. 
Vehicle License Plate Detection	OFF	Detects plates in vehicles.
License Plate Recognition	OFF	Recognizes the plate in vehicles, it also allows extra configuration from Settings tab such as: 

		Geographical region such as Dubai. When you enable blacklist/whitelist you can provide a local path to your directory containing the `blacklist.iv` and `whitelist.iv` encrypted lists of plates. This way you can apply rules for your convenience. Two tools are provided, one installer of UI tool and one CLI tool called `lpr_tool` for creating your encrypted plate lists. `lpr_tool` is a utility is included in your Sentry Server installation directory. Run from CLI: `lpr_tool` –input `blacklist.csv` to create your `blacklist.iv` file. `lpr_tool` –input `whitelist.csv` to create your `whitelist.iv` file. The UI tool can be installed: AESEncryption-1.0.0-x86_64 That way you can run from your Windows programs list as:  You will be presented with the UI tool where you can pick your `blacklist.csv` or `whitelist.csv`. 

		Then you click process and you will be prompted with:  These files must contain the plates information like:  Where the first line is the column title and the following are plate numbers. They must be saved as blacklist.csv or whitelist.csv.
Motion Verification	OFF	
Aurora Verify	OFF	Enables our Aurora Verify model to provide Generative AI insights into alerts. See rules section to configure it. It can be applied to:  For stability reason, its recommended to only enable ONE Aurora per camera (either Verify or Investigate type).
Aurora Investigate	OFF	Enables our Aurora Investigate model to provide Generative AI insights into alerts. See rules section to configure it. It can be applied to:

		 For stability reason, it is recommended to only enable ONE Aurora per camera (either Verify or Investigate type). 
Face Recognition	OFF	Faces can be recognized; you need to configure a Face Recognition Server. See specific manual “Sentry Face Recognition - User Guide” for detailed setup. You need to enable it into FF settings to enable the corresponding menus: 
Keep Watch	OFF	Enables Firefly to use the Keep Watch functionality. It requires saving videos in Video Recording/Settings/misc: 
3rd Party DL	OFF	Enables the sending of alerts to a third-party for applying their DL models to the triggered alert. You should be given the following parameters: **Name URL Exchange Route Username Password**

Each detector of the above has the following advanced options:

Settings	Default	Description
Detection Threshold	25	The higher threshold, the higher confidence to detect objects and vice versa. Range from 0-100 in percentage

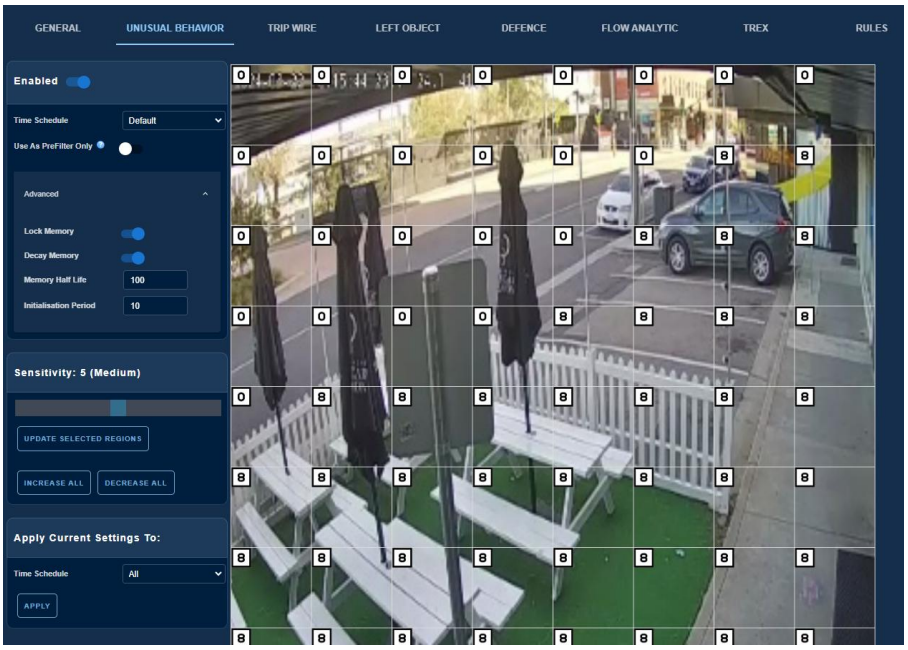
4.2.2.4 Standard Operating Procedure (SOP)

Settings	Default	Description
SOP for Left Object Enable	-	Alert message to the operator to suggest standard action when a specific alert (Left Object, TRex, Tripwire or UB) is triggered.
SOP for Trex Alerts	-	
SOP for Tripwire Alerts	-	
SOP for Unusual Behaviour Alerts	-	

4.2.3 Unusual Behaviour

This sub-menu contains the settings for the camera's Unusual Behaviour (UB) Functionality.

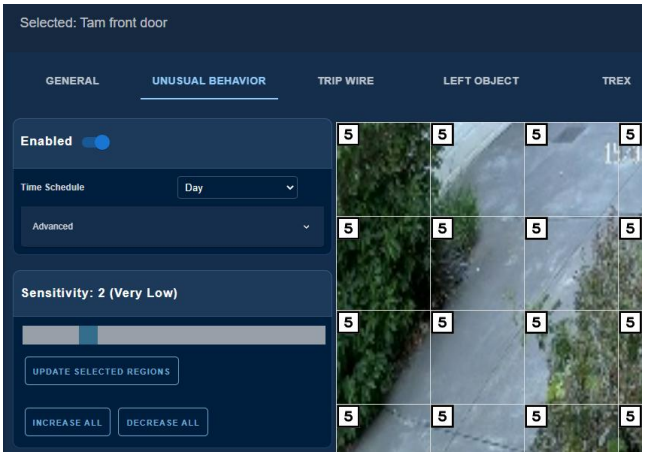
UB can be turned on/off using the **Enabled** button. By default, UB is disabled.



A camera frame is divided into an eight-by-eight region map. By default, all regions have a sensitivity level of 5. Sensitivity levels range from 0 to 10.

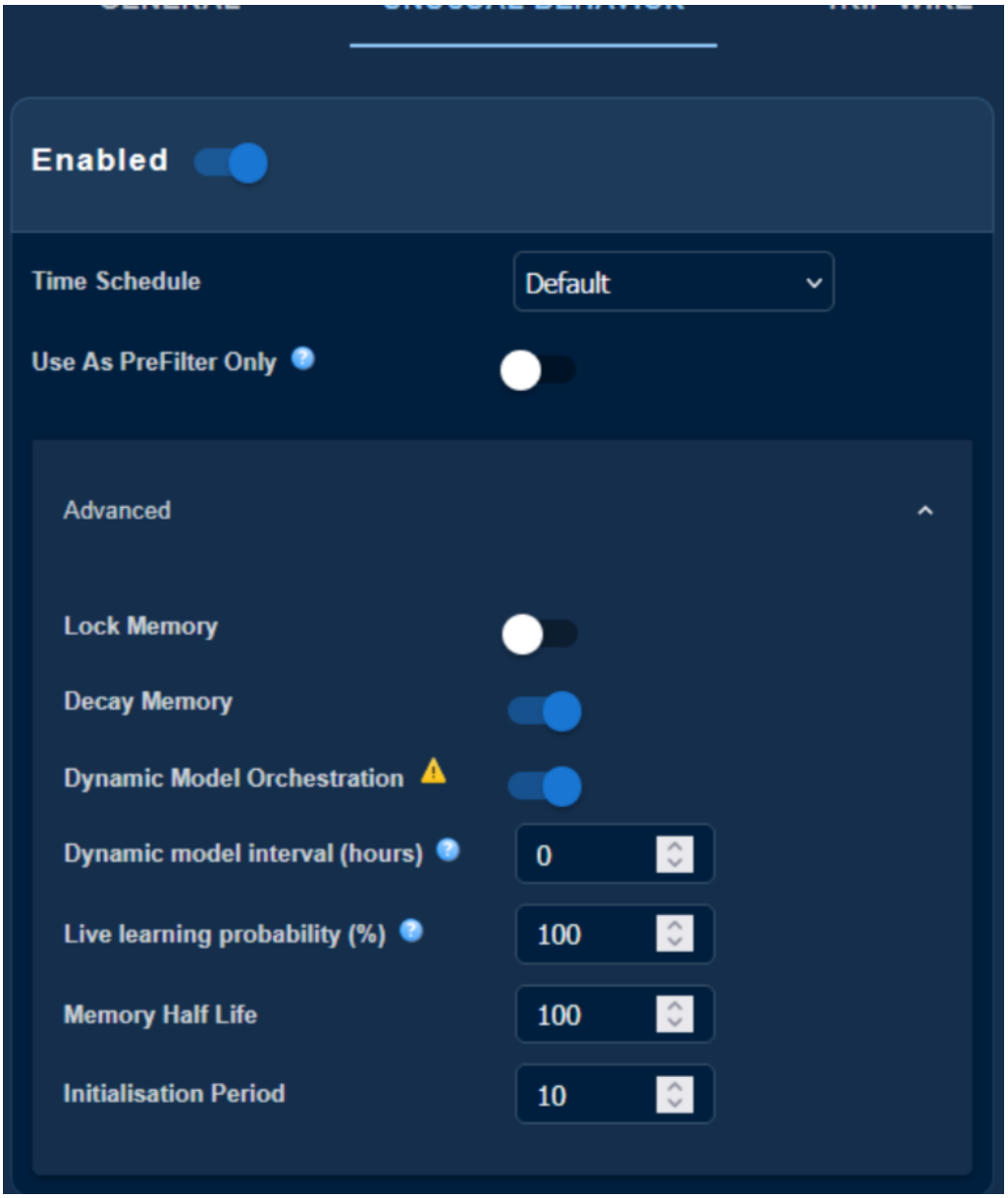
The sensitivities can be altered (only when UB is enabled) by the following steps:

- Select the region(s) by left clicking on them.
- Move the **Sensitivity slider** to the desired level. In the image below 2 means Very Low.
- Click **Update Selected Regions**. You will see the small number updated. The number in the image below is 5 and should update to 2.

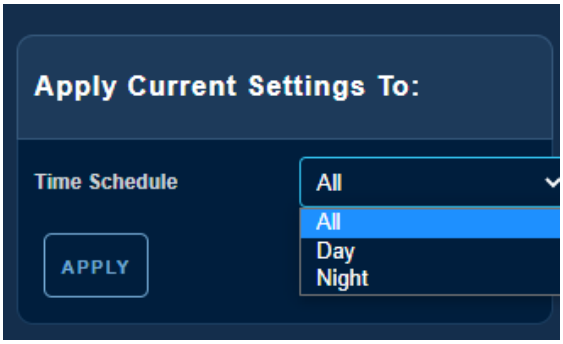


Alternatively, the whole region map's sensitivity can be altered altogether using the **Increase all/Decrease all** button in the **Sensitivity** panel.

There are advanced settings along with general sensitivity map settings, including:



Note that you can apply the current setting to a select Time Schedule only by selecting in the following menu:



Here are all the available Settings:

Settings	Default	Description
Time Schedule	All Schedule	Select a specific schedule to apply current wire settings for. One wire is only active for a single time zone or all schedules.
Use as PreFilter Only	OFF	Only use to trigger further analytic and suppress regular alerts.
Lock Memory	OFF	Set to lock the memory and prevent further learning.
Erase Memory	OFF	Set to ON to erase learning memory.
Decay Memory	ON	Ability to forget old learnt data and learn new one
Memory Half Life	100	How many hours that UB should learn 50%
Initialisation Period	10	Minimum system learnt percentage before alerts can be raised.
Dynamic Model Orchestration	False	More pro-actively learn the scene to reduce over learning. Warning: need to adjust the related settings to suit the number of time schedules
Dynamic model interval (hours)	0	How long to wait before enforcing dynamic model orchestration. Recommended between 20-100 hours depending on the business of the scene
Live learning probability (%)	100	How quickly Sentry should learn the recent events. 100% means learning as quick as possible. 0% means update only after the “Dynamic model interval” has lapsed.

4.2.4 Trip Wire

This sub-menu contains the settings for the camera’s Trip Wire Functionality.

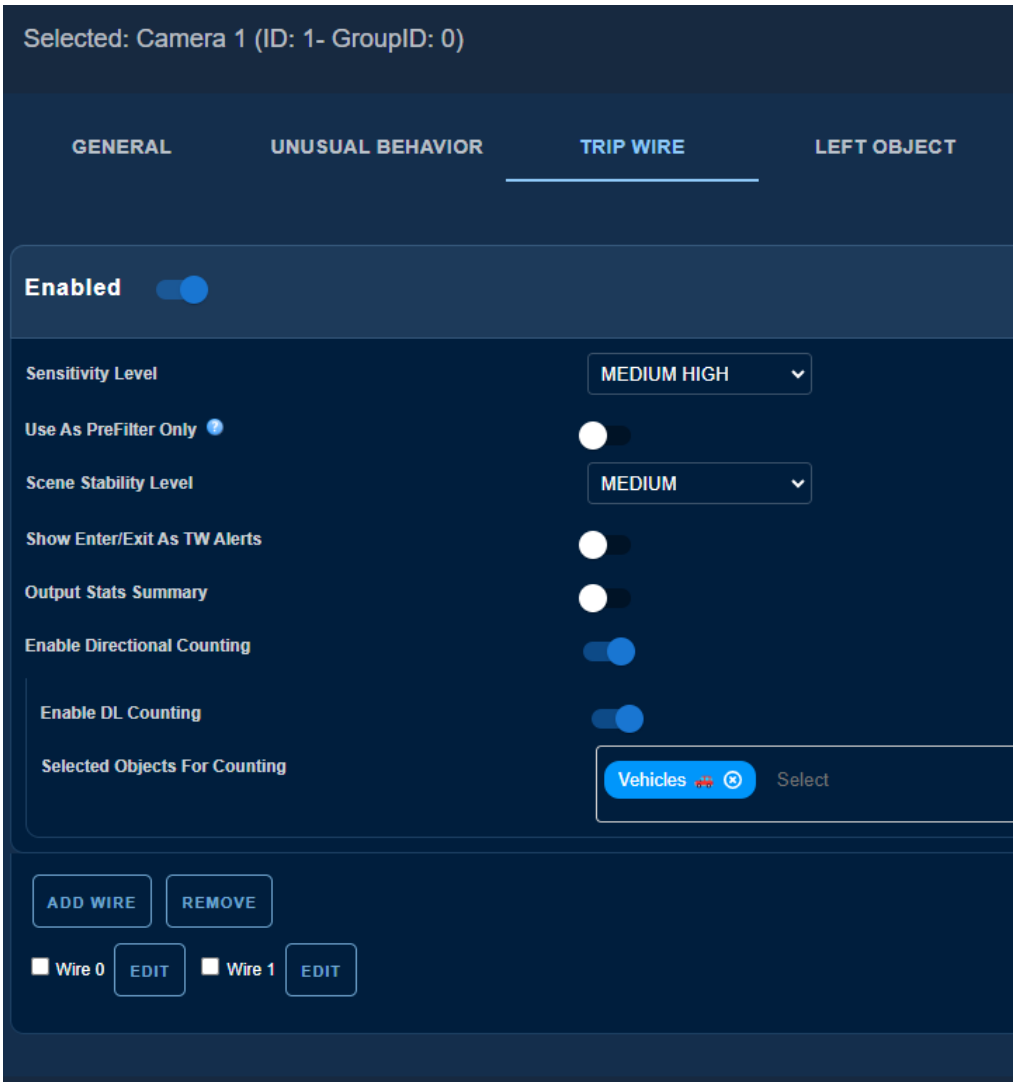
Trip Wire can be turned on/off using the **Enabled** button. By default, Tripwire is disabled.

The Trip Wire will trigger two types of alerts:

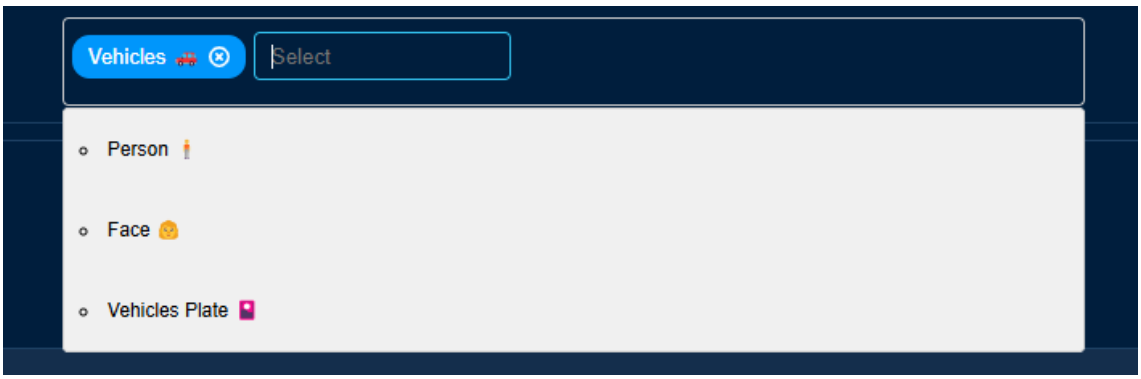
- Entering/Exiting (you can count objects in the BI tool in the WebClient)
    - Speed estimate when you enable it in General/Misc advance.

⚠ It does not work with colour ⚠

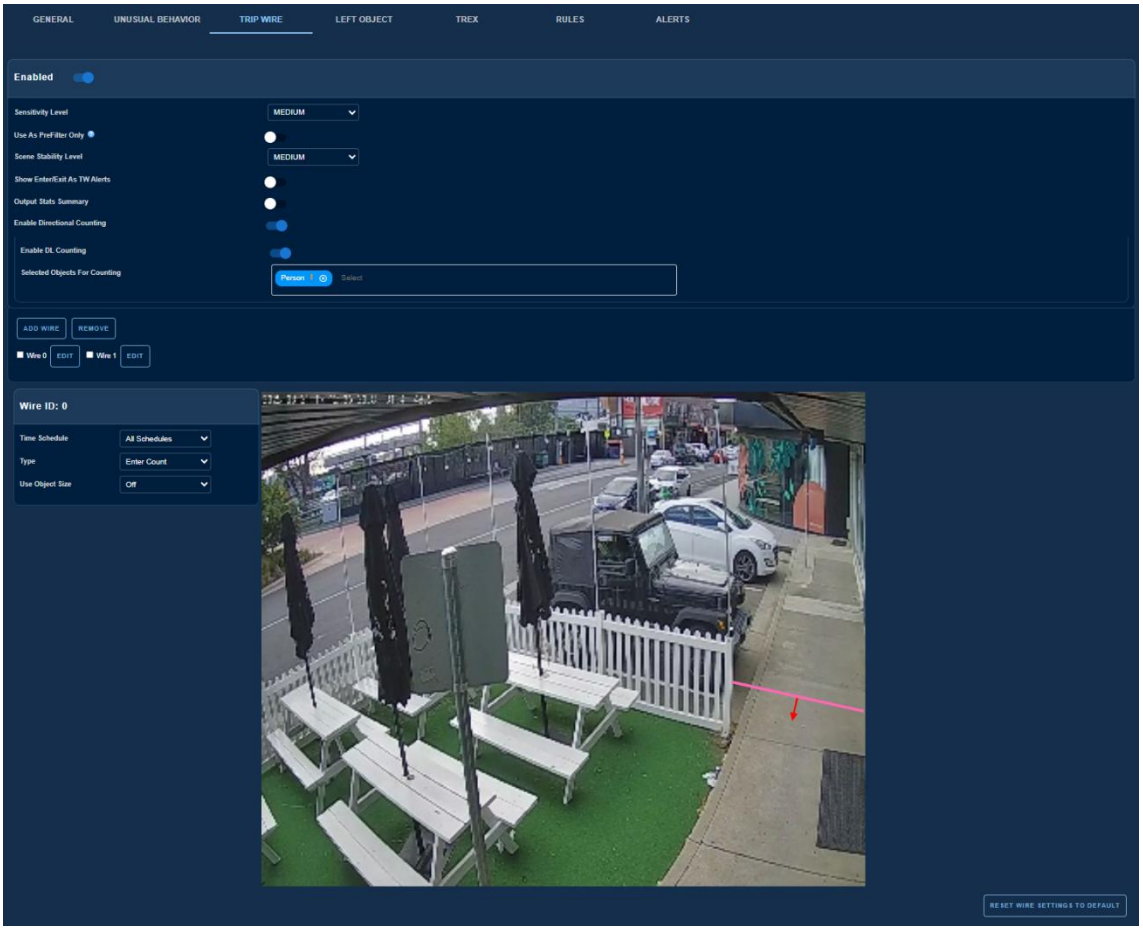
- Tripwire



- **Add/Remove Wire**: Wires can be added/removed from current camera configuration using **Add/Remove** Button (only when Tripwire is Enabled). Once a wire is created, clicking on the **Edit** button to the right of a wire's name will open a panel to configure that wire's settings.
- **Directional Counting**: Wires can be configured to count objects enter (forward) or exit (backward) direction. Activate "Enable DL Counting" option allows to only count on the selected type of objects such as people, vehicles, license plate or face.

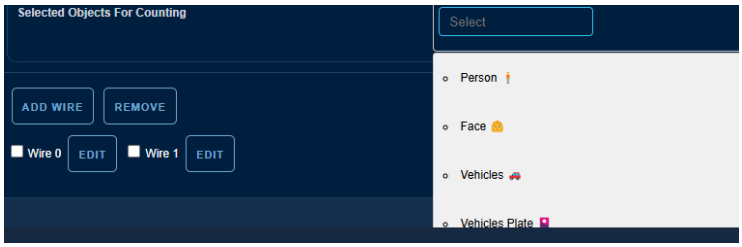


- Speed estimate Ground Resolution: when enabled in General/Misc advanced we can enter the value per wire. See section ([1]) Setting Up Enter/Exit speed alert.
- **Drawing Wire**: On the wire canvas (with or without specific camera image), left click at a start position and drag to the end position to draw a line. **Note:** Only one line segment is allowed in a wire setting, drawing a new line will overwrite the previous one. Below you can see one in pink colour with a red arrow for Enter Count:



- **Configure Wire**: each wire contains several settings including schedule on which the wire is to be triggered and the direction that will trigger the event if an object crosses the wire in the direction of the red arrow:

Settings	Default	Description
Sensitivity Level	MEDIUM	Has 5 levels
Use as PreFilter Only	OFF	Only use to trigger further analytic and suppress regular alerts.
Scene Stability Level	MEDIUM	Has 3 levels.
Show Enter/Exit as TW Alerts	OFF	You can select which type of alert you would like to trigger. Enter/Exit allows you to count objects in BI tools. Both alerts allow rules.

		⚠️ Aurora: when you are using TW DL count (enter/exit) you must enable this option to keep using Aurora. ⚠️
Output Stats Summary	OFF	It creates a file in Logs folder with a file per entering/exiting detected object when enabling DL counting. An example line in the file: 2025-01-14-09:20:55,1,1736806855,Exiting,1169,43,87,7,5,2,100,0 Date, camera id, timestamp, enter/exit, frame number, Detection coordinates, confidence. This information can be consumed by another system in the endpoint: <ServerIP>:<port>/logs?camid=<camid>&type=Counts
Enable directional counting	OFF	The alert will be triggered when an object crosses the wire in the configured direction. The wire Type will change to Enter/Exit and the alert triggered will be Entering/Exiting (not Tripwire).
Enable DL counting.	OFF	When enabled the user can select the ONLY object that will appear in the Entering/Exiting alert.
Selected Objects for Counting	OFF	If Enable DL counting is ON, we can select from Person, Face, Vehicles and Vehicle Plate: 
Time Schedule	All Schedule	Select a specific schedule to apply current wire settings for. One wire is only active for a single time zone or all schedules.
Type	Both	Select the direction of which object movement crosses the current wire. Options include **Both**, **Backward** and **Forward**. The red arrow indicates the direction on which the alert will be triggered. If Enable Directional Counting is ON, you have **Exit Count** and **Enter Count** instead (you cannot count both in this mode).
Speed Estimate ground resolution	OFF	How many pixels correspond to 1m in the scene. Please note that if the objects are moving along the optical axis of the camera the estimate should be calculated on as much as possible vertical line. If the objects are moving

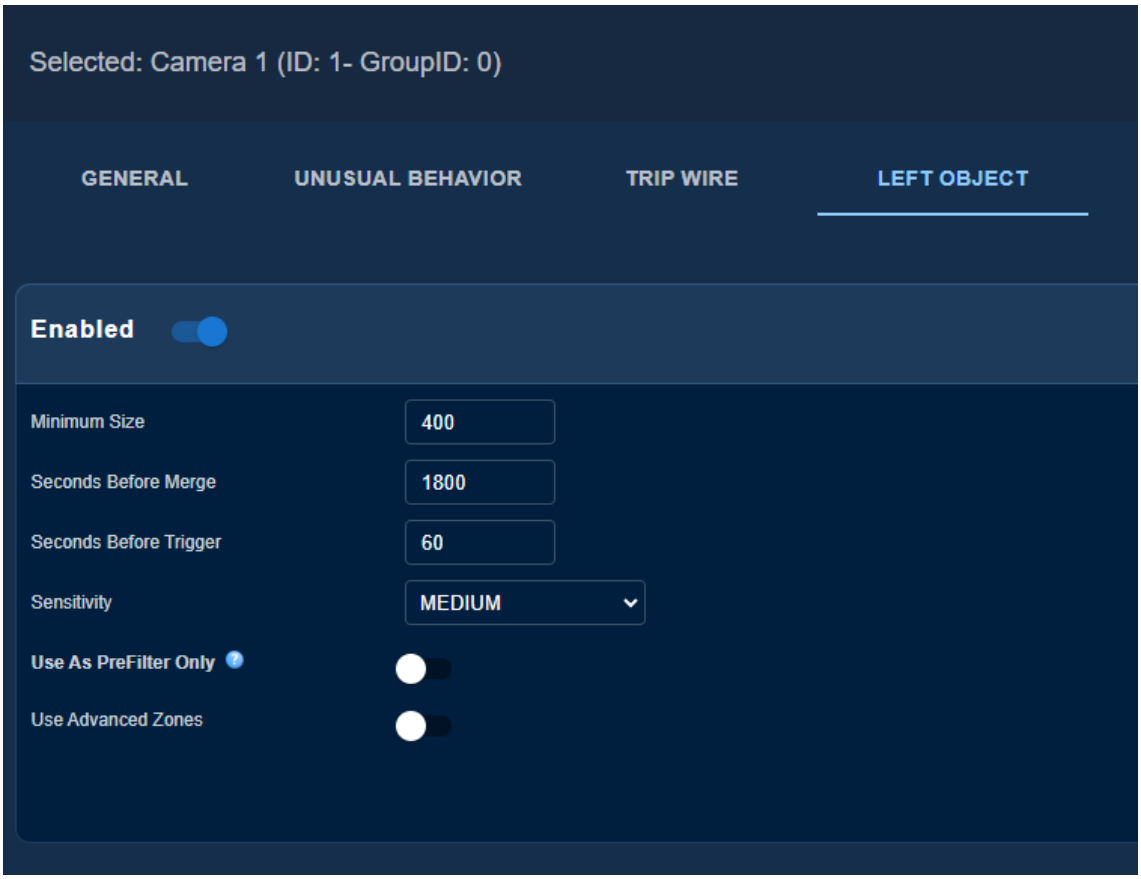
		perpendicular to the optical axis the estimate should be calculated on as much as possible horizontal line. See Trex section for entering/exiting counting ⚠ It does not work with colour detection ⚠
Use Object Size	OFF	Select size of object crossing the wire. Options include **OFF**, **Size Above** and **Size Below**.
Object Size Level	0	Size level of the object crossing the wire.
Sensitivity Level	MEDIUM	Options range from **LOW, MEDIUM LOW, MEDIUM, MEDIUM HIGH** to **HIGH**. The higher the sensitivity, the lower the confidence of tripwire being triggered.

4.2.5 Left Object

This sub-menu contains the settings for the camera's Left Object Functionality.

Left Object can be turned on/off using the **Enabled** button. By default, Left Object is disabled.

- **Left Object General Settings:** Once enabled, there are general settings the user can apply for the overall camera frame. If the user wishes to have a more specific region for Left Object, option **Use Advance Zones** can be turned **ON** to facilitate this.



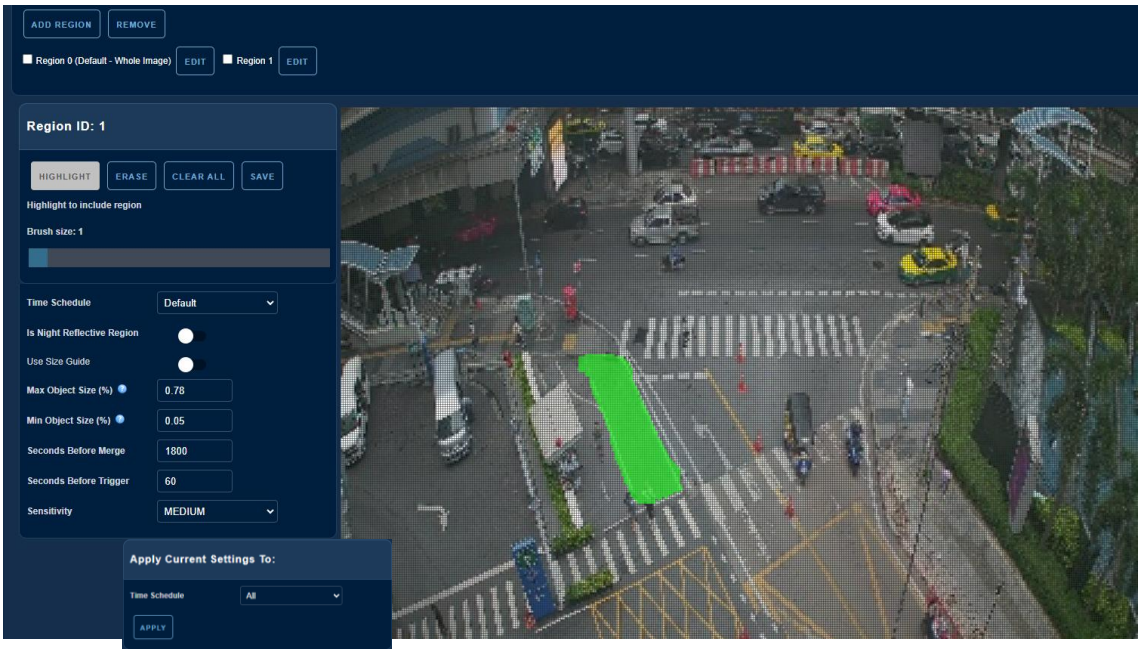
Settings	Default	Description
Minimum size	400	The minimum size for a left object to be detected, measured in total pixel count.
Seconds Before Merge	1800	The length of time in seconds before a detected object is assumed to be part of the background. Once merged, a a secondary alert may be generated when that object departs.
Seconds Before Trigger	60	The length of time in seconds an object must be stationary in the scene before an alert is generated.
Sensitivity	MEDIUM	Options range from LOW, MEDIUM LOW, MEDIUM, MEDIUM HIGH to HIGH. Also DISABLE is possible. The higher the sensitivity, the lower the confidence of Left Object being triggered.
Use Advanced Zones	ON	Determines whether separate data is supplied for different sections of the image. This should be enabled (ON) if left object detection should be disabled for parts of the image, or if different settings are needed for

		different areas (e.g. allow smaller targets in background, larger targets in foreground).

- **Add/Remove Region**: Advance regions can be added/removed from current camera configuration using **Add/Remove** Button (only when **Use Advance Zones** is ON). Once a region is created, clicking on the **Edit** button to the right of a region name will open a panel to configure that region settings.

Note: There is a default region for each camera, which covers the whole camera image. This region cannot be removed.

- **Drawing Region area**: On the region canvas (with or without specific camera image), select the **Highlight** button, then left click on the canvas to highlight the area to be included in the region. Brush size, ranging from 1-25, can be altered to allow fine tune/quick cover purposes.



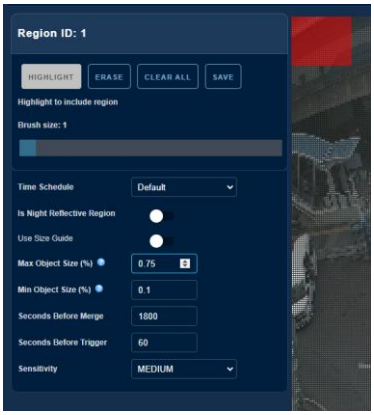
IMPORTANT: Progress on highlighting/clearing regions of interest must be saved using the Save button 

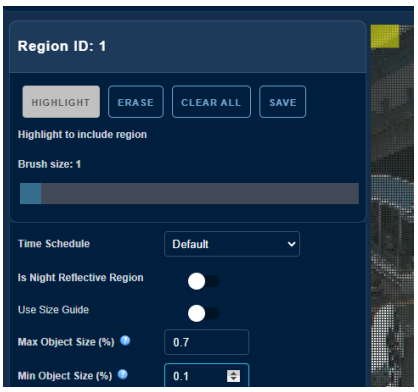
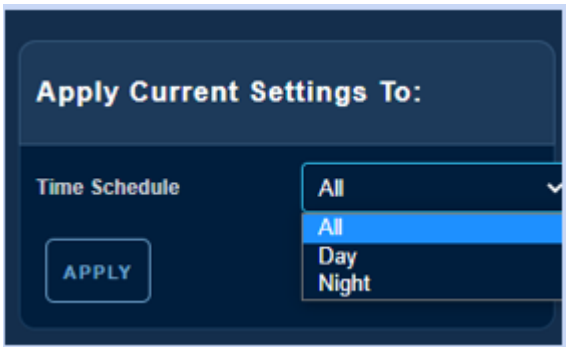
.

The camera image view is exclusive to a single region only. By default, Region 0 (default region) covers the entire image initially. Every time a region (new or old) is edited (highlighted), the latest highlighted area from that region would be uncovered from all other regions. The below image illustrates an example of a camera with three separate Left Object Regions, in which areas highlighted in Region 1 and Region 2 are no longer highlighted in Region 0.

Region 0 Region 1 Region 2

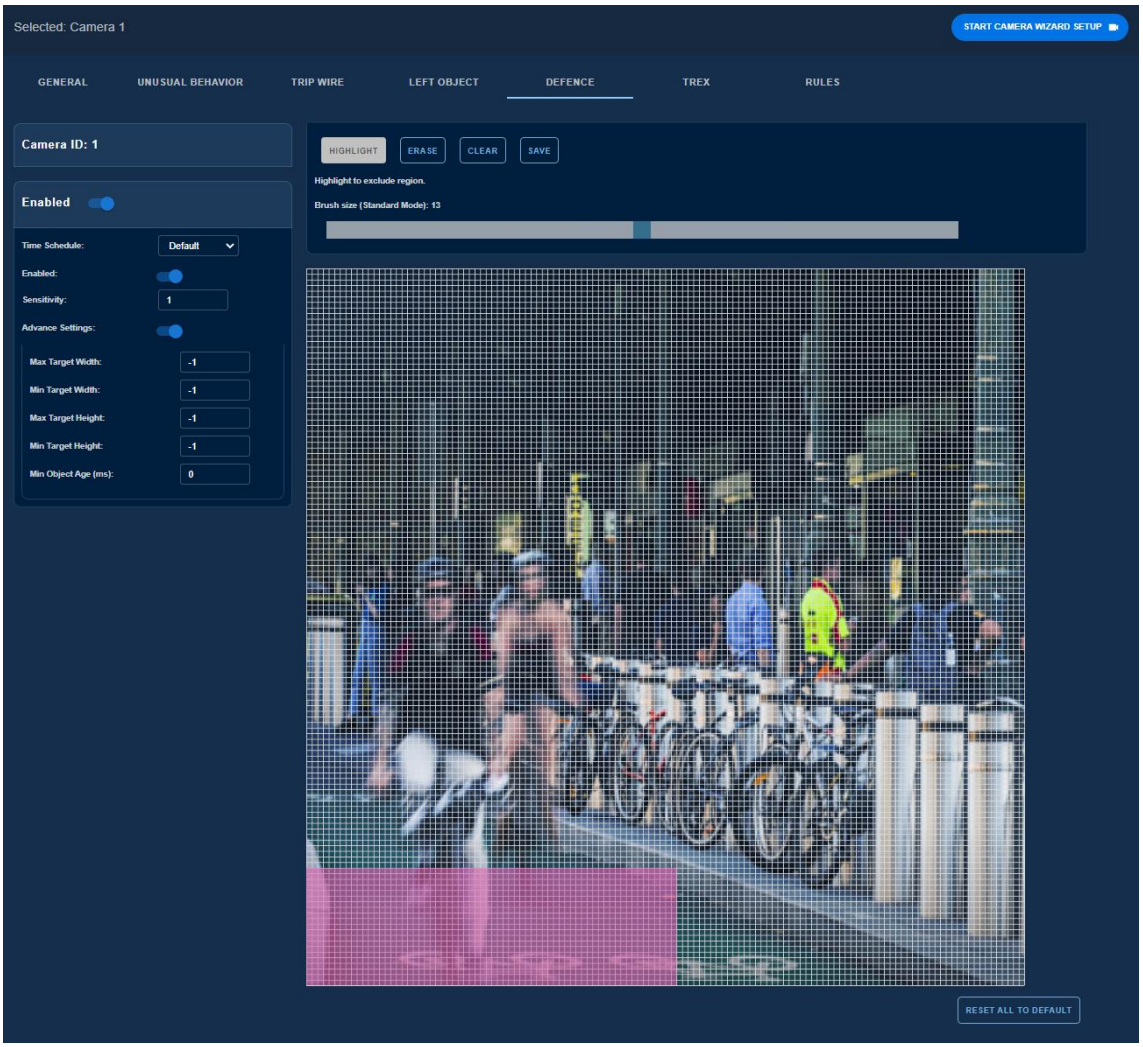
- **Erase Region area:** Select **Erase** button, then left click on the canvas to erase unwanted area. The same brush size is applied to this action. This action also requires the **SAVE** button to be clicked to record users' editing progress.
- **Clear region area:** Click on the **Clear All** button to erase all highlighted areas.
- **Configure Region**: Each region contains several settings including schedule on which the region to be triggered and its associated settings. These settings are quite similar to the **General Left Object** settings, but only available when the general **"Used Advanced Zones"** is set to **ON**.

Settings	Default	Description
Schedule	Default	Select the time zone that the region is active for.
Is Night Reflective Region	OFF	On wet nights, streetlights may be reflected in puddles and cause nuisance alerts when the puddle is disturbed. When this value is set to ON, alerts in these regions are suppressed at night.
Max Object Size	200	The maximum size for a left object to be detected, measured in total pixel count. Use the visual guide for fine adjustment: 
Min Object Size	0	The minimum size for a left object to be detected, measured in total pixel count. Use the visual guide for fine adjustment:

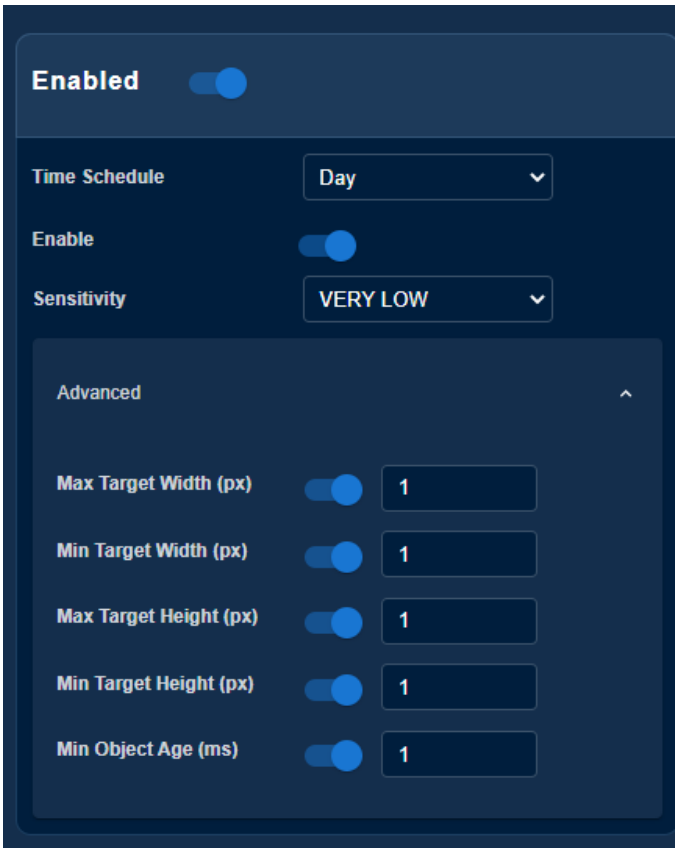
		
Seconds Before Merge	1800	The length of time in seconds before a detected object is assumed to be part of the background. Once merged, a a secondary alert may be generated when that object departs.
Seconds Before Trigger	60	The length of time in seconds an object must be stationary in the scene before an alert is generated.
Sensitivity	Medium	Select the desired sensitivity, it can also be DISABLE. This is useful when you do not want the Region 0 (whole image) to be enabled.
Time Schedule	All	You can apply the current setting to a select Time Schedule only by selecting in the following menu: 

4.2.6 Defence

This sub-menu contains the settings for the camera's Defence functionality. Defence (globally) can be turned on/off using the **Enabled** button. By default, defence is disabled.



- **Enable defence for each schedule:** Once enabled, each schedule in the server can have their own defence settings. Defence must be activated in each schedule before further settings can be configured for that schedule.



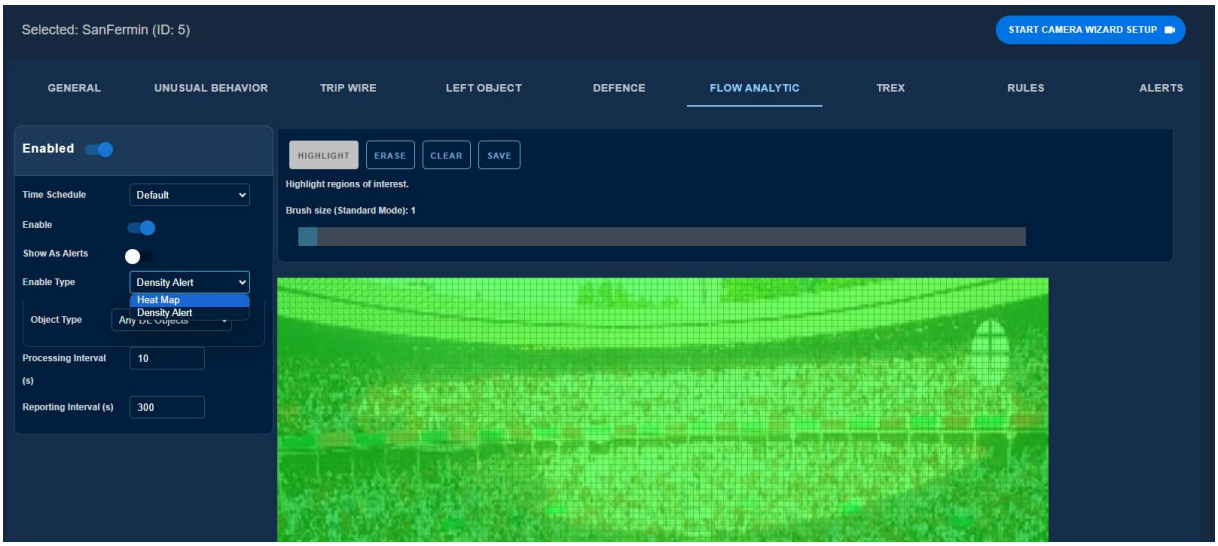
- **Drawing defence area for each schedule**: On the defence canvas (with or without specific camera image), select the **Highlight** button, then left click on the canvas to highlight the area to be included in the region. Brush size, ranging from 1-25, can be altered to allow fine tune/quick cover purposes. The user can only highlight/erase schedule's area once the schedule is enabled.
- **Erase defence area:** Select **Erase** button, then left click on the canvas to erase the unwanted area. The same brush size is applied to this action.

IMPORTANT: Newly highlighted/erased areas are only saved once the **Save** button is clicked.

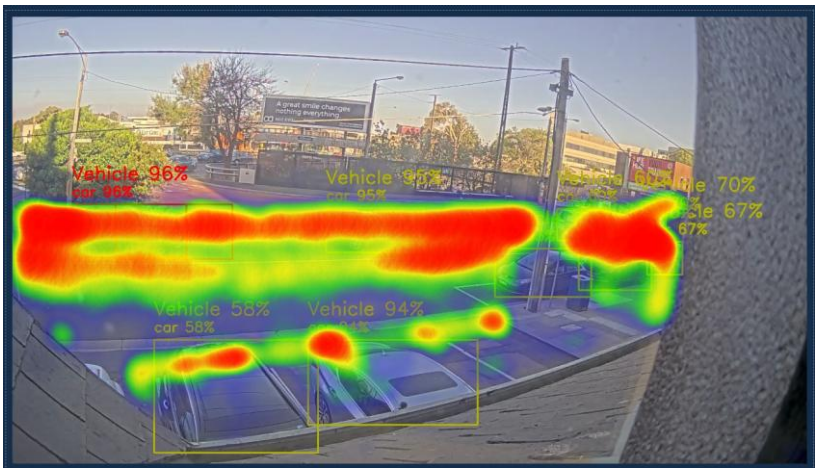
- **Clear region area:** Click on **Clear** button to erase all highlighted areas.

4.2.7 Flow Analytic

This sub-menu contains analytics related to the density of objects in the scene. Two types are available, Heat Map and Density Alert.



Heat Map: it collects information to deliver a visual drawing of past events so is not suitable for real time alert. The user needs to enter a certain period for sampling (i.e. every 5 minutes). The results are shown in the Web Client per alert like the image below (high density areas in red):



Density: Collect an event every x second or millisecond to apply DL and rules to it. This alert that can be shown as Alert in the live tab or in the past alerts tab.

Processing interval: is the sampling rate for the system to run the analytic.

Reporting interval: is the time elapsed between sending Flow Analytic events, only used for Heat Map.

User can add different Detection/Classification models by enabling them.

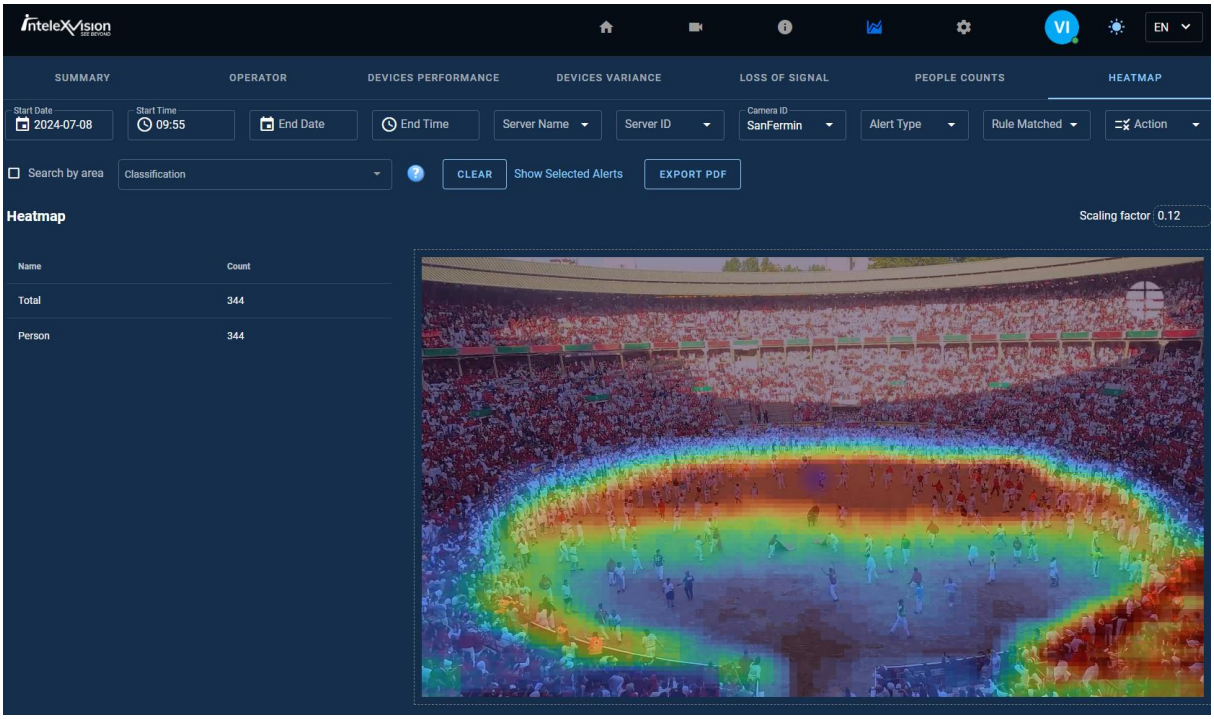
⚠️Keep in mind that if you select People as Object Type, the model used will be General Objects which is not the desired model for crowd detection. Thus, for crowded scenes, select Object Type as “Any DL Objects” and Crowd model in the Detection/Classification menu, this way you will a more accurate prediction for that kind of scenes.

4.2.7.1 Heat map

Offers the user the capability to see areas where a dense concentration of objects is happening.

No rules can be applied because heatmap is to show the summary after the event took place, is not reacting to something in real-time, it will only send the alert every “reporting time”.

You will get an image like below in the BI tools from the **Sentry WebClient**, particularly in Heatmap menu:



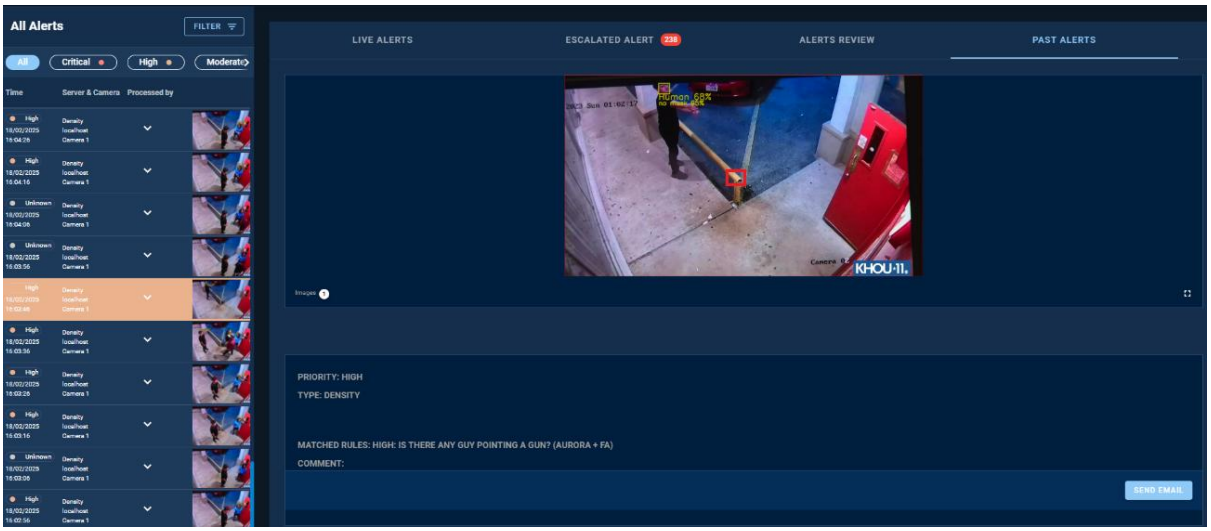
Heatmap analytic will be triggered every Reporting interval (s). For example, with the default value of 300s, the Alert is sent every 5 minutes.

4.2.7.2 Density Alert

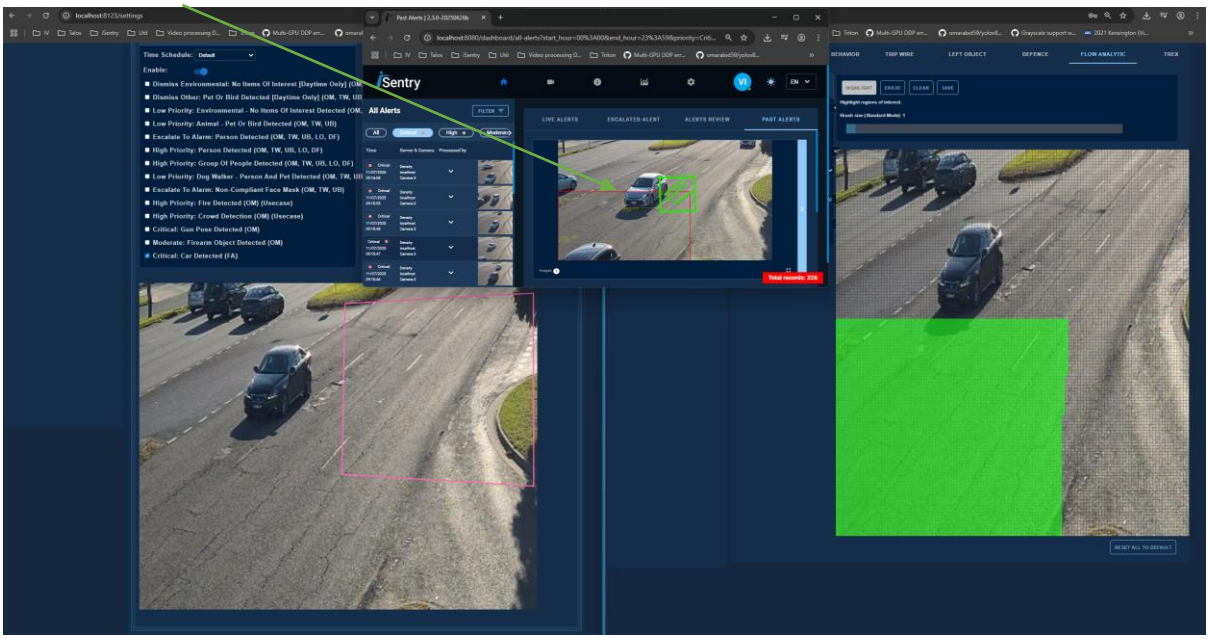
The sending interval will be every processing Interval (seconds or milliseconds) time, this will give the user the opportunity to **setup rules** according to that and make things such as “more than x people in this area” then Rule Action.

⚠️ The triggering point for Density Alert as it is a time-driven event is in the centre of the scene so **all objects will be covered for rule purposes**. The only way to control the area of the rule is by using specific regions and not whole image.

Below is an example of triggered rule for Density Alert for human and the object is outside the triggering point (the centre, as we cannot determine in this type of analytic) and you do not have set a region in the rule. See yellow box in the human below:



Next is another example where there is a region in the rule, note that there is a region or overlap between the ROI (green) and the Rule region marked in green square with lines inside below:

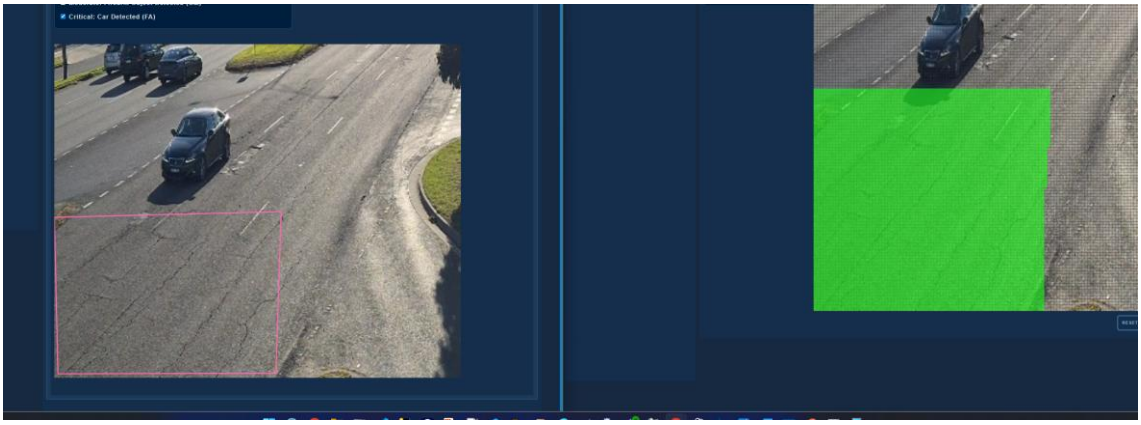


There are particularly interesting insights from the picture above. In the middle of the image there is the output from our **Sentry WebClient** showing a triggered rule for vehicle detected (marked as Critical), however as the alert indicator is in the centre of the scene the bounding box for the car is yellow (outside of the Alert Indicator).

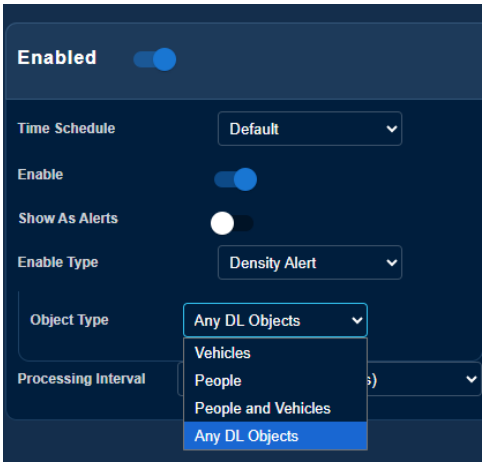
Another thing to note is that the rule is triggered cause there is a small overlap between the ROI (in green) and the Region of rule (in pink). We have painted in the WC a green square with lines to highlight the area of overlap that triggered the rule.

On the contrary if we enter the region for the rule in the bottom-right corner then no rule will be triggered:

⚠️ As a general rule is recommended to match the ROI with the region of the rule:



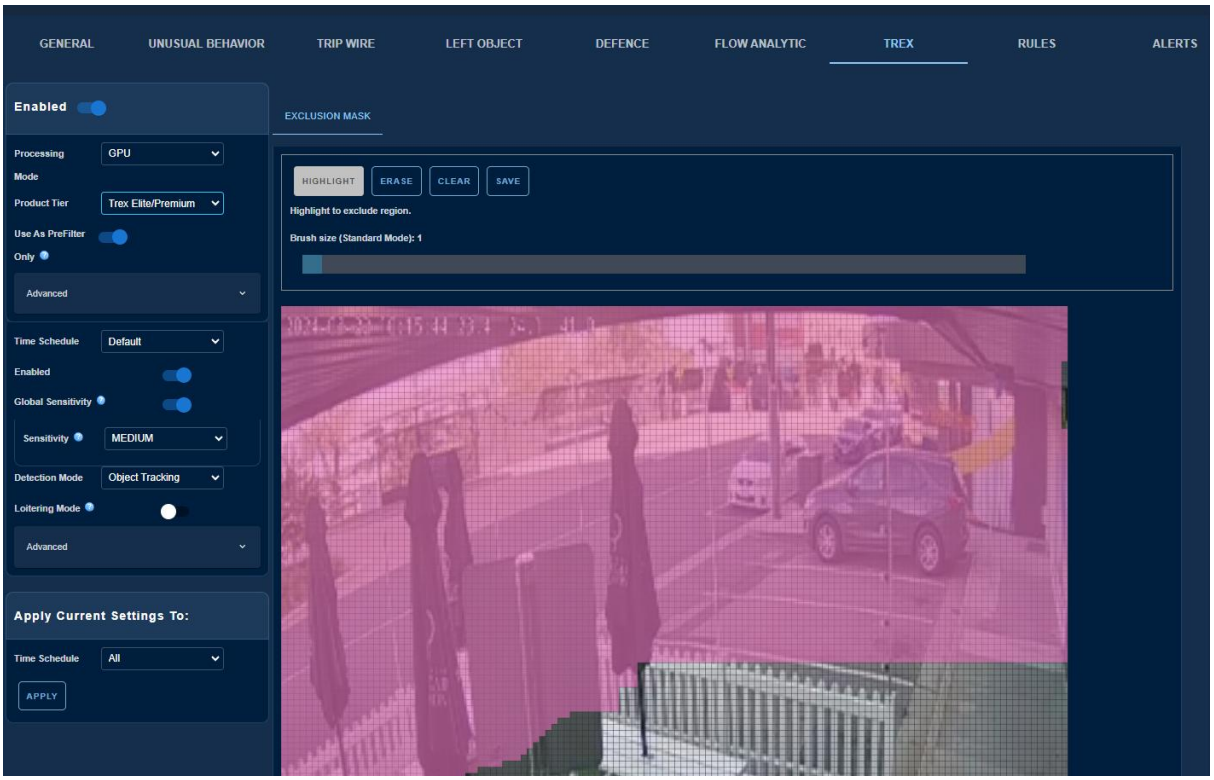
You can select the object types in the images/alerts, which are:



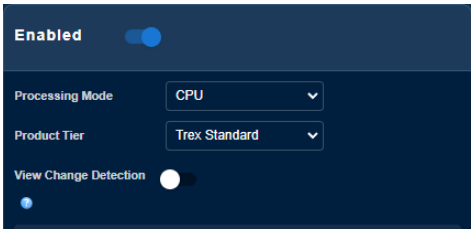
4.2.8 TRex

This sub-menu contains the settings for the camera's TRex Functionality.

TRex (globally) can be turned on/off using the **Enabled** button. By default, TRex is disabled.



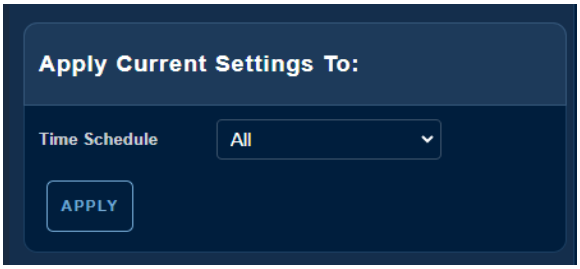
4.2.8.1 TRex global settings per camera:



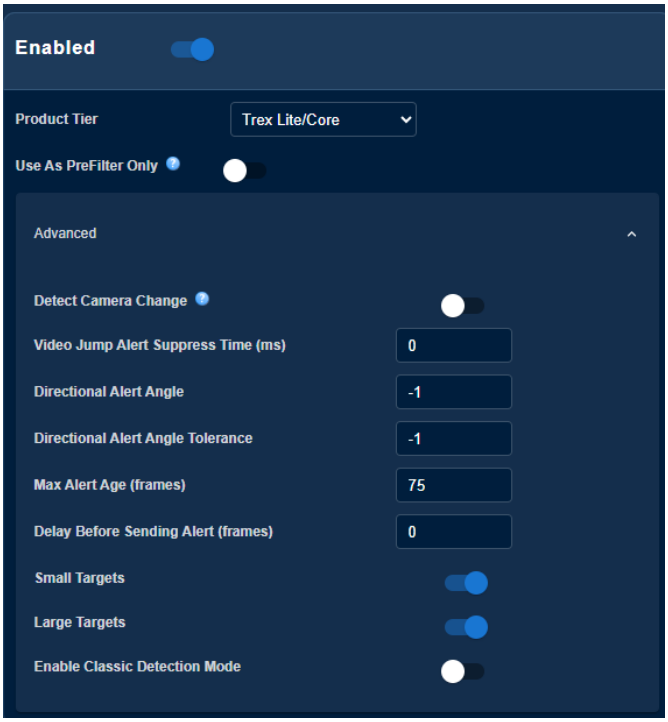
Settings	Default	Description
Enabled	OFF	Enabled/Disable Trex analytic
Processing Mode	GPU	Select CPU/GPU/GPU Emulation mode
Product Tier	Lite/Core	There are 3 product tiers: - Premium/Elite - Standard - Lite/Core
View Change Detection	OFF	Enable/Disable Camera view change detection. If this option is ON, then **Trex Elite licence** is applied.

4.2.8.2 TRex time schedule settings:

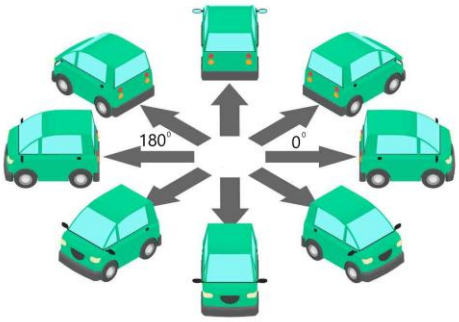
Enable TRex for each schedule: Once enabled, each schedule in the server can have its own TRex Settings. TRex must be activated in each schedule before further settings can be configured for that schedule.



4.2.8.3 Advanced settings



- **Use as PreFilter Only**: OFF by default. Only use to trigger further analytic and suppress regular alerts.
- **Detect Camera Change**: Enable/Disable Camera View Change Detection. TRex Elite License required.
- **Video Jump Alert Suppress Time:** 0 by default. Add this option to suppress alerts that have a large video frame gap. Unless video jumps cause lots of nuisance alerts, it is recommended to keep this option OFF.
- **Minimum total object move threshold (%):** 0% by default.
- **Directional Alert Angle:** Add option to only trigger enter/exit directional alert at particular direction (i.e. motion angle). By default, all angles are accepted (0-360).



- **Directional Alert Angle Tolerance:** represents how much deviation from the selected angle should be allowed to alert.
- **Max Alert Age (frames):** 75 default. Defines the maximum number of frames that will compose the alert. When long alert occurs, like using TREX for a person walking the street, must be a limit to split actual alert and start the next one.
- **Delay Before Sending Alert (frames).** How many frames do we wait until we send the alert? This is to have enough frames for DL classification and rules engine. However, this carry a risk of the camera might be disconnected just now of alert which cause the alert never got sent.
- **Small Target:** This option is enabled at default and should never be disabled UNLESS only big objects are targeted. If users want to filter a specific size, please use the **Min/Max Target Height/Width** options (in percentage of Frame Width/Height). More detailed target age/size filters can be applied by using the advanced settings.
- **Large Target:** This option is enabled at default and suggested not changing unless the user wants to ignore the big objects.
- **Enable Classic Detection Mode**: This option is OFF by default. When turned on, Trex will revert to standard motion/object detection mode (internal to Trex) which has reduced capability to distinguish noise from genuine targets. This option is useful to suppress occasional video compression artefacts (such as those caused by connection issues). However, in less likely cases, Trex under this mode may also miss genuine targets, i.e. false negative.
- **Global Sensitivity:** Apply sensitivity for the entire frame rather than per region. Default value is ON.
    - **Sensitivity:** If sensitivity by region is off, this value is applied for all regions. Default value is MEDIUM.
- **Detection Mode:** There are four detection modes: Object tracking, Directional, Counting and Overcrowding.
    - Edit modes are available including Exclusion Mask, Sensitivity Region, Region of Interest, Min Target age and Min/Max Target Size.
- **Loitering Mode Enabled:** TRex will track the target longer when set to ON (target needs to be large enough).

4.2.8.3.1 TRex Tab options

Exclusion Mask and **Region of Interest** modes utilise the same concept of highlighting tool by left clicking on canvas area, like Left Object drawing. **Erase/Clear/Save** buttons are also performed in the same manner.

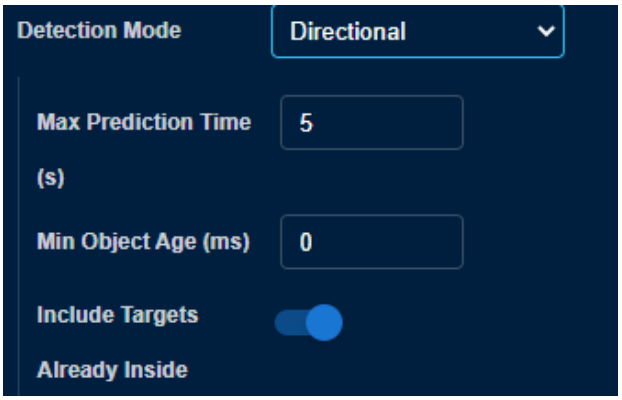
Sensitivity Region, Min Target age and **Min/Max Target Size (in percentage)** modes utilise the same concept of dividing the camera frame into an eight-by-eight region map, like UB region map. Each region sensitivity can be adjusted separately using the **Sensitivity slide**.

Region of Interest is not present in Object tracking.

4.2.8.3.2 Detection mode settings:

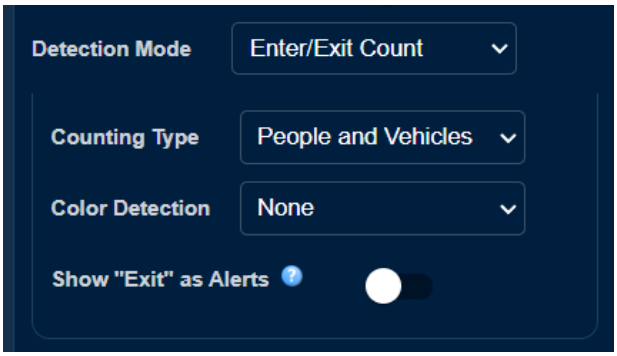
Object Tracking:

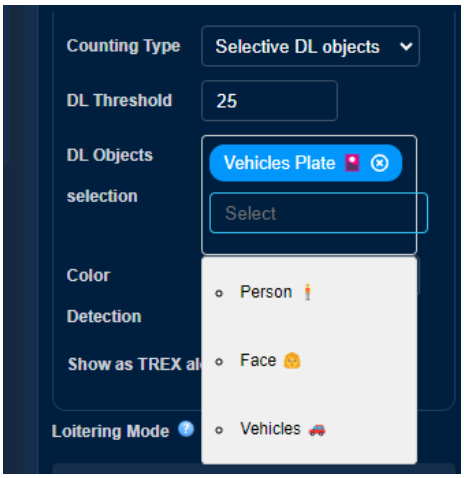
Directional:



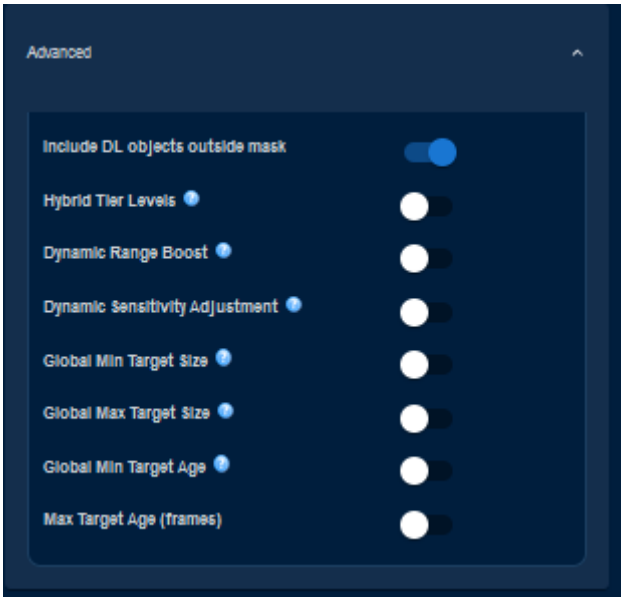
Settings	Default	Description
Max Directional Prediction Time (ms)	5	To alert the operator sooner, this value sets how far ahead of time we predict the position of the suspicious target. The further ahead (smaller value) the less accurate.
Min Object Age (ms)	0	The minimum amount of time (ms) an object must be visible before raising an alert.

Enter/Exit Count:



Settings	Default	Description
Counting type	Moving Objects	Moving objects, Any DL Objects, Selective DL objects such as: 
Colour detection	Colour	Colour (now is always using colour since 3.2.x)
Show “Exit” as Alerts	OFF	Show/No show the “Exiting” alert on live view of **Sentry WebClient**. Example case when turning this option ON: - Detecting vehicles moving in the wrong direction.

4.2.8.3.3 Advance Settings:



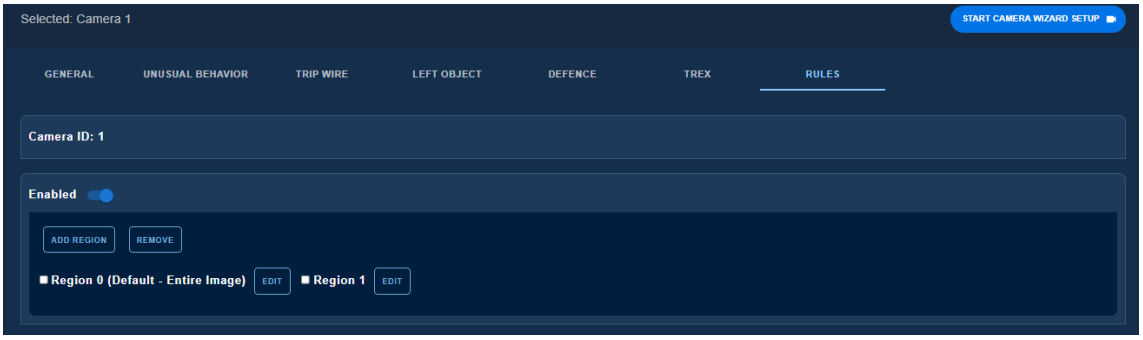
Settings	Default	Description
Include DL objects outside mask	ON	This option is OFF by default to include all DL objects in the frame into the DL rules consideration. However, when turned ON, only classified objects inside the active processing area will be considered when applying rules. Increase video output quality (i.e. higher output bit rate hence bigger video file size)
Hybrid Tier Levels	OFF	Improves nearby target detection and tracking (recommended for thermal cameras in hot environments)
Dynamic Range Boost	None	Improves contrast in low contrast scenes (recommended for thermal cameras in hot environments)
Dynamic Sensitivity Adjustment	OFF	Automatically adjust sensitivity when TREX detects sudden increase in activities, which could be caused by environmental factors such as wind high traffic in peak hours etc.
Global Min Target Size	ON	The global minimum target size is applied to the entire frame. If not set, the minimum target size must be applied per region.
Global Max Target Size	ON	The global maximum target size is applied to the entire frame. If not set, the maximum target size must be applied per region.

Global Min Target Age (frames)	ON	The global minimum target age is applied to the entire frame. If not set, the minimum target age must be applied per region. In a recording, objects move at different speeds: cars, people and birds. So, to target desired objects and discard the undesired ones a right value must be picked here. A person walking the scene can take 2 minutes, however, a car takes 10 seconds and a bird 2. Pick the number considering that 200 frames are 20 seconds with a camera frame rate of 10fps.
Max Target Age (frames)	OFF	The maximum amount of frames an object must be visible before raising an alert. Apply same as above.

4.2.9 Rules

This sub-menu contains the settings for the camera's Classification Rules Functionality.

Rules (globally) can be turned on/off for the target camera using the **Enabled** button. By default, Rules is disabled. Note that even when the **Rules** option is enabled for this camera, users still need to enable other settings such as DL Processing Enable, DL Rule Engine Enable in Server Settings for classification rules to be applied.

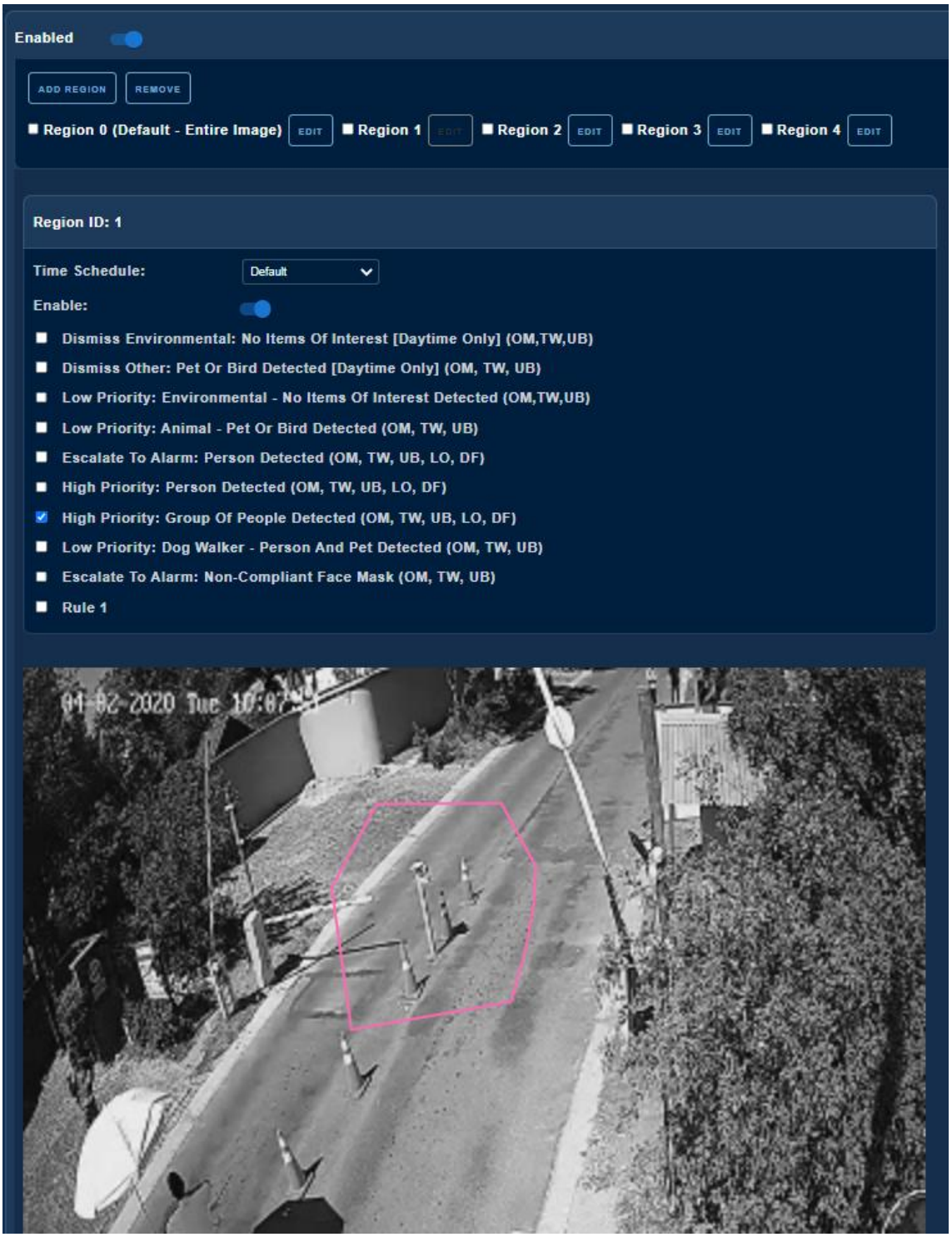


- **Add/Remove Region for Rules**: Rule region can be added/removed from current camera configuration using **Add/Remove** Button (only when **Rule** is enabled). Once a region is created, clicking on the **Edit** button to the right of a region name will open a panel to configure that region settings.

Note: There is a default region for each camera, which covers the whole camera image. This region cannot be removed.

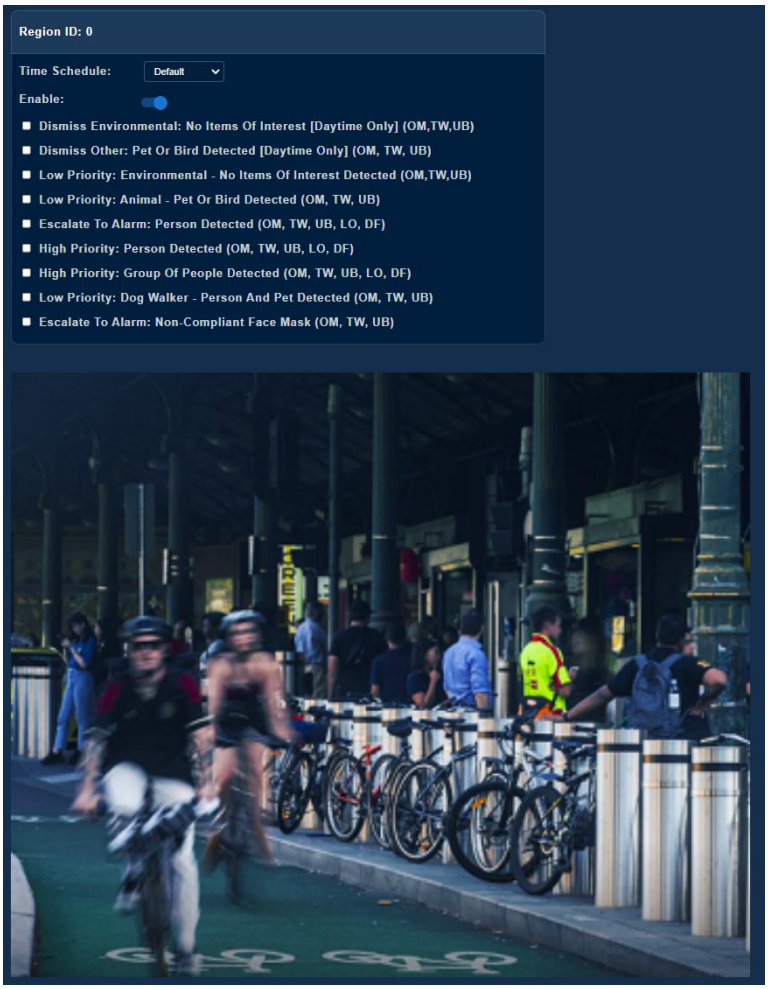
- **Drawing Region area**: On the region canvas (with or without specific camera image), left click at multiple locations to create an area, then close the area by right clicking in the end to form a polygon.

Note: Only one polygon is allowed in a rule region, drawing a new polygon will overwrite the previous one.



- **Configure Region**: each region contains several settings including schedule on which the region to be triggered and its associated classification rules to be applied. Start by selecting the schedule, turn **Enabled** to ON, then tick the appropriate rules.

  Note: The classification rules can be created in the Rules Menu Section.



4.3 Rules Menu

The **Rules** menu contains multiple sub-menus: **Alert Actions**, **Rule Groups** and **Rules**. To create/configure a Classification Rule, users need to create/configure all the rules' elements. In general, each Rule is structured as follows:

- **Classification Rule:** the name, composed by a priority, name and events. Example: "Low Priority: animal - pet or bird detected (OM, TW, UB)".
- **Event Types**: the mode(s) of operation in which the rule is applied. Options consist of: Density, Defence, Entering/Exiting (counting), Left Object, TRex, Tripwire, UB, Speed, Action. Users are allowed to choose multiple event types for each Rule.
- **Rule Groups**: Each rule can contain an unlimited number of Rule Groups. An operator of **"Any of/All off"** must be selected to control how the individual result of each Rule Group contributes to the final outcome of a Rule.
    - ➢ **Any of**: A rule will be triggered if at least one of its Rule Groups is triggered.
    - ➢ **All of**: A rule will be triggered if all of its Rule Groups are triggered.
    - ➢ Each **Rule Group** contains a collection of object classifications with different settings for probability threshold and inclusion. Each Rule Group also contains

an operator of **"Any of/All off"**, functioning in the similar manner mentioned above.

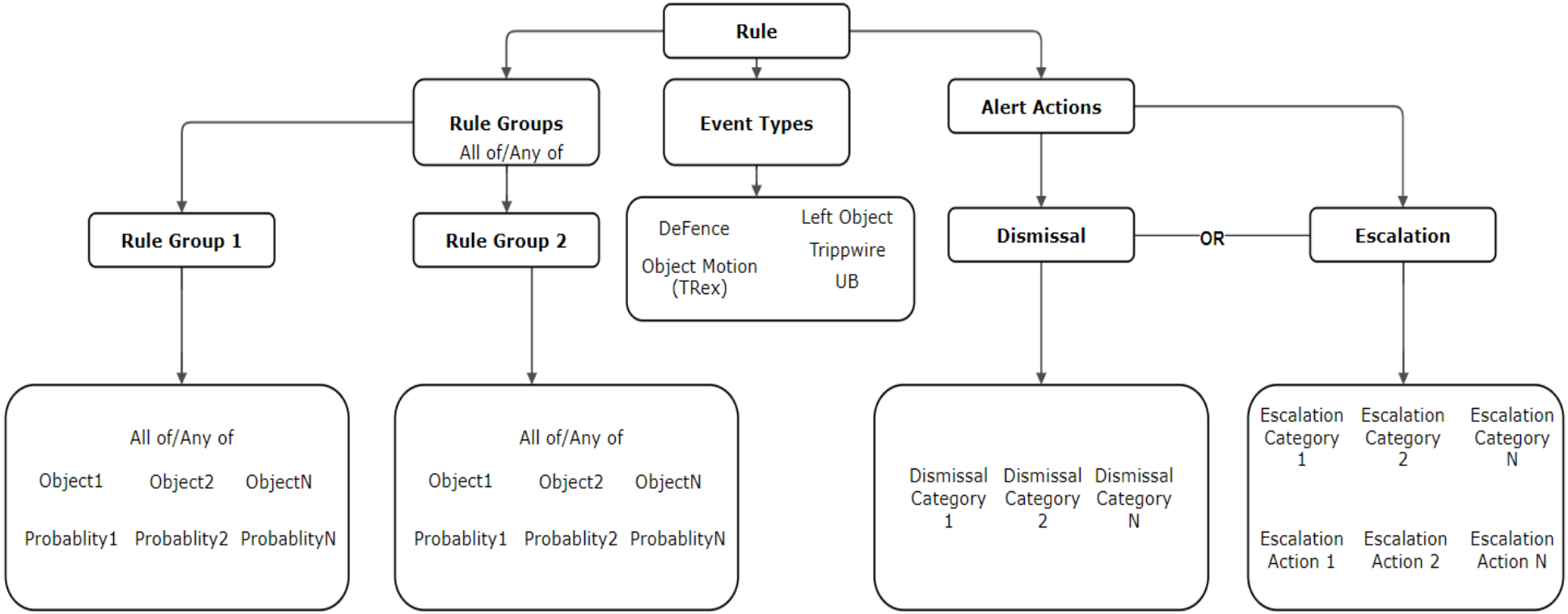
- **Alert Actions**: Users are allowed to choose a dedicated action for each rule in the case that the rule is triggered. This action is either a **Dismissal** or an **Escalation.**

  ➢ Each **Dismissal** is paired with a **Dismissal Category**, outlining the reason why users choose to dismiss an alert: *tree, birds, no item of interests, etc*.

  ➢ Each **Escalation** is paired with an **Escalation Category** and an **Escalation Action**. **Escalation Category** outlines the reason why the type of triggered escalation, e.g. *Armed Robbery* or *Car Crash*. **Escalation Action** is the recommended type of action suggested to the operator who is viewing the alert triggered by the current rule, e.g. *Alert Police* or *Alert Safety Officer*.

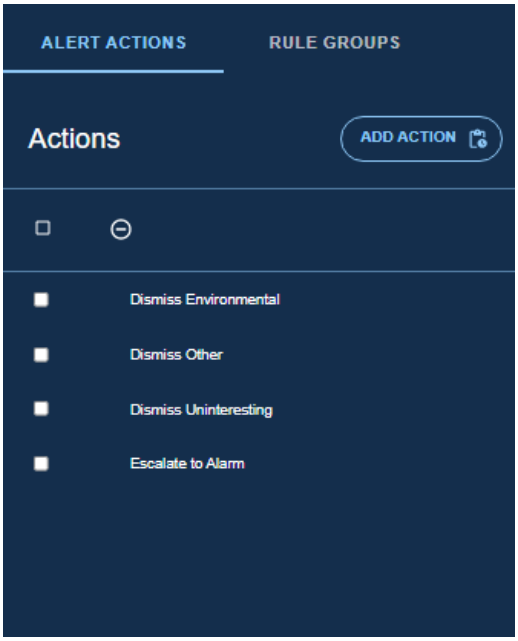
- **Priority:** Users are allowed to enter the priority of the rule. Max 100.
- **Rule Sensitivity:** This setting will automatically change to the recommended option when the Actions submenu is modified: High Sensitivity for Escalation/High Accuracy for Dismissal.

Note: There is a default set of Rules included when the system is freshly created/reset. We strongly recommend keeping this Rules set as is for standard users.


Rule
Rule Groups
All of/Any of
Event Types
Alert Actions
Rule Group 1
Rule Group 2
DeFence
Object Motion (TRex)
Left Object
Trippwire
UB
Dismissal
OR
Escalation
All of/Any of
Object1
Object2
ObjectN
Probablity1
Probablity2
ProbablityN
All of/Any of
Object1
Object2
ObjectN
Probablity1
Probablity2
ProbablityN
Dismissal Category 1
Dismissal Category 2
Dismissal Category N
Escalation Category 1
Escalation Category 2
Escalation Category N
Escalation Action 1
Escalation Action 2
Escalation Action N

4.3.1 Alert Actions

This sub-menu contains the settings of **Alert Action**, one of the components of the classification rules. Alert Actions contains actions for users to perform once a particular rule is triggered.



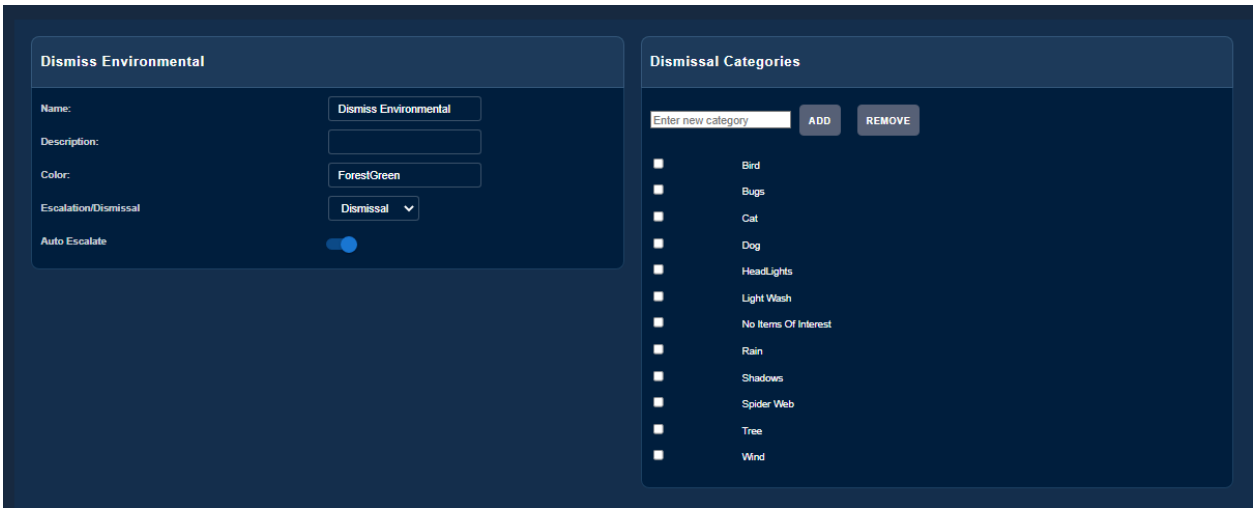
Users can add/remove Alert Category using the **Add//Remove (⊖)** buttons. Clicking on the **Edit** button to the right of the category will allow the user to configure the categories in detail.

Users can configure an alert action in one out of two types: a **Dismissal** or an **Escalation**.

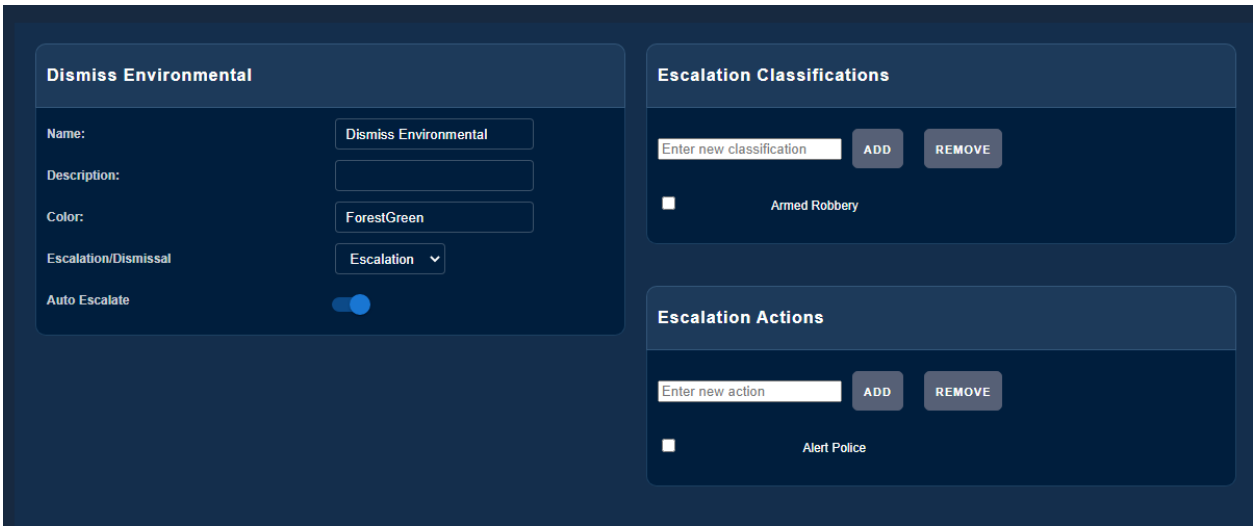
Once set to a certain type, there will be subcategories users can enter for that particular type.

"**Dismissal**" type requires "**Dismissal Categories**" while "**Escalation**" requires both "**Escalation Classification**" and "**Escalation Actions**".

In the first example below, the user has chosen the category as **Dismissal**, with categories labelled as *"Bird", "Bugs", "Cat", "Dog", etc*. These categories will show up in the drop-down menu within the **Rules** Page.



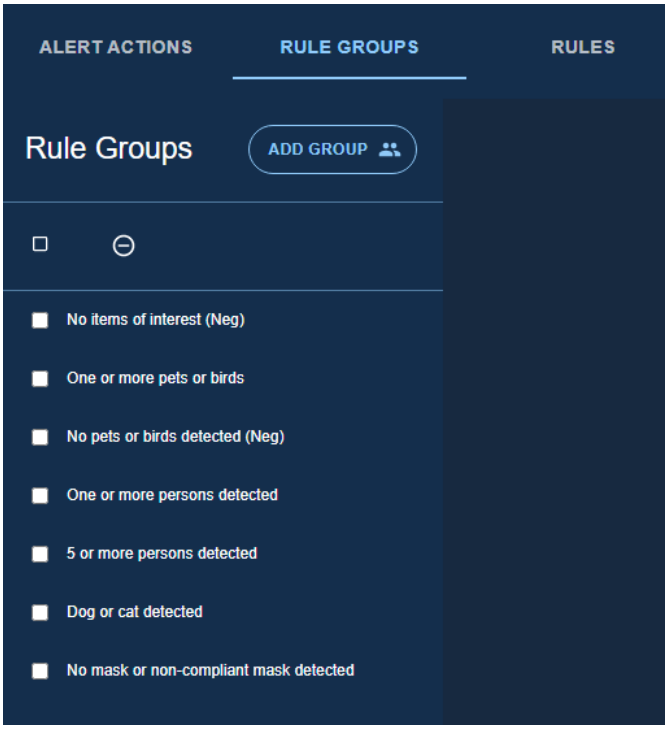
In the second example below, the user has chosen the category to be an **Escalation**, with classification labelled as "*Armed Robbery*" and a collection of corresponding actions as "*Alert Police*", "*Alert Armed Reaction*" and "*Alert Safety Office*". These classification and actions will also be displayed in the drop-down menu within the **Rules** Page.



4.3.2 Rule Groups

This sub-menu contains the settings of **Rule Groups**, one of the components of the classification rules. Each Rule can have multiple rule groups. Each rule group contains items/objects that users are interested in while monitoring the system.

Users can add/remove Rule Groups using the **Add//Remove** buttons. Clicking on the **Edit** button to the right of the rule group will allow the user to configure the group in detail.



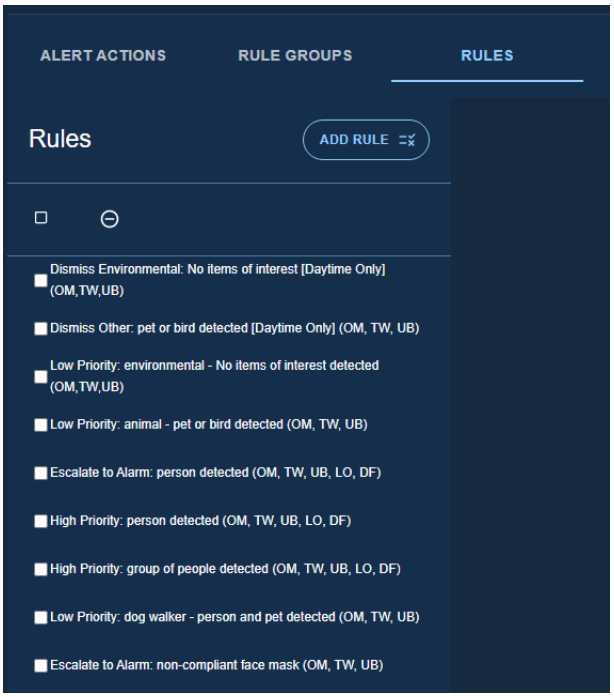
Each rule group contains a group name, a mode of inclusion (**Any Of/All Of**) and the collection of inclusions along with their settings. Users can choose what to include in the group by ticking the select boxes at the beginning of each classification.

Inclusion settings include detection probability threshold, the amount of detection of that particular inclusions and a corresponding compare operator. In the example below, the rule group *"One or more pets or birds"* has the inclusion mode of "*Any Of"*, and the *"Bird"* item ticked, with settings of *"Larger than 0"*. This means that if there is a detection of at least one bird in the frame, this rule group is of interest.

4.3.3 Rules

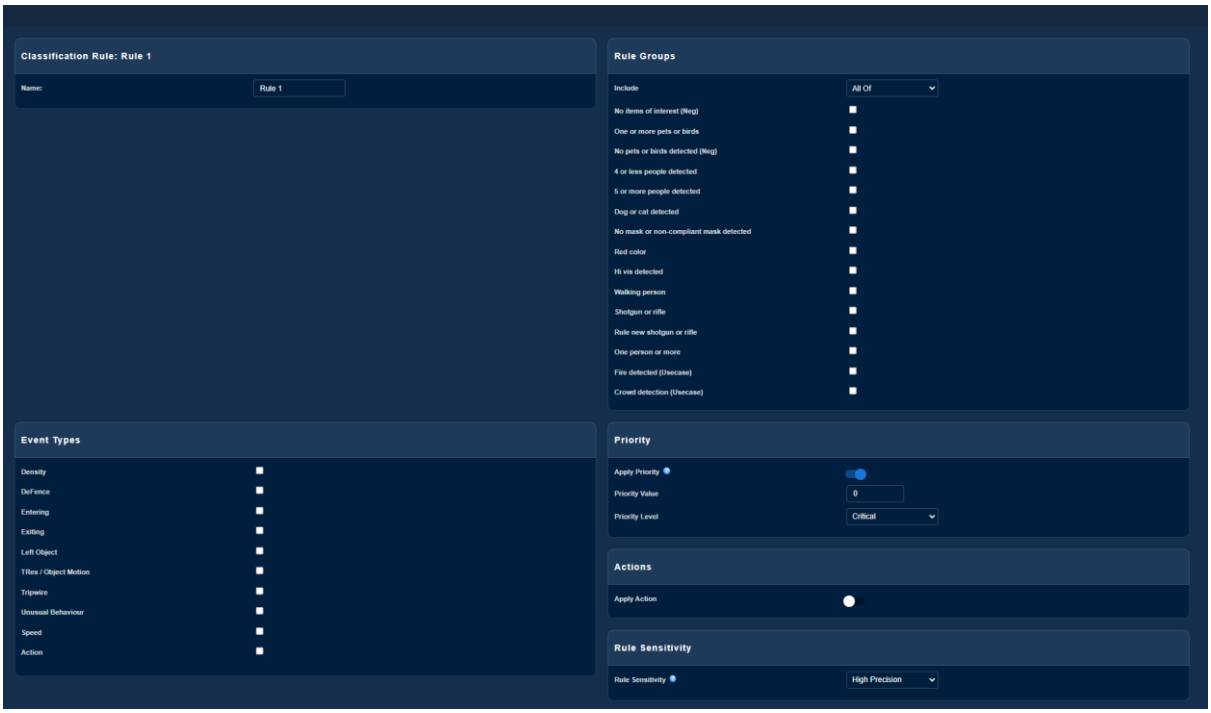
This sub-menu contains the settings of Classification Rules. Classification Rule contains Rule Groups that users are interested in, Alert Actions required for those Rule Groups and Rule Priority/Sensitivity Settings.

Users can add/remove Classification Rules using the **Add/Remove** (⊖) buttons. Clicking on the **Edit** button to the right of the rules will allow the user to configure the rule in detail.

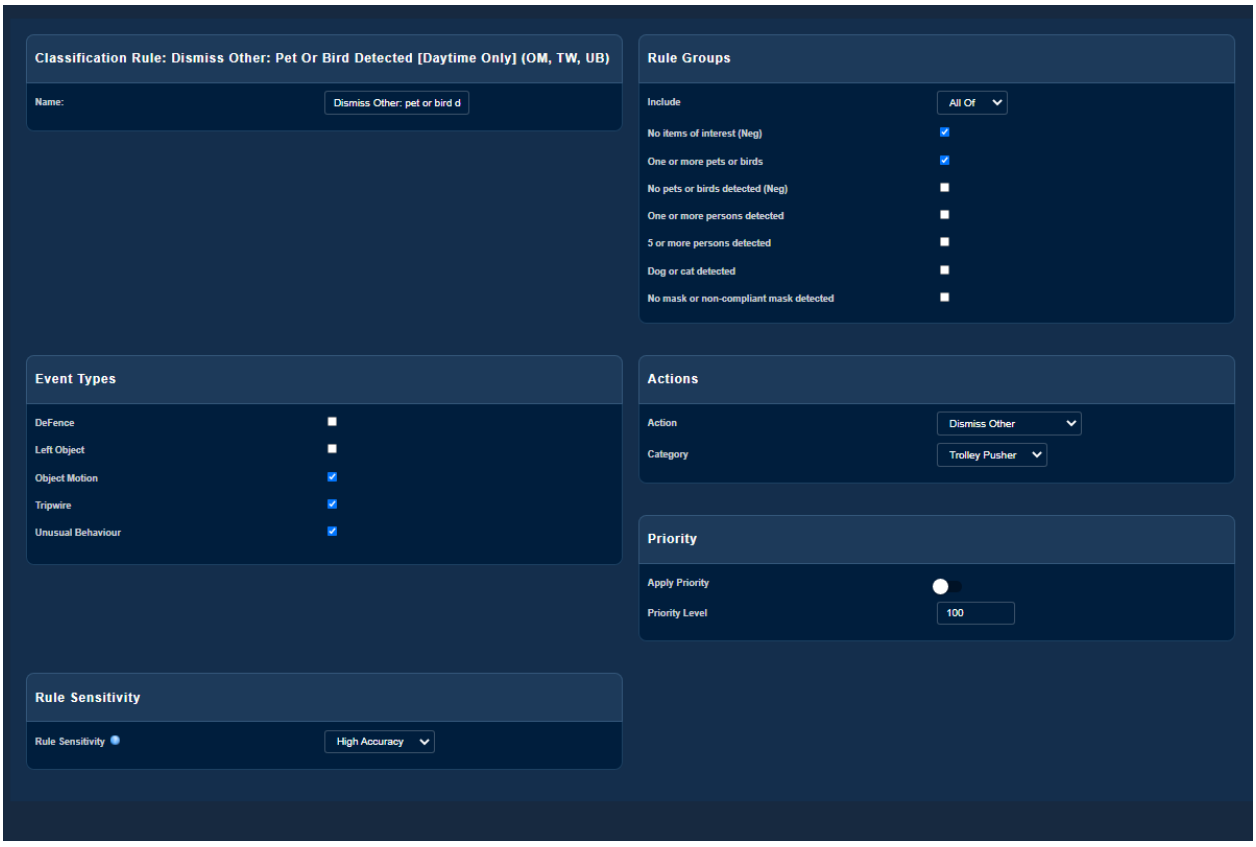


To configure a classification rule, users need to specify:

- **Name:** customised by users.
- **Event Types**: operating modes the classification rule is applicable to.
- **Rule Groups** (created/mentioned in the 3.3.2 Section).
- **Actions** to perform (created/mentioned in the 3.3.1 Section) if a certain rule group is triggered/detected.
- **Rule Sensitivity**:
    - **High Recall (High Sensitivity)**: Suitable for escalation actions. A minimum of one valid frame is needed to trigger the rule.
    - **High Precision (High Accuracy)**: Suitable for dismissal actions. A requirement of all valid frames is needed to trigger the rule.
    - **Majority**: a requirement of majority of frames is needed to trigger the rule.
- **Rule Priority:** Apply when no dismissal/escalation rule is triggered. Acts as a subordinate component to provide more information to the operator/users. As a rule of thumb, the value of 1 corresponds to the highest priority while 100 is the lowest priority.



In the example above, the escalation rule “Escalate to Alarm”, is applied for all event types. This rule will be triggered if one or more persons is detected in a sensitive zone. The user has specified the actions as “**Escalate to Alarm**”, with subcategory as “**Suspicious Person**”, and the follow-up action as “**Alert Armed Reaction**”. Since it is an alarm reaction, this rule should be a high sensitivity rule, since we want to be more cautious.

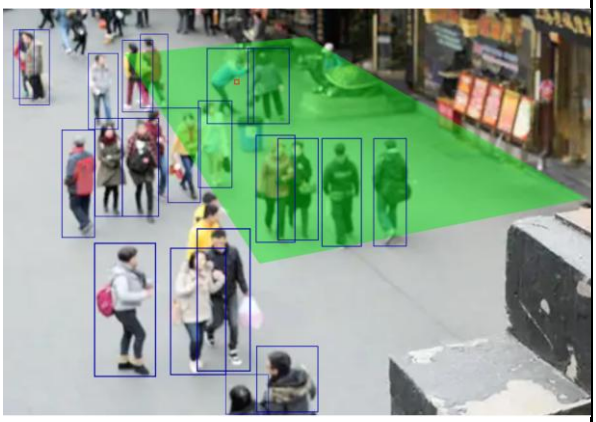
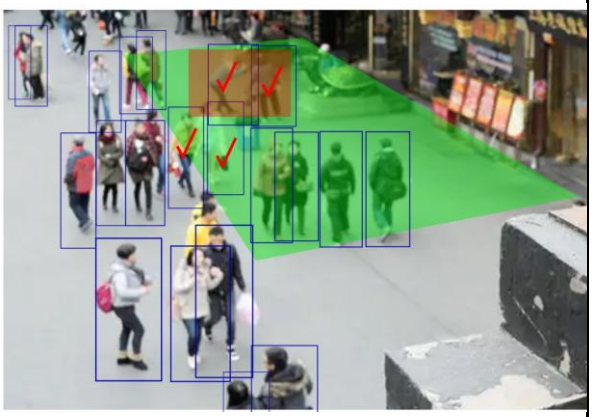


In another example above, the dismissal rule “Dismiss others: Pet or Bird”, is applied for Object Motion, Tripwire and UB only. This rule will be triggered if one or more pets or birds are detected in a sensitive zone. The user has specified the actions as “**Dismiss Other**”, with category as “**Animal**”, and since this is a dismissal rule, there is no option for action required. Due to the nature of dismissal, this rule should be a high accuracy rule, since we need to confirm that all frames are picked up with the dismissal target.

4.3.4 Case study

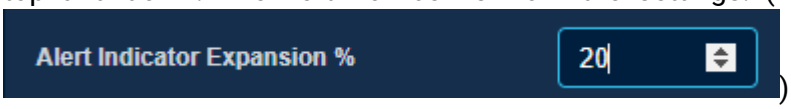
- Alert Indicator Expansion 20%
- Rule: Alert if detect more than 5 people

The colour in the real case may be different. In this example the colour of bounding box is used to differentiate amongst detected objects, indicator and the region of interest

How the original alert can be viewed	How the rule engine views the alert:
	

Output: rule is not trigger

Explanation:

- The indicator box is expanded 20% of image width and height. Start from the centre point of the indicator then 10% of image width to left and right, 10% of image height to top and down. The 20% number is from the settings. (Alert Indicator Expansion 

)
- The bounding box of detected objects is also expanded 10% of its width and height. E.g. 100 x 100 size is be expanded to 110 x 110 size
- The region of interest is configured as the green zone.
- The rule applied is “Alarm if there are 5 people detected in the ROI”. As a result, the rule engine must count how many detected people **INSIDE** the intersection of the RED and GREEN zone. In this case, there are only 4 people.

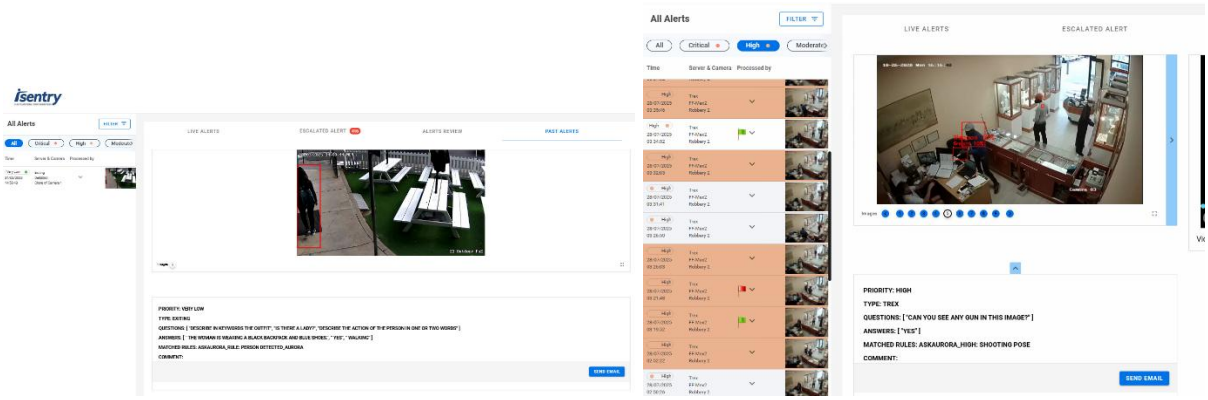
4.3.5 Aurora

Aurora is a Generative AI (LVM) model that can add valuable insights to your alerts by analysing the alert triggered image using natural language questions.

Aurora comes in play when you trigger a rule unleashing a set powerful set of capabilities that we will be covering in this section.

From 2026R1 we have 4 models, comprising two classes: general with three modes: balance, speed and accuracy, and gun in balance mode.

See below an output example from our Web Client where in the left-hand side we describe the outfit and action of the person (Aurora Investigation) and in the right-hand side we verify (Aurora Verification) the robber has a gun in his hand.



Aurora supports both default questions and user input questions that can be added via the UI. In this 2026R1 release, two types of Aurora servers are supported for different purposes:

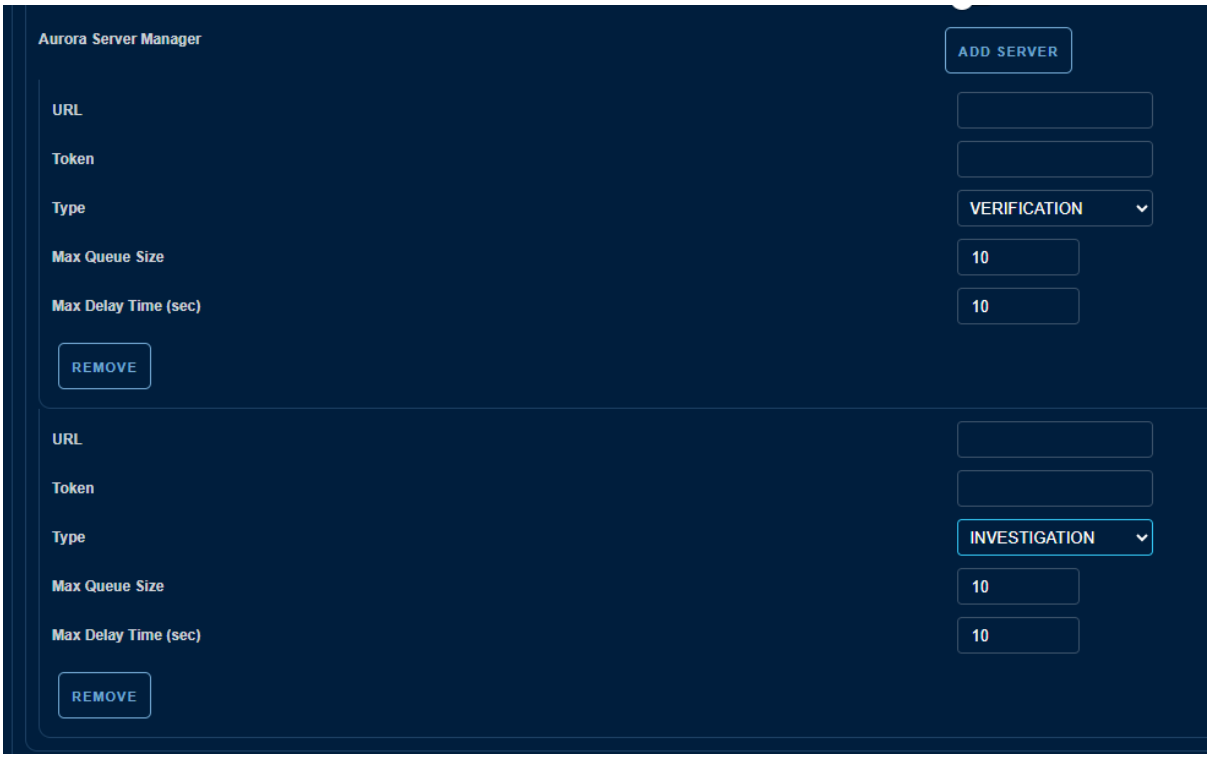
Aurora Verification: Real-time, time critical verification layer to check with object(s) is(are) present in the image or not and take appropriate action accordingly. Generally, this must be done within some time limit (in the order of seconds), and beyond this time limit, the system will have to assume Aurora is not available and proceed to the next alert. LVM models employed for this method could be large and time consuming due to the need to be relatively accurate. Starting with the 2026R1 release, an additional model called **Aurora Gun Verification** has been introduced specifically for gun scene verification.

Aurora Investigation: ability to give objects of interest some general description so that they can be searched later. This mode of operation is generally not time critical, hence longer delay is acceptable. This allows buffering a certain number of alerts to process when resource become available (and it will be overload if no resource available).

Please note, Aurora needs significant processing power in both CPU and GPU. Different modes of Aurora server need different minimum hardware requirements. Please check with Aurora Installation document.

For enabling Aurora(s) you need to first provide the **URL and token** to access Aurora service and decide if it will be investigation or verification, you can add as many servers as you have available, the load will spread among them.

From Firefly go to Settings and enter the provided URL and access token into the Aurora Server info area:

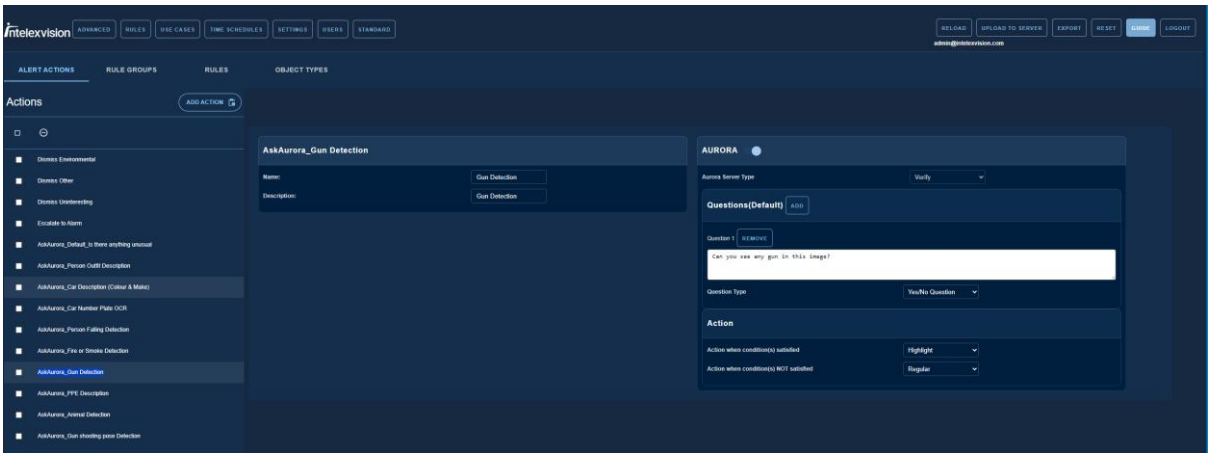


⚠️ **Pay attention to the Max Delay Time when configuring Aurora.** For investigations, the delay is not critical; however, it becomes critical for real-time verification. Keep that in mind when configuring access to your Aurora server(s). The same applies to the Max Queue Size, which limits the number of accumulated alerts waiting to be processed.

⚠️ **When Aurora is under heavy load,** your alerts will not be processed through Aurora until the system recovers.

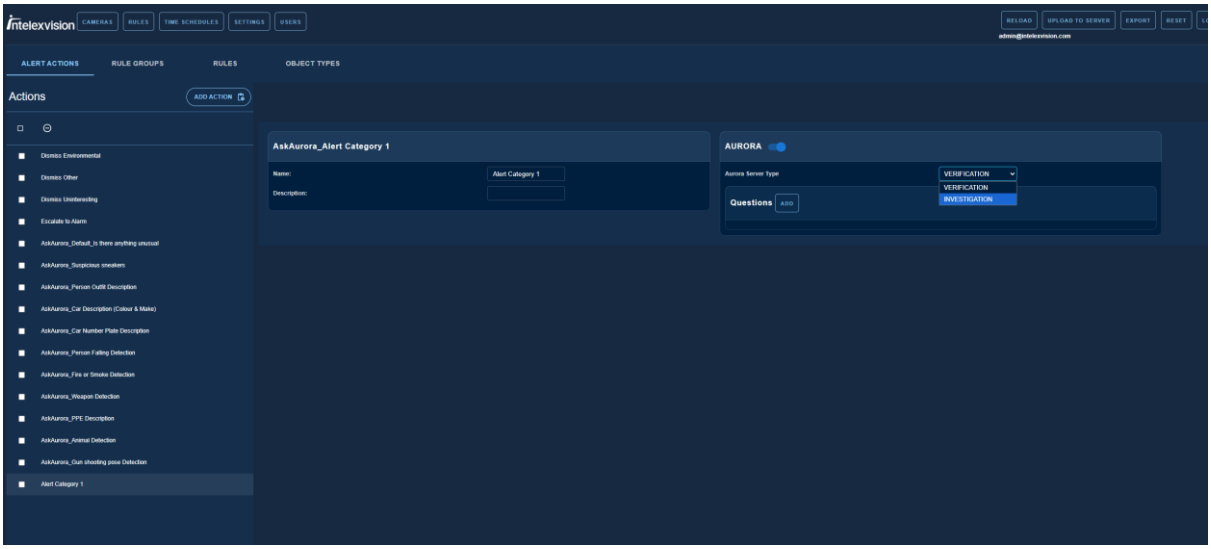
You can check the Aurora workload for Verification an Investigation in the /monitor website (see Section 5 Monitor):

Add an action in Rules menu and decide whether is Verification or Investigation, you can also pick the default ones such as “AskAurora_Gun Detection” (highlighted in blue below).



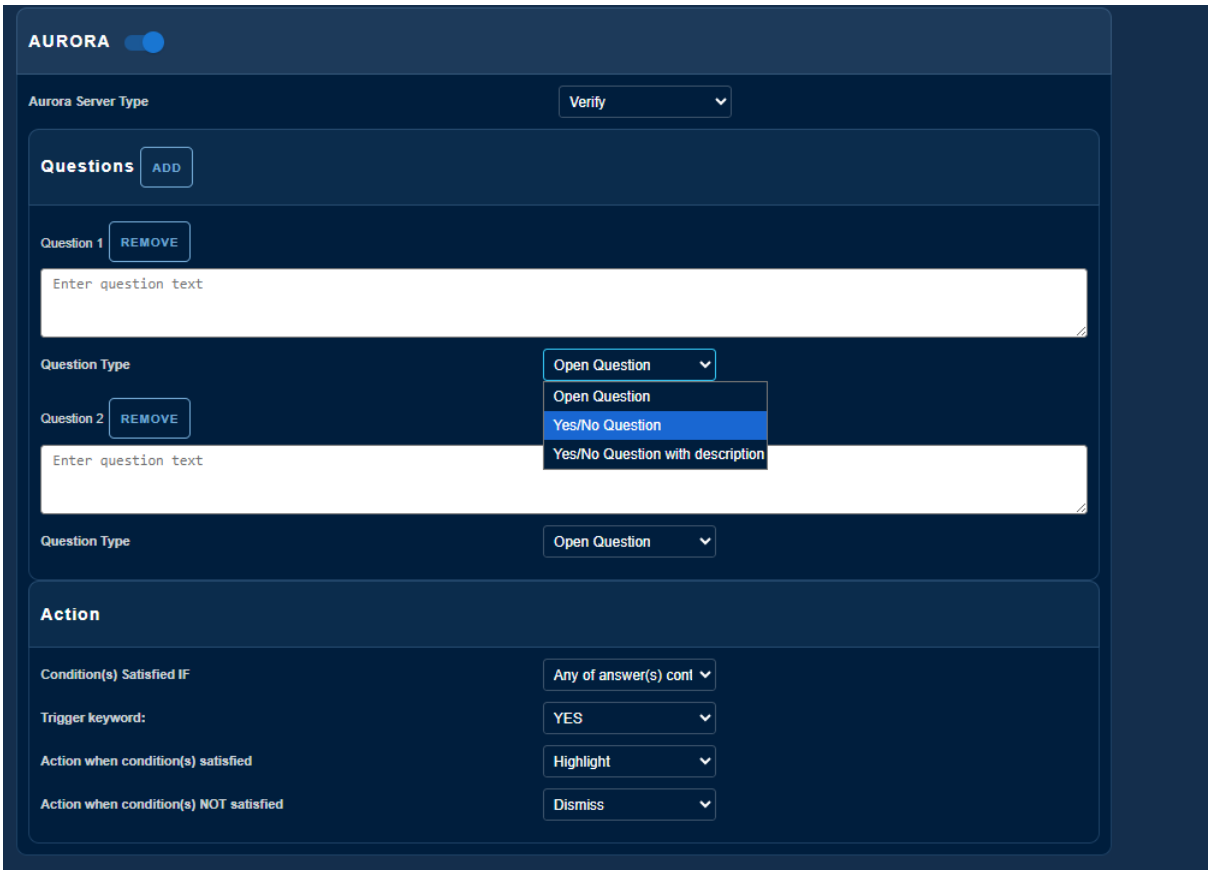
⚠️ Aurora investigate does not allow to trigger other actions, it will add extra information to enrich the description of the alert and that information can be searched later in the WebClient.

Please note that the dropdown menu depends on the server type you have entered in Settings (if you do not have an investigation server added, investigation action will not show up).

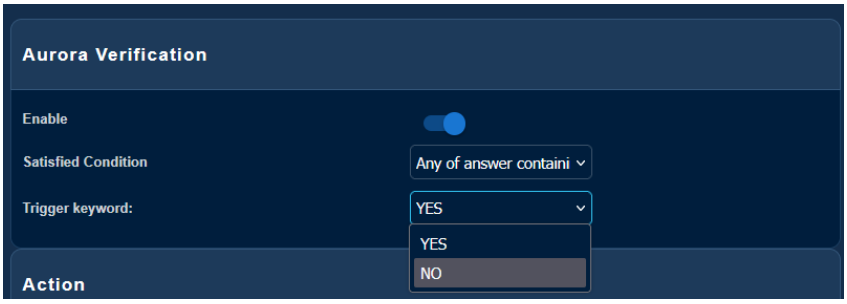


Aurora can be added from Alert Actions in the Rules menu, and it needs a general rule to be triggered first to take any effect. For enabling Aurora verification follow:

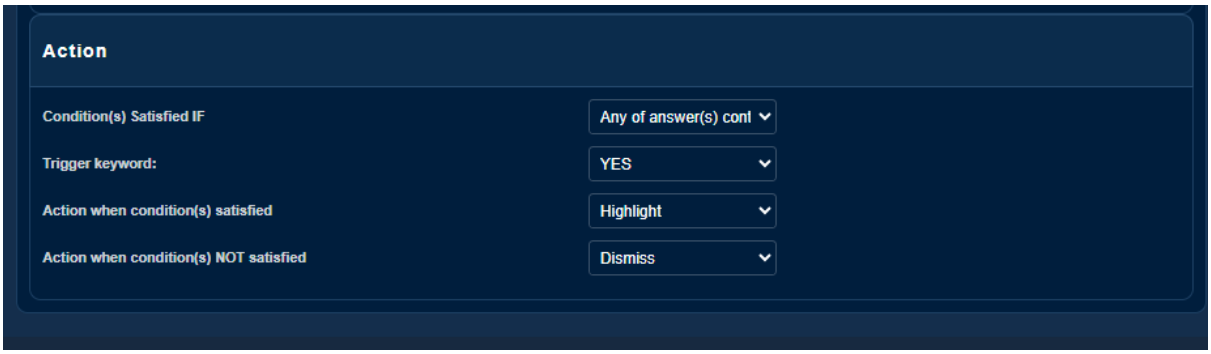
- Select Decision Mode, i.e. how to decide if a rule is matched or not:
    - Any of Answer containing keyword: In case of multiple questions, any answer with keyword will satisfy condition. It is recommended to use this condition when using both yes/no and open question because answer to the open question may not contain the selected keyword
    - All of Answer containing keyword: In case of multiple questions, all of answers MUST contain the keyword to satisfy condition



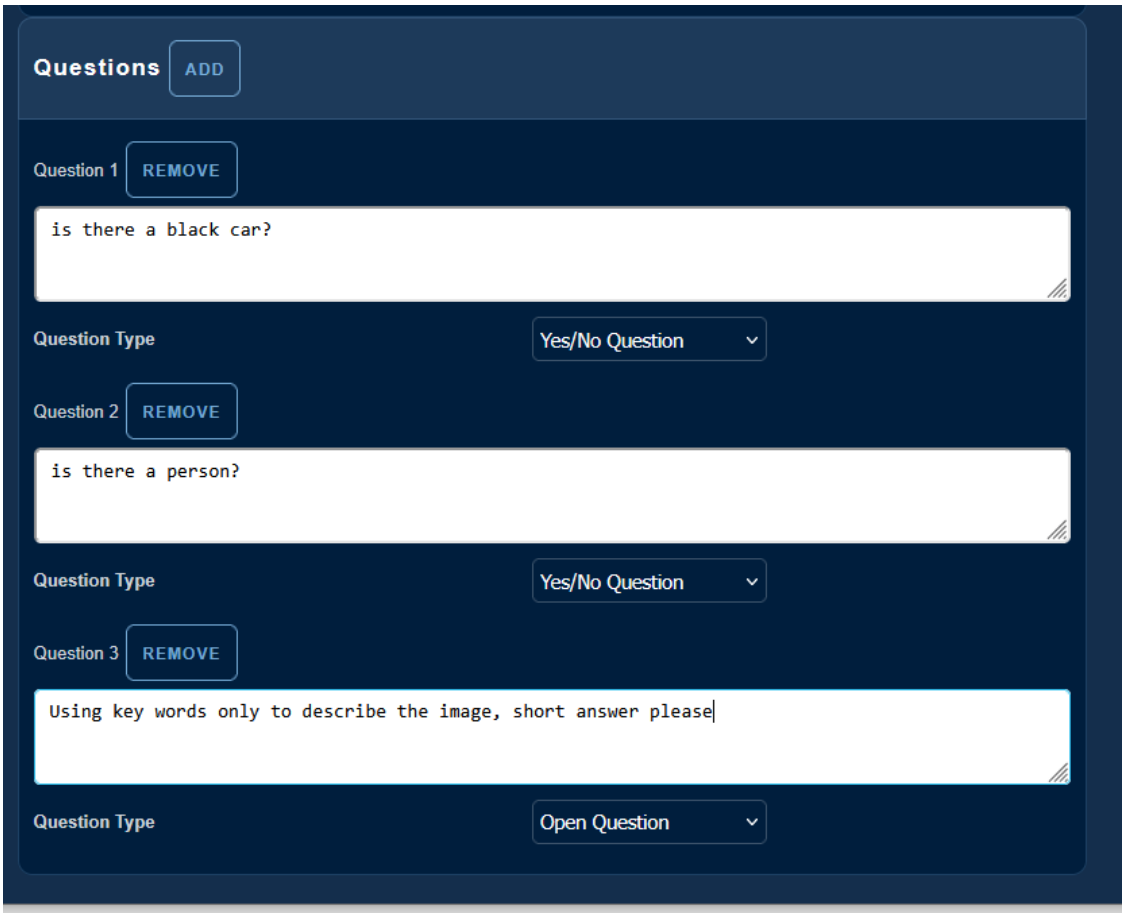
- Triggers keyword:
    - For now, only YES or NO keywords are allowed



- Action type, i.e. what action to take in case the condition is satisfied and what action to take when the condition is not satisfied:
    - Escalate: Escalate alert
    - Highlight: Highlight alert will be classified as Moderate priority level.
    - Regular: Normal Alert following by the DL Rule
    - Dismiss: Dismiss Alert

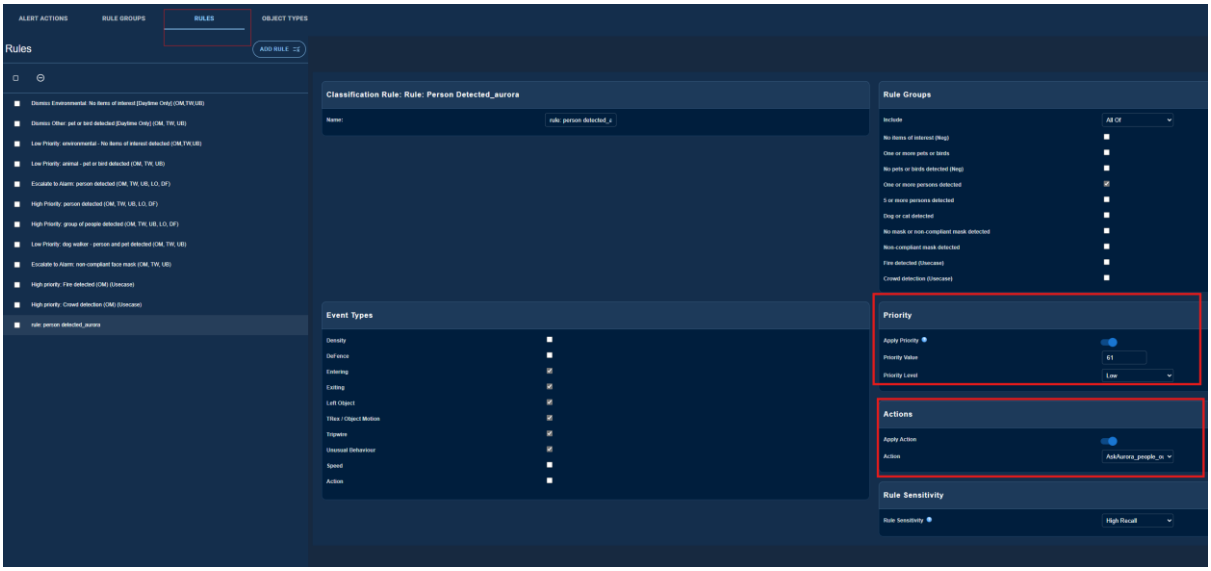


- Two directions:
    - Satisfy matching keyword condition
    - Unsatisfied matching keyword condition.
- Add Question
    - Put question in the white text box
    - Question types: select correct type
        - Open Question
        - Yes/No Question
- E.g.: 3 added questions in the picture:
    - 1 open question for description
    - 2 Yes/No questions



- After setting up Aurora Action, it can be selected in the RULES.

Need to enable rule priority for Aurora to work.



4.3.6 Default Rules with Aurora support

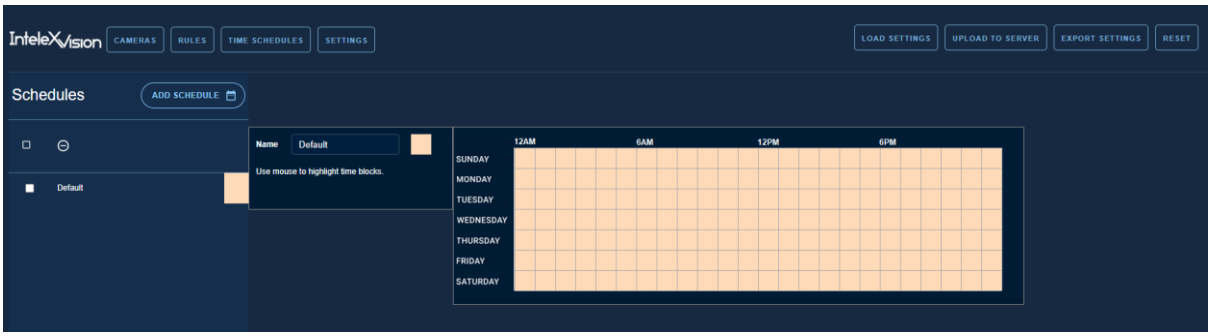
Starting with the 2026R1 release, the Firefly web-settings includes some default Rule associated with Aurora for convenience of users. Please refer to the table below for the checklist

Critical priority: Weapon detection	AskAurora_Gun Detection	Gun Verify
	AskAurora_Gun shooting pose Detection	Gun Verify
Critical priority: Fall detection	AskAurora_Person Falling Detection	Verify
Critical priority: Fire detected	AskAurora_Fire or Smoke Detection	Verify

4.4 Time Schedules menu

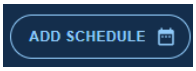
The server menu contains **Schedules**.

4.4.1 Time Schedule Setting

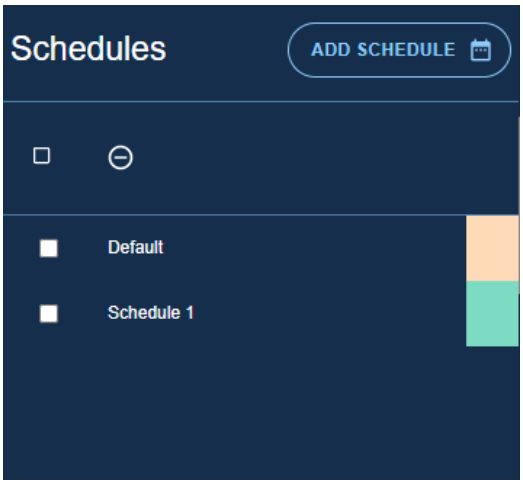


Note: There is a "Default" Time Schedule loaded when a server is initially set up/reset. This "Default" Schedule cannot be removed.

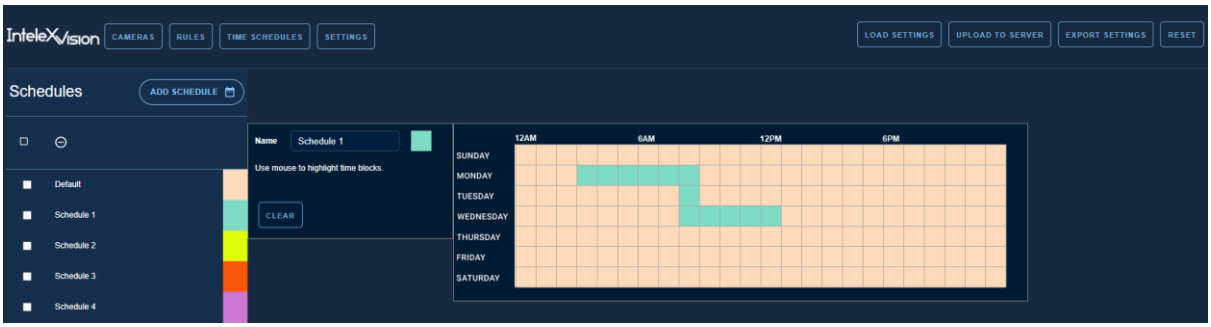
Users can Add/Remove new customised schedules using **Add Schedule/Remove** button:



Once a schedule is created, clicking on the schedule item line allows the user to edit each schedule individually. The new schedule has a different colour.



Users can **click and drag** to highlight time blocks to include in their custom schedule. The image below shows an example of Schedule 1 in light blue.



Users can rename Schedule using the text field.

As shown above, each time block on the weekly grid is exclusive for one unique schedule. Selecting a block position in a specific schedule will result in automatic deselections of the same block position in all other schedules.

4.5 Settings

This sub-menu contains all other server settings, like Server ID and Server Name at the top including:

4.5.1 Deep learning Excluded/Accepted Object Property Item(s)

You can suppress unwanted object types (never show an object in the ban list, even if it is detected) such as person or motorbike, or you can select specific ones to be accepted such as fire in the example below:

⚠ Certain objects are properties, for example colour or PPE equipment when doing PPE Compliance. In that case you need to select an object that has the property such as **person**. Otherwise, it will not show the selected objects in your alerts. ⚠

4.5.2 Focused Object/Property Item(s)

We can select which object to place the alert indicator into. In critical scenarios such as gun shooting pose detection having a firearm focus object can be a useful option. Firefly analytics are triggered under certain circumstances, and we point out the exact point by using the Alert indicator. Rules revolve around the position of the Alert Indicator so in some scenes we might want to place the alert indicator on a very specific object such as “firearm”.

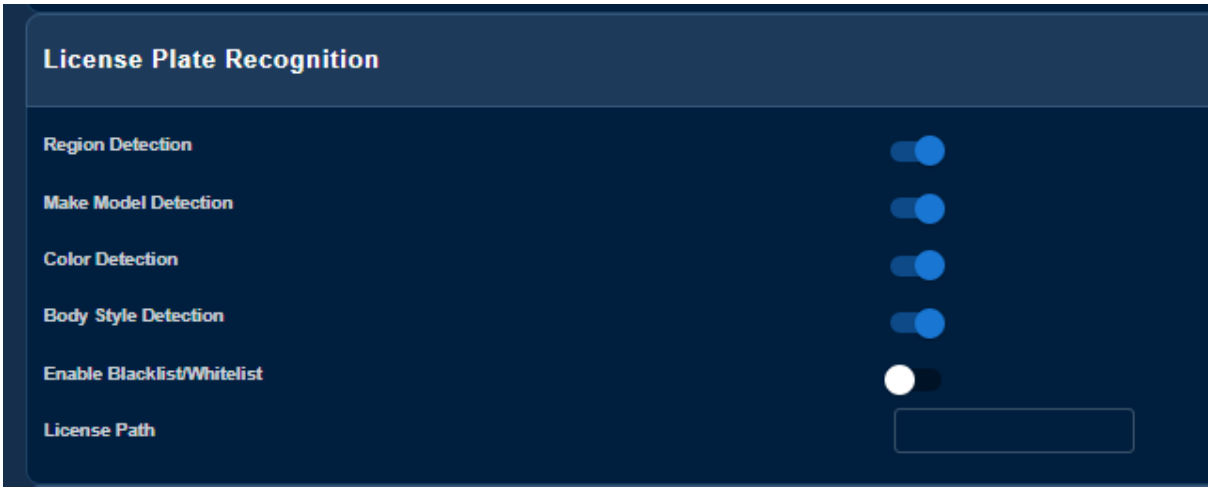
⚠ One counter example could be a scene where there is an armed security guard in the scene all the time and we don’t want to enter “firearm” as focus object altering the position of the

Alert Indicator. Doing so may be a mistake as it would not satisfy the original intentions of a gun shooting pose surveillance setup. ⚠️

4.5.3 License Plate Recognition (LPR)

Firefly now incorporates **License** Plate Recognition model. To use it you must enable the license plate recognition model in Detection / Classification (in advanced camera menu).

The following options are available:



Region Detection, when a supported countries and regions is matched, the alert metadata will contain that information. LPR region support is only Middle East (Dubai, Qatar, UAE, Saudi, Bahrain)

Make Model Detection will be available such attributes in the alert metadata.

Colour Detection, when enabled can be used to apply rules for certain car colours. ⚠️ Please note that it does not work with TW DL counting (enter/exit).

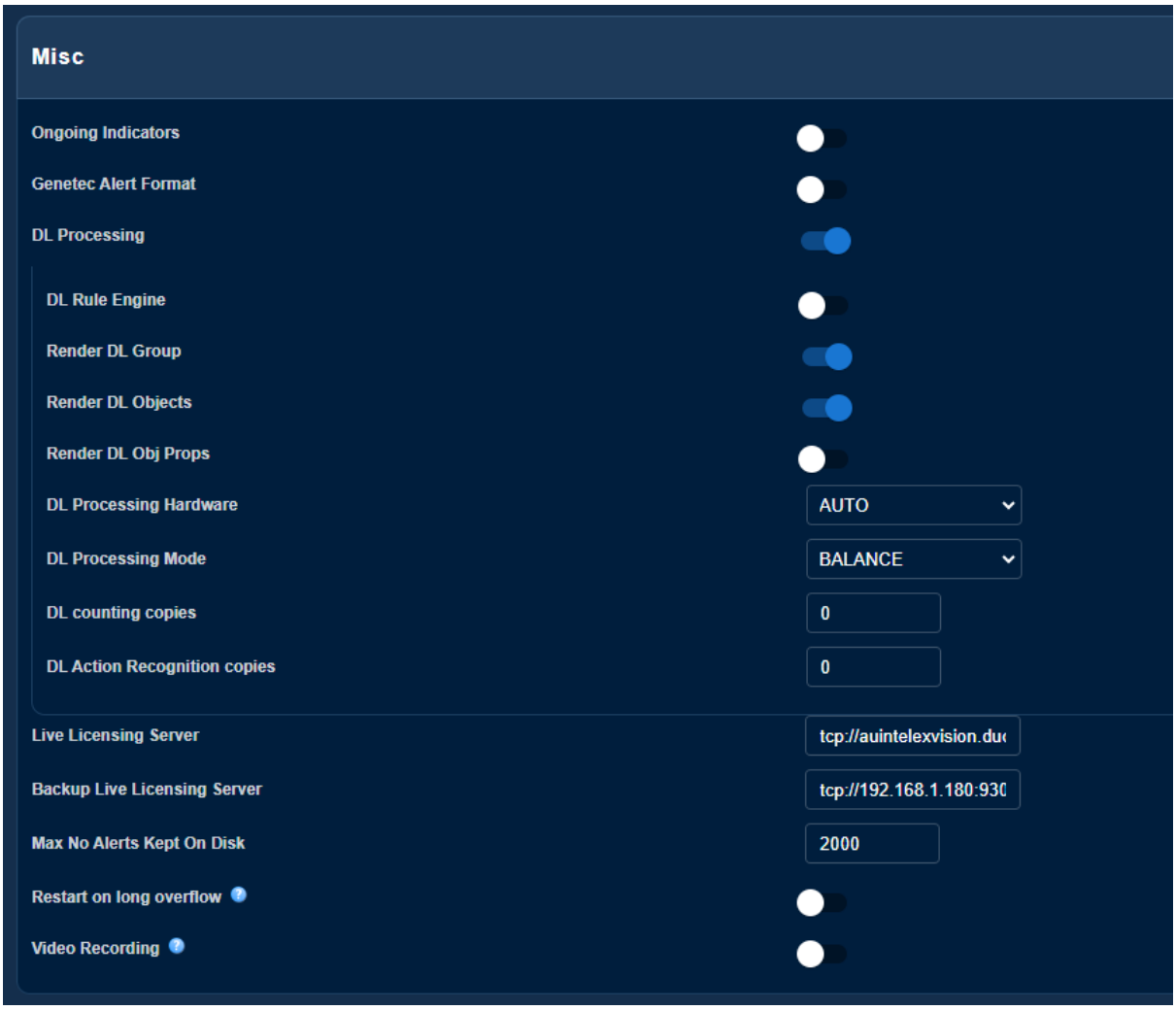
Body Style Detection, when enabled it can be used to display such attributes in the alert metadata.

Enable Blacklist/Whitelist, when enabled the user can leverage a list of plates previously enrolled in Firefly and properly encrypted. You have to provide the path where blacklist.iv and whitelist.iv files are present:

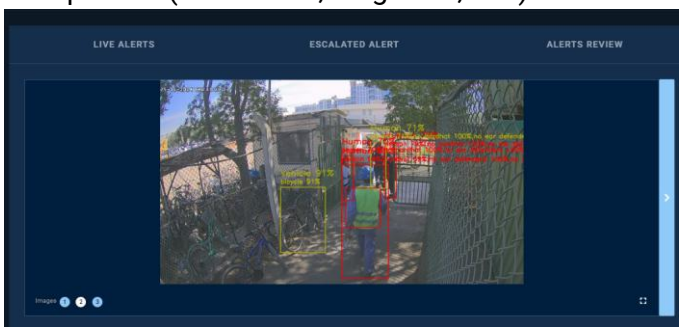
4.5.4 Camera Features

- turn ON/OFF corresponding sub-menus in Cameras Menu. By default, all sub-menus are turned ON. **Note**: This only hides the sub-menu(s) visibly, all underlying functionalities still exist.

4.5.5 Server Miscellaneous Settings



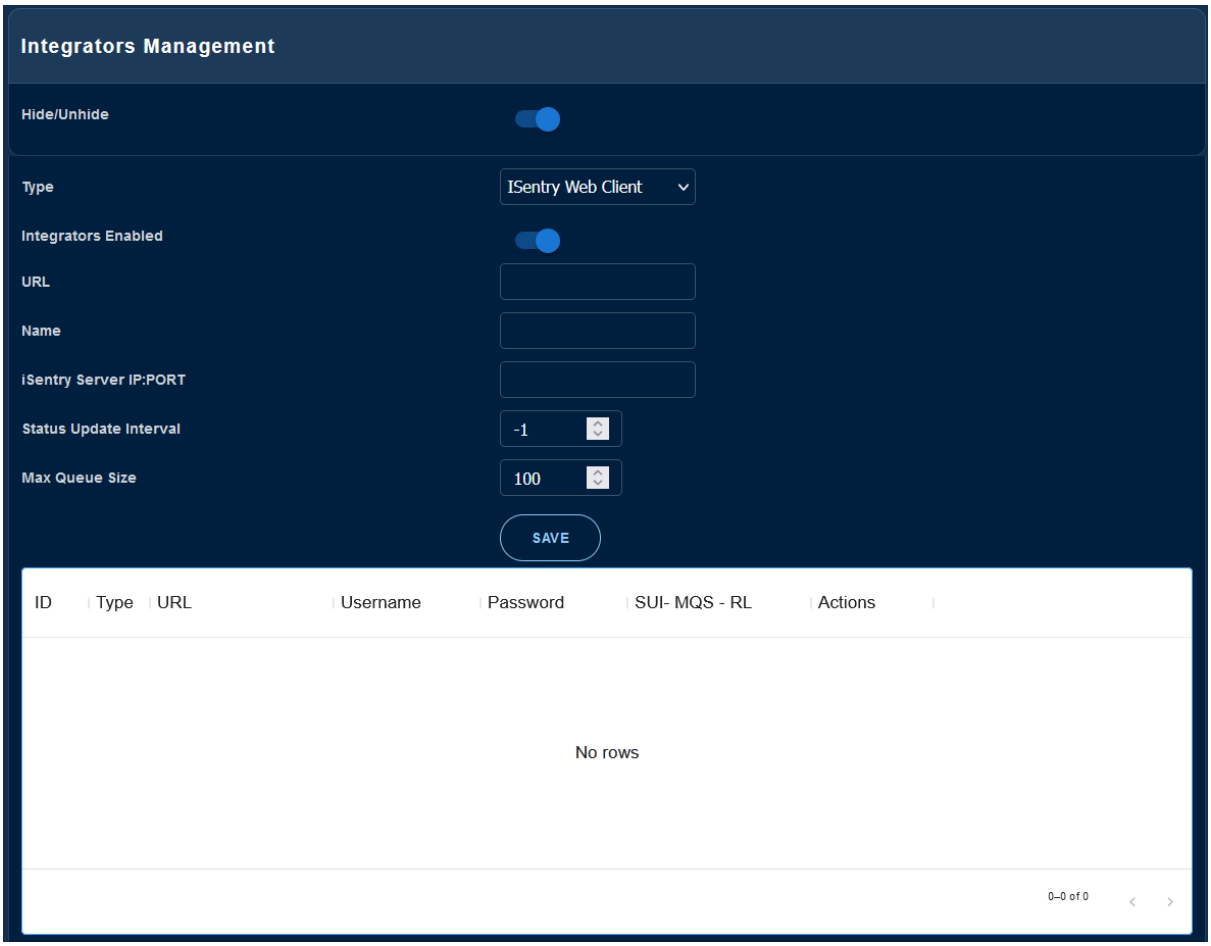
Settings	Default	Description
Ongoing Indicators Enabled	OFF	Enable sending ongoing Alert Indicators during an alert. Default is off.
DL Processing Enabled	ON	Enable deep learning processing in Sentry

DL Rule Engine Enabled	OFF	Enable Rule Engine in Sentry
Save Dismissed/Rejected Alerts	OFF	
Render DL Group	ON	Group of the object such as Vehicle.
Render DL Objects	ON	Name of the object such as Human, Umbrella
Render DL Obj Props	OFF	Such as colour, PPE equipment when doing PPE Compliance (no hardhat, no gloves, etc.) 
DL Processing Hardware	AUTO	Select hardware to process Deep Learning in Sentry. Options include **AUTO**, **NVIDIA PreRTX/Jetson Series, NVIDIA RTX or later**, **INTEL HD** and **CPU**. If the **AUTO** option is selected, Sentry will attempt to detect and select a specific hardware based on the following preferred order: **NVIDIA > INTEL HD (GPU) > CPU.**
DL Processing Mode	BALANCE	Select the manner of which Sentry processes the Deep Learning results. Options range from **HIGH ACCURACY** (Resource intensive), **ACCURACY, BALANCE, SPEED** to **SUPER FAST** based on an incremental processing speed order.
GPU Index	-1	Manual select GPU index for Rule processing deep learning. On a multi-card machine, GPU index (starting from 0) can be specified so Trex and DL can use different GPU for hardware acceleration. This option is only applicable for NVIDIA card(s).
DL counting copies on GPU 0	0	When on TREX counting entering/exiting a region of interest, it indicates to create more copies of the network model that counts. Matching this number with the number of cameras counting is beneficial. This option is only applicable for NVIDIA card(s).

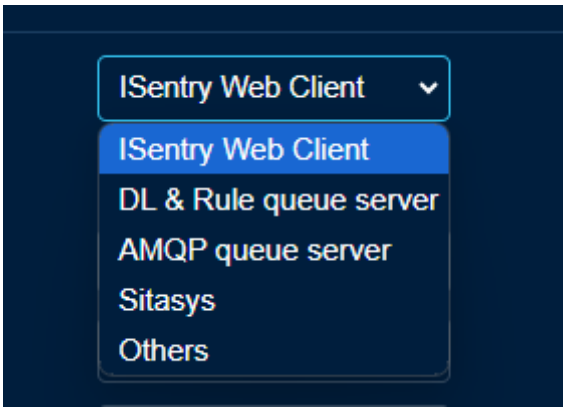
DL counting copies on GPU 1	0	Same as above but applies when you have another GPU available. This option is only applicable for NVIDIA card(s).
Live Licensing Server	-	Enter the URL of the licensing server here to make the system obtain the proper licence.
Backup Live Licensing Server	-	Enter the URL of the backup licensing server here to make the system obtain the proper licence.
Maximum Number Of Alerts Kept On Disk	200	Limit the maximum number of alerts kept on disk before the oldest are replaced by newer alerts
Restart on long overflow	OFF	When ON: if the frame buffer for analytics is overflowed for a long time, Sentry Server will auto restart.
Min Delay Before Overload Reset (minutes)	30	Minimum time to wait from start-up that this feature will apply.
Min Number of Overload Camera for Reset	10	Minimum number of cameras experiencing “overload” at the time of “overload” restart

4.5.6 Integrators Management

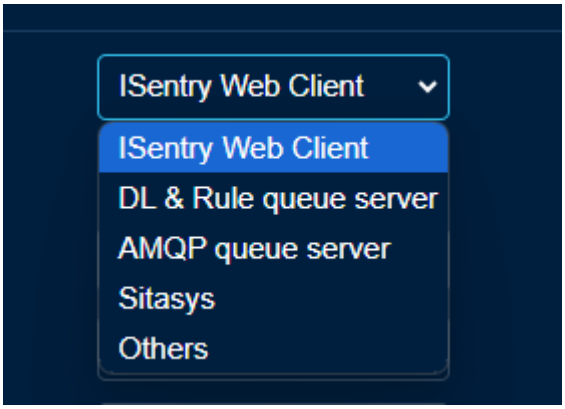
The following section involves the Integrators, which are the systems who will be getting alerts from **Sentry Firefly**.



This menu covers several types of integrators, at the present time:



The parameters can be configured for **iSentryWebClient** like:

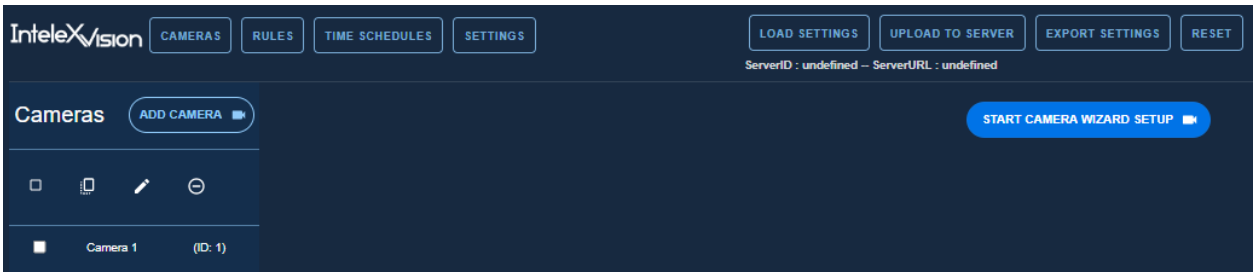
Settings	Default	Description
Type	iSentryWebClient	 DL & Rule queue server will enable an external DL & Rule processor so the internal won't start. Please be careful when enabling this type as an external DL & Rule Processor MUST be up and running.
Integrators Enabled	ON	Indicates if the integrator is enabled or not
URL	-	URL of the WebClient. Web API port is **8000**: Example 1 *192.168.1.124:**8000*** Example 2 *isentryclientdemo1.duckdns.org:**8000***
iSentry Server Name		
iSentry Server IP:PORT		For example: *192.168.1.123:8123*
Parties Name	-	Name of the integration party if any
Parties Authorization	-	Authentication token for access
Parties CompanyId	-	Unique ID provided by Integrator
Status Update Interval	-1	
Max Queue Size	100	Number of alerts that can handle.

The parameters can be configured for **Sitasys** like:

Settings	Default	Description
Type	iSentryWebClient	Type of integrator
Integrators Enabled	ON	Indicates if the integrator is enabled or not
URL	-	URL of the integration party like Sitasys. Examples are: *"https://talos.evalink.io:443"*
Company Name	-	Recommended a word like for example “Sitasys”
Token Bearer	-	Alphanumeric characters with the authorization bearer.
iSentry Server Name		Provided by Talos, for example: API-50dwTXfwI5AZ6zaaRzu12u6CFgHuCJA4
Company ID		Provided by Talos, for example: c6f04e27-5fb2-xxb6-8a17-34d7e808241f
Parties Name	-	Name of the integration party if any
Max Queue Size	100	Number of alerts that can handle.
Relay Port	8200	This port is where the Sentry pushes alerts to be forwarded and where the Alert Forwarded is listening to.

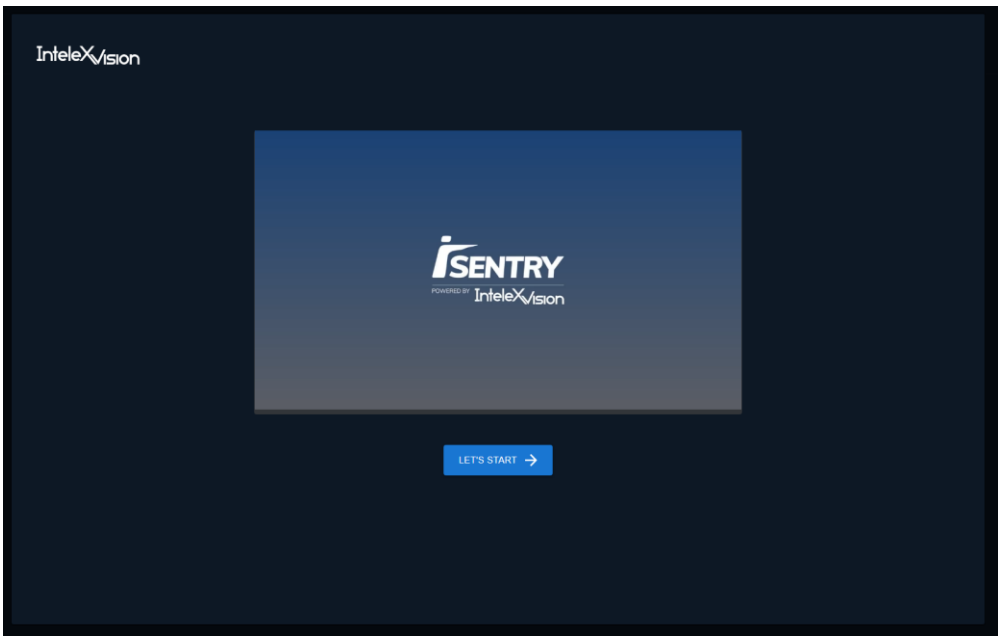
5 Camera Wizard Setup

Cameras can be set up quickly using the Web Setting Wizard feature. The wizard can be started by clicking on the “Start Camera Wizard Setup” button, located just under the main panel, within the Camera Section. Once started, the wizard will guide users through setting up most essential settings for cameras to be functioning.



5.1 Landing Page

This page contains a quick overview of Sentry fundamentals. Click on Let’s start to proceed.



5.2 Import Your Cameras

Users have three methods to add cameras to be set up by the Wizard:

- **From Current Settings**: add all current existing cameras in the server to the Wizard.
- **From CSV file**: created new cameras from a user input .csv file. The csv data needs to contain ***CameraID (unique number)***, ***Name (text)***, ***Group (number)*** and ***RTSP*** (text - optional), ***UUID (text – optional)*** information. The Wizard will create new cameras with the given information.

  Example of a CSV file

CameraID,Name,Group,RTSP,UUID

1000,Camera Test 1,1,rtsp://stream1.test:5555/main_1000,00000001-0000-babe-0008-3a010ac9942d

1001,Camera Test 2,1,rtsp://stream2.test:5555/main_1001, 00000001-0000-babe-0008-3a010ac9942e

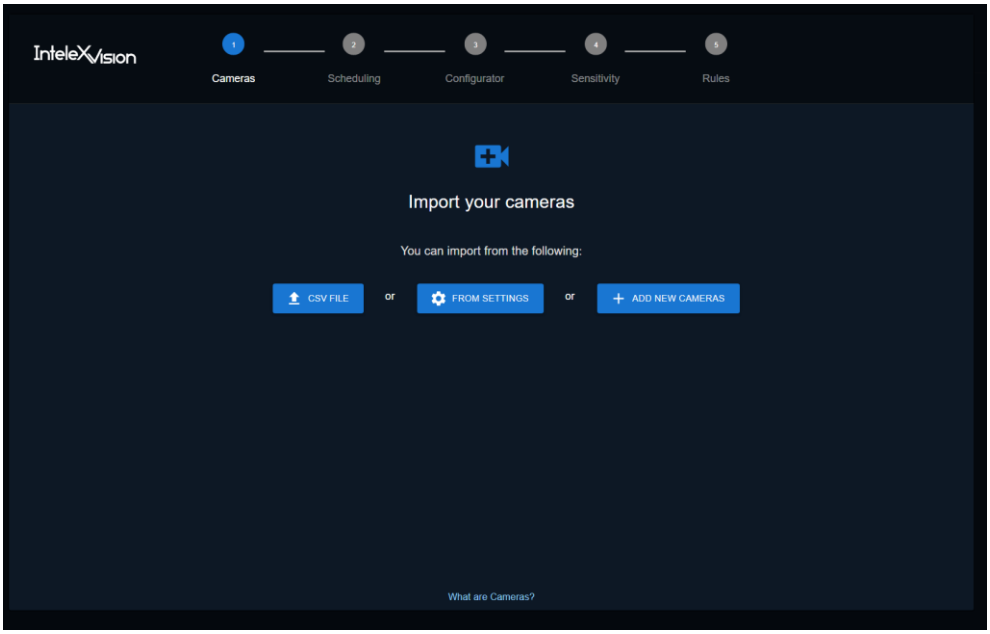
1002,Camera Test 3,1,rtsp://stream3.test:5555/main_1002, 00000001-0000-babe-0008-3a010ac9942f

1003,Camera Test 4,1,rtsp://stream4.test:5555/main_1003, 00000001-0000-babe-0008-3a010ac9942g

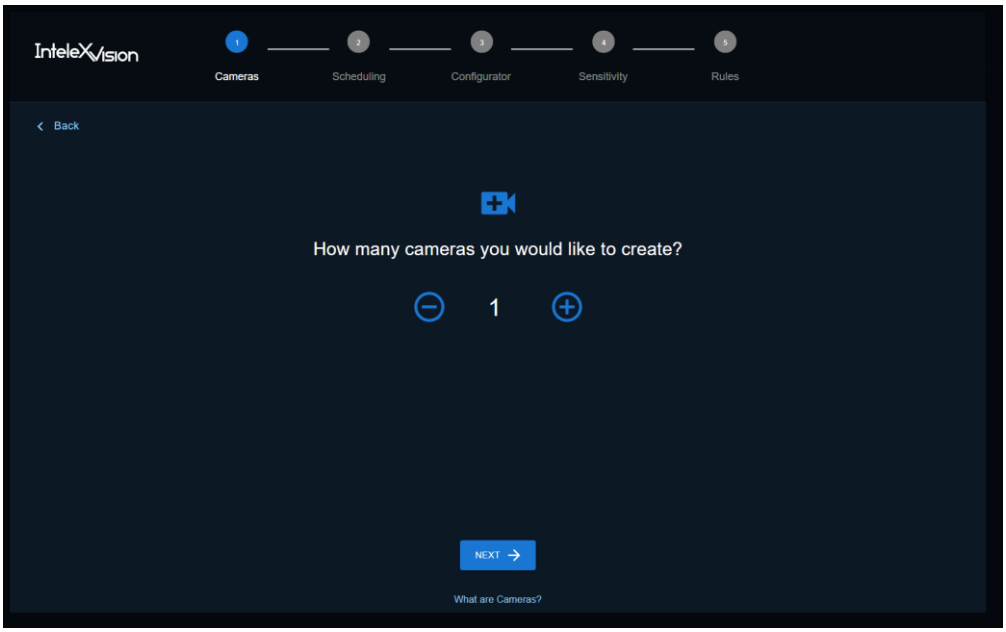
1010,Camera Test 5,2,rtsp://stream5.test:5555/main_1010, 00000001-0000-babe-0008-3a010ac9942h

1012,Camera Test 6,2,rtsp://stream6.test:5555/main_1012, 00000001-0000-babe-0008-3a010ac9942i

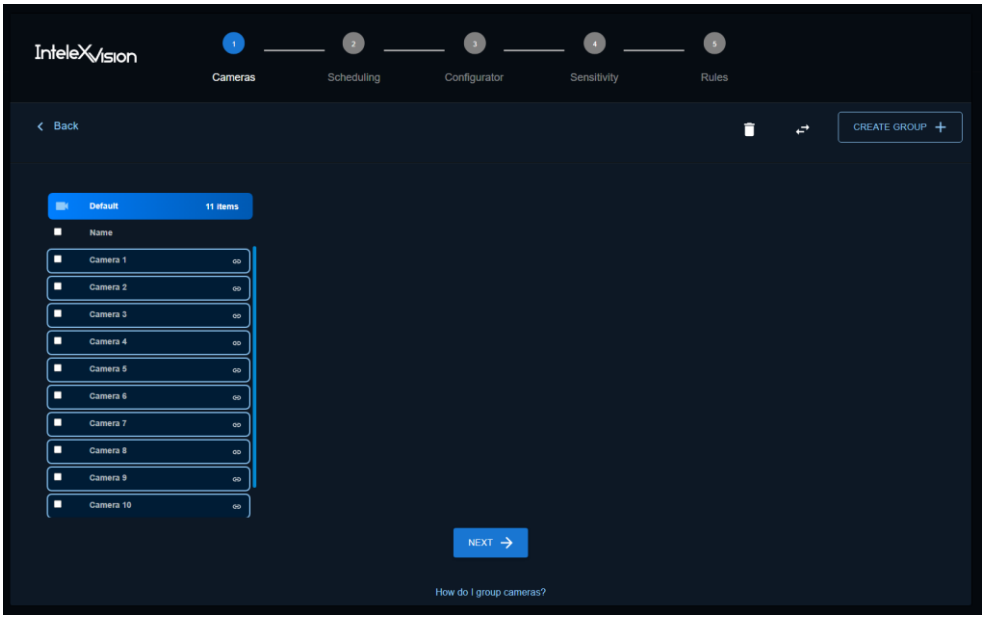
- **Adding new cameras**: Create brand new cameras using the wizard.



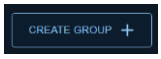
If users choose to “Add new cameras”, the next step is to specify the number of cameras they want. These newly created cameras will be added to the server with progressive unique Id and name.



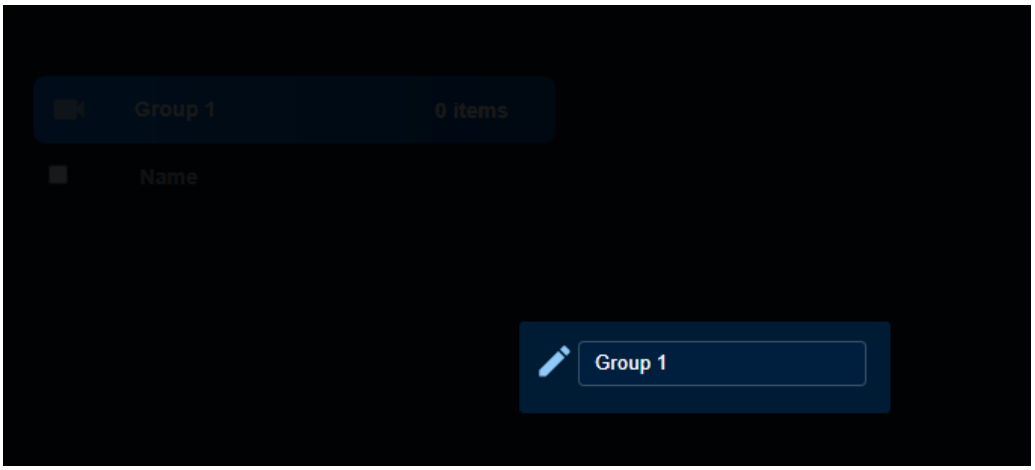
5.3 Group Your Cameras



Once imported/created, the cameras are listed under an initial group “Default” (group Id = 0). Users now have the option to group their cameras into custom groups for bulk configuration.

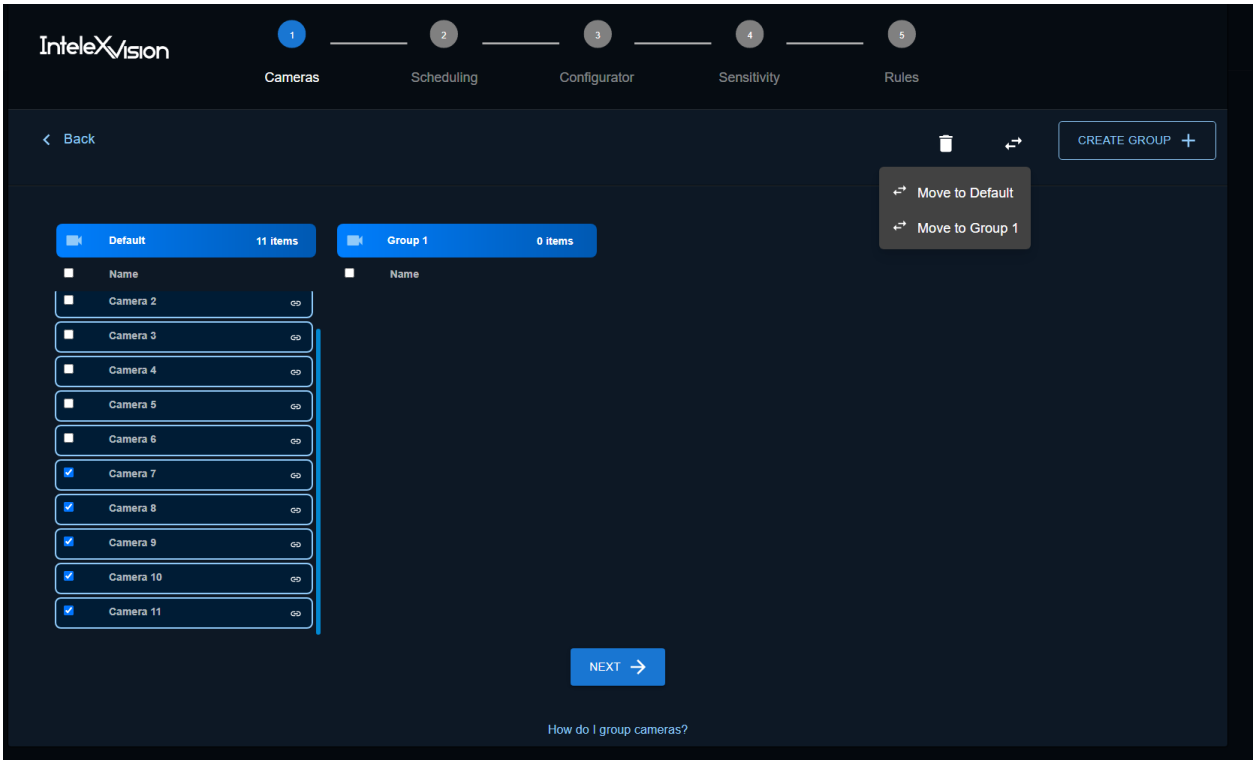
To create new groups, click on button 

on the top right corner. Once created, left clicking on the group name will bring up an input box for renaming the group.

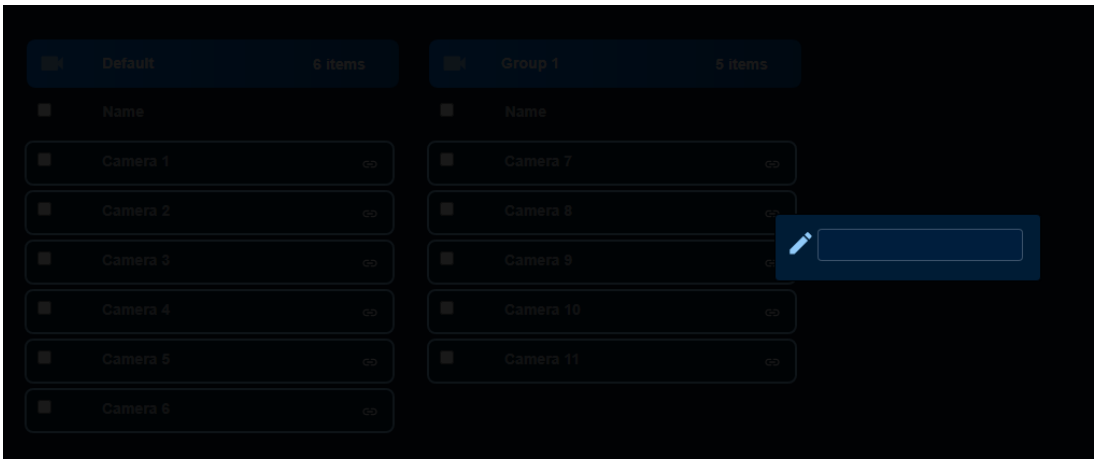


Users can drag and drop cameras into groups or select multiple cameras and click on **Move To (**  **)** to move all of them into another group (selected within the drop-down menu).

User can also remove cameras out of the wizard by selecting unwanted cameras and choose **Remove (**  **)**.

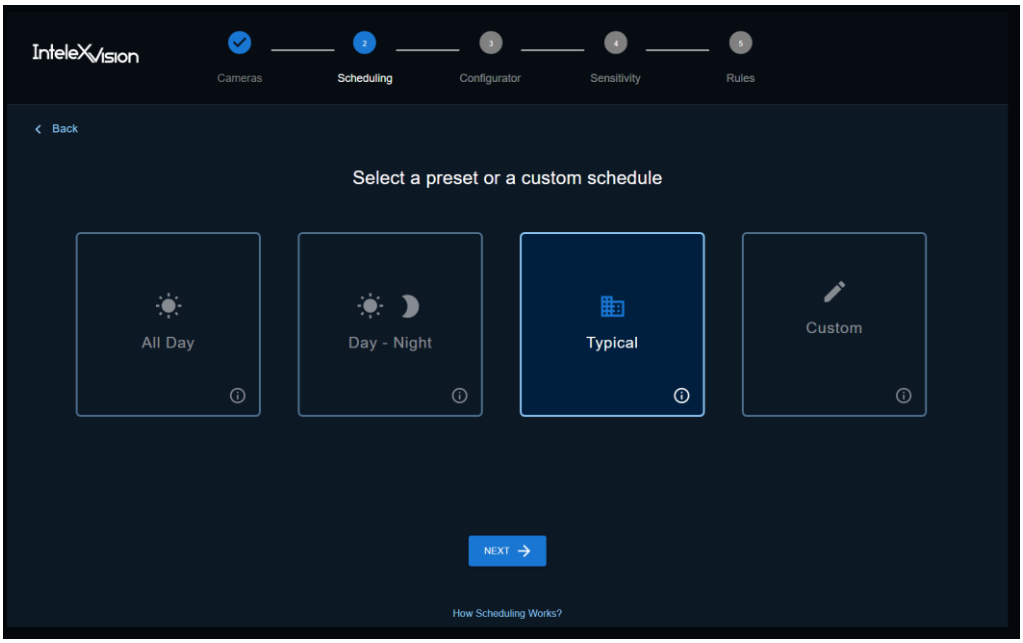


Moreover, clicking on the **Link (**  **)** icon to the right of camera names brings up an input box for customising/adding the camera RTSP.



Once happy with the grouping, users can select **Next** to proceed to the next stage.

5.4 Scheduling

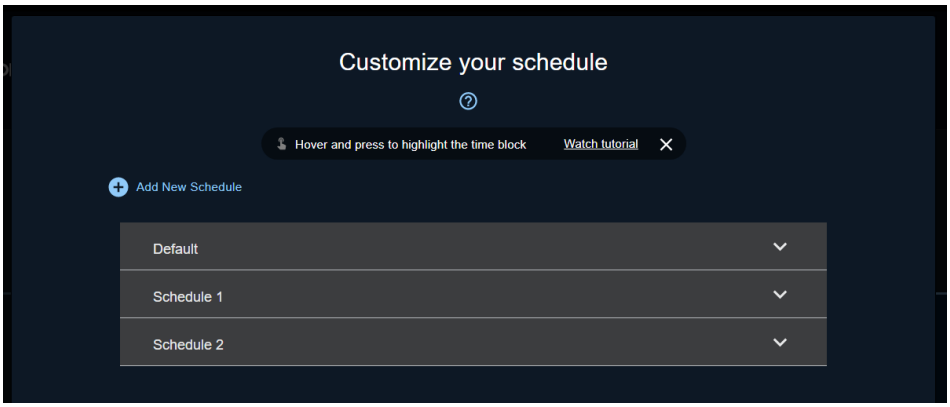


Once cameras are all grouped together, users need to set up scheduling for the server. There are 3 different presets to choose from ranging from:

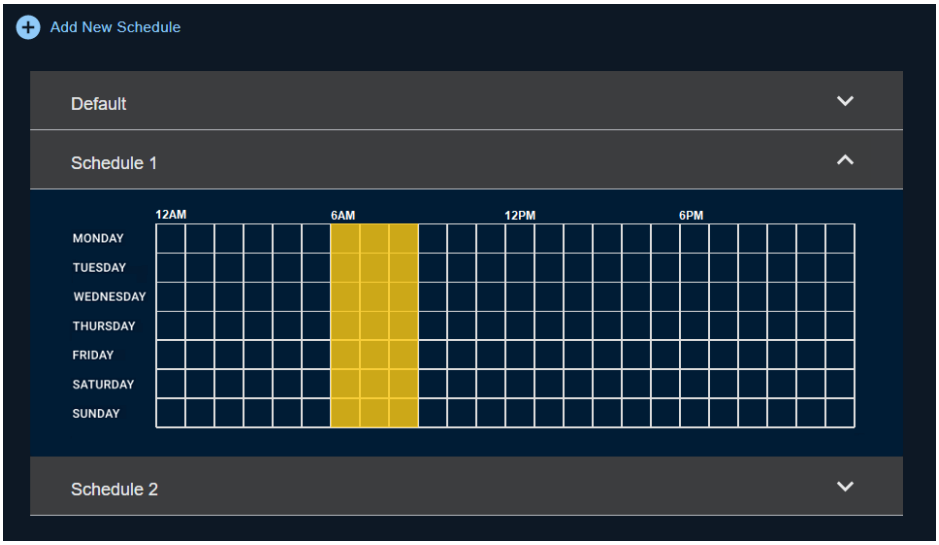
- **All Day:** 12am-12pm every day.
- **Day-Night:** 6am-5pm, 6pm-5am every day.
- **Typical:** 7pm-5am, 6am-9am,10am-2pm, 3pm-6pm.

Hovering over the info icons of each preset outlines the presets' details.

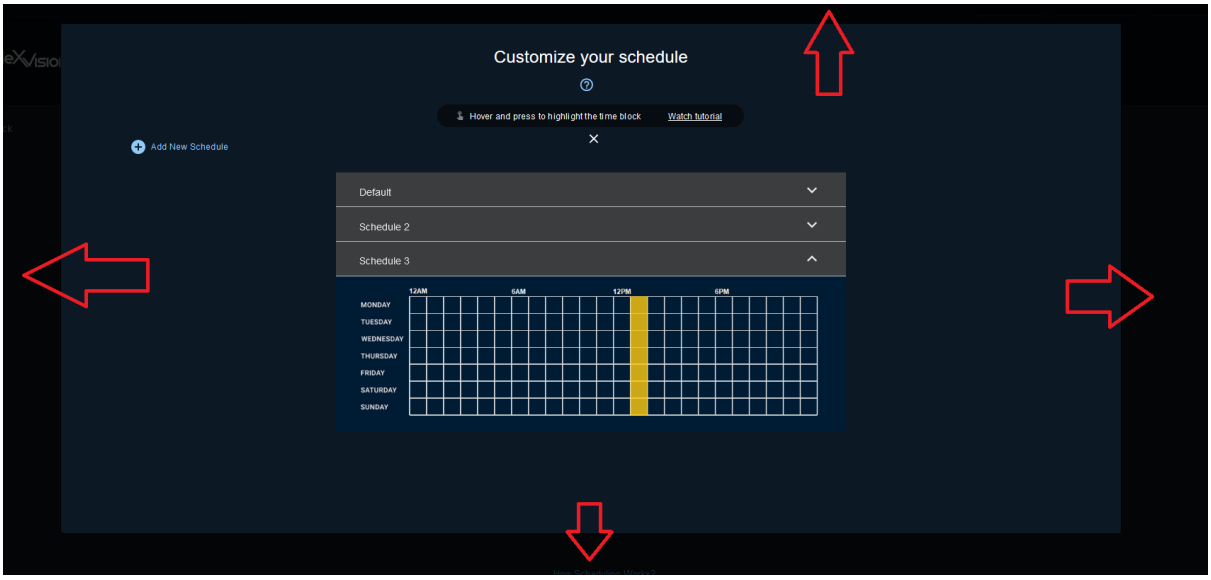
Alternatively, users can customise their own scheduling using the Custom Option. This will bring up a Custom Preset Page.



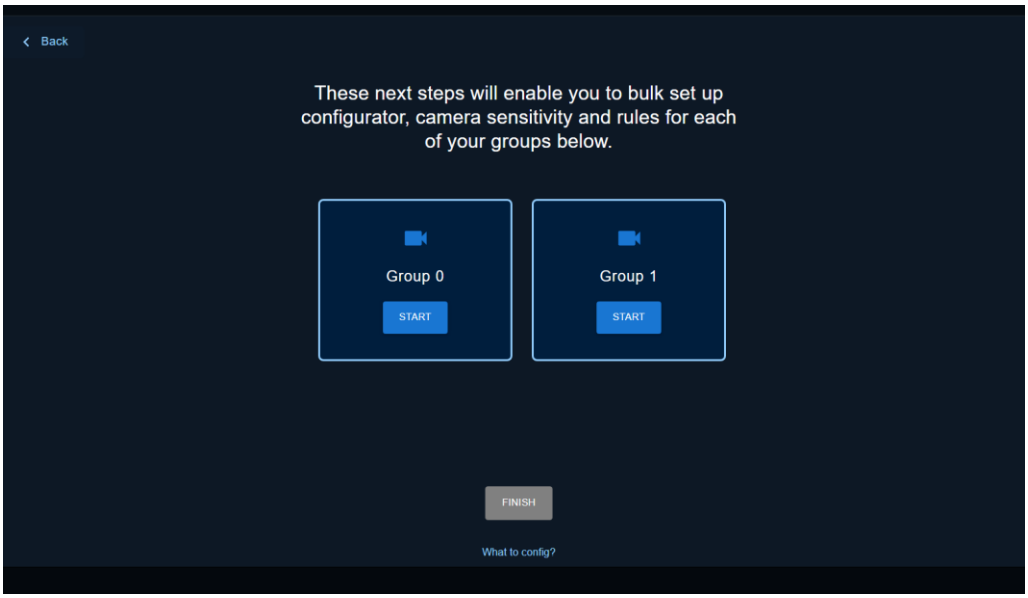
There is a tutorial video to show users how to create custom schedules. Simply click on **"Watch Tutorial"** to bring up the video widget. Users can **"Add new schedule"**, hover and press on time block to highlight desired slots. Clicking on the name of the schedule allows users to rename it. Users can create as many schedules as they like to fully customize the whole week of operation.



After finishing the custom scheduling configuration, use mouse to click to edge areas of the configuration page to return to the wizard.

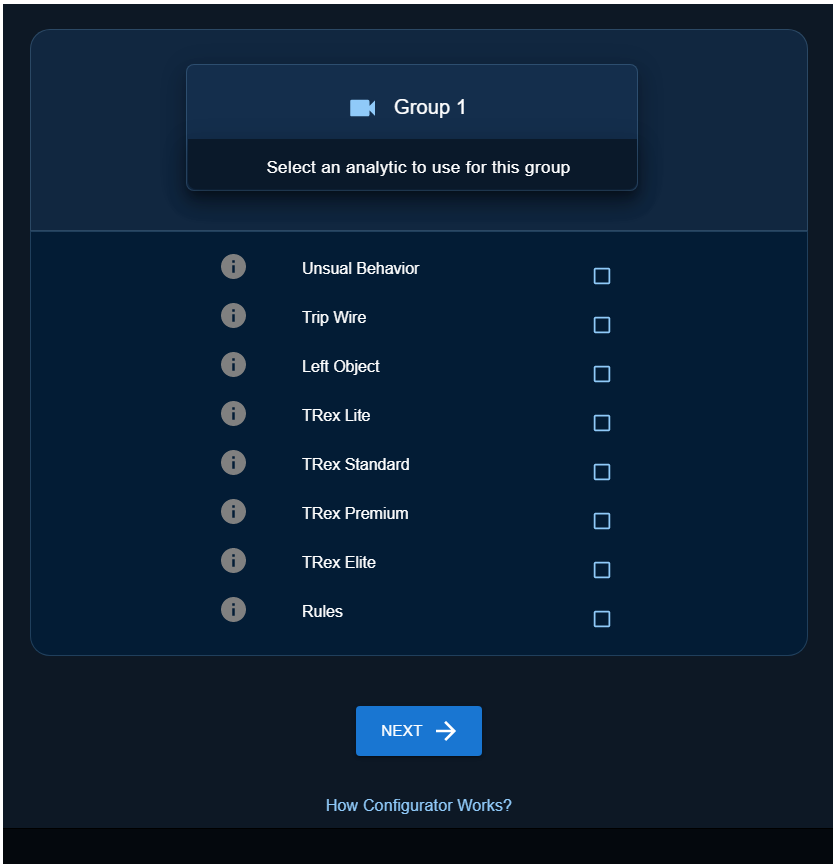


5.5 Group Configuration

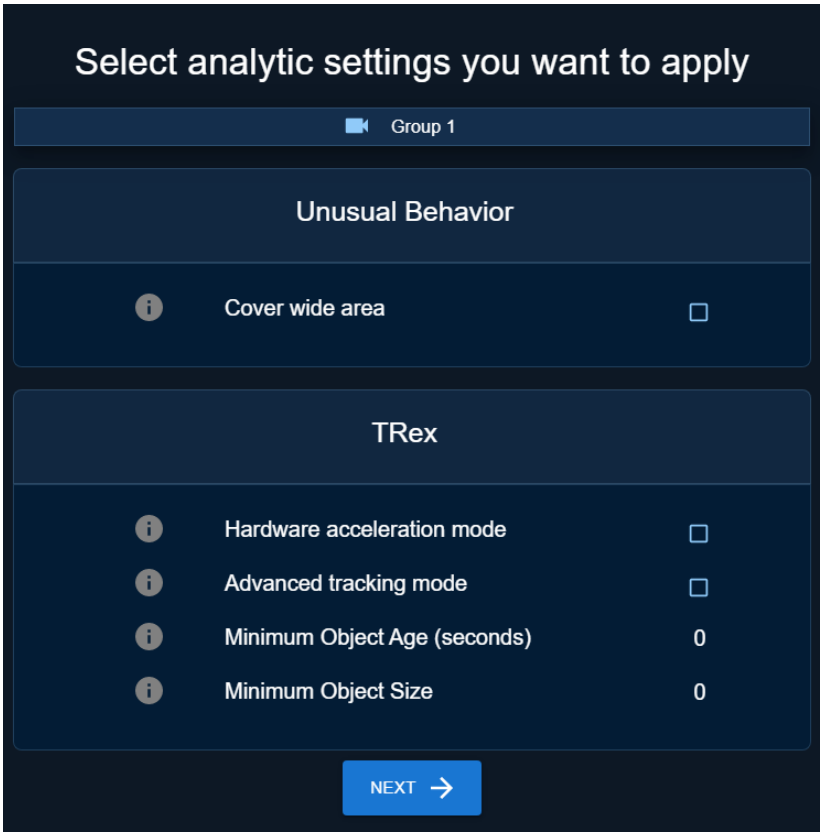


Once schedules are created/set up, users now can start to configure their cameras in groups. Only when all the groups are fully configured then users can finish the wizard.

Once a group is chosen to be configured, the next step is to select the analytics users want to include for this group.



Depending on the options that users select at this stage, there would be extra settings presented in the next step.

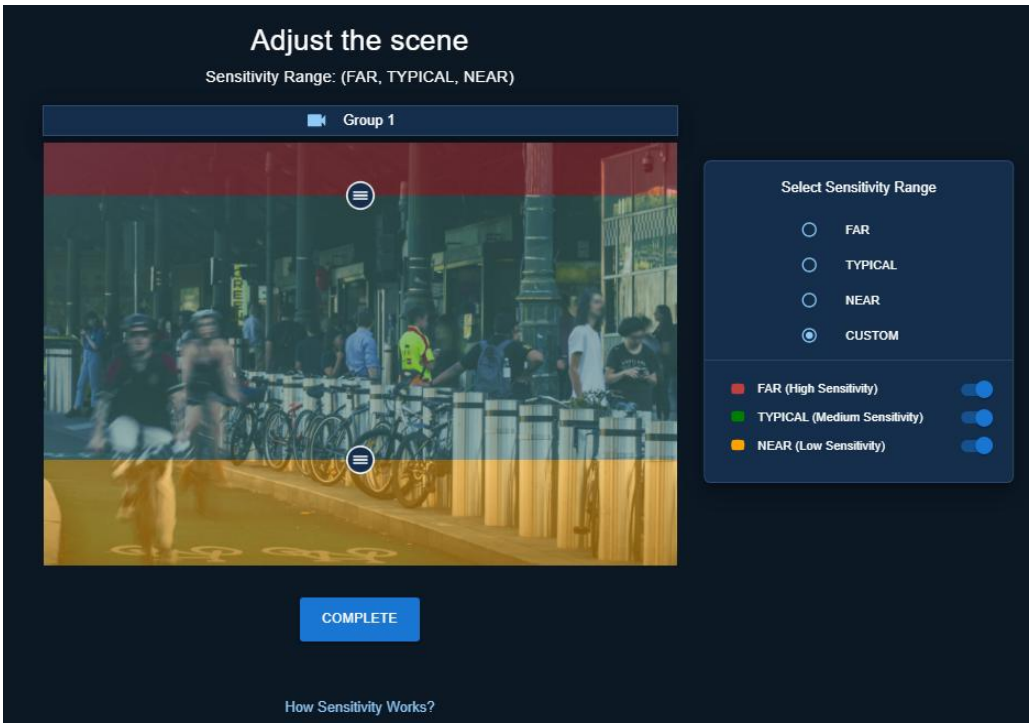


If users select either Unusual Behaviour or any of the TRex options, the next page will allow them to further customise these analytic settings. This menu has the similar interaction with previous pages when clicking on numbers allows users to input their desired value.

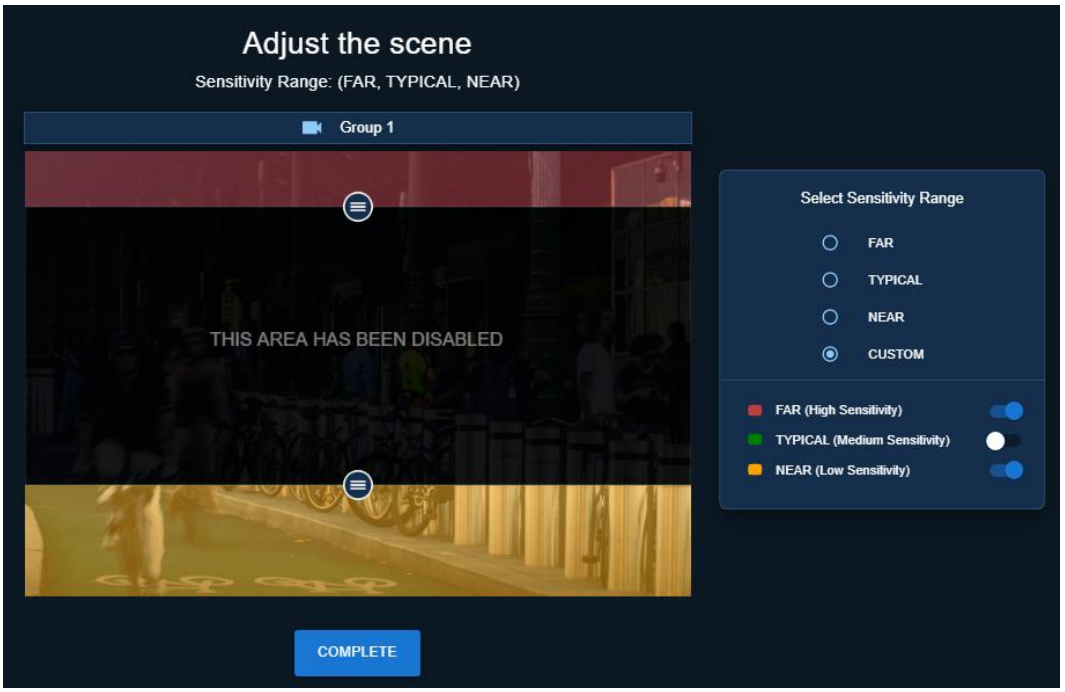
5.6 Group Sensitivity

Once finalising the analytic options, the next stage of the wizard is for users to customise their sensitivity levels of the camera view. These sensitivity settings will only be applied to the analytic modes selected in the previous stage of the Wizard.

There are three different presets for sensitivity under **Custom**, ranging from **FAR** (High Sensitivity), **TYPICAL** (Medium Sensitivity) and **NEAR** (Low Sensitivity). Users can adjust the range of sensitivity by dragging the dividers on the scene. There is a video tutorial included when users first enter this settings page. Alternatively, users can choose to set the whole scene to Far, Typical or Near, by selecting the option accordingly. These settings will help to define the depth of view of the cameras, which in turn affects further advanced settings.

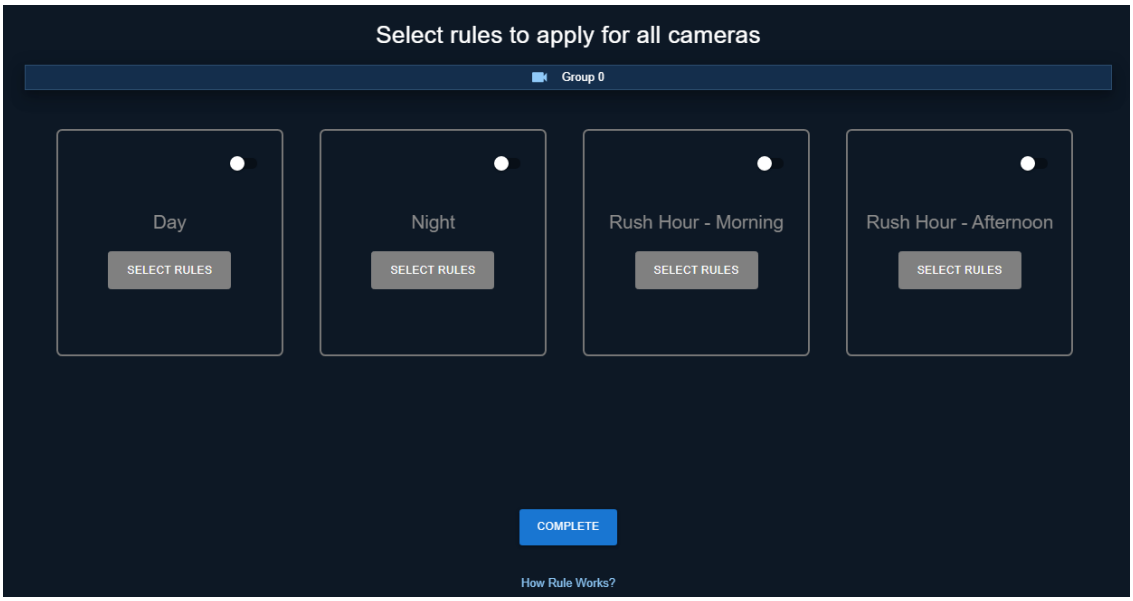


Users also have the option to turn off the sensitivity for a certain portion of the scene. To do this simply switch off the desired range. The example below shows that the middle of the scene is disabled by switching off the TYPICAL range.



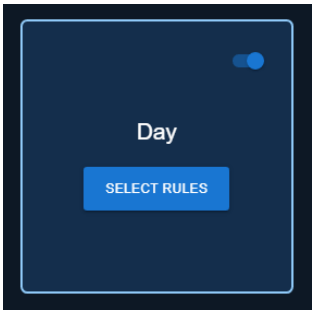
5.7 Group Rules

If users select Rules option within the Analytic Feature selection, the next page will allow them to further customize the classification rule applied for the current camera group.



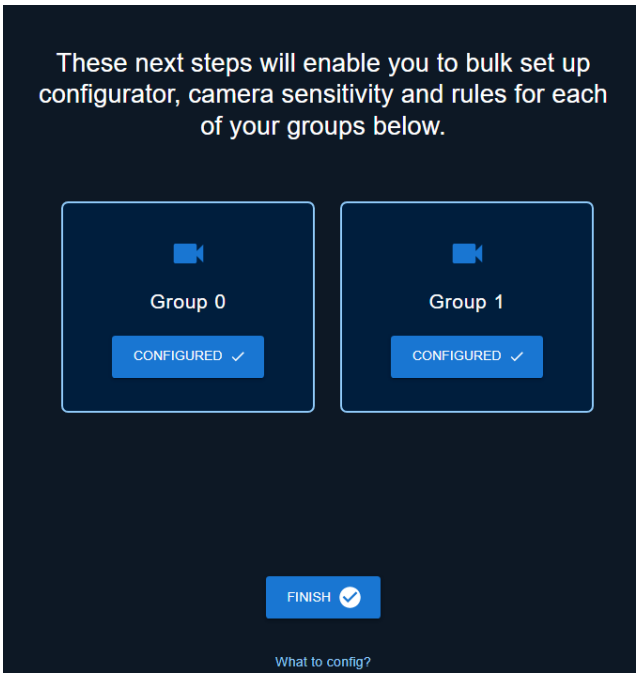
Based on users' previous settings of time schedules, each schedule will have its own panel displayed on this Rules menu. The example above outlines the initial state of the Rules menu when users select the **Typical** presets for time schedules.

All rule panels initially are disabled. If a schedule remains disabled, no classification rule will be applied within its time periods. Users can choose to enable the panels using the switches on the top right corner of each panel. Once turned on, users have the option to select which specific rules applied within that schedule. Click on **"Select Rules"** to start customising the rules for a schedule.



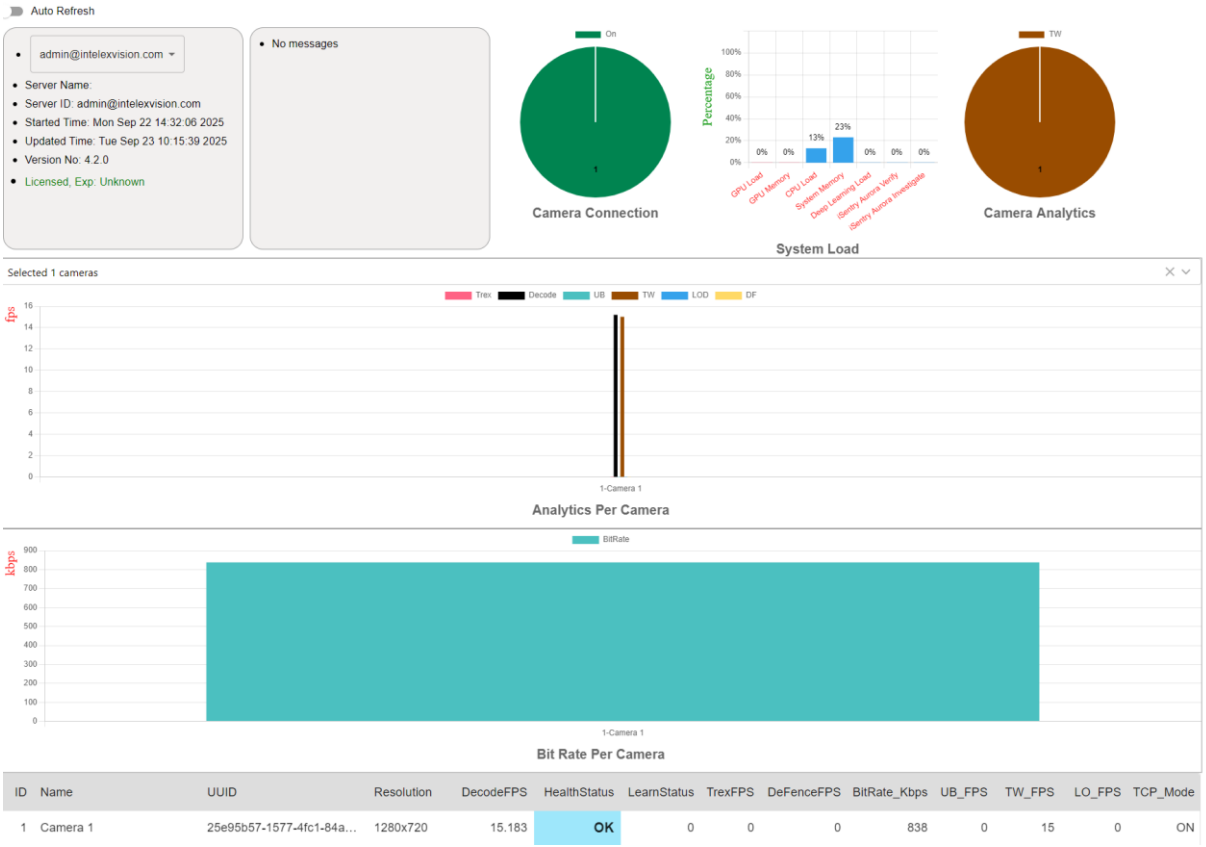
Users can select which preset classification rules to be applied for this time schedule from a list. This list is composed of either the default set of classification rules or the current set of classification rules customised by users under Advanced Settings Mode. If users want to add more rules to be selected within a schedule, they need to customize their own using the Rules tab, within Advance Settings Mode.

Once Rules is configured, the **Next** button will take the user back to the display of all groups to be configured. Only once all groups are **configured,** users can finish the Wizard.



6 Monitor Website

This section covers the performance monitoring of **Sentry Firefly**. The user can open the monitor website by going to the URL <IP FF server>:<port>/monitor (e.g. http://localhost:8123/monitor) and it will be presented with:



ID	Name	UUID	Resolution	DecodeFPS	HealthStatus	LearnStatus	TrexFPS	DeFenceFPS	BitRate_Kbps	UB_FPS	TW_FPS	LO_FPS	TCP_Mode
1	Camera 1	25e95b57-1577-4fc1-84a...	1280x720	15.183	OK	0	0	0	838	0	15	0	ON

There are several panels where you can find different information about the performance of the system and its cameras such as FPS or resolution (see image above).

Information about Deep learning load, Aurora Verify and Investigate loads are displayed in the System Load panel.

Any overflow error will be displayed in the second grey panel. If no overflow error a “no messages is displayed”.

7 Troubleshooting and Common Issues

7.1 Support Information

If you need Technical Support with Intelex Vision systems, please write an email to customerservices@intelexvision.com and we will certainly help to solve the problem.

8 Appendices

8.1 Glossary

UB	Unusual Behaviour
LO	Left Object
OM	Object Motion
TREX	Threat Detection and Extraction
DL	Deep Learning
GPU	Graphics Processing Unit
CPU	Central Processing Unit
SOP	Standard Operating Procedure
ROI	Region of interest
UI	User interface
LVM	Large Vision Model

8.2 Related Resources

Visit https://intelexvision.com for more information.