Sentry WebClient User Manual

Version 2026R1

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.

Introduction

Scope

This User Guide offers comprehensive instructions on how to use the **Sentry WebClient**. It provides all the essential information needed to help users navigate and operate the application effectively.

Abbreviations, Acronyms and Definitions

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

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.
- **Operations Personnel:** Tasked with the daily operation and monitoring of the system to maintain optimal performance and address any operational issues as they arise.
- **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.

Pre-requisites

Technical Knowledge

- **Basic Operating System Proficiency.** Ability to navigate applications, log into systems, and manage basic settings.
- **Data Entry Skills.** Proficiency in entering data into various software applications.
- **System Navigation.** Understanding of how to access and use installed systems, including logging in and performing routine operations.

System Access

Access Privileges. Access with proper access to Sentry WebClient application.

Preparatory Tasks

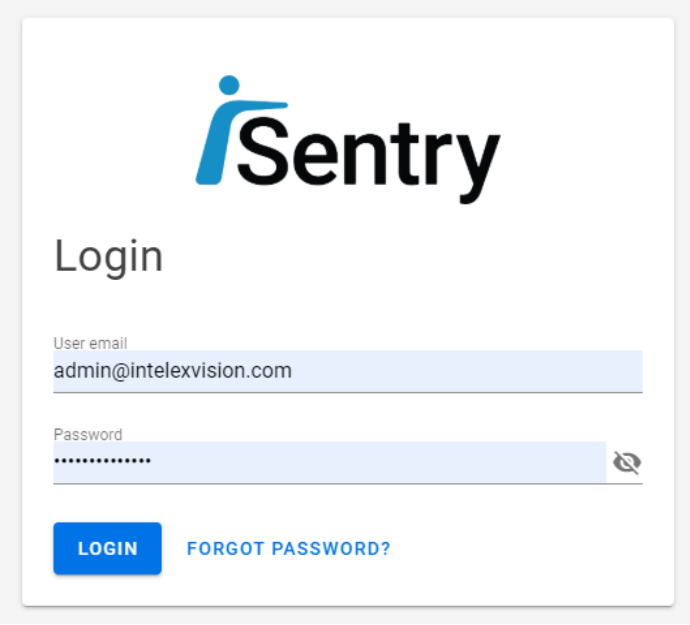
Review Documentation. Familiarize yourself with this guide and any other documentation.

Deployment

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

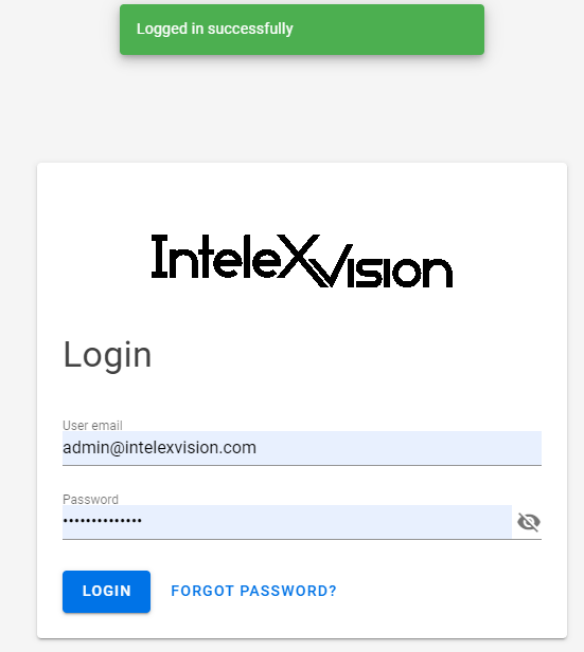
For example, successfully going into the following URL shows the login screen below.

`http://isentryclientdemo1.duckdns.org`



Credentials

To login into the **Sentry 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.

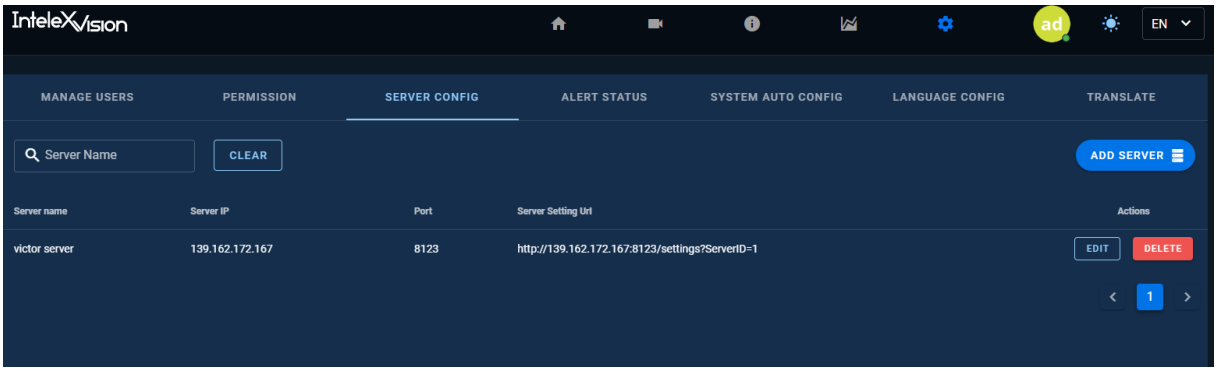


Pairing with a Sentry Firefly server

To receive alerts from Sentry **Firefly's** with cameras a two-way pairing must be done, first add the **Sentry Firefly** to the **Sentry WebClient**, second add the **Sentry WebClient** to **Sentry Firefly**.

> **IMPORTANT NOTE**
>
> **The order of pairing is crucial.** You must first add the **Sentry Firefly** server to the **Sentry WebClient**, and only after that, add the **Sentry WebClient** to the **Sentry Firefly** server. Failing to follow this sequence may result in unsuccessful pairing or missed alerts.

To add **Sentry Firefly** to the **Sentry WebClient,** go to *Settings > Server Config.*



Press the button *Add Server* to link the **Sentry WebClient** with an up and running **Sentry Firefly**.

For that, provide the details for Name, Server IP and Port. Do not forget to click Save.

Then, add the **Sentry WebClient** to the **Sentry Firefly** following the steps in **Sentry Firefly Configuration Guide**.

System Overview

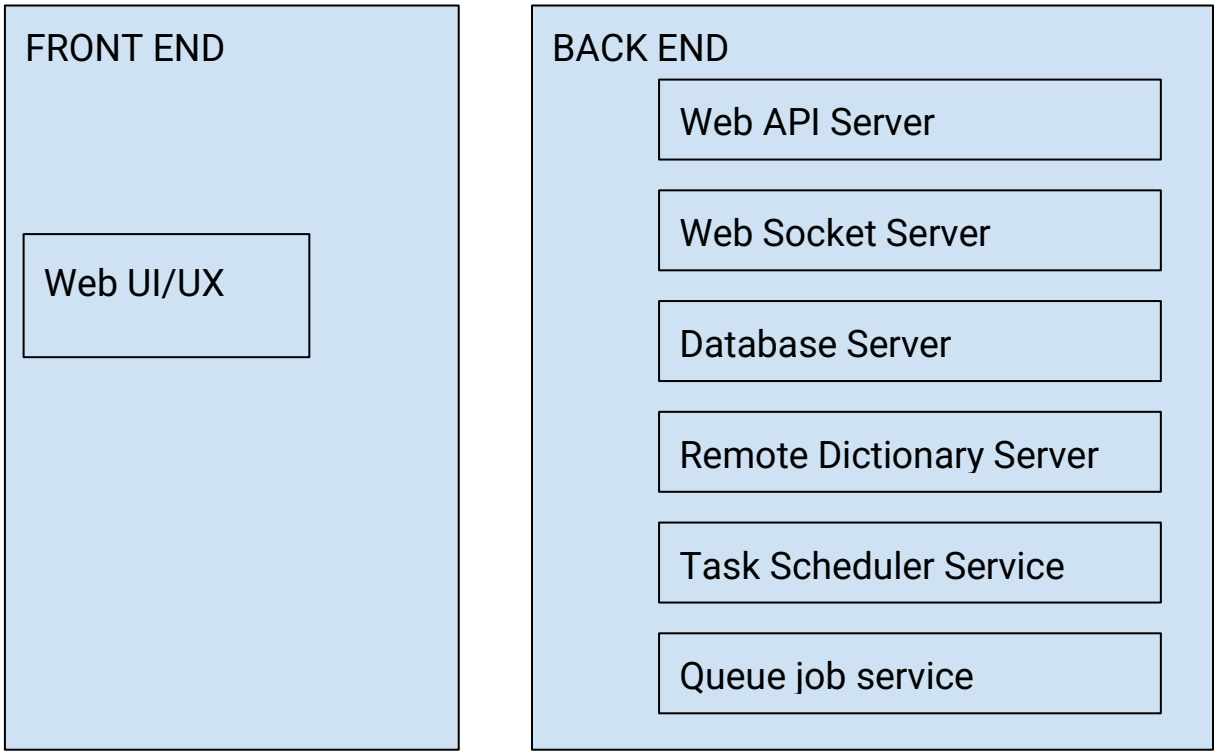
WebClient Components

Sentry WebClient architecture is divided into two core layers: a *Front End* and a *Back End*, each hosting dedicated components that work together to deliver a reliable and scalable user experience.

The *Front End* consists of the **Web UI/UX**, which serves as the primary interface through which users interact with the system via a web browser.

The *Back End* comprises six components. The **Web API Server** handles incoming client requests and orchestrates business logic. The **Web Socket Server** manages real-time, bidirectional communication between the client and server. The **Database Server** is responsible for persistent data storage and retrieval. The **Remote Dictionary Server** provides fast, in-memory data caching to optimise performance. The **Task Scheduler Service** manages the execution of time-based and recurring operations. Finally, the **Queue Job Service** handles asynchronous job processing, ensuring efficient distribution of background workloads.

Together, these components form a modular architecture designed for operational efficiency, maintainability, and a seamless user experience.



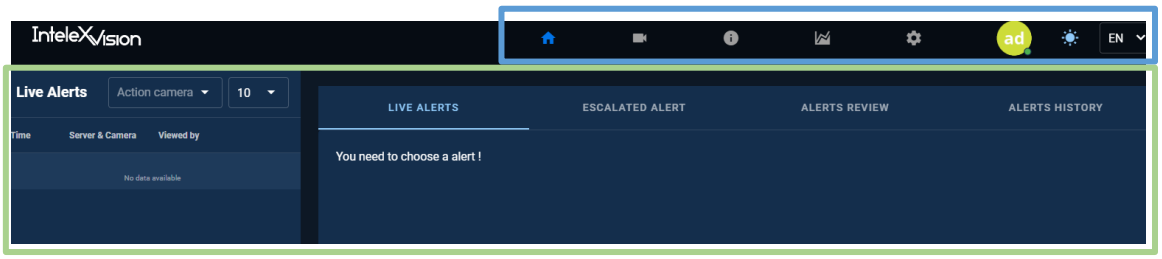
Prepare Installation

To begin the installation process, you will need to download *Sentry WebClient Installers* under latest Release available.

The Sentry software can be downloaded from the official Download Portal. Navigate to the portal, locate the product for which you need the installation files, and select the latest available release. After downloading the software, ensure it is saved and readily accessible on the appropriate servers for installation.

WebClient Configuration and Use

After successful login as an **administrator**, the main screen of **Sentry Web Client** is presented as a Web Page 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

Settings

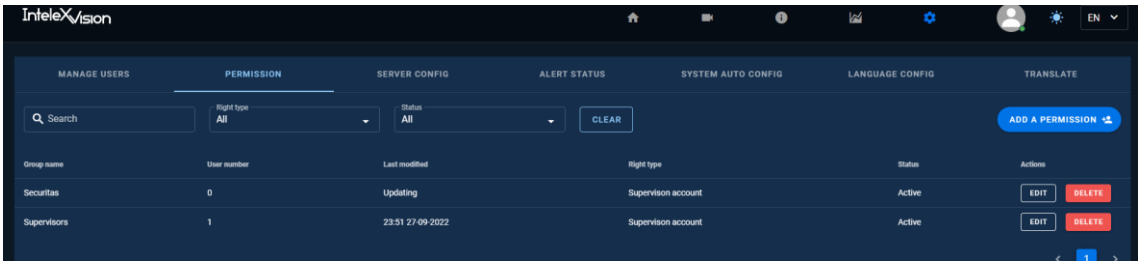
The options included in this menu are depicted in the following table:

Menu	Description
Permission	Add, edit or delete permissions
Manage Users	Add, edit or delete users
Server Config	Allows you adding a server

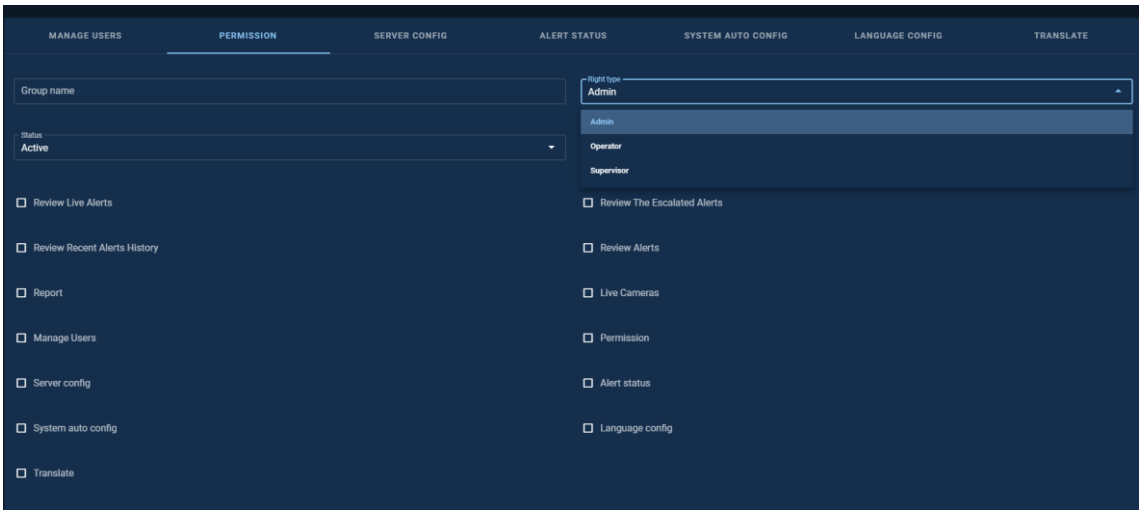
Alert status	Allows you adding statuses
System Auto Config	Allows you entering auto config details
Language Config	Allows you changing language configuration
Translate	Allows you translating the interface
User Match Rule	Allows you to send emails to user matching a selected rule
Camera Config	Allow you to see the list of cameras, their alert count and last received alert. This way you can remove not used cameras.

Permission

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

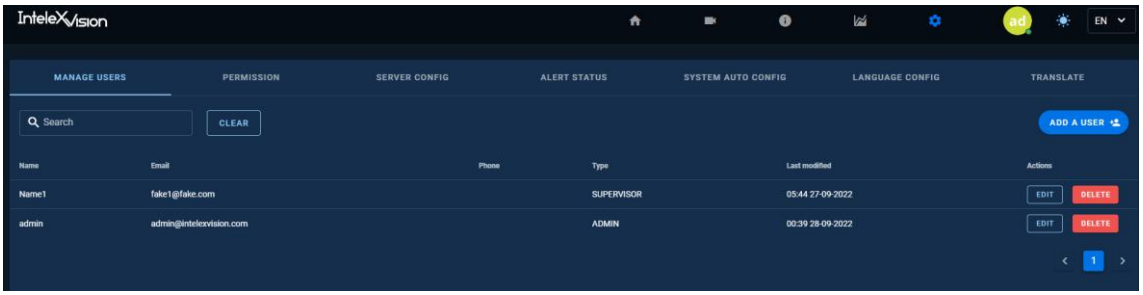


Provide rights that match your current organization, for example Operator (security personnel will fall in this category) and Admin (IT personnel trained).

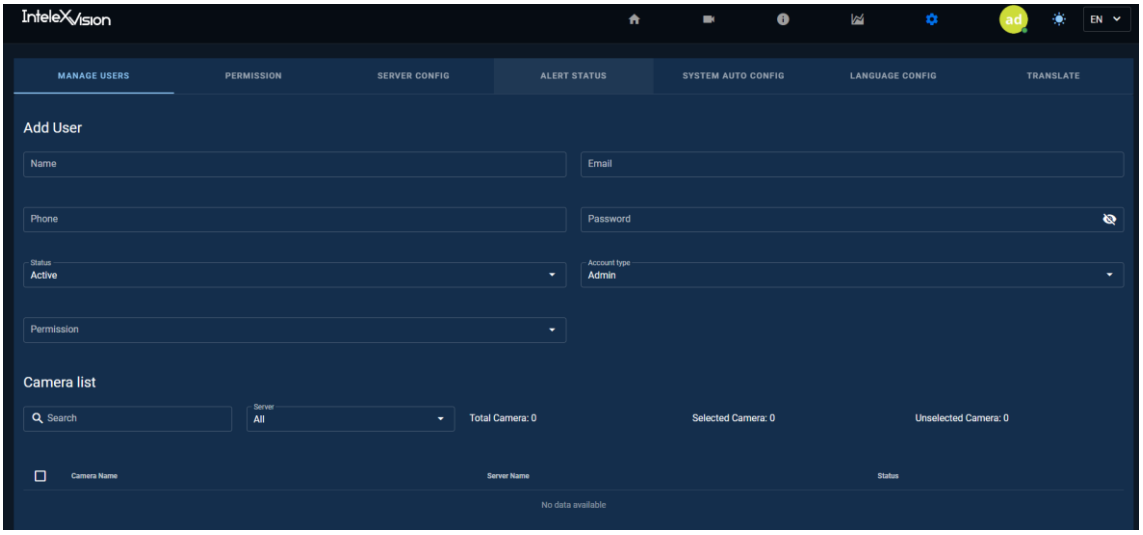


Manage Users

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

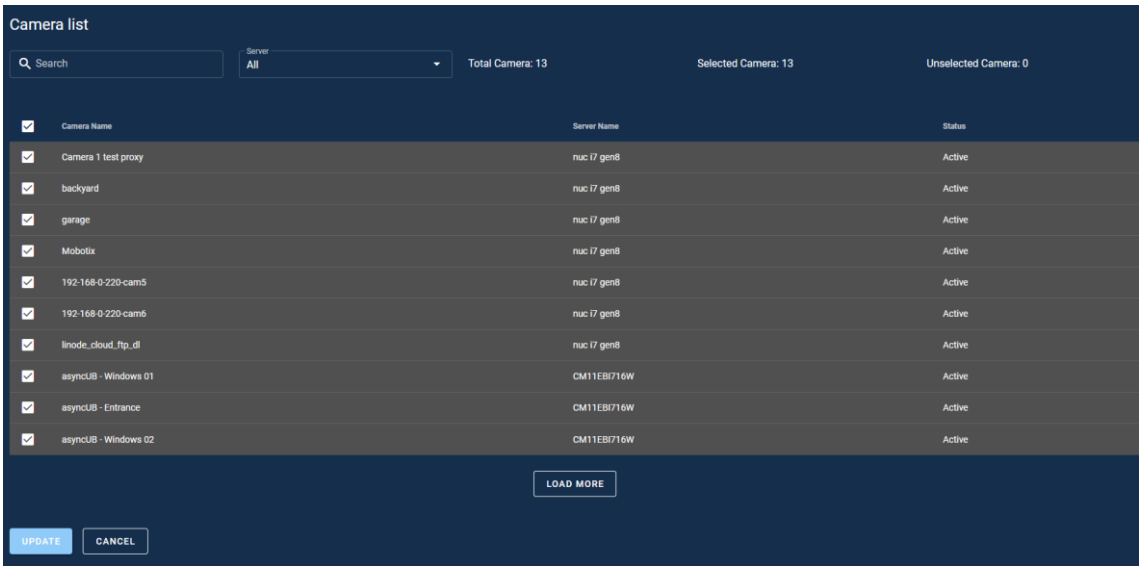


Enter details such as name, email and a minimum 6 characters password. It is important to assign this new user a Permission from the previous step.



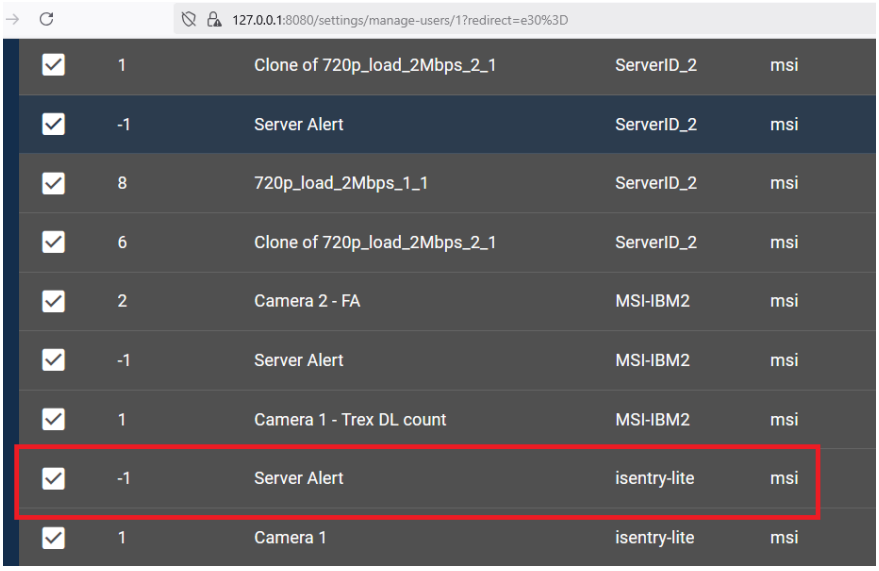
> **IMPORTANT NOTE**
>
> In the Camera List you can add cameras but remember that if you have not set the server yet, it will be empty. You can come back after adding the server and assign the cameras.

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



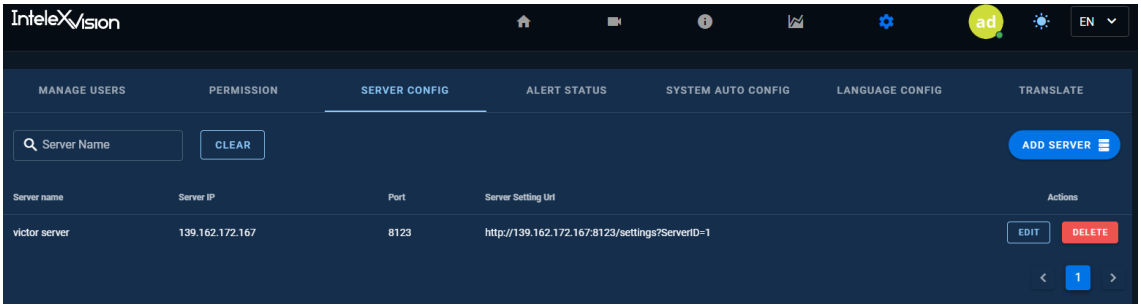
This provides a wide variety of possible combinations by assigning cameras to different users.

> **INFORMATION**
>
> From version 2025R2, there is an extra camera called Server Alert camera (id=-1) to receive global alerts e.g. License Request failure.
>
> From version 2025R3 the list of global alerts has been increased to the following:
>
> - LLSmain failed.
> - LLSbackup failed.
> - Unoptimized DL.
> - DL overload.
> - Aurora overload.



Server Config

Press the button Add Server from the image below to link the **Sentry WebClient** with an up and running **Sentry Firefly.**



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

System auto config

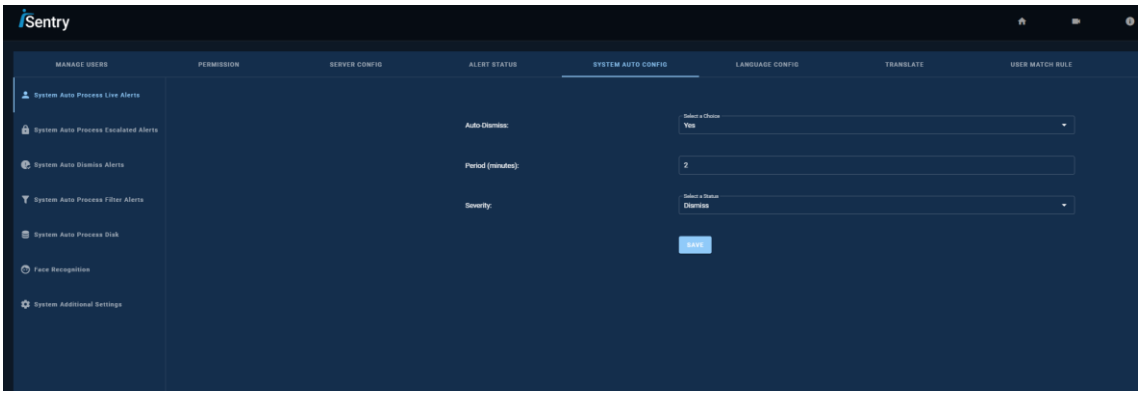
In this menu you can find the following options.

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 deletion.
Face Recognition	Enter the details to connect to the FR system.
System Additional Settings	Decide whether to show Aurora Questions

System Auto Process Live Alerts

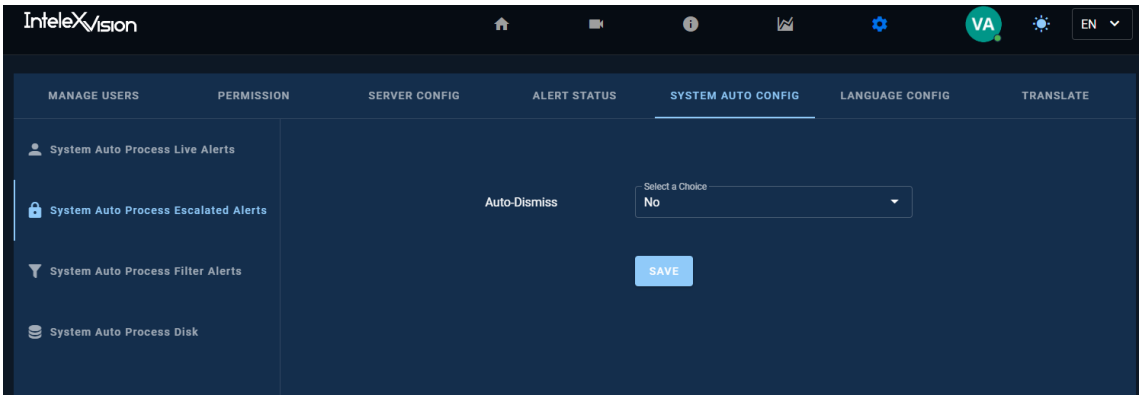
By setting this value we have more control of the alerts detected. Select YES and enter the value for the period of minutes before Auto-dismiss and the Alert Severity level.

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

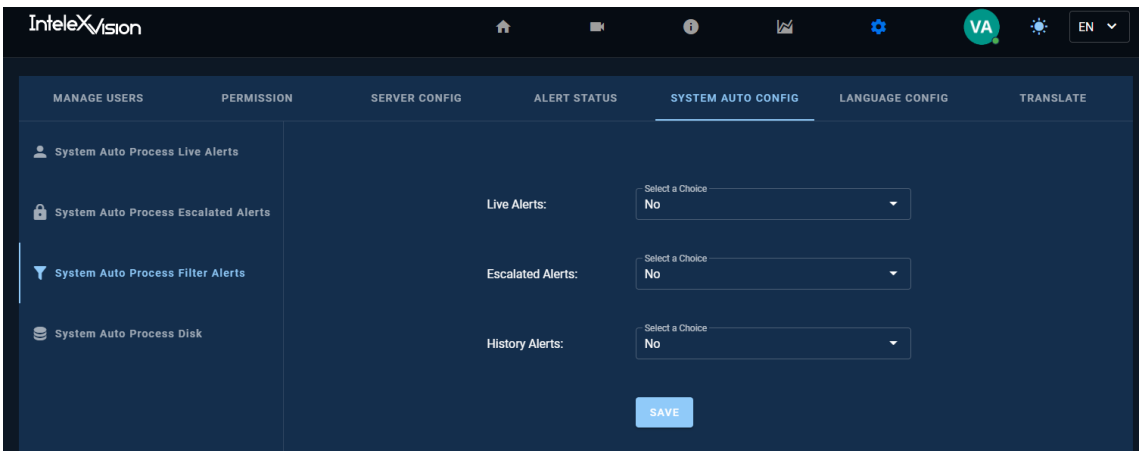


System Auto Process Escalated Alerts

By default, it is set to No, the user can decide whether the system takes care of Escalated Alerts. When entering YES, the system will ask for a period of minutes before dismissing the Escalated Alert.



System Auto Process Filter Alerts



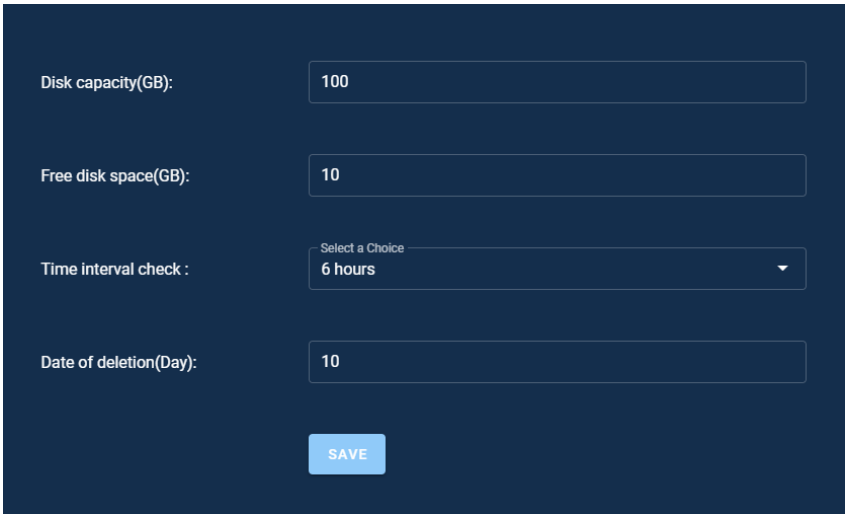
System Auto Process Disk

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.

> **IMPORTANT NOTE**
>
> Skipping to set this up could end up with your local drive full, causing the Sentry WebClient to stop responding.

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

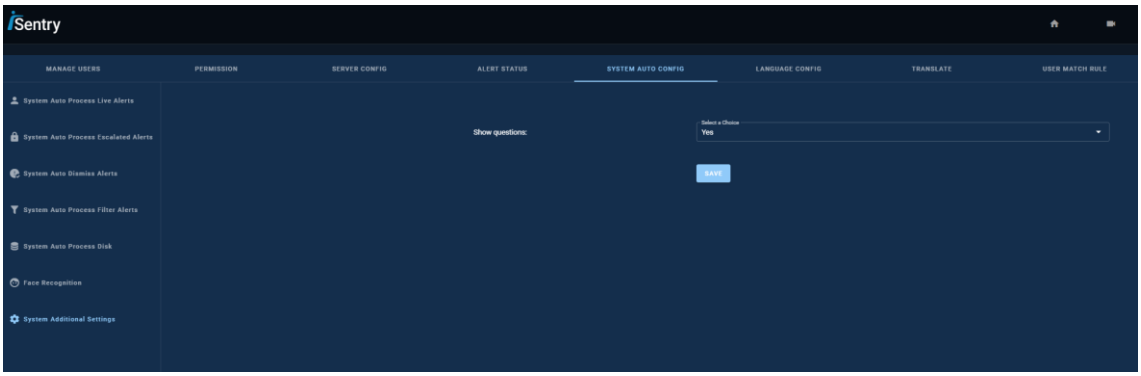
Date of deletion (Days): The number of days data on Disk must remain. Please note this depends on the Disk capacity and free disk space. If you enter 30 and it is 1st of September, you will delete 2nd of August (cause August has 31 days).



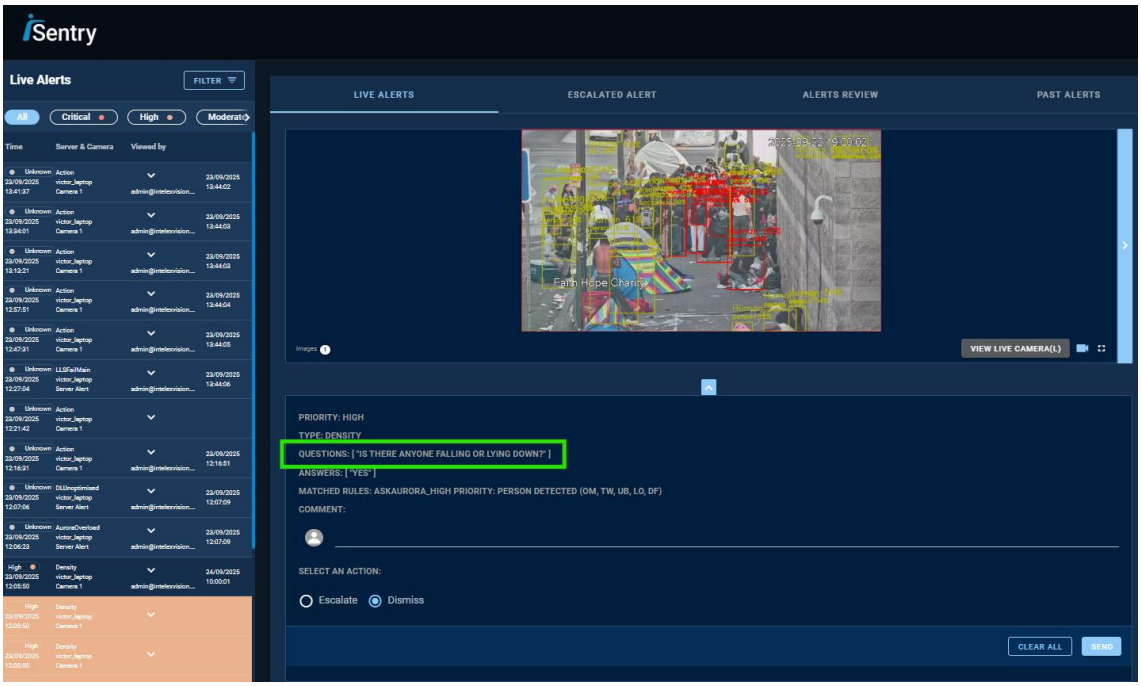
Face Recognition

System additional settings

This setting allows to choose whether the question defined in Aurora's Rules is displayed in the alert view. If enabled, operators will see both the question that prompted the answer and the answer itself, providing greater clarity when reviewing alerts.

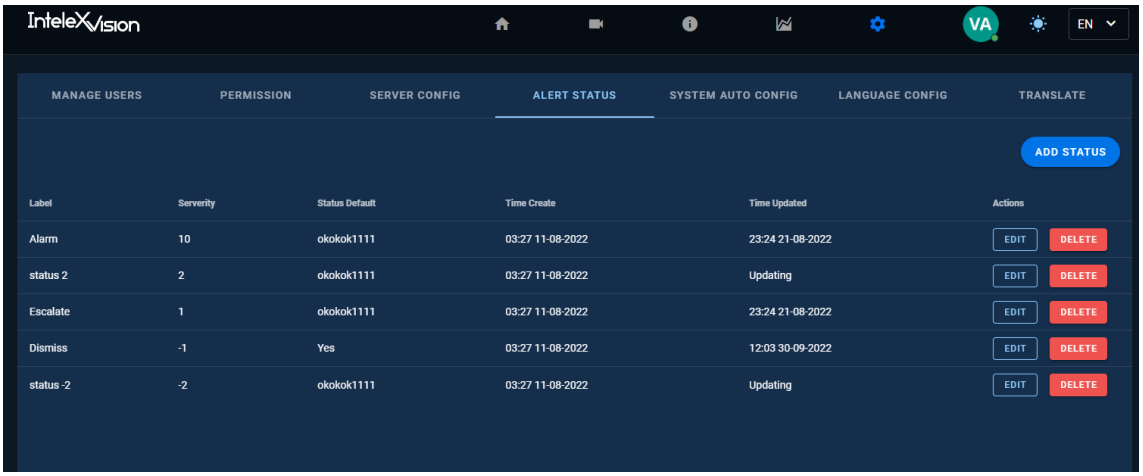


If you choose YES (which is the Default Value), the question will appear when accepting the alert as it's shown below.

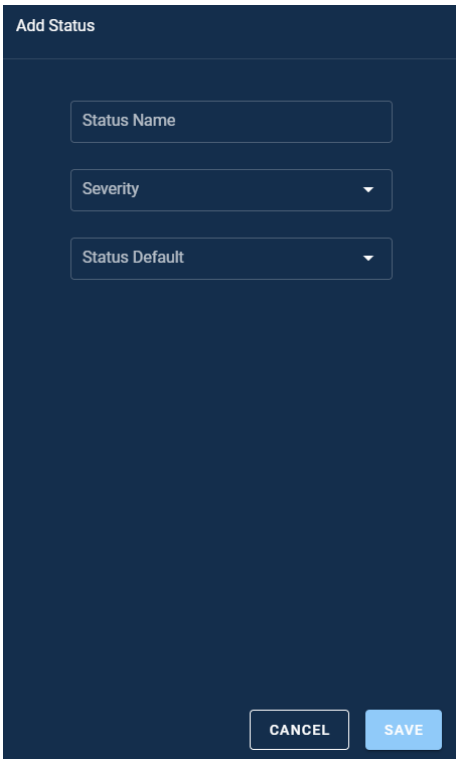


Alert Status

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

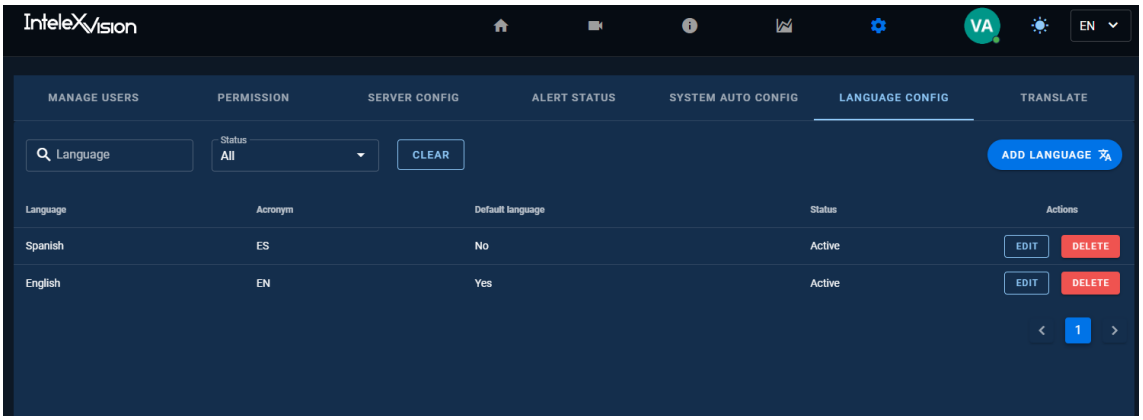


Adding a new status involves providing a name, level of severity (10 higher, -10 lowest) and whether the status has a default behavior. The severity plays an important role when moving alerts to different views, high priority moves the alert to Escalated in the Dashboard while low priority moves them to Alerts History in the Dashboard.

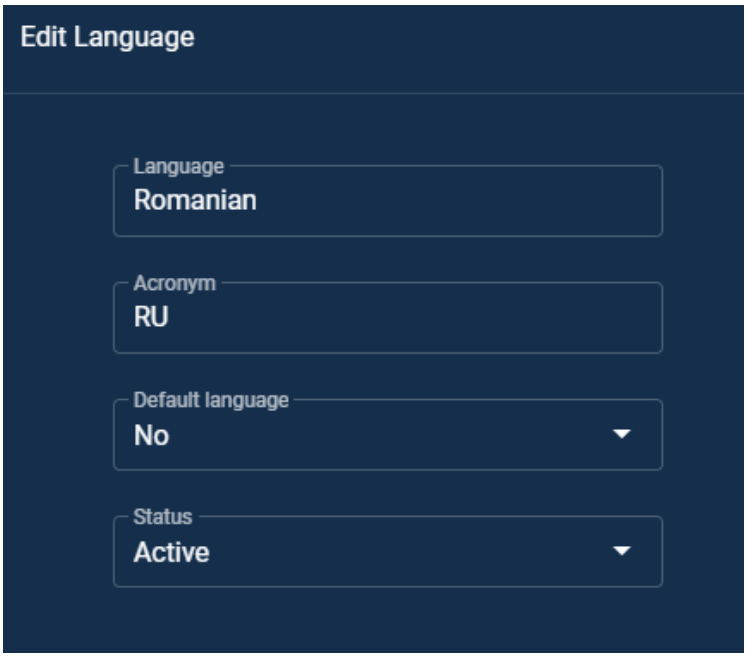


Language config

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.



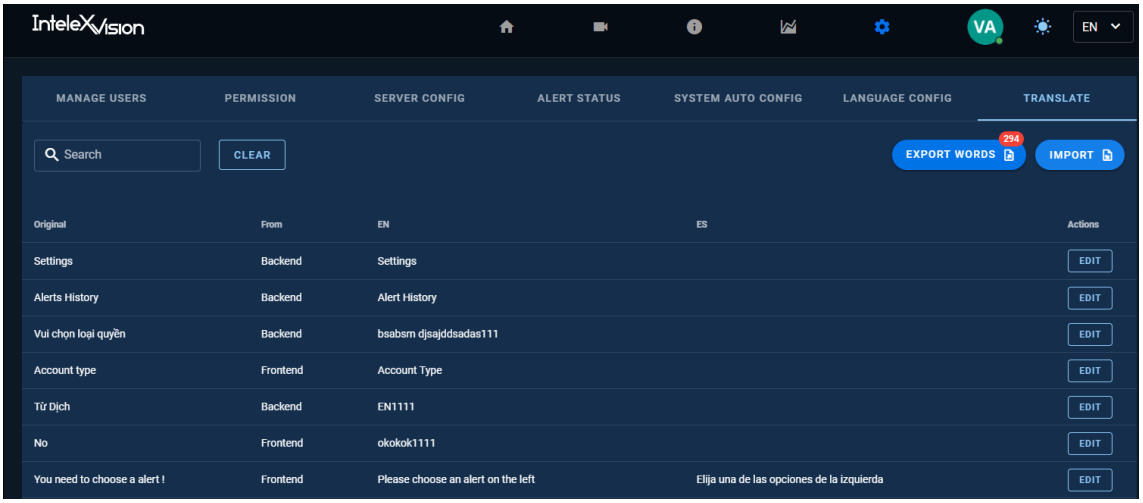
For example, we'd like to create a new language, let's go with Romanian:

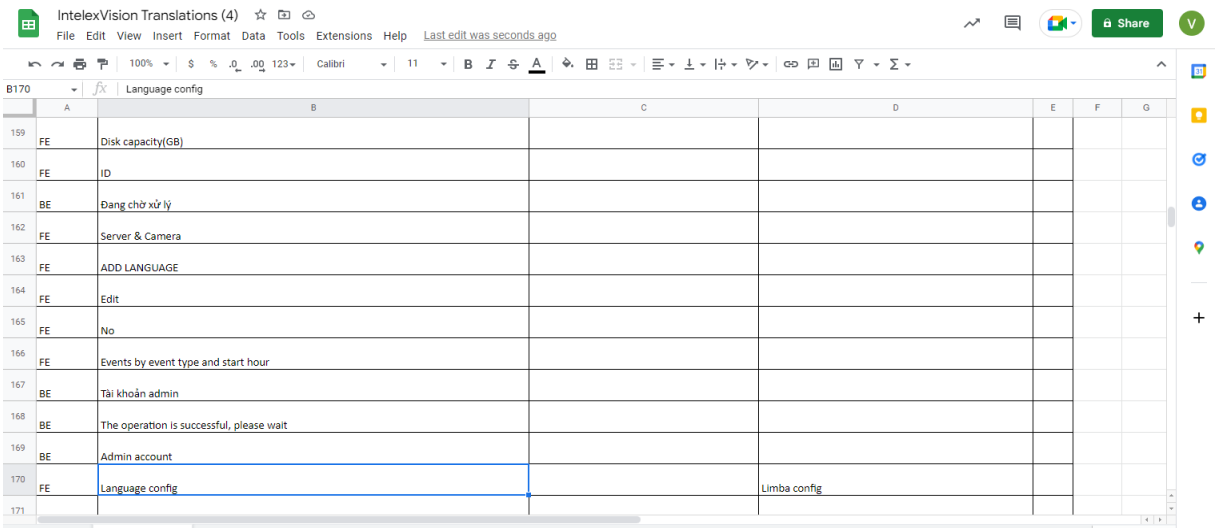


Now go to the next section Translate to enter specific translations for specific words. In this example we will translate the word "Language" from English to the Romanian equivalent which is "Limba".

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.

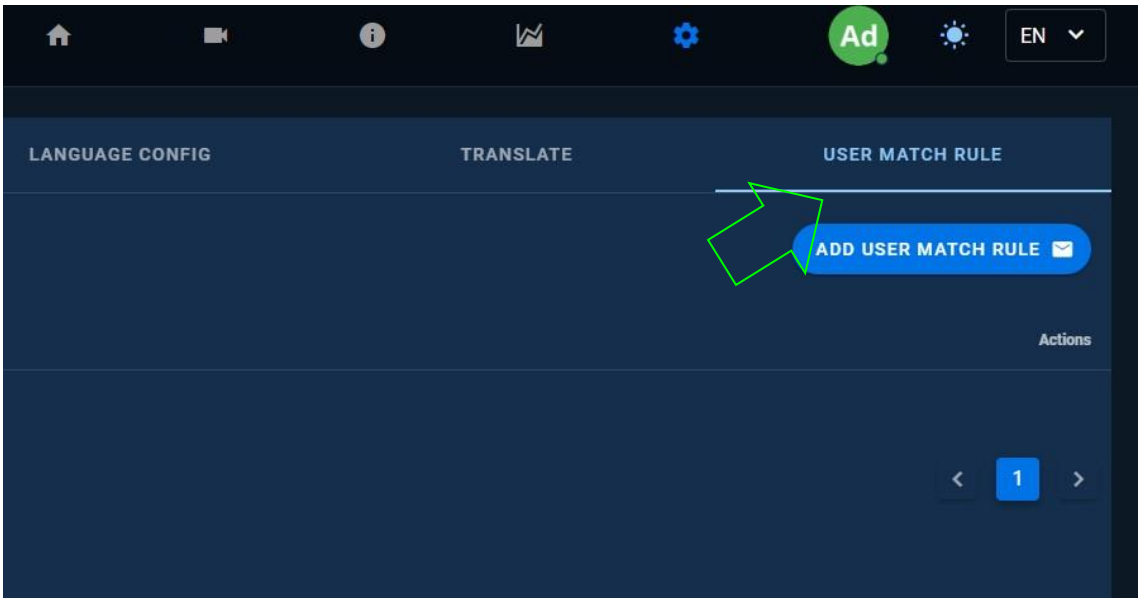


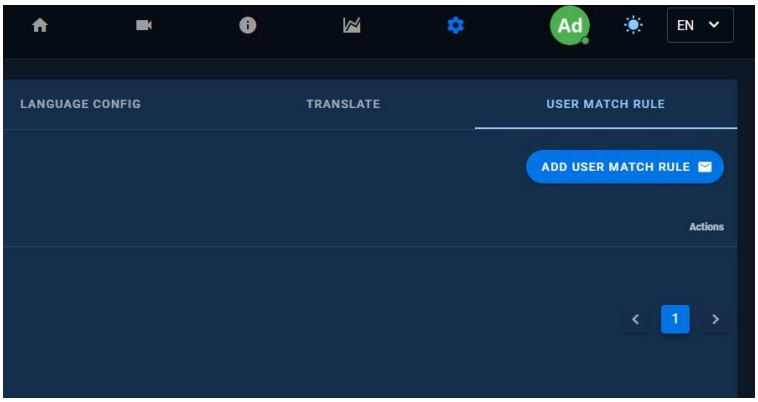


Once finished, click save and proceed with Import, you will see the results after refreshing your view in your browser.

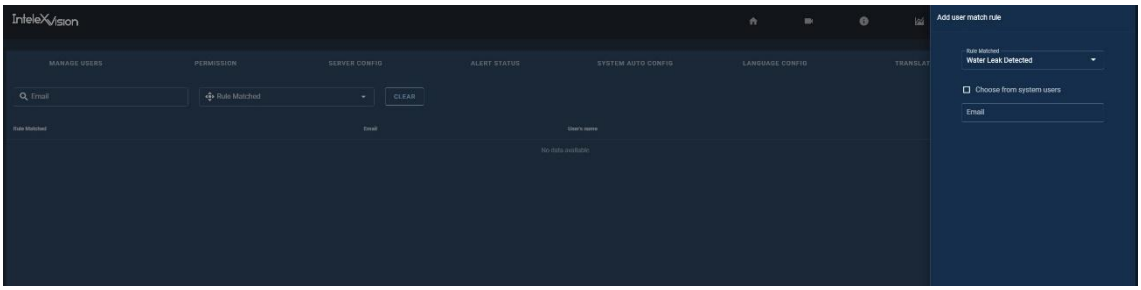
User Match Rule

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.





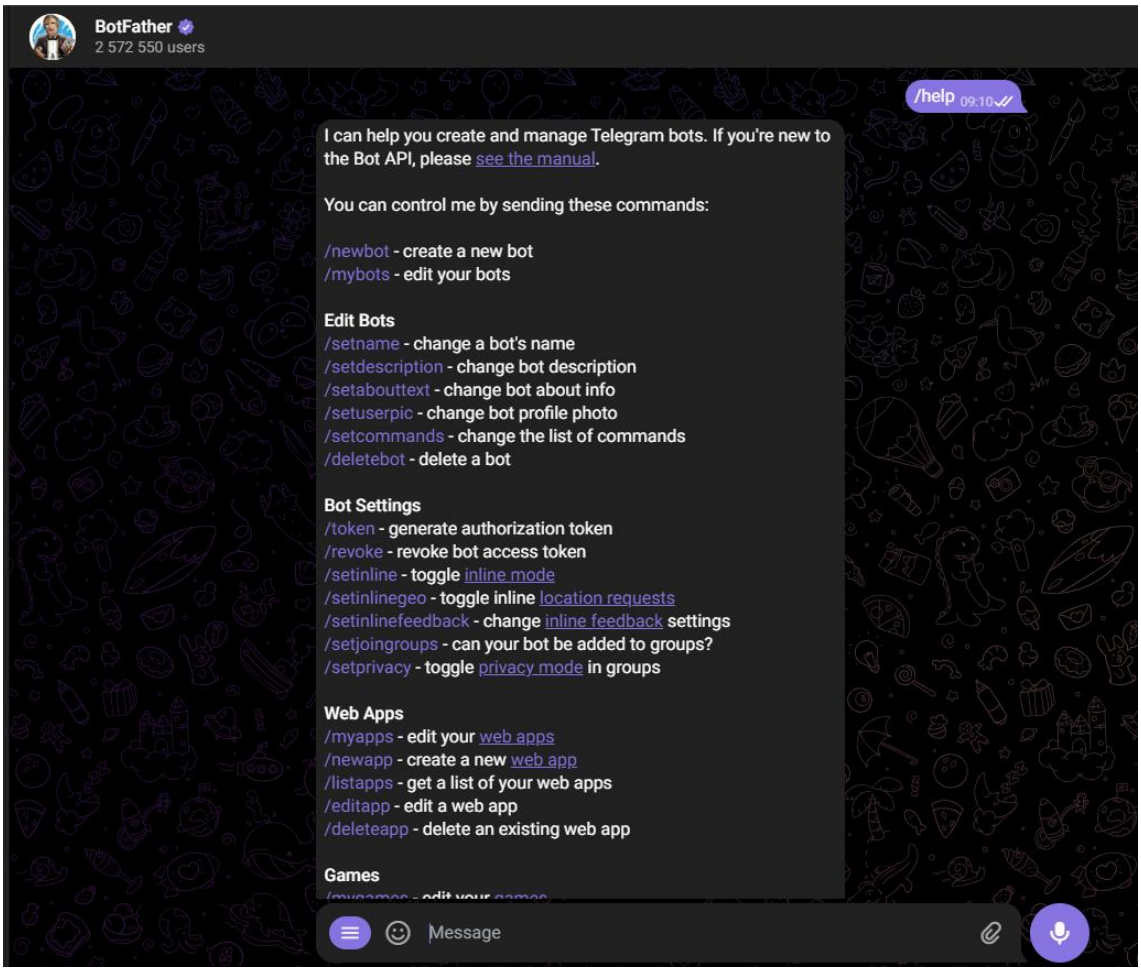
From the menu we select the Rule we want to act as a trigger for the email, also select the email from the system list of users, or enter a custom one. Please be advised that this can cause spam when the Rule is highly triggered (like cars in highway with TREX).



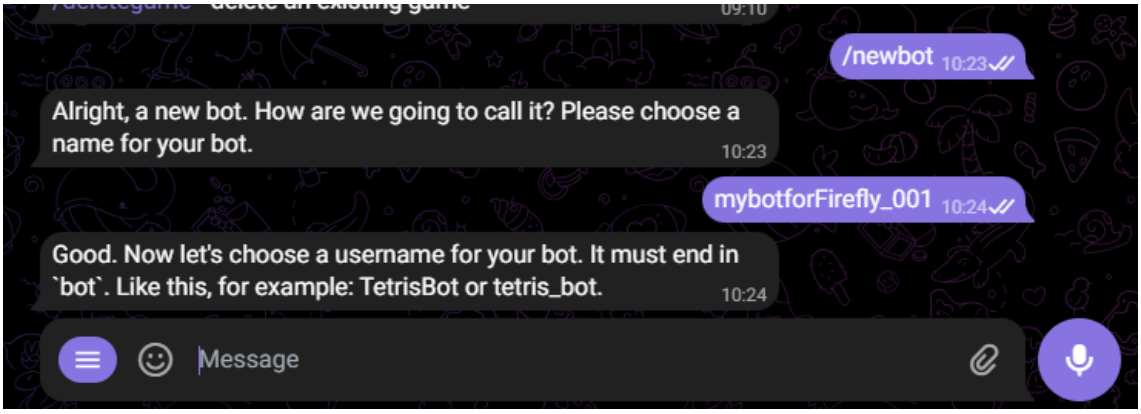
Telegram

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. Please follow the following steps.

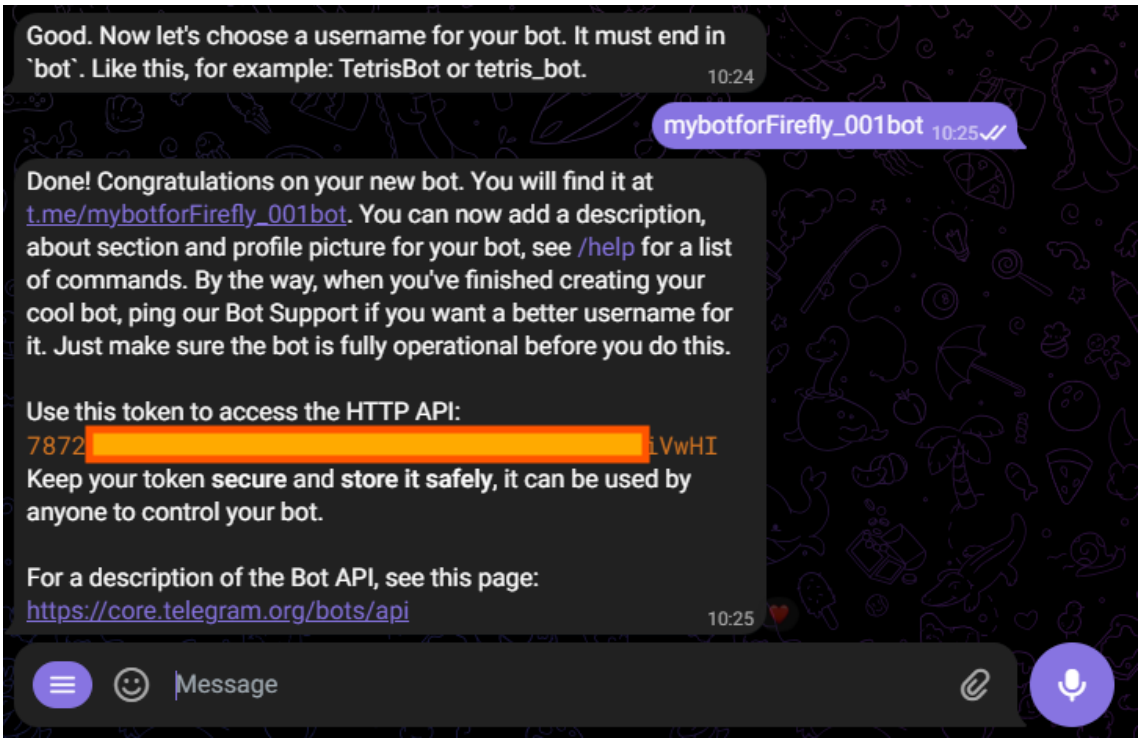
Install telegram then install @BotFather, type /help to see the list of available commands, we will use /newbot.



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

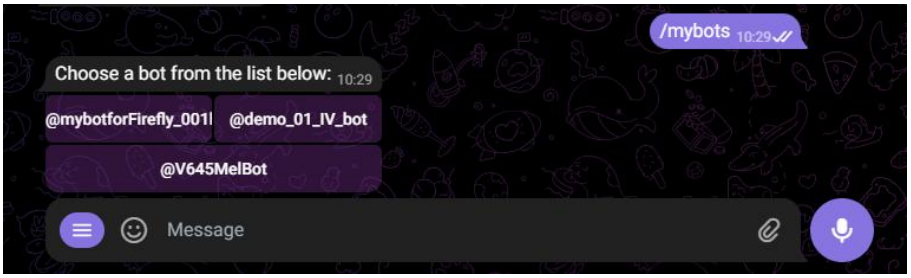


Give it a name having into account that it must end with ‘bot’.

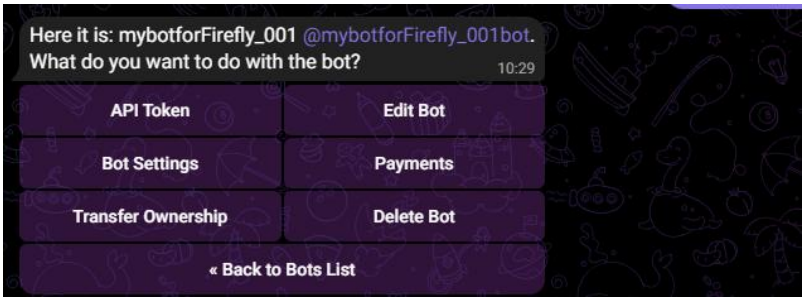


Get the API Token (8196639422:AAF....) and do not share it as it is sensitive. We click on "API Token" we still can copy anytime we want. Now set two commands for your bot, one to subscribe to the rule and another to mute it (or unsubscribe).

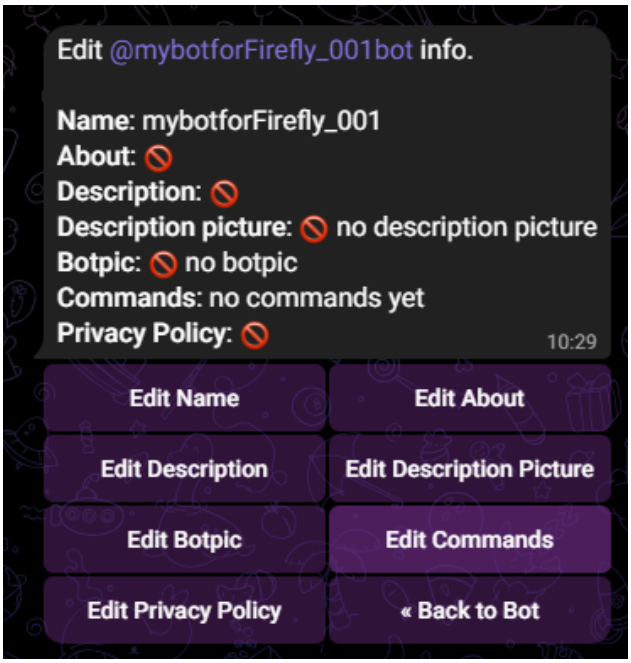
Select our created bot by entering /mybots and clicking on it.



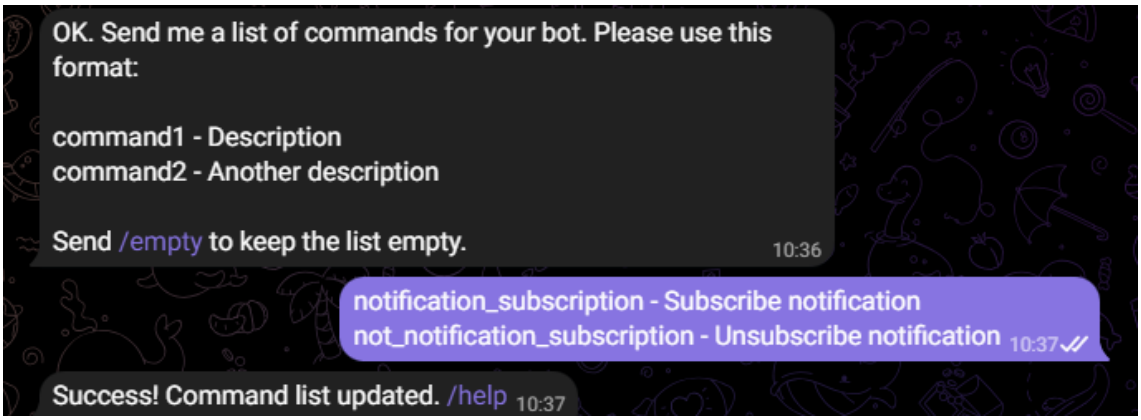
Then click on edit bot:



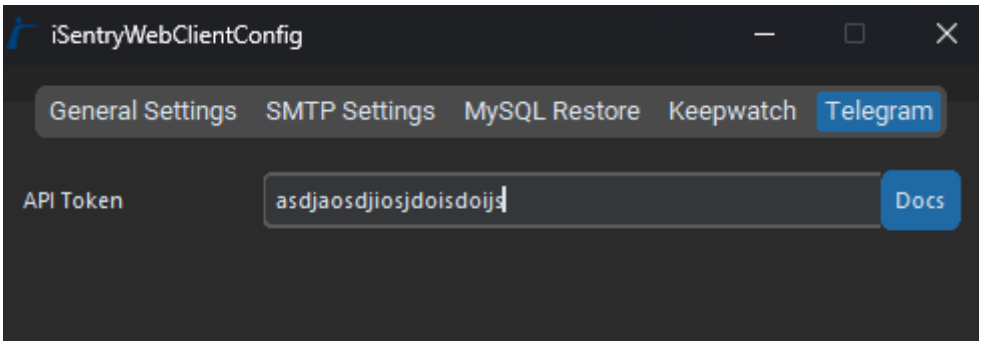
And then edit commands:



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.

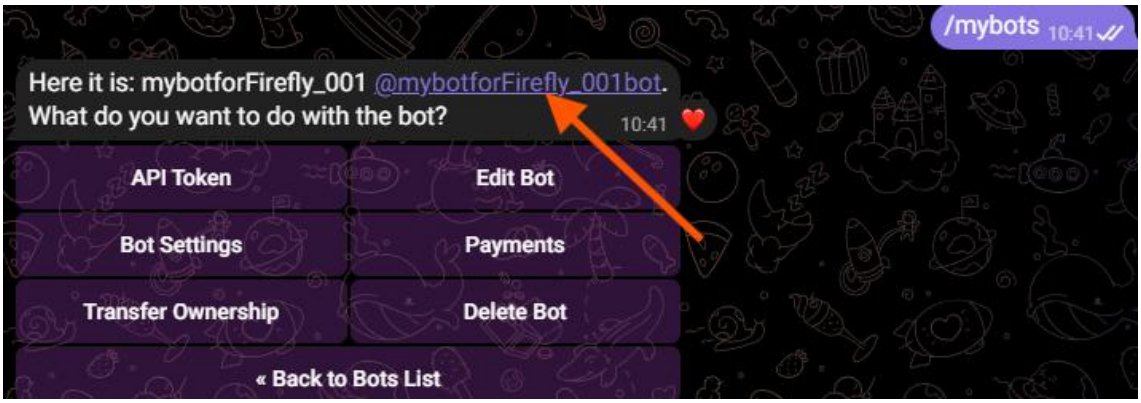


Now open your isentryWebClientConfig by pressing windows key and typing it.



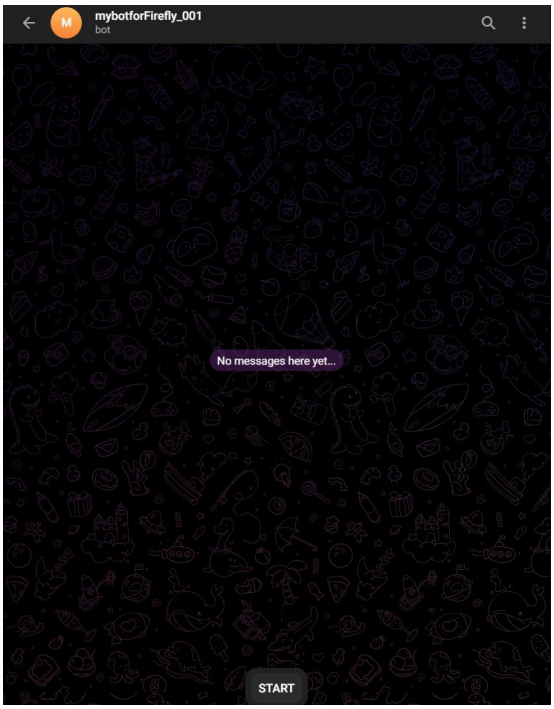
Enter your API token obtained in the earlier steps. Click Save and Restart.

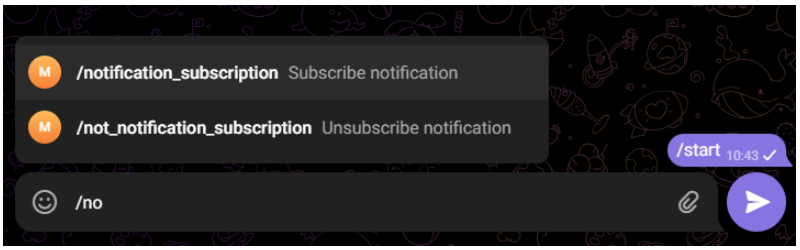
Now let's back to Telegram and talk to your bot by going to @BotFather again and click onto the bot:



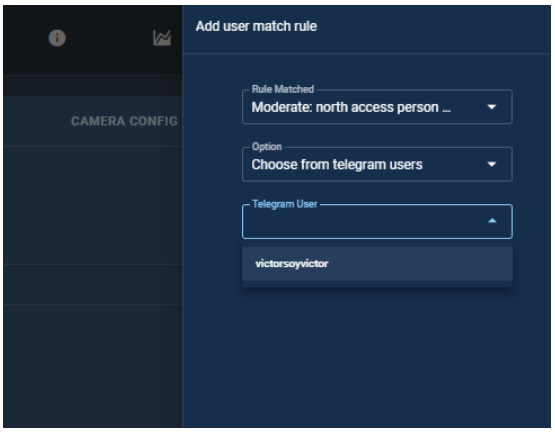
Then click START in the image below and send the command you previously created:

/notification_subscription





Finally, we go to the **Sentry 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 must verify your steps.

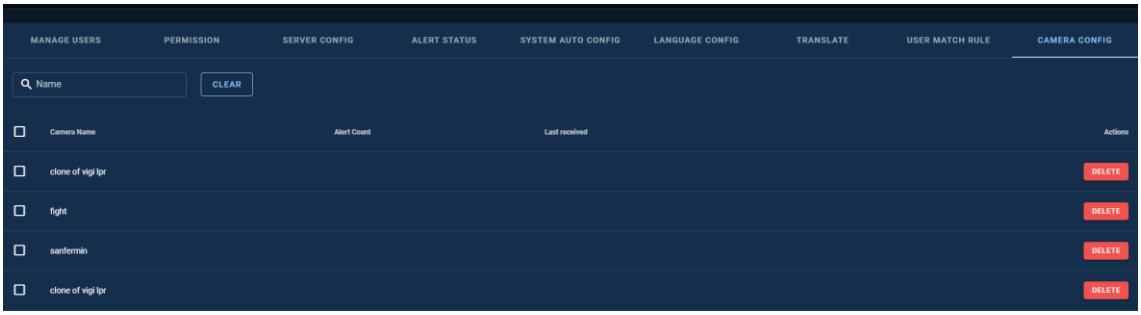
Hit save at the bottom of the website.

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

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.



Group Camera Config

This tab is part of the Keep Watch, section 3.6, where you can monitor and manage your surveillance activities.

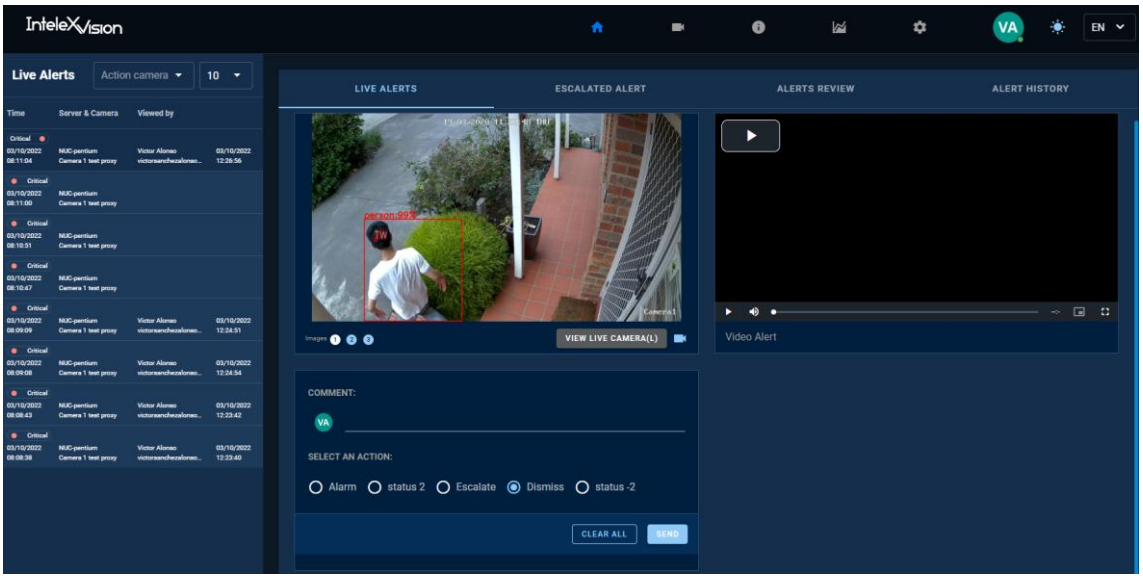
Dashboard

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 is displayed, on the right side we have 4 views: Live alerts, Escalated Alert, Alerts review and Alert History.

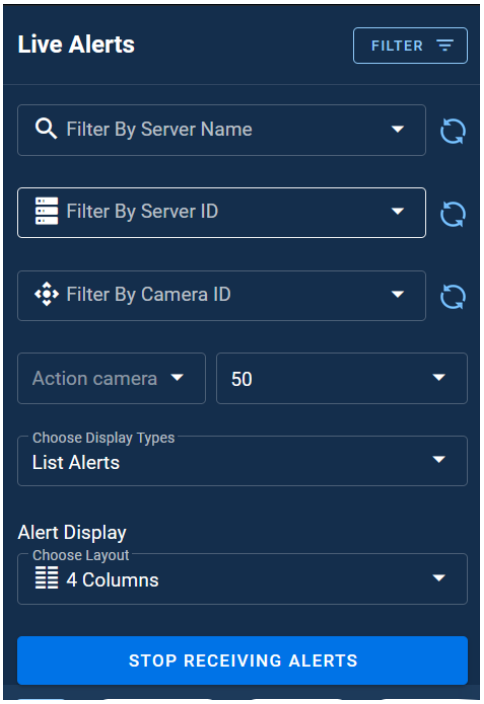
Live alerts	Main view of the Alert that is selected, with 3 sub views: Video, Detection and Comment. You can also activate the Live View of the camera, shortcut L key from your keyboard.
Escalated Alert	From this view, the operator or supervisor can now Dismiss or Approve the Escalated Alert.
Alerts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

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).



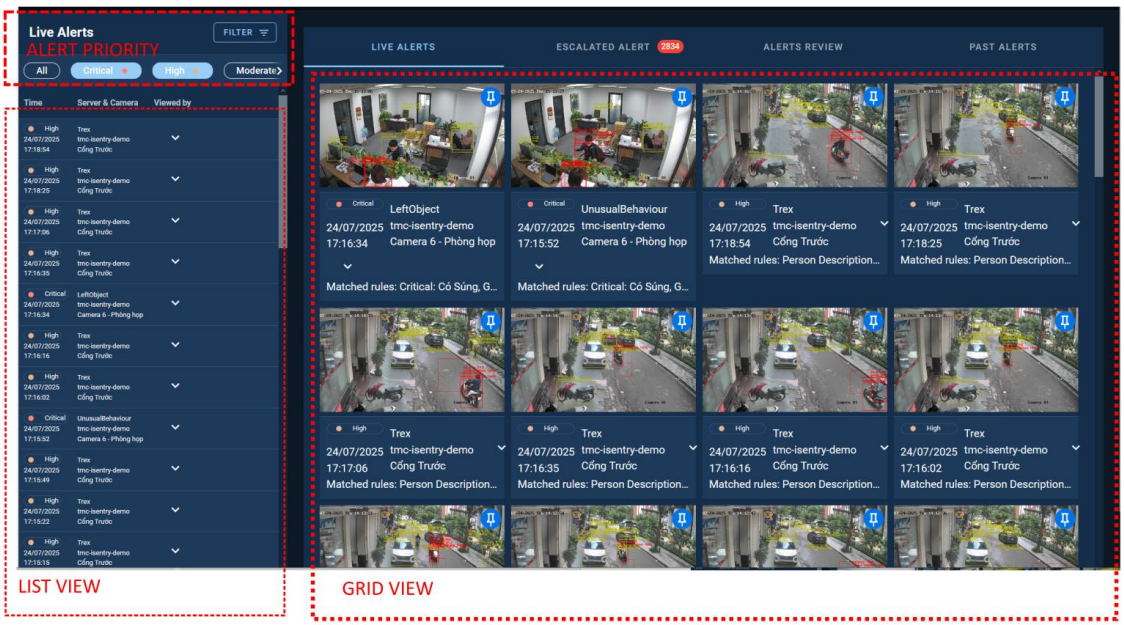
Live Alert Filter



Live Alert – Sort by Priority

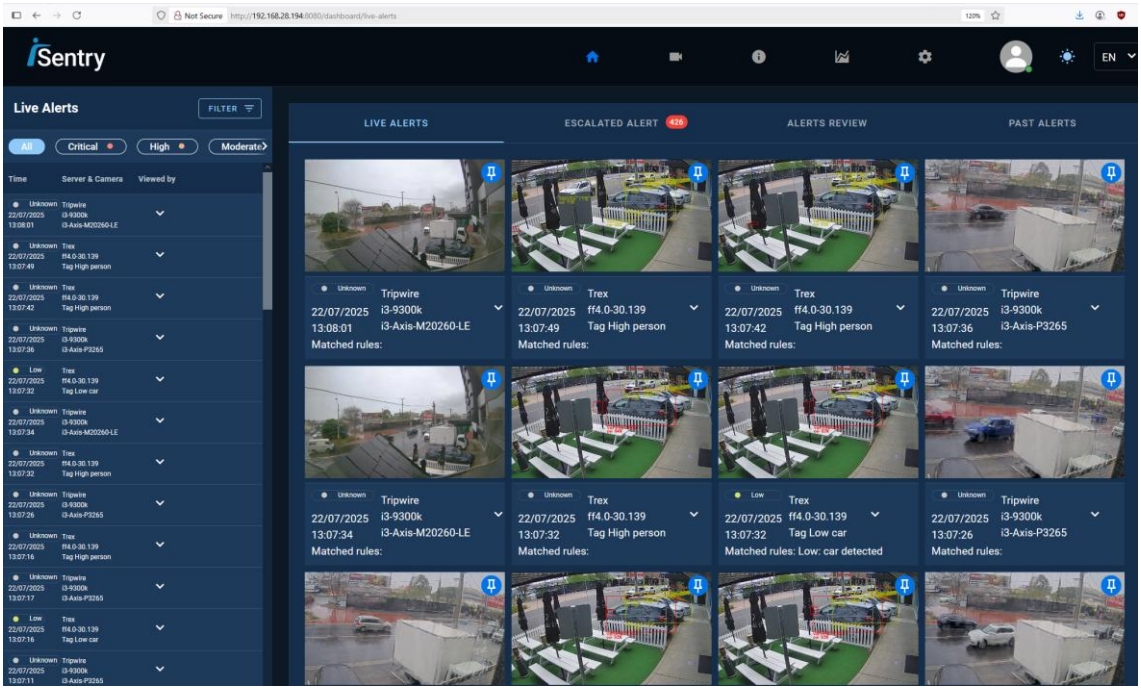
At default, all alert types are enabled (ALL). When one of priorities is selected, while the list view shows only alerts with selected priority, the grid view sorts alert in order of priority level then timestamp.

Priority level: Critical → High → Moderate → Low → Very Low



Grid View

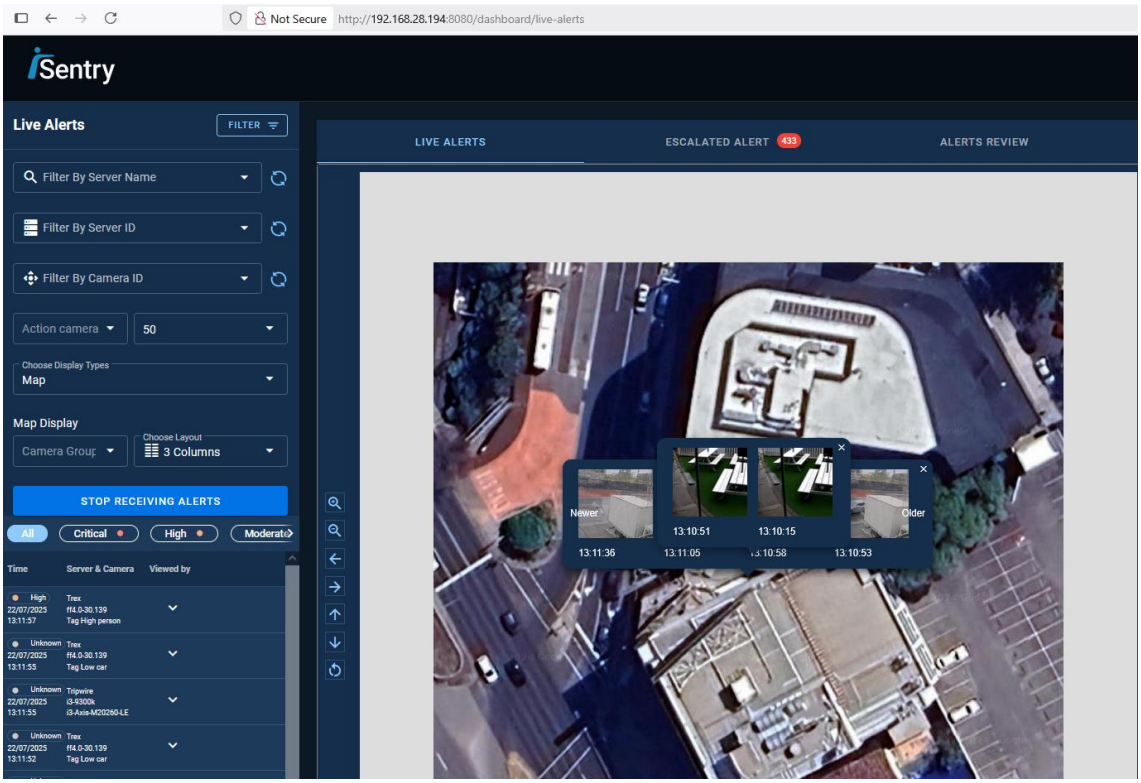
This feature is available from version 2.3.0, allows user to view Alerts in grid layout.



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

Map view

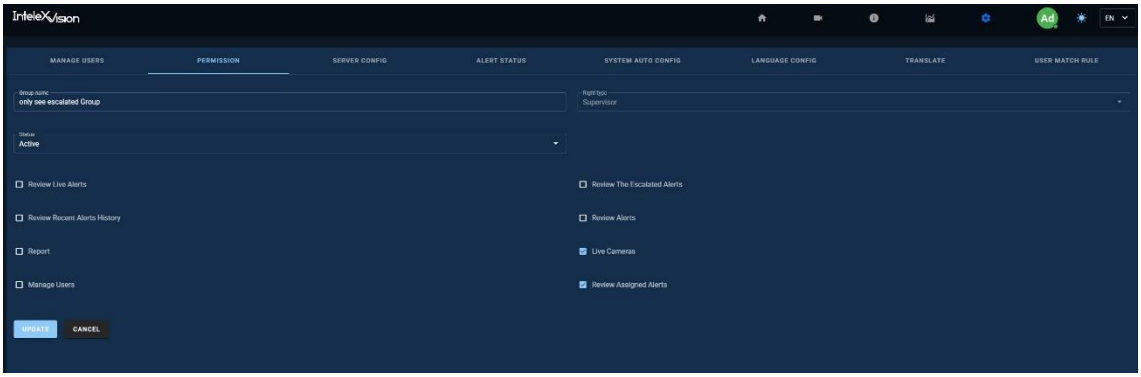
Map is selected from Choose Display Types. The map image defaults are not available and need to be configured in Group Camera Config settings.



Send live alert to selected user

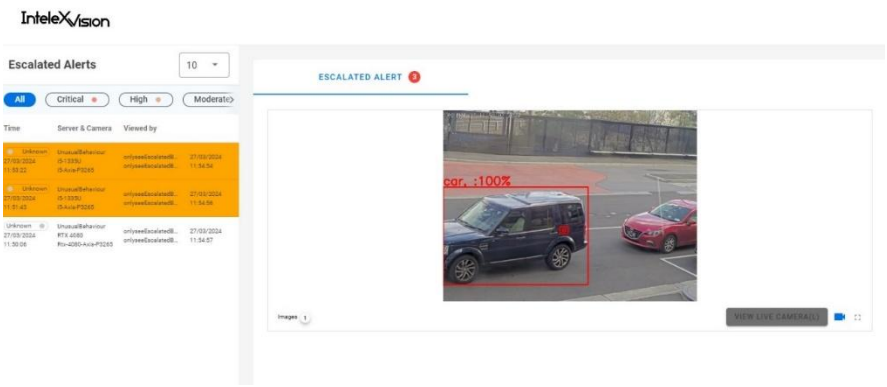
The user can send an alert to an operator with elevated permissions (Supervisor, Administrator, etc.).

For this first step is to create a permission group and add this user as Supervisor with Review Assigned Alerts box selected:



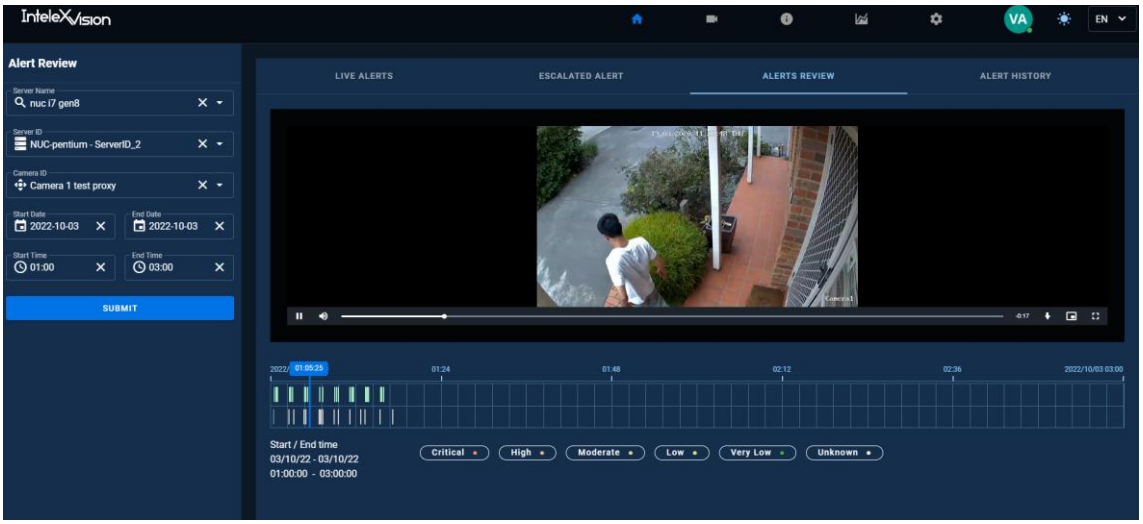
After that from the Live alert view you can click and send to that user:

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



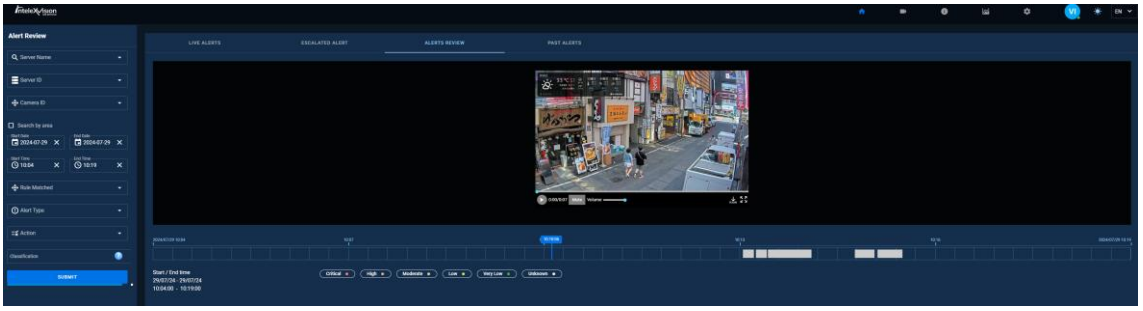
Alerts review

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.



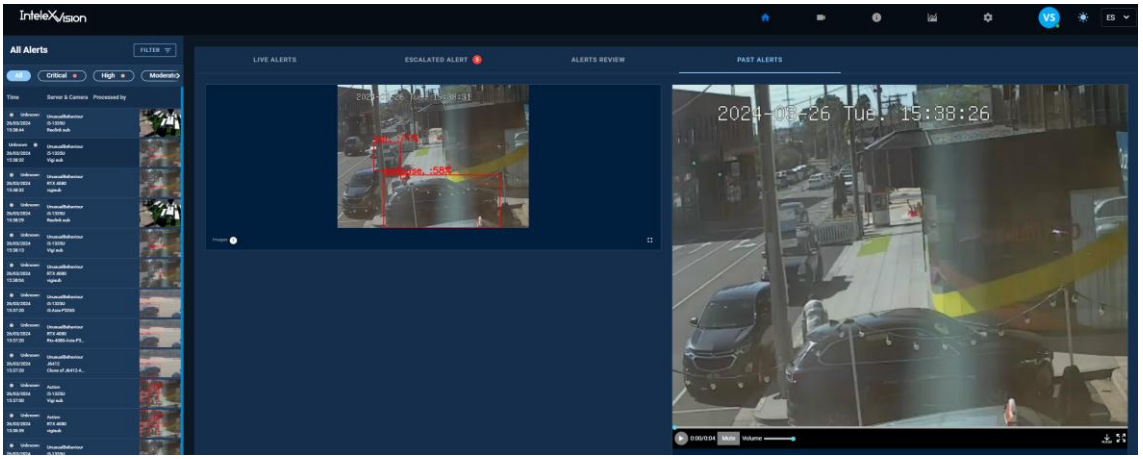
The web client can play playback videos from a **Sentry Firefly** when they are in the same local network. In the lower panel the user can see the timeline and marked in colors corresponding to the severity of the alert the access to the video of the alert.

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

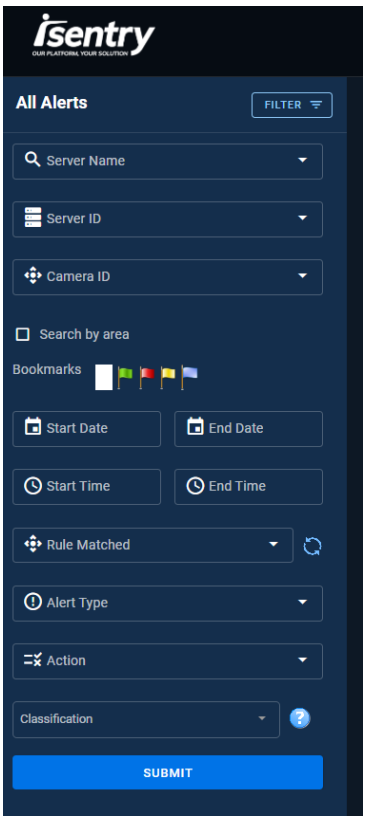


Alert History (Past Alerts)

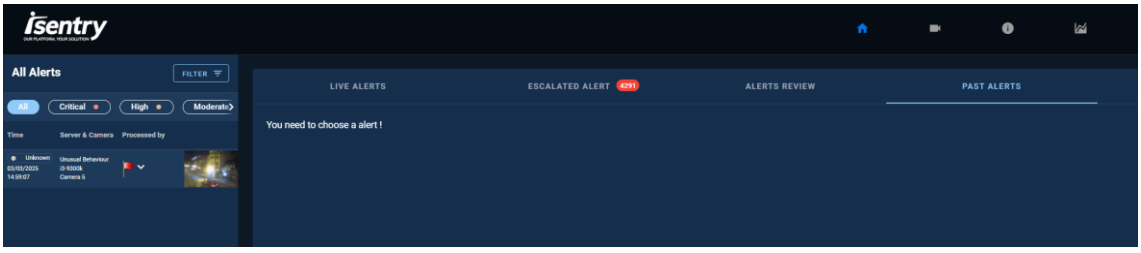
At any time, the user can have a look at the past alerts to see what actions were taken (Comment panel) plus the short and 20 seconds videos of the selected alert.



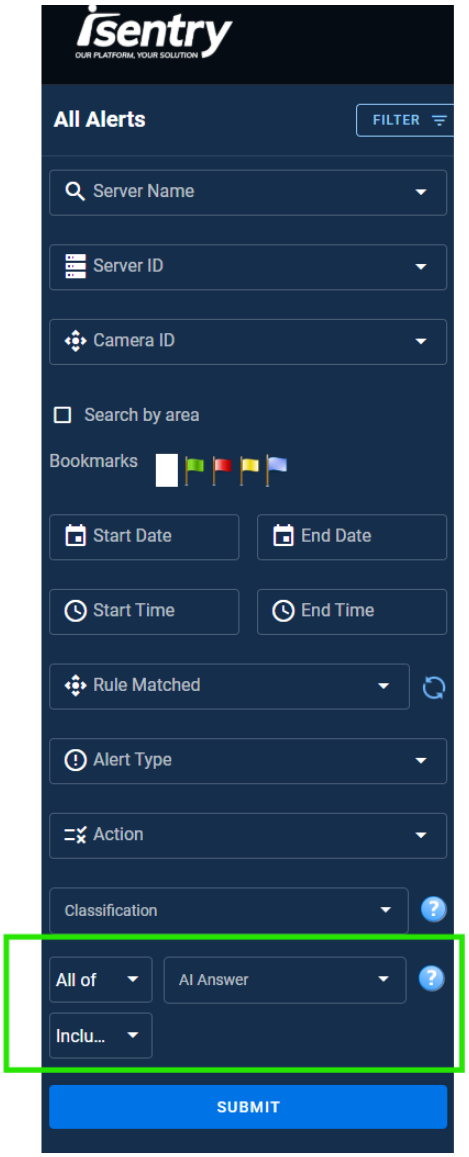
The user can apply filters to find what is of interest. Filters can be applied to the fields shown in the image below. A new button appears next to the Rule Matched to refresh any recently created rule and refresh the browser cache.



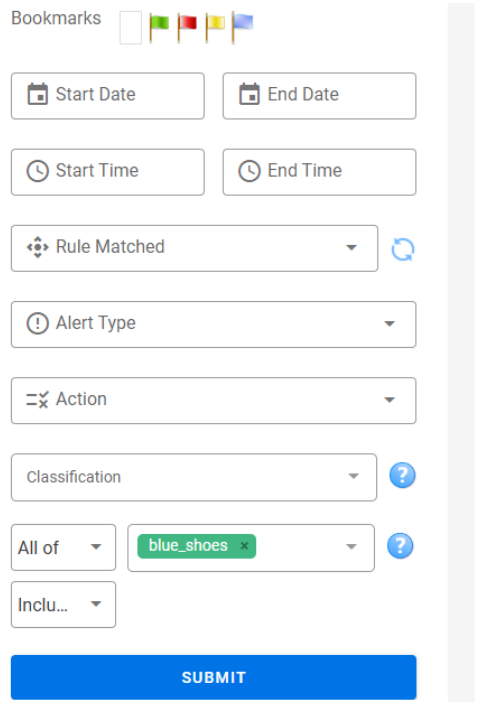
Now the user can bookmark the alerts for later retrieval and inspection using the flags like the colored flags above to see them.



The user can also inspect the alerts using the **Aurora** model. For example, one can retrieve information regarding the questions made to **Aurora** as part of a Rule configured in **Sentry Firefly**.

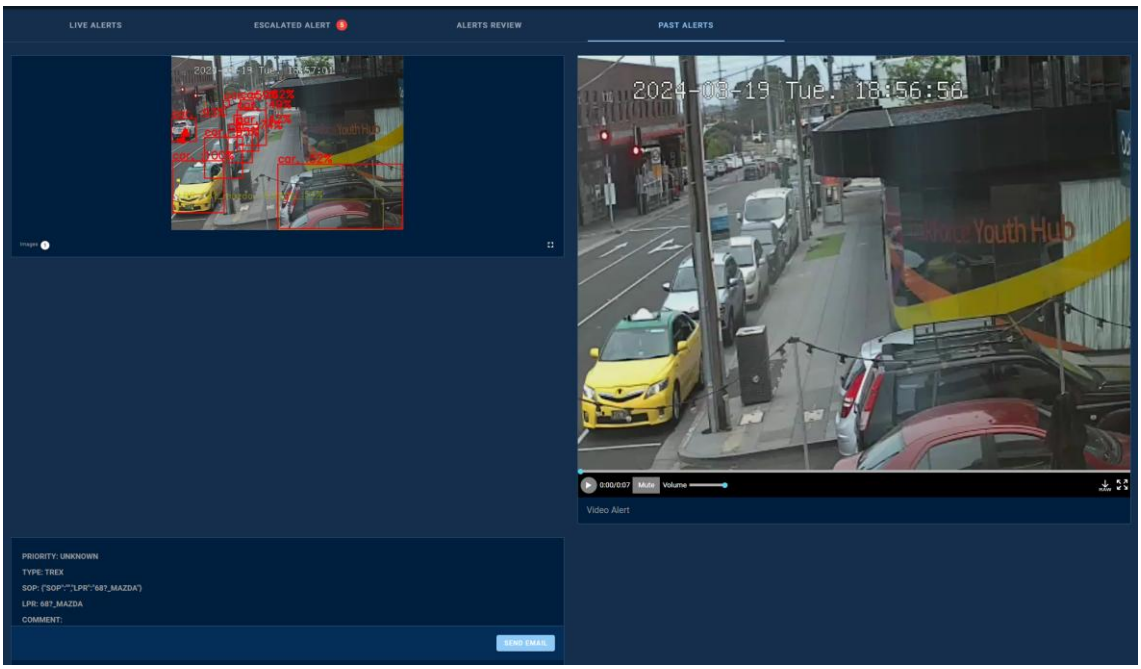


Given alerts such as below when you configure **Sentry Firefly** with **Aurora**, one can easily go to the filter menu and enter keywords from the questions above to retrieve alerts that matched the criteria, some examples could be “find a person wearing blue shoes”.



Show Alert SOP and third-party result per alert

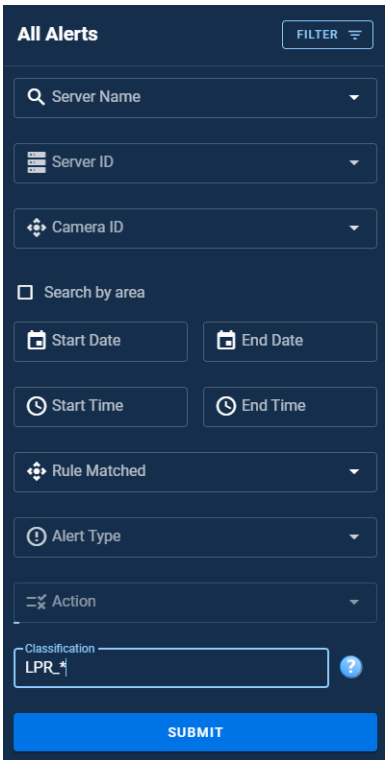
Now you can see the SOP and the 3rd party per alert below the alert image:



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

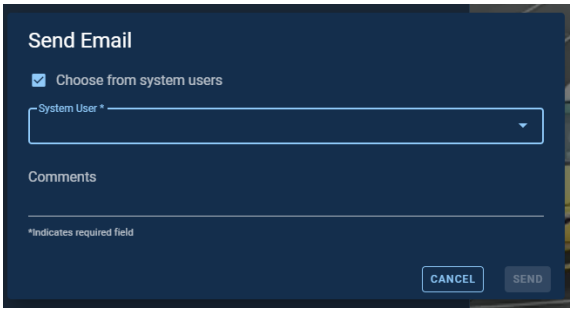
Regex search (and exact search)

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



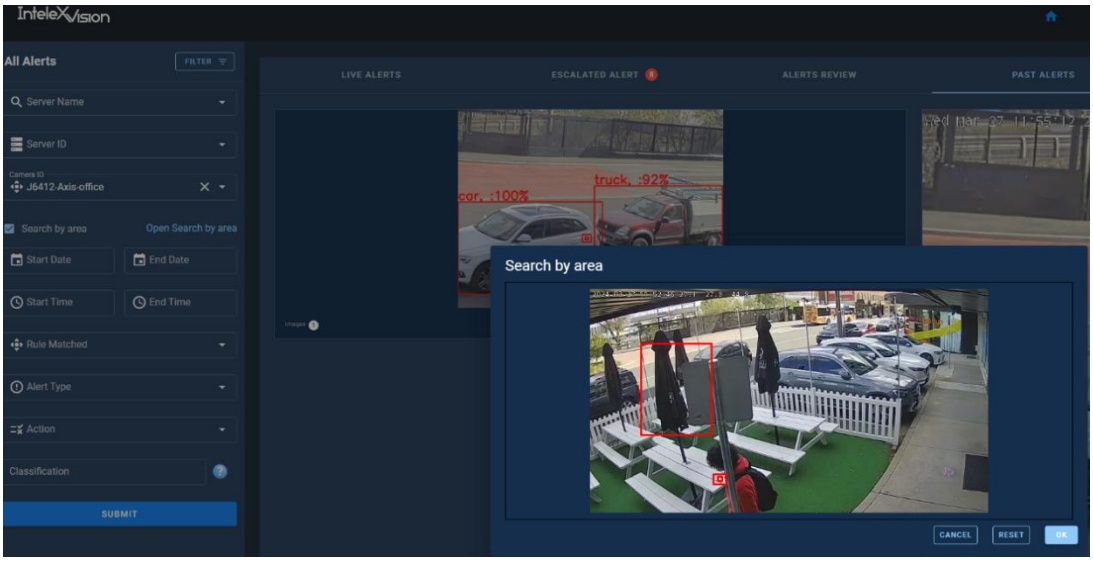
E-mail alert report to user(s)

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

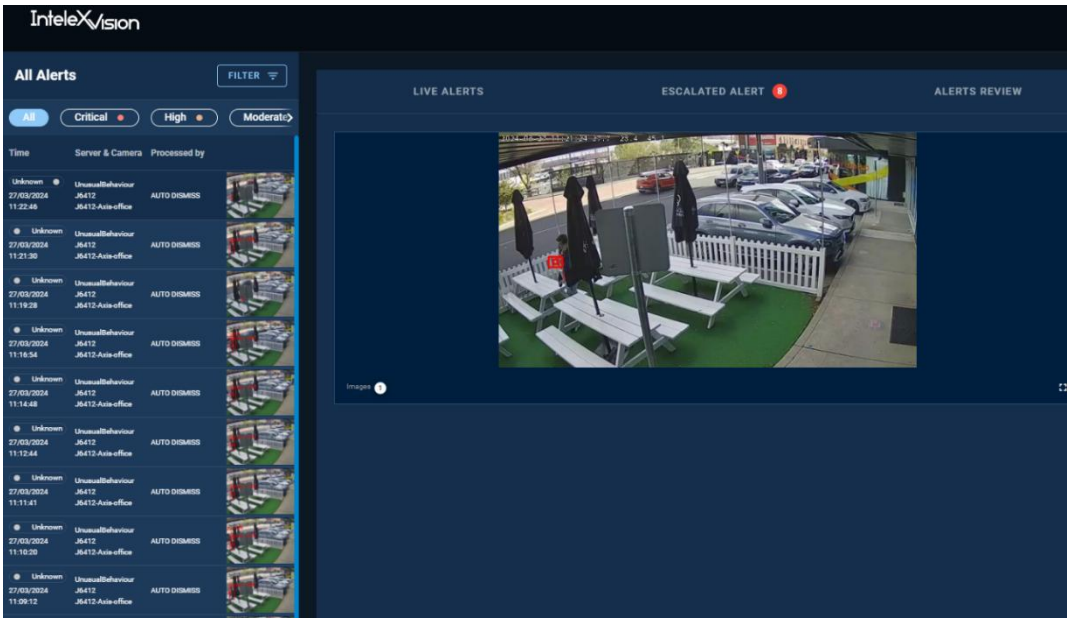


Search by area

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.

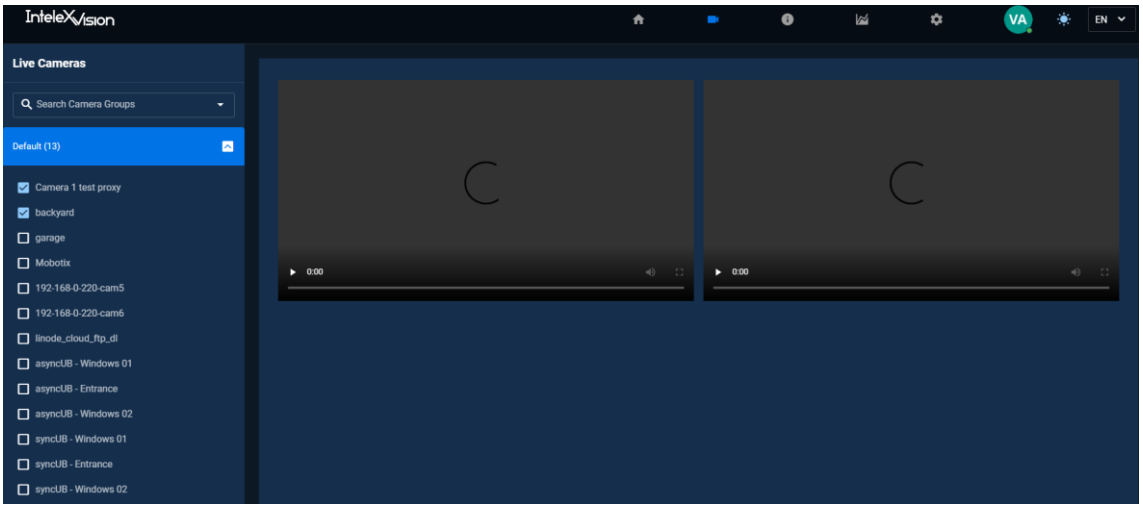


Once you press the button “ok” the alerts listed in the lefthand side will be the ones containing detections matching your selected area.



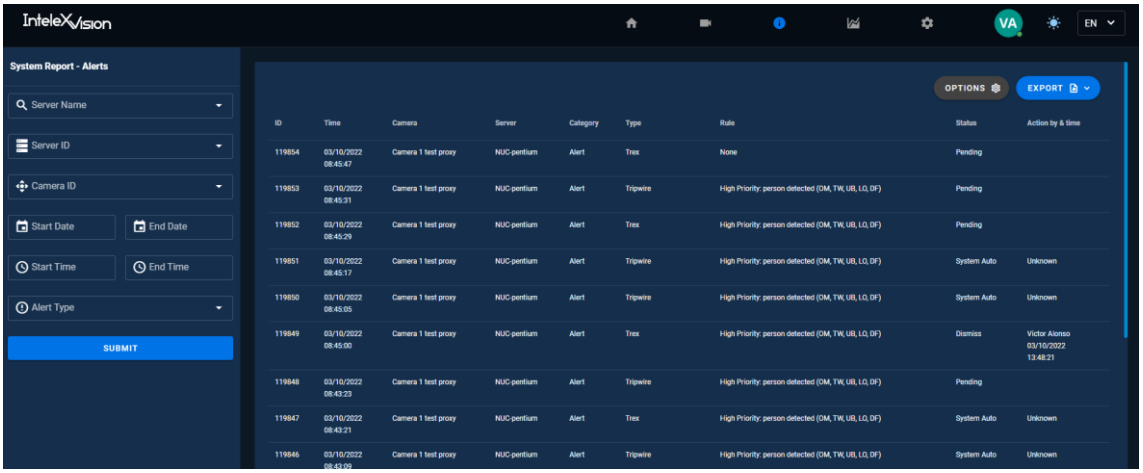
Live Cameras

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 into groups, so every group contains a set of cameras.

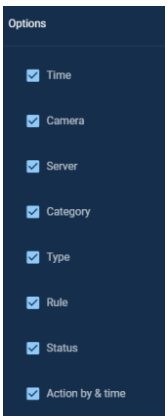


Reports

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).



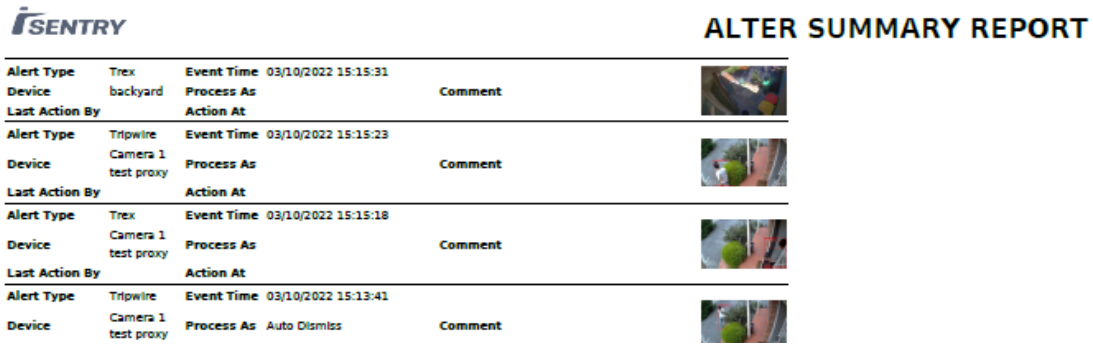
By clicking into the Options menu, a user can specify which columns to include in the report view before exporting it.



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

> **INFORMATION**
>
> Please note allowing 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 with delays in their reports to be generated.

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

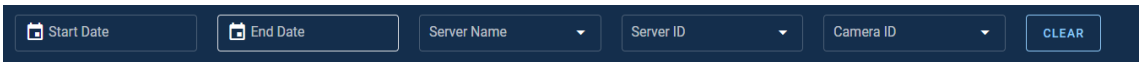


BI Tool

Here the user is presented with different charts and graphs about the overall system status. The main menus can be resumed on 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).

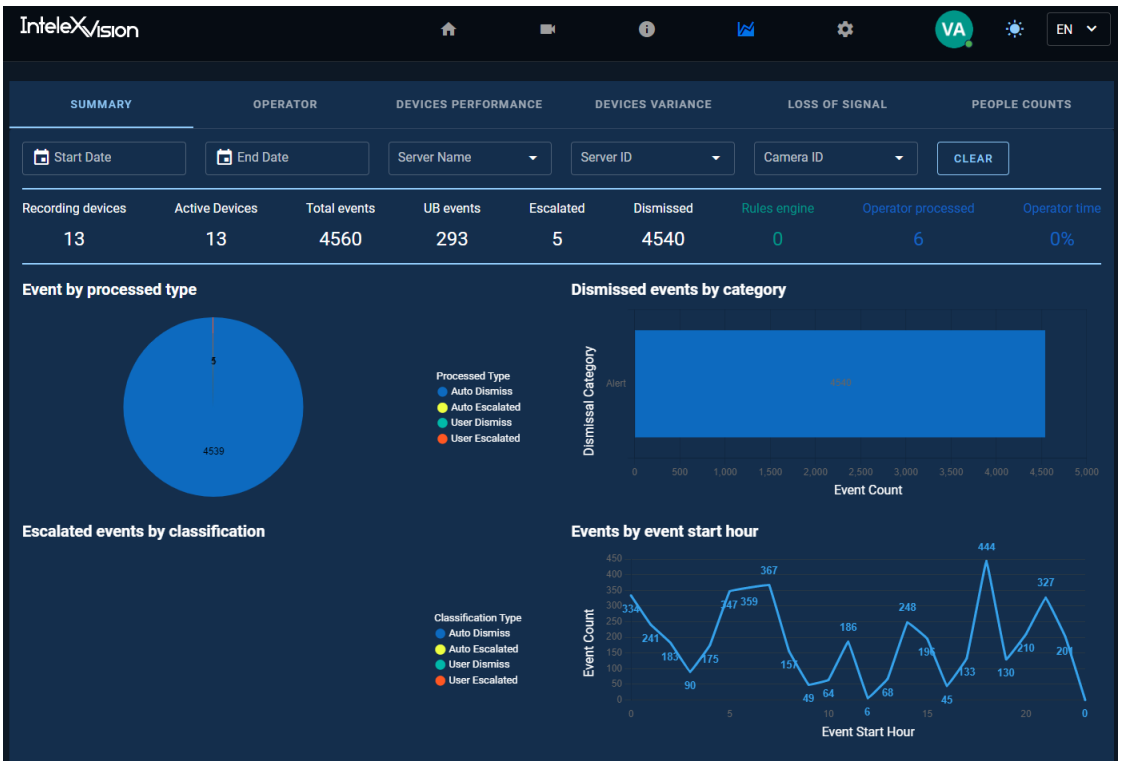


Following this panel the user gets the summary of the overall situation:

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

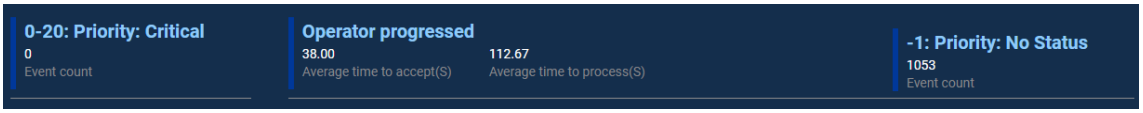


Operator

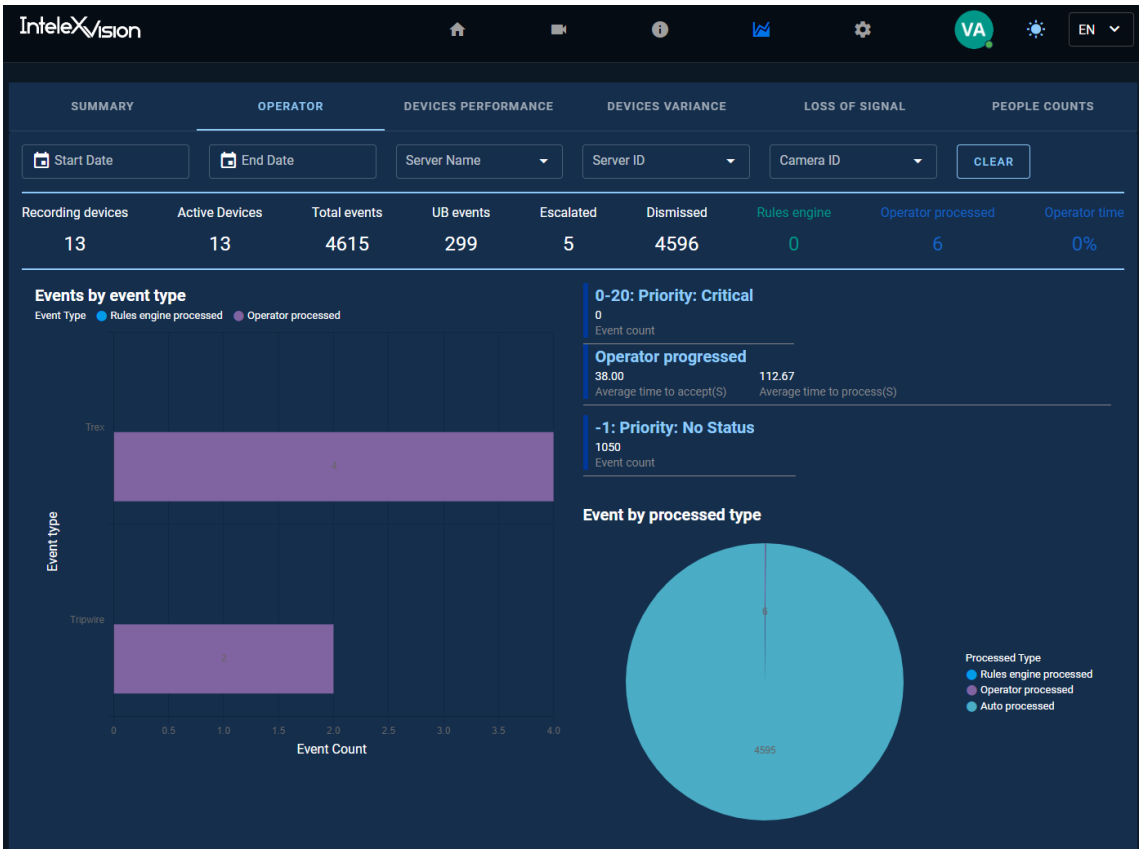
In the following panel the information displayed to the user is the following one.

Events by event type	Bar chart 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.

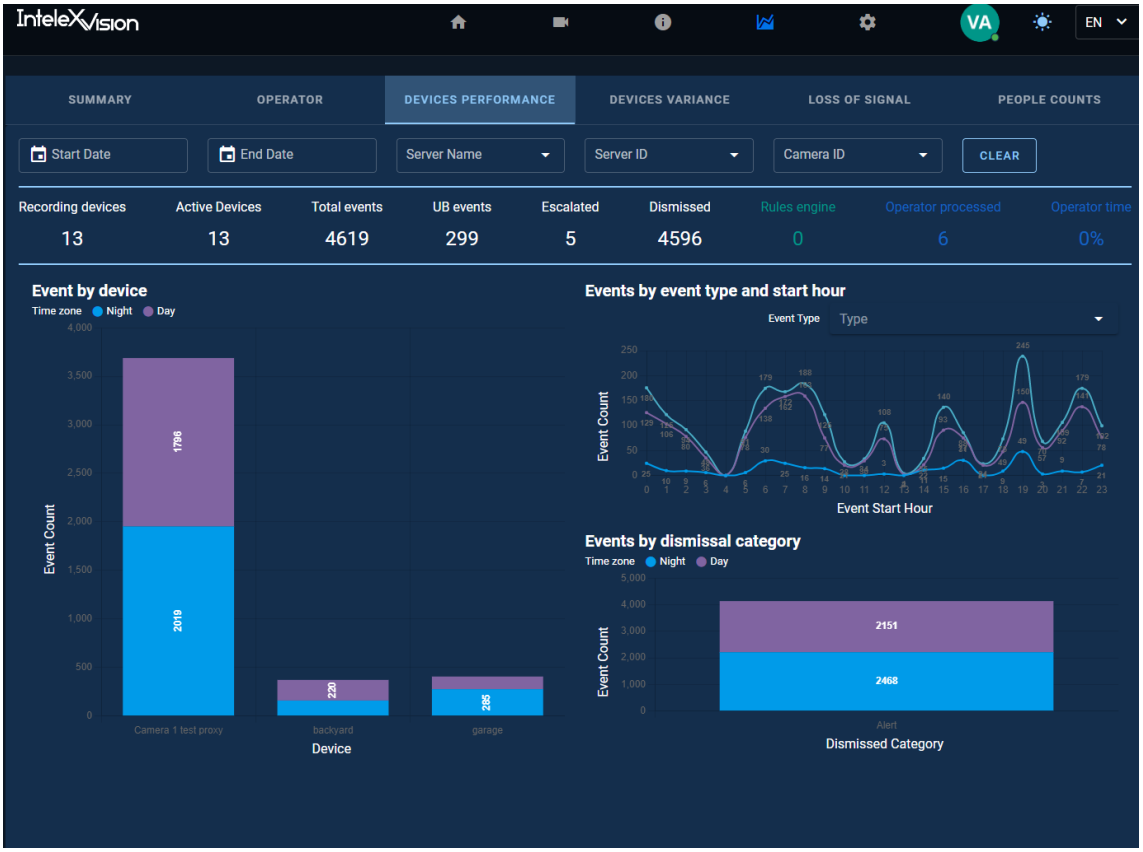


Devices Performance

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.

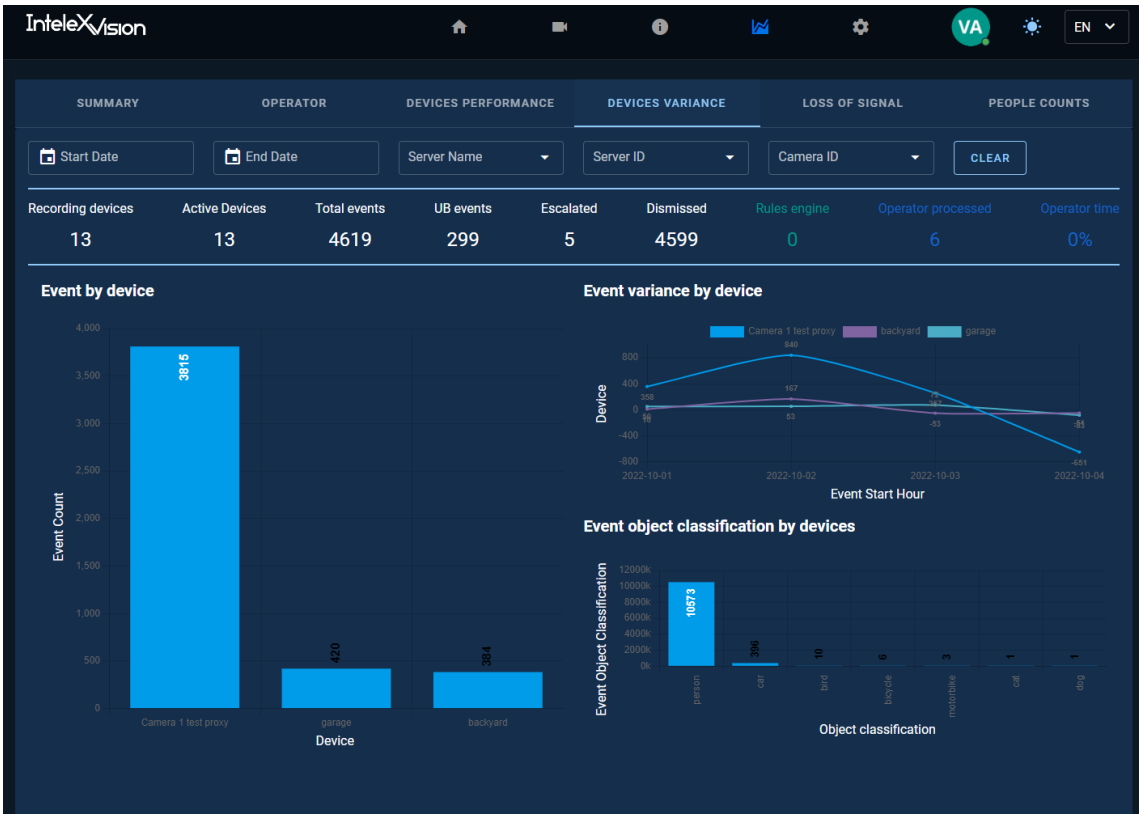
Events by event type and start hour	Filtering by event type the graph shows the number of events per start hour
Events by dismissal category	Filtering by time zone it shows the number of events by dismissed category.



Devices Variance

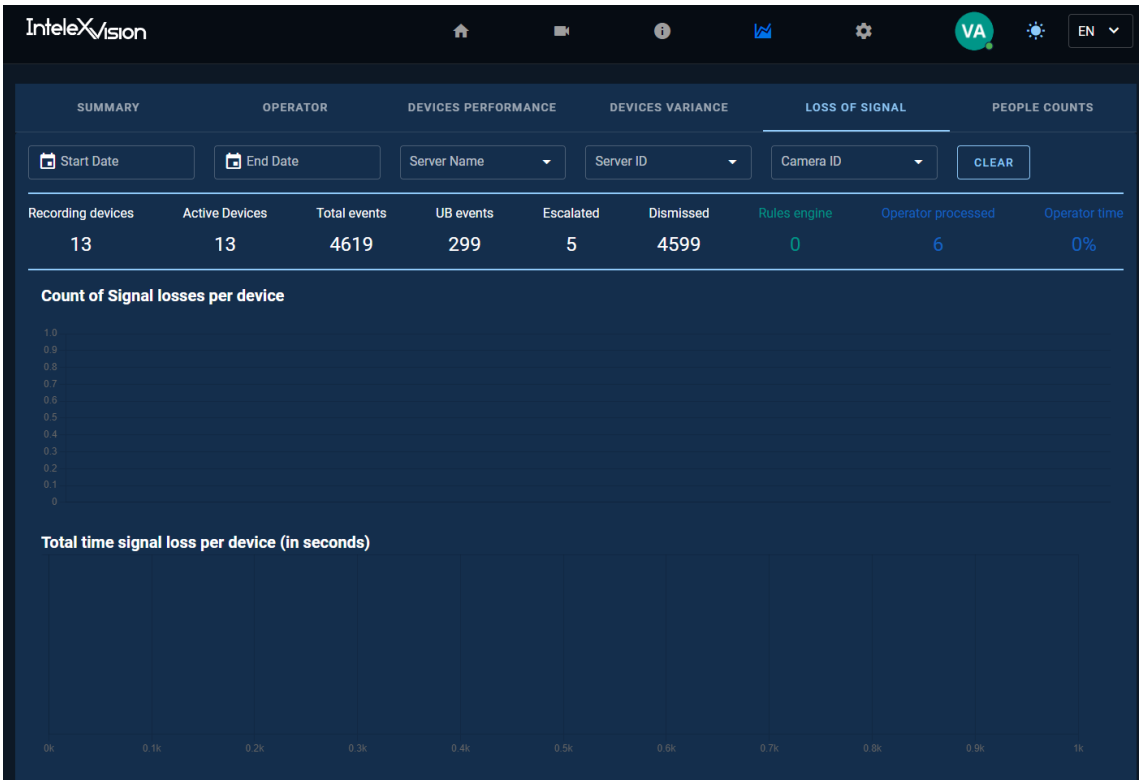
In this panel the user can have a look into 3 different subpanels.

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



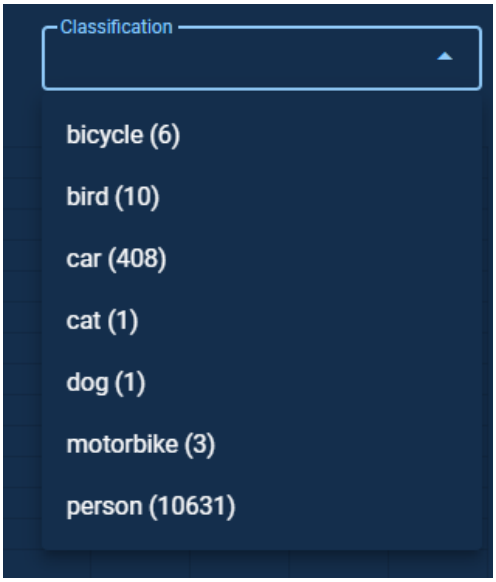
Loss of Signal

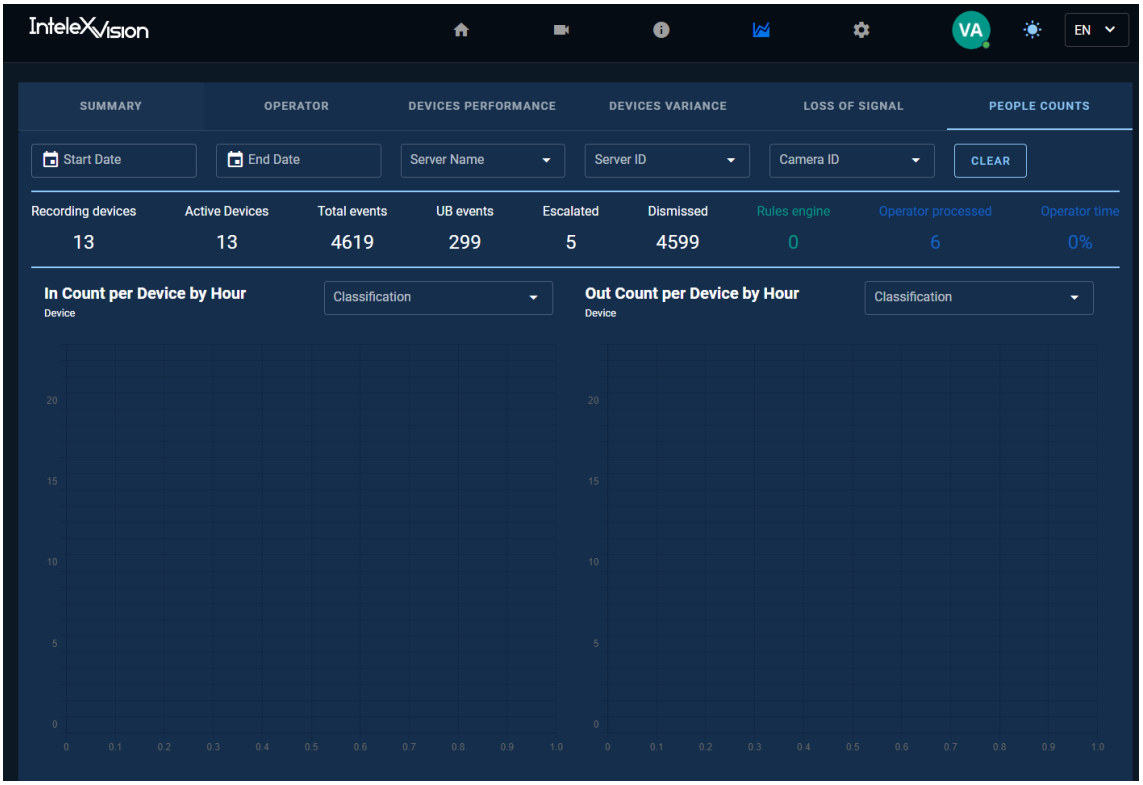
In this panel the user will display the Count of Signal losses per device and the Total time signal loss per device (in seconds).



People Counts

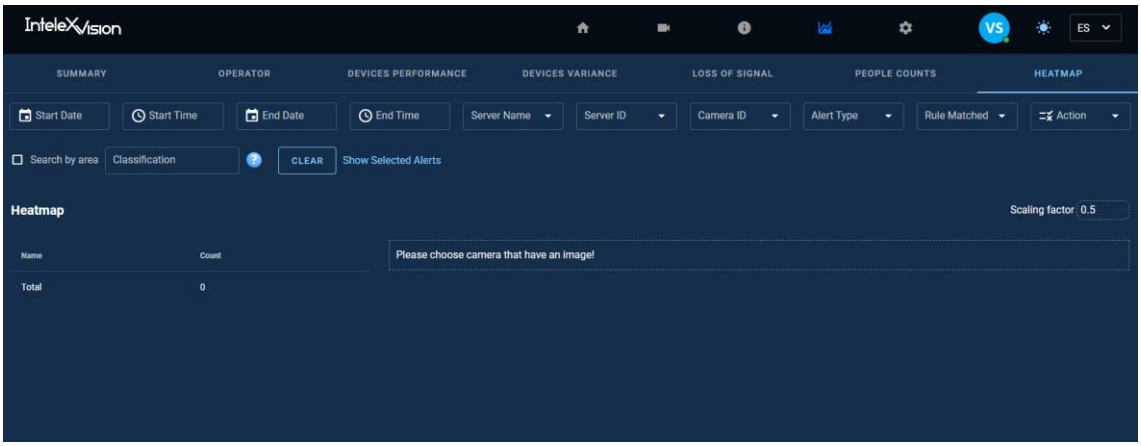
In this panel the user will display the In Count per Device by Hour and the Out Count per Device by Hour. A classification selection menu is shown where you can choose from different categories like:



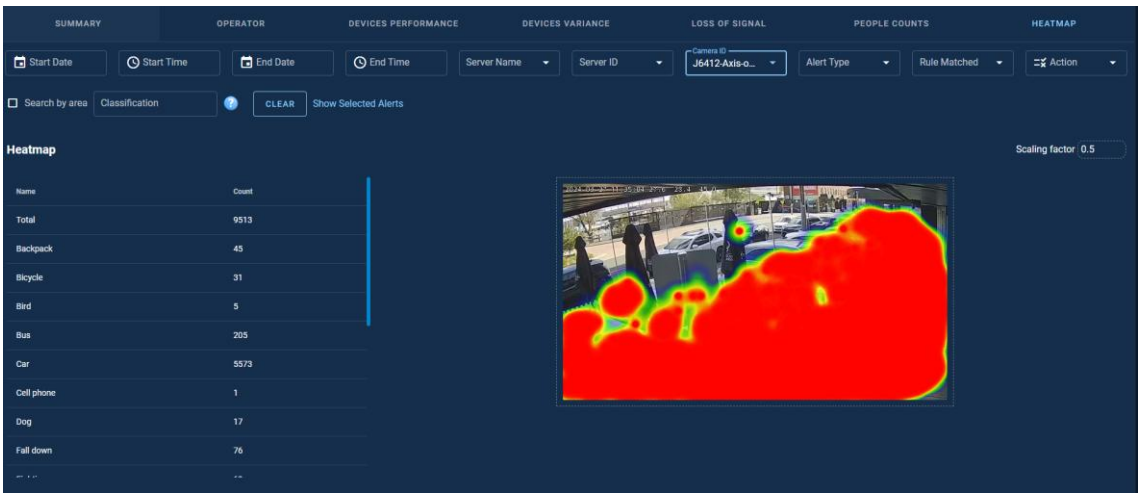


Heatmap

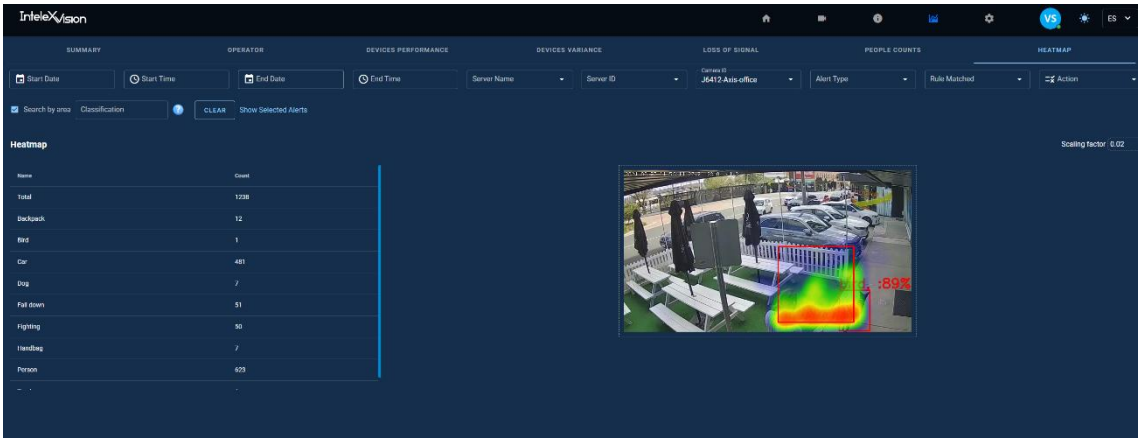
In this panel the user will be displayed the Heatmap.



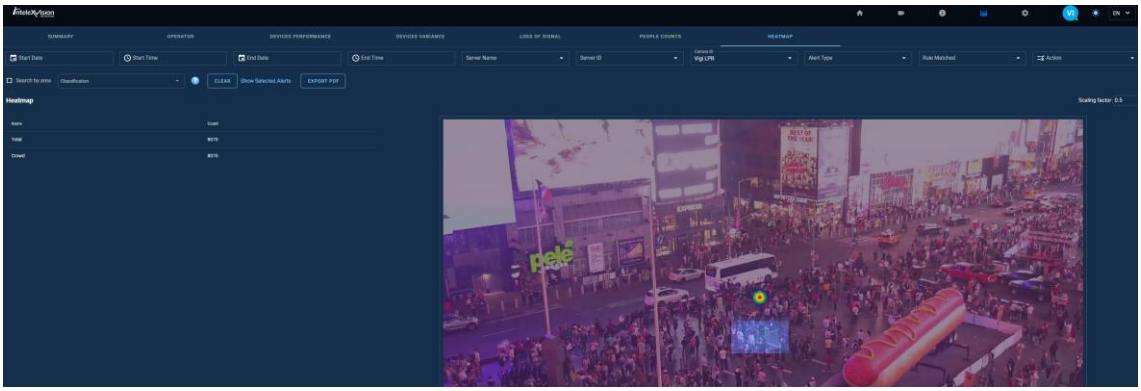
From here the user should pick a camera that have an image.



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.



Keep watch

Web Client also provided dedicated UI to work with another product call Keep Watch. Please refer to the separate document “Sentry Keep Watch user manual” for how to use web client with Keep Watch product.

Related UI sections: Past Alert, Group Camera Config and Permission

Troubleshooting and Common Issues

Common Issues

No information.

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.