Smart Sense

GATEWAY G404-POE1

USER MANUAL

Version: G404-POE1-D00-UM-EN-1.0.1

SMART, CONNECTED.

KAIRO

WARNING:
IMPORTANT INFORMATION FOR THE READER

1. This manual is intended for the gateway G404-POE1 with a firmware version greater than or equal to 1.7.0.

2. Please check “www.kairo.solutions/downloads” for its PDF version and for any available updates.

3. Before installing and using the equipment, please carefully read all the instructions contained herein, and pay particular attention to the safety information. Kairo Srl will not be responsible for the consequences of improper use of the equipment.

The information in this manual is subject to change without notice.
It is the user’s responsibility to verify that the hardware in his possession is among those covered by this manual.

CONTACTS

Kairo Srl
Registered office: Via Enzo Ferrari, 16
25030 Roncadelle (BS) ITALY
Head office: via Papa Giovanni XXIII 3/G
25086 Rezzato (BS) ITALY
info@kairo.solutions

WARRANTY CONDITIONS

Kairo Srl, hereinafter referred to as Kairo, guarantees the product for a period of twelve months from the delivery date certified by the delivery documents.

Kairo's products will be free from defects in conditions of normal use and service.

Kairo's obligation is limited to the repair or replacement of parts that are returned to Kairo, without alteration or further damage, and which, in the opinion of Kairo, were defective or became defective during normal use.

Kairo cannot be held responsible for any direct, indirect, accidental or consequential damage or injury caused by the correct or improper operation of its equipment, whether defective or non-defective.

Before returning any equipment to Kairo, it is necessary to request authorization; once the parts to be repaired arrive at Kairo, these will be inspected to verify that they are eligible for repair or replacement.

Kairo will not be obliged to repair or replace products returned as defective but damaged by misuse, negligence or transport damage.

End customers must ensure that defective products are properly packaged for return.

The above warranty is unique and exclusive and no other warranties, written or oral, are expressed or implied.

Kairo's warranty does not extend and does not apply to products:
- which have been repaired or altered by personnel not authorized by Kairo;
- which have been subject to misuse, negligence, accident, damage, improper installation;
- which have been connected to equipment other than that supplied or envisaged by Kairo;
- which have been damaged by natural disasters;
- in which hardware or software or accessories not installed by Kairo and / or without any approval by Kairo have been installed.

SAFETY RECOMMENDATIONS

Before commissioning the system, carefully read the following safety recommendations.

WARNING	Do not use the system for purposes other than those indicated in this manual.
WARNING	For a correct use of the equipment, refer to the relevant sections in this manual.
CAUTION	Protect the equipment from dust, rain, water and / or other liquids..
CAUTION	Do not place anything on the equipment.
CAUTION	Do not operate the system if the antenna or the network connection cable is damaged.
WARNING	Install the equipment following the instructions provided in this manual. The equipment must be installed according to the national regulatios in force. Install the equipment so as to guarantee correct ventilation, as well as safe accessibility to the connctors and buttons located on the front panel.
CAUTION	Carry out maintenance of the sensor following the instructions provided in this manual. Before carrying out any operation, disconnect the power cable as indicated in this manual.
DANGER	Electric shock hazard. Do not open the sensor and / or modify any internal or external part. Do not operate the equipment if the external case or the or the external cable are damaged.
RADIO FREQUENCY	The equipment contains a radio frequency section. The external antenna must be positioned so that there are no obstacles in the immediate vicinity.

If technical assistance is needed during normal operations or maintenance, contact the reseller or the manufacturer.

DISPOSAL

	In accordance with the requirements of Directive 2012/19/EU as regards waste from electrical and electronic equipment (WEEE), the user is required to ensure that this product is separated from other waste at the end of its life cycle and delivered to the WEEE collection for proper recycling.

CONTENTS

1. INTRODUCTION

1.1 Recommendations

Thank you for purchasing the Kairo G404-POE1 gateway (hereinafter also referred to as “gateway” or “gateway G404”). This document describes the device and provides the main concepts that the user must learn before its use. We strongly recommend to read the manual before installing and commissioning the device. To properly understand the terms and parameters mentioned in this manual and, therefore, for an effective use of the gateway, the reader must have:

- the knowledge and the information necessary to connect the gateway to the network;
- basic notions relating to electromagnetic waves, useful for understanding specific terms and parameters.

We recommend that the equipment is used only by trained and qualified personnel. Failure to observe these conditions and safety instructions may result in personal injury or damage.

1.2 How to use this manual

This manual consists of the following chapters:

- Chapter 1: Introduction - This chapter introduces the device and the manual.
- Chapter 2: System Operation - This chapter provides the reader with basic information on the operation of the IoT platform of which the gateway is part.
- Chapter 3: Technical Specifications - This chapter lists the technical characteristics of the gateway.

• Chapter 4: Interfaces - This chapter describes the gateway interfaces for connecting to the network and for local diagnostics.

• Chapter 5: Installation - This chapter provides the user with all the necessary information for the correct installation of the equipment.

• Chapter 6: Configuration - This chapter explains to the user how to configure the gateway through the internal web server.

• Chapter 7: Mainteinance - This chapter indicates the operations to be performed to keep the gateway in perfect working order over time.

• Chapter 8: Troubleshooting - This chapter lists the most common errors that can be ecountered during gateway operation and the actions to be taken to restore correct operation.

1.3 Acronyms and definitions

ACRONYM	MEANING
TCP/IP	Transmission Control Protocol/Internet Protocol
DHCP	Dynamic Host Configuration Protocol
HTML	HyperText Markup Language
LAN	Local Area Network
POE	Power Over Ethernet
PC	Personal Computer
RF	Radio Frequency

2. SYSTEM OPERATION

The G404 gateway, together with the self-powered radio sensors (S101 series) and the cloud service, constitutes the Kairo system called SmartSense for data collection and monitoring of process data. SmartSense can be adopted in countless contexts: from individual monitoring of molds and/or molding machines to both manual and automatic workstations or equipment. Using self-powered sensors without cables and without batteries, the system can be installed in a very short time and in a non-invasive way both on latest generation machines/devices and on traditional systems without intelligence or PLC.

In particular, the gateway is an electronic device capable of receiving radio messages transmitted by the peripheral sensors powered by Kairo S101, as well as forwarding the related notification in real time to a Cloud server, which registers it and carries out all statistical processing requested by the user.

The peripheral sensors transmit a message, always the same, upon the occurrence of an event that corresponds to the pressure on the actuator that triggers the energy generation mechanism. Each radio message consists of the transmission of two identical messages at a distance of a certain time interval. Once the transmission is over, the peripheral sensors remain off until the next event. The transmission on the radio channel occurs unidirectionally without acknowledgment.

In order for the gateway to receive the radio signals correctly, certain conditions must be verified:

1. The transmitters must be within the working range of the radio signal, which is usually a few tens of meters. The working range may be significantly reduced in case of obstacles and interference between the transmitter and the gateway;

2. Before activation, each peripheral sensor must be registered in the network, with a so-called teach-in procedure. If no registration is

carried out, the signals transmitted by that sensor are ignored by the gateway;

3. There must be fewer sensors in the network than the maximum allowed number. Some signals may be lost otherwise.

Since all sensors use the same radio frequency, in the event that two or more of them transmit simultaneously, a conflict may occur and the gateway may be unable to interpret the individual messages, which would be actually lost. This circumstance is rather unlikely since each sensor engages the radio channel for a very small time, but the probability increases with the increase in the number of sensors in the network and with the increase in the frequency of events recorded by the sensors.

In the unlikely event of a conflict on the radio channel, there is however a mechanism by which the Cloud server can detect the loss and reconstruct afterwards the correct sequence of messages.

The transmission of reception notifications from the gateway to the Cloud can only take place in the presence of a broadband Internet connection, with low latency. With lower speed connections delays of the order of several seconds may occur between the occurrence of the single event and the display on the server.

In the event of an interruption of the Internet connection, the gateway is able to store data for a few minutes and transmit the related notifications when the connection is restored.

3. TECHNICAL SPECIFICATIONS

3.1 Physical dimensions

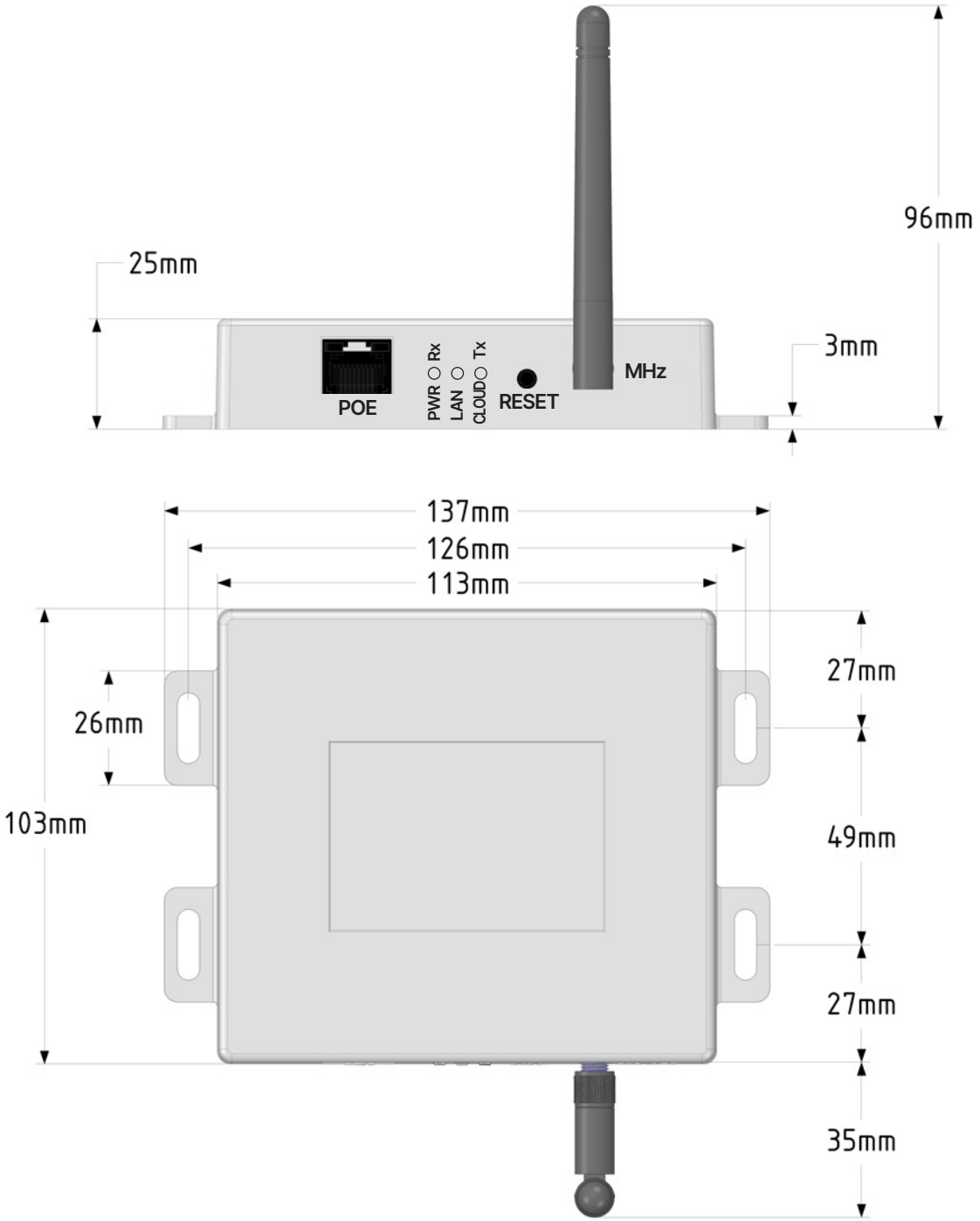

Figure 1: gateway G404-POE1 outer dimensions

3.2 Declaration of conformity

CE	Kairo srl declares under its own responsibility that the Gateway G404 complies with the 2014/53/UE directive.

3.3 Specifications

The G404 Gateway consists of a radio section for communication with peripheral sensors and a processing section which deals with data processing and interfacing with the Cloud. The characteristics of both are shown below.

RADIO SECTION	
OPERATING FREQUENCY	868 MHz
RADIO INTERFACE	SMA female connector, external antenna supplied
IMPEDANCE	50 Ohm

Table 1: radio characteristics

PROCESSING AND CLOUD INTERFACE	
INPUT/OUTPUT INTERFACE	Ethernet (RJ45), TCP/IP
COMMUNICATION PROTOCOL	HTTP (a broadband Internet connection is required)
POWER SUPPLY	POE (Power Over Ethernet), IEEE 802.3at or IEEE 802.3af. Maximum consumption 1 Watt. Optional external POE power supply.
LOCAL USER INTERFACE	Three LEDs, two of which two-colored, reset button
DIMENSIONS	See paragraph 3.1
IP PROTECTION LEVEL	IP40
OPERATING TEMPERATURE	-10 °C / +50 °C
STORAGE TEMPERATURE	-20 °C / +70 °C
EMI/EMC	ETSI 301 489-1 V.2.1 - ETSI 301 489-3 V.2.1.1 - ETSI EN302802
ELECTRICAL SAFETY	EN60950-1

Table 2: interface characteristics

4. INTERFACE

Gateway G404 is a device that provides the interface between peripheral radio sensors and the Cloud server. It therefore includes a radio module (radio receiver) and a section for processing and interfacing to the network. All gateway interfaces are arranged on one side of the case, as shown in Figure 2.

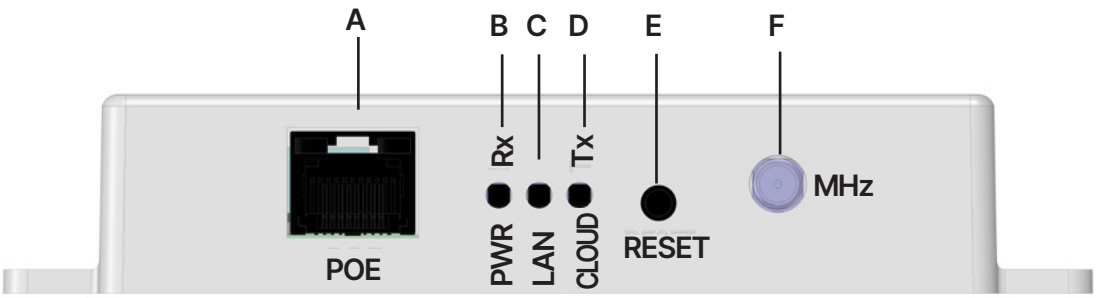

Figure 2: gateway G404-POE1 interfaces

The radio module has as its only interface a female SMA connector (F) to which the supplied antenna must be screwed. The connector is marked with the 'MHz' label. The gateway must not be operated without the antenna in place, and with an antenna other than the one supplied.
The RJ45 connector (A) with the 'POE' label, on the far left, is used for data connection and, jointly, for powering the system according to the Power Over Ethernet standard. Since the gateway does not have a power switch, turning on occurs by connecting the Ethernet cable.

On the panel there are three LEDs, one of which is single color (B) and two two-color (C and D). These LEDs provide indications on the operating status of the gateway, as described in Table 3, Table 4 and Table 5.

LED	LABEL	OPERATING MODE
LED1	PWR RX	
COLOR	**EXAMPLE**	**MEANING**
GREEN - SOLID		System on and operational. No reception on the radio channel.
GREEN - BLINKING		Data reception on the radio channel. Each flash of the LED corresponds to the reception of a radio message from a peripheral sensor.

Table 3: operating mode of LED 1

LED	LABEL	OPERATING MODE
LED2	LAN	
COLOR	**EXAMPLE**	**MEANING**
RED - SOLID		Ethernet link error. See the system log for a more detailed description of the error.
GREEN – QUICK BLINKING		DHCP search: the IP configuration is being acquired by the DHCP server.
GREEN - SOLID		DHCP valid: the gateway has acquired a valid IP configuration from the DHCP server.
RED - BLINKING		DHCP fail - factory reset. A valid IP address could not be acquired from the DHCP server and the gateway restored the factory IP configuration.
GREEN - SLOW BLINKING		Fixed IP set. The gateway is working with the IP configuration set by the user.

Table 4: operating mode of LED 2

LED	LABEL	OPERATING MODE
LED3	CLOUD TX	
COLOR	**EXAMPLE**	**MEANING**
RED - SOLID		Failure to connect to the Cloud Server. This condition can occur in the case of incorrect setting of the server address, invalid access credentials or temporary unavailability of the server. Consult the system log for a detailed description of the error.
GREEN - SOLID		Connection with Cloud Server established. No data transmission in progress.
GREEN - BLINKING		Data transmission to the Cloud Server.

Table 5: operating mode of LED 3

Moreover, on the panel there is a hole (E) through which it is possible to access a reset button for restoring the factory configuration. The button can be actioned by pressing it gently for a few seconds with a pointed object (for example a thin screwdriver or the tip of a ballpoint pen) until the LEDs start flashing as indicated in Table 6. The operation is described in Table 6.

ACTION	RESULT	LED
Reset button pressed when the router is turned on	Restore factory configuration	Once the factory settings have been restored, the three LEDs behave as shown below: LED1:  LED2 and LED3: 

Table 6: operating mode of the reset button

Finally, when a teach-in is performed on a sensor that is within the range of the gateway, the LEDs start a short blinking sequence with the pattern specified in Table 7.

ACTION	RESULT	LED
Teach-in performed on a sensor.	Sensor acquired by the gateway and the cloud.	Once teach-in operation is recognized by the gateway, the three LEDs behave as shown below: LED1, LED2 and LED3: 

Table 7: teach-in operation

5. INSTALLATION

WARNING	
	Before starting the installation, the operator must carefully read the indications listed in this paragraph.

5.1 Positioning the gateway

All installation operations must be performed with the gateway disconnected from the power supply, or with the Ethernet cable disconnected.

Before installing the gateway, you must carefully select the position and orientation. The quality of the radio connection with the sensors is influenced by the presence of obstacles between the gateway and the sensors, especially in the case of metal objects or load-bearing walls.

The gateway is a device for indoor use, and must not be installed in locations exposed to rain, splashes of water or other liquids or dust.

The best position for installing the gateway is usually attached to a vertical wall, at the top, with the LEDs oriented downwards so as to be viewed by an operator positioned on the ground. In this case, the antenna must be left oriented vertically downwards. Alternatively, the gateway can be fixed with the interfaces side up, with the antenna left in a vertical position.

The gateway must be fixed through the four slots in the two lateral flanges. Avoid leaving the gateway hanging on its ethernet cable.

5.2 Connection to power supply and to the network

CAUTION 	Before carrying out any operation on the power supply, make sure that all the applicable requirements are observed according to current legislation.

Gateway G404 does not have a power switch. Power is supplied through the Ethernet cable according to the POE (Power Over Ethernet) standard. As soon as the cable is connected to the gateway port, the latter turns on.

For the power supply, a POE power source compatible with the IEEE 802.3at or IEEE 802.3af standard must be used.

Check that the Ethernet cable, the RJ-45 connector and its fixing clip are intact. Connect the cable to the gateway port indicated with ‘A’ in Figure 2 until the fixing clip snaps into place.

Once connected to the power source, the gateway turns on and the LED indicated by the letter ‘B’ in Figure 2 lights up green. If this does not happen, check that the connection has been made correctly and that the power source is turned on.

6. CONFIGURATION

6.1 Introduction and default credentials

The default setting of the gateway requires that the DHCP network service is active in order to receive the network configuration necessary to operate on the network itself. The gateway has an internal web server through which it is possible to configure all the operating parameters and verify that the system works correctly; to access it use the login credentials, which, by default, are as follows:

- Gateway Username: 'admin'
- Gateway Password: 'password'

To access the web server, use a browser on a device connected to the same network to which the gateway is connected, and type in the URL field the IP address assigned to the gateway. The assigned IP address is shown at the bottom of the gateway configuration page on the Cloud. The gateway IP address can be also easily identified by your network administrator. Once connected to the correct IP, the browser displays the page for entering the login credentials, as shown in Figure 3.

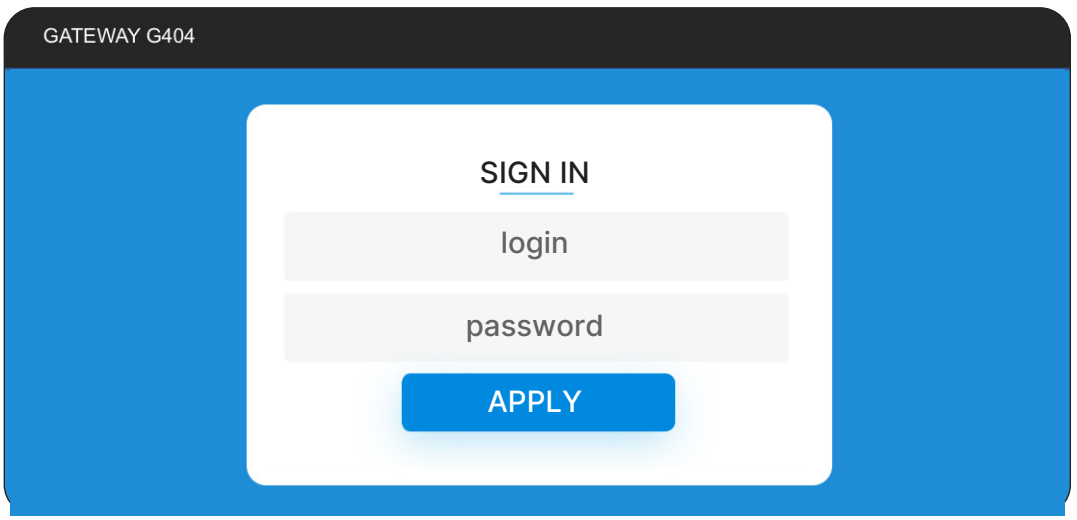

Figure 3: Login page of the gateway internal web server

After logging in, you'll get access to the Configuration page, for the configuration of the operating parameters of the gateway (see section 6.2). The menu at the top right enables access to the two available sections:

1. Configuration: the landing page already described;
2. Logs: for viewing the event log

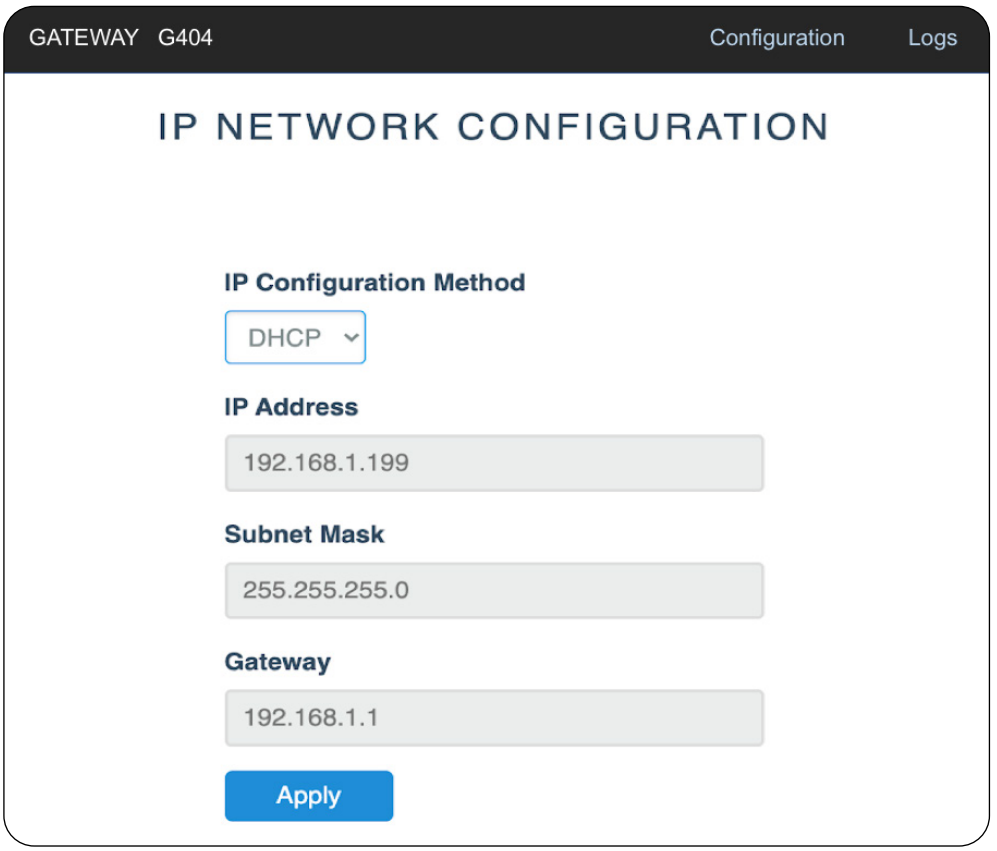

Figure 4: Landing page (after login) of the gateway internal web server

6.2 Configuration

In the configuration section it is possible to set all the parameters necessary for the correct functioning of the gateway. All the settings are examined in detail below. To make any changes effective, press the “Setup” button. If changes are correctly executed, the system displays a confirmation text message

6.2.1 IP network configuration

IP configuration is necessary to operate correctly in the network where the gateway is installed. The settings are those shown in Figure 4. By default, the gateway is set up to receive the IP configuration through the DHCP service. In this way the parameters “IP address”, “Subnet mask” and “Gateway” are configured by the DHCP server. If you want to set a fixed IP for the gateway, in the “IP Configuration Method” box, select the appropriate item (Static) and manually set the three fields below (IP address, Subnet mask and Gateway) with the appropriate information, to be requested to your network administrator

6.2.2 Cloud server settings

This section sets the parameters necessary for correct communication with the Cloud service accessible at the following link https://smartsense.kairo.cloud/login. In particular, the parameter “Cloud Server URL” is provided by the operator of the Cloud service, while the parameter “Cloud Password” is defined by the user of the Cloud service, in the section on activation and configuration of the gateway (Section “Gateway”, choice “New Gateway”). “Gateway ID” is instead a read-only parameter and it is filled by the gateway itself. The user of the Cloud service must provide it in the same section as the “Cloud Password” administrator.

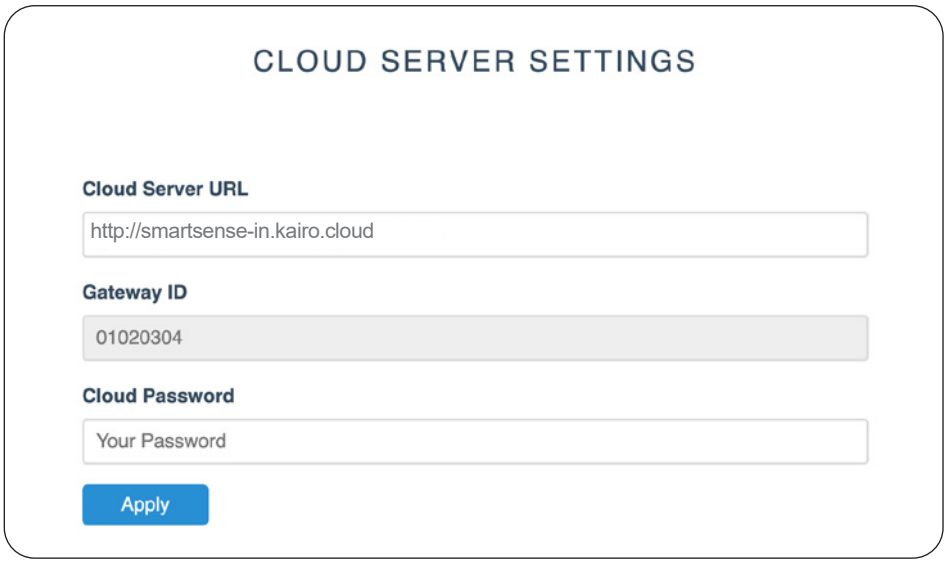

Figure 5: Cloud Server Settings

6.2.3 Gateways access

In this section it is possible to reset the credentials for accessing the gateways's web server, as shown in Figure 6.

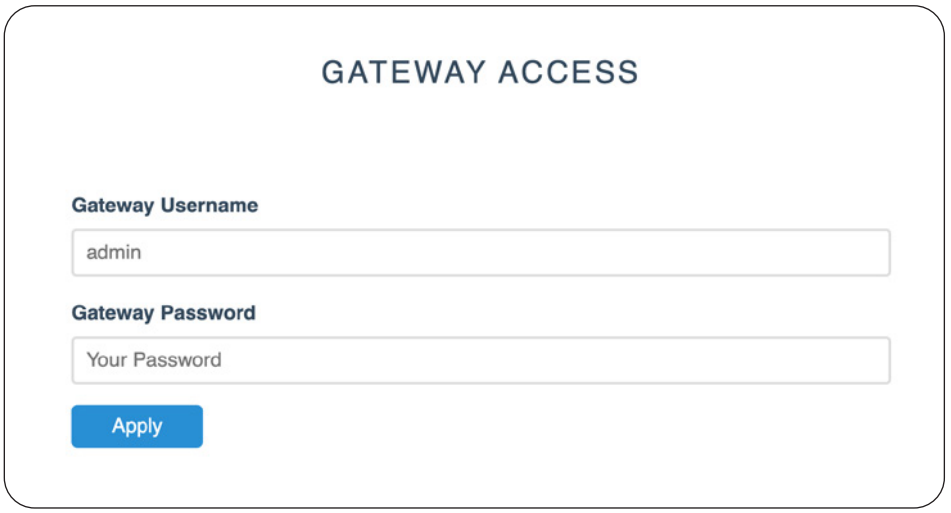

Figure 6: Gateway Access

Through the Reset procedure the default credentials are restored (see paragraph 6.1).

6.3 Logs

In the “Logs” section you can:

- obtain information on the operational status of the gateway and view notifications of various system events and errors.
- Perform a set of administrative tasks as described at the end of this section.

The log file, shown in Figure 7, is updated by pressing the “Reload Logs” button. At the top, the current firmware version, the status of the connection to the Cloud Server, the update of the internal clock and the acquisition of the table of sensors registered in the network (Teach-in Table) are indicated.

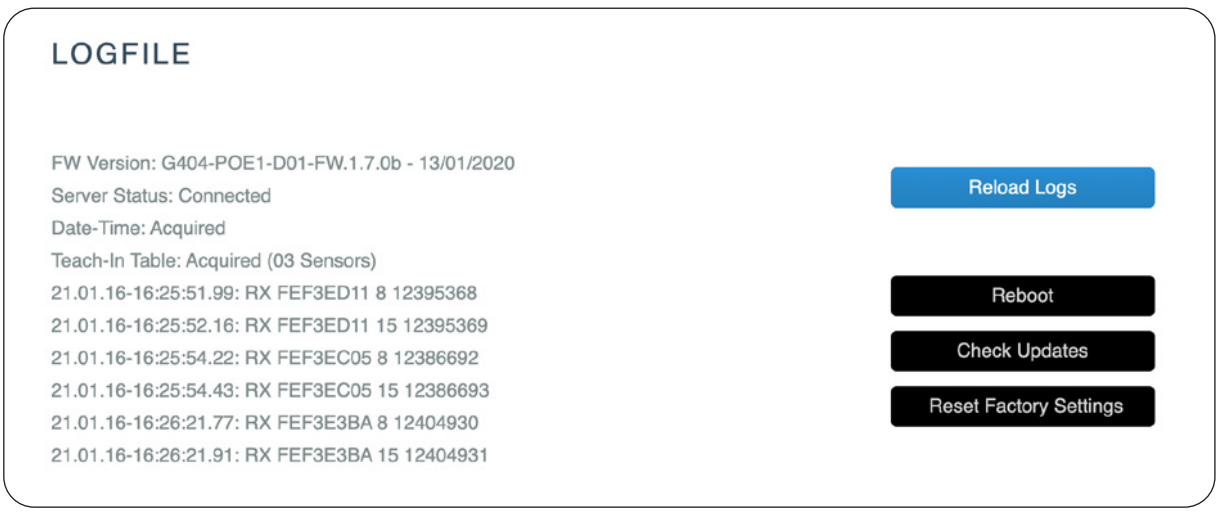

Figure 7: Log file

Further down, event notifications are shown, such as the reception of a radio message from a remote sensor or the occurrence of an error. The gateway can be restarted by pressing the “Reboot” button, while the “Check Updates” button triggers a reload of the page to check if there are updates (for the gateway). Finally, by pressing “Reset Factory Settings”, the user restores the factory parameters of the gateway.

7. MAINTENANCE

The G404 Gateway does not require any particular maintenance operations.

Depending on the environment in which it is placed, it is sufficient to periodically check that the external surface of the case is not damaged and that it is free of dust or other residues. In environments with a lot of dust, a more frequent check is recommended.

It is also suggested to check with the same frequency the correct tightening and the correct positioning of the antenna, as well as the integrity of the Ethernet cable and its connection.

8. TROUBLESHOOTING

The G404 Gateway is an electronic device controlled by a microprocessor, and may be subject to malfunctions. In case of malfunction, refer to Table 8 where possible corrective actions are indicated.

PROBLEM	POSSIBLE CAUSES	CORRECTIVE ACTIONS
The Gateway does not turn on (green power LED does not turn on)	• Incorrect Ethernet cable connection or damaged Ethernet cable • POE power supply not present in the switch / network • Wrong power supply voltage.	• Check the connection, integrity and functioning of the Ethernet cable • Install a POE power supply between the network and the gateway • Check that the power supply is capable of delivering the necessary power (1 Watt)
Failure to connect to the Cloud Server	• Lack of Internet connection • The server address is incorrect • Server login credentials are invalid	• Verify that the Internet connection is up and running • Check that the server address is correctly set • Verify that the server login credentials are correct

Failure to receive messages from peripheral sensors on the radio channel	• Obstacles between the sensor and the gateway, or excessive distance • The sensor is not registered in the network • The sensor is registered in the network but the gateway has not downloaded the teach-in table correctly	• Remove any obstacles between the gateway and the sensors. Try moving the gateway closer to the sensors. • Register the sensor in the network • Restart the gateway by removing and re-inserting the Ethernet cable after a few seconds, so that it correctly downloads the teach-in table.
Unable to access local web server	• The PC and the gateway are not in the same subnet • The gateway IP address is incorrect • Forgot password	• Connect the PC to the same subnet of the gateway • Check the correctness of the gateway IP address • Perform the reset procedure to factory settings as indicated in chapter 5
Local web server pages are not rendered properly and/or provide error pop-ups	• Browser retrieves some old cached data	Clean web browser's cache (e.g. with Chrome, press CTRL+Shift+Del → set 'Time Range' to 'All Time' → checkmark 'Cookies and other site data' + 'Cached images and files' and finally press 'Clear Data')

Table 8: Corrective actions for malfunctions

If the above actions do not solve the problem and the malfunction persists, please contact the device vendor.

NOTES

NOTES

SMART, CONNECTED.

KAIRO Srl
Via Papa Giovanni XXIII 3/G
25086 Rezzato (BS) ITALY
info@kairo.solutions
www.kairo.solutions