

User Manual.

Product documentation



OBSERVE | UNDERSTAND | PROTECT



DATE: 31/08/2026

REFERENCE: User Manual

VERSION: 1.0

This document has been prepared by Greinfort for Greinfort's exclusive use and its contents are confidential. It may not be disclosed to third parties or used for purposes other than those for which it was delivered without Greinfort's prior written permission. If delivered under a contract, its use and disclosure shall be limited to what is expressly authorised in that contract. Greinfort shall not be held liable for any errors or omissions in the preparation of this document.

Contents:

1. Introduction.....	5
2. Getting started.....	6
2.1. Access to web consoles	6
2.2. Device list organization.....	9
2.3. Wireless Device Analytics	11
2.4. Rule settings	11
2.5. Scenarios	14
2.6. Active Device Scanner (Optional)	14
2.7. Active Response Settings.....	14
2.8. Setting up reports	14
2.9. Export alerts (optional).....	14
2.10. Continuous control panel (optional)	15
2.11. Licenses	15
2.12. Access Control and Roles	15
2.13. Custom fields.....	16
3. Quick Guide.....	16
3.1. Menu	16
3.2. Main panel	17
3.3. Network Map.....	18
3.4. Device List	20
3.5. Alerts dashboard	21
3.6. List of communications.....	22
3.7. Reports.....	22
3.8. Scenarios	23
3.8.1. User Profile	24
3.8.2. User preferences.....	24
3.8.3. Notification of alerts.....	25
3.8.4. User Management.....	25
3.8.5. Traffic Blocking Settings	26
3.8.6. Information	27
4. Application Management.....	28
4.1. Main panel	28
Greinfort Solutions S.L.	3
info@greinfort.com	
www.greinfort.com	

4.1.1. Asset Summary	28
4.1.2. Quick Links	29
4.1.3. Network Traffic Graph.....	30
4.1.4. Alert Graph.....	30
4.1.5. Latest reports.....	30
4.2. Network map and device list.....	31
4.2.1. Network Map	31
4.2.2. Device List.....	32
4.3. Alerts dashboard	41
4.3.1. Public IP.....	43
4.3.2. IP Reputation and Blocking Policy.....	44
4.3.3. IP Whitelisting.....	46
4.4. Vulnerability analysis.....	47
4.4.1. Vulnerability Dashboard	47
4.4.2. Device Stats.....	50
4.4.3. Global Statistics	50
4.5. Communications	50
4.6. Reports	51
4.7. Other scenarios.....	51
5. ANNEX I: Device Classification and Alerts	53
5.1. Device Classification	53
5.1.1. According to the State.....	53
5.2. Alert Classification.....	53
5.2.1. According to the State.....	53
5.2.2. Depending on the severity.....	53
6. ANNEX II: Purdue Asset and Level Icons.....	54
7. ANNEX III: Alert Icons.....	56

1. Introduction

Greinfort is an asset detection and anomaly monitoring tool capable of identifying cybersecurity threats in industrial environments. It analyzes network traffic, identifies assets, produces comprehensive reports, and issues alerts using static rules, IDS signatures, and artificial intelligence to facilitate threat mitigation in the industrial network.

Greinfort's interface is interactive, easy to understand and simple to use. In addition, it is available in English, Spanish, Catalan, Basque and Galician.

The interface has been developed with the Angular framework and following the best security practices and methodologies, in order to guarantee safe navigation through information.

The web application provides a comprehensive overview of the following:

- **Continuous Dashboard:** Self-updating dashboard to monitor key asset, threat, and reporting aspects 24/7 in an operations center.
- **Quick access:** Alerts, vulnerabilities, algorithms, and active rules.
- **Network traffic graph:** Representation of traffic sent and received during the last 24 hours and comparison to the same period seven days earlier.
- **Alert graph:** Graph of the alerts received in the last 7 days, differentiated by color according to their level of severity and the trend they follow over time.
- **Network map:** Visualization of all network devices, their connections, and the network structure of the organization. It also allows to identify connected devices that have not been considered legitimate.
- **Device Manager:** List of wired or wireless assets for identification and management. It includes the identification and tagging of devices, as well as their blacklisting according to the level of criticality. In addition, it allows to define custom fields to classify and filter network devices using a virtual inventory that can be organized, filtered, and exported.
- **Alert Manager:** List of events and alerts from your organization's OT network, classified by severity level. They are color-coded and detailed with dynamic information. They are categorized according to their status (resolved or muted) and are generated from heuristics, IDS signatures, and artificial intelligence or machine learning.
- **Integration with third-party systems (SIEM):** Greinfort offers the ability to send the active alerts generated to a third-party system such as a SIEM (Security Information and Event Management), for ingestion and correlation with other log sources. To do this, it uses the *rsyslog protocol*.
- **Vulnerability Manager:** Ability to perform vulnerability scans on demand and only on selected devices.
- **Public IP Address Reputation:** When connections are established with public IP addresses, their reputation is automatically analyzed, and those for which active mitigation action is recommended are visually highlighted. It is also possible to upload a list of IP addresses that will always be allowed.
- **Communications list:** list of all communications made between OT devices in the organization's network and information about them.
- **Reporting:** Compilation of information about the network, devices, indicators, etc., for future analysis and verification at both technical and business levels.

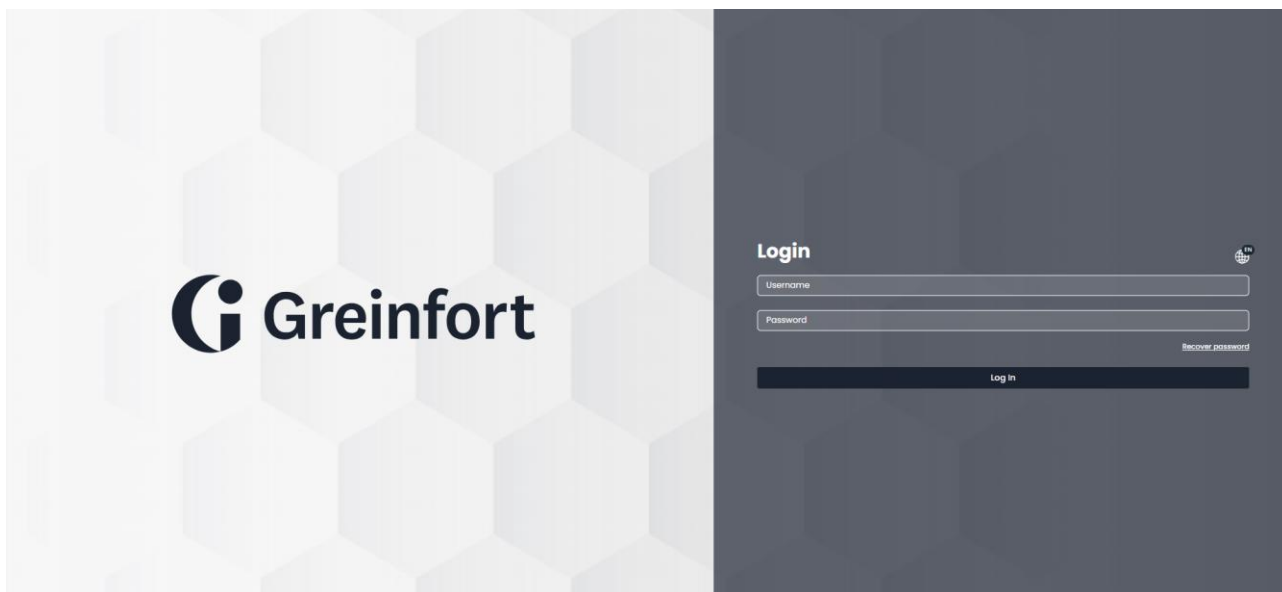
In addition to the use of the application, the service requires a number of preparations for initial onboarding, including proper data collection, deployment, installation, and fine-tuning of the

solution. These tasks allow for maximum performance from the service and are based on actions such as those outlined in the next section.

2. Getting started

2.1. Access to web consoles

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

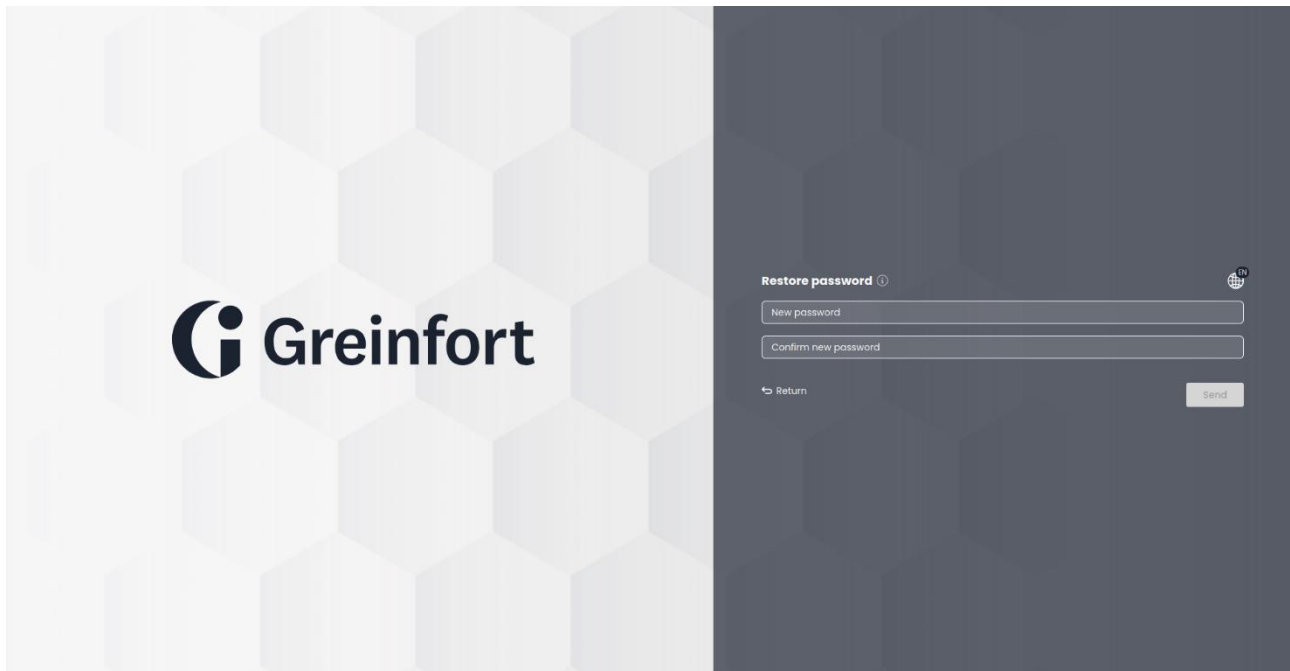


Greinfort login screen

The language can be selected at any time using the world map icon (English, Spanish, Catalan, Basque or Galician).

To authenticate, user must enter your assigned username and password. If the second authentication factor is enabled, must also enter the one-time token received via email into the account associated with the service.

For security reasons, when a user logs in for the first time, or when an administrator has flagged 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:

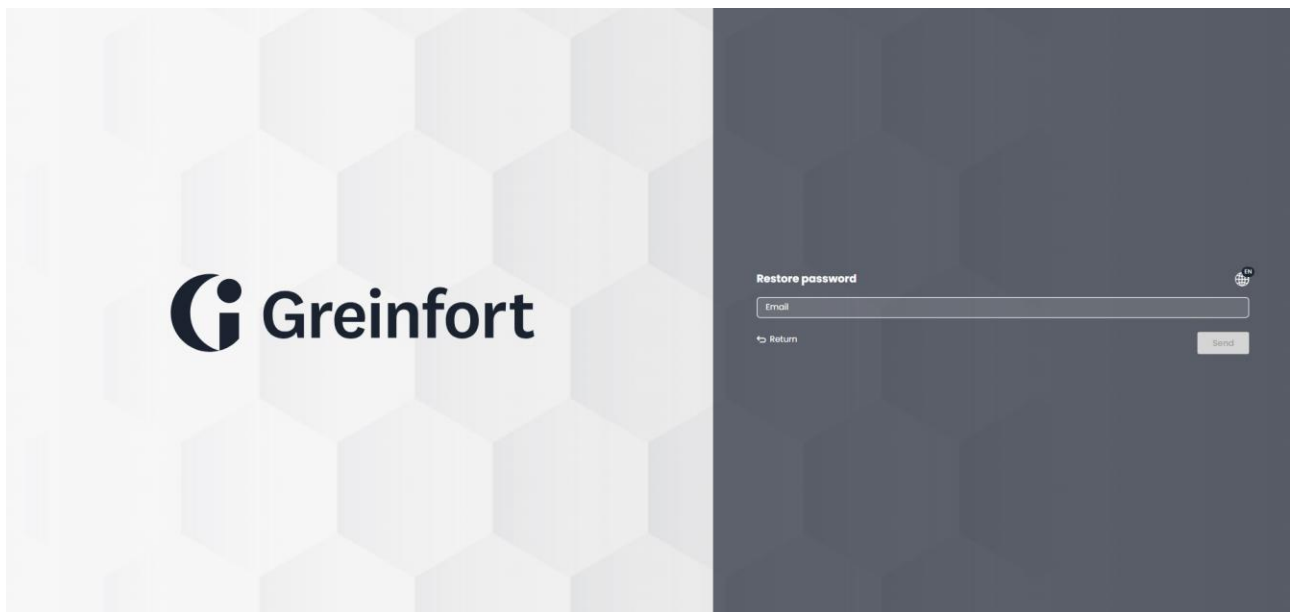
- Enter the new password in the first field.
- Confirm the new password in the second field.
- Click on the "Change Password" button to complete the process.

Once the password has been successfully changed, a confirmation message will be displayed and the user will have 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: has access to all the information presented by the application and can make the necessary configurations for algorithms, factory identifiers, production modes, etc.
- Operator: Has the same access as the administrator, except for the specific settings listed above.
- Monitor: It has only read permissions. It can download manuals and reports, as well as export search results and certain lists (devices, alerts, vulnerabilities, communications, traffic analysis, etc.).

In case the user has forgotten or locked their password, they will have the option to recover it by clicking on the "I forgot my password" option.

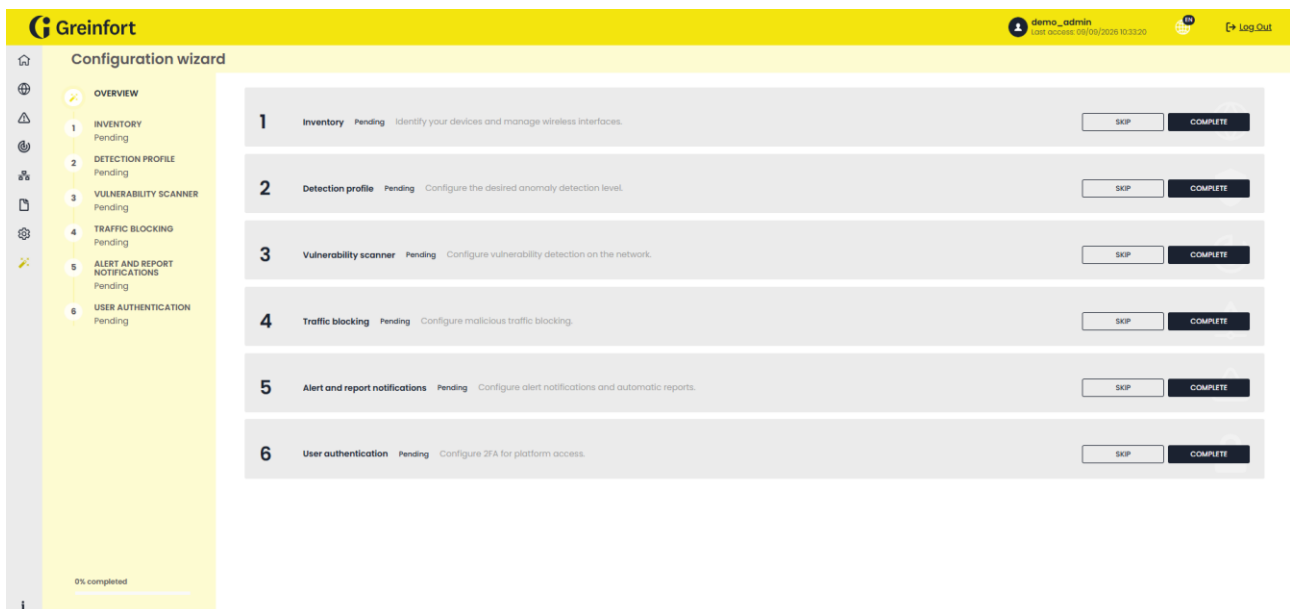


Password Recovery Screen

When a valid email address is entered, a link to reset the access password using a one-time token will be sent to that address.

**This functionality, as well as other functionality required for Greinfort software updates or remote access, requires connectivity between the system and certain Greinfort services or the Internet. For this reason, the list of rules that must be applied in the firewall will be provided.*

When log in for the first time, the Greinfort Setup Wizard opens, which guides the initial configuration of the solution. The process is divided into six stages, each of which must be completed or, alternatively, skipped.



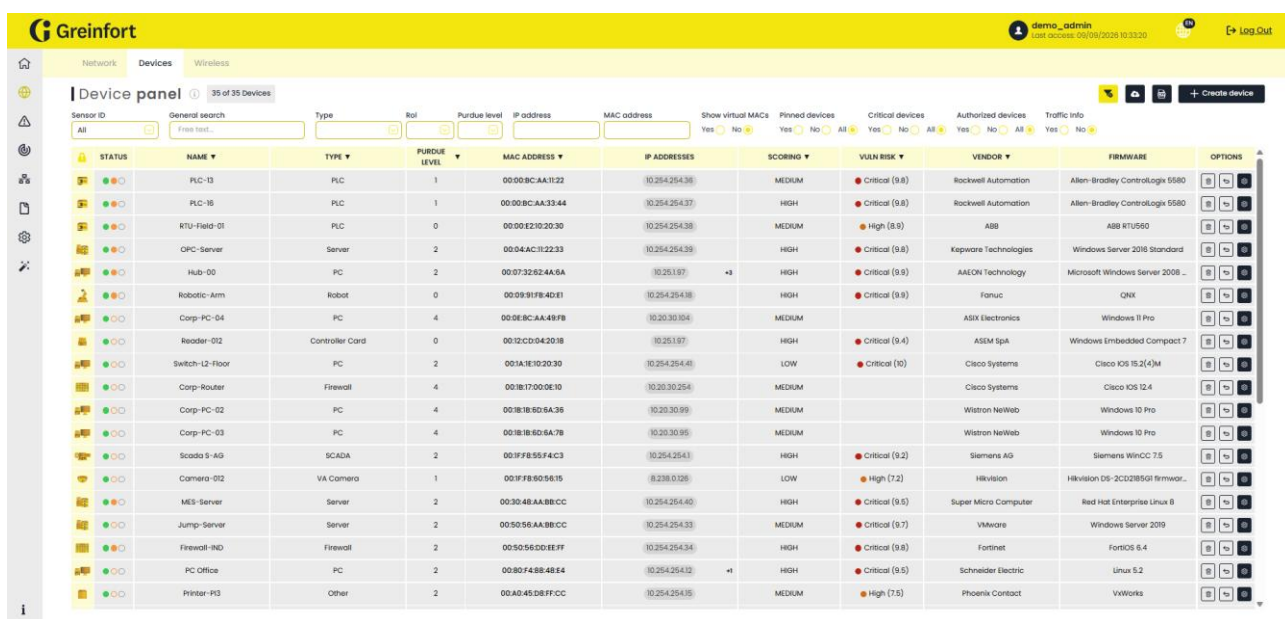
Initial Setup Wizard

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](#) (optional, as it will be calculated automatically) and its status (see Annex I). Through this declaration, the user will find it easier to identify each device in the different windows of the application and, therefore, will be able to perform operations on each device with greater agility, in addition to extracting more value from the service.

In the first phase of the wizard, a dashboard is displayed that summarizes the number of unidentified devices currently present.

The list of devices must be accessed by clicking on the wizard counters. This displays the already filtered list with the devices pending identification. This list can also be accessed using the menu icon and the "Device list" tab. 



The screenshot shows the Greinfort application interface. At the top, there's a yellow header with the Greinfort logo, a user profile (demo_admin), and a 'Log Out' button. Below the header, there's a navigation bar with 'Network', 'Devices', and 'Wireless' tabs. The 'Devices' tab is active, showing a 'Device panel' with 35 of 35 devices. The panel includes search filters for Sensor ID, General search, Type, Role, Purdue level, IP address, MAC address, Show virtual MACs, Pinned devices, Critical devices, Authorized devices, and Traffic info. Below the filters is a table with columns: STATUS, NAME, TYPE, PURDUE LEVEL, MAC ADDRESS, IP ADDRESSES, SCORING, VULN RISK, VENDOR, FIRMWARE, and OPTIONS. The table lists various devices like PLC-13, RTU-Field-01, OPC-Server, Hub-00, Robotic-Arm, Corp-PC-04, Reader-012, Switch-12-Floor, Corp-Router, Corp-PC-02, Corp-PC-03, Scada 9-AG, Camera-012, MES-Server, Jump-Server, Firewall-IND, PC Office, and Printer-P13. Each row has icons for status, actions, and options.

STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS
	PLC-13	PLC	1	00:00:BC:AA:11:22	10.254.254.36	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	PLC-16	PLC	1	00:00:BC:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
	RTU-Field-01	PLC	0	00:00:E2:10:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560	
	OPC-Server	Server	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critical (9.8)	Keapware Technologies	Windows Server 2016 Standard	
	Hub-00	PC	2	00:07:32:62:4A:6A	10.26.1.97	HIGH	Critical (9.9)	AALON Technology	Microsoft Windows Server 2008 ..	
	Robotic-Arm	Robot	0	00:09:91:F8:4D:E1	10.254.254.38	HIGH	Critical (9.8)	Fanuc	QNX	
	Corp-PC-04	PC	4	00:0E:9C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.26.1.97	HIGH	Critical (9.4)	ASEM Spa	Windows Embedded Compact 7	
	Switch-12-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M	
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
	Corp-PC-02	PC	4	00:1B:1E:6D:5A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Corp-PC-03	PC	4	00:1B:1E:6D:5A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Scada 9-AG	SCADA	2	00:1F:F8:55:F4:C3	10.254.254.41	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5	
	Camera-012	VA Camera	1	00:1F:F8:6D:56:15	8.238.0.126	LOW	High (7.2)	Hikvision	Hikvision DS-2CCD2850G1 firmwar...	
	MES-Server	Server	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
	Jump-Server	Server	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019	
	Firewall-IND	Firewall	2	00:50:56:CD:EE:FF	10.254.254.34	HIGH	Critical (9.8)	Fortinet	FortiOS 6.4	
	PC Office	PC	2	00:80:F4:9B:4B:84	10.254.254.12	HIGH	Critical (9.5)	Schneider Electric	Linux 5.2	
	Printer-P13	Other	2	00:A0:45:D8:FF:CC	10.254.254.16	MEDIUM	High (7.5)	Phoenix Contact	VWorks	

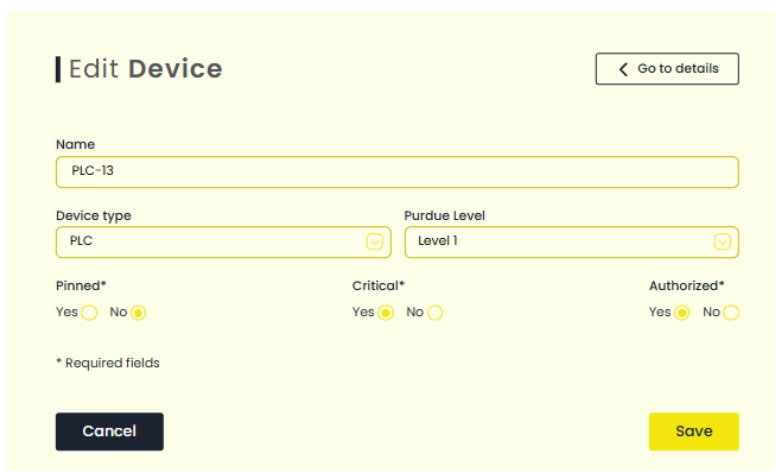
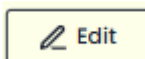
Device List Screen



The screenshot shows the 'Device Details' pop-up window. It has tabs for 'Customized fields', 'Traffic insights', and 'Edit'. The 'Customized fields' tab is active, showing details for the device 'PLC-13'. The details are organized into sections: NAME (PLC-13), SITE ID (1), UDP SCAN (Not applicable), MAC (00:00:BC:AA:11:22), SENSOR IDs (probe), TCP SCAN (44818 - enip, 80 - http), IPs (10.254.254.36), ROL (Transmitter-Receiver), SCORING (MEDIUM), SCORING DATE (31/08/2026 13:20:53), STATUS (AUTHORIZED, UNPINNED, CRITICAL), LAST CONNECTION (31/08/2026 13:20:53), TYPE (PLC), PURDUE LEVEL (1), VULN RISK (Critical (9.8)), LAST SCAN (31/08/2026 13:20:00), VENDOR (Rockwell Automation), and SCAN STATUS (Not available). A 'Close' button is at the bottom.

Device details pop-up

To modify a device, click on the corresponding button; then the edit tab opens. After that, click on the edit button to modify the selected device.

A form titled "Edit Device" with a "Go to details" button. It contains fields for "Name" (PLC-13), "Device type" (PLC), and "Purdue Level" (Level 1). Below these are three sections: "Pinned*" with "Yes" and "No" radio buttons (No is selected), "Critical*" with "Yes" and "No" radio buttons (Yes is selected), and "Authorized*" with "Yes" and "No" radio buttons (Yes is selected). At the bottom are "Cancel" and "Save" buttons. A note indicates "* Required fields".

Device Editing Screen

The device's name and Purdue level must then be manually filled in, and its status must be selected to indicate whether it is fixed, critical, or authorized (see definitions in Annex I).

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

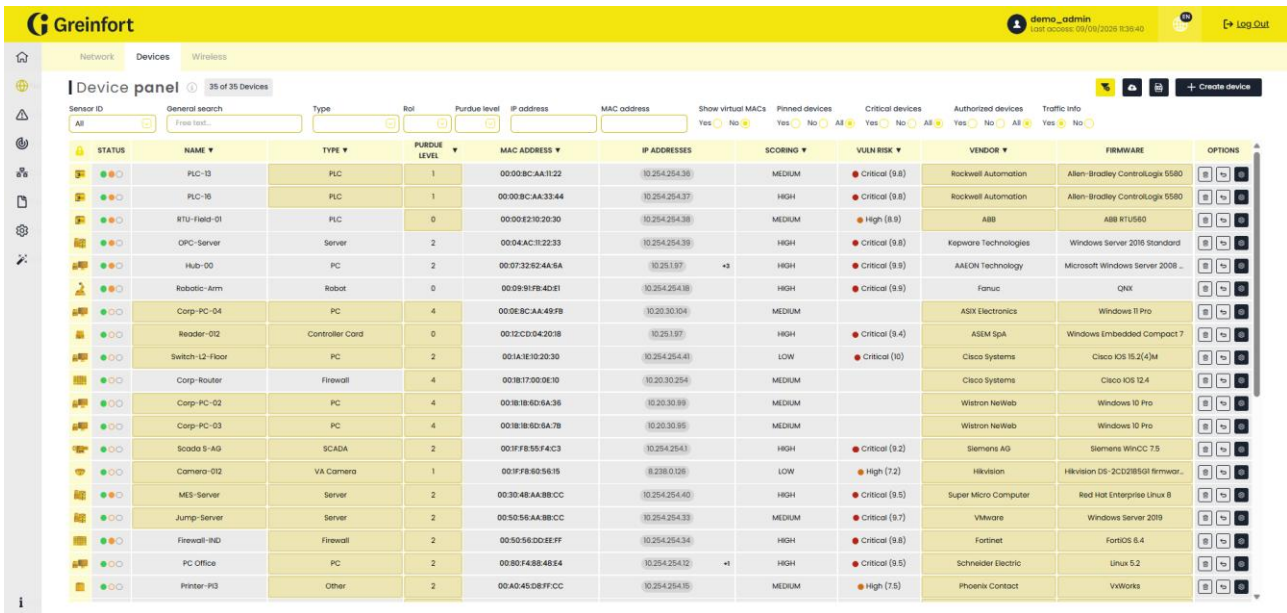
Once done, click on the "Save" button to make the changes effective in the system.

If the passive inventory system is enabled in the probe (default option), some device fields are automatically updated, either in the corresponding column or within a collection called "Traffic Insights", accessible from each device's menu.

A pop-up titled "Traffic Insights" with a "Go to details" button. It displays four lines of text: "rack_slot: 0/2", "cpu_module: M340 P34", "firmware_ver: 2.8.11", and "name_from_passive_insights: plc-13". At the bottom is a "Close" button.

Traffic Information Pop-Up

Changes made directly by the user in some of the columns take precedence over these automatic updates, which will be relegated to this collection in the event of a conflict. There is a filter in the panel, "Traffic Info", which allows to highlight which fields come from inferences made by the passive inventory system.



The screenshot shows the 'Device panel' in the Greinfort interface. It displays a list of 35 devices with columns for Status, Name, Type, Purdue Level, MAC Address, IP Addresses, Scoring, Vuln Risk, Vendor, Firmware, and Options. The 'Traffic info' filter is turned on, and the 'Vuln Risk' column shows various risk levels and scores.

STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS
PLC-13	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.36	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
PLC-16	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix 5580	
RTU-Field-01	RTU-Field-01	PLC	0	00:00:E2:10:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560	
OPC-Server	OPC-Server	Server	2	00:04:AC:12:22:33	10.254.254.39	HIGH	Critical (9.8)	Kapware Technologies	Windows Server 2016 Standard	
Hub-00	Hub-00	PC	2	00:07:32:82:4A:5A	10.25.197	HIGH	Critical (9.9)	AAEON Technology	Microsoft Windows Server 2008 ..	
Robotic-Arm	Robotic-Arm	Robot	0	00:05:91:FB:4D:E1	10.254.254.38	HIGH	Critical (9.9)	Fanuc	QNX	
Corp-PC-04	Corp-PC-04	PC	4	00:0E:8C:AA:48:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
Reader-012	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	ASEM SpA	Windows Embedded Compact 7	
Switch-12-Floor	Switch-12-Floor	PC	2	00:1A:1E:19:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M	
Corp-Router	Corp-Router	Firewall	4	00:1B:17:00:DE:30	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
Corp-PC-02	Corp-PC-02	PC	4	00:1B:18:6D:5A:36	10.20.30.99	MEDIUM		Watson NetWeb	Windows 10 Pro	
Corp-PC-03	Corp-PC-03	PC	4	00:1B:18:6D:5A:7B	10.20.30.95	MEDIUM		Watson NetWeb	Windows 10 Pro	
Scada-S-AG	Scada-S-AG	SCADA	2	00:1F:7F:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5	
Camera-012	Camera-012	VA Camera	1	00:1F:7F:55:F4:C3	8.238.0.106	LOW	High (7.2)	Hikvision	Hikvision DS-2CD2850G-I firmware..	
ME3-Server	ME3-Server	Server	2	00:30:4B:AA:8B:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
Jump-Server	Jump-Server	Server	2	00:50:56:AA:9B:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019	
Firewall-IND	Firewall-IND	Firewall	2	00:50:56:D0:EE:FF	10.254.254.34	HIGH	Critical (9.8)	Fortinet	FortiOS 6.4	
PC-Office	PC-Office	PC	2	00:80:F4:38:4B:54	10.254.254.12	HIGH	Critical (9.5)	Schneider Electric	Linux 5.2	
Printer-P13	Printer-P13	Other	2	00:AD:45:D8:FF:CC	10.254.254.15	MEDIUM	High (7.5)	Phoenix Contact	VWWorks	

Device dashboard with the "Traffic info" filter turned on

2.3. Wireless Device Analytics

If desired and the traffic collection probes have the appropriate hardware, wireless device scanning can be configured at this first stage. To do this, the interfaces to be used must be configured; the probe will search for wireless devices in its area of influence.

For more details, see the "Air Watcher" section of "Application Management".

2.4. Rule settings

The Greinfort system performs threat detection based on multiple behavioral criteria, such as:

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

Starting with the second stage of the configuration wizard, can simplify configuration by selecting one of the three predefined security profiles (basic mode), or manually edit the rules, parameters, and filters from one of them (advanced mode).

| 2. Detection profile

Select the configuration mode

Choose your security profile (anomaly detection).

Standard mode

Quick setup with predefined profiles. Ideal to start.

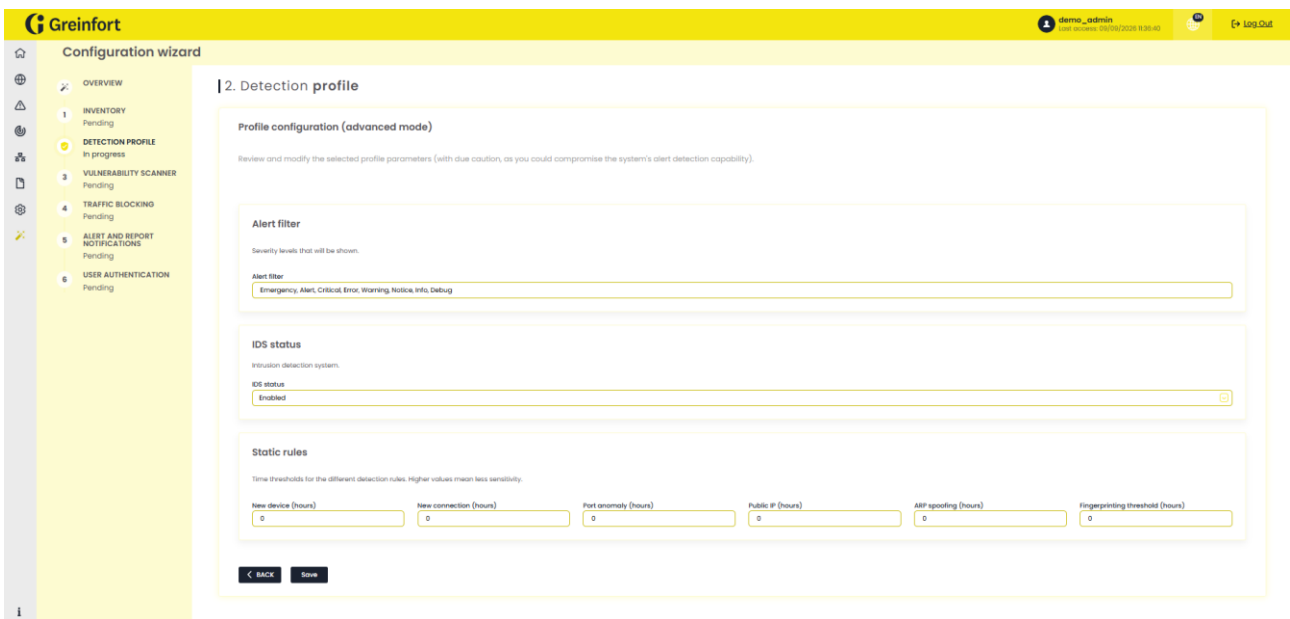
Advanced mode

Configure the specific parameters for each profile as needed.

Selecting the Security Profile

In manual editing, can be configured the rules that user desires to keep active to analyze the organization's network, as well as the suppression intervals for each alert when applicable. It is also possible to set a filter to determine the severity level at which alerts are sent to the web portal.

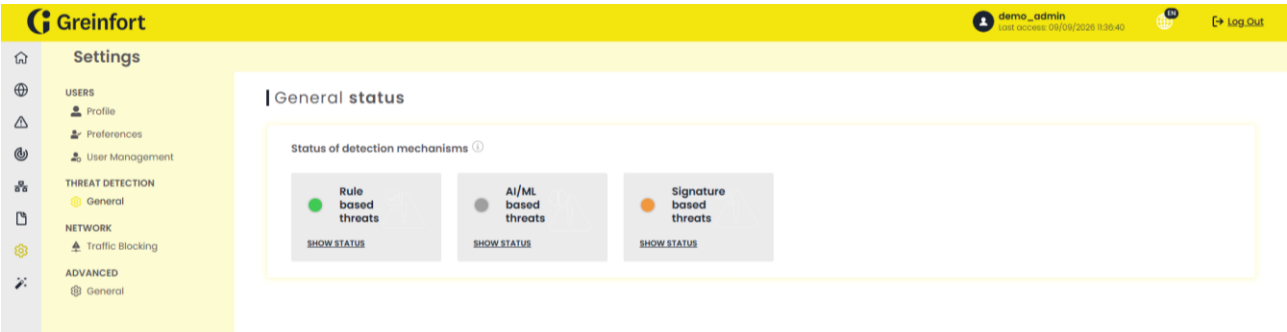
The suppression interval of a rule allows to set a time threshold during which the configured rules do not generate a new alert in an identical scenario. This avoids unnecessary warnings about already known situations.



The screenshot shows the Greinfort Configuration Wizard interface. The left sidebar lists the steps: OVERVIEW, INVENTORY, DETECTION PROFILE (selected), VULNERABILITY SCANNER, TRAFFIC BLOCKING, ALERT AND REPORT NOTIFICATIONS, and USER AUTHENTICATION. The main content area is titled '2. Detection profile' and 'Profile configuration (advanced mode)'. It includes an 'Alert filter' section with a text input field containing 'Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug'. Below this is the 'IDS status' section with a dropdown menu set to 'Enabled'. The 'Static rules' section contains six input fields for time thresholds: 'New device (hours)' (0), 'New connection (hours)' (0), 'Port anomaly (hours)' (2), 'Public IP (hours)' (0), 'ARP spoofing (hours)' (0), and 'Fingerprinting threshold (hours)' (0). At the bottom are 'BACK' and 'Save' buttons.

Advanced Rule Settings

In addition, other parameters can be configured, which are described below. To configure these intervals, open the side menu and select Threat Detection > General > Rule-Based Threats > VIEW STATUS. 



Status of detection mechanisms

Rules engine ⓘ 6 Rules ⓘ

	NAME	STATUS	THRESHOLDS	OPTIONS
✓	NewDevice	Production	1 ⓘ	✎
✓	ARPAttack	Production	1 ⓘ	✎
✓	Fingerprinting	Production	5-3-3 ⓘ	✎
✓	PublicIP	Production	1 ⓘ	✎
✓	PortAnomaly	Production	1 ⓘ	✎
✓	NewConnection	Production	1 ⓘ	✎

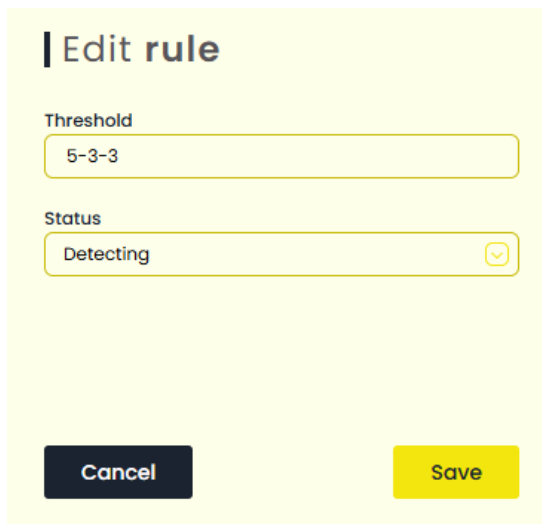
Rules Engine

In the threshold column, values configured for each rule can quickly be revised.

THRESHOLDS	OPTIONS
1 ⓘ	✎
1 ⓘ	✎
5-3-3 ⓘ	✎
1 ⓘ	✎
1 ⓘ	✎
1 ⓘ	✎

Detection rule thresholds

These parameters can be edited from the actions column.



Rule editing

When available, this section will also include settings for messages associated with alert notifications and reports that user want to receive.

2.5. Scenarios

Basic user profile, security, and notification preferences settings can be found in the "Settings" section of the Quick Guide. It is recommended that those are reviewed and adapt them to the needs of a given environment.

2.6. Active Device Scanner (Optional)

Optionally, the third stage of the wizard can activate the device query engine and configure the scan frequency to obtain additional properties of the nodes, such as firmware version, open ports, and running services. It should be noted that this is an active scan and may interfere with certain devices.

For more details, see the "Smart View" section of "Application Management".

2.7. Active Response Settings

In the fourth stage of the wizard, configuration of the reputation check system and traffic blocking can be done. Activating these functions, selecting the mode of operation, and configuring the firewall integration to use traffic blocking. The available modes and parameters are described below.

2.8. Setting up reports

In the next step, Greinfort reporting can be configured. The functionality can be turned on or off, and the generation frequency can also be defined.

2.9. Export alerts (optional)

Optionally, in this same fifth stage of the wizard, the automatic sending of the generated alerts to a syslog server of a SIEM or similar system can be enabled, for their ingestion and correlation* with other log sources.

Only the IP address and destination port of the messages should be provided, as well as the protocol to be used (syslog or encrypted syslog).

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

2.10. Continuous control panel (optional)

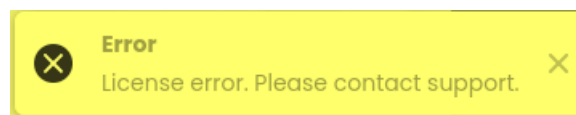
To permanently check the status of Greinform and its main indicators (unauthorized devices, network traffic, alerts, etc.), the main dashboard of the application can be displayed on a monitor in the customer's operations room, with automatic updating every five minutes.

To do this, a request to the Greinform Support service in order to create a monitoring user must be raised.

2.11. Licenses

It allows the Greinform service to be provided on a temporary basis for trial purposes and a limited window of use.

If the message "License Error. Contact Support." is displayed, it means that the license files are missing or have expired.



License Error Detail

2.12. Access Control and Roles

This feature allows to control access and actions performed on the system. Its implementation adds a layer of security and privacy to the processing of information and resources.

This role and access control system has the following features:

1. **Predefined roles and permissions:** Determine the levels of access and control of the system.
2. **Assigning permissions to users and groups:** The system allows to assign permissions to users and groups based on their roles and responsibilities in the organization.
3. **User group management:** Allows to assign permissions to multiple users at the same time and makes them easier to manage.
4. **Resource Access Control:** Allows to control access to the various resources in Greinform using specific permissions.

The roles to be implemented will be the following:

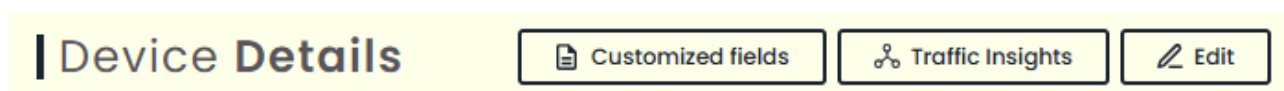
- **Administrator:** Has full access to configuration, service operations, and logs. Admin can also switch between training and production environments, and modify AI algorithm sets when necessary.
- **Operator:** Factory privileged user mode. Allows to modify visible interface data, such as device data, and mark alerts as resolved or muted.
- **Monitor:** Standard factory user mode, with more restricted permissions. Only allows to view data and download reports or CSV files.

2.13. Custom fields

If new fields are needed in the device list to improve their categorization, they can be defined in key-value format using a CSV file.

A file must be added from the button in the Devices Panel. The rows must include the devices that the user wants to add, along with the new custom fields in any of the formats described in the "Device List" > "Import via CSV" section .

Uploaded fields can be viewed from the Devices Dashboard using the "View Customized Fields" button.



Device Custom Fields

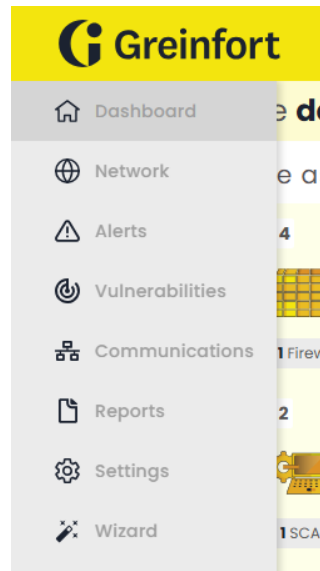
This action opens a new modal window in which the fields can be viewed.



Custom fields detail

3. Quick Guide

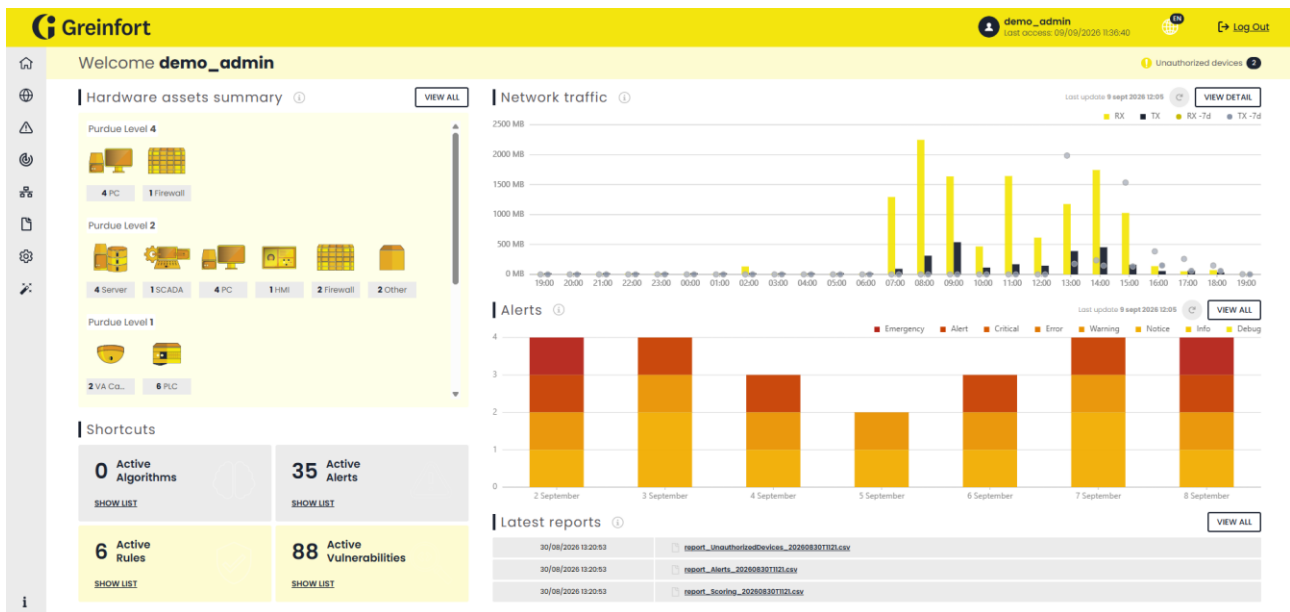
3.1. Menu



Access window detail

- 1: Home: Main Panel
- 2: Network: Network map and device list
- 3: Alerts: List of alerts
- 4: Vulnerabilities: List of vulnerabilities
- 5: Traffic Sessions: List of Communications Between Devices
- 6: Reports: List of automatic reports
- 7: Settings: Parameter Configuration Window
- 8: Wizard: Guide to Performing the Initial Configuration of the Solution
- 9: Information: documentation, system version, and changelog

3.2. Main panel



Control Panel Main View

Top Bar:

Type of session and date of previous access.

Application language.

Close of the active session.

Unauthorized devices detected.

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 bit/s, during the last 24 hours, and comparison with the same period seven days earlier.

Bottom left widget:

Shortcuts to listings

Active vulnerabilities (under construction)

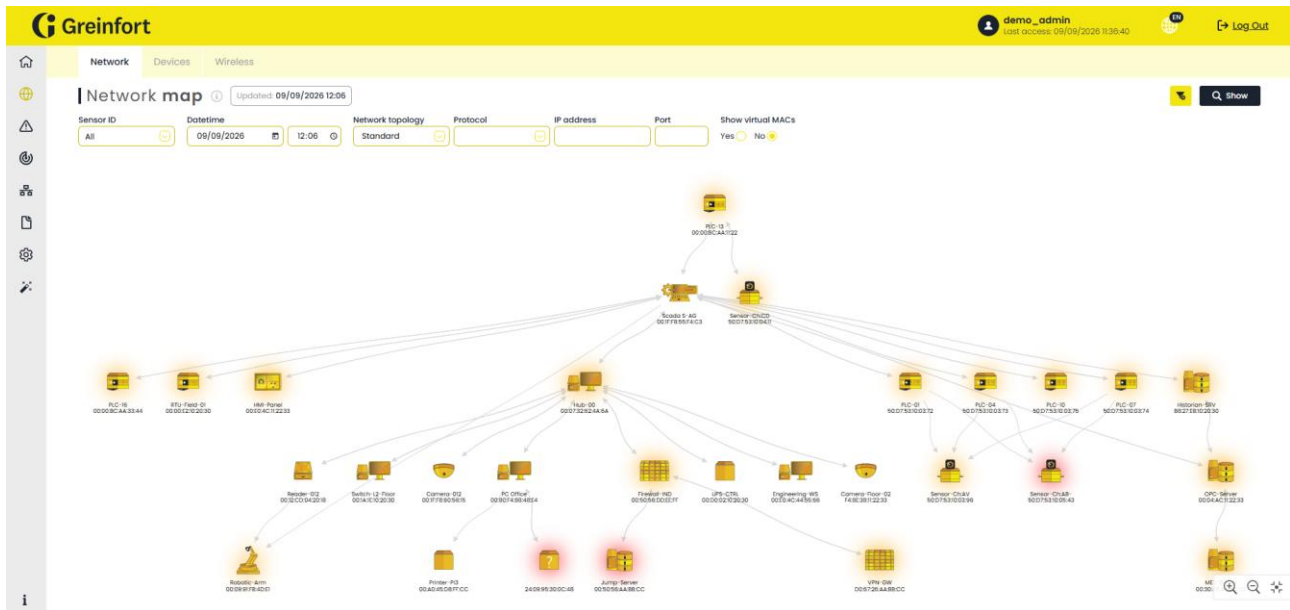
Widgets at the bottom right:

Graphical representation of the number of alerts according to their severity.

Access to the list of generated reports

3.3. Network Map

The network map presents two topological views: classic or [PURDUE tiered](#) network. 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 introduced filters effective.

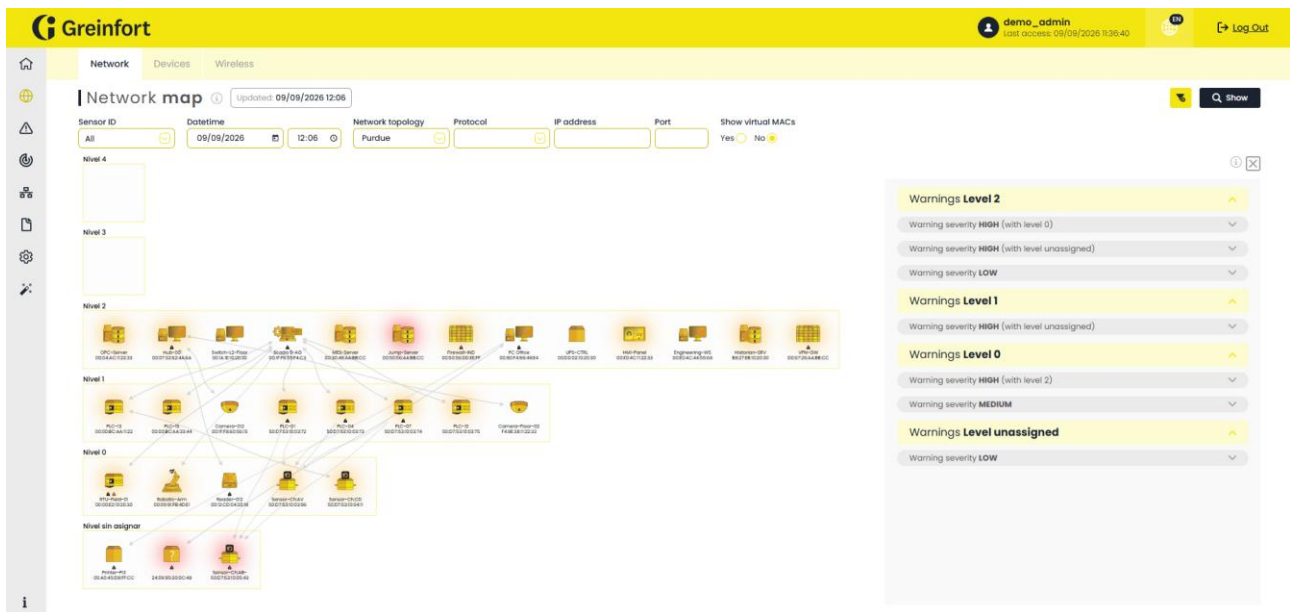
The next row shows the possible filters to see the devices of interest on the screen.

Below is the map and topology of the devices on a given organization's network.

The following should be taken into account:

- Hovering over a node or link displays its properties.
- Clicking on a node or link takes to the detail view to edit the device properties or to the communications section filtered by the link source, respectively.

In the Purdue view of the topology, communications compliance is analyzed according to ISA/IEC 62443. Warnings are classified as high severity (communications between non-adjacent levels), medium (Purdue level assignments that may be questionable), or low (unassigned levels or manual review recommendation for certain device types).



Network Map in Purdue View

In the graphical view, located on the left side of the window:

- Only communications between different levels are displayed, not those between devices of the same level.
- Triangular icons below the device image indicate if the device is affected by any compliance warnings. The different colors represent warnings of high, medium, or low severity, as appropriate.
- Devices can be clicked to filter the warnings on the right side that apply to the node in question. If the filter is unchecked, all detected devices are displayed, in descending order of levels and severity.

The rest of the filtering options are the same as in Classic View. On the right side of the window, global warnings or warnings associated with the selected device are displayed.

3.4. Device List

The device list tab shows, next to the dashboard title, the number of devices that meet the current filter against the total registered in the database. On the right side is placed the button panel to remove filters, export the list in CSV format, and manually register a device.

Greinfort											
										demo_admin last access: 09/08/2028 1:36:40	Log Out
Network Devices Wireless											
Device panel 35 of 35 Devices											
Sensor ID	General search	Type	Role	Purpose level	IP address	MAC address	Show virtual MACs	Pinned devices	Critical devices	Authorized devices	Traffic info
All	Free text...						Yes No	Yes No All	Yes No All	Yes No All	Yes No
STATUS	NAME	TYPE	PURPOSE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS	
	PLC-13	PLC	1	00:00:8C:AA:11:22	10.254.254.38	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix		
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix		
	RTU-Field-01	PLC	0	00:00:82:30:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560		
	OPC-Server	Server	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critical (9.8)	Keyware Technologies	Windows Server 2016 Sta...		
	Hub-00	PC	2	00:07:32:62:4A:5A	10.25.197	HIGH	Critical (9.9)	AAEON Technology	Microsoft Windows Serve...		
	Robotic-Arm	Robot	0	00:09:91:FB:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Fanuc	QNX		
	Corp-PC-04	PC	4	00:0E:8C:AA:49:FB	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro		
	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	ASEM SpA	Windows Embedded Ca...		
	Switch-12-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M		
	Corp-Router	Firewall	4	00:1B:17:00:0E:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4		
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro		
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro		
	Scada S-A0	SCADA	2	00:3F:FB:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5		
	Camera-012	VA Camera	1	00:1F:FB:50:56:15	8.238.0.126	LOW	High (7.2)	Hikvision	Hikvision DS-2CD21850I FL		
	MES-Server	Server	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8		
	Jump-Server	Server	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019		

Device List Window

The next row includes any applicable filters to see devices of interest.

The list of assets contains information about them and buttons to perform certain actions (view details, edit them, delete them, or access alerts, communications, or vulnerabilities present). It is possible to sort 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 functionality is enabled).

3.5. Alerts dashboard

Alerts section

Next to the section title is the number of alerts in the organization's network that meet the filter criteria against the total. On the right side is the button panel to remove filters, export the list in CSV format, or manually create an alert.

The next row lists the available filters. Note that the general search field uses the CONTAINS criterion and allows to search the alert's internal notes field, visible under "Details".

Finally, the list of alerts with the associated information and buttons to update their status*, access details or add notes is displayed.

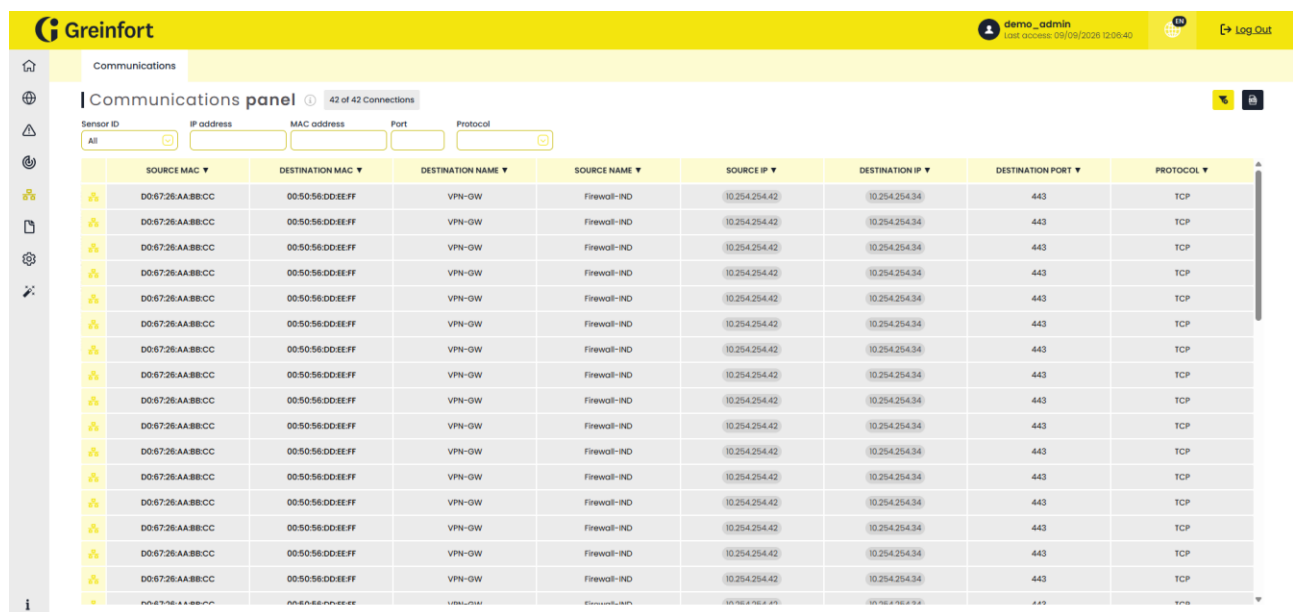
As can be seen in the image, when a device has a name assigned to it, an exclamation point appears next to the MAC address. When hover over it, the name associated with that address is displayed.

If the blocking policy is active in any of its modes (informational, manual, or automatic), alerts associated with public IP addresses classified as malicious are highlighted in bright red. The tone is dimmed if the address is on the industrial firewall block list.

*For options related to status, please refer to the definitions in Annex I.

3.6. List of communications

A communication is defined as a set of connections that share MAC addresses, IP addresses, and source and destination ports. If the protocol changes, it is considered a distinct communication.



SOURCE MAC	DESTINATION MAC	DESTINATION NAME	SOURCE NAME	SOURCE IP	DESTINATION IP	DESTINATION PORT	PROTOCOL
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP

Communications List Window

This section shows, next to the title, the number of communications that meet the current filter against the total registered in the database. On the right side are the buttons to remove the filters and export the list in CSV format.

The following row shows the filters available to locate the communications of interest.

Finally, the list of communications and their information is displayed. Communications can be sorted alphabetically, ascending or descending, by clicking on any of the columns.

3.7. Reports

This section allows to download reports of various types automatically generated by the system. By default, Greinfort generates weekly reports in downloadable CSV files from the following areas:

- Unauthorized connected devices

- Last detected alerts
- MAC-IP partnerships
- Public IPs (external IPs connected)
- Risk Score Report (scoring)
- Vulnerabilities

If the device has a name assigned, it replaces the MAC address in the alert reports. For manual downloads of searches from the alert dashboard or device list, the "Latest reports" section displays both fields separately.

The user will be able to download the most recent reports generated from the main shortcut of the Control Panel.

Latest reports ⓘ		VIEW ALL
30/08/2026 13:20:53	 report_UnauthorizedDevices_20260830T1121.csv	
30/08/2026 13:20:53	 report_Alerts_20260830T1121.csv	
30/08/2026 13:20:53	 report_Scoring_20260830T1121.csv	

Latest reports on the Main Dashboard

In addition, Greinfort has a section dedicated to reports, where the search engine can be used to filter and download the report of interest:

Report list view

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

The following row shows the different search filters.

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

3.8. Scenarios

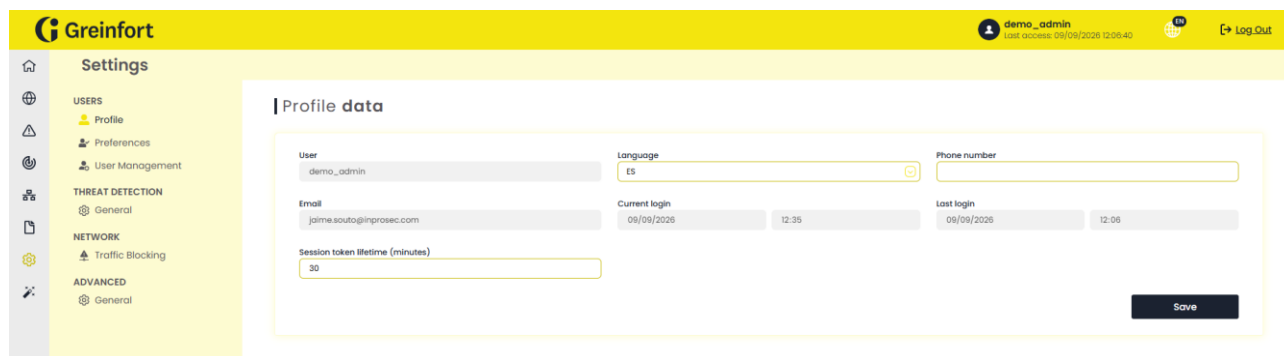
In this section, profile and service can be adjusted, as well as modify parameters related to threat detection, alerting, and user management.

The most relevant aspects at the user level are summarized below.

3.8.1. User Profile

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

The user can access it from  "Settings" in the left side menu.



The screenshot shows the 'Settings' menu on the left with 'Profile' selected. The main area is titled 'Profile data' and contains a form with the following fields:

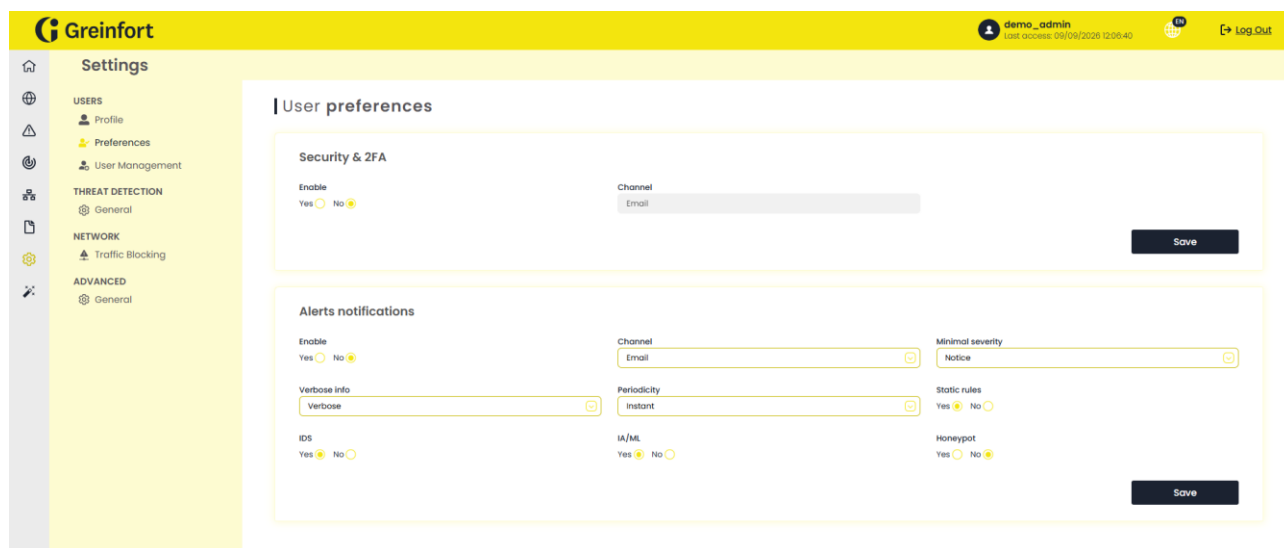
- User:** demo_admin
- Language:** ES
- Phone number:** (empty)
- Email:** jaime.souto@linprosec.com
- Current login:** 09/09/2026 12:35
- Last login:** 09/09/2026 12:06
- Session token lifetime (minutes):** 30

A 'Save' button is located at the bottom right of the form.

User Profile Data View

3.8.2. User preferences

In Advanced > Preferences, in the "Security & 2FA" section, the second authentication factor can be enabled as an additional security mechanism (recommended) to prevent identity theft. After identifying yourself with username and password, a one-time token received via email is requested.



The screenshot shows the 'Settings' menu on the left with 'Preferences' selected. The main area is titled 'User preferences' and contains two sections:

- Security & 2FA:**
 - Enable:** Yes (selected) / No
 - Channel:** Email
- Alerts notifications:**
 - Enable:** Yes (selected) / No
 - Channel:** Email
 - Minimal severity:** Notice
 - Verbose info:** Verbose
 - Periodicity:** Instant
 - Static rules:** Yes (selected) / No
 - IDS:** Yes (selected) / No
 - IA/ML:** Yes (selected) / No
 - Honeypot:** Yes (selected) / No

'Save' buttons are located at the bottom right of each section.

User Preferences View

It should be noted that a role-based access control mechanism has been implemented, with permission groups associated with three user levels, described earlier in "Access Control and Roles":

- Administrator
- Operator
- Monitor

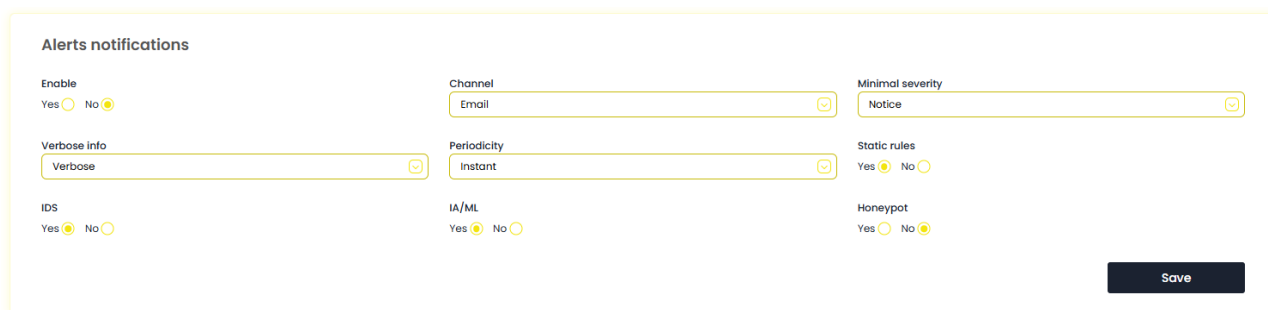
3.8.3. Notification of alerts

If deemed appropriate, proactive notifications of system-generated alerts can be configured. Alerts and warnings are produced from the detection of anomalies using the strategies implemented in Greinfort (heuristics, AI/ML, IDS, honeypot, or manual creation).

Thus, Greinfort warns of possible incidents without the need to regularly check the web interface.

The following aspects can be configured:

- Receipt or non-receipt of security alert notifications.
- The severity threshold from which notifications are sent.
- Type of alerts: heuristics, AI/ML, IDS, honeypot, or all.
- Submission Format:
 - Individual: One notification per alert
 - Grouped: A daily notification with a summary of all alerts, selectable from Monday to Friday or Monday to Sunday.
 - If the format is individual, a summarized or verbose version can be selected.



The image shows a web form titled "Alerts notifications". It contains several configuration options with radio buttons and dropdown menus. The "Enable" option is set to "No". The "Channel" dropdown is set to "Email". The "Minimal severity" dropdown is set to "Notice". The "Verbose info" dropdown is set to "Verbose". The "Periodicity" dropdown is set to "Instant". The "Static rules" option is set to "Yes". The "IDS" option is set to "Yes". The "IA/ML" option is set to "Yes". The "Honeypot" option is set to "Yes". A "Save" button is located at the bottom right of the form.

Alert Notifications View

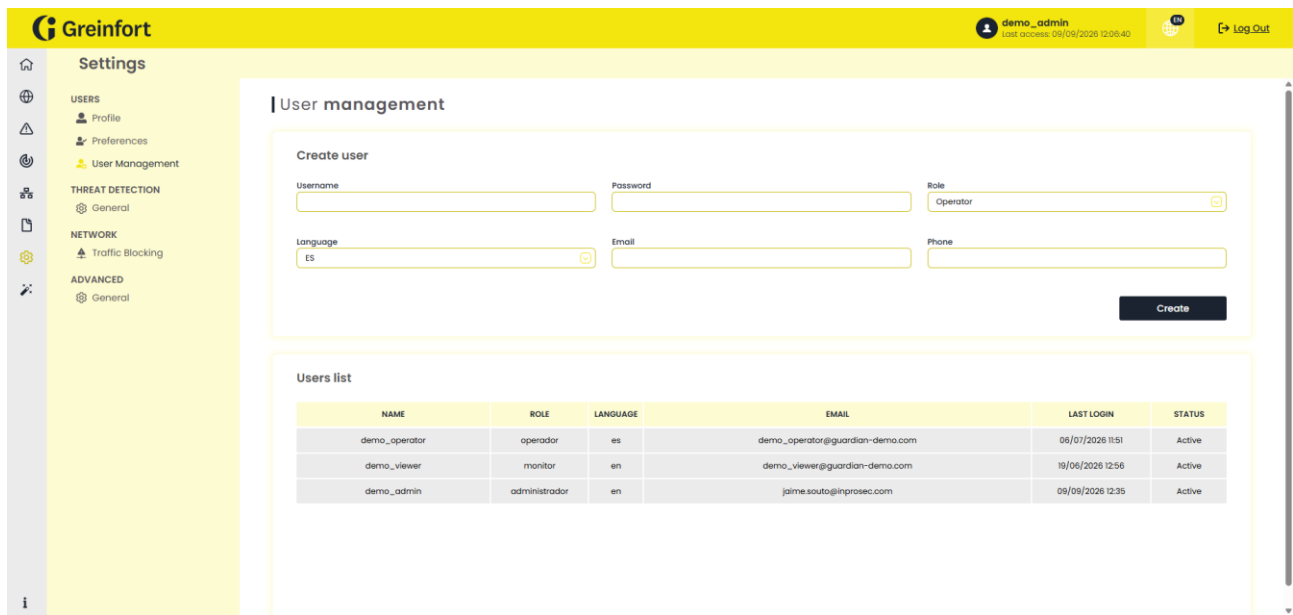
Notifications will be sent via email to the user's account.

Important:

- The alert notification must be enabled on the backend to allow the user to enable proactive sending.
- In the event that, with the established conditions, too many alerts are generated per unit of time, the functionality will be automatically deactivated for security reasons (previously informing the user by email about this situation), so that other more demanding notification sending conditions (with a lower volume of events) can be selected.

3.8.4. User Management

In the User Management section, a user with the administrator role can create users in the same factory and read the corresponding user list.



User management

Create user

Username: Password: Role:

Language: Email: Phone:

Create

Users list

NAME	ROLE	LANGUAGE	EMAIL	LAST LOGIN	STATUS
demo_operator	operator	es	demo_operator@guardian-demo.com	06/07/2026 11:51	Active
demo_viewer	monitor	en	demo_viewer@guardian-demo.com	19/06/2026 12:56	Active
demo_admin	administrador	en	jaime.souto@inprosec.com	09/09/2026 12:35	Active

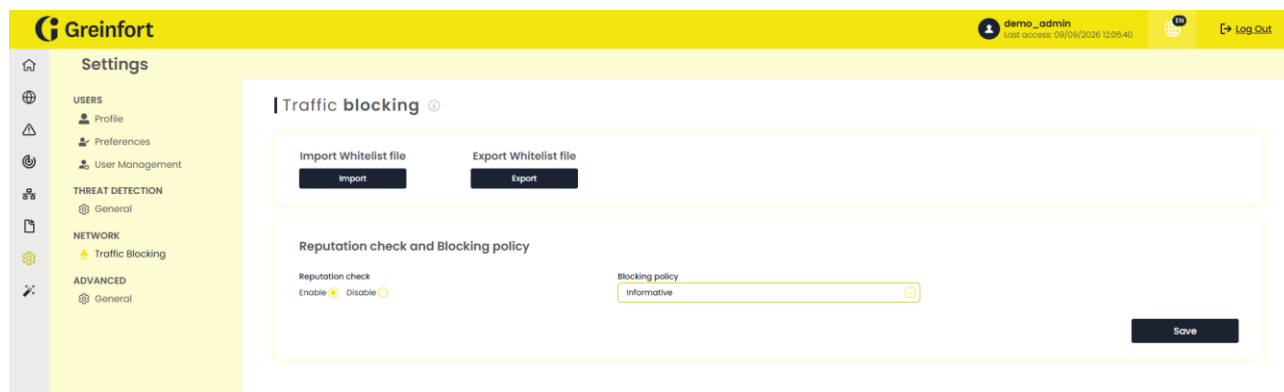
User Management View

3.8.5. Traffic Blocking Settings

In this section, can be enabled the import and export of a whitelist of IP addresses, IP ranges, or MAC addresses that will never be blocked.

The following two parameters can also be configured:

- Reputation Check: Turn public IP reputation query on or off for inbound or outbound traffic.
- Blocking policy: Allows to select one of four modes of blocking malicious public IP addresses:
 - **Informational:** notifies the user and suggests blocking that IP.
 - **Manual:** provides a user-actionable button in the alert panel that sends the malicious IP to a blocklist managed by the industrial firewall.
 - **Automatic:** communicates with the firewall without user intervention and adds the malicious IP address to a block list.
 - **Off:** does not modify the alert panel or attempt to communicate with the industrial firewall.



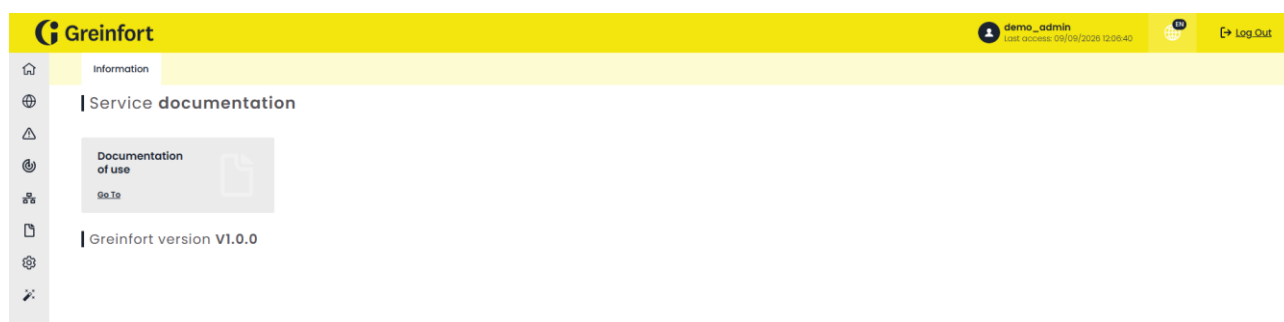
Traffic Blocking View

3.8.6. Information

Section that allows to download the latest version of the Greinfort user manual. Points to the Greinfort website, where the relevant documentation is published.

It also displays the current version of the platform and the changelog for version control.

To access it, click on the menu icon located in the lower left corner.

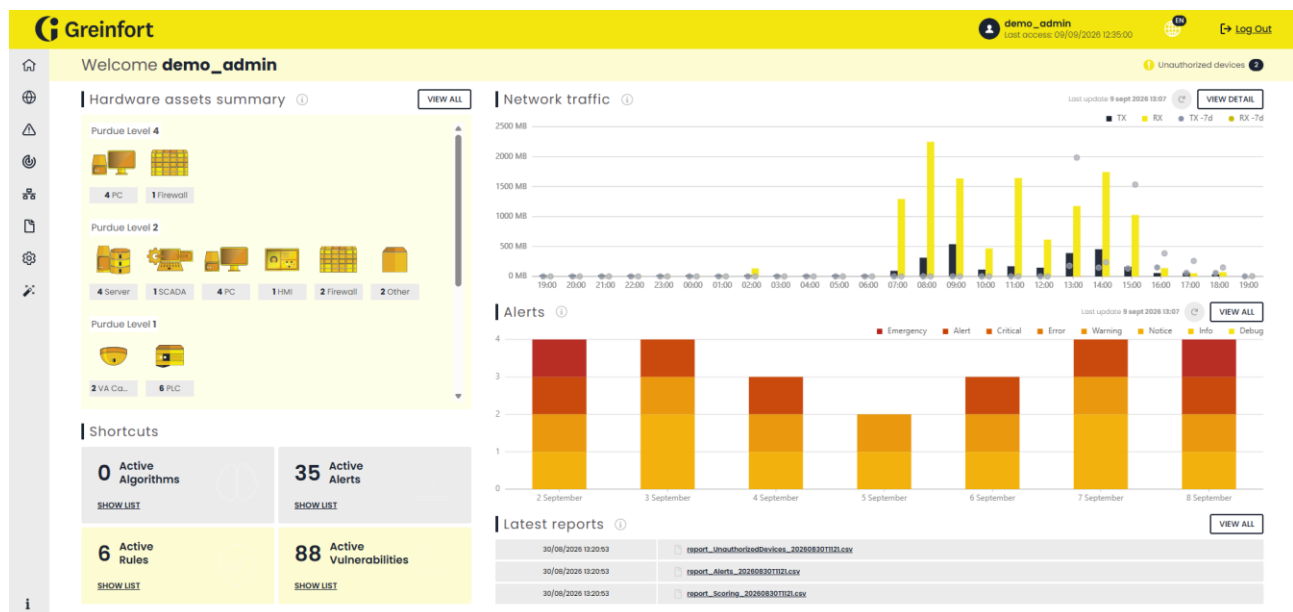


Information View

For any technical issue, contact Greinfort Support.

4. Application Management

4.1. Main panel



Home Panel

4.1.1. Asset Summary



Asset Summary

The number of devices connected to the network is displayed, differentiated by type (PLC, RTU, switch, router, robot, PC, SCADA, DCS, HMI, firewall, variable frequency drive, controller card, sensor, V.A. camera, tablet, telephone, honeypot or other equipment) and classified according to the Purdue model described in Annex II (informed manually or automatically).

4.1.2. Quick Links

Shortcuts

0

Active Algorithms



[SHOW LIST](#)

35

Active Alerts



[SHOW LIST](#)

6

Active Rules



[SHOW LIST](#)

88

Active Vulnerabilities



[SHOW LIST](#)

Quick Links

a. Active algorithms

Clicking "VIEW LIST" displays the list of AI algorithms active for threat detection on a given organization's network. This section is described below.

Amenazas basadas en IA/ML

Gestión de algoritmos IA/ML

De Sonda

Búsqueda general

Todos

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

List of algorithms

b. Active alerts

Clicking "VIEW LIST" displays the full list of active alerts.

c. Active Rules

Clicking "VIEW LIST" displays the list of active fixed rules for threat detection on a given organization's network. This section is described below.

Rules engine 6 Rules

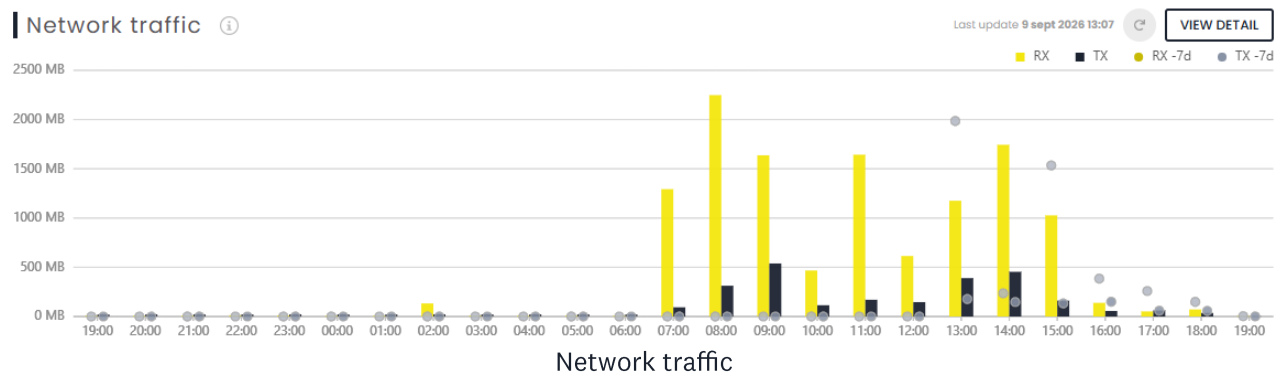
	NAME	STATUS	THRESHOLDS	OPTIONS
	NewDevice	Production	1 ⓘ	
	ARPAAttack	Production	1 ⓘ	
	Fingerprinting	Production	5-3-3 ⓘ	
	PublicIP	Production	1 ⓘ	
	PortAnomaly	Production	1 ⓘ	
	NewConnection	Production	1 ⓘ	

List of active rules

d. Active vulnerabilities

Clicking "VIEW LIST" displays the list of active vulnerabilities pending management.

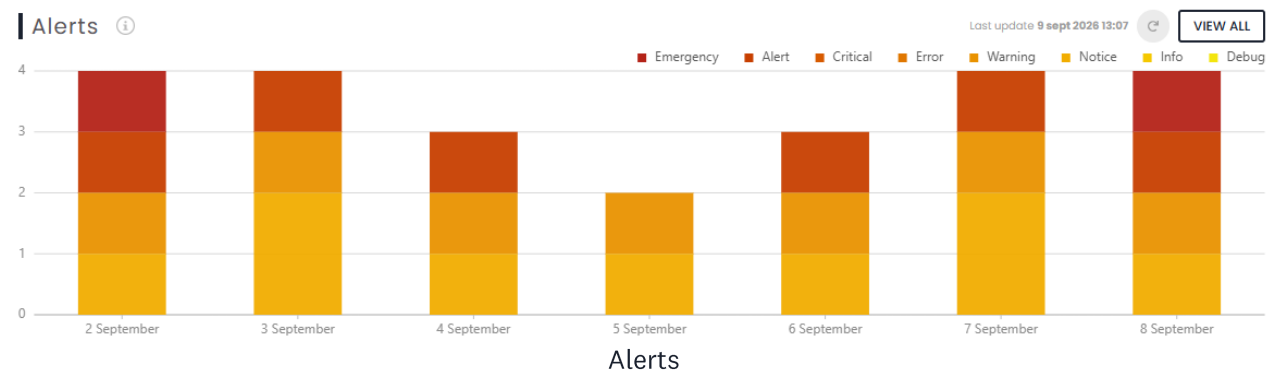
4.1.3. Network Traffic Graph



The dashboard graphically represents the traffic generated, in bit/s or multiples of this unit, during the last 24 hours, both sent and received. The data is updated automatically and can also be updated manually. The circular dots on each bar indicate, for comparison, the traffic recorded seven days earlier.

Clicking on "VIEW DETAIL" opens the Greinfort Network Sessions window, described below.

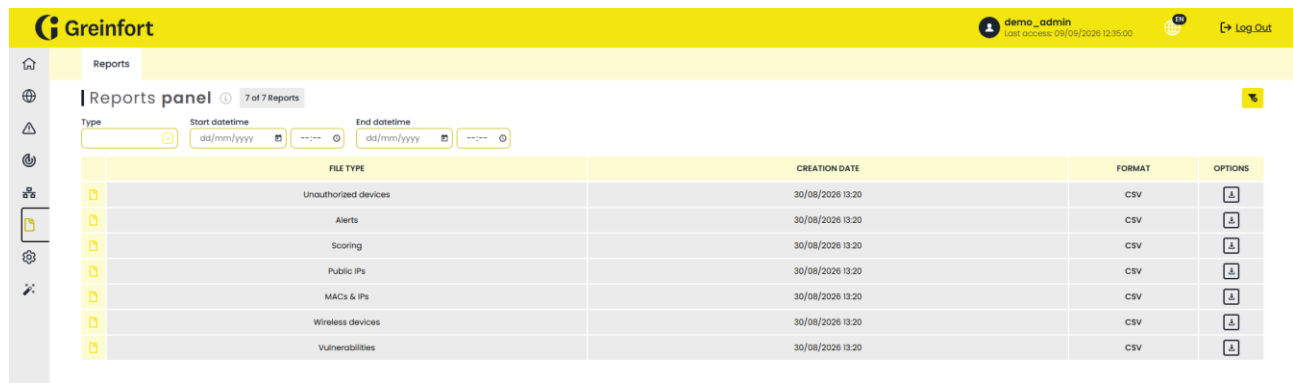
4.1.4. Alert Graph



A graphical representation of the number of alerts in the last five days is displayed, differentiated by severity level (see Annex I) and color, as well as their trend. The data is updated automatically and can also be updated manually.

Hovering over the day bar displays the exact number of alerts logged so far. Clicking on "VIEW ALL" opens the Greinfort alert window, described below.

4.1.5. Latest reports



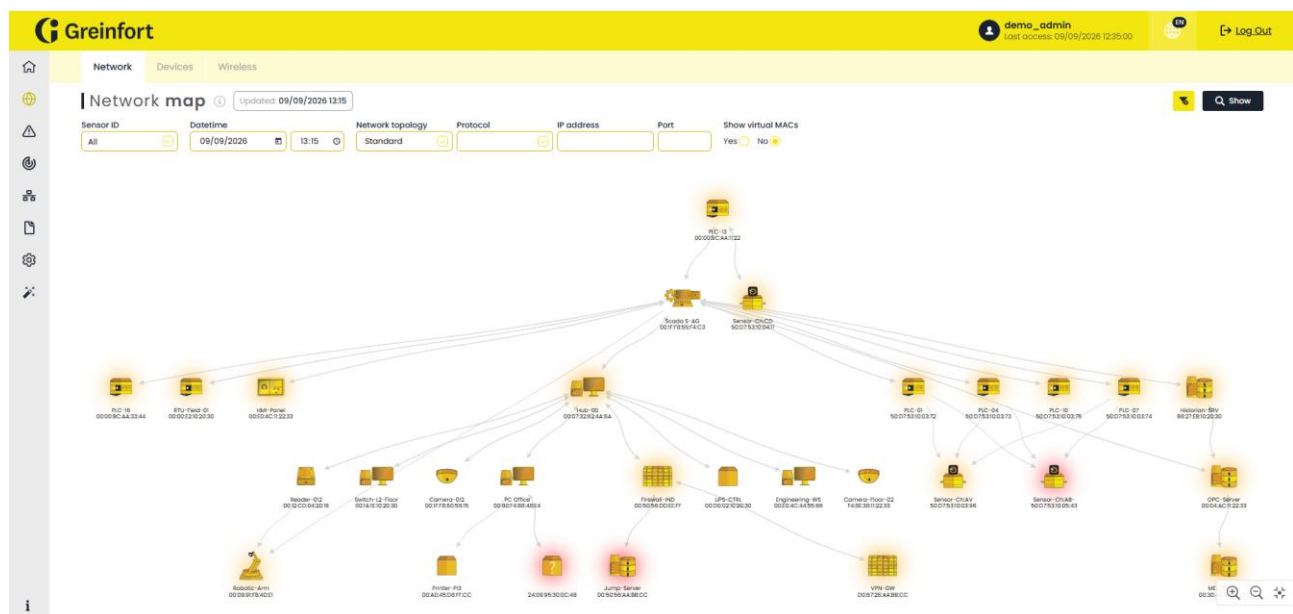
Latest reports available

Clicking "VIEW ALL" displays the list of the most recent reports, generated automatically or at the customer's request.

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

The "Network Map" tab shows all connected devices and their communication links in real time. Each device is represented by an image and a series of properties, such as the MAC address or the manually assigned name. The map reflects the implemented topology.

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

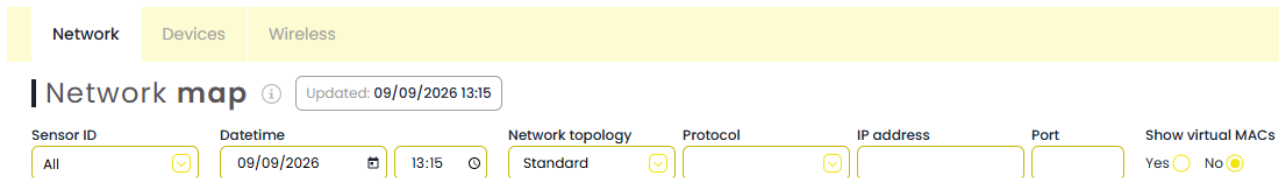
Unauthorized devices will be shown on the network map shaded with a red background. Fixed and critical devices will also have their corresponding halo (see Annex I for definitions).

When hovering over a device, a pop-up window with its basic information is displayed.

Clicking on a device opens the window with all its information.

Hovering over a link displays a pop-up window with basic communication information. Clicking on a link opens the window with all the connection information.

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



The screenshot shows the 'Network map' interface. At the top, there are three tabs: 'Network' (selected), 'Devices', and 'Wireless'. Below the tabs, the title 'Network map' is followed by an information icon and a timestamp 'Updated: 09/09/2026 13:15'. Below this, there are several filter fields: 'Sensor ID' with a dropdown menu showing 'All', 'Datetime' with a date '09/09/2026' and a time '13:15', 'Network topology' with a dropdown menu showing 'Standard', 'Protocol' with a dropdown menu, 'IP address' with a text input field, and 'Port' with a text input field. To the right of these fields, there is a 'Show virtual MACs' section with 'Yes' and 'No' radio buttons, where 'No' is selected.

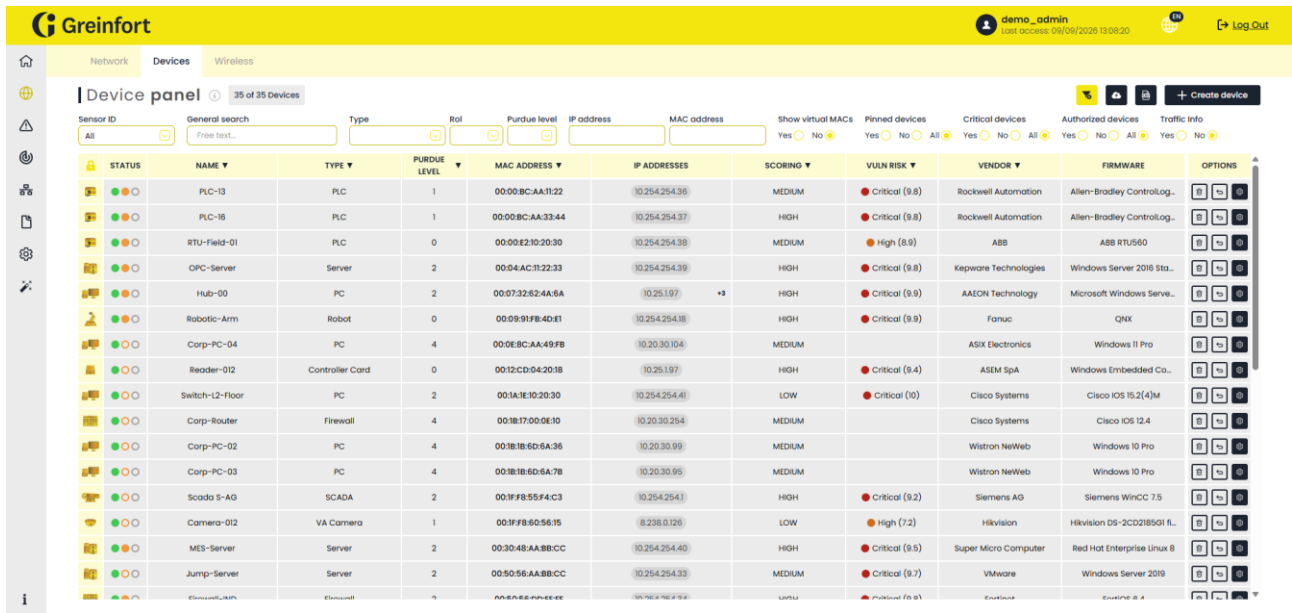
Filters available on the network map

The filters can be applied as follows:

- Date and time: A time range displayed on the screen.
- Network topology: model of representation of the organization's network.
- Protocol: Displays only connections that use the selected protocol.
- IP address: shows only the devices and connections with the selected address.
- Port: Displays only the connections associated with the selected port.
- Display of virtual MAC addresses (multicast or broadcast), automatically calculated by the system.

4.2.2. Device List

To access the device list, the user needs to 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
	PLC-13	PLC	1	00:00:9C:AA:11:22	10.254.254.36	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix	
	PLC-16	PLC	1	00:00:9C:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLogix	
	RTU-Field-01	PLC	0	00:00:23:10:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560	
	OPC-Server	Server	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critical (9.8)	Keypware Technologies	Windows Server 2016 Sta...	
	Hub-00	PC	2	00:07:32:62-AA:5A	10.25.197	HIGH	Critical (9.9)	AAEON Technology	Microsoft Windows Serve...	
	Robotic-Arm	Robot	0	00:09:91:FB:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Fanuc	QNX	
	Corp-PC-04	PC	4	00:0E:8C:AA:49:FB	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	ASEM SpA	Windows Embedded Ca...	
	Switch-12-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M	
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:76	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	
	Scada S-AG	SCADA	2	00:1F:FB:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5	
	Camera-012	VA Camera	1	00:1F:FB:60:56:15	8.238.0.126	LOW	High (7.2)	Hikvision	Hikvision DS-2CD21850I FL	
	MES-Server	Server	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
	Jump-Server	Server	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019	

Device List

An expanded list of all devices present in the organization and their information is displayed:

- **STATUS:**
 - The first of the circles will indicate whether the device is authorized (approved by the administrator as known), or not.
 - The second of the circles will indicate whether the device is critical or not (if due to its relevance or criticality it is not allowed to be carried out on active actions).
 - The third circle indicates whether the device is fixed or not (if it is desired that it continues appearing on the network map regardless of whether it stops generating traffic).
- **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:** MAC address assigned to the device.
- **IP ADDRESSES:** IP addresses assigned to the device.
- **SCORE:** importance or risk of the device (low, medium or high) by means of a proprietary algorithm that gives a measure of its criticality within the network.
- **VULN RISK:** highest level of severity of the vulnerabilities detected in the device.
- **SUPPLIER:** Device manufacturer.
- **FIRMWARE:** Information about the firmware built into the device.
- **CUSTOMIZED FIELDS:** In addition to the existing fields, users can create their custom fields in JSON format with key-value pairs. Each customizable field will appear in the device list as a new virtual column, allowing the user to catalog, organize, and filter devices at their convenience. These customizable fields will also appear in reports.
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.
- **TRAFFIC INSIGHTS:** The passive inventory system automatically infers variables of interest from each device, which are stored in this field in key-value format. The field is also included in the export CSV file.
- **ACTIONS:**

View device information in detail.

Device Details

Customized fields

Traffic Insights

Edit

NAME PLC-13	SITE ID 1	UDP SCAN Not applicable
MAC 00:00:BC:AA:11:22	SENSOR IDs probe	TCP SCAN 44818 - enip 80 - http
IPs 10.254.254.36	ROL Transmitter-Receiver	
LAST CONNECTION 31/08/2026 13:20:53	SCORING MEDIUM	
TYPE PLC	SCORING DATE 31/08/2026 13:20:53	
PURDUE LEVEL 1	STATUS AUTHORIZED UNPINNED CRITICAL	
VULN RISK Critical (9.8)	LAST SCAN 31/08/2026 13:20:00	
VENDOR Rockwell Automation	SCAN STATUS Not available	

Close

Device details

Edit Device

Go to details

Name
PLC-13

Device type
PLC

Purdue Level
Level 1

Pinned*
Yes No

Critical*
Yes No

Authorized*
Yes No

* Required fields

Cancel

Save

Device Editing

The screen can be filtered to show only the devices of interest.

Greinfort

demo_admin
Last access: 05/09/2026 13:08:20

Log Out

Network

Devices

Wireless

Device panel 35 of 35 Devices

Sensor ID
All

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

Traffic info
Yes No

Create device

Device filtering

Filtering can be performed according to the following criteria:

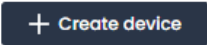
- Probe ID, to filter by area of the industrial network and/or headquarters.
- Device Name

- Device Type (PLC, RTU, SCADA, Honeypot, FIREWALL, etc.)
- Device function (transmitter, receiver, or both)
- Purdue Level, according to Annex II
- Device IP address
- MAC address of the device
- View of virtual MACs reserved by broadcast (Y/N).
- Fixed devices (Y/N), see Annex I.
- Critical devices (Y/N), see Annex I.
- Approved devices (Y/N), see Annex I.
- Traffic filter (i.e. information passively aggregated by the Greinfort engine).

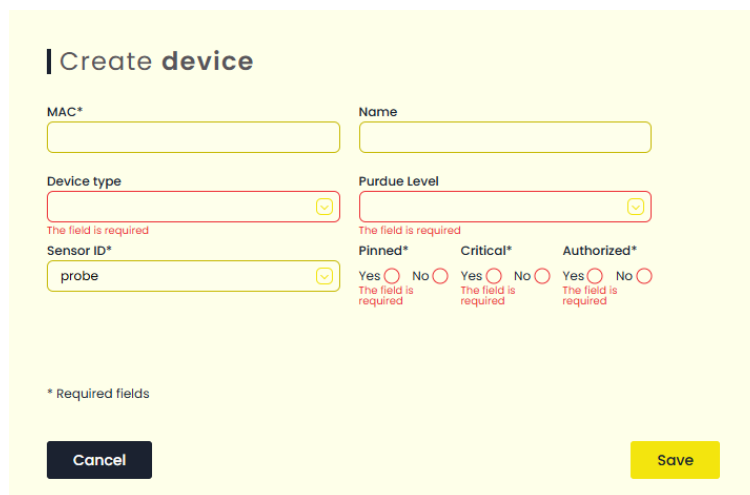
The user can also perform a general search using a text string.

Pressing the button  resets the filters and Greinfort returns to display the full list of devices.

Using the corresponding button , the list of devices and their information is exported to a CSV file.

A new device can be manually added to the network and organization list using the corresponding button. 

The following pop-up window will appear:



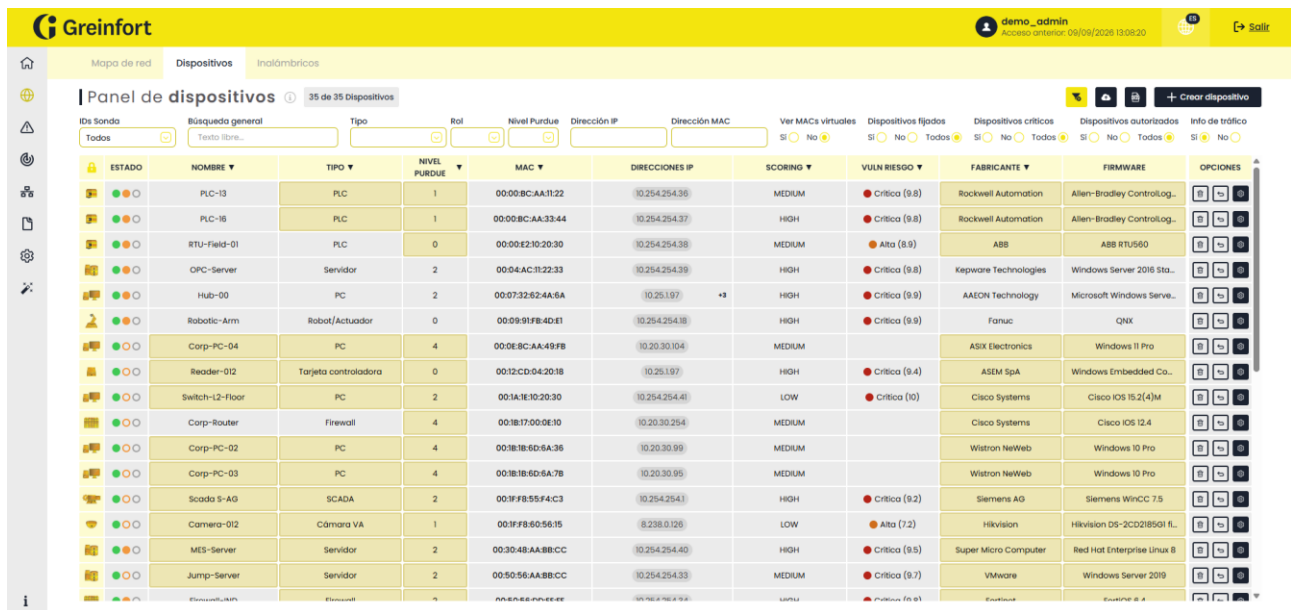
The "Create device" pop-up window contains the following fields and controls:

- MAC***: Text input field.
- Name**: Text input field.
- Device type**: Dropdown menu with a checkmark icon. Below it, a red error message states "The field is required".
- Purdue Level**: Dropdown menu with a checkmark icon. Below it, a red error message states "The field is required".
- Sensor ID***: Text input field with the value "probe" and a checkmark icon.
- Pinned***: Radio button group with "Yes" and "No" options. Below it, a red error message states "The field is required".
- Critical***: Radio button group with "Yes" and "No" options. Below it, a red error message states "The field is required".
- Authorized***: Radio button group with "Yes" and "No" options. Below it, a red error message states "The field is required".
- * Required fields**: Legend text.
- Cancel**: Button at the bottom left.
- Save**: Button at the bottom right.

Fields available for creating a device

The information of the new device must be entered manually. To complete the creation, "Save" must be clicked.

The "Traffic Info" filter will highlight those fields that have been inferred from the passive inventory system (rather than edited directly by the user):



ESTADO	NOMBRE	TIPO	NIVEL PURDUE	MAC	DIRECCIONES IP	SCORING	VULN RIESGO	FABRICANTE	FIRMWARE	OPCIONES
	PLC-13	PLC	1	00:00:9C:AA:11:22	10.254.254.36	MEDIUM	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix...	[Edit] [Delete]
	PLC-16	PLC	1	00:00:8C:AA:33:44	10.254.254.37	HIGH	Critica (9.8)	Rockwell Automation	Allen-Bradley ControlLogix...	[Edit] [Delete]
	RTU-Field-01	PLC	0	00:00:23:10:20:30	10.254.254.38	MEDIUM	Alta (8.9)	ABB	ABB RTU560	[Edit] [Delete]
	OPC-Server	Servidor	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critica (9.8)	Keeware Technologies	Windows Server 2016 Sta...	[Edit] [Delete]
	Hub-00	PC	2	00:07:32:62:AA:5A	10.25.197	HIGH	Critica (9.9)	AAEON Technology	Microsoft Windows Serve...	[Edit] [Delete]
	Robotic-Arm	Robot/Actuador	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critica (9.9)	Fanuc	QNX	[Edit] [Delete]
	Corp-PC-04	PC	4	00:0E:8C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	[Edit] [Delete]
	Reader-012	Tarjeta controladora	0	00:12:CD:04:20:18	10.25.197	HIGH	Critica (9.4)	ASEM SpA	Windows Embedded Ca...	[Edit] [Delete]
	Switch-L2-floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critica (10)	Cisco Systems	Cisco IOS 15.2(4)M	[Edit] [Delete]
	Corp-Router	Firewall	4	00:1B:17:00:DE:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	[Edit] [Delete]
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Edit] [Delete]
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Wistron NetWeb	Windows 10 Pro	[Edit] [Delete]
	Scada S-A0	SCADA	2	00:1F:FB:55:F4:C3	10.254.254.1	HIGH	Critica (9.2)	Siemens AG	Siemens WinCC 7.5	[Edit] [Delete]
	Camera-012	Cámara VA	1	00:1F:FB:60:56:15	8.238.0.126	LOW	Alta (7.2)	Hikvision	Hikvision DS-2CD21850I RL	[Edit] [Delete]
	MES-Server	Servidor	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critica (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	[Edit] [Delete]
	Jump-Server	Servidor	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critica (9.7)	VMware	Windows Server 2019	[Edit] [Delete]

Device dashboard with the "Traffic info" filter turned on

a. Import via CSV

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

In the "Network" section, under the "Device List" tab, the import icon appears. Clicking on it opens the next pop-up.

From this window a CSV file can be selected or dragged with the data of the devices to add or modify, in the format indicated below.

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

- A maximum of 250 devices.
- Header with the following columns (column names can be customized):
 - MAC
 - Device Name
 - Authorized (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)
 - Custom fields.
- The field delimiter must be ";".
- It must not contain empty fields.
- It can contain new device records or existing records whose attributes need to be modified. One row is required per device, in the format indicated.
- New records will simply have all CSV fields covered with the desired information.
- The existing records to be changed must contain the literal *CURRENT* in the fields that must remain unchanged. In the fields to be updated, the new information must be entered.

- Records to be modified must include ***CURRENT*** in one of their properties; this allows them to be distinguished from new records.
- The MAC field cannot contain the literal ***CURRENT***, as it uniquely identifies the device.
- New records may also contain the literal ***CURRENT*** in some fields; this indicates that the default values should be retained. In Boolean fields, the value will be false; text fields, such as name, Purdue level, and device type, will remain null and can be modified from the web interface.
- There are two possible ways to define a custom fieldset, respecting its key-value structure:
 - JSON format: {"key1": "value1", "key2": "value2"}
 - Pairs: key1 | value1 | key2 | value2

Previously defined custom fields can be deleted by overwriting the data using a new CSV file. The ***DELETE*** literal should be included in the place of these fields, analogous to the use of ***CURRENT***.

- It is crucial to write literals between asterisks.

Notice: If in doubt, please consult Support, as improper use of this feature can significantly affect the integrity of the information on the devices. Once the file has been selected, "Confirm" must be clicked.

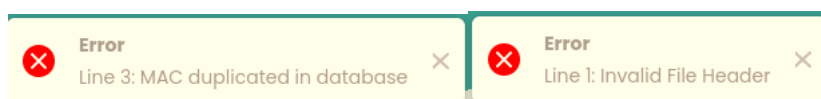
This is a high-impact operation, as it allows to add devices and modify their properties.

If the submitted CSV file does not contain any devices, the following error message is 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 located.



Import Error

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

b. Air Watcher (list of wireless devices)

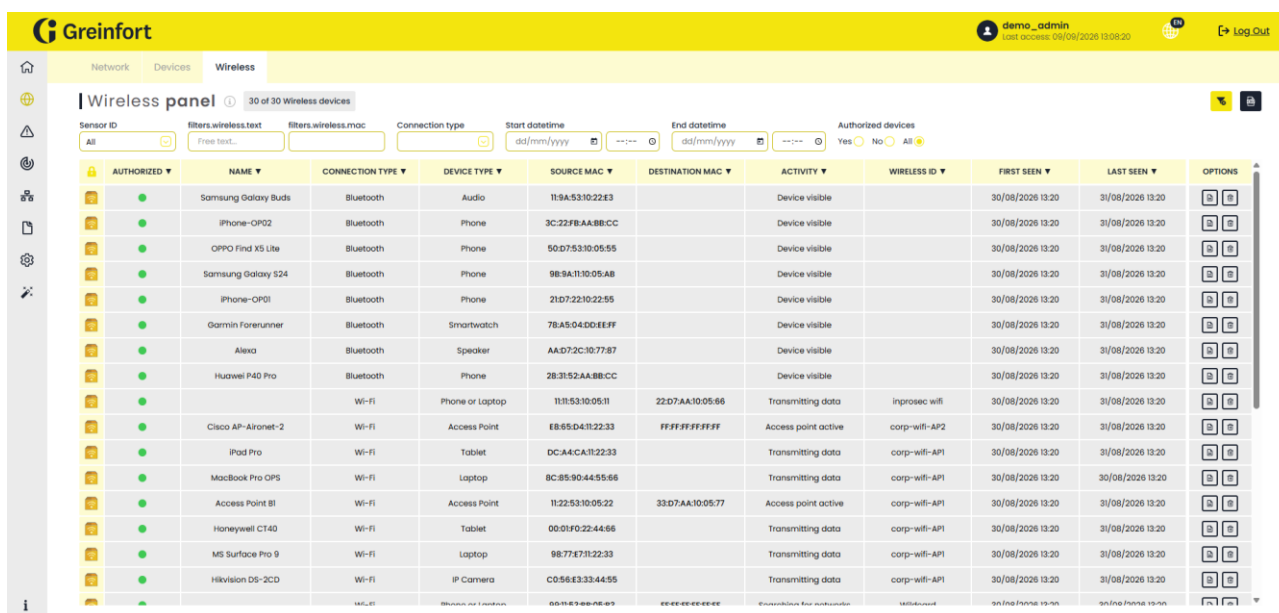
In the network section, the third tab allows to access the list of wireless devices registered on the network.

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

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

The information provided in this section will be as follows, 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:** Corresponds to the name of the device.
- **Connection Type:** It could be Wi-Fi or Bluetooth.
- **Device type:** Values may vary for Bluetooth devices. For Wi-Fi devices, it can display values such as "Access Point" or "Smartphone or Laptop" in addition to "Unknown."
- **Source MAC:** The source MAC address of the packet. Identifies the device itself in the captured communication.
- **Destination MAC:** The destination MAC address of the packet. Identifies the receiving device of the packet.
- **Activity:** Reflects the status of the device or the type of activity performed:
 - Network scanning: The device has the Wi-Fi antenna turned on and is searching for hotspots.
 - Connection attempt: The device has attempted to connect to an access point.
 - Active access point: The device functions as an access point.
 - Data transmission: The device is sending information to an access point.
 - Visible device: This only applies to Bluetooth devices; the device has Bluetooth turned on and is visible to other devices.
- **Wireless ID:** The name or identifier of the Wi-Fi network (it could be empty if, for example, the connection is Bluetooth).
- **First time detected:** dd/mm/yyyy format hh:mm.
- **Last detected:** dd/mm/yyyy format hh:mm.



Wireless panel 30 of 30 Wireless devices

Sensor ID: All | filters.wireless.text: Free 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	FIRST SEEN	LAST SEEN	OPTIONS
	Samsung Galaxy Buds	Bluetooth	Audio	11:9A:53:10:22:E3		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	iPhone-OP02	Bluetooth	Phone	3C:22:F8:A8:8B:CC		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	OPPO Find X5 Lite	Bluetooth	Phone	50:D7:53:10:05:55		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	Samsung Galaxy S24	Bluetooth	Phone	98:9A:11:10:05:A8		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	iPhone-OP01	Bluetooth	Phone	21:D7:22:10:22:55		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	Garmin Forerunner	Bluetooth	Smartwatch	78:A5:04:D0:EE:FF		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	Alexa	Bluetooth	Speaker	AA:D7:2C:10:77:87		Device visible		30/08/2026 13:20	31/08/2026 13:20	
	Huawei P40 Pro	Bluetooth	Phone	28:31:52:AA:8B:CC		Device visible		30/08/2026 13:20	31/08/2026 13:20	
		Wi-Fi	Phone or Laptop	11:9A:53:10:05:11	22:D7:AA:10:05:66	Transmitting data	inprosec willi	30/08/2026 13:20	31/08/2026 13:20	
	Cisco AP-Aironet-2	Wi-Fi	Access Point	E8:65:D4:11:22:33	FF:FF:FF:FF:FF:FF	Access point active	corp-wifi-AP2	30/08/2026 13:20	31/08/2026 13:20	
	iPad Pro	Wi-Fi	Tablet	DC:A4:CA:11:22:33		Transmitting data	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	
	MacBook Pro OPS	Wi-Fi	Laptop	8C:85:90:44:55:66		Transmitting data	corp-wifi-API	30/08/2026 13:20	30/08/2026 13:20	
	Access Point B1	Wi-Fi	Access Point	11:22:53:10:05:22	33:D7:AA:10:05:77	Access point active	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	
	Honeywell CT40	Wi-Fi	Tablet	00:01:F0:22:44:66		Transmitting data	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	
	MS Surface Pro 9	Wi-Fi	Laptop	98:77:47:11:22:33		Transmitting data	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	
	Hikvision DS-2CD	Wi-Fi	IP Camera	C0:56:E3:33:44:55		Transmitting data	corp-wifi-API	30/08/2026 13:20	31/08/2026 13:20	
		Wi-Fi	Unknown or Unknown	00:11:22:33:44:55	EE:EE:EE:EE:EE:EE	Transmitting data	Unknown	30/08/2026 13:20	31/08/2026 13:20	

List of wireless devices

Below are the filters available to locate the devices of interest:

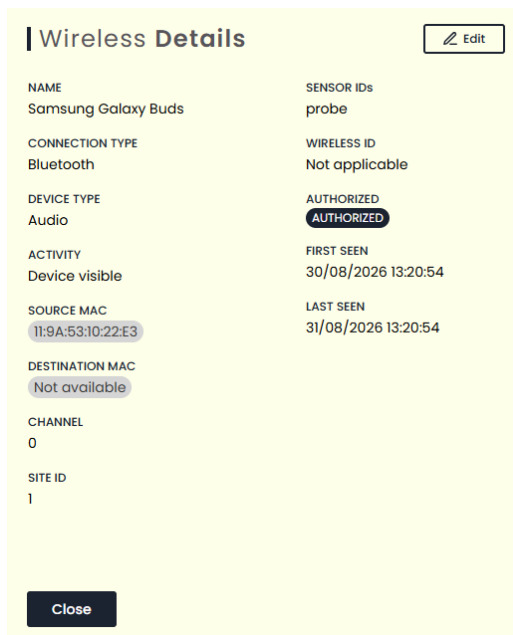
Wireless panel 30 of 30 Wireless devices

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

Wireless device filters

Devices can be sorted alphabetically, ascending or descending, by clicking on any of the columns.

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



The image shows a modal window titled "Wireless Details" with a yellow background. It contains a list of device attributes in two columns. The left column includes: 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), and SITE ID (1). The right column includes: SENSOR IDs (probe), WIRELESS ID (Not applicable), AUTHORIZED (AUTHORIZED), FIRST SEEN (30/08/2026 13:20:54), and LAST SEEN (31/08/2026 13:20:54). There is an "Edit" button with a pencil icon in the top right and a "Close" button in the bottom left.

Wireless Details		Edit
NAME	Samsung Galaxy Buds	SENSOR IDs probe
CONNECTION TYPE	Bluetooth	WIRELESS ID Not applicable
DEVICE TYPE	Audio	AUTHORIZED AUTHORIZED
ACTIVITY	Device visible	FIRST SEEN 30/08/2026 13:20:54
SOURCE MAC	11:9A:53:10:22:E3	LAST SEEN 31/08/2026 13:20:54
DESTINATION MAC	Not available	
CHANNEL	0	
SITE ID	1	

Close

Wireless Device Details

The following additional fields are displayed in this modal window:

- Channel: Transmission channel identifier.
- Site ID: Represents the factory.
- Sensor Identifiers: Identify the sensor.
- Wireless Identification: Unique identifier of the device.

By clicking on the corresponding button, the name of the device can be changed and determine if it is authorized.

c. Smart View (Device Scanning)

This feature allows for active scanning of devices on the OT network, to identify some additional properties of each node using a lightweight query: device version, firmware, open ports, and services running on the machine itself.

To do this, the ports of 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 updated by means of a periodic query based on what is defined by the system by default, or the frequency set in the Wizard.

Greinfort

demo_admin

Last access: 30/08/2026 13:43:26

Log Out

Network

Devices

Wireless

Device panel 35 of 35 Devices

Sensor ID

General search

Type

Role

Purdue level

IP address

MAC address

Show virtual MACs

Pinned devices

Critical devices

Authorized devices

Traffic Info

STATUS	NAME	TYPE	PURDUE LEVEL	MAC ADDRESS	IP ADDRESSES	SCORING	VULN RISK	VENDOR	FIRMWARE	OPTIONS
	PLC-13	PLC	1	00:00:BC:AA:11:22	10.254.254.36	MEDIUM	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLog...	
	PLC-16	PLC	1	00:00:BC:AA:33:44	10.254.254.37	HIGH	Critical (9.8)	Rockwell Automation	Allen-Bradley ControlLog...	
	RTU-Field-01	PLC	0	00:00:12:30:20:30	10.254.254.38	MEDIUM	High (8.9)	ABB	ABB RTU560	
	OPC-Server	Server	2	00:04:AC:11:22:33	10.254.254.39	HIGH	Critical (9.8)	Keypware Technologies	Windows Server 2016 Sta...	
	Hub-00	PC	2	00:07:32:62:4A:6A	10.25.197	HIGH	Critical (9.9)	AAEON Technology	Microsoft Windows Serve...	
	Robotic-Arm	Robot	0	00:09:91:F8:4D:E1	10.254.254.18	HIGH	Critical (9.9)	Fanuc	QNX	
	Corp-PC-04	PC	4	00:0E:8C:AA:49:F8	10.20.30.104	MEDIUM		ASIX Electronics	Windows 11 Pro	
	Reader-012	Controller Card	0	00:12:CD:04:20:18	10.25.197	HIGH	Critical (9.4)	ASEM SpA	Windows Embedded Co...	
	Switch-L2-Floor	PC	2	00:1A:1E:10:20:30	10.254.254.41	LOW	Critical (10)	Cisco Systems	Cisco IOS 15.2(4)M	
	Corp-Router	Firewall	4	00:1B:17:00:0E:10	10.20.30.254	MEDIUM		Cisco Systems	Cisco IOS 12.4	
	Corp-PC-02	PC	4	00:1B:1B:6D:6A:36	10.20.30.99	MEDIUM		Watson NetWeb	Windows 10 Pro	
	Corp-PC-03	PC	4	00:1B:1B:6D:6A:7B	10.20.30.95	MEDIUM		Watson NetWeb	Windows 10 Pro	
	Scada S-AG	SCADA	2	00:1F:FB:55:F4:C3	10.254.254.1	HIGH	Critical (9.2)	Siemens AG	Siemens WinCC 7.5	
	Camera-012	VA Camera	1	00:1F:FB:56:56:15	8.238.0.126	LOW	High (7.2)	Hikvision	Hikvision DS-2CD2185G1 I...	
	MES-Server	Server	2	00:30:4B:AA:BB:CC	10.254.254.40	HIGH	Critical (9.5)	Super Micro Computer	Red Hat Enterprise Linux 8	
	Jump-Server	Server	2	00:50:56:AA:BB:CC	10.254.254.33	MEDIUM	Critical (9.7)	VMware	Windows Server 2019	
	Device 1	Device	5	Device 1	Device 1	Device 1	Device 1	Device 1	Device 1	

Device List

The scanner information can be viewed using the icon on the right. The pop-up window displays all device information, as well as the "TCP Scan" and "UDP Scan" sections. They indicate the ports opened, the date of the last scan, whether it was successful, and any errors.

Device Details

Customized fields

Traffic Insights

Edit

NAME

PLC-13

MAC

00:00:BC:AA:11:22

IPs

10.254.254.36

LAST CONNECTION

31/08/2026 13:20:53

TYPE

PLC

PURDUE LEVEL

1

VULN RISK

Critical (9.8)

VENDOR

Rockwell Automation

SITE ID

1

SENSOR IDs

probe

ROL

Transmitter-Receiver

SCORING

MEDIUM

SCORING DATE

31/08/2026 13:20:53

STATUS

AUTHORIZED

UNPINNED

CRITICAL

LAST SCAN

31/08/2026 13:20:00

SCAN STATUS

Not available

UDP SCAN

Not applicable

TCP SCAN

44818 - enip 80 - http

Close

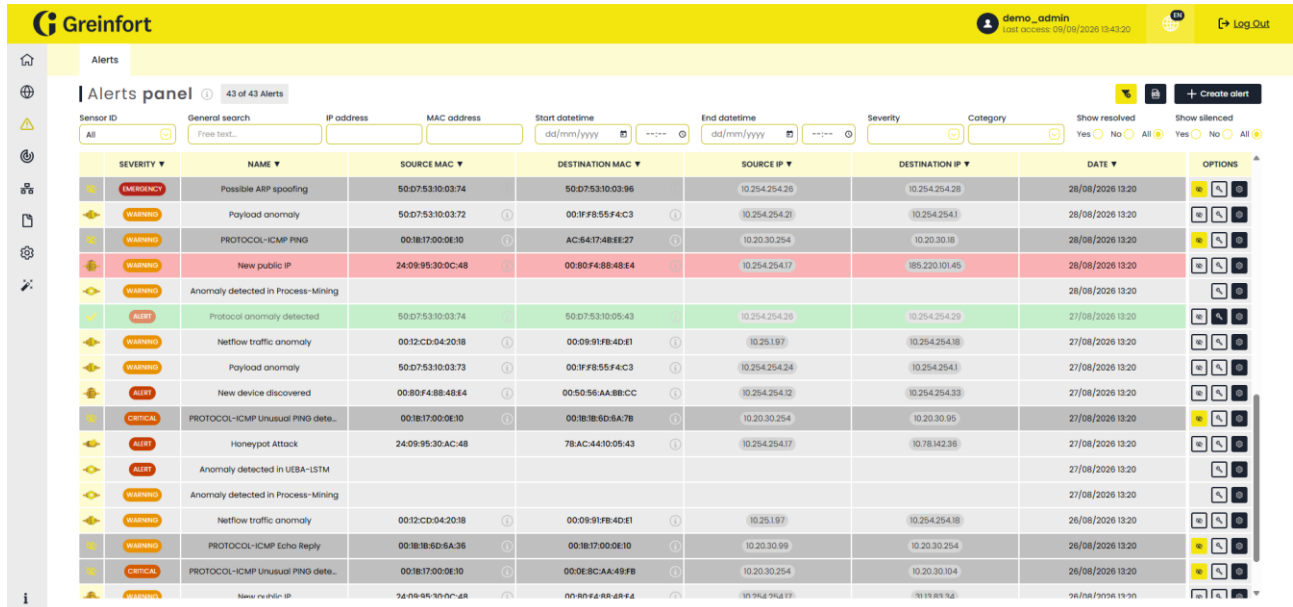
Device details

NOTE: Given the active nature of this operation, a potential impact cannot be completely ruled out, even if none has been observed. It is up to the customer to decide whether to activate the feature. To exclude certain devices from scanning, the "Critical" property must be enabled on the inventory, individually or through a bulk update.

In addition, honeypot devices labeled as such are also exempt due to their behavior as decoys with vulnerable ports. This helps prevent excessive generation of false positives.

4.3. Alerts dashboard

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



The screenshot shows the Greinfort Alerts dashboard. At the top, there's a yellow header with the Greinfort logo, a user profile for 'demo_admin' with 'last access: 09/09/2028 13:43:20', and a 'Log Out' button. Below the header, the 'Alerts' section is active. It features a search bar with '43 of 43 Alerts' and filters for Sensor ID, General search, IP address, MAC address, Start/End datetime, Severity, and Category. There are also checkboxes for 'Show resolved' and 'Show silenced'. The main area is a table of alerts with columns: SEVERITY, NAME, SOURCE MAC, DESTINATION MAC, SOURCE IP, DESTINATION IP, DATE, and OPTIONS. The table lists various alerts such as 'Possible ARP spoofing', 'Payload anomaly', 'PROTOCOL-ICMP PING', 'New public IP', 'Anomaly detected in Process-Mining', 'Protocol anomaly detected', 'Netflow traffic anomaly', 'Honeypot Attack', and 'Anomaly detected in UEBA-LSTM'. Each row has a severity icon (yellow for warning, red for critical) and a set of action buttons in the 'OPTIONS' column.

SEVERITY	NAME	SOURCE MAC	DESTINATION MAC	SOURCE IP	DESTINATION IP	DATE	OPTIONS
EMERGENCY	Possible ARP spoofing	50:D7:53:10:03:74	50:D7:53:10:03:96	10.254.254.29	10.254.254.28	28/08/2028 13:20	[Icons]
WARNING	Payload anomaly	50:D7:53:10:03:72	00:3F:F8:55:F4:C3	10.254.254.21	10.254.254.1	28/08/2028 13:20	[Icons]
WARNING	PROTOCOL-ICMP PING	00:1B:17:00:0E:10	AC:64:17:4B:E2:27	10.20.30.254	10.20.30.18	28/08/2028 13:20	[Icons]
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:8B:4B:E4	10.254.254.17	85.220.101.45	28/08/2028 13:20	[Icons]
WARNING	Anomaly detected in Process-Mining					28/08/2028 13:20	[Icons]
ALERT	Protocol anomaly detected	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.29	10.254.254.29	27/08/2028 13:20	[Icons]
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.251.197	10.254.254.18	27/08/2028 13:20	[Icons]
WARNING	Payload anomaly	50:D7:53:10:03:73	00:3F:F8:55:F4:C3	10.254.254.24	10.254.254.1	27/08/2028 13:20	[Icons]
ALERT	New device discovered	00:80:F4:8B:4B:E4	00:50:56:AA:8B:CC	10.254.254.12	10.254.254.33	27/08/2028 13:20	[Icons]
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:1B:1B:6D:6A:7B	10.20.30.254	10.20.30.95	27/08/2028 13:20	[Icons]
ALERT	Honeypot Attack	24:09:95:30:AC:48	7B:AC:44:10:05:43	10.254.254.17	10.78.142.36	27/08/2028 13:20	[Icons]
ALERT	Anomaly detected in UEBA-LSTM					27/08/2028 13:20	[Icons]
WARNING	Anomaly detected in Process-Mining					27/08/2028 13:20	[Icons]
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.251.197	10.254.254.18	26/08/2028 13:20	[Icons]
WARNING	PROTOCOL-ICMP Echo Reply	00:1B:1B:6D:6A:36	00:1B:17:00:0E:10	10.20.30.99	10.20.30.254	26/08/2028 13:20	[Icons]
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:0E:9C:AA:49:F8	10.20.30.254	10.20.30.104	26/08/2028 13:20	[Icons]
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:8B:4B:E4	10.254.254.17	10.19.87.52	26/08/2028 13:20	[Icons]

List of alerts

A list of alerts present in a given organization and information about them will be displayed.

- Severity: Classification of the alert according to its potential impact on the organization.
- Name: Name assigned to the alert.
- Source MAC: MAC address of the device that generates the alert.
- Destination MAC: MAC address of the device to which the action is directed.
- Source IP: IP address of the device that generates the alert.
- Destination IP: IP address of the device to which the action is directed.
- Date: Date and time the alert is generated.
- Actions (see Annex I for definitions):



: Hovering over it displays the name of the device assigned to that MAC address.



: Button to change the alert status to muted or unmuted (see "Alert classification" in Annex I).



: Button to change the status of the alert (resolved or unresolved), according to the logic indicated in Annex I.



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

Alert details			
NAME	DATE	SOURCE NAME	NOTE CREATOR
Possible ARP spoofing	28/08/2026 13:20:53	PLC-07	Not available
CATEGORY	SOURCE MAC	DESTINATION NAME	
STATIC	50:D7:53:10:03:74	Sensor-Ch:AV	
PROTOCOL	DESTINATION MAC	VALUE	
Not available	50:D7:53:10:03:96	50:d7:53:10:03:74	
SEVERITY	SOURCE IP	DESCRIPTION	
EMERGENCY	10.254.254.26	IP 10.254.254.28 MAC change: old -> 50:d7:53:10:05:55, new -> 50:d7:53:10:03:74	
STATUS	DESTINATION IP	NOTE	
SILENCED ACTIVE	10.254.254.28	Not available	
SITE ID	SOURCE TYPE	NOTE UPDATE	
1	1	Not available	
SENSOR ID	DESTINATION TYPE		
probe	13		
Close			

Alert Details

It is possible to apply filters to show only the alarms of interest. This filtering can be done as follows:

- Probe ID, to filter by industrial network zone and/or headquarters
- General search: Entering a text contained in the alert, including notes
- Device IP address
- MAC address of the device
- Start date and time of the alert search
- Alert search end date and time
- Severity, according to Annex I
- Alarms resolved or unresolved, according to Annex I
- Silenced or unsilenced alarms, according to Annex I

Pressing the button resets the filters and displays the full list of alarms again.



Using the corresponding button, the list of alarms and their information is exported to a CSV file.



A specific alarm can be manually created on the organization's network using the corresponding button.

+ Create alert

The following pop-up window will appear:

Crear alerta

Título*

IP Origen

IP Destino

MAC Origen

MAC Destino

Protocolo

Descripción*

Severidad*

Fecha

dd/mm/yyyy

Valor

* Campos obligatorios

Cancelar

Guardar

Creating alerts

The new alarm information must be entered manually. To complete the creation, "Save" must be clicked.

4.3.1. Public IP

This alert is connected to a cyber intelligence service that allows additional information to be obtained about the communication endpoint located outside the trusted network, in order to determine if it could be malicious.

Alert details

Public IP data

NAME	DATE	SOURCE NAME	NOTE CREATOR
New public IP	28/08/2026 13:20:53	Unknown-Dev-01	Not available
CATEGORY	SOURCE MAC	DESTINATION NAME	
STATIC	24:09:95:30:0C:48	PC Office	
PROTOCOL	DESTINATION MAC	VALUE	
TCP	00:80:F4:88:48:E4	185.220.101.45	
SEVERITY	SOURCE IP	DESCRIPTION	
WARNING	10.254.254.17	Connection with public IP (destination IP: 185.220.101.45)	
STATUS	DESTINATION IP	NOTE	
ACTIVE	185.220.101.45	Not available	
SITE ID	SOURCE TYPE	NOTE UPDATE	
1	Not applicable	Not available	
SENSOR ID	DESTINATION TYPE		
probe	Not applicable		

Close

Alert Details

To access the alert details, click on the gear icon on the right of the panel and select "View Details". Here's the following information:

At the top of this tab is the "Public IP Data" button. Clicking on it displays additional information about the IP address, such as the city and region of origin, time zone, continent, country, coordinates, organization, and zip code.

Public IP Details

[Go to details](#)

Country name	Geo location
 Germany	50.1155,8.6842
City	Organization
Frankfurt am Main	AS205100 F3 Netze e.V.
Region	Postal
Hesse	60306
Timezone	Reputation
Europe/Berlin	Bad IP
Continent	Reputation source
Europe	AbuseIPDB
Hostname	
tor-exit-45.relay.quintex.org	
IP	
185.220.101.45	

Close

Public IP details

4.3.2. IP Reputation and Blocking Policy

When the system detects a new alert associated with a connection to a public IP address, Greinfort queries several public lists reporting activities considered abusive (spam, hacking, etc.). This information enriches the alert with reputational data and, if the public IP address is considered suspicious, modifies the severity and description, and highlights it in red.

Alerts

Alerts panel 43 of 43 Alerts

Sensor ID

General search

IP address

MAC address

Start datetime

End datetime

Severity

Category

Show resolved

Show silenced

SEVERITY

NAME

SOURCE MAC

DESTINATION MAC

SOURCE IP

DESTINATION IP

DATE

OPTIONS

EMERGENCY	Possible ARP spoofing	50:D7:53:10:03:74	50:D7:53:10:03:96	10.254.254.26	10.254.254.28	28/08/2026 13:20	
WARNING	Payload anomaly	50:D7:53:10:03:72	00:1F:F8:55:F4:C3	10.254.254.21	10.254.254.1	28/08/2026 13:20	
WARNING	PROTOCOL-ICMP PING	00:1B:17:00:0E:10	AC:54:17:4BEE:27	10.20.30.254	10.20.30.18	28/08/2026 13:20	
WARNING	New public IP	24:09:95:30:0C:48	00:80:F4:8B:4B:E4	10.254.254.17	185.220.101.45	28/08/2026 13:20	
WARNING	Anomaly detected in Process-Mining					28/08/2026 13:20	
ALERT	Protocol anomaly detected	50:D7:53:10:03:74	50:D7:53:10:05:43	10.254.254.26	10.254.254.29	27/08/2026 13:20	
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.25.197	10.254.254.18	27/08/2026 13:20	
WARNING	Payload anomaly	50:D7:53:10:03:73	00:1F:F8:55:F4:C3	10.254.254.24	10.254.254.1	27/08/2026 13:20	
ALERT	New device discovered	00:80:F4:8B:4B:E4	00:50:56:AA:8B:CC	10.254.254.12	10.254.254.33	27/08/2026 13:20	
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:1B:1B:6D:5A:7B	10.20.30.254	10.20.30.99	27/08/2026 13:20	
ALERT	Honeypot Attack	24:09:95:30:AC:48	7B:AC:44:10:05:43	10.254.254.17	10.78.142.36	27/08/2026 13:20	
ALERT	Anomaly detected in UEBA-LSTM					27/08/2026 13:20	
WARNING	Anomaly detected in Process-Mining					27/08/2026 13:20	
WARNING	Netflow traffic anomaly	00:12:CD:04:20:18	00:09:91:F8:4D:E1	10.25.197	10.254.254.18	26/08/2026 13:20	
WARNING	PROTOCOL-ICMP Echo Reply	00:1B:1B:6D:5A:36	00:1B:17:00:0E:10	10.20.30.99	10.20.30.254	26/08/2026 13:20	
CRITICAL	PROTOCOL-ICMP Unusual PING dete...	00:1B:17:00:0E:10	00:0E:8C:AA:49:F8	10.20.30.254	10.20.30.104	26/08/2026 13:20	

Malicious public IP address highlighted in red

Public IP Details

Country name

Germany

City

Frankfurt am Main

Region

Hesse

Timezone

Europe/Berlin

Continent

Europe

Hostname

tor-exit-45.relay.quintex.org

IP

185.220.101.45

Geo location

50.1155.8.6842

Organization

AS205100 F3 Netze e.V.

Postal

60306

Reputation

Bad IP

Reputation source

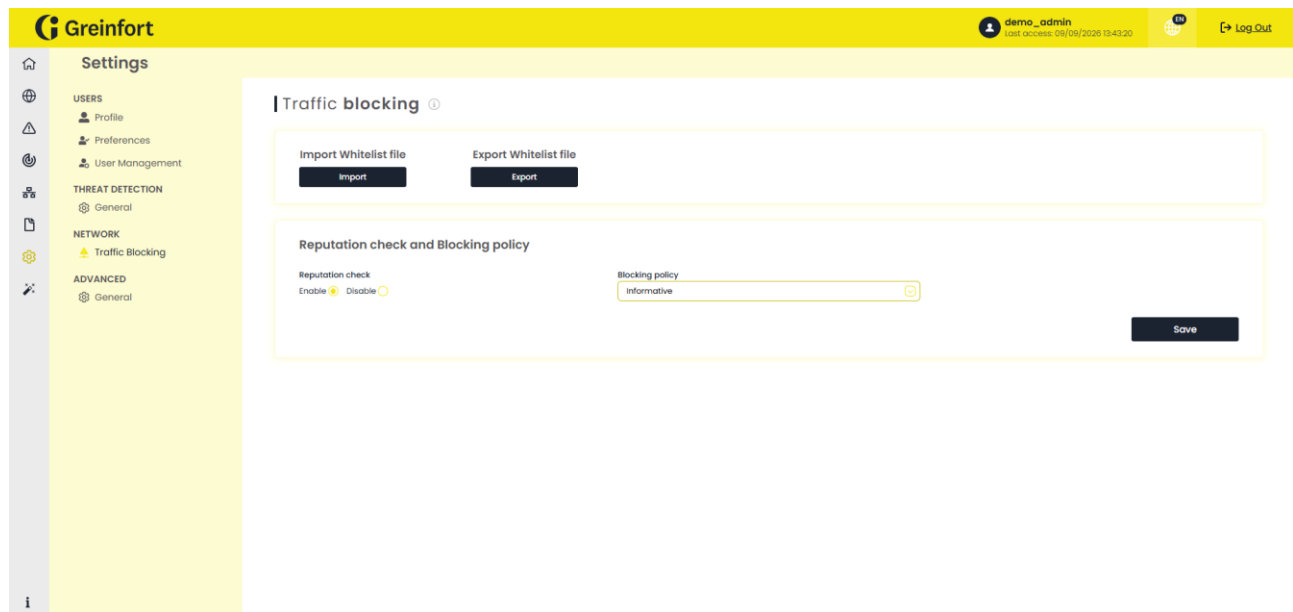
AbuseIPDB

Go to details

Close

Details of a public IP address with reputational information

Reputation check can be turned on and off in the settings menu in the Traffic Blocking section. This option affects incoming alerts, i.e., enabling reputation will not retroactively affect public IP alerts that arrived while reputation was disabled.



Reputation and blocking settings

When the system receives an alert associated with a public IP address that is considered malicious, Greinfort responds by applying one of three available blocking policies:¹

- **Informative:** the situation is notified and it is recommended to check and block traffic to or from that address;
- **Manual or semi-automatic:** a button is enabled to block or unblock the IP address by means of an instruction to the firewall;
- **Automatic:** Greinfort sends the instruction to the firewall without human intervention.

The Blocking Policy can also be disabled. In this case, all IP reputation information in the alerts will be disabled, as well as the blocking rules (by sending a command to the firewall to remove the address blocking rule). This information is not deleted and will be reapplied if the Blocking Policy is reselected as an active value. A drop-down selector for the Blocking Policy can be found in the same menu. Public IP alerts that arrive in the system while the Blocking Policy is disabled do not change retroactively when the Blocking Policy is reactivated.

4.3.3. IP Whitelisting

A list of IP addresses or ranges can be provided in CIDR format that will always be allowed (whitelisted). Their reputation is not evaluated, even if the check is enabled when a related alert is received. In the public IP data menu, the reputation field identifies them as whitelisted.

The upload file must be in CSV format and contain a single column per row, with an IP address (192.168.0.1) or a CIDR range (192.168.1.0/24). The upload is atomic: a single piece of data with incorrect or invalid formatting invalidates the entire operation. Address and range redundancies (repeated addresses, addresses included in CIDR ranges, or overlapping ranges) are not considered errors.

¹ The availability of non-informative options will depend on the customer's context, in particular the manufacturer/model of the firewall Greinfort will communicate with. In case of additional questions, contact the Support team.

The import is done from the lock options using the button under "Import whitelist file". In the pop-up window the file can be grabbed to the green area or selected from the file directory. 

Subsequent imports completely replace the previous whitelist. To not apply any whitelists, an empty file must be uploaded.

Uploading a new whitelist influences public IP alerts that are already in the database:

- Alerts whose IP addresses have already been processed and are included in the new whitelist return to their original state and are marked as "whitelisted".
- Alerts whose IP addresses were whitelisted in the old but not in the new whitelist are subject to reputation calculation and their description is modified accordingly.

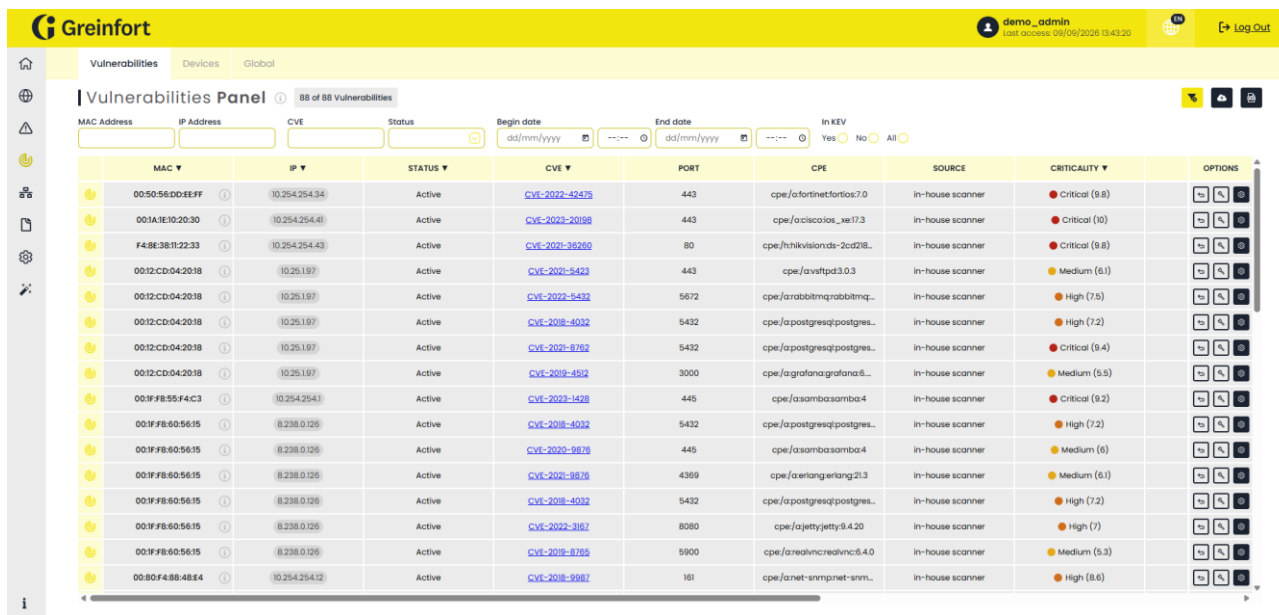
The uploaded whitelist can be downloaded for review using the uploaded button, which generates a CSV file with the saved data. 

4.4. Vulnerability analysis

4.4.1. Vulnerability Dashboard

To access the Vulnerability Dashboard, the user must click on the icon  that appears on the left side of the screen and select the "Vulnerability Dashboard" tab.

The "Vulnerability Dashboard" tab displays a list of all vulnerabilities present in the network. They are located in the services associated with the open ports detected by Smart View and are compared to the NIST National Vulnerability Database (NVD) and the CISA catalog.



The screenshot shows the Greinfort Vulnerability Dashboard. At the top, there's a yellow header with the Greinfort logo, user info (demo_admin, last access: 05/05/2026 13:43:20), and a Log Out button. Below the header, there's a navigation bar with tabs: Vulnerabilities (selected), Devices, and Global. The main area is titled "Vulnerabilities Panel" and shows "88 of 88 Vulnerabilities". It includes search filters for MAC Address, IP Address, CVE, Status, Begin date, End date, and In KEY. The table below lists various vulnerabilities with columns for MAC, IP, STATUS, CVE, PORT, CPE, SOURCE, CRITICALITY, and OPTIONS.

MAC	IP	STATUS	CVE	PORT	CPE	SOURCE	CRITICALITY	OPTIONS
00:50:56:0D:EE:FF	10.254.254.34	Active	CVE-2022-42475	443	cpe:/a:fortinet:fortios:7.0	in-house scanner	Critical (9.8)	
00:1A:1E:10:20:30	10.254.254.41	Active	CVE-2023-20188	443	cpe:/a:cisco:ios_xe:17.3	in-house scanner	Critical (10)	
F4:9E:38:31:22:33	10.254.254.43	Active	CVE-2021-36260	80	cpe:/h:hikvision:ds-2cd218...	in-house scanner	Critical (9.8)	
00:12:CD:04:20:18	10.25.197	Active	CVE-2021-5423	443	cpe:/a:avast:avast3.0.3	in-house scanner	Medium (6.1)	
00:12:CD:04:20:18	10.25.197	Active	CVE-2022-5432	5672	cpe:/a:rabbitmq:rabbitmq...	in-house scanner	High (7.5)	
00:12:CD:04:20:18	10.25.197	Active	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	High (7.2)	
00:12:CD:04:20:18	10.25.197	Active	CVE-2021-8762	5432	cpe:/a:postgresql:postgres...	in-house scanner	Critical (9.4)	
00:12:CD:04:20:18	10.25.197	Active	CVE-2019-4502	3000	cpe:/a:grafana:grafana...	in-house scanner	Medium (5.5)	
00:1F:F8:55:F4:C3	10.254.254.1	Active	CVE-2023-1428	445	cpe:/a:samba:samba:4	in-house scanner	Critical (9.2)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	High (7.2)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2020-8876	445	cpe:/a:samba:samba:4	in-house scanner	Medium (6)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2021-9876	4369	cpe:/a:erlang:erlang:21.3	in-house scanner	Medium (6.1)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2018-4032	5432	cpe:/a:postgresql:postgres...	in-house scanner	High (7.2)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2022-3167	8080	cpe:/a:jetty:jetty:9.4.20	in-house scanner	High (7)	
00:1F:F8:50:56:15	8.238.0.126	Active	CVE-2019-8765	5900	cpe:/a:realvnc:realvnc:6.4.0	in-house scanner	Medium (5.3)	
00:80:F4:88:4B:E4	10.254.254.72	Active	CVE-2018-3987	161	cpe:/a:net-snmp:net-snmp...	in-house scanner	High (8.6)	

Vulnerability Dashboard

Vulnerabilities Panel 88 of 88 Vulnerabilities										
MAC Address	IP Address	CVE	Status	Begin date	End date	In KEV				
				dd/mm/yyyy	dd/mm/yyyy	Yes No All				
CPE	SOURCE	CRITICALITY	CWE	DISCOVERED DATE	PUBLISHED DATE	LAST SEEN DATE	KEV ADDED	KEV DUE	OPTIONS	
cpe:/fortinet:fortios7.0	In-house scanner	Critical (9.8)	CWE-787	31/08/2026	19/06/2026	31/08/2026	13/12/2022	03/01/2023		
cpe:/cisco:ios_xe17.3	In-house scanner	Critical (10)	CWE-269	31/08/2026	19/06/2026	31/08/2026	16/10/2023	20/10/2023		
cpe:/hikvision:ds-2cd218...	In-house scanner	Critical (9.8)	CWE-78	31/08/2026	19/06/2026	31/08/2026	10/01/2022	24/01/2022		
cpe:/avast:avastp3.0.0	In-house scanner	Medium (6.1)	CWE-364	31/08/2026	19/06/2026	31/08/2026				
cpe:/arabitsmq:rabbitmq...	In-house scanner	High (7.5)	CWE-390	31/08/2026	19/06/2026	31/08/2026				
cpe:/postgresql:postgres...	In-house scanner	High (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/postgresql:postgres...	In-house scanner	Critical (9.4)	CWE-382	31/08/2026	19/06/2026	31/08/2026				
cpe:/agratana:grafana5...	In-house scanner	Medium (5.5)	CWE-839	31/08/2026	19/06/2026	31/08/2026				
cpe:/asambasamba4	In-house scanner	Critical (9.2)	CWE-382	31/08/2026	19/06/2026	31/08/2026				
cpe:/postgresql:postgres...	In-house scanner	High (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/asambasamba4	In-house scanner	Medium (6)	CWE-476	31/08/2026	19/06/2026	31/08/2026				
cpe:/aerlang:erlang21.3	In-house scanner	Medium (6.1)	CWE-476	31/08/2026	19/06/2026	31/08/2026				
cpe:/postgresql:postgres...	In-house scanner	High (7.2)	CWE-287	31/08/2026	19/06/2026	31/08/2026				
cpe:/jetty:jetty9.4.20	In-house scanner	High (7)	CWE-476	31/08/2026	19/06/2026	31/08/2026				
cpe:/aradivinc:radvinc6.4.0	In-house scanner	Medium (5.3)	CWE-200	31/08/2026	19/06/2026	31/08/2026				
cpe:/anet-smmp:net-smm...	In-house scanner	High (8.6)	CWE-119	31/08/2026	19/06/2026	31/08/2026				

Vulnerability dashboard detail

The information displayed in each row is as follows:

- **MAC address:** The MAC address of the device where the vulnerability was detected.
- **Status:** Indicates whether the vulnerability is active, resolved, muted, or a false positive.
- **CVE:** "Common vulnerabilities and exposures". Identifier according to the vulnerability classification glossary.
- **Port:** The 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 according to the level of severity of the vulnerability.
- **CWE:** "Common Enumeration of Weaknesses." Identifier of the common weakness associated with the vulnerability found.
- **Date of discovery:** The date on which the vulnerability was detected.
- **Publication date:** The date on which the CVE-referenced vulnerability was published to the NVD database.
- **"Last Seen":** The timestamp where the vulnerability was last seen.
- **KEV ADDED:** KEV stands for "Known Exploited Vulnerabilities". This is the CISA catalog of actively exploited CVEs in real-world environments; the inclusion date and a ♦ are displayed when the CVE is linked to ransomware campaigns.
- **KEV EXPIRATION:** deadline proposed by CISA for the resolution of the corresponding CVE.
- **Options (actions):**



Go to: View alerts generated by this vulnerability or the devices on which it is present.



Change status (active, resolved, muted, or false positive).



Other actions: View the details of a vulnerability and add a note.

Show Vulnerability

SITE ID 1	CWE CWE-787	DESCRIPTION Heap-based buffer overflow in FortiOS SSL-VPN allows
MAC 00:50:56:DD:EE:FF	STATUS Active	
IP 10.254.254.34	NOTE Not available	KEV DATE ADDED 13/12/2022
CVE CVE-2022-42475	NOTE CREATOR Not available	KEV DUE DATE 03/01/2023
PORT 443	NOTE UPDATE Not available	<i>This vulnerability has been linked to ransomware campaigns</i>
CPE cpe:/o:fortinet:fo	DATE DISCOVERED 31/08/2026 13:20:54	
SOURCE in-house scanner	DATE PUBLISHED 19/06/2026 12:36:57	
CRITICALITY Critical (9.8)	DATE LAST SEEN 31/08/2026 13:20:54	

Close

Details of a vulnerability

Next to the header is the number of visible vulnerabilities and the total count.

Vulnerabilities Panel

88 of 88 Vulnerabilities

MAC Address	IP Address	CVE	Status	Begin date	End date	In KEV
				dd/mm/yyyy	dd/mm/yyyy	Yes ☐ No ☐ All ☐

Number of vulnerabilities and filters

The screenshot above shows that filters can be applied to show only the vulnerabilities of interest. Filtering is done by:

- MAC Address
- CVE
- Status
- Start Date and Time
- End Date and Time
- Presence in the KEV catalogue

Pressing the button  will reset the filter values and the full list of all vulnerabilities will be displayed again.

Using the corresponding button, the user can import a CSV file with the vulnerabilities to add. The file must contain the following fields and keep 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's Note (optional)
- Timestamp discovered
- Published timestamp
- Last seen with timestamp



The user can export a CSV file with the list of vulnerabilities and their information.

4.4.2. Device Stats

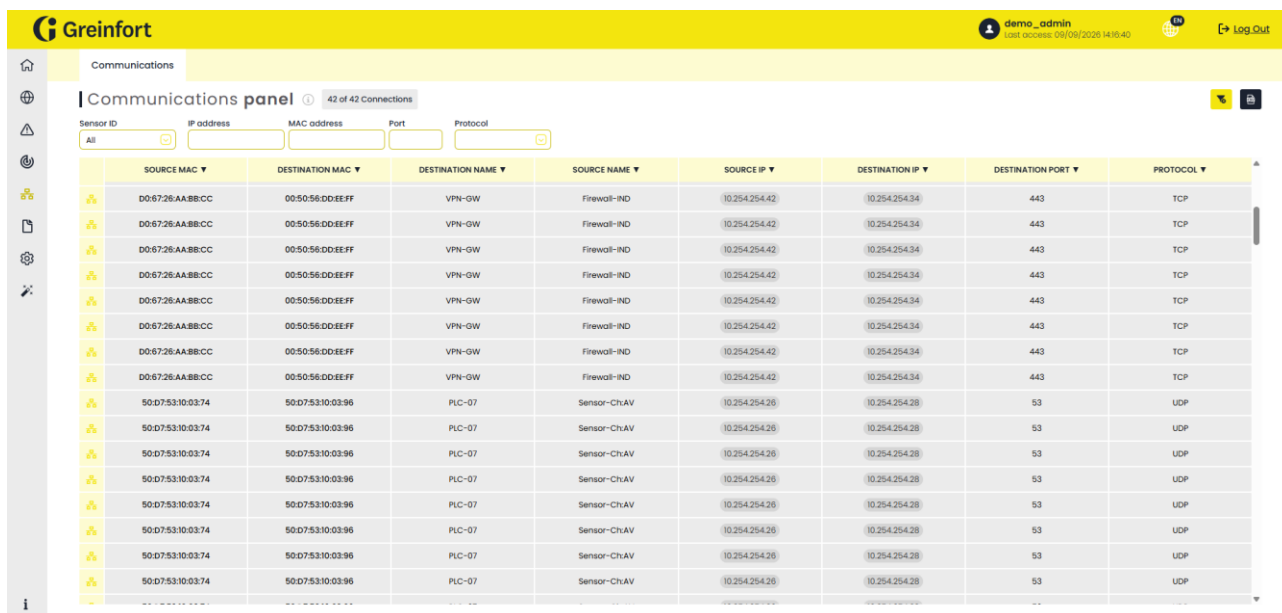
Displays vulnerabilities found in the network, categorized by device.

4.4.3. Global Statistics

It provides global network statistics based on its vulnerabilities.

4.5. Communications

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



Source MAC	Destination MAC	Destination Name	Source Name	Source IP	Destination IP	Destination Port	Protocol
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
D0:67:26:AA:BB:CC	00:50:56:DD:EE:FF	VPN-GW	Firewall-IND	10.254.254.42	10.254.254.34	443	TCP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP
50:07:53:10:03:74	50:07:53:10:03:96	PLC-07	Sensor-ChAV	10.254.254.26	10.254.254.28	53	UDP

List of communications

A list of all communications made between OT devices on the organization's network is displayed, as well as information about them.

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

Communications panel

42 of 42 Connections

Sensor ID

All

IP address

MAC address

Port

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.

Greinfort

demo_admin

Last access: 09/08/2026 14:06:40

Log Out

Reports

7 of 7 Reports

Type

Start datetime

dd/mm/yyyy

End datetime

dd/mm/yyyy

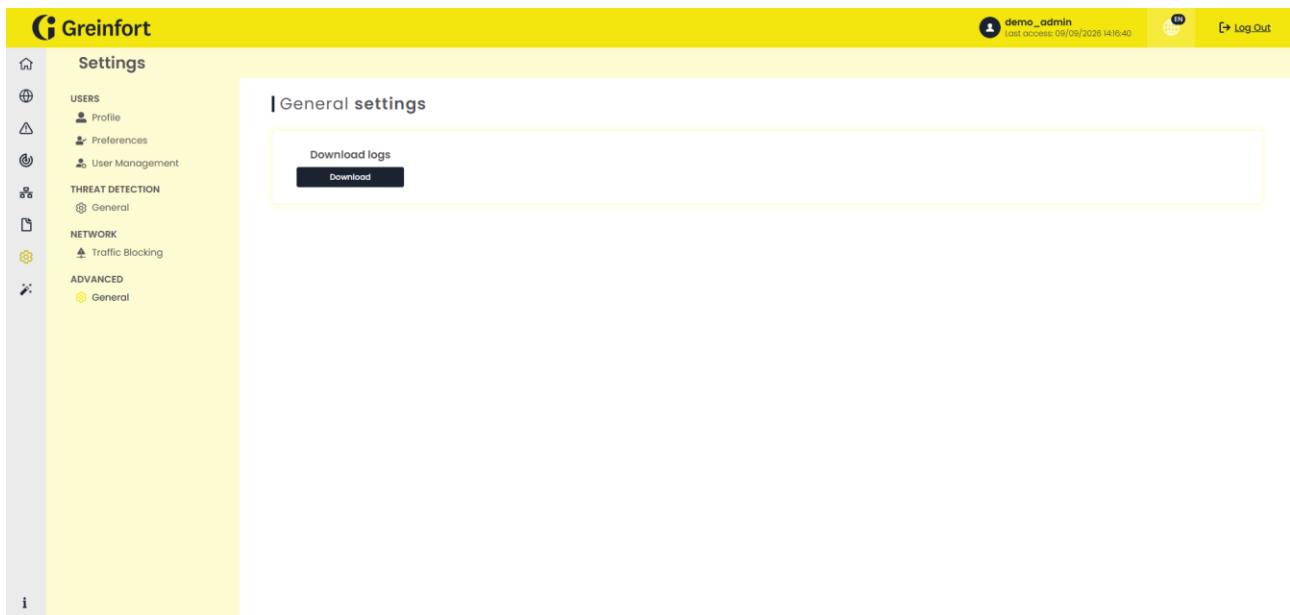
	FILE TYPE	CREATION DATE	FORMAT	OPTIONS
	Unauthorized devices	30/08/2026 13:20	CSV	
	Alerts	30/08/2026 13:20	CSV	
	Scoring	30/08/2026 13:20	CSV	
	Public IPs	30/08/2026 13:20	CSV	
	MACs & IPs	30/08/2026 13:20	CSV	
	Wireless devices	30/08/2026 13:20	CSV	
	Vulnerabilities	30/08/2026 13:20	CSV	

Latest reports available

The screen displays a list of manually or automatically generated reports with a given periodicity. The reports are available for download.

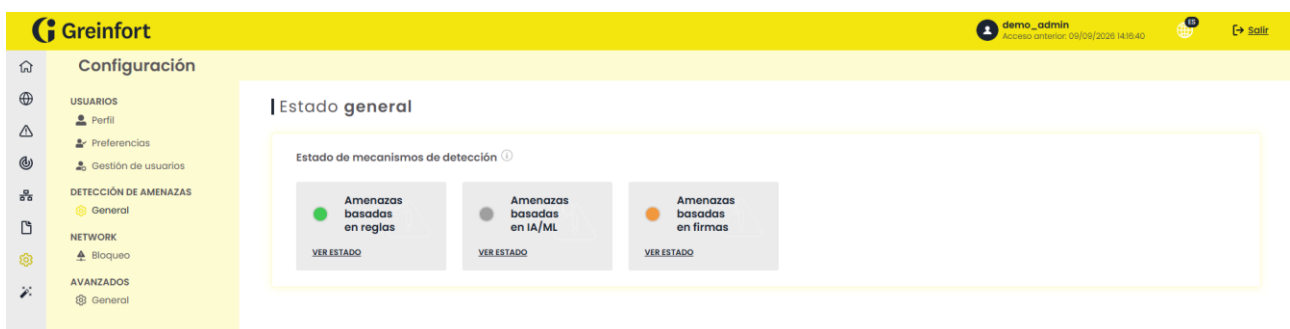
4.7. Other scenarios

In the configuration, different parameters of the Service can be customized.
In the Advanced General section, the user can download the system logs to a file.



Export Logs Section

In Threat Detection, the general status of the different anomaly detection strategies is initially presented in traffic light mode:



Algorithm Settings Screen

Rule-based threats

- Red: All rules are in training mode, inactive, or not covered by their status field.
- Orange: Some rules are in production mode, but not all.
- Green: All rules are in production mode.
- Gray: There are no rules.

AI/ML-based threats

- Red: All rules are in training mode, inactive, or not covered by their status field.
- Orange: Some algorithms are in production mode, but not all.
- Green: All algorithms are in production mode.
- Gray: There are no algorithms.

Signature-based threats

- Red: All items are in training mode or inactive, or their status field is not covered.

- Orange: Some of the items have a value other than active, but not all.
- Green: All items have a status equal to active and the signature_timestamp field is less than seven days old.
- Gray: there are no elements.

5. ANNEX I: Device Classification and Alerts

5.1. Device Classification

5.1.1. According to the Status

- **Authorized/Unauthorized:** Authorized devices are those that the customer has explicitly acknowledged as legitimate.
- **Critical/Non-Critical:** Greinfort does not actively interact with devices marked as critical, e.g., older equipment, no maintenance support, or no spare parts.
- **Fixed/Non-fixed:** Fixed devices will appear in the Greinfort app even if they have not established any communication on the organization's network. For example, devices temporarily isolated from the network for maintenance.

5.2. Alert Classification

5.2.1. According to the Status

- **Resolved/Unresolved:** the resolved alarms have already been managed, but it is desired to preserve their appearance in future identical situations (same typology, MAC addresses, IP addresses and ports involved). Unresolved alarms are pending management.
- **Mute/Unmuted:** Muted alarms are not regenerated in the same network context. For example, a device's communication with a public IP address that is known and controlled by the organization can be muted.

It is worth mentioning that silenced alarms, even if they are not shown to the user, are stored in a database for later consultation by Greinfort staff at the customer's request, if necessary.

5.2.2. Depending on the severity

The severity levels used for the alerts are based on RFC 5424, although they are not equivalent, as the events have been cataloged according to the experience of the technical staff.

From highest to lowest severity, alerts are categorized as follows:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informative
- Debug

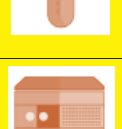
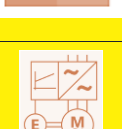
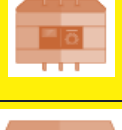
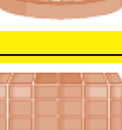
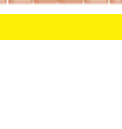
6. ANNEX II: Purdue Asset and Level Icons

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: Business management devices, such as ERP, CRM or SCM systems.

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

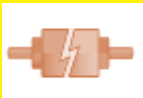
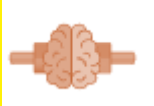
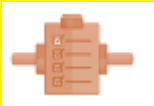
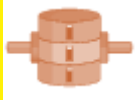
Icon	Description	PURDUE Level
	PC	2
	SCADA	2
	DCS	2
	Virtual	2
	HMI	2
	TABLET	2
	VOIP PHONE	2
	SERVER	2

	PHONE	2
	RTU	1
	VS-CAM	1
	BARCODE READER	1
	PLC	1
	ROBOT	0
	VARIABLE FREQUENCY DRIVE	0
	CONTROLLER CARD	0
	SENSOR	0
	AFD	0
	SWITCH	Depending on context
	ROUTER	Depending on context
	FIREWALLS	Depending on context

	OTHERS	Depending on context
	HONEYPOT	Depending on context

Device Representative Icons

7. ANNEX III: Alert Icons

Icon	Description
	Manual Alert
	Machine Learning Alert
	Static Rule Alert
	IDS Alert
	Honeypot Alert

Representative alert icons



Greinform Solutions S.L

Maria Berdiales 20, 4th fl.
36203 | Vigo | Spain

(+34) 886 251 058

info@greinform.com

sales@greinform.com