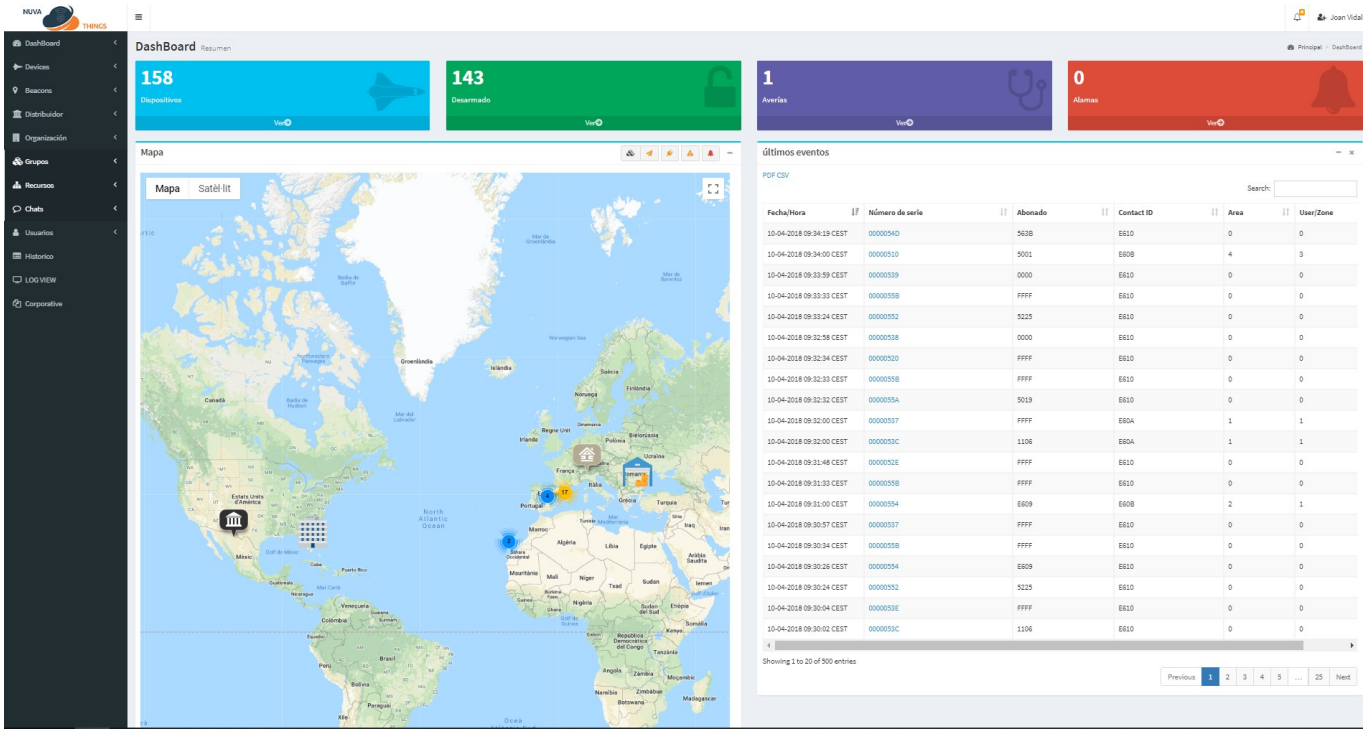
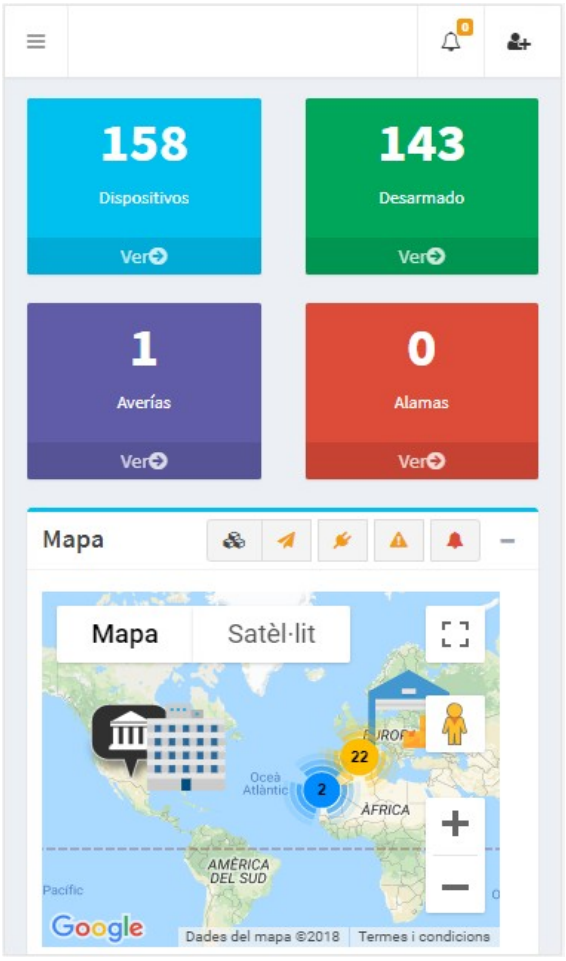
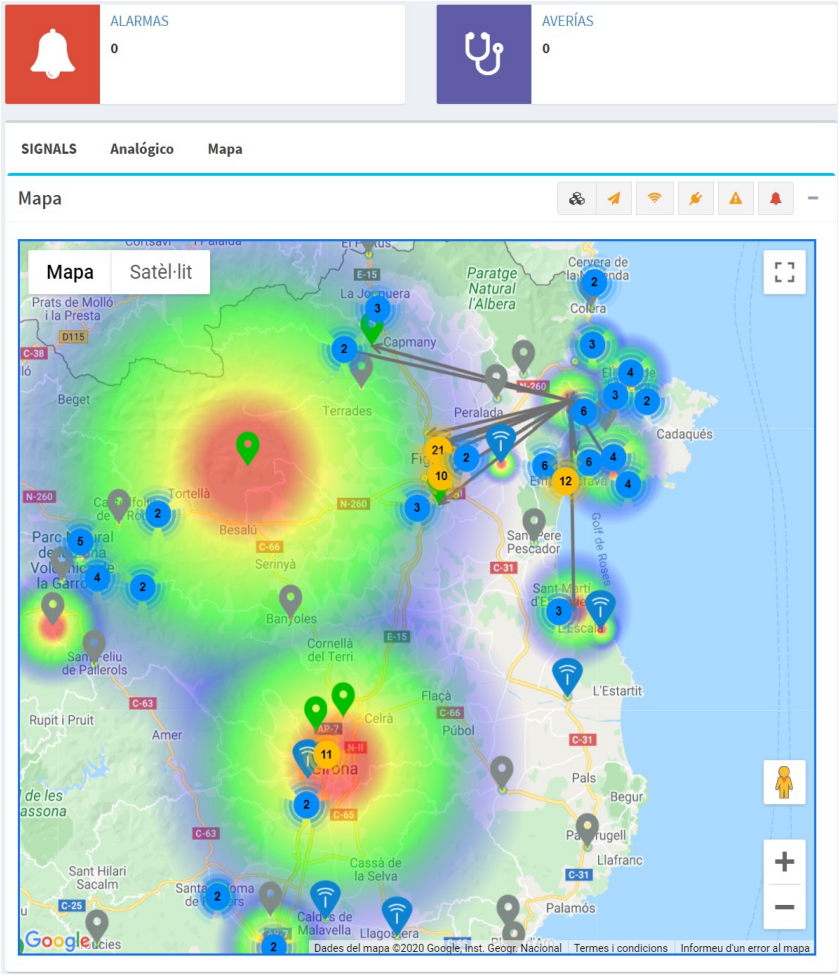
NUVA-CLOUD







Version 2.11 (06/10/2021)

Cloud Nuva

The Nuva cloud is a powerful tool for analysis, monitoring, configuration, control and diagnosis of both the equipment and the system as a whole.

The system automatically adapts to the credentials of the user who logs in, and for this it defines 5 access levels: End user, group users, Installer user, administrator user and Distributor user..

Fina User: It is the end customer, who only has control over the equipment he owns..

Group User : It is an end customer with visibility to a group of equipment.

Installer: He is the installation and maintenance technician, he can see all the equipment assigned to the group to which he belongs, although he can be assigned a view of all the groups. He can create users of equal or lower level than his according to rolel.

Admin: It is circumscribed within a company, a person who is in charge of creating groups within the cloud, as well as users of a level equal to or lower than theirs..

Distributor: It is the one that can create companies within the cloud, as well as administrator users within the company..

Respect EN50136, the corresponding levels are as follows

- Level 2 : final user / group user.
- Level 3: Installer / admin
- Level 4: Distributor.

Distributors

Resellers manage companies and have visibility into their groups, users, and devices.

Companies:

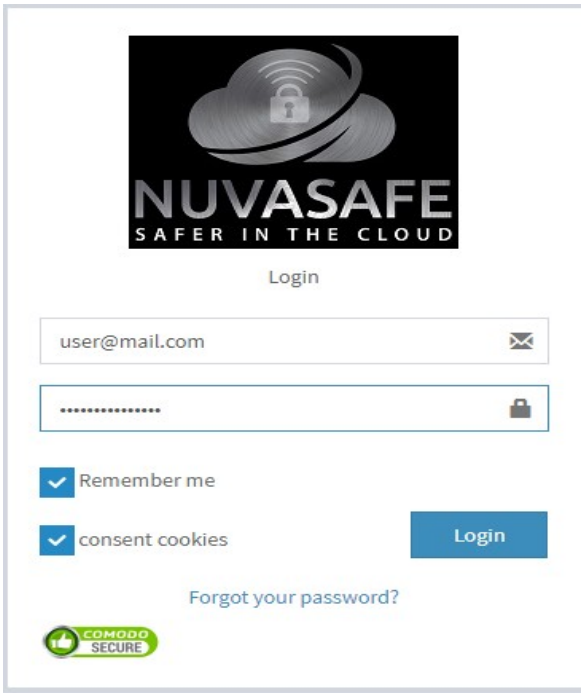
Companies can be treated as companies or as delegations of the same company, teams and users are assigned to companies

Groups:

Groups can be created within a company, which can have a geographical or logical organization (by degree of security), or represent a sub-contractor, the users assigned to a group will only have vision of the devices in the group.

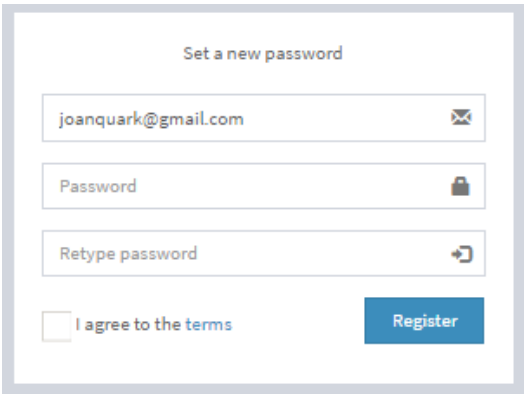
The administrator is capable of creating users who can see all the groups created within the same company, while the Distributor user is capable of creating users who can see all the companies and all the groups.

Login



The Remember me option enables the system to remember your logged in user for at least one week.
If the cookie consent tab is not checked, login to the server is not allowed, since the Login result is saved in a Cookie.

The link "I forgot my password", sends a link to the user's email to recover it



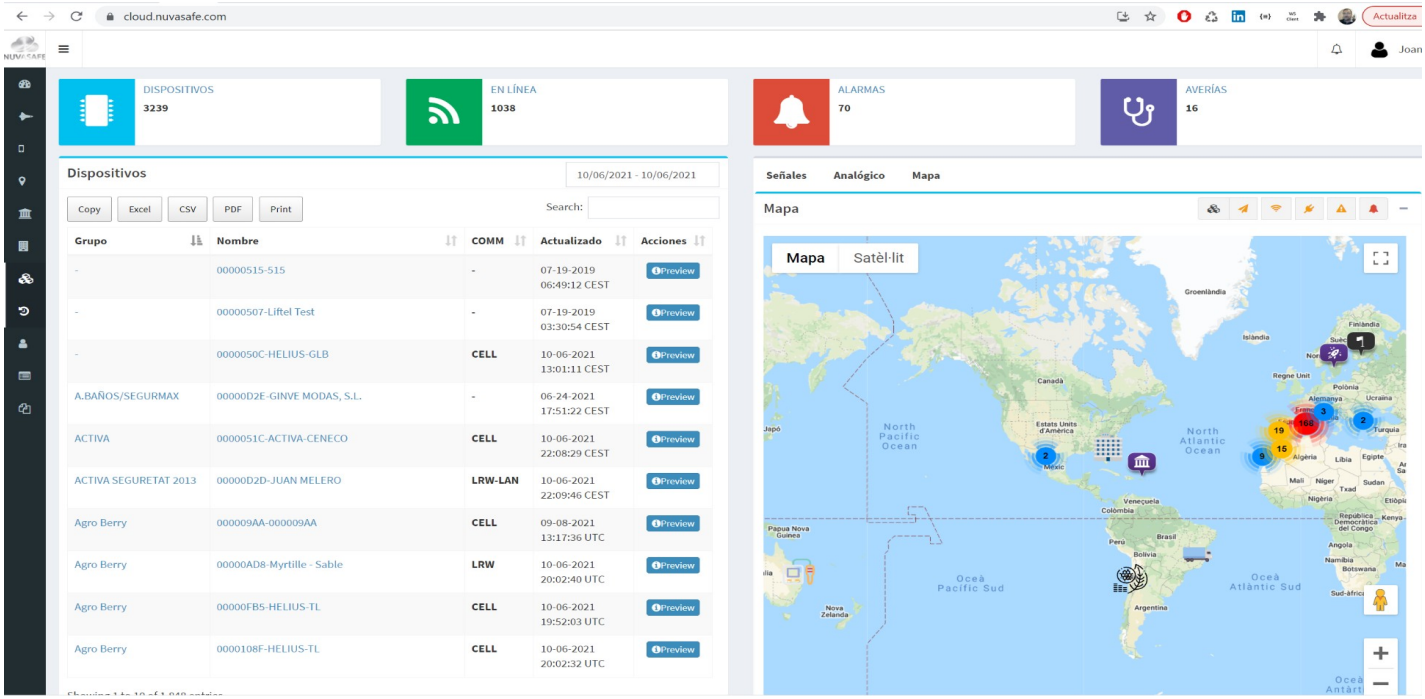
In both cases, once the correct password has been entered, we will enter the main screen or Dashboard

Login Errors

The attempt of 3 erroneous logins will lead to the blocking of the login screen for 90 seconds, on the other hand, the time limit for entering the password is 60 seconds, if the password is not completed in that time, it will be counted as an erroneous attempt.

Dashboard -

The dashboard is the main screen of the cloud and summarizes the general status of the equipment. (administrator view)



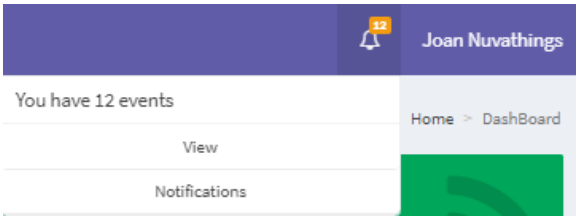
We can see on the left the navigation bar that allows us to access the main sections of the server that consists of:

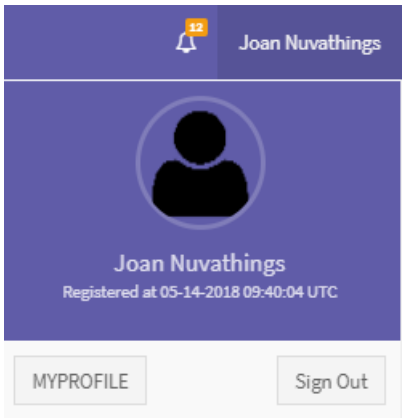
- Devices
- Beacons
- Groups.
- Users.
- Historic.

In the upper part there are 4 colored boxes that summarize the total number of units, which of them are online, how many of them have a fault in the area and how many units have an alarm in progress, if we click on "view" each one of the boxes, the devices screen will be displayed with the list, which can be exported to pdf or csv.

Access to profile and notifications

From the top right we can display access to notifications pending review and the activation / deactivation of 'push' notifications.

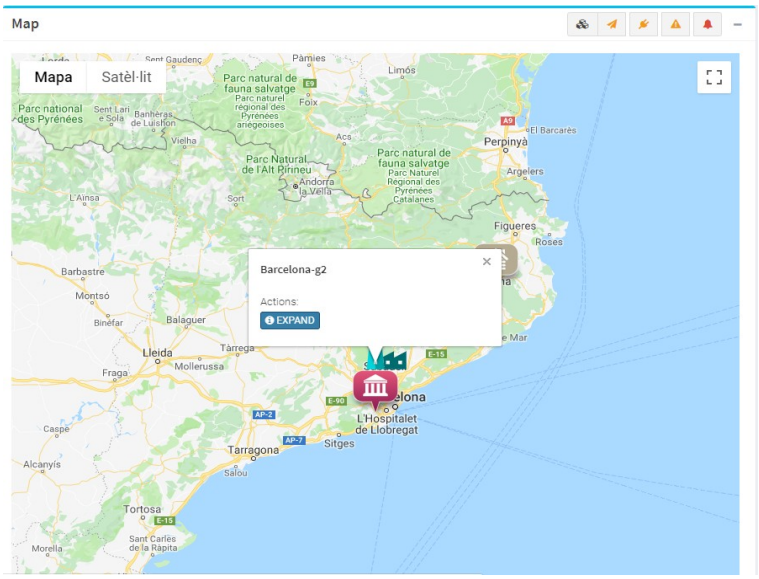




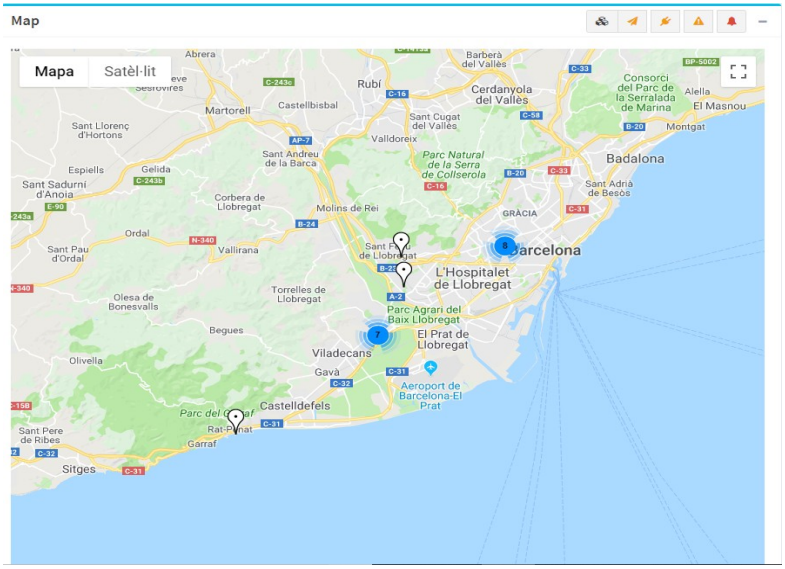
To its right is the user drop-down for profile, which will take us to the user editing screen, as well as being able to log out of the platform.

Map

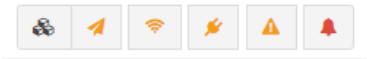
If the user login level has visibility in more than one group, the map view shows the identification icons of the groups, clicking on the group icon brings up an InfoWin:



that offers us the option to expand the group to see the devices that make it up.
This is the map view by devices, which will be by default in the event that the user's login level only has visibility over a group or only over assigned devices (in the case of an end user)



All the devices belonging to the user are displayed on the map, the default display shows the devices with the color that has been assigned to the group to which they belong, there are 5 display filters:



- Group Filter.
- Communication / polling.
    - Shows in black color devices not online.
- LORA link and gateways
- Power failures filter
    - Shows in yellow devices with battery or mains failure
- Zones failure
    - Shows in violet devices with failures in its inpts.
- Alarm filter
- Shows in red, devices with active alarm.

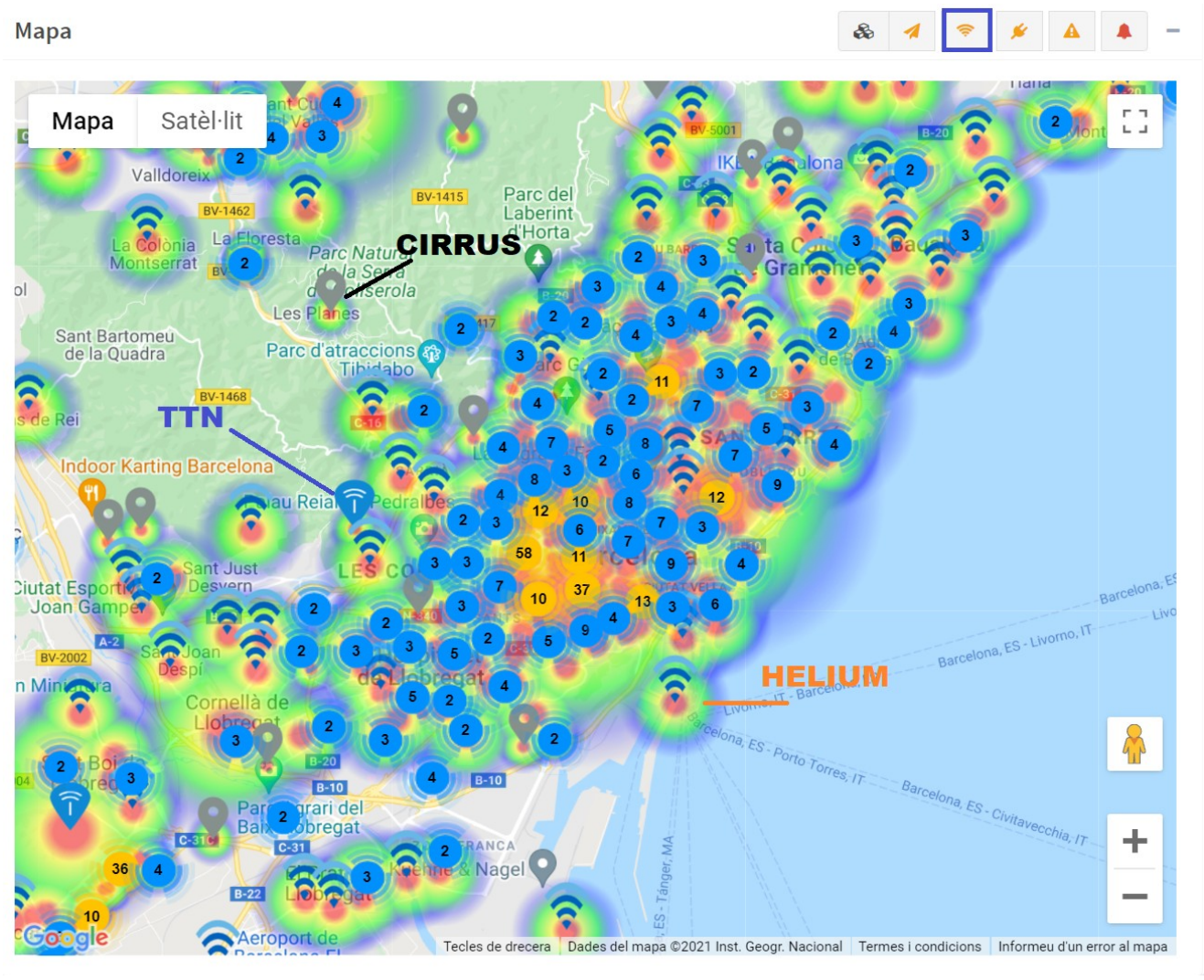
LORA maps

Both the installed Nuva equipment and The Things Network gateways form an anti-inhibition network with availability in many parts of the Spanish and European geography.

By pressing the "Lora Links" button, once a specific area of the map has been selected (it is important not to select an area that is too high so as not to overload the browser's memory), a heat map will be displayed with the approximate coverage of the devices and/or gateways In the area:

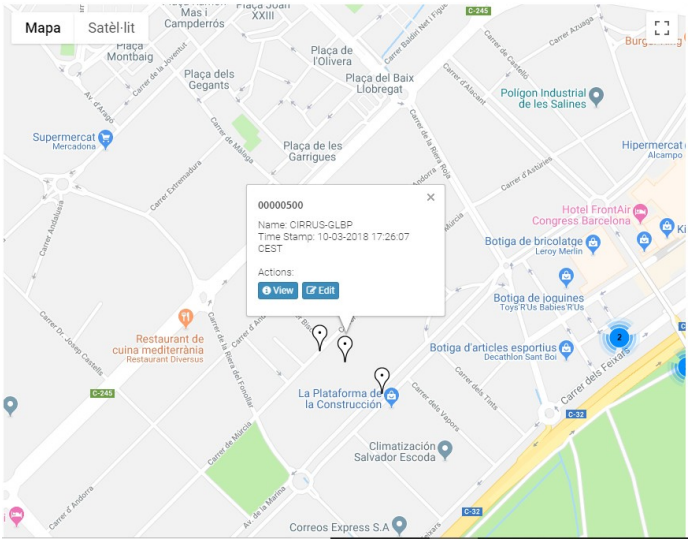
For a Nuva device whose “LORA antenna elevation” in the Equipment Edition is different from 0, it is interpreted as “exterior” therefore a circle of greater range will be drawn than one that is interior (Antenna elevation = 0) and proportional to its elevation.

For the LORAWAN gateways (blue pins + Wi-Fi type) in the area, those of the “Indoor” type will draw a circle with a radius equivalent to an indoor Nuva device, the “outdoor” type gateways will draw a circle with a radius 4 times greater . Approximately, the red area indicates that indoor coverage could be had, the yellow / green area would indicate outdoor coverage and some favorable interiors (such as equipment located near windows or on the upper floors of buildings), finally the gray area indicates that coverage would be exterior only

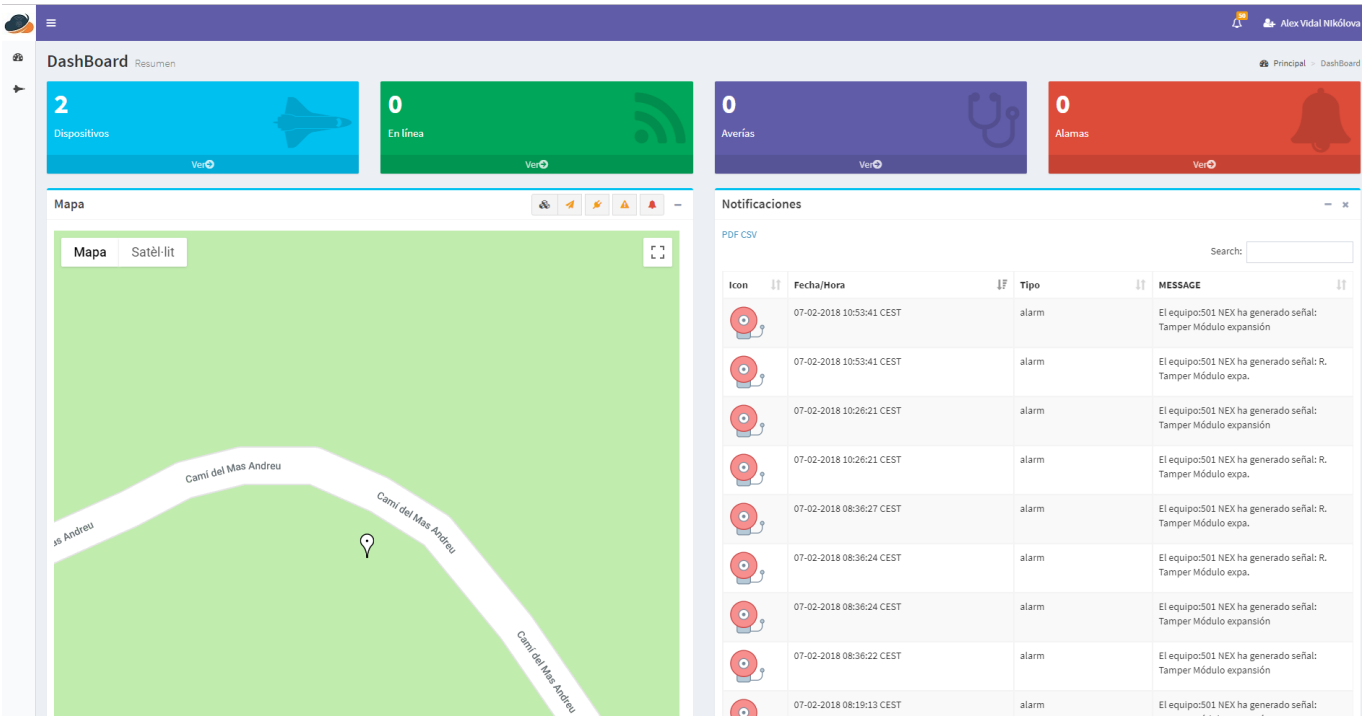


Finally, indicate that the Nuva equipment pins, in gray, indicate that they do not have a Lora link, while the green pins indicate that they have a LORA backup.

Once we select a marker of a specific piece of equipment, when clicking on it a contextual menu appears that gives us the serial number and name of the equipment as well as two buttons that allow us to view the state of the equipment while editing the data of it.



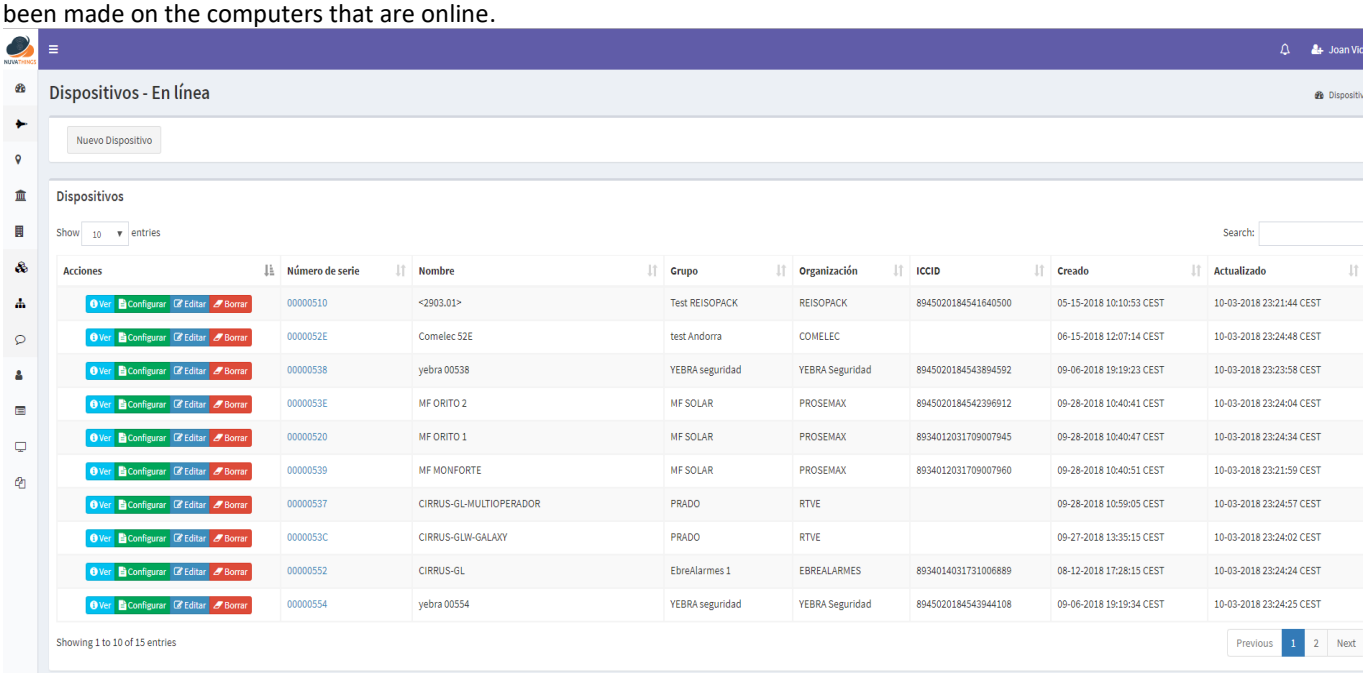
Finally, the view has a queue of the latest events received by the existing devices in the view. If we are in view mode within a group or the user only has visibility of a specific group, the list shows the input of signals in real time.
For an end-user level, the view changes the event input to a list of user notifications.



Said list of notifications is accessible for any level of user in the upper right part of the screen where the user's PROFILE, notifications and LogOut can be accessed.

Devices

The devices screen shows a list of available devices for the login level of the user operating on the platform. We can get to this screen from the menu or by clicking on the upper boxes of the Dashboard screen, in the case of the image, a filter has been made on the computers that are online.



The list has a search field that looks for matches in any of the list columns, so if we insert the name of the client or group, we will quickly reduce the number of selected devices

New device creates a team from 0, anyway the teams automatically when signaling to the platform generate a team by default visible from the administrator user level.

Edit device – Edits the data of the devices
View Status – Enters display and control screen
Config – Enables to configure internal devices settings.
Delete – Deletes device from user's company.

Register new device

When a device is purchased, it will not appear in the list of registered devices, so it is necessary to use the "New device" button.

The Edit screen will appear, the first thing we must do is enter the 8 digits of the serial number in the SN box.

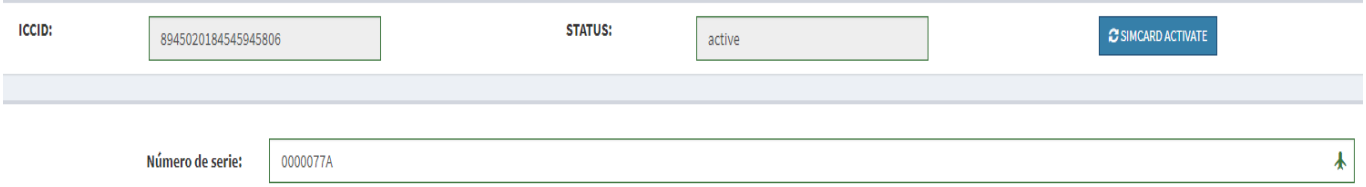


Once the serial number has been entered, the box will light up green indicating that the serial exists, then we proceed to enter the equipment data, until the update button, at that moment it will ask us for the VC code, which is on the label of the equipment to verify that the equipment is ours.

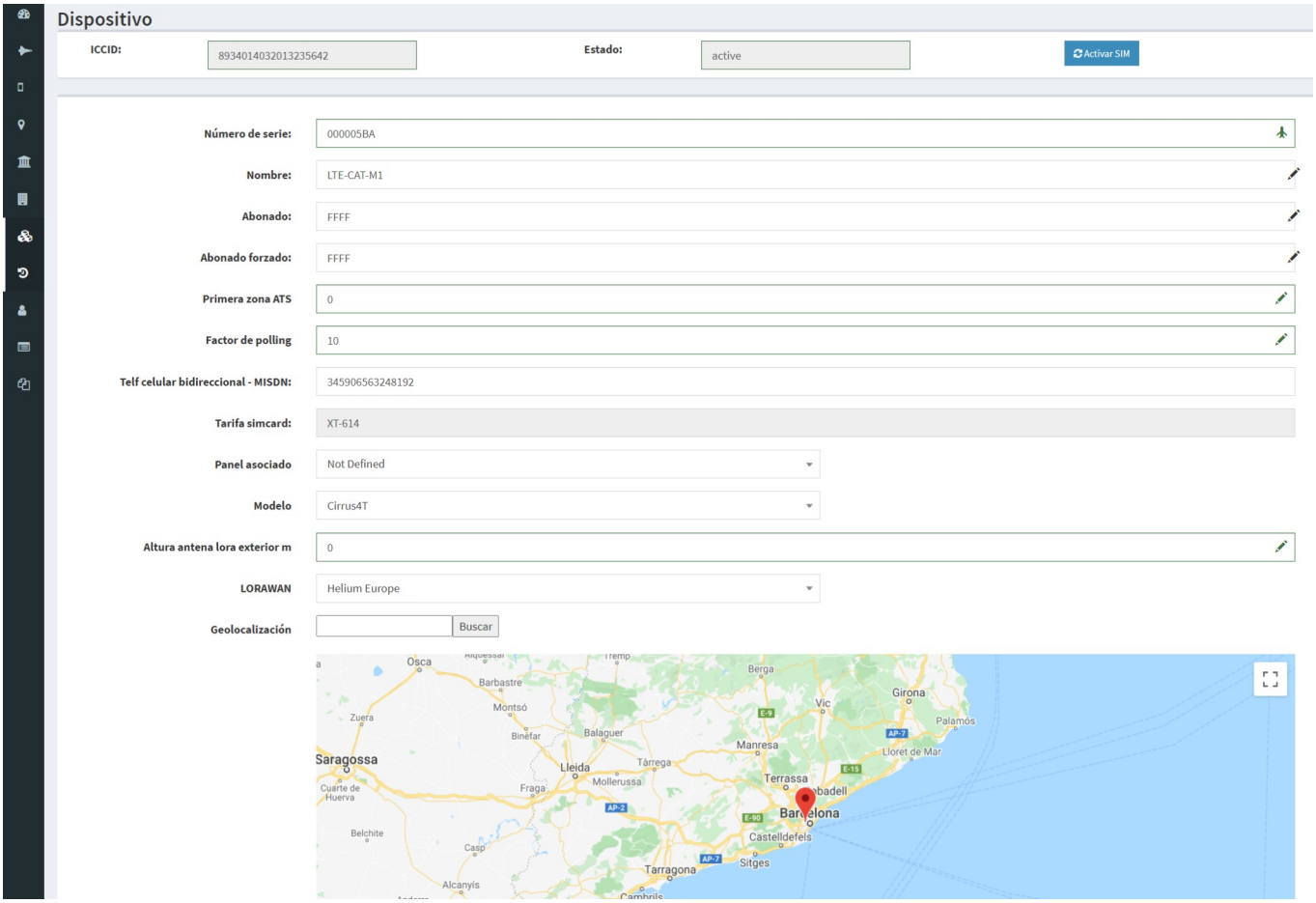
If an invalid code is entered, the system will indicate "VC code doesn't match", if we enter it correctly, the equipment will be registered in our company while entering the edition for the second time, we will be able to activate the SIM associated with the equipment.

Device Edit

Once the equipment is registered, the upper part of the editing window shows us the SIMCARD and its status, if it is inactive we can activate it



On this screen we can enter the basic data of the device, as well as assign company, group, and locate the position of the installation.

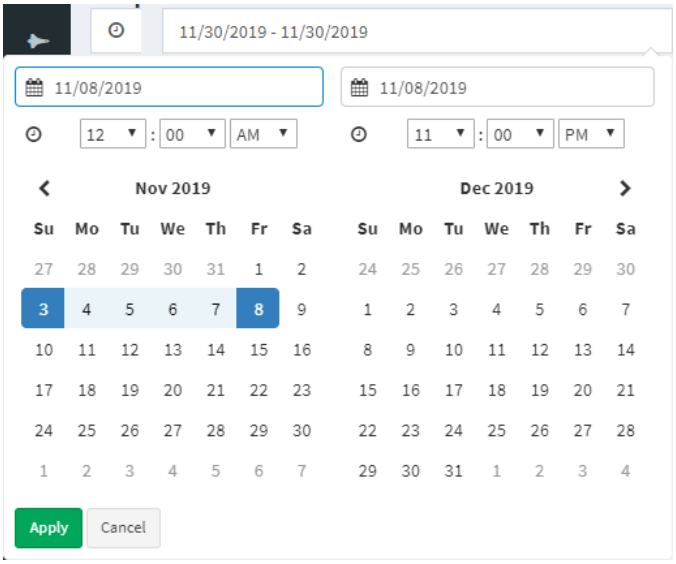


In the LORAWAN box we are allowed to select the LORAWAN network that offers us the best coverage in the area, being the options The Things Network, Helium or Everynet.

In the Geolocation box we can enter the address and/or company name and a geocode search will be generated, by which the icon will be automatically located on the map.

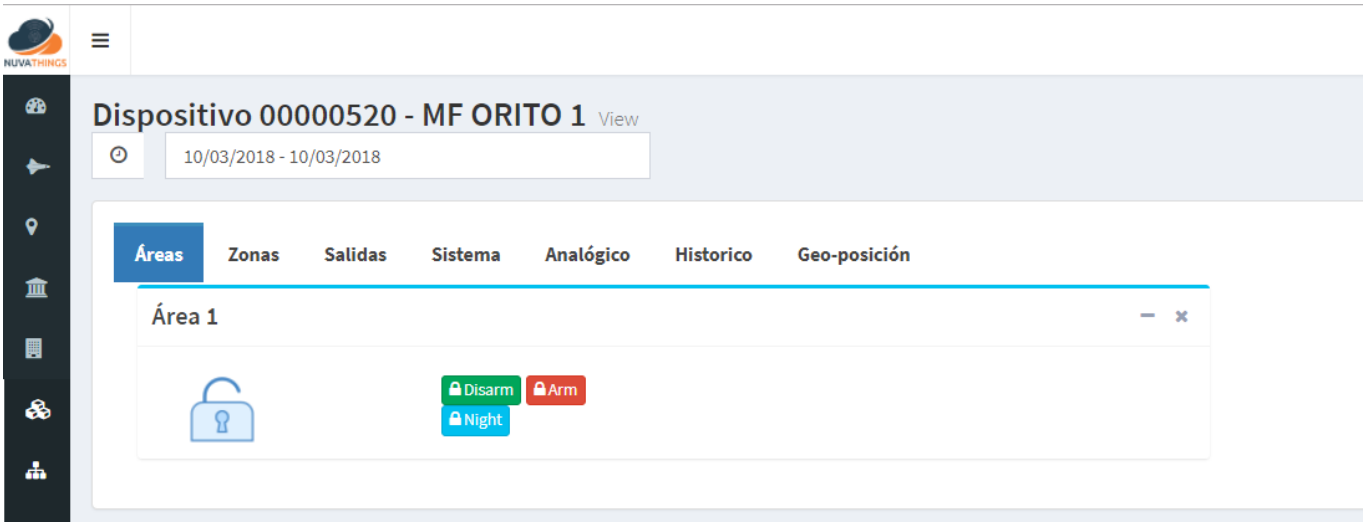
View / Control device

This screen allows you to view the status of the device as well as control partition arming/disarming, enable/disable outputs and omit/restore zones.
Depending on the application of the device, said screen may have a different format.
When entering the screen we will have a view with TABS, however in the upper part of these tabs, there is a calendar selector that allows us to select dates and view the analog data, history and device positions on the selected dates.

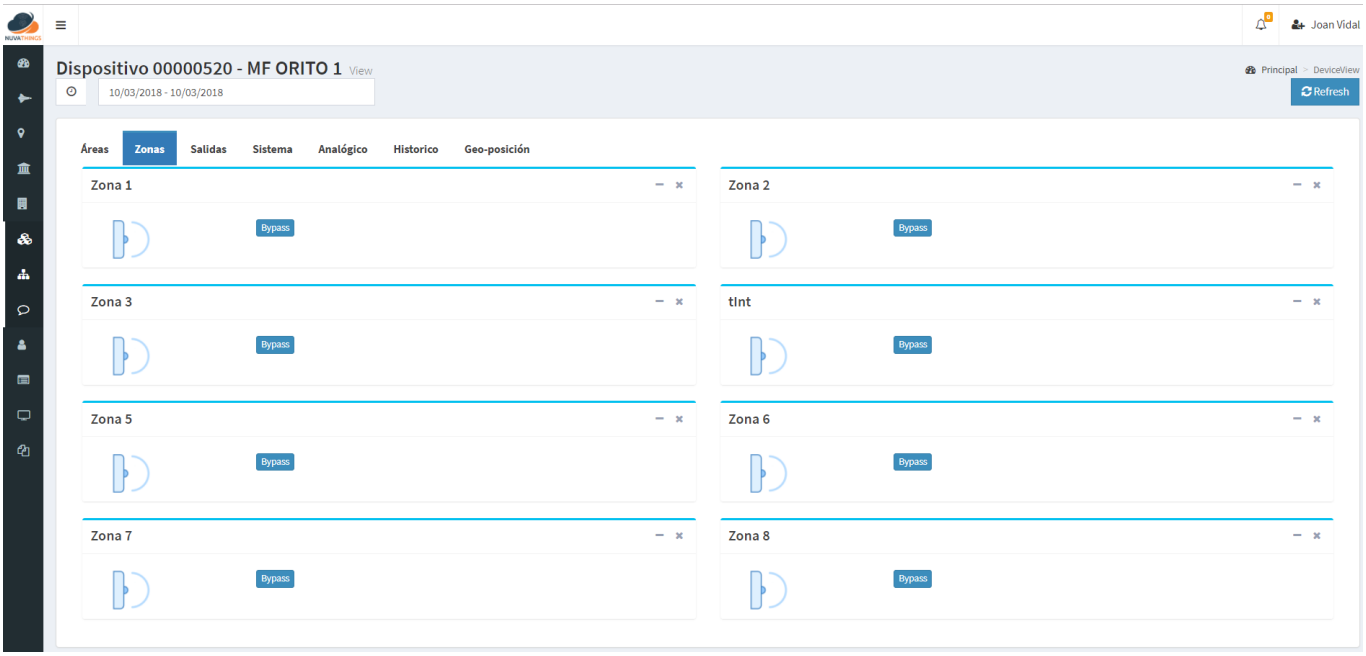


Once the date range of interest has been selected, press the green “Apply” button and finally the “Update” button located at the top right of the view.

Partitions

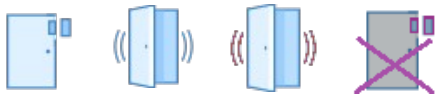


Inputs



It is important to note that the channel icon depends on the name configured for the channel.

By default the icon is that of a PIR, if the name of the channel contains "CN", if it will display a magnetic contact:



If the channel name contains “SMK”, “FIRE” or “GAS”



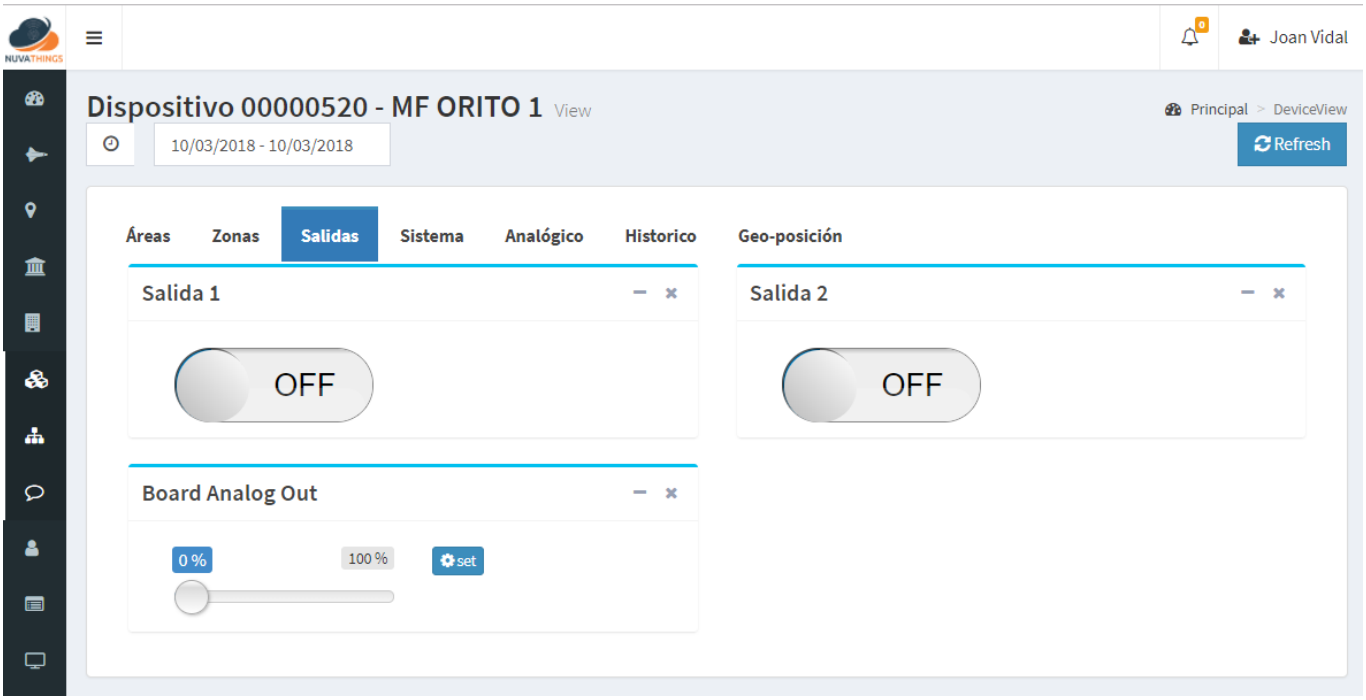
If the channel name contains “TEMP”



If the channel name contains “HYGRO”

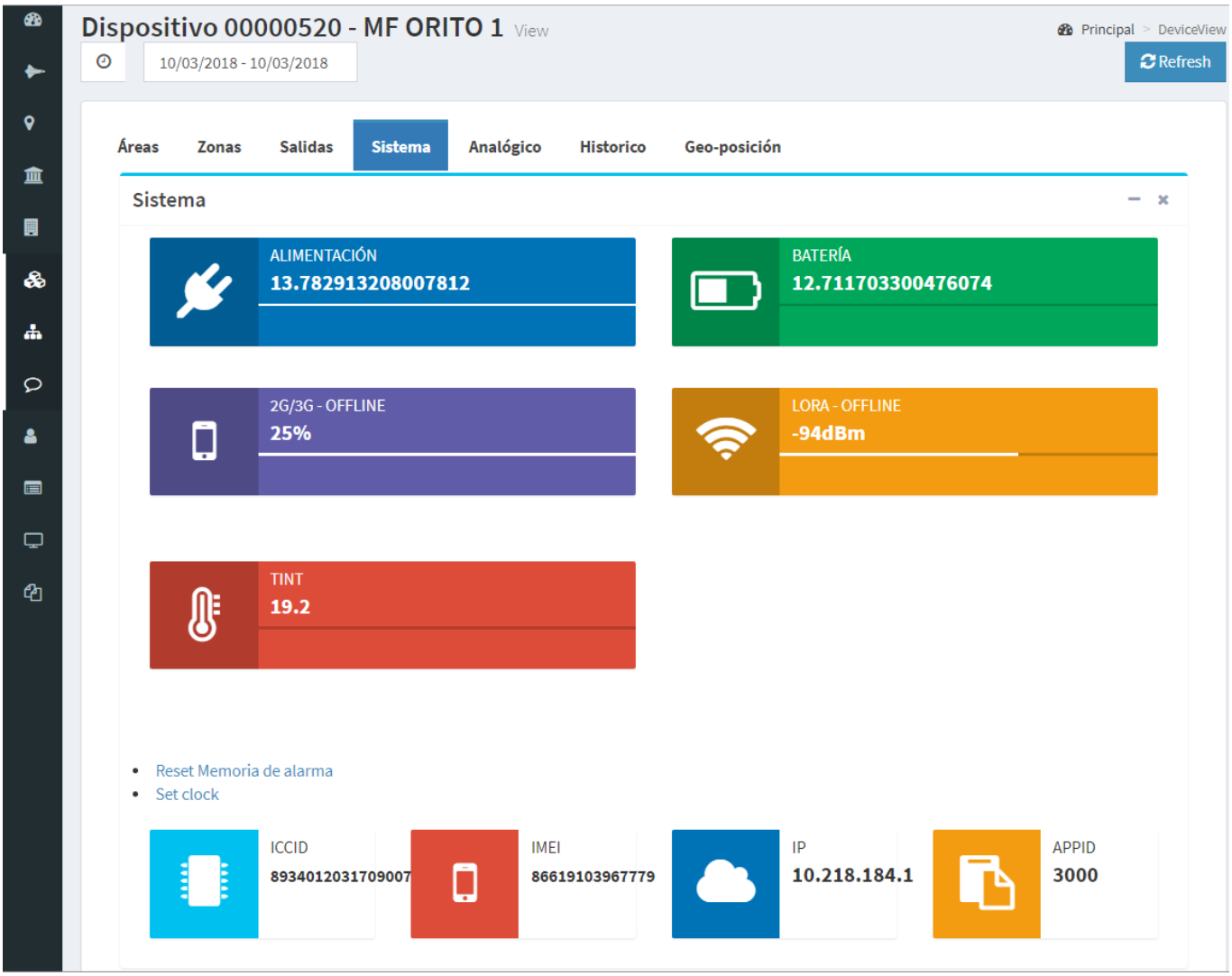


Outputs



By pressing the ON-OFF button in its positions we can control the device's outputs, if the device has a 0-10V output we can also dim its value.

Synoptic



Analog

The screen allows viewing and exporting the data of the analog measurements of sensors connected to the equipment, the name of the sensor is the one that has been given in the device configuration.

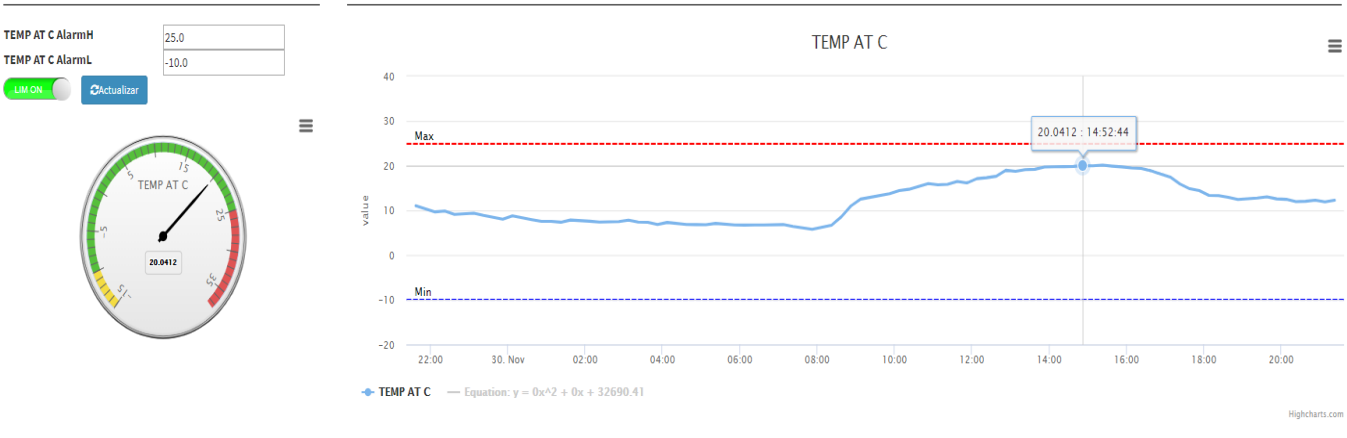


On the left side of each variable we have two data entries in which we can set the alarm limits for high level and low level, once said data has been entered, with the Update button, the changes will be saved on the server at Once they are sent to the device, the equipment upon receiving them will generate a programming change event.

For equipment powered by batteries, said change will be made in all safety in the following communication of the same.

The alarms will be processed in the device, so that when in low consumption mode a device detects a condition above/below the set limits, it will wake up and send an alarm event for high/low level, respectively.

With the LIM ON-OFF button, the alarm limits can be displayed on the graph.

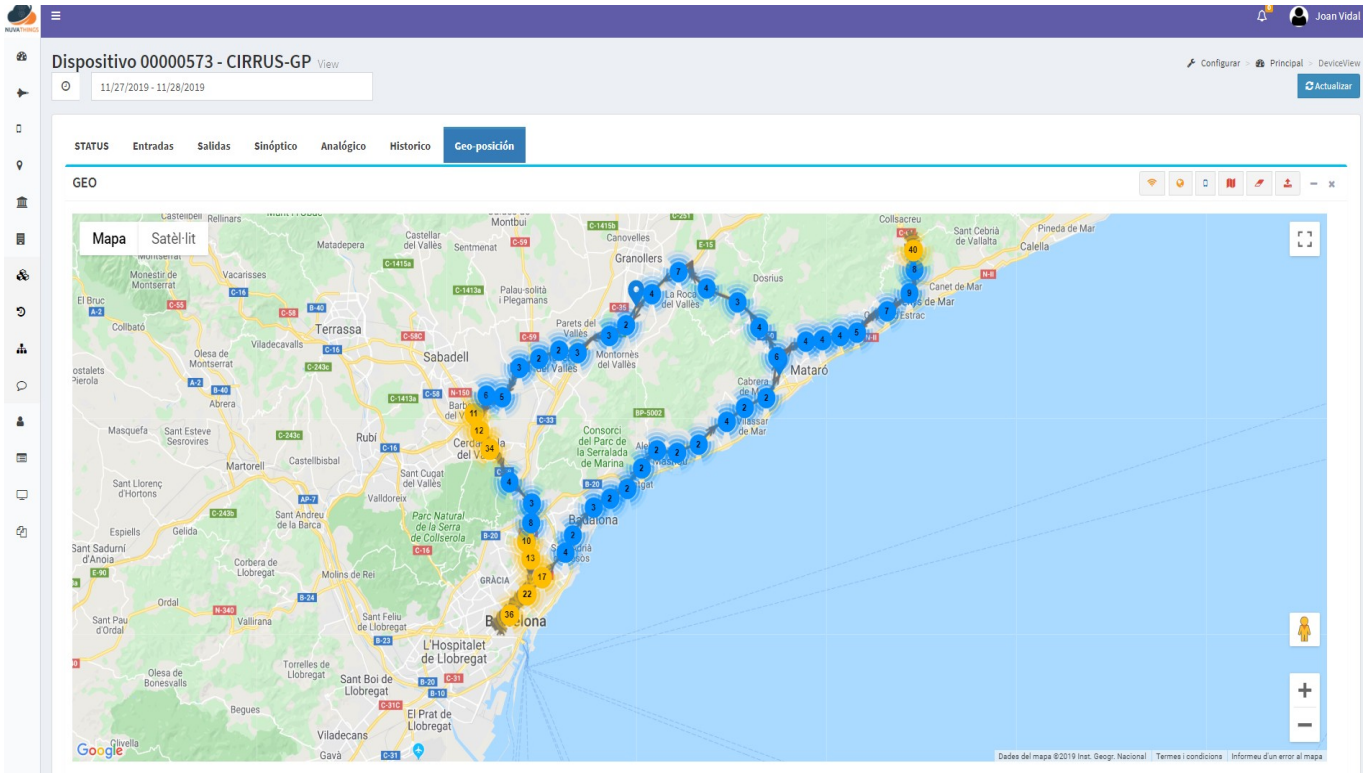


At the top right of each chart is the chart export menu.

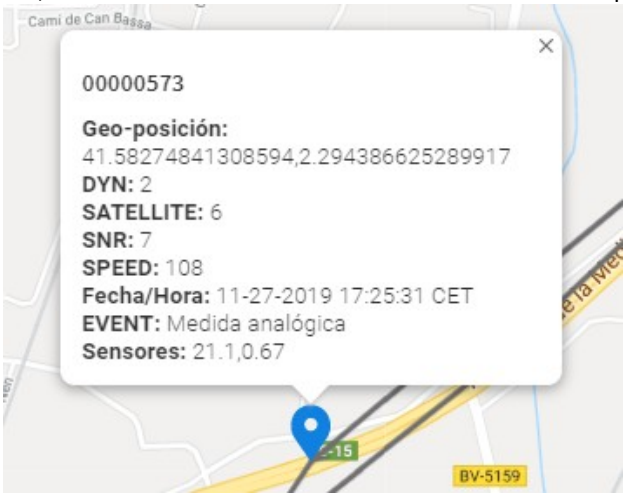
Geo-location

The geolocation tab has several selectable icons at the top right of the map.

Display of the history of positions for mobile equipment / GPS. (default)



When clicking on one of the positions, it shows us an infowin with the relevant data of the position

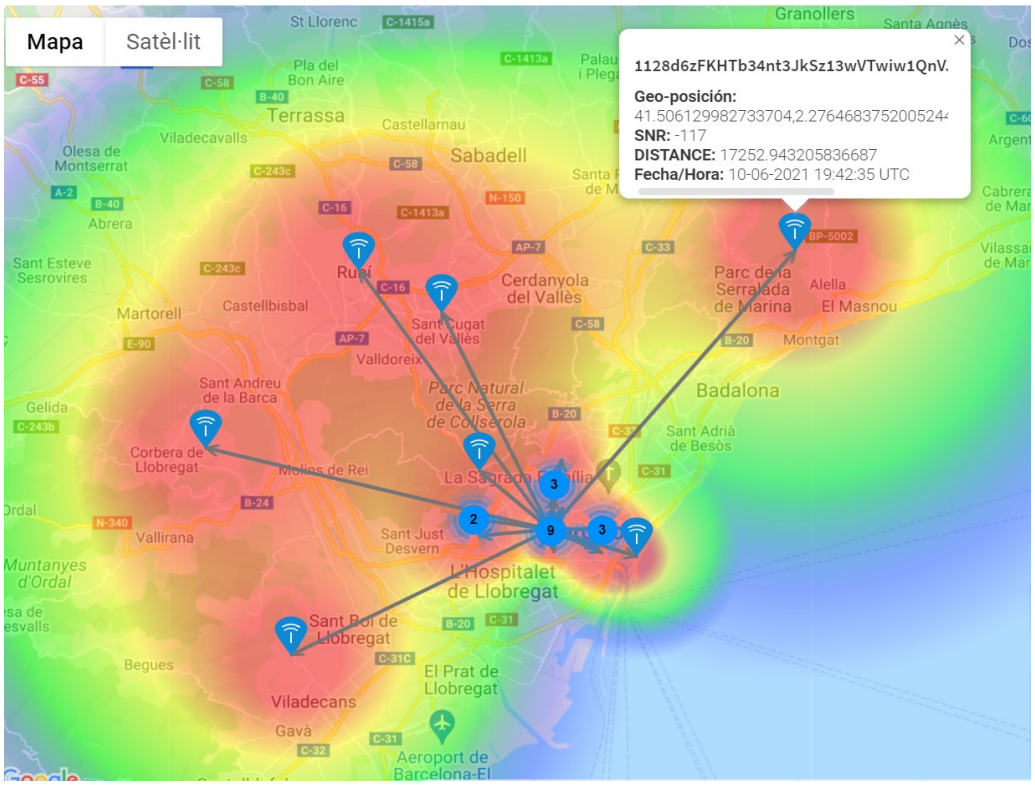


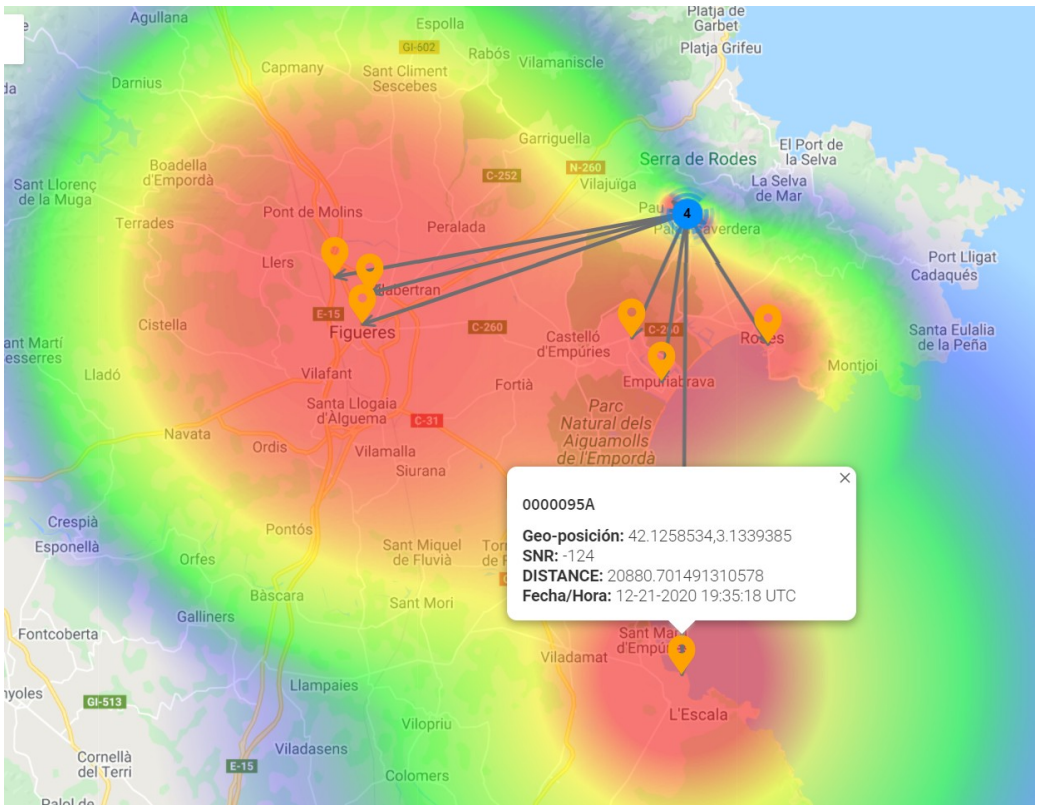
DYN: Dynamic state: 0 = stop, 2 = movement
SNR : GPS Signal to noise ratio
SATELLITE : Satellites used for the fix
SPEED: Speed in km/h
EVENT: Associated signal event
Sensors: Value of device sensors at that fix

The upper right part of the map contains an array of buttons that allow us to perform the following functions:

Visualization of LORA communication links

The screen shows us, for each device, that other devices are offering a support point for forwarding signals through the LORA network.
By clicking on one of the markers, it will give us the information on the distance in meters and the signal level of the links.
Indicate that the Orange pins correspond to Nuva equipment and the Blue pins correspond to LORAWAN gateways.





Geolocation by GSM cells

This option sends an order to the equipment so that it locates itself through cellular cells, the function may take a few moments to execute.

Creation of geo-fences

This button enables the creation of geofences, clicking the button enables three corresponding icons for the 3 geofences that can be configured for each device.



By clicking on the circle, the creation of a geofence is enabled, if it already existed the new one would replace the existing one.



By clicking on a position on the map and holding down the left mouse button we will create a circle that will delimit the geofence,



Once created, we press the "hand" button on the equipment and then we click the geofence creation button again to exit the creation mode. From this moment on, the geofence will be on the map and we can select it and modify its position / radio at any time.

Delete geo-fence.

Once out of the geofence creation mode, having a geofence selected, we can delete it by pressing this button

Send geo-fences to the team

Once the geo-fences have been created/edited, pressing this button will save the geo-fences on the server at the same time as they will be sent to the device. When the device receives them, it will generate a programming change event.

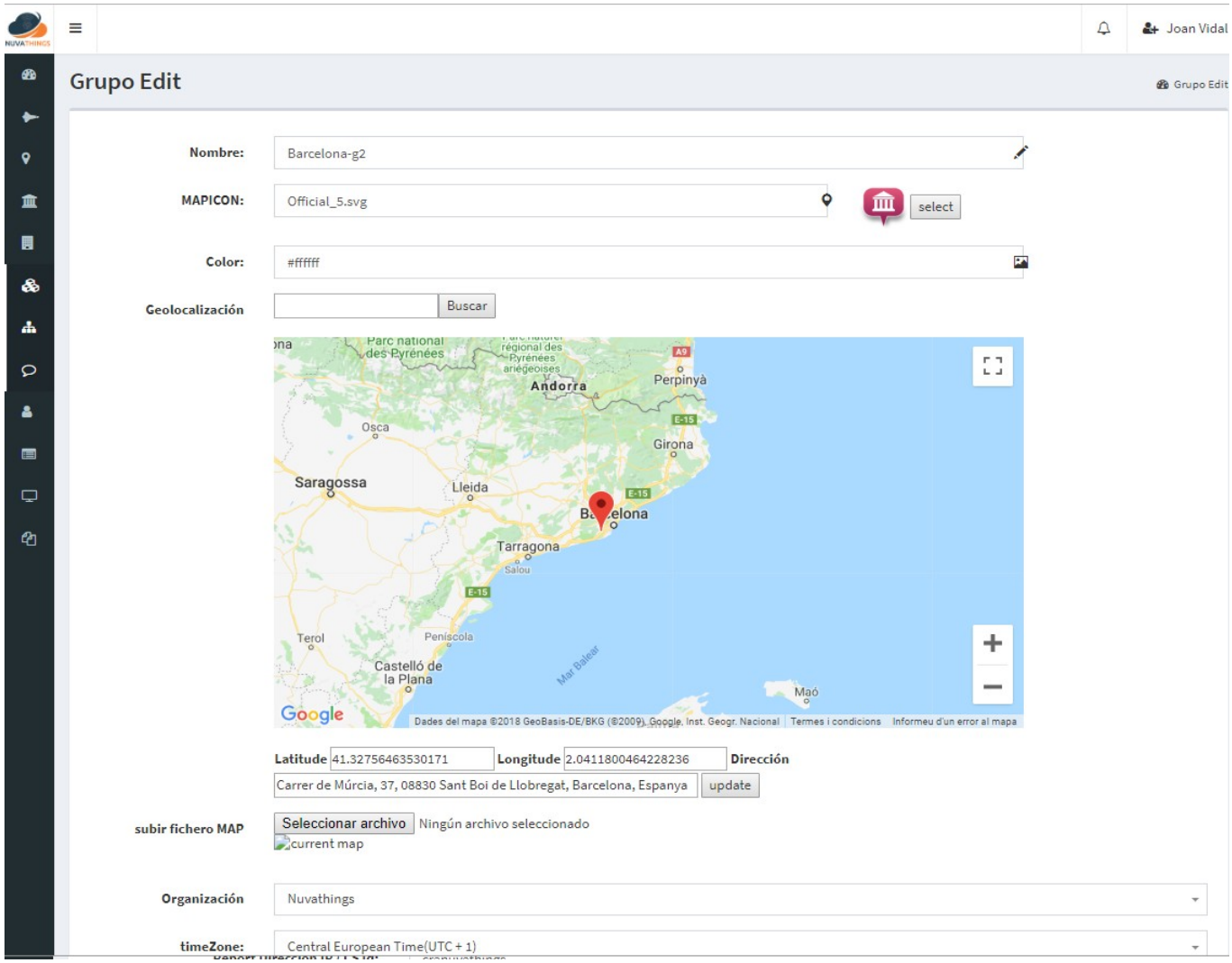
For equipment powered by batteries, said change will be made in all safety in the next transmission of the same.

The geofences will be processed on the device, so when in low power mode a device detects a geofence entry/exit, it will wake up and send a geofence entry/exit event.

Groups

The groups constitute logical groupings of equipment and users, the groups could be related to a certain type of installation, either to a sub-contractor, or to a delegation of an installer that connects its equipment in a ARC.

The groups panel allows you to manage existing groups as well as create new ones.
Within the group editing panel, we can assign a name to the group and assign the color of the group to be displayed on the dashboard map.



In the lower part, there are the connection options with other systems, such as a CRA, for this it is necessary to enter the craId (check with the CRA) and then select the NuvaCS-sever protocol.

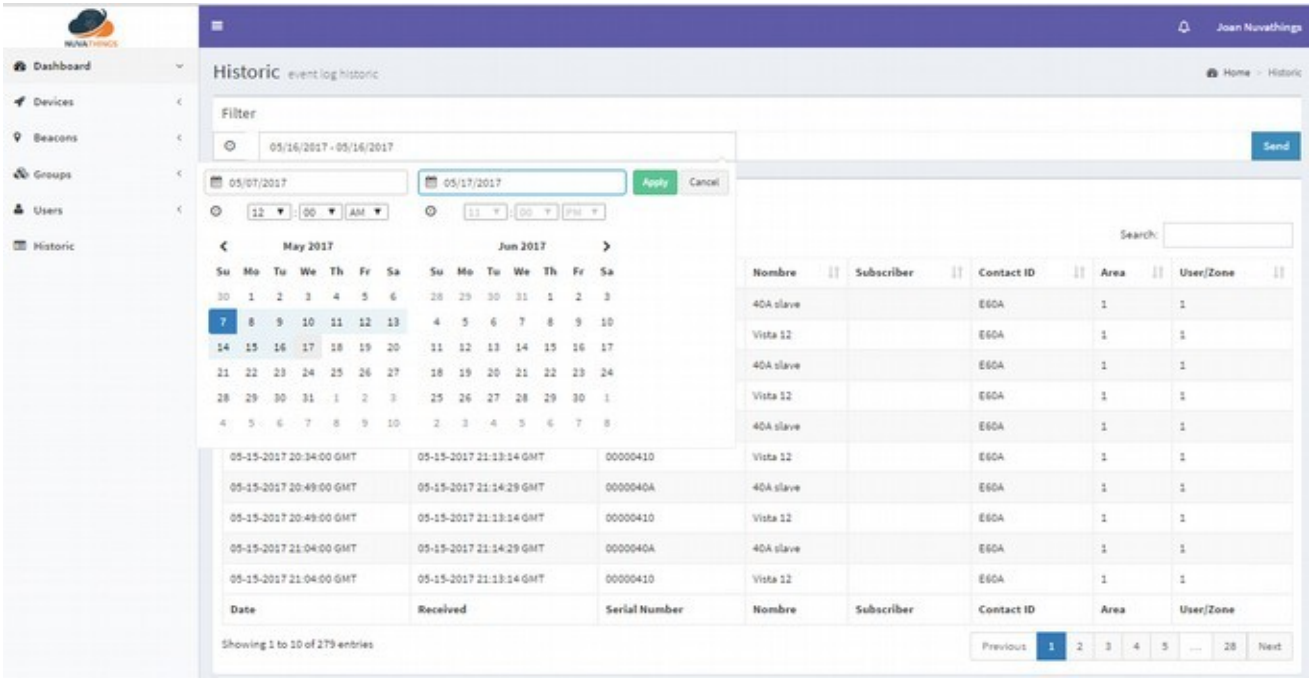


Once a group has been created, we must edit and assign the devices and users that will be linked to it.

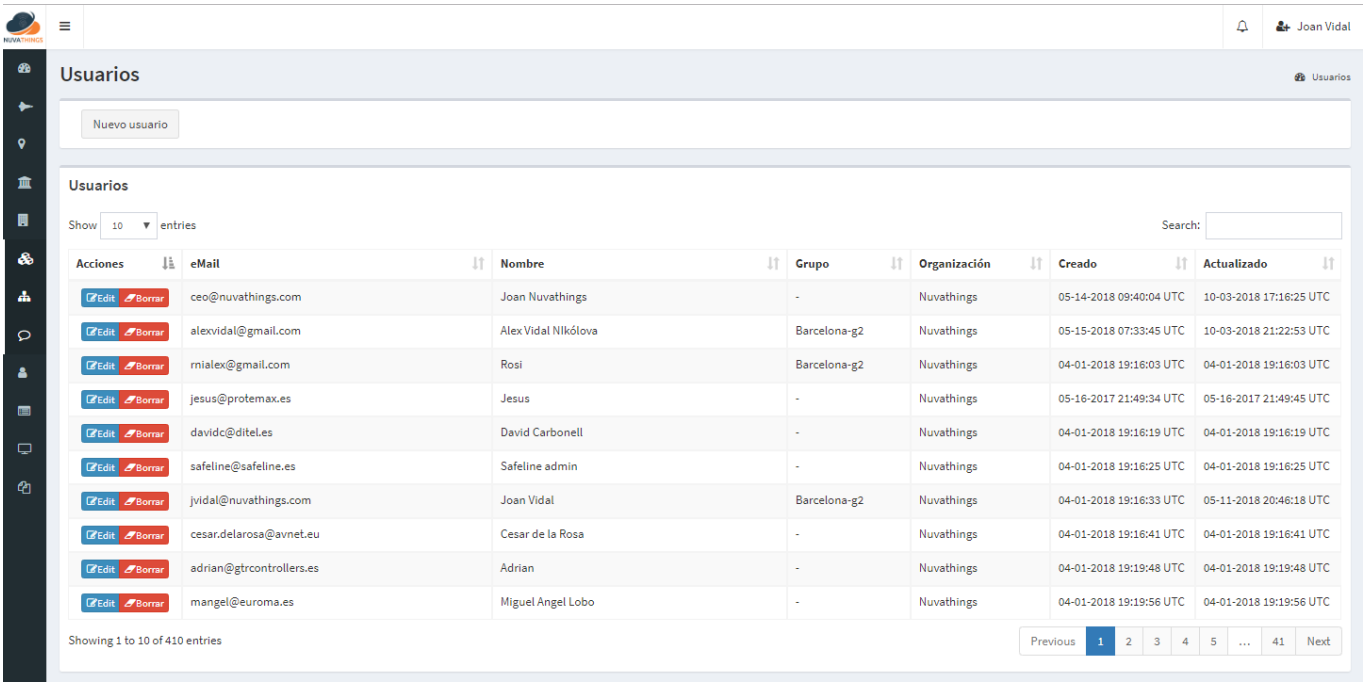
Historic

The history window allows temporary search in the event database,
- Filter by days, once a time range has been selected, it is necessary to press send to apply the filter.

On the downloaded data, the search box allows an intelligent search on any of the columns of the table.



Users



The user panel shows all the users that are under the visibility of the user who entered the platform, the panel allows you to search, edit, create and delete users from different companies in the case of a "super user" or from different groups to the users Company administrators

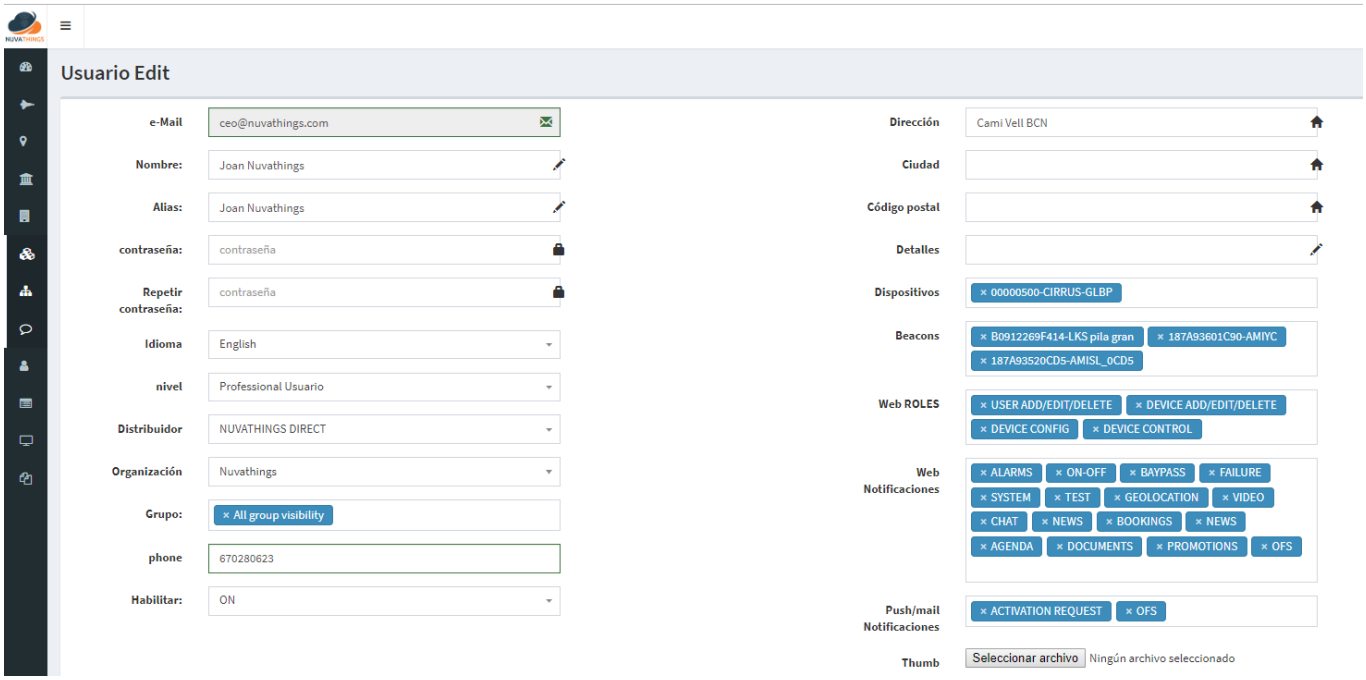
User edit

Editing a user is the most important process in the system setup, since this operation assigns the user to the following entities and concepts.
- Assign user data, such as name, alias, telephone, only the e-mail and password are required, the rest of the parameters can be ignored.
- Assign Privilege Level: End User, Installer, Administrator, or Distributor.
- Assign company or visibility over all companies (from distribution level or higher)
- Assign group or visibility over all groups. (from administrator level)
- Assign devices you own.
- Assign beacons / trackers of your property.
- Assign the roles, (set of operations allowed on the platform or APP)
- Assign the types of notifications to receive via mail, push or on the platform.

These last two functions are aimed at offering end users the option of being able to control devices from the web or from an APP, while also allowing panels to be assigned to installers or system administrators, who are owned by them.
Android and IOS applications use such user-to-device mapping to provide installation control functionality.

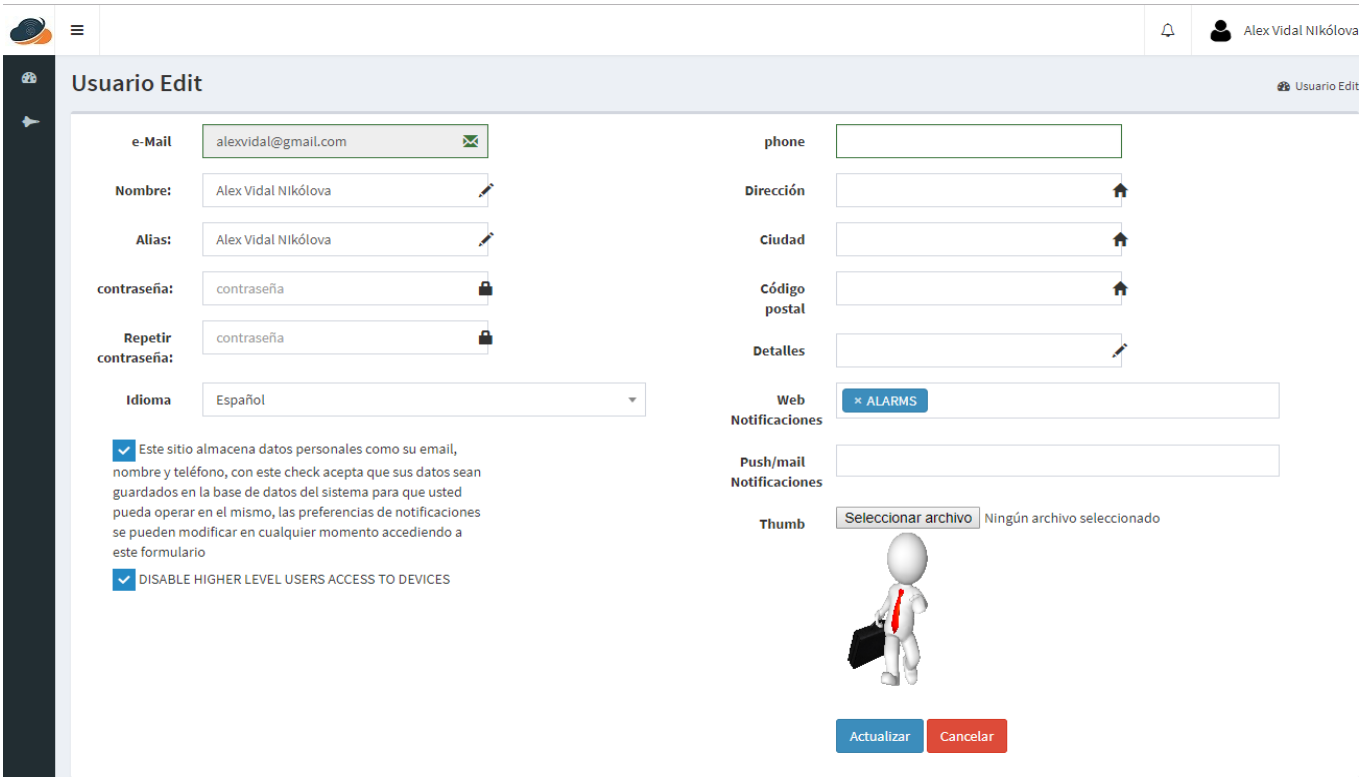
Password/Repeat Password – Allows you to change a user's password. It is important to use at least one capital letter and some numbers to create a strong password..
Level – Assign user access level from: Final User, Installer User, Admin User and Super-user
Company – Only in the view of a super user, it allows assigning a company to the user or having visibility over all the companies.
Group – Only in the view of a super user or an administrator, it allows assigning a group to a user or visibility over all the groups that comprise a company.

Editing of another user by the administrator.



User edition from "My Profile"

The display of said screen for a base or group level user varies as shown, it is important that the user must give their explicit consent for their data to be saved on the server in compliance with the GDPR regulations.

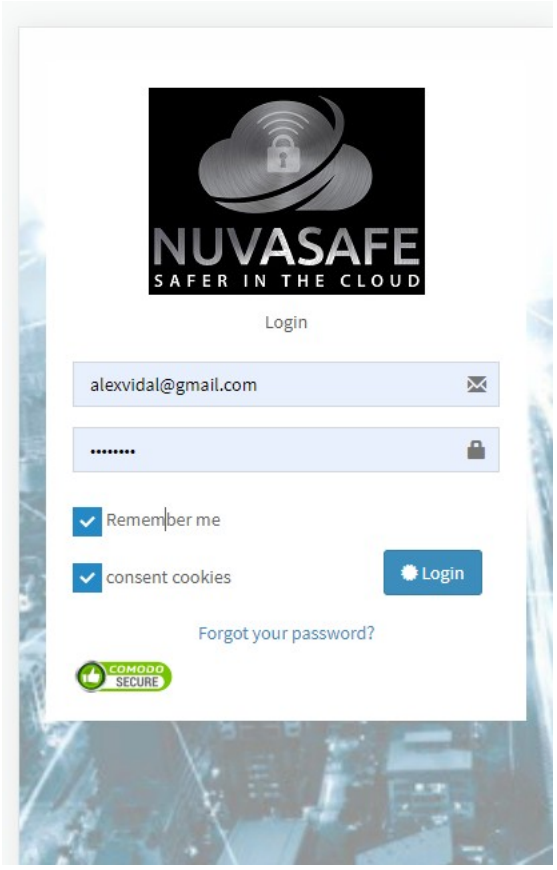


Also in this same profile screen you can modify the notifications and communications of the system, by virtue of compliance with the GDPR.

There is a tab, to disable the access of higher level users to your equipment, in case the technical service requires access to your device, you must contact you.

Activate the NuvApp application for end user.

Once a “final user” level user has been created, we will be able to make it install the webApp on its terminal.
In the first place, it is necessary for that user to have visibility over a device or several devices that they own, the process is a little different if it is an Android or IOS terminal.



Android

Enter from chrome : https://cloud.nuvasafe.com
enter username / password of the end user created, important to accept cookies!

When the dashboard is loaded, it will ask us if we want to install NuvApp.
We say yes and an icon will be created on the desktop.

iOS

Entrar en safari : https://cloud.nuvasafe.com
enter username / password of the end user created, important to accept cookies!
Loading the dashboard, go to options and hit "add to desktop"

