Manual – DynaGateway
Models: LTE, IoT and Ex

1. Introduction 2
2. Product description 2
  2.1 Product structure 2
  2.2 Models and features 4
3. Pre-installation 6
  3.1 Evaluation of internet availability 6
  3.2 Positioning recommendations 6
    3.2.1 Strategic positioning 7
    3.2.2 Environmental assessment 7
    3.2.3 Connectivity test 7
  3.3 Network access release 7
4. Installation 7
  4.1 Power supply 8
  4.2 Configuration 9
    4.2.1 Mobile network 13
    4.2.2 Ethernet 14
    4.2.3 Wi-Fi 15
  4.3 LED indication 17
  4.4 Mounting 18
5. Adoption and setup 21
  Figure: Gateways Dashboard 22
  5.1 Adopting a DynaGateway 22
  5.2 Batch Spot Configuration 25
    5.2.1 DynaGateway configuration practical example 27
  5.3 Individual spot configuration 29
6. Status 29
  6.1 Connecting to Spots 30
  6.2 Visibility update 30
7. Additional resources 31
  7.1 Connectivity 31
    7.1.1 Network interface 31

7.1.1.1 Wifi 31
7.1.1.2 Ethernet 31
7.1.1.3 Mobile 31
7.1.2 LAN Configuration 32
7.1.3 NTP 32
7.2 System reboot 32
7.3 Restore factory setting defaults 33
7.3.1 Restoring the configuration via Gateway Setup 33
7.3.2 Restoring configuration via external button 33
7.3.3 Default factory configurations 33
7.4 Firmware update 34
7.5 Search for sensors within Bluetooth range 35
7.6 Mesh network 36
7.6.1 Configuring the mesh network for root mode 36
7.6.2 Configuring the mesh network for node mode 37

1. Introduction

This document addresses the configuration, usage, and operation processes of the DynaGateway (LTE, IoT, and Ex models), the automatic data collector for DynaLoggers for monitoring the health of industrial assets.

The main objective of the DynaGateway is to interact with the DynaLoggers located within its Bluetooth range, collecting vibration and temperature data, and requesting waveform analysis at the specified interval. This information is sent to the DynaPredict Web Platform, where the data can be viewed graphically.

In this sense, it is necessary for the DynaGateway to have access to the internet. Connectivity can be established through a Wi-Fi network, an Ethernet cable, or a mobile data network.

The following chapters provide recommendations for installing the product, a step-by-step configuration, and its key features. It is essential that the information presented in this document is followed for the solution to work properly.

2. Product Description

DynaGateway works with the purpose of making vibration and temperature sensor data available on the DynaPredict Web Platform in an automated way, generating a history of measurements that enable future analyses.

2.1 Product Structure

The main product-user interaction interfaces are located on the inside front of the DynaGateway. These interfaces will be used in the installation and configuration processes:

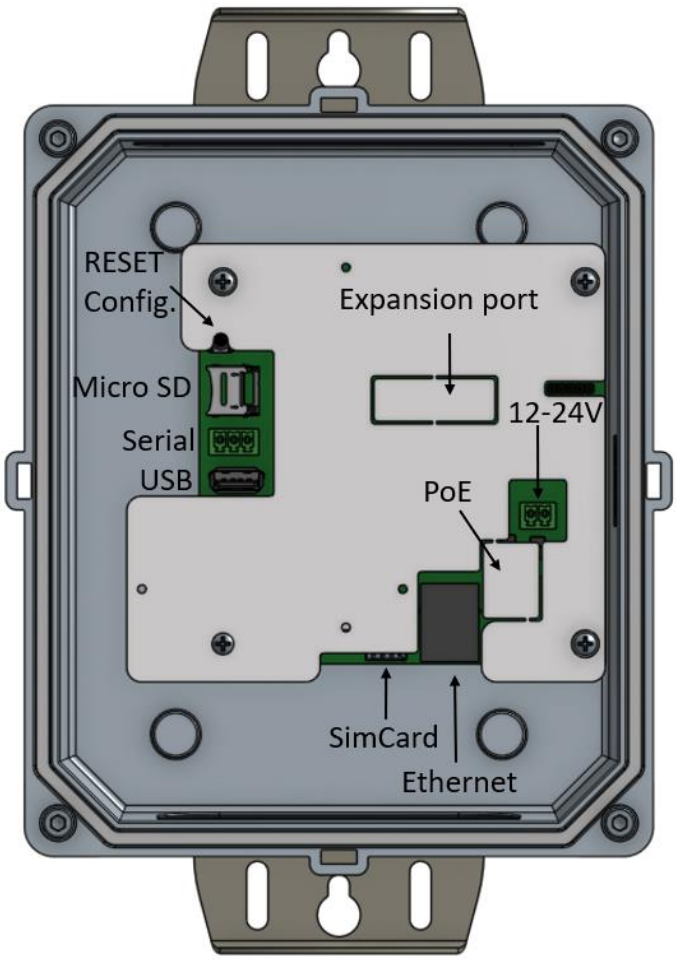


Figure: Physical Product-User Interaction Interfaces

1. Power Input - DC Voltage:

Connection port for power supply at 12/24Vdc

2. Reset Config Button:

Causes the Gateway to generate an Access Point (AP), allowing the user to access a DynaGateway settings interface, and provides reset functionality.

3. USB gate:

Enables the use of an external device to save Gateway logs (Dynamox Support exclusive use).

4. SD Card:

Local storage of offline collection data for later submission to the Web Platform.

5. Ethernet:

RJ45 port for connecting the device to the internet, via Ethernet cable.

6. Nano Sim Card:

SIM card insertion for connection to mobile networks.

7. Expansion port:

Provides GPIO pins for connection to external devices.

8. SERIAL:

Port for connecting the communication bar compatible with the ISO11898-1 standard.

9. PoE:

Connection Port of the external module to use the active mode.

The DynaGateway also offers an indication of the operating status through three LEDs positioned on the side of the product. They indicate *power*, *status,* and *network* indication, which respectively concern power supply, internal status, and connectivity. The functionalities of each LEDs and their respective colors are detailed in section 4.3 of this document.

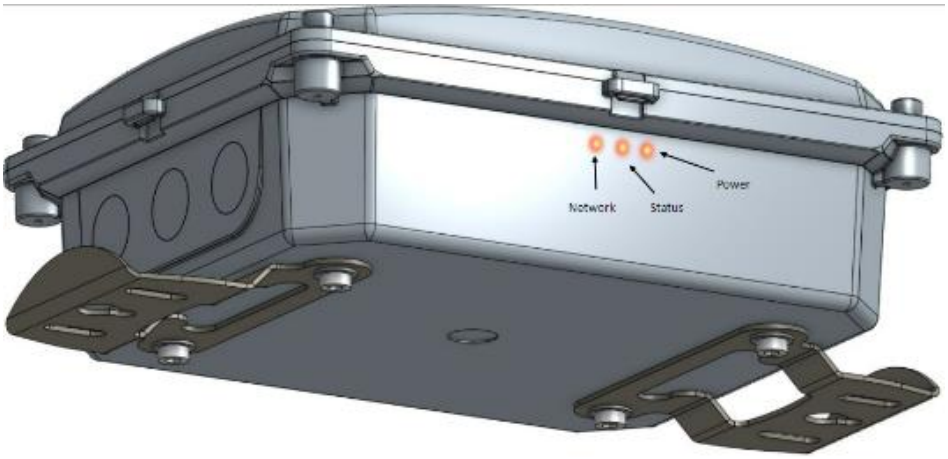


Figure: Product connectivity LEDs

2.2 Models and features

In the central part of the device cover, there is information about the name, model, serial number, PIN, and MAC address of the DynaGateway. This product offers three different models: the DynaGateway LTE, the DynaGateway IoT, and the DynaGateway Ex.

Figure: Product Series Information

These IDs are described below:

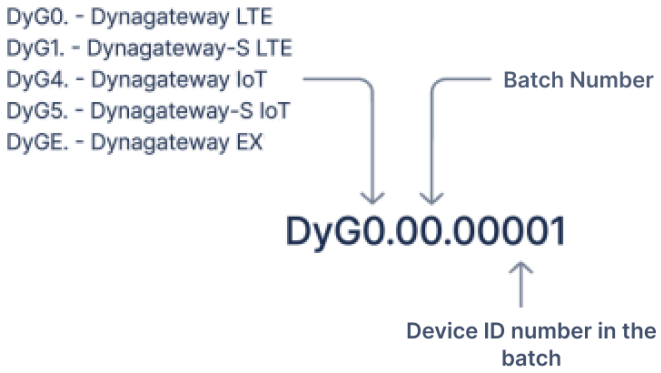
- Part Number (PN): Identification code of the product model
- DyG: Serial number of the DynaGateway. It is used in connection with the DynaPredict Web Platform
- PIN: Used for device adoption on the DynaPredict Web Platform
- MAC ETH: MAC address of the device on wired networks
- Wi-Fi MAC: MAC address of the device on Wi-Fi networks

The characteristics of the different models are presented in the following table.

Model	Serial Number	Ethernet	Wi-Fi + Bluetooth (2.4Ghz)	Mobile Networks					EX (Anti-explosive cases)	Power Supply 110/220 ~12/24V
				2G GSM	3G E-UTRAN	4G				
						LTE CAT-1	LTE Nb-IoT	LTE CAT-M1		
DynaGateway LTE	0	✓	✓	✓	✓	✓				✓
DynaGateway-S LTE	1	✓	✓	✓	✓	✓				
DynaGateway IoT	4	✓	✓	✓			✓	✓		✓
DynaGateway-S IoT	5	✓	✓	✓			✓	✓		
DynaGateway EX	E	✓	✓	✓	✓	✓			✓	

Table 1: DynaGateways Models

The formatting of the DynaGateway ID number follows a construction pattern in the form DyGx.xx.xxxxx, where,



3. Pre-installation

The interaction between DynaGateway and the DynaPredict Web Platform depends on an internet connection. Information regarding data collection, requests for Waveform Analysis and parameterization of the DynaLoggers and the Gateway itself are included in this interaction.

In this context, to ensure that DynaGateway works well, before its installation, it is recommended to:

- Checking the availability of an internet connection at the installation site;
- Check the need for network traffic release.
- Plan the installation location of the Gateway in relation to the sensors. These processes are detailed individually below.

3.1 Assessing internet availability

Checking network availability is particularly critical when using Mobile Networks, as there may be unavailability of carrier, technology and frequency, or the signal may simply not be strong enough to provide connectivity for the DynaGateway. It is worth noting that the DynaGateway can work with a SIM card from any operator and use GSM (2G) technology and either CAT-M1/NB-IoT (4G) or CAT-1 (4G). More information on network technologies is available in section 4.2.1. In addition, the product datasheet describes the frequencies supported by each model.

If the DynaGateway connects to a Private LTE network, either via Wi-Fi or Ethernet, it is necessary to ensure that it is allowed to connect to the local network and that the data it sends can travel outside the network. More details are given in section 3.3. In addition, it is recommended to check that the plant's Wi-Fi network has sufficient range and that the network point intended for the DynaGateway is functional in the wired infrastructure present at the installation site.

3.2 Recommendations for positioning

Proper positioning for the DynaGateway directly impacts the quality of its connection with the DynaLoggers. The maximum range for connecting to a DynaLogger, in open space and line of sight, is 200m.

3.2.1 Strategic positioning

It is recommended that the DynaGateway be installed at a level above the machinery in the plant, aiming to reduce potential communication barriers that could hinder Bluetooth connection. Installing the device at a central point in the plant may allow for optimal range utilization in all directions.

It is worth highlighting that installing the DynaGateway inside metal enclosures drastically reduces the range of Bluetooth communication.

3.2.2 Environmental Assessment

Before installation, carefully assess the environment in which the device will be used. Consider the presence of reflective objects, radio frequency interference and other factors that may affect line of sight and the quality of the connection.

3.2.3 Connectivity Test

To estimate the sensors within the range of the DynaGateway before field installation, it is recommended to use the DynaPredict application, available on the Play Store and App Store. In the side menu, the "Search Spots" option displays all sensors already registered in the platform in a Bluetooth visibility list on the phone screen. This can be used to estimate the feasibility of connection between the sensors and the Gateway.

After installation, perform connectivity tests with the Gateway itself to ensure that the line of sight is adequate and that there are no significant interferences. The test can be conducted using the functionality described in 7.5.

3.3 Network Access Release

When using a private LTE, Wi-Fi, or Ethernet network for communication, it is necessary to allow data traffic on the network for the following hostnames:

Domain	Port	Description
*.dynamox.solutions	443	Release of all Gateway interactions (optional)
dyg.Gateways.dynamox.solutions	443/8883	MQTTs/HTTPs communication for posting collections
time.google.com	123	Time synchronization via SNTP *Note: the address of the NTP server is configurable.

Dynamox is a company certified by the ISO 27001 standard, which relates to information protection and security. The certification ensures that Dynamox complies with the criteria established by the standard regarding information security in its processes.

For more information about network release, contact Dynamox Technical Support (support@dynamox.net).

4. Installation

After completing the Pre-Installation step, the next step is to connect the device to the power supply and the selected communication interface. This section presents the necessary instructions for this process.

It is recommended that the procedures described below be performed in a location where the product can be easily handled, as it is more convenient to configure its communication interface before positioning it in the chosen location for operation, aiming to ensure greater productivity and safety for the individuals responsible for the installation.

4.1 Power Supply

The DynaGateway can be powered through a DC source with an output between 12 and 24V. To do so, it is necessary to connect the power cables according to the following figure:

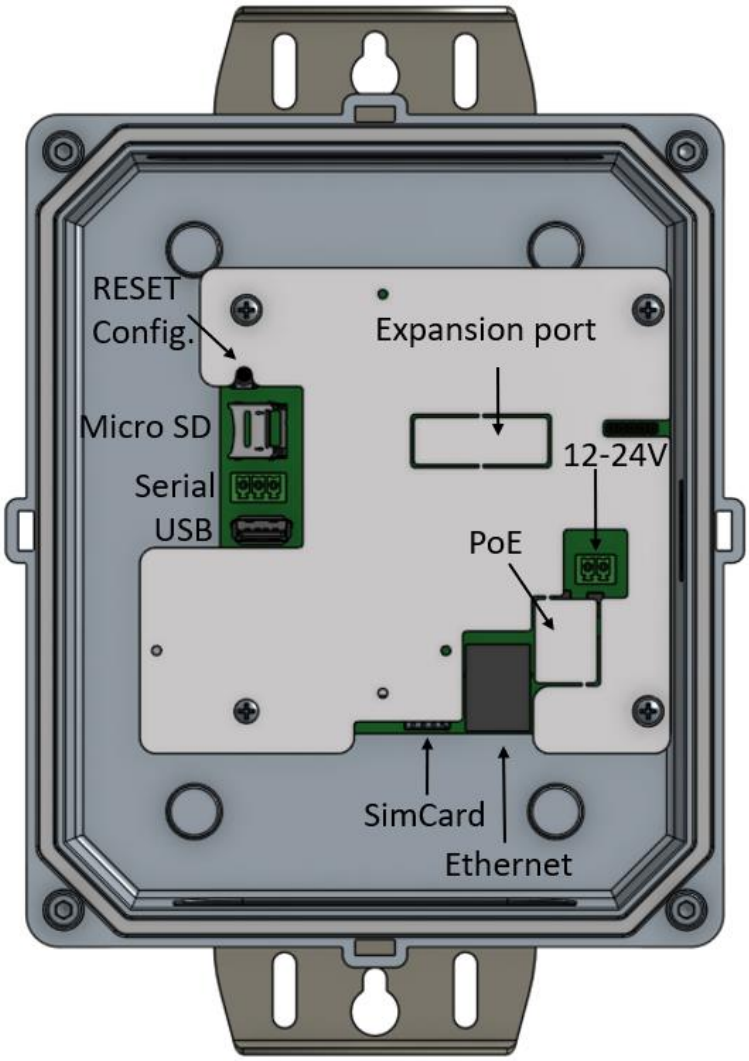


Figure: Connection of the power cables

Power terminals are in the internal compartment of the product, next to the physical interfaces (Nano SIM Card slot, RJ45 port, Reset/Config button, etc.). The image below shows the connection of the ethernet cable and power supply:

Figure: Ethernet Connection and power cables

4.2 Configuration

To configure the DynaGateway's communication interface with the Internet, you need to start the device's configuration mode by following these steps:

1. Press and hold the Reset/Config button for approximately 5 seconds, after which time the power LED will flash yellow. When you release the button, the LED will change to a steady yellow and a Wi-Fi network with the name of the DynaGateway's serial number will be generated.

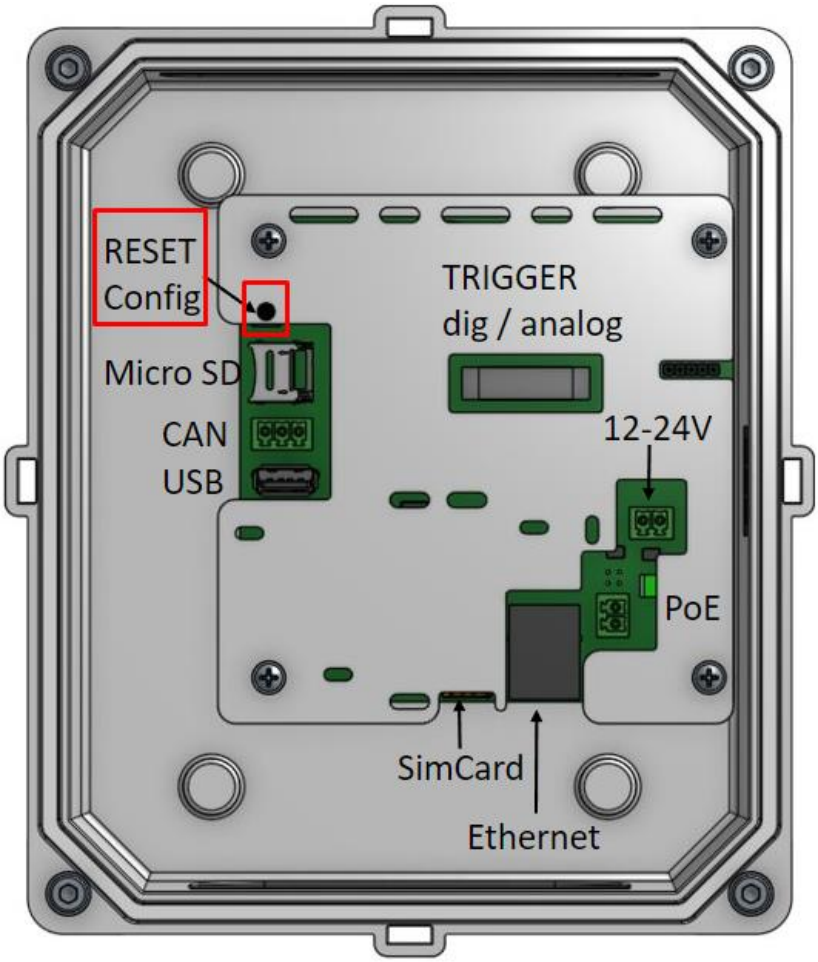


Figure: Reset/Config Button

2. Connect to the Wi-Fi network generated by the device using a computer or mobile device nearby. The network generated by the Gateway has the following credentials:

- SSID (name): Device serial number (printed on its casing) mentioned in chapter 2 - Product Description.
- Password: 12345678

Figure: Network access /Wi-Fi generated by DynaGateway

3. In a web browser, you should access the Gateway's configuration interface page using the URL: http://dynaGateway-setup.local/ or the IP address: 192.168.10.1. On this page, initially, you should log in using the following credentials:

- User: admin
- Password: admin

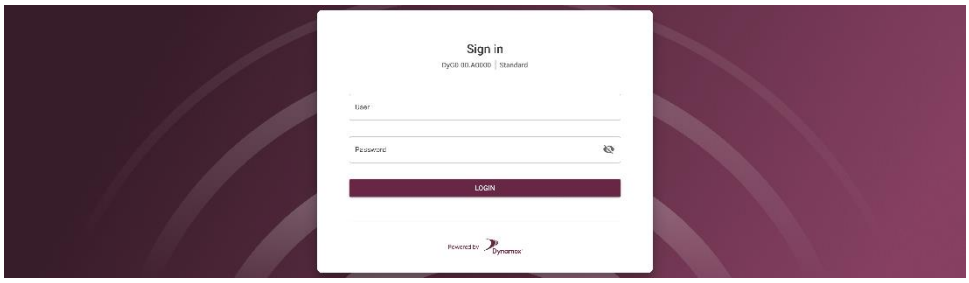


Figure: Authentication procedure

When logging in to the system, the user will have access to the *Quick Setup* tab. It can also be accessed through the side menu. The first step is optional and involves reading visibility from the Dynaloggers near the Gateway. If it is not necessary, you can select " ***No, skip to the next step***", otherwise "***Yes, let's scan the sensors***" option should be selected. Next, you must press the button NEXT.

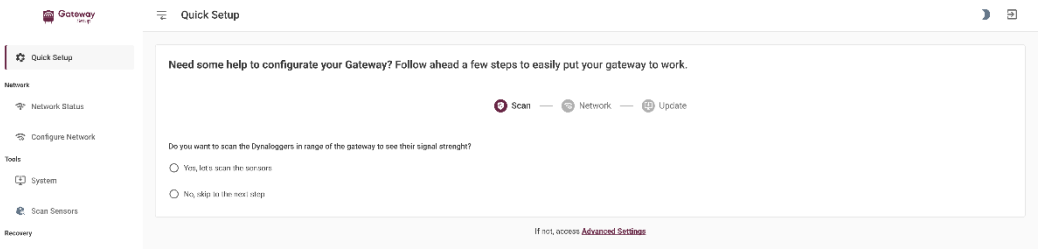


Figure: Quick Setup – Step to scan the Dynaloggers

If the option "***Yes, let's scan the sensors***" has been selected, the next screen will provide a list of the Dynaloggers that have been identified by the DynaGateway. This section is described in detail in section 7.5. To proceed to the next step, press the button NEXT.

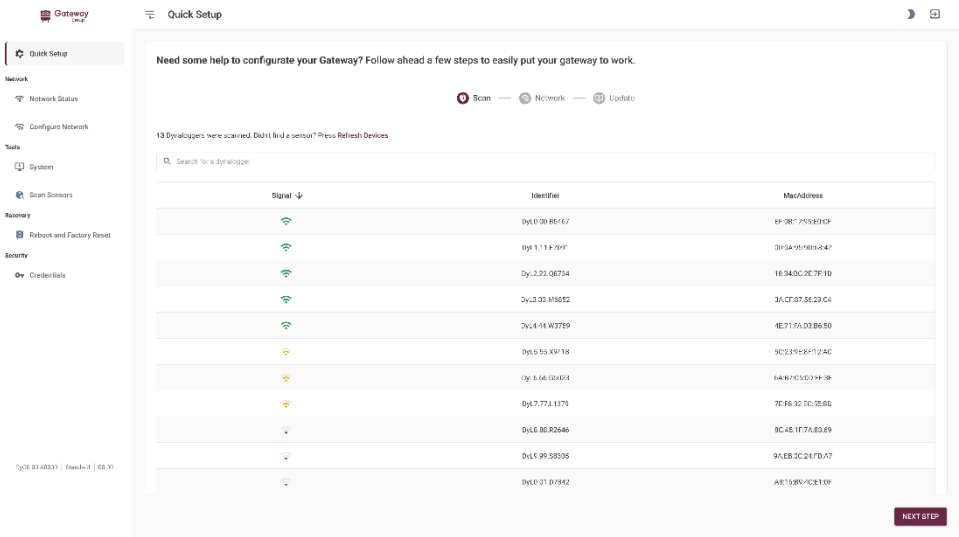


Figure: Quick Setup – Visualization step of the Dynaloggers visible to the DynaGateway

The second step in the Quick *Setup* is Network, to select the network interface on which the DynaGateway should connect to the internet.

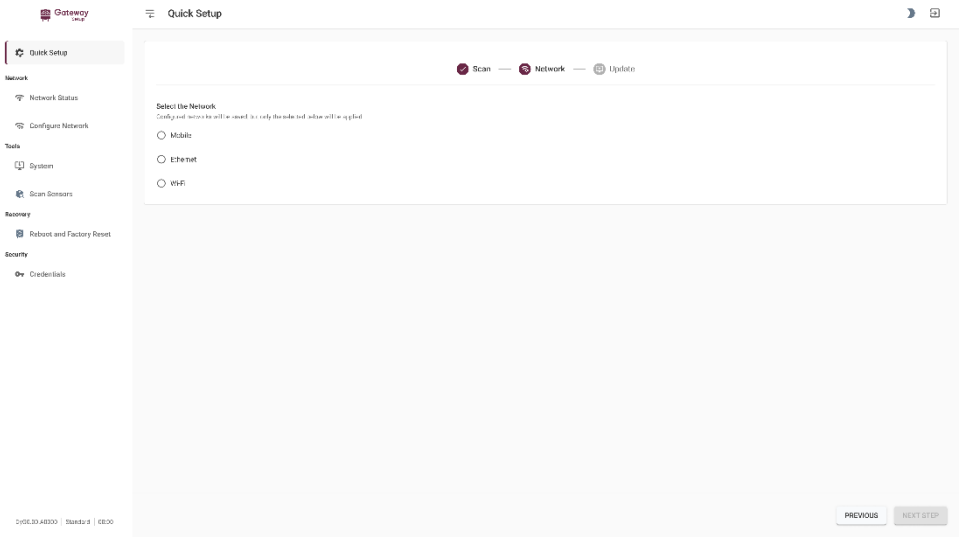


Figure: Quick Setup – Network Interface Selection Step

The following will detail the communication interfaces for the operation of the Gateway, as well as its installation and configuration process.

4.2.1 Mobile Network

The Gateway model purchased will provide different communication technologies, previously mentioned in Table 1 of section 2. It is important for the user to find out about local coverage, taking into account the technologies that your Gateway model can connect to and the bands provided in the Datasheet.

If you want to use the DynaGateway via mobile data, you need to insert a Nano SIM Card from the mobile service provider of your choice. The user must not insert or remove the Nano SIM Card while the Gateway is powered on to avoid product failures. Next, select the "Mobile" option and fill in the fields.

The "**APN**" option is optional and can be left blank, if you wish. Next, provide the correct access point, according to the one provided by the Nano SIM Card's operator. In the "**Select mobile settings manually**" option, select the option that best suits your operator. You can select more than one option if you want to cover more than one technology. The options provided in this section will vary depending on the model you have purchased. Here are the fields that the user must fill in, respectively: APN, username, password and connection technology according to those available in your region.

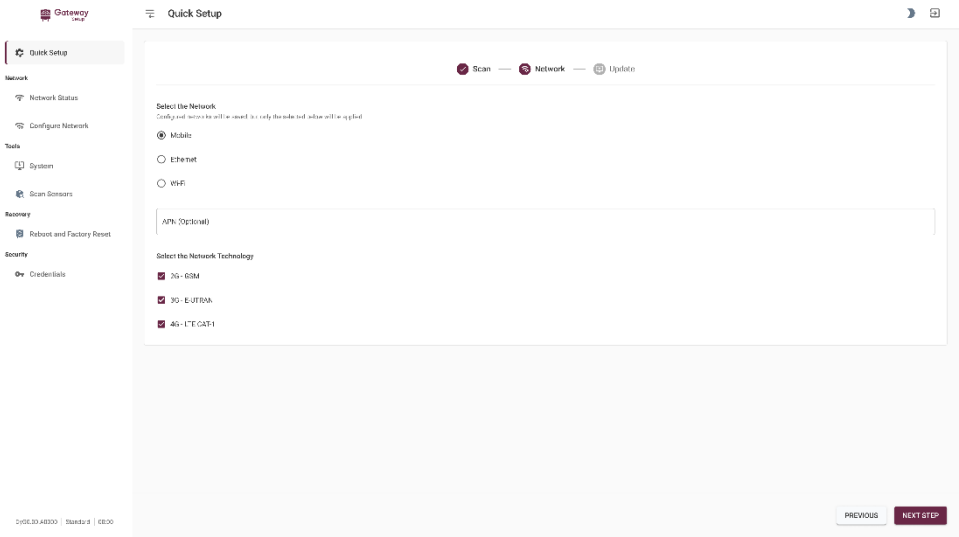


Figure: Quick Setup – Mobile Data communication configuration step

After completion, select the option NEXT STEP to proceed to the next step.

4.2.2 Ethernet

If you want to connect to the internet through a wired network, in addition to releasing network traffic, an RJ45 cable is required to connect you to a network access point. After the cable is connected, select the "**Ethernet**" option and then the option NEXT STEP.

After that, the screen to configure the wired network will appear. By default, the "***Dynamic IP***" option will be pre-selected, as it is recommended for common connections. If you want to keep this option selected, proceed by selecting the option NEXT STEP to continue.

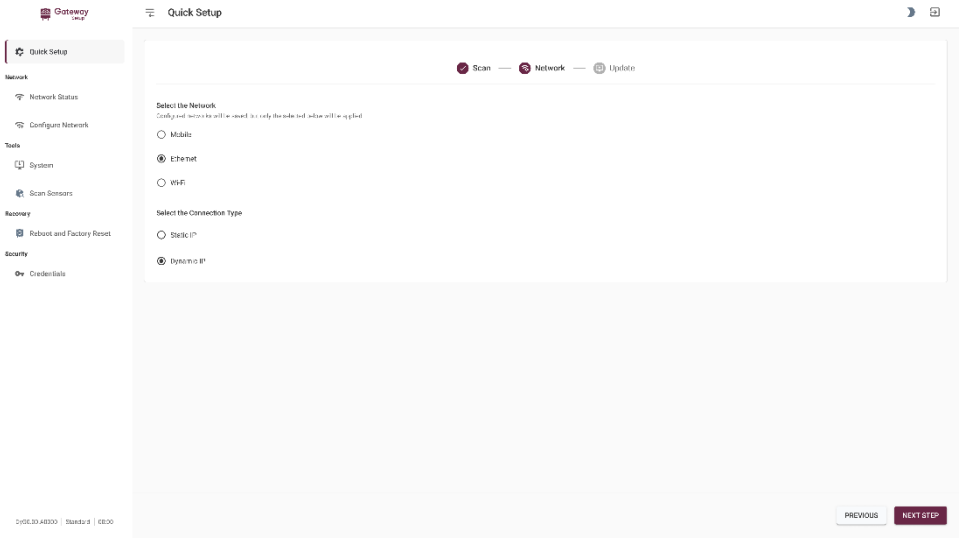


Figure: Quick Setup – Configuration step for communicating over Ethernet with *dynamic IP*

If necessary, you can select the ***Static IP*** option to assign a fixed IP address, used in networks where IP release is required. The department responsible for local network IP release in your company will provide the data to be filled in on this screen. After completed, select the button NEXT STEP to proceed.

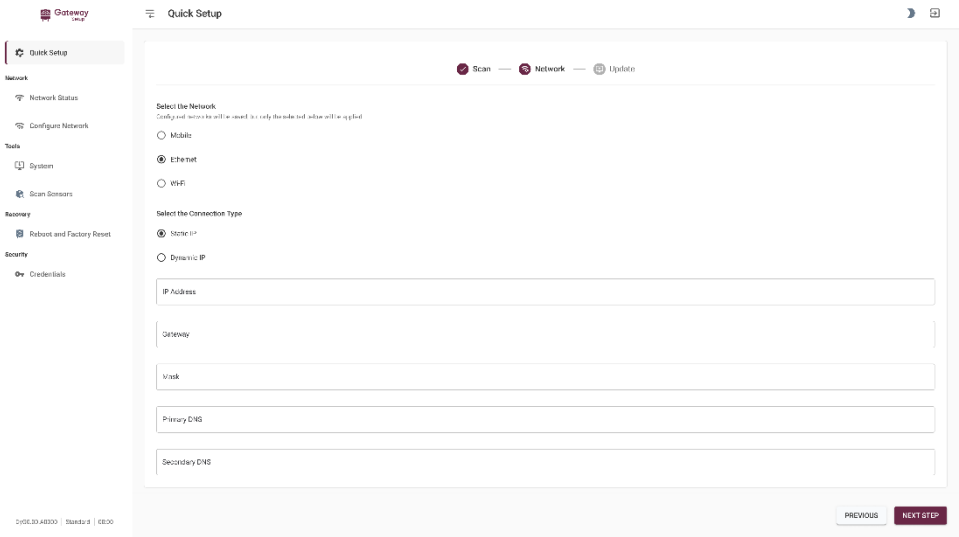


Figure: Quick Setup – Configuration step for communication over Ethernet with fixed IP

4.2.3 Wi-Fi

If you want to connect to the internet via wireless network, select the **Wi-Fi** option, and then select NEXT STEP to proceed.

In the "***SSID (network name)"*** field, it must be filled in with the name of the Wi-Fi network to which you want to connect the DynaGateway. If the default setting "***WPA/WPA2-PSK (Recommended)****" is maintained*, the "***Password***" field must be filled in with the password of the Wi-Fi network to which you want to connect the DynaGateway.

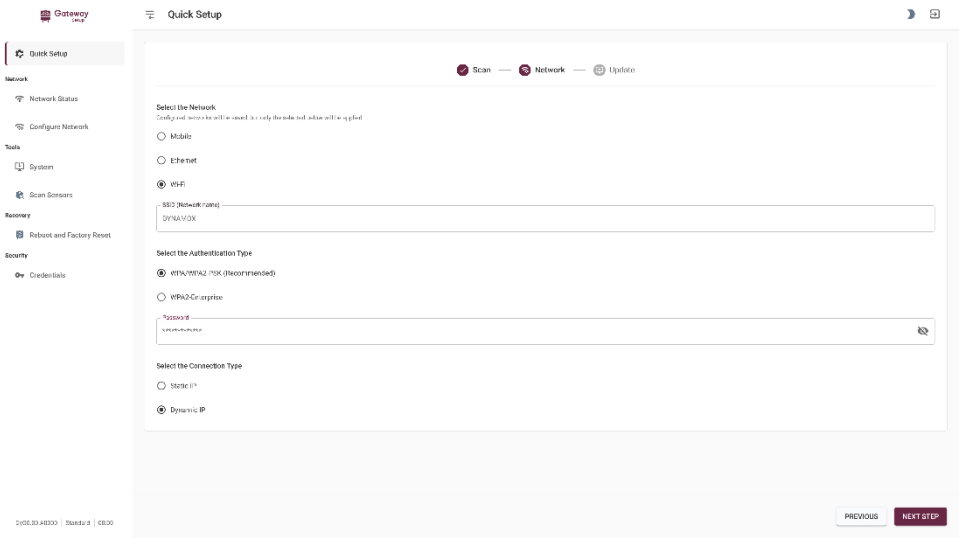


Figure: Quick Setup – Wi-Fi Communication Setup

As mentioned in the Ethernet configuration, it is possible to use a fixed IP address by selecting the "***Static IP***" option. If it is not desired, the "***Dynamic IP***" option will already be pre-selected and will not require any additional configuration.

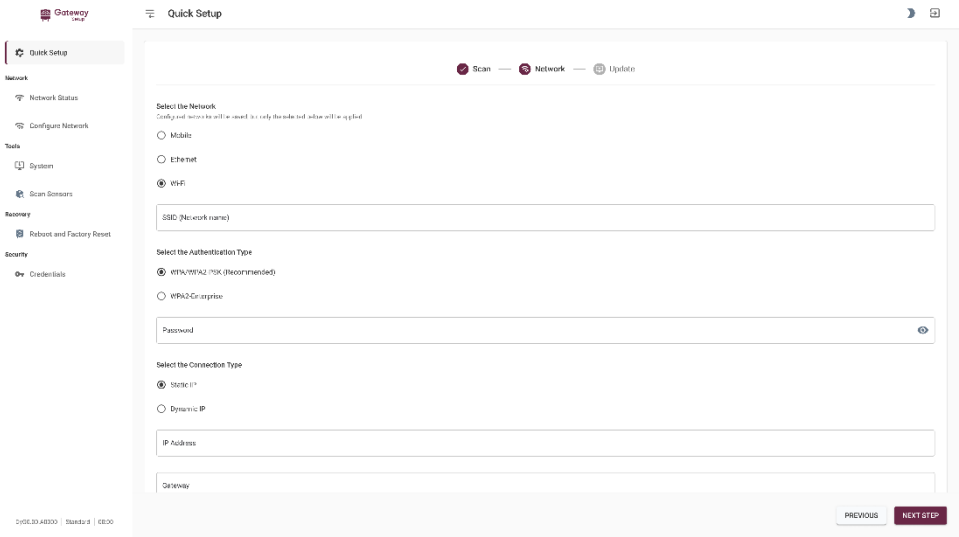


Figure: Quick Setup – Configuration of communication via Wi-Fi with fixed IP

In specific cases, it may be necessary to configure the Gateway on a WPA-Enterprise Wi-Fi network (with username and password per employee). In this case, select the "**WPA2-Enterprise**" option. After that, the "***Username***" and "***Password***" fields will appear, which must be filled in with the information regarding the username and password of the corporate network.

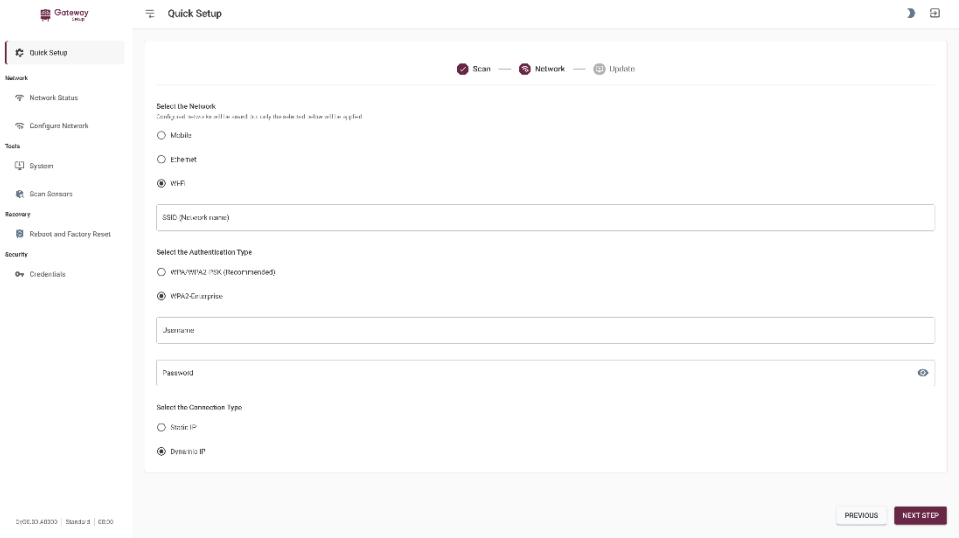


Figure: Quick Setup – Configuration of communication over Wi-Fi with WPA2- Enterprise

Once completed, select the option NEXT STEP to proceed.

The third step in the Quick *Setup* is the *Update,* to update the DynaGateway firmware. This step is described in detail in Section 7.4 but is optional. If you do not want to make any changes to this step, select the "***No, don't need to update***" option and click NEXT STEP to finish the Quick Setup.

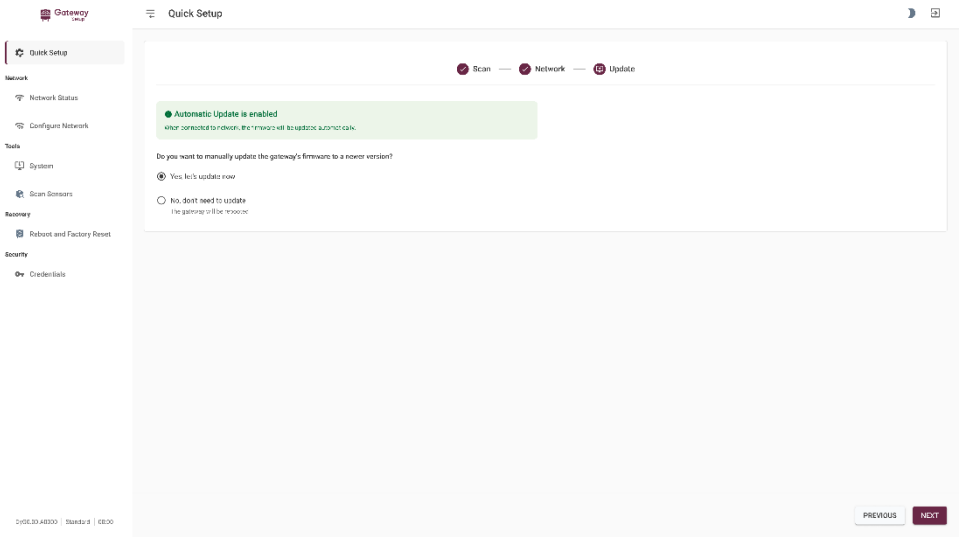


Figure: Quick Setup – Firmware Update Setup

After completing the settings in the Quick Setup tab, you need to restart DynaGateway.

Section 4.3 - Communication Interface Status - refers to the status of the communication interface configured for the Gateway. This is where you can check that the entire configuration process is correct and that the device is ready to communicate with the cloud.

4.3 LED indication

On the DynaGateway casing, there are indicators of the connection status and relevant information for the user through LEDs. Each of the three LEDs on the product relates to: *Power, Status* and **Network**. The color and behavior of the LED can vary according to the activity the Gateway is currently performing or the state it is in:

1. Power

Green and steady: powered

Yellow and blinking: ready to start Gateway Setup mode

Yellow and steady: Gateway Setup mode

Red and steady: Factory reset

2. Status

Switches between on and off while the Gateway is performing one of the following activities, depending on the color of the LED:

Light blue and blinking: communicating with DynaLoggers

White and blinking: communicating with the DynaPredict Web Platform

Purple and blinking: updating the Gateway firmware

Orange and blinking: internal processing

3. Network

Switches color according to the selected communication interface:

White and blinking: connecting to Wi-Fi

Blue and blinking: connecting to Ethernet

Purple and blinking: connecting to mobile networks

Green and steady: successfully connected to network

Red and steady: connection problem (incorrect Wi-Fi password, Ethernet cable removed or Mobile Network connection denied)

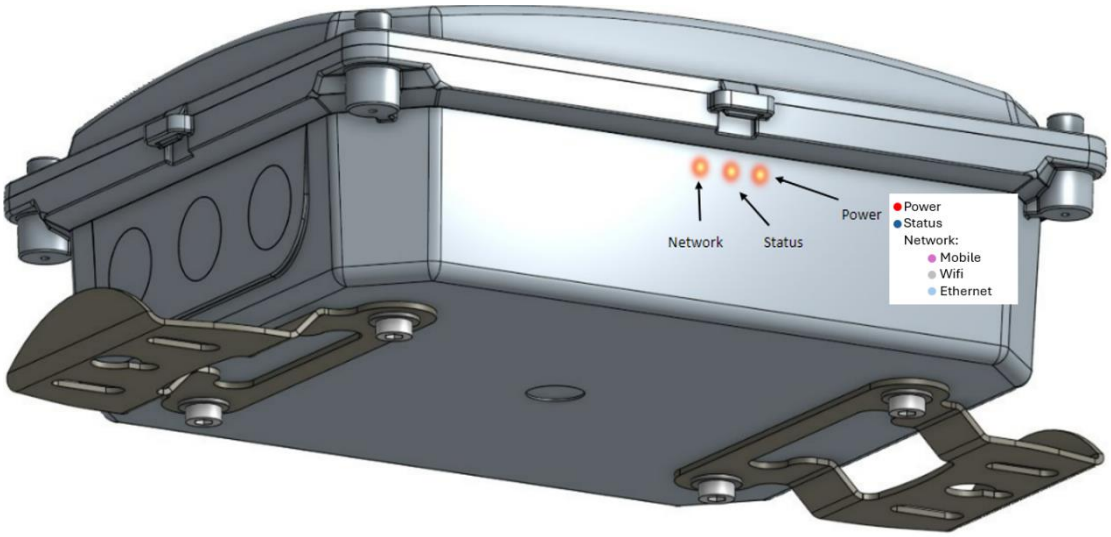


Figure: LED settings

4.4 Mounting

After configuring the communication interface, it is necessary to proceed to the designated location to position the DynaGateway. To conduct the mounting process, it is important to consider the product dimensions and pay attention to the drilling patterns and the recommended screw size for mounting (M4), as shown in the figure below:

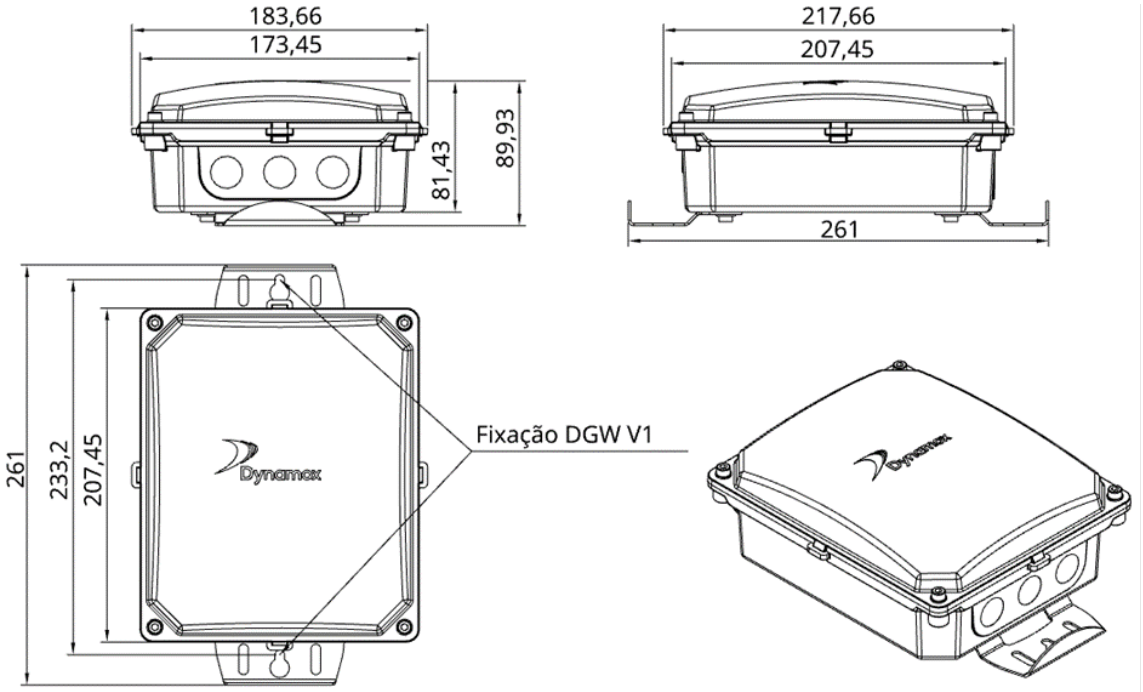


Figure: DynaGateway dimensions and mounting holes

To access the physical interfaces of the product (USB port, RJ45 connection, etc.), it is necessary to unscrew the front bottom cover. It is worth noting that the tightening torque of this component should be approximately 4 N.m, considering the screw size and the manufacturing material of the casing.

In the image below, the cable glands at the bottom give access to where the cables pass through: on the left, where the power cables pass through (Vac or Vdc supply); and on the right, where the RJ45 (ethernet) cable passes through.

Figure: Procedure for connecting the RJ45 cable (ethernet)

To ensure proper operation, it is recommended to access the device's configuration interface and check the visible sensors within its range before closing the front cover and positioning it at the final installation location. To perform this check, refer to section 7.5 of this document.

Finish installing your DynaGateway by closing its front cover, tightening the screws previously removed and attaching it to the installation place. The positions indicated in the image below represent the Gateway's three fixing points on the desired structure.

- **Central perforation:** M5 or 3/16” hexagon socket screws should be used to secure the product to the central hole, which can be seen in red.
- **Side perforations:** Hellerman tape or screws (M5 or 3/16") should be used to secure the product to the side holes, which can be seen in the blue indication.
- **Fixing tabs**: For fixing to poles or large metal structures, it can also be done using an APC (Adjustable Pole Clamp), shown in green in the figure.

Figure: Mounting options

After configuring the communication interface and positioning the Gateway in its operating location, the user can check the success of the process through the Power and Network LEDs (colored according to the chosen communication interface, see section 4.3), both of which light up continuously.

Finally, to configure which Spots will be collected by the Gateway, the user must perform the adoption and configuration process of the Gateway's collections through the DynaPredict Web Platform, as described in the subsequent sections.

5. Adoption and Setup

After making the appropriate network and communication interface settings for the Gateway, the user needs to access the Web Platform to adopt the device on a workspace and indicate the operating parameters, such as the sensors to be collected and the interval for collecting continuous values and requesting spectra.

To do this, the user must access the Platform (https://dyp.dynamox.solutions/) and, in the side menu, access the Gateways tab. Once logged in, a table with the list of Gateways already registered in the user's workspace will be displayed.

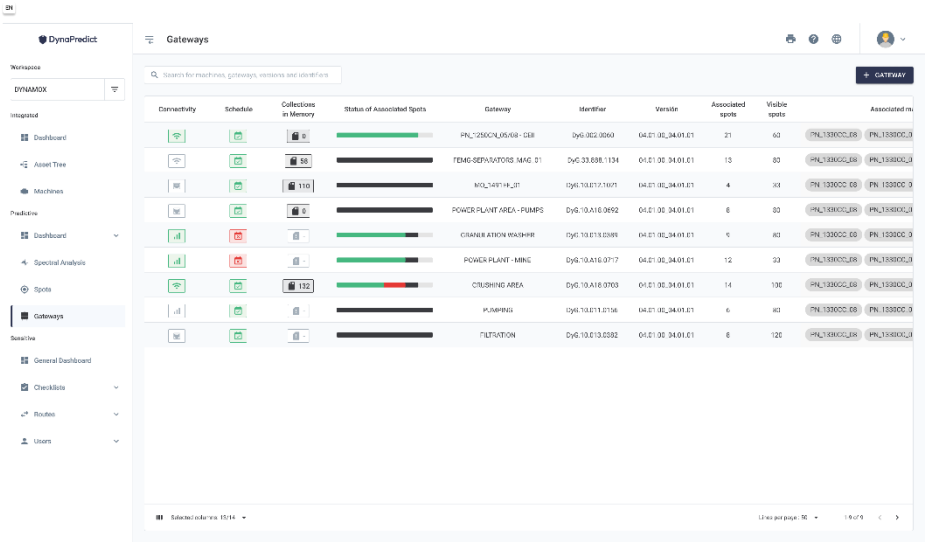


Figure: Gateways Dashboard

5.1 Adopting a DynaGateway

To adopt a DynaGateway, in the Gateways tab, the user must select the **+Gateway** option in the upper right corner.

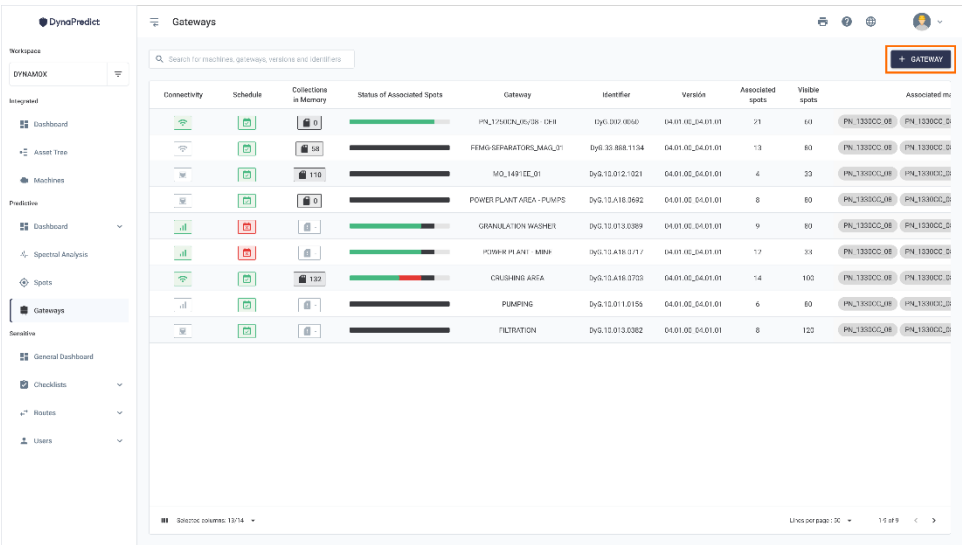


Figure: +Gateway Button

On the right-hand side of this screen, the user must enter the device's PIN, printed on its casing. Using the Asset Tree in the left-hand corner, the user must select which sub-area the Gateway will be positioned in. This will influence the restriction of the group of sensors that can be associated with the Gateway, as well as which users can edit its configuration parameters.

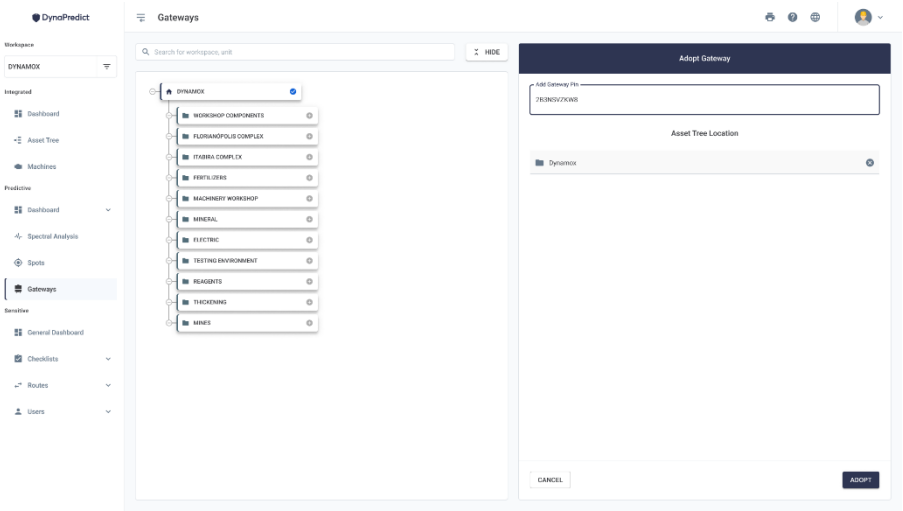


Figure: Adopting a Gateway

The selection follows the same pattern as the company's Asset Tree, where higher levels can use the same benefits at lower levels. By clicking on the **"Adopt"** option, the Gateway Settings page will be displayed to the user.

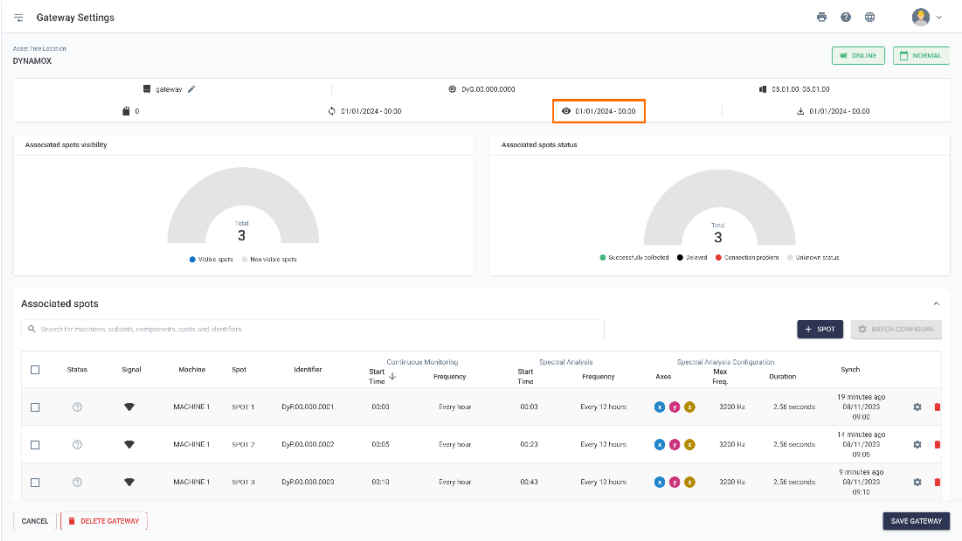


Figure: Gateway configuration details

At the top of the screen, general information about the Gateway is displayed, such as the assigned name (which can be edited), product serial number, last edit made in the Web Platform, and the last visibility update.

At the bottom, there is information related to the status of the Spots within the Gateway's range and the sensors associated with it. The status of each icon is detailed in section 6. The Spots visible to the Gateway are all those within its range, including sensors that are not associated with this Gateway. This concept can help determine the best use for the device, ensuring that it is configured to collect data only from Dynaloggers that are within its range.

By selecting the "**+SPOT"** option, it is possible to associate the Spots that should have their data collected by the Gateway. To do so, select the option to see the Spots available for association.

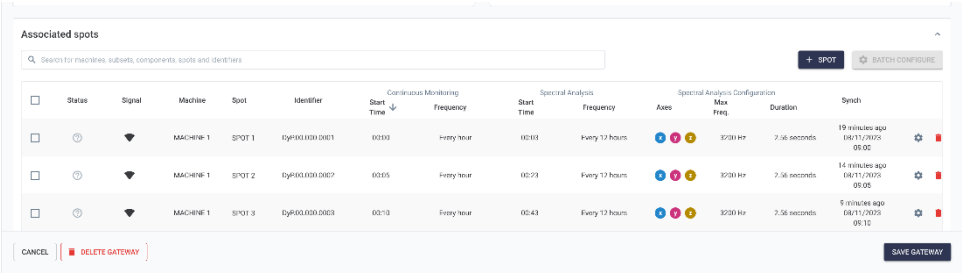


Figure: Spots associated with the Gateway

The list of Spots below will be shown according to the workspace in which the Gateway was previously configured. The **"Only visible Spots"** option allows you to filter out Spots whose DynaLoggers are within the DynaGateway's Bluetooth range. It is important to note that to use this option, the device must be powered on and have recently updated its visibility. This update does not take place at the same time as the Gateway is connected to the network, meaning this process may take some time to complete.

It is still possible, in all cases, to uncheck the "**Only visible Spots**" option to associate the Spots, bearing in mind that the Gateway does not yet have information about whether the sensor is within its communication range. Likewise, it is interesting that the device is already positioned in its installation location, as this will inform the user which Spots are visible to them for future association.

To add a Spot, simply select the icon on the right, causing it to change to . If the Spot in question is already associated with another Gateway, the icon shown will be . In the left corner of the screen, the signal strength of each Spot visible to the Gateway will be shown, which can assist in the process of positioning the device.

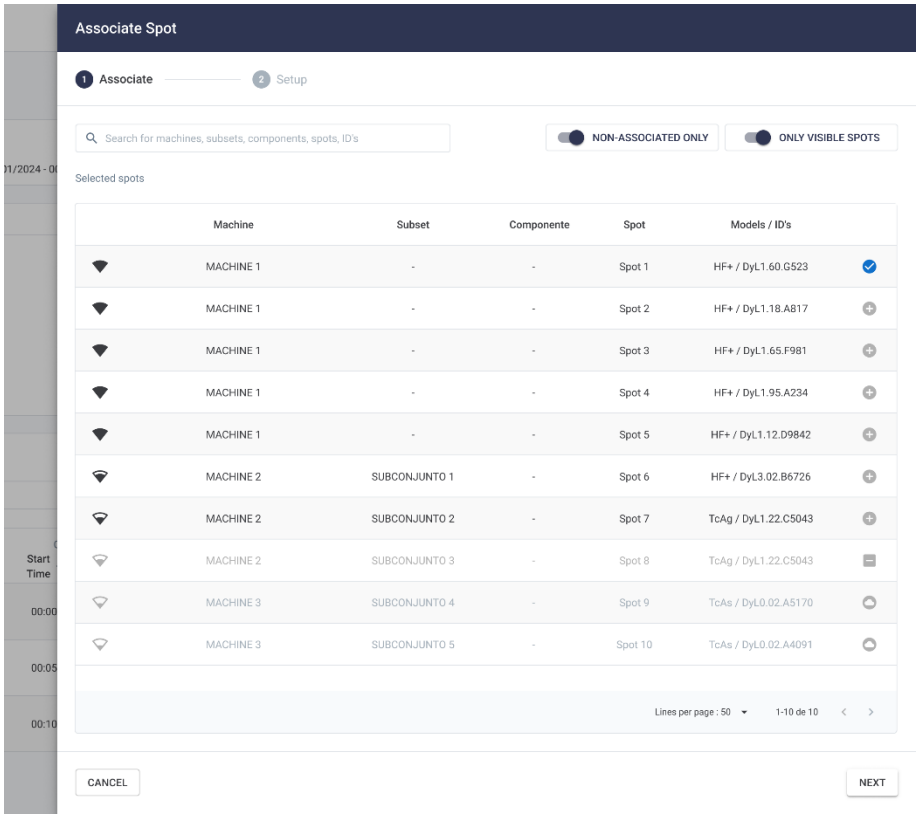


Figure: Spot Association

At the end of the process, select the "Next" option to proceed to the screen for configuring the Spots on the Gateway's schedule. It is also important to ensure that the collection intervals for each Spot are set correctly, in order to avoid overloading the Gateway, as described below.

5.2 Batch Spot Configuration

Once the Spots to be collected by the Gateway have been associated, the user needs to configure the desired data collection and spectral request intervals.

By selecting the "⚙" option, the user can configure the parameters for continuous data collection and spectral analysis of a specific Spot.

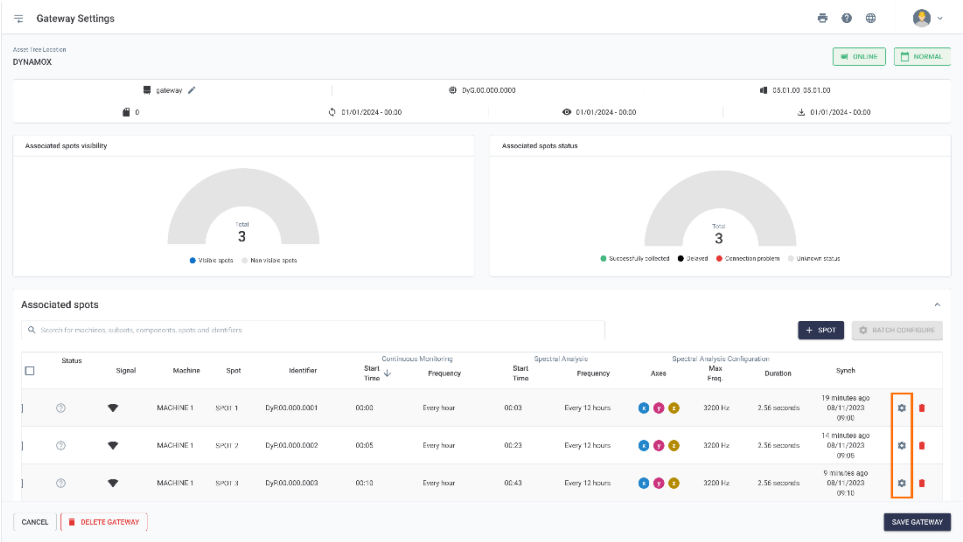


Figure: Spot Selection for Individual Configuration

In cases where there are several DynaLoggers associated with the Gateway, it is interesting to configure all the Spots in a standardized way, generating consistency in registering data and speeding up the parameterization process. This way, in the top right-hand corner, the user can select the “Configure in batch” option, which becomes available for selection when more than one Spot is marked in the list.

To define which Spots will be configured simultaneously, check the checkbox to the left of the corresponding spots. To select all at once, check the checkbox above the list of Spots.

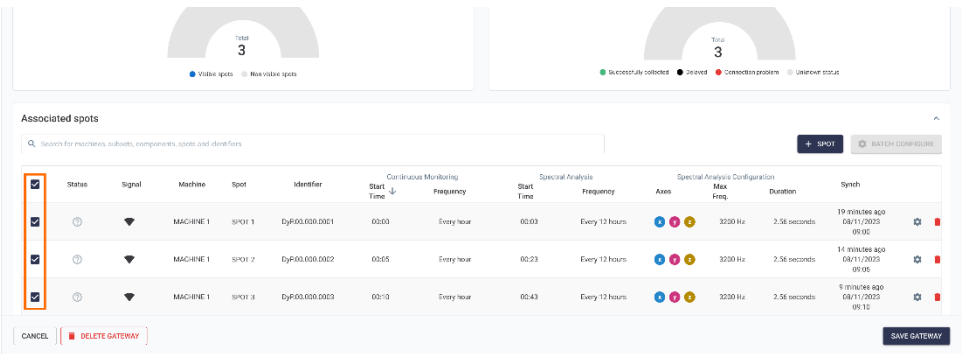


Figure: Spot Selection for Batch Configuration

The screen for configuring the collection and spectral analysis schedules determines how often the DynaGateway will communicate with the sensors and send data to the Platform. This screen consists of two monitoring options:

- Collection: setting the times at which the Gateway will communicate with the DynaLogger to request the collection of global data stored in its internal memory.
- Spectral Analysis: setting the times at which the Gateway will communicate with the DynaLogger to request a spectral analysis at the Spot.

In each type of monitoring, it is necessary to define the start time of the collections and the periodicity with which the Gateway will repeat the monitoring, which is the collection interval.

It is important to differentiate between the concepts of collection interval and sample interval. The former relates to the Gateway, while the latter is the configuration defined when creating the Spot for the DynaLogger. The sensor takes measurements according to its sample interval and stores them in its internal memory until the Gateway performs data transfer to the Platform and empties the sensor's memory according to its collection interval.

Example: A DynaLogger with a sample interval of 5 minutes generates vibration and temperature samples according to this interval and stores them in its internal memory. A Gateway, with a collection interval of 3 hours (180 minutes), will collect this data and send it to the Platform every 3 hours, collecting 36 samples (180 min / 5 min) of vibration and temperature at a time.

In the case of Batch Configuration, it is also necessary to inform the Action Interval between Spots so that from the start time of the collection of the first Spot on the list, the Gateway sets the schedules for the other Spots. When selecting the option, the configuration window will be displayed for the user to fill in the following fields:

Continuous Monitoring:

- Start time: Start time of the schedule, that is, the moment when the first Spot on the list will be collected.
- Action Interval between Spots: The time interval between Spot collections, starting from the immediately preceding point. For example, for the second Spot on the list, its collection time will be the start time of the first Spot plus the action interval between Spots, and so on.
- Interval: The interval of the complete spectral collection cycle. Unlike the action interval between Spots, this value refers to the periodicity of the collection cycle, i.e., how often the monitoring point will have its data collected again. For example, start time at 09:00 with a 3-hour interval, resulting in collection cycles at 09:00, 12:00, 15:00, and so on.

Spectral Monitoring:

- Start time: start time of the schedule, that is, the moment when the first Spot on the list will have its spectral data requested.
- Action Interval between Spots: The time interval between spectral data requests for the Spots, starting from the immediately preceding point. This field is analogous to continuous monitoring, except for the type of action by the Gateway, which will be different.
- Interval: The interval of the complete spectral collection cycle. Unlike the action interval between Spots, this value refers to the periodicity of the collection cycle, i.e., how often the monitoring point will have its spectral data requested again. For spectral monitoring, the minimum value for this field is 1 (one) day.

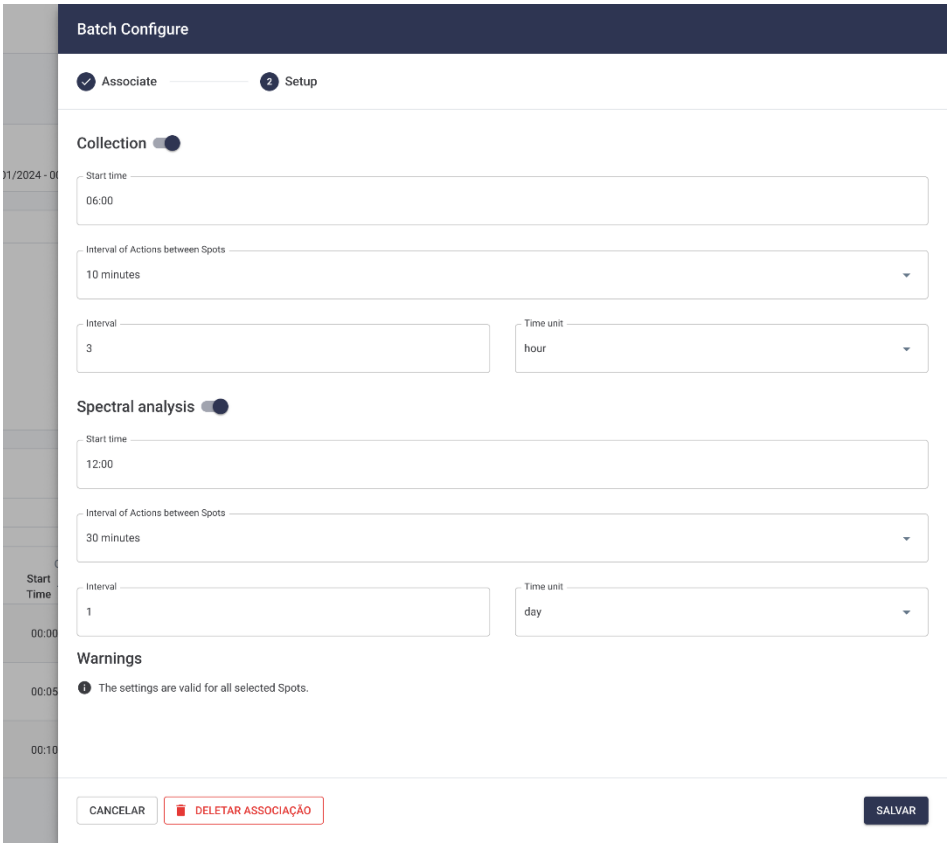


Figure: Batch parameterization of collection intervals and spectral analysis

<u>It is possible to perform as many batch configurations as necessary independently, meaning that the collection and spectral parameters can be different for each configured batch.</u>

It should be noted that if at least one selected Spot is parameterized for the acquisition of triaxial spectral analyses with a maximum frequency greater than 1600 Hz, a warning will be displayed. This indicates that each axis will be collected sequentially and then grouped into a single measurement, which requires more execution time on the part of the Gateway. For these cases, it is recommended to use a longer time interval between Spots to avoid delays.

If the "Operations Accumulate More Than 24 Hours" Icon appears, it means that the volume of actions associated with this Gateway may be exceeding the time to execute them. In this situation, the daily operations of continuous and spectral data collection together have an estimated time that exceeds 24 hours to be carried out, which may result in a progressive delay of the Gateway's processes. In this case, we recommend reconsidering the volume of collections or the spectral configurations of the Spots to avoid delays.

Upon completing the setup process, the user must select the "Save" button to finish it. To save the Gateway changes, click "Save Gateway".

5.2.1 DynaGateway Configuration Practical Example

In this section, a practical example will be introduced regarding the configuration of a DynaGateway, as well as best practices for carrying out this process, considering a data collection interval of 4 hours and daily spectral analysis for 20 associated Spots: as mentioned earlier, the time taken for the Gateway to perform a spectral analysis depends on the volume of data in the analysis and the stability of the internet. Typically, intervals of 30 minutes are considered for this action and 10

minutes for continuous data collection. In this example, data collection and spectral analysis are alternated in a schedule with 20 Spots, according to the configuration below:

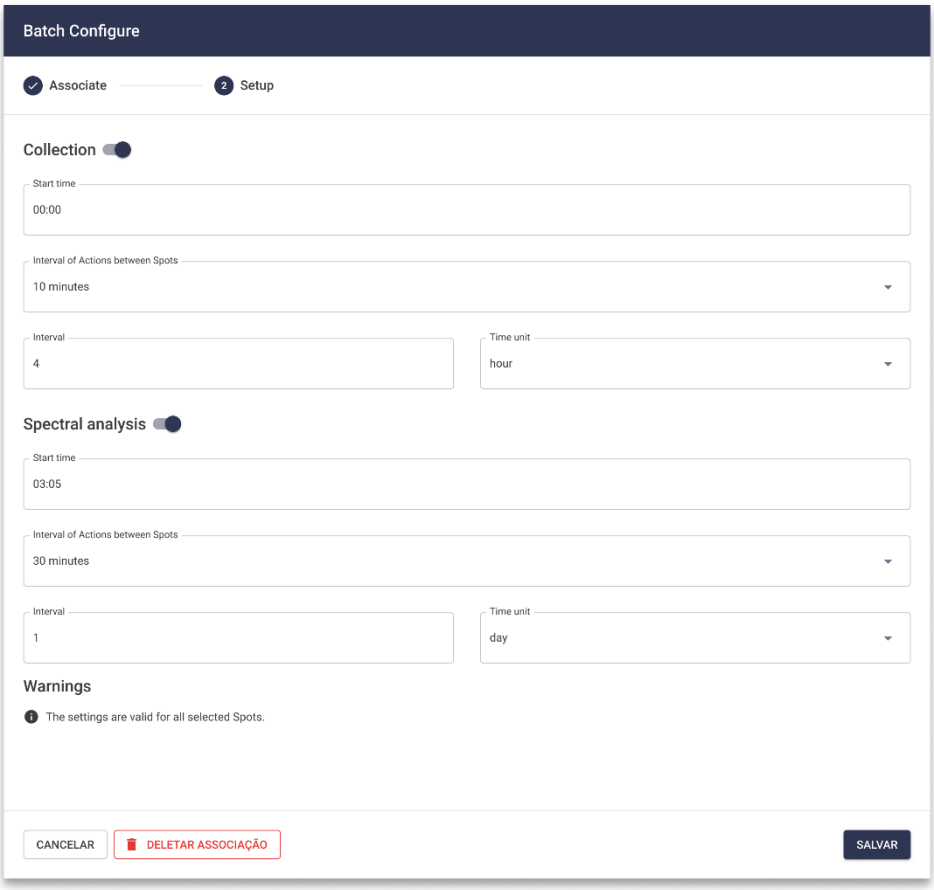


Figure: Batch configuration of collection intervals

Thus, all continuous data from the spots will be collected within 4 hours (20 spots x 10 minutes equals about 4 hours), and therefore, this is a valid periodicity. Additionally, the intervals considered between actions respect the feasible time for the Gateway to perform them.

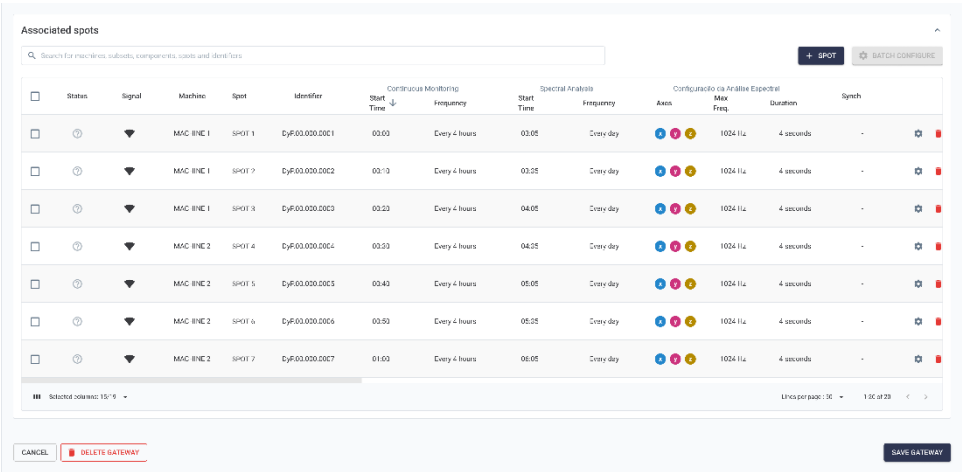


Figure: Gateway operations schedule

In this way, the first Spot is collected at 00:00 and begins its spectral analysis at 03:05. The second Spot is collected at 00:10 and starts its spectral analysis at 03:35, and so on. The collection cycle is repeated every 4 hours; therefore, at 04:00, the first Spot will be collected again. Good practices for

configuring the Gateway's schedule ensure that the actions are spaced out and that there is enough time for them to be processed before the repetition of an action cycle.

5.3 Individual Spot Configuration

In some cases, it may be interesting to configure Spots individually. To do so, the user should select the "⚙" option next to the desired Spot, and a window similar to the batch configuration will be displayed. The fields and functionalities follow the same pattern discussed in the previous section regarding batch Spot configuration.

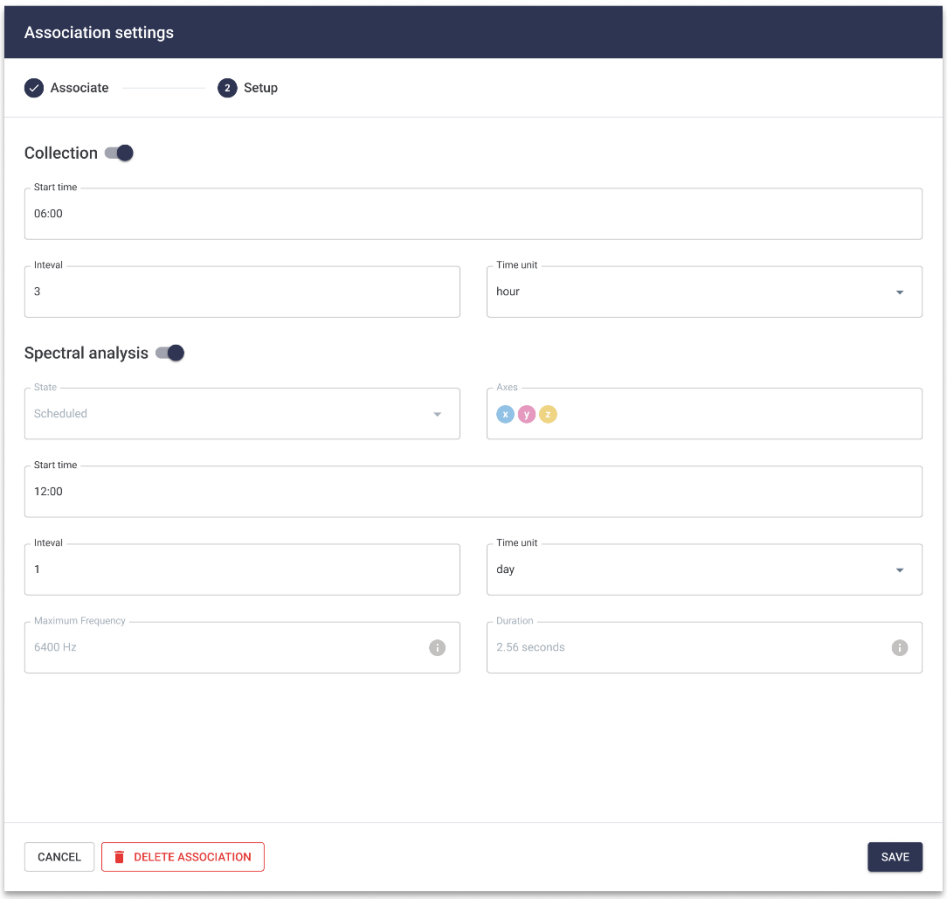


Figure: Parameterization of collection intervals and spectral analysis

As in the batch configuration, if the selected Spot is parameterized to perform triaxial spectral analysis with a maximum frequency greater than 1600 Hz, a warning about the execution time of the action will be displayed.

Upon clicking the "Save" button, the user will be returned to the Spots screen to configure the remaining selected points.

6. Status

Once the DynaGateway has been configured and adopted, it is possible to monitor the connection status with the DynaLoggers to ensure that all the assets associated with the gateway are being effectively monitored. The status of each Spot will vary according to the connection attempts made by the gateway at the times programmed when it was set up.

6.1 Connecting to Spots

When accessing the Gateway Configurations screen, you can check the data collection status of the spots associated with the selected Gateway. The colored icons on the left corner of the list indicate the last collection status of each point, as follows:

Collected: The Gateway was able to collect data from the Spot associated with it at the scheduled time.

Collection Delay: The Gateway did not send the last collection from the Spot at the expected time.

Collection Issue: The Gateway was unable to collect data from the associated Spot in the last attempt.

Unknown: The Gateway has not yet sent any collections from the Spot. If all Spots remain in this status, it is recommended to check the connection interface (Ethernet, Wi-Fi, or Mobile Network) and the power supply of the product. If there are isolated cases of Spots with this status, check the signal strength of the sensors. With each update of the Gateway's schedule, the status of all spots remains Unknown until the scheduled time for their first collection. After the scheduled time, the status is updated to Collected, Collection Delay, or Collection Issue, depending on the Spot's collection performance. The status icon is updated with each new collection, as defined in the Gateway's configuration.

The status icon is updated with each new collection, which is set in the Gateway configuration.

6.2 Visibility Update

The DynaGateway periodically scans the sensors within its Bluetooth range. Therefore, by default, the device performs a visibility update every 2 hours when properly connected to network. The information about the time since the last update is available in the last visibility field on the Web Platform:

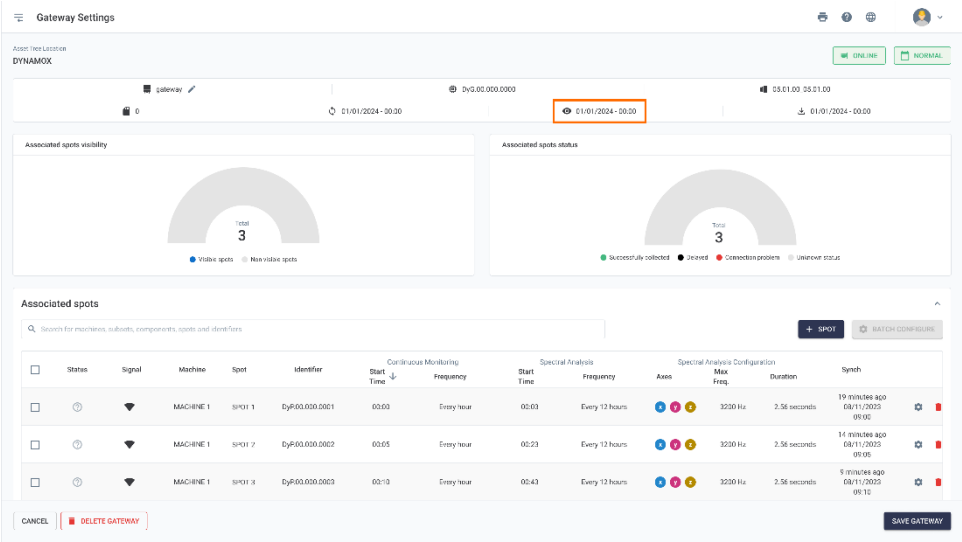


Figure: Last Visibility Field

The visibility update procedure ensures that the status shown on the Platform reflect the reality of the last 2 hours, identifying which monitoring points need individual verification.

7. Additional Resources

DynaGateway has several tools that can help with troubleshooting and contribute to the usability of the device. These include system reboots, restoring factory defaults, updating firmware and searching for sensors within its range.

This section details the functionalities and procedures for using the device's tools. All described processes are carried out through the device's Web interface, the same one used in configuring the communication interface (accessing http://dynaGateway-setup.local/ or 192.168.10.1 in the browser).

7.1 Connectivity

The connectivity of the DynaGateway is one of its main features and is essential for its proper functioning, enabling the collected data to be sent to the Dynapredict application, which is why the device provides a wide range of network interfaces and configurations, adding to the product's adaptability and security.

7.1.1 Network Interface

Three network interface options are available: Wi-Fi, Ethernet and Mobile Networks.

7.1.1.1 Wi-Fi

The Gateway has 2.4Ghz Wi-Fi connectivity, and the following parameters can be set:

- **SSID:** In this field you must enter the name of the Wi-Fi network to which the user is trying to connect.
- Security configuration:
    - **WPA/WPA2-PSK**:
        - Password: In this field you must enter the network password if there is one.
    - **WPA/WPA2-Enterprise**: For this type of authentication, you must enter the user information and password for the corporate network.
        - Username: Information about the user of the corporate network.
        - Password: Information about the enterprise network password.

7.1.1.2 Ethernet

The Gateway has Ethernet connectivity, it is necessary to connect a twisted pair network cable with an RJ-45 connector.

7.1.1.3 Mobile

In many locations, the availability of Wi-Fi and Ethernet infrastructures is a problem, requiring the use of mobile networks as a connectivity solution. To use mobile networks, it is necessary to use a Sim Card from a provider with coverage in the region of installation and with an active mobile data plan.

Some network technologies are only available for specific models; information on models is described in section 2.2. The following options are set:

- APN: The Access Point Name is an optional setting.
    - Default: By default, this field is empty, in this mode the device uses the information on the SIM card to select the APN automatically.
        - Only public APNs from operators work in this model.
    - Private APN: For this network type, the field must be filled in.
- Radio Access Technology (RAT): the devices

- 2G - GSM
- LTE CAT-M1
- LTE NB-IOT
- LTE CAT1
- 3G

7.1.2 LAN Configuration

Access to LAN settings is limited to the Wi-Fi and Ethernet interfaces and some configuration options are available:

- Static IP: When selecting this setting, it is necessary to know some network information, such as: IP address, Gateway, mask, and primary DNS.
- Dynamic IP: By default, this setting is selected at the factory and no additional configuration is required.
- DNS

7.1.3 NTP

The Gateway uses the SNTP protocol for time synchronization

- Server
  - Default: time.google.com
- Port 123

7.2 System Reboot

The reboot of the DynaGateway can be used in cases where the device is not performing its functions as expected. To do this, the user must access, in the device's Web interface, the Reboot and Factory Reset tab, located in the side menu.

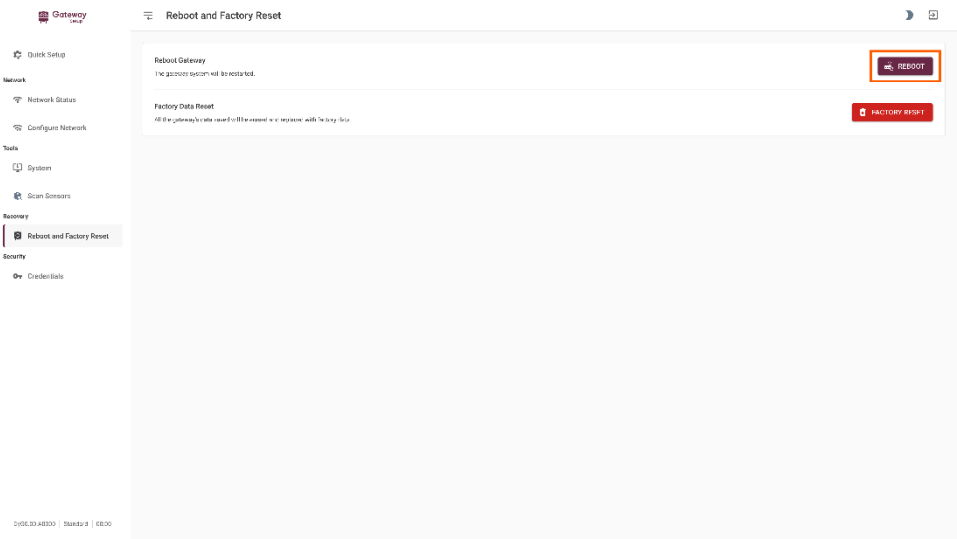


Figure: System Reboot Tool

By selecting the Reboot button and confirming, the device will automatically start the reboot process.

This procedure can also be performed through the physical Reset/Config button, requiring only a single press for the Gateway to restart. It is important to note that this process does not affect the configurations but rather the operating system, which will be restarted.

7.3 Restore Factory Setting Defaults

Restoring the settings to factory defaults reboots the device and erases all its existing settings, including the registered users, access password and communication interface, which will need to be reconfigured later. After the reset, the Gateway reboots and adopts the factory settings specified in 7.3.3.

7.3.1 Restoring the configuration via Gateway Setup

To perform the reset, the user must access the device's web interface, access the Reboot and Factory Reset tab from the side menu and then select the Reset button. The process will start automatically after confirmation.

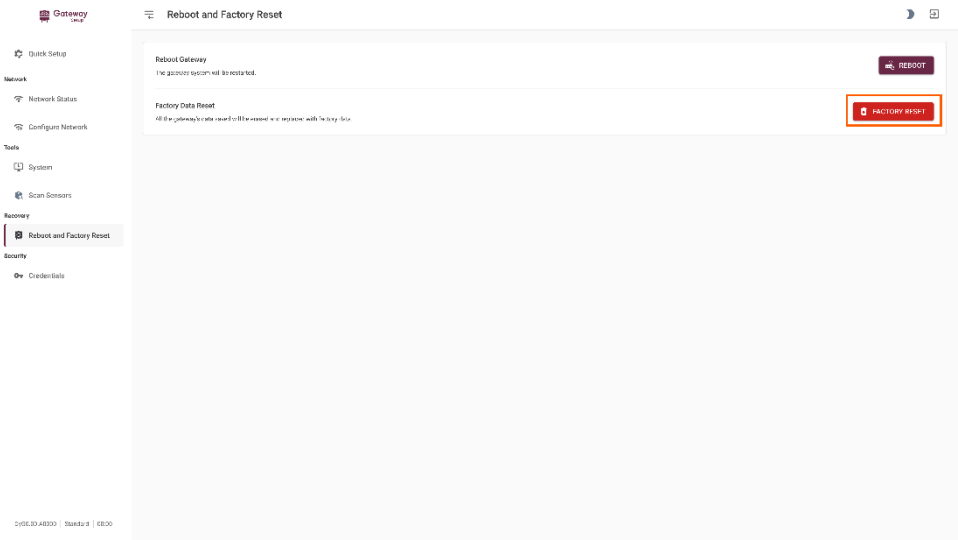


Figure: Factory Reset Tool

7.3.2 Restoring configuration via external button

It is also possible to restore factory defaults by pressing the Reset button for 20 to 30 seconds, during which time the Power LED will turn red. If you release the button during this time, the LED will blink red for 3 seconds. To continue with the reset, the button must be pressed once, otherwise the Gateway will reboot without erasing any data. Finally, the Power, Status and Network LEDs will blink red if the reset is successful.

If the user forgets the username and password registered for the device's web interface, it will be necessary to perform a factory reset using the button.

7.3.3 Default factory configuration:

The factory settings are the settings that the Gateway has when it is produced and that it takes over again after a factory reset action takes place.

- Network configuration
  - o Ethernet
  - o Dynamic IP
- Access credential:
  - o User: admin
  - o Password: admin

- NTP
  - Server address: time.google.com
  - Server port: 123

7.4 Firmware Update

To keep your devices up to date with the latest features, Dynamox provides automatic updates for internet-connected gateways. In some cases, however, it may be necessary to update the firmware locally. To do this, the user must have the update file for the gateway module at hand. To obtain the latest update file, contact Dynamox technical support at support@dynamox.net.

When accessing the side menu in the "**Tools**" tab, select the "**System**" option. The user will have access to the information of the firmware already installed and the fields to perform the update. In the "**Select the firmware file**" field, it is necessary to select the "**CHOOSE FILE**" option and upload the file (already saved on your computer) with .bin extension.

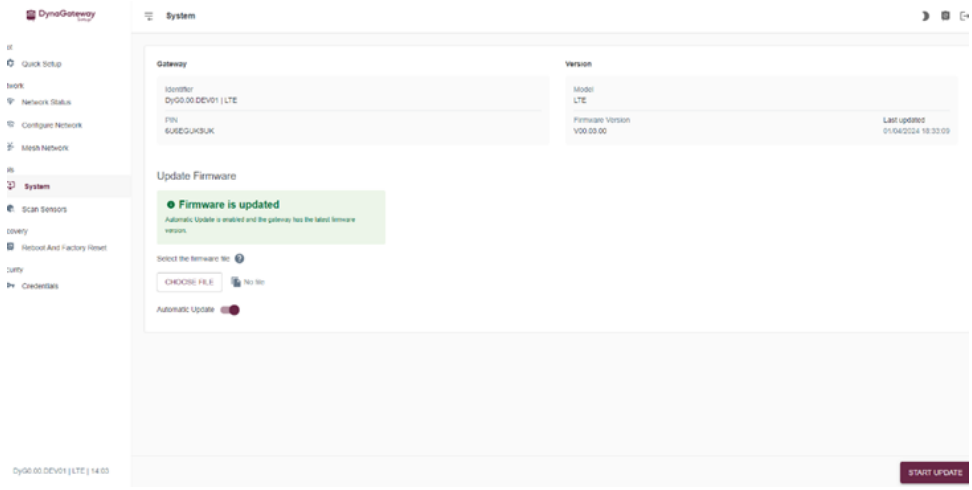


Figure: Firmware update

By selecting the **"START UPDATE"** option, a confirmation window will be displayed to complete the process. When completed, the user will be notified with a window indicating the success of the operation and the Gateway will restart. The LEDs display the Gateway's start-up behavior.

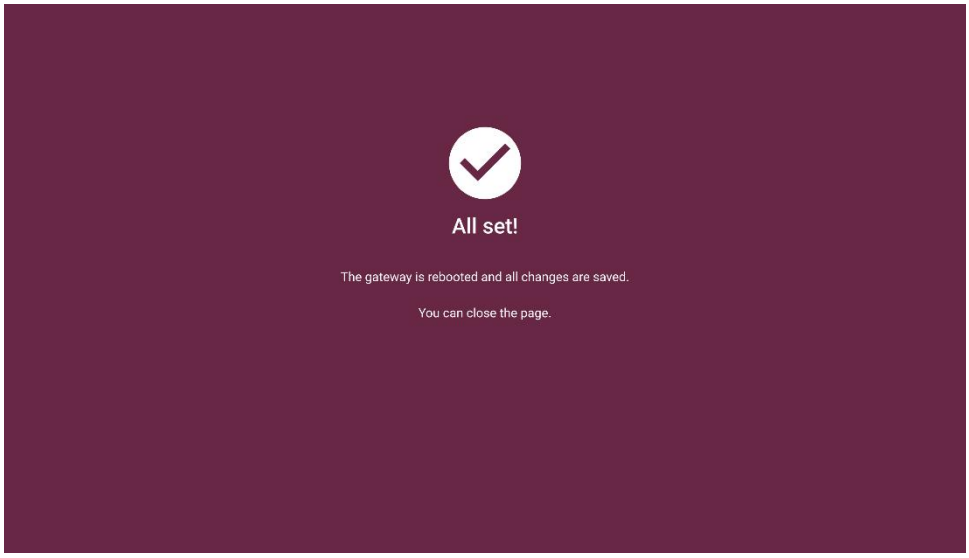


Figure: Gateway restarted successfully

7.5 Search for sensors within Bluetooth range

In addition to the sensor visibility information, which is sent to the Web Platform every 2 hours, it is possible for the user to request a scan of all the sensors within DynaGateway's range at any time, via the Gateway Setup.

This option can be found in the side menu under the "**Tools**" tab. Select the "**Sensors Visibility**" option. This will bring up a screen with a central **"SEARCH DEVICES"** option. When you select this, the device will start searching for all the sensors within Bluetooth range. When finished, a table will be displayed containing relevant information such as: number of sensors, identification, MAC address and signal strength at the time the visibility was performed.

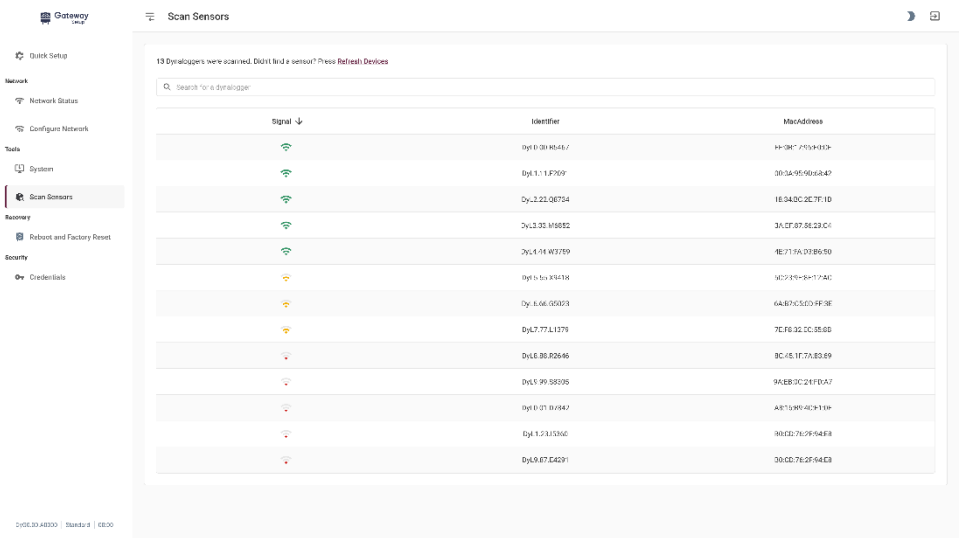


Figure: Search tool for sensors within Bluetooth range

This mapping does not update the "Last Visibility" field in the Web Platform. The process only instantly shows the sensors within the Bluetooth range of the Gateway and can be used to assist in determining the best location for positioning the device.

7.6 Mesh Network

A mesh network is a network topology where each device is connected directly to all the others, forming an interconnection mesh, allowing efficient and reliable communication, even where individual connections may fail. In DynaGateway it is possible to activate this type of network.

By accessing the side menu in the "**Network**" tab and selecting the "**Mesh Network**" option, the user can access the Mesh Network configuration screen. To activate this network, the "**Enable Mesh Network"** option must be enabled.

There are two configuration options for this network:

- **Root:** Responsible for communicating with the external network.
- **Node:** Devices that will be connected to the subnet created by Root.

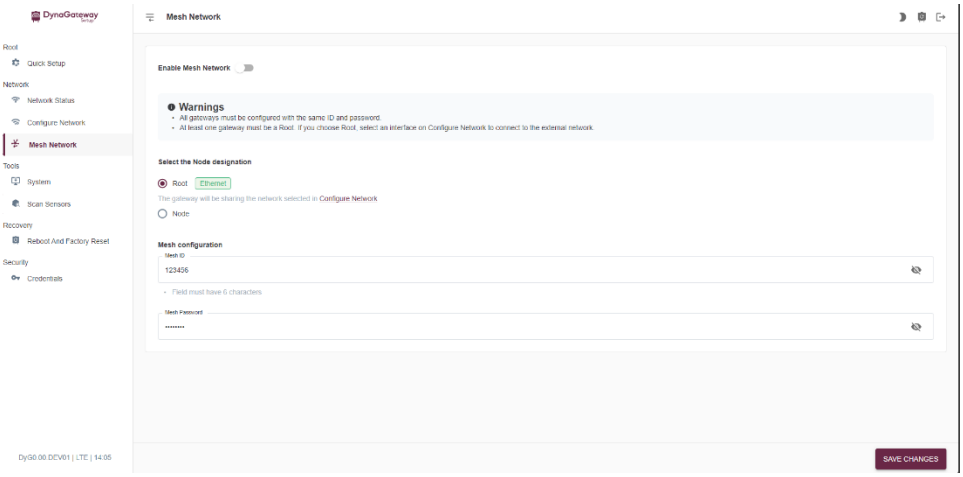


Figure: Mesh Network - Mesh network configuration screen

7.6.1 Configuring the Mesh Network for Root mode

To use the DynaGateway as the Mesh Network Root, in "**Select the Node designation**" the option "**Root**" must be selected. Then, in the "**Mesh configuration**" section, the "**Mesh ID**" and "**Mesh Password**" fields must be filled in to configure the Mesh Network access credentials.

Click on "**Save Changes**" to save the settings.

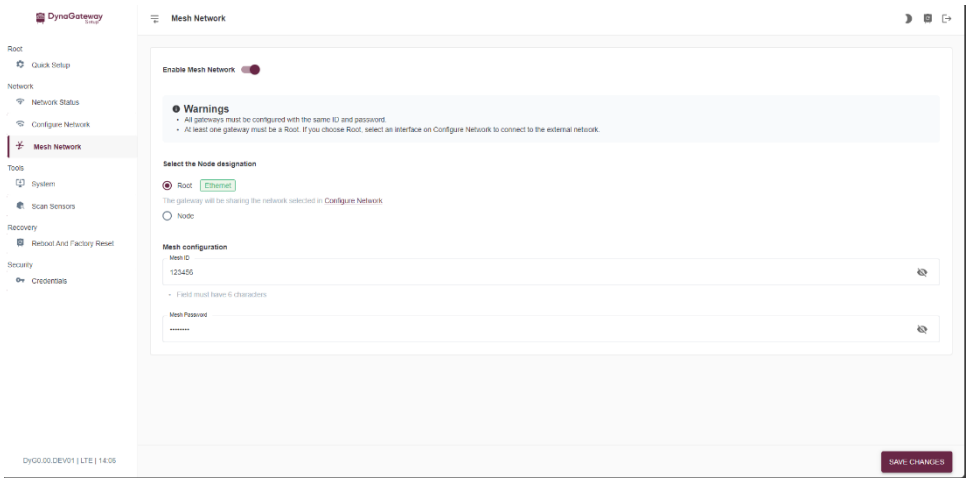


Figure: Mesh Network - Mesh network configuration for Root mode

Finally, you should check in "**Configure Network**" if the interface that root will use to generate the network mesh network (the same one indicated next to the "**Root**" option in "**Select the Node designation"**) is configured correctly, then restart the Gateway so the settings can be applied.

7.6.2 Configuring the Mesh Network for Node mode

To use the DynaGateway as a Mesh Network Node, in "**Select the Node designation"** the option "**Node**" must be selected. Then, in the "**Mesh configuration**" section, the "**Mesh ID**" and "**Mesh Password**" fields must have the same values as those set in the Root Gateway. Click on "**Save Changes"** to save the settings made and restart the Gateway so that the settings can be applied.

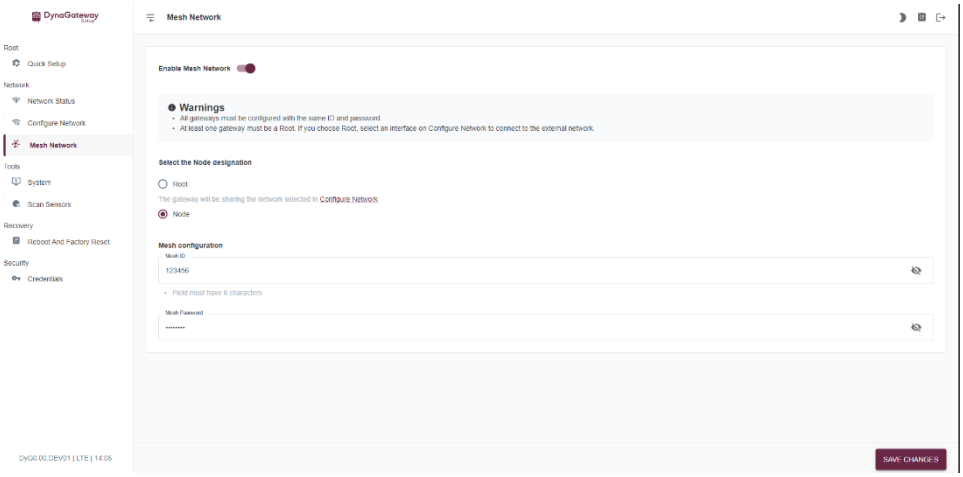


Figure: Mesh Network - Mesh network settings for Node mode

FCC Statement

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

To comply with RF exposure requirements, a minimum separation distance of 20mm must be maintained between the user’s body and the handset, including the antenna.

IC STATEMENT

This device complies with ISED licence-exempt RSS standard(s)

Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End user must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

To comply with RF exposure requirements, a minimum separation distance of 20mm must be maintained between the user’s body and the handset, including the antenna.

Le pré sentappareil est conforme aux CNR d'ISED applicables aux appareils radio exempts de licence.

C L'exploitation est autorisé e aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioé lectrique subi, mê me si le brouillage est susceptible d'en compromettre le fonctionnement.Cet é quipement est conforme avec l'exposition aux radiations IC dé finies pour un environnement non contrô lé . L'utilisateur final doit respecter les instructions de fonctionnement spé cifiques pour satisfaire la conformité aux expositions RF. Cet é metteur ne doit pas ê tre co-localisé es ou opé rant en conjonction avec une autre antenne ou transmetteur.

Pour se conformer aux exigences d’exposition aux RF, une distance de séparation minimale de 20 mm doit être maintenue entre le corps de l’utilisateur et le combiné, y compris l’antenne.