iSentry Web Client

User Manual

Web Client

Version 2025R3

Oct 2025

Table of Contents

1. Introduction

This user manual will guide you through all the steps needed to make iSentry Web Client work.

1.1 Abbreviations, Acronyms and Definitions

URL	The address of a web page.
GUI	Graphical user interface
LPR	License plate recognition

2. Pre-requisites

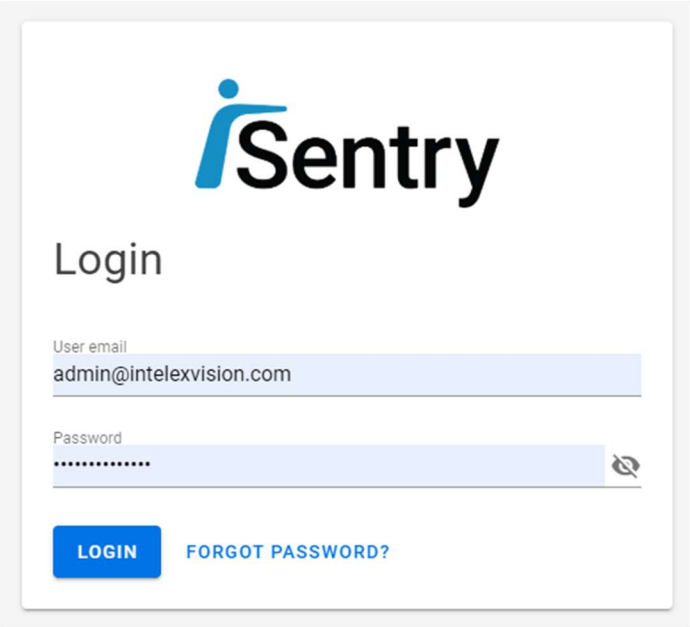
2.1 Deployment

A proper Web Client deployment should have been done previously by the technician. Check that the Web Client is up and running entering the URL provided in a web browser. If not please ensure that the Web Client has been properly deployed.

For example successfully going into:

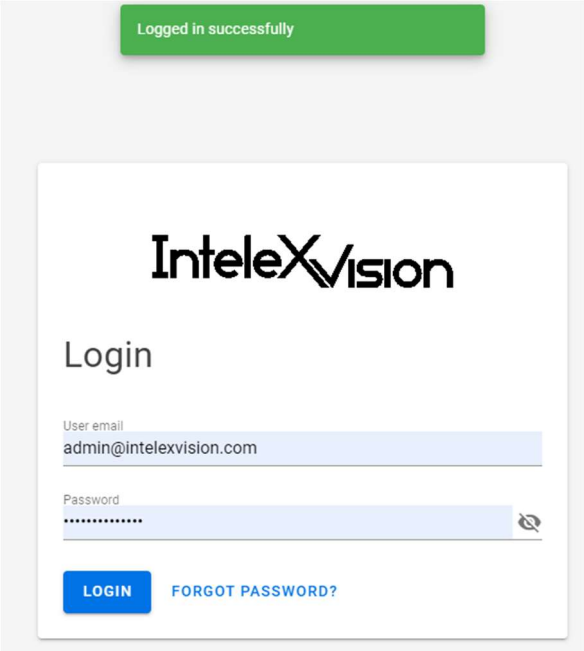
http://isentryclientdemo1.duckdns.org

shows the login screen below:



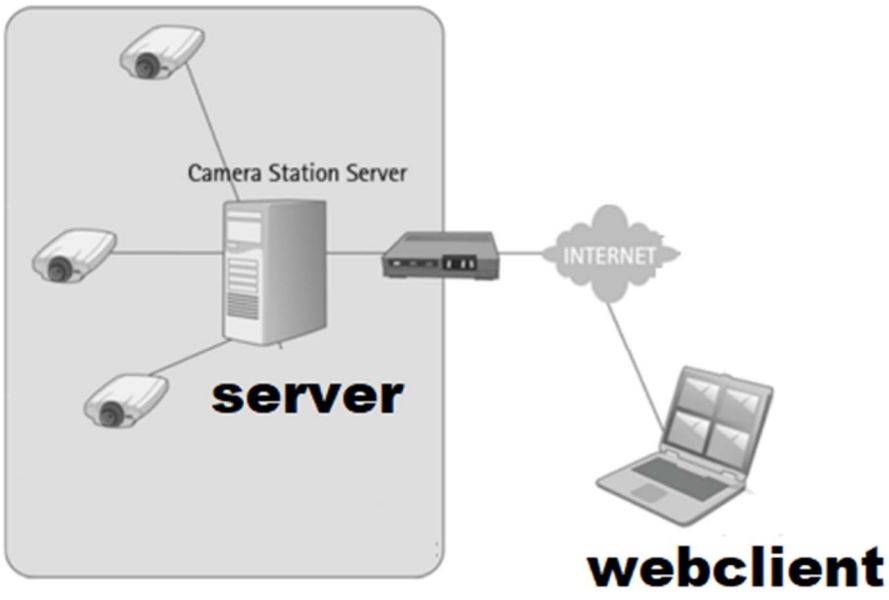
2.2 Credentials

In order to login into the Web Client you have been provided with an administrator **user email** and **password**, please enter those credentials to go into the main screen of the Web Client.

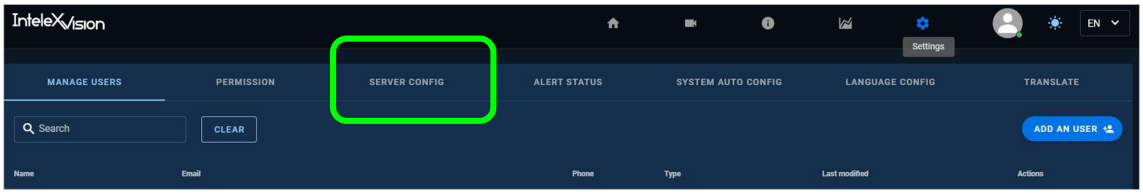


2.3 Pairing with an iSentry server

In order to receive alerts from a server with cameras a two-way pairing must be done, first add the server to the client, second add the client to the server.

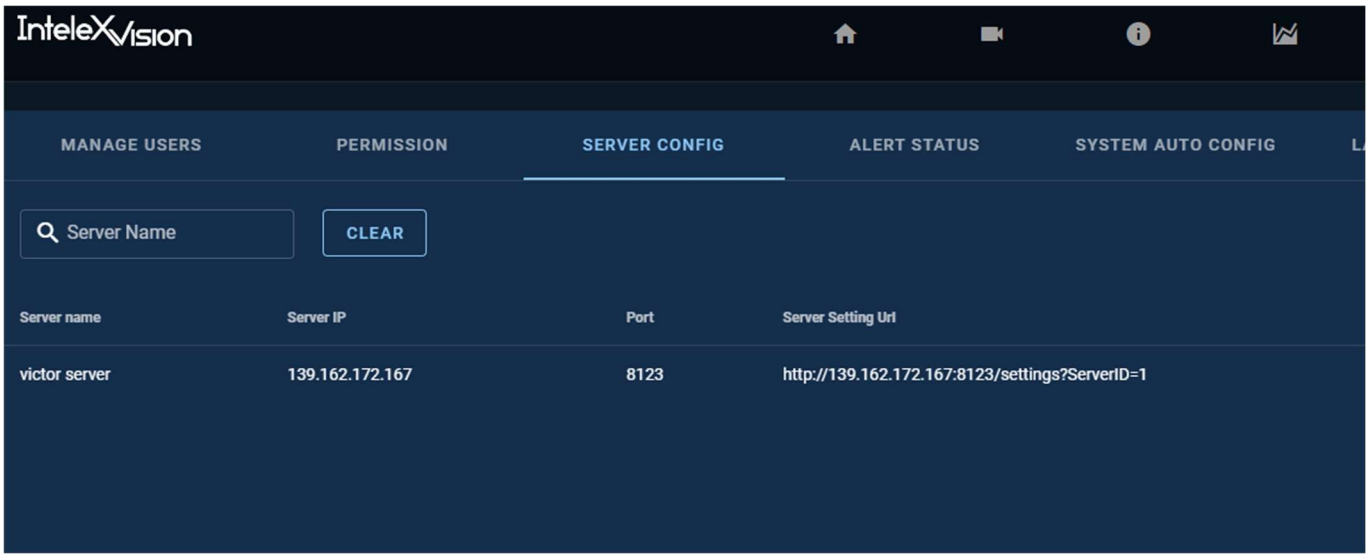


Adding the server to the Webclient is the first thing one should do (**before adding the webclient to the server**). Go to:

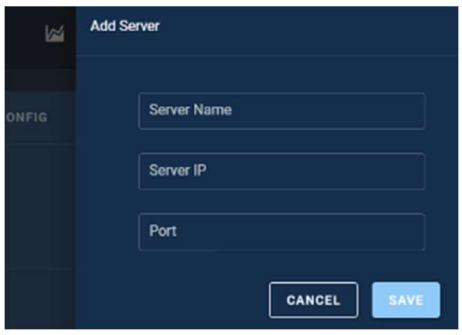


and press SERVER CONFIG in the image above.

Press the button Add Server from the image below in order to link the Webclient with an up and running iSentry Firefly:



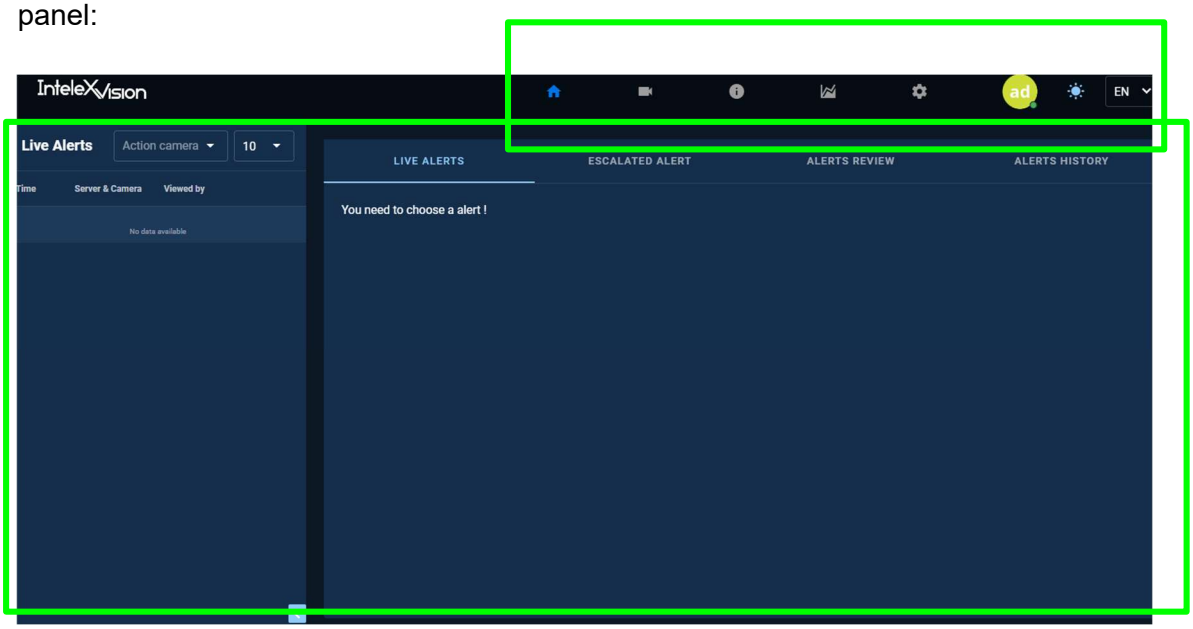
In the following screen, enter the details provided for Name, Server IP and Port. Do not forget to click Save.



Secondly add the Webclient to the iSentry Firefly (server) following the steps in the correspondent manual.

3 Interface

After successful login, the main screen of the Web Client is presented as a graphical user interface (GUI) separated into two main areas; upper menu buttons and the lower panel:



Button	Description
Dashboard	Data folder
Live Cameras	Access to your cameras
Reports	Collect information in a report style document
BI Tool	Business Intelligence charts
Settings	Settings menu. See Settings
User	Access to personal info
Change Mode	Go to dark mode or bright
Language selector	Change language

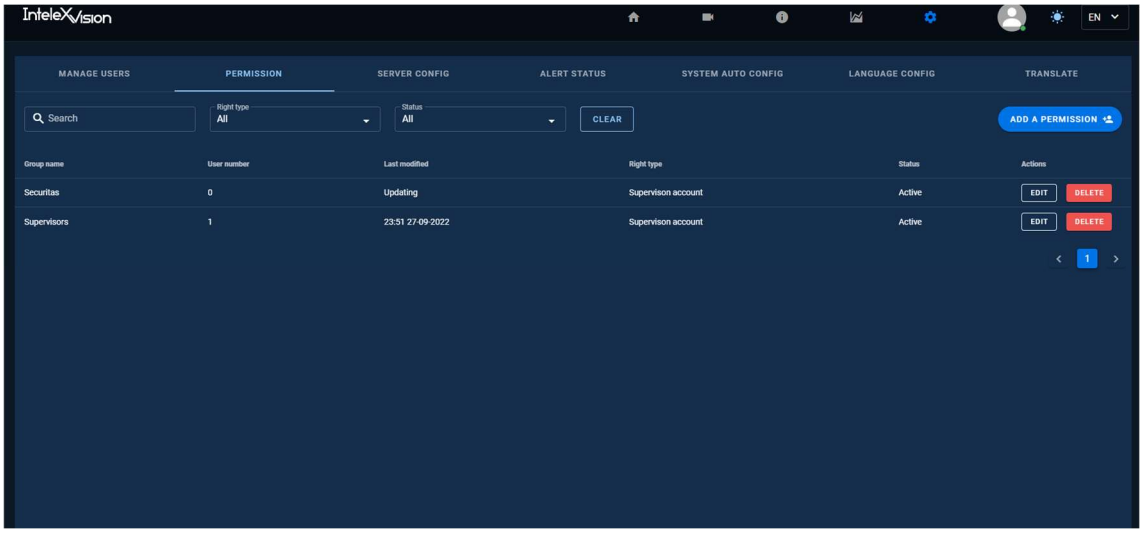
3.1 Settings

The options included in this menu are depicted in the following table:

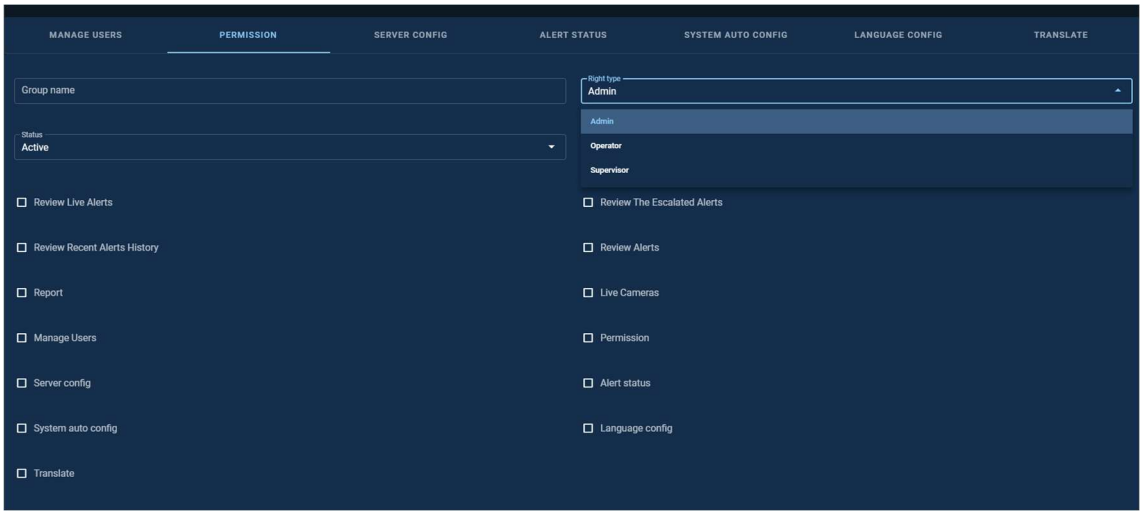
Menu	Description
Permission	Add, edit or delete permissions
Manage Users	Add, edit or delete users
Server Config	Allows you adding a server
Alert status	Allows you adding statuses
System Auto Config	Allows you entering auto config details
Language Config	Allows you changing language configuration
Translate	Allows you translating the interface
User Match Rule	Allows you to send emails to user matching a selected rule
Camera Config	Allows you to see the list of cameras, their alert count and last received alert. This way you can remove not used cameras.

3.1.1 Permission

First we need to provide rights for our user, so we click in add a permission:

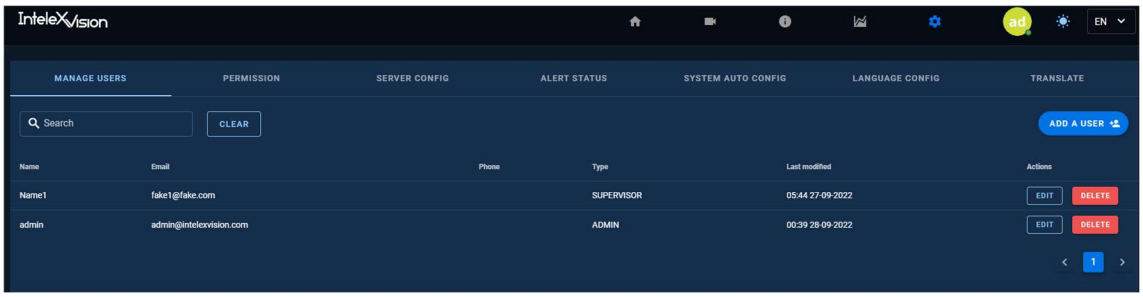


Provide rights that match your current organization, for example Operator (security personnel will fall in this category) and Admin (IT personnel trained).

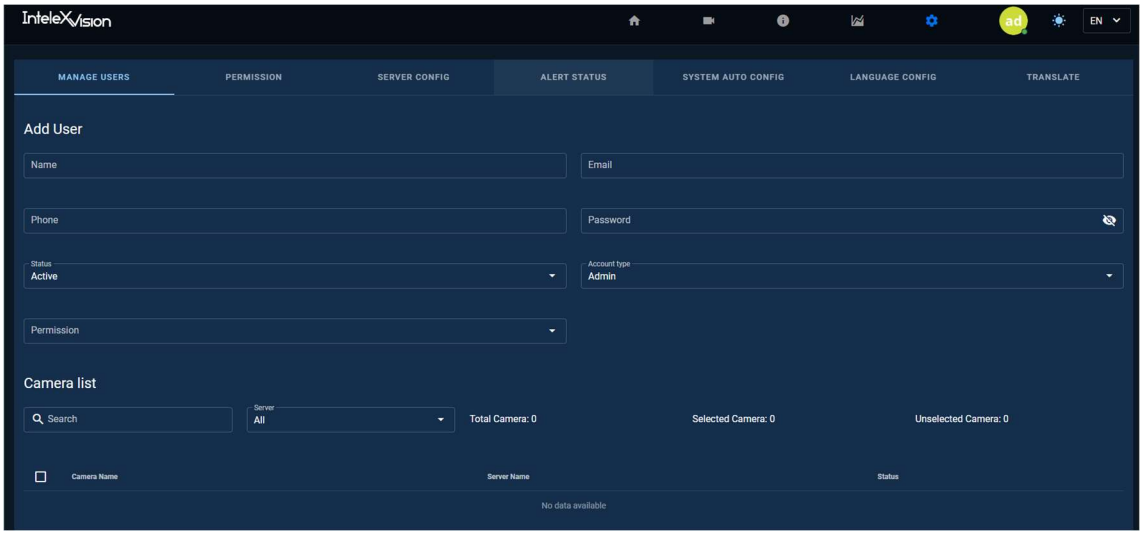


3.1.2 Manage users

After setting permissions you can add users in the next screen press add user:

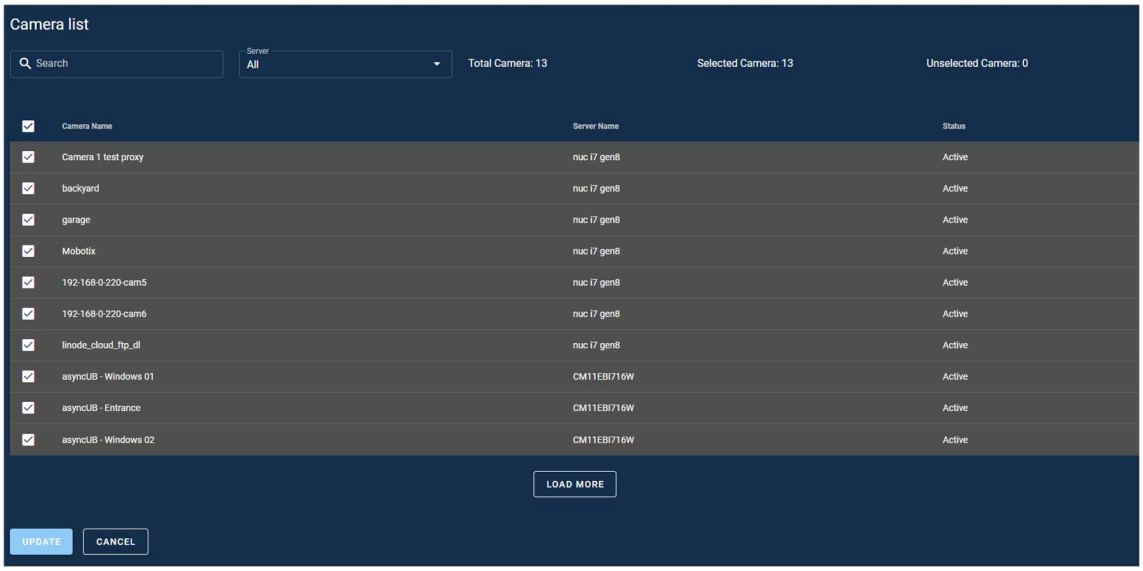


Enter the details such as name, email and a minimum 6 characters password. It is important to assign this new user a Permission from the previous step.



In the Camera List you can add cameras, but remember that if you have not set the server yet, it will be empty. You can come back after adding the server and assign the cameras.

After setting up the server, a list of cameras is shown under the Manage Users menu. Pick from the list and click update:

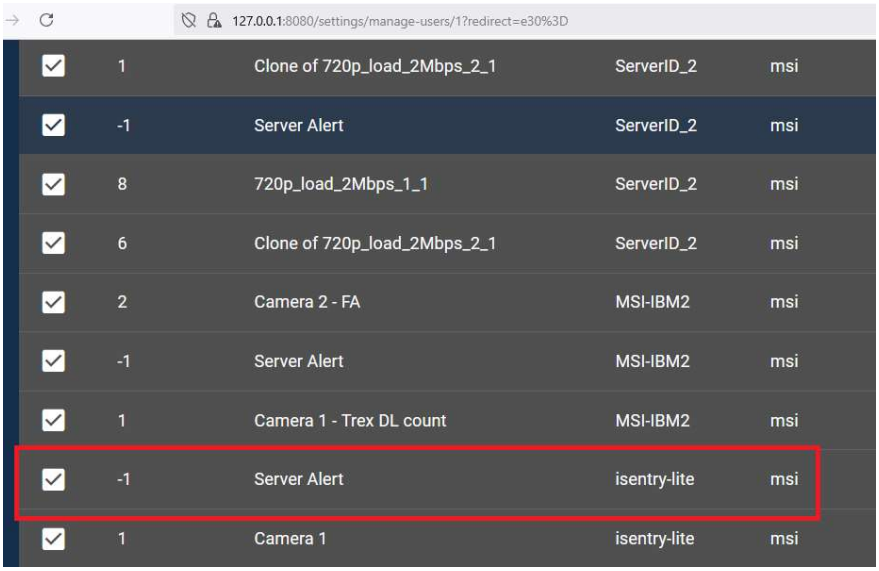


This provides a wide variety of possible combinations by assigning cameras to different users.

Note: from version 2025R2, there is an extra camera called Server Alert camera (id=-1) to receive global alerts e.g. License Request failure.

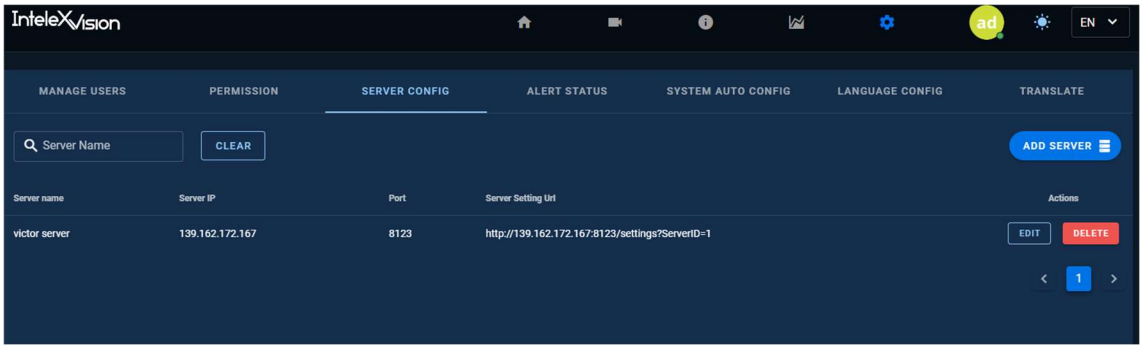
In version 2025R3 the list of global alerts has been increased to the following:

- LLSmain failed
- LLSbackup failed
- Unoptimized DL
- DL overload
- Aurora overload

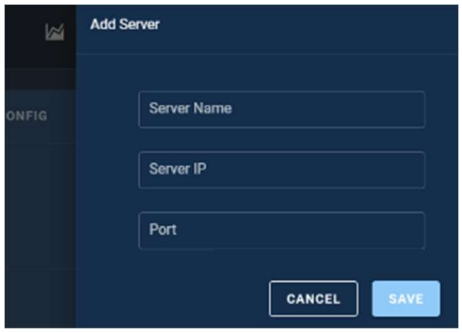


3.1.3 Server Config

Press the button Add Server from the image below in order to link the Webclient with an up and running iSentry Firefly:



In the following screen, enter the details provided for Name, Server IP and Port. Do not forget to click Save.



3.1.4 System auto config

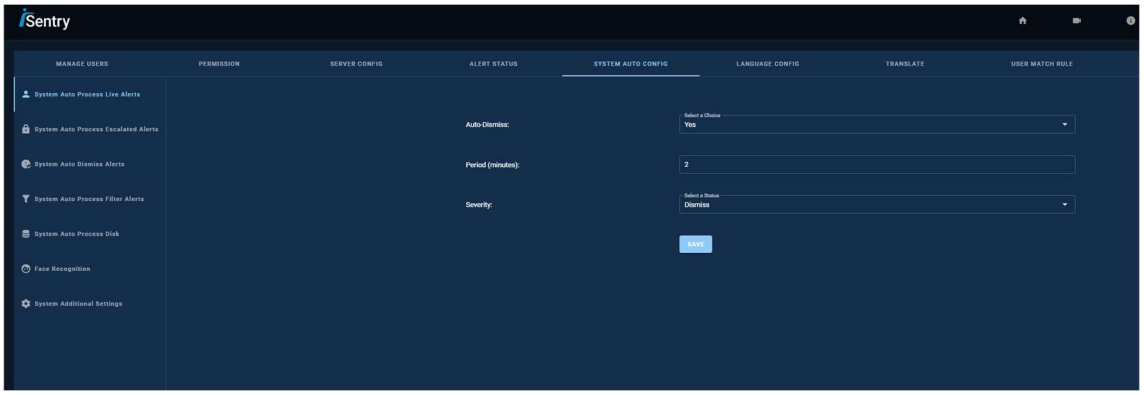
In this menu you can find the following options:

Menu	Description
System Auto Process Live Alerts	Select how the system will automatically deal with Live Alerts
System Auto Process Escalated Alerts	Select how the system will automatically deal with Escalated
System Auto Process Filter Alerts	Select how the system will automatically deal with Filter Alerts
System Auto Process Disk	Select the quota for disk management and days old before for deletion.

3.1.4.1 System Auto Process Live Alerts

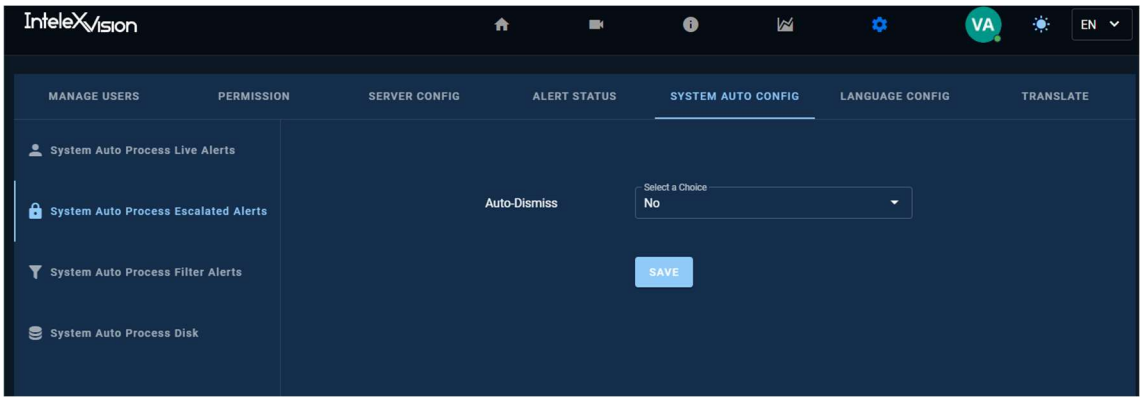
By setting this value we have more control of the detected alerts. Select YES and enter the value for the period of minutes before Auto-dismiss and the Alert Severity level.

For example, it is a good practice to Auto-dismiss after 2 minutes alerts with a Severity of “Dismiss”.

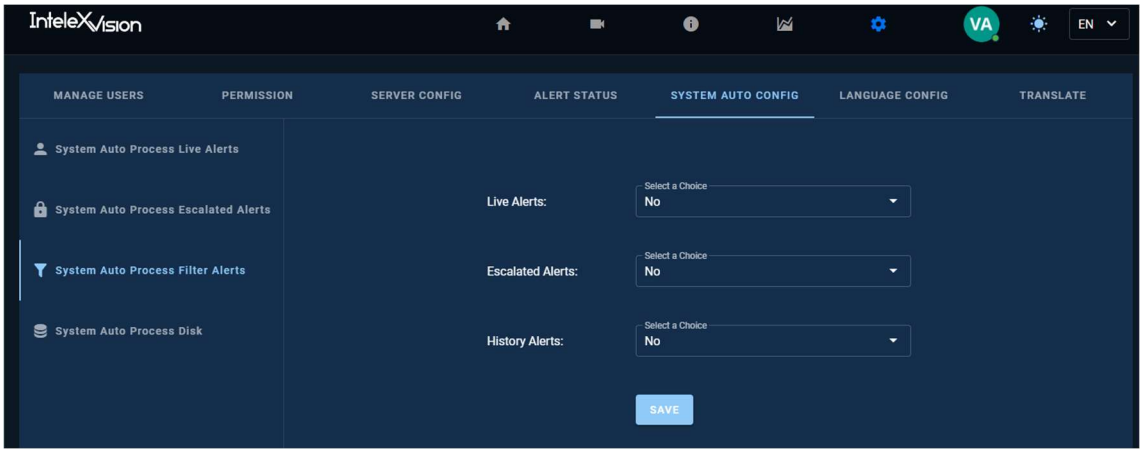


3.1.4.2 System Auto Process Escalated Alerts

By default is set to No, the user can decide whether or not the system takes care of the Escalated Alerts. When entering YES the system will ask for a period of time in minutes before dismissing the Escalated Alert.



3.1.4.3 System Auto Process Filter Alerts



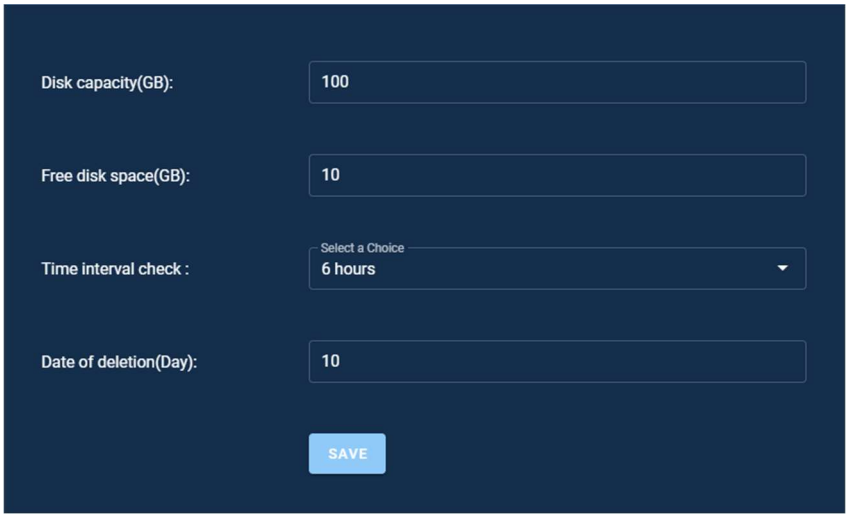
3.1.4.4 System Auto Process Disk

Set how much disk storage the Web Client can use as events are continuously arriving and filling up storage. The Web Client must be configured to know how it should delete the old events.

⚠ Not setting this up might fill up your local drive and make the Web Client irresponsive ⚠

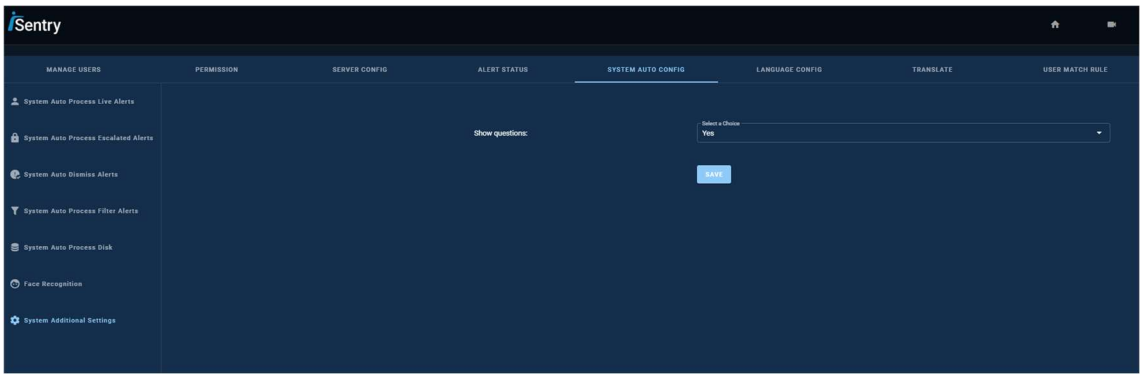
The recommended values depend on your current scenario but something like 10% of the disk capacity should remain free.

Date of deletion(Day): How many days do you want to keep. Please note this depends on the Disk capacity and free disk space. If you enter 30 and it is 1st of September you will delete 2nd of August (cause August has 31 days).

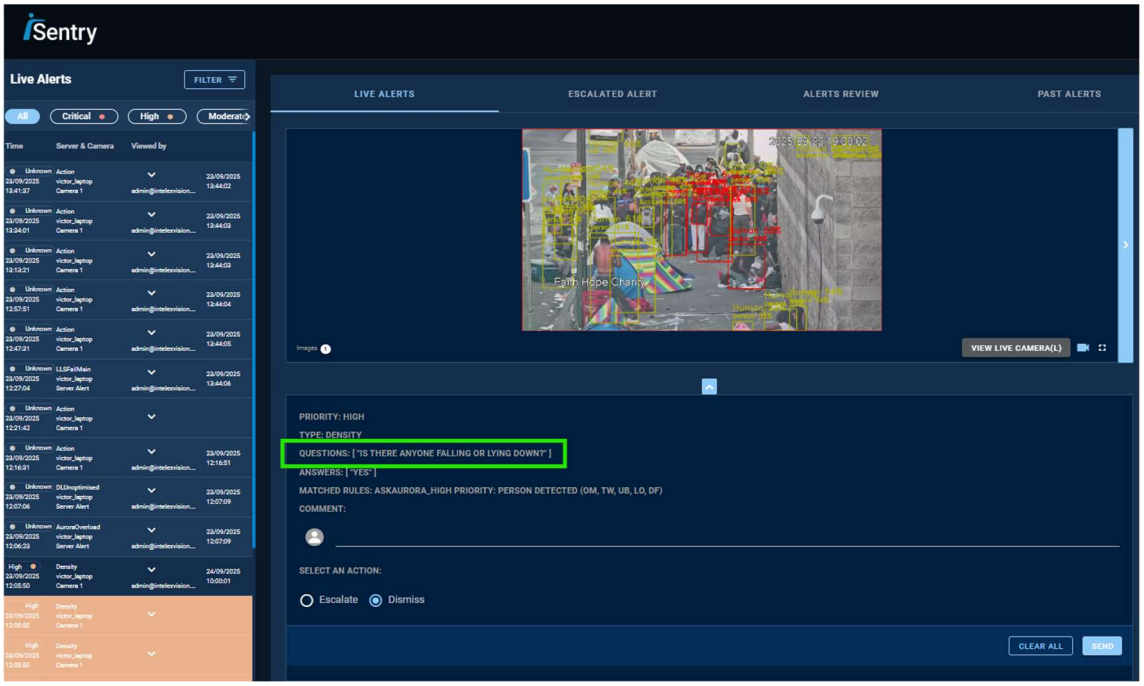


3.1.4.5 System additional settings

Adjust this value to show in the alert view the question asked to Aurora.



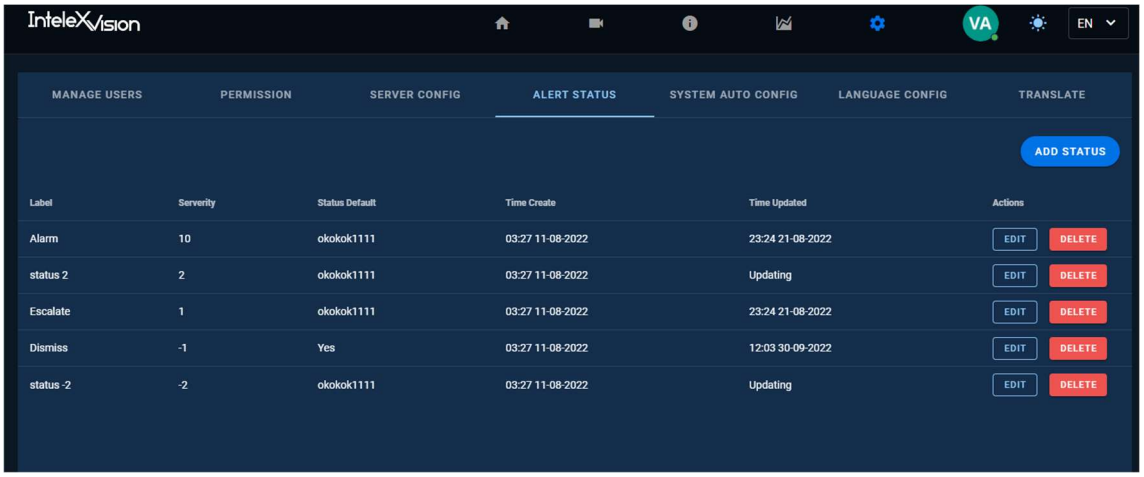
When **yes** which is the default value you will see the question as in below example **Questions: ["Is there anyone falling or lying down?"]:**



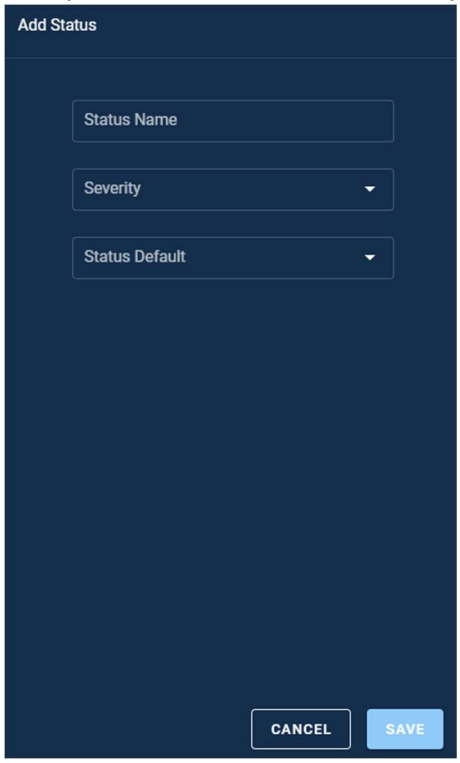
This way you can hide/unhide the question from the Webclient.

3.1.5 Alert Status

From this menu you can manage your alert statuses. Adding a new one, edit or delete the current ones. Roles such as Escalate, Dismiss or Alert are highly recommended.

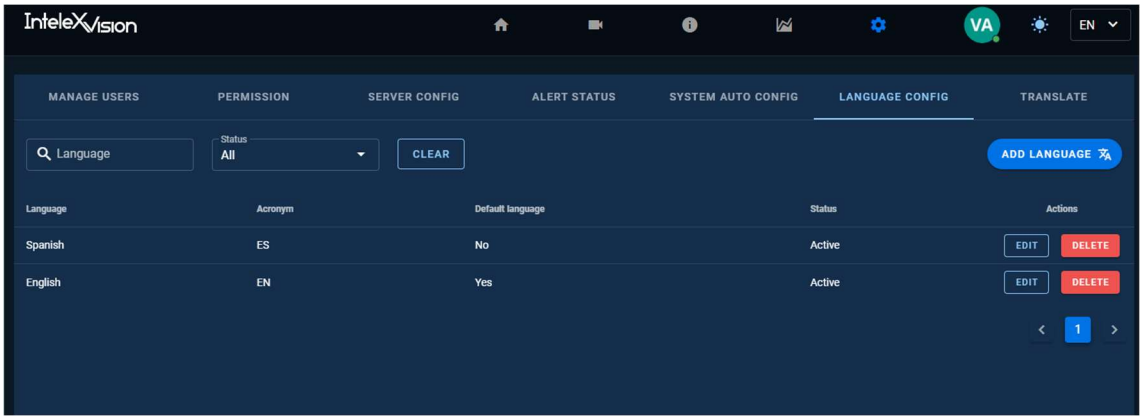


Adding a new status involves providing a name, level of severity (10 higher, -10 lowest) and whether or not the status has a default behavior. The severity plays an important role when moving alerts to different views, high priority moves the alert to Escalated in the Dashboard while low priority moves them to Alerts History in the Dashboard.

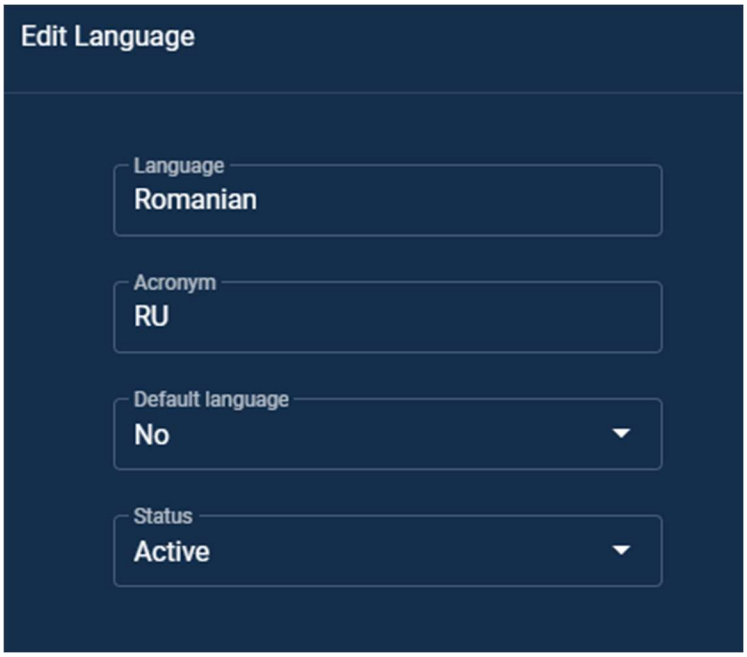


3.1.6 Language config

The user can add several languages. By selecting the Add Language option, you can enter a new language easily, think of them like word containers. Provide a Language name, Acronym and decide if you want to make it your default language. The user can now start translating any word seen on the screen.



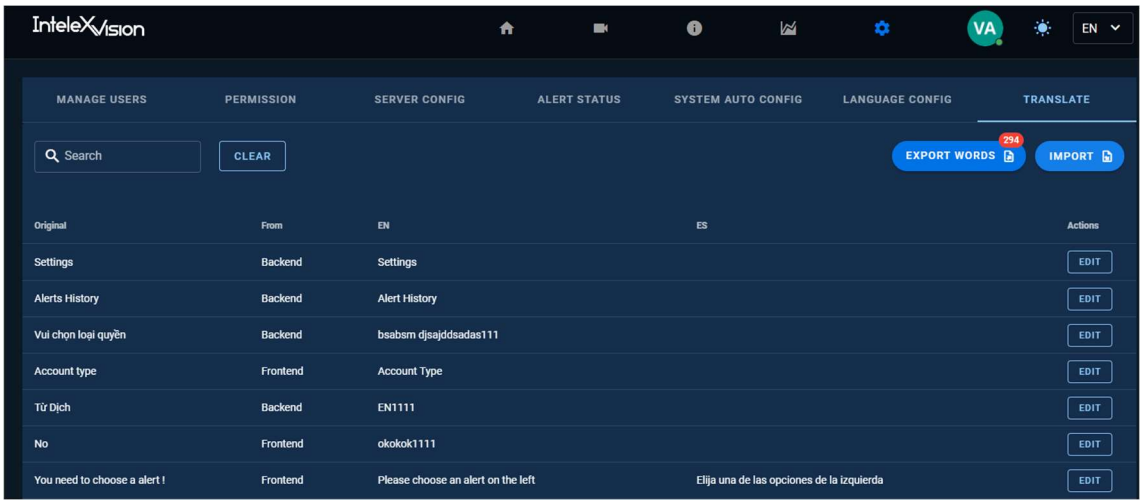
For example we'd like to create a new language, let's go with Romanian:



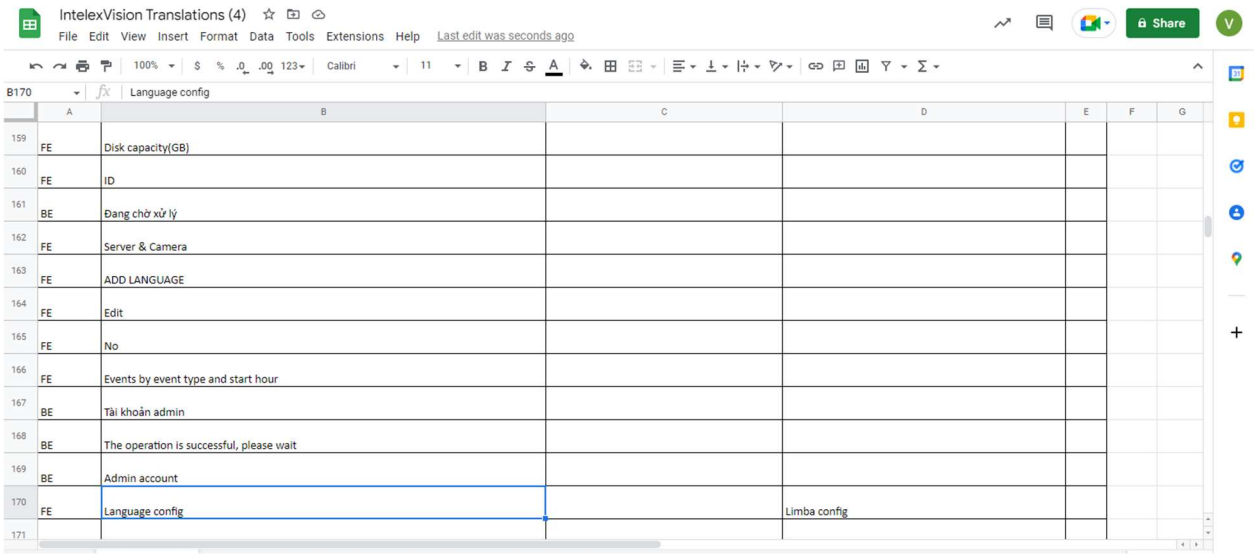
Now go to the next section Translate to enter specific translations for specific words. In this example we will translate the word "Language" from English to the Romanian equivalent which is "Limba".

3.1.7 Translate

Click Export Words and open the .xls file with an Excel compatible program, for example Google Spreadsheets. Find the word “Language” and translate it. In our example we are translating from English to Romanian.



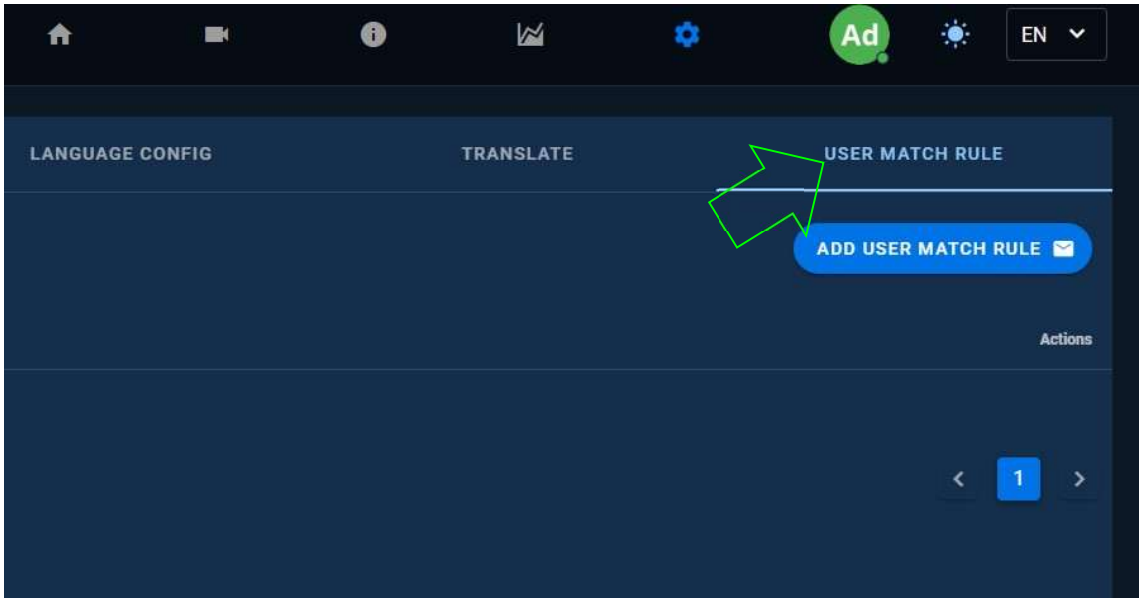
Once finished, click save and proceed with Import, you will see the results after

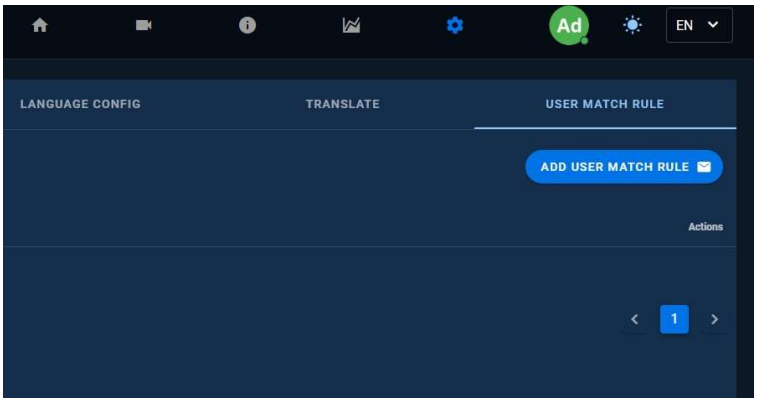


refreshing your view in your browser.

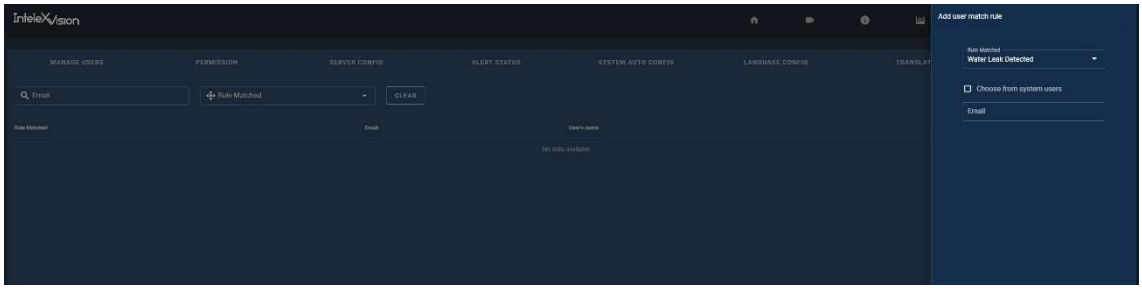
3.1.8 User Match Rule

Allows the user to send emails or Telegram messages to users when there is a match in the rules selected and the alert. Administrative permissions are needed to apply this.



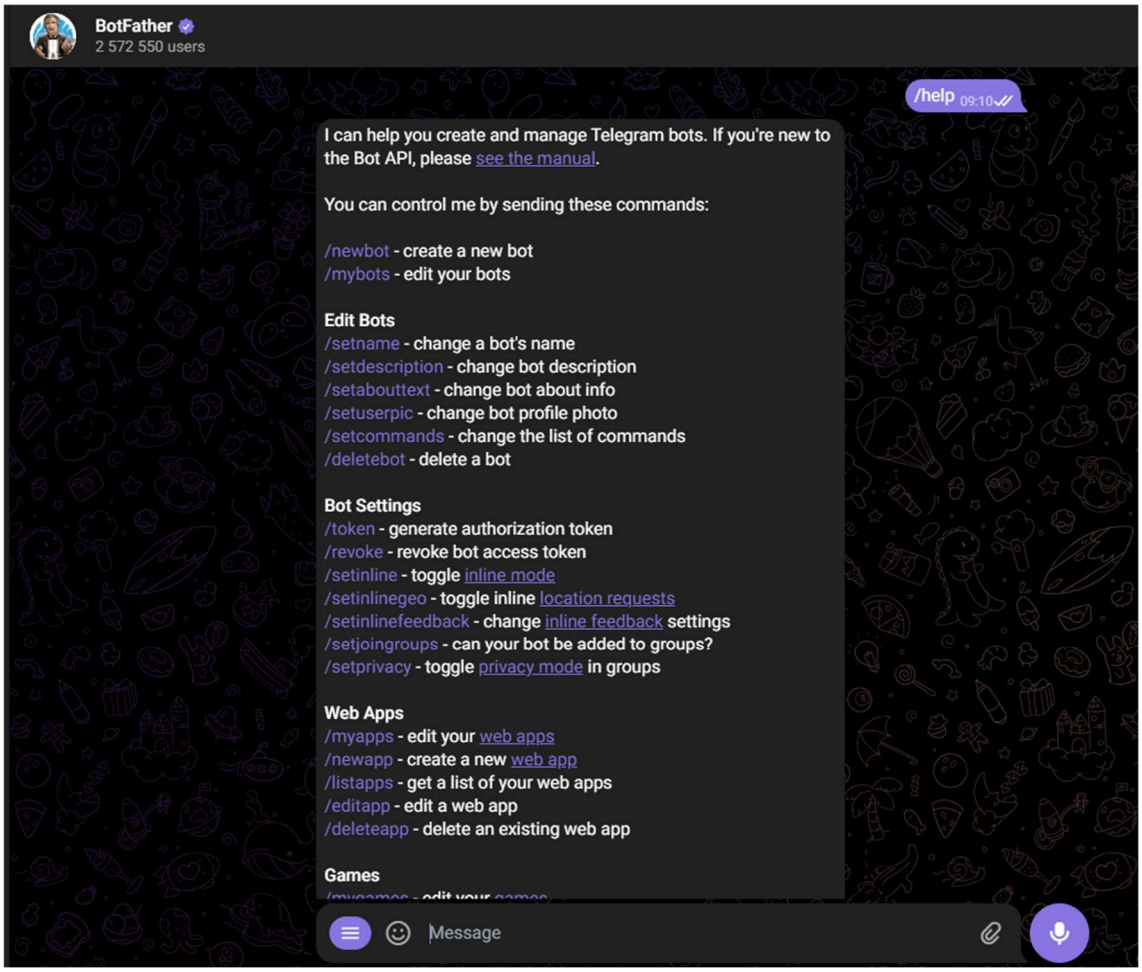


From the menu we select the rule we want to act as a trigger for the email, also select the email from the system list of users, or enter a custom one. Please be advised that this can cause spam when the Rule is highly triggered (like cars in highway with TREX).

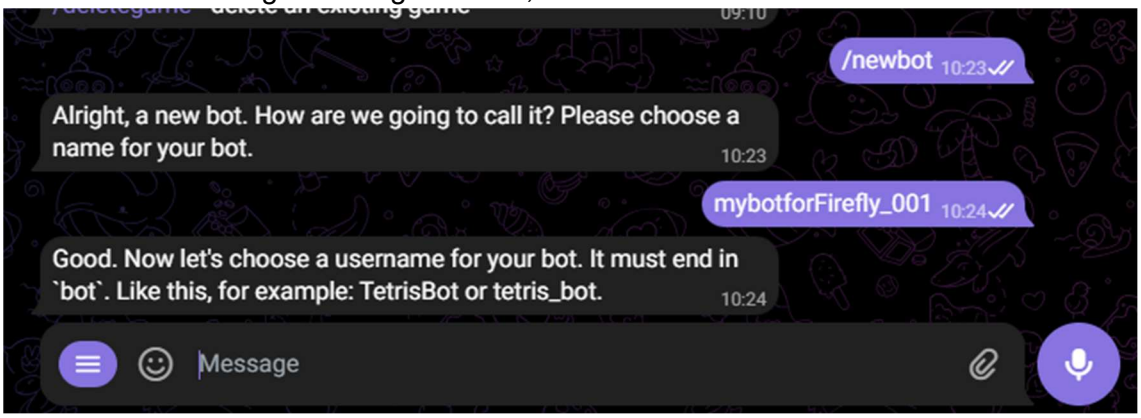


3.1.8.1 Telegram

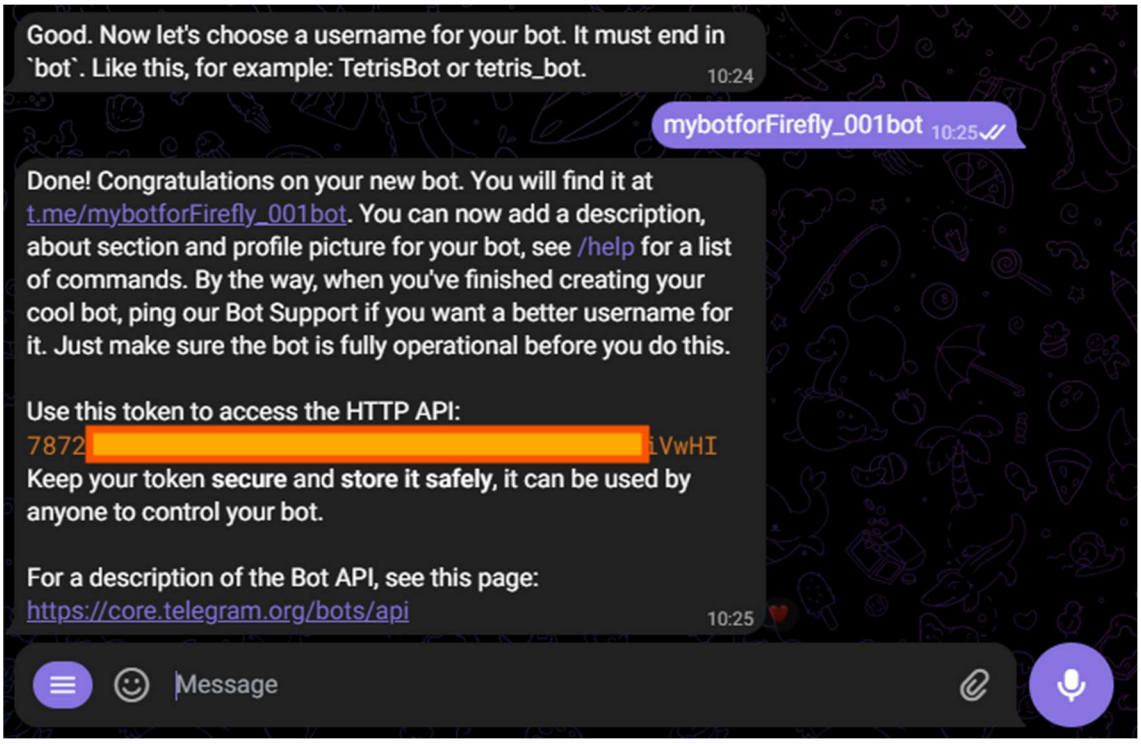
For configuring Telegram you will need first to have Telegram account, use this feature for a very important rule to be sent to a supervisor. Follow this steps:
Install telegram then install @BotFather, type /help to see the list of available commands, we will use /newbot



Create a bot in Telegram using: /newbot, below we created one:

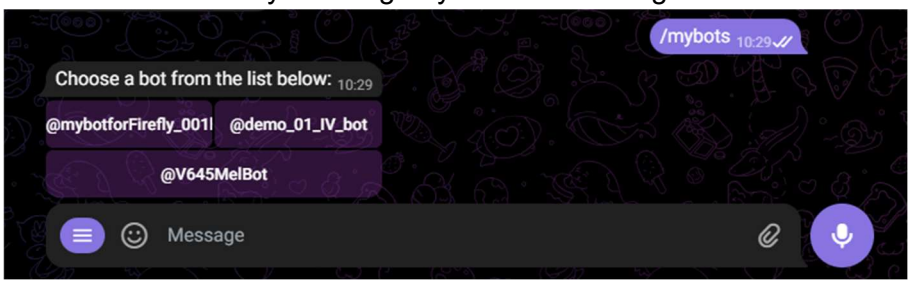


Give it a name having into account that it must end with ‘bot’.

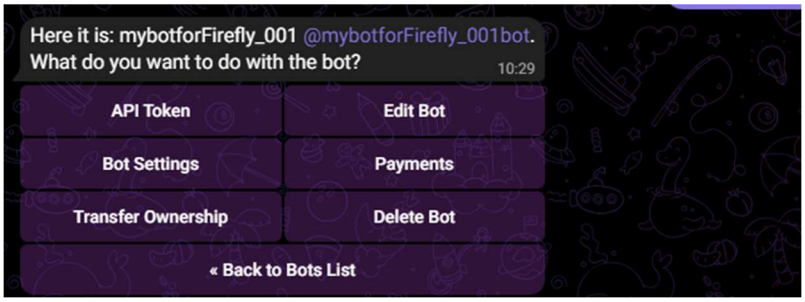


Get the api token (8196639422:AAF....) and do not share it as it is sensitive.
We click on "API Token" we still can copy anytime we want.
Now set two commands for your bot, one to subscribe to the rule and another to mute it (or unsubscribe)

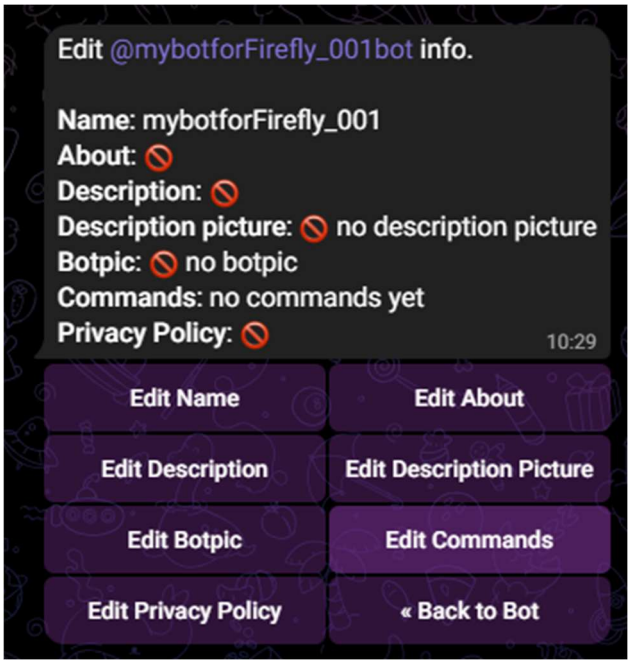
Select our created bot by entering /mybots and clicking on it.



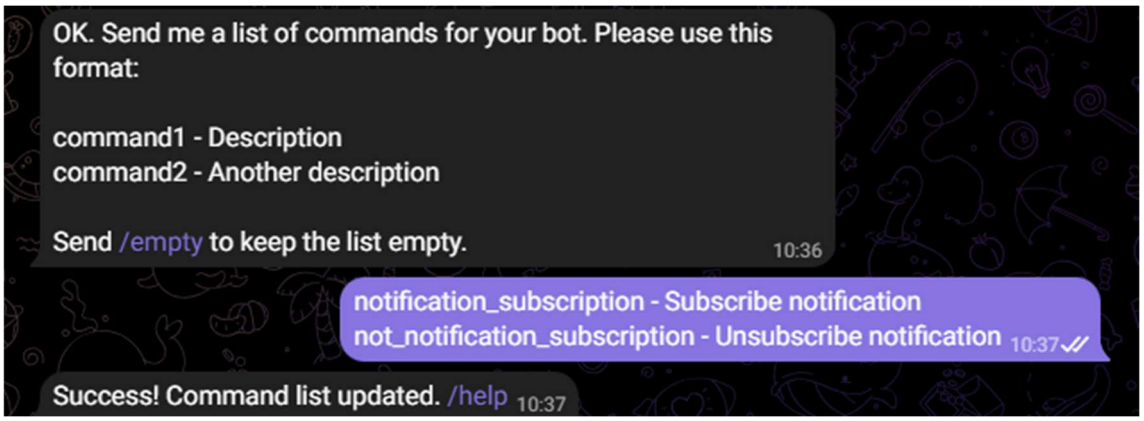
Then click on edit bot:



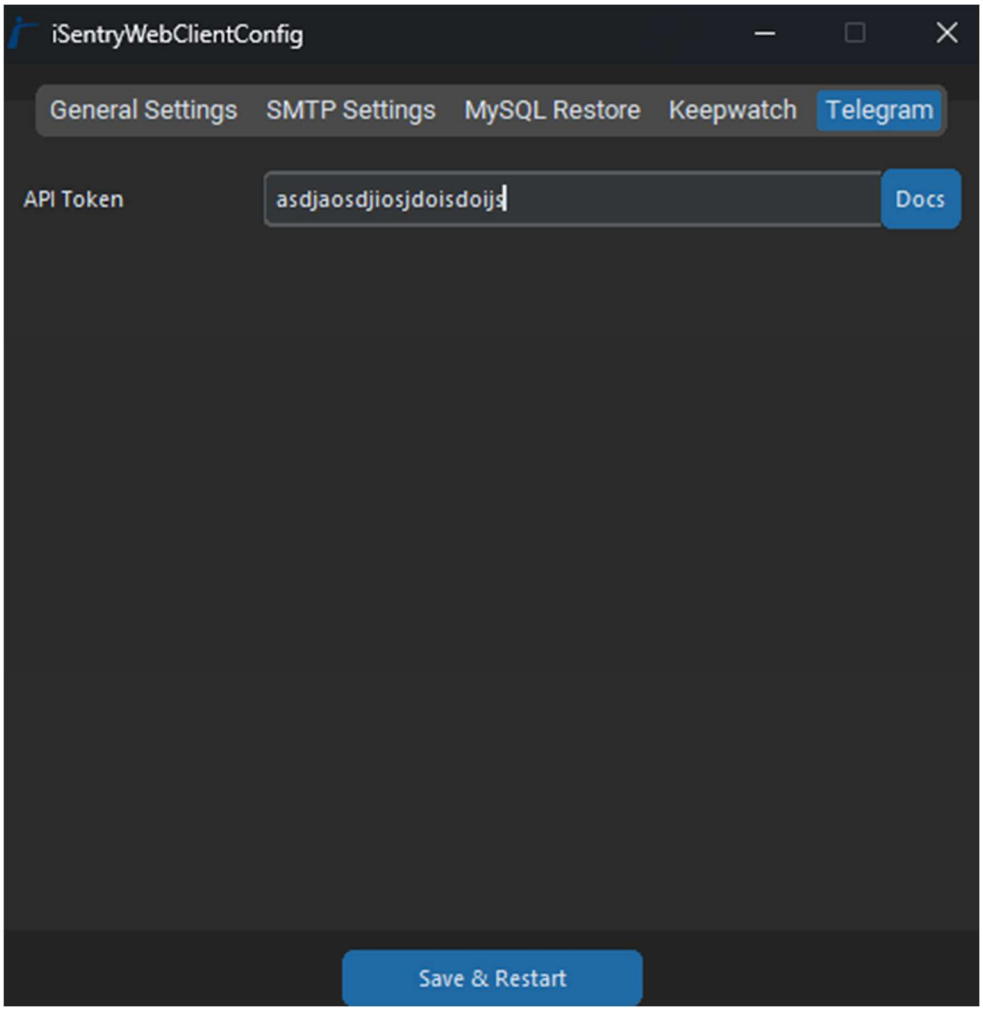
And then edit commands:



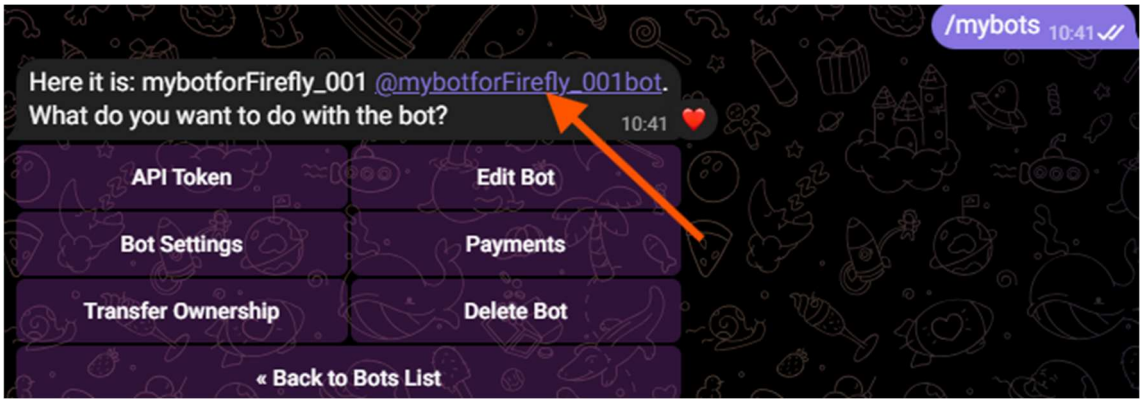
Enter: "notification_subscription - Subscribe notification
not_notification_subscription - Unsubscribe notification" (copy whole text as it will enter the 2 commands), hit enter to confirm our commands.



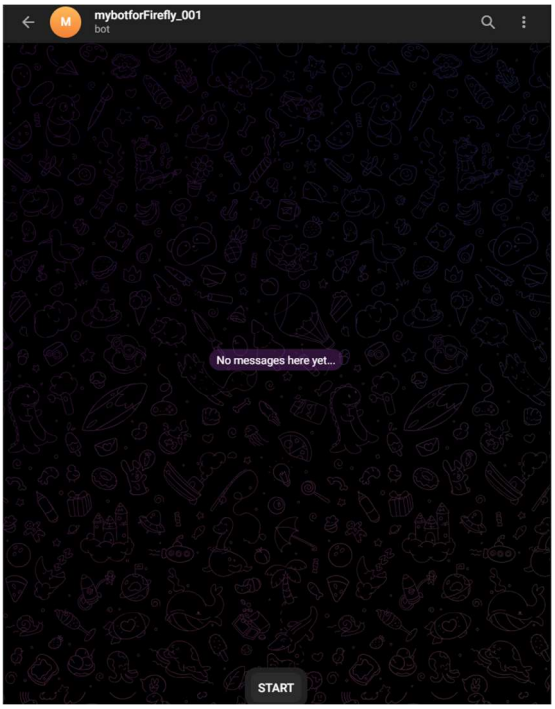
Now open your isentryWebClientConfig by pressing windows key and typing it.

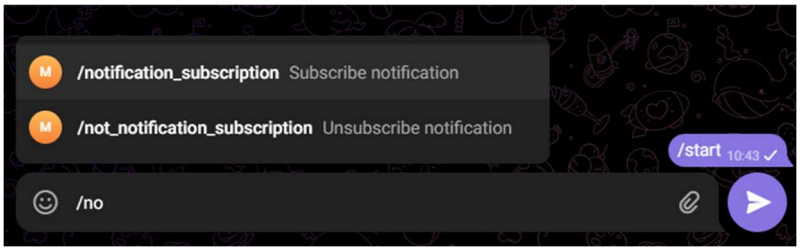


Enter your API token obtained in the previous steps. Click Save and Restart.
Now let's back to Telegram and talk to your bot by going to @BotFather again and click onto the bot:

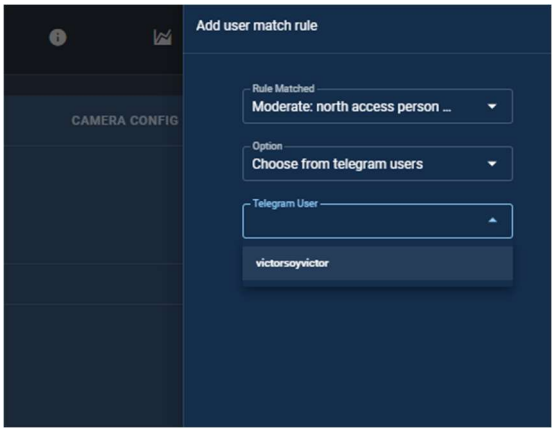


Then click START in the image below and send the command you previously created: /notification_subscription





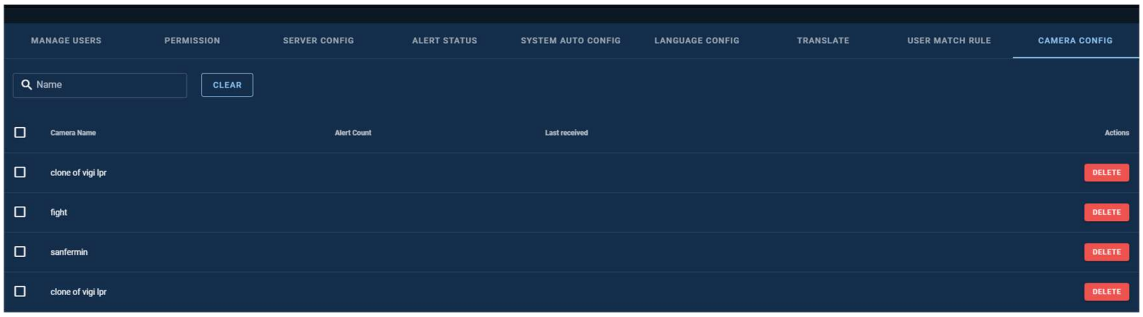
Finally we go to the Webclient an enable a User Match Rule for your bot to relay:



Please note if you don't see your user listed, in the example above "victorsoyvictor" you have to verify your steps.
Hit save at the bottom of the website.
The rule can flood your Telegram chat with the bot, so be aware of that. Also to disable you can run the command:
/not_notification_subscription

3.1.9 Camera config

Here you can see the list of cameras:



With the alert count and last received column you can decide to delete cameras you are no longer using.

3.1.10 Group Camera config

This tab is related to the Keep Watch section 3.6

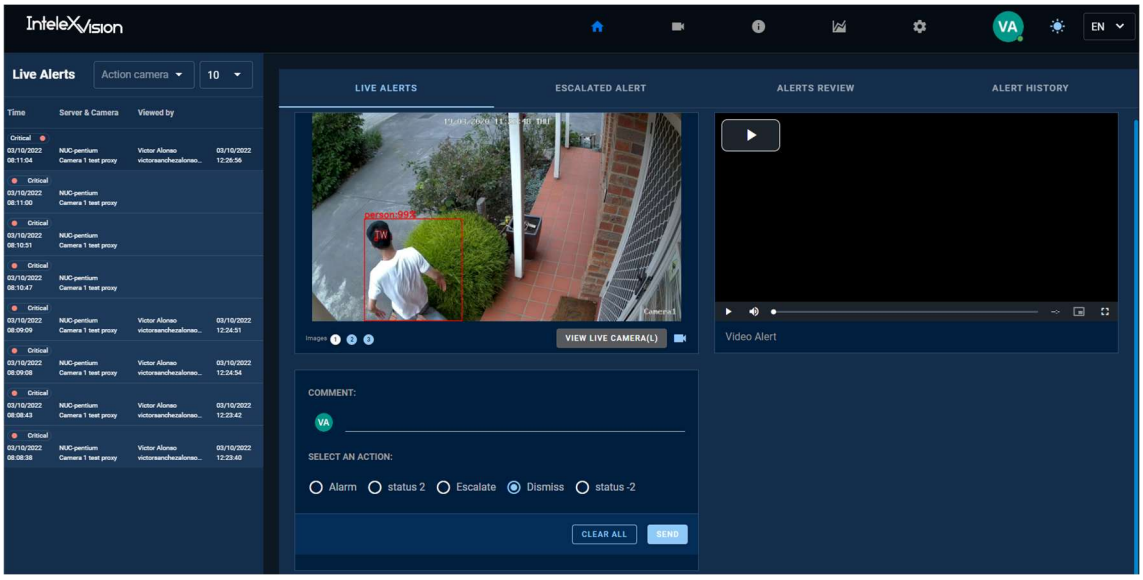
3.2 Dashboard

This is the main screen where the operator can handle the alerts triggered by events. On the left navigation menu a list of live alerts are displayed, on the right side we have 4 views: Live alerts, Escalated Alert, Alerts review and Alert History.

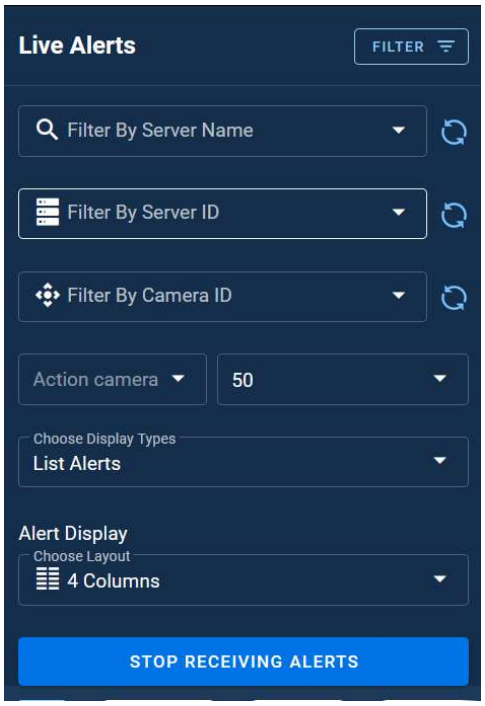
Live alerts	Main view of the Alert selected, with 3 subviews: Video, Detection and Comment. You can also activate the Live View of the camera, shortcut L key from your keyboard.
Escalated Alert	From this view, the operator or supervisor can now Dismiss or Approve the Escalated Alert.
Alerts review	This is a timeline panel for alerts review.
Alert History	This menu gives the user access to the historical view of the past alerts.

3.2.1 Live alerts

Here is an example view of the selected Live alert from the left panel. In the middle we can see the 3 main views, a loop short video of the alarm, a 20 seconds video of the alarm and the actions to take (Alarm, Escalate, Dismiss, status 1 or others set in previous step).

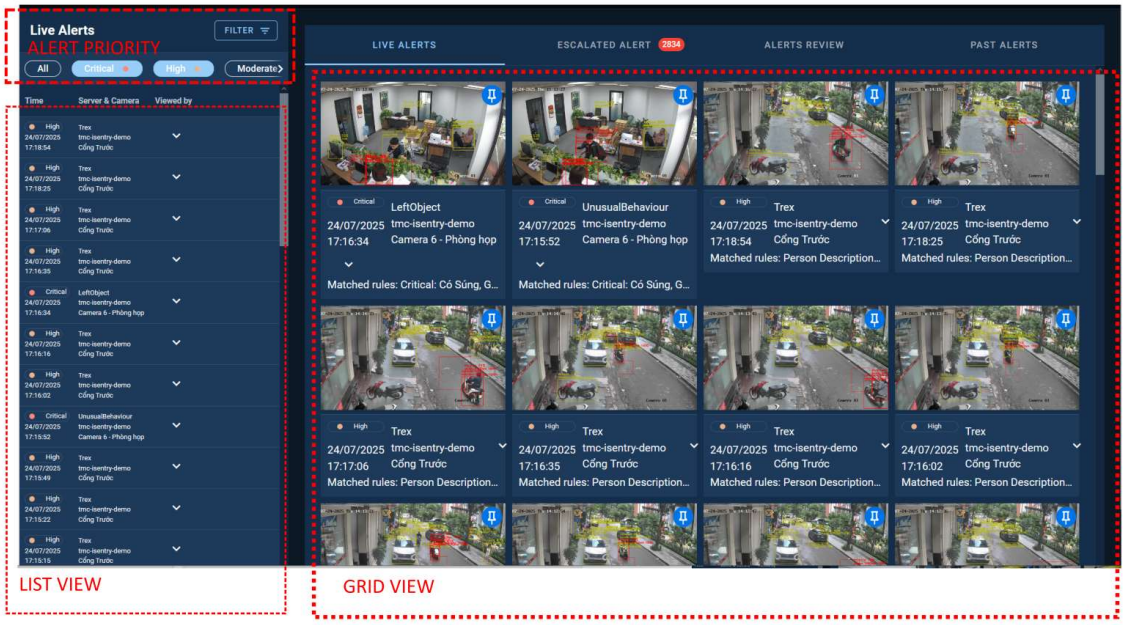


3.2.1.1 Live Alert Filter



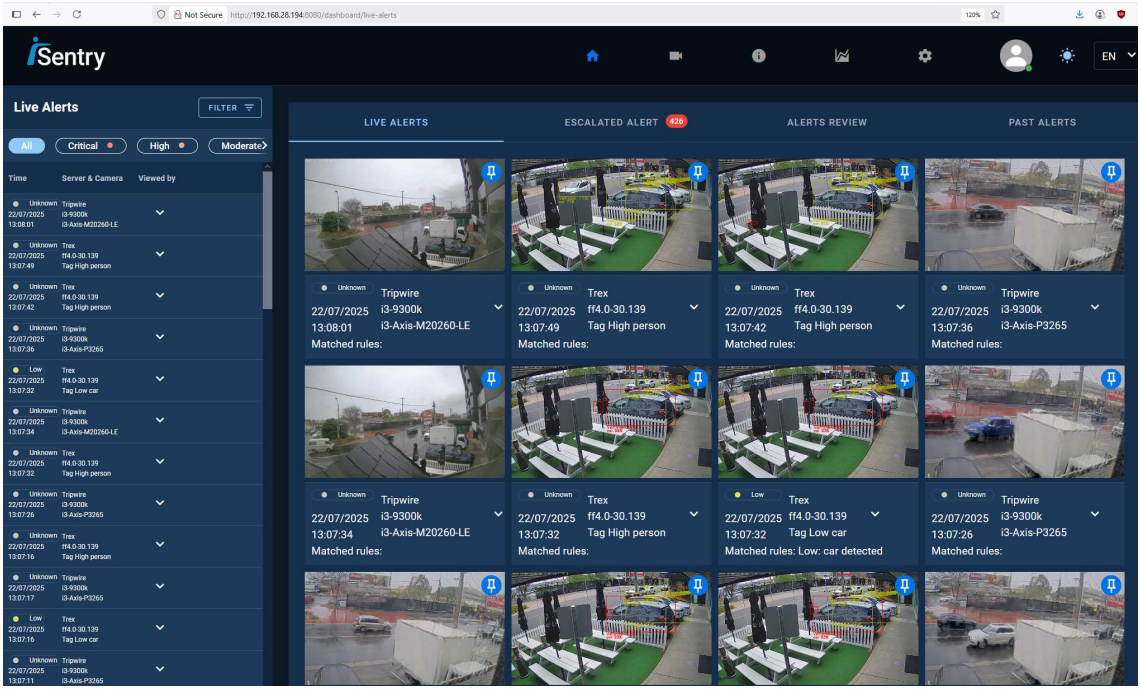
3.2.1.2 Live Alert – Sort by Priority

At default, all alert type are enabled (ALL).
When one of priorities is selected, while the list view show only alerts with selected priority, the grid view sorts alert in order of priority level then timestamp.
Priority level: Critical → High → Moderate → Low → Very Low



3.2.1.3 Grid view

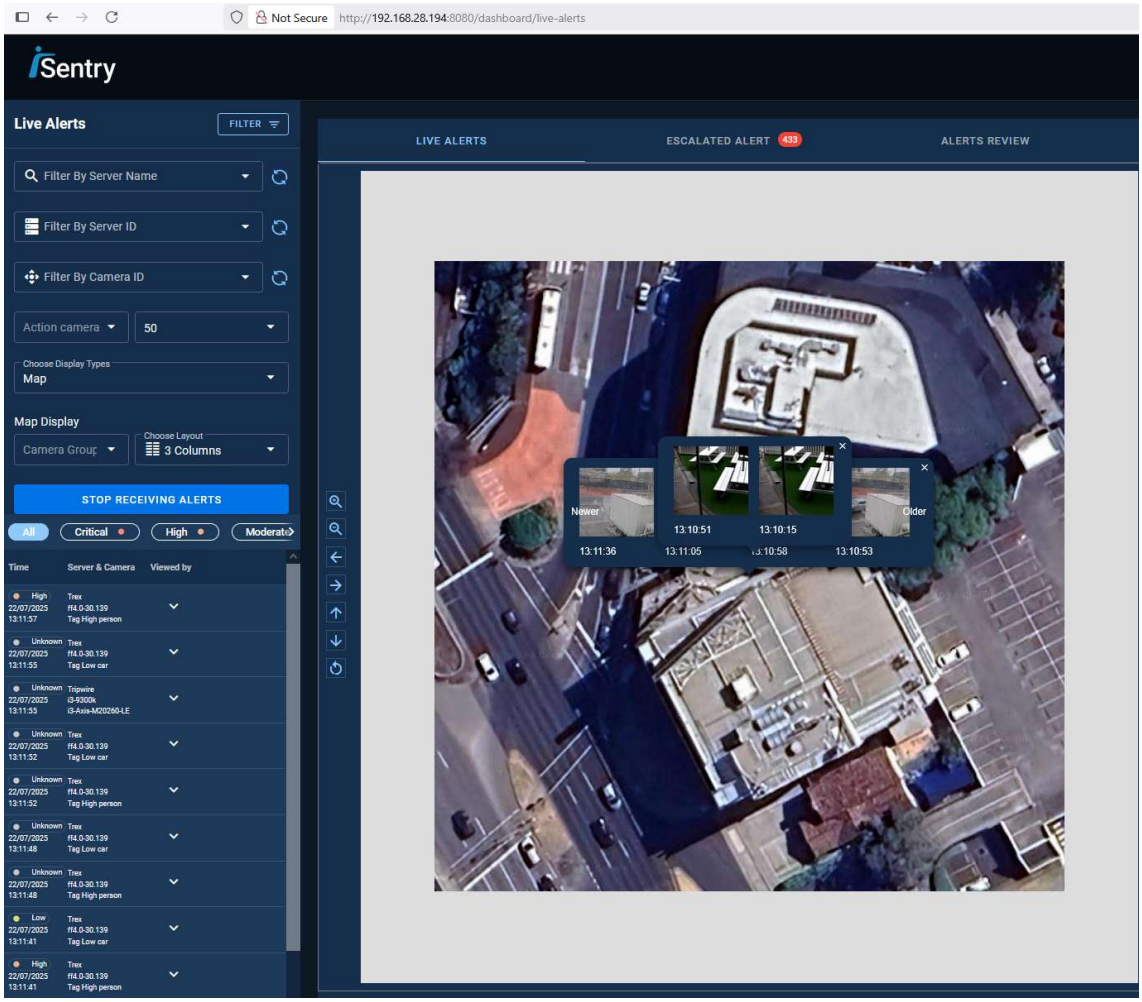
This feature is available from version 2.3.0, allows user to view alert in grid layout



The layout can be adjusted with several options in the filter box

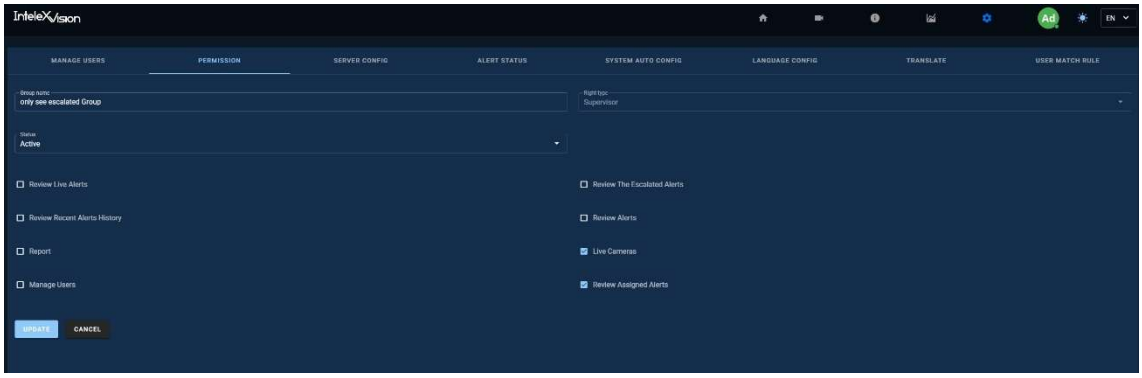
3.2.1.4 Map view

Map is selected from Choose Display Types. The map image defaults is not available and need to be configured in Group Camera Config settings.

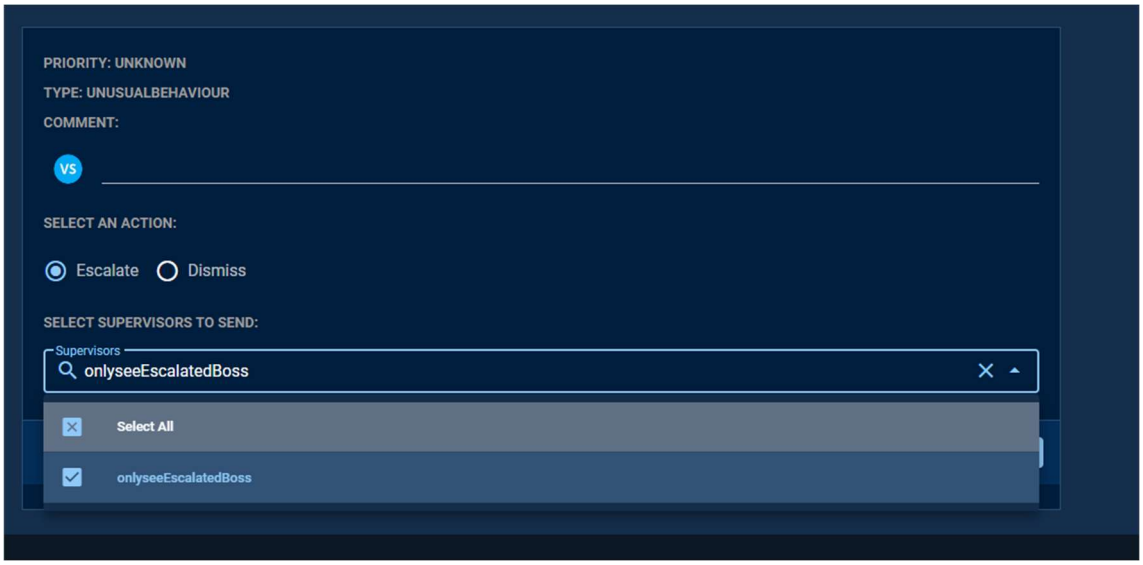


3.2.1.5 Send live alert to selected user

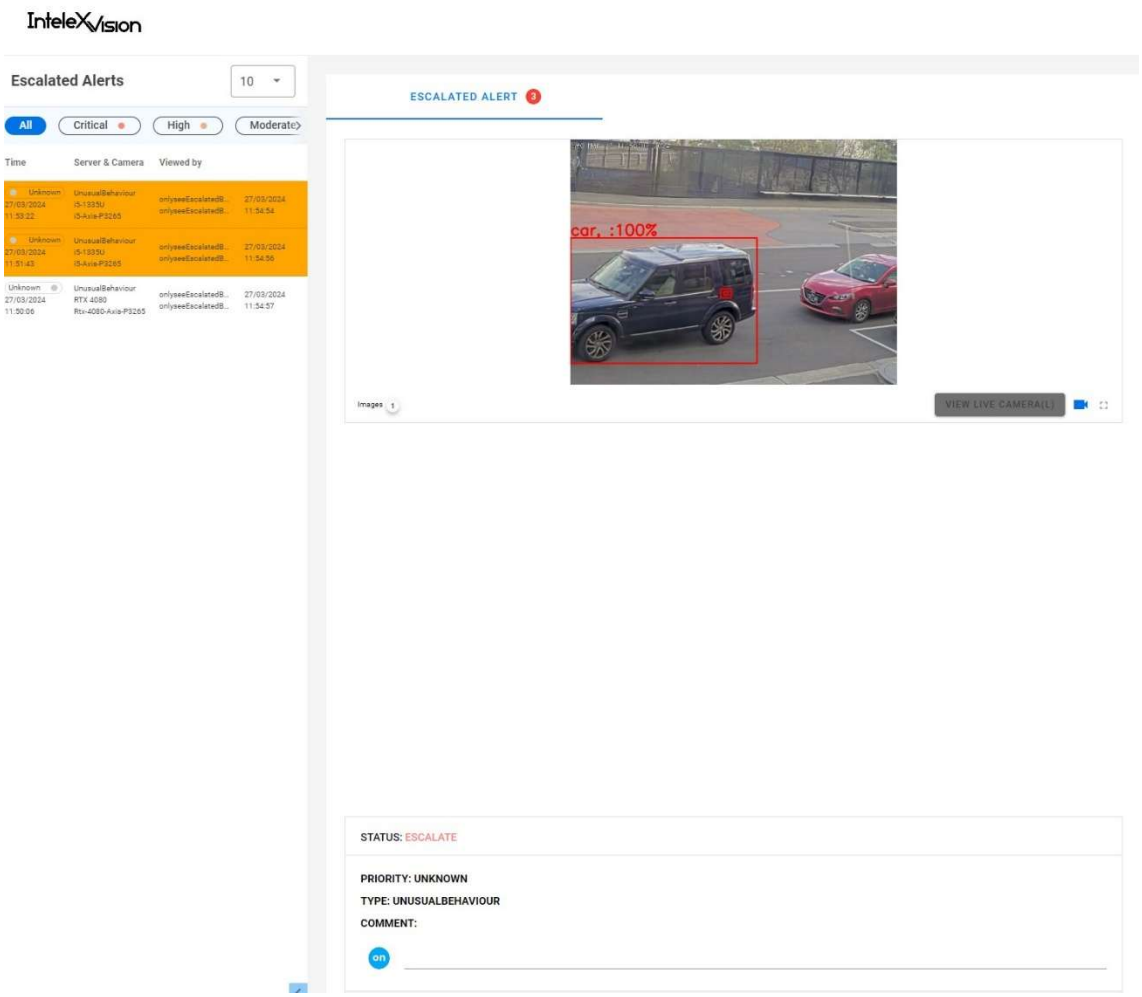
The user can send an alert to high elevated operator. For this first step is to create a permission group and add this user as Supervisor with Review Assigned Alerts box selected:



After that from the Live alert view you can click and send to that user:

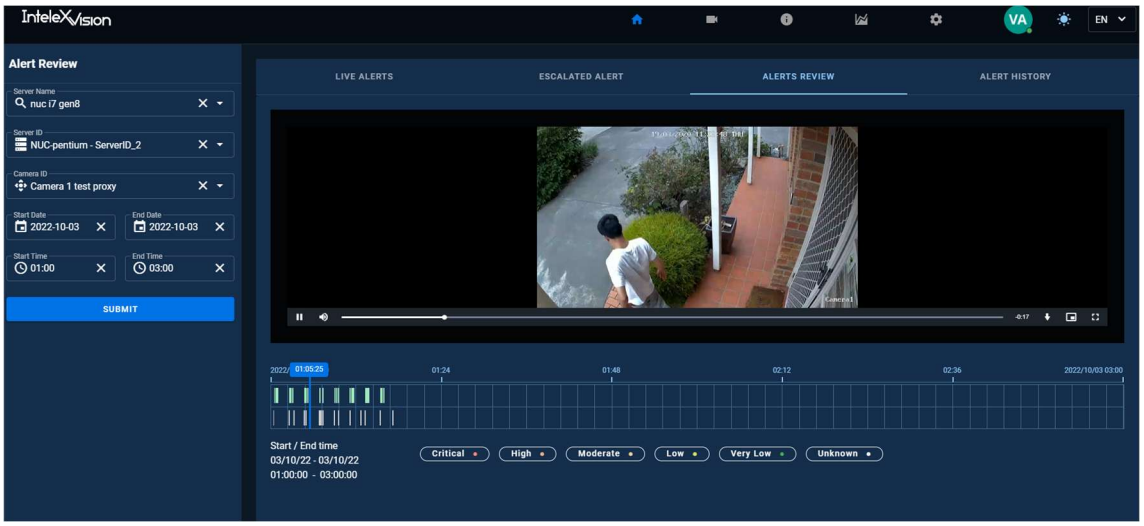


After doing that, the aforementioned user will have the option to review the alerts in its Escalated tab view:



3.2.2 Alerts review

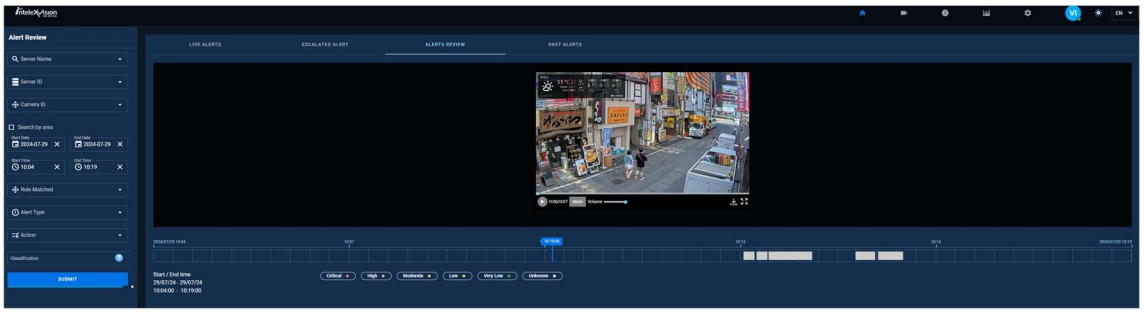
This is an enhanced view of the alerts within the selected filter (date, time, server, camera). The user can have a look in a detailed view of the alerts triggered in a timeline view:



The web client can play playback video from an iSentry server when they are in the same local network.

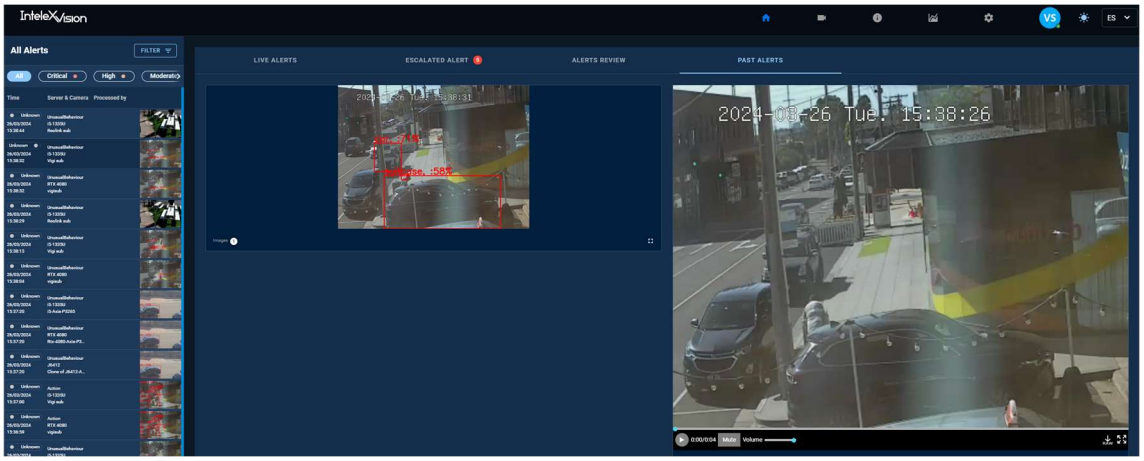
In the lower panel the user can see the timeline and marked in colors corresponding to the severity of the alert the access to the video of the alert.

If the bars are too “thin” please use the filter to adequately stretch the timeline to a better view like:

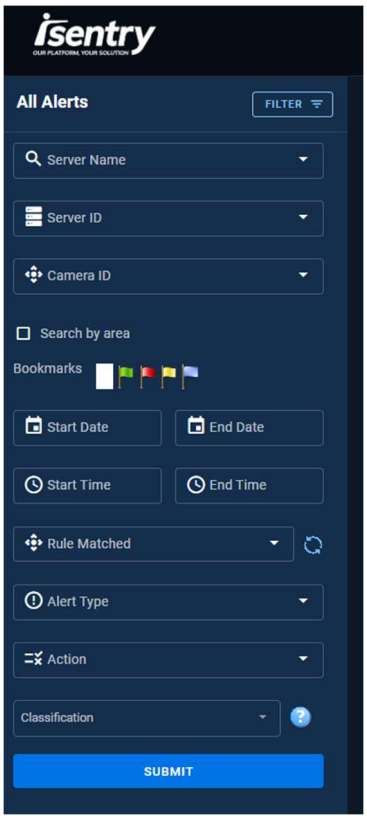


3.2.3 Past Alerts

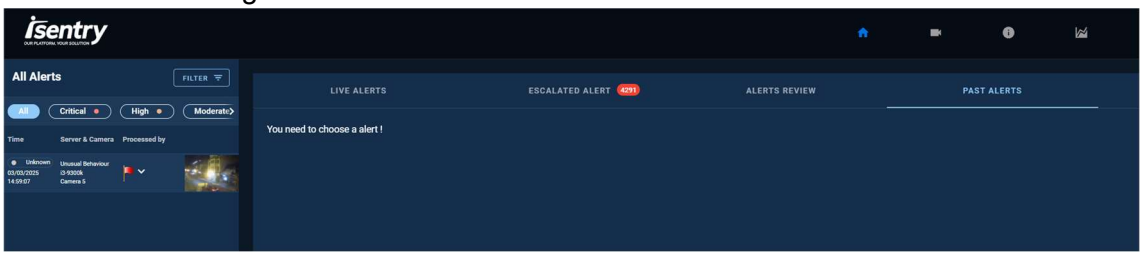
At any time the user can have a look at the past alerts to see what actions were taken (Comment panel) plus the short and 20 seconds videos of the selected alert.



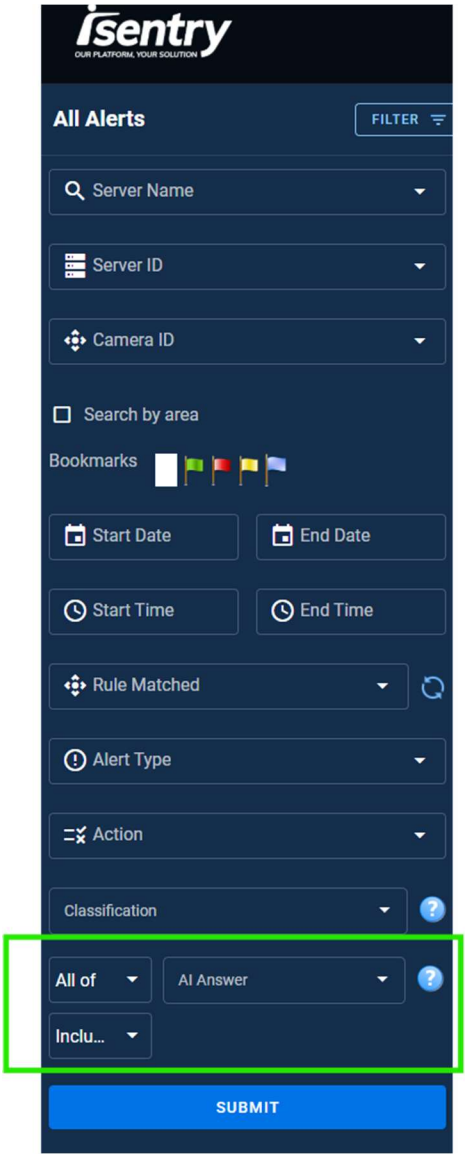
The user can apply filters to find what it is of interest. Filters can be applied to the fields shown in the image below. A new button appears next to the Rule Matched to refresh any recently created rule and refresh the browser cache.



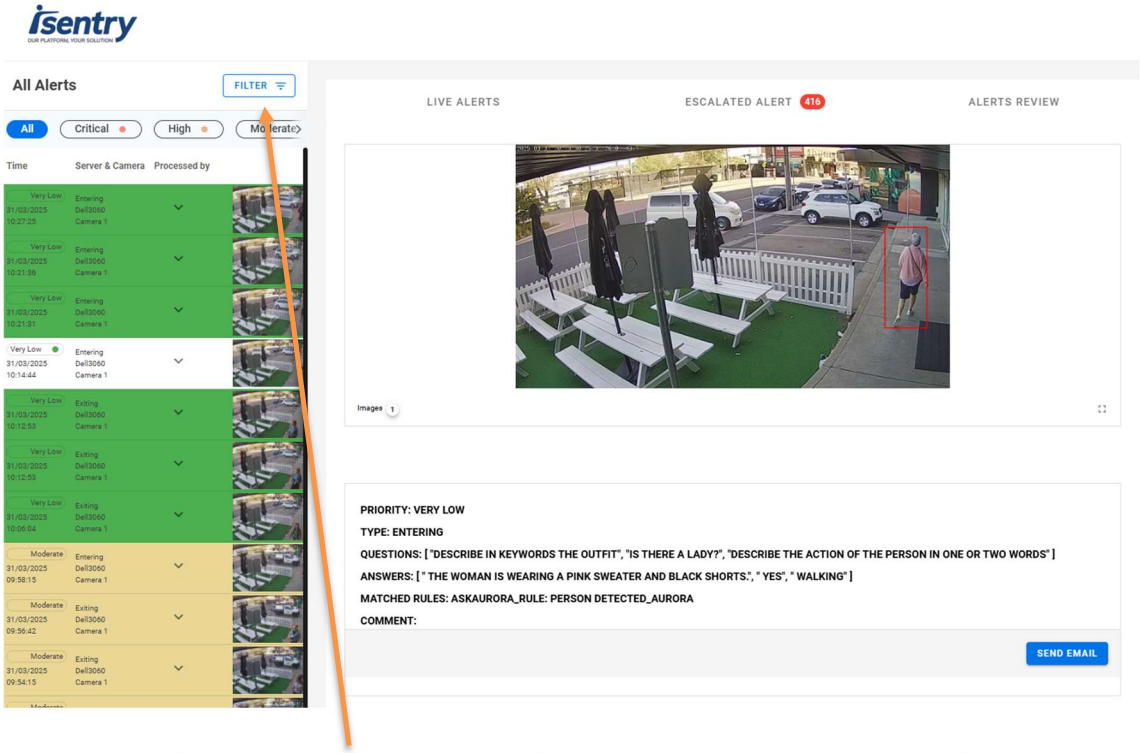
Now the user can bookmark the alerts for later retrieval and inspection using the flags like the colored flags above to see them like below:



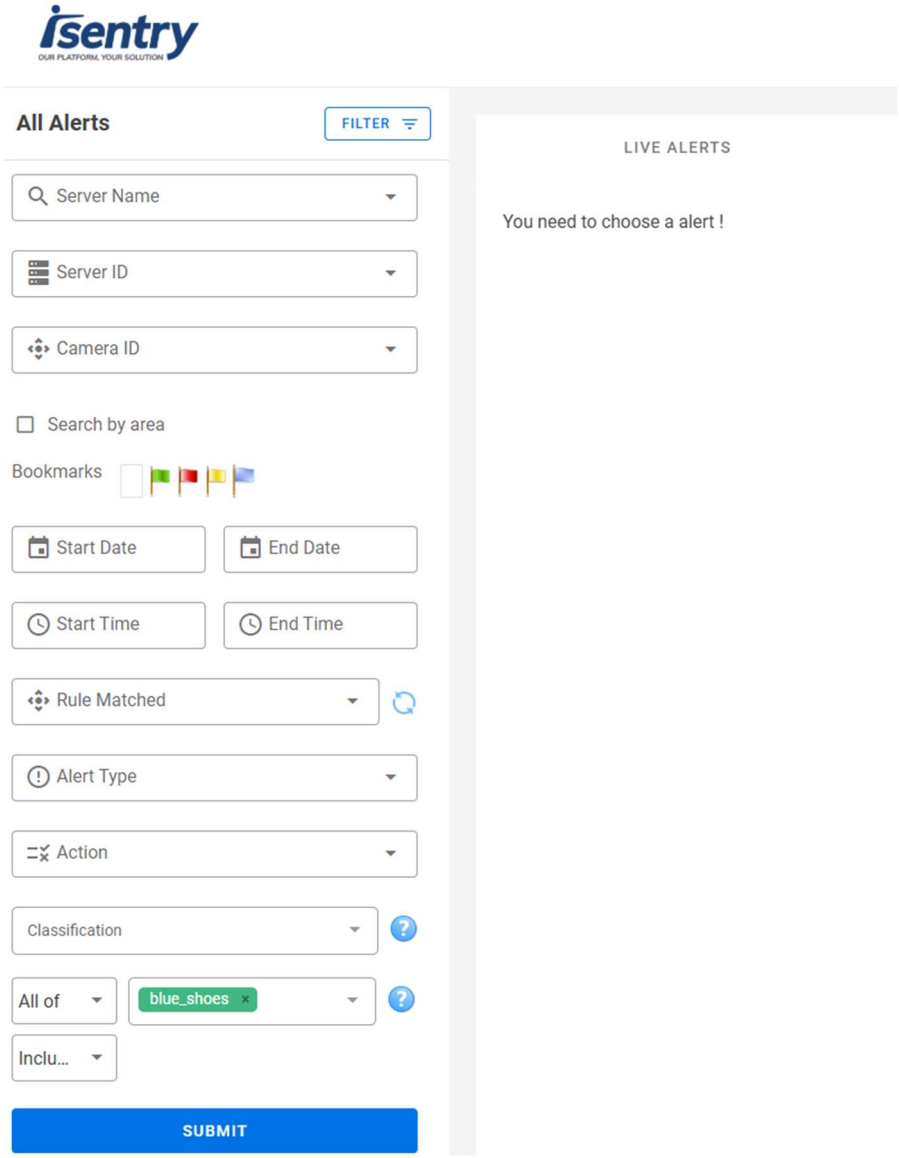
Now the user can inspect the alerts using the Aurora model. For example one can retrieve information regarding the questions configured in iSentry Firefly.



Given alerts such as below when you configure iSentry Firefly with Aurora:

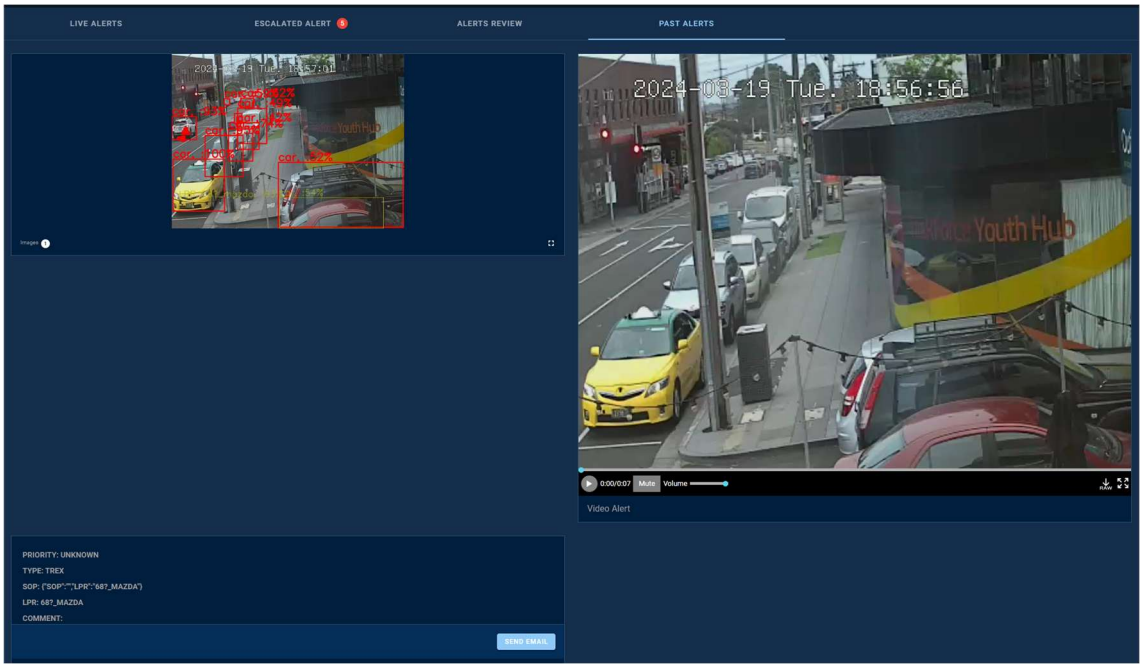


One can easily go to the filter menu and enter keywords from the questions above to retrieve alerts that matched the criteria, some examples could be “find a person wearing blue shoes” for such one should enter:



3.2.3.1 Show Alert SOP and third party result per alert

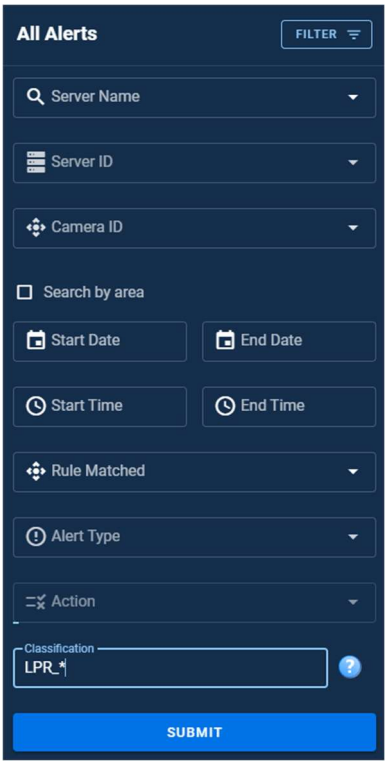
Now you can see the SOP and the 3rd party per alert below the alert image:



In the image above we see the results from License Plate Recognition (LPR) for a clear reading and also the possibility to send by email.

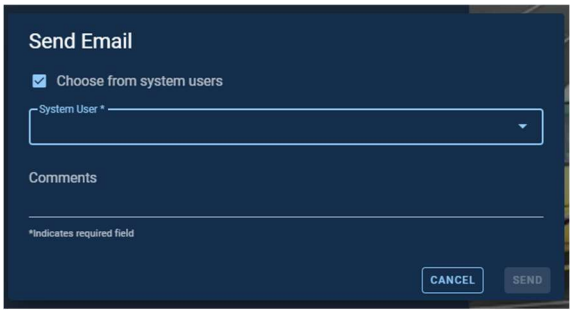
3.2.3.2 Regex search (and exact search)

For example: Enter object name exactly as rules setup, such as person, LPR_abc-123, FR_Name, fig*, fall*



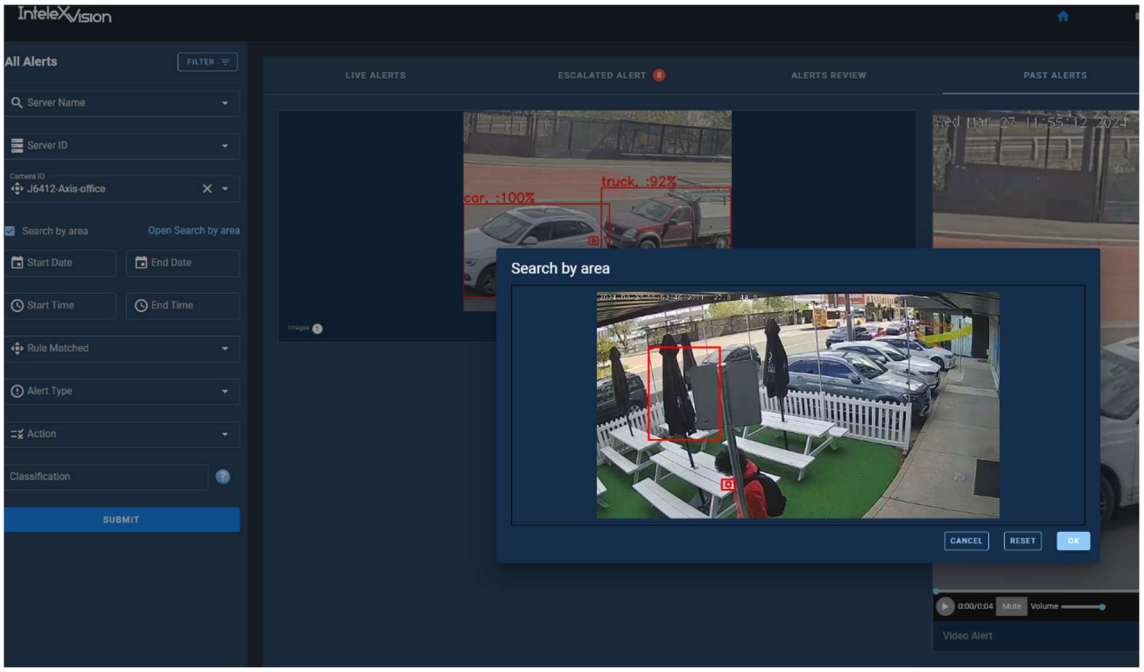
3.2.3.3 E-mail alert report to user(s)

When you have one alert selected you can send an email picking one user from the System user list.

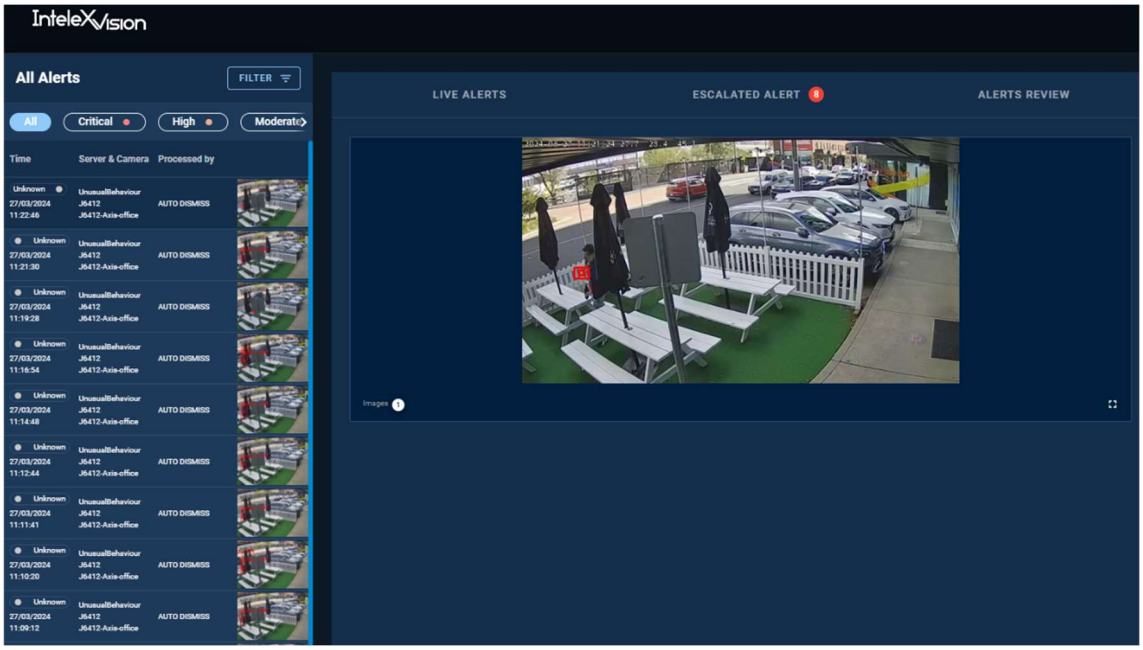


3.2.3.4 Search by area

This feature allows the user to search by drawing a rectangle. A camera must be selected first to allow the user to draw in the screen:

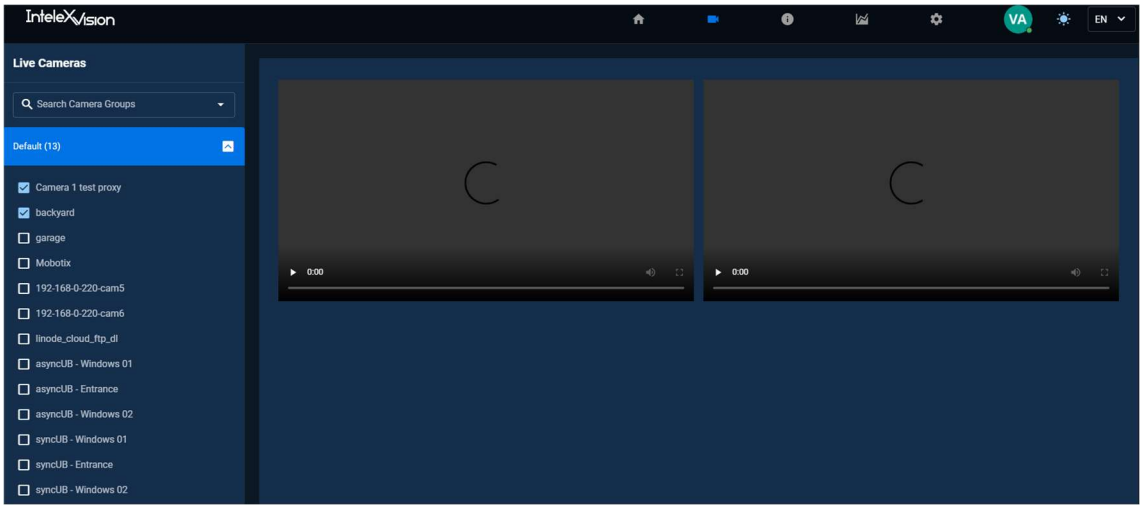


Once you press the button “ok” the alerts listed in the lefthand side will be the ones containing detections matching your selected area.



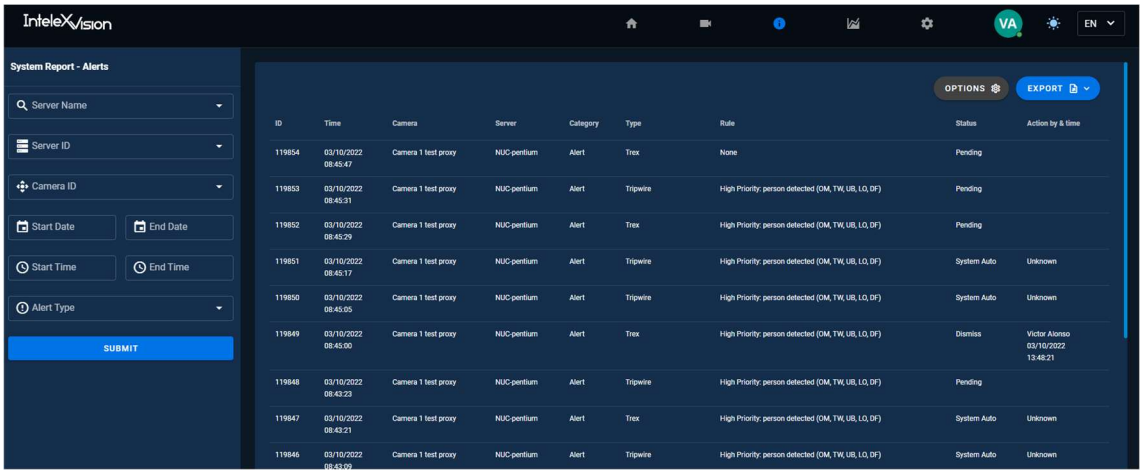
3.3 Live Cameras

In this menu the user can access the live view of the cameras. The user can filter from the left panel which cameras would like to watch. They are organized in groups, so every group contains a set of cameras.

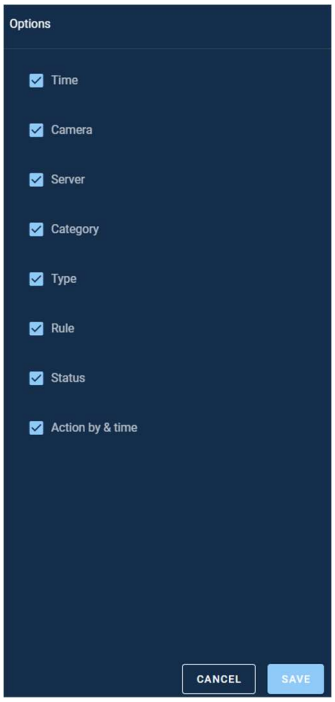


3.4 Reports

This menu allows the user to perform a customized report of the alarms reported and export them in different formats (.pdf and .xls). From the left side panel the user can filter by different fields (server name, server ID, camera ID), time (date and hour) and Alert type (TREX, Tripwire, Unusual Behavior).



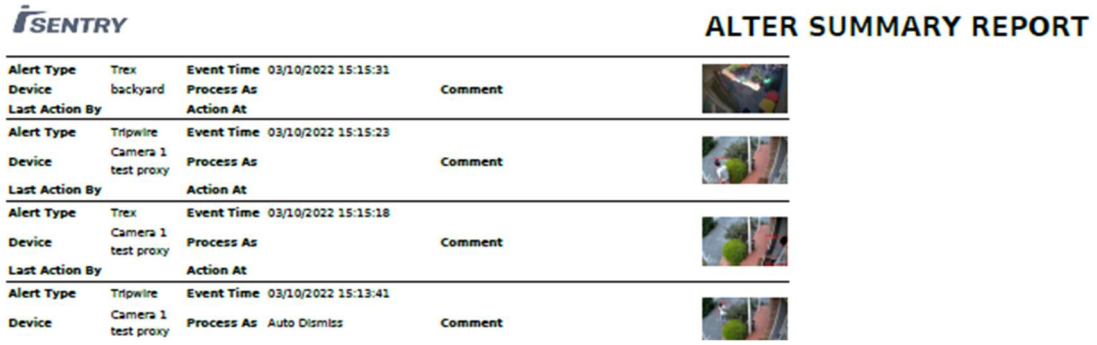
By clicking into the Options menu, an user can specify which columns to include in the report view before exporting it.



Once the filters and the columns have been selected, the user can press the button Export and select the desired output format.

- **Please note to allow pop ups in your browser before selecting exporting the report. That will save you time.**
- **Also keep in mind that requesting a detailed report can be time consuming to generate and can cause other users to experiment delays in their reports to be generated.**

Here you can see an example of a .pdf report created:



iSENTRY

ALTER SUMMARY REPORT

Alert Type	Trex	**Event Time**	03/10/2022 15:15:31		
Device	backyard	**Process As**		**Comment**	
Last Action By		**Action At**			
Alert Type	Tripwire	**Event Time**	03/10/2022 15:15:23		
Device	Camera 1 test proxy	**Process As**		**Comment**	
Last Action By		**Action At**			
Alert Type	Trex	**Event Time**	03/10/2022 15:15:18		
Device	Camera 1 test proxy	**Process As**		**Comment**	
Last Action By		**Action At**			
Alert Type	Tripwire	**Event Time**	03/10/2022 15:13:41		
Device	Camera 1 test proxy	**Process As**	Auto Dismiss	**Comment**	

3.5 BI Tool

Here the user is presented with different charts and graphs about the overall system status. The main menus can be resumed in the following table:

Summary	Main panel showing the most relevant overview of the system.
Operator	
Devices performance	
Devices variance	
Loss of signal	
People counts	

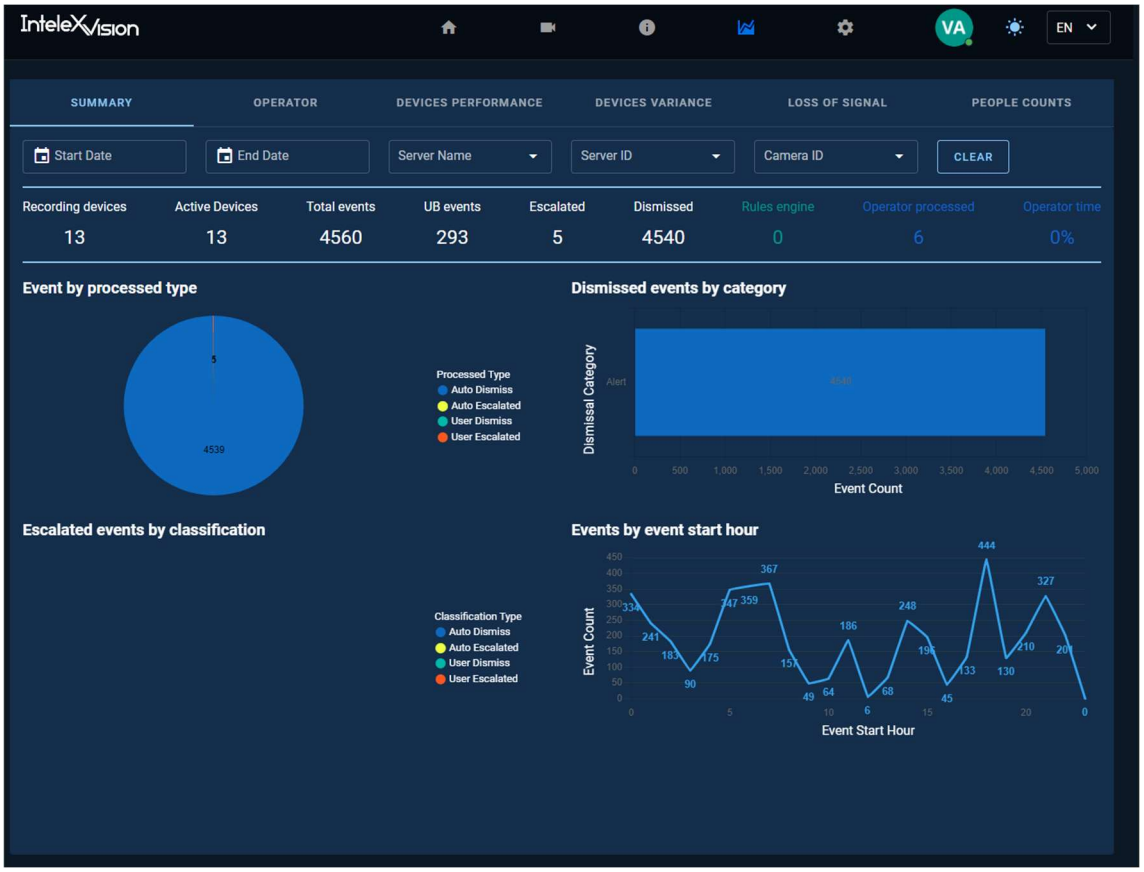
In the upper part the user can filter by different fields (server name, server ID, camera ID), time (date and hour):

Following this panel the user gets the summary of the overall situation:

3.5.1 Summary

In this panel the user can have a look into 4 different subpanels:

Event by processed type	Pie chart showing events by processed type
Dismissed events by category	Bar chart showing dismissed events by category
Escalated events by classification	Chart showing escalated events by object classification.
Events by event start hour	Graph showing the number of events starting hour

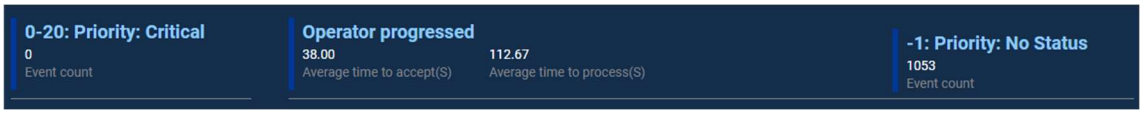


3.5.2 Operator

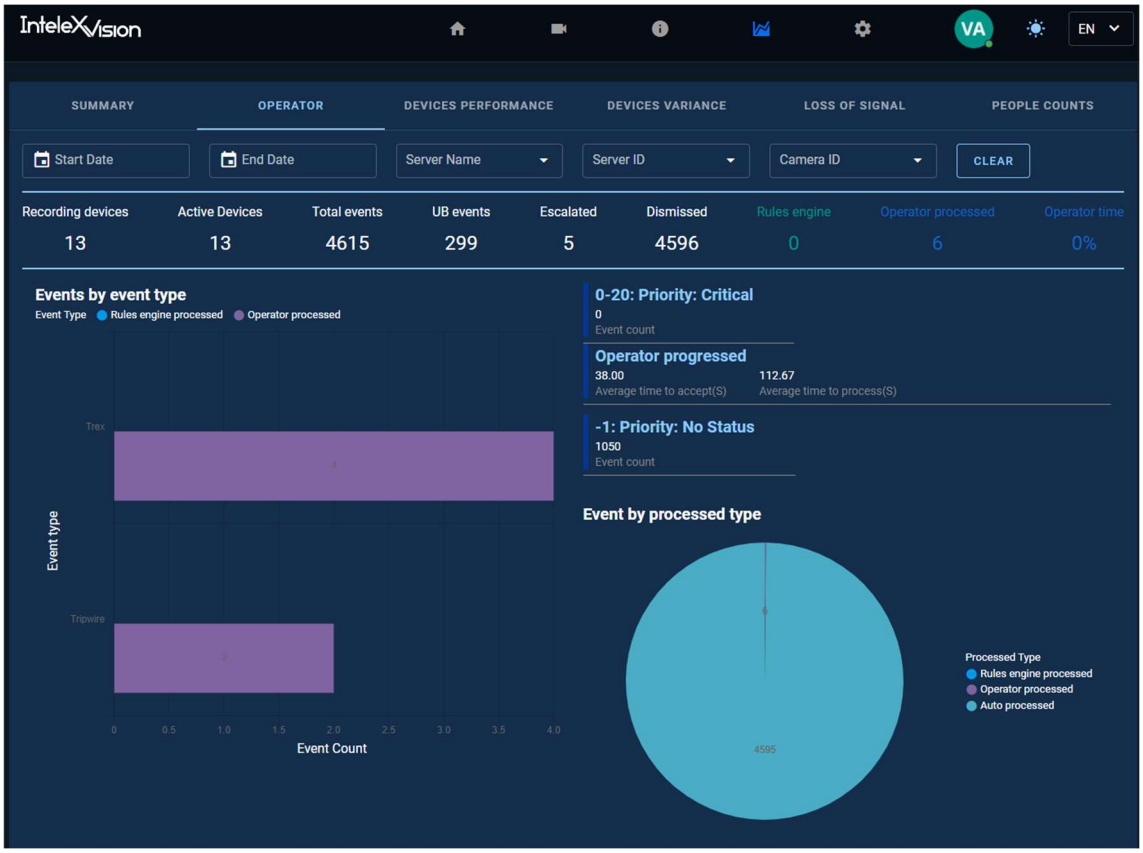
In the following panel the information displayed to the user is:

Events by event type	Bar chart, the bar shows the number of events horizontally and every bar represents an event type.

In the right panel you can find the priority of the alarm triggered and the performance of the Operator measured in seconds after the alarm notice.



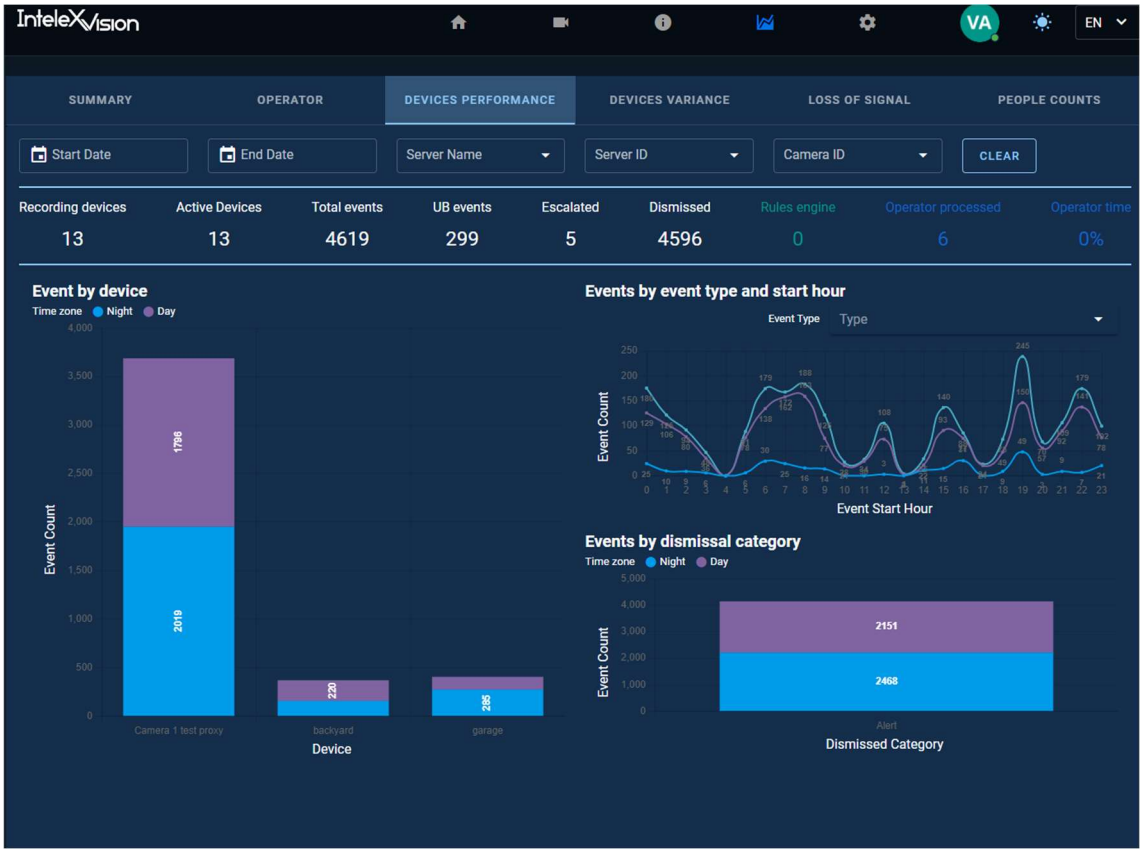
In the bottom right panel there is a pie chart showing the Event by processed type.



3.5.3 *Devices Performance*

In this panel the user can have a look into 3 different subpanels:

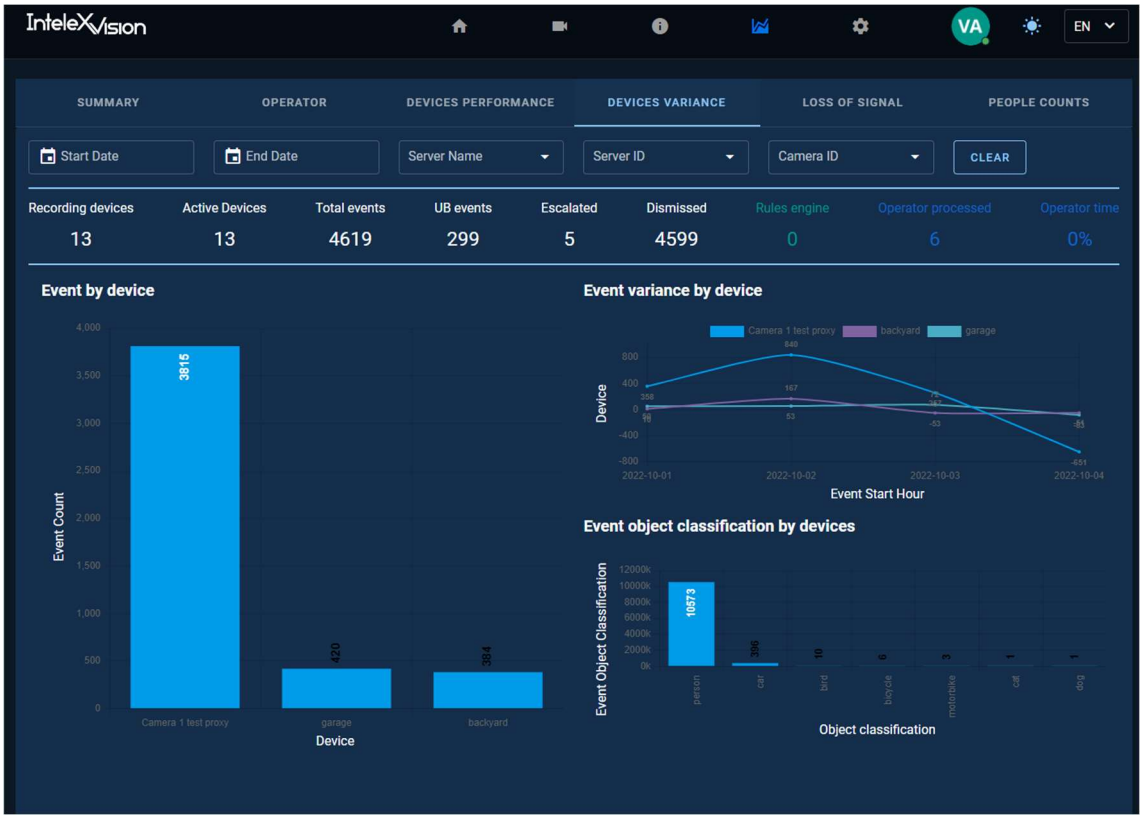
Event by device	Filtering by device and time zone the bar chart shows the number of events occurred.
Events by event type and start hour	Filtering by event type the graph shows the number of events per start hour
Events by dismissal category	Filtering by time zone it shows the number of events by dismissed category.



3.5.4 Devices Variance

In this panel the user can have a look into 3 different subpanels:

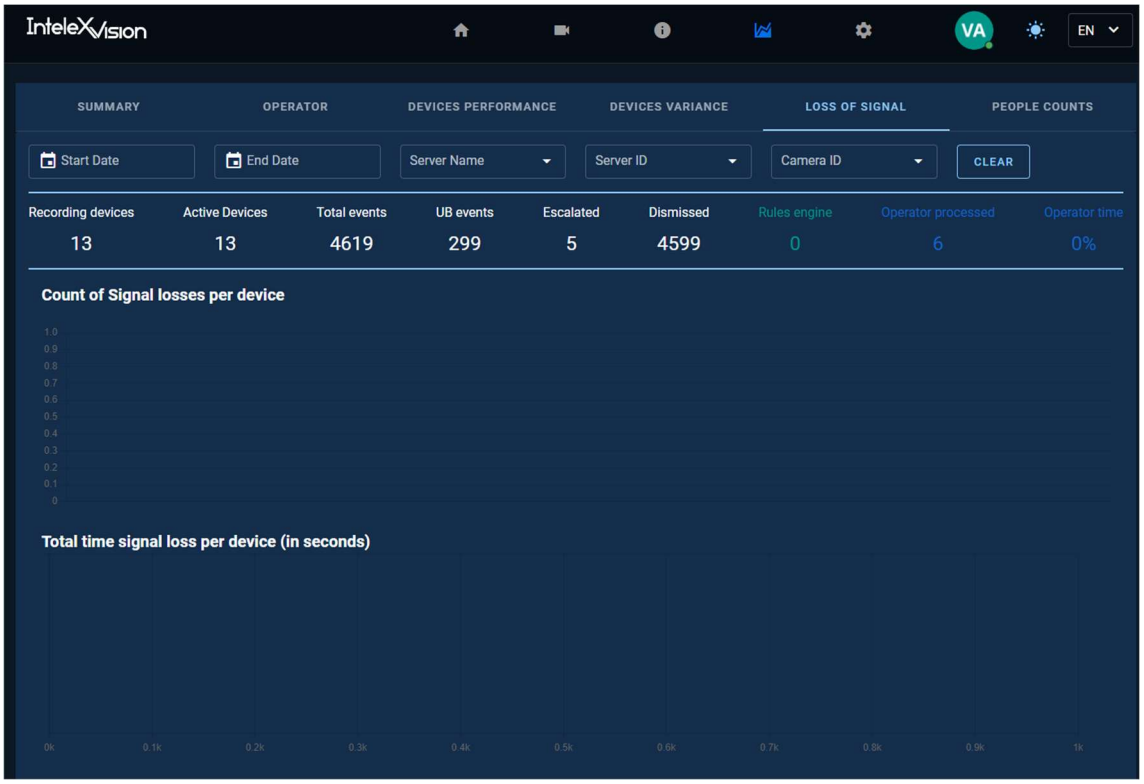
Event by device	Number of events detected per device in a bar chart.
Event variant by device	Graph showing the variance per device in the Y axis and the Event Start hour in the X axis
Event object classification by devices	Bar chart showing the number of event object classification by object type attending to the type of device



1.4.1.1

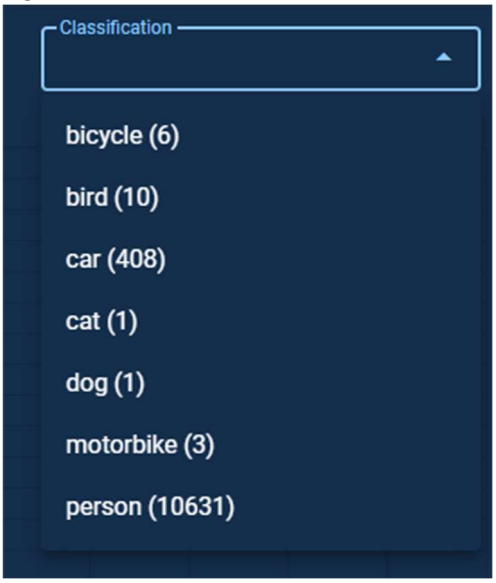
3.5.5 Loss of Signal

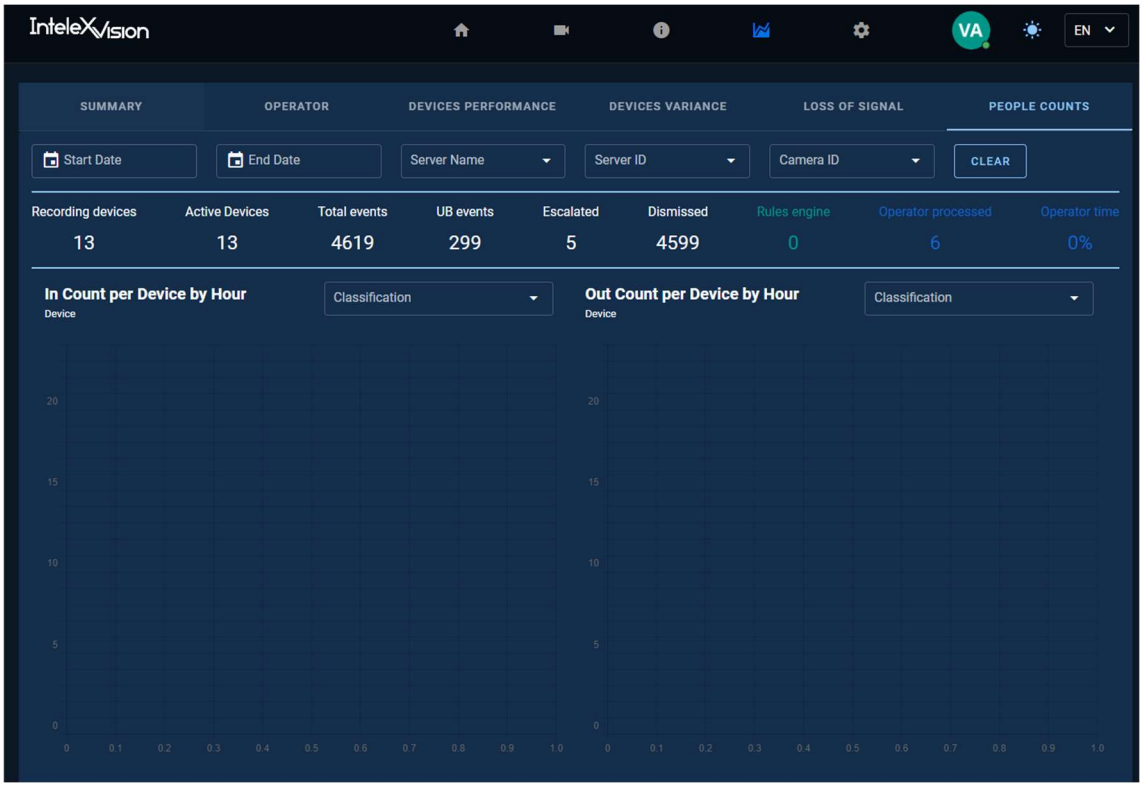
In this panel the user will be displayed the Count of Signal losses per device and the Total time signal loss per device (in seconds).



3.5.6 People Counts

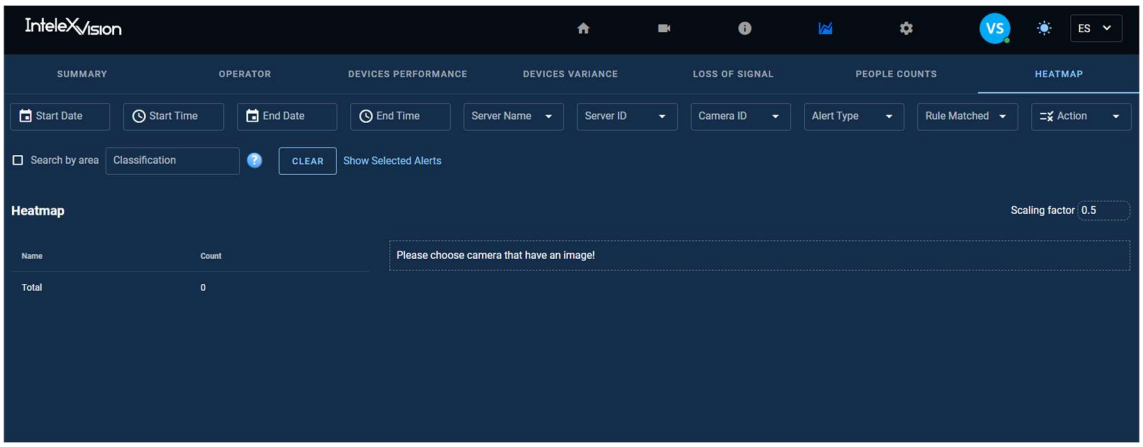
In this panel the user will be displayed the In Count per Device by Hour and the Out Count per Device by Hour. A classification selection menu is shown where you can choose from different categories like:



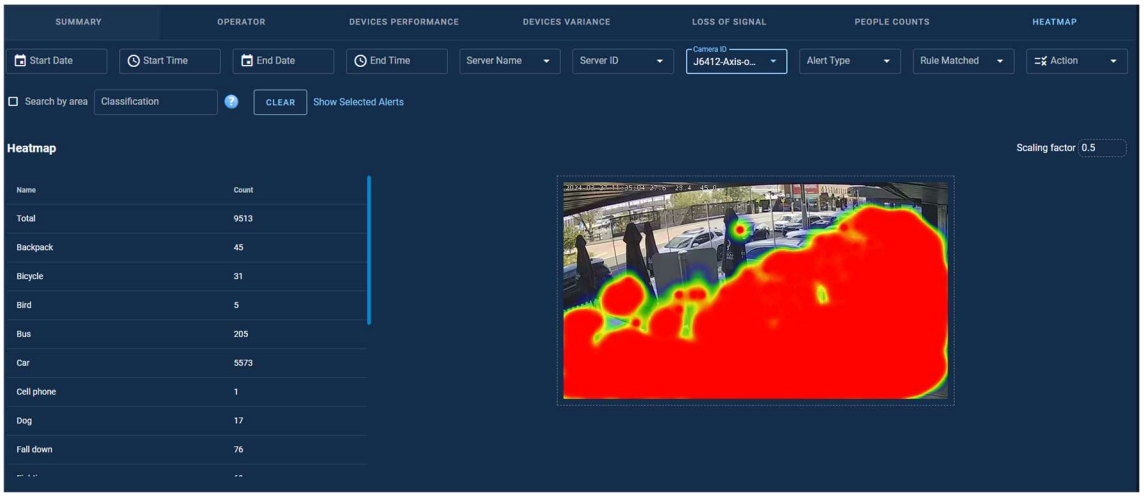


3.5.7 Heatmap

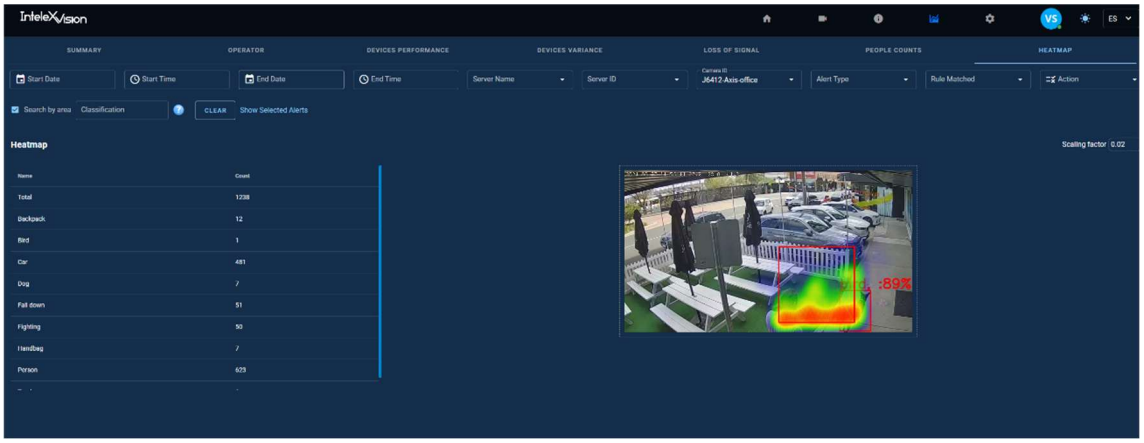
In this panel the user will be displayed the Heatmap screen like:



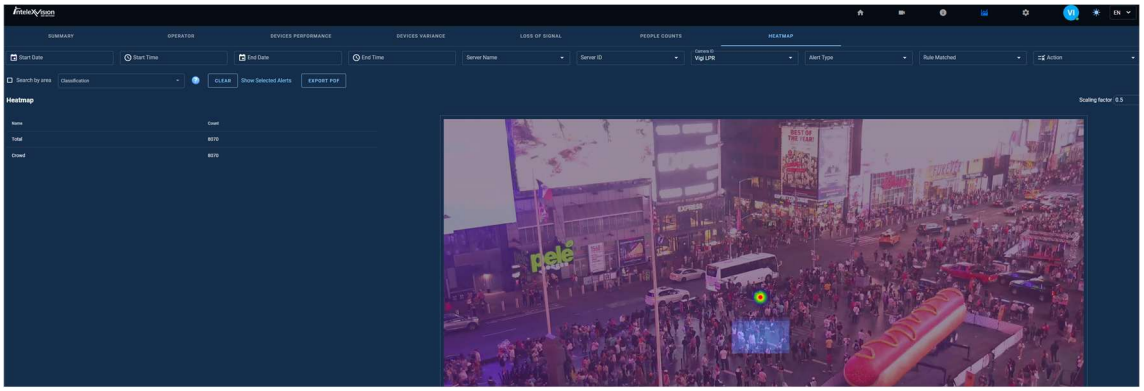
From here the user should pick a camera that have an image for example:



Search by area is also allowed by clicking in the selection box shown below:



You can also count the number of people in the crowd:



3.6 Keep watch

Web Client also provided dedicated UI to work with another product call Keep Watch. Please refer to the separate document “iSentry Keep Watch user manual” for how to use web client with Keep Watch product.
Related UI sections: Past Alert, Group Camera Config and Permission


InteleXVision
SEE BEYOND