



InprOTech

Smart security for your industry

User Manual InprOTech Guardian

Date: 06/2026

Doc Reference: IN-User Manual InprOTech Guardian

Version: 0.18

*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	Introduction.....	4
2	First steps	5
2.1	Web console access	5
2.2	Device list organization	7
2.3	Analysis of Wireless devices	9
2.4	Rules configuration.....	10
2.5	Settings	12
2.6	Active device scanner (optional)	12
2.7	Active response configuration	13
2.8	Reports configuration.....	13
2.9	Alerts exportation (optional)	13
2.10	Continuous dashboard (optional).....	13
2.11	Licences.....	13
2.12	Access control and roles	14
2.13	Customized Fields.....	15
3	Quick Guide.....	15
3.1	Menu	15
3.2	Main Dashboard	17
3.3	Network Map.....	19
3.4	Device List	20
3.5	Alerts panel.....	22
3.6	Communications List	22
3.7	Reports.....	23
3.8	Settings	26
3.8.1	Users profile.....	26
3.8.2	Users preferences	27
3.8.3	Alerts notification.....	28
3.8.4	Users Management.....	29
3.8.5	Traffic Blocking Configuration	30
3.9	Info.....	31
4	Application management.....	32
4.1	Main Dashboard.....	32
4.1.1	Actives summary.....	32
4.1.2	Quick links	33
4.1.3	Network traffic graph.	34

4.1.4	Alerts graph.....	34
4.1.5	Last reports	35
4.2	Network map and device list	36
4.2.1	Network map.....	36
4.2.2	Device list.....	38
4.3	Alerts panel.....	47
4.3.1	Public IP	49
4.3.2	Ip Reputation and Blocking Policy.....	50
4.3.3	IP whitelist.....	53
4.4	Vulnerability analysis	54
4.4.1	Vulnerabilities Panel	54
4.4.2	Device statistics	57
4.4.3	Global statistics.....	57
4.5	Communications.....	57
4.6	Reports.....	58
4.7	Other settings.....	58
5	ANNEX I: Devices and alerts classification.....	61
5.1	Devices classification	61
5.1.1	According to State.....	61
5.2	Alerts classification.....	61
5.2.1	According to State.....	61
5.2.2	According to Severity	61
6	ANNEX II: Asset Icons and Purdue Level.....	62
7	ANNEX III: Alert icons	64

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, Spanish, Catalan, Vasque, and Galician.

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.
- **Public IP reputation:** In case of connections to public IP addresses, their reputation will be automatically analyzed, visually highlighting those for which active mitigation action is recommended. The user will have the possibility to upload a list of IPs that will always be allowed.

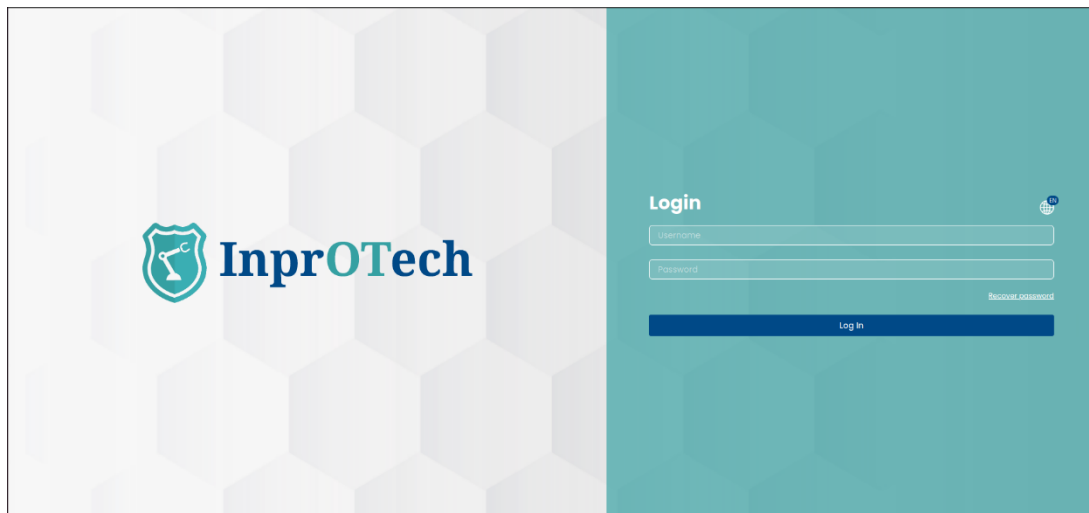
- **Communications list:** List with all the communications that have been made between OT devices in the organization's network, and information about them.
- **Report generation:** Compilation of information about the network, devices, indicators, etc., for future analysis and verification at both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

The user must authenticate by entering the username and password assigned to them. In case of having the second authentication factor activated, they must additionally enter the single-use token received via email in their user email account of the service.

For security reasons, when a user logs in for the first time, or when an administrator has marked the account to require a password change, the system will automatically display the "Change Password" screen before allowing access to the application.



Mandatory password change screen

On this screen, the user must:

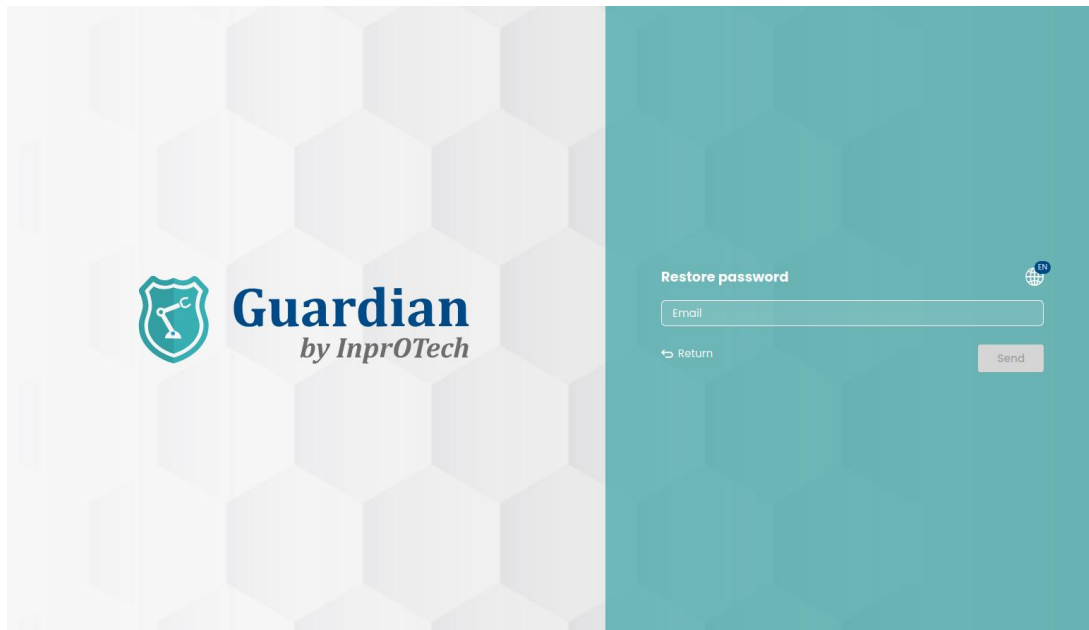
1. Enter the new password in the first field.
2. Confirm the new password in the second field.
3. Click the "Change Password" button to complete the process.

Once the password has been successfully changed, a confirmation message will be displayed, and the user will be granted access to the application. If two-factor authentication is enabled, the user must also enter the verification code received via email.

The user can be:

- **Administrator:** Will have access to all the information presented by the application and will be able to make the configurations they deems appropriate for algorithms, factory Ids, production modes, etc.
- **Operator:** Access like the previous case, except for the specific configuration part mentioned above.
- **Monitor:** Exclusive reading permissions user. They 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 their password, they will have the option to recover it by clicking on the "I forgot my password" option.

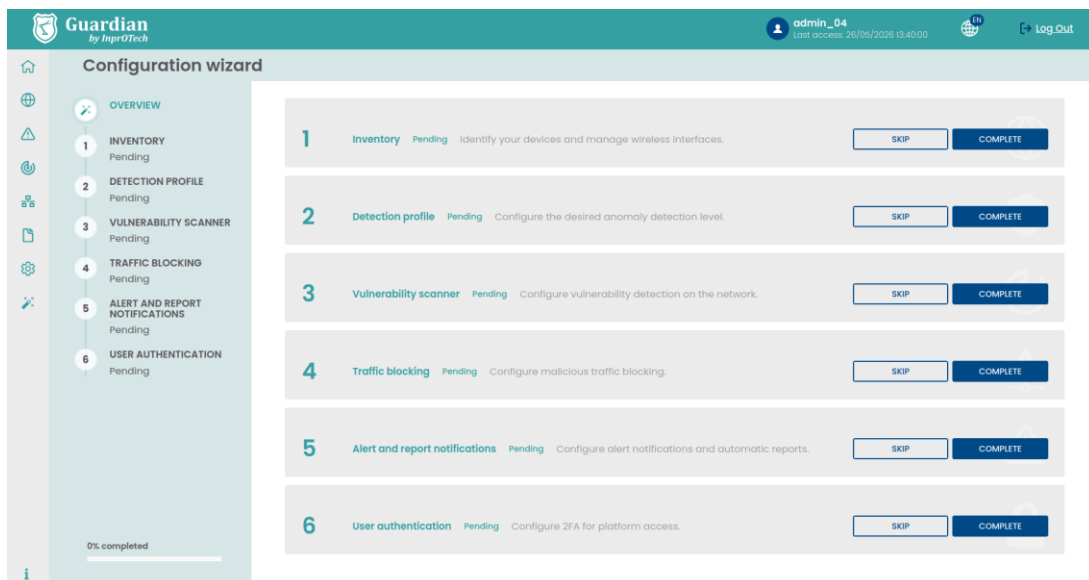


Password recovery screen

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.*

When you log in for the first time, the Guardian setup wizard will open. Here, the user will be guided through the initial configuration of the solution. It will be divided into six stages, each of which must be completed (or, alternatively, skipped).



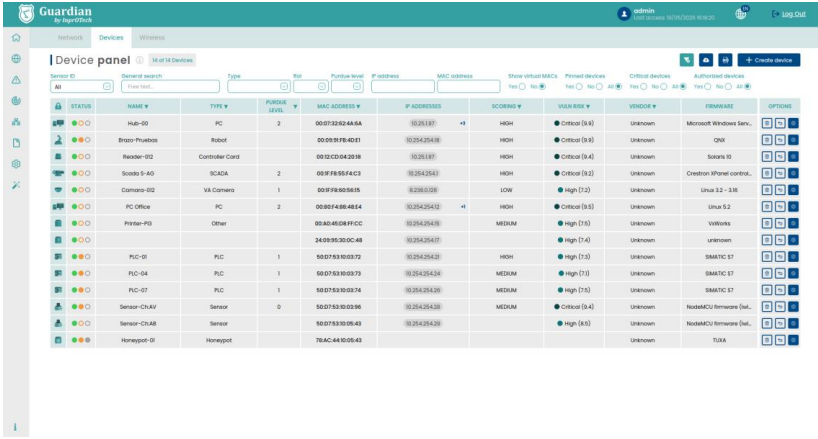
2.2 Device list organization

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.

In the first stage of the wizard, a panel is displayed summarizing the number of unidentified devices currently present.

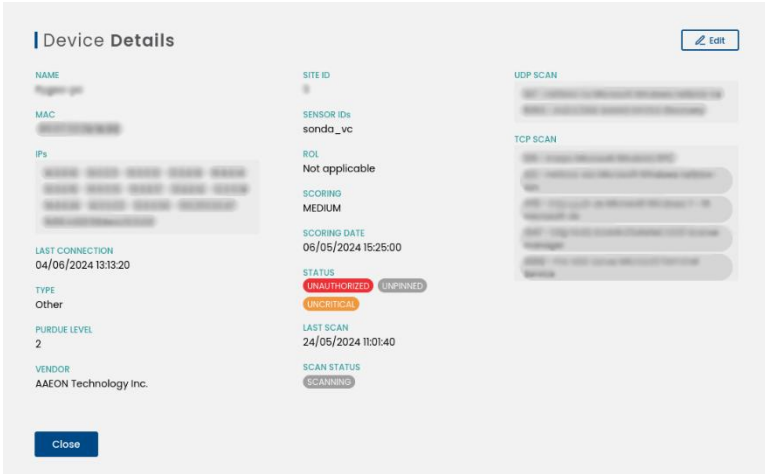
The user should navigate to the device list by clicking on the counters in the wizard. This will take them to the device list already filtered to show those devices pending identification. Alternatively, by clicking on the  icon and selecting the “Device List” tab, it can also be accessed.



STATUS	NAME	TYPE	PURPOSE	MAC ADDRESS	IP ADDRESS	SCORING	Vendor	REMARKS	OPTIONS
Unidentified	Hub-00	PC	2	00:07:2D:62:AA:6A	10.254.254.1	HIGH	Critical (S 5)	Microsoft Windows Serv...	[Edit] [Delete]
Unidentified	Bravo-Phonics	Robot		00:09:5F:FB:4D:01	10.254.254.10	HIGH	Critical (S 5)	QNX	[Edit] [Delete]
Unidentified	Reader-02	Controller Card		00:0C:0D:04:20:38	10.254.254.1	HIGH	Critical (S 4)	Solaris 10	[Edit] [Delete]
Unidentified	Scada-5-A0	SCADA	2	00:0F:FB:85:5F:43	10.254.254.1	HIGH	Critical (S 2)	Crestron XPanel control...	[Edit] [Delete]
Unidentified	Camera-02	VA Camera	1	00:0F:FB:85:5F:43	10.254.254.1	LOW	High (T 2)	Unknown	Linux 3.2 - 3.18
Unidentified	PC Office	PC	2	00:00:74:0B:48:E4	10.254.254.12	HIGH	Critical (S 5)	Unknown	Linux 5.2
Unidentified	Printer-03	Other		00:80:45:08:FF:0C	10.254.254.12	MEDIUM	High (T 2)	Unknown	Windows
Unidentified	PIC-06	PIC	1	34:09:95:30:0C:48	10.254.254.17	MEDIUM	High (T 2)	Unknown	Unknown
Unidentified	PIC-04	PIC	1	90:07:53:90:09:79	10.254.254.18	HIGH	High (T 2)	Unknown	SMARTC 57
Unidentified	PIC-07	PIC	1	90:07:53:90:09:79	10.254.254.18	MEDIUM	High (T 2)	Unknown	SMARTC 57
Unidentified	Sensor-CHUV	Sensor	0	90:07:53:90:09:79	10.254.254.18	MEDIUM	Critical (S 4)	Unknown	NodeMCU firmware (S...
Unidentified	Sensor-CHAM	Sensor		90:07:53:90:09:40	10.254.254.19	MEDIUM	High (S 5)	Unknown	NodeMCU firmware (S...
Unidentified	Homeport-01	Homeport		78:AC:AA:50:05:43			Unknown	TUX	[Edit] [Delete]

Device list screen

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



NAME

Hub-00

MAC

00:07:2D:62:AA:6A

IPs

10.254.254.1

LAST CONNECTION

04/05/2024 13:13:20

TYPE

Other

PURPOSE LEVEL

2

VENDOR

AAEON Technology Inc.

SITE ID

1

SENSOR IDs

sonda_vc

ROL

Not applicable

SCORING

MEDIUM

SCORING DATE

06/05/2024 15:25:00

STATUS

UNAUTHORIZED UNPINNED

LAST SCAN

24/05/2024 11:01:40

SCAN STATUS

SCANNING

UDP SCAN

UDP Scan results...

TCP SCAN

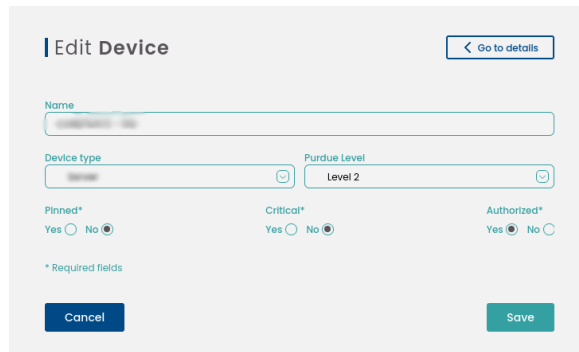
TCP Scan results...

Edit

Close

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 Analysis of Wireless devices

If desired, and if the traffic collection probes have the appropriate hardware, the user can configure wireless device scanning from this first stage. To do so, they must configure the interfaces to be used, and the probe will scan for wireless devices in its vicinity.

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

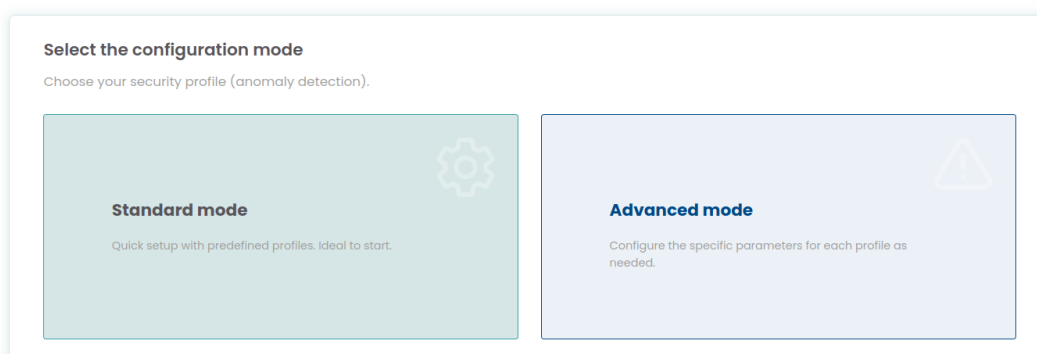
2.4 Rules configuration

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

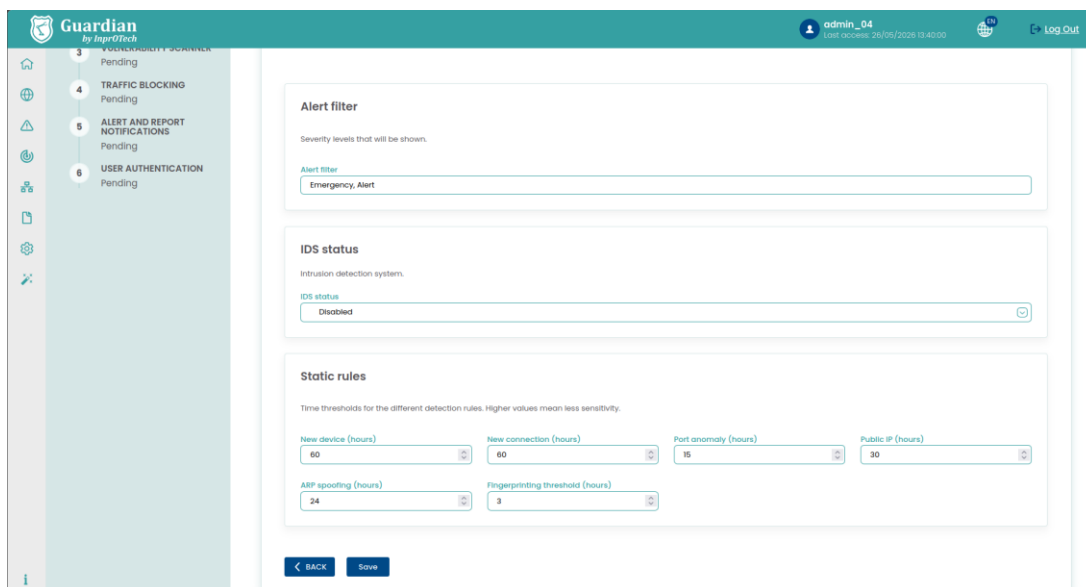
From the second stage of the setup wizard, the user will be able to abstract their entire configuration and choose one of the three predefined security profiles (basic mode), or manually edit the rules, parameters, and filters based on one of them (advanced mode).

| 2. Detection profile



For manual editing, the user must configure which rules they want to be active for analysing their organization's network, as well as the time ranges to suppress each of the alerts if deemed appropriate. They can also set a filter to determine the severity level at which alerts are sent to the web portal.

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.



Guardian
by InprOTech

admin_04
Last access: 26/05/2026 13:40:00

Log Out

Alert filter
Severity levels that will be shown.
Alert filter: Emergency, Alert

IDS status
Intrusion detection system.
IDS status: Disabled

Static rules
Time thresholds for the different detection rules. Higher values mean less sensitivity.

New device (hours): 60
New connection (hours): 60
Port anomaly (hours): 15
Public IP (hours): 30
ARP spoofing (hours): 24
Fingerprinting threshold (hours): 3

BACK Save

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.



Guardian
by InprOTech

admin_04
Acceso anterior: 27/05/2026 00:50:00

Salir

Configuración

PERFIL
Usuario

DETECCIÓN DE AMENAZAS
General

NETWORK
Bloqueo

AVANZADOS
General
Preferencias

Estado general

Estado de mecanismos de detección

Amenazas basadas en reglas
VER ESTADO

Amenazas basadas en IA/ML
VER ESTADO

Amenazas basadas en firmas
VER ESTADO

Status screen detection mechanism

Rules engine 6 Rules

	NAME	STATUS	THRESHOLDS	OPTIONS
☒	New device	Production	15	
☒	New connection	Production	15	
☒	Network port anomaly	Production	15	
☒	New public IP	Production	15	
☒	Possible fingerprinting	Production	5-3-3	
☒	Possible ARP spoofing	Production	1	

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.

Edit rule

Threshold

Status

Detecting


* Required fields

Cancel

Save

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.

2.5 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.

2.6 Active device scanner (optional)

If the client wishes, in the third stage of the wizard they can enable the active query engine for devices, as well as configure the scan frequency, in order to obtain additional properties of the nodes (such as firmware version, open ports, and running services, among others). It is important to note that this is an active scan and may potentially interfere with some devices.

See the “Device Scanner” section under Web Application Management for more details.

2.7 Active response configuration

In the fourth stage of the wizard, we can configure the reputation checking system and traffic blocking. The client can decide whether to enable these functionalities and choose the operating mode. They can also configure the integration with their firewall here to make use of traffic blocking. The modes and configurations of these functionalities will be detailed later.

2.8 Reports configuration

In the next stage, the generation of Guardian reports can be configured. The client can decide whether to enable or disable this functionality, as well as set the frequency at which the reports are generated.

2.9 Alerts exportation (optional)

If the client wishes, in this same fifth stage of the wizard, they have the option to enable the automatic sending of generated alerts to a syslog server of a SIEM or similar system, for ingestion and correlation* with other log sources.

The only information they need to provide is the IP address and port to which they want the messages to be sent, as well as the protocol to be used (encrypted syslog or not).

* For these purposes, it is important to note that all timestamps returned by the web application are displayed in UTC.

2.10 Continuous dashboard (optional)

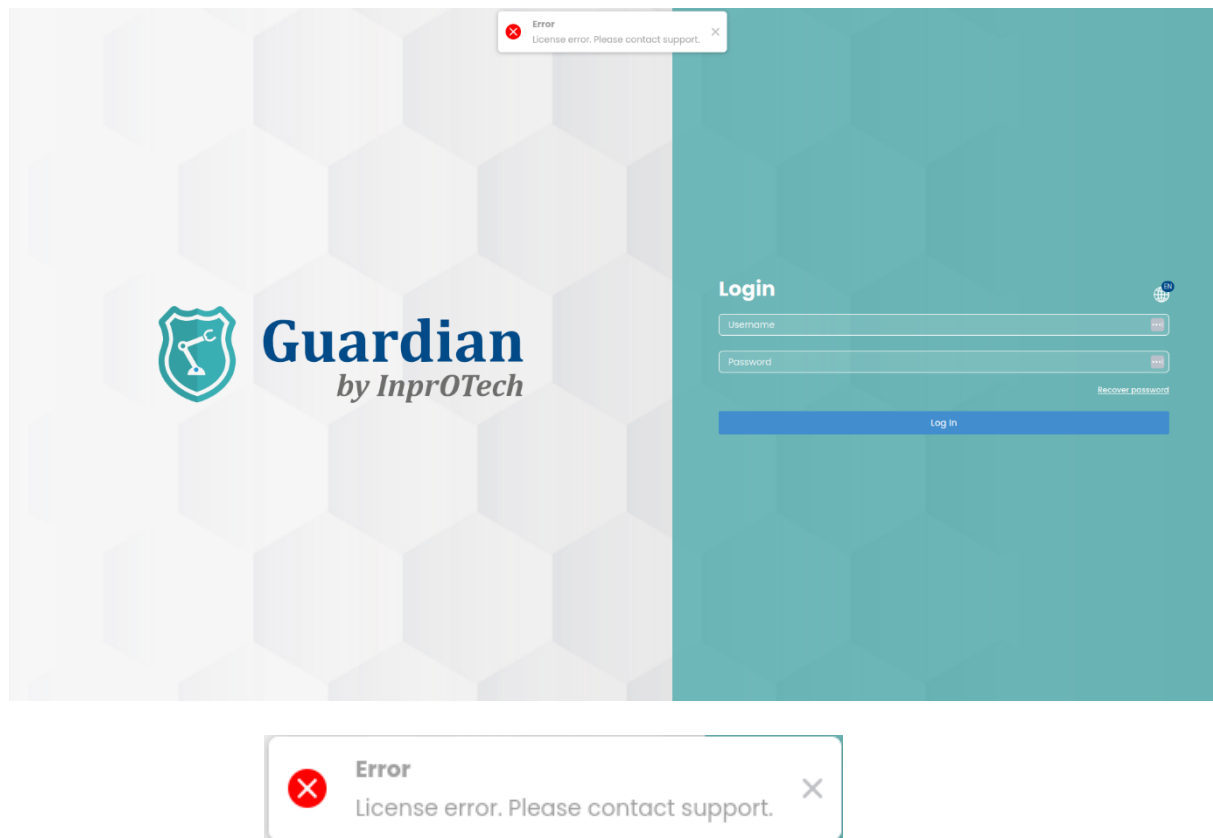
If you are interested in being able to permanently consult the status of Guardian and the main associated indicators (unauthorized devices, network traffic, alerts, etc.), you can have the main Guardian dashboard on a monitor in your operations room with auto-refresh every 5 minutes.

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

2.11 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.



2.12 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:

- **Administrator:** 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.

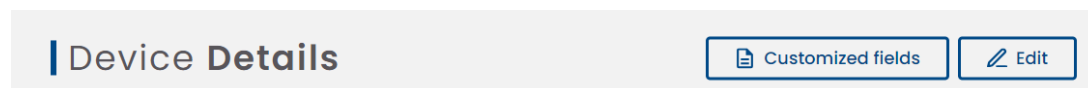
- **Operator:** Factory's privileged user mode, changes can be made to the visible data on the frontend, such as device data, and alerts can be marked as resolved or muted.
- **Monitor:** standard factory user mode, permissions are more restricted. Users can only view data and download reports or CSVs.

2.13 Customized Fields

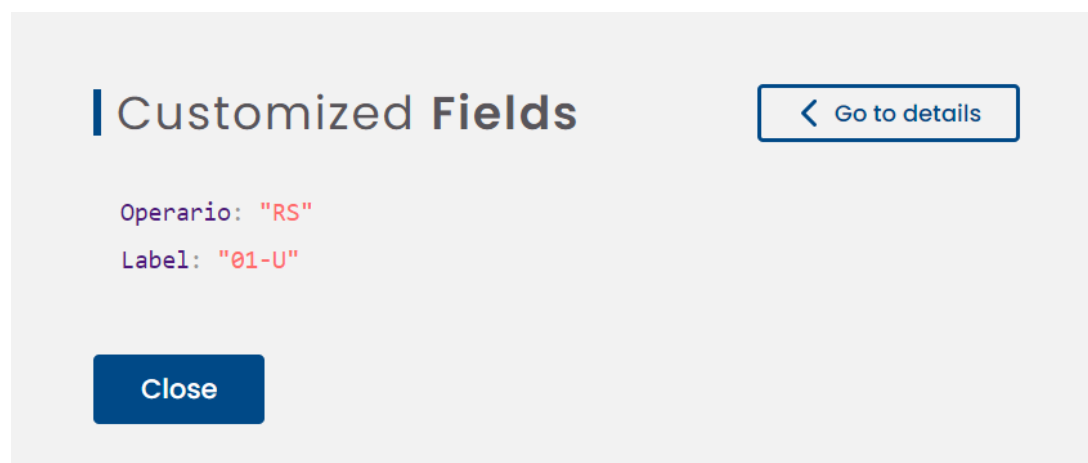
If the user believes any new fields can be added to the device list to allow for their better categorization, they can define them on a key-value format using a “.csv” file.

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.

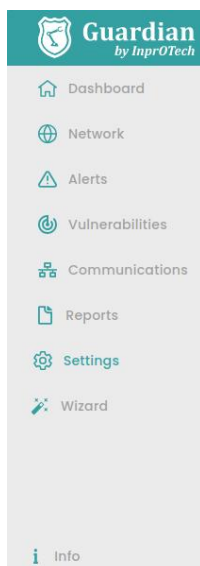


This action will open a new modal that allows the user to view them.



3 Quick Guide

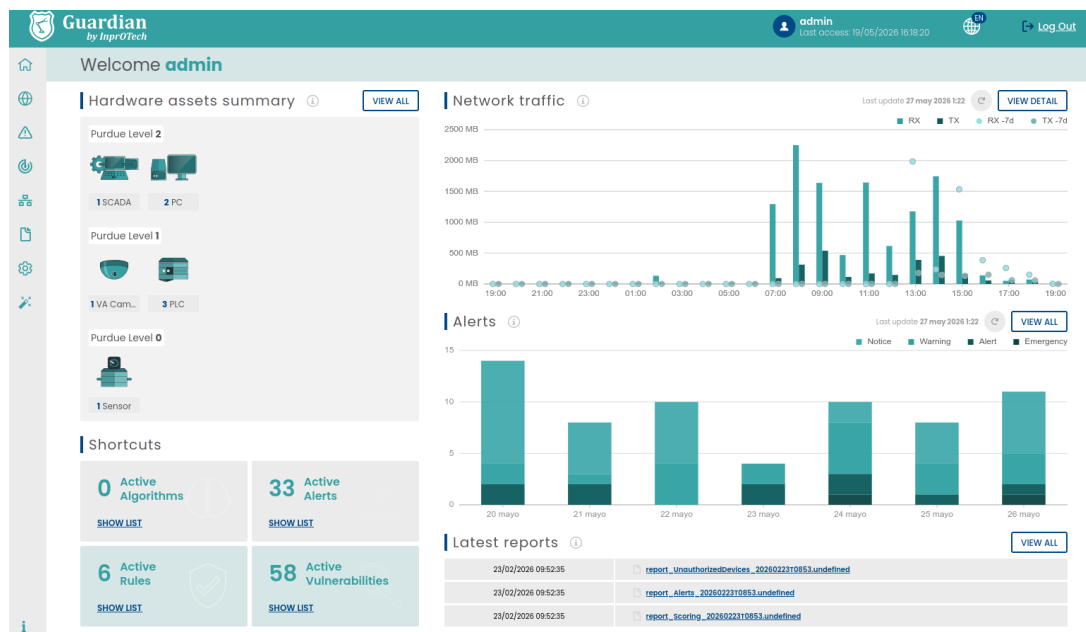
3.1 Menu



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: Wizard: Assisted guide to set up the initial configuration of the solution
- 9: Info: documentation, system version and changelog

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:

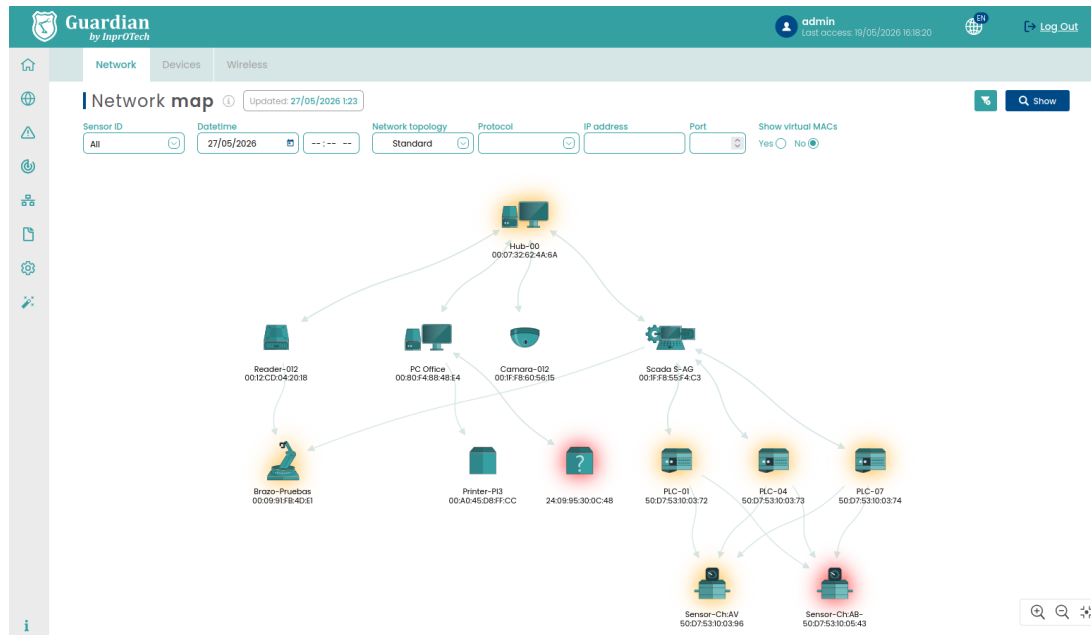
Graphical representation of number of alerts according to their severity.

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.

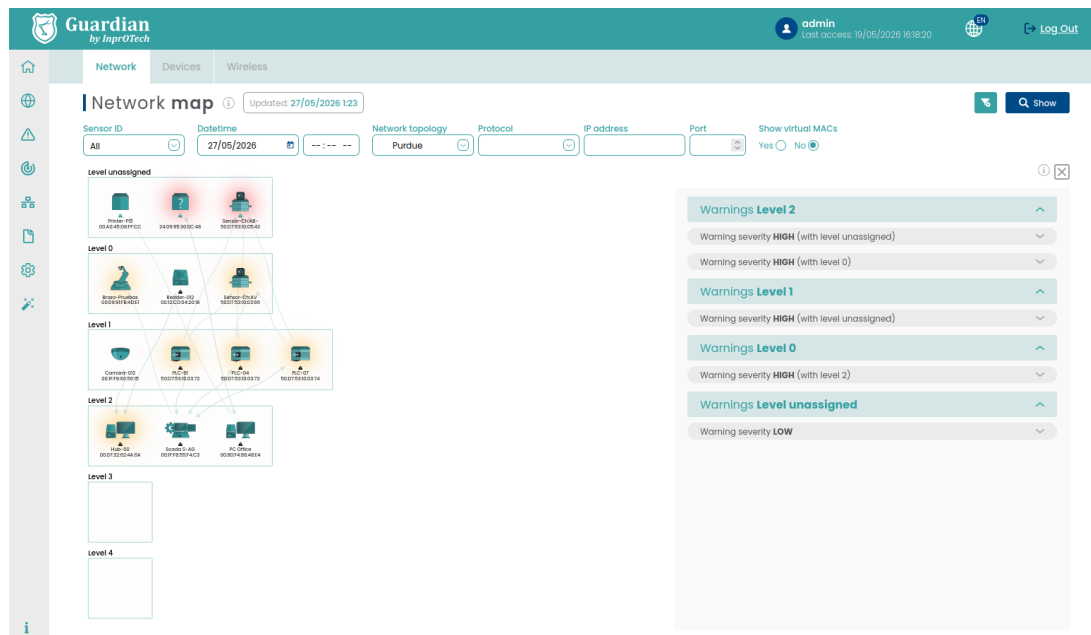
The next row shows the possible filters to view the devices of interest on the screen.

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).



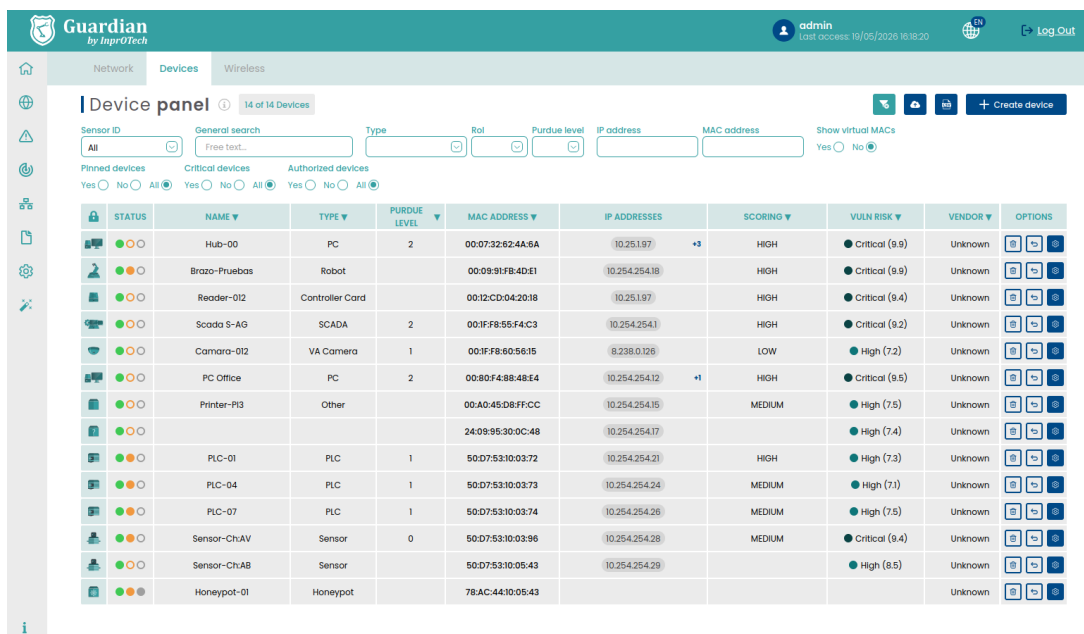
Network map in PURDUE view.

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



Guardian
by InproTech

admin
Last access: 19/05/2026 16:18:20

Log Out

Network **Devices** Wireless

Device panel 14 of 14 Devices

General search: Free text... Type: Rol: Purdue level: IP address: MAC address: Show virtual MACs: Yes No

Pinned devices: Yes No All Critical devices: Yes No All Authorized devices: Yes No All

STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	OPTIONS
	Hub-00	PC	2	00:07:32:62:4A:6A	10.254.254.197	HIGH	Critical (9.9)	Unknown	
	Brazo-Pruebas	Robot		00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Unknown	
	Reader-012	Controller Card		00:12:CD:04:20:18	10.254.254.197	HIGH	Critical (9.4)	Unknown	
	Scada S-AG	SCADA	2	00:1F:F8:5F:4C:3	10.254.254.1	HIGH	Critical (9.2)	Unknown	
	Camara-012	VA Camera	1	00:1F:F8:5D:56:15	8.238.0.126	LOW	High (7.2)	Unknown	
	PC Office	PC	2	00:80:F4:8B:4B:E4	10.254.254.12	HIGH	Critical (9.5)	Unknown	
	Printer-P13	Other		00:A0:45:D8:FF:CC	10.254.254.15	MEDIUM	High (7.5)	Unknown	
				24:09:95:30:0C:48	10.254.254.17		High (7.4)	Unknown	
	PLC-01	PLC	1	50:D7:53:10:03:72	10.254.254.21	HIGH	High (7.3)	Unknown	
	PLC-04	PLC	1	50:D7:53:10:03:73	10.254.254.24	MEDIUM	High (7.1)	Unknown	
	PLC-07	PLC	1	50:D7:53:10:03:74	10.254.254.26	MEDIUM	High (7.5)	Unknown	
	Sensor-ChuAV	Sensor	0	50:D7:53:10:03:96	10.254.254.28	MEDIUM	Critical (9.4)	Unknown	
	Sensor-ChuAB	Sensor		50:D7:53:10:05:43	10.254.254.29		High (8.5)	Unknown	
	Honeypot-01	Honeypot		78:AC:44:10:05:43				Unknown	

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.

SEVERITY	NAME	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DATE	OPTIONS
Alert	ping test	12:23:34:45:78:89	12:23:34:45:78:90	10.11.1	10.11.2	04/05/2026 18:00	
Alert	Conexión con puerto IT	00:07:32:62:4A:6A	00:1F:F8:55:F4:C3	0.0.0.0	10.254.254.1	24/02/2026 09:52	
Warning	Anomalia en tráfico netflow	00:12:CD:04:20:18	00:09:91FB:4D:E1	10.25.197	10.254.254.18	24/02/2026 09:52	
Warning	Anomalia en payload	50:D7:53:10:03:72	00:1F:F8:55:F4:C3	10.254.254.21	10.254.254.1	24/02/2026 09:52	
Notice	Nueva conexión	00:80:F4:88:48:E4	00:A0:45:DB:FF:CC	10.254.254.12	10.254.254.15	24/02/2026 09:52	
Critical	PROTOCOL-ICMP Unusual PING ..	00:1B:17:00:0E:10	00:0E:8C:AA:49:FB	10.20.30.254	10.20.30.104	24/02/2026 09:52	
Critical	PROTOCOL-ICMP Unusual PING ..	00:1B:17:00:0E:10	00:1B:1B:6D:6A:7B	10.20.30.254	10.20.30.95	24/02/2026 09:52	
Emergency	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	3113.83.34	24/02/2026 09:52	
Alert	Descubierta nueva anomalia d..	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.26	10.254.254.29	23/02/2026 09:52	
Alert	Descubierta nueva anomalia d..	00:80:F4:88:48:E4	00:A0:45:DB:FF:CC	10.254.254.12	10.254.254.15	23/02/2026 09:52	
Alert	Conexión con puerto IT	00:07:32:62:4A:6A	00:80:F4:88:48:E4	0.0.0.0	10.254.254.12	23/02/2026 09:52	
Alert	Nuevo dispositivo	00:80:F4:88:48:E4	24:09:95:30:0C:48			23/02/2026 09:52	
Warning	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	378.142.36	23/02/2026 09:52	
Warning	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	20.54.36.229	23/02/2026 09:52	
Alert	Honeypot Attack	24:09:95:30:AC:48	78:AC:44:10:05:43	10.254.254.17	10.78.142.36	23/02/2026 09:52	

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.

If the Blocking Policy is active in any way (informative, manual, or automatic), public IP alerts whose IP has been classified as malicious will be marked with a striking red color, which will be softened if that address is on the industrial firewall's block list.

*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.

Guardian
by InproTech

admin
Last access: 19/05/2026 16:18:20

Log Out

Communications

Communications panel 22 of 22 Connections

Sensor ID: All IP address: MAC address: Port: Protocol:

	SOURCE MAC ▼	DESTINATION MAC ▼	DESTINATION NAME ▼	SOURCE NAME ▼	SOURCE IP ▼	DESTINATION IP ▼	DESTINATION PORT ▼	PROTOCOL ▼
	50:D7:53:10:03:74	50:D7:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	UDP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	TCP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	UDP
	50:D7:53:10:03:73	50:D7:53:10:03:96	PLC-04	Sensor-ChAV	10.254.254.24	10.254.254.28	53	UDP
	50:D7:53:10:03:73	50:D7:53:10:05:43	PLC-04	Sensor-ChAB	10.254.254.24	10.254.254.29	53	UDP
	50:D7:53:10:03:72	50:D7:53:10:03:96	PLC-01	Sensor-ChAV	10.254.254.21	10.254.254.28	5353	UDP
	50:D7:53:10:03:72	50:D7:53:10:05:43	PLC-01	Sensor-ChAB	10.254.254.21	10.254.254.29	53	UDP
	00:80:F4:88:48:E4	00:A0:45:D8:FF:C0	PC Office	Printer-P13	10.254.254.12	10.254.254.15	5353	UDP
	00:80:F4:88:48:E4	00:A0:45:D8:FF:C0	PC Office	Printer-P13	10.254.254.12	10.254.254.15	5353	GRE
	00:80:F4:88:48:E4	24:09:95:30:0C:48	PC Office		10.254.254.12	10.254.254.17	53	UDP
	00:1F:F8:55:F4:C3	00:09:91:F8:4D:E1	Scada S-AG	Brazo-Pruebas	10.254.254.1	10.254.254.18	53	UDP
	00:1F:F8:55:F4:C3	50:D7:53:10:03:72	Scada S-AG	PLC-01	10.254.254.1	10.254.254.21	53001	TCP
	00:1F:F8:55:F4:C3	50:D7:53:10:03:73	Scada S-AG	PLC-04	10.254.254.1	10.254.254.24	52771	TCP
	00:1F:F8:55:F4:C3	50:D7:53:10:03:74	Scada S-AG	PLC-07	10.254.254.1	10.254.254.26	42120	TCP
	00:12:CD:04:20:18	00:09:91:F8:4D:E1	Reader-012	Brazo-Pruebas	10.25.1.97	10.254.254.18	0	UDP

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:

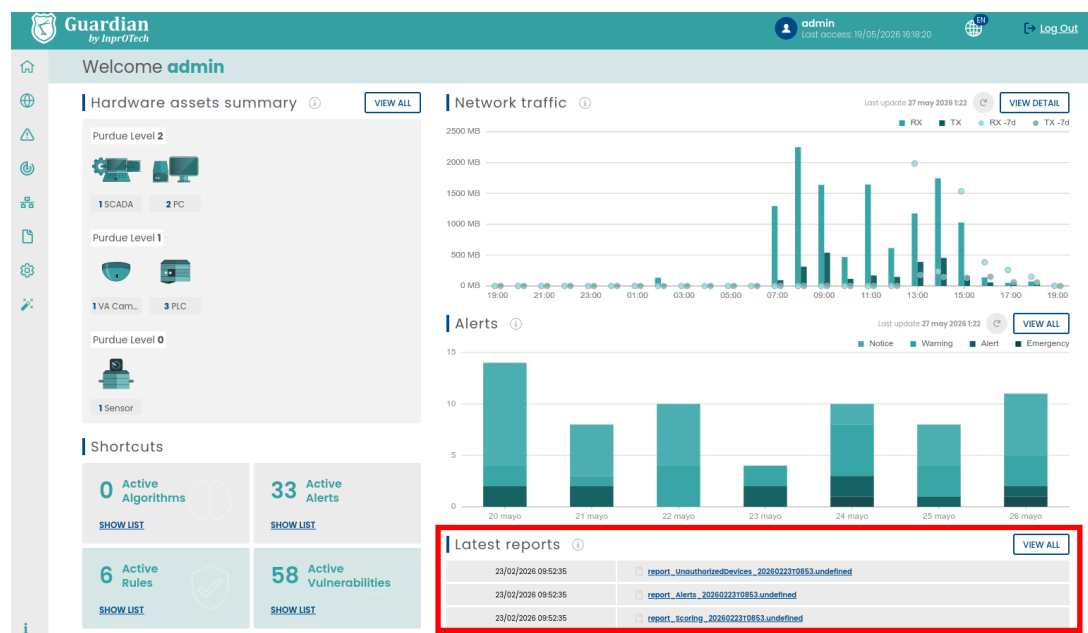
- Unauthorized connected devices:
 - Name: Name of the device
 - MAC of the device
 - Vendor: Manufacturer
 - Role: Role
 - Discovery date: Date of discovery
 - Ips
 - Purdue level
 - Fixed (Y/N)
 - Critical (Y/N)
 - Device type
 - Score and score timestamp.

- 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
 - Criticality
 - Description
 - Timestamp published.
 - CWE
 - URL

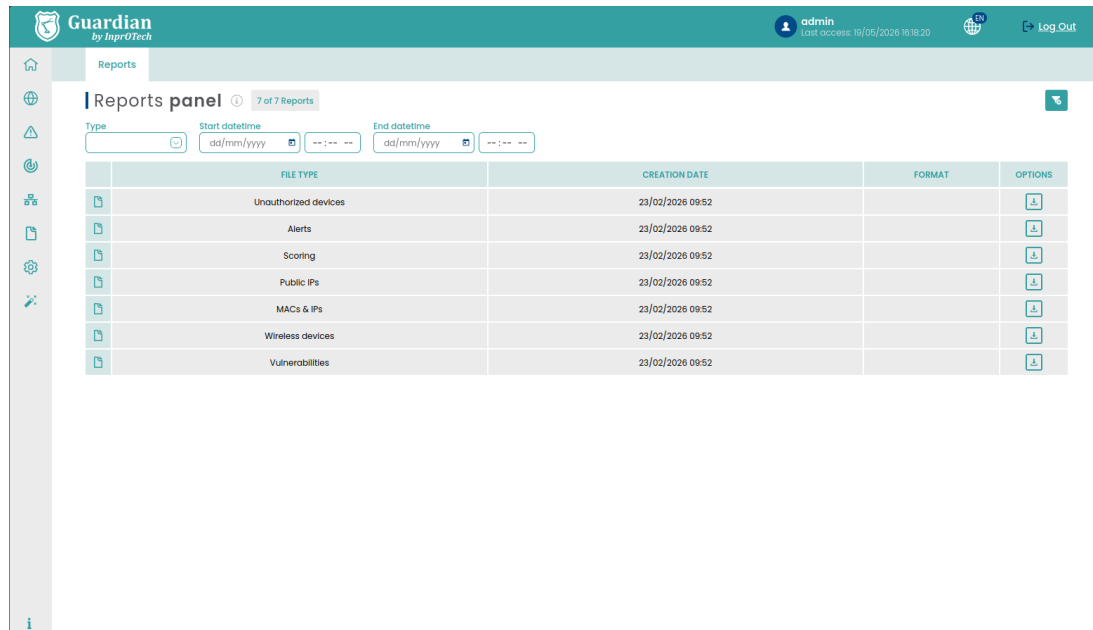
If the device has the label Name reported, it will replace the MAC field in the alert's reports. On the other hand, in manual downloads of user searches from the alerts panel or the device list, the "Latest reports" section will display both fields independently.

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:



The screenshot shows the Guardian Reports panel. At the top, there's a header with the Guardian logo, user 'admin', and a 'Log Out' button. Below the header, the 'Reports panel' is displayed, showing '7 of 7 Reports'. There are filters for 'Type', 'Start datetime', and 'End datetime'. The main content is a table with the following data:

FILE TYPE	CREATION DATE	FORMAT	OPTIONS
Unauthorized devices	23/02/2026 09:52		
Alerts	23/02/2026 09:52		
Scoring	23/02/2026 09:52		
Public IPs	23/02/2026 09:52		
MACs & IPs	23/02/2026 09:52		
Wireless devices	23/02/2026 09:52		
Vulnerabilities	23/02/2026 09:52		

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 Settings

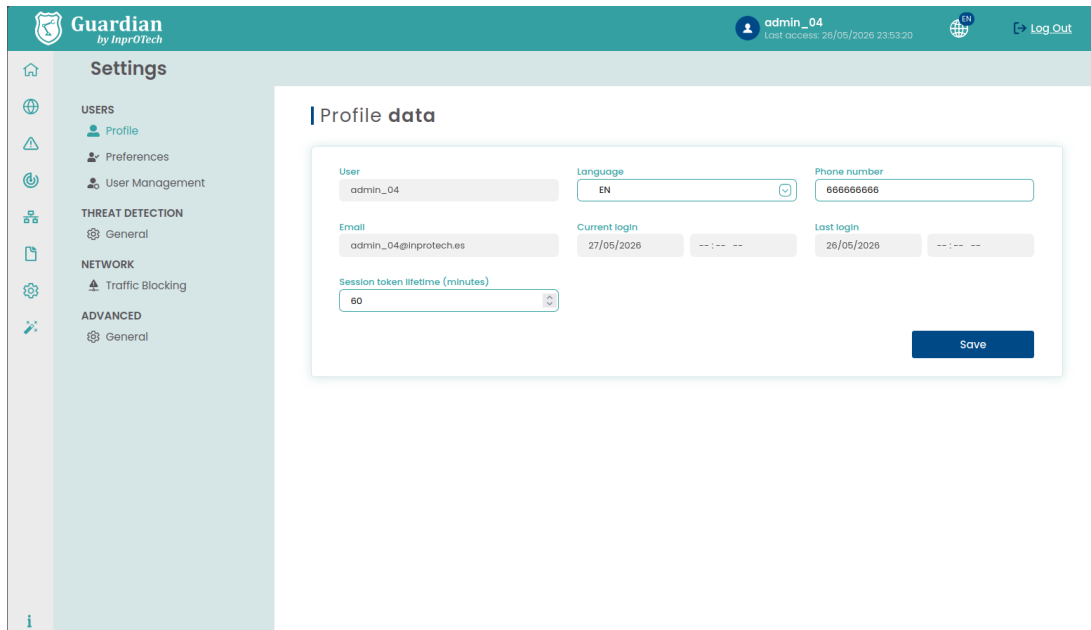
In this section we can adjust our profile or the service, modify some parameters related to threat detection, or different configurations of alerts, threats, and user management.

The most relevant aspects at user level are summarized below.

3.8.1 Users profile

This section displays basic information such as username, associated email, date and time of last and current connection, language preference (EN/ES/CAT/EU/GL), contact telephone number, and session token lifetime measured in minutes. The last three fields are editable by the user.

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



Guardian
by InprOTech

admin_04
Last access: 26/05/2026 23:53:20

Settings

USERS

- Profile
- Preferences
- User Management

THREAT DETECTION

- General

NETWORK

- Traffic Blocking

ADVANCED

- General

Profile data

User: admin_04

Language: EN

Phone number: 666666666

Email: admin_04@inprotech.es

Current login: 27/05/2026

Last login: 26/05/2026

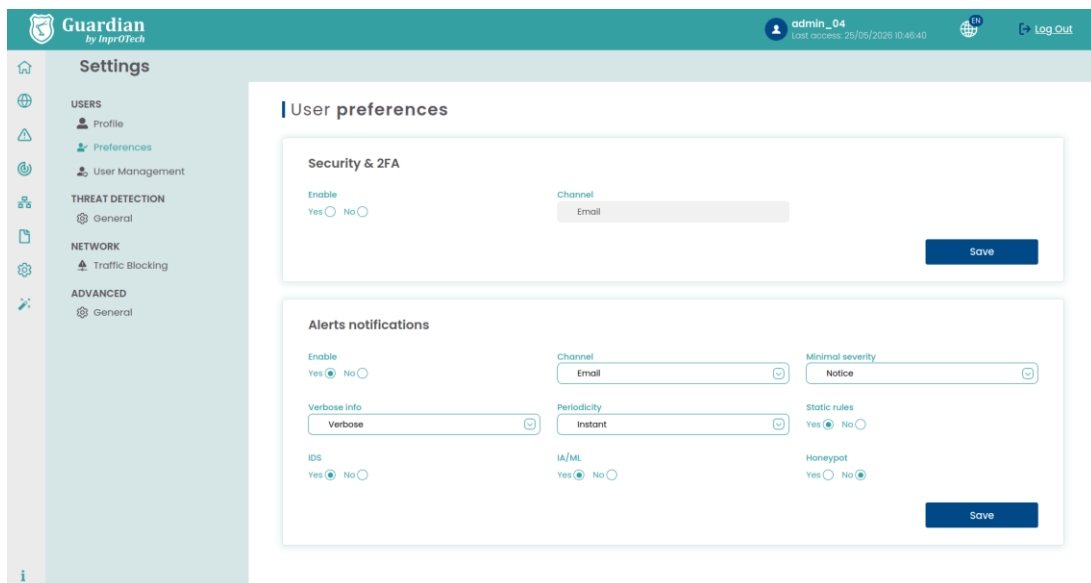
Session token lifetime (minutes): 60

Save

User profile data view

3.8.2 Users preferences

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).



Guardian
by InprOTech

admin_04
Last access: 26/05/2026 10:46:40

Settings

USERS

- Profile
- Preferences
- User Management

THREAT DETECTION

- General

NETWORK

- Traffic Blocking

ADVANCED

- General

User preferences

Security & 2FA

Enable: Yes ☐ No ☐

Channel: Email

Save

Alerts notifications

Enable: Yes ☒ No ☐

Channel: Email

Minimal severity: Notice

Verbose info: Verbose

Periodicity: Instant

Static rules: Yes ☒ No ☐

IDS: Yes ☒ No ☐

IA/ML: Yes ☒ No ☐

Honeypot: Yes ☐ No ☒

Save

User preferences 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:

- Administrator
- Operator
- Monitor

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 they want 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 notifications

Enable Yes ☐ No ☒	Method Email ☒	Minimal severity Notice ☒
Verbose info Verbose ☒	Periodicity Instant ☒	Static rules Yes ☒ No ☐
IDS Yes ☒ No ☐	IA/ML Yes ☒ No ☐	Honeypot Yes ☐ No ☒

[Save](#)

Alerts notification view

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

Important:

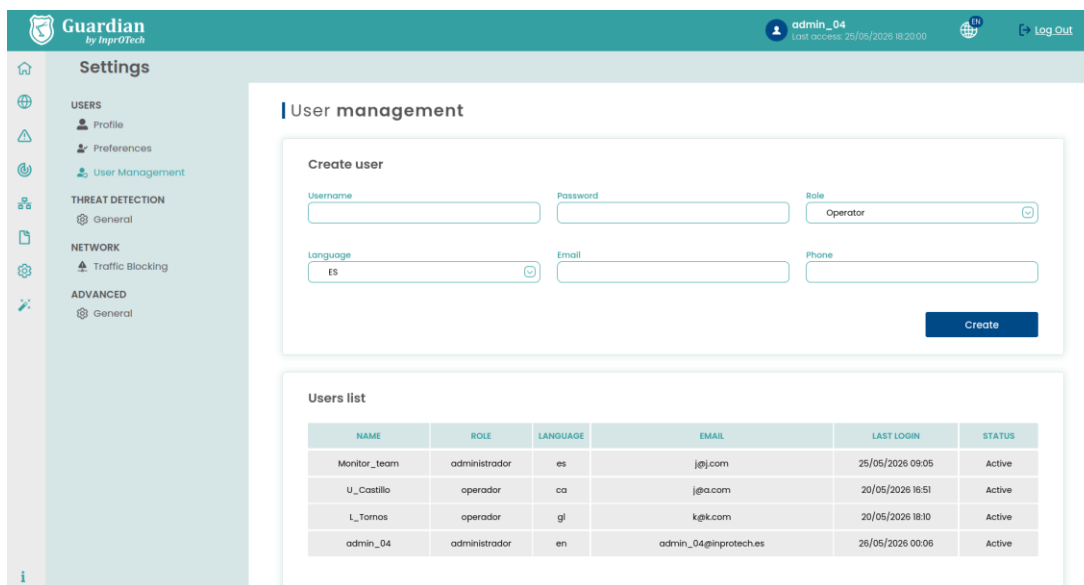
- Alert notification must be enabled in the backend to allow the user to enable proactive sending.
- In case that with the established conditions too many alerts are generated per time unit, the functionality will be auto-disabled for security (previously informing via email to the user about this circumstance), 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:

Summarized individual alert notification example.

Grouped daily alert notification example.

 www.inprotech.es
info@inprosec.com
inprosec.com



Guardian
by InproTech

admin_04
Last access: 25/05/2026 18:20:00

Log Out

Settings

- USERS
 - Profile
 - Preferences
 - User Management
- THREAT DETECTION
 - General
- NETWORK
 - Traffic Blocking
- ADVANCED
 - General

User management

Create user

Username: Password: Role:

Language: Email: Phone:

Create

Users list

NAME	ROLE	LANGUAGE	EMAIL	LAST LOGIN	STATUS
Monitor_team	administrador	es	j@j.com	25/05/2026 09:05	Active
U_Castillo	operador	ca	j@a.com	20/05/2026 16:51	Active
L_Tornos	operador	gl	k@k.com	20/05/2026 18:30	Active
admin_04	administrador	en	admin_04@inprotech.es	26/05/2026 00:06	Active

User management view

3.8.5 Traffic Blocking Configuration

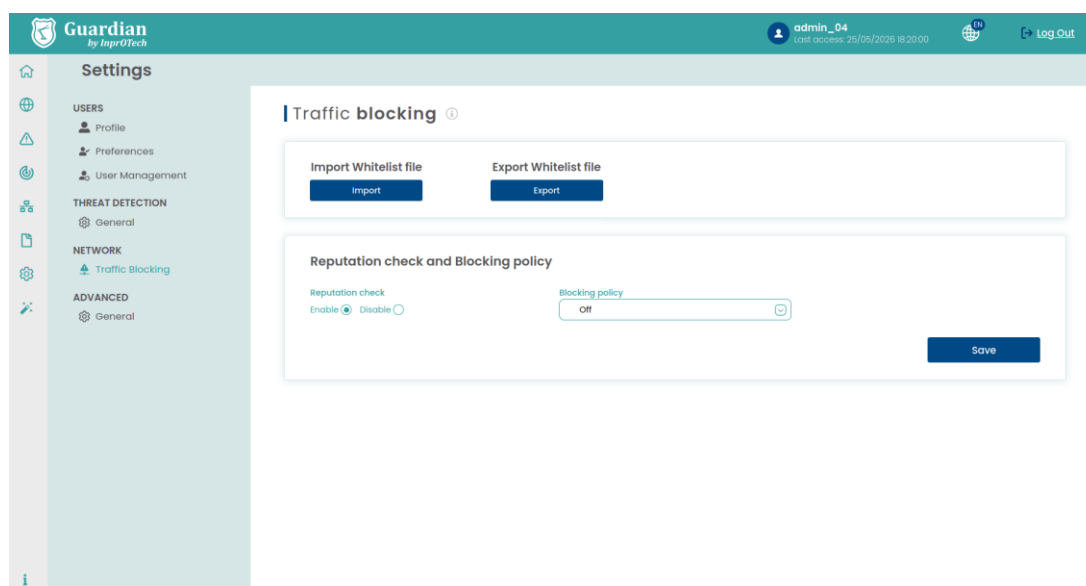
In this section, you can enable the import of a whitelist of IP addresses, IP ranges, or MAC addresses (addresses to which this block will never be applied), as well as export it to a CSV file.

In addition, you can configure the two parameters in this section:

-Reputation Check: enables or disables the search for the reputation of public IPs in incoming or outgoing traffic.

-Blocking Policy: selects the mode for blocking malicious public IPs from among four modes:

- **Informative:** notifies the user and suggests blocking that IP.
- **Manual:** provides a user-actionable button on the alert panel that sends the malicious IP to a block list managed by the industrial firewall.
- **Automatic:** Communicates with the firewall without user intervention, adding the malicious IP to a block list.
- **Off:** Makes no changes to the alert panel and does not attempt to communicate with the industrial firewall. English Spanish translator



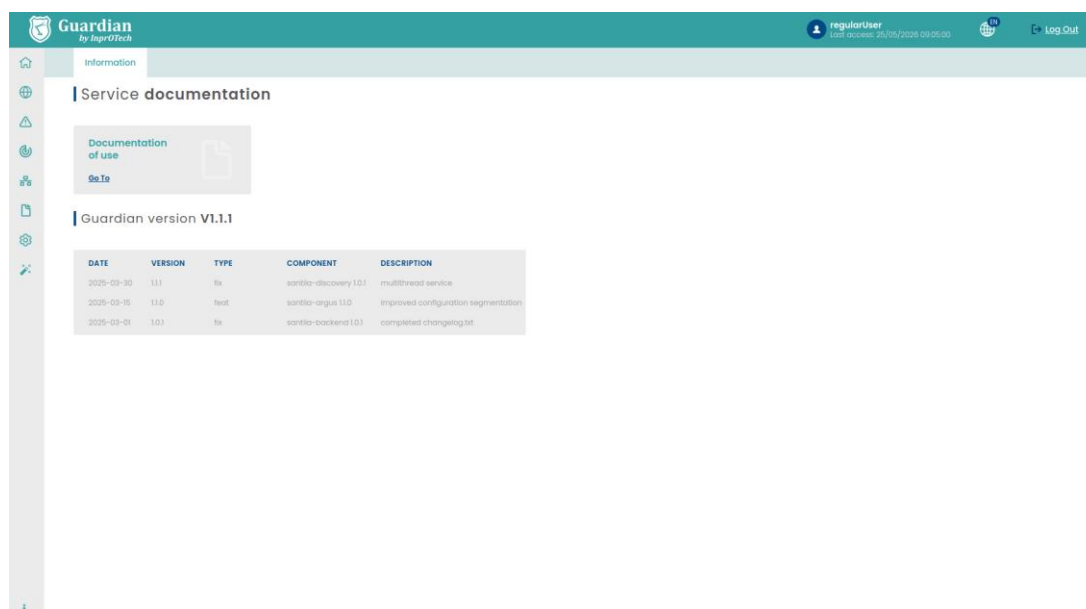
Traffic Blocking view

3.9 Info

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.

It also shows the current platform version and changelog for versioning control.

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

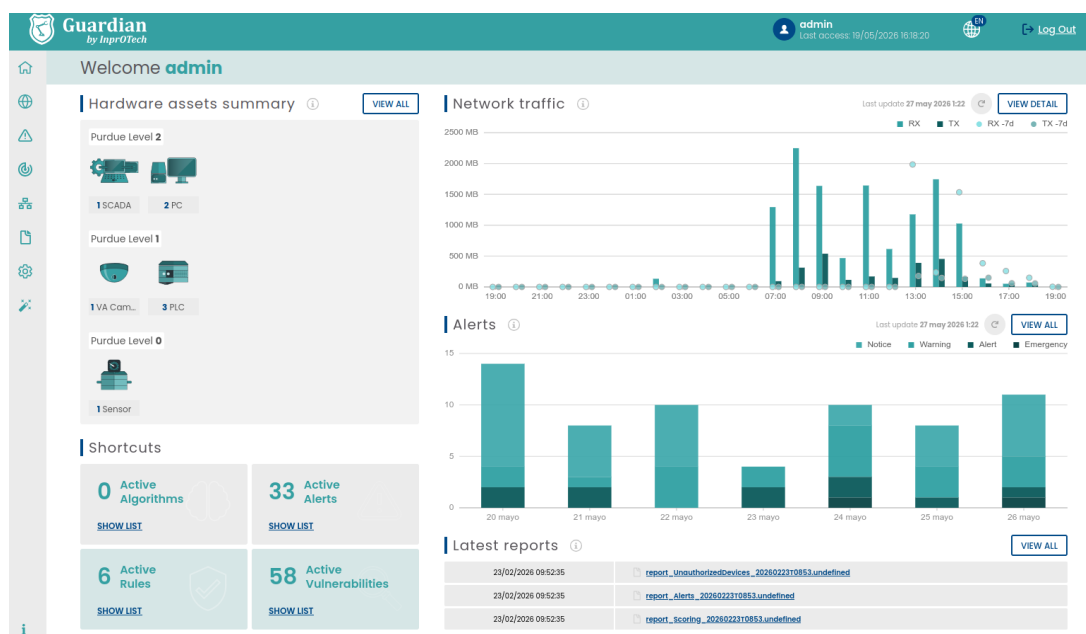


Info view

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

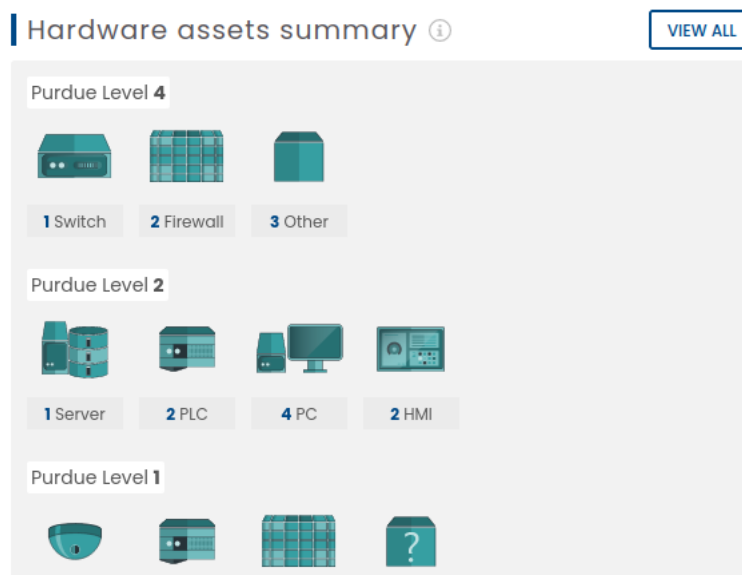
4 Application management

4.1 Main Dashboard



Dashboard principal

4.1.1 Actives summary

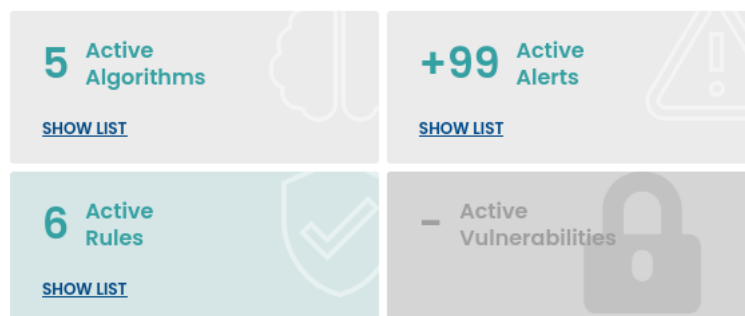


Asset summary

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

| Shortcuts



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).

| Amenazas basadas en IA/ML

Gestión de algoritmos IA/ML

IDs Sonda

Todos

Búsqueda general

ALGORITMO		ESTADO	ACCIONES		
	_anagram	Inactivo	Entrenar	Detectar	Parar
	_deep-payload	Inactivo	Entrenar	Detectar	Parar
	_ext-iforest	Detectando	Entrenar	Detectar	Parar
	_Process-Mining	Detectando	Entrenar	Detectar	Parar
	_isolation-forest	Detectando	Entrenar	Detectar	Parar
	_autoencoder	Inactivo	Entrenar	Detectar	Parar
	_UEBA-LSTM	Preparado	Entrenar	Detectar	Parar

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).

Rules engine ⓘ 6 Rules

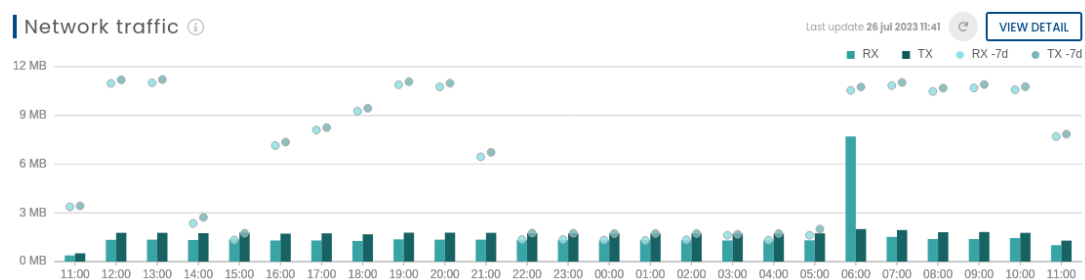
	NAME	STATUS	THRESHOLDS	OPTIONS
✓	New device	Production	15 ⓘ	⌵
✓	New connection	Production	15 ⓘ	⌵
✓	Network port anomaly	Production	15 ⓘ	⌵
✓	New public IP	Production	15 ⓘ	⌵
✓	Possible fingerprinting	Production	5-3-3 ⓘ	⌵
✓	Possible ARP spoofing	Production	1 ⓘ	⌵

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.

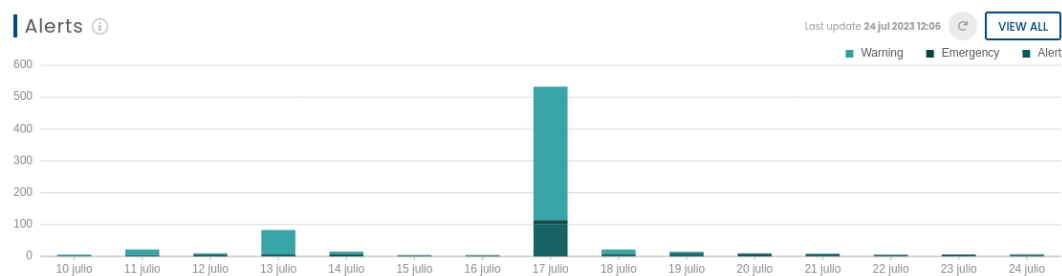


Network traffic

The user can graphically display the traffic generated (in bit/s, or multiple of that unit) in the last 24 hours, both sent (darker green) and received (lighter 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.



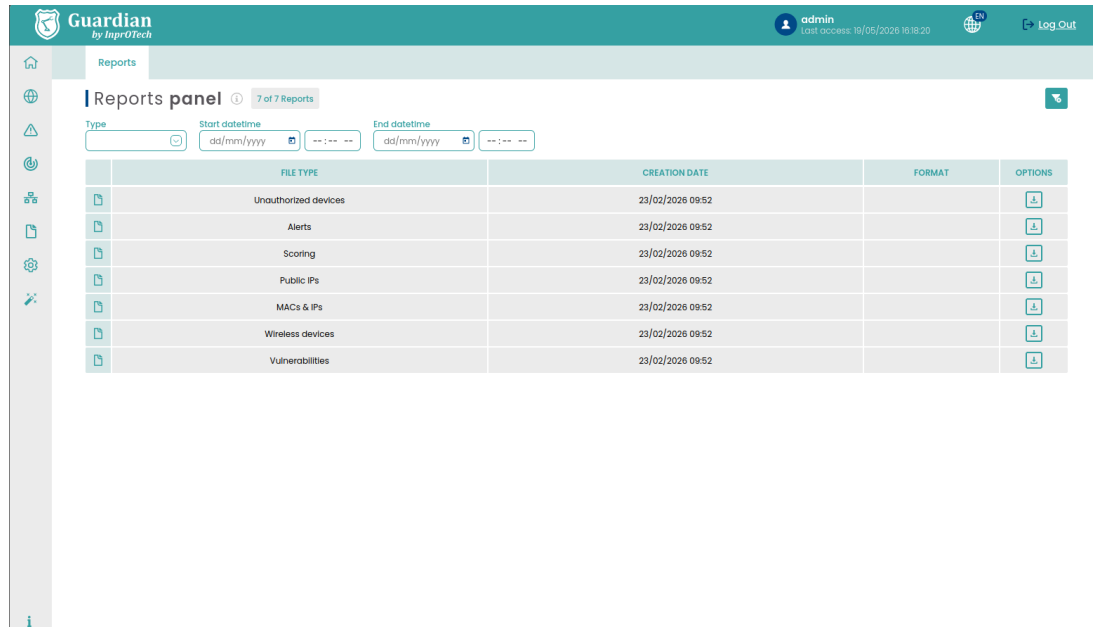
Alerts

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



The screenshot shows the 'Reports' panel in the InprOTech Guardian application. The panel displays a table of reports with the following columns: FILE TYPE, CREATION DATE, FORMAT, and OPTIONS. The table contains 7 reports, all generated on 23/02/2026 at 09:52. The report types are: Unauthorized devices, Alerts, Scoring, Public IPs, MACs & IPs, Wireless devices, and Vulnerabilities. Each report has a download icon in the OPTIONS column.

FILE TYPE	CREATION DATE	FORMAT	OPTIONS
Unauthorized devices	23/02/2026 09:52		
Alerts	23/02/2026 09:52		
Scoring	23/02/2026 09:52		
Public IPs	23/02/2026 09:52		
MACs & IPs	23/02/2026 09:52		
Wireless devices	23/02/2026 09:52		
Vulnerabilities	23/02/2026 09:52		

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.

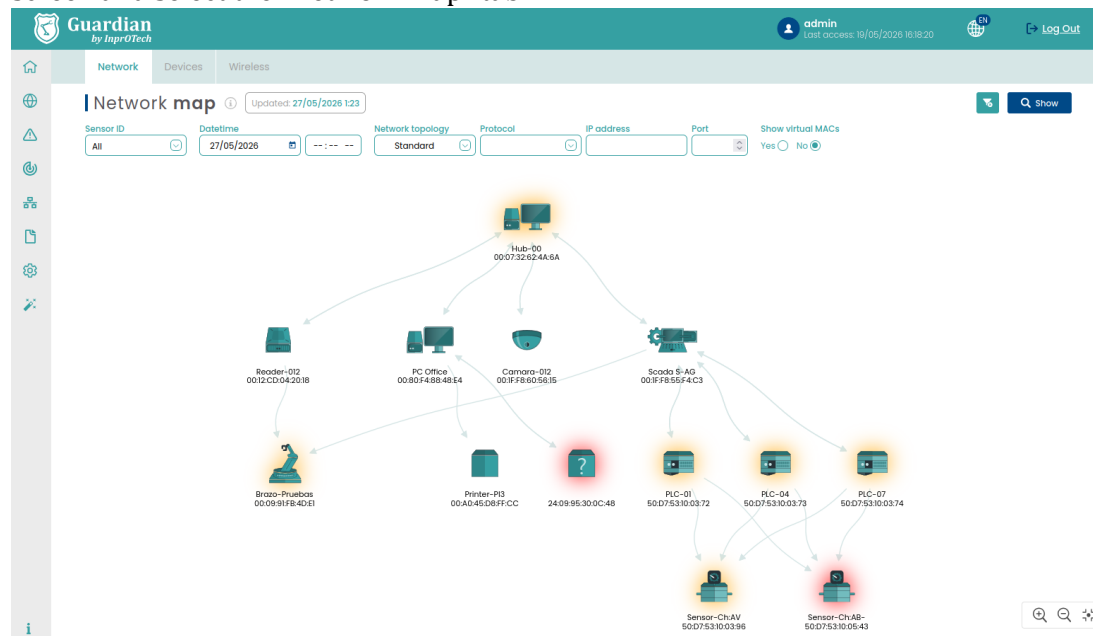
Currently, the reports generated on a weekly basis are:

- 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.

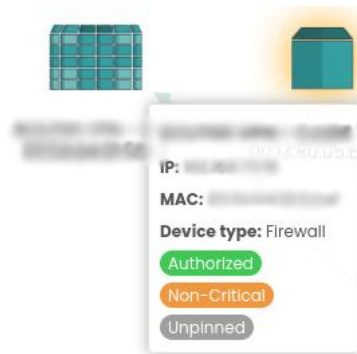
The icons represented will correspond to those described in Annex II.

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

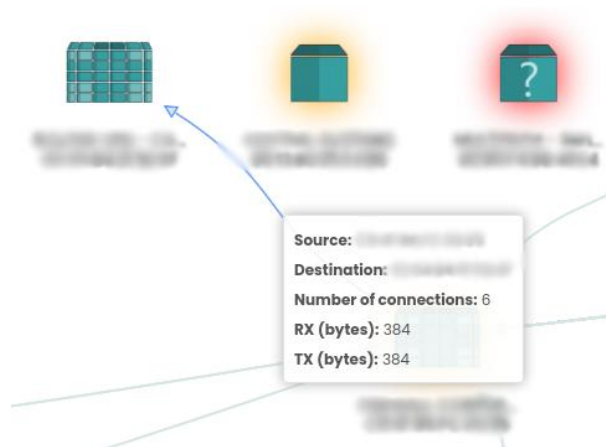
If we place the cursor over a device, we will get a pop-up window where we will see the basic information of the device.



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

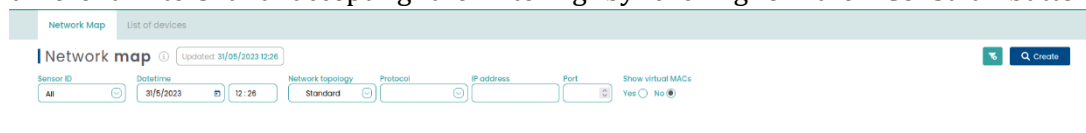


information of that communication.

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

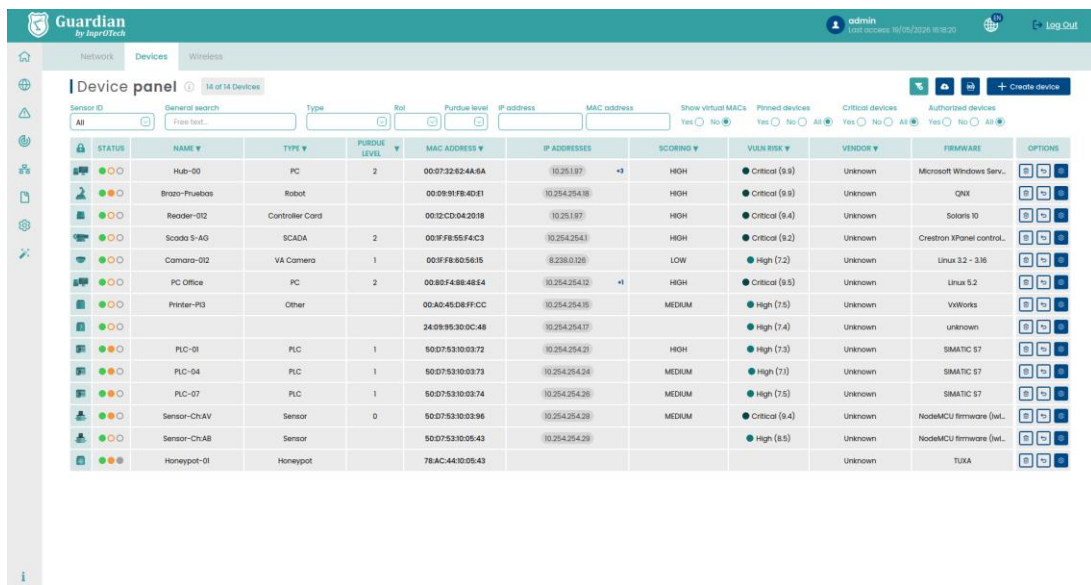
Filters can be applied according to:

- 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.



STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS
	Hub-00	PC	2	00:07:32:62:4A:5A	10.254.197	HIGH	Critical (9.8)	Unknown	Microsoft Windows Serv...	
	Brato-Pueblas	Robot		00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critical (9.8)	Unknown	QNX	
	Reader-012	Controller Card		00:12:CD:04:20:18	10.254.197	HIGH	Critical (9.4)	Unknown	Solaris 10	
	Scada S-AQ	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Unknown	Crestion XPanel control...	
	Camera-012	VA Camera	1	00:1F:F8:50:56:15	8.238.0.128	LOW	High (7.2)	Unknown	Linux 3.2 - 3.16	
	PC Office	PC	2	00:80:F4:86:48:54	10.254.254.12	HIGH	Critical (9.5)	Unknown	Linux 5.2	
	Printer-P3	Other		00:A0:45:D8:FF:CC	10.254.254.16	MEDIUM	High (7.5)	Unknown	VWorks	
				24:09:95:30:0C:48	10.254.254.17		High (7.4)	Unknown	unknown	
	PLC-01	PLC	1	50:07:53:10:03:72	10.254.254.21	HIGH	High (7.3)	Unknown	SMATIC S7	
	PLC-04	PLC	1	50:07:53:10:03:73	10.254.254.24	MEDIUM	High (7.1)	Unknown	SMATIC S7	
	PLC-07	PLC	1	50:07:53:10:03:74	10.254.254.26	MEDIUM	High (7.5)	Unknown	SMATIC S7	
	Sensor-CHAV	Sensor	0	50:07:53:10:03:96	10.254.254.28	MEDIUM	Critical (9.4)	Unknown	NodeMCU firmware (bet...	
	Sensor-CHAB	Sensor		50:07:53:10:05:43	10.254.254.29		High (8.5)	Unknown	NodeMCU firmware (bet...	
	Honeypot-01	Honeypot		78:AC:44:10:05:43				Unknown	TUXA	

Device list

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

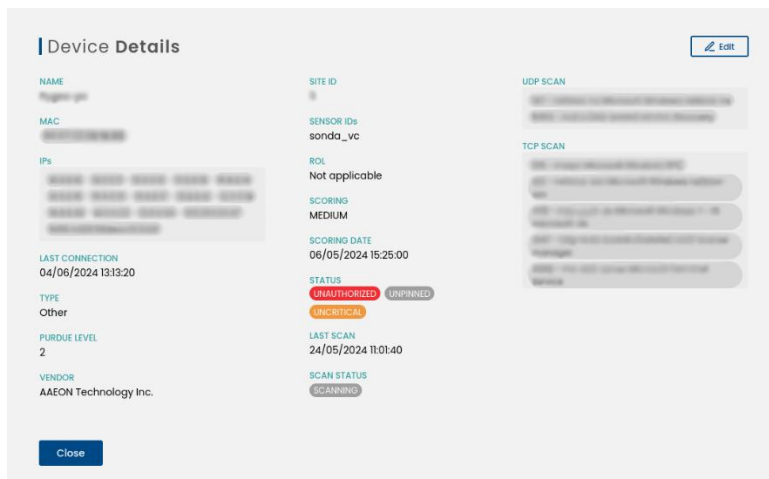
- **STATUS**
 - The first of the circles will indicate whether the device is authorized (green colour) or unauthorized (red colour).
 - The second of the circles will indicate whether the device is critical (orange colour with fill) or non-critical (orange colour without fill).
 - The third circle indicates 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:



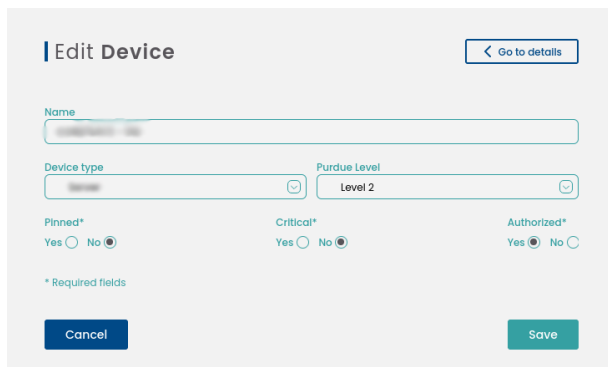
: Button to view device information in detail.



Device details



: Button to modify device parameters.

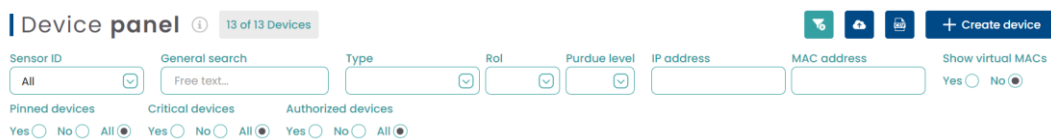


Device parameters



: 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 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.

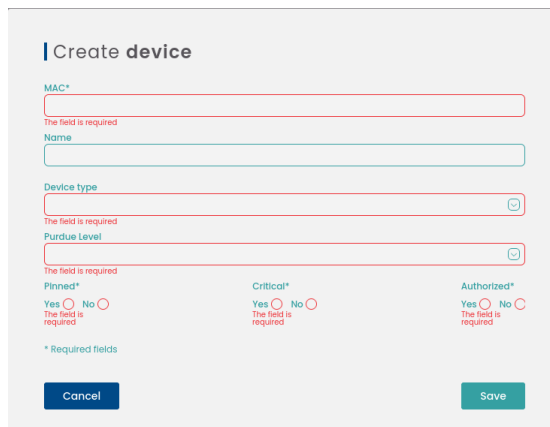
Pressing the button  will reset the filtering values and Guardian will display the complete list with all devices again.

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.

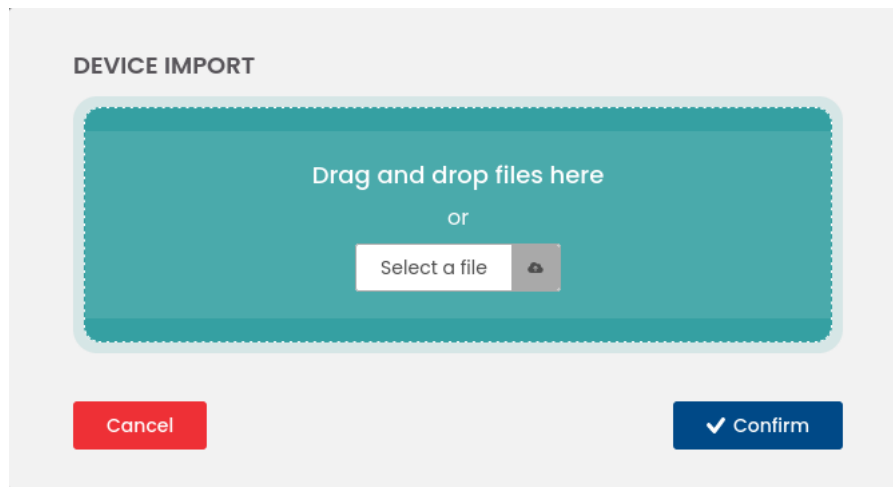
The requested information about the device to be added must be entered manually and to make the creation effective, click on the "Save" button.

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.

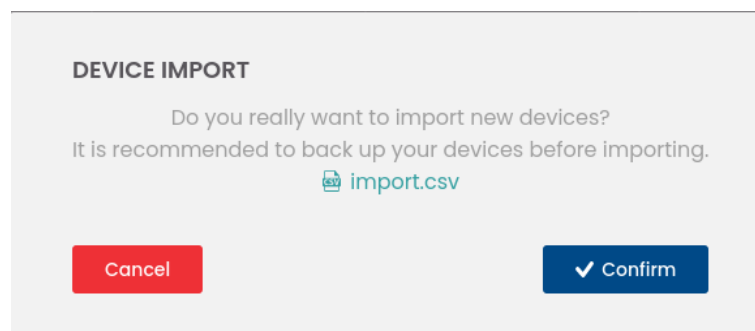
- New records may also contain the literal `*CURRENT*` in some of their fields; this means leaving those fields with default values. In the case of Boolean data, it will be false, and text fields, such as name, Purdue, and device type, will remain as NULL, and the user can modify it through the web interface.
- There are two possible 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):



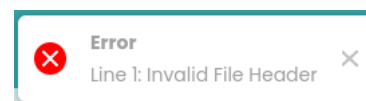
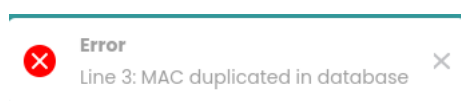
"Device import" drop-down.

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)

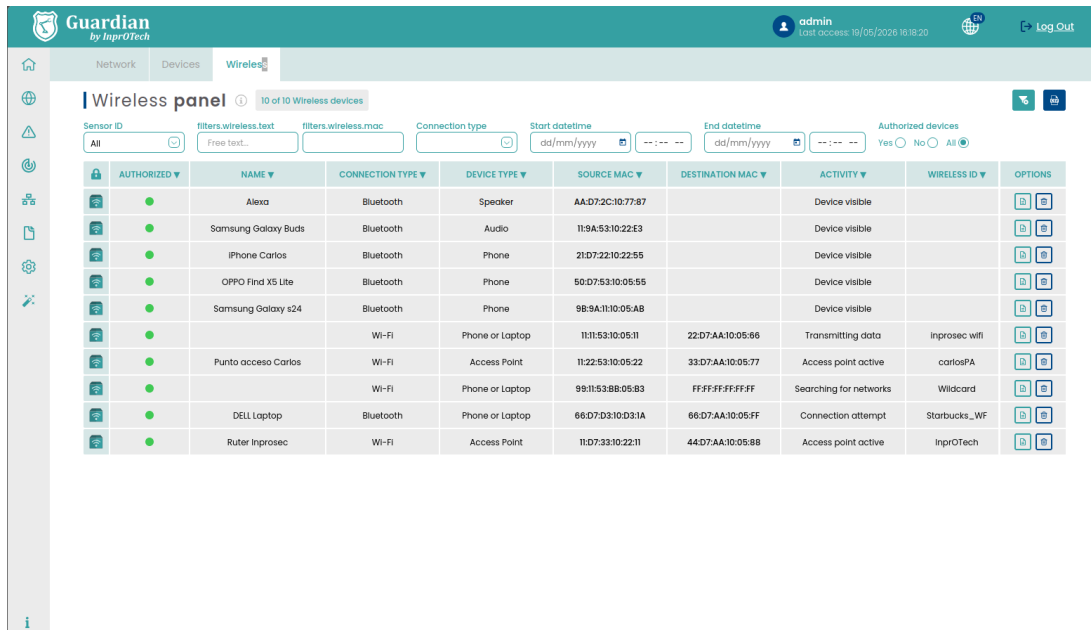
In the network section, there third tab allows access to the list of Wireless devices registered in the network.

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:
 - o Searching for networks: the device has the Wi-Fi antenna on and is searching for access points.
 - o Connection attempt: the device has tried connecting to an access point.
 - o Access point active: the device is functioning as an Access point.
 - o Transmitting data: the device is sending information to an access point.
 - o 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.



Guardian
by InproTech

admin
Last access: 19/05/2026 16:18:20

Log Out

Network Devices **Wireless**

Wireless panel 10 of 10 Wireless devices

Sensor ID: All filters.wireless.text filters.wireless.mac Connection type: Start datetime: dd/mm/yyyy End datetime: dd/mm/yyyy Authorized devices: Yes No All

AUTHORIZED	NAME	CONNECTION TYPE	DEVICE TYPE	SOURCE MAC	DESTINATION MAC	ACTIVITY	WIRELESS ID	OPTIONS
☒	Alexa	Bluetooth	Speaker	AA:D7:2C:10:77:87		Device visible		 
☒	Samsung Galaxy Buds	Bluetooth	Audio	11:9A:53:10:22:E3		Device visible		 
☒	iPhone Carlos	Bluetooth	Phone	21:D7:22:10:22:55		Device visible		 
☒	OPPO Find X5 Lite	Bluetooth	Phone	50:D7:53:10:05:55		Device visible		 
☒	Samsung Galaxy s24	Bluetooth	Phone	98:9A:11:10:05:A8		Device visible		 
☒	Punto acceso Carlos	Wi-Fi	Phone or Laptop	11:11:53:10:05:11	22:D7:AA:10:05:66	Transmitting data	inprosec wifi	 
☒		Wi-Fi	Access Point	11:22:53:10:05:22	33:D7:AA:10:05:77	Access point active	carlosPA	 
☒		Wi-Fi	Phone or Laptop	99:11:53:8B:05:83	FF:FF:FF:FF:FF:FF	Searching for networks	Wildcard	 
☒	DELL Laptop	Bluetooth	Phone or Laptop	66:D7:D3:10:D3:1A	66:D7:AA:10:05:FF	Connection attempt	Starbucks_WF	 
☒	Ruter Inprosec	Wi-Fi	Access Point	11:D7:33:10:22:11	44:D7:AA:10:05:88	Access point active	InproTech	 

Wireless device list



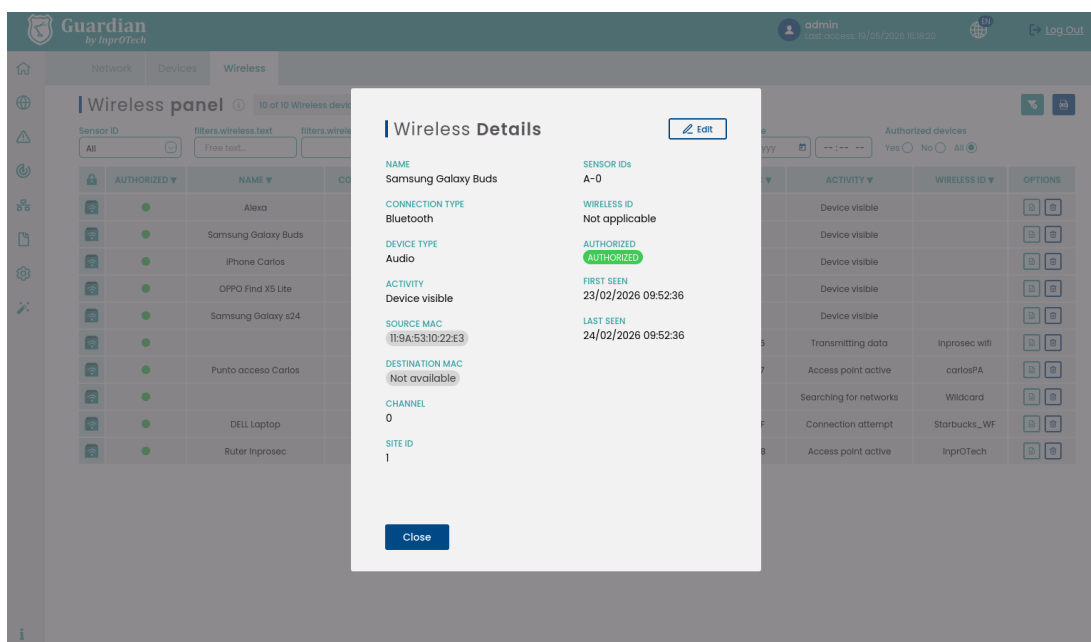
Wireless panel 10 of 10 Wireless devices

Sensor ID: All filters.wireless.text filters.wireless.mac Connection type: Start datetime: dd/mm/yyyy End datetime: dd/mm/yyyy Authorized devices: Yes No All

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

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).



Guardian
by InproTech

admin
Last access: 19/05/2026 16:18:20

Log Out

Network Devices **Wireless**

Wireless panel 10 of 10 Wireless devices

Sensor ID: All filters.wireless.text filters.wireless.mac Connection type: Start datetime: dd/mm/yyyy End datetime: dd/mm/yyyy Authorized devices: Yes No All

AUTHORIZED	NAME	CONNECTION TYPE	DEVICE TYPE	SOURCE MAC	DESTINATION MAC	ACTIVITY	WIRELESS ID	OPTIONS
☒	Alexa	Bluetooth	Speaker	AA:D7:2C:10:77:87		Device visible		 
☒	Samsung Galaxy Buds	Bluetooth	Audio	11:9A:53:10:22:E3		Device visible		 
☒	iPhone Carlos	Bluetooth	Phone	21:D7:22:10:22:55		Device visible		 
☒	OPPO Find X5 Lite	Bluetooth	Phone	50:D7:53:10:05:55		Device visible		 
☒	Samsung Galaxy s24	Bluetooth	Phone	98:9A:11:10:05:A8		Device visible		 
☒	Punto acceso Carlos	Wi-Fi	Phone or Laptop	11:11:53:10:05:11	22:D7:AA:10:05:66	Transmitting data	inprosec wifi	 
☒		Wi-Fi	Access Point	11:22:53:10:05:22	33:D7:AA:10:05:77	Access point active	carlosPA	 
☒		Wi-Fi	Phone or Laptop	99:11:53:8B:05:83	FF:FF:FF:FF:FF:FF	Searching for networks	Wildcard	 
☒	DELL Laptop	Bluetooth	Phone or Laptop	66:D7:D3:10:D3:1A	66:D7:AA:10:05:FF	Connection attempt	Starbucks_WF	 
☒	Ruter Inprosec	Wi-Fi	Access Point	11:D7:33:10:22:11	44:D7:AA:10:05:88	Access point active	InproTech	 

Wireless Details Edit

NAME: Samsung Galaxy Buds

CONNECTION TYPE: Bluetooth

DEVICE TYPE: Audio

ACTIVITY: Device visible

SOURCE MAC: 11:9A:53:10:22:E3

DESTINATION MAC: Not available

CHANNEL: 0

SITE ID: 1

SENSOR ID: A-0

WIRELESS ID: Not applicable

AUTHORIZED: AUTHORIZED

FIRST SEEN: 23/02/2026 09:52:36

LAST SEEN: 24/02/2026 09:52:36

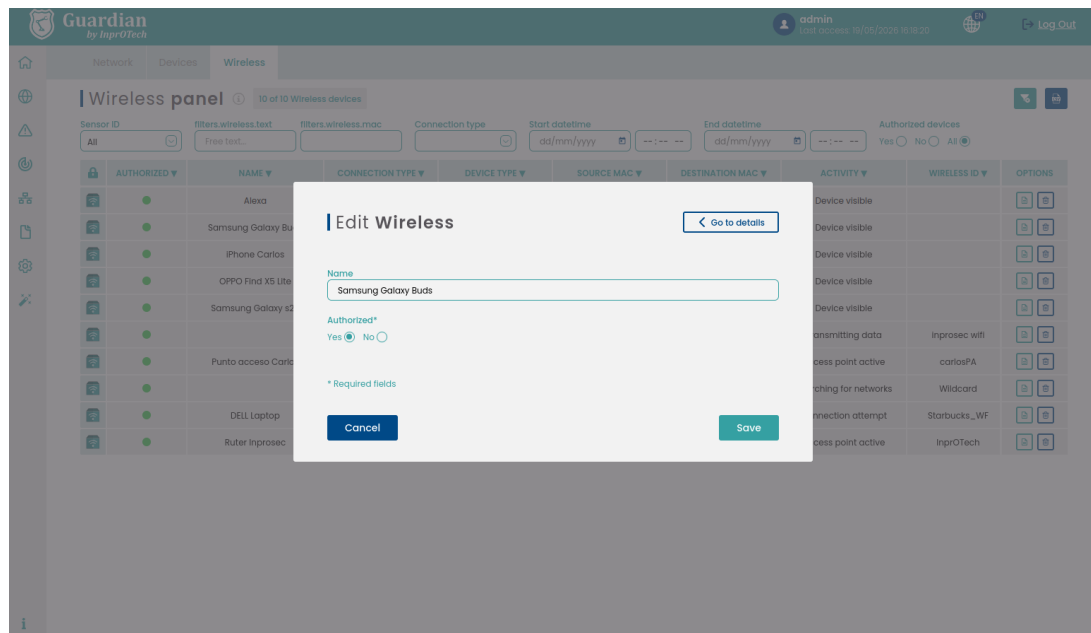
Close

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  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.

Guardian

by InprOTech

admin

Last access: 19/05/2026 16:18:20

Log Out

Network

Devices

Wireless

Device panel

14 of 14 Devices

Sensor ID

General search

Type

Role

Purdue level

IP address

MAC address

Show virtual MACs

All

Free text...

Yes

No

Pinned devices

Critical devices

Authorized devices

Yes

No

All

Yes

No

All

Yes

No

All

Yes

No

All

	STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	OPTIONS
		Hub-00	PC	2	00:07:32:62:4A:6A	10.25.197	HIGH	Critical (9.9)	Unknown	
		Brazo-Pruebas	Robot		00:09:91:FB:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Unknown	
		Reader-012	Controller Card		00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	Unknown	
		Scada S-AG	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Unknown	
		Camara-012	VA Camera	1	00:1F:F8:50:56:15	8.238.0.126	LOW	High (7.2)	Unknown	
		PC Office	PC	2	00:80:F4:88:4B:E4	10.254.254.12	HIGH	Critical (9.5)	Unknown	
		Printer-P13	Other		00:A0:45:D8:FF:CC	10.254.254.15	MEDIUM	High (7.5)	Unknown	
					24:09:95:30:0C:48	10.254.254.17		High (7.4)	Unknown	
		PLC-01	PLC	1	50:D7:53:10:03:72	10.254.254.21	HIGH	High (7.3)	Unknown	
		PLC-04	PLC	1	50:D7:53:10:03:73	10.254.254.24	MEDIUM	High (7.1)	Unknown	
		PLC-07	PLC	1	50:D7:53:10:03:74	10.254.254.26	MEDIUM	High (7.5)	Unknown	
		Sensor-ChuAV	Sensor	0	50:D7:53:10:03:96	10.254.254.28	MEDIUM	Critical (9.4)	Unknown	
		Sensor-ChuAB	Sensor		50:D7:53:10:05:43	10.254.254.29		High (8.5)	Unknown	
		HoneyPot-01	HoneyPot		78:AC:44:10:05:43				Unknown	

Create device

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

Edit

NAME

Hub-00

MAC

00:07:32:62:4A:6A

IPs

10.25.197 10.254.254.1 10.254.254.12 10.254.254.15 10.254.254.17 10.254.254.21 10.254.254.24 10.254.254.26 10.254.254.28 10.254.254.29

LAST CONNECTION

04/06/2024 13:13:20

TYPE

Other

PURDUE LEVEL

2

VENDOR

AAEON Technology Inc.

SITE ID

1

SENSOR IDs

sonda_vc

ROLE

Not applicable

SCORING

MEDIUM

SCORING DATE

06/05/2024 15:25:00

STATUS

UNAUTHORIZED UNPINNED

UNCRITICAL

LAST SCAN

24/05/2024 11:01:40

SCAN STATUS

SCANNING

UDP SCAN

10.25.197:10.254.254.1:10.254.254.12:10.254.254.15:10.254.254.17:10.254.254.21:10.254.254.24:10.254.254.26:10.254.254.28:10.254.254.29

TCP SCAN

10.25.197:10.254.254.1:10.254.254.12:10.254.254.15:10.254.254.17:10.254.254.21:10.254.254.24:10.254.254.26:10.254.254.28:10.254.254.29

Close

Device details

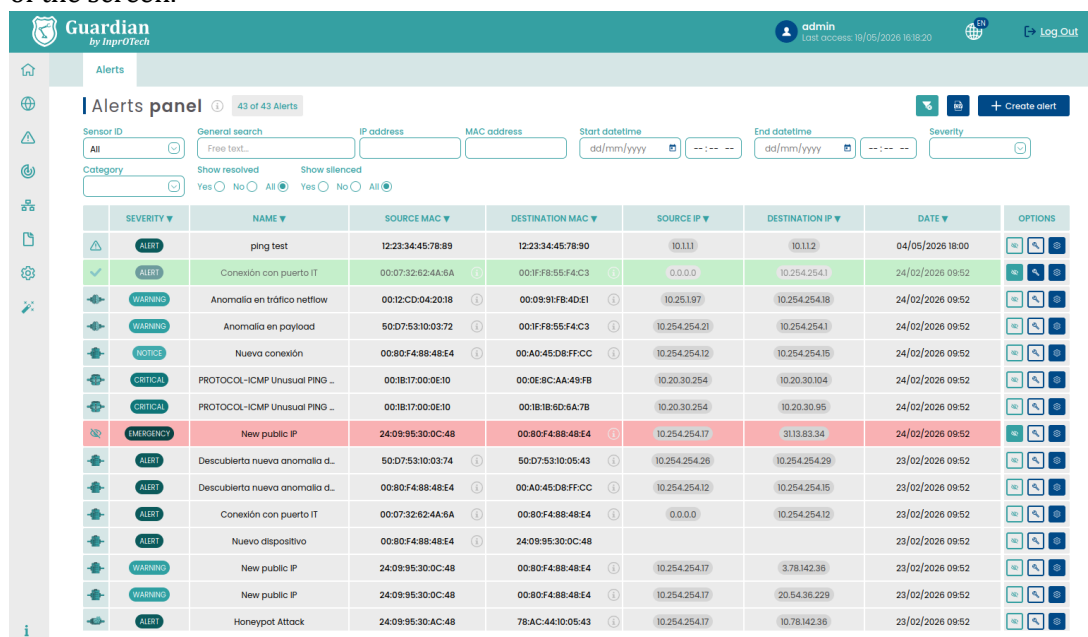
DISCLAIMER: Given the active nature of this operation, although no operational impact has been observed, it cannot be completely ruled out. It is therefore up to the customer to

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.



SEVERITY	NAME	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DATE	OPTIONS
ALERT	ping test	12:23:34:45:78:89	12:23:34:45:78:90	10.11.1	10.11.2	04/05/2026 18:00	
ALERT	Conexión con puerto IT	00:07:32:62:4A:6A	00:1F:F8:55:F4:C3	0.0.0.0	10.254.254.1	24/02/2026 09:52	
WARNING	Anomalia en tráfico netflow	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.254.197	10.254.254.18	24/02/2026 09:52	
WARNING	Anomalia en payload	50:D7:53:10:03:72	00:1F:F8:55:F4:C3	10.254.254.21	10.254.254.1	24/02/2026 09:52	
NOTICE	Nueva conexión	00:80:F4:88:48:E4	00:A0:45:D8:FF:C0	10.254.254.12	10.254.254.15	24/02/2026 09:52	
CRITICAL	PROTOCOL-ICMP Unusual PING ..	00:1B:17:00:0E:10	00:0E:8C:AA:49:FB	10.20.30.254	10.20.30.104	24/02/2026 09:52	
CRITICAL	PROTOCOL-ICMP Unusual PING ..	00:1B:17:00:0E:10	00:1B:1B:6D:8A:7B	10.20.30.254	10.20.30.95	24/02/2026 09:52	
EMERGENCY	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	3113.83.34	24/02/2026 09:52	
ALERT	Descubierta nueva anomalia d..	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.26	10.254.254.29	23/02/2026 09:52	
ALERT	Descubierta nueva anomalia d..	00:80:F4:88:48:E4	00:A0:45:D8:FF:C0	10.254.254.12	10.254.254.15	23/02/2026 09:52	
ALERT	Conexión con puerto IT	00:07:32:62:4A:6A	00:80:F4:88:48:E4	0.0.0.0	10.254.254.12	23/02/2026 09:52	
ALERT	Nuevo dispositivo	00:80:F4:88:48:E4	24:09:95:30:0C:48			23/02/2026 09:52	
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	3.78.142.36	23/02/2026 09:52	
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:88:48:E4	10.254.254.17	20.54.36.229	23/02/2026 09:52	
ALERT	Honeypot Attack	24:09:95:30:AC:48	78:AC:44:10:05:43	10.254.254.17	10.78.142.36	23/02/2026 09:52	

Alerts list.

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

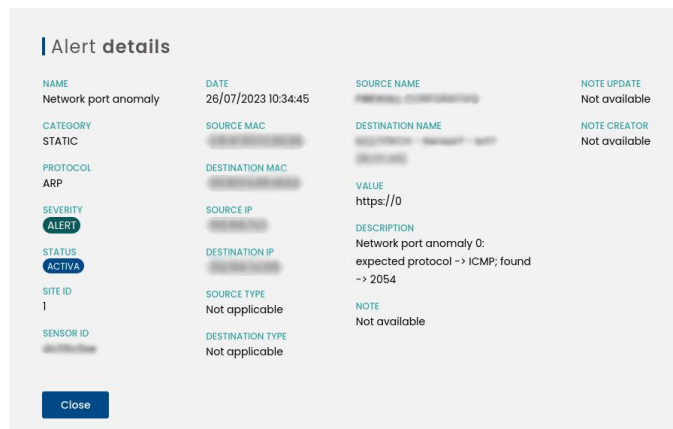
- Severity: Classification of the alert according to the impact it could have on the organization.
- Name: Defined name of the alert.
- Source MAC: MAC of the alert generating device.
- Destination MAC: MAC of the device to which the action was directed.
- Source IP: IP of the device generating the alert.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

NAME Network port anomaly	DATE 26/07/2023 10:34:45	SOURCE NAME [redacted]	NOTE UPDATE Not available
CATEGORY STATIC	SOURCE MAC [redacted]	DESTINATION NAME [redacted]	NOTE CREATOR Not available
PROTOCOL ARP	DESTINATION MAC [redacted]	VALUE https//0	
SEVERITY ALERT	SOURCE IP [redacted]	DESCRIPTION Network port anomaly 0: expected protocol -> ICMP; found -> 2054	
STATUS ACTIVA	DESTINATION IP [redacted]	NOTE Not available	
SITE ID 1	SOURCE TYPE Not applicable		
SENSOR ID [redacted]	DESTINATION TYPE Not applicable		

Close

Alert details

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



Alerts panel 37091 of 37091 Alerts

Sensor ID: [dropdown] General search: [text input] MAC address: [text input] IP address: [text input] Start datetime: [datetime picker] End datetime: [datetime picker] Severity: [dropdown] Category: [dropdown]

Show resolved: Yes ☐ No ☐ All ☒ Show silenced: Yes ☐ No ☐ All ☒

+ Create alert

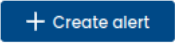
Available alert filters

This filtering can be done according to:

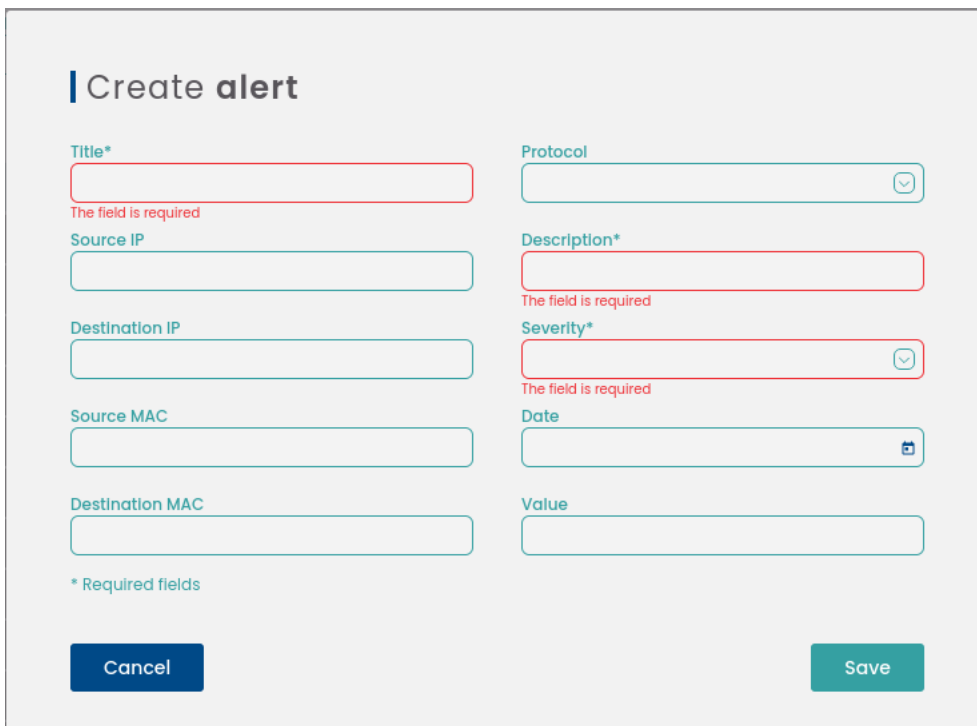
- Probe ID, to filter by zone of the industrial network and/or headquarters.
- General search: Search by entering a text containing the alarm (including in your notes).
- IP address of the device
- MAC address of the device
- Date and time of start of alert search
- Date and time of alert search end 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:



The image shows a 'Create alert' pop-up window. It has a title bar 'Create alert'. The form is divided into two columns. The left column contains: 'Title*' (text input, red border, 'The field is required' error), 'Source IP' (text input), 'Destination IP' (text input), 'Source MAC' (text input), and 'Destination MAC' (text input). The right column contains: 'Protocol' (dropdown), 'Description*' (text input, red border, 'The field is required' error), 'Severity*' (dropdown, red border, 'The field is required' error), 'Date' (calendar icon), and 'Value' (text input). At the bottom left is a 'Cancel' button and at the bottom right is a 'Save' button. A note '* Required fields' is at the bottom left of the form area.

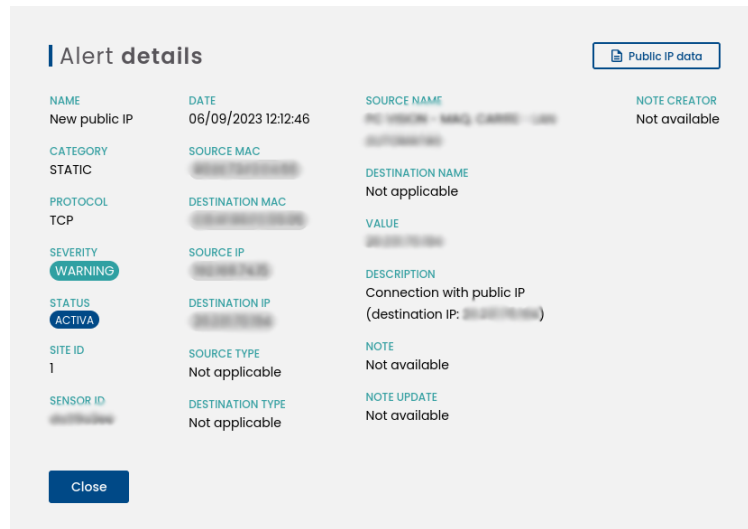
Alert creation

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:



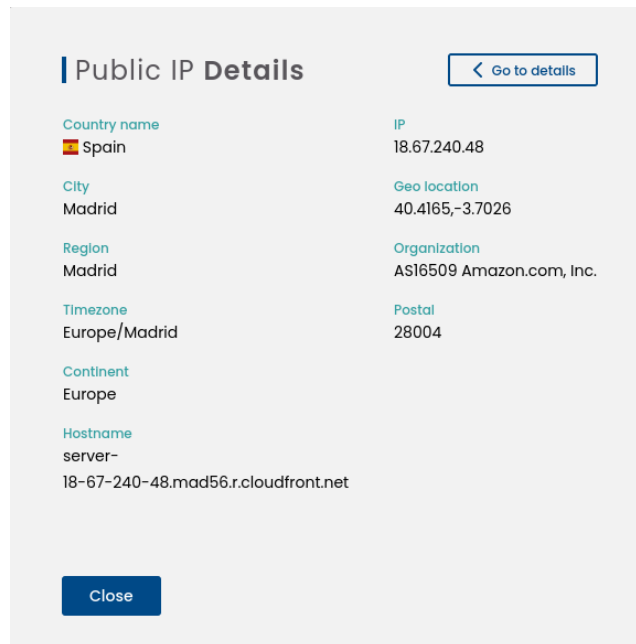
Alert details [Public IP data](#)

NAME New public IP	DATE 06/09/2023 12:12:46	SOURCE NAME [REDACTED]	NOTE CREATOR Not available
CATEGORY STATIC	SOURCE MAC [REDACTED]	DESTINATION NAME Not applicable	
PROTOCOL TCP	DESTINATION MAC [REDACTED]	VALUE [REDACTED]	
SEVERITY WARNING	SOURCE IP [REDACTED]	DESCRIPTION Connection with public IP (destination IP: [REDACTED])	
STATUS ACTIVA	DESTINATION IP [REDACTED]	NOTE Not available	
SITE ID 1	SOURCE TYPE Not applicable	NOTE UPDATE Not available	
SENSOR ID [REDACTED]	DESTINATION TYPE Not applicable		

[Close](#)

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 [Go to details](#)

Country name Spain	IP 18.67.240.48
City Madrid	Geo location 40.4165,-3.7026
Region Madrid	Organization AS16509 Amazon.com, Inc.
Timezone Europe/Madrid	Postal 28004
Continent Europe	
Hostname server-18-67-240-48.mad56.r.cloudfront.net	

[Close](#)

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. This information enriches the alert with more reputational details, and in case it detects that the public address involved is suspicious, it changes the severity, the description, and marks it in red.

Guardian

by InprOTech

admin

Last access: 19/05/2026 16:18:20

EN

Log Out

Alerts

Alerts panel

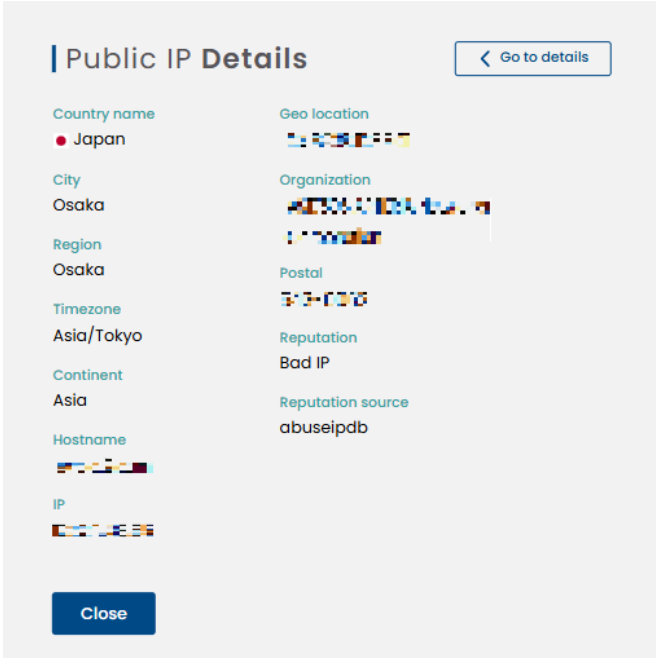
43 of 43 Alerts

<

Malicious public IP alert highlighted in red

Alert details			
Public IP data			
NAME	DATE	SOURCE NAME	NOTE
New public IP	09/06/2025 09:09:53	Not applicable	Not available
CATEGORY	SOURCE MAC	DESTINATION NAME	NOTE UPDATE
STATIC	00:80:F4:88-48:E4	Not applicable	Not available
PROTOCOL	DESTINATION MAC	VALUE	NOTE CREATOR
TCP	00:80:F4:88-48:E4	10.254.254.17	Not available
SEVERITY	SOURCE IP	DESCRIPTION	
EMERGENCY	10.254.254.17	Connection with public IP (destination IP: 10.254.254.26). This IP has been listed as abusive and/or malicious. We recommend to block traffic to and from this IP.	
STATUS	DESTINATION IP		
ACTIVE	10.254.254.12		
SITE ID	SOURCE TYPE		
1	Not applicable		
SENSOR ID	DESTINATION TYPE		
sonda	Not applicable		
Close			

Alert details with enriched information



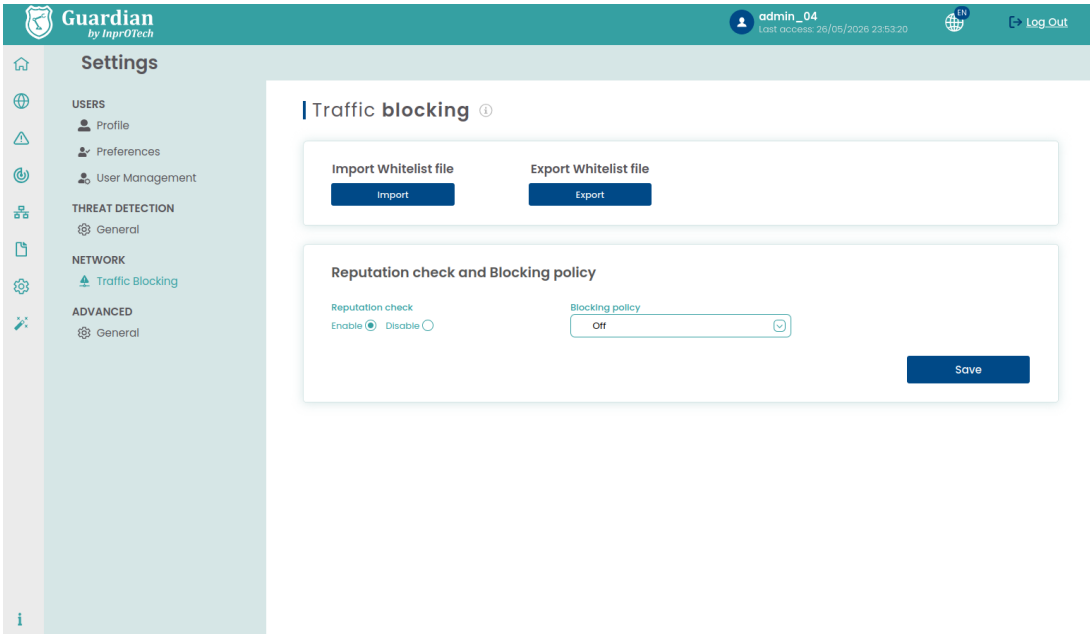
Public IP Details [Go to details](#)

Country name	Geo location
Japan	
City	Organization
Osaka	
Region	Postal
Osaka	
Timezone	Reputation
Asia/Tokyo	Bad IP
Continent	Reputation source
Asia	abuseipdb
Hostname	
	
IP	
	

[Close](#)

Public IP details with reputational information

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.



Guardian by InprOTech admin_04 Last access: 26/05/2026 23:53:20 [Log Out](#)

Settings

- USERS
 - Profile
 - Preferences
 - User Management
- THREAT DETECTION
 - General
- NETWORK
 - Traffic Blocking**
- ADVANCED
 - General

Traffic blocking

Import Whitelist file [Import](#) Export Whitelist file [Export](#)

Reputation check and Blocking policy

Reputation check: ☒ Enable ☐ Disable

Blocking policy: [Save](#)

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

* The availability of the non-informative options will depend on the customer context, in particular the manufacturer/model of the firewall that Guardian has to communicate with. In case of doubt or if you require more information, please contact the support team.

- 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.

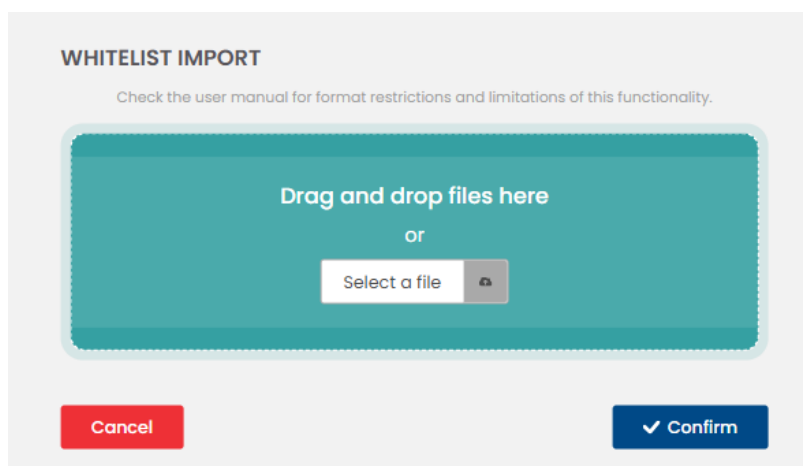
The Blocking Policy can also be disabled. In this case, all information regarding the IP reputation in the alerts will be disabled, as well as the blocking rules (via sending command to the firewall to lift the address blocking rule). This information is not deleted, and will be reapplied if the Blocking 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.

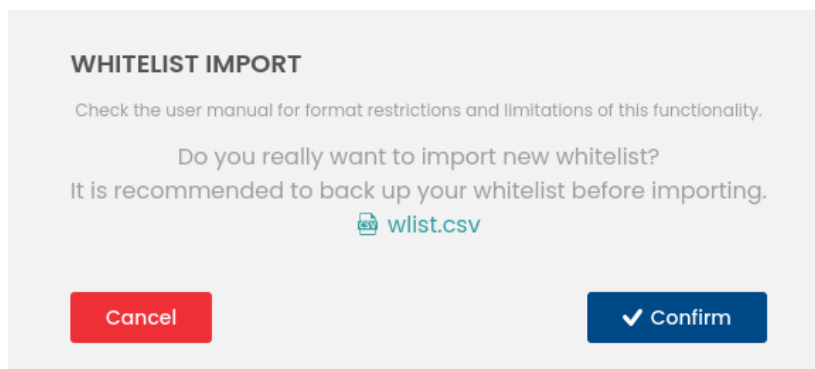
4.3.3 IP whitelist

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  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 influences the public IP alerts already in the database:

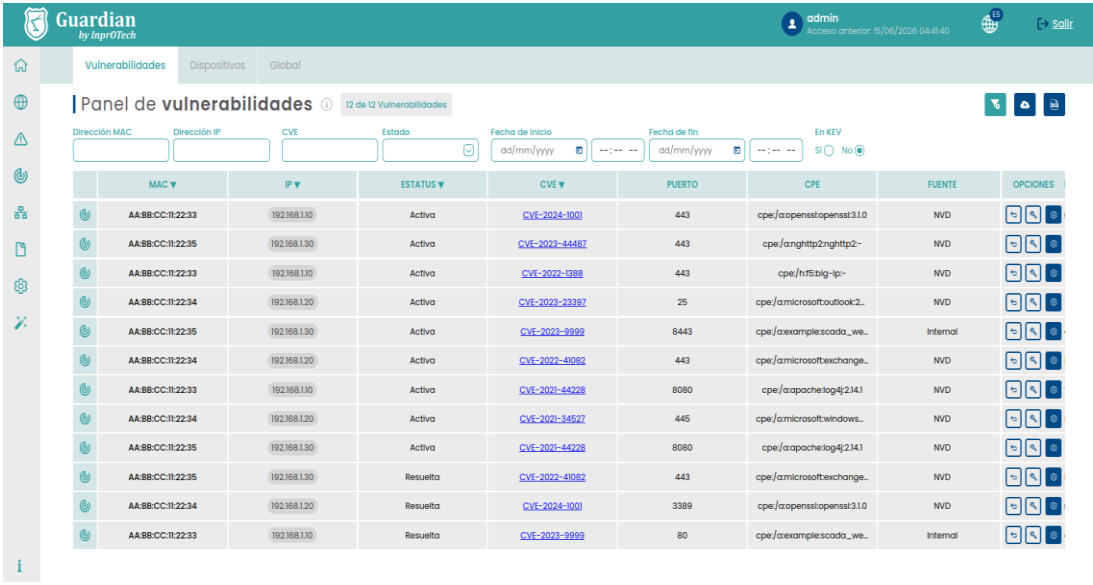
- those alerts with IPs that have the reputation already processed before, and that are included in the new whitelist, are returned to the original state with the status *'reputation: Wlisted'*.
- Those alerts with IPs within the previous whitelist, but which are outside the new whitelist, have their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



Guardian
by InprOTech

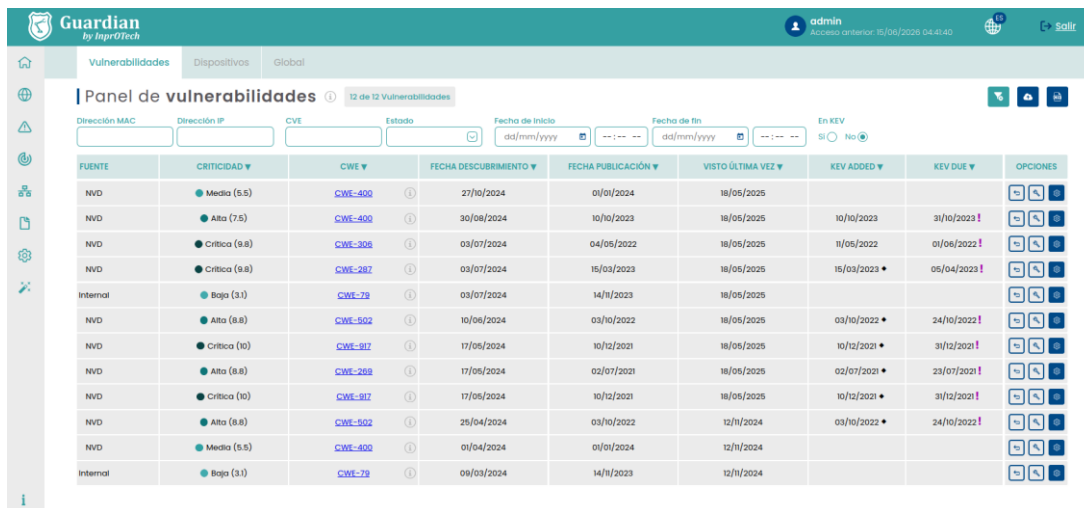
admin
Acceso anterior: 15/06/2026 04:40:40

Vulnerabilidades | Dispositivos | Global

Panel de vulnerabilidades 12 de 12 Vulnerabilidades

Dirección MAC: Dirección IP: CVE: Estado: Fecha de inicio: Fecha de fin: En KEV: Si No

MAC	IP	ESTATUS	CVE	PUERTO	CPE	FUENTE	OPCIONES
AA:BB:CC:11:22:33	192.168.1.10	Activa	CVE-2024-1001	443	cpe:/a:openstopenst:3.1.0	NVD	  
AA:BB:CC:11:22:35	192.168.1.30	Activa	CVE-2023-44487	443	cpe:/a:nghttp2:nghttp2-	NVD	  
AA:BB:CC:11:22:33	192.168.1.10	Activa	CVE-2022-1388	443	cpe:/h:fs:ip-	NVD	  
AA:BB:CC:11:22:34	192.168.1.20	Activa	CVE-2023-23397	25	cpe:/a:microsoft:outlook2-	NVD	  
AA:BB:CC:11:22:35	192.168.1.30	Activa	CVE-2023-9999	8443	cpe:/a:examplescoda_we...	Internal	  
AA:BB:CC:11:22:34	192.168.1.20	Activa	CVE-2022-41082	443	cpe:/a:microsoft:exchange...	NVD	  
AA:BB:CC:11:22:33	192.168.1.10	Activa	CVE-2021-44228	8080	cpe:/a:apache:log4j2:1.4.1	NVD	  
AA:BB:CC:11:22:34	192.168.1.20	Activa	CVE-2021-34527	445	cpe:/a:microsoft:windows...	NVD	  
AA:BB:CC:11:22:35	192.168.1.30	Activa	CVE-2021-44228	8080	cpe:/a:apache:log4j2:1.4.1	NVD	  
AA:BB:CC:11:22:35	192.168.1.30	Resuelta	CVE-2022-41082	443	cpe:/a:microsoft:exchange...	NVD	  
AA:BB:CC:11:22:34	192.168.1.20	Resuelta	CVE-2024-1001	3389	cpe:/a:openstopenst:3.1.0	NVD	  
AA:BB:CC:11:22:33	192.168.1.10	Resuelta	CVE-2023-9999	80	cpe:/a:examplescoda_we...	Internal	  



FUENTE	CRITICIDAD	CVE	FECHA DESCUBRIMIENTO	FECHA PUBLICACIÓN	VISTO ÚLTIMA VEZ	KEV ADDED	KEV DUE	OPCIONES
NVD	Media (5.5)	CWE-400	27/10/2024	01/01/2024	18/05/2025			
NVD	Alta (7.5)	CWE-509	30/08/2024	10/10/2023	18/05/2025	10/10/2023	31/10/2023	
NVD	Critica (9.8)	CWE-308	03/07/2024	04/05/2022	18/05/2025	11/05/2022	01/06/2022	
NVD	Critica (9.8)	CWE-287	03/07/2024	15/03/2023	18/05/2025	15/03/2023	05/04/2023	
Internal	Baja (3.1)	CWE-79	03/07/2024	14/11/2023	18/05/2025			
NVD	Alta (8.8)	CWE-502	10/08/2024	03/10/2022	18/05/2025	03/10/2022	24/10/2022	
NVD	Critica (10)	CWE-917	17/05/2024	10/12/2021	18/05/2025	10/12/2021	31/12/2021	
NVD	Alta (8.8)	CWE-289	17/05/2024	02/07/2021	18/05/2025	02/07/2021	23/07/2021	
NVD	Critica (10)	CWE-917	17/05/2024	10/12/2021	18/05/2025	10/12/2021	31/12/2021	
NVD	Alta (8.8)	CWE-502	25/04/2024	03/10/2022	12/11/2024	03/10/2022	24/10/2022	
NVD	Media (5.5)	CWE-400	01/04/2024	01/01/2024	12/11/2024			
Internal	Baja (3.1)	CWE-79	09/03/2024	14/11/2023	12/11/2024			

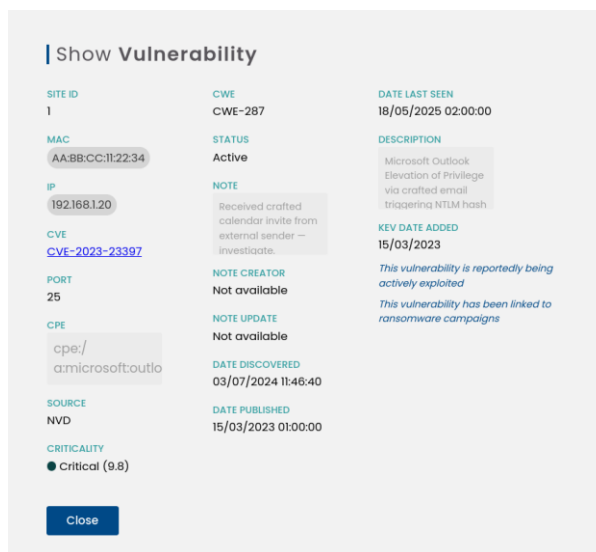
View of the Vulnerabilities Panel

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) and the CISA catalogue.

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 of 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.
- **Criticality:** 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.
- **KEV ADDED:** KEV stands for "Known Exploited Vulnerabilities." CISA catalogue of CVEs actively exploited in the wild, with the inclusion date and a ♦ when the CVE is being linked to ransomware campaigns.
- **KEV DUE:** Deadline proposed by the CISA administration to encourage the resolution of the corresponding CVE.
- **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
- Presence in KEV catalogue

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

- Criticality
- 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

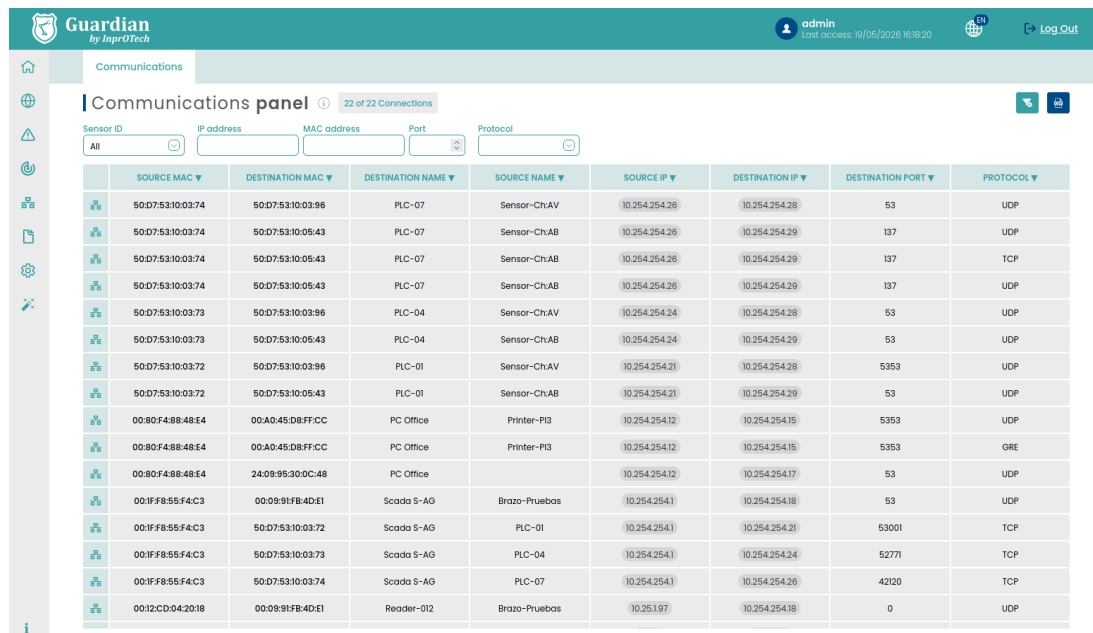
Offers the vulnerabilities found in the network, sorted by the available devices.

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.



Guardian
by InprOTech

admin
Last access: 19/05/2026 16:18:20

Log Out

Communications panel 22 of 22 Connections

Sensor ID: All IP address: MAC address: Port: Protocol:

	SOURCE MAC ▼	DESTINATION MAC ▼	DESTINATION NAME ▼	SOURCE NAME ▼	SOURCE IP ▼	DESTINATION IP ▼	DESTINATION PORT ▼	PROTOCOL ▼
	50:D7:53:10:03:74	50:D7:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	UDP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	TCP
	50:D7:53:10:03:74	50:D7:53:10:05:43	PLC-07	Sensor-ChAB	10.254.254.26	10.254.254.29	137	UDP
	50:D7:53:10:03:73	50:D7:53:10:03:96	PLC-04	Sensor-ChAV	10.254.254.24	10.254.254.28	53	UDP
	50:D7:53:10:03:73	50:D7:53:10:05:43	PLC-04	Sensor-ChAB	10.254.254.24	10.254.254.29	53	UDP
	50:D7:53:10:03:72	50:D7:53:10:03:96	PLC-01	Sensor-ChAV	10.254.254.21	10.254.254.28	5353	UDP
	50:D7:53:10:03:72	50:D7:53:10:05:43	PLC-01	Sensor-ChAB	10.254.254.21	10.254.254.29	53	UDP
	00:80:F4:8B:48:E4	00:A0:45:D8:FF:C0	PC Office	Printer-P13	10.254.254.12	10.254.254.15	5353	UDP
	00:80:F4:8B:48:E4	00:A0:45:D8:FF:C0	PC Office	Printer-P13	10.254.254.12	10.254.254.15	5353	GRE
	00:80:F4:8B:48:E4	24:09:95:30:0C:48	PC Office		10.254.254.12	10.254.254.17	53	UDP
	00:1F:85:F4:C3	00:09:91:F8:4D:E1	Scada S-AG	Brazo-Pruebas	10.254.254.1	10.254.254.18	53	UDP
	00:1F:85:F4:C3	50:D7:53:10:03:72	Scada S-AG	PLC-01	10.254.254.1	10.254.254.21	53001	TCP
	00:1F:85:F4:C3	50:D7:53:10:03:73	Scada S-AG	PLC-04	10.254.254.1	10.254.254.24	52771	TCP
	00:1F:85:F4:C3	50:D7:53:10:03:74	Scada S-AG	PLC-07	10.254.254.1	10.254.254.26	42120	TCP
	00:12:CD:04:20:18	00:09:91:F8:4D:E1	Reader-012	Brazo-Pruebas	10.25.197	10.254.254.18	0	UDP

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.

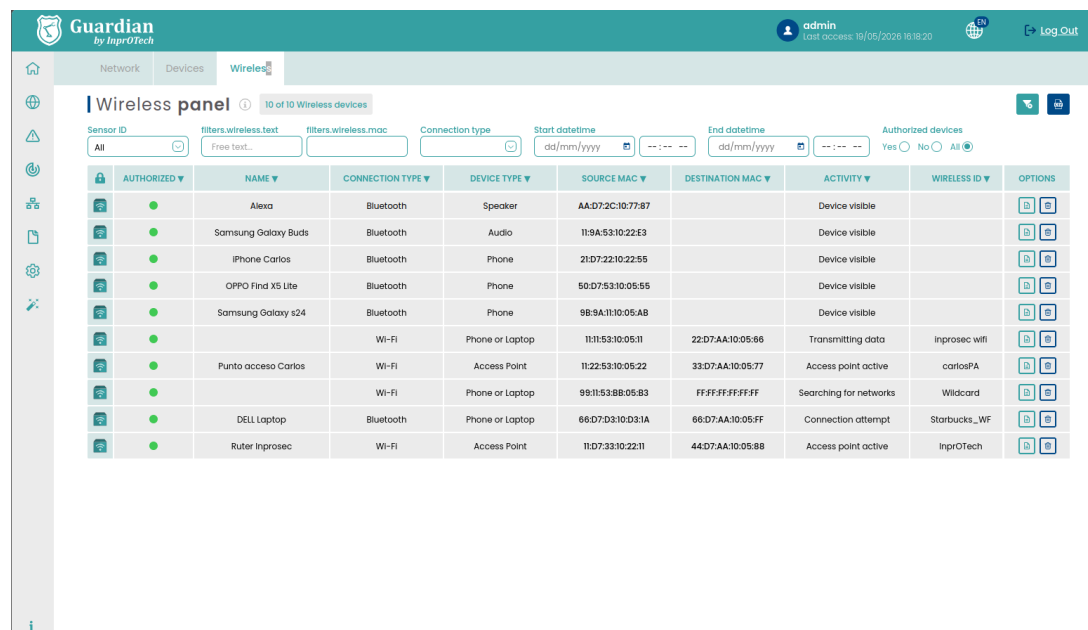
A communication is understood as the grouping of connections between MAC, IP, and source port, and the same for the destination. It is considered a new communication if there is a change of protocol.



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 section Advanced General, the user can download the system logs to a file on their Download folder. The log format is a small variation over the python logging standard:

```
[2026/05/26 23:42:33] DEBUG loggingguardian >> GET /alert
[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {"count": "100", "offset": "0", "order_type": "desc", "order_property": "timestamp", "silenced": "false", "resolved": "false"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> Response | HTTP 200 | [{"elements": [{"id": 1, "title": "aparici\u00f3n fantasmal", "timestamp": 1779832800.0, "severity": "emergency", "silenced": false, "resolved": false, "blocked": false, "id_fabrica": 1, "id_sonda": null, "category": null, "description": "Prepara los datos de la muerte", "value": null, "src_ip": "127.1.1.2", "src_mac": "aa:bb:cc:11:22:33", "src_device_type": null, "src_device_name": "jarl", "dst_ip": "192.121.1.2", "dst_mac": "11:22:11:22:11:22", "dst_device_type": null, "dst_device_name": null, "protocol": "17", "note": null, "creator": null, "timestamp_note": null, "others": null}], "has_more_elements": false, "offset": 0}

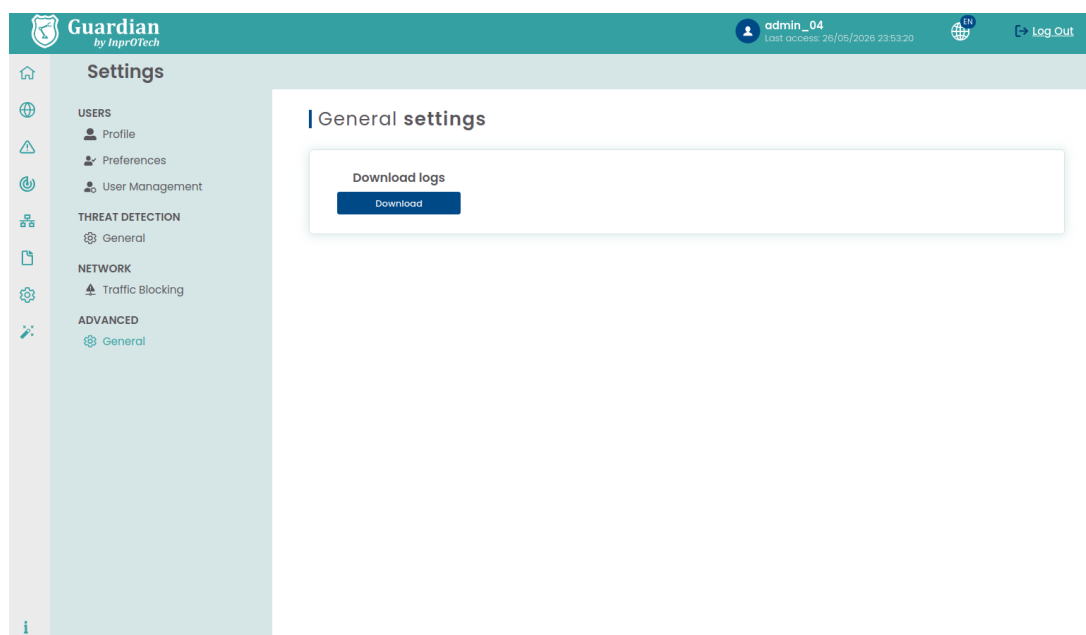
[2026/05/26 23:42:33] DEBUG loggingguardian >> GET /alert/module
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /alert HTTP/1.1 ::200::

[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {"order_property": "id", "order_type": "asc"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> GET /vulnerabilities/count
[2026/05/26 23:42:33] DEBUG loggingguardian >> Response | HTTP 200 | []
```

```
[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {"status": "active"}
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /alert/module HTTP/1.1 ::200::

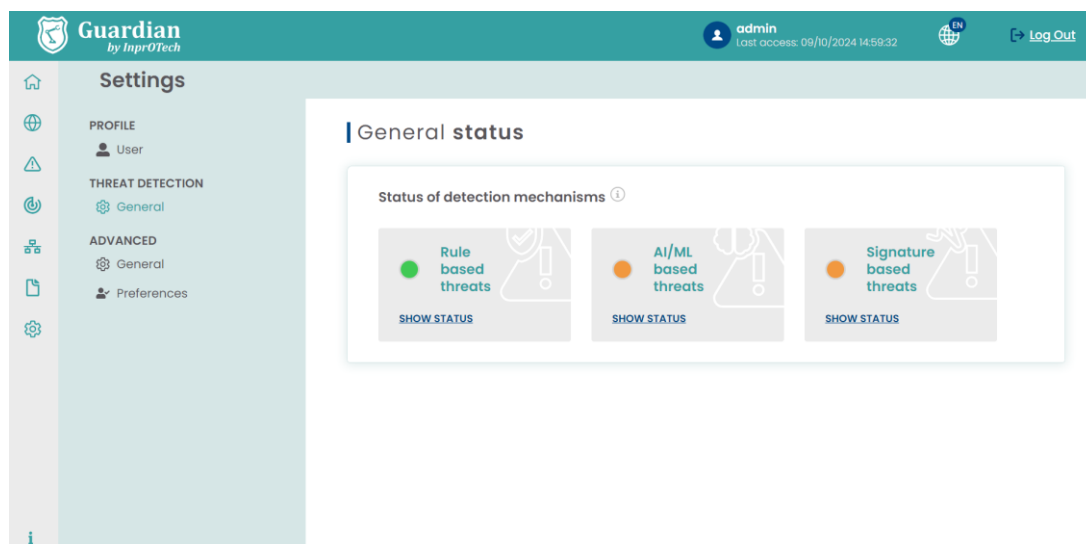
[2026/05/26 23:42:33] DEBUG loggingguardian >> Response | HTTP 200 | {"count": 18}
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /vulnerabilities/count HTTP/1.1 ::200::

[2026/05/26 23:42:33] DEBUG loggingguardian >> → GET /algorithm/status
[2026/05/26 23:42:33] DEBUG loggingguardian >> Params: {}
[2026/05/26 23:42:33] DEBUG loggingguardian >> Response | HTTP 200 | [{"id": 5, "id_fabrica": 1, "status": "Inactive",
"algorithm": "inprotech_anagram", "timestamp": 1779667846.648889}]
[2026/05/26 23:42:33] DEBUG loggingguardian >> 192.168.1.64 [f001|u000] GET /algorithm/status HTTP/1.1 ::200::
```



Export logs section

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

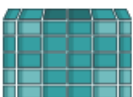
	HANDSET	2
	RTU	1
	VS-CAM	1
	BARCODE READER	1
	PLC	1
	ROBOT	0
	FREQUENCY VARIATOR	0
	CONTROLLER CARD	0
	SENSOR	0
	AFD	0
	SWITCH	Various
	ROUTER	Various
	FIREWALL	Various
	OTHER	Various
	HONEYPOT	Various

Table 1: Representative Icons of Devices

7 ANNEX III: Alert icons.

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