



# InprOTech

*Smart security for your industry*

## User Manual InprOTech Guardian

Date: 07/2023

Doc Reference: IN-USer Manual InprOTech Guardian

Version: 0.11

*This document has been generated by **InprOTech** for the exclusive use of the **CLIENT** and its content is confidential. This document may not be disclosed to third parties, nor used for purposes other than those for which it was provided, without the prior written permission of **InprOTech**. In the case of delivery under a contract, its use and dissemination shall be limited to what is expressly authorized in the contract. **InprOTech** cannot be held responsible for any errors or omissions in the edition of the document.*

# INDEX

## 1 Content

---

<b>1 Introduction</b>	<b>4</b>
<b>2 First steps</b>	<b>5</b>
2.1 Web console access	5
2.2 Device list organization	6
2.3 Rules configuration	8
2.4 Settings	9
2.5 Reports configuration	9
2.6 Continuous dashboard (optional)	9
2.7 Alerts exportation (optional)	10
<b>3 Quick Guide</b>	<b>11</b>
3.1 Menu	11
3.2 Main Dashboard	12
3.3 Network Map	13
3.4 Device List	14
3.5 Alerts panel	15
3.6 Vulnerabilities	15
3.7 Communications List	16
3.8 Reports	16
3.9 Settings	19
3.9.1 User profile	20
3.9.2 Security	20
3.9.3 Alerts notification	21
3.10 Settings	22
3.11 Help	23
<b>4 Application management</b>	<b>23</b>
4.1 Main Dashboard	23
4.1.1 Actives summary	24
4.1.2 Quick links	24
4.1.3 Network traffic graph	25
4.1.4 Alerts graph	25
4.1.5 Last reports	26
4.2 Network map and device list	26
4.2.1 Network map	26
4.2.2 Device list	28
4.3 Alerts panel	31
4.4 Vulnerabilities	33



4.5 Communications	33
4.6 Reports	34
4.7 Settings	34
<b>5 ANNEX I: Devices and alerts classification</b>	<b>34</b>
5.1 Devices classification	34
5.1.1 According to State	34
5.2 Alerts classification	35
5.2.1 According to State	35
5.2.2 According to Severity	35
<b>6 ANNEX II: Asset Icons</b>	<b>36</b>
<b>7 ANNEX III: Alert icons</b>	<b>39</b>



# 1 Introduction

---

**InprOTech Guardian** is an asset discovery and anomaly monitoring and detection tool capable of identifying cybersecurity threats in industrial environments. It analyzes network traffic, identifies assets on the network, generates comprehensive reports, and raises alerts through the use of static rules, IDS signatures and artificial intelligence in order 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 of time 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 for identification and management. Including the identification and labelling of devices, or the inclusion of devices in the blacklist according to their criticality level...
- **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).
- **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.

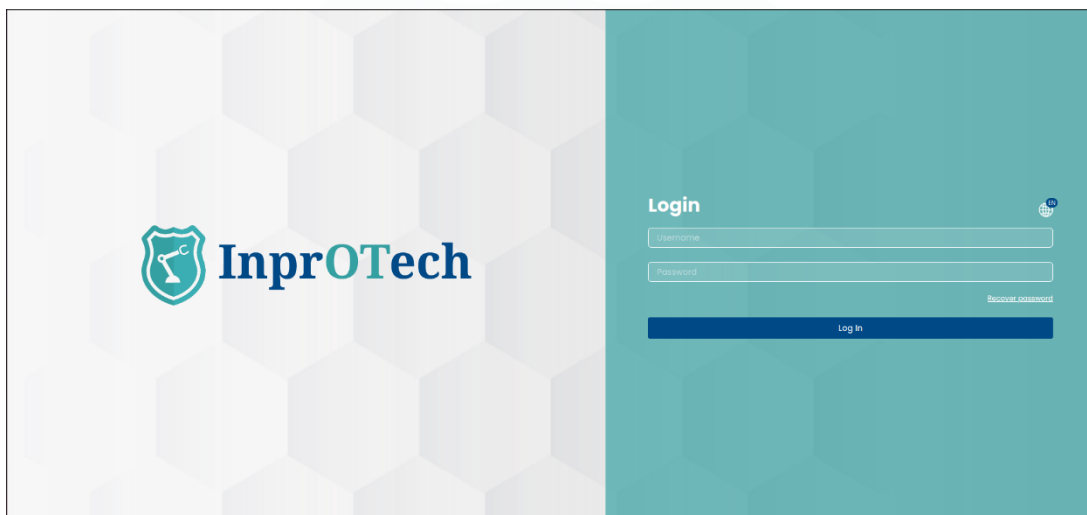
It is important to note that in addition to the use of the application itself, the service involves a series of preparations for onboarding, which include adequate data collection, deployment, installation, and fine-tuning of the solution to get the most out of it, based on actions such as those indicated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

## 2 First steps

---

### 2.1 Web console access

First, access the browser and enter the address [http://\[IP\]:9000](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 similar to 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

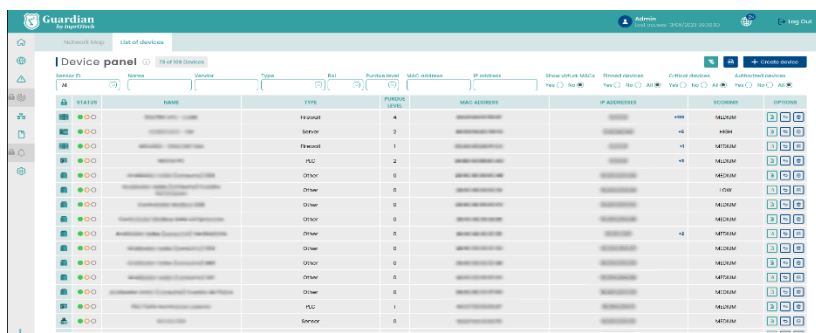
When entering the e-mail address, if valid, a link will be sent to the e-mail address to reset the access password by means of a one-time use token.

*\*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

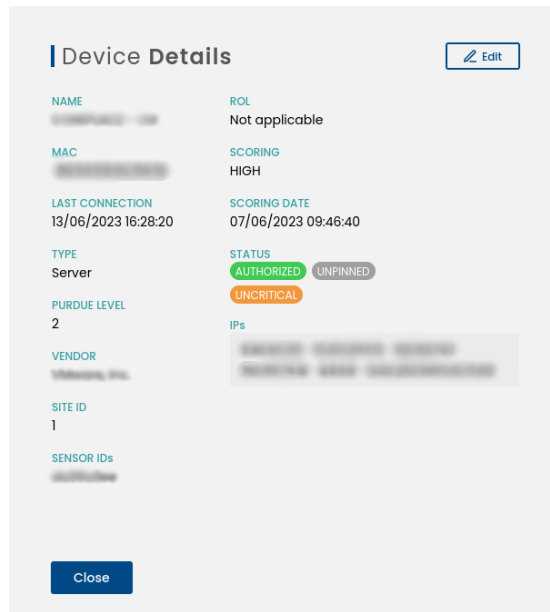
The list of devices must be organized by declaring the name of each device, as well as its PURDUE level and its status (See Annex I). By means of this declaration, the user will find it easier to identify each device in the different windows of the application, and thus be able to carry out operations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



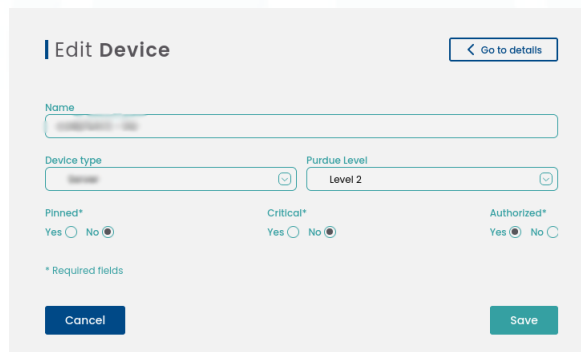
STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESS	SCORES	OPTIONS
●	...	Firewall	4	...	...	HIGH	[+][-]
●	...	Server	2	...	...	HIGH	[+][-]
●	...	Firewall	1	...	...	MEDIUM	[+][-]
●	...	PLC	2	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	LOW	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	Other	0	...	...	MEDIUM	[+][-]
●	...	PLC	1	...	...	MEDIUM	[+][-]
●	...	Server	0	...	...	MEDIUM	[+][-]

Device list screen



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

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

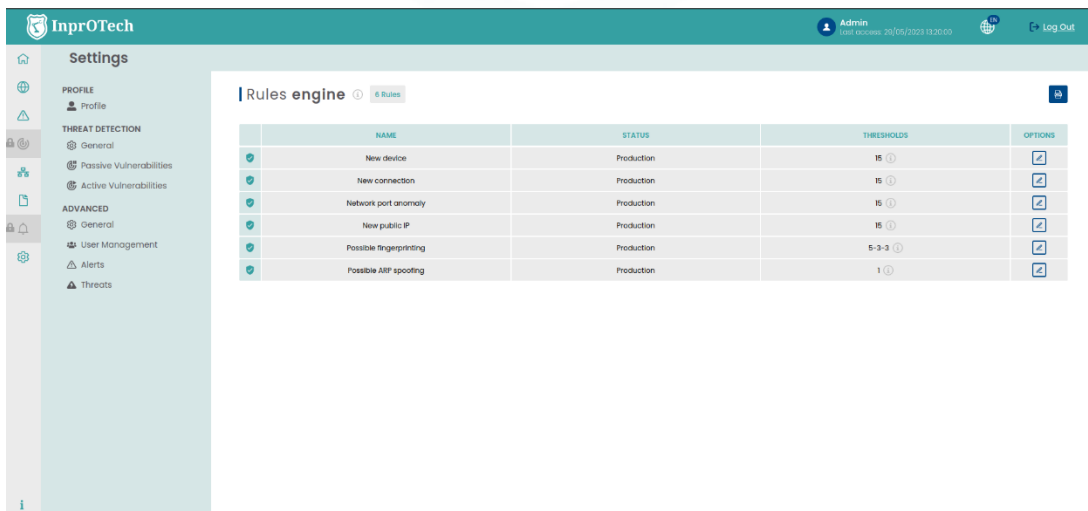
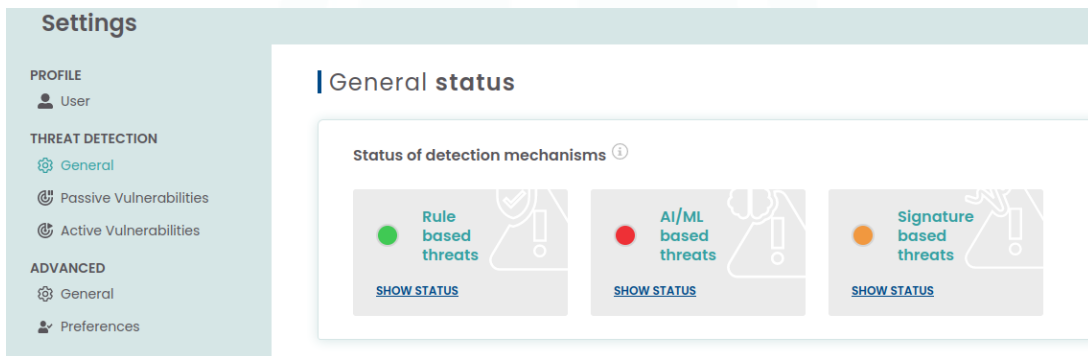
The Guardian system performs threat detection based on multiple behavioural criteria, such as:

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

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 period 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.



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



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

In the actions column we can edit these parameters.

### | Edit rule

**Threshold**

**Status**

\* Required fields

Cancel
Save

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

At the moment, 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.

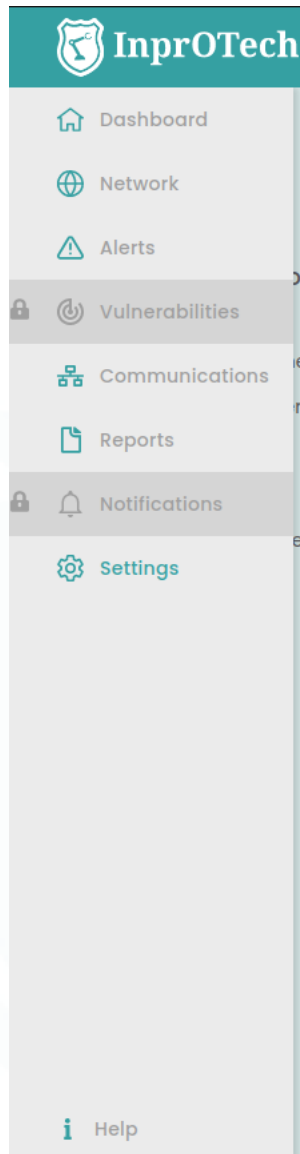
\* For this purpose it is important to note that all dates returned by the web application are shown in UTC time.



## 3 Quick Guide

---

### 3.1 Menu

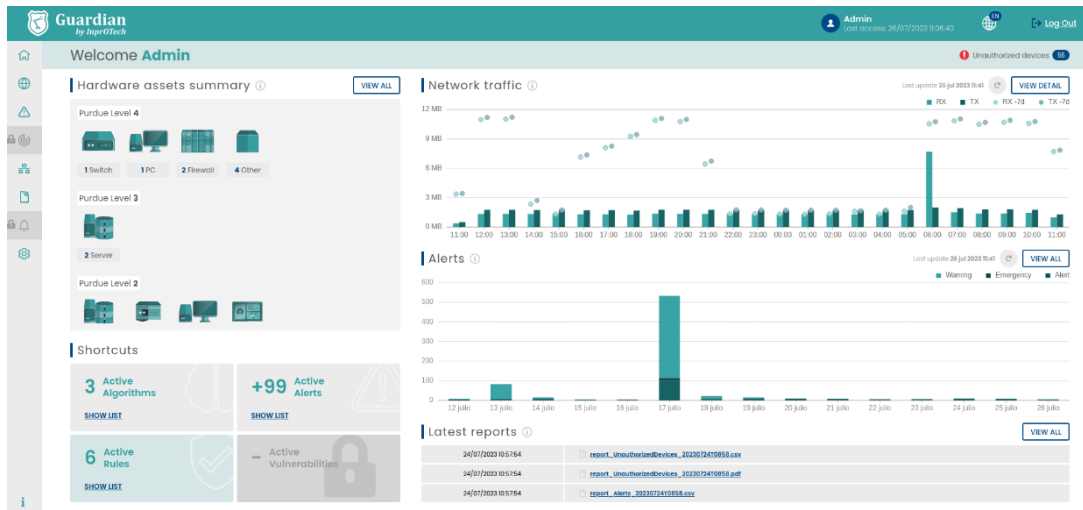


*Access window detail*

- 1: Home: Main Dashboard
- 2: Network: Network map and device list
- 3: Alerts: Alerts list
- 4: Vulnerabilities: List of vulnerabilities (under construction)
- 5: Traffic Sessions: List of inter-device communications
- 6: Reports: List of automatic reports
- 7: Notifications: Service notifications menu (under construction)

- 8: Settings: Parameters setting window
- 9: 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)

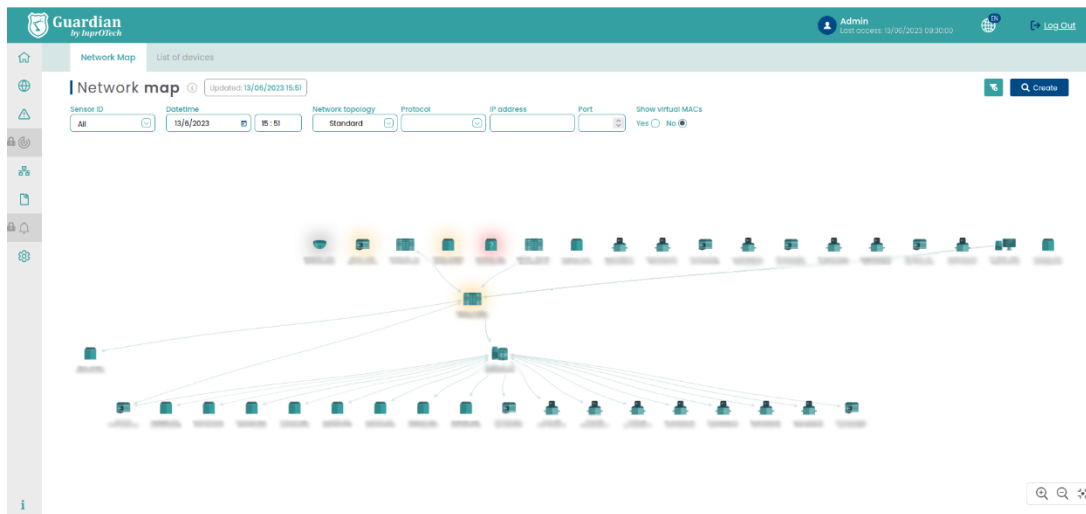
Bottom right widgets:

- 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).

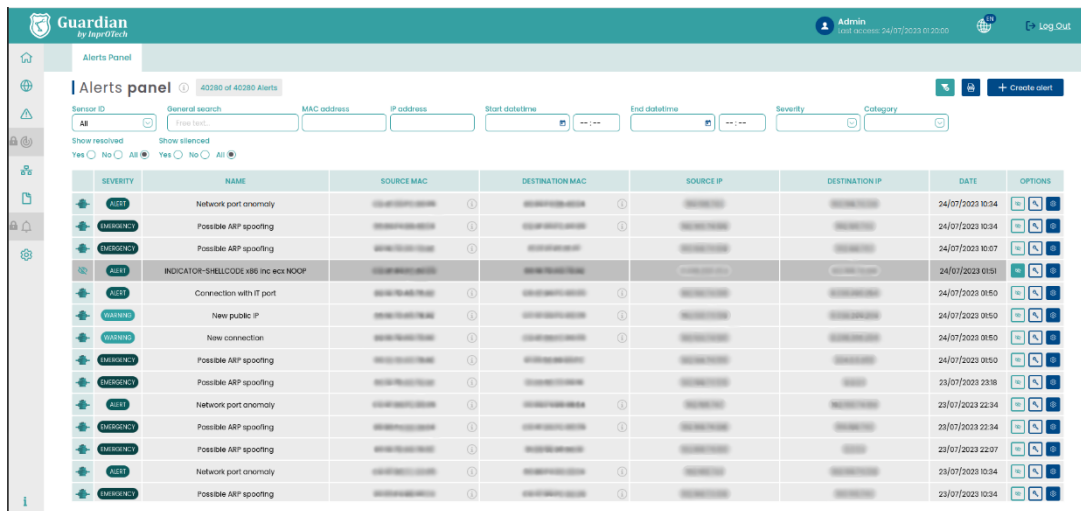


In the tab to select the view of the list of devices registered in the network, the number of devices with the current filter applied versus the total number of devices in the database is displayed next to the panel title. On the right side, the button panel for deleting previously applied filters, exporting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

Finally, 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.

### 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 also 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.

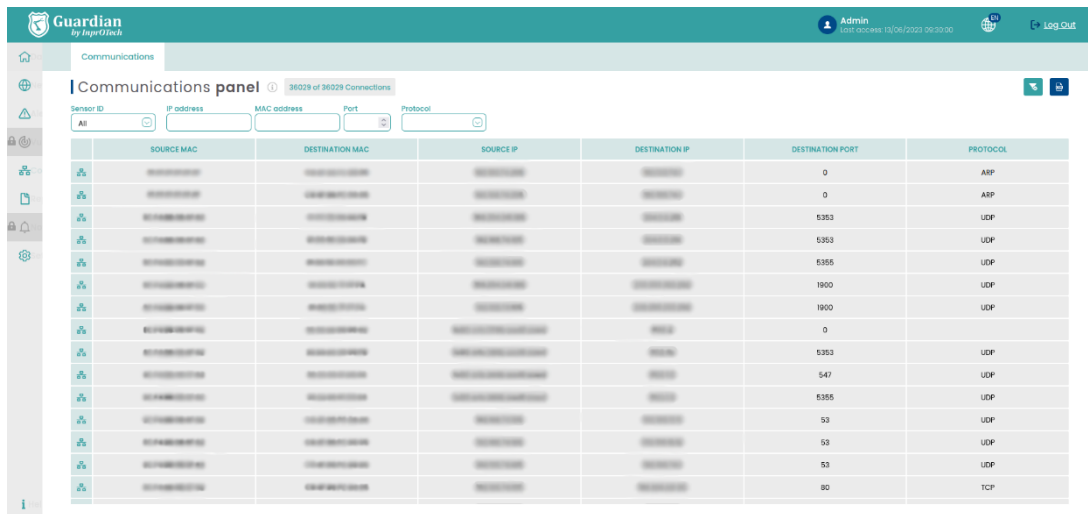
\*To check the status change options, see definitions in Annex I.

### 3.6 Vulnerabilities

(under construction)

### 3.7 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.



SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DESTINATION PORT	PROTOCOL
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	0	ARP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	0	ARP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	5353	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	5353	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	5355	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	1900	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	1900	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	0	
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	5353	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	547	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	5355	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	53	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	53	UDP
08:00:27:00:00:00	08:00:27:00:00:00	192.168.1.1	192.168.1.1	80	TCP

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.

### 3.8 Reports

This section will allow downloading reports of different types, automatically generated by the system. As of today, weekly reports are generated on Monday mornings, with downloadable files in both PDF and CSV format, with the following information:

- Last detected alerts:

- o ID
- o Title
- o Category
- o Severity
- o Silenced
- o Resolved
- o Value
- o Source IP



- o Source ID
- o Destination IP
- o Destination ID
- o Protocol
- o Creation date

\*\* In the Source ID and Destination ID fields, we can find one of these two types of information. Either the MAC address of the source/destination device, or we can see the name of the source/destination device of the alert, as long as we have this device stored in the database.

- Unauthorized connected devices: Every time Guardian detects a new device connected to the network, it generates an alert. The information displayed in this report is as follows:

- o Name: Name of the device
- o MAC of the device
- o Vendor : Manufacturer
- o Role: Role
- o Discovery date: Date of discovery

- MAC-IP associations seen on the network: The MAC address and its associated IP address have a relationship to each other.

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

- External IPs connected from the network : Public IPs contacted outside the network

- o Destination IP
- o Destination ID
- o Source IP
- o Source ID
- o Discovery date

- Network scoring (Network risk scores): This scoring will include an aggregated value at customer level, as well as a comparison with another indicator at cluster level in case of cloud architecture.

o Aggregated customer scoring: Scoring of the customer network.

o Overall cluster scoring: Overall scoring of all Guardian customers in the DDBB.

o Individual scoring per device (Individual device scoring):

- Name: Device name
- MAC: MAC of the device
- Vendor: Manufacturer
- Score
- Calculation date: Date on which the scoring is performed.

\*\* In addition, the following information section will appear:

Info: scoring is not a measure of risk, but a representation of the device criticality level according to a proprietary algorithm based on network topology, communications and alerts. Individual values are indicated per node (LOW, MEDIUM, HIGH), aggregated at client level, and compared to other clients in the same cloud cluster, if with other clients of the same cloud cluster, and if applicable (in both cases on a scale from 0 to 10, with 10 being the maximum criticality).

- Technical key performance indicators report:

o Nodes and routing.

- Total devices: Total devices detected
- Unauthorized devices: Unauthorized devices detected
- Devices unavailable/disabled: Unavailable/disabled devices
- New IPs detected: New IPs detected.

o Traffic:

- Open communication sessions: Open communication sessions.

o Threats:

- Average number of daily alerts: Average number of daily alerts
- Average number of alerts per device: Average number of alerts per device
- Number of intrusion attempts: Number of intrusion attempts

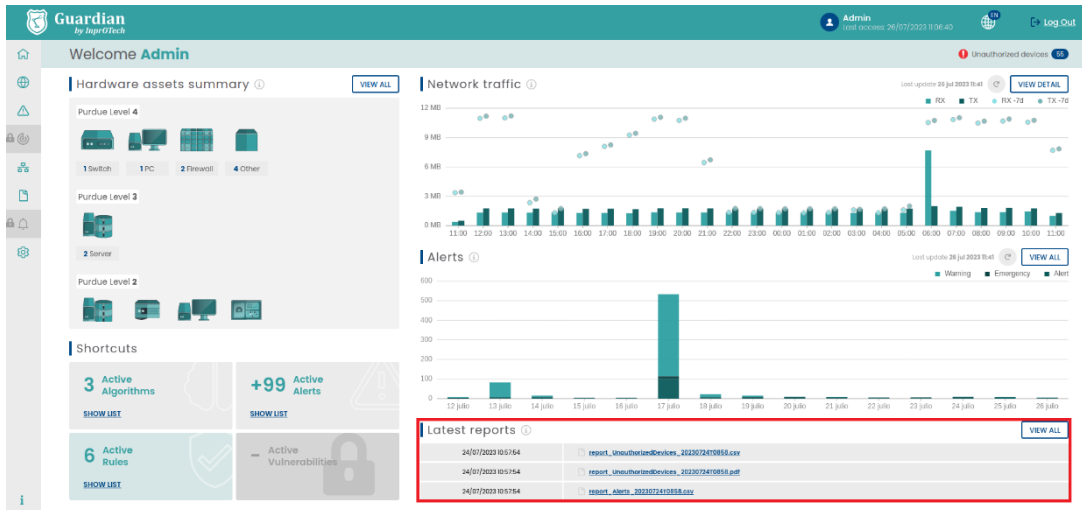
o Top 5 protocols

o Top 5 IPs

o Top 5 ports

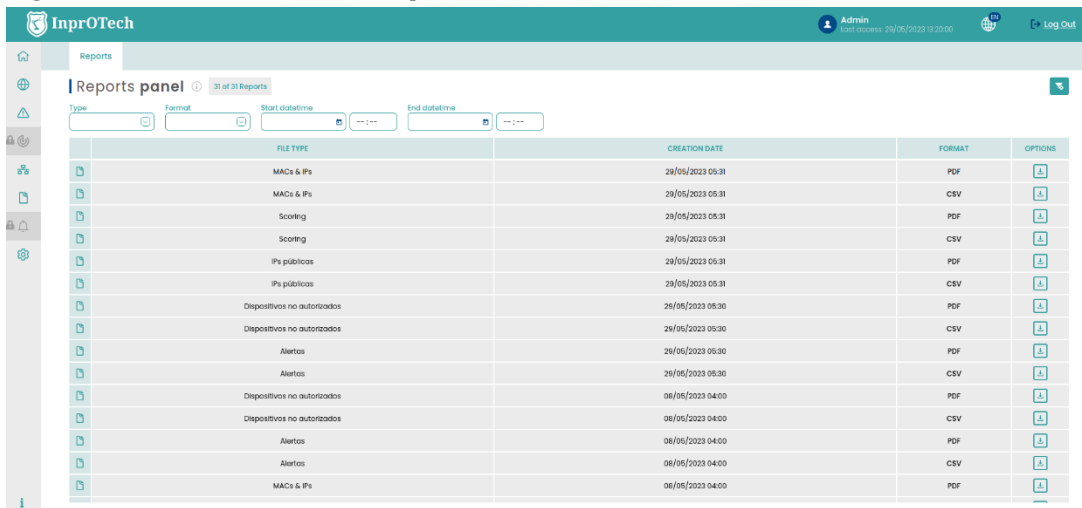
The MAC field in the alert report, in case the device has the label Name reported, will be replaced by that value in these reports. On the other hand, in manual downloads of user searches from the alerts panel or the device list, both fields will be displayed independently.

The latest generated reports can be downloaded 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 in PDF and CSV for downloading.

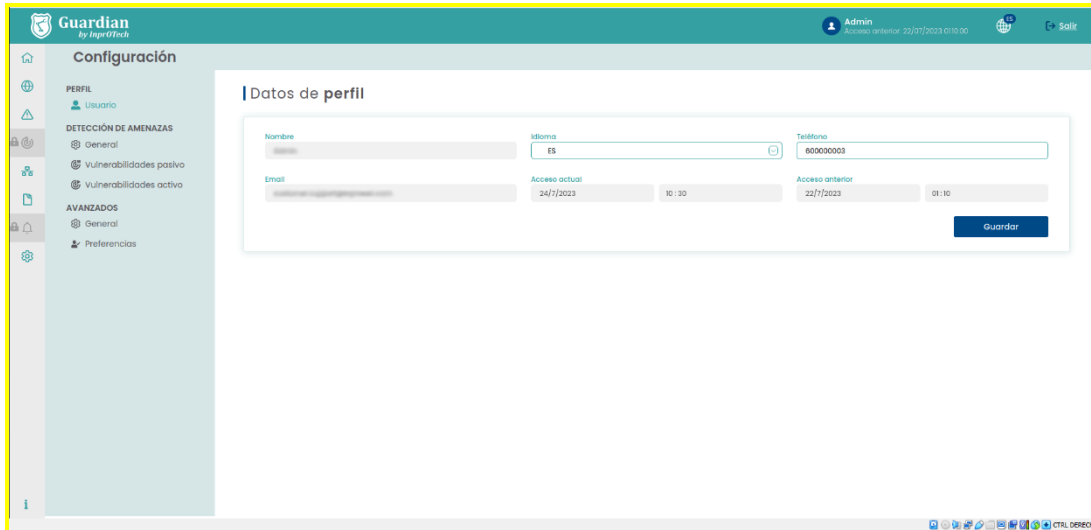
### 3.9 Settings

In this section we can make adjustments to 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.

### 3.9.1 User profile

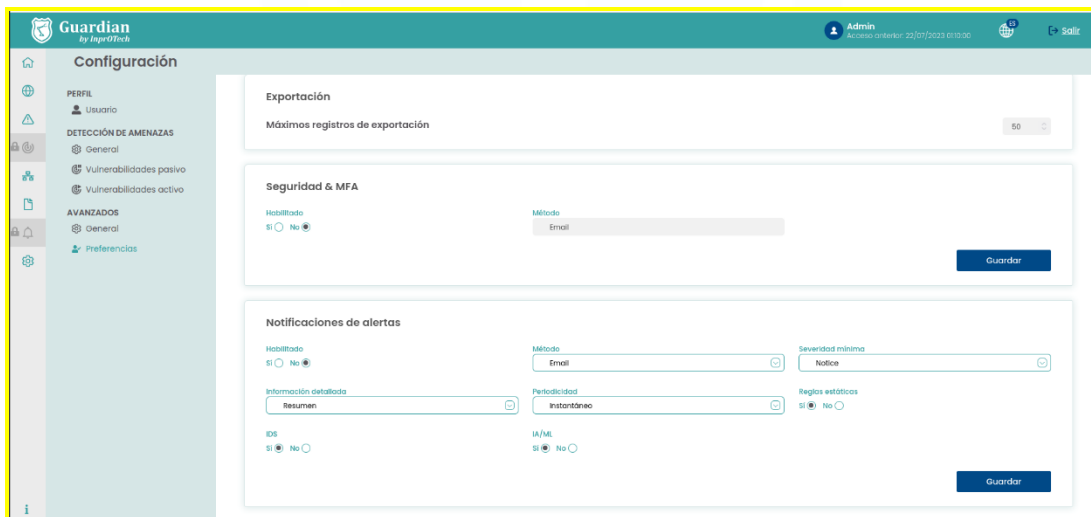
This section displays basic information such as user name, associated email, date and time of last and current connection, language preference (EN/ES), and contact telephone number. The last two are editable by the user.



User profile view

### 3.9.2 Security

In the 'Security & MFA' section, we can indicate whether or not 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.

### 3.9.3 Alerts notification

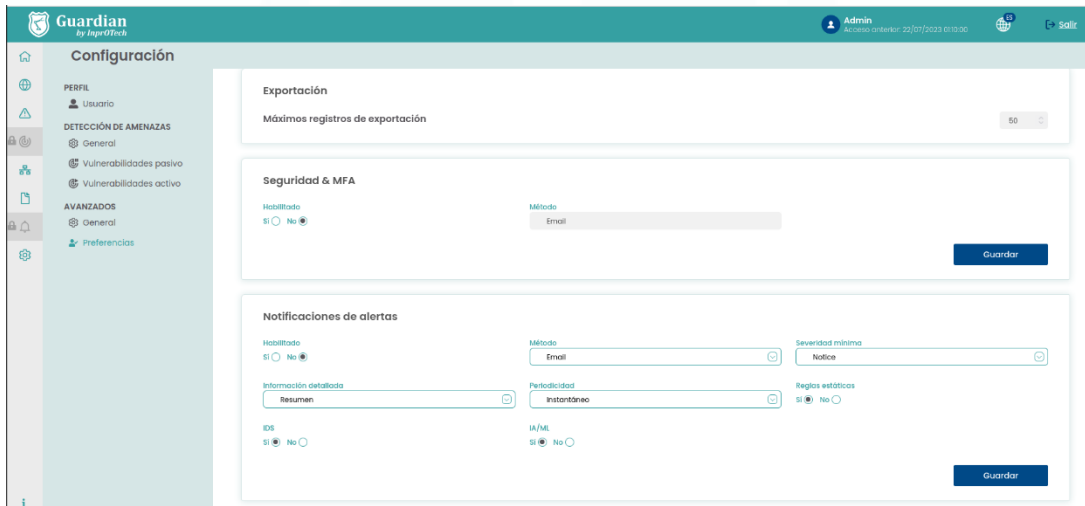
In case it is considered appropriate, proactive alerts can be configured to generate alerts in the system. The alerts and warnings are generated based on the detection of anomalies according to the different strategies implemented in Guardian (heuristics, IA/ML, IDS, manuals...).

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, all...)
- In what format
  - o Individual: one notification per alert
  - o 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.



The screenshot shows the 'Configuración' (Configuration) page in the Guardian web interface. The left sidebar contains navigation options: PERFIL (User), DETECCIÓN DE AMENAZAS (General, Vulnerabilities pasivo, Vulnerabilities activo), AVANZADOS (General, Preferencias), and a search icon. The main content area is divided into three sections:

- Exportación:** 'Máximos registros de exportación' set to 50.
- Seguridad & MFA:** 'Habilitado' (Enabled) with radio buttons for 'SI' (selected) and 'No'. 'Método' (Method) is set to 'Email'.
- Notificaciones de alertas:** 'Habilitado' (Enabled) with radio buttons for 'SI' (selected) and 'No'. 'Método' (Method) is 'Email'. 'Severidad mínima' (Minimum severity) is 'Notice'. 'Información detallada' (Detailed information) is 'Resumen' (Summary). 'Periodicidad' (Periodicity) is 'Instantáneo' (Instantaneous). 'Reglas estáticas' (Static rules) has radio buttons for 'SI' (selected) and 'No'. There are also checkboxes for 'IDS' and 'IA/ML', both currently unchecked.

Each section has a 'Guardar' (Save) button at the bottom right.

*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 sendings.
- 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:

**SG Soporte Guardian Para** 11:20

**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**

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
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	1	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	1	New connection discovered	NA
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	17	New device discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	17	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	17	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	17	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New public IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	Connection with public IP (source IP: [redacted])	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New connection	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New connection discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New device discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New device discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:56 +0000	STATIC	New device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New device discovered	[redacted]
15/10/2018 06:44:55 +0000	STATIC	New IP	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New IP discovered	[redacted]
15/10/2018 06:44:55 +0000	STATIC	New device	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	sonda1	6	New device discovered	[redacted]

Grouped daily alert notification example

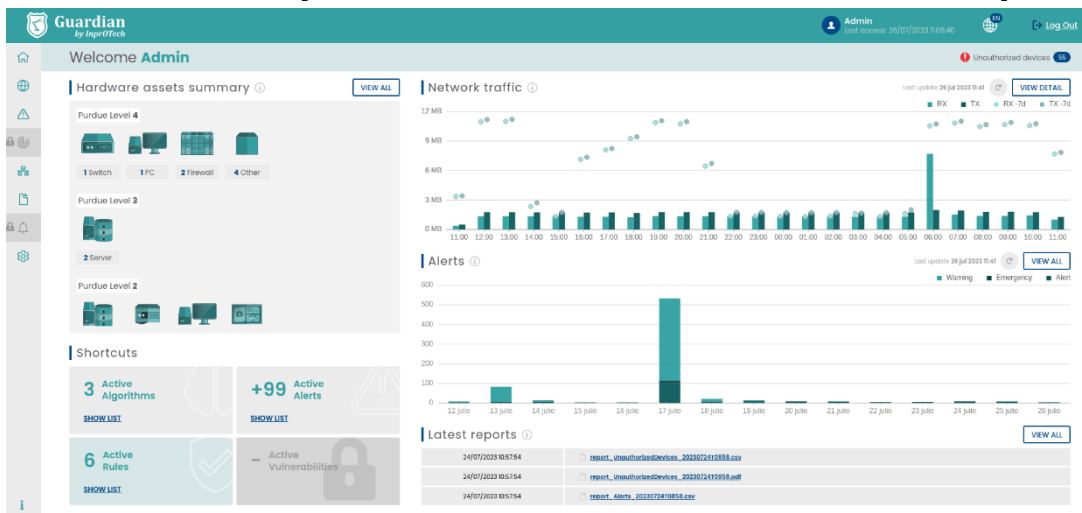
### 3.10 Settings

In this section we can make adjustments to 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.

### 3.11 Help

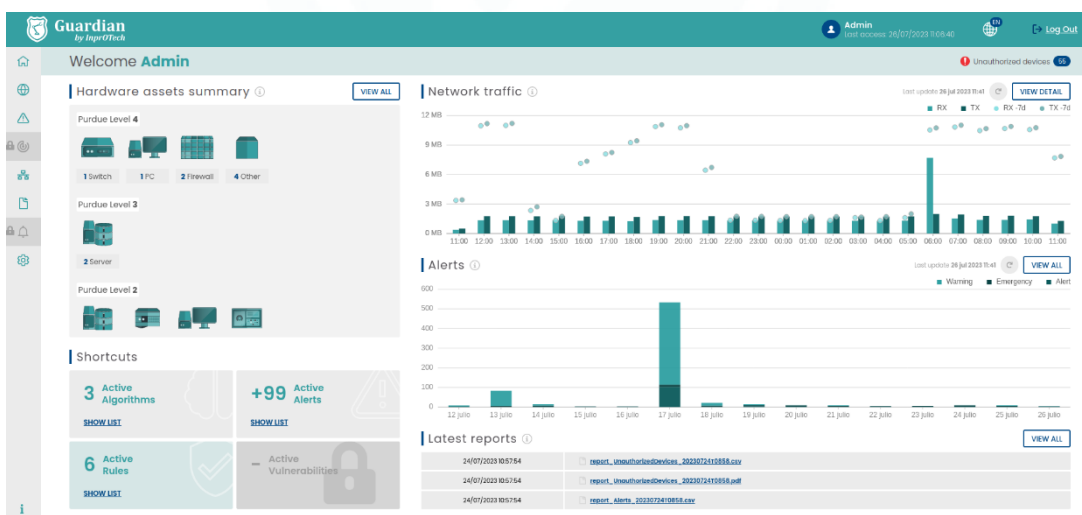
Section that enables the download of the latest version of the InprOTech Guardian user manual. Leads to the InprOTech website, where the relevant documentation is posted.



Access to the documentation is in the lower left corner. For any technical issue, please contact [customer.support@inprosec.com](mailto:customer.support@inprosec.com).

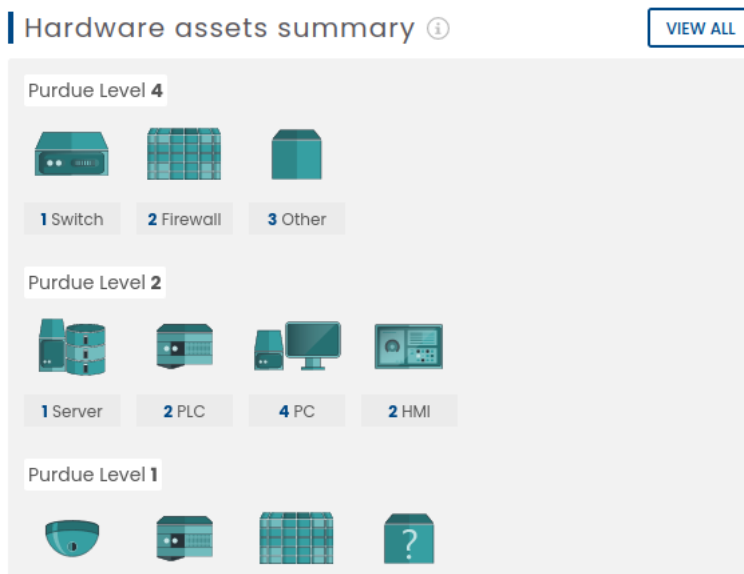
## 4 Application management

### 4.1 Main Dashboard



Dashboard

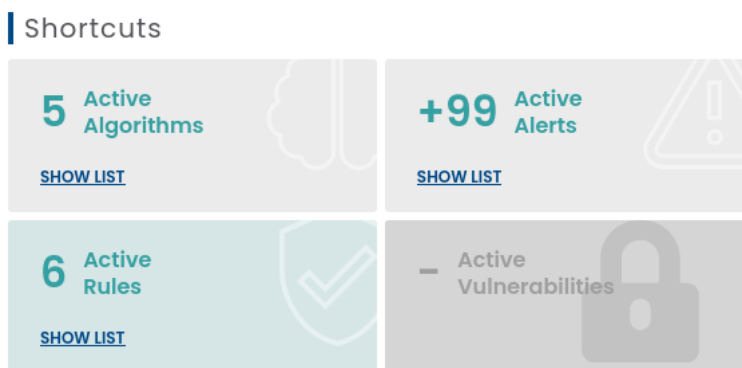
### 4.1.1 Actives summary



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, 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).

#### 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.



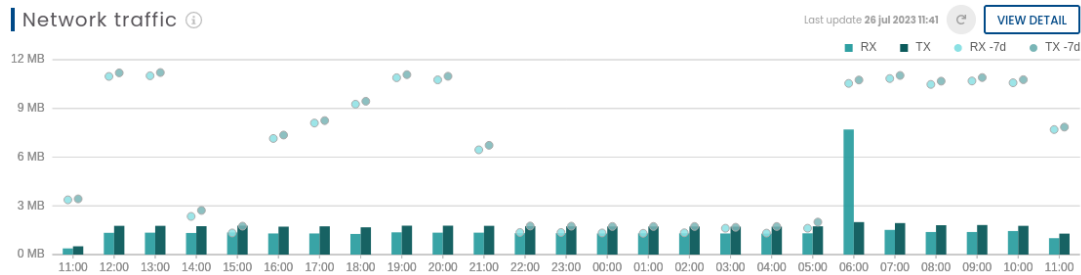
#### 4.1.2.3 Active Rules

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).

#### 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

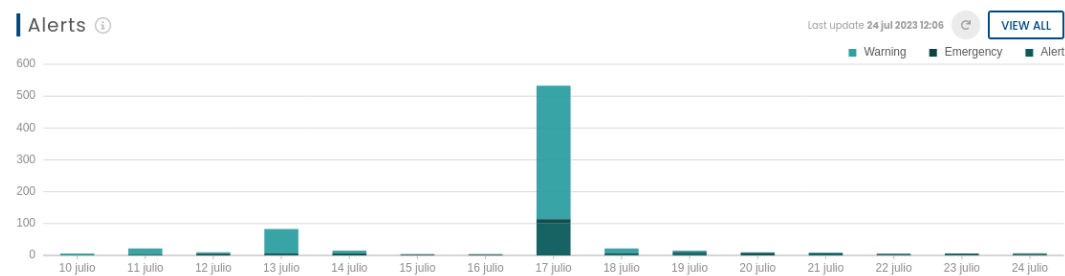


Network traffic

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



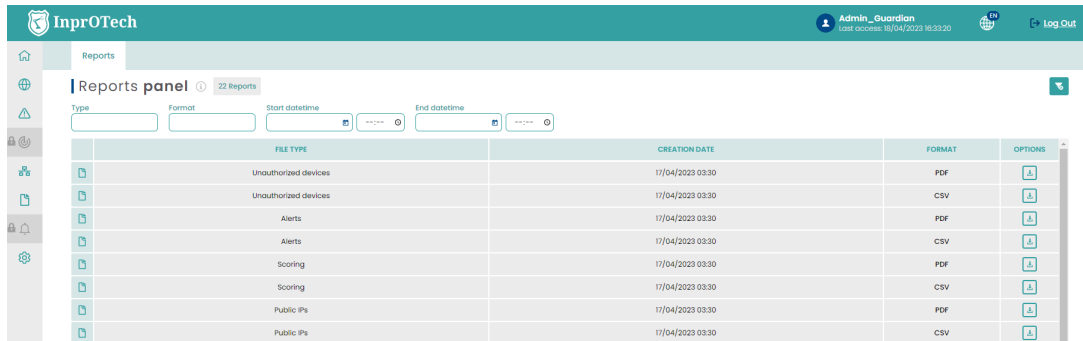
Alerts

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



*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.

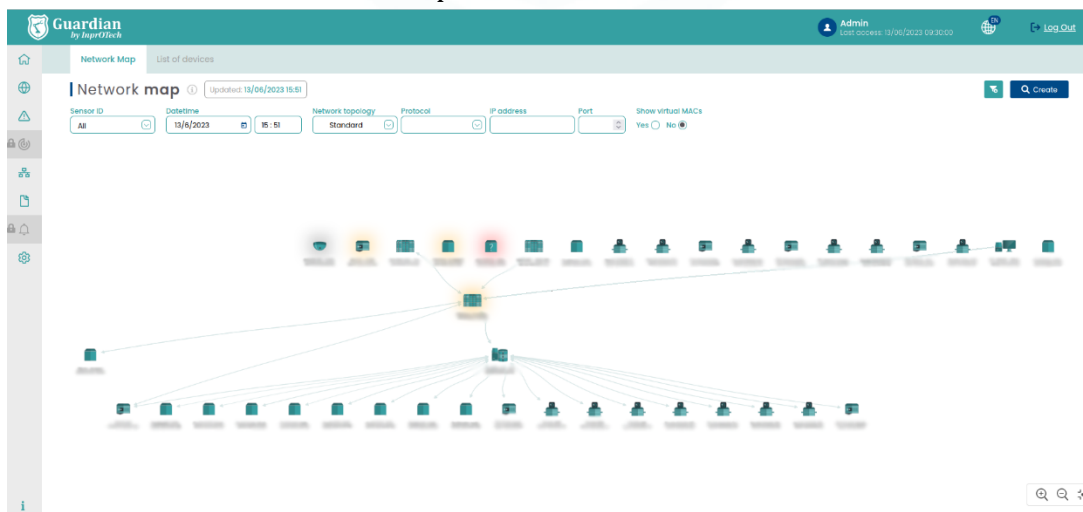
Currently, the reports generated on a weekly basis are:

- 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.

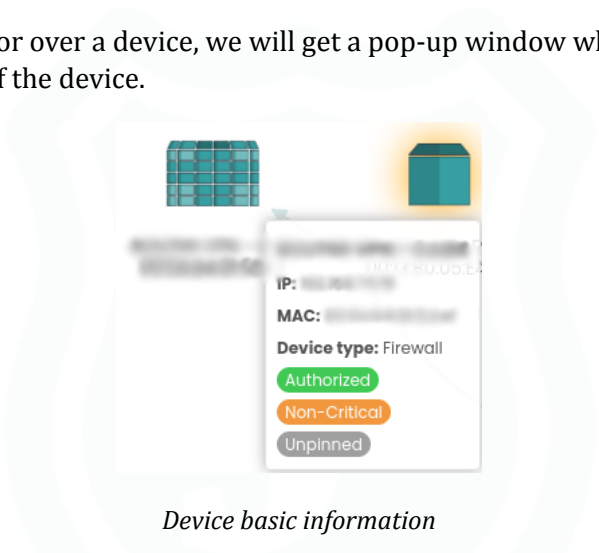
The icons represented will correspond to those described in Annex II.

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*

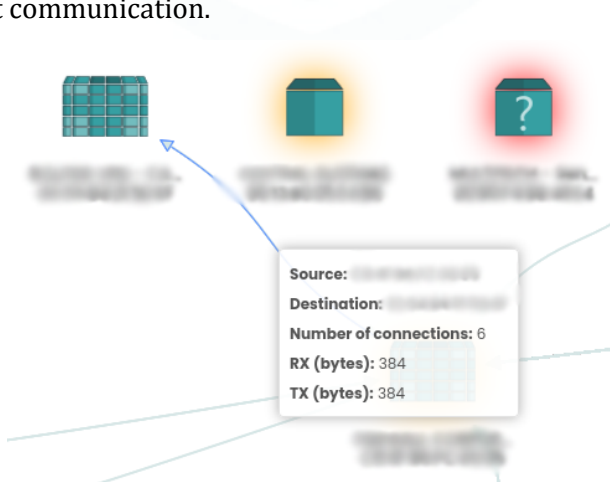
If we place the cursor over a device, we will get a pop-up window where we will see the basic information of the device.



*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.




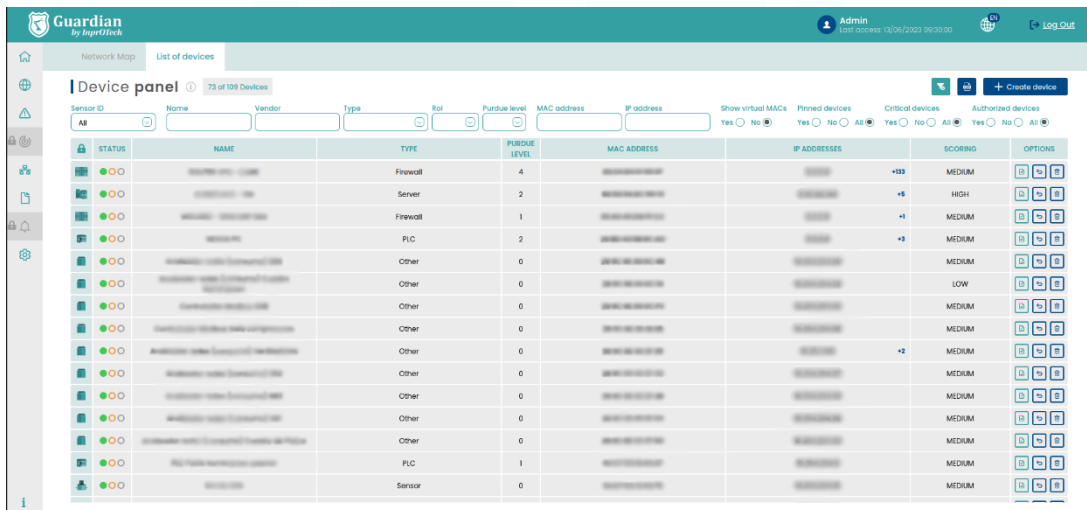
Available filters in network map

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

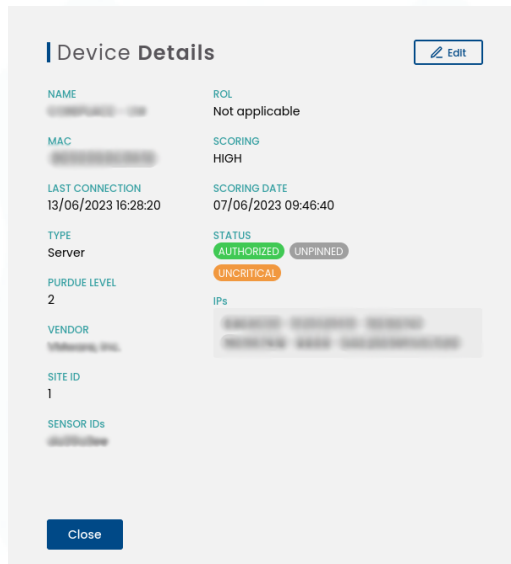
A list of all the devices present in the organization will be displayed along with their information in a more expanded form:

- STATUS


o The first of the circles will indicate whether the device is authorized (green colour) or unauthorized (red colour).

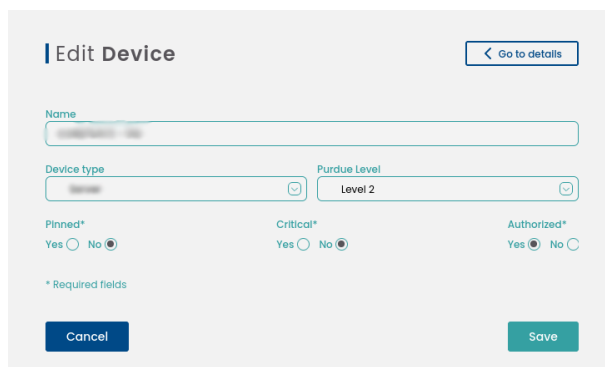
- o The second of the circles will indicate whether the device is critical (orange colour with fill) or non-critical (orange colour without fill).
- o The third circle indicates whether the device is fixed (grey colour with fill) or not fixed (grey colour without fill).
- NAME: Name assigned to each device.
- TYPE: Differentiation of the type of device (PLC, RTU, SCADA, 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.
- ACTIONS:

: Button to view device information in detail.




*Device details*

: Button to modify device parameters.



*Device 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 we are interested in.




### Device filtering

This filtering can be performed according to:

- Probe ID, to filter by zone of the industrial network and/or headquarters.
- Device name
- Device manufacturer
- Device Type (PLC, RTU, SCADA, 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
- Fixed devices, see Annex I
- Critical devices, see Annex I
- Authorized devices, see Annex I

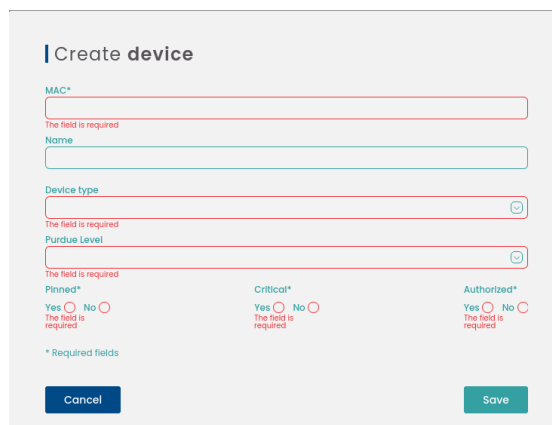
Pressing the button  will reset the filtering values and the complete list with all devices will be displayed again.

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

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:

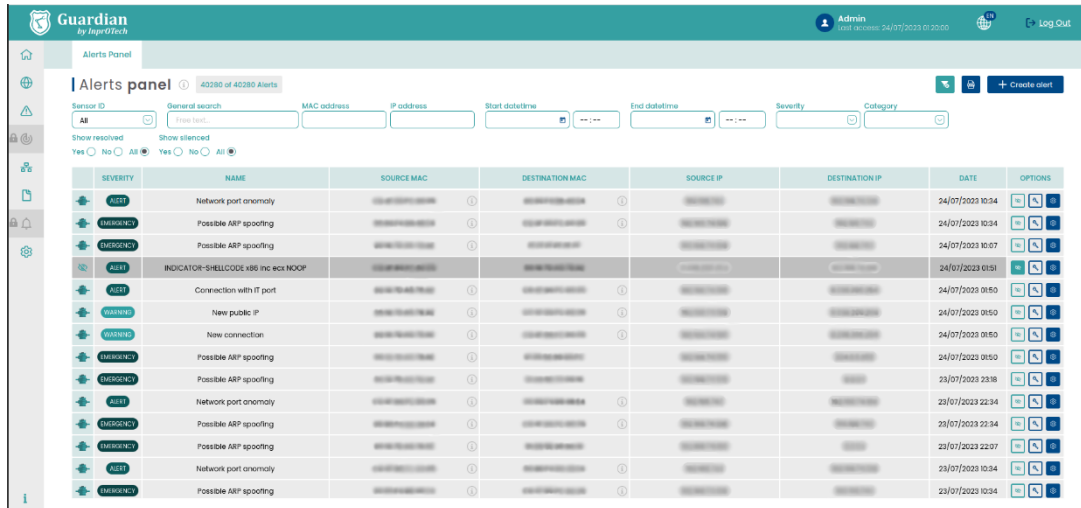


*Available fields to create a device*

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

### 4.3 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.

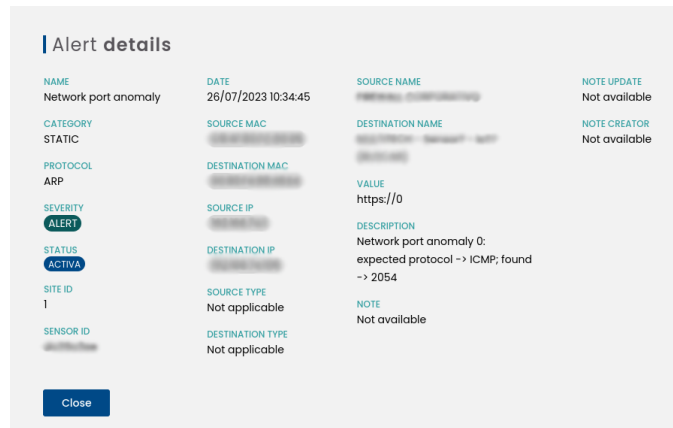
- Severity: Classification of the alert according to the impact it could have on the organization.
- Name: Defined name of the alert.
- Source MAC: MAC of the alert generating device.
- Destination MAC: MAC of the device to which the action was directed.
- Source IP: IP of the device generating the alert.
- 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.




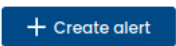
*Available alert filters*

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:

**Create alert**

Title\*  The field is required

Source IP

Destination IP

Source MAC

Destination MAC

Protocol

Description\*  The field is required

Severity\*  The field is required

Date

Value

\* Required fields

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.

#### 4.4 Vulnerabilities

To access the list of vulnerabilities, the user must click on the icon that appears on the left side of the screen. (under construction)

#### 4.5 Communications

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

SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DESTINATION PORT	PROTOCOL
...	...	...	...	0	ARP
...	...	...	...	0	ARP
...	...	...	...	5353	UDP
...	...	...	...	5353	UDP
...	...	...	...	5355	UDP
...	...	...	...	1900	UDP
...	...	...	...	1900	UDP
...	...	...	...	0	...
...	...	...	...	5353	UDP
...	...	...	...	547	UDP
...	...	...	...	5355	UDP
...	...	...	...	53	UDP
...	...	...	...	53	UDP
...	...	...	...	80	TCP

### 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.

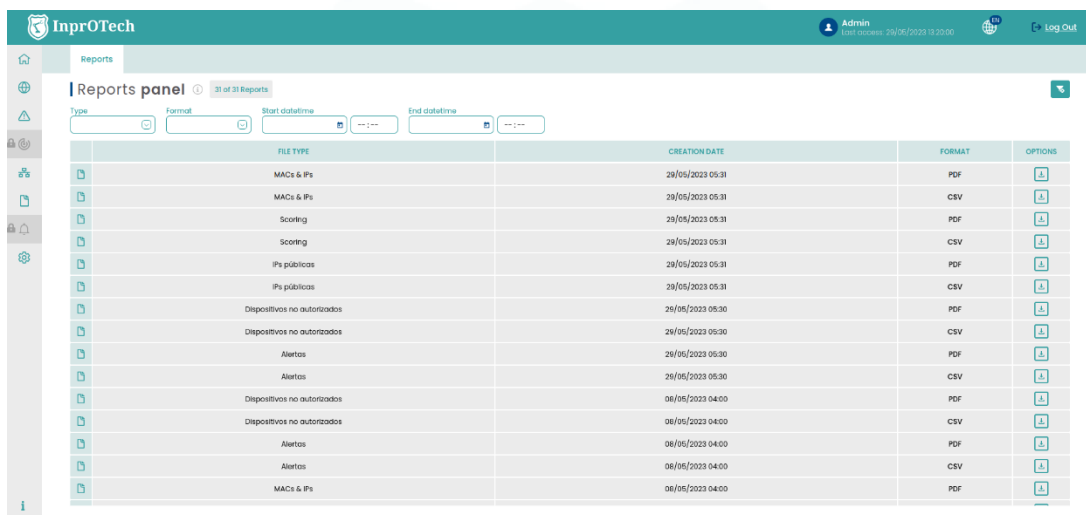
A communication is understood as the grouping of connections between MAC, IP and source port, and the same for the destination. It is considered a new communication if there is a change of protocol.



### 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 Settings

Check the section of the same name in the Quick Guide above.

# 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. very 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.





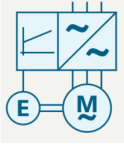


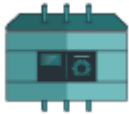



From greater to lesser severity, alerts are classified as follows:


- Emergency
- Alert
- Critical
- Error
- Warning
- Warning
- Informational
- Debug



## 6 ANNEX II: Asset Icons

Icono	Descripción	Nivel PURDUE
	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
---	-------	---------

*Tabla 1: Iconos representativos de dispositivos*



## 7 ANNEX III: Alert icons

Icono	Descripción
	Manual alert
	Machine Learning alert
	Static rule alert
	IDS alert