

HUMITEMP®

INTERNET OF THINGS INTELLIGENT DEVICE FOR REMOTE
MONITORING

For LoRaWan™, Sigfox, and Wi-Fi Networks

User's Manual



Version control

The following table contains the record of changes per manual version.

Version	Date	Description
1.6	20/03/2023	Format change. Extensive revision and correction of content. Technical background information update.
1.7	24/06/2023	Version control implemented. Device image changed.

NOTICE

Read this manual before working with the product. For personal and system safety, and optimal product performance, make sure you thoroughly understand the contents before installing, using, or maintaining this product.

If you encounter a problem with your **Humitemp®**, review the configuration information to verify that your selections are consistent with your application: input configurations; chosen limits; etc. If the problem persists after checking the above, you can have technical assistance at (+57) 3176478281, Monday through Friday, 7:00 a.m. to 5:00 p.m. Eastern Standard Time. You can also write to solutions@omicroniot.com, specialized personnel will discuss your application case.

Please have the following information available:

- All Configuration Information.
- All Provided Manuals.
- Device ID and the Parts List provided with the equipment.

Contact Information

To reach the **Humitemp®** manufacturer for commercial information, refer to:

- Landline: +57 (604) 2328381
- Mobile: +57 (317)4365062
- comercial@omicroning.co

To reach the **Humitemp®** manufacturer for technical information, refer to

- Landline: +57 (604) 2328381
- Mobile: +57 (317)6478281
- solutions@omicroniot.com

Visit us at: <https://omicroniot.com/>

Warning notice standard

This manual contains notices that must be observed in order to ensure personal safety, prevent damage to properties, and guarantee proper installation, use, and maintenance of the equipment.

The notices referring to personal safety or the integrity of the device are highlighted in the manual by an alert symbol; notes regarding recommendations or complementary information to the topics covered in this manual have no safety alert symbol. The notices shown below are graded according to the previous definitions.

Refer to the safety messages indicated by this standard at the beginning of each section before interacting with the device or its components:

⚠ WARNING

Indicates observations that, if not followed, could cause serious personal injuries, or damages to the device. The information in these tables indicates the risks related to each of the topics covered in this manual.



⚠ CAUTION

Indications on the correct use of the equipment, useful to avoid improper operation.



NOTE:

Recommendations and clarifications to take into account in the different topics covered in the manual.

Contents

Section 1: Introduction	6
1.1 Product Recycling / Disposal	6
1.2 Storage and Transport	6
Section 2: Quick Start	7
2.1 Connect the external sensors	7
2.2 Power the device	7
2.3 Turn on the device	7
2.4 Send data wirelessly	8
2.4.1 Enter the Service Mode	8
2.4.2 Connect the device to a Wi-Fi® Network	9
2.5 Mount the device	10
Section 3: Configuration	12
3.1 Remote Configurator	12
3.1.1 Elements of the Remote Configurator	12
3.1.2 Use of the interface for remote configuration	13
3.2 Configure the device parameters manually	14
3.2.1 Review or modify the value of a parameter	14
Section 4: Configuration on Sigfox Backend	18
4.1 Configuration of Callbacks for Uplink messages	18
4.2 Configuring Callbacks for Downlink messages	20
Section 5: Configuration on Lorawan™ TTN	22
5.1 Configuring Callbacks for Uplink messages	22
5.1.1 Downlink API Key	24
5.2 Uplink payload formatters	26
Section 6: Centriomega® Remote Control and Monitoring Platform	29
6.1 Access the Centriomega® Remote Monitoring Platform	29
6.2 Reviewing historical data	30
6.3 Reviewing Devices, their Variables, and Configuration	31
6.4 Reviewing Alarms and Programmed Events	32
Section 7: Troubleshooting Guide	35
7.1 I cannot log in to the remote monitoring platform	35
7.2 The device displays erroneous measurements on its screen or on the monitoring platform	35
7.3 The display of the device does not show information	35
7.4 The device has stopped updating data on the monitoring platform	36
7.5 When trying to save the configuration with the remote configurator, I see the message: "You do not have permission to perform this configuration. It is recommended to check the device ID entered, or the type of device selected."	36
7.6 I can't see the device ID on its label	37

⚠ WARNING

Failure to follow safe installation guidelines could result in death or serious injuries.



- Make sure the Humitemp® is installed by qualified personnel and in accordance with the applicable practice code.
- Use the device only as specified in this manual. Failure to do so may impair the protection provided by it.
- Inappropriate or incorrect use of the product may result in hazards and application-specific malfunctioning; such as damage to system components, due to incorrect mounting or adjustments.
- Do not perform any services besides those covered in this manual, unless you are qualified.
- Any substitution of non-authorized parts or repair, other than exchanging the sensors is prohibited.
- Unauthorized changes to the product are strictly prohibited as they may unintentionally and unpredictably alter the performance and safety.
- Unauthorized changes that interfere with the integrity of the enclosure or mounting holes, such as making additional perforations, compromise the product integrity and safety.
Equipment ratings and certifications are no longer valid on any products that have been damaged or modified without the prior written permission of Omicron IoT Solutions. Any continued use of a product that has been damaged or modified without prior written authorization is at the customer's sole risk and expense.

Explosions could result in death or serious injuries.

- Verify that the operating environment of the device is consistent with its environmental specifications.
- **This device is not intended for use in flammable or combustible atmospheres.**

Section 1: Introduction

This reference manual provides detailed product-related information, installation, setup, and operation instructions for the Humitemp®. These devices have an internal sensor to measure the Ambient Temperature and Relative Humidity; as well as 2 ports for submersible temperature sensors, or for digital sensors that detect the opening of doors. The information collected by the devices is sent to the Centriomega® monitoring platform.

To follow this guide you will need:

- Humitemp®.
- AA batteries (not included)
- Micro USB power cable and 5V voltage adapter.
- A web-enabled device (PC, tablet, smartphone, etc).
- External sensors for the Humitemp® (optional).

This manual is designed for trained personnel. Read it entirely and carefully before installing and setting up the product.

⚠ WARNING

The procedures and instructions in this manual may require special precautions to ensure the safety of the personnel performing the operations. The information that raises potential safety issues is indicated by a warning symbol. Refer to the safety messages listed at the beginning of each section before performing an operation preceded by this symbol.



1.1 Product Recycling / Disposal

Recycling of device components and packaging should be taken into consideration and disposed of in accordance with local and national legislation/regulations.

1.2 Storage and Transport

The **Humitemp®** is protected by a special packaging during transport and is guaranteed to handle normal loads during transport.

Section 2: Quick Start

2.1 Connect the external sensors

1. Remove approximately 1.5 cm of insulation from the end of the wires of the external sensors to be used, to expose the inner wires. Also, strip approximately 5 mm from each inner wire.
2. Connect the external sensors to the device, according to the following indications:

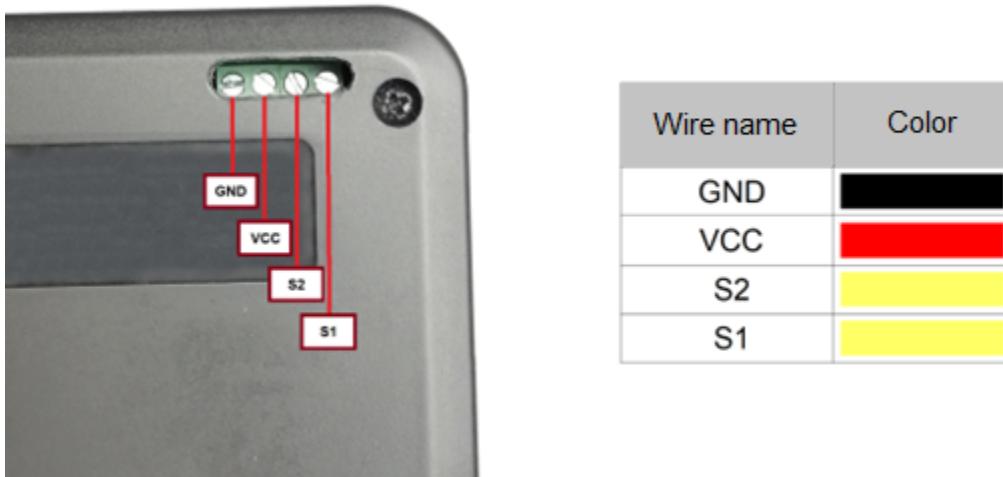


Figure 2-1 Pin-out of the Humitemp® sensor port

If you want to connect a sensor to the external port 1, connect its black, red, and yellow wires to GND, VCC, and S1, respectively. Similarly, connect GND, VCC, and S2 to the corresponding colored wires if you wish to connect a sensor to the external port 2.

3. Make sure that the connections made are tight; do not pull sharply on the connected wires, as this may damage the ports of the device.

2.2 Power the device

The **Humitemp®** is powered by **2 AA batteries** (not provided by the manufacturer) or a **MicroUSB power cable**. The batteries are inserted into the battery box at the back of the device. Check that the batteries are inserted correctly according to their polarity and the indications on the box.

2.3 Turn on the device

Once the batteries are charged, or the device is connected to the electrical network, the device will indicate on its display the firmware version it is using, and then it will present the measurements taken by its sensors (internal or external, if enabled); when this is achieved, **the device will be in Normal Operating Status**.

In case the device does not show information on its display, press the button (∇) for 2 seconds to turn it on. The device can also be turned off by pressing the (∇) button for 2 seconds.

2.4 Send data wirelessly

While the device is in Normal Operating State, it will proceed to periodically send the data measured by its enabled sensors (according to the minutes specified by the tPU parameter); via the Sigfox or LoRaWAN™ network (in case the device is not registered in the Sigfox Backend or LoRaWAN™ TTN platform, please refer to section 4 or 5, respectively), or via a Wi-Fi® network (to which you must connect the device following the steps in section 2.4.1 and 2.4.2); to the Centriomega® remote monitoring platform.

NOTE:

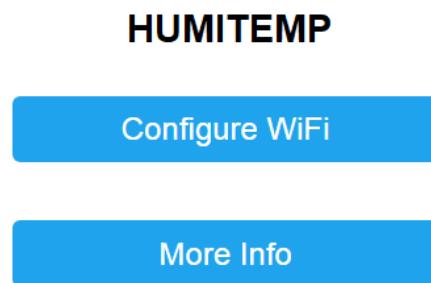
In order to be able to connect to a Wi-Fi® network, the device must have an internal communication module that allows it. In case you have not ordered it, you can request it to the manufacturer. Remember that contact information is provided at the beginning of this document.

2.4.1 Enter the Service Mode

While the device is on, you can force it to enter the Service Mode to configure aspects of the Wi-Fi® network you wish to connect to. **To enter the Service Mode, press the (▽) and (△) buttons simultaneously for 2 seconds.** The device will confirm the entry to the Service Mode by displaying the expression 'rEd' on its screen.

While being in the Service Mode, the Humitemp® device generates a temporary Wi-Fi® network using its built-in Wi-Fi® module, named "IoTDevice_ ", followed by the device ID (e.g., "IoTDevice_bcddc212345"). You will need to connect to that network using some device capable of browsing on the Internet (such as a Smartphone, Tablet, or PC).

Once connected to the network, you should access a page with the IP address: 192.168.4.1 (whose interface is shown in Figure 2-2). It is possible to access the indicated page through any internet browser; there you will find a menu with the buttons "Configure WiFi", and "More Info".



Omicron- IoT Solutions

Figure 2-2 Humitemp® General Configuration Page

To exit the Service Mode, press the (▽) and (△) buttons simultaneously until 'rEd' disappears from the display.

NOTE:

Exit the Service Mode only after performing or reviewing the desired settings on the web interface with IP: 192.168.4.1.

2.4.2 Connect the device to a Wi-Fi® Network

To configure the credentials (name and password) of the network that will provide internet access to the **Humitemp®** device, proceed as follows:

1. **On the General Setup Page (Figure 2-2), press the Configure Wi-Fi button** to go to a page where you can see a scan of the Wi-Fi® networks detected by the Humitemp®, two fields to enter data, and two buttons (Save and Scan).

The page that loads after selecting "Configure Wi-Fi", on the Home Page, is presented in the following image:

HUMITEMP

OMICRON1	100%
ConsulsarSAS	94%
MARIAPRECIADO	40%
GUTIERREZ	36%
Agencia De Seguros	28%
HP-Print-16-LaserJet 1102	26%
OMICRON1	
password	

[save](#)

[Scan](#)

Omicron- IoT Solutions

Figure 2-3 Humitemp® Wi-Fi® configuration page

2. In the fields at the bottom of the Wi-Fi® setup page (Figure 2-3), **enter the credentials (name and password) of the network to which you wish to connect the Humitemp®**; then press "Save". If you want to connect the device to an open network, you do not need to enter a password.

After pressing the "Save" button, you will see the following page with the message: "Trying to connect your device to the network... Wait 30 seconds and press the button to verify if the WiFi connection was successful".

HUMITEMP CONFIG.

Trying to connect your Device to network...
Wait for 30 seconds and press to view if
WiFi connection was correct

WiFi Results

Omicron IoT Solutions

Figure 2-4 Waiting page for the connection to the Wi-Fi® network

If the entered credentials are not correct, after pressing the "WiFi Results" button, the following page will appear:

HUMITEMP CONFIG.

!! ERROR: Check Your SSID And Password !!

Back to Home

Figure 2-5 Wi-Fi® configuration page invalid

Otherwise, you will see:

HUMITEMP CONFIG.

!! CORRECT !!
Settings Saved

Back to Home

Figure 2-6 Wi-Fi® configuration page correct

After this, if desired, you can exit the Service Mode as described in 2.4.1.

2.5 Mount the device

1. Attach the device to a flat vertical surface (e.g. a wall). To do this, use the wall mounting accessories supplied with the device.

It is indispensable to ensure that the device is within the coverage area of the wireless network you are using, so try to place it in a high location where its wireless transmissions will not be obstructed (away from metal surfaces or objects, and away from sturdy objects such as walls or shelves). High locations may also make it easier to check its display.

2. Use the cable clamp and strap supplied with the instrument to secure the external sensor cables as shown in the picture below:



Figure 2-7 Humitemp® wall mounting.

Securing the cables this way prevents the manipulation of the sensors from generating tension or dangerous bending near the connector, which minimizes the risk of them coming out or being damaged; it also allows manipulation of the device to change its batteries or sensors, minimizing the risk of damaging the connections.

3. Install the external sensors where they correspond.

Section 3: Configuration

3.1 Remote Configurator

Centriomega® platform users have access to a Dashboard that allows them to set commands to remotely configure their devices (to find it, login to the remote monitoring platform following the steps described in Section 6.1, and look for the Dashboard with the name "Remote Configurator", following the steps described in Section 6.2).

The "Remote Configurator" Dashboard presents to the users a summary of the configuration options available for each type of the Omicron IoT solutions devices, and only requires them to choose a parameter to configure, after indicating the device model, and the elements or general aspects of the device to be configured. The elements it contains are:

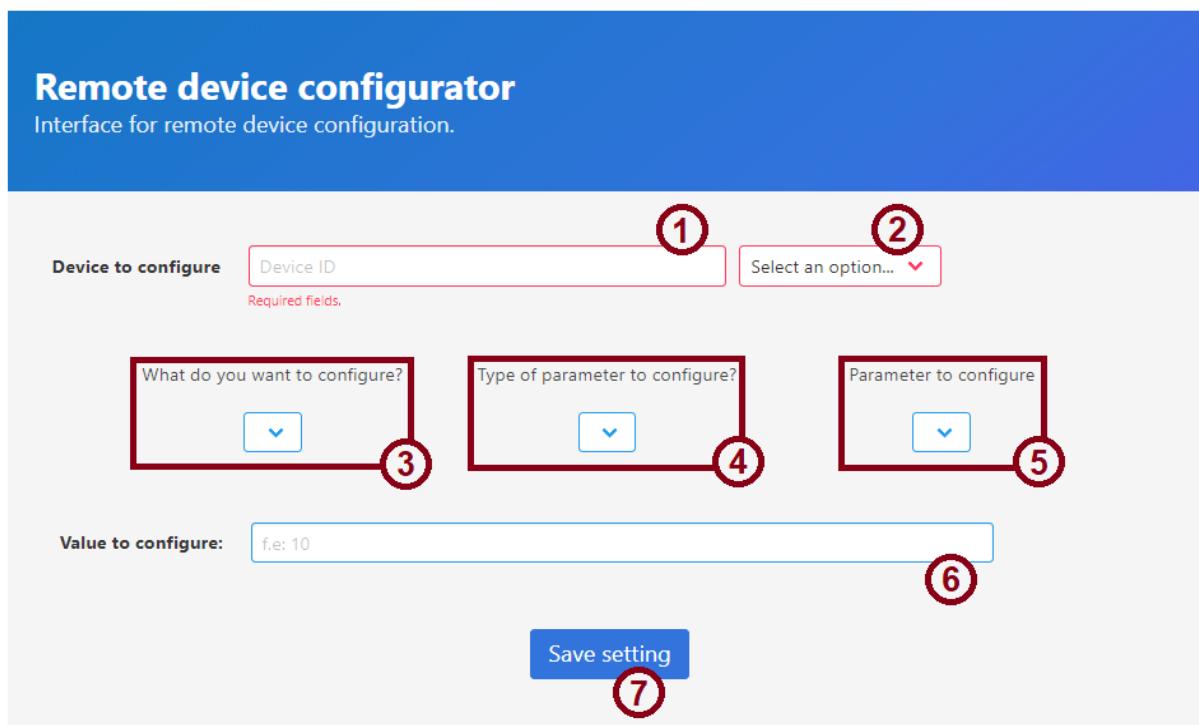


Figure 3-1 Elements of the Remote Configurator

3.1.1 Elements of the Remote Configurator

1. Field for the ID of the device to be configured

In this field, users must specify the UID of the device they wish to configure remotely. This UID is printed on the labels of the devices; or it can be checked in the Device information stored by the platform (to do this, refer to section 7.6).

2. Device type selector to be configured

Allows you to select the model of the device to be configured.

3. General aspect selector to be configured

Here you must select the general aspect of the device to be configured.

4. Parameter type selector to be configured

This list allows you to specify the type of parameter to be configured for the general

aspect of the device, chosen with selector 3.

5. Parameter to be configured selector

Finally, this list shows the parameters available for configuration, as chosen in lists 3 and 4.

6. Field for the value to be configured

In this field the user must specify the desired value for the parameter to be configured, following the instructions that the interface presents as a text over this field when the cursor is placed there.

7. Save command button

Once the user has chosen the parameter to be configured, and has specified a configuration value, the user must save the command in the platform so that the device will download it once it is ready to do so.

3.1.2 Use of the interface for remote configuration

To configure a parameter using the Remote Configurator, follow the steps below:

1. Enter the identification information of the device to be configured in fields 1 and 2.
2. Select the parameter to be configured using selection lists 3, 4, and 5.
3. Enter the value you wish to assign to the configured parameter in field 6, **following the indications that the interface presents** as a text on this field, after choosing the parameter to be configured.
4. Having selected the parameter to be configured, and having entered the value with which you wish to configure it, **press the 'Save Setting' button**. You will then be prompted to confirm the action on a pop-up window; and in the case that the configuration is successfully saved, the page will display a message indicating this below the button.

Pressing the button will not clear the entered or selected information, in order to facilitate configuring another device in the same way.

Based on the above, it can be concluded that in the case of selecting and entering in the Remote Configurator, for what is shown in the following image (as an example), the Humitemp 44fa0e device will set the publishing time of its internal sensors to 10 minutes:

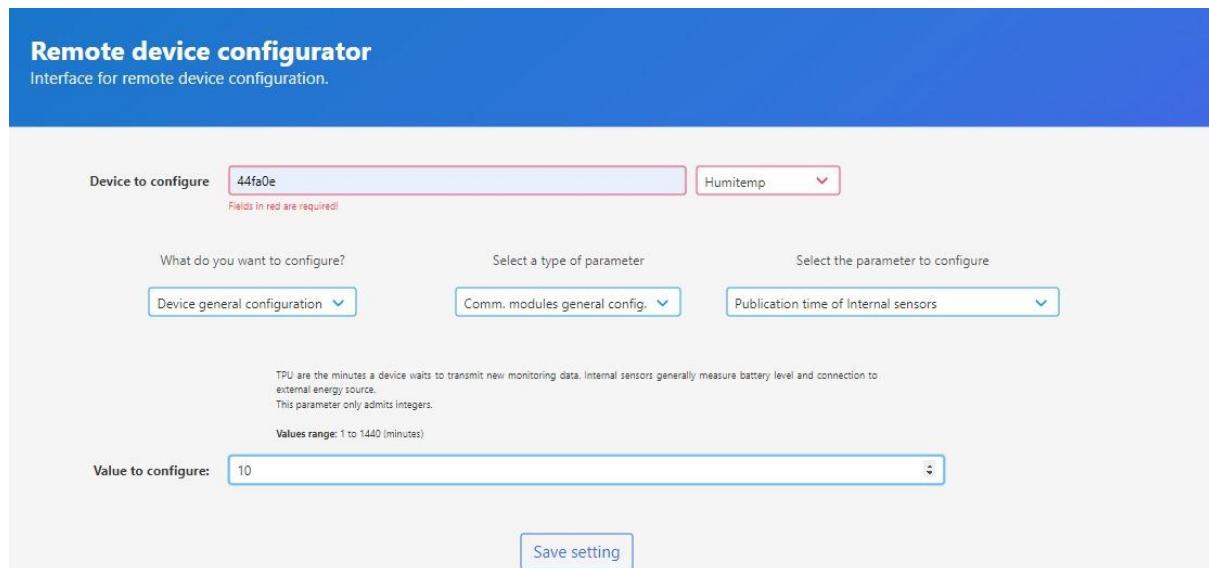


Figure 3-2 Example of the configuration made with the Remote Configurator

3.2 Configure the device parameters manually

If you do not want to use the Remote Configurator to configure the parameters of a **Humitemp®**, **you can manually access the list of configurable parameters of the device**. To do this, perform the following steps:

1. While the device is in normal operating state, indicating the measurements of its enabled sensors on its display, **press the (Δ) button for 2 seconds**.
2. Then, the expression CLA will briefly appear on the display and then the number 0; at this point you can change the number displayed with the (▽) and (△) buttons; **you should get the value to 251** (it is recommended to use the (▽) button), **and then wait a couple of seconds** to be able to access the list of configurable parameters.
3. If you performed the previous step correctly, **you should briefly see the expression Ot on the screen, and then the label of one of the configurable parameters** (if you did not perform step 2 correctly, you will see Err on the screen, and then the device will display the measurements of your enabled sensors).

When you accomplish this, you can move through the list of configurable parameters using the (▽) and (△) buttons. To review or change the value of any parameter, follow section 3.2.1.

The complete list of configurable parameters is presented in Table 3-1. **Note that after 4 seconds of inactivity, the device stops displaying the list of configurable parameters**, and returns to display the measurements of its enabled sensors on its screen; so to access the parameters you must perform the above steps again.

3.2.1 Review or modify the value of a parameter

1. **To modify a specific parameter, you must first view its label on the display.** Remember that you can navigate through the list of configurable parameters with the (▽) and (△) buttons.

2. When you see the label of the parameter of interest, **access the parameter value by pressing (▽) for 2 seconds.**
3. You will then be able to see the value of the parameter in question on the display. **You can change this value with the (▽) and (△) buttons.** When the parameter value has the value you want, wait a couple of seconds, then you will see again on the display the label of the parameter whose value you set or revised: this means that the indicated value was set, and you can again browse through the list of configurable parameters.

Remember that after 4 seconds of inactivity, the device stops displaying the list of configurable parameters, and returns to displaying on its screen the measurements of its enabled sensors.

The complete list of configurable parameters is presented below:

Table 3-1 Humitemp® configurable parameters

Parameter Label	Parameter Name	Description
t0.b	Ambient Temp. lower limit.	If the measurement of the internal Ambient Temp. sensor is lower than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
t0.A	Ambient Temp. upper limit.	If the measurement of the internal Ambient Temp. sensor is higher than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
H0.b	Ambient Hum. lower limit.	If the measurement of the internal Ambient Hum. sensor is lower than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
H0.A	Ambient Hum. upper limit.	If the measurement of the internal Ambient Hum. sensor is higher than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
t1.b	Sensor Temp. 1 lower limit..	If the measurement of the external Temp. sensor 1 is lower than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
t1.A	Sensor Temp. 1 upper limit.	If the measurement of the external Temp. sensor 1 is higher than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
t2.b	Sensor temp. 2 lower limit.	If the measurement of the external Temp. sensor 2 is lower than this value, the audible alarm of the device is activated (after the delay indicated by SIL).
t2.A	Sensor Temp. 2 upper limit.	If the measurement of the external Temp. sensor 2 is higher than this value, the audible alarm of the device is activated (after the delay indicated by SIL).

At.0	Ambient Temp. measurement adjustment.	This value will be added to the measurements of the internal Ambient Temp. sensor, to correct any offset (it can take negative values to subtract).
AH.0	Ambient humidity measurement adjustment.	This value will be added to the measurements of the internal Ambient Hum. sensor, to correct any offset (can take negative values for subtraction).
At.1	Sensor Temp. 1 measurement adjustment.	This value will be added to the measurements of the external Temp. sensor 1, to correct any offset (can take negative values for subtraction).
At.2	Sensor Temp. 2 measurement adjustment.	This value will be added to the measurements of the external Temp. sensor 2, to correct any offset (can take negative values for subtraction).
EHr	Enable/Disable Ambient Temp. and Humidity sensor.	0: Disable internal Ambient Temp. and Hum. sensor. 1: Enable internal ambient Temp. and Hum. sensor. (If you disable the sensor, you will not see its measurements on the device screen, nor on the platform).
Et1	Enable/Disable Temp. sensor 1.	0: Disable external sensor on port 1. 1: Enable external Temp. sensor 1. (If you disable the sensor, you will not see your measurements on the device screen, nor on the platform).
Et2	Enable/Disable Temp. sensor 2.	0: Disable external sensor on port 2. 1: Enable external Temp. sensor 2. (If you disable the sensor, you will not see your measurements on the device screen, nor on the platform).
ALn	Audible alarm level	Duration of the audible alarm sound: 0, disables the audible alarm (and also the SIL parameter); 10, makes it sound for up to 2 seconds. Intermediate values make it sound proportionally. Note that the alarm is repeated every 10 seconds, with a duration of 'ALn' seconds, until it is manually turned off or until the variable in alarm returns to its normal range. Keep in mind that a higher level of audible alarm means a faster discharge of the batteries.

SIL	Audible alarm start delay	Minutes the device waits for the alarm to sound after detecting a measurement outside the admissible range.
tPU	Publication time	Minutes that the device waits to publish (or store in its internal memory for publication, if the parameter nSE is different from 1) new measurements on the Centriomega platform.
nSE	Multiplication factor	<p>Number that will multiply the Time of Publication, and that corresponds to the number of measurements to send in each publication.</p> <p>Example: If you set a Publishing Time equal to 2 minutes and nSE equal to 3, the device will send 3 measurements every 6 minutes.</p>
CON	Connectivity type	<p>Wireless connectivity technology used by the device:</p> <ul style="list-style-type: none"> 0: None. 1: Sigfox. 2: Wi-Fi. 3: LoRaWAN. <p>(You will only find the ZON parameter available if you choose Connectivity type: 1).</p>
ZON	Sigfox Zone	<p>Zone of the Sigfox network in which the device operates:</p> <ul style="list-style-type: none"> 1: Zone 1 (Europe, Oman, South Africa). 2: Zone 2 (USA, Mexico, Brazil). 3: Zone 3 (Japan). 4: Zone 4 (Australia, New Zealand, Singapore, Taiwan, Hong Kong, Colombia, Argentina).
GrA	Temp. unit of measure	<p>Unit of measurement of temperature values:</p> <ul style="list-style-type: none"> 0: Celsius. 1: Fahrenheit.

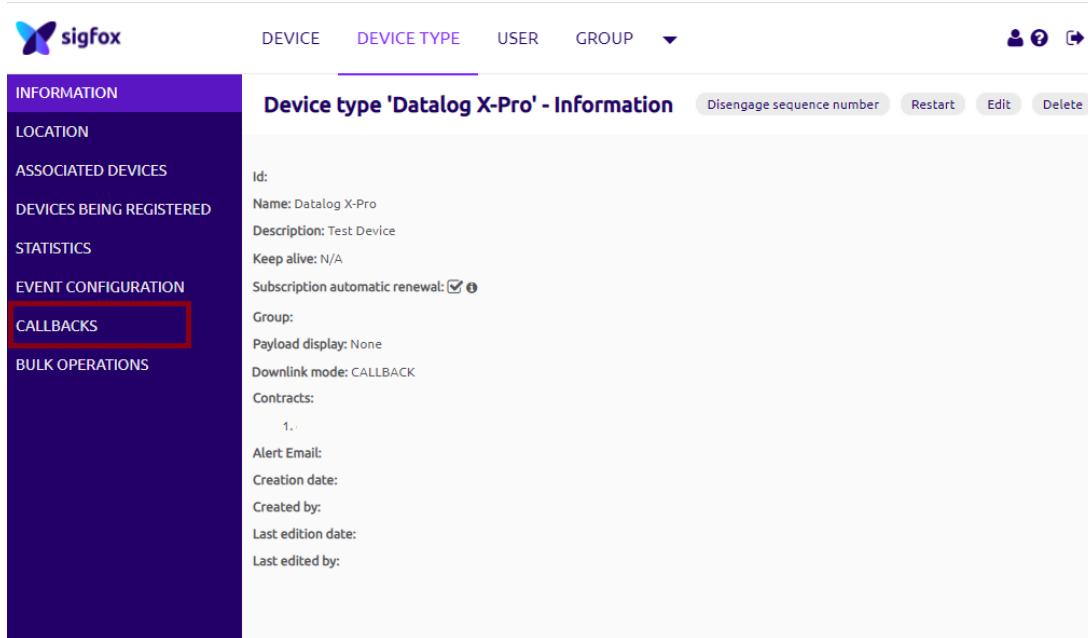
Section 4: Configuration on Sigfox Backend

If it is desired that the **Humitemp** devices work with the Omicron IoT Solutions monitoring platform, using the Sigfox telecommunications network, the user can enable bidirectional communication with the platform by associating Callbacks to the Uplink and Downlink messages of the devices on the Sigfox Backend.

4.1 Configuration of Callbacks for Uplink messages

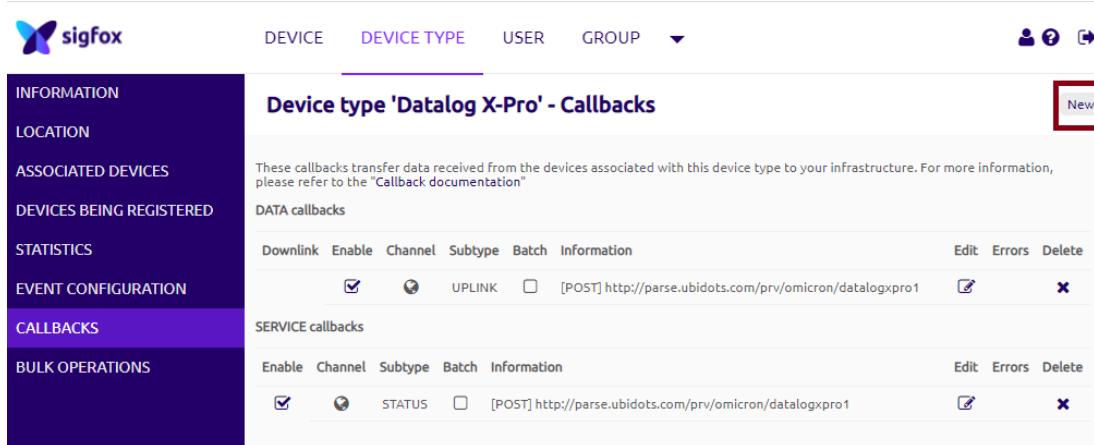
Perform the following steps:

1. On the Sigfox backend, enter the device type to which you have associated the Sigfox modules used by your Humitemp devices, and select CALLBACKS from the menu located on the left side.



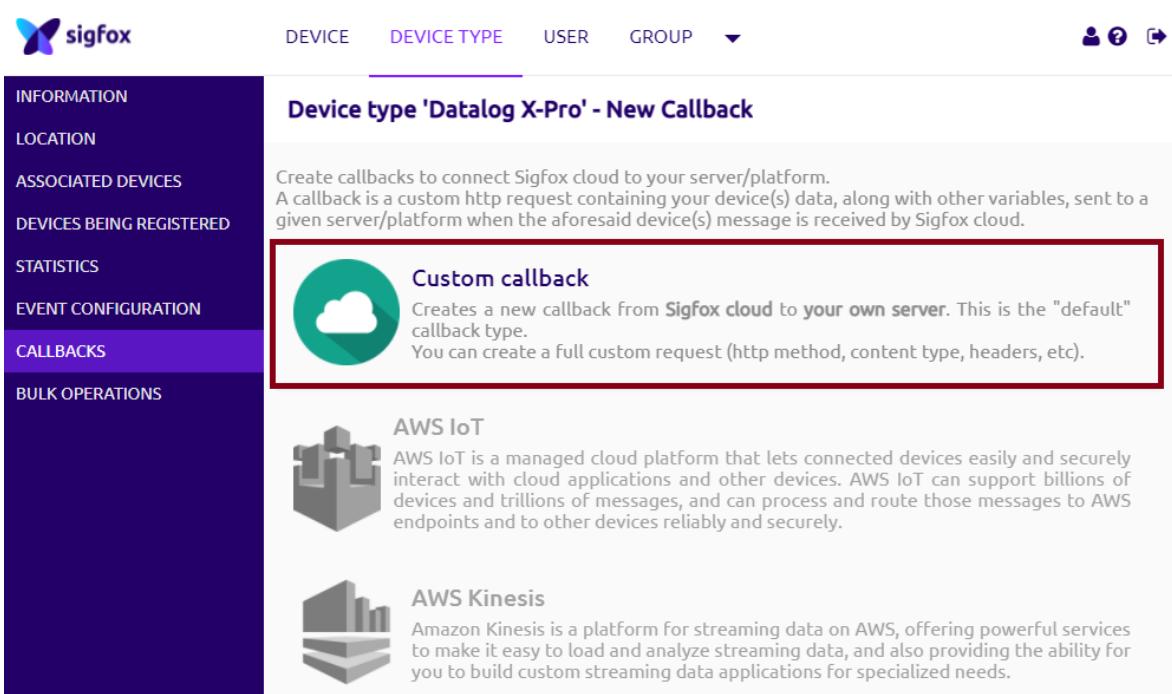
The screenshot shows the 'Device type 'Datalog X-Pro' - Information' page. The sidebar on the left has a 'CALLBACKS' option highlighted with a red box. The main content area displays device details: Name: Datalog X-Pro, Description: Test Device, Keep alive: N/A, Subscription automatic renewal: checked, Group: None, Payload display: None, Downlink mode: CALLBACK, Contracts: 1, Alert Email: None, Creation date: None, Created by: None, Last edition date: None, Last edited by: None. At the top right, there are buttons for Disengage sequence number, Restart, Edit, and Delete.

2. Create a new Callback by selecting the option "New".



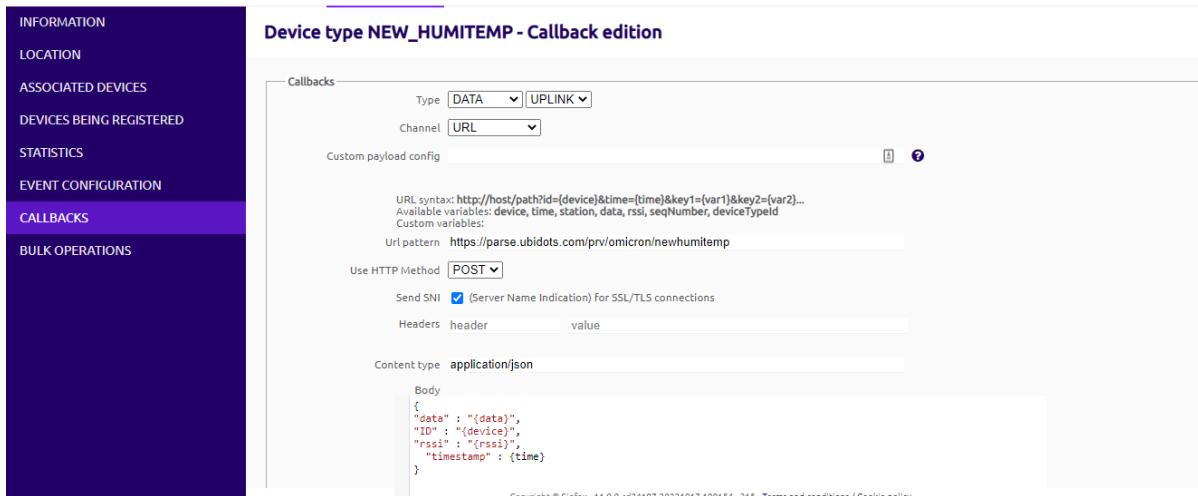
The screenshot shows the 'Device type 'Datalog X-Pro' - Callbacks' page. The sidebar on the left has a 'CALLBACKS' option highlighted with a red box. The main content area contains a note about callbacks and a link to 'Callback documentation'. It lists two types of callbacks: DATA callbacks and SERVICE callbacks. Under DATA callbacks, there is one entry: Enable: checked, Channel: UPLINK, Subtype: [POST] http://parse.ubidots.com/prv/omicron/datalogxpro1. Under SERVICE callbacks, there is one entry: Enable: checked, Channel: STATUS, Subtype: [POST] http://parse.ubidots.com/prv/omicron/datalogxpro1. At the top right, there is a 'New' button.

3. Select "Custom Callback".



The screenshot shows the Sigfox Device Type 'Datalog X-Pro' configuration page. The left sidebar has a purple background and lists: INFORMATION, LOCATION, ASSOCIATED DEVICES, DEVICES BEING REGISTERED, STATISTICS, EVENT CONFIGURATION, CALLBACKS (which is highlighted in purple), and BULK OPERATIONS. The main content area has a white background and displays the title 'Device type 'Datalog X-Pro' - New Callback'. Below it, a message says: 'Create callbacks to connect Sigfox cloud to your server/platform. A callback is a custom http request containing your device(s) data, along with other variables, sent to a given server/platform when the aforesaid device(s) message is received by Sigfox cloud.' There are three options listed: 'Custom callback' (with a green cloud icon), 'AWS IoT' (with a grey building icon), and 'AWS Kinesis' (with a grey bar chart icon). The 'Custom callback' option is highlighted with a red border.

4. Configure the Callback as shown in the following image, and then press OK.



The screenshot shows the Sigfox Device Type 'NEW_HUMITEMP' configuration page. The left sidebar has a purple background and lists: INFORMATION, LOCATION, ASSOCIATED DEVICES, DEVICES BEING REGISTERED, STATISTICS, EVENT CONFIGURATION, CALLBACKS (which is highlighted in purple), and BULK OPERATIONS. The main content area has a white background and displays the title 'Device type NEW_HUMITEMP - Callback edition'. It shows a 'Callbacks' section with the following configuration: Type: DATA UPLINK, Channel: URL, URL pattern: <https://parse.ubidots.com/prv/omicron/newhumitemp>, Use HTTP Method: POST, Headers: header value, Content type: application/json, Body: { "data": "{data}", "ID": "{device}", "rssi": "{rssi}", "timestamp": "{time}" }. At the bottom, there is a small note: 'Copyright © Sigfox - 11 Q Derv74107-00271017 100154 - 315 - Terms and conditions / Cookies policy'.

- Use the URL pattern: <https://parse.ubidots.com/prv/omicron/newhumitemp>
- Use the body:

```
{
  "data": "{data}",
  "ID": "{device}",
  "rssi": "{rssi}",
  "timestamp": "{time}"
}
```

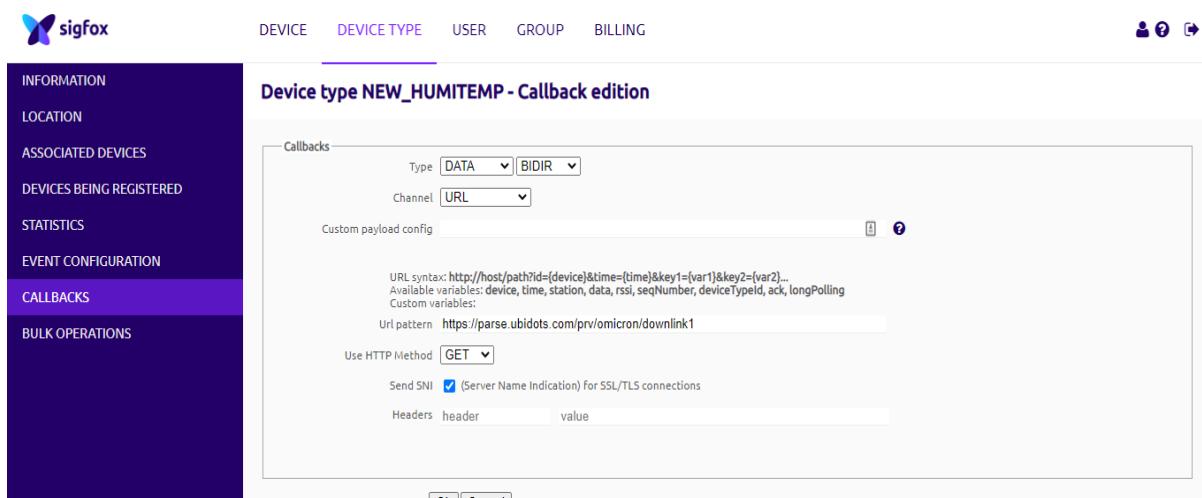
5. Then, in the Callbacks section of the edited device type, you will see a Callback like the following one:



Downlink	Enable	Channel	Subtype	Batch	Information	Edit	Errors	Delete
<input checked="" type="checkbox"/>	<input type="radio"/>	UPLINK	<input type="checkbox"/>	[POST]	https://parse.ubidots.com/prv/omicron/newhumitemp			

4.2 Configuring Callbacks for Downlink messages

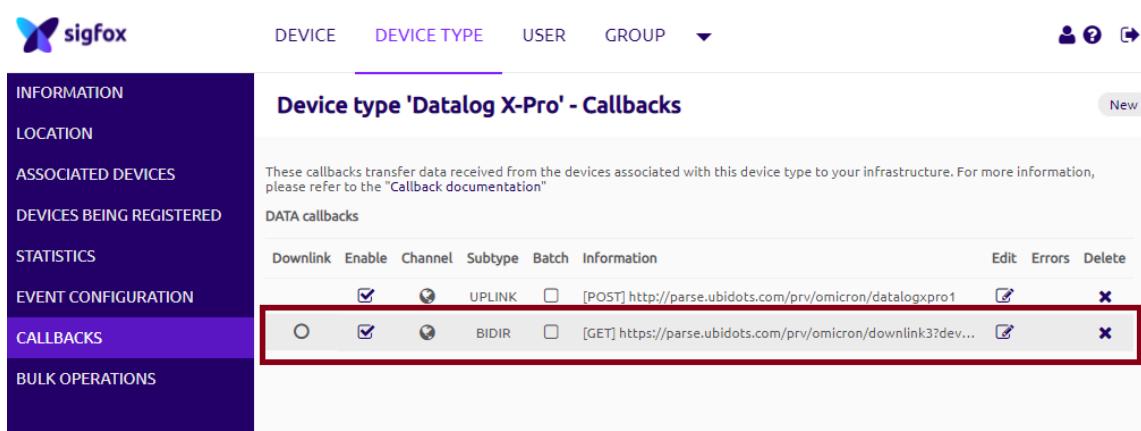
1. Follow steps 1 to 3 of section 4.1, then, configure the new Custom Callback as the following one, and then press "OK":



Type	DATA	BIDIR
Channel	URL	
Custom payload config		
URL syntax: http://host/path?id={device}&time={time}&key1={var1}&key2={var2}... Available variables: device, time, station, data, rssi, seqNumber, deviceTypeId, ack, longPolling Custom variables:		
Url pattern https://parse.ubidots.com/prv/omicron/downlink1		
Use HTTP Method GET		
Send SNI <input checked="" type="checkbox"/> (Server Name Indication) for SSL/TLS connections		
Headers header value		

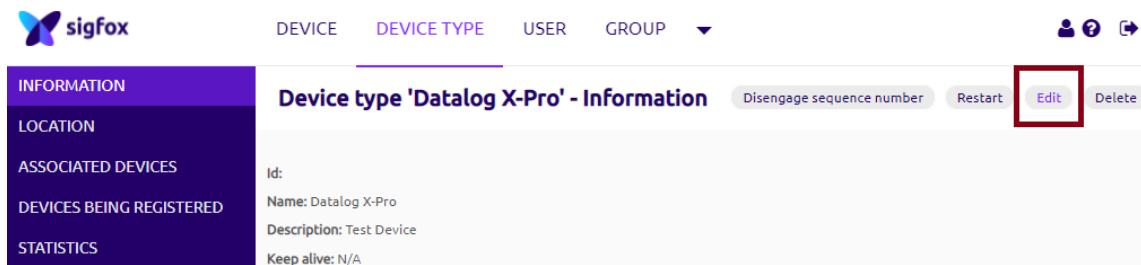
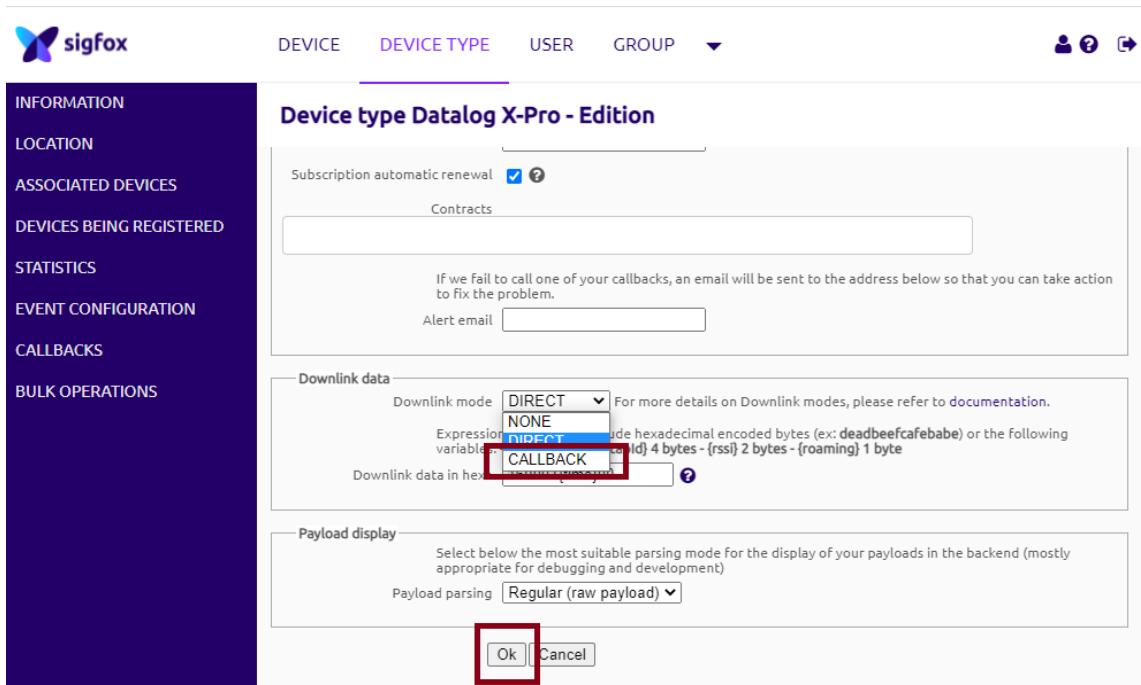
- Type DATA: BIDIR
- Channel: URL
- Use HTTP Method: GET
- Use the URL pattern:
<https://parse.ubidots.com/prv/omicron/downlink1>

2. Then, in the Callbacks section of the edited device type, you will see a new Callback of type BIDIR like the following one:

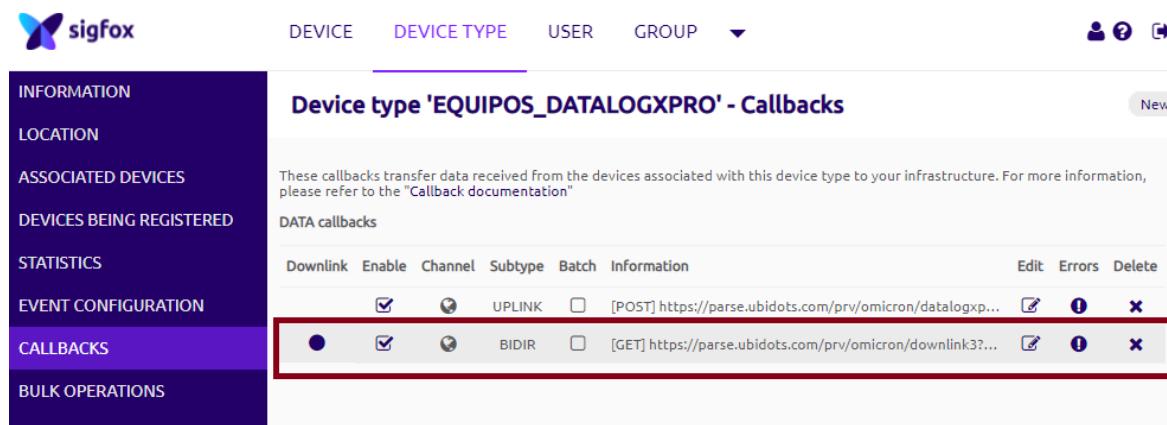


Downlink	Enable	Channel	Subtype	Batch	Information	Edit	Errors	Delete
<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="radio"/>	BIDIR	<input type="checkbox"/>	[POST] http://parse.ubidots.com/prv/omicron/datalogxpro1			

3. You will notice that this Callback is accompanied by an unfilled circle in its Downlink category. This means that the Callback has not been manually selected to handle Downlink messages of the device type. Before making this selection, check the following:
4. Go to the INFORMATION section of the device type, and edit the Downlink Data option to assign the value CALLBACK. Finally press "OK".

5. Now you can select the new BIDIR Callback available as a Callback to handle Downlink messages in the CALLBACKS section of the edited device type, by clicking on the unfilled circle (after selecting it, the circle will be filled):



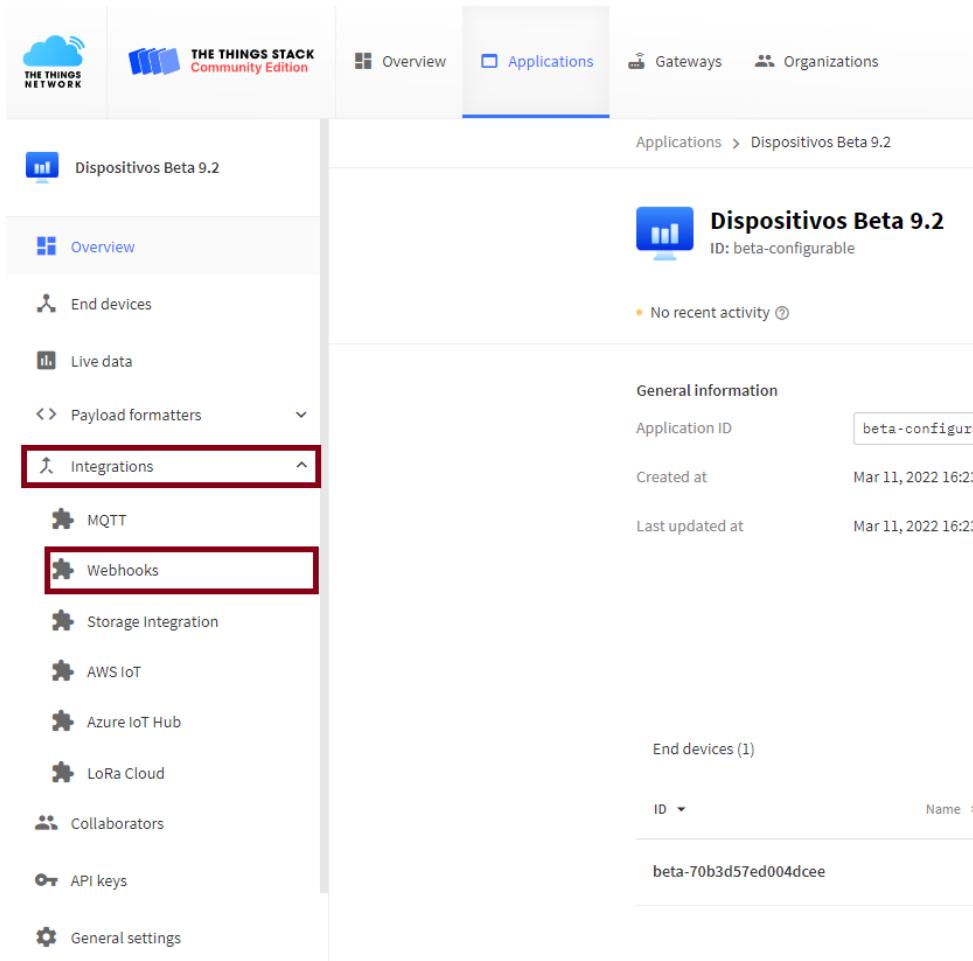
Section 5: Configuration on Lorawan™ TTN

If it is desired that **Humitemp** devices work with the Omicron IoT Solutions monitoring platform, using the LoRaWAN™ telecommunications network, the user can enable bidirectional communication with the platform by associating Callbacks to the Uplink and Downlink messages of the devices in **The Things Network (TTN)** platform.

5.1 Configuring Callbacks for Uplink messages

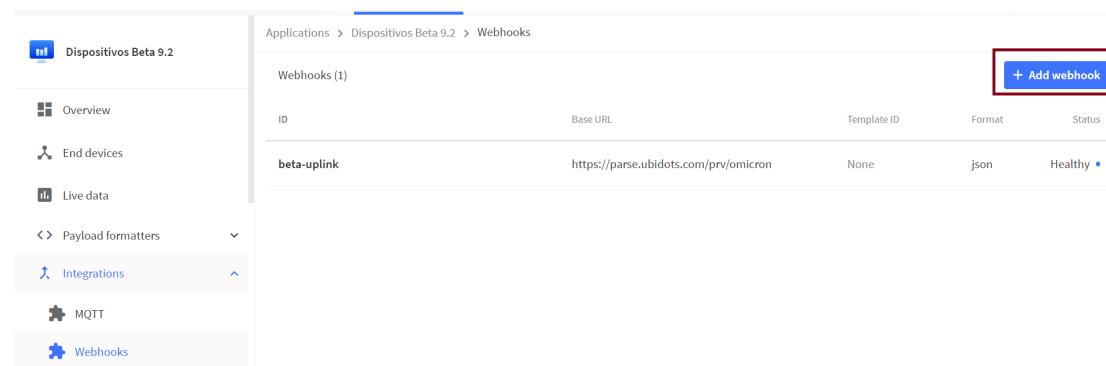
Perform the following steps:

1. In The Things Network, log in to the application to which you have associated the LoRaWAN™ modules used by your **Humitemp** devices, and select "Webhooks", displaying the Integrations menu located on the left side.



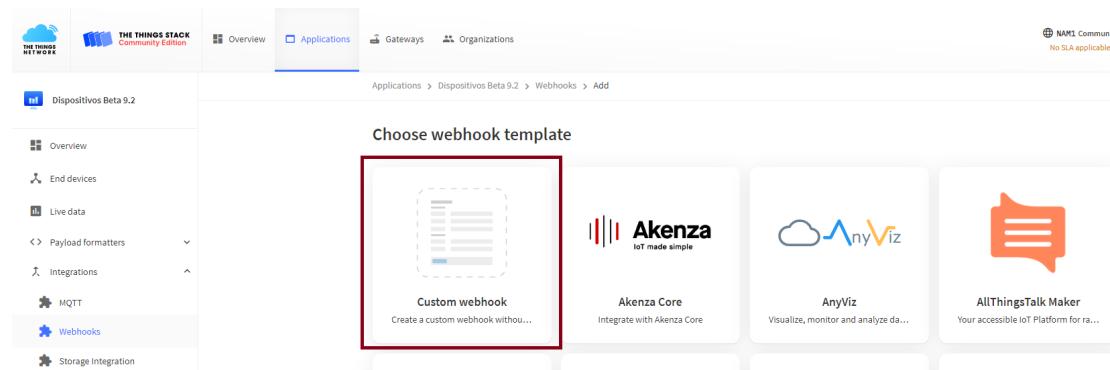
The screenshot shows the 'Applications' section of the The Things Network web interface. On the left, there's a sidebar with various menu items: Overview, Applications (which is selected and highlighted in blue), Gateways, Organizations, Dispositivos Beta 9.2 (selected), Overview, End devices, Live data, Payload formatters (with 'Integrations' expanded), Integrations (highlighted with a red box), MQTT, Webhooks (highlighted with a red box), Storage Integration, AWS IoT, Azure IoT Hub, LoRa Cloud, Collaborators, API keys, and General settings. The main content area shows the 'Dispositivos Beta 9.2' application details: Application ID (beta-configurable), Created at (Mar 11, 2022 16:23), Last updated at (Mar 11, 2022 16:23). Below this, there's a table for 'End devices (1)' with one entry: ID (beta-70b3d57ed004dcee) and Name (beta-70b3d57ed004dcee).

2. Create a new Webhook by selecting the option "Add Webhooks".



The screenshot shows the OMICRON IoT Solutions platform interface. On the left, there's a sidebar with various options like Overview, End devices, Live data, Payload formatters, Integrations (MQTT, Webhooks), and Storage integration. The main area shows the 'Webhooks' section under 'Dispositivos Beta 9.2'. It lists one webhook named 'beta-uplink' with the base URL 'https://parse.ubidots.com/prv/omicron'. There's a red box around the '+ Add webhook' button.

3. Then select "Custom Webhook".



The screenshot shows the THE THINGS STACK Community Edition interface. On the left, there's a sidebar with options like Overview, End devices, Live data, Payload formatters, Integrations (MQTT, Webhooks), and Storage integration. The main area shows the 'Choose webhook template' screen. It lists several options: 'Custom webhook' (selected and highlighted with a red box), 'Akenza Core', 'AnyViz', and 'AllThingsTalk Maker'. The 'Custom webhook' card says 'Create a custom webhook without...'. There's a red box around the 'Custom webhook' card.

4. Configure the Webhook as shown in the following image, and then press "Save changes".

General settings

Webhook ID *
xpro2-sji-ubidots

Webhook format *
JSON

Base URL *
https://parse.ubidots.com/prv/omicron

Downlink API key
.....
The API key will be provided to the endpoint using the "X-Downlink-Apikey" header

Request authentication ⓘ
 Use basic access authentication (basic auth)

Additional headers
+ Add header entry

Filter event data ⓘ
+ Add filter path

Enabled event types

For each enabled event type an optional path can be defined which will be appended to the base URL

Uplink message /uplink-lora-xpros-generico

An uplink message is received by the application

- **Webhook ID:** Name that the user wants to assign
- **Webhook format:** JSON
- **Base URL:** Base URL chosen by the user. In the case of the Omicron IoT Solutions monitoring platform: <https://parse.ubidots.com/>
- **Downlink API key:** See section 5.1.1
- **Uplink Message:** Enable and specify the following URL plugin: [prv/omicron/uplink-lora-humitemps-generico](#)

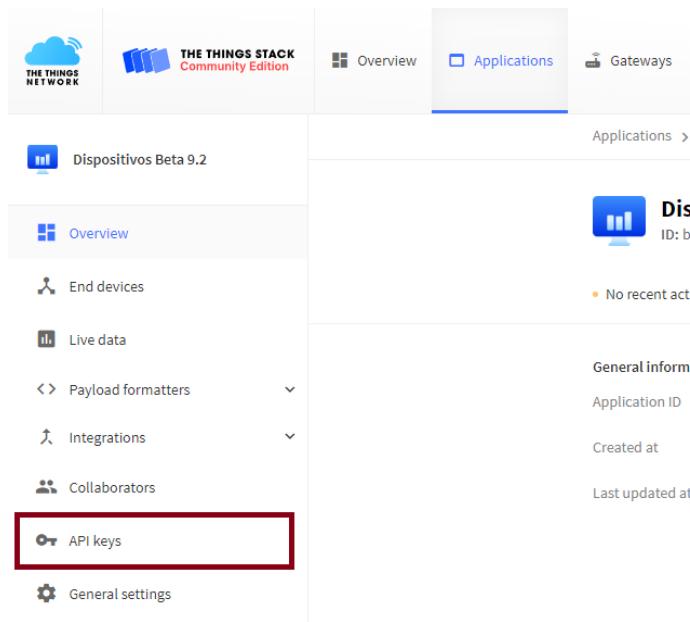
5. Then, in the webhooks section, you will see an image like the following one:

Webhooks (1)					+ Add webhook
ID	Base URL	Template ID	Format	Status	
beta-uplink	https://parse.ubidots.com/prv/omicron	None	json	Healthy •	

5.1.1 Downlink API Key

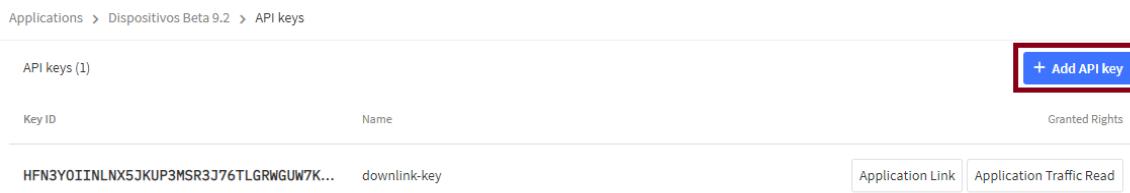
To obtain this parameter follow the steps below.

1. In TTN, enter the application to which you have associated the LoRaWAN™ modules used by your **Humitemp** devices, and select “API Keys”



The screenshot shows the 'Applications' tab selected in the top navigation bar. Below it, a list of applications is shown, with 'Dispositivos Beta 9.2' selected. On the left, a sidebar lists 'Overview', 'End devices', 'Live data', 'Payload formatters', 'Integrations', 'Collaborators', and 'API keys'. The 'API keys' option is highlighted with a red box. To the right, detailed information about the selected application is displayed, including its ID (b), no recent activity, general information, application ID, creation date, and last update date.

2. Select the “Add API Key” option



The screenshot shows the 'API keys' page for the 'Dispositivos Beta 9.2' application. It displays a table with one existing API key entry: 'HFN3Y0IINLNX5JKUP3MSR3J76TLGRWGUW7K...' with the name 'downlink-key'. The 'Granted Rights' column shows 'Application Link' and 'Application Traffic Read'. A red box highlights the '+ Add API key' button at the top right of the page.

3. Configure the Webhook as shown in the following image, and then press "Create API key".

Add API key

Name

Rights *

 Grant all current and future rights Grant individual rights Select all Delete application View devices in application View device keys in application Create devices in application Edit device keys in application View application information Link as Application to a Network Server for traffic exchange, i.e. read uplink and write downlink

This implicitly includes the rights to view application information, read application traffic and write downlinks

 View and edit application API keys Edit basic application settings View and edit application collaborators View and edit application packages and associations Write downlink application traffic Read application traffic (uplink and downlink) Write uplink application traffic

4. The following window will appear, copy the API key, because after closing it it will never be shown again, and then press "I have copied the key".

Please copy newly created API key

You won't be able to view the key afterward

Granted rights

- ✓ Link as Application to a Network Server for traffic exchange, i.e. read uplink and write downlink
- ✓ Read application traffic (uplink and downlink)

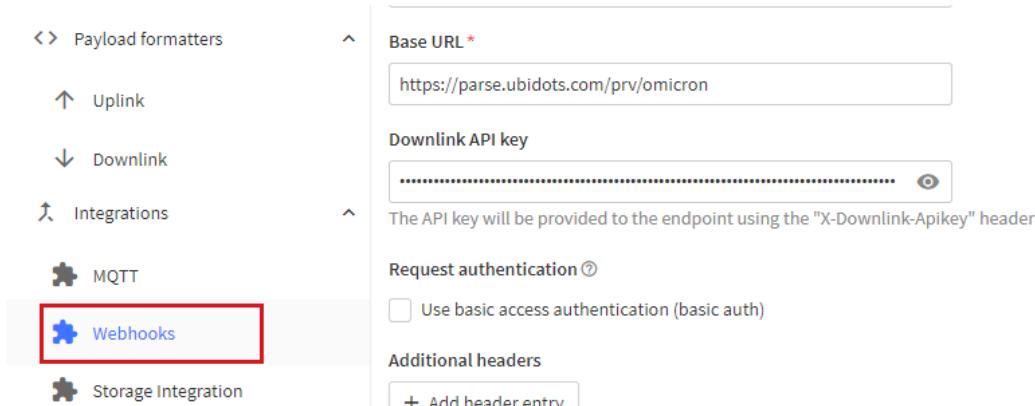
Your API key has been created successfully. Note: After closing this window, the value of the key secret will not be accessible anymore. Make sure to copy and store it in a safe place now.

API key

.....
Copy
Eye

✓ I have copied the key

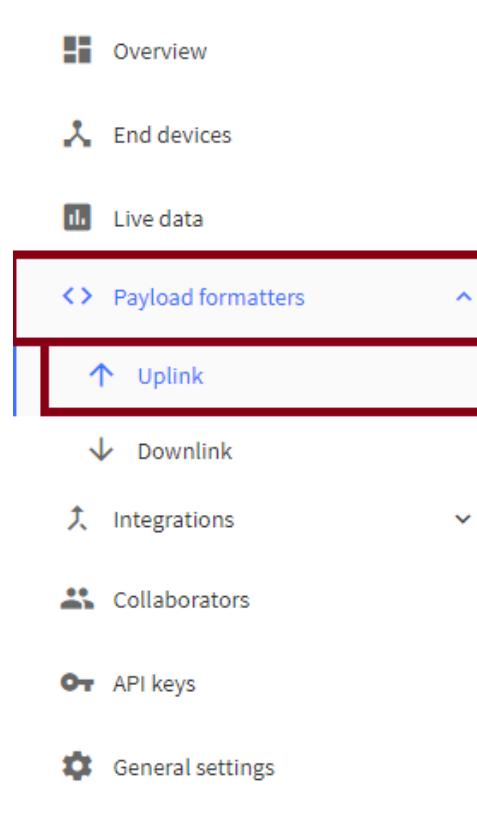
5. Then edit and copy this API key in your Webhook: "Downlink API Key".



The screenshot shows the 'Payload formatters' configuration for 'Uplink'. On the left, there's a sidebar with 'Payload formatters' expanded, showing 'Uplink', 'Downlink', 'Integrations' (with 'MQTT' and 'Webhooks' under it, where 'Webhooks' is highlighted with a red box), and 'Storage Integration'. On the right, there are fields for 'Base URL *' (set to 'https://parse.ubidots.com/prv/omicron') and 'Downlink API key' (a masked input field). Below these, there's a note: 'The API key will be provided to the endpoint using the "X-Downlink-Apikey" header'. Under 'Request authentication', there's a checkbox for 'Use basic access authentication (basic auth)' which is unchecked. At the bottom, there's a section for 'Additional headers' with a '+ Add header entry' button.

5.2 Uplink payload formatters

1. In The Things Network, log into the application to which you have associated the LoRaWAN™ modules used by your **Humitemp** devices, and select "Uplink", by pulling down the Payload Formatters menu located on the left side.



- Configure the Uplink as shown in the following image, and then press "Save Changes".

Formatter type *

Formatter code *

```

11  var time = bytes[12] | bytes[13] * 256 + bytes[14] * 65536 + bytes[15] * 16777216;
12  var downlink_byte = bytes[17];
13  if(time !== 0){
14      return {
15          data: {
16              type: {value: type_b, timestamp: time*1000},
17              tamb: {value: tamb / 10, timestamp: time*1000},
18              hamb: {value: hamb / 10, timestamp: time*1000},
19              text1: {value: text1/10, timestamp: time*1000},
20              text2: {value: text2/10, timestamp: time*1000},
21              vbat: {value: vbat/1000, timestamp: time*1000},
22              dc: {value: DC/10, timestamp: time*1000},
23              posi: {value: pos_stored, timestamp: time*1000},
24              downlink: downlink_byte
25          },
26          warnings: [],
27          errors: []
28      };
29  } else
30      return {
31          data: {
32              type: {value: type_b},
33              tamb: {value: tamb / 10},
34              hamb: {value: hamb / 10},
35              text1: {value: text1 / 10}
36          }
37      };

```

- Formatter Type:** Custom Javascript formatter
- Formatter Code:** Copy and paste the next function code:

```

function decodeUplink(input) {
    var bytes = input.bytes;
    var type_b = (bytes[0]);
    var tamb = (bytes[1] << 8) | bytes[2]; if(tamb > 32768) tamb -= 65535;
    var hamb = (bytes[3] << 8) | bytes[4]; if(hamb > 32768) hamb = 0;
    var text1 = (bytes[5] << 8) | bytes[6]; if(text1 > 32768) text1 -= 65535;
    var text2 = (bytes[7] << 8) | bytes[8]; if(text2 > 32768) text2 -= 65535;
    var vbat = (bytes[9] << 8) | bytes[10];
    var DC = bytes[11];
    var pos_stored = bytes[16];
    var time = (bytes[12] << 24) | (bytes[13] << 16) | (bytes[14] << 8) | bytes[15];
    var downlink_byte = bytes[17];
    if(time !== 0){
        return {
            data: {
                type: {value: type_b, timestamp: time*1000},
                tamb: {value: tamb / 10, timestamp: time*1000},
                hamb: {value: hamb / 10, timestamp: time*1000},
                text1: {value: text1/10, timestamp: time*1000},
                text2: {value: text2/10, timestamp: time*1000},
                vbat: {value: vbat/1000, timestamp: time*1000},
                dc: {value: DC/10, timestamp: time*1000},
                posi: {value: pos_stored, timestamp: time*1000},
                downlink: downlink_byte
            },
            warnings: [],
            errors: []
        };
    }
    else
        return {
            data: {
                type: {value: type_b},
                tamb: {value: tamb / 10},
                hamb: {value: hamb / 10},
                text1: {value: text1/10},
                text2: {value: text2/10},
                vbat: {value: vbat/1000},
                dc: {value:DC/10},
                posi: {value: pos_stored},
                downlink: downlink_byte
            },
            warnings: [],
            errors: []
        };
    }
}

```

Section 6: Centriomega® Remote Control and Monitoring Platform

The Humitemp® works in conjunction with the Remote Monitoring WEB platform.

Users can access the Remote Monitoring Platform via WEB, to perform, among other things:

- Remote monitoring and visualization of historical data records, in graphs and data tables, for up to 2 years.
- Alarm management for variables out of range, battery levels, and main power supply failure.
- Add comments to alarm records.
- Set alarm limits, among other custom settings, like sensors' names.
- Configure alarm events, such as external notifications by email, SMS, voicemail, Telegram messaging service or via webhooks.

6.1 Access the Centriomega® Remote Monitoring Platform

Using the credentials provided by the manufacturer, the device's user can log in at iot.omicroning.co



Figure 6-1 Access to the Remote Monitoring Platform

NOTE:

If you don't have the login credentials, please contact the supplier or manufacturer of the device. **Remember that you can find the contact information at the beginning of this document.**

The platform uses some basic elements to organize the information it manages and facilitate interaction with users. These are: **Dashboards, Devices, and Events**.

An introduction to the use of each of them will be offered in this guide.

6.2 Reviewing historical data

Dashboards are interfaces where relevant data is presented to the users. The referred platform allows to edit or create custom Dashboards to integrate any information desired (if using an account with permission to do so); however, by default, it offers panels for remote monitoring of the data published by all the devices linked to the platform, and panels to display Alarms or Events that have recently occurred.

To review a Dashboard, initially follow what is indicated in Section 6.1, to access the platform.

Inside the platform, users can find a link to the section that includes all the Dashboards available to their accounts. There, they can select the Dashboard of their interest:

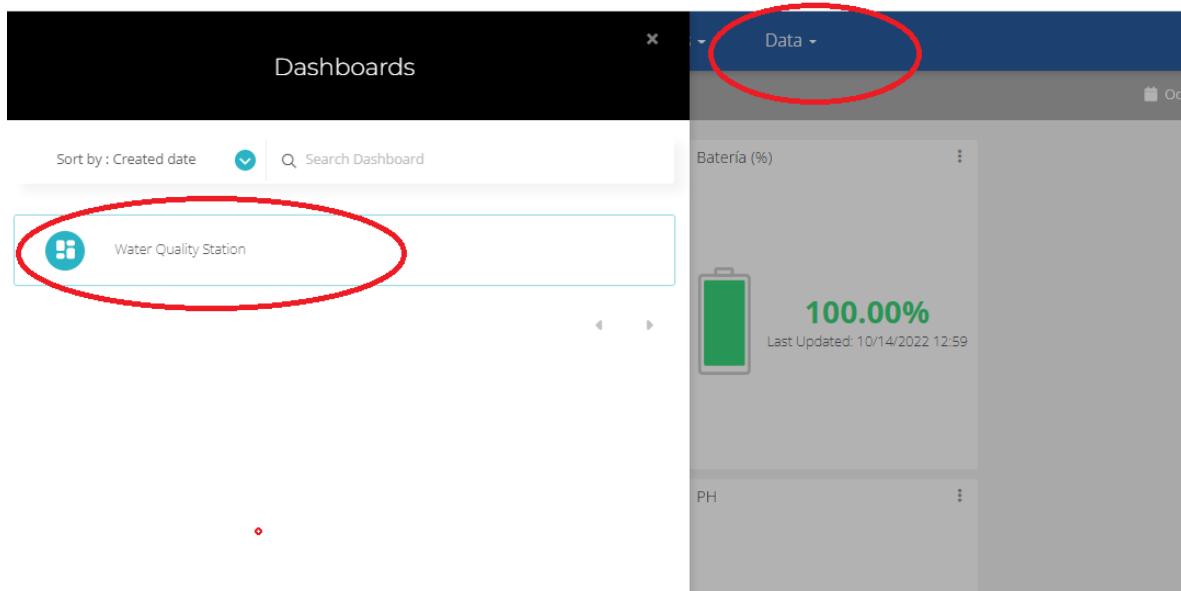


Figure 6-2 Dashboard selection

After selecting a particular Dashboard, users are able to see the information that corresponds to that panel in multiple graphs and visual elements:



Figure 6-3 Dashboard visualization example

To learn how to modify said elements and how to configure a Dashboard, **you can contact the manufacturer of the Humitemp®**. Remember that Contact Information is provided at the beginning of this document.

6.3 Reviewing Devices, their Variables, and Configuration

A Device is a virtual representation of a physical device that takes data from sensors and transmits them through a particular network to the platform. Thus, each Device visible to an account receives the data of the physical equipment acquired by the administrator of the account.

The data received by a device is stored and organized in multiple variables.

To review a specific Device, initially follow what is indicated in Section 6.1, to access the platform.

Inside the platform, users can find a link to the section that includes all the available Devices to their accounts and select the Device of their interest:

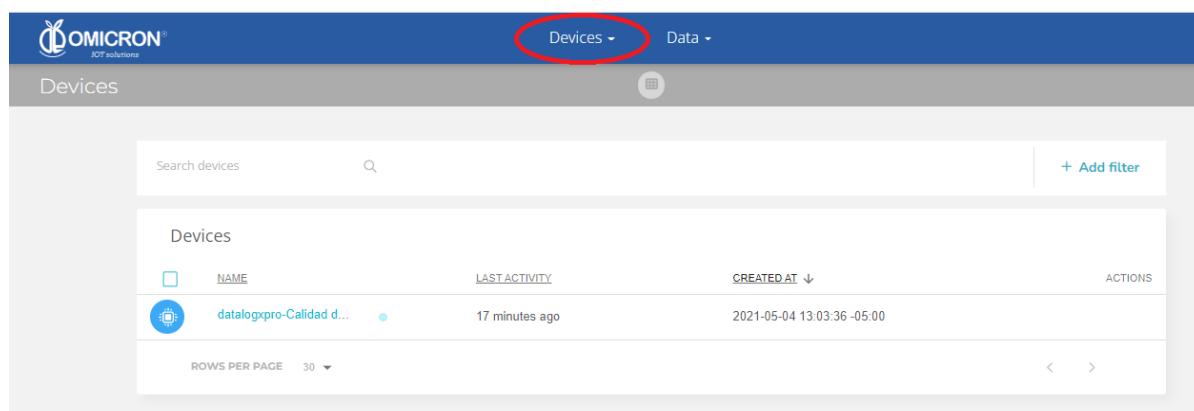


Figure 6-4 Device selection page

After selecting a particular Device, the user is able to see the information that corresponds to that Device in multiple panels and Variables.

Reviewing the Variables of a certain Device allows for checking the update status and the current measure of each Variable. If it is suspected that one variable is not being updated properly, after entering the Device panel that should include it, its last activity period could be reviewed.

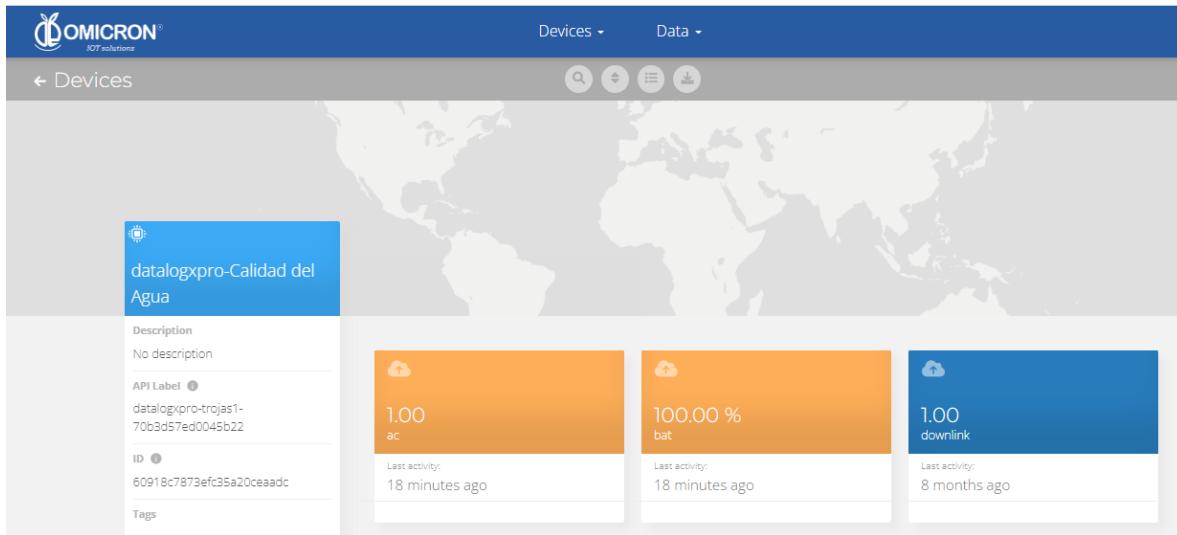


Figure 6-5 Reviewing the Variables of a Device

To review the historical data of a certain Variable, in a Device, select the Variable.

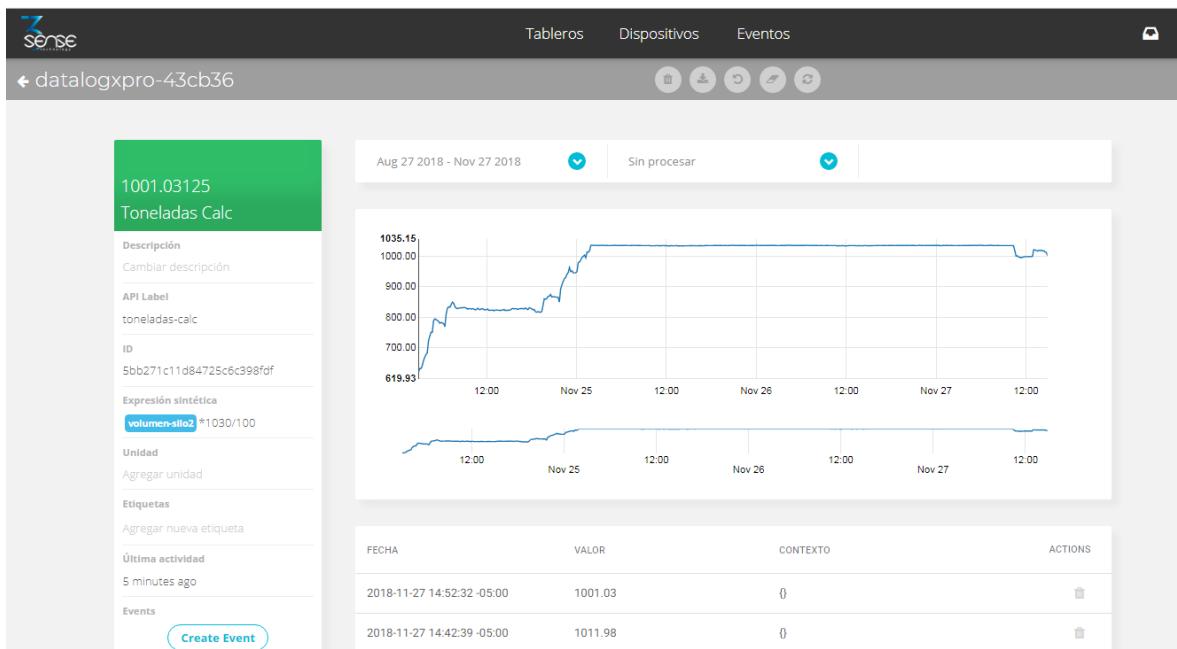


Figure 6-6 Variable Historical Data

6.4 Reviewing Alarms and Programmed Events

Events (or Incidents) are configurable conditions that activate the sending of alert messages via email, SMS, Telegram, or Webhooks. Violated conditions, which may have been responsible for sending messages to users, can be reviewed in a Dashboard associated with your account, in whose name the suffix -Alarms is included.

To review an Event, initially follow what is indicated in Section 6.1, to access the platform.

Inside the platform, users can find a link to the section that includes all the Events available to their accounts and locate the Event of their interest:

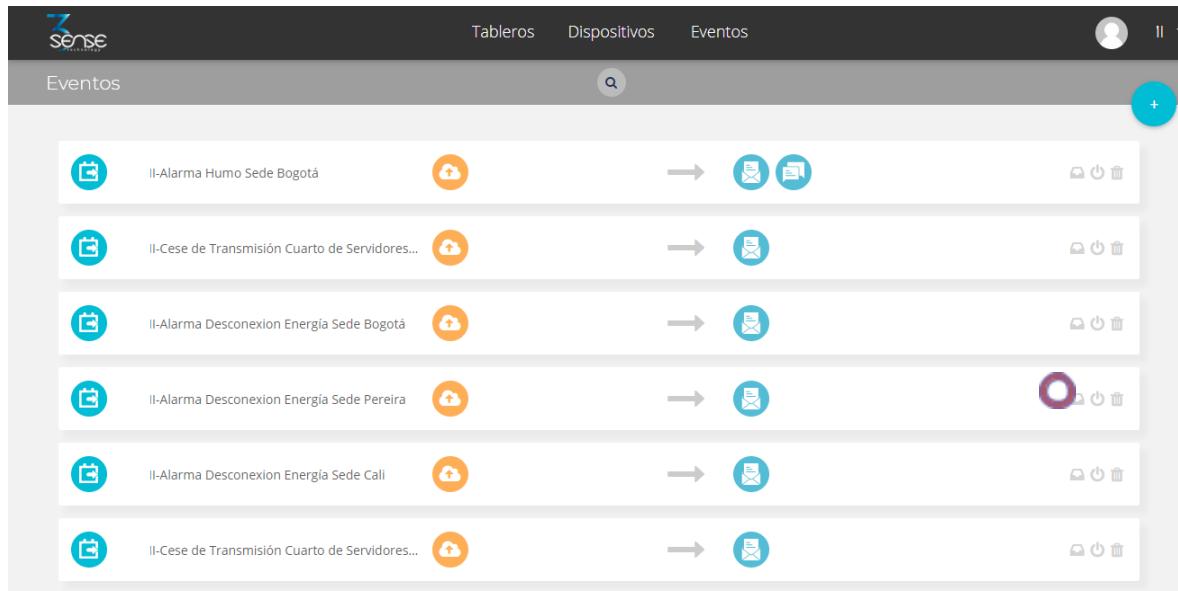


Figure 6-7 Events Configuration

To review the last activity of an Event (its log of updates, or the times in which one of its conditions where violated), the user can press the Log icon associated to any Event to see a table like the following one:



Tipo	Fecha	Mensaje
SMS	2018-06-26 13:57:03 -05:00	Sms sent to [REDACTED]
Email	2018-06-26 13:57:03 -05:00	Email sent to [REDACTED]
Email	2018-06-26 13:57:03 -05:00	Email sent to [REDACTED]

Figure 6-8 Events historical record

To review the Dashboard with the recently activated Alarms, refer to section 6.2, and look for the Dashboard whose name contains the suffix -Alarms.

This Dashboard will contain a table like the following one:

Incidentes							
	Dispositivo	Variable	Activado	Reconocido	Resuelto	Mensaje	Comentarios
●	II-Sede Medellín		Agosto 02 2018 - 08:55:06	-	-	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Agosto 01 2018 - 15:27:40	-	Agosto 01 2018 - 15:30:42	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Agosto 01 2018 - 11:00:28	-	Agosto 01 2018 - 15:26:42	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Julio 31 2018 - 12:04:02	-	Agosto 01 2018 - 10:47:27	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Junio 05 2018 - 01:36:58	-	Julio 31 2018 - 11:31:16	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Mayo 25 2018 - 11:57:34	-	Junio 05 2018 - 01:35:47	II-ALARMA Temperatura Sede Medellín	Ver comentarios
●	II-Sede Medellín		Mayo 25 2018 -		Mayo 25 2018 -	II-ALARMA Temperatura Sede	

Figure 6-9 Events Dashboard

To learn how to modify the configuration of an Event, **you can contact the manufacturer of the Humitemp®**. Remember that Contact Information is provided at the beginning of this document.

Section 7: Troubleshooting Guide

7.1 I cannot log in to the remote monitoring platform

To log in to the remote monitoring platform, **use the credentials given by the manufacturer exactly as they were provided**; that is, if you were assigned a username or password with capitalized characters: you must enter them as they were assigned.

If you verify that the username or password provided by the manufacturer does not allow you to log in, ask the manufacturer to change them.

7.2 The device displays erroneous measurements on its screen or on the monitoring platform

Humitemp® devices assign extreme values to measurements from enabled sensors that are not properly connected or are malfunctioning. The following table summarizes the outliers that a **Humitemp®** can associate with each sensor, and what each of them can indicate:

Table 7-1 Outliers associated with each sensor

Predefined Humitemp® Abnormal Values	
Values	Possible cause
99.9	Internal humidity and ambient temperature sensor, malfunctioning
80.1	Internal humidity and ambient temperature sensor, malfunctioning
-50.1 / 121.1	External temperature sensor disconnected or damaged.

If your device reports that any enabled external sensor is disconnected or damaged, try disconnecting and reconnecting it properly, carefully. Also, verify that the sensor cables are free of cuts, wear, corrosion, discontinuities, or physical hazards.

If you notice that the device is displaying values from a sensor that you do not wish to have connected, refer to section 3.2.1 to learn how to disable or enable the display of measurements from a specific sensor.

If you are unable to correct the abnormal measurements reported by the device through the reconnection of the sensors, if you do not identify physical damage to the sensors, if your device reports incorrect measurements that do not correspond to those listed in the table, or if it displays a specific value uninterruptedly, it is suggested that you contact the manufacturer; remember that you can find the contact information at the beginning of this document.

7.3 The display of the device does not show information

If the device does not show information on its display, despite briefly pressing its (∇) and (Δ) buttons, or pressing the (Δ) button for 2 seconds; it can be assumed that the device is turned off or discharged. To turn it on, press the button (∇) for 2 seconds; if this has no

effect, in case it is running on batteries only, replace the batteries in the device or connect it to the electrical supply.

If you are unable to correct the problem with the suggestions given, it is suggested to contact the manufacturer; remember that you can find contact information at the beginning of this document.

7.4 The device has stopped updating data on the monitoring platform

If the monitoring platform does not record recent measurements from the device, perform the following to try to identify the problem:

1. Verify that the device is in its Normal Operating State:

The Normal Operating State of a **Humitemp®** can be recognized when the device presents on its display the different correct measurements taken by its sensors; whether they are internal or external, as long as they are properly connected.

In case the device does not show information on its display, or presents erroneous measurements, refer to the recommendations given in the previous points of this section.

2. Avoid obstructing the device's wireless signals:

It is essential to ensure that the device is within the coverage area of the wireless network it is using, therefore, try to locate it in a place that does not obstruct its wireless transmissions (away from metallic surfaces or objects, and sturdy objects such as walls or shelves; and preferably located in a high place).

3. If it transmits data via Wi-Fi, check the status of the Wi-Fi network to which it should be connected, and the device's connection to it:

Make sure that the configuration of the network to which the device is connected does not restrict access to the device (consult the personnel in charge of the network infrastructure in your organization); on the other hand, **verify that the network access credentials configured on the device correspond to those managed by the network** to which you wish to connect it; that is, that the SSID or password you have configured for the device match those of the Access Point of the network to which you intend to connect it. To ensure such a match, you can reconfigure the device with the correct credentials.

4. Contact the manufacturer

If after verifying that the problem with your device cannot be corrected by following the recommendations given in the previous points, contact the manufacturer. Remember that contact information is provided at the beginning of this document.

7.5 When trying to save the configuration with the remote configurator, I see the message: "You do not have permission to perform this configuration. It is recommended to check the device ID entered, or the type of device selected."

The interface does not allow you to configure devices that do not exist, or to which you do not have access from your account; therefore, the message will appear if you enter the ID of a device not associated with your account, or if you select a device type that does not

correspond to the one of the ID entered. It is recommended that you check the ID and type of the device you intend to configure before attempting to configure it. If you receive the message, even if you enter the correct device ID information, request assistance from Omicron IoT Solutions technical staff. Remember that contact information is provided at the beginning of this document.

7.6 I can't see the device ID on its label

Each device is delivered with a label on its back where you can find the ID, or MAC fields (these are different from the FCC ID, which you should ignore). However, if you are unable to locate the ID information on a device label, you can review the ID information of the devices associated with your account on the remote monitoring platform.

To do this, after logging into the platform, in the 'Devices' tab, select the 'Devices' option (1, in Figure 7-1); then, in the list that appears, find and select the device for which you want to know the identification information (2, in Figure 7-1); and finally, locate the ID in the "API Label" field on the page with the device information (3, in Figure 7-1).

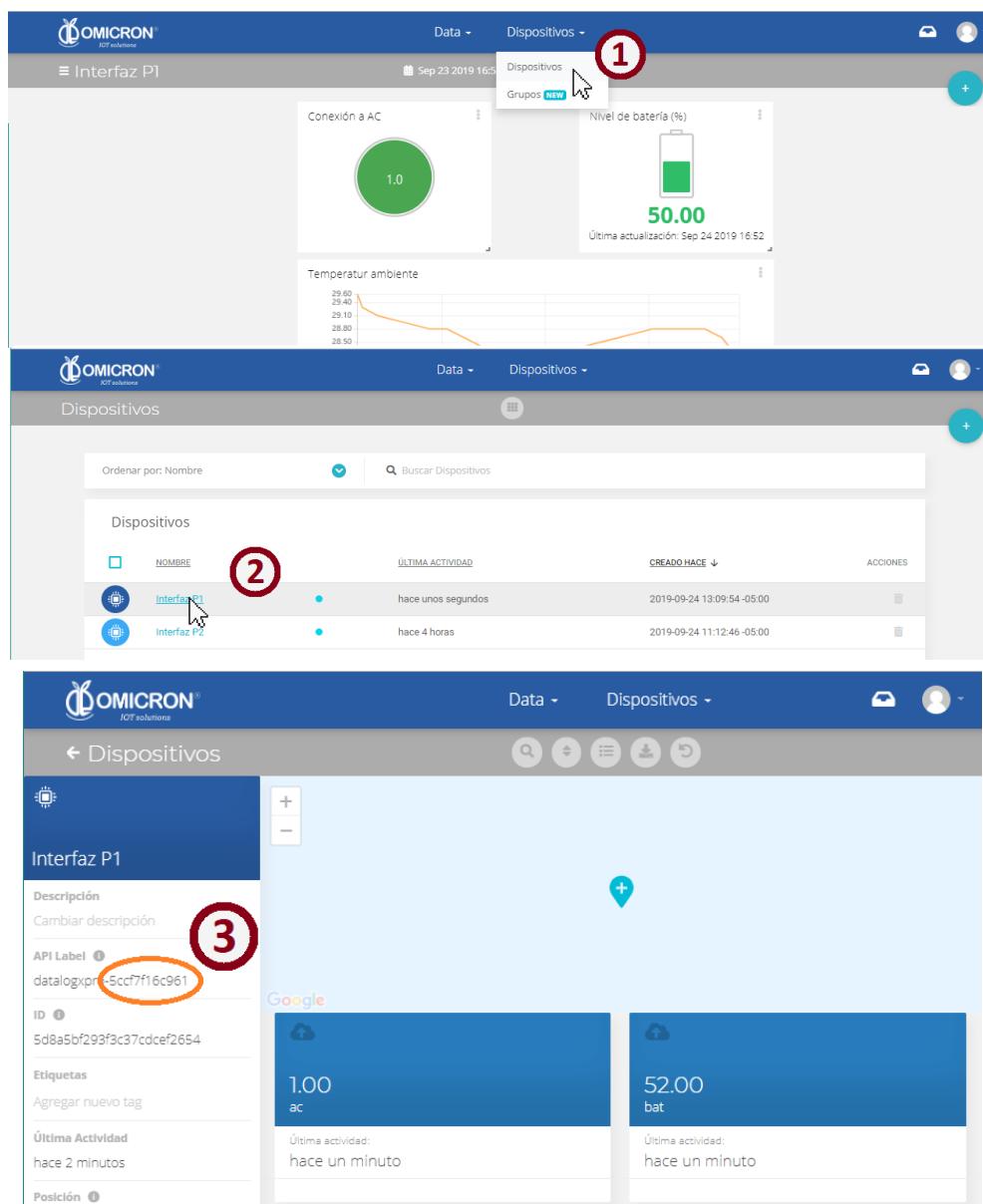


Figure 7-1 Search for the device ID in the remote monitoring platform

The API Label of each device is composed of its type and its ID, separated by a hyphen (e.g. humitemp-123abc). Once you have identified the ID of interest, you can use it to specify the device to be configured with the Remote Configurator.

⚠ CAUTION

Do not modify the "API Label" of a device associated with your account for any reason.



Global Headquarters

America Regional Office

Omicron IoT Solutions

Address: Carrera 46 # 38 - 62 Off. 502 Medellín - Colombia

Phone: +57 (604) 2328381

WhatsApp +57 (317)4365062

comercial@omicroning.co

www.omicroniot.com



© 2023 Omicron IoT Solutions. All rights reserved.