PUMATRONIX

LINCE

Lince

SCALABLE SOLUTION FOR ANY PROJECT SIZE

Integration

Pumatronix Equipamentos Eletrônicos Ltda.

Rua Bartolomeu Lourenço de Gusmão, 1970. Curitiba, Brasil

Visit our website https://www.pumatronix.com

Send feedback on this document to suporte@pumatronix.com

Information contained in this document is subject to change without prior notice.

Pumatronix reserves the right to modify or improve this material without obligation to notify of changes or improvements.

Pumatronix grants permission to download and print this document, provided that the electronic or physical copy of this document contains the full text. Any alteration to this content is strictly prohibited.

Revision History

Date	Revision	Updated Content
03/06/2024	1.0	Edition regarding the initial version of the Lince system

Overview

LINCE is an **Electronic Fencing** platform that utilizes the Amazon AWS (Amazon Web Services) cloud infrastructure, distributed and commercialized in the Software as a Service (SaaS) model, where Pumatronix is responsible for all the necessary infrastructure for system availability, and the client uses the software via the internet, paying a fee for the service. The result is a **robust solution with a high level of security in managing the information** and data collected from capture points and also from user data.

The solution proposed by LINCE is a distributed architecture with **intelligent equipment** installed on streets and highways **capable of detecting, classifying, and reading vehicle license plates within images**. Once the information is collected by the equipment, it is sent to the platform to provide additional functionalities for users.

LINCE allows users to **search records** by capture point (each capture point corresponds to a geographic coordinate), capture device, date and time, license plate, make, model, color, and vehicle class, among others. It also allows users to access reports, analytics, dashboards, and big data mechanisms on the mass of vehicle records.

The platform access portal and integration APIs **have a secure HTTPS communication protocol with TLS 1.2**, **ensuring security in the exchange of information between the browser and the server through an encrypted and secure channel.**

Key features:

- Search for captures by class, make, model, or color and period;
- Registration and import of monitored vehicle lists;
- Mobile capture point through Android application or mobile devices (patrol car solutions);
- Public Safety Panel with monitoring portraits;
- Mobility Panel with information about vehicles circulating at capture points;
- Integration with Public Safety Systems (Detecta, SPIA- PRF, and Cortex);
- Reports with capture data, convoys, vehicle monitoring, incidents, and integration with public safety system data.

……

This document aims to guide the developer in using the available operation interfaces that allow operating the Lince system. If there are any doubts, please contact Pumatronix's technical support.

Summary

1. Lince Interface

The screens of Lince are divided into 3 parts, as highlighted in the image below:

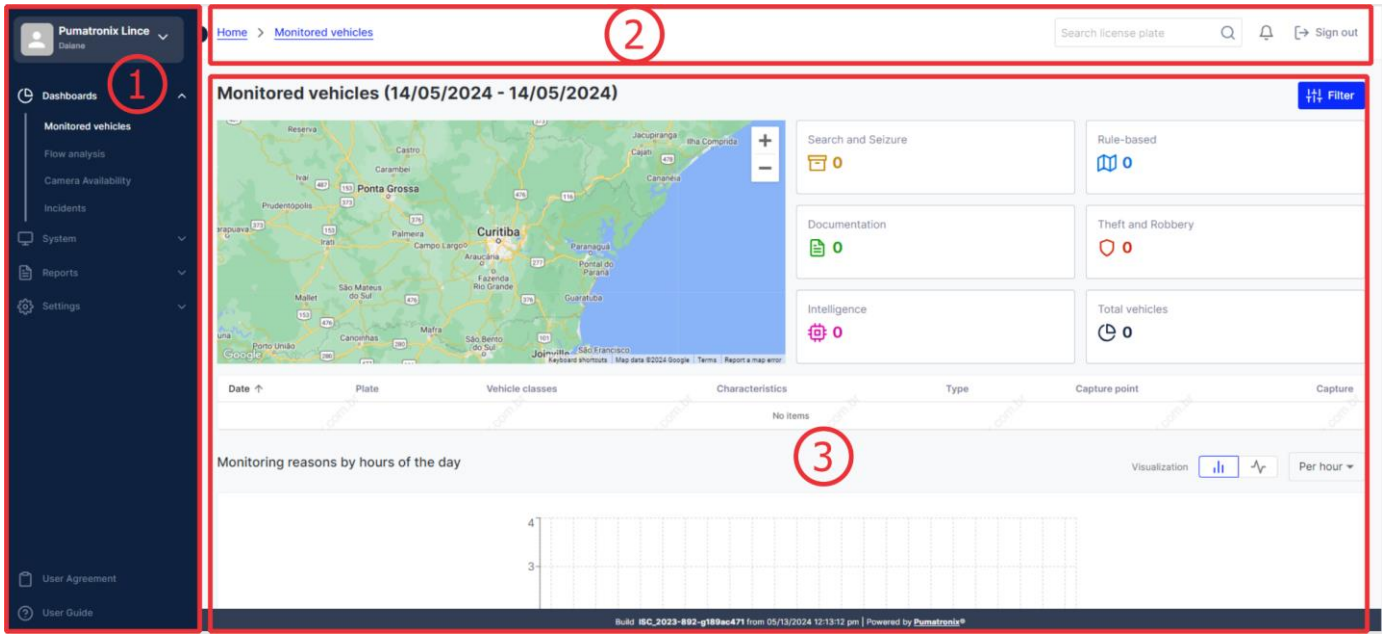


Figure 1 – Lince Interface: 1) Collapsible side menu, 2) Top menu, 3) Viewing area

1) Collapsible side menu: access to menus and the section allowing editing of the logged-in user's account settings, as well as changing the interface language;
2) Top menu: contains the following information and functionalities:
    a. Indication of steps/path within the system;
    b. Search field for captured plates stored in Lince, directing to the Capture Report;
    c. Icon indicating new notifications from the Notification Panel;
    d. Button to log out of the system.
3) Viewing area: region where the content of the menus is displayed.

Tile view

The *Camera Tile* displays thumbnail images of real-time records, which come from all capture devices that the user has access to. The *Filter Cameras* button allows selecting which devices will have their records displayed in the tile.

At the bottom of the screen, the data of monitored vehicles identified by the devices are displayed in a list format. In this list, the ID, date and time of capture, identified plate, and equipment data that performed the capture are presented.

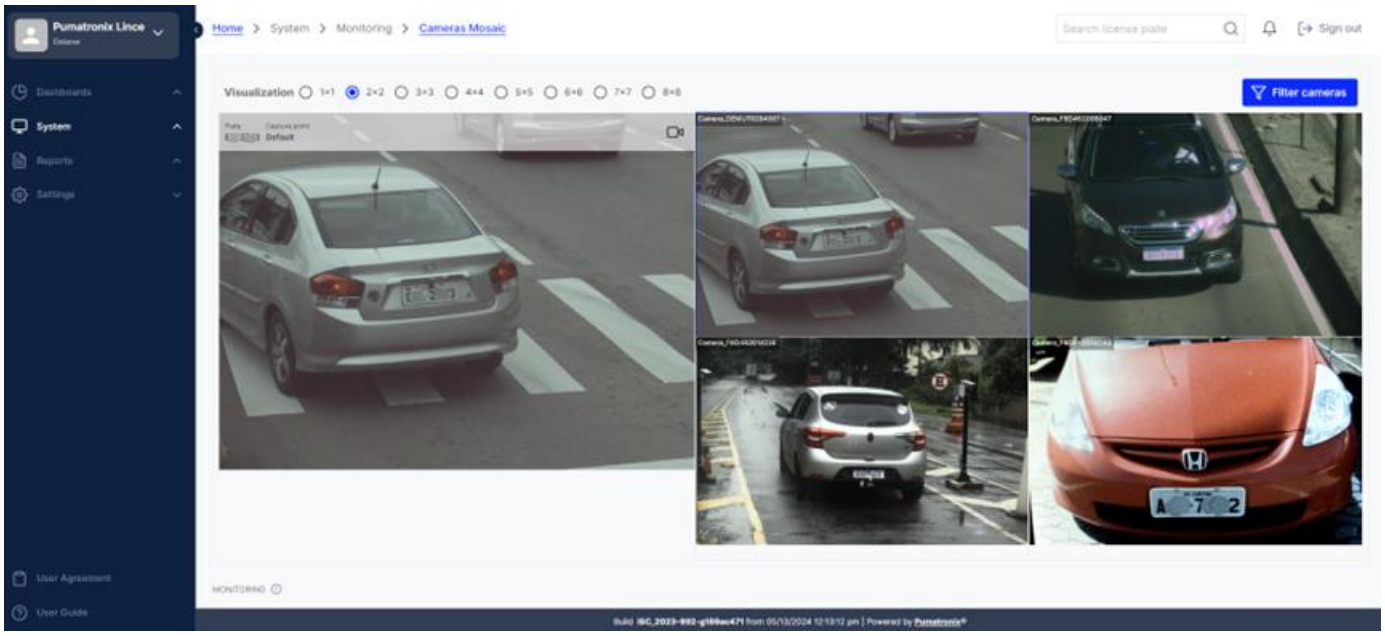


Figure 2 – Example of 2x2 tile view

Notifications

Notifications are messages generated by the system to communicate the occurrence of vehicle monitoring events, located in the top menu, on the bell symbol to the right, and when clicked, it opens the side window with the list of the latest notifications.

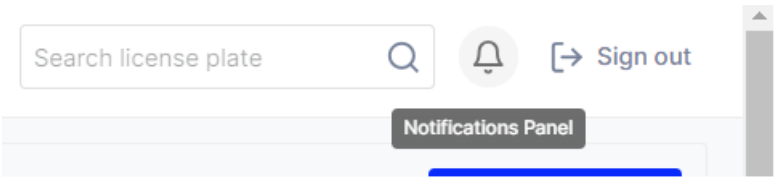


Figure 3 - Location of the Notification Panel

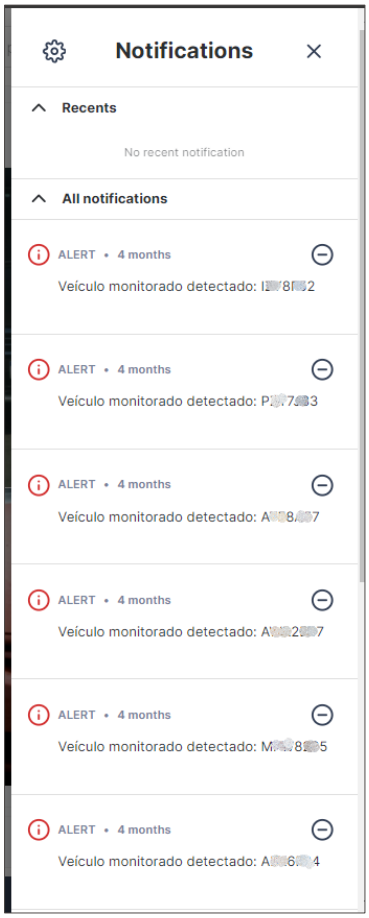


Figure 4 - Notification Panel Side Window

Configure Notification Panel

Monitoring Alert notifications can be activated for the notification panel by clicking on the gear icon, located in the upper left corner of the *Notification panel*. It is possible to select to *Receive notifications* through *the Notification panel* and/or by *Email.* Each adjustment made will only take effect after clicking on the *Confirm* button.

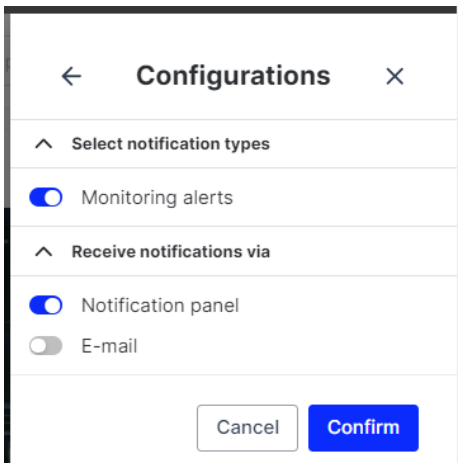


Figure 5 - Settings available for the Notification Panel

2. Panels

The *Panels* provide statistical analysis of data in charts, lists, and maps by selecting the information of interest and applying the filter in each panel separately. The data to be displayed on the panel must be selected by clicking on the *Filter* button in the respective viewing area:

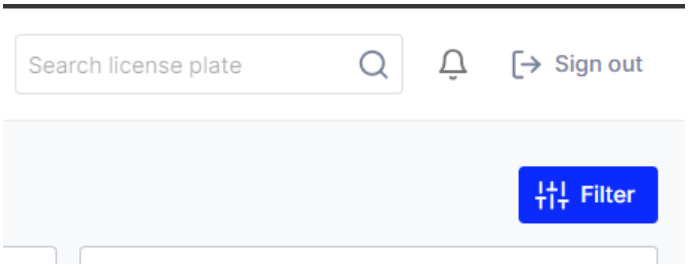


Figure 6 - Location of the Filter functionality

Chart data is updated only after clicking on *Filter*.

Chart data is generated after registering *Capture Points* and *Cameras*.

Monitored Vehicles

The first panel on the *Panels* list displays on the map the location and type of detected monitoring, providing information used to identify monitoring patterns for a particular region and allowing visualization of the magnitude of an event's incidence.

When accessing the *Monitored Vehicles* panel, the initial filter considers captures from the current date, and the following are applicable:

- Initial date & time;
- End date & time;
- Today or Current month;
- License plate;
- Vehicle classes;
- Monitoring reasons;
- Capture Points.

The listing of detected vehicles is displayed just below the map, with the main capture data shown, sorted by the most recent detections, and allows access to the vehicle information page by clicking on the license plate link, as well as details of the capture by clicking on the respective capture image:

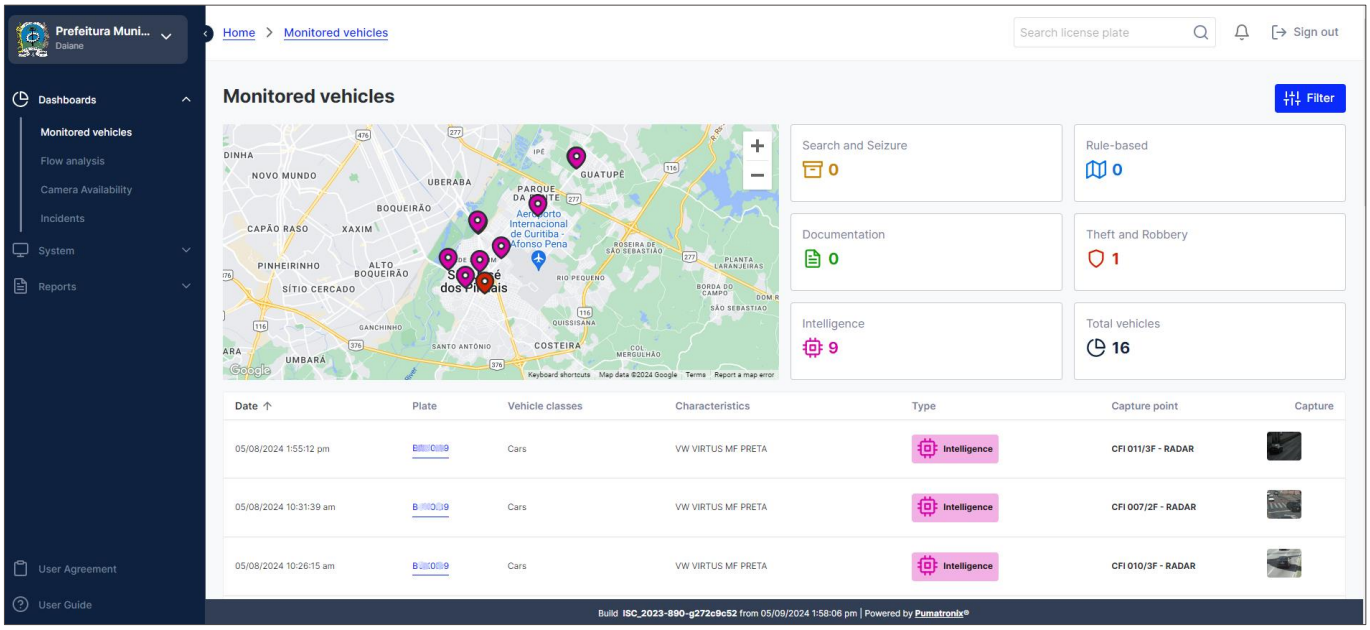


Figure 7 – Example of the initial screen in Panels > Monitored Vehicles

When clicking on each capture, the details of the captured data are displayed individually, containing tabs for Capture *Information*, *Renavam* data, and *Location* on the map:

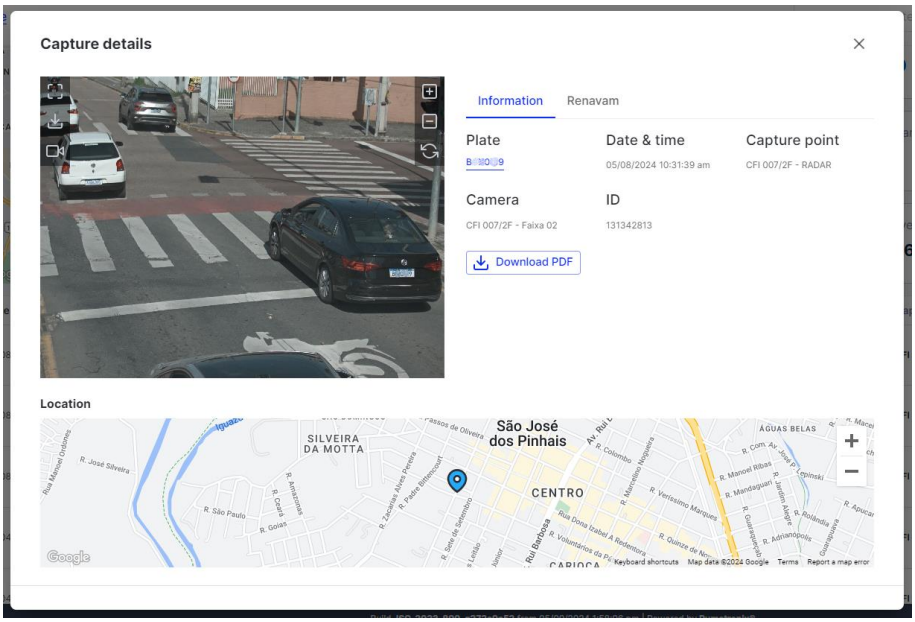


Figure 8 – Screen with Capture Details

Monitoring Reasons by Hour or Day

The chart showing monitoring reasons allows identifying behavior patterns by hours of the day or by days of the week, by selecting the option in the box on the right:

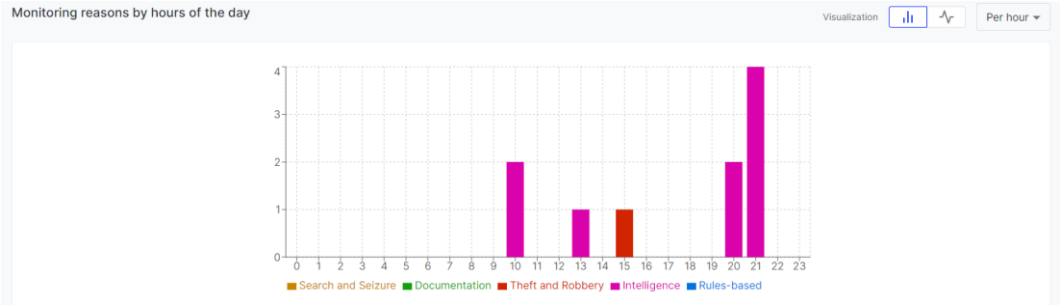


Figure 9 – Example of the chart of detected vehicles by hours of the day

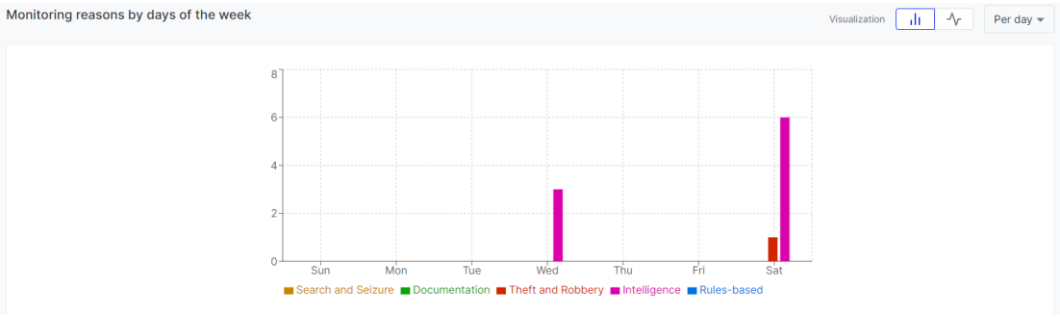


Figure 10 - Example of the chart of detected vehicles by days of the week

Capture Point Analysis

The chart with the number of detections of monitored vehicles by capture points displays the number of captures made and the efficiency rate of the devices in red, yellow, or green colors, as identified in the legend, both by hours of the day or by days of the week, as selected in the box on the right. More detailed information can be accessed in the *Camera Performance* panel.

The efficiency rate calculation considers the total number of captures made by the device and the number of captures with plate 0000000, which indicates a problem in identifying the vehicle's plate. In other words, if a device's efficiency rate is 62%, it can be concluded that 38% of the captures are errors. With this data and color visualization in the system, the user can quickly identify times with difficulties in plate identification or the performance of devices over the days.

Figure 11 - Example of the capture point efficiency analysis chart

Flow Analysis

The traffic flow analysis for a certain group of capture points is possible with the quantity raised by the Lince system and displayed according to the registered sections. When accessing the *Flow Analysis* panel, the initial filter considers captures from the current date, and the following filters are applicable:

- Initial date & time;
- End date & time;
- Today or Current month;
- Capture Points;
- Cameras;
- Ranking of the most captured vehicles.

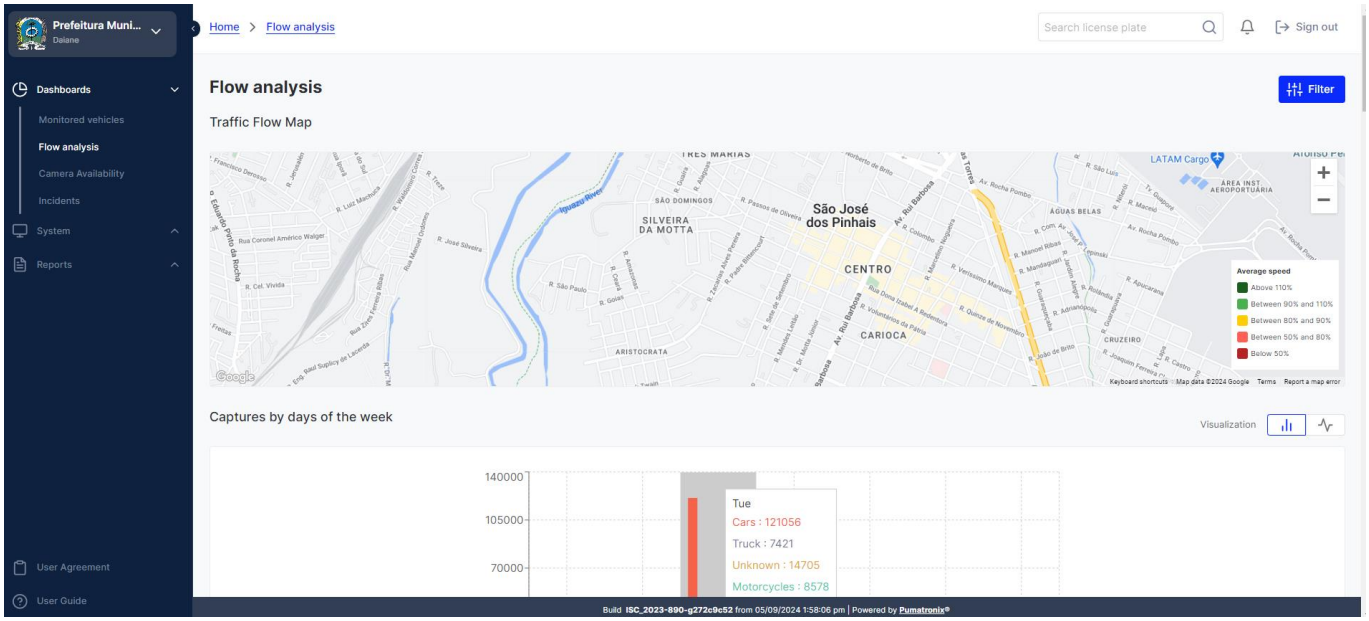


Figure 12 - Example of the initial screen in Panels > Flow Analysis

Traffic Flow Map

The *Traffic Flow Map* displays the average speed information for the registered *Monitored Sections* and shows on the map the color corresponding to the average speed detected in the monitored section, as per the legend.

Captures by Day of the Week or by Hour of the Day

The quantity of vehicles by day of the week or by hour of the day is displayed considering the vehicle class for a certain group of selected capture points:

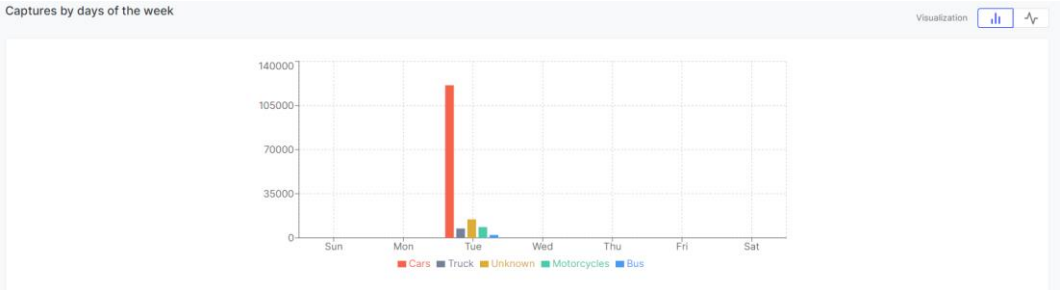


Figure 13 – Example of the chart of captures by day of the week

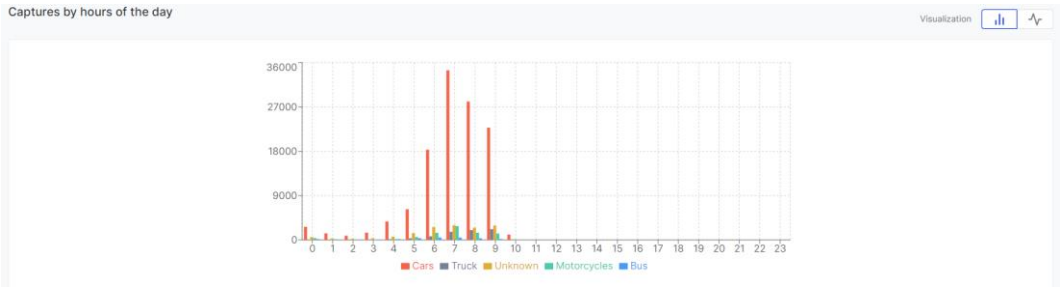


Figure 14 - Example of the chart of captures by hour of the day

Ranking of Captures by Vehicle Class

The ranking list of captures by vehicle class displays the quantity by vehicle class, listing which class has the highest quantity for a certain group of selected capture points in the filter.

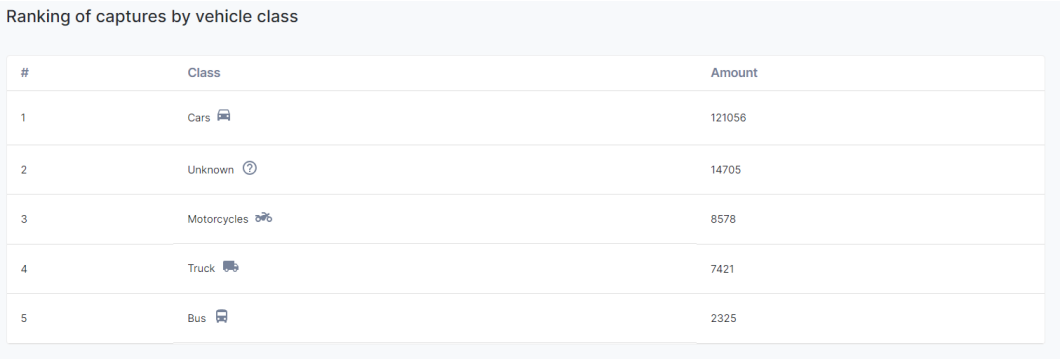


Figure 15 – Example of the ranking of captures by vehicle class

Flow Intelligence

From the Flow *Intelligence* section, the presented data result from the analysis of flow data and provide relevant information for monitoring vehicle flows by capture points.

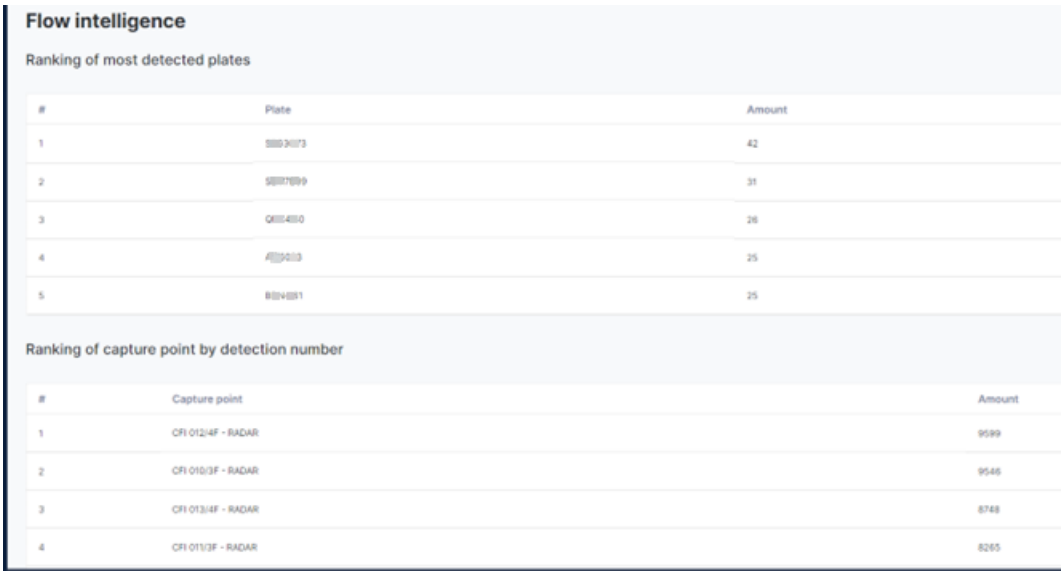
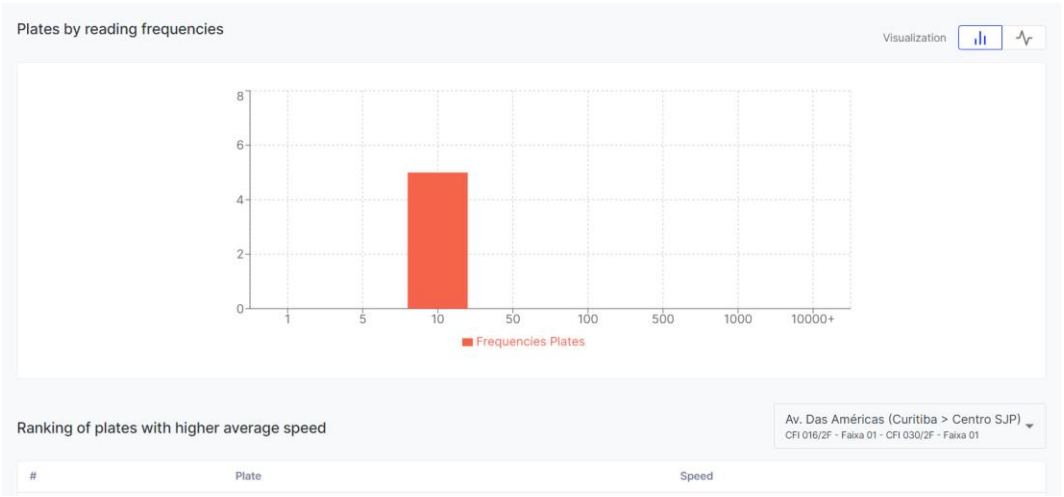


Figure 16 - Example of the quantities of most captured plates and by capture points

1) *Ranking of most detected plates* lists the plates with the highest number of detections and shows the number of times they were captured in the images;
2) *Ranking of capture points by number of detections* lists the capture points with the highest number of detections and shows the number of captures made at each point;
3) *Plates by reading frequencies* displays the quantity of plates that have some reading frequency, grouped by average capture frequency;



4) *Ranking of plates with the highest average speed* lists the plates with the highest average speed calculated for a registered section, selected on the right.

Camera Availability

The *Camera Availability panel provides an overview of* the efficiency of a device registered in the system, indicating in the graph the number of records per hour of the day. When accessing the panel, the initial filter considers captures from the current week, and the following filters are applicable:

- Initial date & time;
- End date & time;

- Cameras.

With color visualization, the user can quickly identify the most problematic times of the day, during which there may be some difficulty in identifying plates, considering the device selected in the filter. Thus, when *Null Records* occur between 11 pm and 5 am, the cause may be related to lighting issues. When there are *Null Records* at all times of the day, it is likely caused by poor device framing.

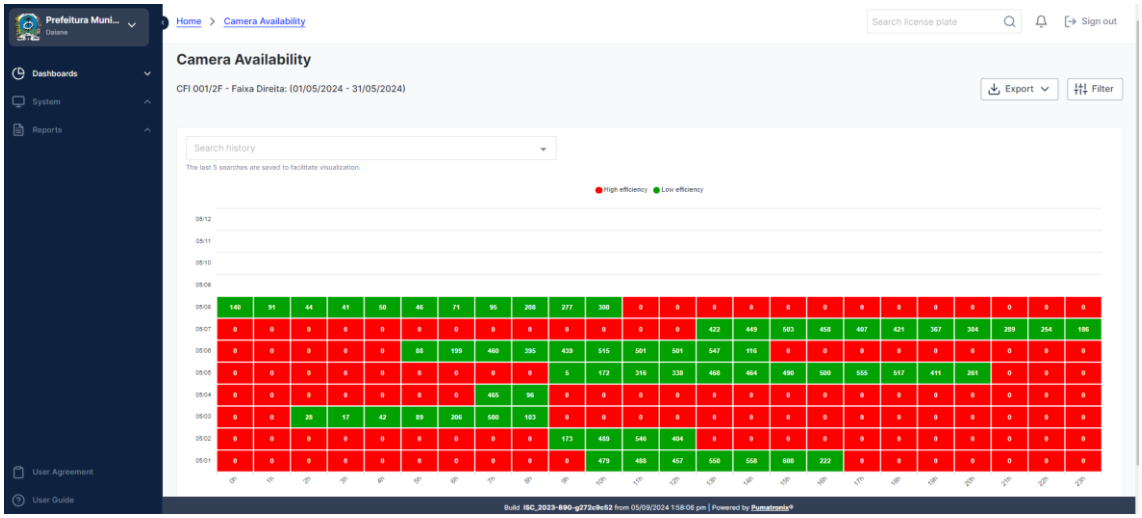


Figure 17 - Graph of Camera Availability Visualization

Cloning Suspects

The *Cloning Suspects* panel presents possible captures indicating vehicle plate cloning as it tracks images with the same plates detected at times with incompatible movements. This validation is done using all devices sending images to the system but with vehicles of different characteristics. When accessing the panel, the initial filter considers captures from the current month, and the following filters are applicable:

- Initial date & time;
- End date & time;
- License plate;
- Capture Points;
- Cameras.

The map with the location of the records allows focusing on all by clicking on the button below to the right. The list of captures of cloning suspects displayed allows some *Actions,* in the column to the right, during panel viewing:

- *Focus*: clicking on the button displays the location where the plate was detected;
- *Monitor*: clicking on the button directs the user to the page for creating a new monitored vehicle when the *Status* is *No Monitoring*.

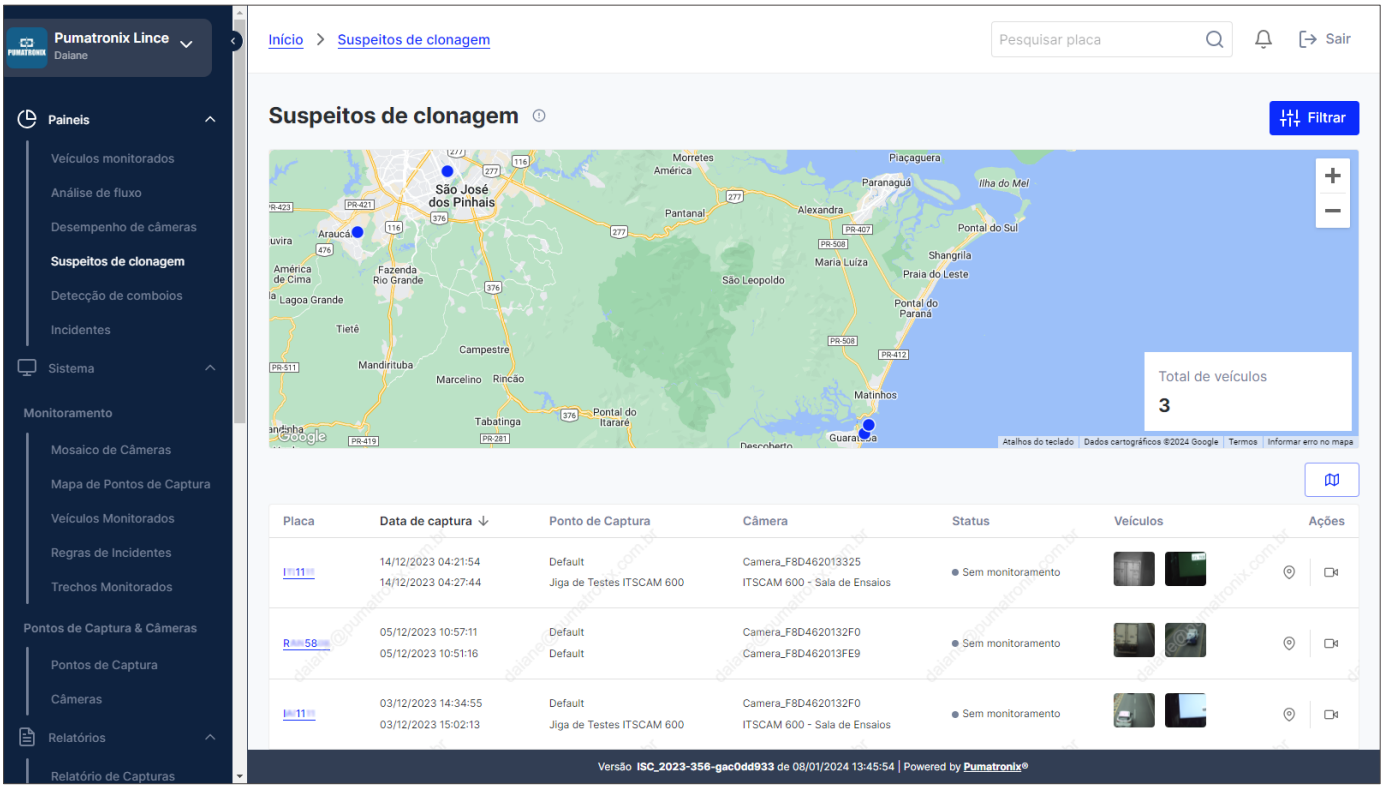


Figure 18 – Example of the initial screen of the Cloning Suspects panel

Convoy Detection

The *Convoy Detection* panel presents the plates of at least 2 vehicles that have been detected traveling together, repeating this behavior at least once. When accessing the panel, the initial filter considers captures from the current month, and the following filters are applicable:

- Initial date;
- End date;
- License plate;
- Repetition period;
- Repetitions.

The map with the location of the records allows focusing on all by clicking on the button below to the right. The list of detected convoys is displayed just below the map and allows some *Actions,* in the column to the right, during panel viewing:

- *Focus*: clicking on the button displays the location where the convoy was detected;
- *Monitor*: clicking on the button directs the user to the page for creating a new monitored vehicle when the *Status* is *No Monitoring*.

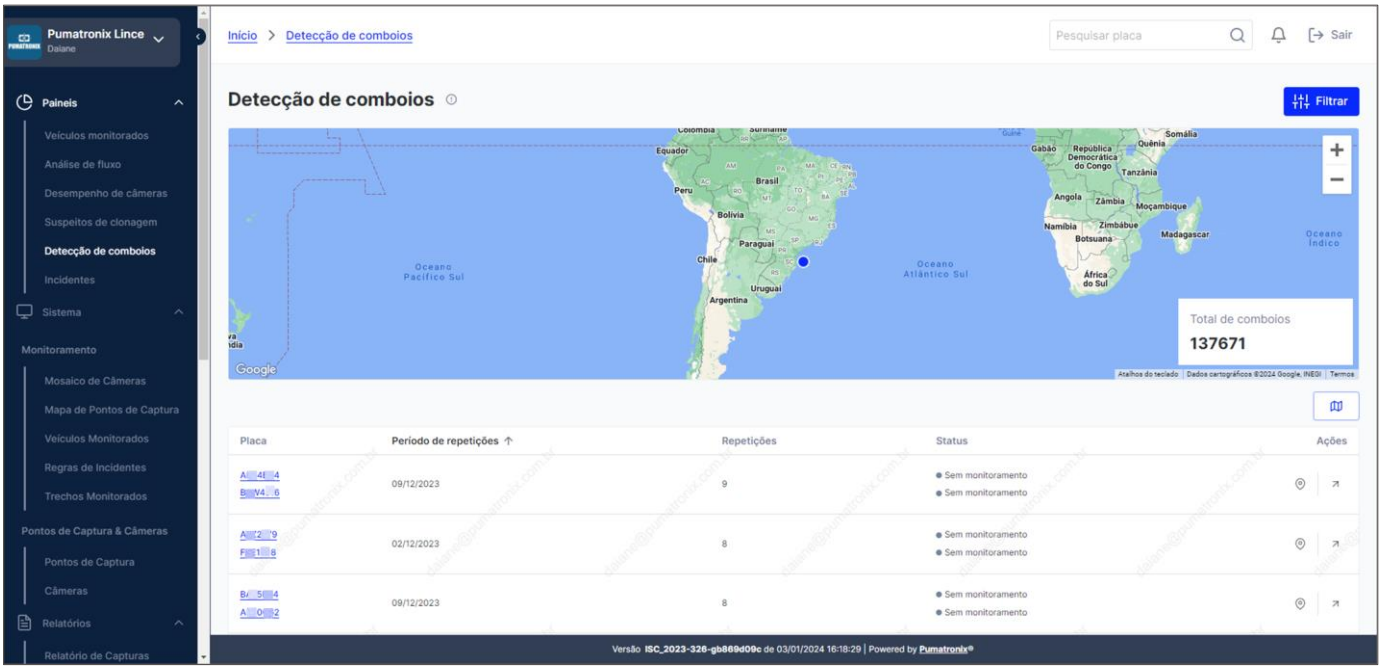


Figure 19 – Example of the initial screen of the Convoy Detection panel

Incidents

The *Incidents* panel presents the quantity and location on the map of incident records detected as configured in the Incident Rules, including Speeding, Exclusive lane, Roadblock, Car rotation, and Border control.

When accessing the panel, the initial filter considers captures from the current month, and the following filters are applicable:

- Initial date & time;
- End date & time;
- Today or Current month;
- Type of rule for incidents;
- Capture Points;
- Cameras.

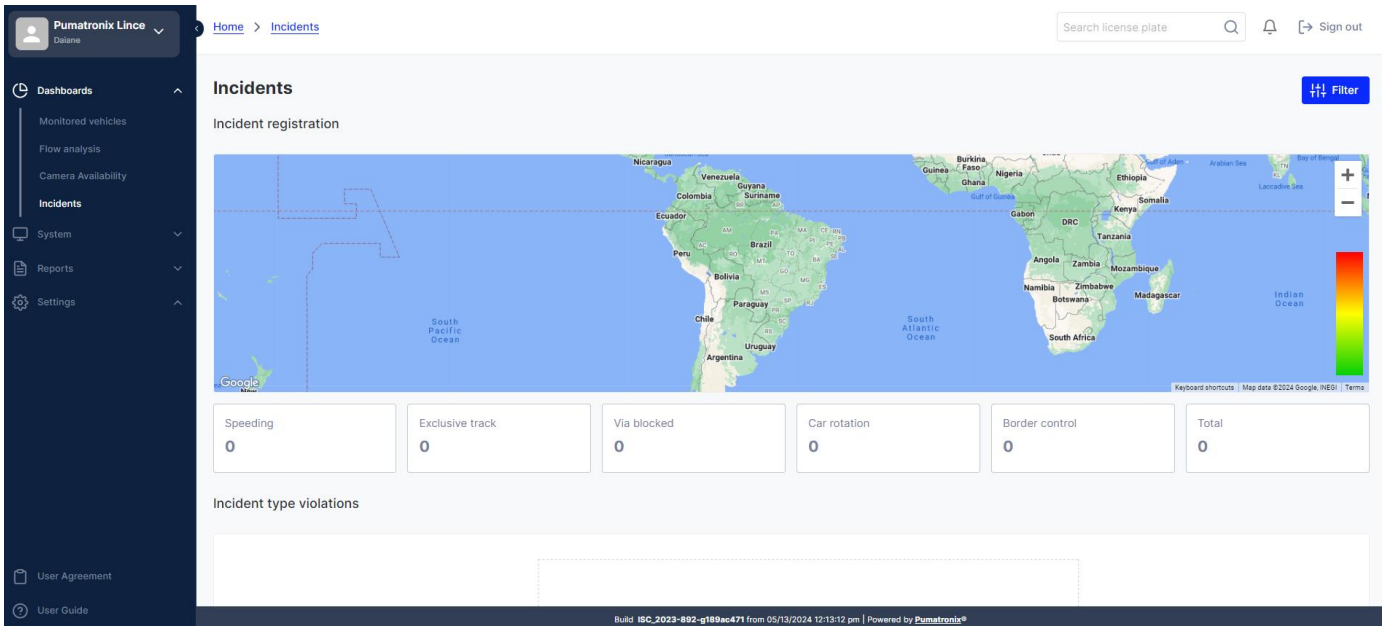
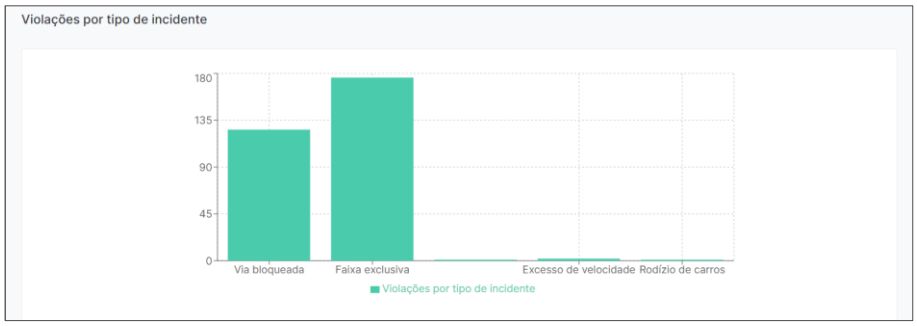


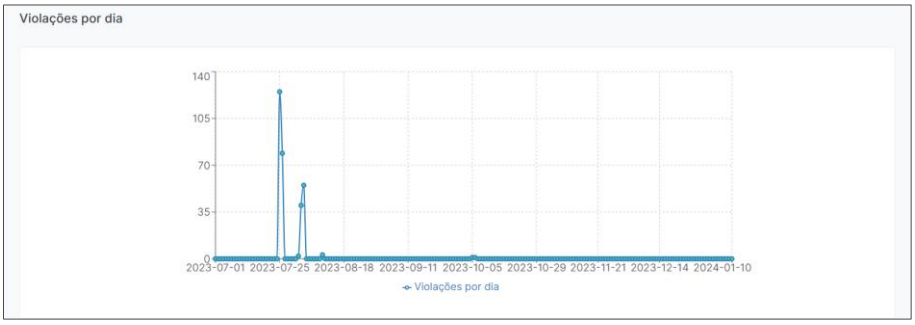
Figure 20 - Example of the initial screen of the Incidents panel

The graphs presented in the panel offer statistical information on the incidents detected within the filtered period:

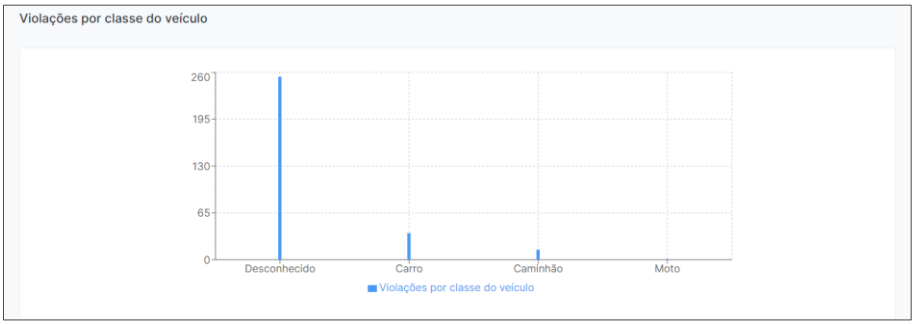
1) *Violations by type of incident*: presents the number of incidents in a graph that allows quick identification of those with the highest number of occurrences;



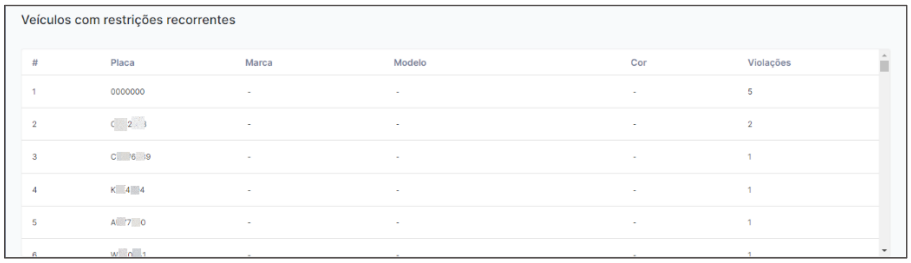
2) *Violations by day*: optimizes data in a graph that allows identification of days with the highest incidence of incidents;



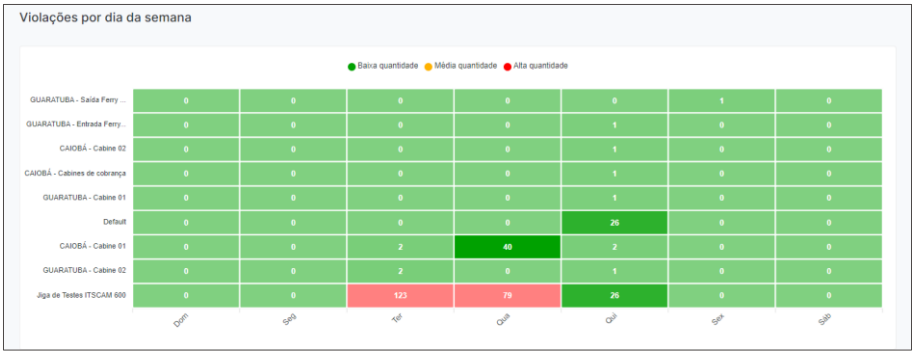
3) *Violations by vehicle class*: graph with data on the number of violations detected for each vehicle class;



4) *Vehicles with recurring restrictions*: list with the ranking of vehicles detected with the highest number of violations;



5) *Violations by day of the week*: quantity of incidents detected per day of the week on devices, with indicative colors of the days with the highest quantity, as per legend;



6) *Violations by hour of the day*: quantity of incidents detected per hour of the day on devices, with indicative colors of the hours with the highest quantity, as per legend;

3. System

Monitoring

Camera Mosaic

The monitoring option with the *Camera Mosaic* allows live viewing of the images from each registered device, aiming to monitor roads and vehicles added to the Monitored Vehicles list. Below the displayed images is a list of the last 50 occurrences in 24 hours detected on the devices of the filter applied in *Camera Filter*.

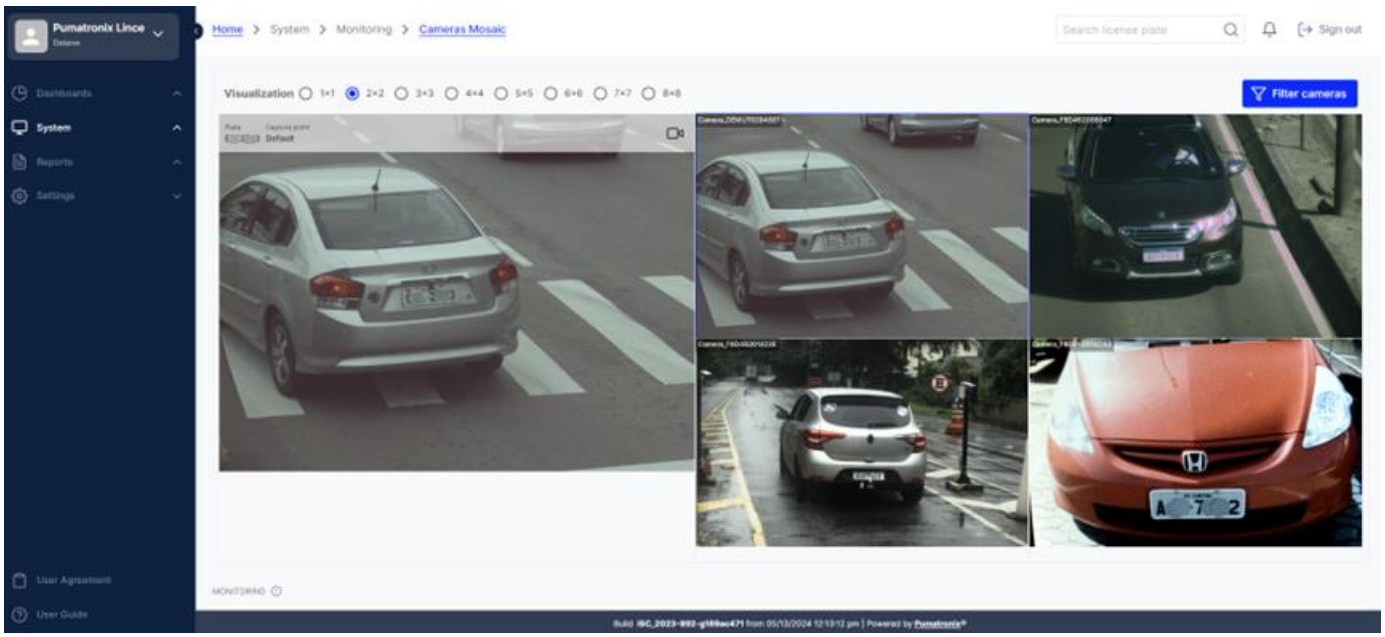


Figure 21 - Example of the Camera Mosaic screen

When accessing the mosaic, which devices will be monitored live in the *Camera Filter* must be selected. The list of all registered devices is displayed and can be searched by name. They must be selected by clicking on the checkbox to the left of each device, and at the end, *Apply* must be clicked to confirm the selection:

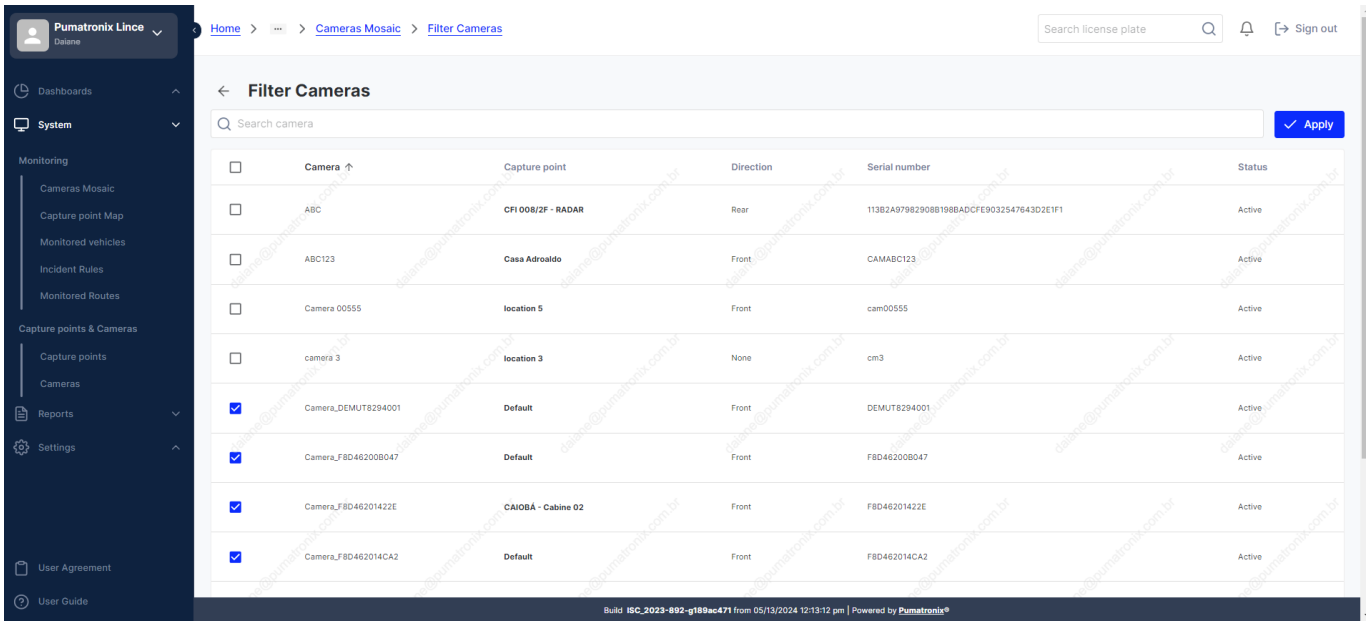


Figure 22 – Camera Filter screen for the mosaic

Capture Points Map

The monitoring option with the *Capture Points Map offers a* joint visualization of the location and status of the registered capture points. By clicking on the legend, points can be removed from the map and the list below the view, for example, those that are disabled. All capture points are listed below the map, and their location can be viewed separately by clicking on the listed capture point.

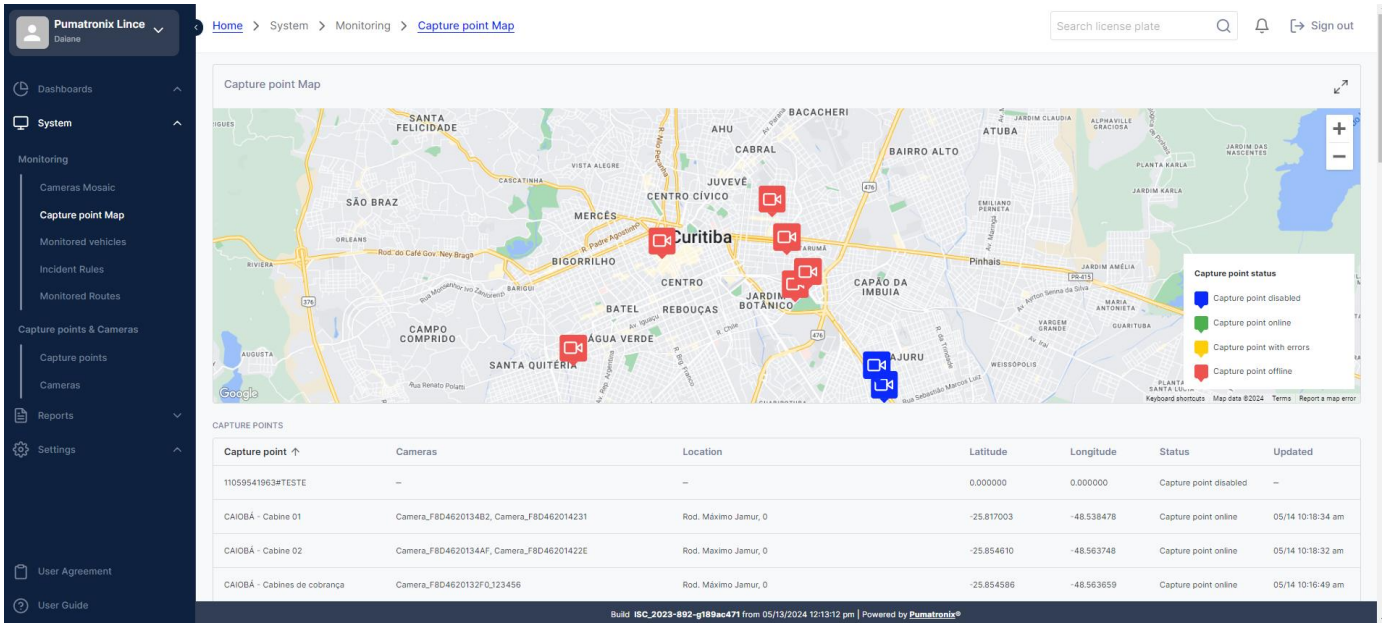


Figure 23 – Initial screen of the Capture Points Map

Monitored Vehicles

When accessing *System* > *Monitored Vehicles*, a list of all monitored vehicles registered in the system is displayed. They can be edited or removed from monitoring, and there are options for registering new monitoring.

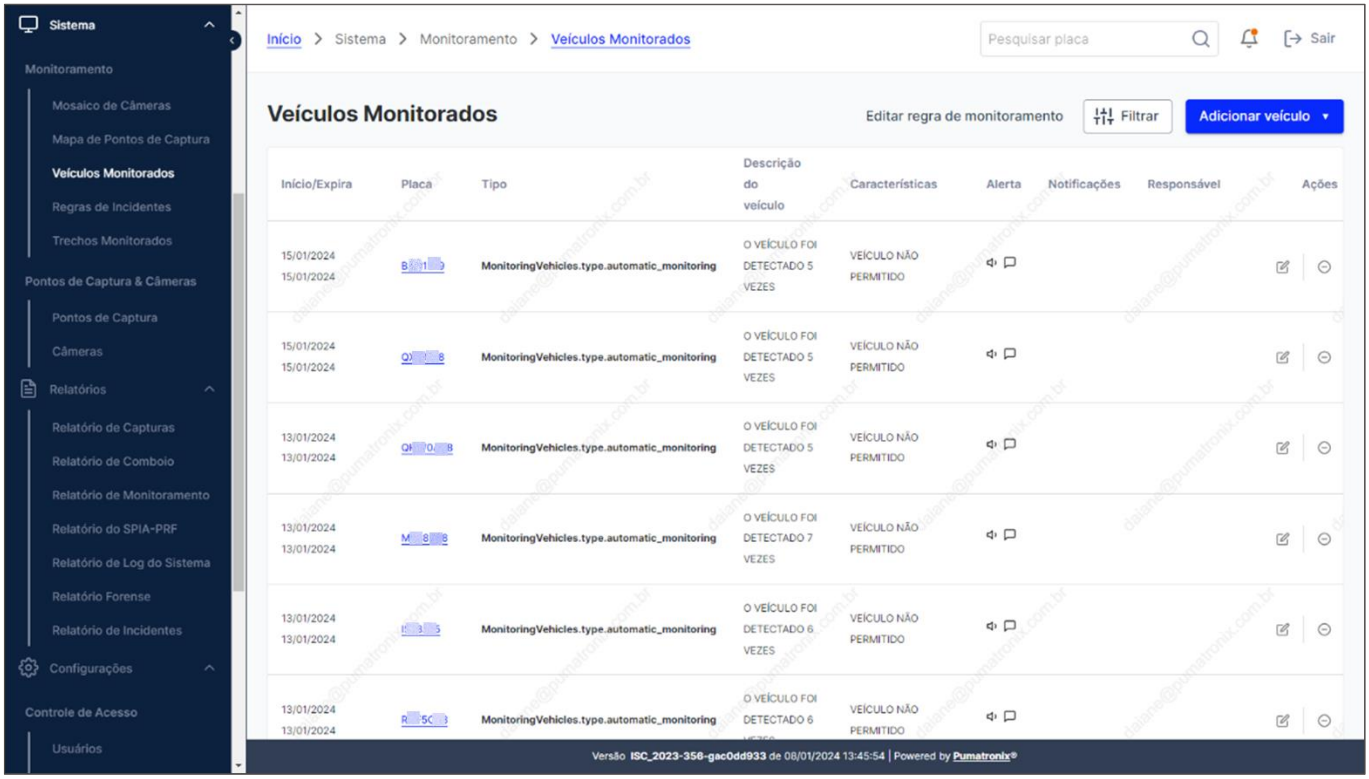


Figure 24 – Screen in System > Monitored Vehicles in the option of Adding monitoring rule

In the *Adding rule* or *Editing monitoring rule*, the validity times of the monitoring of all registered vehicles are determined, and among the configuration options are:

- *General* Tab
  - Activation time: selection of the start time for the daily monitoring of the plates of registered vehicles;
  - Expiration time: selection of the end time for the daily monitoring of the plates of registered vehicles;
  - Repetitions: indication of the number of times the plate can be detected before being included in the monitored vehicles list;
  - Expiration > Monitoring time: definition of the period in which the vehicle remains in the monitored vehicles list, in days.
- *Exception* Tab
  - Allowed vehicles: inclusion of plates that should be ignored by the monitoring because they are allowed for the Incident;
  - Upload CSV: inclusion of the list of allowed plates using the CSV file;
- *Notifications* Tab:
  - Notification channels: can be received via *Email* and/or *Telegram;*

- Alert type: can be *Audible* and/or *Visual* (Pop-up);
- Notified people: selecting a Group of responsible individuals and the Users to be notified;
- Customization of alert notification: the audible alert allows configuration of the sound type and the Pop-up color;
- *Pop-up retention* can be selected, which keeps the pop-up window open;
- Alert audio playback: audio volume and playback speed are adjusted.

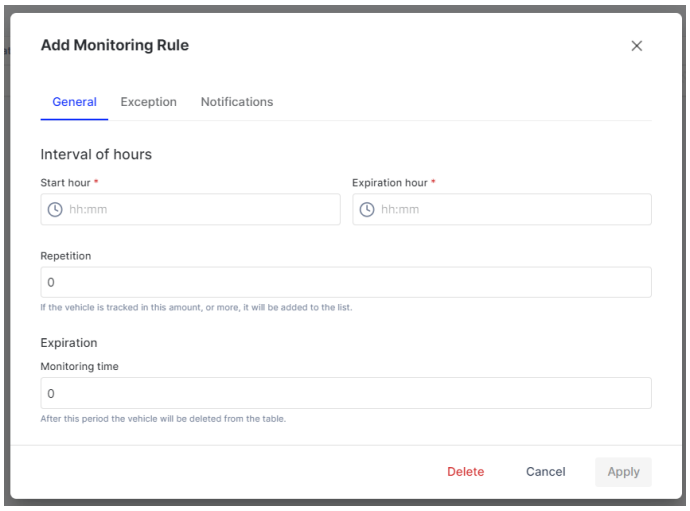


Figure 25 – Screen of the Add Vehicle> Import Vehicles option

The registration is done through the *Add Vehicle button.* It is possible to import a list of plates of interest through the *Import Vehicles* option. In the opened window is the place to send the CSV file, by clicking on *the Upload CSV* button:

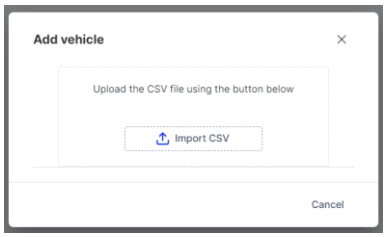


Figure 26 – Screen example in Create new monitored vehicle > General tab

Selecting the option to add a *New Vehicle* opens the window to *Create a new monitored vehicle* and the fields with the vehicle data can be filled in:

- *General* Tab:
  - *Monitoring name*: name of the monitoring (mandatory field);
  - *Type*: select between the options Search and Seizure, Documentation, Theft and Robbery, and Intelligence (mandatory field);
  - *Vehicle description: vehicle* description, such as the model (example);
  - *Characteristics*: vehicle characteristics, such as color (example);
  - *Activation date*: start date set for monitoring analysis (mandatory field);
  - *Expiration* date: end date set for monitoring analysis (mandatory field).

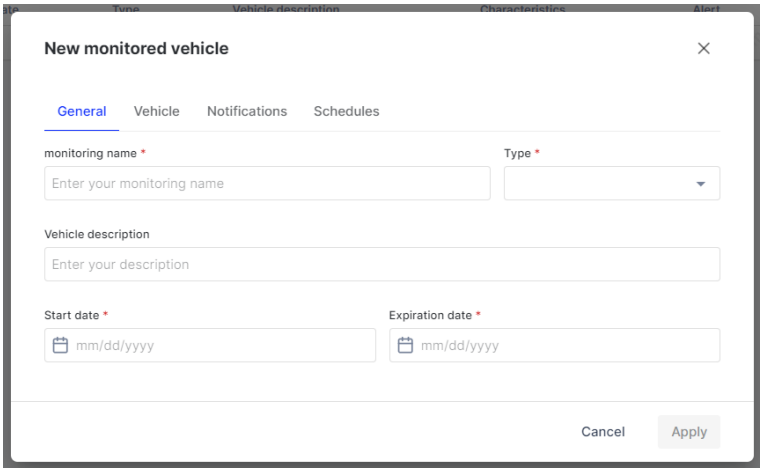


Figure 27 – Example screen in Create new monitored vehicle > General tab

- *Vehicle* Tab:
  - Plate;
  - Brand;
  - Model;
  - Color;
  - Vehicle classes;
  - Number of characters identified on plates: allows identification of partially obscured plate characters, with up to 1 or 2 unidentified characters.

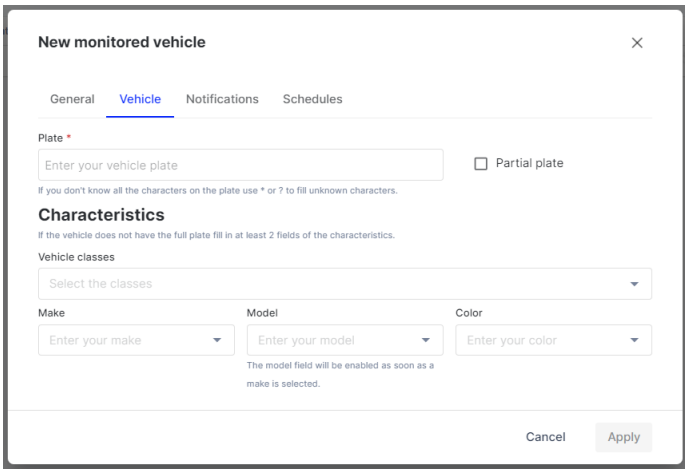


Figure 28 - Example screen in Create new monitored vehicle > Vehicle tab

- *Notifications* Tab:
  - Notification channels: can be received via *Email* and/or *Telegram;*
  - Alert type: can be Audible and/or Visual (Pop-up);
  - Notified people: selecting a Group of responsible individuals and the Users to be notified;
  - Customization of alert notification: the audible alert allows configuration of the sound type and the Pop-up color;
  - *Pop-up retention* can be selected, which keeps the pop-up window open;
  - Alert audio playback: audio volume and playback speed are adjusted.

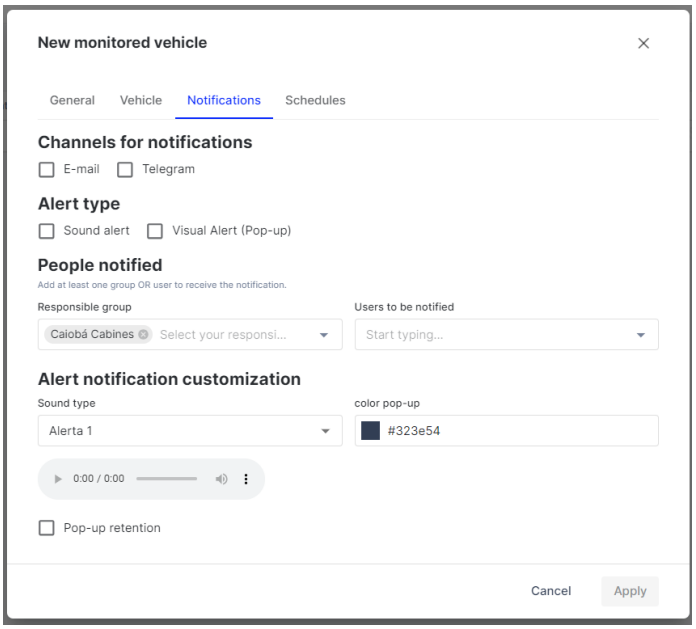


Figure 29 - Example screen in Create new monitored vehicle > Notifications tab

In *Schedules*, the initial and final alert reception times for the vehicle when identified can be specified by day of the week:

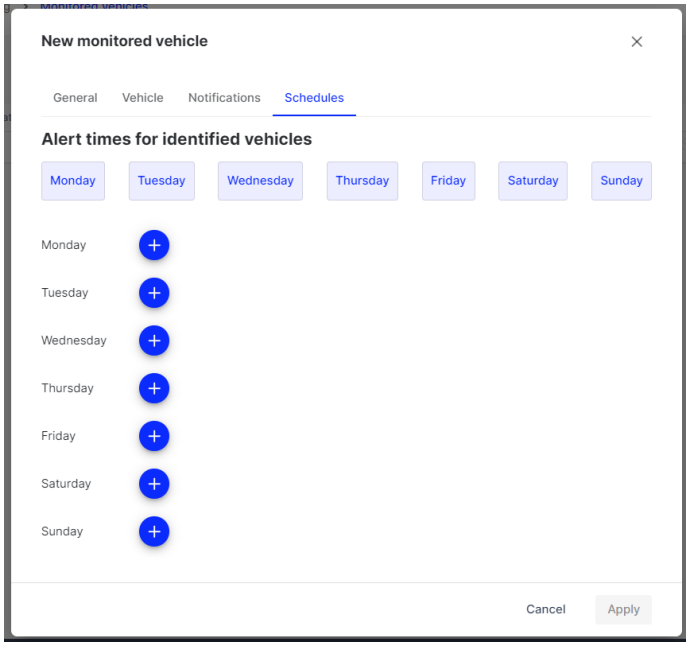


Figure 30 - Example screen in Create a new monitored vehicle, Time tab

About the CSV File

The CSV (Comma-Separated Values) file is used for importing monitoring data and must have fields written in the order and format below:

- License plate;
- Monitoring_name;
- Description;
- Vehicle_characteristic;

- Monitoring_type;
- Start_date;
- End_date;
- Audible_alert;
- Pop-up_alert;
- Email_notification.

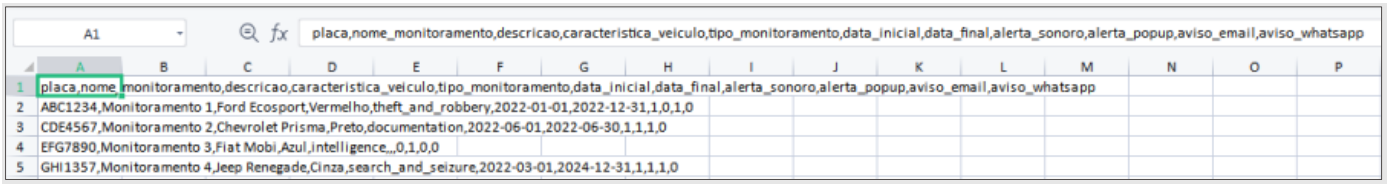


Figure 31 – Example spreadsheet with data in CSV format

Incident Rules

The captures displayed in the *Incidents* panel were made considering the created *Incident Rules* that consider the type of incident, for different purposes:

1) *Border Control*: monitor state borders and neighboring countries' borders;
2) *Speeding*: monitor vehicles' maximum speed on roads, additionally configuring alert times for identified vehicles, by day of the week;
3) *Exclusive lane*: monitor lanes exclusive for buses and, in some cases, taxis and school vehicles, specifying the allowed vehicle class and defining alert times for identified vehicles, by day of the week;
4) *Car rotation*: monitor traffic in areas with vehicle plate rotation, specifying restricted plates, and prohibited vehicle types, and defining alert times for identified vehicles, by day of the week;
5) *Blocked road*: monitor pedestrian-permitted roads blocked for vehicles, defining alert times for identified vehicles, by day of the week.

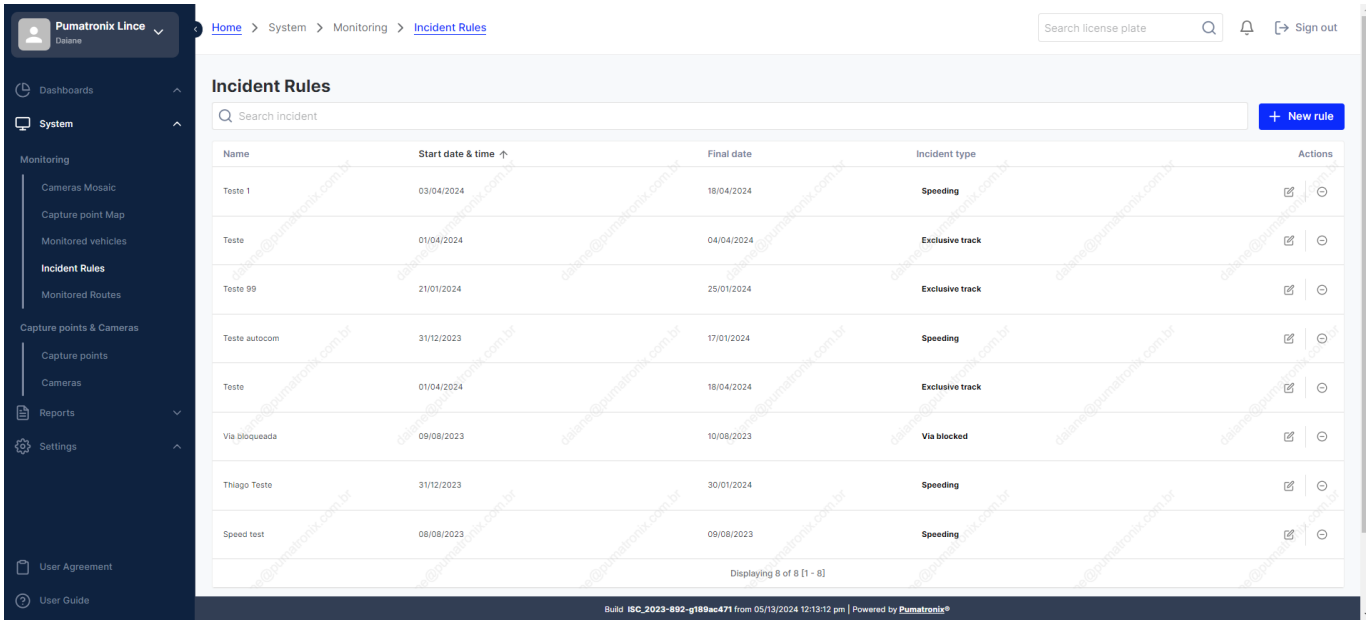


Figure 32 – Example of the initial screen in System > Incident Rules

Creating a new incident rule with *+New rule* opens the window with fields to be filled out according to the type of incident, with common fields for all:

- *Activation date*: selection of the start day of the new rule's validity;
- *Expiration date*: selection of the day when the new rule's validity expires;
- *Name*: identification of the new rule;
- Incident rule type: selection of the rule type among possible incidents like Speeding, Exclusive lane, Blocked road, Car rotation, and Border control;
- *Capture Point*: selection of the Capture Point where the set of devices of interest is located;
- *Cameras*: selection of the devices where incident records should be detected.

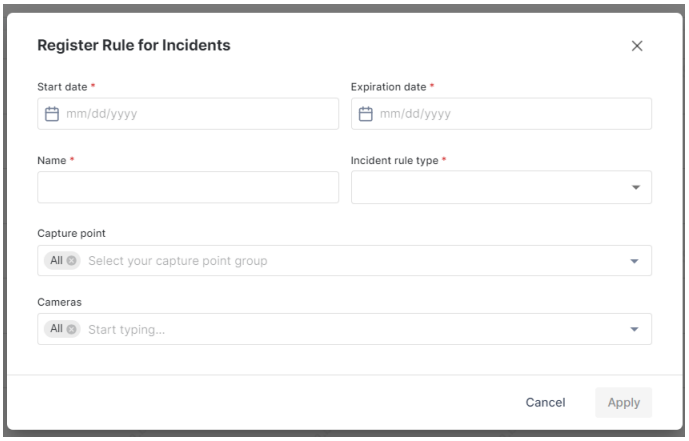


Figure 33 - Initial screen for creating a new incident rule

Monitored Segments

The registered *monitored segments* are used in the database for the *Flow Analysis* panel and are responsible for controlling the speeds practiced in the registered segments. In the actions column, it is possible to edit or remove a created segment:

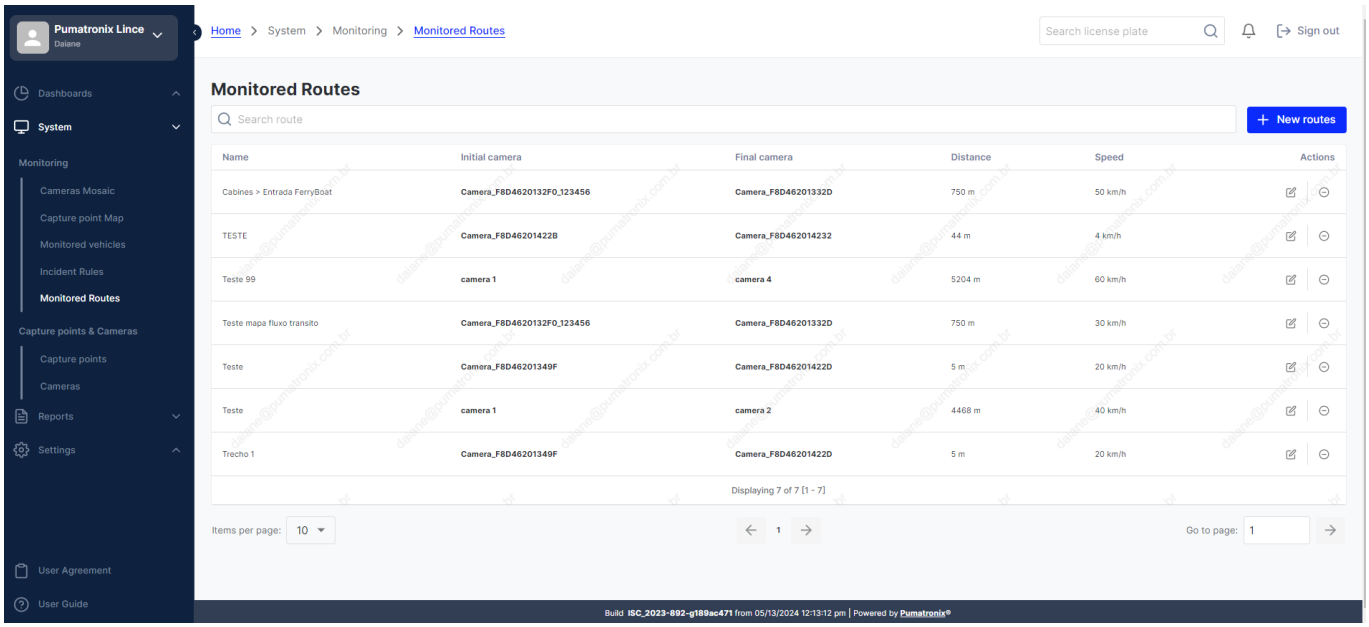


Figure 34 - Example of the initial screen in System > Monitored Segment

Registering a segment with *+New segment* opens the window with fields to be filled out:

- *Segment name*: the identification of the segment should be inserted;
- *Initial camera*: select the device that will be considered at the beginning of the segment;
- *Final camera*: select the device that will be considered at the end of the segment;
- *Distance between cameras*: indication of the distance between the initial and final devices of the segment, in meters;
- *Segment speed*: indicate the value, in km/h, of the speed that can be practiced on the segment;
- *+ Add new segment*: by clicking, it is possible to indicate an additional segment as a sequence of the same segment;

Figure 35 – Initial screen for registering a new segment

Capture Points

A *Capture Point* refers to a group of devices that are located in the same region when *fixed*, or to *Mobile* or *Smartphone* devices. Registering new devices depends on the existence of the *Capture Point* to which they can be linked.

When accessing *System > Capture Points*, all devices inserted in the system are listed alphabetically by name, and they can be edited and/or removed in the actions column:

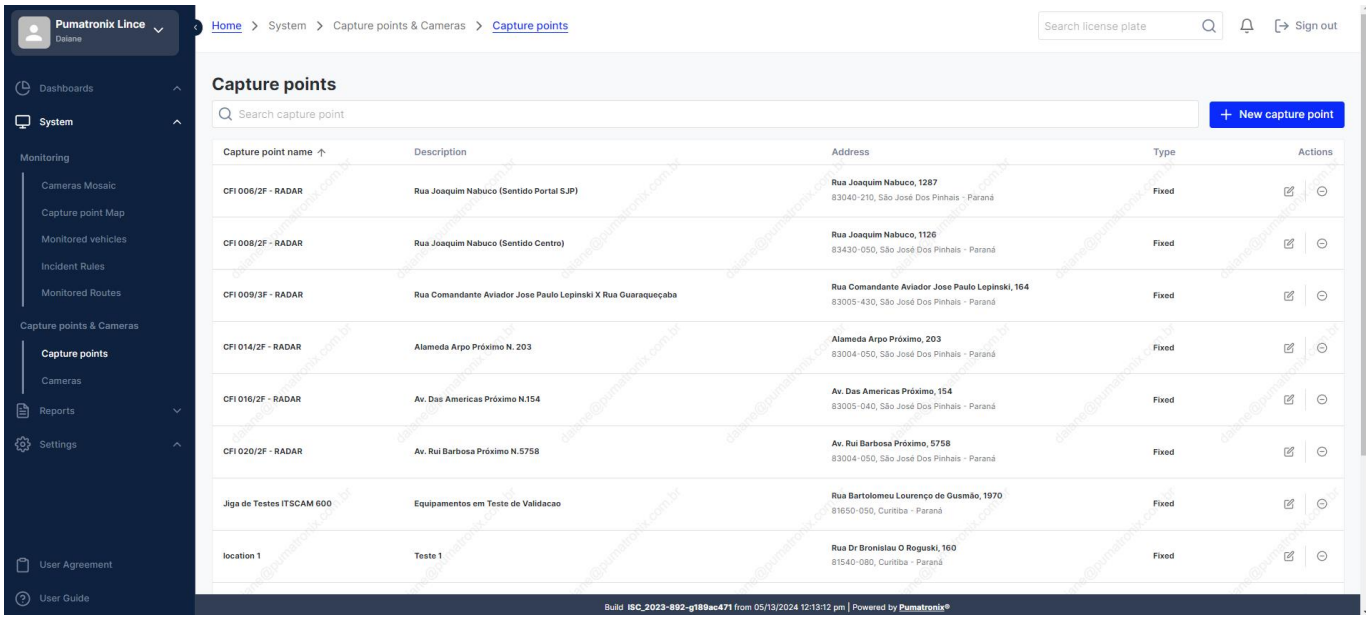


Figure 36 - Example of the initial screen in System > Capture Points

Registering a new location with *+New capture point* opens the window with fields to be filled out:

- *Capture point name: identification of* the device in the system;
- *Type*: characteristic of the capture device installation, it can be *Fixed* (poles) and *Mobile* (stationary or moving vehicles), or even a *Smartphone*;
- *Description*: additional information about the item.

In the case of Fixed-type equipment (poles), it will be necessary to indicate the location by entering the Address, Number, State, City, ZIP Code, and Latitude and Longitude data, indicating the geographical coordinates of the installation. Suppose the latitude and longitude are not known. In that case, the user can click on *Select address and enter* the location's address, or mark the point on the map, and the tool will return the latitude and longitude of the indicated location.

Figure 37 - Initial screen for registering a new capture point

A *capture point* registered in the Lince system should be considered as a grouping of capture devices in the same location.

Cameras

When accessing *System* > *Cameras*, the image capture devices inserted into the system are listed in alphabetical order, can be edited or removed separately, and display the data of the current *Status* and the *Last communication* made by the device, in addition to the data *of the Capture Point* to which it refers and the *Serial number of* the device.

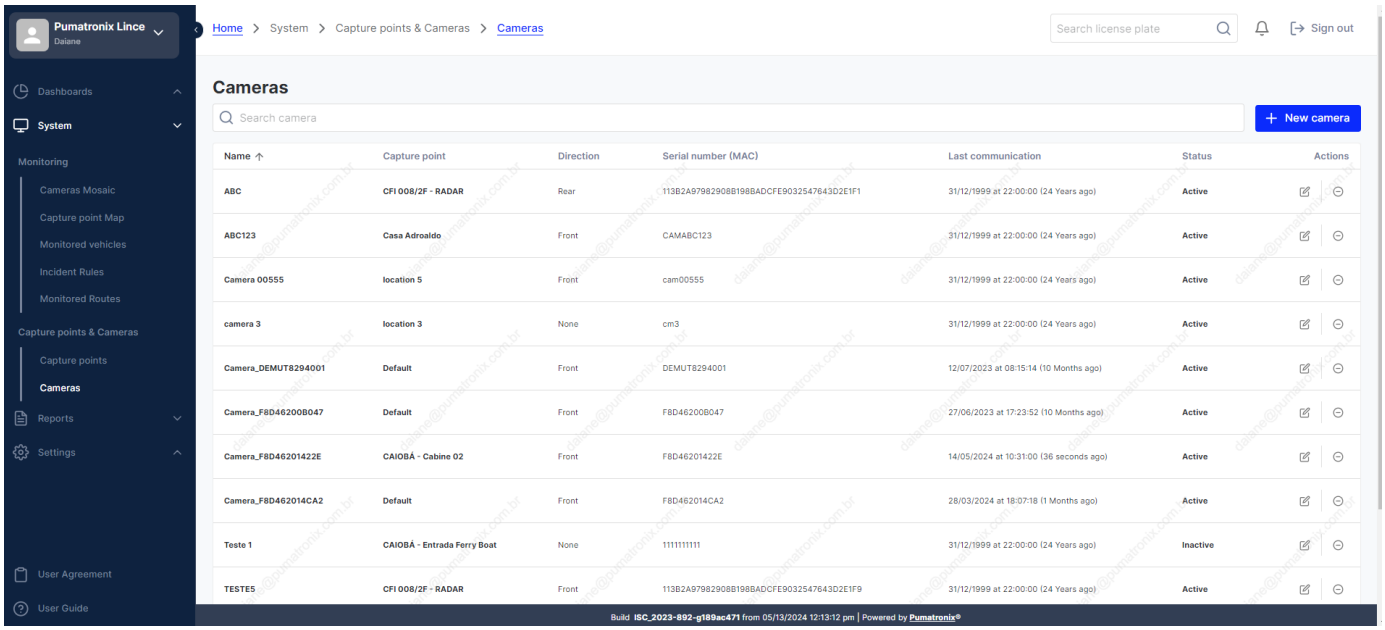


Figure 38 - Example of the initial screen in System > Cameras

Registering a new device with *+New camera* opens the window with fields to be filled out:

- *General* Tab:
  - *Name*: identification of the device in the system.
  - *Status*: keeps the registration active when selected;
  - *Capture Point*: selection of the location to which the device is associated;
  - *Direction*: characteristic of how the device is installed, identifying the direction of the road. This installation can capture Front, Rear, or Undefined direction images;
  - *Serial Number*: data for identifying the installed device;
  - *Save images with recognized plate*: when *Active*, images of captures with recognized plates will be stored in Lince, along with capture information;
  - *Save images without recognized plate*: when *Active*, images of captures without recognized plates will be stored, along with capture information;
  - *VMS Configuration*: by enabling integration of the Lince system with a video recording system (VMS), the image capture device must be registered by entering an identification in the *Camera name* and selecting the registered VMS integration.

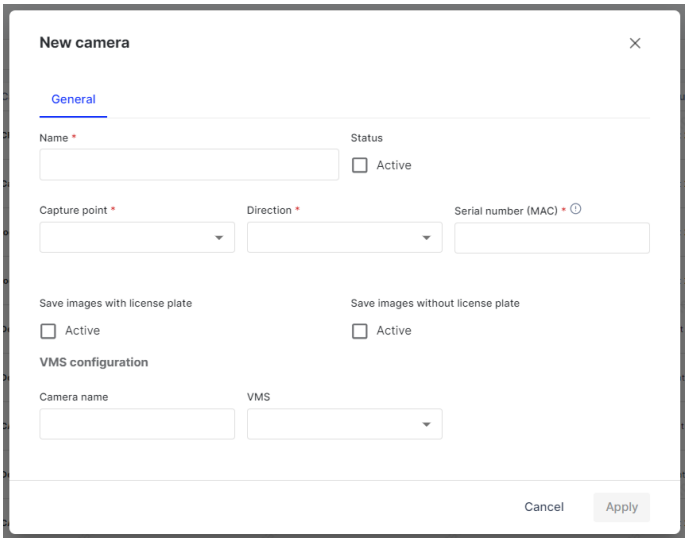


Figure 39 - Initial screen for registering a new capture device

In the *SPIA PRF* tab, the device ID connected to the SPIA system of the Federal Highway Police (PRF) must be entered. It is only possible to send images and records to the SPIA using the device identifier, as registered in the PRF, and data entered in *Settings > Integrations*.

To register a new capture device, it must be linked to a *Capture Point* already registered in the system.

4. Reports

Lince also allows all stored vehicle records to be retrieved and exported in report form.

To generate a report, only the desired results can be selected by choosing among the available records, through the *Filter* button. Additionally, all listed data in the system can be exported using the *Export* button, selecting the file export option.

Capture Report

The *Capture Report* presents on a single page the following information: *Date & Time, Capture Point, Camera, Plate, Make, Model* and *Color, Vehicle Class,* and image of the *Capture*.

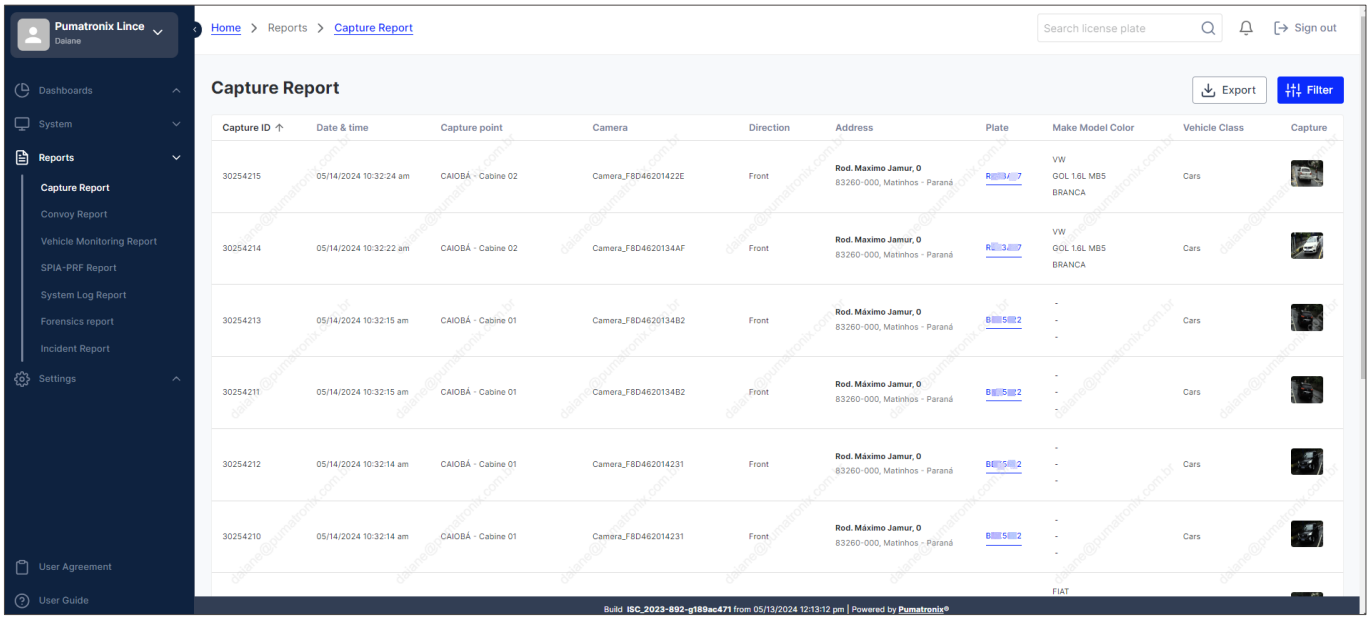


Figure 40 - Example of the initial screen in Reports > Capture Report

It is possible to access the *details of the capture* by clicking on the image of the capture, which opens a window with the registration information. In addition to the registration information, the enlarged image of the detected plate, *Renavam* data, and *location* on the map can be viewed:

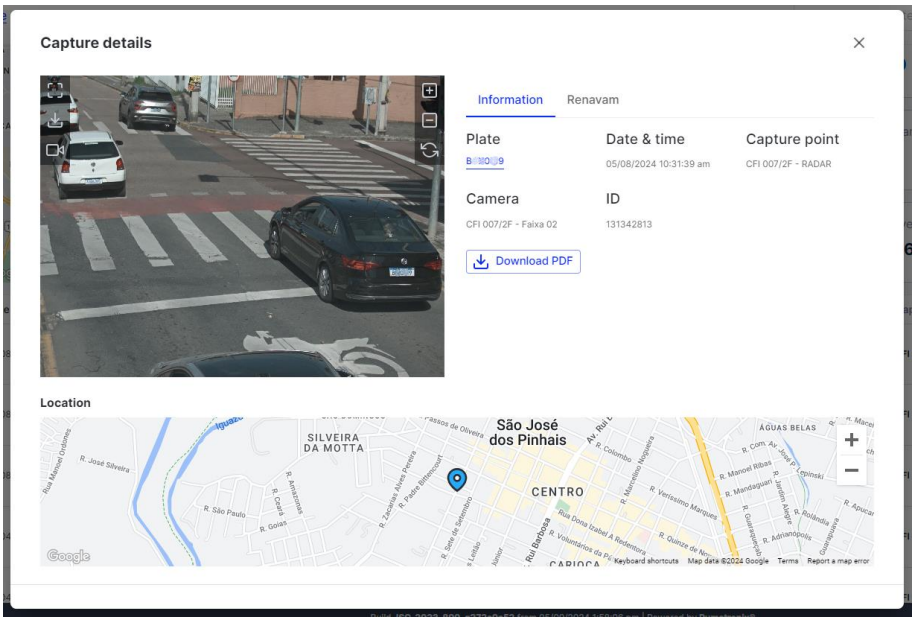


Figure 41- Screen with Capture Details

Clicking *on the vehicle's Plate link* redirects to the *vehicle information* page, which presents all vehicle records. Only the desired results can be selected by clicking on the *Filter* button.

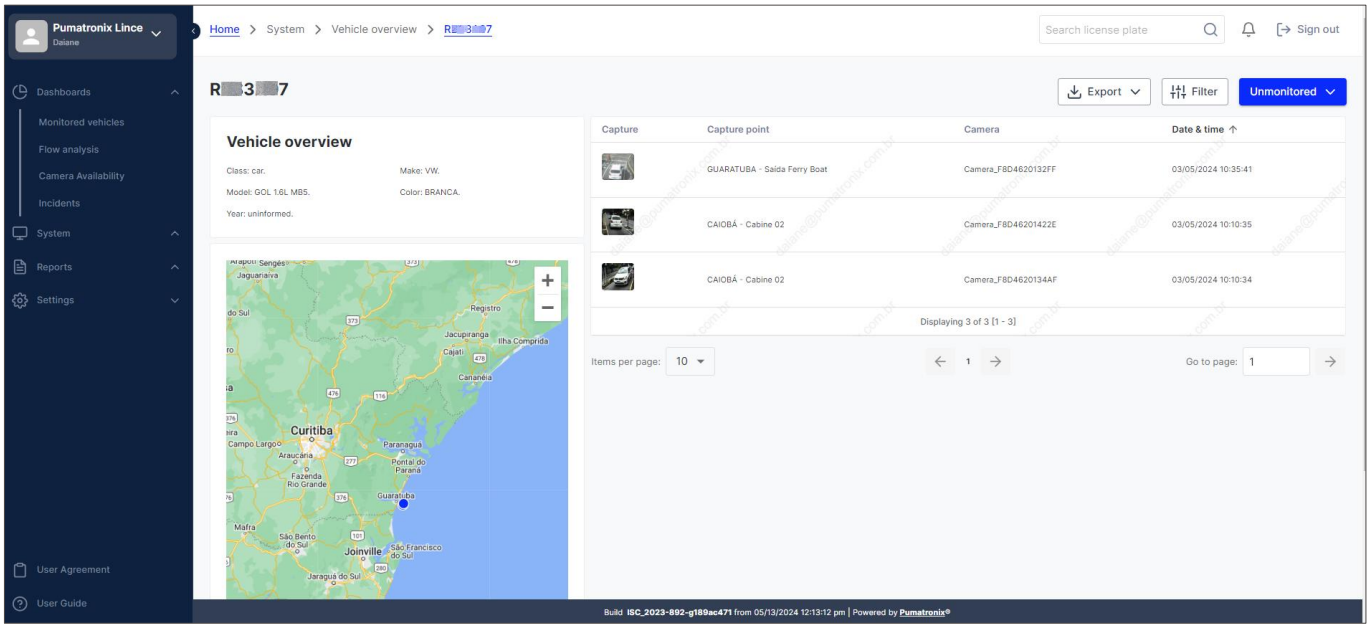


Figure 42 - Example of the Vehicle Information screen

Convoy Report

The *Convoy Report* allows filtering of vehicle records by *License Plate* and *Equipment* (*Capture Point*) within a set of vehicles over a time interval (1-120 minutes).

In *Table* view mode, the following information is presented: *Date & Time, Interval* between captures, *Equipment (Capture Point), Camera, License Plate, Make, Model, Color*, and image of the *Capture*.

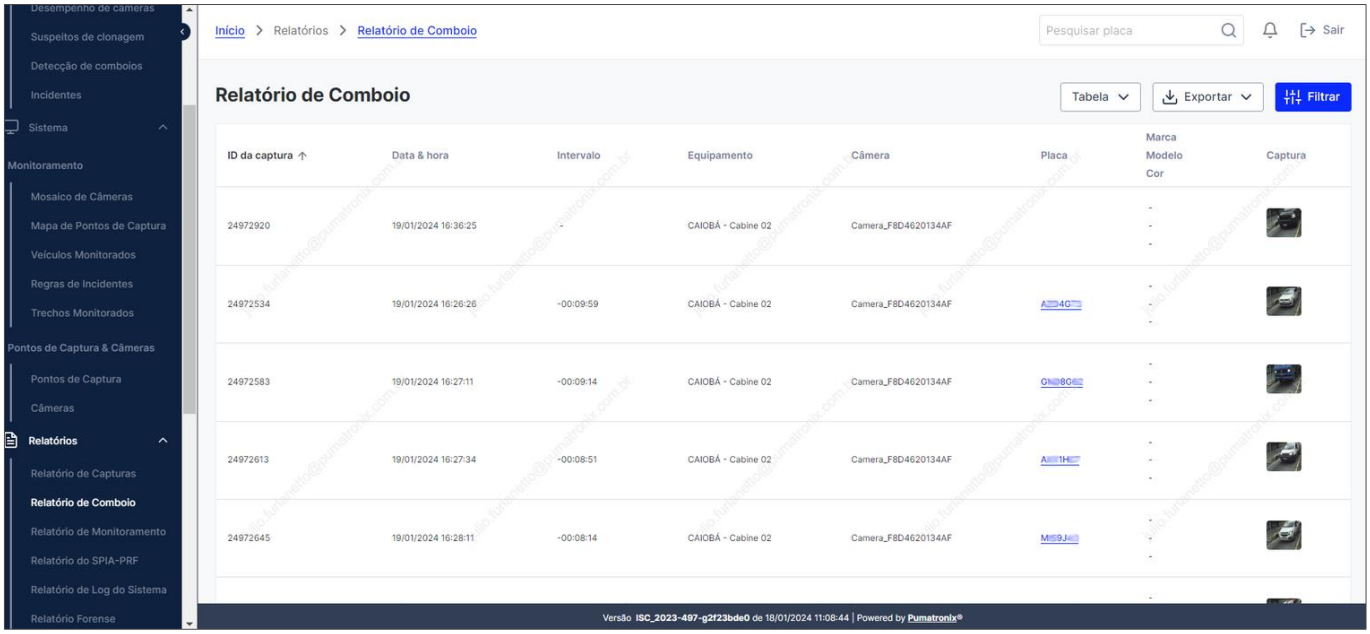


Figure 43 - Example of the initial screen in Reports > Convoy Report

In *Timeline* view mode, images of the convoy captures are presented within the selected time interval.

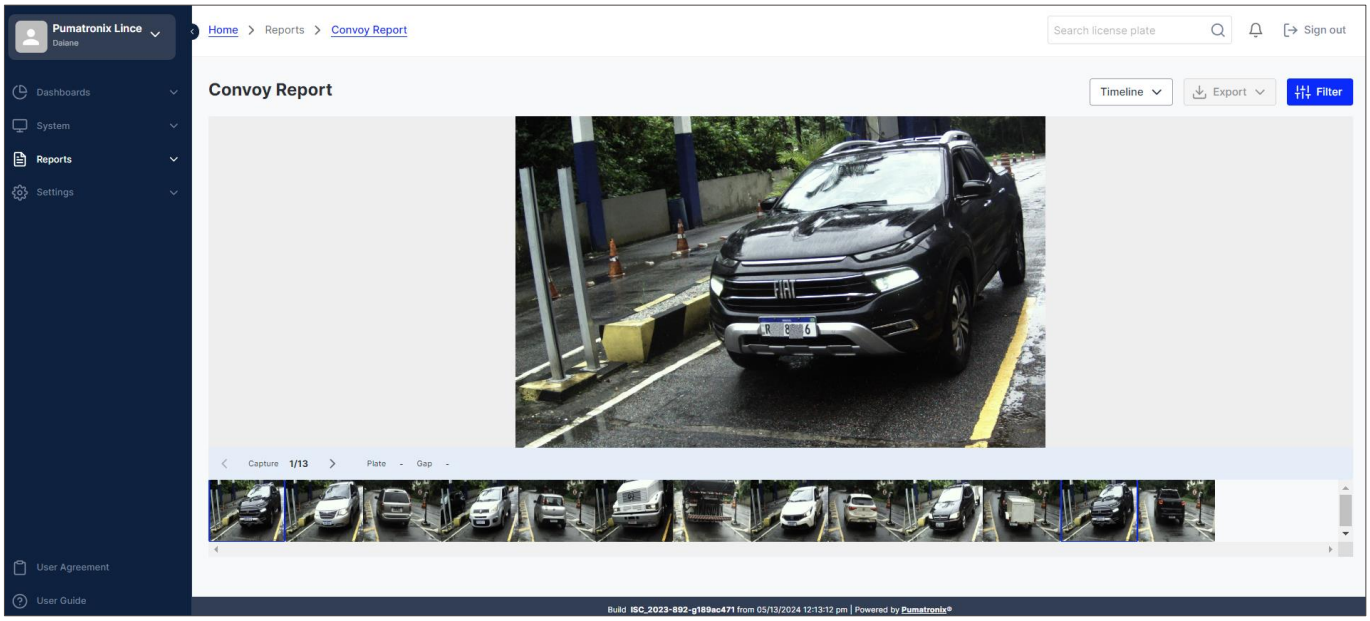


Figure 44 - Example of the initial screen of the Convoy Report in Timeline view mode

Monitoring Report

In addition to the *Date & Time, Capture Point, Camera, License Plate, and Capture* image, the *Monitoring Report* presents the number of times the vehicle was detected within the filtered period.

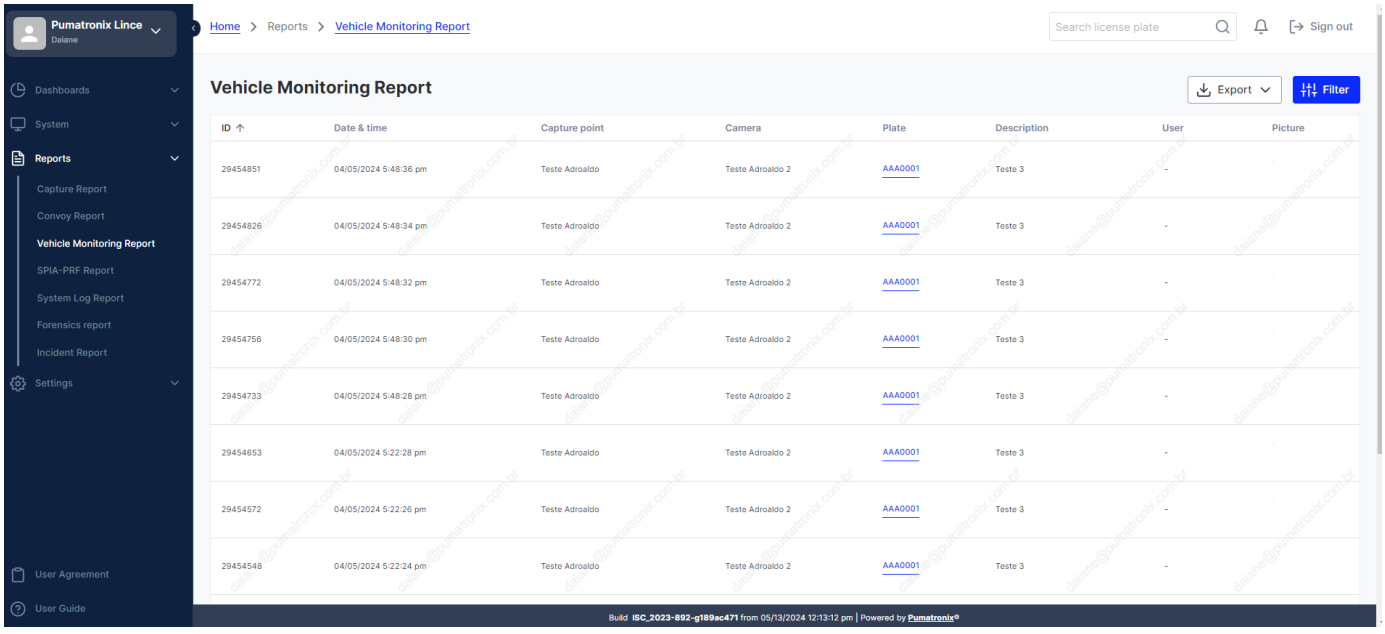


Figure 45 - Example of the initial screen in Reports > Monitoring Report

SPIA-PRF Report

The *SPIA-PRF Report* is only available when integration with the PRF's SPIA system is *configured in Settings*. It presents data such as Detected *Plate*, *Insertion Date (Lince)*, *Update Date (SPIA)*, *Make/Model/Color*, *Year*, *City/State*, *and Administrative and/or Judicial vehicle restrictions*.

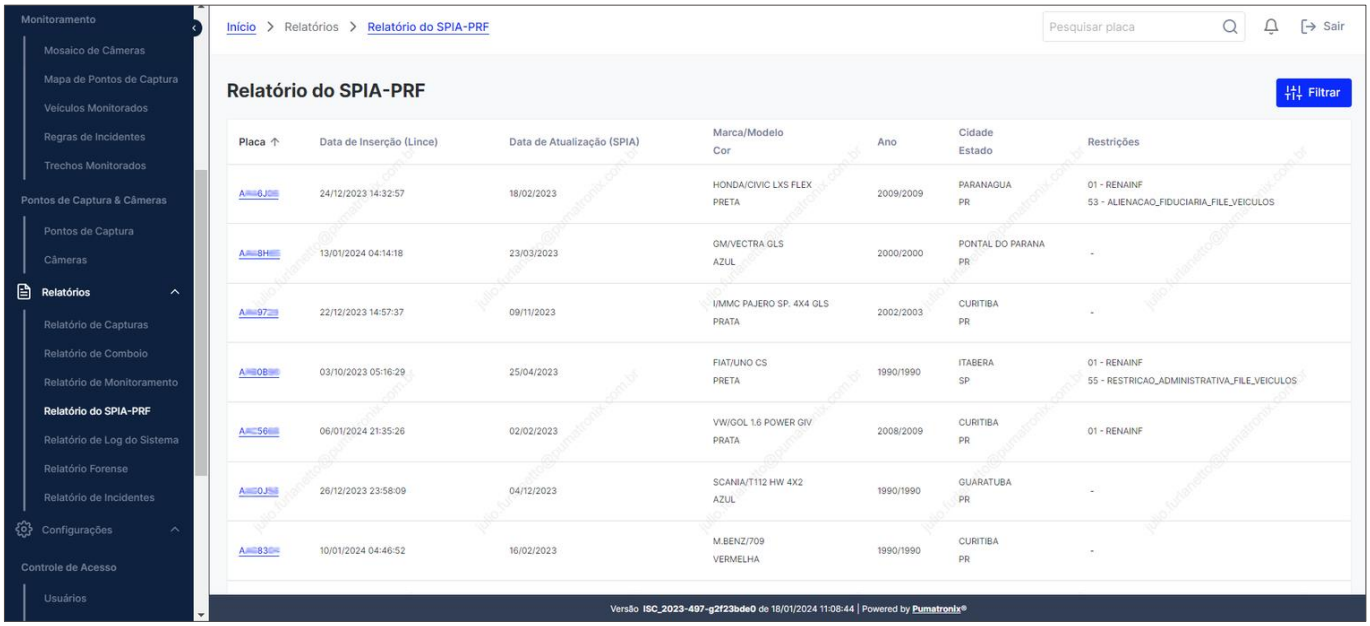


Figure 46 - Example of the initial screen in Reports > SPIA-PRF Report

System Log Report

The *System Log Report* presents all accesses made in the system with *Date & Time, User,* and *Message* information showing the menu accessed by the user and whether they succeeded in accessing it or not.

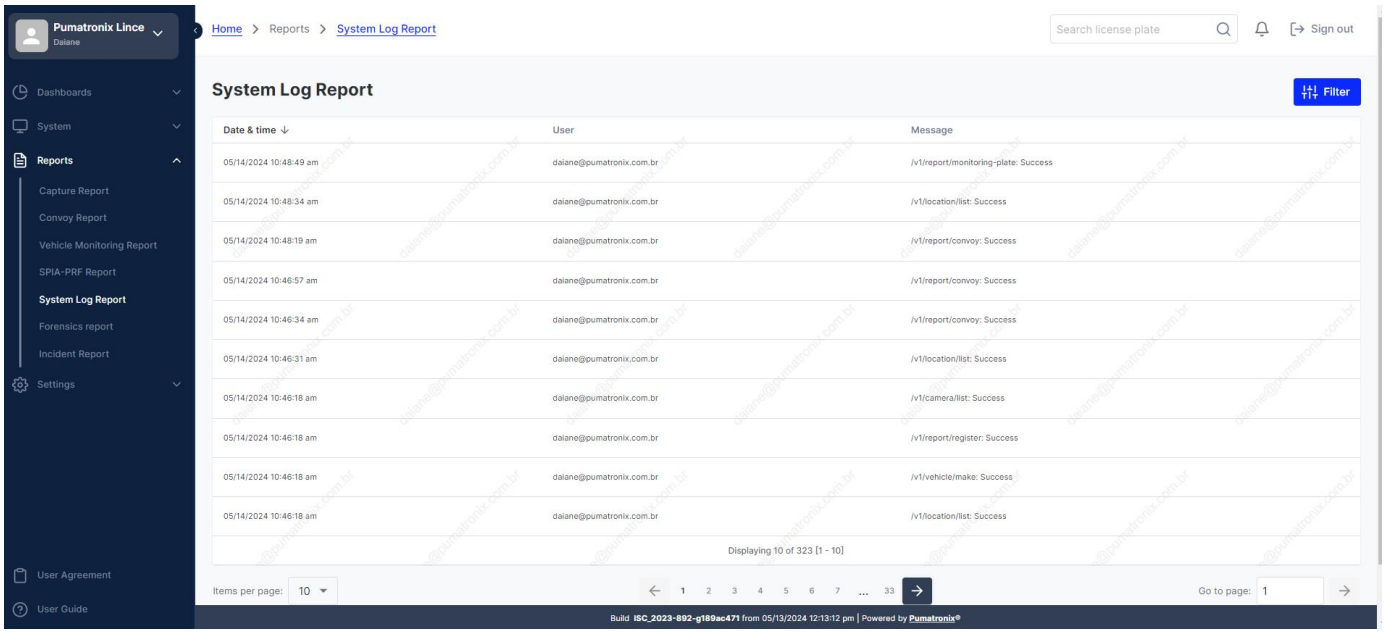


Figure 47 - Example of the initial screen in Reports > System Log Report

Forensic Report

The *Forensic Report* is a feature of the Lince system that allows the creation of a report with free text input, including images and tables, related to any event involving a vehicle listed in the system. With the possibility of user participation in the comments field, the report author can grant editing access to specific users, creating a collaborative point in describing an event.

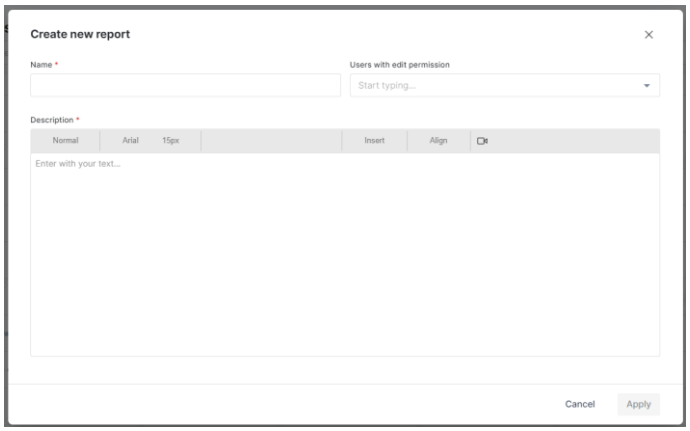


Figure 48 - Initial screen for creating a new report

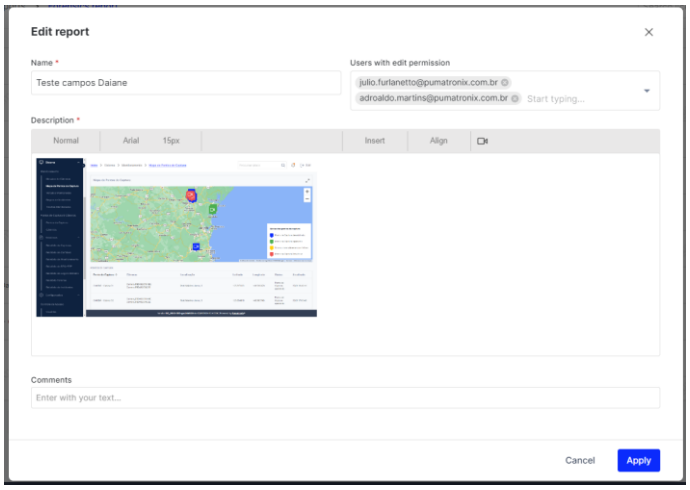


Figure 49 - Initial screen for editing a report

Incident Report

The *Incident Report*, in addition to providing *Date & Time, Camera, License Plate, City, State,* and *capture* image information, also displays the *type of incident* detected during the filtered period.

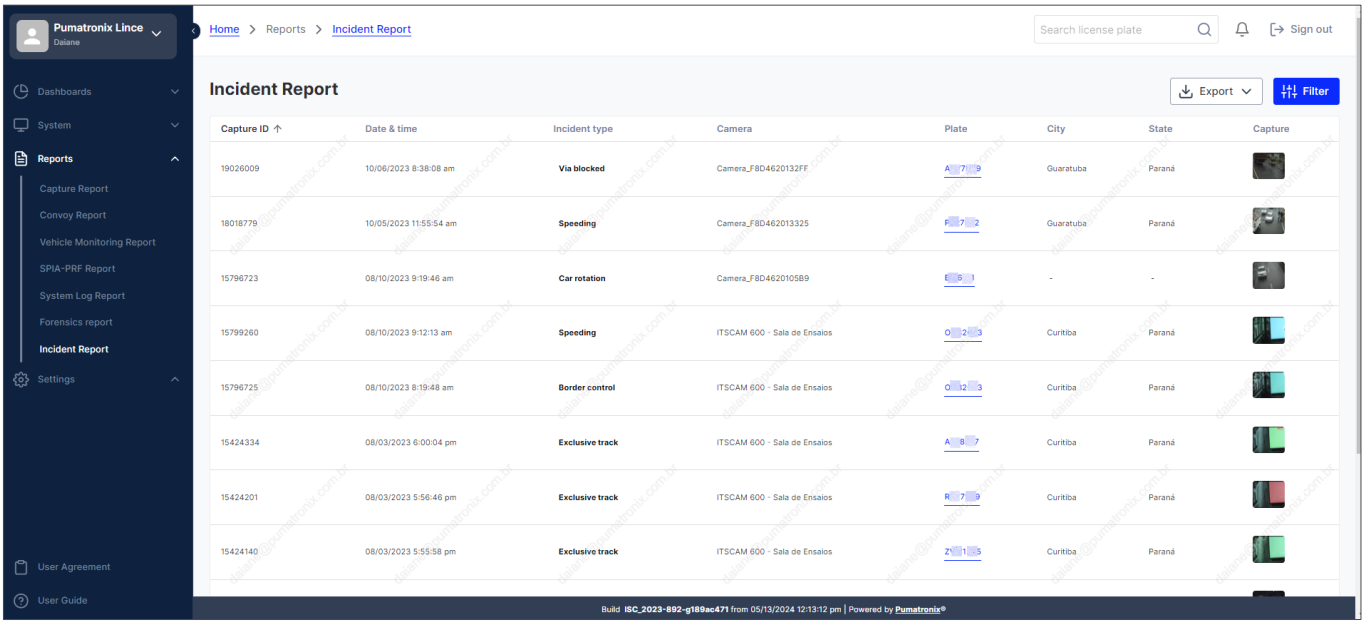


Figure 50 - Example of the initial screen in Reports > Incident Report

5. Settings

This menu contains options for general adjustments available for the system, grouped under *Access Control*, *System, and Settings*. These will be addressed in the sequence of this manual, by configuration group.

Access Control Configuration

To manage access to the system, users and access profiles must be registered. All actions performed in the system will be recorded in *the System Log*.

First Access

Upon accessing the Lince system address at https://lince.app.br, the first screen displayed is the login page, with fields for *Username* and *Password*:

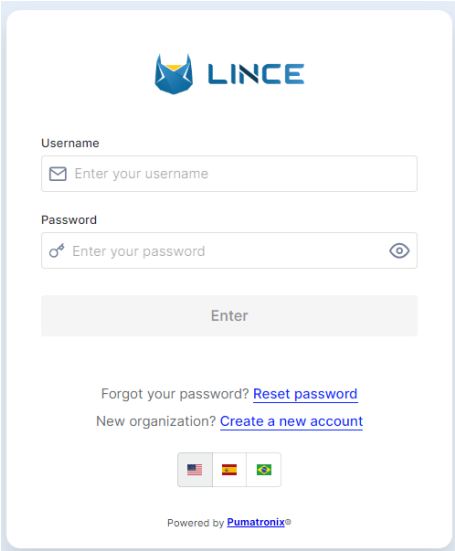


Figure 51 - Login Screen

To create an account, you need to access the "*Create a new account*" link and then fill out the form with the following fields:

- Organization Identification: Identification with CPF or CNPJ and *Organization Name;*
- Address: Valid user or company address with *Number and Complement, ZIP code*, *Country*, *State*, and *City;*
- Contact Person: Indication of the organization's contact with the insertion of the *Telephone;*
- Username (email): Valid user email address, intended for user identification in the system and receipt of monitored vehicle alerts;
- Password: User access protection to the system, with a minimum of 6 characters and must contain lowercase or uppercase letters combined with 1 numeral and at least 1 special character (@, #, $, or %).

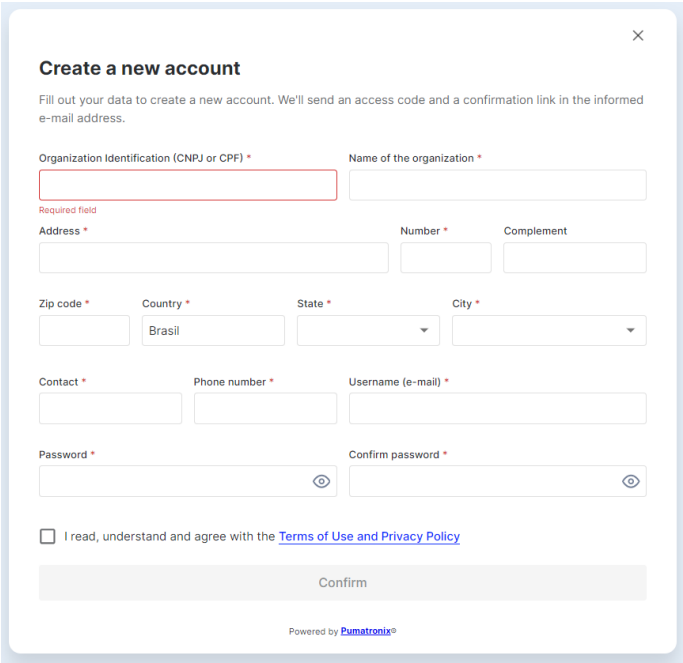


Figure 52 - New Account Registration

After filling out all the above data, an **access code** and a **confirmation link** will be sent to the email address provided.

By entering the value received by email and completing this procedure, it will be possible to log in to access the system.

Reset password

If you forget your password, the reset can be done through the "*Reset Password" link,* also located on the login page. Then, the registered email must be provided, and the request completed through the "*Continue*" button. A message with instructions for setting a new password will be received at the email address provided.

Account information can be accessed, and the previously registered password in the system can be changed by accessing "*My Account*," located in the upper left corner of the screen.

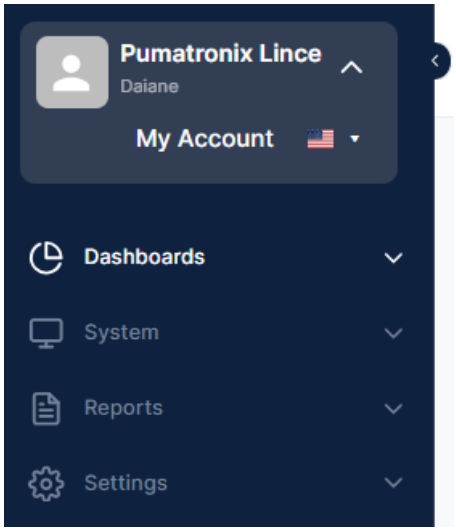


Figure 53 - Access to Account Information

On the next screen, the fields for *Current Password, New Password*, and *Confirm New Password* must be filled out:

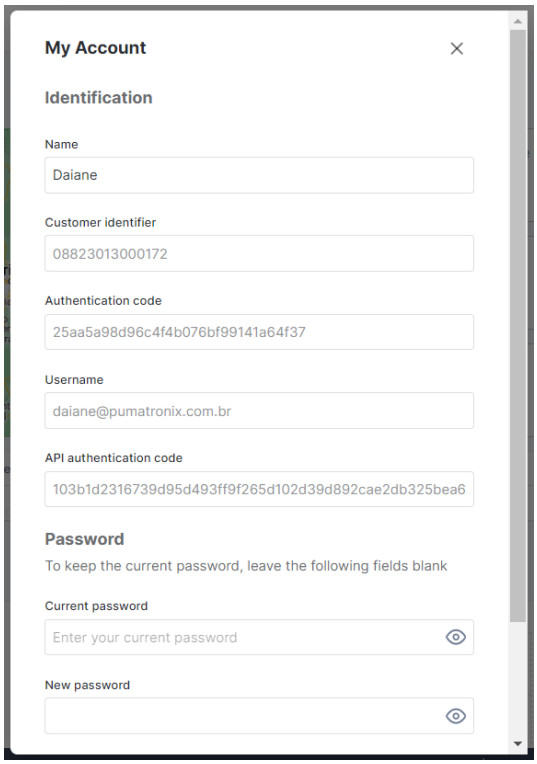


Figure 54 - Initial Password Change Screen

Language Setting

In Lince, it is possible to set the system language at the bottom of the login screen, which remains changed during access and can be modified in a new access. Optionally, the language can be set after logging in, next to the "*My Account*" field. Currently, Portuguese, *English*, or *Spanish* can be chosen.

Users

In the *Users* menu, it is possible to view all registered users, register new users, edit data, or remove users.

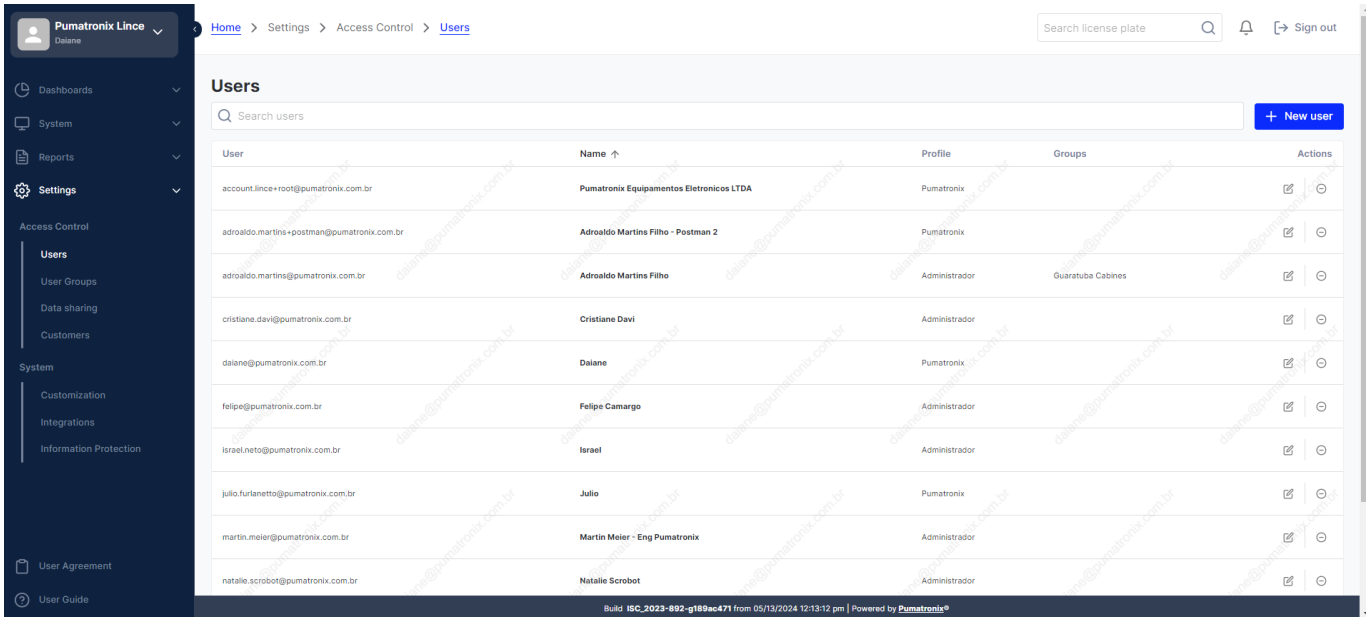


Figure 55 - Example of the initial screen in Settings > Access Controls > Users

Registering a new user by clicking on "*+ New User*" opens a window with the following fields to be filled out:

- Name
- Email
- Password
- Access level (Administrator or Client)
- Sub-level of access

After filling out the required information, it is necessary to save the information by clicking on the "*Apply" button.*

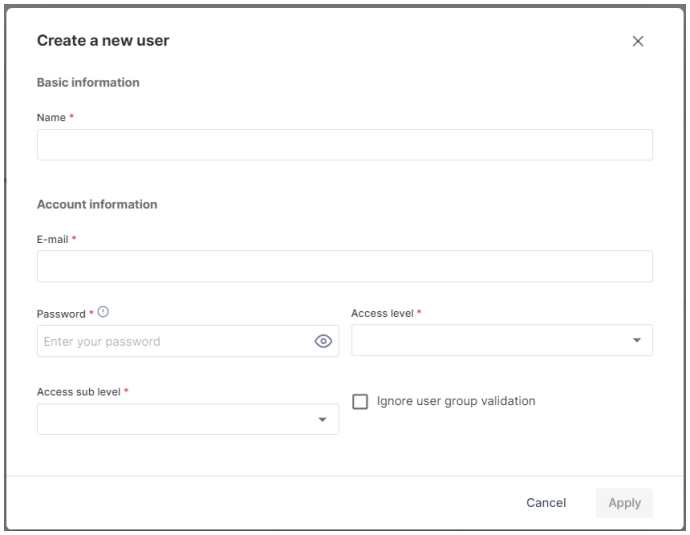


Figure 56 - Initial screen for registering a new user

User Groups

In Lince, access control is possible using the *User Groups* functionality in conjunction with monitoring. By adding a user to a group, all members can receive notifications regarding a monitoring event created in *System > Monitored Vehicles*, which may refer to a *Monitoring Rule* and/or a *Monitored Vehicle*, respectively.

In the *User Groups* menu, you can view all created user groups, edit existing ones, or remove them, and register a new *User Group by clicking "+ New Group,"* which opens a window with fields to be filled out with the *Name* and *Description.*

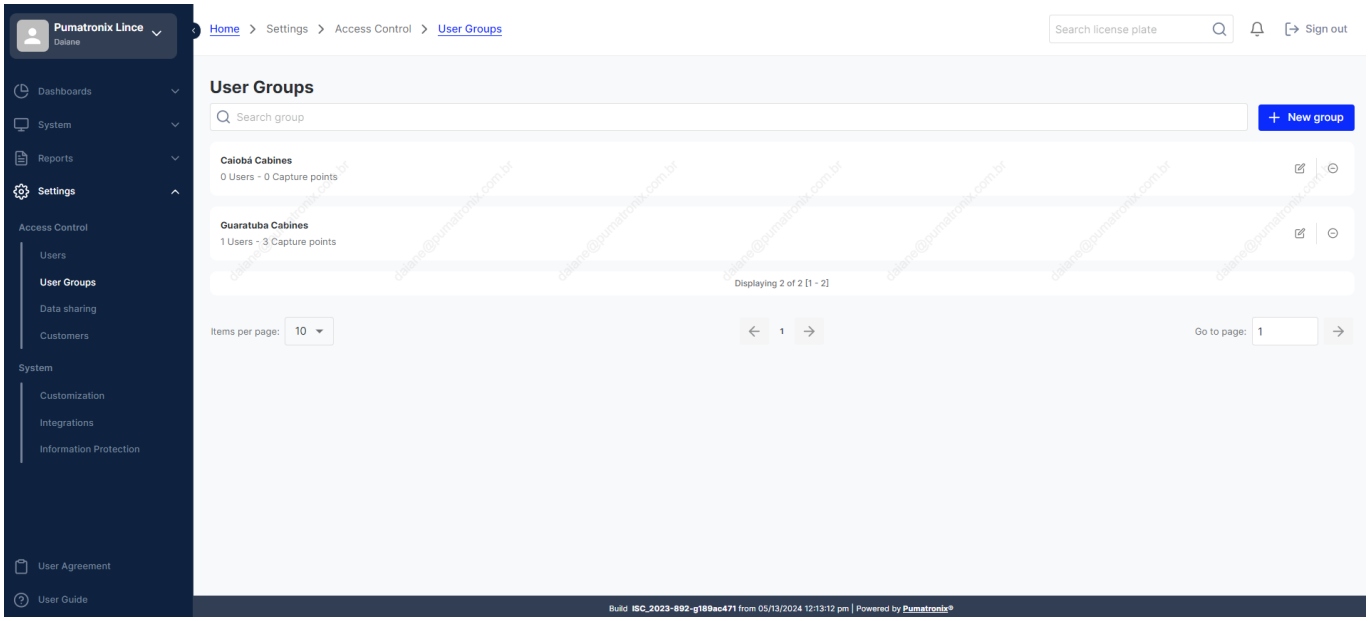
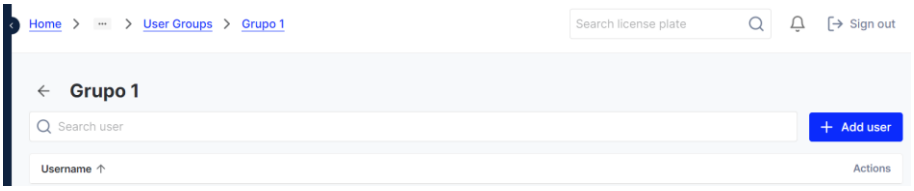


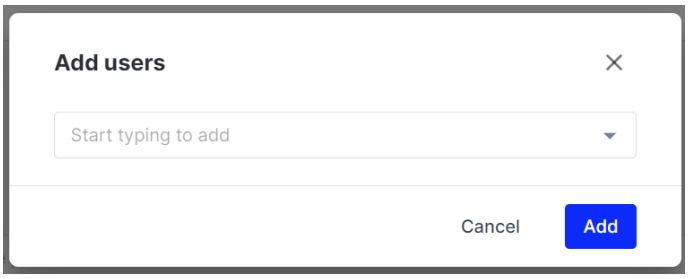
Figure 57 - Example of the initial screen in Settings > Access Controls > User Groups

To add users to a group:

1) Click on the group name, and the new page displays the corresponding users:



2) Click on the *+ Add User* button.
3) Search for and select a user from the registered ones.
4) Click on *Add:*



Data Sharing

In the *Data Sharing* option, it is possible to share information *from a Capture Point* or a specific image capture device with the *Clients* previously registered in the system. The shares are organized in the *Received* and *Shared* tabs:

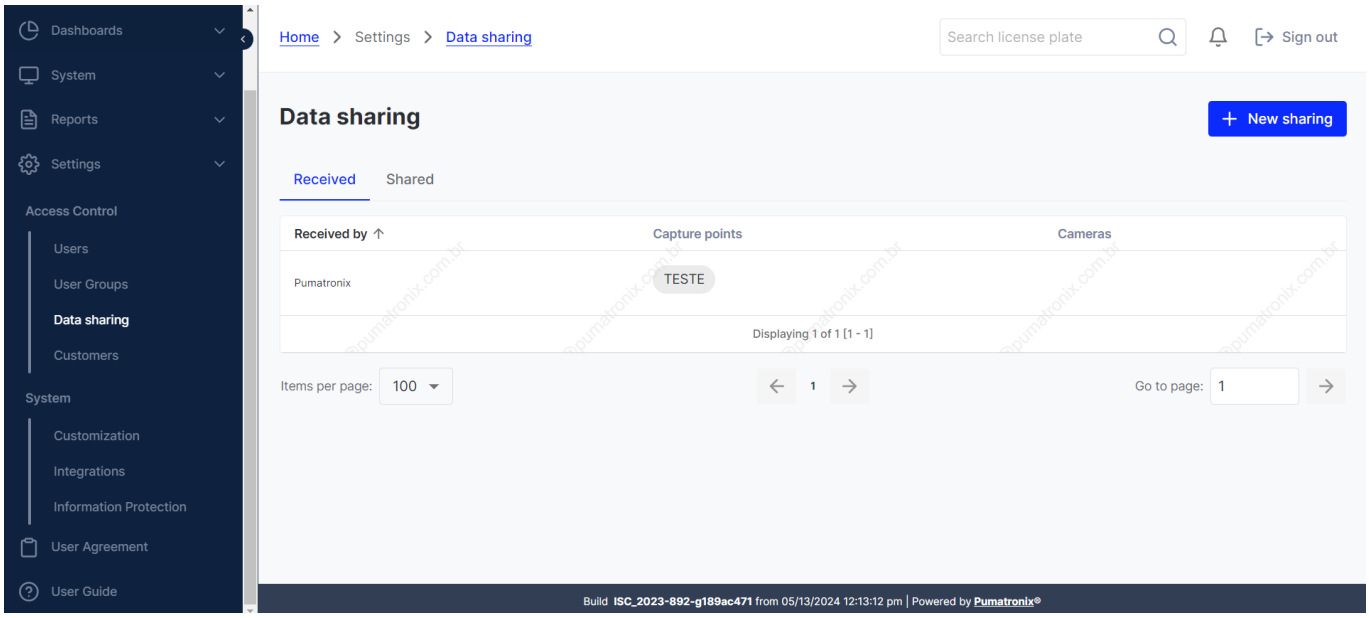


Figure 58 - Example of the initial screen of received data in Data Sharing

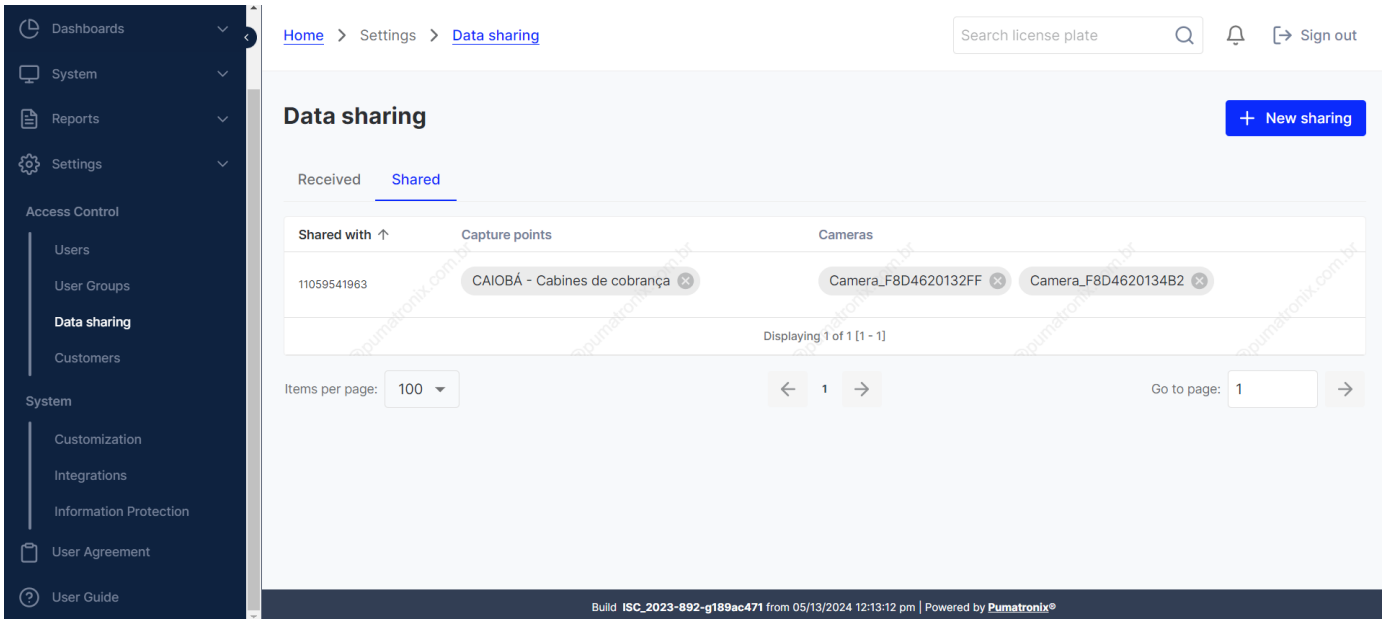


Figure 59 - Example of the initial screen of shared data

Sharing data by clicking "*+ New sharing*" opens a window to select the client who will have access to the data and the capture point or camera to be shared. After filling in the information, click on the "*Apply*" button to save the information.

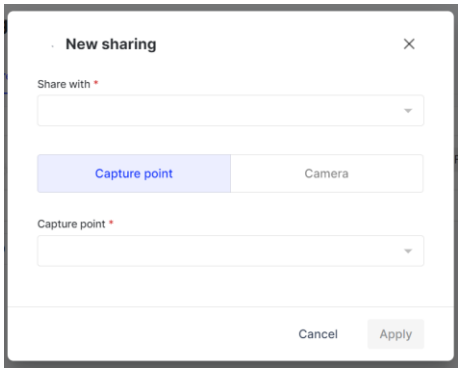


Figure 60 - Initial screen for registering a new sharing

Clients

In the *Clients* menu, you can view registered clients, add new clients, and edit or remove them from the system.

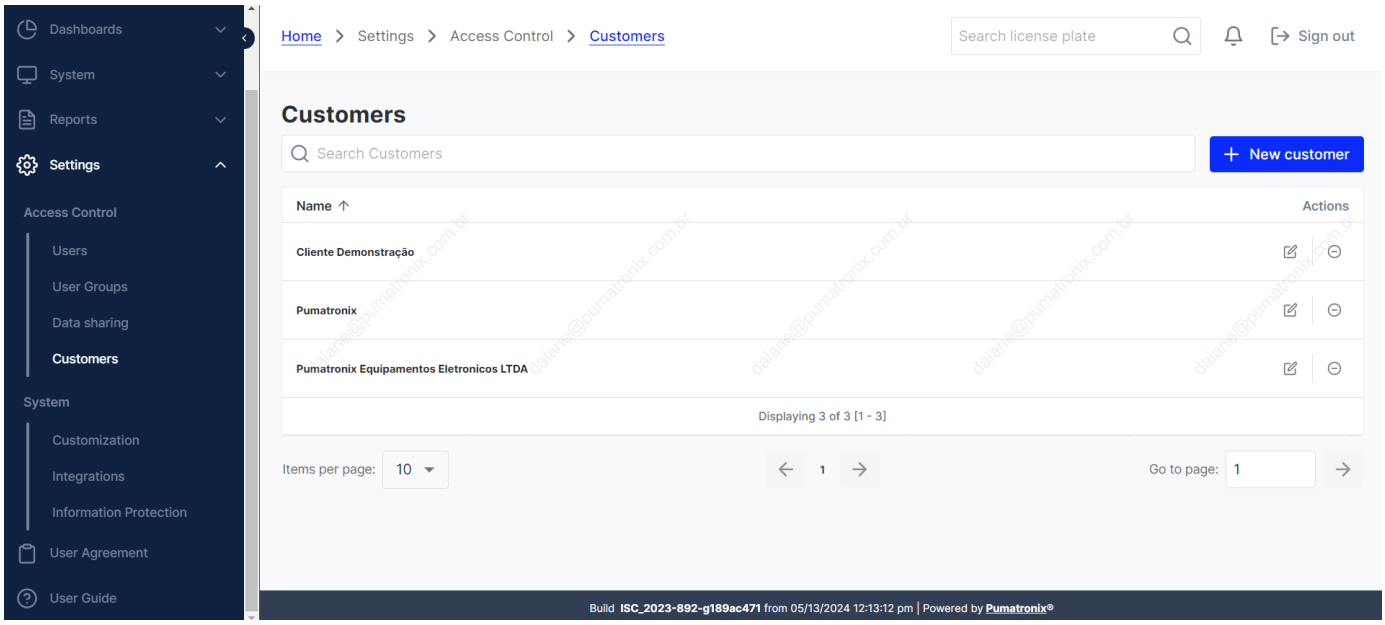


Figure 61 - Example of the initial screen in Settings > Access Controls > Clients

Registering a new client by clicking "*+ New Client*" opens a window to fill in the following fields:

- Organization identification: CPF or CNPJ identification
- Organization name
- Address: valid address of the user or company indicating *Number and Complement,* ZIP code, Country, State, and City
- Contact person: indicate the representative person of the organization who is responsible for contact, indicating their *Telephone* and *Time Zone*
- Verticals: select the set of standard functionalities according to the client's segment

After filling in the information, click on the "*Apply*" button to save the information.

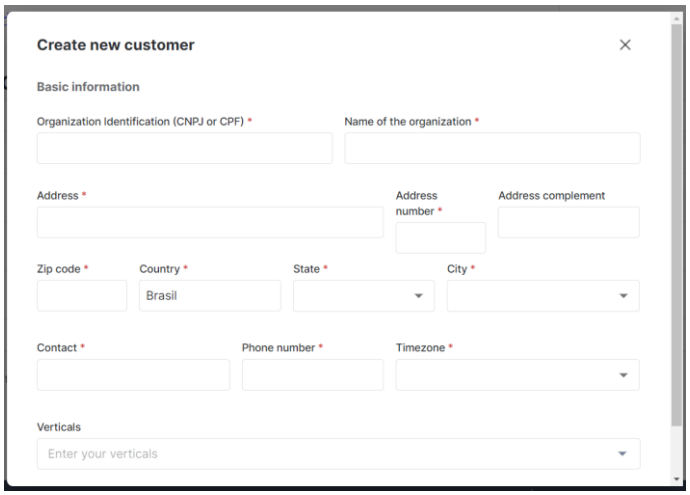


Figure 62 - Initial screen for registering a new client

System configuration

The options for *Customization*, *Integrations*, and *Information Protection* constitute the system configuration available for Lince.

Customization

The Lince system interface can be customized in the following options: it is possible to change the name displayed on the main screen (located in the upper left corner), the header image (located next to the left of the name), and the primary and secondary colors of the system.

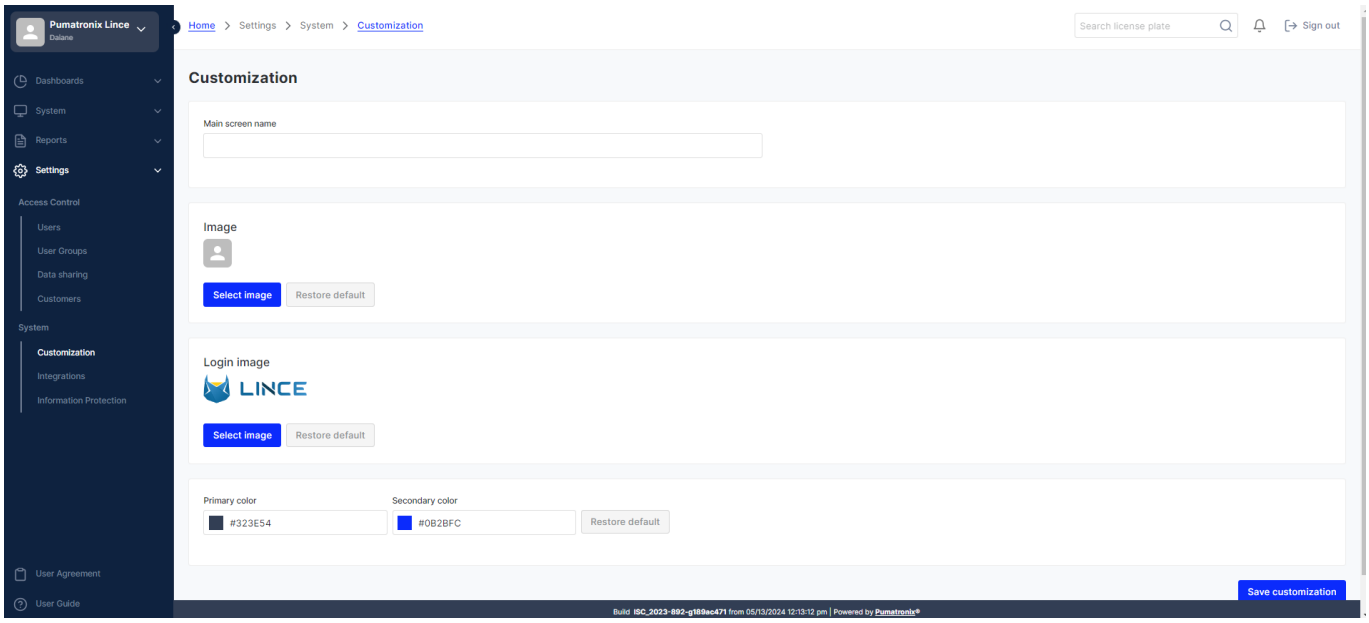


Figure 63 – Example of the initial screen in Settings > System > Customization

Integrations

In the *Settings > Integrations* menu, it is possible to enable and configure integration of the Lince system with the security systems *Detecta-SP* and *SPIA-PRF*. Integration with *Telegram* allows the sending of monitoring alerts, and with *VMS*, integration with a video recording system can be configured.

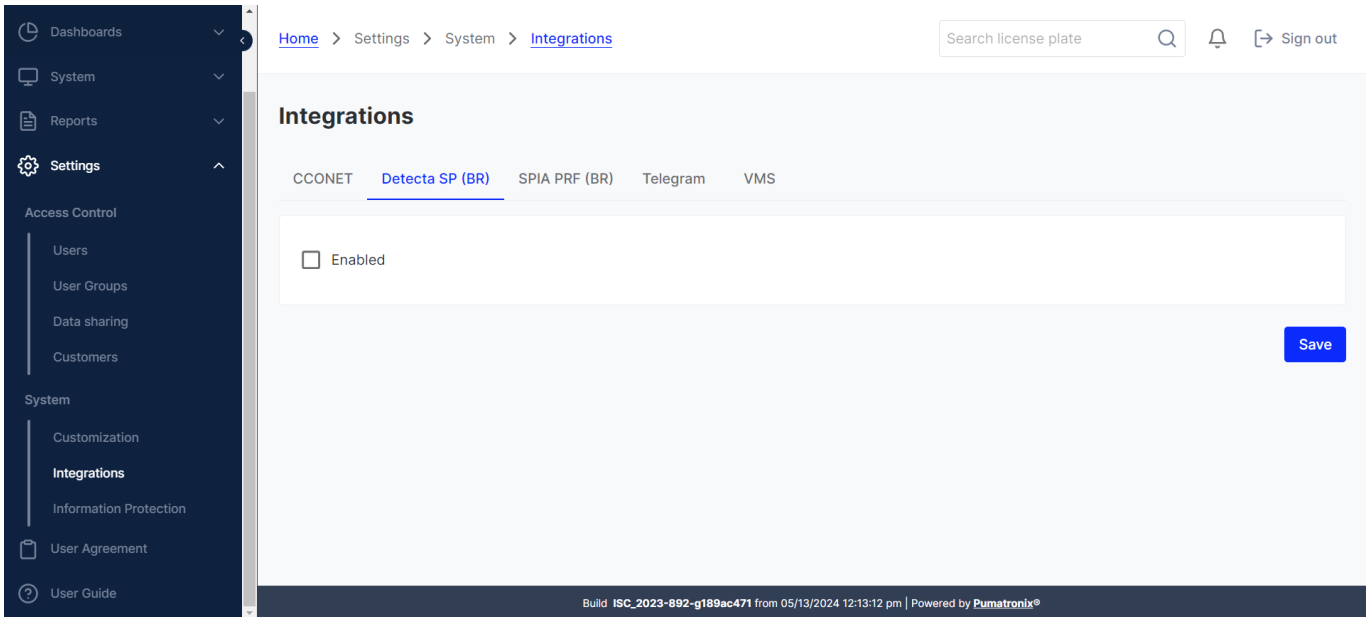


Figure 64 - Example of the initial screen in Settings > System > Integrations

Integrate with Detecta SP

To integrate the system with Detecta *SP*, it is necessary to select *Enabled* and click on *Save*:

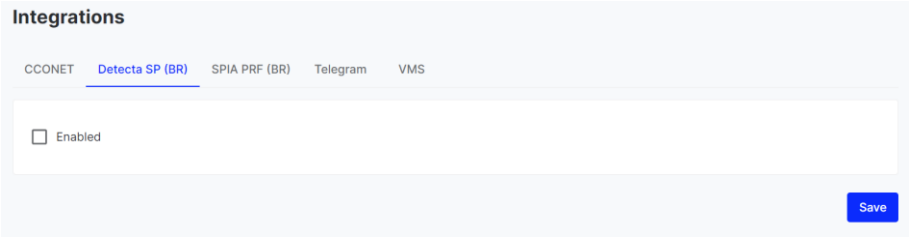


Figure 65 - Configuration screen for integration with Detecta SP

When the integration is enabled, it is necessary to specify which devices will receive the integration data by accessing *System > Cameras.* When locating the device in the list that will be integrated with Detecta SP, *clicking Edit* opens the window with the device registration information:

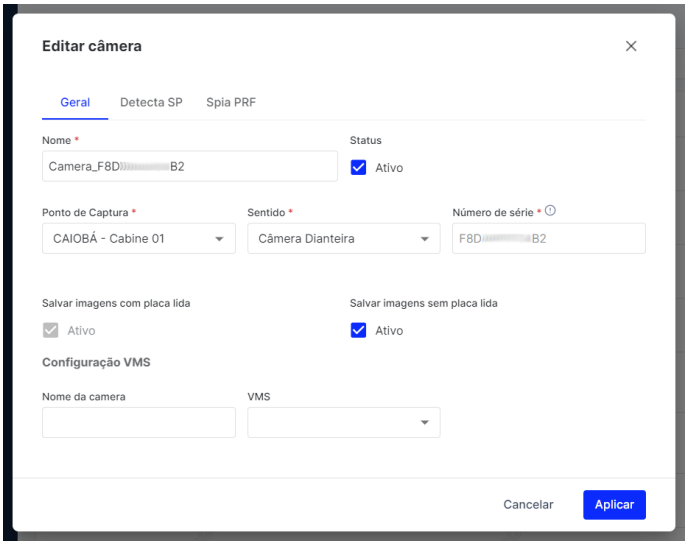


Figure 66 - Initial configuration screen for device integration with Detecta SP

In the *Detecta-SP* tab, the device ID provided with PM-SP must be entered:

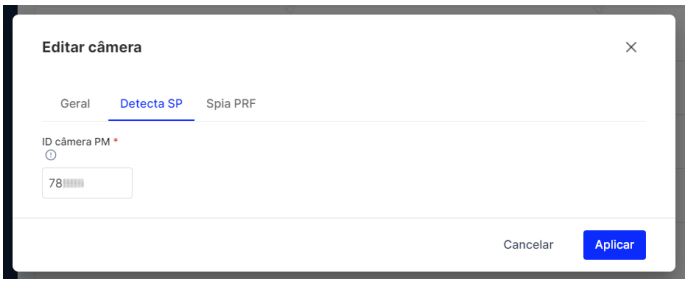


Figure 67 - Configuration screen for device integration with Detecta SP

Integrate with SPIA PRF

To integrate the system with *SPIA PRF*, it is necessary to select *Enabled*, fill in the *Name*, *Key*, and *Access Token* data, and *Save*. This integration occurs on a per-user basis, meaning each account has its agreement with PRF and its access token to the PRF system. Therefore, it is only possible to send images and records to SPIA using the device identifier, as registered with PRF.

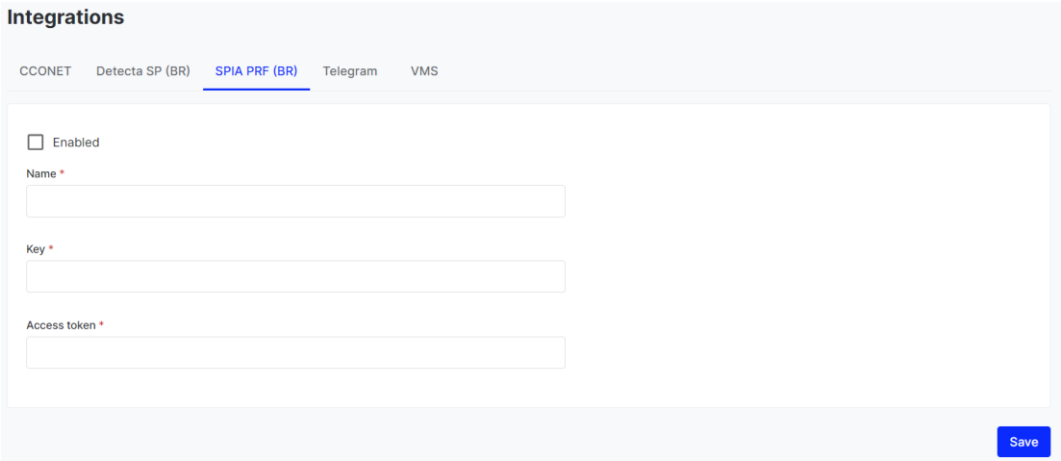
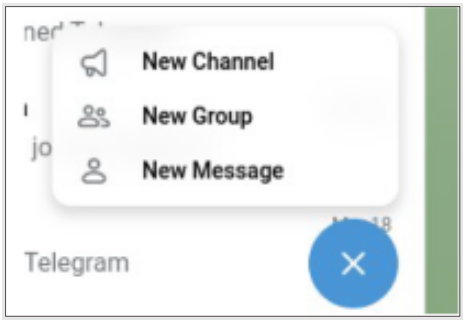


Figure 68 - Configuration screen for integration with SPIA PRF

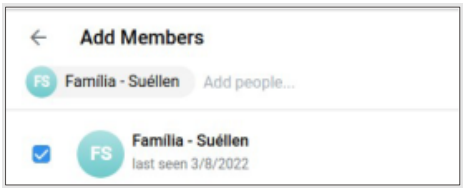
Integrate with Telegram

The integration setup with the Telegram application must be performed in both pieces of software. Firstly, in the Telegram app on a mobile device:

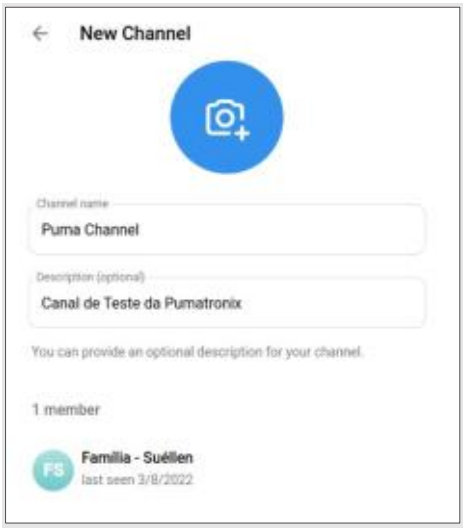
1) Create a new channel (*New Channel)*:



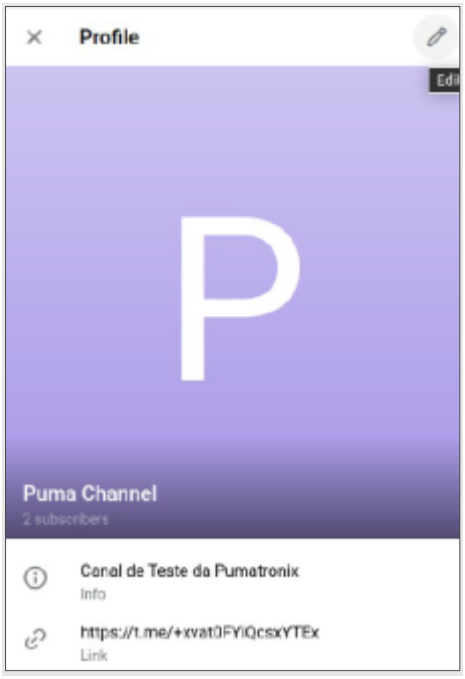
2) Add the contacts that will participate in this channel:



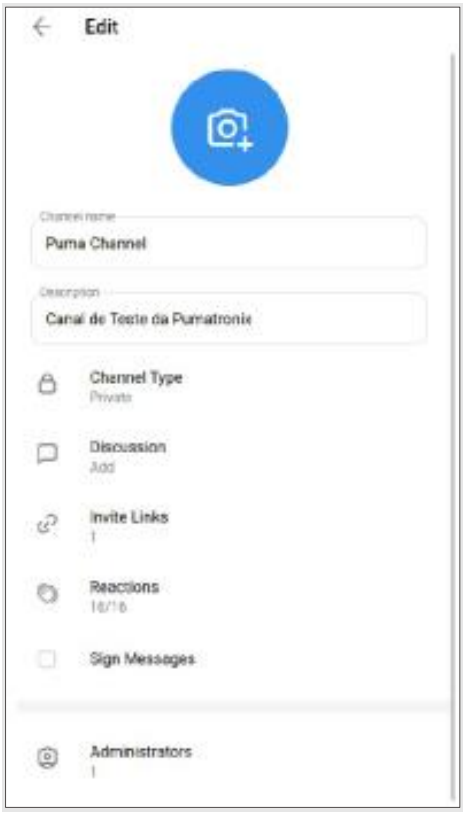
3) Give the channel a name and a brief description:



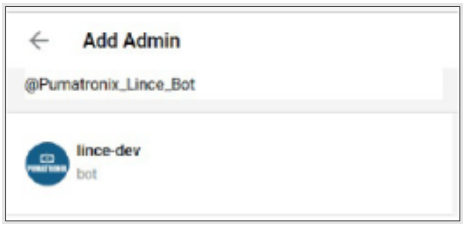
4) Once the channel is created, add the Pumatronix bot by clicking on the channel edit icon:



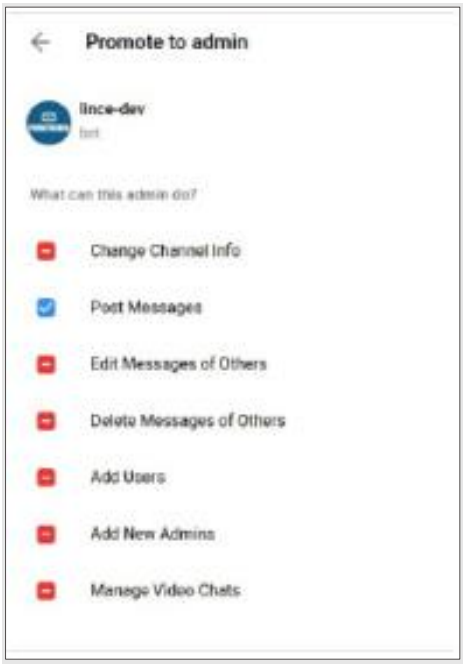
5) Click on *Administrators* and then on *Add Admin*:



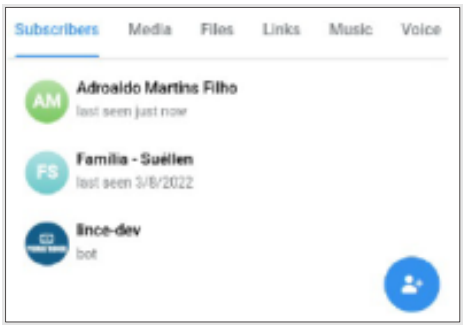
6) In the search bar, search for **@Pumatronix_Lince_Bot.** For now, the name will appear as ***lince-dev***:



7) Then, the permissions of the bot in the channel should be configured and click on **OK**;



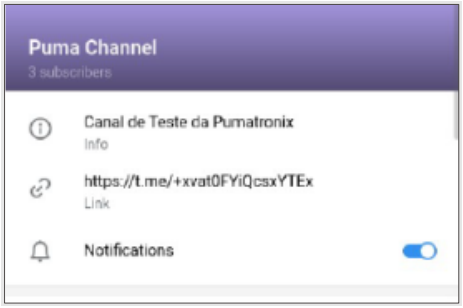
8) Once the bot is added, it will be shown in the list of *Subscribers*:



With the channel created, the bot will be able to send messages to the users. Then, the following steps should be executed:

1) Add to your contacts list the bot named ***IDBot - @username_to_id_bot.*** It will be responsible for giving us the chat_id that will be used within Lince.

2) Access the newly created channel and copy the access link to the channel.



3) Start a conversation with the IDBot bot by sending the following commands:
    a. /start
    b. https://t.me/+xvat0FYiQcsxYTEx (the link copied in the previous step).
4) The Bot will return an ID starting with the value *-100*. To integrate the system, the bot, and the users of the channel, this value must be entered in *the Chat ID* field, located in the *Integrations > Telegram* area".

Figure 69 - Chat with IDBot on Telegram

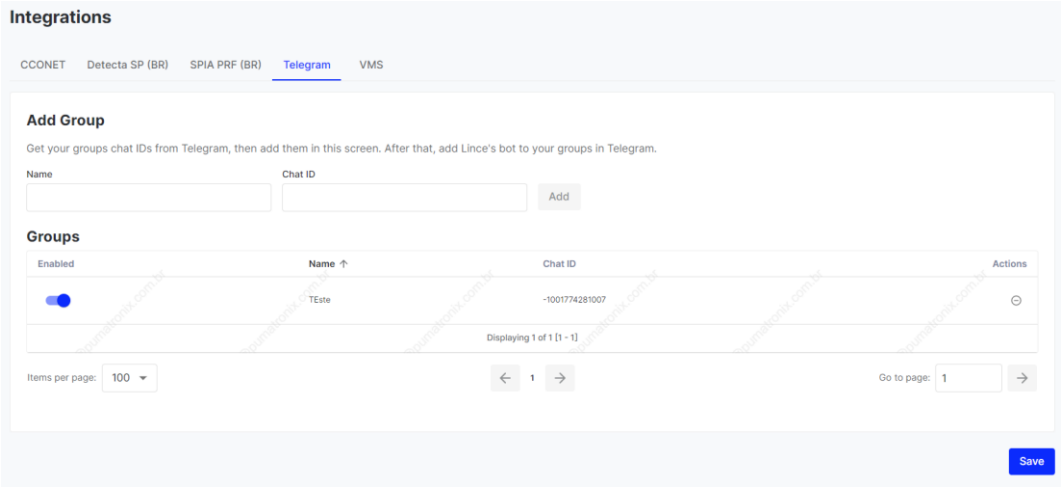


Figure 70 - Configuration screen for integration with Telegram

Integrate with VMS

In the *VMS* tab, it is possible to enable integration of the Lince system with a video recording system (VMS), in which the image from the CCTV device is recorded by the VMS. At the moment a license plate is captured, the recording is made considering seconds before and after the passage, providing a view of the passage context.

When accessing the *VMS* tab, it is possible to register new integrations, and the existing ones are displayed, with the options to edit or remove:

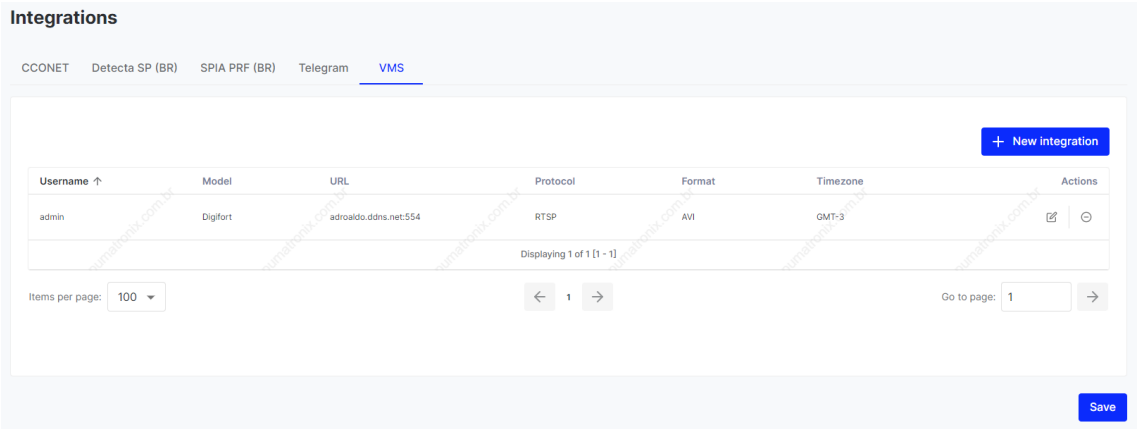


Figure 71 - Configuration screen for integration with VMS

The registration of a new VMS video integration in *+New integration* opens the window to fill in the following fields:

- URL
- User
- Password
- Model
- Protocol: select between the options RTSP and RTSPS;
- Format: select between AVI and MP4;
- Time Zone: select the corresponding time zone.

After filling in the information, click the *Apply* button to save the information.

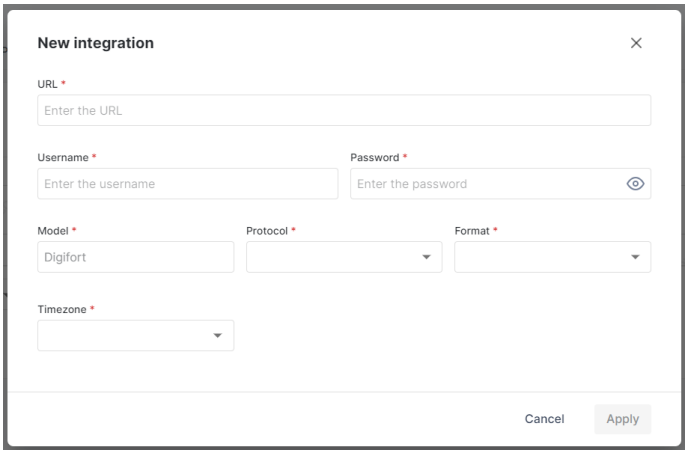


Figure 72 - Initial screen for registering a new VMS integration

Information Protection

Lince allows the inclusion of an extra factor *of Information Protection*, which is the application of a watermark on documents containing confidential information, preventing the leakage of confidential data. Thus, when the application of a watermark is selected, the document generated by the system records the information of the user's email generating the document or the client's CNPJ + the user's email. These data are displayed in the header, footer, and diagonally in the body of the generated document.

By selecting the client to be used in the watermark and selecting the option to *Apply a watermark to documents containing confidential information.* The text to be displayed in the watermark can be *Email* or *CNPJ + Email*. After selecting the information, click on *Save* to apply.

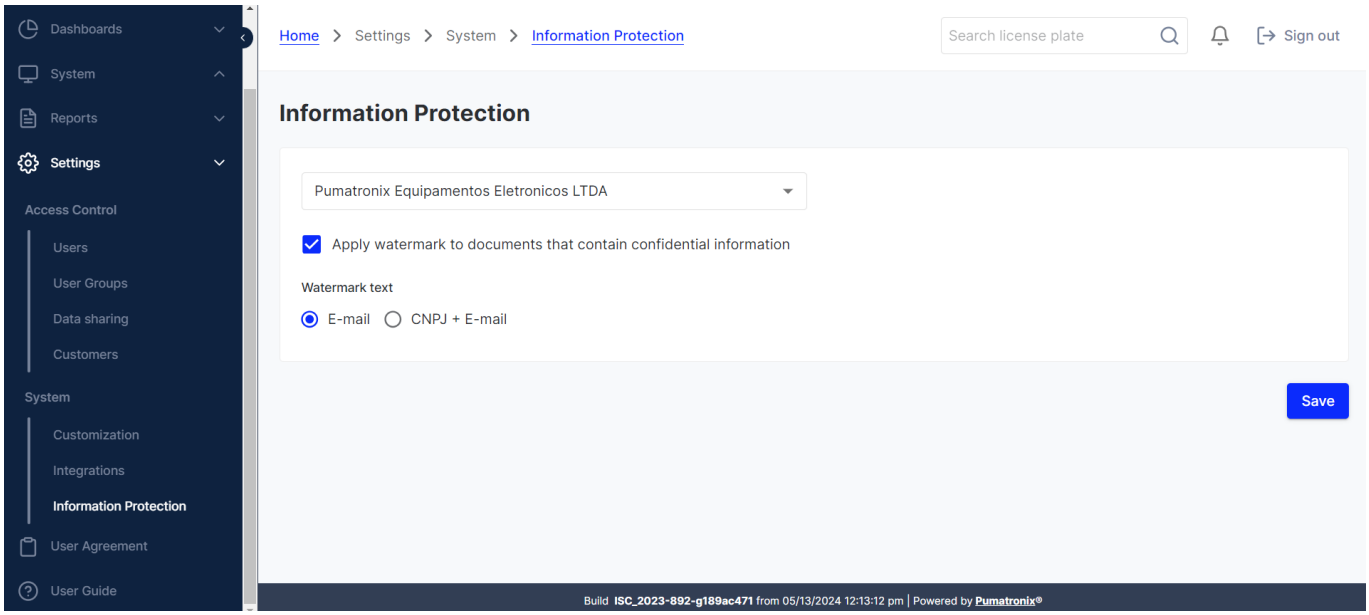


Figure 73 - Example of the initial screen in Settings > System > Information Protection

6. Terms of Use

In this menu, the file of *the Lince USAGE AGREEMENT is* available in.*PDF format.* This document contains the terms and rules for the user of the system to use the service being offered.

If you have any questions about using Lince, please contact Pumatronix technical support at support@pumatronix.com or WhatsApp (41) 99203-8327.

7. User Guide

In this menu, the *User Guide* file is available*. PDF format.* This is the latest published version of the Integration Manual.

8. Lince API Documentation

Lince has a Rest API for integration with other applications, and the documentation of this API uses the *open-source* Swagger application*.* Since the available operations may vary depending on the application's version, the documentation must be accessed through the Lince system itself: https://swagger.lince.app.br.


PUMATRONIX
www.pumatronix.com