InprOTech

Smart security for your industry

User Manual

InprOTech Guardian

Date: 07/2025

Doc Reference: IN-User Manual InprOTech Guardian

Version: 0.17

INDEX

1 Introduction

InprOTech Guardian is an asset discovery and anomaly monitoring and detection tool capable of identifying cybersecurity threats in industrial environments. It analyses network traffic, identifies assets on the network, generates comprehensive reports, and raises alerts using static rules, IDS signatures and artificial intelligence to mitigate threats in the industrial network.

The InprOTech Guardian interface is highly interactive, easy to understand and manageable. In addition, it is available in both English and Spanish.

This interface is developed using the Angular framework following best practices and security methodologies to ensure secure information navigation.

Through the InprOTech Guardian application the user will have a complete view and knowledge of the following aspects:

- **Continuous Dashboard**: self-refreshing dashboard to monitor the main aspects of assets, threats and 24x7 reporting in an operations centre.
- **Asset summary**: Visualization of the number of devices connected to the network, classified according to the PURDUE model.
- **Quick access**: To alerts, vulnerabilities, algorithms, and active rules.
- **Network traffic graph**: Graph of the traffic generated, both sent and received, in the last 24 hours and compared to the same period 7 days before.
- **Alerts graph**: Graph of the alerts received in the last 7 days, differentiated by colour according to their severity level and the trend they follow over time.
- **Network mapping**: Visualization of all network devices, how they are connected and how the organization's network is structured. It will also visualize all those devices connected and that have not been considered legitimate.
- **Device manager**: List of assets, wired or wireless, for identification and management. Including the identification and labelling of devices, or the inclusion of devices in the blacklist according to their criticality level Additionally, the user can define customizable fields to classify and filter the network devices, with a virtual inventory of the created fields that can be organized, filtered, and exported.
- **Alert manager**: List of events and alerts in the organization's OT network, classified according to their level of severity. They are color-coded and detailed with dynamic information. They will be classified according to their status (resolved and silenced), and are generated based on heuristics, IDS signatures and artificial intelligence/machine learning.
- **Integration with third party systems (SIEM)**: Guardian provides the ability to send the generated active alerts to a third-party system such as a SIEM (Security Information and Event Management), for ingest and correlation with other log sources. To do so, it makes use of the rsyslog protocol.
- **Vulnerability manager**: Possibility to perform vulnerability scans upon customer request and only to selected devices (under development).
- **Public IP reputation:** Connections to public IP addresses will be analyzed to check the reputation of that address. In case it is determined that it is an IP listed as malicious, the corresponding alert will be conveniently highlighted in the panel.
- **Blocking bad traffic:** In case of connections to public IP addresses considered malicious, it is possible to establish strategies to communicate with the system's

firewall and include that address in a list of filtered IPs. Among these strategies we have an informative mode, where we only report the situation, a manual mode, where the user themself blocks or unblocks the connections, and an automatic mode, where the communication with the firewall is done without human intervention (manual and automatic policies under development).

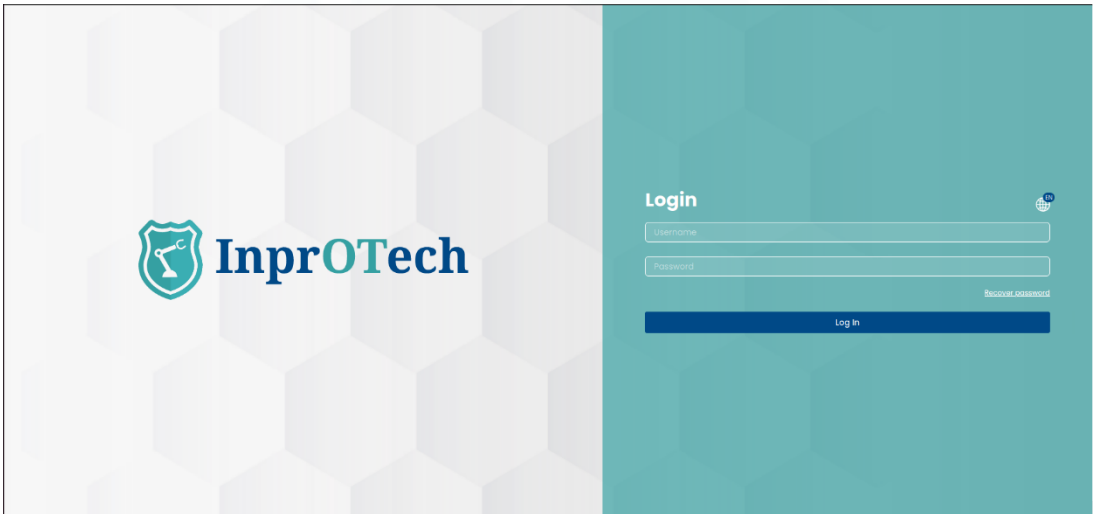
- **Communications list**: List with all the communications that have been made between OT devices in the organization's network, and information about them.
- **Report generation**: Compilation of information about the network, devices, indicators, etc., for future analysis and verification at both technical and business level.

It is important to note that in addition to the use of the application itself, the service involves a series of preparations for onboarding, which include adequate data collection, deployment, installation, and fine-tuning of the solution to get the most out of it, based on actions such as those indicated in the following section.

2 First steps

2.1 Web console access

First, access the browser and enter the address http://[IP]:9000, where IP is the address assigned to the management interface.



InprOTech Guardian Log in screen

At any time, you can select the language of your choice in the world map icon (English or Spanish).

The user must authenticate by entering the username and password assigned to him/her. In case of having the second authentication factor activated, he/she must additionally enter the single-use token received via email in his/her user email account of the service.

The user can be:

- **Admin Inprotech**: Will have access to all the information presented by the application and will be able to make the configurations he/she deems appropriate for algorithms, factory Ids, production modes, etc.

- **Factory Admin**: Access like the previous case, except for the specific configuration part mentioned above.

- **Guardian Operator**: Exclusive reading permissions user. He/she will have access to download manuals, reports and export search results and certain lists (Devices, Alerts, Vulnerabilities, Communications, Traffic Analysis, etc.).

In case the user has forgotten or blocked his/her password, he/she will have the option to recover it by clicking on the "I forgot my password" option.

Password recovery screen

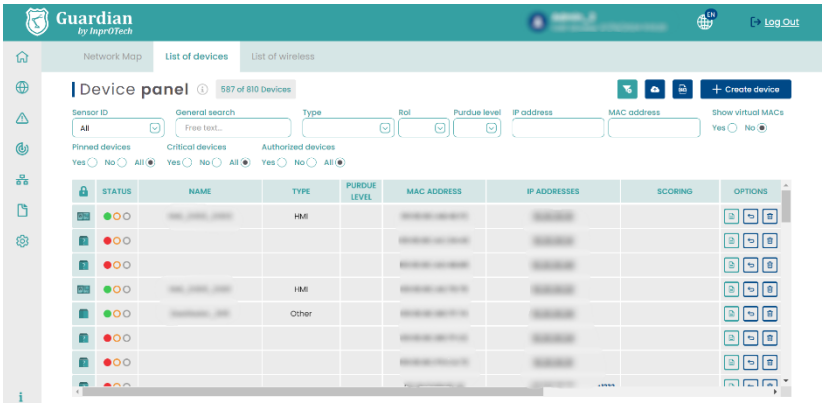
When entering the e-mail address, if valid, a link will be sent to the e-mail address to reset the access password by means of a one-time use token.

**This functionality, as well as others necessary for Guardian software updates or remote access, require connectivity between the system and certain InprOTech or internet services, so the list of rules to be applied in the firewall will be provided.*

2.2 Device list organization

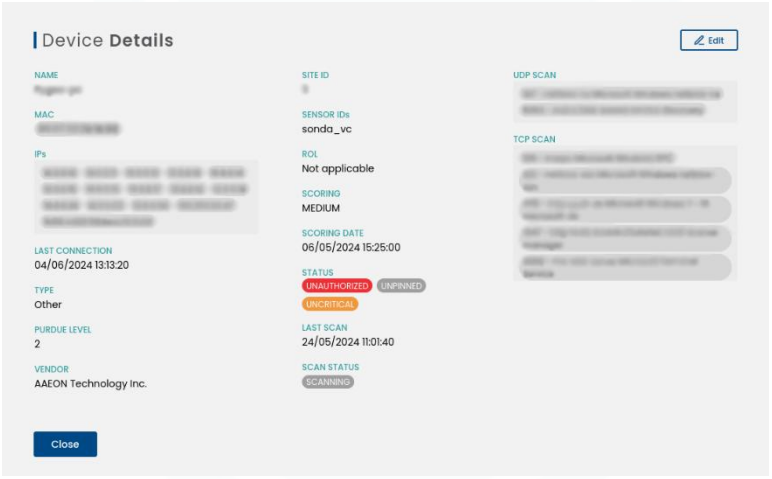
The list of devices must be organized by declaring the name of each device, as well as its PURDUE level and its status (See Annex I). By means of this declaration, the user will find it easier to identify each device in the different windows of the application, and thus be able to carry out operations on each device with greater agility, as well as to extract more value from the service.

The user must go to the list of devices by clicking on the icon  on the left side of the screen and selecting the "Device list" tab.



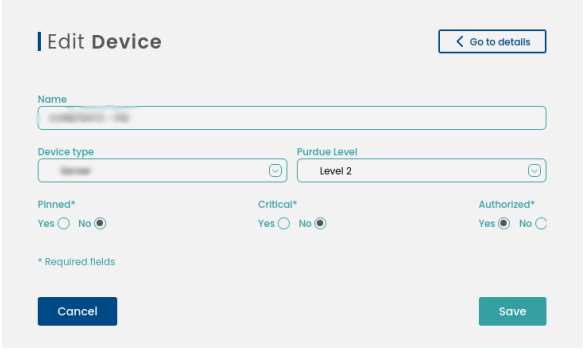
Device list screen

To be able to modify a device, we will have to click on the button  and the next tab will open.



Device details pop-up

Then click on the button  to modify the selected device.



Edit devices screen.

And manually fill in the device name, PURDUE level to which the device belongs and select its status indicating whether the device is fixed, critical and/or authorized (see definitions in Annex I).

To make massive changes in a more agile way, this configuration can be made directly in the list of assets by clicking on the padlock icon and accepting in the confirmation pop-up.

Once this has been done, the "Save" button is clicked to make the changes effective in the system.

2.3 Rules configuration

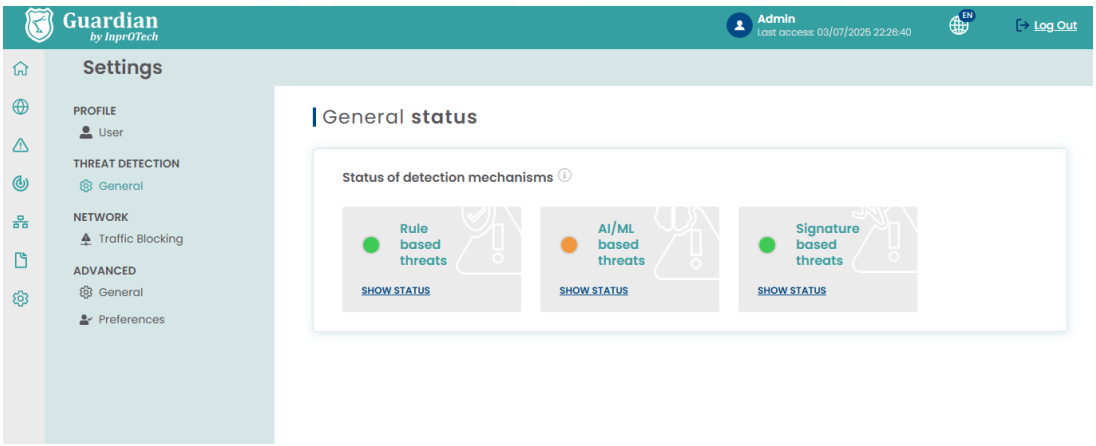
The Guardian system performs threat detection based on multiple behavioural criteria, such as:

- Threats based on predefined parameterizable rules
- Threats based on IDS signatures
- Threats based on AI/ML algorithms
- Honeypot threats

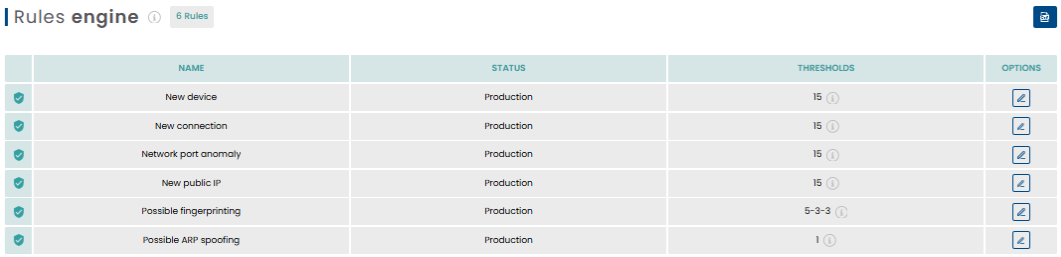
The user must configure which rules he wants to be operational for the analysis of his organization's network, as well as the time ranges to bypass each of the alarms if he deems it appropriate. This would be done in mutual agreement with InprOTech in the onboarding; in principle, the user will only see the rules and thresholds but will not be able to edit them.

The time range to bypass a rule means that we can set a threshold or time in which the established rules will not generate an alert in an identical scenario, and thus avoid unnecessary warnings and alerts of which we are already aware.

Additionally, other parameters can be configured. These will be detailed later. To configure these time ranges, click on the left menu button on the screen and click on Threat Detection > General > Rule-based threats, VIEW STATUS.



Status screen detection mechanism



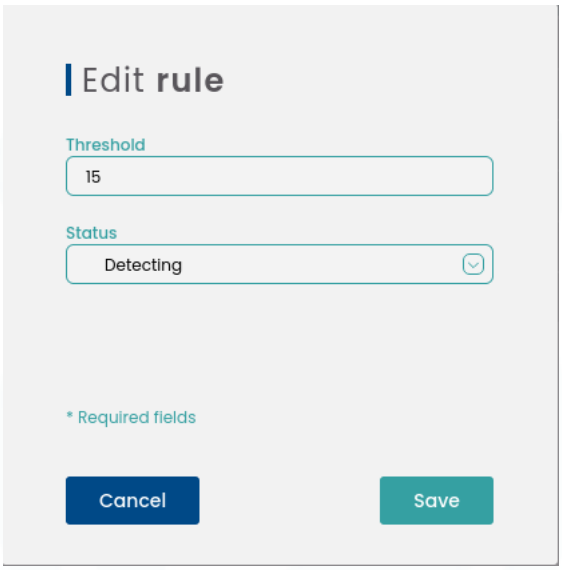
Rules engine screen

In the threshold's column, we can quickly see the thresholds configured for each rule.

THRESHOLDS	OPTIONS
15	
15	
15	
15	
5-3-3	
1	

Umbral screen

In the actions column we can edit these parameters.



Rules edit screen.

In addition, this section will include, once available, the configuration of the messaging associated with notifications of alerts that you wish to receive, and reports.

2.4 Settings

Basic settings for user profile data, security settings, and alert notification preferences can be found in the Settings section of the Quick Guide. It is recommended to review and adapt them to the environment needs.

2.5 Reports configuration

Now, reports are generated automatically on a weekly basis.

2.6 Continuous dashboard (optional)

If you are interested in being able to permanently consult the status of Guardian and the main associated indicators (unauthorized devices, network traffic, alerts, etc.), you can have the main Guardian dashboard on a monitor in your operations room with auto-refresh every 5 minutes.

To do so, contact your Guardian Support and request the creation of a Monitoring user.

2.7 Alerts exportation (optional)

If the customer wishes, he can contact his Guardian Support to enable the automatic sending of the generated alerts to a syslog server of a SIEM or similar, for their ingestion and correlation* with other log sources.

The only thing you need to provide is the IP and port to which you want the messages to be sent.

* For this purpose, it is important to note that all dates returned by the web application are shown in UTC time.

2.8 Active device scanner (optional)

Guardian Support can be contacted to enable the active device query engine to obtain additional properties of the nodes (firmware version, open ports and services running on them, among others).

See the Devices Scanner Section within Application Management for more details.

2.9 Analysis of Wireless devices (optional)

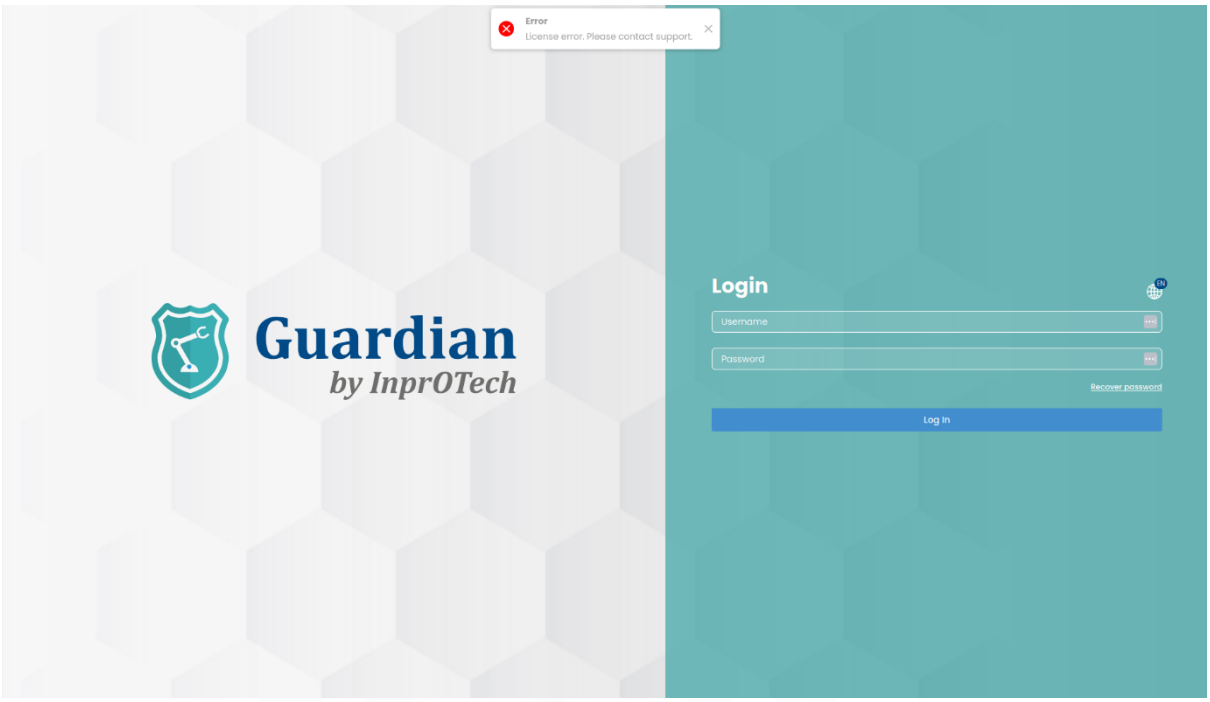
If traffic collectors have the appropriate hardware for it, Guardian Support can be contacted to enable scanning of Wireless devices in the vicinity.

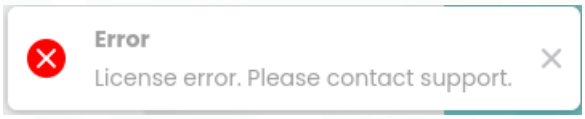
Refer to the Wireless Device List section within Application Management for more details.

2.10 Licences

This will allow to provide the Guardian Service on a temporary basis only, so that it can be provided for testing purposes limiting the usage time window.

If you see the message **"License error. Contact support."**, means that the license files are missing or the license has expired.





2.11 Access control and roles

This feature allows control of user access and actions performed in the system. The implementation of this system provides an additional layer of security and privacy in the handling of information and system resources.

This role and access control system has the following features:

- **Predefined roles and permissions:** different predefined roles and permissions can be established in the system, which will be granted to determine their levels of access and control in the system.
- **Assignment of permissions to users and groups:** the system allows assigning permissions to users and groups according to their roles and responsibilities in the organisation.
- **User group management:** users' groups should be established to allow the assignment of permissions to multiple users at the same time, which will facilitate the management of permissions.
- **Resources access control:** the system will allow control of access to different Guardian resources by assigning specific permissions.

The roles to be implemented will be as follows:

- **INPROTECH:** Full access is granted to configuration, service operations, logs, etc., including the ability to transition between training and production environments, and modify AI algorithm sets as needed.

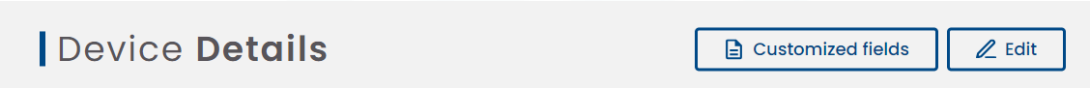
- **ADMIN:** Factory's privileged user mode, changes can be made to the visible data on the frontend, such as device data, and alerts can be marked as resolved or muted.
- **OPERATOR:** standard factory user mode, permissions are more restricted. Users can only view data and download reports or CSVs.

2.12 Customized Fields

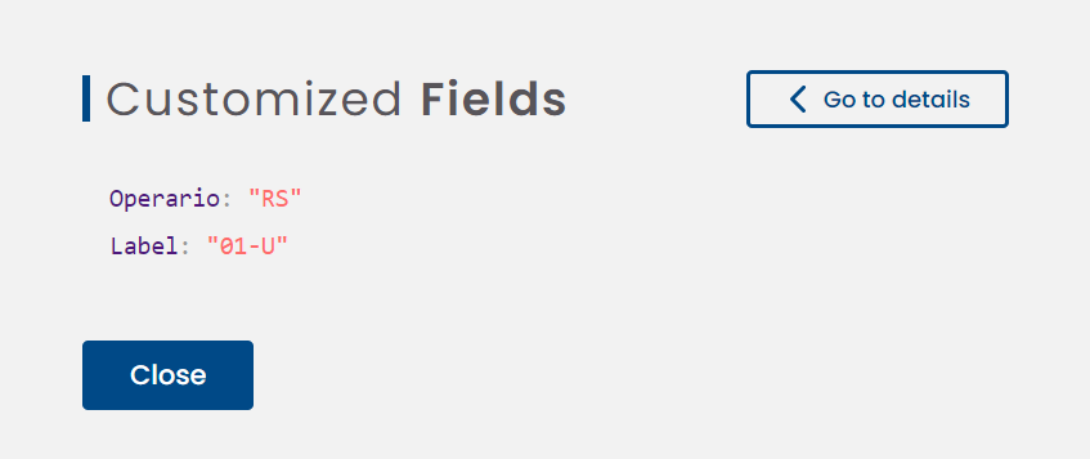
If the user believes any new fields can be added to the device list to allow for their better categorization, they can define them on a key-value format using a ".csv" file.

Just add a new file from the button on the device panel, including the devices we want in the rows along with the new customizable fields in any of the formats explained in section 4.2.2.1.

The user can check the loaded fields from the device panel by either clicking on the link 'Show fields' on the devices with any fields configured or on 'Device Details' and then continuing by clicking the 'Customized fields' button.

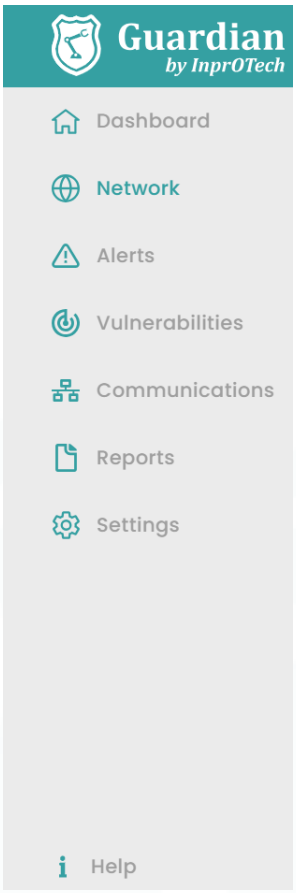


This action will open a new modal that allows the user to view them.



3 Quick Guide

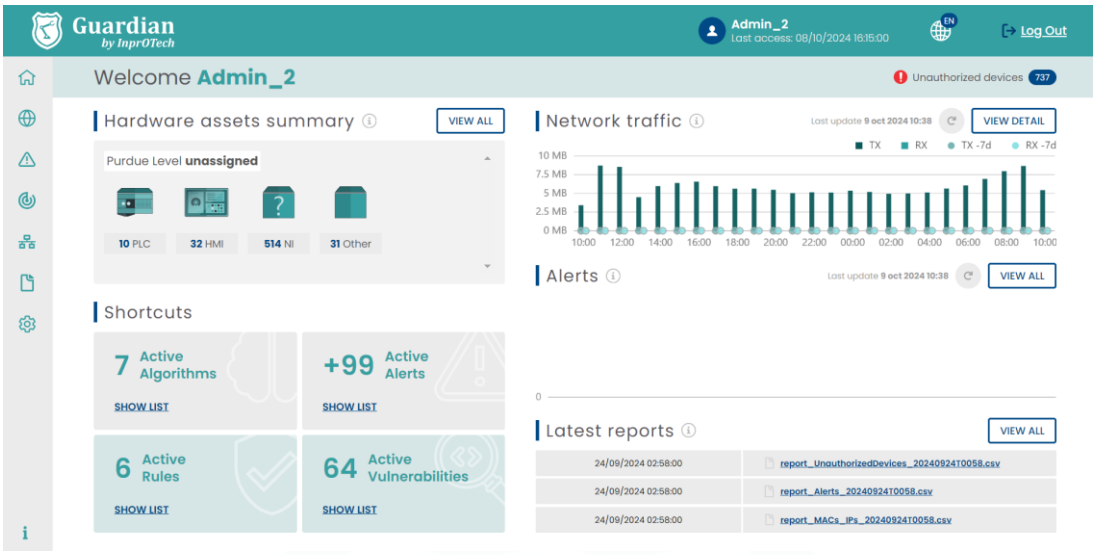
3.1 Menu



Access window detail

- 1: Home: Main Dashboard
- 2: Network: Network map and device list
- 3: Alerts: Alerts list
- 4: Vulnerabilities: List of vulnerabilities
- 5: Traffic Sessions: List of inter-device communications
- 6: Reports: List of automatic reports
- 7: Settings: Parameters setting window
- 8: Help documentation

3.2 Main Dashboard



Main dashboard view

Top bar:

Type of session and date of previous access

Change application language.

Log out from logged in session.

Unauthorized devices counter.

Top left widget:

Number of assets in the organization sorted by Purdue model.

Top right widget:

Graphical representation of network traffic sent and received in bits/sec the last 24 hours, and comparison with respect to the same magnitude just 7 days earlier.

Lower left widget:

Shortcuts to listings

Active vulnerabilities (under construction)

Bottom right widgets:

Graphical representation of number of alerts according to their severity.

Access to list of generated reports

3.3 Network Map

The network map presents two topology views: classic network, or by PURDUE levels.

In the first case:

Network map window in classic view.

At the top, there is a tab to select the network map view, the date of the last update of the graphical representation of the topology, as well as a button to make the filters entered effective.

The next row shows the possible filters to view the devices of interest on the screen.

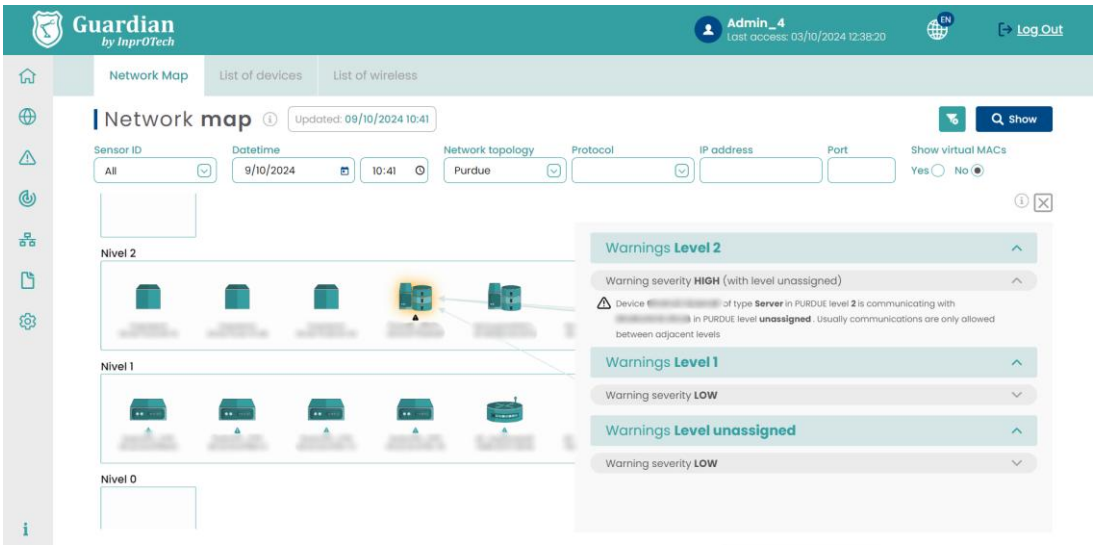
Below, we already have the map and topology of the organization's network devices.

Note that:

- By hovering with the mouse, you can see the properties of a node or a link.

- By clicking on them, you can go to the detail view and edit device properties, or to the filtered communications section for that link source, respectively.

In the PURDUE view of the topology, the communications compliance is analysed based on the ISA/IEC 62443 standard. The warnings are classified as **high severity** (communications type, indicating the existence of communications between non-adjacent levels), **medium severity** (PURDUE level assignment to device types that seem questionable) or **low severity** (no level assignment and/or recommendation of manual review for certain device types).



Network map in PURDUE view.

Note that in the graphical version (left side of the window):

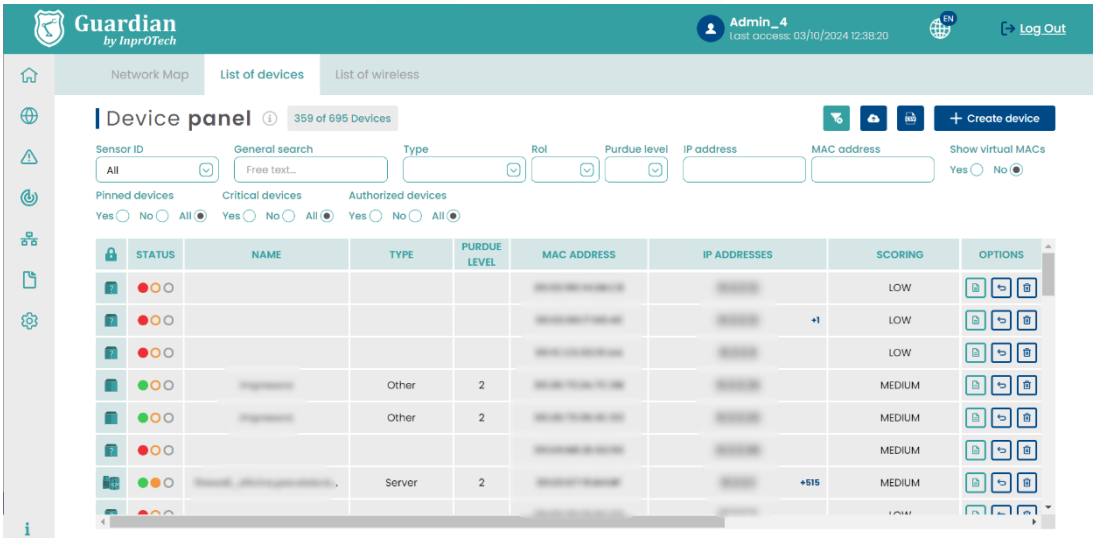
- Only communications between distinct levels are shown, not those between devices of the same level.

- It is indicated with triangular icons under the image of the device, if it is affected by any regulatory compliance warning. The colours are red, orange and teal, and represent high, medium, and low severity warnings, respectively.

- The devices can be clicked to filter the warnings on the right-hand side that apply to the node in question. If the filter is unchecked, all the detected devices are displayed, in descending order of levels and severity.

The rest of the filtering capabilities are the same as in the classic view, and on the right side of the window, as mentioned above, the global warnings or those associated with a selected device are listed.

3.4 Device List



Device list window

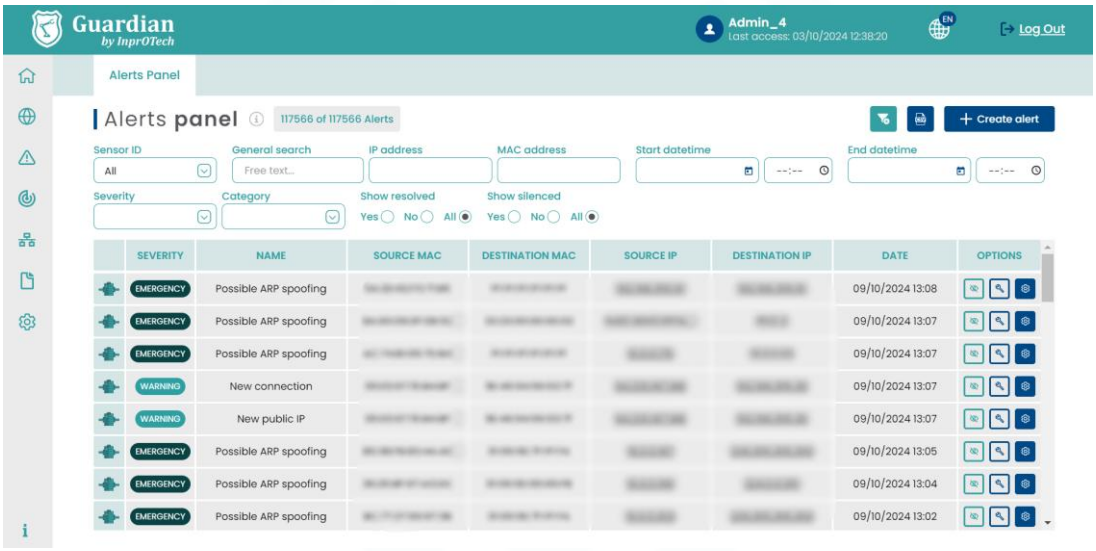
In the tab to select the view of the list of devices registered in the network, the number of devices with the current filter applied versus the total number of devices in the database is displayed next to the panel title. On the right side, the button panel for deleting previously applied filters, exporting the list of devices in CSV format, and manually registering a device in the application.

The next row includes the possible filters applicable to keep the devices of interest.

The list of assets itself with information about them, and buttons to perform certain actions (view details, edit them, delete them, or access alerts, communications or vulnerabilities present, the latter pending development). It is possible to sort the devices alphabetically directly or inversely by clicking on any of the columns.

The third tab contains the inventory of wireless devices detected in the vicinity of the traffic collectors (if compatible hardware is available and the functionality is enabled by Guardian support staff).

3.5 Alerts panel.



Alerts list explanatory window.

Next to the section title, the number of alerts in the organization's network (filtered vs. total) is displayed. On the right side, there is a button panel for deleting the set filters, exporting the list of alerts in CSV format, or manually creating an alert in the application.

The next row includes the possible filters to view the alerts of interest on the screen. Note that the general search field is of type CONTAINS and allows to perform searches on the internal notes field of the alert, visible in Details.

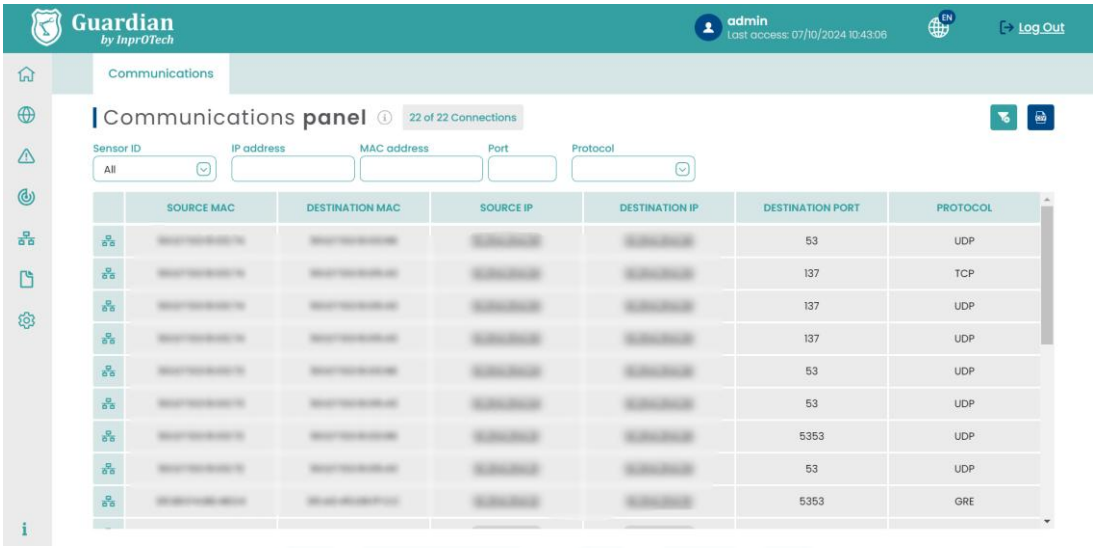
Finally, we have the list of alerts with associated information and buttons to perform actions on them (status updates*, access to detail and addition of notes).

As you can see in the image, if a device has a name assigned to it, next to the MAC we can see an exclamation mark which, if we place the cursor over it, will show us the name assigned to that MAC address.

*To check the status change options, see definitions in Annex I.

3.6 Communications List

Communications, understood as a grouping of connections between MAC, IP, and source port, and the same at the destination. Unbundled if there is a change of protocol.



Communications list window.

In this section, the number of devices with the current filter applied is shown next to the title, compared to the total number of devices in the database. On the right side, the buttons to remove the set filters and to export the list of connections in CSV format, respectively.

In the next row, there are the possible filters to view the connections of interest on the screen.

Finally, the list of connections with information about them. It is possible to sort the communications alphabetically, either directly or inversely, by clicking on any of the columns.

3.7 Reports

This section will allow downloading reports of several types, automatically generated by the system. As of today, Guardian generates weekly reports on Monday mornings, with downloadable files in CSV format, with the following information:

- Unauthorized connected devices:
    - Name: Name of the device
    - MAC of the device
    - Vendor: Manufacturer
    - Role: Role
    - Discovery date: Date of discovery
    - Ips

- Purdue level
- Fixed (Y/N)
- Critical (Y/N)
- Device type
- Score and score timestamp.
- Scan status and last scan.
- Vulnerability risk number
- Vulnerability risk label
- OS
- Blocked (Allowed/Not allowed).
- Customized field

- Last detected alerts:
  - ID
  - Title
  - Category
  - Severity
  - Silenced
  - Resolved
  - Value
  - Source IP
  - Source ID
  - Destination IP
  - Destination ID
  - Protocol
  - Creation date
  - Location (City / Continent / Country / Latitude /Longitude…)
  - Hostname
  - IP
  - Source device (name / type)
  - Destiny device (name / type)
  - Creator

- MAC-IP associations:
  - MAC
  - Associated IP
  - Vendor: Manufacturer
  - Public IP: Whether it is public or not.
  - Discovery date: Date and time of discovery

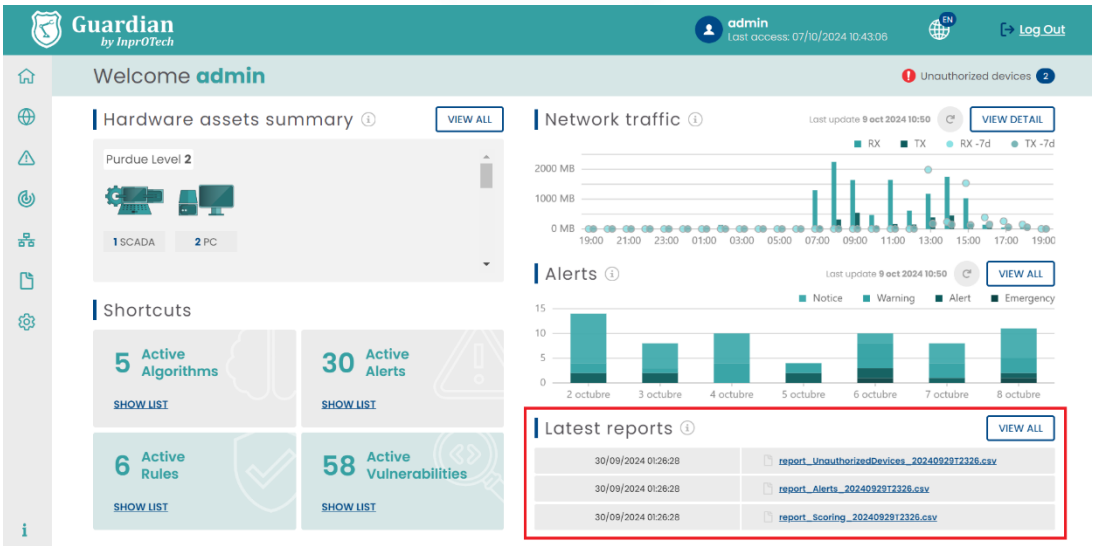
- Public Ips (External IPs connected):
  - IP (source/destination)
  - MAC (source/destination)
  - Discovery date

- Risk Score Report (scoring)
  - Name
  - MAC
  - Manufacturer
  - Individual score

    - Date of scoring
    - Overall factory score
    - Overall cloud score
- Wireless devices
    - IP
    - MAC
    - Connection type
    - Authorized (Y/N)
    - Device type
    - Channel
    - Signal power
    - AP Mode
    - Frequency Band
- Vulnerabilities
    - MAC
    - IP
    - CVE
    - Status
    - Source
    - Discovery Date
    - Last Seen
    - Port
    - CPE
    - Criticity
    - Description
    - Timestamp published.
    - CWE
    - URL

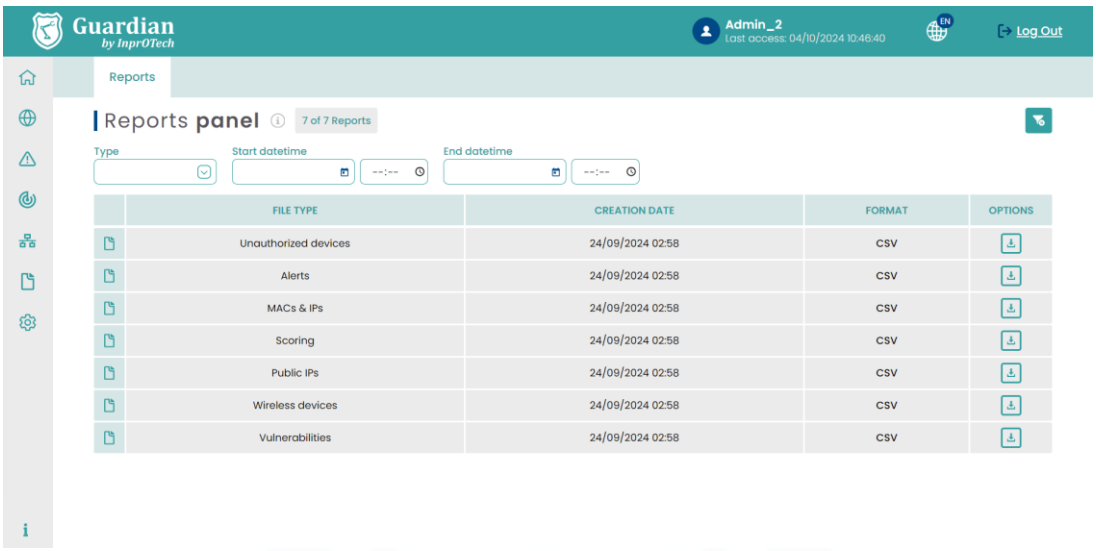
If the device has the label Name reported, it will replace the MAC field in the alert's reports. On the other hand, in manual downloads of user searches from the alerts panel or the device list, the "Latest reports" section will display both fields independently.

The user will be able to download the latest generated reports from the main Dashboard shortcut.



Latest reports on main Dashboard

Additionally, Guardian has its own section dedicated to Reports, where you can use the search engine to filter and download the report of interest:



Report list view.

Next to the title, the total reports generated are shown, and to the right the filter reset button.

In the next row, we have the different search filters.

Finally, there is the grid with the reports available CSV format for downloading.

3.8 Parameter settings window

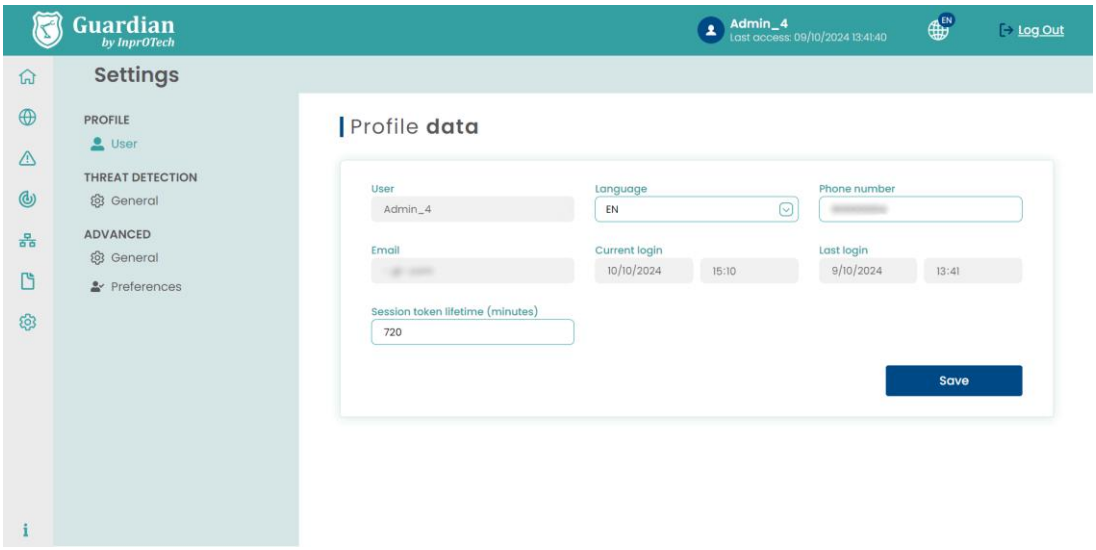
In this section we can adjust our profile or the service, modify some parameters related to threat detection, or different configurations of alerts, threats, and user management.

The most relevant aspects at user level are summarized below.

3.8.1 User profile

This section displays basic information such as username, associated email, date and time of last and current connection, language preference (EN/ES), and contact telephone number. The last two are editable by the user.

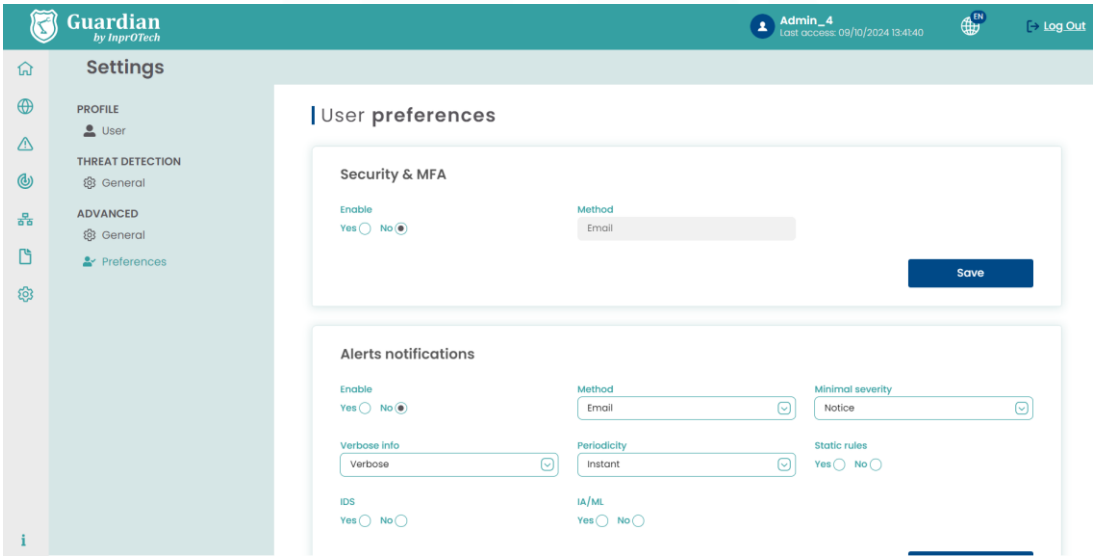
The user can reach it from  "Settings" on the left side Menu.



User profile view

3.8.2 Security

In Advanced > Preferences, in the 'Security & MFA' section, we can indicate whether we want to activate the second authentication factor as an additional (recommended) security mechanism to prevent identity theft. In this case, after identification with username and password, we will be invited to enter a single-use token that we will have received (initially by email).



Security & MFA view

Remember that as access control method, a role-based mechanism has been implemented, by means of which there are groups of permissions associated to three user levels:

- InprOTech Administrator
- Plant Administrator
- Plant operator

The assignment of roles to users cannot be managed directly by your organization but is defined with InprOTech at the time of deployment of the solution. Contact us for further information.

3.8.3 Alerts notification

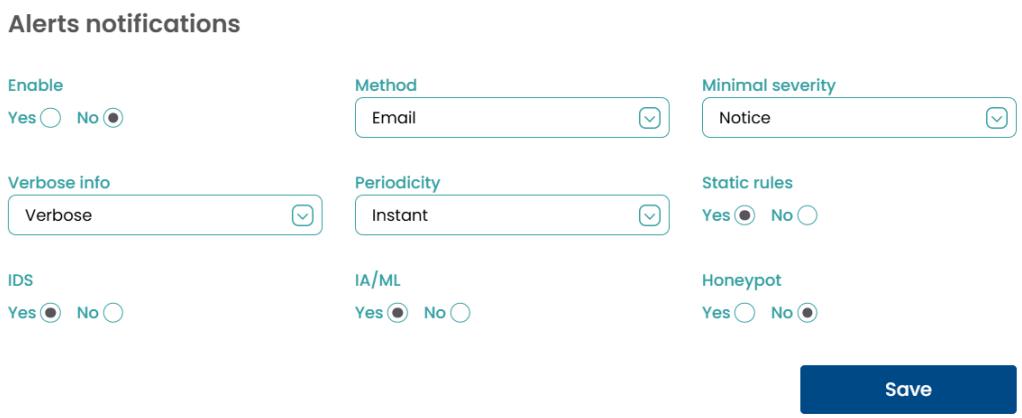
In case it is considered appropriate, initiative-taking alerts can be configured to generate alerts in the system. The alerts and warnings are generated based on the detection of anomalies according to the different strategies implemented in Guardian (heuristics, IA/ML, IDS, Honeypot, manuals...).

This allows Guardian to warn of potential incidents, instead of having to periodically go to the web interface to check if events have been generated.

The user will therefore be able to:

- Decide if he/she wants to receive security alert notifications.
- If so, from what severity threshold they will be sent to the user.
- What type of alerts (heuristics, IA/ML, IDS, Honeypot, all...)
- In what format
    - Individual: one notification per alert
    - Grouped: a daily notification with the summary of all alerts, selectable from Monday to Friday or from Monday to Sunday.

- If individual, whether summary or verbose format is desired.



Alerts notification view

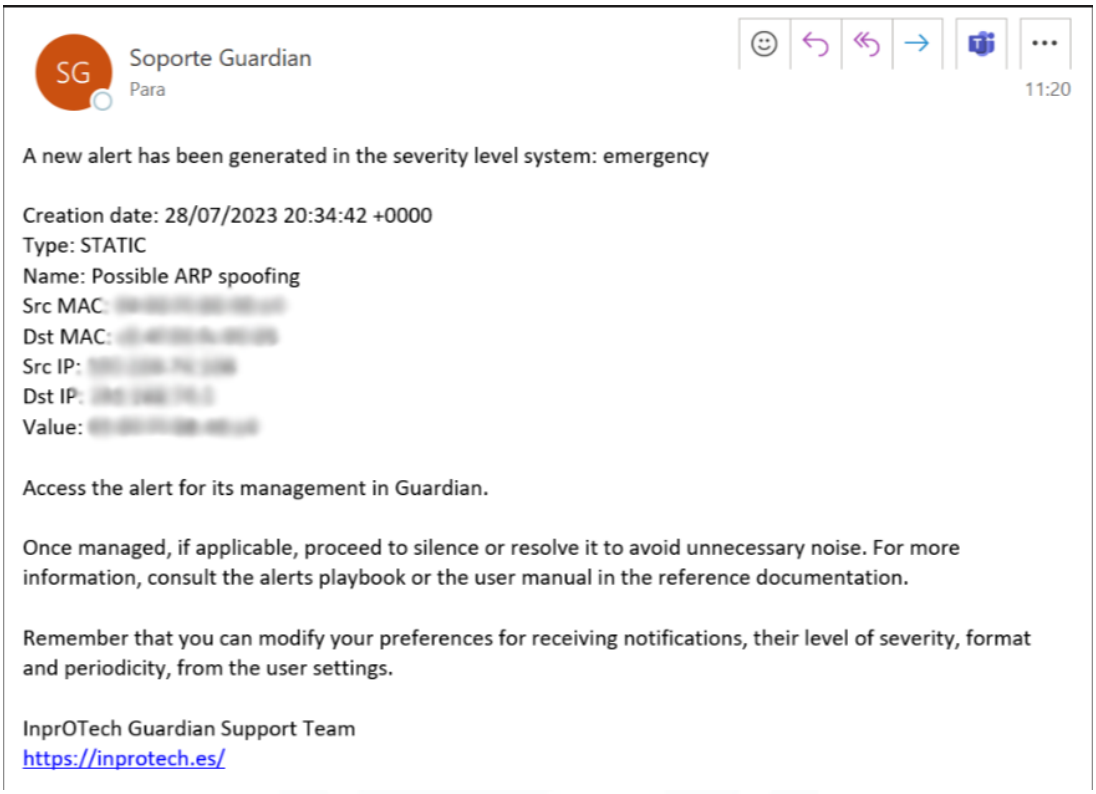
For the time being, notifications will be sent via email to the user's account.

Important:

- Alert notification must be enabled in the backend to allow the user to enable proactive sending.

- In case that with the established conditions too many alerts are generated per time unit, the functionality will be auto-disabled for security (previously informing via email to the user about this circumstance), so that other more demanding notification sending conditions (of lower volume of events) can be selected.

A couple of examples of alert notifications with different formats are shown below:



Soporte Guardian
Para

A new alert has been generated in the severity level system: emergency

Creation date: 28/07/2023 20:34:42 +0000
Type: STATIC
Name: Possible ARP spoofing
Src MAC: [redacted]
Dst MAC: [redacted]
Src IP: [redacted]
Dst IP: [redacted]
Value: [redacted]

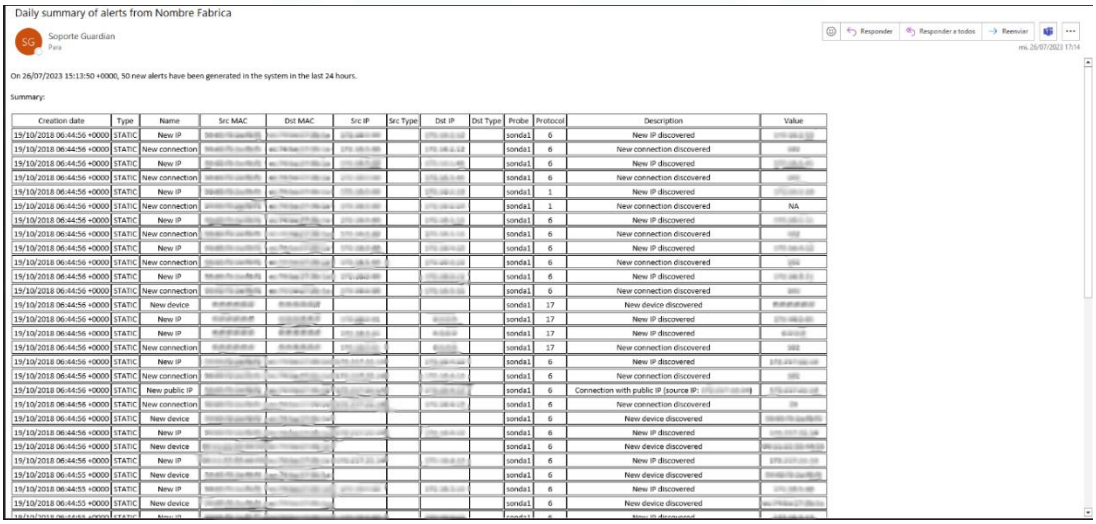
Access the alert for its management in Guardian.

Once managed, if applicable, proceed to silence or resolve it to avoid unnecessary noise. For more information, consult the alerts playbook or the user manual in the reference documentation.

Remember that you can modify your preferences for receiving notifications, their level of severity, format and periodicity, from the user settings.

InprOTech Guardian Support Team
https://inprotech.es/

Summarized individual alert notification example.



Daily summary of alerts from Nombre Fabrica

Soporte Guardian
Para

On 26/07/2023 15:13:50 +0000, 50 new alerts have been generated in the system in the last 24 hours.

Summary:

Creation date	Type	Name	Src MAC	Dst MAC	Src IP	Src Type	Dst IP	Dst Type	Probe	Protocol	Description	Value
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	1	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	1	New connection discovered	NA
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]					sonda1	17	New device discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	17	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	17	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	17	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New public IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	Connection with public IP (source IP: [redacted])	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New connection discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]					sonda1	6	New device discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]					sonda1	6	New device discovered	[redacted]
19/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:55 +0000	STATIC	New device	[redacted]	[redacted]					sonda1	6	New device discovered	[redacted]
19/10/2018 06:44:55 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]		[redacted]		sonda1	6	New IP discovered	[redacted]
19/10/2018 06:44:55 +0000	STATIC	New device	[redacted]	[redacted]					sonda1	6	New device discovered	[redacted]

Grouped daily alert notification example.

3.9 Settings

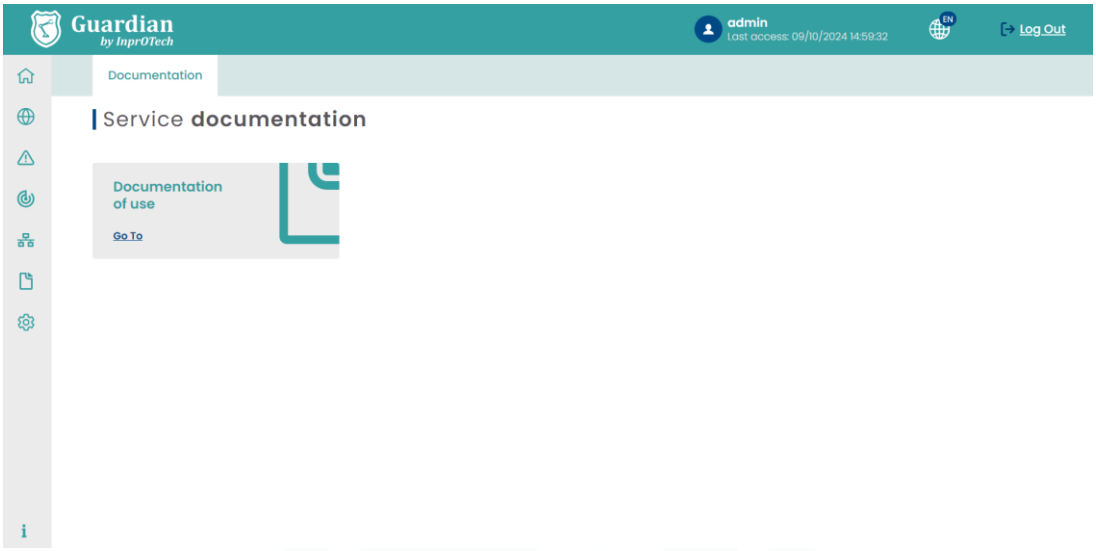
In this section we can adjust our profile or authorized employee profile, adjust some parameters related to threat detection or different configurations of alerts, threats, and user management.

Under development, subject to change.

3.10 Help

Section that enables the download of the latest version of the InprOTech Guardian user manual. Leads to the InprOTech website, where the relevant documentation is posted.

To access it, click on the Menu icon  in the bottom left corner.

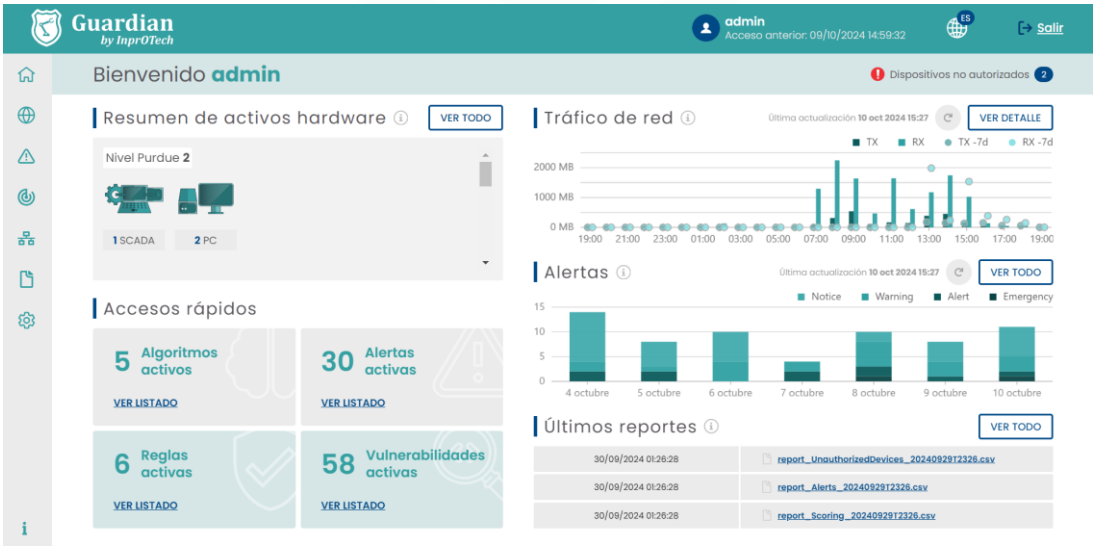


Dashboard principal

Access to the documentation is in the lower left corner. For any technical issue, please contact customer.support@inprosec.com.

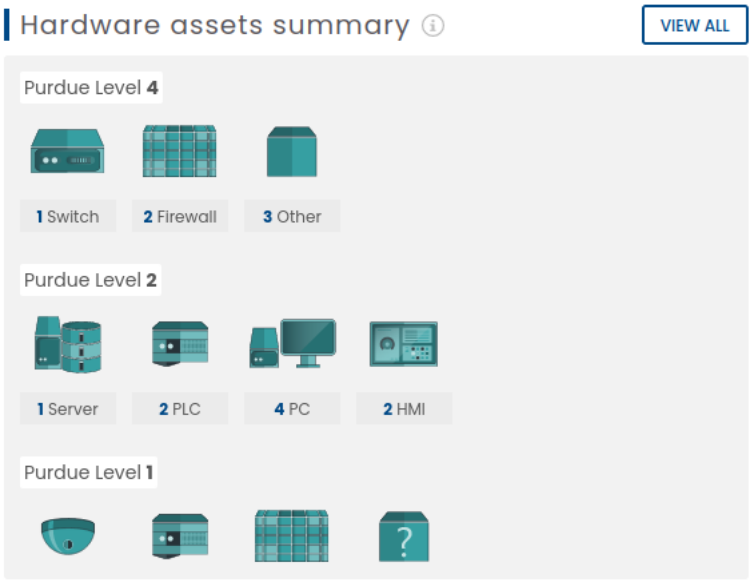
4 Application management

4.1 Main Dashboard



Dashboard principal

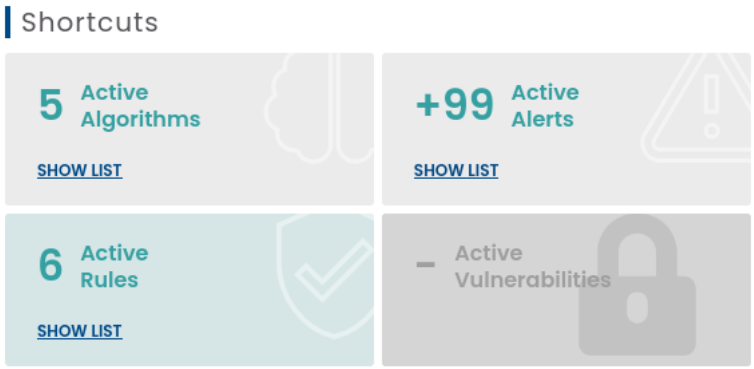
4.1.1 Actives summary



Asset summary

The user can visualize the number of devices connected to the network, differentiated by type (PLCs, RTU, Switch, Router, Robot, PC, SCADA, DCS, HMI, Firewall, frequency inverter, Controller cards, sensors, V.A. Cameras, tablets, Phones, Honeypots, other equipment), and classified according to the Purdue model as indicated in Annex II (provided that it has been reported as indicated in section 4.4).

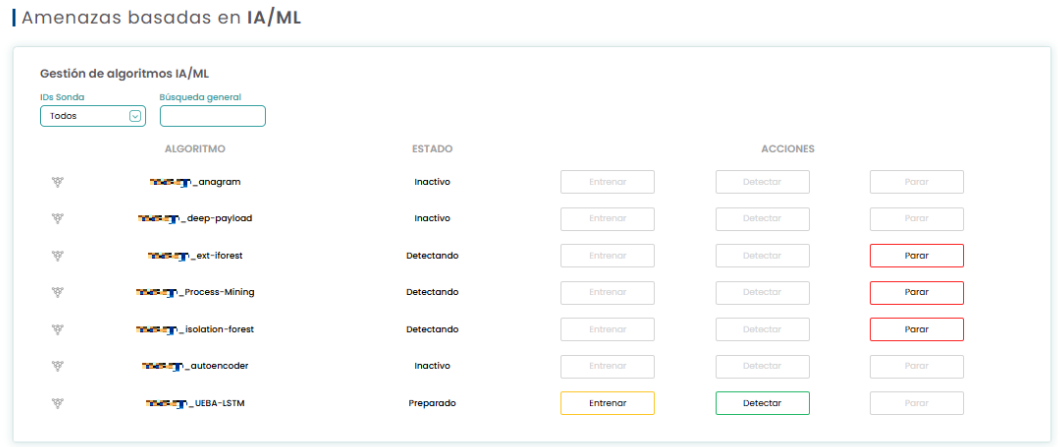
4.1.2 Quick links



Quick links

4.1.2.1 Active Algorithms

By clicking on the "VIEW LIST" link, the user will be able to view the list of artificial intelligence algorithms that are active for threat detection within the organization's network (this section will be discussed later in this manual).



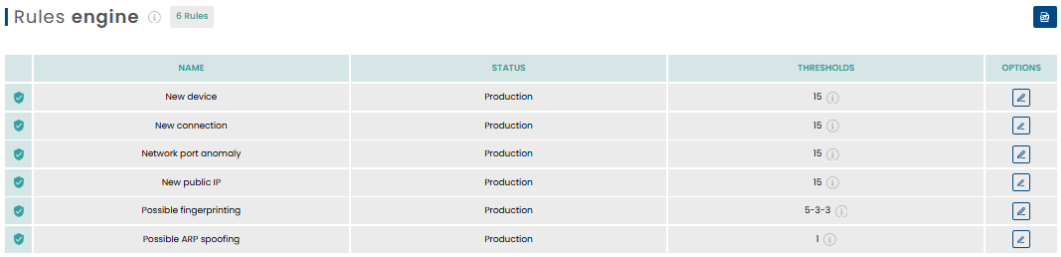
Algorithm list

4.1.2.2 Active Alerts

By clicking on the "VIEW LIST" link, the user will be able to view a list of the total active alerts.

4.1.2.3 Active Rules

By clicking on the "VIEW LIST" link, the user will be able to view a list of the fixed rules that are active for threat detection within the organization's network (this section will be discussed later in this manual).

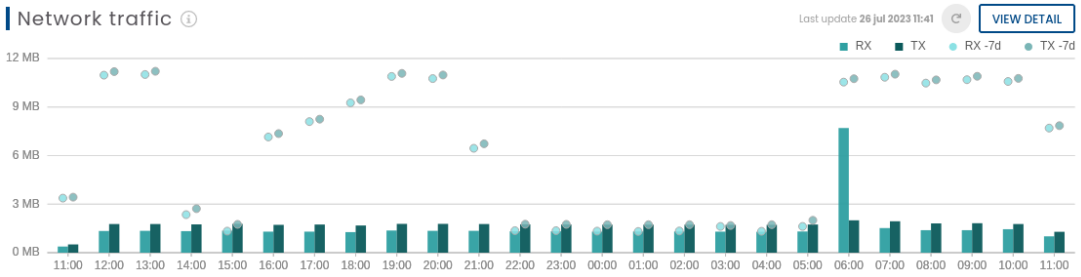


List of active rules

4.1.2.4 Active Vulnerabilities

By clicking on the "VIEW LIST" link, the user can view a list of the total active vulnerabilities that are not managed. Pending development.

4.1.3 **Network traffic graph.**

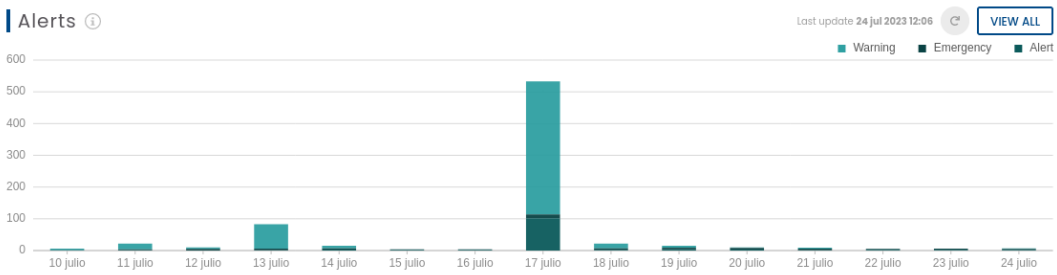


Network traffic

The user can graphically display the traffic generated (in bit/s, or multiple of that unit) in the last 24 hours, both sent (orange) and received (green). It will also have an automatic refresh in that time interval and a button for a manual refresh by the operator. The circled dots on each of the bars will indicate the traffic that occurred 7 days before, as a comparison.

By clicking on the "VIEW DETAIL" button, the user will see on the screen the network sessions window of the InprOTech Guardian application (Section that will be discussed later in this manual).

4.1.4 Alerts graph.



Alerts

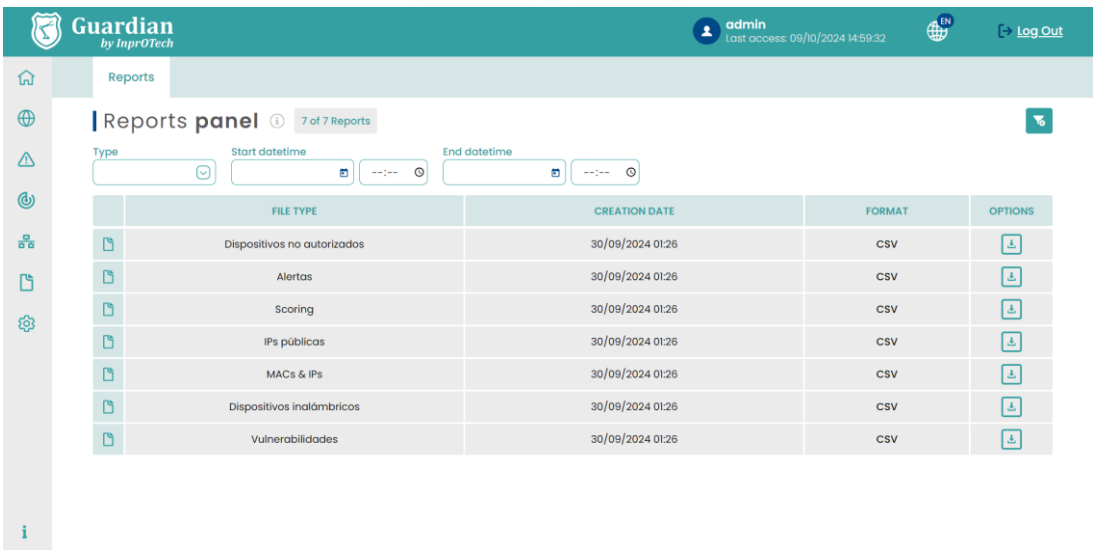
The user will have a graphic representation of the number of alerts differentiated according to their severity level (See Annex I) and colours, per day of the last five days, and the trend they have followed. It will also have an automatic refresh at that time interval and a button for a manual refresh by the operator.

If the user places the cursor over the graphic bar of one of the days, the exact number of alerts and emergencies captured so far can be displayed.

By clicking on the "VIEW ALL" button, the user will see on the screen the alerts window of the InprOTech Guardian application (Section that will be discussed later in this manual).

4.1.5 Last reports

WAIT NEW REPORTS



Last available reports

By clicking on the "VIEW ALL" button, the user can view a list of the latest reports generated automatically or at the customer's request.

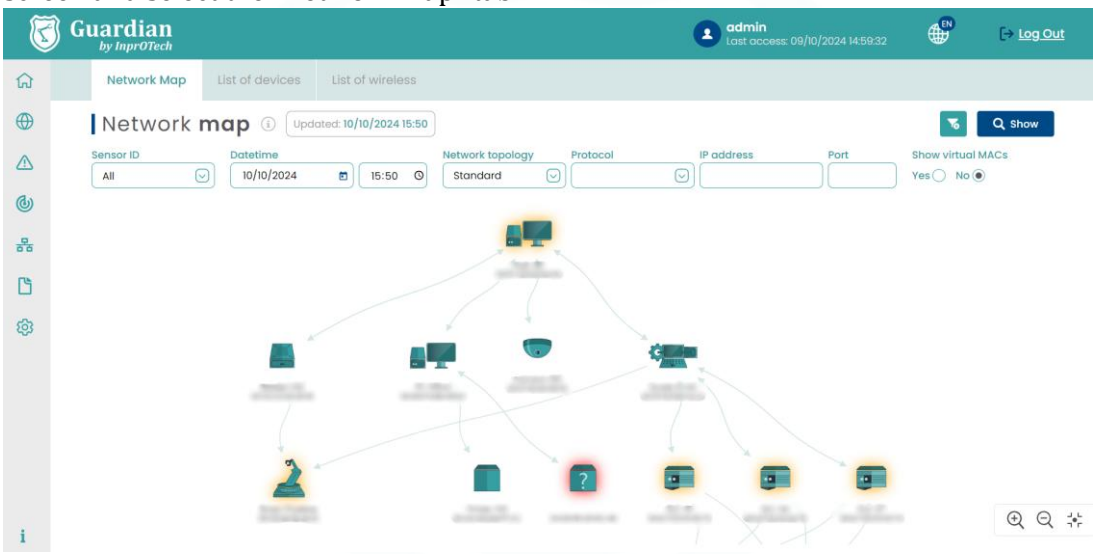
Currently, the reports generated on a weekly basis are:

- List of last alerts detected.
- List of unauthorized devices connected to the network.
- MAC-IP relationship seen on the network.
- Network scoring scores.
- Report of technical service indicators (KPIs)

4.2 Network map and device list.

4.2.1 Network map

To access the network map, the user must click on the icon  on the left side of the screen and select the "Network Map" tab.



Network map

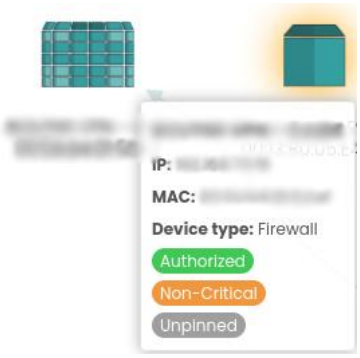
In the network map tab, the user will be able to visualize all the devices connected to the network in real time, as well as the communication links between them. Each device will be referenced with a representative image and a series of properties such as its MAC address or name in case it has been informed manually. The network map will show the implemented topology.

The icons represented will correspond to those described in Annex II.

Unauthorized devices will be displayed on the network map shaded with a red background. Fixed and critical devices will also have their corresponding halo (see Annex I for definitions).

Unauthorized device

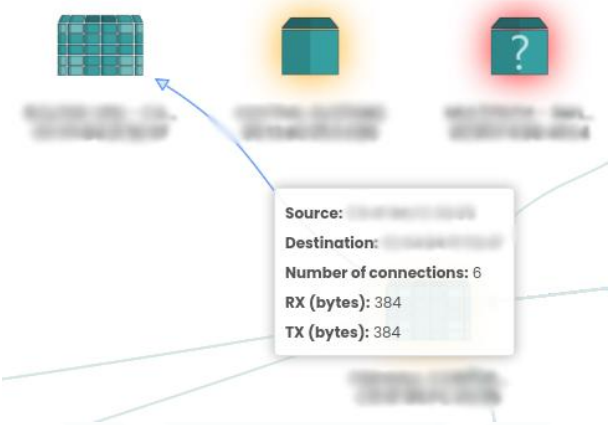
If we place the cursor over a device, we will get a pop-up window where we will see the basic information of the device.



Device basic information

If we click on the device, the window with all the device information will be displayed.

If we place the cursor over one of the links, we will see a pop-up window with the basic information of that communication.



Link basic information.

If we click on the link, the window with all the connection information will be displayed.

The network map can be simplified to display only the devices of interest by using the different filters and accepting the filtering by clicking on the "Consult" button.

Available filters in network map

Filters can be applied according to:

- Date and time: Time frame to be displayed per screen.

- Network topology: Sampling model of the organization's network per screen.

- Protocol: Sampling by screen of only connections using the selected protocol.

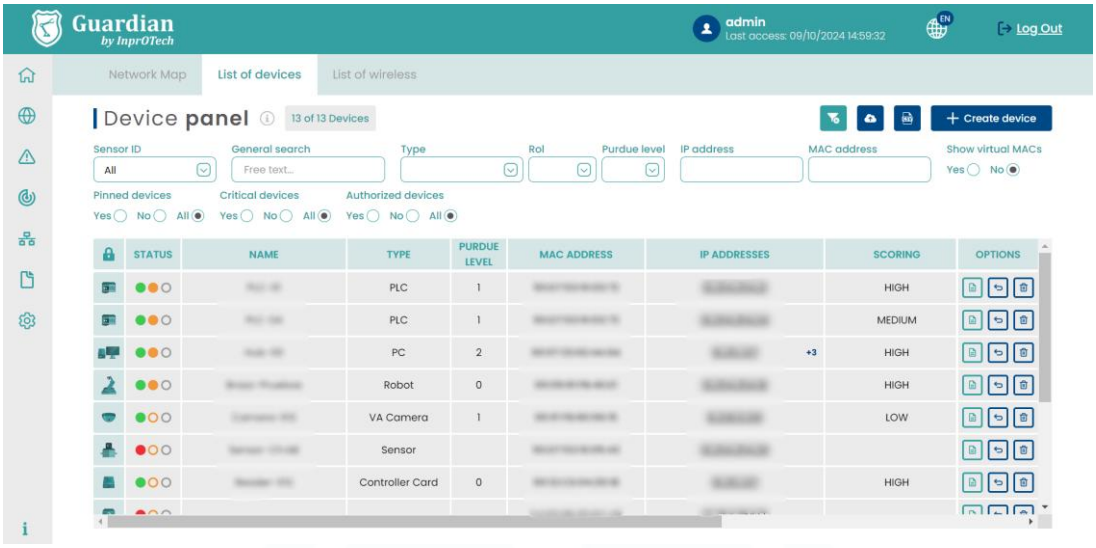
- IP Address: Sampling only of device and connections with the selected IP.

- Port: Sampling by screen of connections to the selected port.

- Viewing or not of virtual MACs (multicast/broadcast), automatically calculated by the system.

4.2.2 Device list

To access the list of devices, the user must click on the icon on the left side of the screen and select the "Device list" tab.



Device list

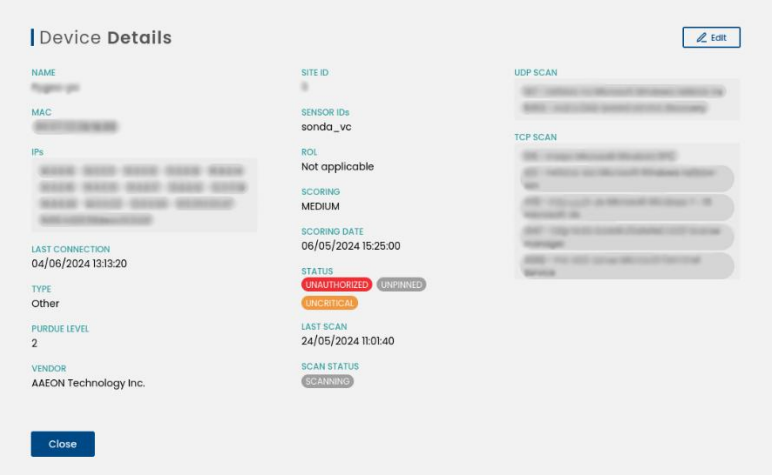
A list of all the devices present in the organization will be displayed along with their information in a more expanded form:

- STATUS
  - The first of the circles will indicate whether the device is authorized (green colour) or unauthorized (red colour).
  - The second of the circles will indicate whether the device is critical (orange colour with fill) or non-critical (orange colour without fill).
  - The third circle indicates whether the device is fixed (grey colour with fill) or not fixed (grey colour without fill).
- NAME: Name assigned to each device.
- TYPE: Differentiation of the type of device (PLC, RTU, SCADA, Honeypot, etc.).
- PURDUE LEVEL: Classification level according to the Purdue model.
- MAC: Assigned MAC address of the device.
- IP ADDRESSES: Assigned IP address of the device.
- SCORING: device importance/risk (low, medium, or high).
- VULN RISK: highest criticality level for all the device's vulnerabilities.
- VENDOR: device manufacturer, identified by the first three fields of its MAC address.
- FIRMWARE: integrated firmware device.
- CUSTOMIZED FIELDS: In addition to the existing fields, users can create their custom fields in key-value format. Each customizable field will appear in the

device list as a new virtual column, allowing the user to catalogue, organize, and filter the devices. These customizable fields will also appear in the reports.
The columns created as customizable fields will be part of a virtual inventory. The user can apply filters to this inventory as desired. This field inventory is also exportable.

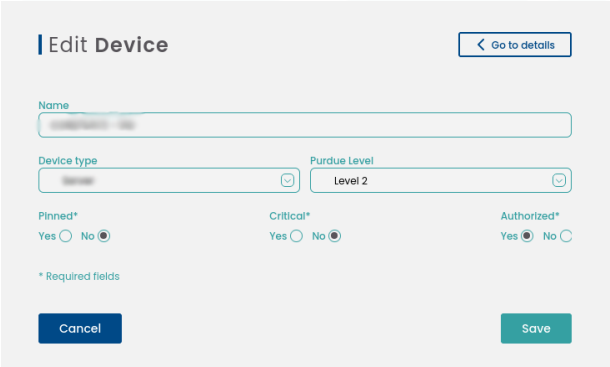
- ACTIONS:

: Button to view device information in detail.



Device details

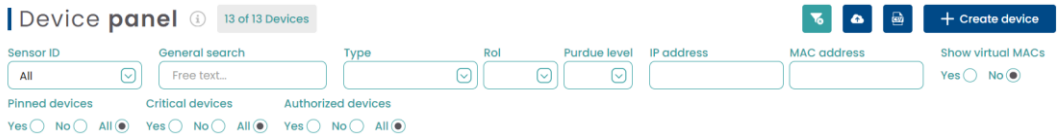
Editar: Button to modify device parameters.



Dice parameters

: Button to perform other actions on the device, such as access with pre-filtered view to the list of alerts, vulnerabilities (under development), as well as node deletion.

There is the possibility of filtering so that the screen displays only the devices in which we are interested.



Device filtering

The user can perform this filtering according to:

- Probe ID, to filter by zone of the industrial network and/or headquarters.
- Device name
- Device Type (PLC, RTU, SCADA, Honeypot, FIREWALL, etc.)
- Device Role (Transmitter, Receiver, or both)
- Purdue level, according to Annex II
- Device IP address
- Device MAC address
- View of broadcast reserved virtual MACs (Y/N).
- Fixed devices (Y/N), see Annex I.
- Critical devices (Y/N), see Annex I.
- Authorized devices (Y/N), see Annex I.

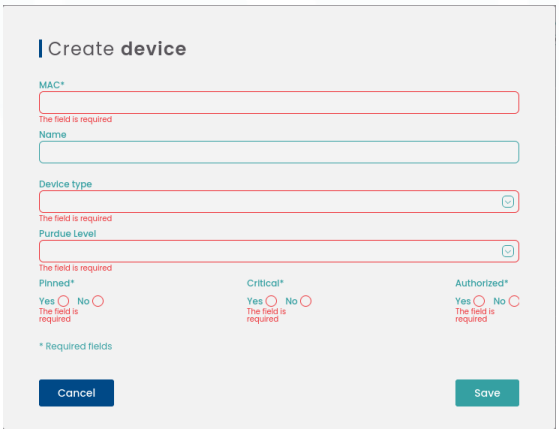
The user can also perform a general search using a text string.

Pressing the button  will reset the filtering values and Guardian will display the complete list with all devices again.

By means of the button  our product will perform a CSV file export of the list of devices with their information.

It is possible to manually add a new device to the organization's network and list by clicking on the button  .

The following pop-up window will appear:



Available fields to create a device.

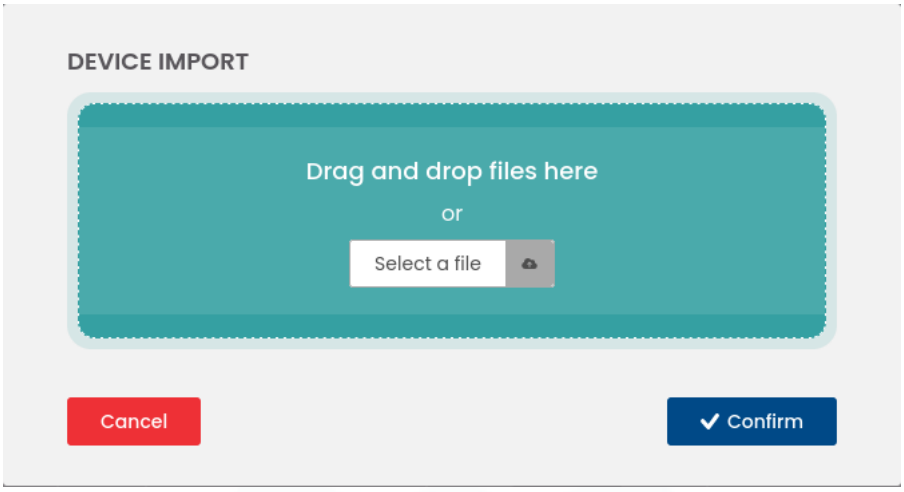
The requested information about the device to be added must be entered manually and to make the creation effective, click on the "Save" button.

4.2.2.1 Import CSV

The system allows mass import/editing of devices, to avoid unnecessary alerts during initial onboarding or major changes in the industrial network.

In the network section and the "Device List" tab, you will see the following icon:  . Clicking on this icon will open the following pop-up window.

From this window, you can select or drag a file with ".csv" extension containing the data of the devices you wish to add or modify, in the format indicated below.



Import CSV pop-up.

For the CSV file to be valid, it must comply with the following characteristics:

- A maximum of 250 records.

- Header with the following columns (we can name the columns as we wish):

  - MAC
  - Device name
  - Authorised (Y/N)
  - Critical (Y/N)
  - Fixed (Y/N)
  - Device type (from the allowed list: virtual, plc, rtu, switch, router, robot, pc, scada, hmi, firewall, adjustable_frequency_drive, controller_card, sensor, va_camera, tablet, voip_phone, server, code_bar_scanner, other)
  - PURDUE level (0 to 4, as explained in Annex II)
  - Customized fields.

- The field delimiter shall be ";".
- It shall not contain empty fields.
- It may contain new device records, or existing devices in the database to which you want to change one or more of the attributes mentioned in the previous point. One row per device is required, in the format indicated.
- The new records will simply have all the CSV fields covered with the desired information.
- The existing records that we want to modify, will contain the literal *CURRENT* in all those fields that must remain fixed. In the fields to be updated, we will simply put the latest information based on what has been previously established.
- The ones we want to modify must have *CURRENT* in some of their properties; this allows us to distinguish these records from the new ones.
- The mac field cannot contain the literal *CURRENT* since it univocally identifies the device.

- New records may also contain the literal *CURRENT* in some of their fields; this means leaving those fields with default values. In the case of Boolean data, it will be false, and text fields, such as name, Purdue, and device type, will remain as NULL, and the user can modify it through the web interface.
- There are two posible ways to define a set of customized fields, respecting their key-value structure:
    - .json format: {"key1": "value1", "key2": "value2"}
    - Bars: key1 | value1 | key2 | value2

  You could delete previously defined customizable fields by overwriting the data with a new CSV document. This document should contain the literal *DELETE* in place of those fields, like the use of the literal "CURRENT."

- It is crucial to write literals between asterisks.

Notice: Please consult Support if you have any doubts, as improper use of this functionality can significantly impact the integrity of the node information.

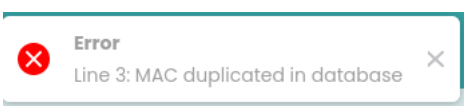
Once the file has been selected, click on "Confirm", as this is a high impact operation (it allows both adding and modifying device properties):

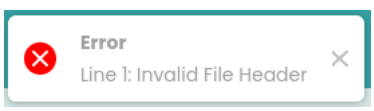
"Device import" drop-down.

If the ".csv" file we have sent does not contain any device, the following error message will be displayed.

Import error.

If there are errors in the data within the ".csv" file, a message will be displayed with details of the errors found, along with the line number where each error is found.





Import error.

If no errors are detected, it shall be possible to verify that the devices have been correctly added to the database.

4.2.2.2 Air Watcher (Wireless devices list)

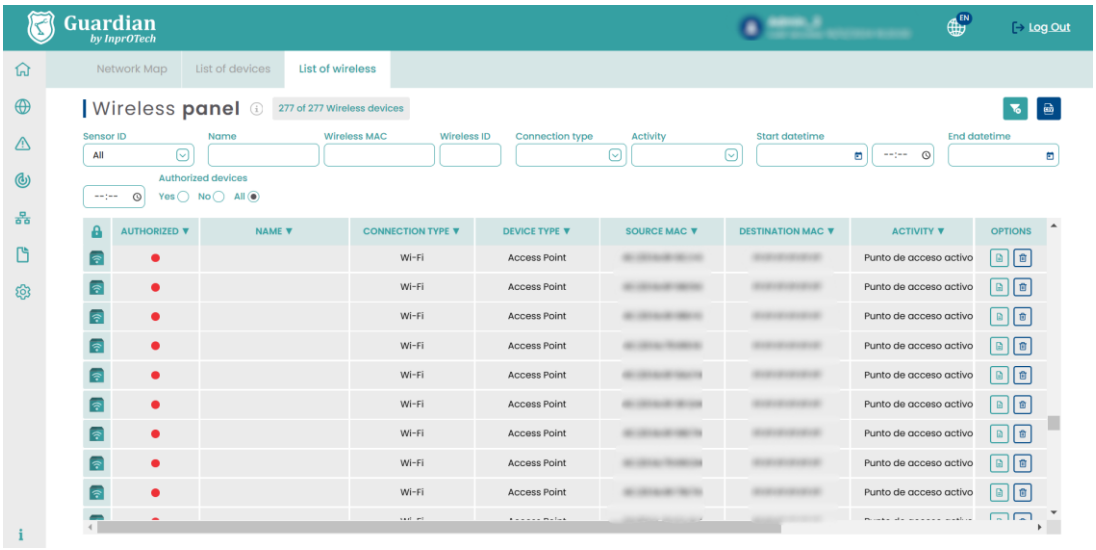
In the network section, there third tab allows access to the list of Wireless devices registered in the network.

At the top, the total number of devices in the database can be seen and, if with a filter applied, how many match that filter in relation to the total.

On the right side, there is a button panel to delete the previously applied filters and export the list of devices in CSV format.

The information provided by this section will be the following, for all those devices with Wi-Fi or Bluetooth capability detected in the vicinity of the collectors:

- **Authorized**: determines whether the device has been authorized by an administrator (green) or not (red).
- **Name**: it corresponds to the name of the device.
- **Connection Type**: could be Wi-Fi or Bluetooth.
- **Device Type**: values can vary for Bluetooth devices. For Wi-Fi devices, it can take values such as "Access Point" or "Smartphone or Laptop," in addition to "Unknown."
- **Source MAC**: source MAC address of the packet. Identifies the device itself in the captured communication.
- **Destination MAC**: destination MAC address of the packet. Identifies the receiving device of the packet.
- **Activity**: reflects the state of the device or the type of activity it has performed:
    - Searching for networks: the device has the Wi-Fi antenna on and is searching for access points.
    - Connection attempt: the device has tried connecting to an access point.
    - Access point active: the device is functioning as an Access point.
    - Transmitting data: the device is sending information to an access point.
    - Device visible: this only applies to Bluetooth devices; the device has Bluetooth on and is visible to other devices.
- **Wireless ID**: name or identifier of the Wi-Fi network (could be empty if, for example, the connection is Bluetooth).
- **First Seen**: format dd/mm/yyyy hh:mm.
- **Last Seen**: format dd/mm/yyyy hh:mm.



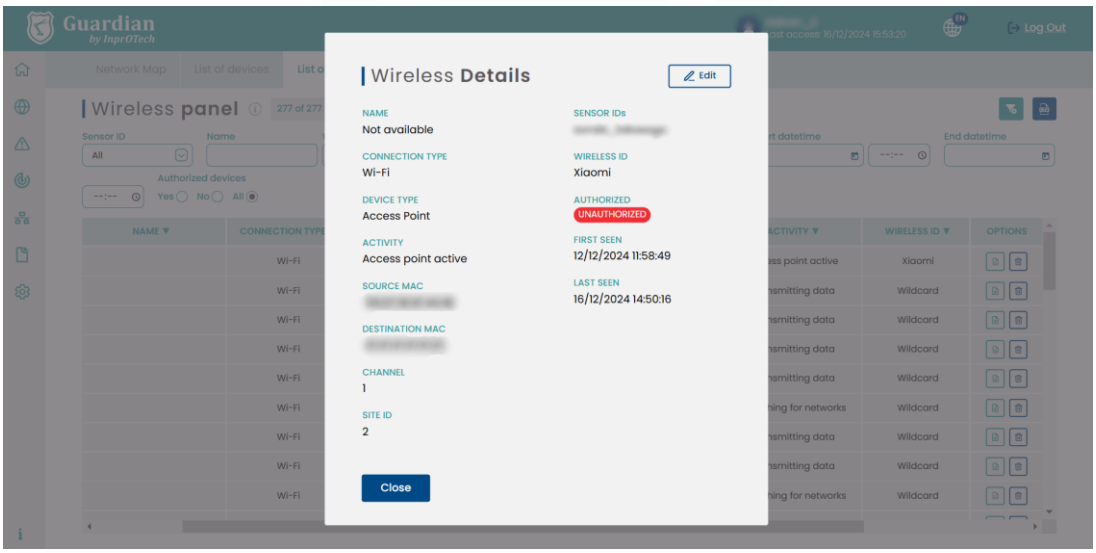
Wireless device list

Below are the possible filters that can be applied to keep the devices we are interested in:

Wireless list filters

Remember that it is possible to sort the devices alphabetically either directly or inversely by clicking on any of the columns.

Finally, the actual list of assets contains information details about them, as well as buttons to perform certain further actions (view more details or delete).

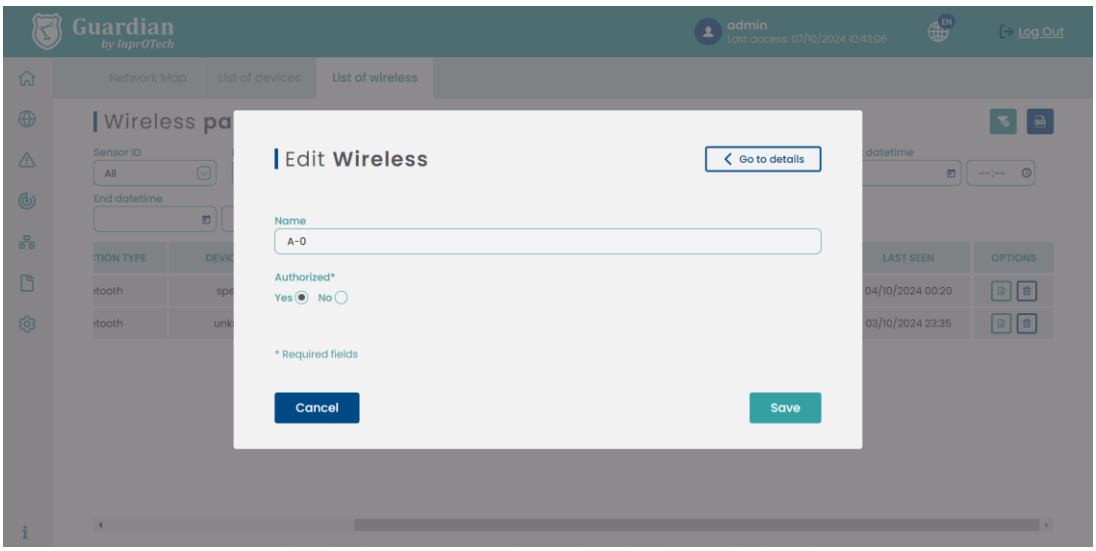


Wireless devices details

We will also be able to see some additional fields in this new modal window:

- Channel: transmission channel identifier.
- Site ID: represents the factory.
- Sensor IDs: identifies the sensor.
- Wireless ID: device unique identifier.

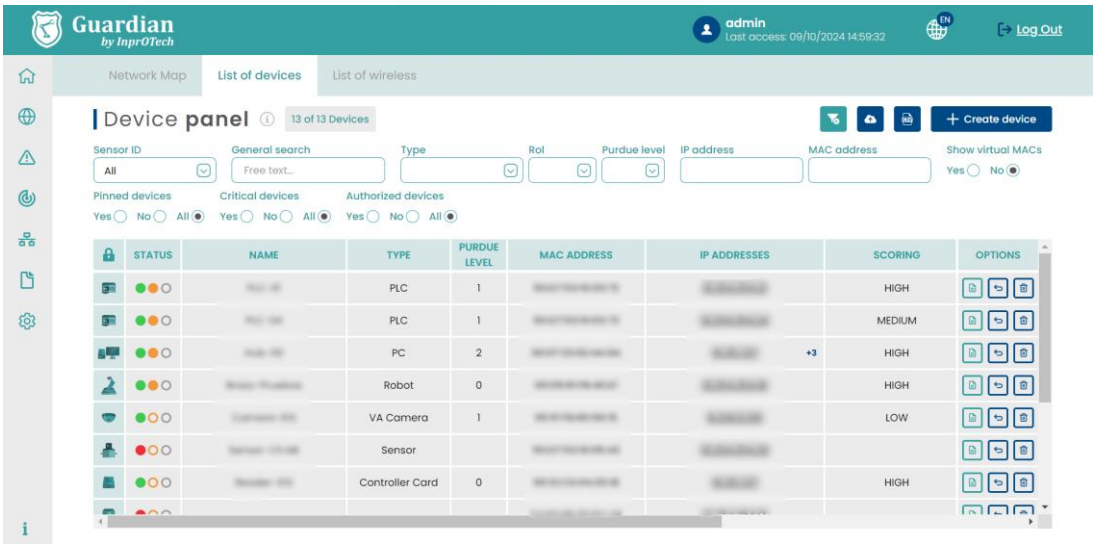
If we click on the Edit button, we can rename the device and determine whether it is authorized or not.



4.2.2.3 Smart View (Device scan)

This capability allows an active scan of the devices in the OT network, to identify some additional properties of each node by means of a light fingerprinting: device version, firmware, open ports, and services running on the machine itself.

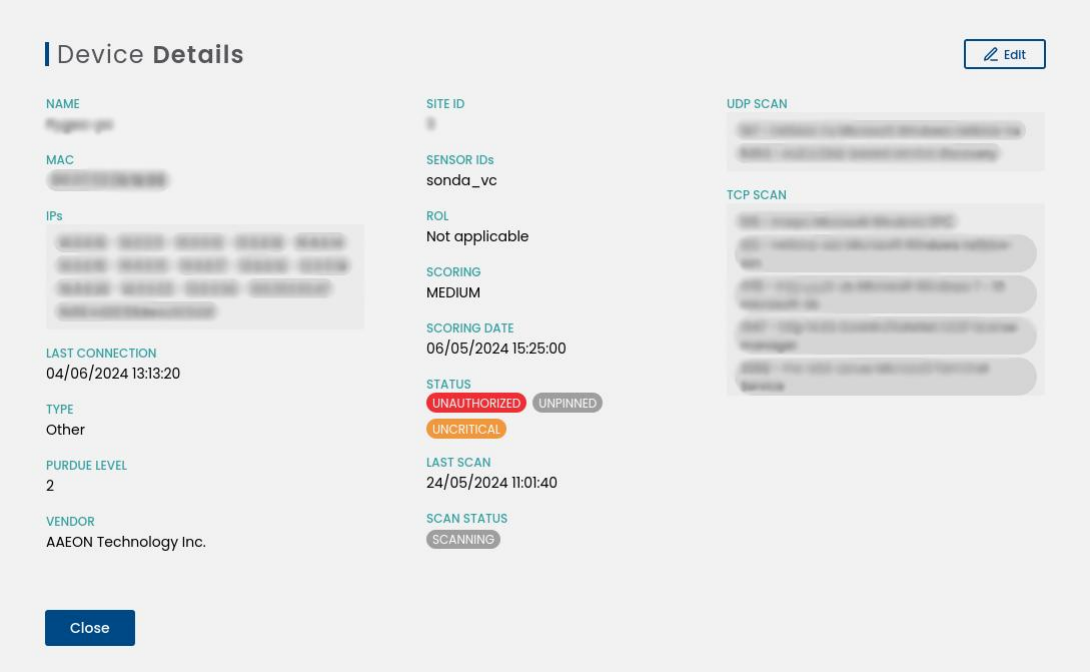
For this purpose, the nmap tool will be used, and the ports on the TCP and UDP network protocols will be scanned. This information will be recorded in the system database and can be extracted as additional attributes of each device, which will be refreshed by a periodic pooling.



Device list

As can be seen, once the scanner has been run, information associated with the firmware of some of the devices is showed in the list.

The rest of the scanner information can be viewed by clicking on the icon on the right . In the pop-up will appear all the information of the device in question, and two sections called 'TCP Scan' and 'UDP Scan.' There all the open ports found for a given device will be displayed, as well as the date of the last scan and if it has finished correctly or if there has been some kind of error.



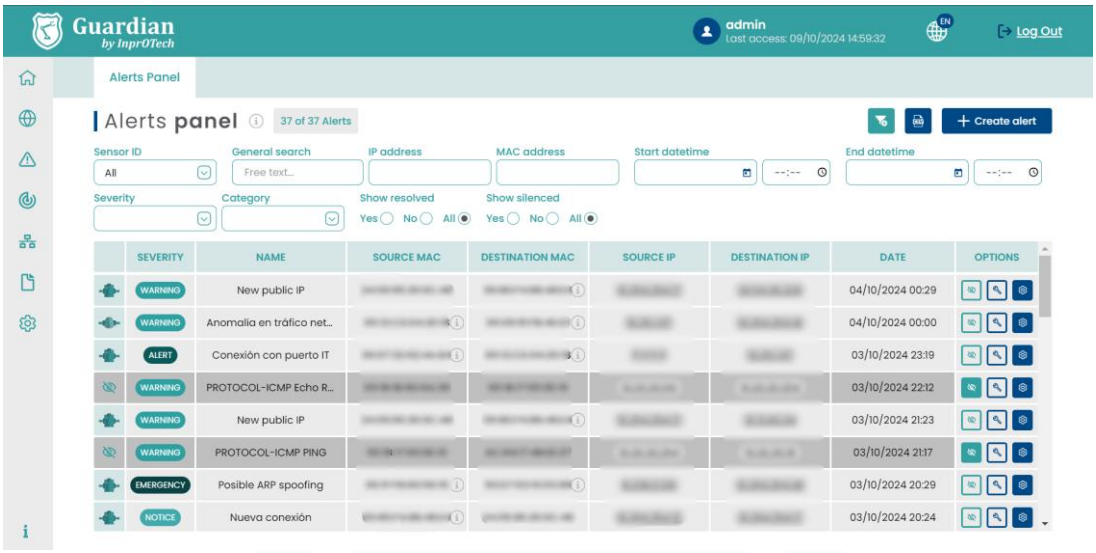
Device details

DISCLAIMER: Given the active nature of this operation, although no operational impact has been observed, it cannot be completely ruled out. It is therefore up to the customer to decide whether to activate this functionality (for which InprOTech support should be consulted). If you would like to activate it in your instance but leave some subset of devices excluded from the list of nodes to be analysed, just tag them with the 'Critical' property enabled in the device inventory (individually or through a mass update).

Additionally, honeypot devices labelled as such are also exempt due to their behaviours as decoys with vulnerable ports. This helps prevent the excessive generation of false positives.

4.3 Alerts panel.

To access the list of alerts, the user must click on the following icon  on the left side of the screen.



Alerts list.

A list will be shown with all the alerts present in the organization and information about them.

- Severity: Classification of the alert according to the impact it could have on the organization.

- Name: Defined name of the alert.

- Source MAC: MAC of the alert generating device.

- Destination MAC: MAC of the device to which the action was directed.

- Source IP: IP of the device generating the alert.

- Destination IP: IP of the device to which the action was directed.

- Date: Date and time of alert appearance.

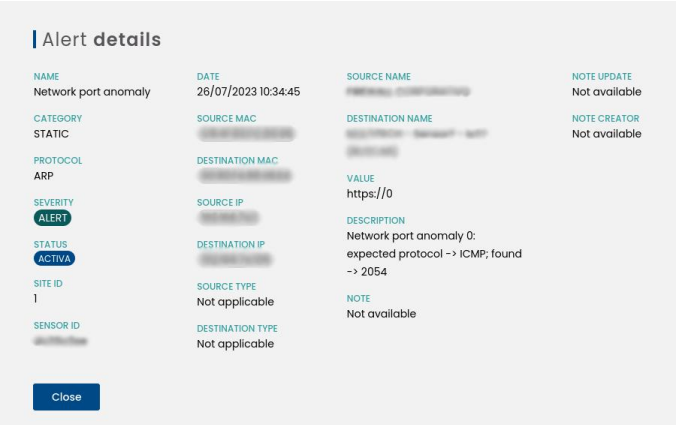
- Actions (see annex I for definitions):

 : If we place the cursor over it, we will be able to know the name of the device assigned to that MAC address.

 : Button to change the alert status to muted or unmuted (see section 6.2 in Annex I).

 : Button to change the alert status (solved or not solved), according to the logic indicated in Annex I.

 : Button to perform further actions on the alert, such as viewing the details or adding notes.



Alert details

It is possible to filter the display to show only the alarms of interest.

Available alert filters

This filtering can be done according to:

- Probe ID, to filter by zone of the industrial network and/or headquarters.

- General search: Search by entering a text containing the alarm (including in your notes).

- IP address of the device

- MAC address of the device

- Date and time of start of alert search

- Date and time of alert search end date and time

- Severity, according to Annex I

- Alarms resolved or not resolved, according to Annex I

- Alarms silenced or not silenced, according to annex I

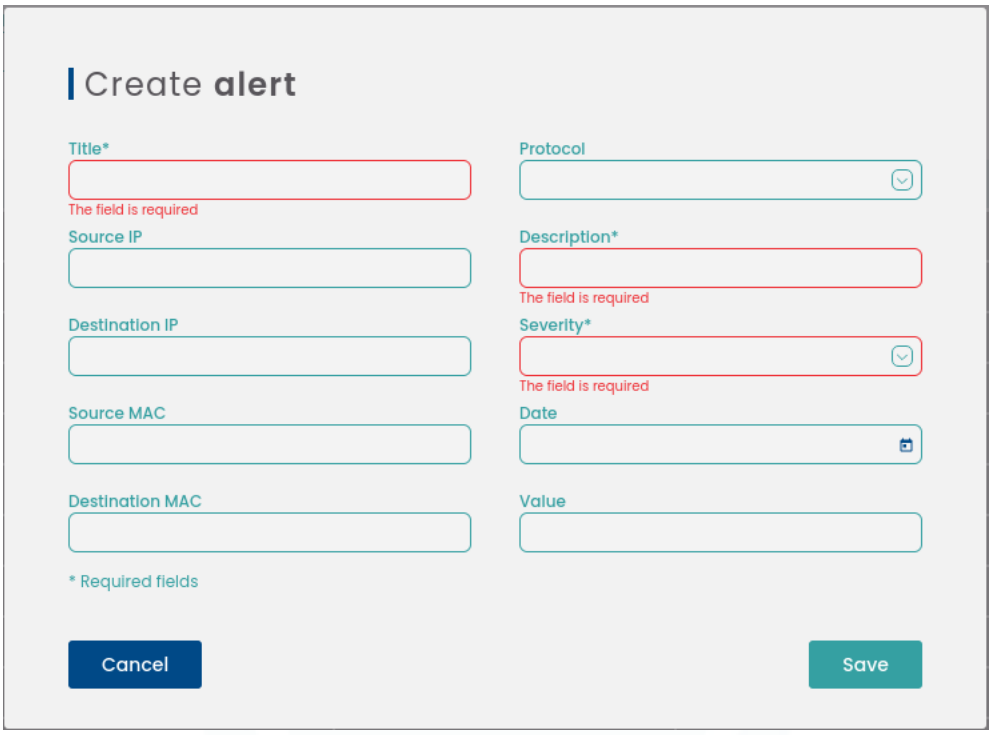
Pressing the button  will reset the filtering values and the complete list with all the alarms will be displayed again.

By means of the button  a CSV file export of the list of alarms with their information will be made.

It is possible to manually create a specific alarm in the organization's network by clicking on the button 

.

The following pop-up window will appear:



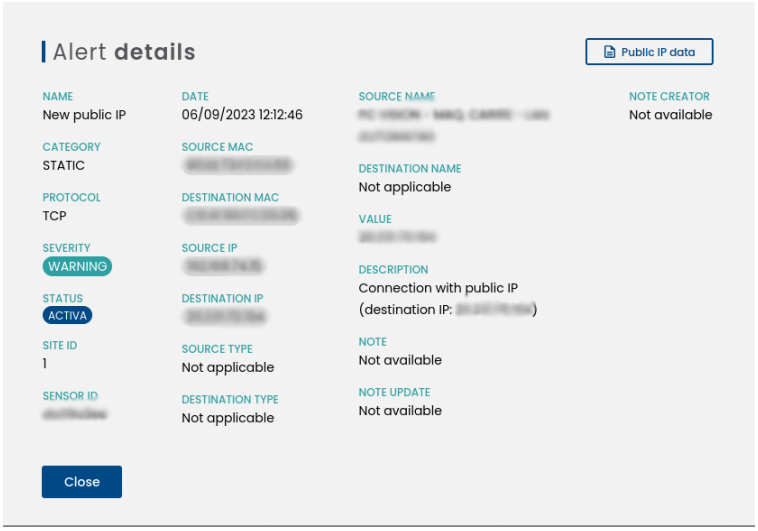
Alert creation

The requested information about the new alarm created must be entered manually and to make the creation effective, click on the "Save" button.

4.3.1 Public IP

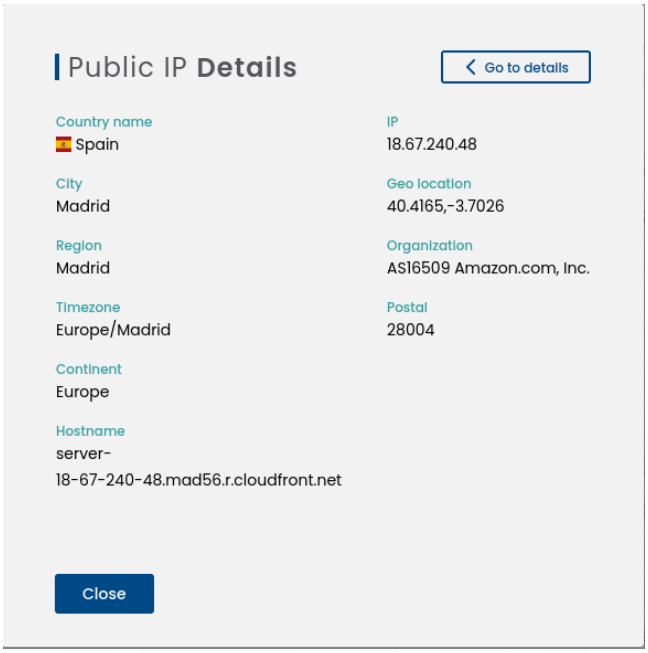
This alert is connected to a cyber-intelligence service that allows us to obtain more information about the communication endpoint outside the trusted network, to try to determine whether it may be malicious.

To access the details of the alert, click on the gear icon, which can be seen on the right-hand side of the panel. Then, by clicking on "View details", you can access this information:



Screen with alert details.

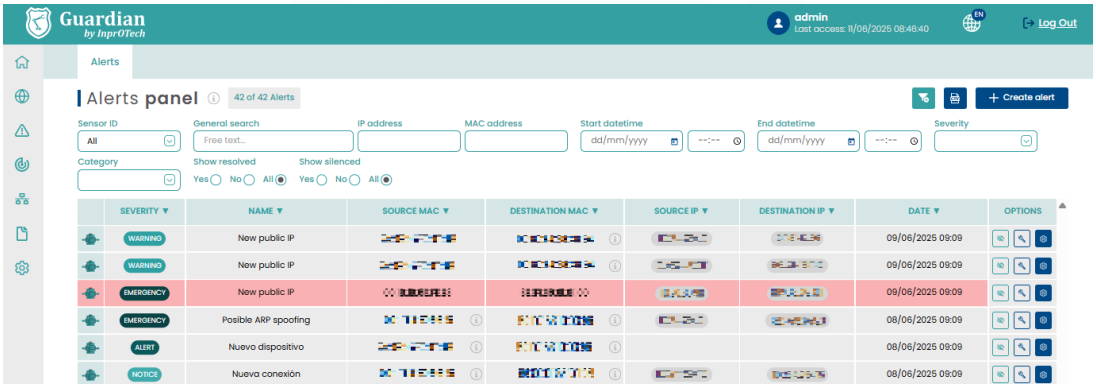
At the top of this tab, there is a button called 'Public IP Data'. Clicking this button will take you to additional information about the IP, which may include details such as home city, region, time zone, continent, country name, public IP address, coordinates, organisation, and postcode.

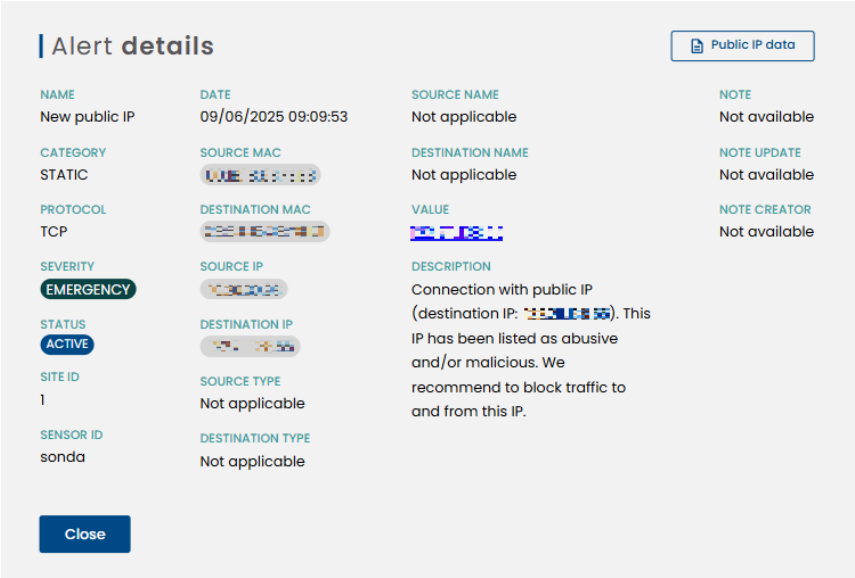


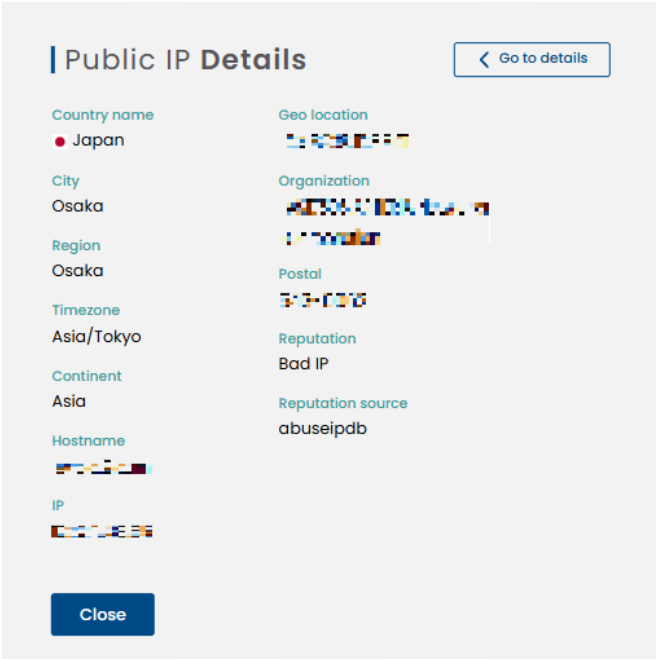
Public IP details

4.3.2 Ip Reputation and Blocking Policy

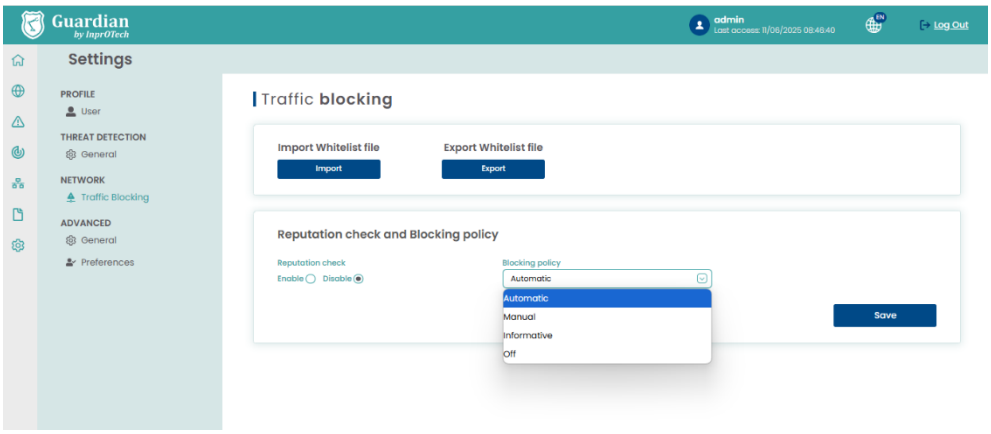
When the system detects a *New public IP* connection alert, Guardian connects to a series of public listings where activities considered abusive (spamming, hacking, etc) are reported. The alert is enriched with this information, visible in the public IP details, and in case it detects that the public address involved has a bad reputation, it changes the severity, the description, and marks it in red.







The Reputation Check can be enabled and disabled in the configuration menu, Network/Blocking section. This option affects incoming alerts, i.e., enabling reputation will not retroactively affect those public IP alerts that came in while reputation was disabled.



When the system receives a public IP alert considered malicious, Guardian will respond applying one of the three available Blocking Policies:

-**Informative**, where the user is informed and recommended to review and block traffic from/to that address.

-Manual or semi-unattended, where a button is enabled to block/unblock the malicious IP by sending the firewall an instruction to include that address in a filter.

-**Automatic**, where Guardian sends this instruction to the firewall without human intervention.

The Blocking Policy can also be disabled. In this case, all information regarding the IP reputation in the alerts will be disabled, as well as the blocking rules (via sending command to the firewall to lift the address blocking rule). This information is not deleted, and will be reapplied if the Blocking Policy is re-selected to an active value. A drop-down selector for the Blocking Policy can be found in the same menu. Public IP alerts that reach the system while the Blocking Policy is disabled are not retroactively changed when the Blocking Policy is re-enabled.

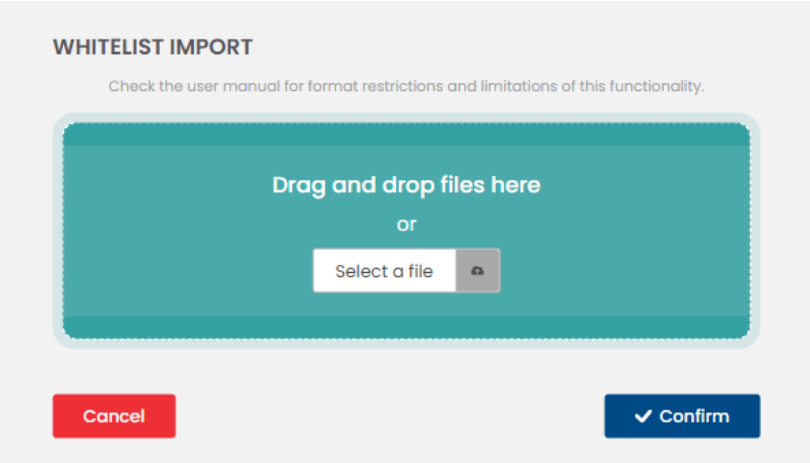
Automatic and semi-automatic options are currently under development

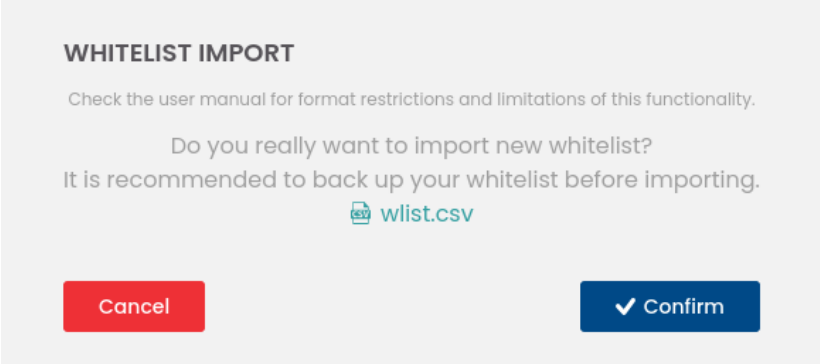
4.3.3 IP whitelist

The user can provide a list of always-allowed IP addresses, or also address ranges in CIDR format (whitelist). These addresses will never have their reputation calculated even if the check is enabled when a related alert is received. This will only be reflected in the public IP data menu in their reputation field as *whitelist*.

The upload file must be in *csv* format, with only one column per row, which must contain either an IP address (192.168.0.1) or a CIDR range (192.168.1.0/24). The loading is performed atomically: a single misformatted or invalid data invalidates the entire operation. Possible redundancies in the list of addresses and ranges (repeated IPs, IPs contained in CIDR ranges, overlapping CIDR ranges) are not treated as errors.

The import will be performed in the blocking options, through the screen displayed after pressing the button Import under the "*Import Whitelist file*" option, which will present the following pop-up window where you can either drag the file to the green box, or find it in the users's filetree.





Next imports will completely replace the previous whitelist. Thus, if you do not want to implement any whitelist, simply load an empty file.

Uploading a new whitelist has an effect on the public IP alerts already in the database:

- those alerts with IPs that have the reputation already processed before, and that are included in the new whitelist, are returned to the original state with the status '*reputation: Wlisted*'.

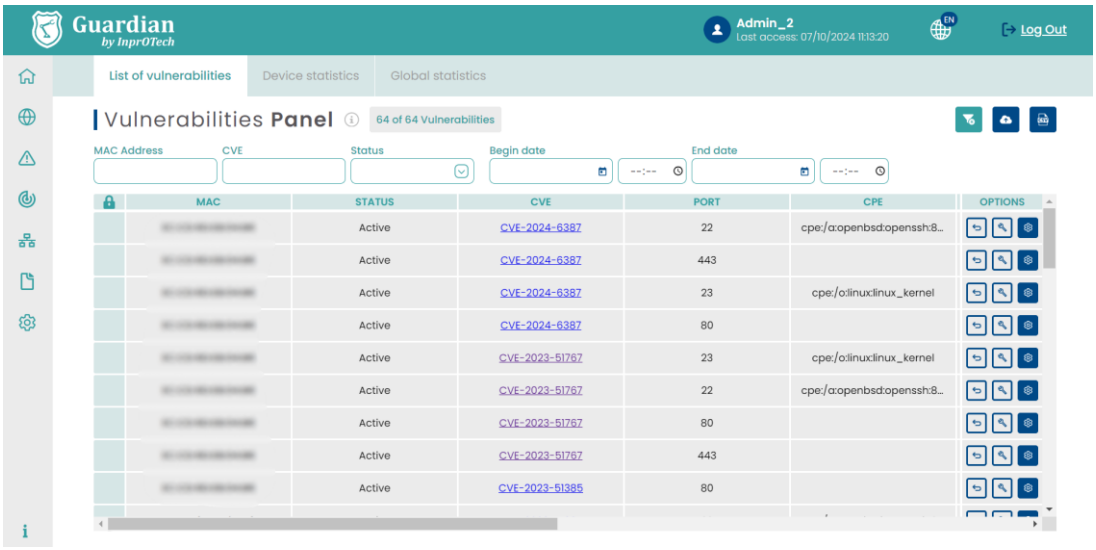
- Those alerts with IPs within the previous whitelist, but which are outside the new whitelist, have their reputation calculated and the alert description modified accordingly.

The loaded whitelist can be downloaded for examination by clicking on the button Export, which will download a csv file with the saved data.

4.4 Vulnerability analysis

4.4.1 Vulnerabilities Panel

To access the vulnerabilities panel, the user must click on the icon  that appears on the left side of the screen and select the "Vulnerabilities Panel" tab.

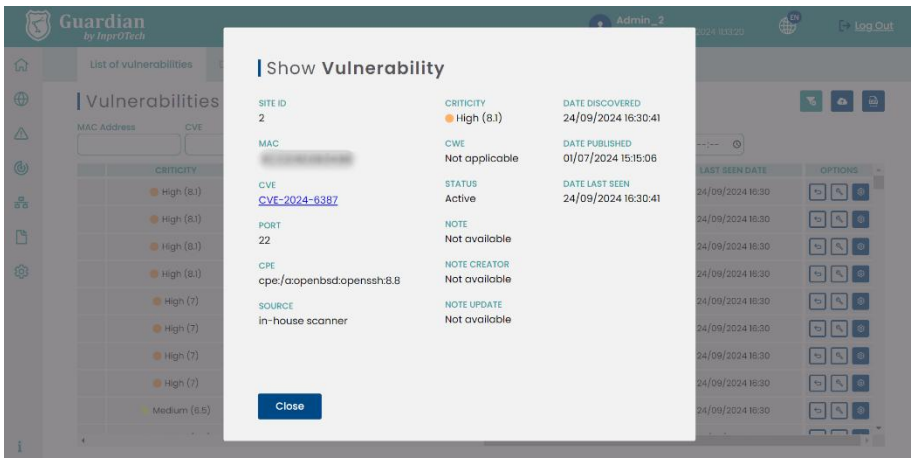


View of the Vulnerabilities Panel

In the vulnerabilities panel tab, the user can view a list of all the vulnerabilities present in the network. These are found in the services detected after the open ports discovered by Smart View and checked against the NIST vulnerability database, the National Vulnerability Database (NVD).

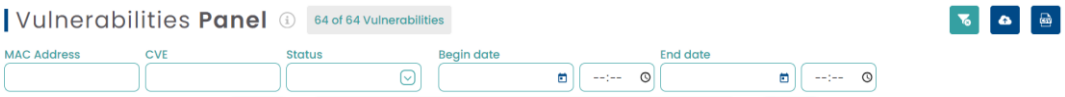
The information displayed in each row is as follows:

- MAC Address: the MAC address of the device where the vulnerability has been detected.
- Status: indicates whether the vulnerability is active, resolved, silenced, or a false positive.
- CVE: "Common Vulnerabilities and Exposures." Identifier according to the vulnerability classification glossary.
- Port: port f the device
- CPE: "Common Platform Enumeration." Identifier of the product or system affected by the vulnerability in question.
- Source: system or device that found the vulnerability.
- Criticity: score from 0 to 10, assigned based on the criticality level of the vulnerability.
- CWE: "Common Weakness Enumeration." Identifier of the common weakness associated to the vulnerability found.
- Discovered date: Date when the vulnerability has been found.
- Published Date: the documentation date when the vulnerability with the referenced CVE was reported in the NVD vulnerability database.
- "Last seen": timestamp when the vulnerability was seen for the last time.
- Options (Actions):
  - Go To: allows viewing the alerts generated by this vulnerability or the devices on which it is present.
  - Change status (active, resolved, silenced, or false positive.).
  - Other actions: allows to view the details of a vulnerability and add a note.



Details of a vulnerability.

Next to the header, we can see the number of vulnerabilities displayed, along with the total count.



Number of de vulnerabilities and filters.

In the upper screenshot, we can also see that it is possible to apply filters, so the display only shows the desired vulnerabilities. This filtering is done by:

- MAC Address
- CVE
- Status
- Start Date and Time
- End Date and Time

By pressing the button  , the filter values will be reset, and the complete list with all vulnerabilities will be displayed again.

Using the button, you can import a file with a ".csv" extension containing the vulnerabilities you want to add. They must contain the following fields, keeping the dates in the format YYYY-MM-DDTHH:MM:SS.000GMT+XX:XX:

- Vendor ID
- MAC Address
- CVE
- Port
- CPE (Optional)
- Source
- Criticity
- CWE (Optional)
- Status
- URL
- Note (Optional)
- Creator Note (Optional)

- Timestamp Discovered
- Timestamp Published
- Timestamp Last Seen

On the other hand, using the  button, it is possible to export a CSV file containing the list of devices and their information.

4.4.2 Device statistics

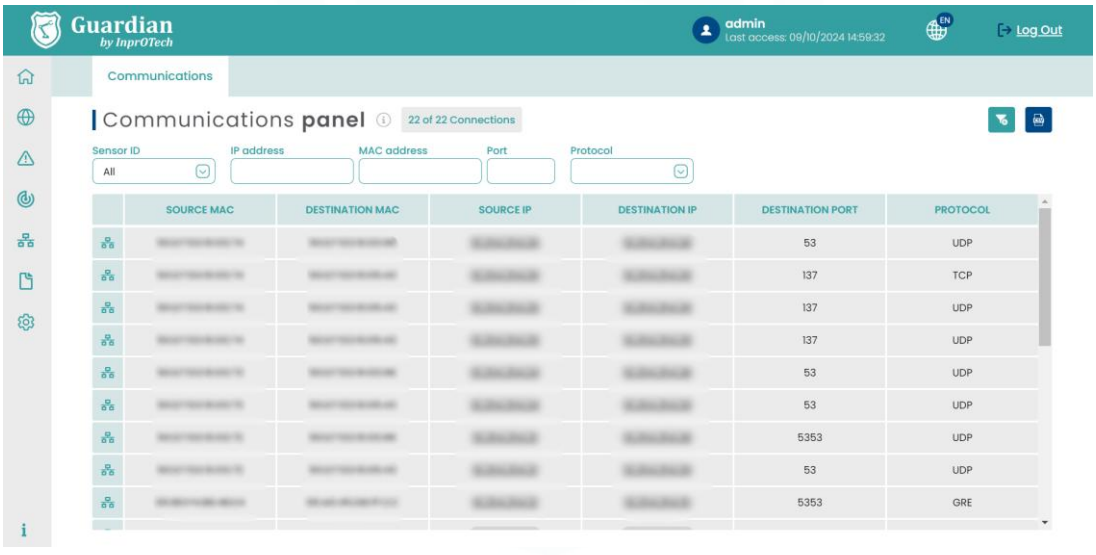
Offers the vulnerabilities found in the network, sorted by the available devices.

4.4.3 Global statistics

Offers global statistics of the network given its vulnerabilities.

4.5 Communications

To access the communications list, the user must click on the icon  that appears on the left side of the screen.



Communications list.

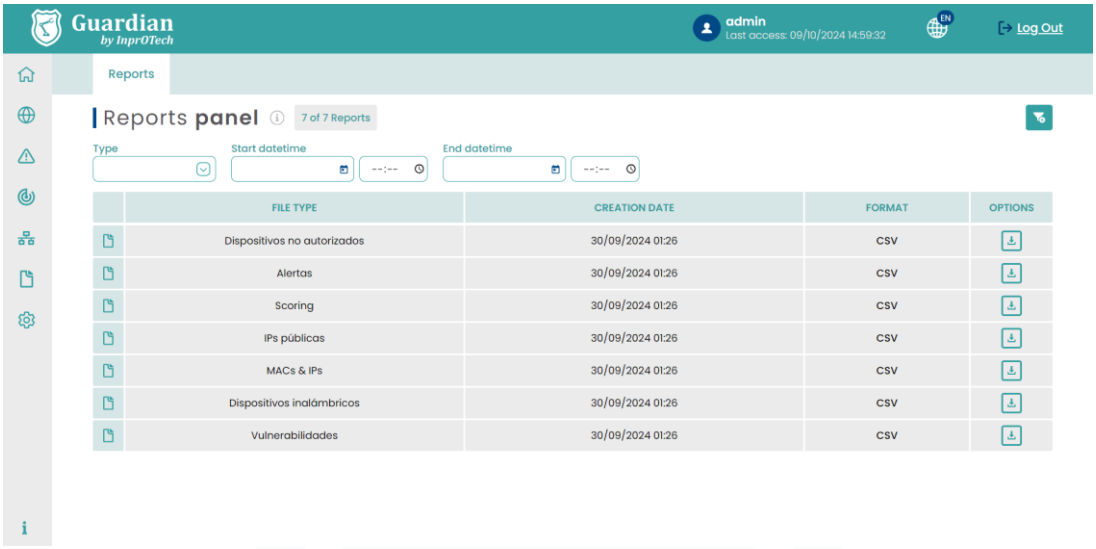
A list of all the communications that have been made between the OT devices of the organization's network, and information about them, will be displayed.

A communication is understood as the grouping of connections between MAC, IP, and source port, and the same for the destination. It is considered a new communication if there is a change of protocol.

Available communications filters

4.6 Reports

To access the list of reports, the user must click on the icon that appears on the left side of the screen.



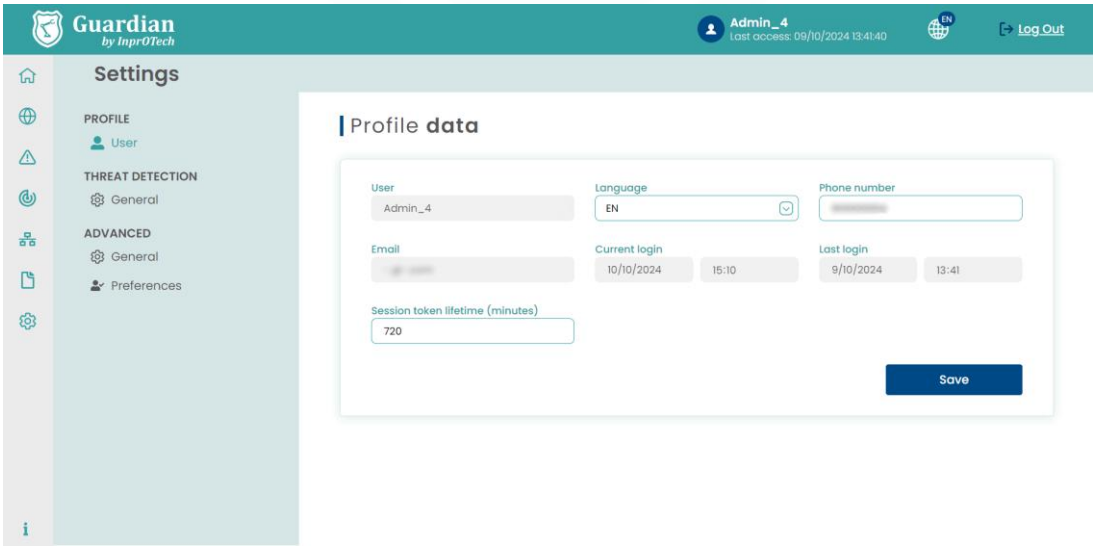
Last available reports

A list of the reports generated both manually and automatically with a certain periodicity, available for downloading, will be displayed on the screen.

4.7 Other settings

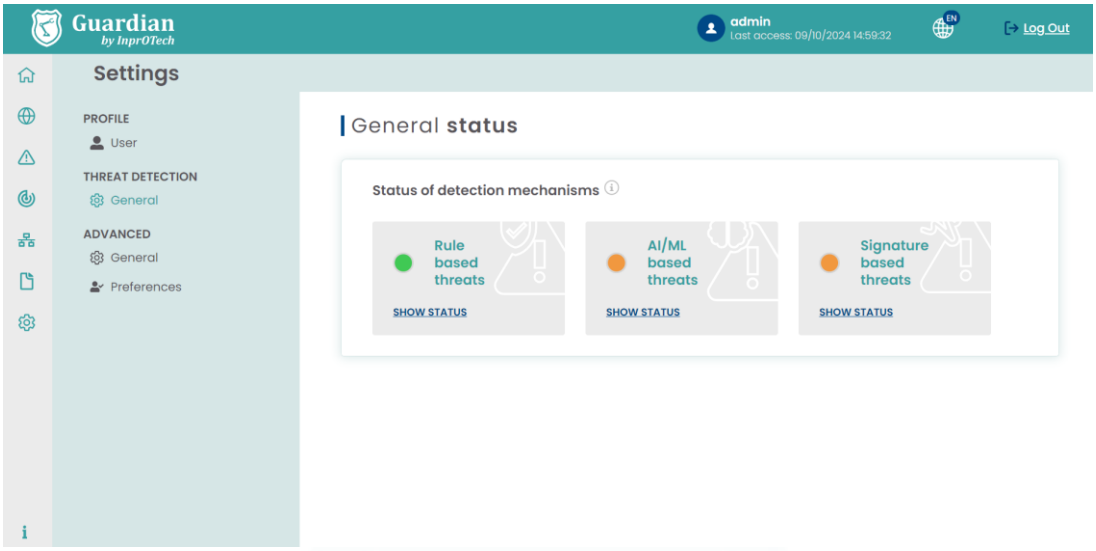
In configuration, different parameters of the Service can be customised.

In the user profile, there is all the information associated with the identity with which the system is accessed. Some of the fields can be edited, such as the language, the telephone number, and the duration of the session token in minutes:



Profile data screen.

In Threat Detection, the overall status of the different anomaly detection strategies is initially presented in traffic light mode (red, Orange, green):



Algorithm setting screen.

Rule-based threats

- Red: all rules are in training mode, inactive or not covered by their status field.
- Orange: some of the rules have production status, but not all of them.
- Green: all rules are in production mode.
- Grey: no rules exist.

AI/ML based threats

- Red: all rules are in training mode, inactive or not covered by their status field.
- Orange: some of the algorithms are in production mode, but not all of them.
- Green: all the algorithms are in production mode.
- Grey: No algorithms exist

Signature-based threats

- Red: all elements have a training value, inactive or some not covered in their status field.
- Orange: some of the elements have a value other than active, but not all of them.
- Green: all elements have a status equal to active and the signature_timestamp field is less than seven days old.
- Grey: no elements exist.

5 ANNEX I: Devices and alerts classification.

5.1 Devices classification

5.1.1 According to State

- **Authorized/Unauthorized**: Authorized devices are those that the customer has explicitly recognized as legitimate.
- **Critical/Non-critical**: The Guardian system will not actively interact with those devices marked as critical. E.g. old devices, unmanned for maintenance, no spare parts, etc.
- **Fixed/Not fixed**: Fixed devices will appear in the Guardian application even if they have not established any communication in the organization's network. E.g. devices temporarily isolated from the network for maintenance.

5.2 Alerts classification

5.2.1 According to State

- **Resolved/Unresolved**: Alarms marked as resolved are those that have been dealt with, but you want to maintain the occurrence of the alarm in future identical situations (same typology, MACs, IPs, and ports involved). Those not resolved are pending management.
- **Silenced/Unsilenced**: Alarms declared as silenced will not occur again in the same network context*. E.g. a device communicating with a public IP known and controlled by the organization, and you do not want alarms to be generated for this situation.

* It is worth mentioning that silenced alarms, although not displayed to the user, are still stored in a database for later consultation by InprOTech staff at the customer's request, if necessary.

5.2.2 According to Severity

The severity levels of the application in terms of alert generation are taken from RFC 5424, although they are not equivalent since the severity of the events has been catalogued based on the experience of our technicians.

From greater to lesser severity, alerts are classified as follows:

- Emergency

- Alert

- Critical

- Error

- Warning

- Warning

- Informational

- Debug

6 ANNEX II: Asset Icons and Purdue Level

The Purdue model defines the following levels for existing devices:

Level 0: Field devices, such as sensors or actuators.

Level 1: Basic controllers, PLCs, I/O devices, and the first layer of security.

Level 2: Monitoring, supervision, and representation devices (SCADA and HMI systems, interfaces, or historical data servers).

Level 3: Operations and systems management devices, such as database servers and MES. Real-time planning and production control.

Level 4: Enterprise management devices, such as ERP, CRM, or SCM systems.

Certain devices may change their Purdue level depending on their function and location.

Icon	Description	PURDUE Level
	PC	2
	SCADA	2
	DCS	2
	Virtual	2
	HMI	2
	TABLET	2
	VOIP PHONE	2
	SERVER	2

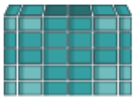
	HANDSET	2
	RTU	1
	VS-CAM	1
	BARCODE READER	1
	PLC	1
	ROBOT	0
	FREQUENCY VARIATOR	0
	CONTROLLER CARD	0
	SENSOR	0
	AFD	0
	SWITCH	Various
	ROUTER	Various
	FIREWALL	Various
	OTHER	Various
	HONEYPOT	Various

Table 1: Representative Icons of Devices

7 ANNEX III: Alert icons.

Icon	Description
	Manual alert
	Machine Learning alert
	Static rule alert
	IDS alert
	Alerta de Honeypot