User manual IQIO SENS

Dear Customer

Thank you very much for choosing our product. At the same time, please read this manual carefully before using it, as it indicates the most appropriate ways to handle this appliance, taking into account basic safety and maintenance principles. Please also retain the manual for future reference.

Remember!

The manufacturer will not be held liable for any damage caused by improper use of the device or improper handling, nor for any malfunctions of the controller resulting from improper operation.

Table of contents

1 Introductory information

Before working with the controller, read the User Manual and follow the instructions contained therein!

Description of symbols used in this manual:

Warning	This symbol indicates that it is necessary to read a specific section of the User Manual that contains important information and warnings. Ignoring these warnings may lead to injury or damage to the device.

Tip	Important instructions and information. Observing the texts marked with this sign will facilitate operation.

The screenshots shown in this manual may differ from their actual appearance. Due to the continuous development of the module software, some functions may differ from those described in the manual. The manufacturer is not responsible for any undesired effects resulting from software differences.

2 Guarantee and liability of the manufacturer

Warning	The manufacturer provides a two-year warranty for the device and a post-warranty service for a period of 10 years from the date the device was placed on the market. The warranty covers all defects in materials and workmanship.

The manufacturer undertakes to comply with the guarantee agreement if the following conditions are met:

- all repairs, modifications, extensions and calibrations of the appliance are carried out by the manufacturer or an authorised service centre,
- the mains power supply system complies with the applicable standards,
- the appliance is operated in accordance with the instructions given in this manual,
- the appliance is used in accordance with its intended use.

The manufacturer shall not be held liable for any consequences resulting from incorrect installation, improper use of the device, non-compliance with the operating instructions or repairs carried out by persons not authorised to do so.

Warning	There are no user-serviceable parts inside the appliance.

3 Safety in use

The module was constructed using modern electronic components in line with the latest trends in world electronics. Particular emphasis was placed on ensuring optimum operational safety and control reliability. The unit has a housing made of high-quality plastic.

3.1 Storage, operating and transport conditions

The device should be stored in closed rooms where the atmosphere is free of vapours and corrosive agents and:

- an ambient temperature of -35°C to +65°C,
- humidity between 25% and 90% (no condensation allowed)
- an atmospheric pressure of 700 to 1060hPa.

The unit is designed to operate under the following conditions:

- ambient temperature of -30°C to +60°C,
- humidity between 30% and 75% (no condensation allowed),
- atmospheric pressure of 700 to 1060hPa.

Recommended transport conditions:

- ambient temperature of -40°C to +85°C,
- humidity between 5% and 95% (no condensation allowed),
- atmospheric pressure 700 to 1060hPa.

3.2 Installation and use

The controller should be operated as described in the following section.

3.3 Disposal and decommissioning

In the event that it becomes necessary to dispose of the device (e.g. at the end of its useful life), contact the manufacturer or the manufacturer's representative, who is obliged to respond appropriately, i.e. to collect the device from the user. The user may also contact companies dealing with the disposal and/or decommissioning of electrical or computer equipment. Under no circumstances should the appliance be placed with other waste.

4 Purpose of the device

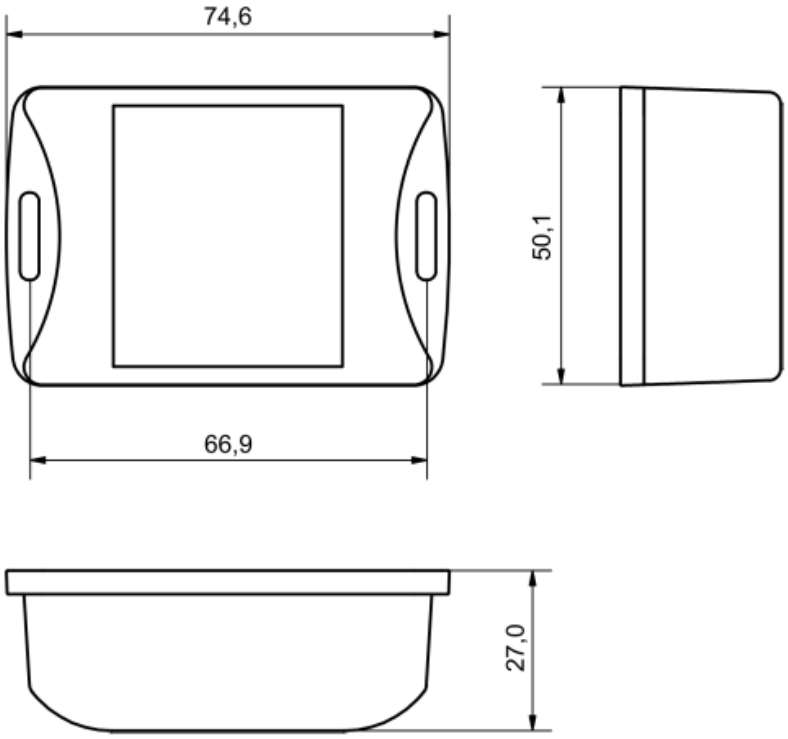
IQIO Sens is an advanced environmental monitoring and management system. It is dedicated to monitoring various environmental parameters such as temperature, humidity, pressure, air quality or the presence of harmful substances. The main objective is to allow users to remotely monitor and manage these parameters in real time. IQIO Sens offers a wide range of features, including configurable notifications, integration with various communication protocols and flexible configuration, allowing its versatile use in industry, agriculture, construction and urban infrastructure monitoring. Thanks to the configurable notification capabilities, users can react quickly to changes in environmental conditions or failures. In addition, thanks to the LWT (Last Will and Testament) mechanism, the system can automatically send notifications in the event of loss of connection to the MQTT broker, ensuring continuity of monitoring even in the event of network disruptions. IQIO Sens contributes to efficiency, safety and productivity in various areas of the business by effectively monitoring, controlling and optimising processes and systems.

5 Assembly of the device

5.1 Technical data

Power supply	Three optional power supply types are available: 1. PoE: 33-57V PoE IEEE 802.3af 2. DC: 12-24VDC (3.5mm screw connector) 3. USB: 5VDC USB C cable
Power consumption	1,5W
Bus	1-wire - 3-wire cable or RJ12 flat cable using adapter*. support for up to 6 sensors dedicated sensors: temperature, humidity, water pressure, air pressure, analogue voltage, analogue current, CO, CO_2, NO_x gases
Communication	Wi-Fi optional 10/100 Mbps Ethernet port
Display	LED 7-segment, red
Operating temperature	from -10°C to +55°C
Enclosure	Enclosure class: IP30

5.1 Dimensions



5.2 Connection diagram

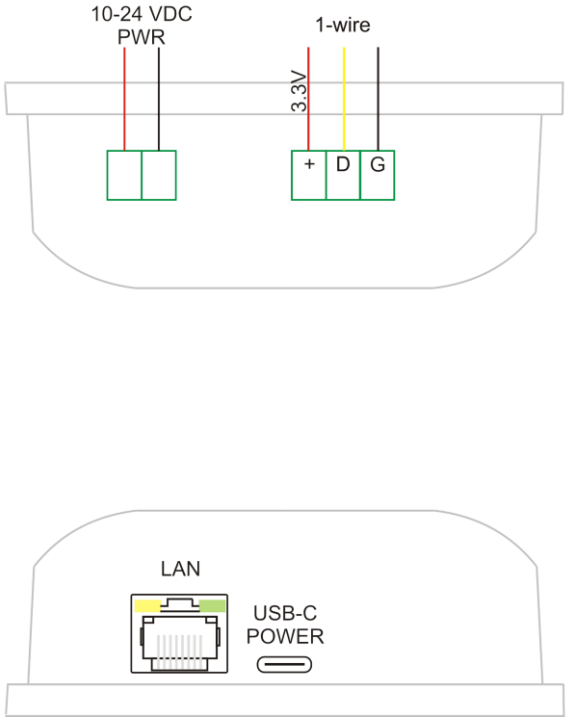
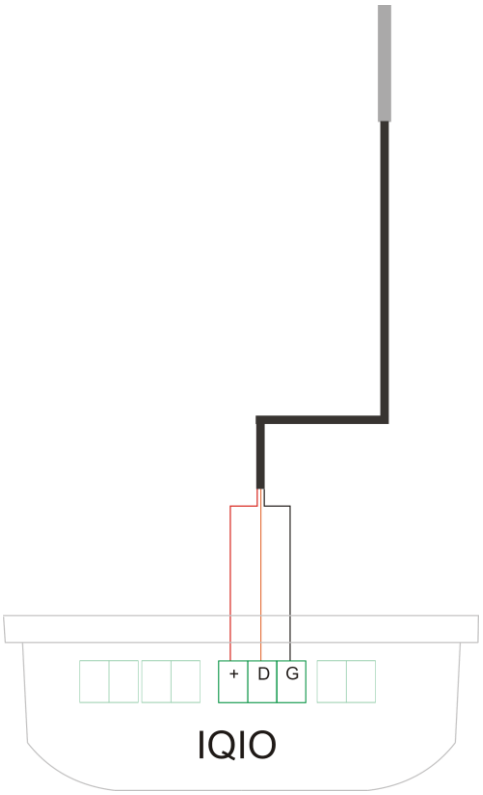
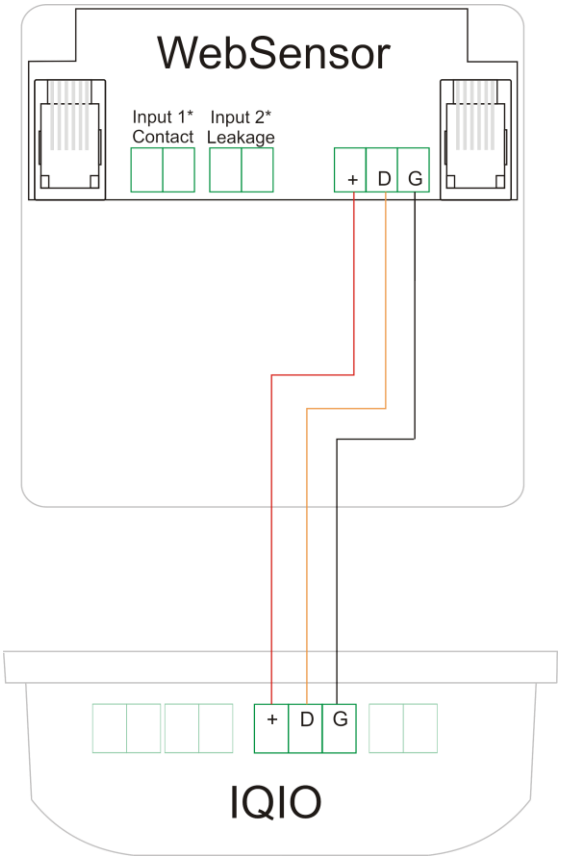


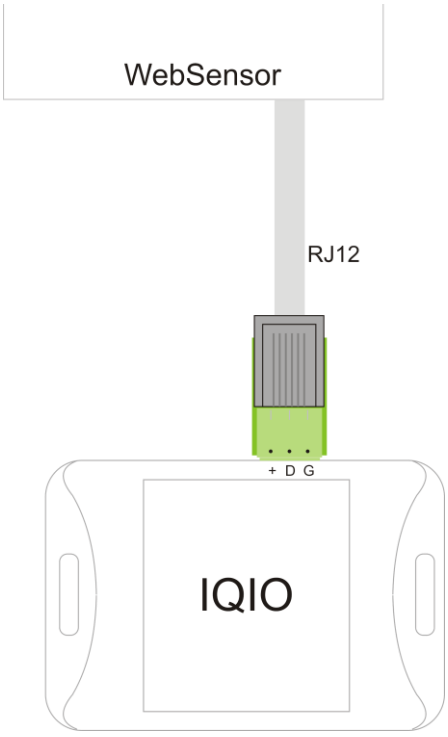
Diagram of the connection of the sensor to the IQIO device:



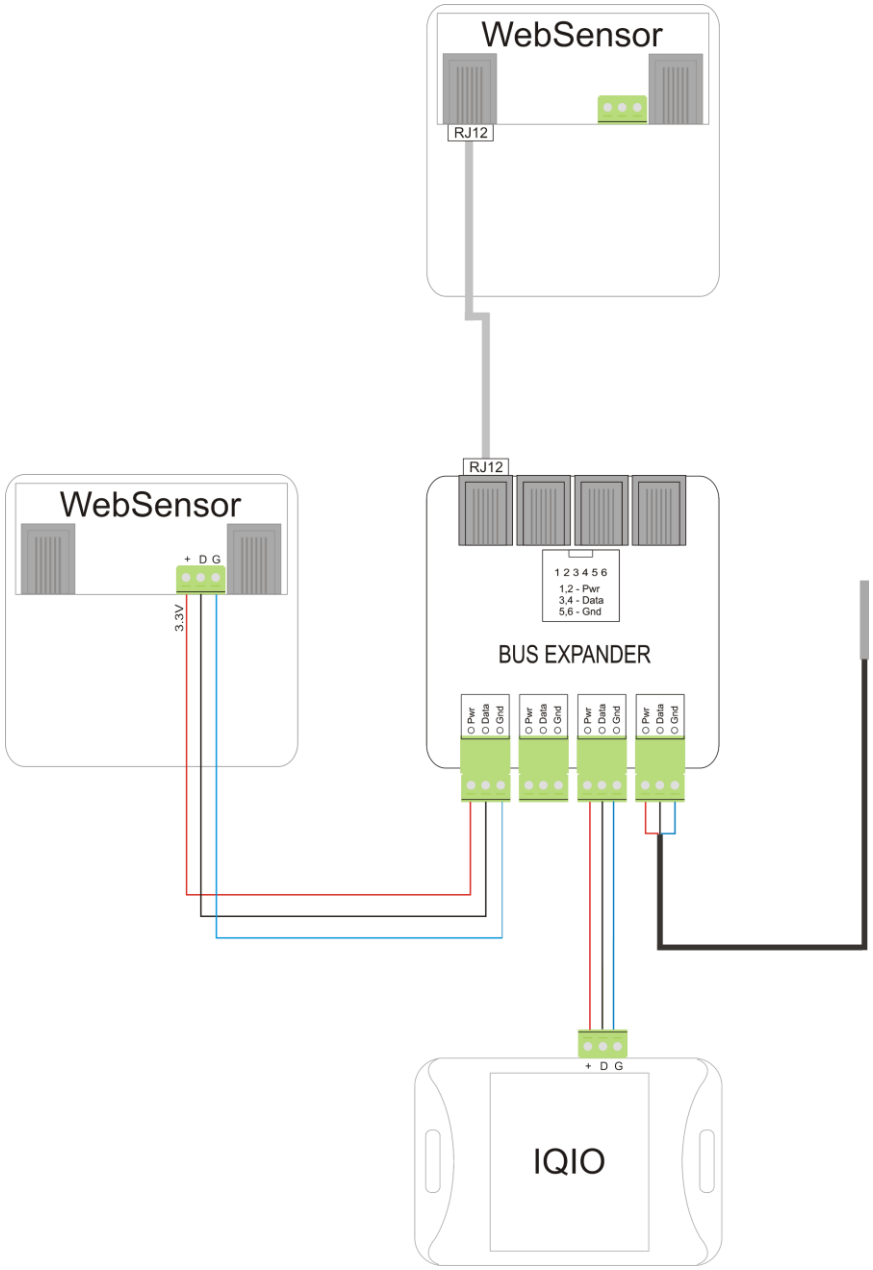
Ways to connect WebSensor devices with IQIO:
- 3-wire cable:



- RJ12 cable + adapter:



- Connection of multiple WebSensors:

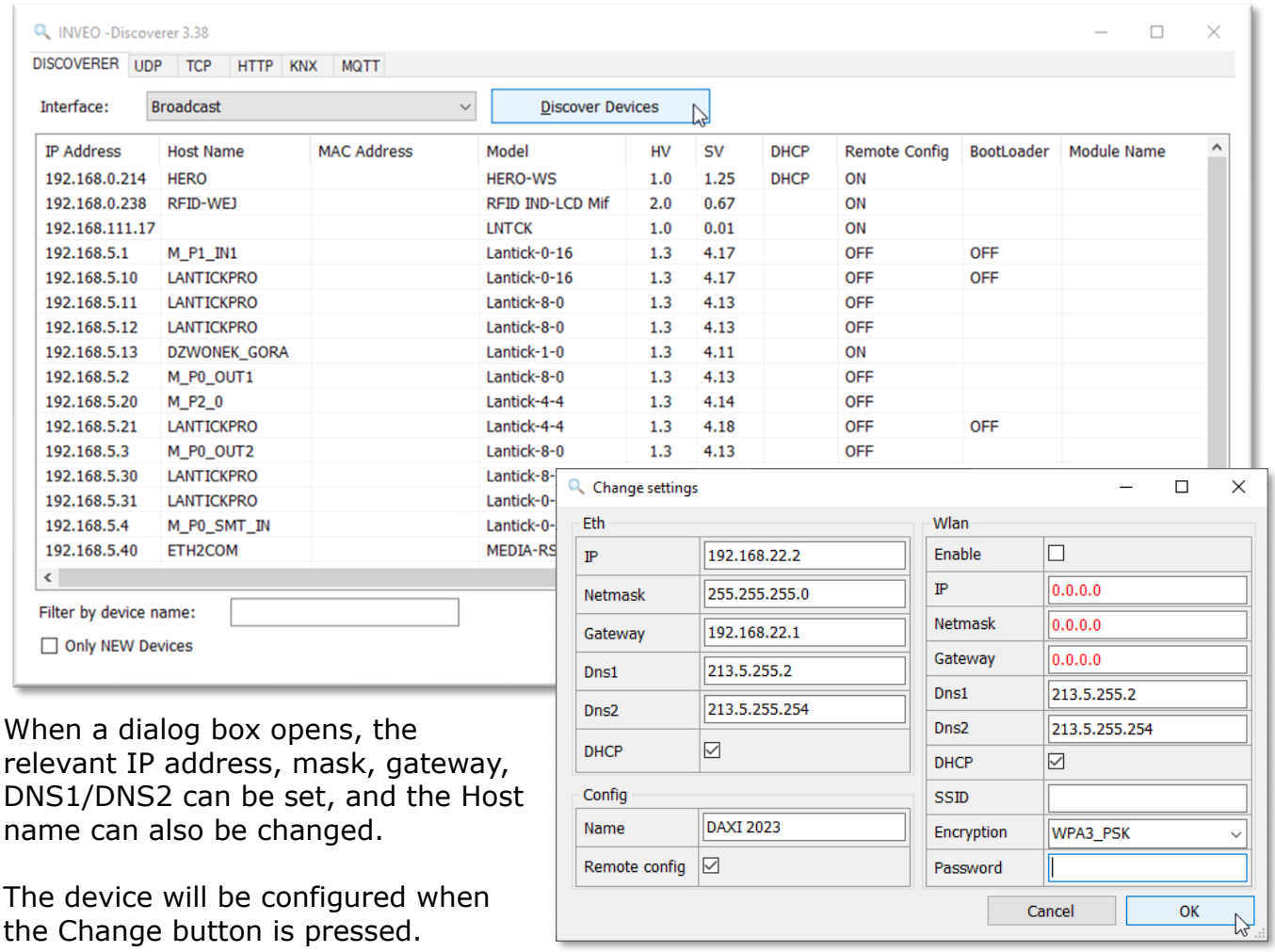


6 Device configuration

On first start-up, it is necessary to configure the device. This can be done in two ways. The simplest method is to use the Discoverer programme from Inveo.

6.1 7.1 Changing the IP address via the Discoverer program

After starting the Discoverer program (available at www.inveo.com.pl) and searching for a suitable device, right-click and then press Change settings.

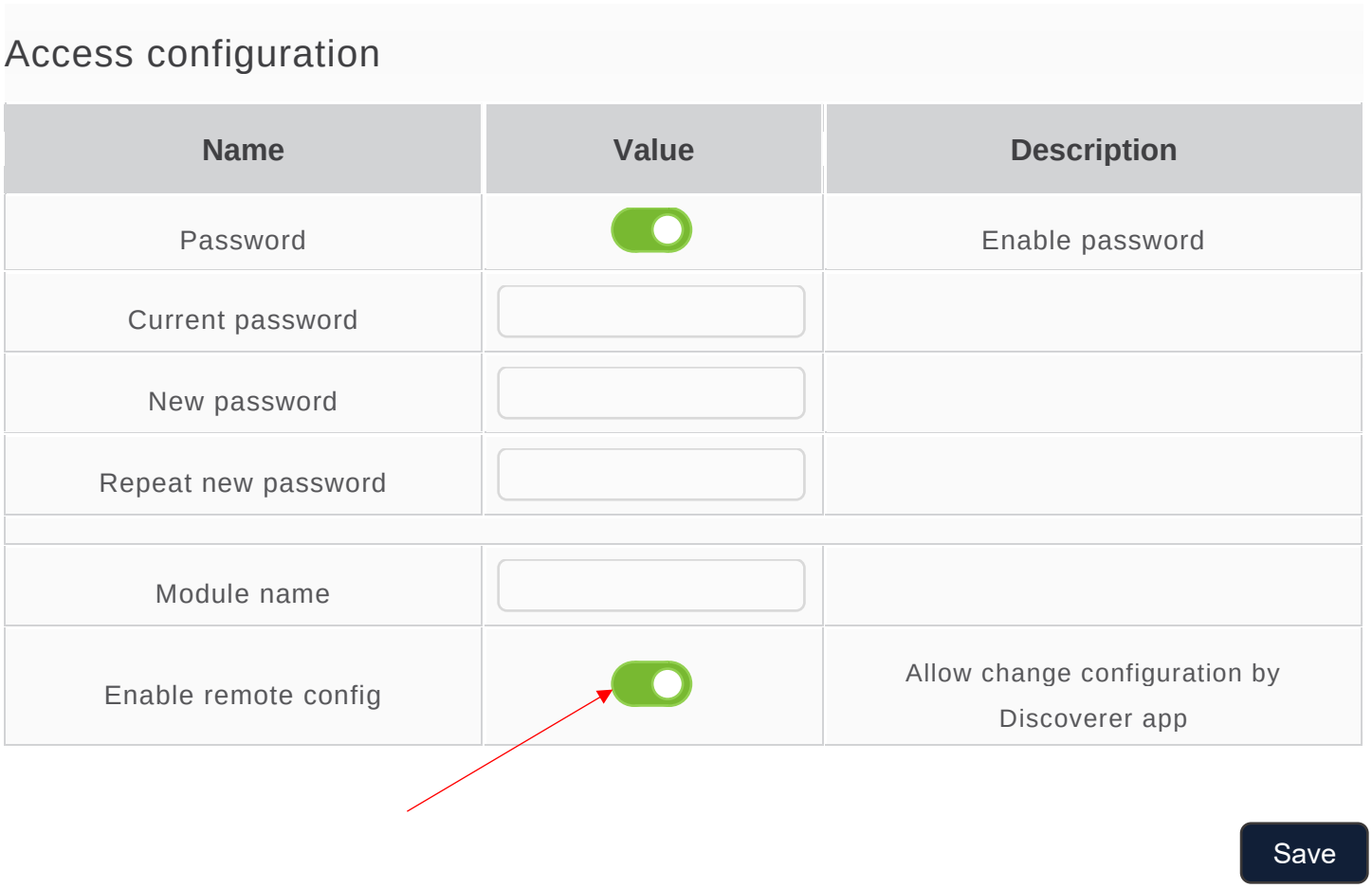


When a dialog box opens, the relevant IP address, mask, gateway, DNS1/DNS2 can be set, and the Host name can also be changed.

The device will be configured when the Change button is pressed.

If Remote Config is disabled (enabled by default), it is necessary to configure the device by changing the subnet of the computer (section 6.2 Changing the subnet of the computer to be configured).

To enable Remote Config, go to the Administration tab, in the Access configuration window select Enable Remote Config.



Then click Save to save the settings.

6.2 Changing the subnet of the computer to be configured

When configuring the device bypassing the Discoverer application, you must first change the subnet address of the computer connected to the same network.
To do this, go to the network configuration of the computer:

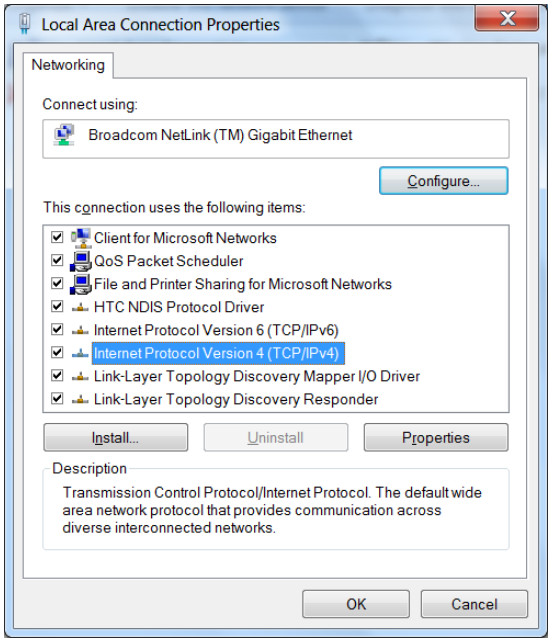
- Press Win + R, type ncpa.cpl and press Enter,

OR

- Start → Control Panel → Network and Internet → Network and Sharing Centre → Change network adapter settings.

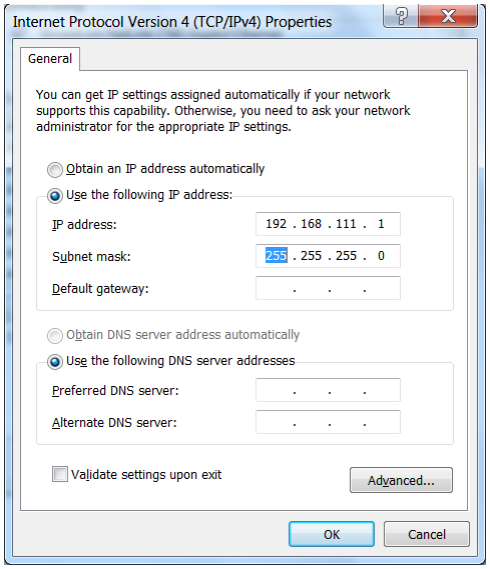
Select your network connection, press the right mouse button and click Properties.

Once selected, the configuration screen will appear:



Changing the network configuration in WINDOWS

Then select the "Internet Protocol (TCP/IP)" setting and enter the following parameters:

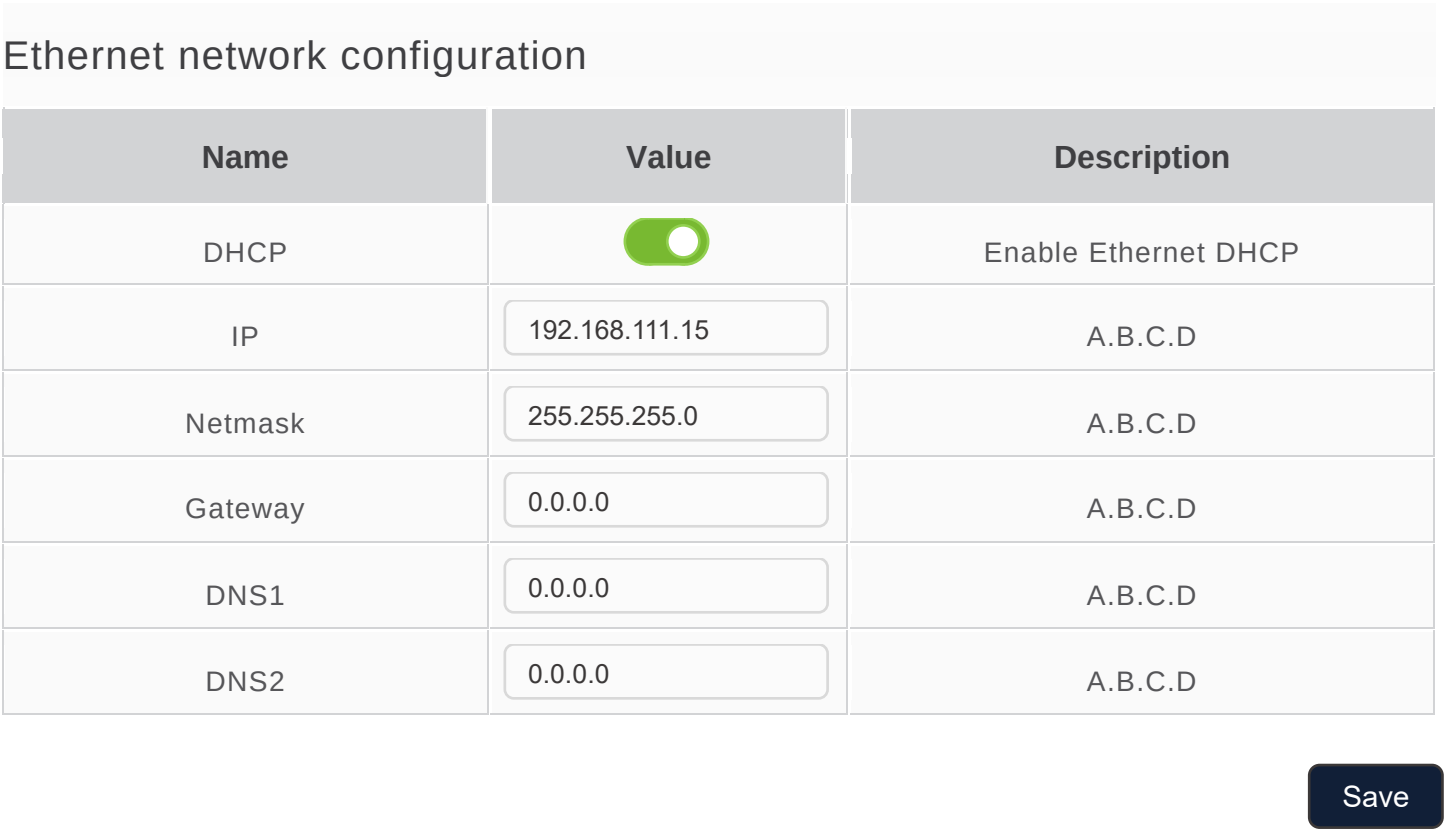


Examples of TCP/IP protocol settings

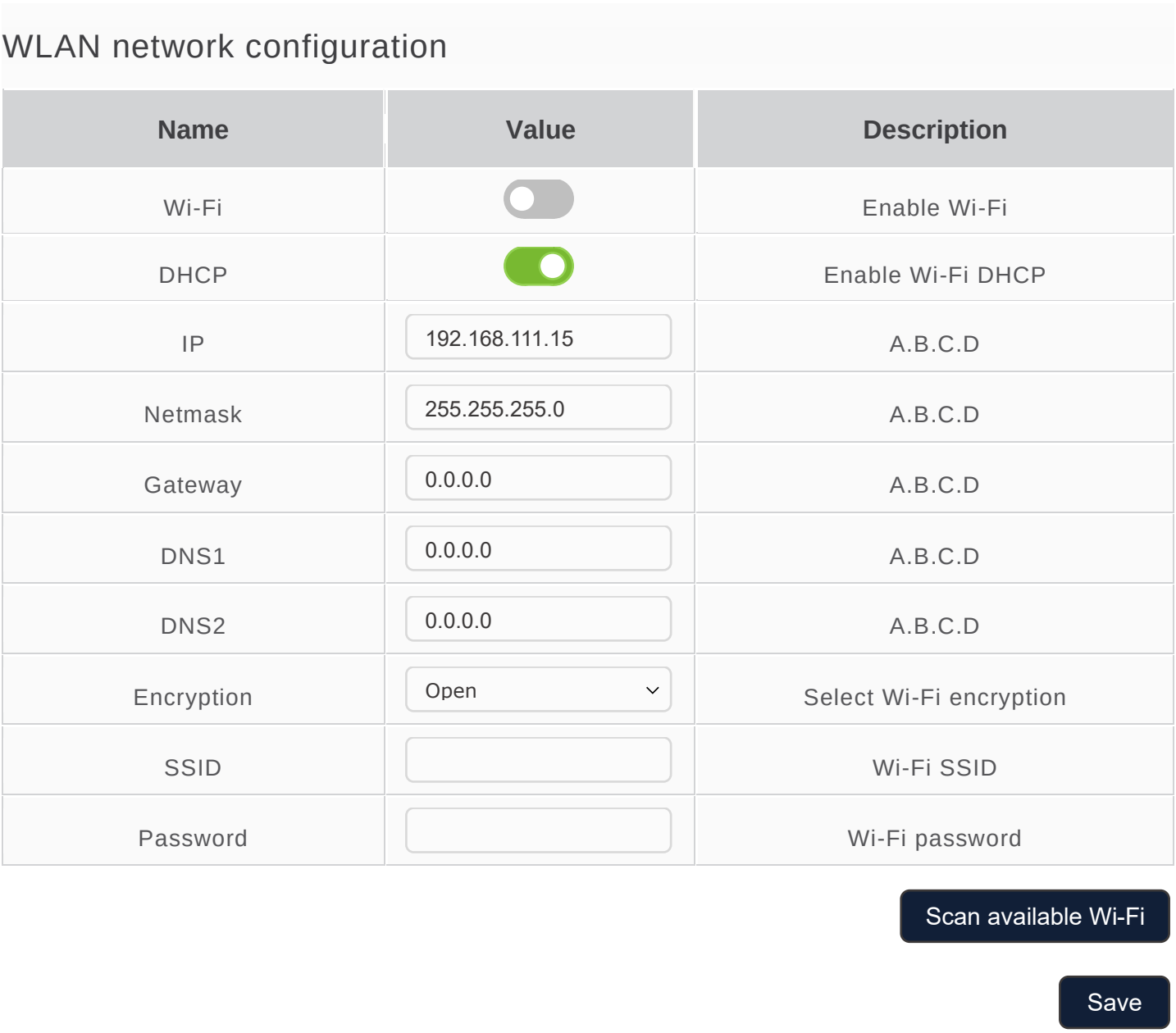
After accepting the settings with the OK button, start your web browser and enter the address: 192.168.111.15. (Default user and password: admin/admin).

6.3 Configuring network settings

To adjust the network settings of the device, go to the Administration / Network tab. Here it is possible to configure parameters such as IP address, subnet mask, gateway, DNS and other network-specific options. This tab enables both wired network configuration (Ethernet network configuration section) and wireless network configuration (WLAN network configuration section).



- **DHCP** – enabling/disabling the DHCP server function,
- **IP** – device IP address,
- **Netmask** – IP subnet mask,
- **Gateway** – network gateway,
- ***DNS1, DNS2*** – DNS server addresses



- **Wi-Fi** - Enable / disable Wi-Fi wireless network support,
- **DHCP** - Enable/Disable DHCP server function in Wi-Fi network, DHCP - Enable/Disable DHCP server function in Wi-Fi network,
- **IP** - device IP address,
- **Netmask** - IP subnet mask,
- **Gateway** - network gateway,
- **DNS1, DNS2** - DNS server addresses,
- **Encryption** - selection of Wi-Fi encryption type:
  - Open
  - WEP
  - WPA-PSK
  - WPA2_PSK
  - WPA_WPA2_PSK
  - WPA3_PSK
- **SSID** - the name of your network,
- **Password** - the password for accessing the Wi-Fi network.

The button 

allows you to search for and display available Wi-Fi wireless networks within the range of the device.

6.4 Configuration mode

Pressing and holding the RESET button will display the IP address.

Configuration Mode – for 3 minutes after power is applied, the unit is in a state where it is possible to change or view some settings. Pressing and holding the RESET button during this time will sequentially display:

- **IP** the current IP address of the device,
- **dhcp eth** – if the RESET button is released at this time, the DHCP function will be disabled / enabled,
- **AP** – releasing the RESET button at the moment when this caption is displayed will enable the configuration of WiFi on the device - see section 6.5 Instructions for setting up the WiFi connection ,
- **rst def** – releasing the button while this text is displayed will restore the device to factory settings.

If the RESET button is released during the interval between subtitles or after the last subtitle is displayed - no changes will be made.

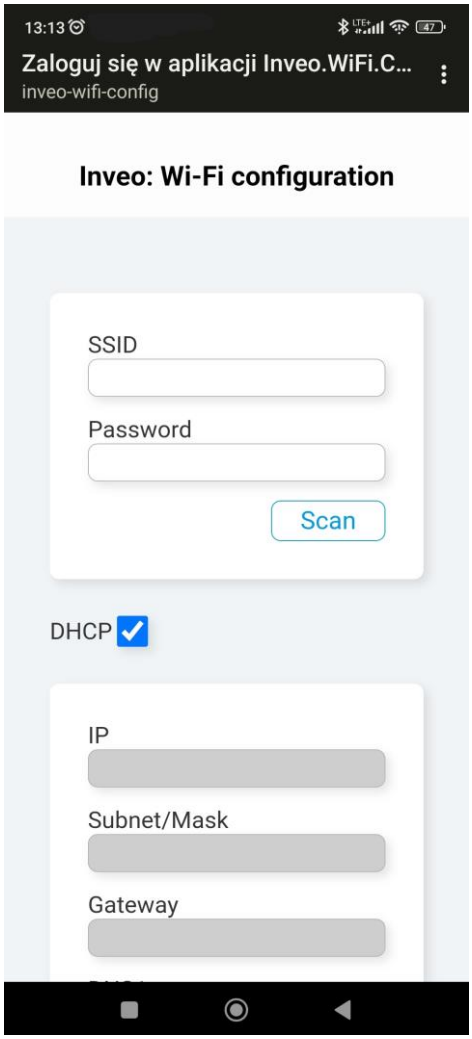
6.5 Instructions for setting up the WiFi connection

Step 1. For three minutes after the device has been powered up (during Configuration Mode, see section 6.4 Configuration mode) it is possible to configure the WiFi connection. To do this, press and hold the "RESET" button until "AP" appears on the device display.

Step 2. Turn on the search for available Wi-Fi networks on your phone or other device. A network named "Inveo-wifi-config" should appear.

Step 3. A network named "Inveo-wifi-config" will appear - connect to it.

Step 4. When the connection is established, press the 'scan' button in the configuration interface or enter the WiFi SSID name in the SSID field.



Step 5. Select the network from the list of available ones to which the device is to be connected.

Step 6. Enter the appropriate password for the selected network.

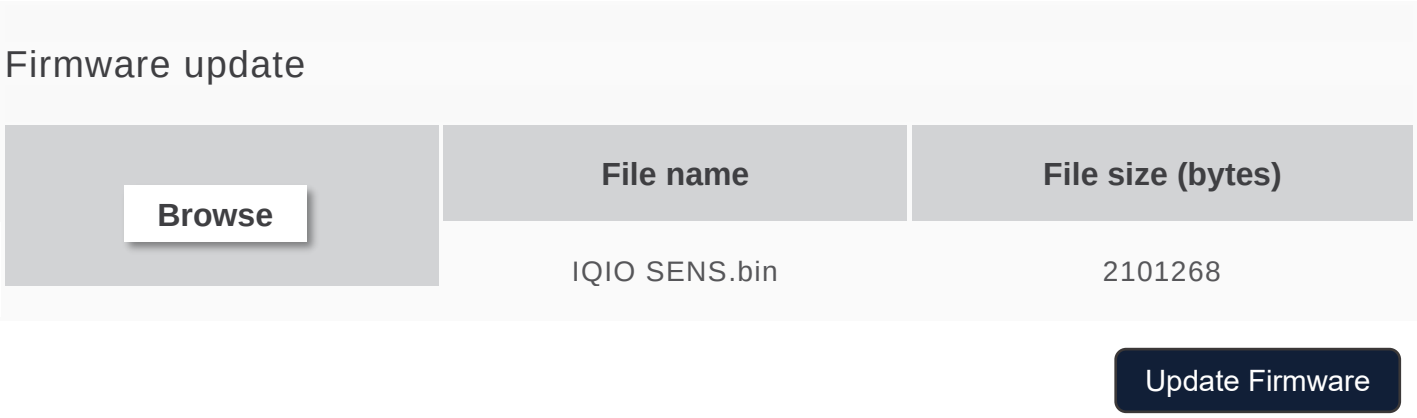
Step 7. If the DHCP server is not available, you can configure the network settings manually after unchecking the "DHCP" option.

Step 8. If the settings are successfully saved, this "SUCCESS" message will appear.

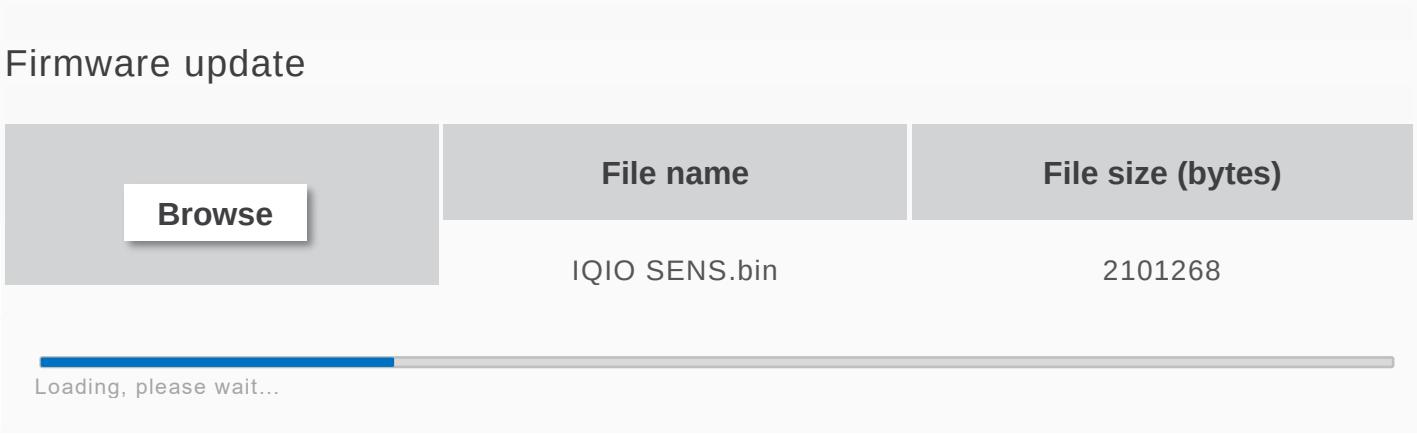
7 Software update

The DAXI device is equipped with a software update facility. The software is supplied as a file with the extension .bin.
To update the software, please follow the following steps:

Step 1. Go to the device's web page to the Administration/Update tab.
Step 2. Using the "Browse" button, locate the previously saved software file on your device.



Step 3. Step 3. Once you have selected the correct file, press the "Update Firmware" button. The progress of the update can be seen.

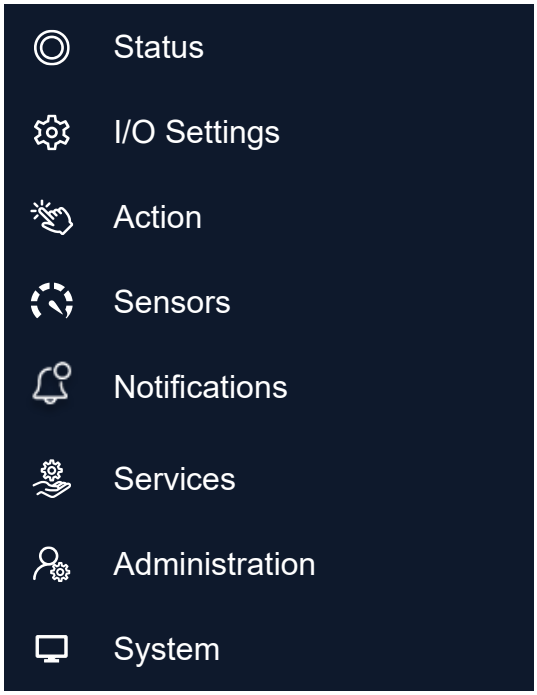


Step 4. Step 4. Once the update is complete, the screen will display the message "Firmware updated, rebooting...". (Firmware has been updated, rebooting takes place). The device will automatically reboot.

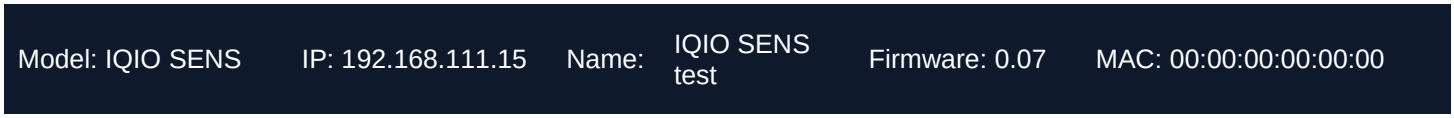
8 Appliance website

The web page interface of the DAXI appliance enables intuitive and advanced management of the device. After entering the device's IP into the browser, a page opens allowing full configuration and customisation of the device's operating parameters according to the individual user's needs.

On the left-hand side of the screen is a list of tabs for quick access to various functions and settings. Available tabs:



An information bar at the top of the page presents itself, providing key data about the device, such as the name, unique name given by the user, model, IP address, software number and MAC address.



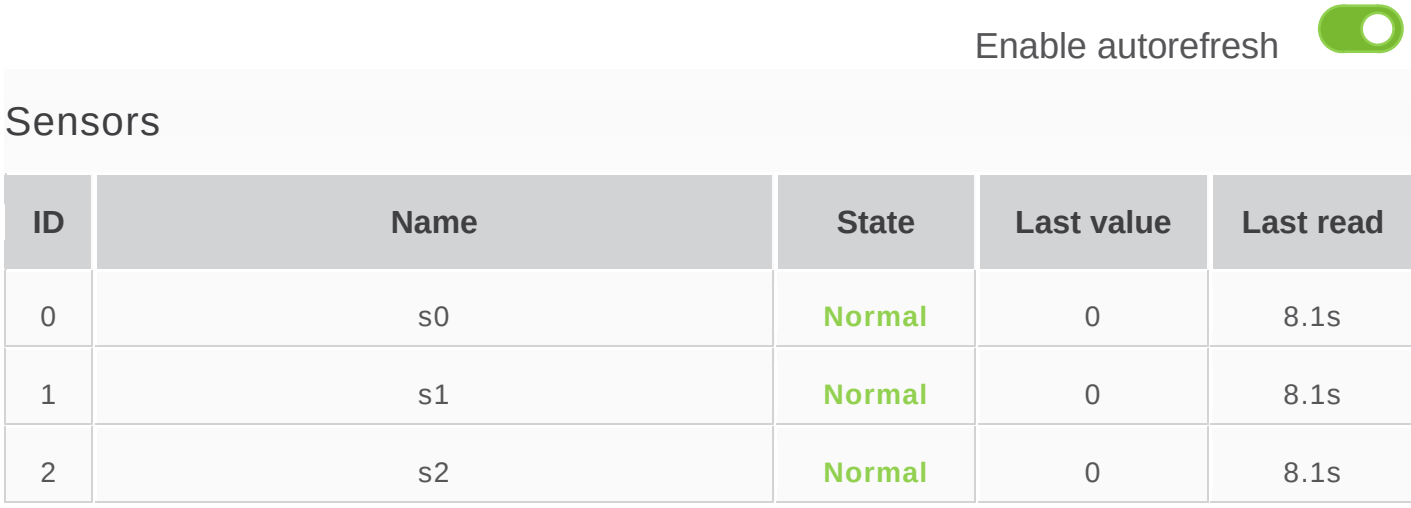
With this website, the user can modify settings, configure parameters and monitor the performance of the device in real time. The DAXI website is a central point of control, enabling the device to be effectively managed and adapted to the user's changing needs.

9 Device status overview (Status)

Under the Status tab, you can find all the information about sensor readings etc.

9.1 Sensors window

The window displays the current readings from the sensors defined on the Sensors tab.



The Enable autorefresh  button can be used to enable automatic refresh of the readings. In the individual columns of the sensor data table, you can find the data:

- **Name** - the name of the sensor as defined in the Sensors tab,
- **State** - status of the sensor:
  - **Error** - reading error (damaged sensor, incorrectly connected, etc.),
  - **Normal** - sensor is providing valid readings that are within normal limits,
  - **Warn L** - low level warning,
  - **Warn H** - high level warning,
  - **Alert L** - low level alert condition,
  - **Alert H** - high level alert condition,
- **Last value** - last value read,
- **Last read** - time elapsed since last read (value updated continuously with automatic refresh enabled).


Tips

The Sensors window is only displayed in the Status tab after any sensor has been configured in the Sensors tab.

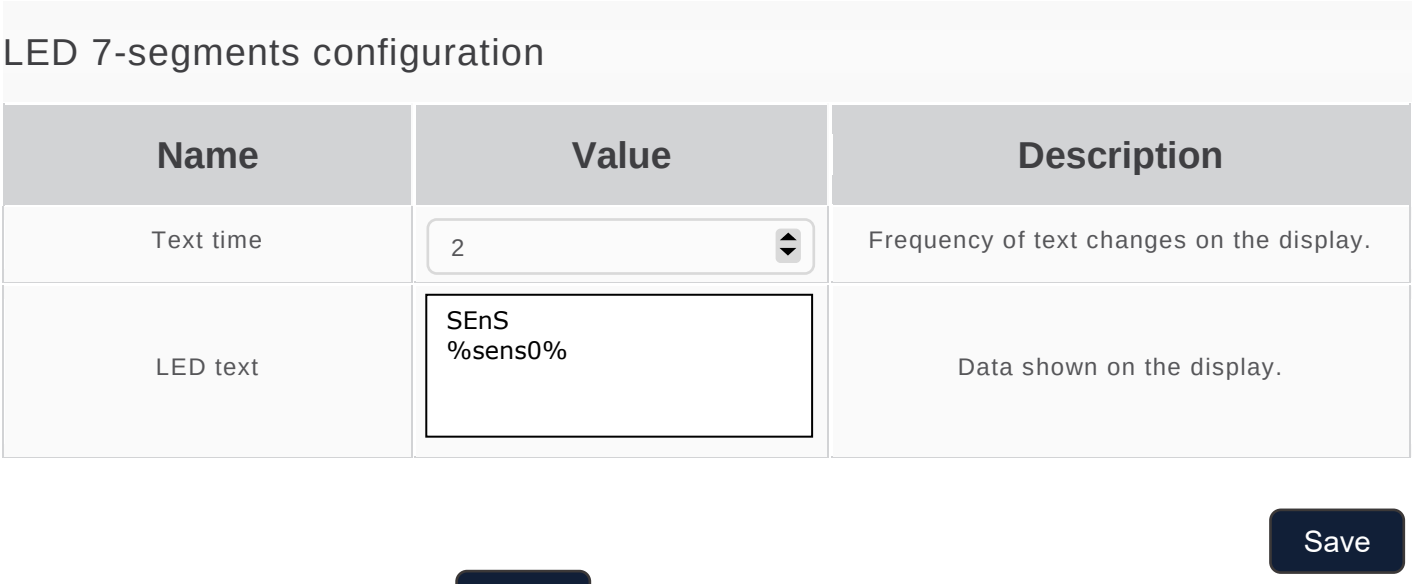
10 Configuring inputs/outputs (I/O Settings)

Under the I/O Settings tab, the user has access to advanced configuration options to configure the display.

Display LED

In this tab, the display settings can be configured.

- Test time – frequency of text changes on the display - expressed in seconds,
- LED text – data displayed on the main screen, you can use the built-in variables described in detail in chapter 17 Built-in variables.



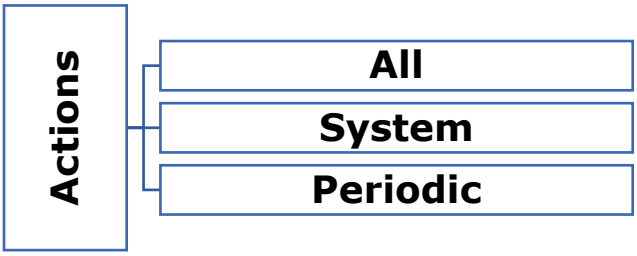
Confirm the settings using the Save .

11 Defining tasks (Action)

IQIO Sens actions are user-defined actions that the device takes in response to specific signals or sensor readings. These can include:

- Sending notifications in the form of an email, MQTT frame, More specifically: automatically sending an alert or message to the user or another system in response to specific conditions.
- Other user-defined actions: actions specific to a particular system or need, such as writing data to a database, activating an alarm, changing the settings of other devices, etc.

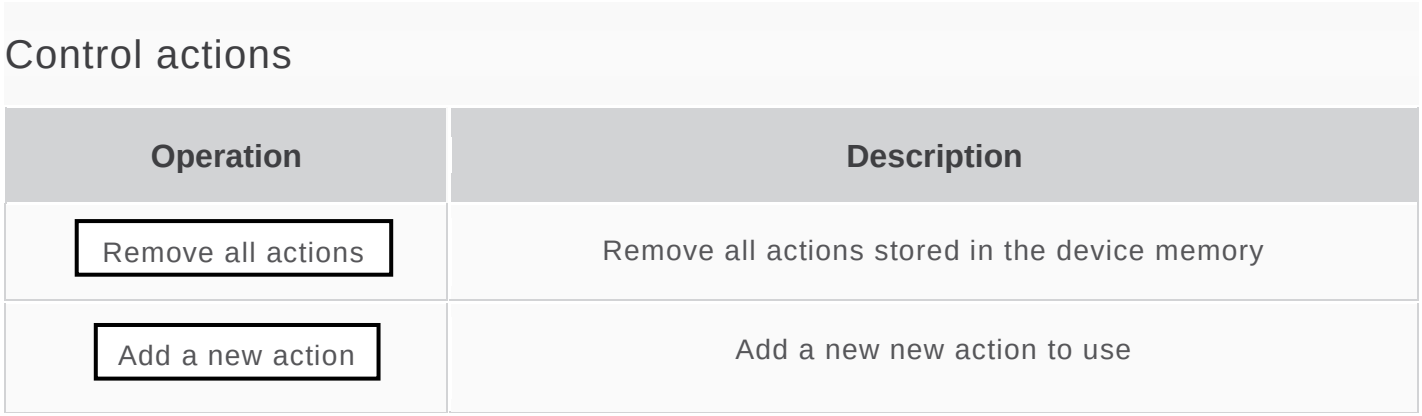
Actions are specific reactions of the IQIO Sens device to received signals and input data, acting according to instructions set by the user. Many functions can be carried out in a number of different methods, depending on your preferences and needs.



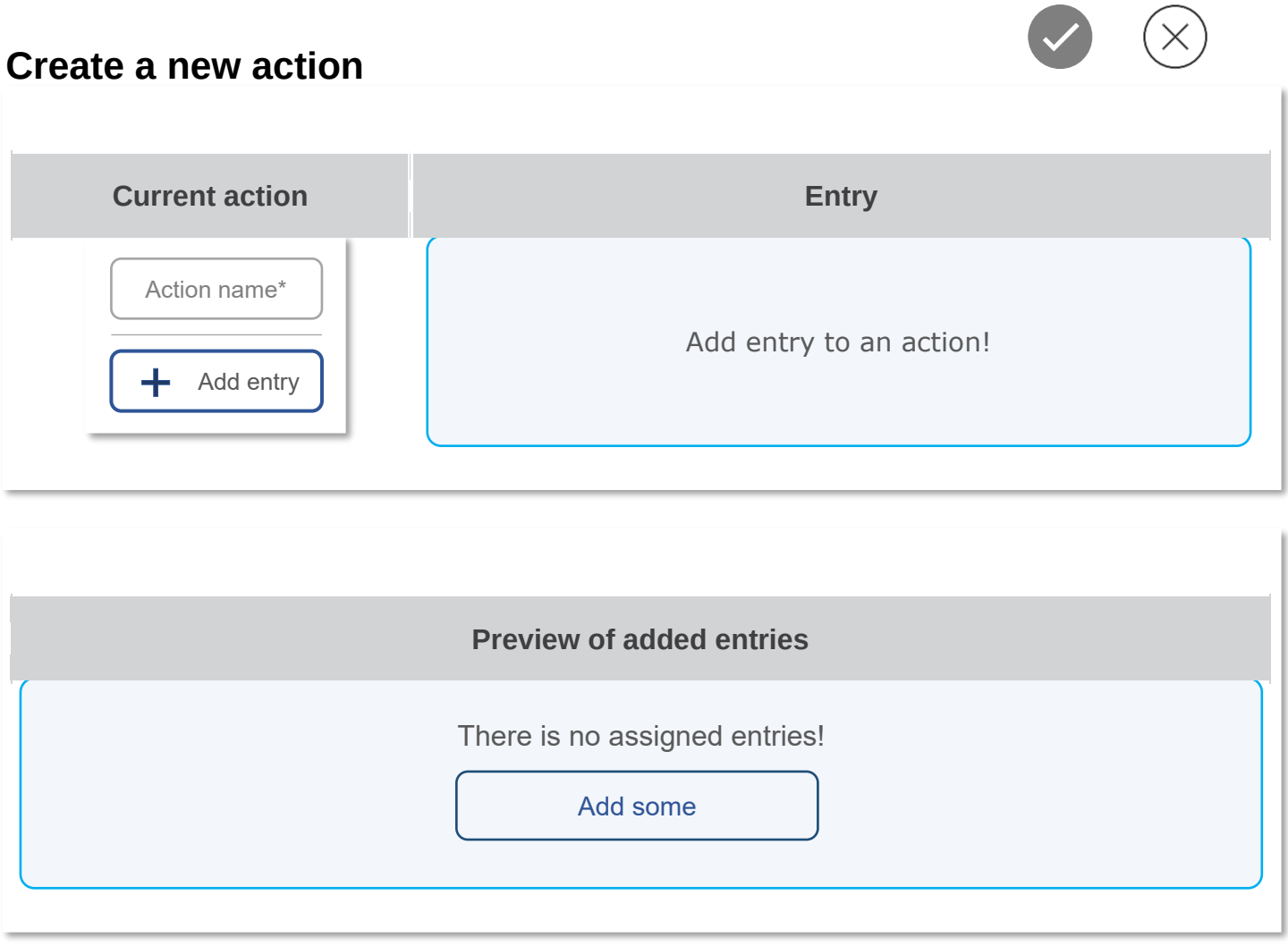
11.1 All

This tab allows you to view and manage the defined actions supported by the IQIO device.

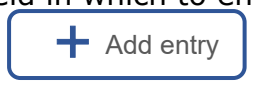
11.1.1 Okno Control Actions



- **Remove all actions** – this button allows you to remove all actions defined on the device,
- **Add a new action** – button enables adding new actions. After clicking on the button, a window is displayed, which allows defining particular parameters of the added action:



Action name – a field in which to enter the assigned name of the action,

Pressing the button 

will enable the selection of the communication protocol and further configuration.

Protocol	Available options	Description
MQTT*	Input MQTT topic	topic to which device sends data
	Input data	
Internal log	Input log message	message body
E-mail*	Input e-mail receiver	target e-mail address
	Input e-mail message	content of e-mail message

*For detailed configuration of communication via protocols, please refer to the Services tab - see chapter 18 System administration (Administration)

After configuring the details of the action to be programmed, press the button 

. It is possible to configure several actions for one event. After defining all required entries, confirm the settings with the button  .

11.1.2 All available actions and All system actions window

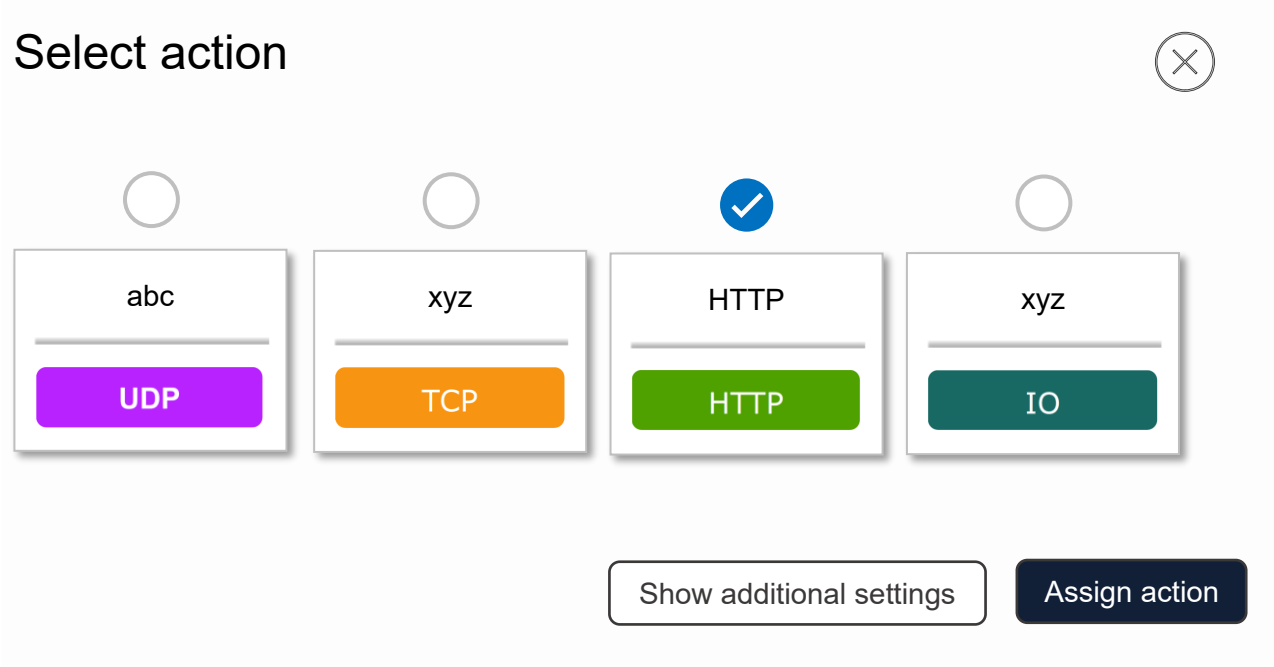
The window shows all defined actions and system actions. Each of them can be:

- edit by clicking the button:  ,
- try it out by clicking the button: 

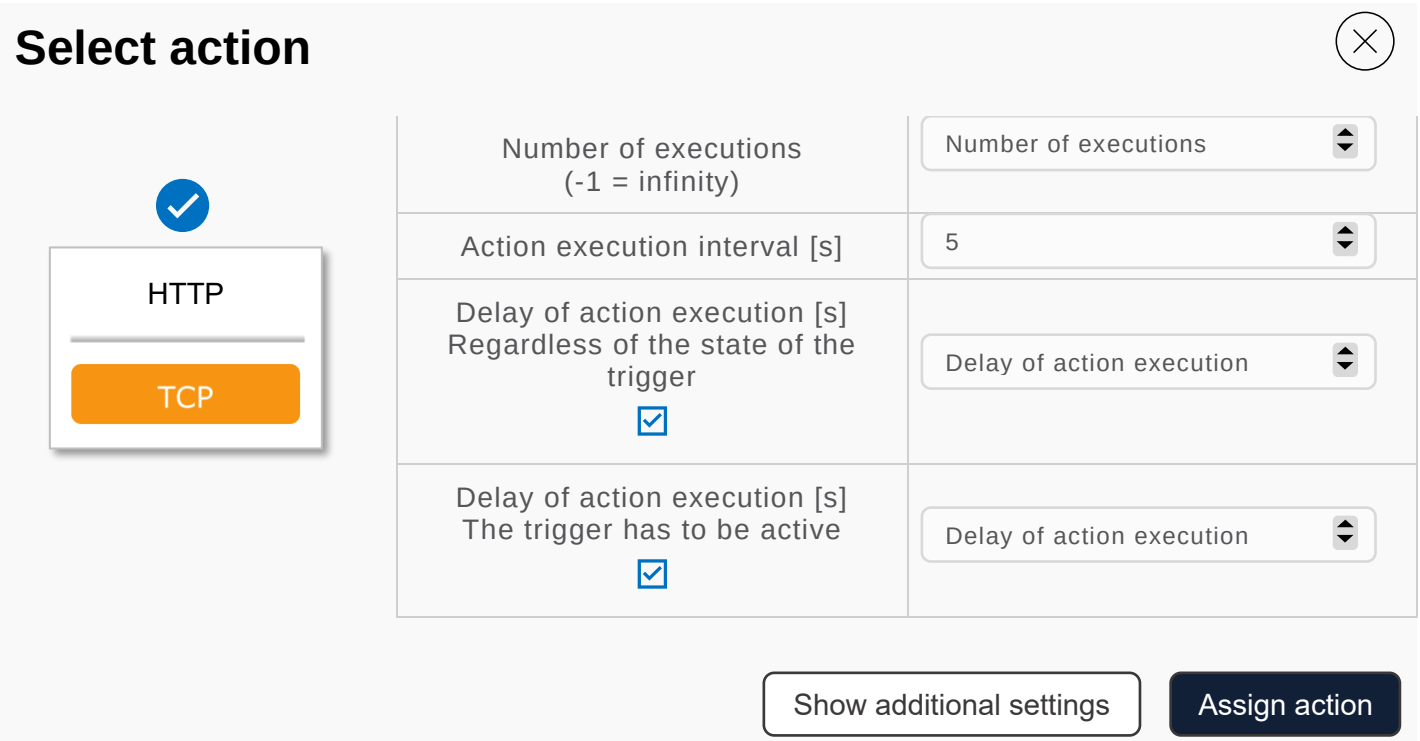
,
- delete it, using the button:  .

11.1.3 Assigning an action

To assign an action to a selected event, click the + button. A dialog box will be displayed where you can select the desired action, previously defined in the All tab - see section 11.1 All.



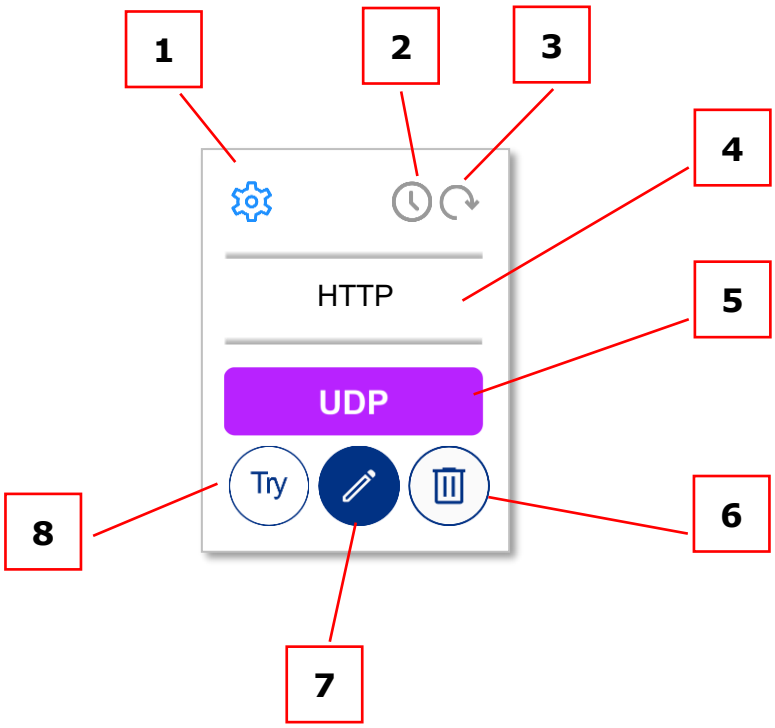
Clicking on the button Show additional settings will display another window, allowing additional settings to be made:



- **Number of executions** – number of actions performed
- **Interval between action executions [s]** – interval between executed actions, if left blank the action will be executed only once,
- **Delay of action execution [s] Regardless of the state of the trigger** – delay of action execution, regardless of the state of the trigger,

- **Delay of action execution [] The trigger has to be active** – delay of action execution, only if the trigger is active.

Confirm the settings with the button Assign action.
After assigning the action, a window appears in the table:



1. Icon for editing additional settings (repetition and delay),
2. Action repetition icon: grey - repetition disabled, green - repetition enabled,
3. Action delay icon: grey - delay off, green - delay on,
4. Action name - assigned by the user when adding or editing settings. action settings,
5. Communication protocol used,
6. Bin icon - clicking in its area will remove the action assignment,
7. Edit icon - clicking in its area will edit the action settings. 8,
8. Action test icon - clicking in its area will cause execution of the action.

11.2 System

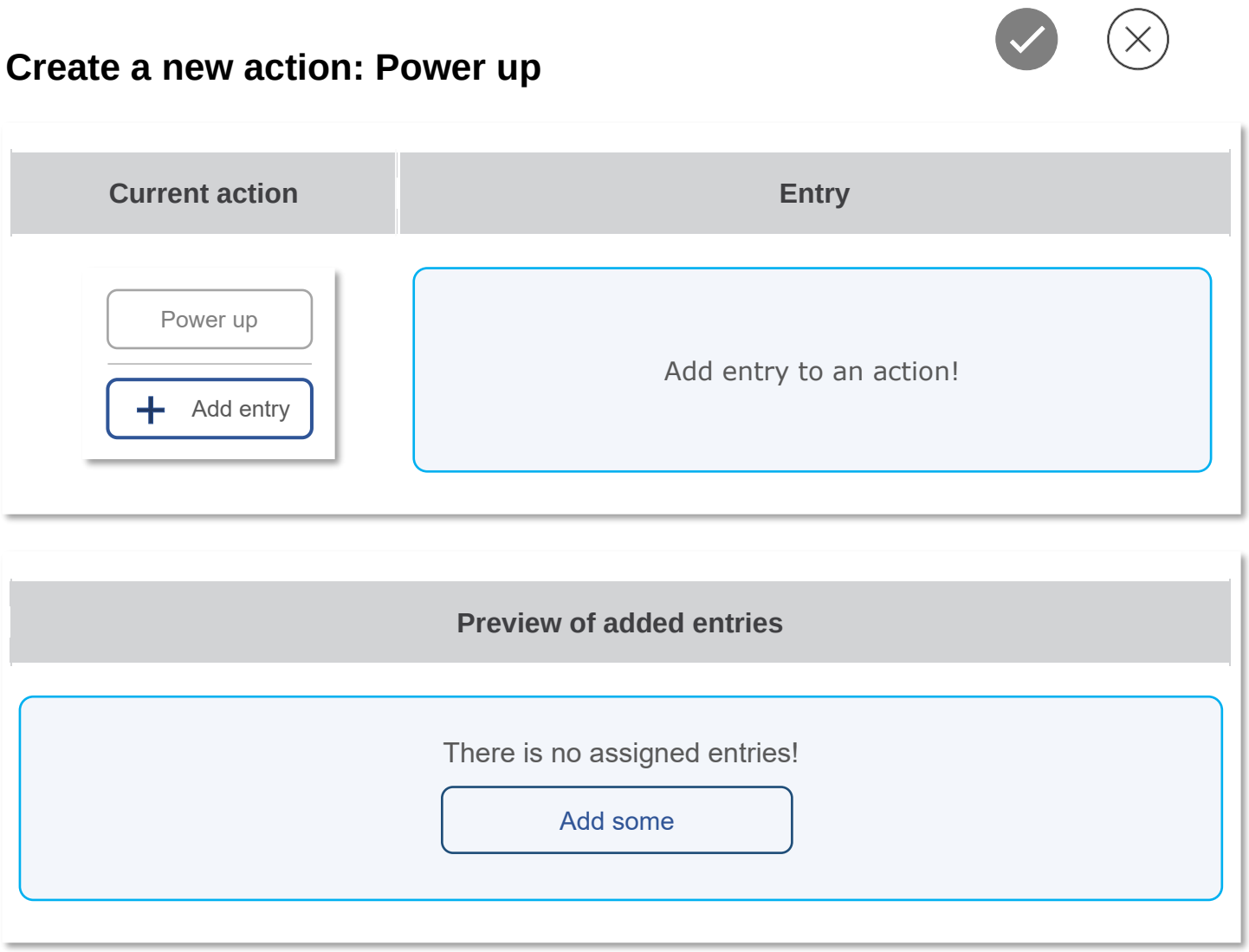
The tab allows you to define the system actions to be performed by the DAXI device when the following events occur:

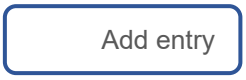
- **Wi-Fi up** – accessing the Wi-Fi network (parameter only available for devices with WiFi),
- **Power up** – restoring power to the device,
- **Ethernet up** – gaining access to Ethernet network,
- **Ethernet down** – Ethernet access lost,
- **Wi-Fi up** – access to Wi-Fi network,
- **Wi-Fi down** – loss of access to Wi-Fi network,
- **Modbus safe mode**

All constant actions

Action type	Entries
Power up ⊕	
Ethernet up ⊕	
Ethernet down ⊕	
Wi-Fi up ⊕	
Wi-Fi down ⊕	
Modbus safe mode ⊕	

To assign an action to the selected event, click the + button. A new dialog box will be displayed:



Press the button  to select the communication protocol and configure it further

- **Select protocol** – the parameters of the individual protocols are described in detail in section 11.1.1 Okno Control Actions.

After configuring the details of the action to be programmed, press the button  . It is possible to configure several actions for one event.

After defining all required entries, confirm the settings with the button  .

11.3 Periodic

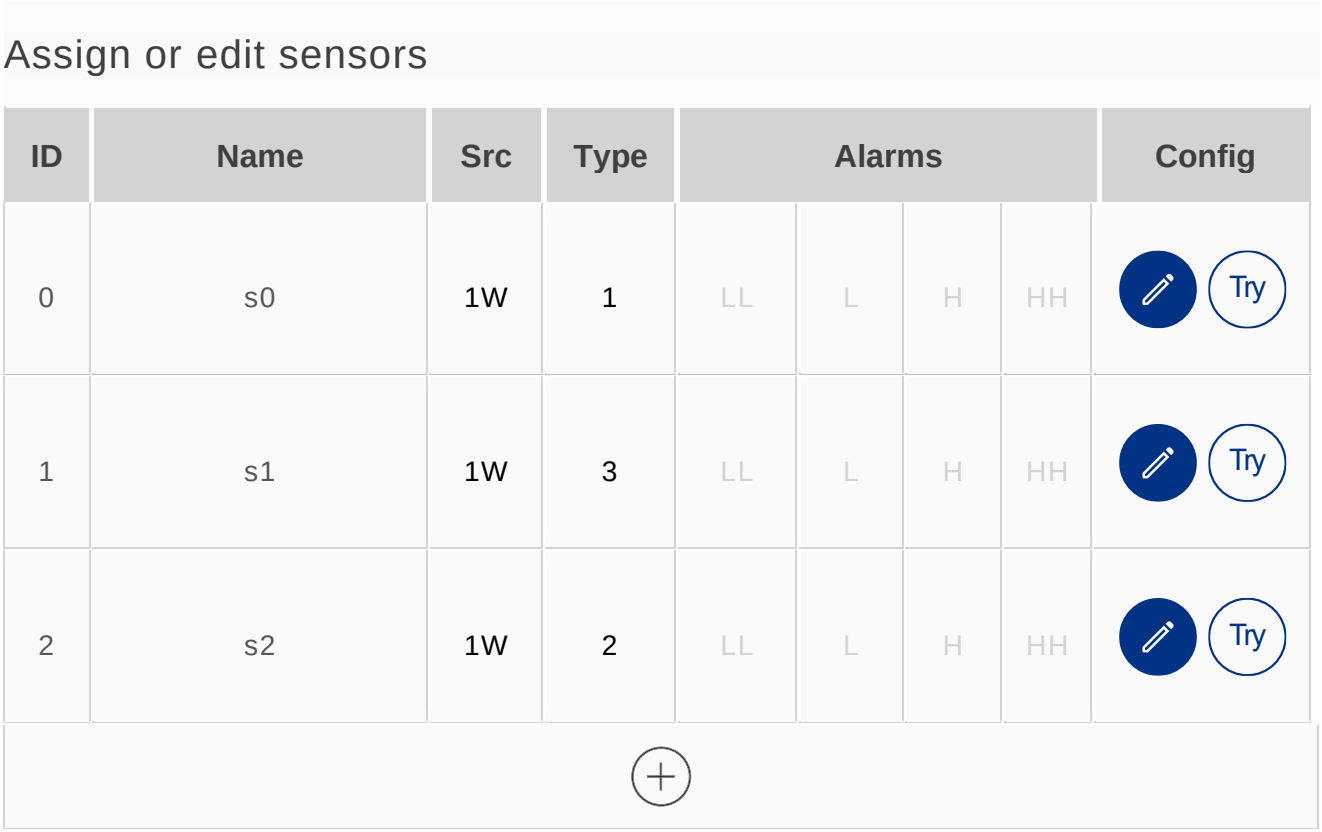
The tab allows the definition of periodic actions - performed at specific intervals.

12 Configuration of sensors (Sensors)

The tab allows individual sensors to be assigned to dedicated memory slots and their parameters to be configured in detail. Allows individual management of each sensor, setting specific parameters and modes of operation.

12.1 All

With this tab, the user has full control over sensor configuration, measurement correction and notification management. It is possible to add new sensors, which automatically integrate with the DAXI system. The user can precisely define the parameters for each sensor, adapting them to their individual needs and operating conditions. In addition, this tab offers tools for editing existing sensors, allowing their settings to be adapted on an ongoing basis to changing conditions or user requirements.

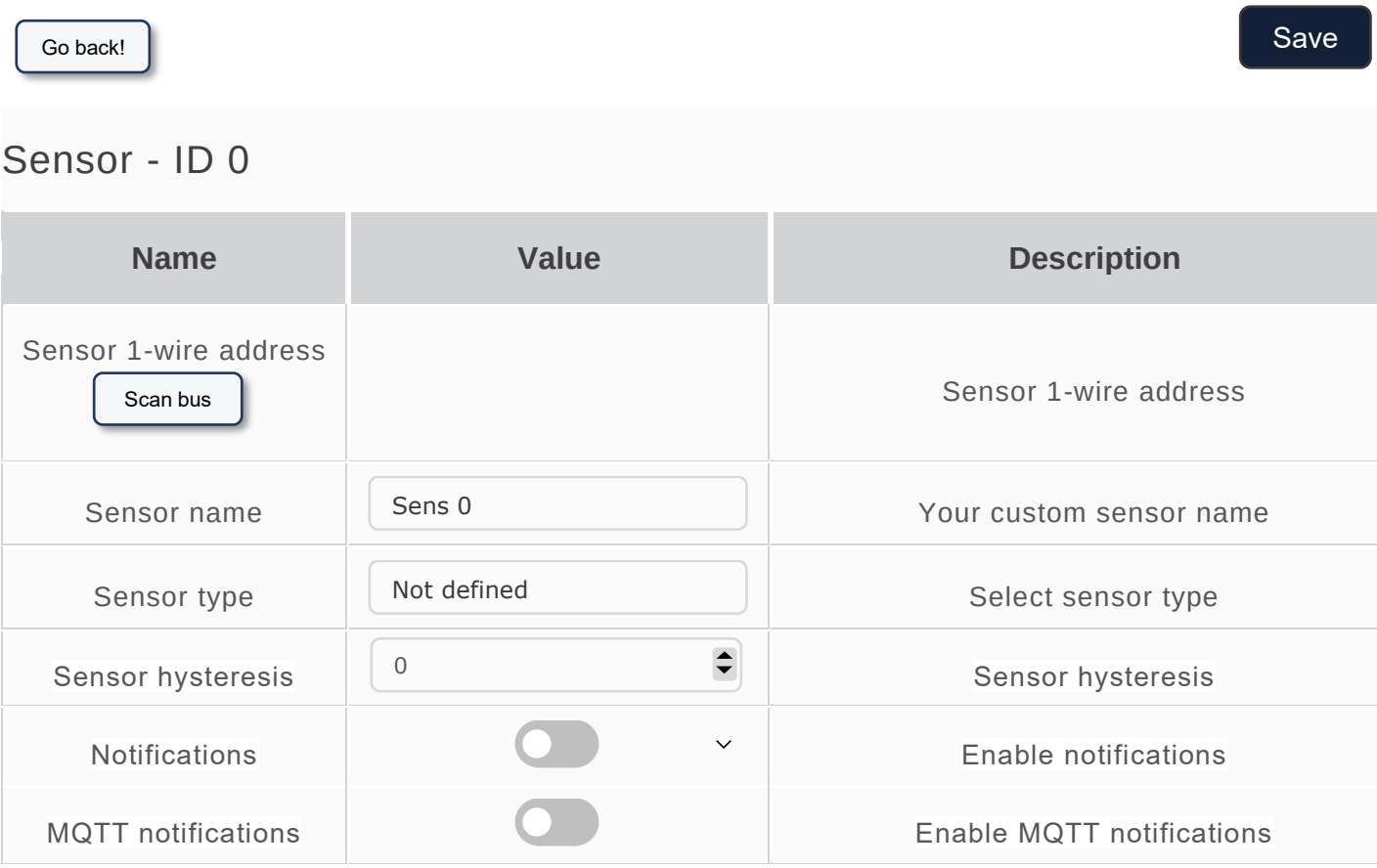


The individual columns of the sensor table contain the following information:

- **ID** – sensor identification number,
- **Name** – sensor name,
- **Src** – source from which the sensor readings are taken (1-Wire or Modbus poller)
- **Type** – type of connected sensor:
  - – temperature sensor,
  - – humidity sensor,
  - – input,
  - – analogue current sensor 4-20mA,
  - – pressure sensor,
  - – 0-10VDC analogue voltage sensor,
- **Alarms** – activated alarms:
  - **LL** – low level alarm threshold activated,

  - **L** – low level warning alarm threshold activated,
  - **H** – high level warning alarm threshold activated,
  - **HH** – high level warning alarm threshold activated
- **Config** – sensor configuration buttons:
  -  - button for editing sensor parameters,
  -  - delete sensor

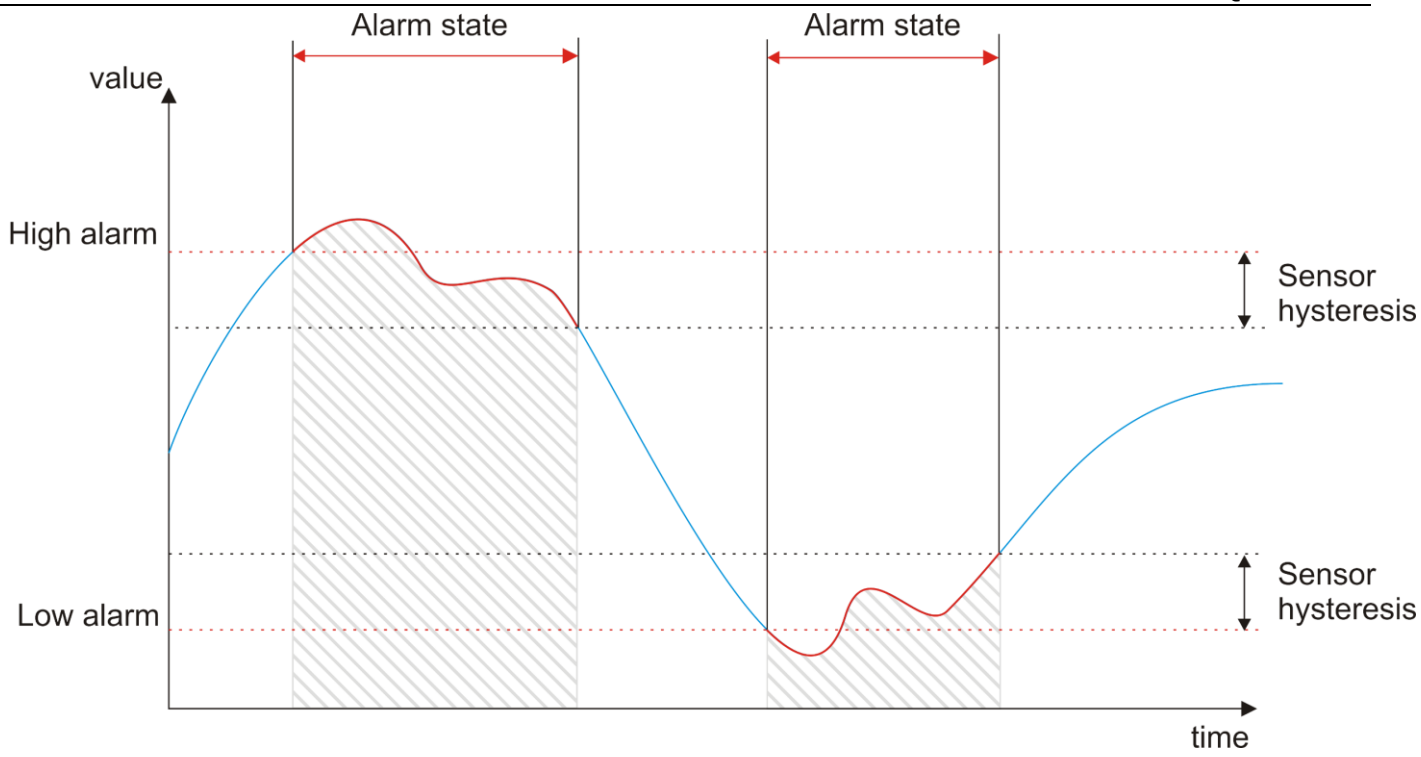
After clicking on the button for editing sensor parameters, a dialog box is displayed on the screen:



- **Sensor 1-wire address** – the Assign button is used to find and assign the sensor connected to the device,
- **Sensor name** – name of the sensor,
- **Sensor type** – type of sensor: temperature sensor, humidity sensor, input, raw value, pressure sensor, voltage detection sensor,
- **Sensor hysteresis** – (parameter not active when sensor type Input is selected) - applies to alarm and warning states. The hysteresis defines the maximum permissible difference between the alarm/warning value and the return to normal state.

Example:
The alarm value set in the High warning parameter is 30 degrees, the hysteresis is 2 degrees. When the sensor reaches 30°C, the device will enter the sensor alarm state, which will be maintained until the value on the sensor drops to 28°C (30-2=28).

The hysteresis is the interval between activation and deactivation of the alarm / warning, it provides stability by eliminating the possibility of frequent switching of alarm states in case of small fluctuations in the measured value.

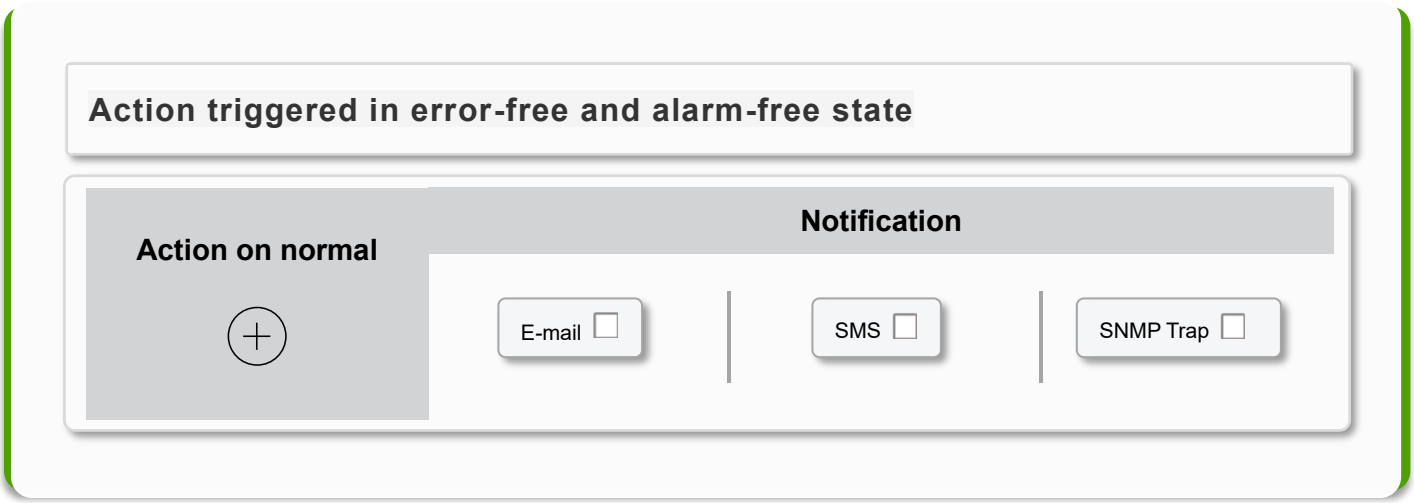


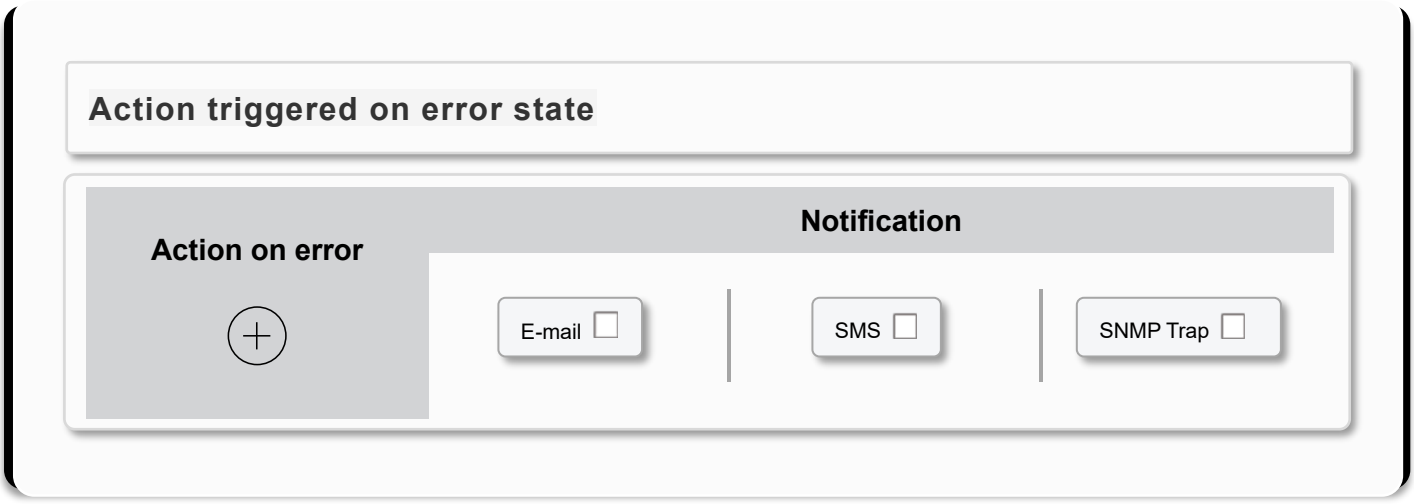
- **Channel** – channel selection - parameter active only when Input sensor type is selected,
- **Sensor log** - switching on / off the recording of sensor data in the device memory,
- **Notifications** – switching on/off of notifications,
- **MQTT notification** – enabling/disabling MQTT notifications.

Enabling Notifications allows editing the device's response window to:

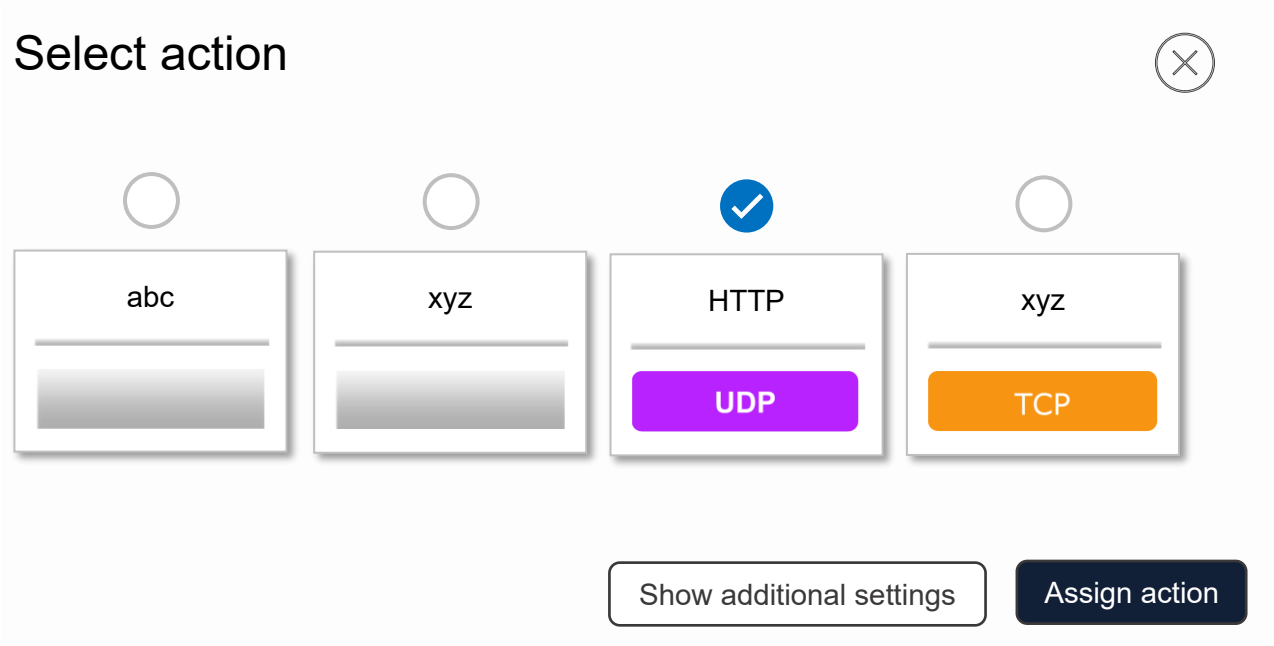
- Transition of the sensor into non-alarm and non-error mode
- Transition of the sensor to an error state

The user can choose the type of notification that will be sent in response to the above events. In order for notifications to be sent, the relevant functions must be configured in advance in the Services tab.





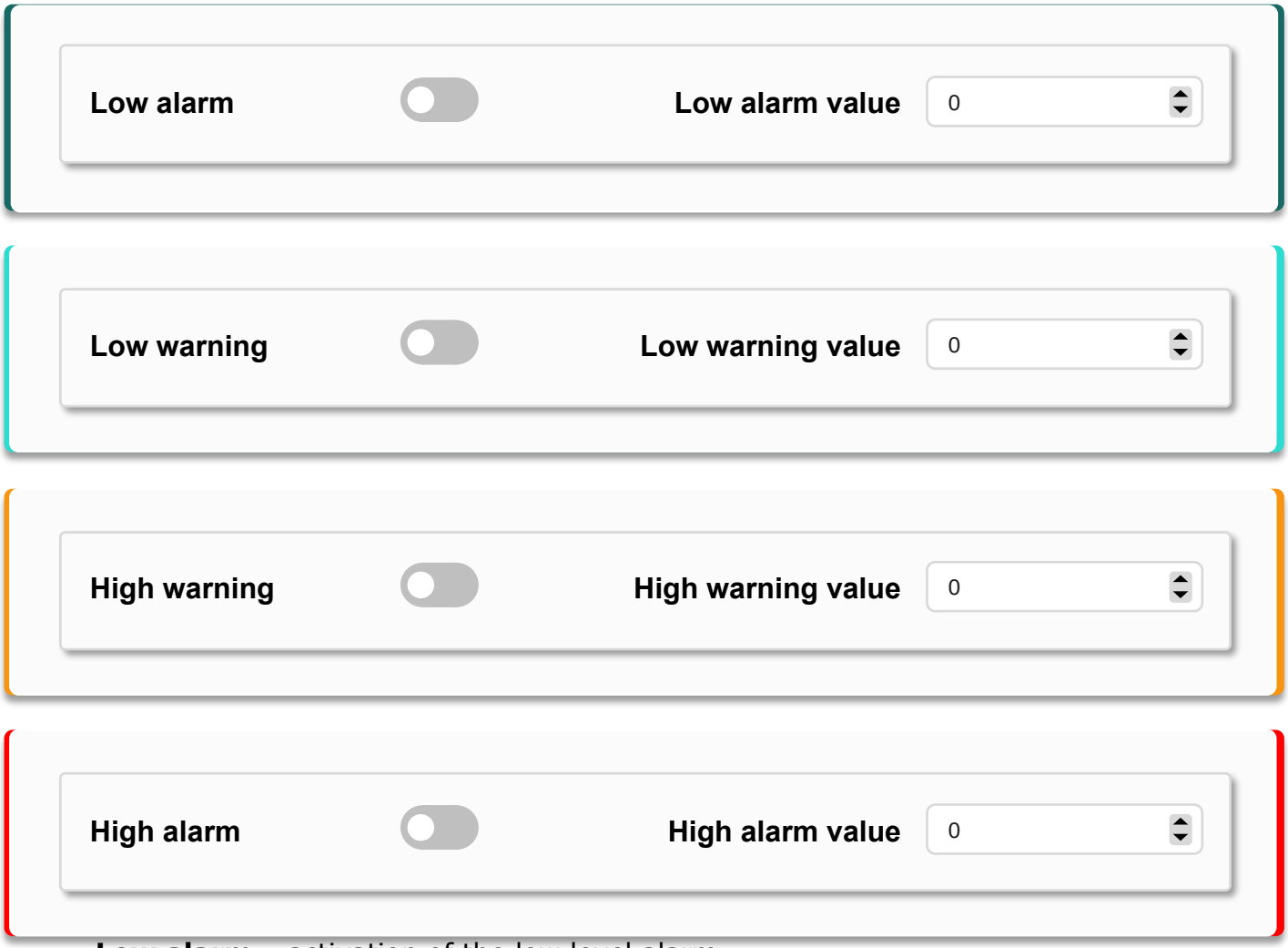
To assign an action, click the + button. A dialog box will appear in which you can select the desired action, previously defined in the All tab - see section 11.1 All.



The procedure for assigning an action is described in detail in chapter 11.1.3 Assigning an action.

12.1.1 Alarm configuration

In the settings section dedicated to the configuration of sensor alarms, the user gains full control over the customisation of alarm parameters. This allows you to configure precise alerts and responses to significant sensor events.



- **Low alarm** – activation of the low level alarm,
- **Low alarm value** – the sensor value at which the sensor will go into alarm,
- **Low warning** – activation of low level warning, approaching alarm state,
- **Low warning value**– the sensor value at which the sensor will go into warning state,
- **High warning** – activation of high level warning, approaching alarm state,
- **High warning value** – sensor value at which the sensor will go into alarm state,
- **High alarm** – activation of high level alarm,
- **High alarm value** – sensor value at which the sensor will go into a warning state,

When an alarm is activated, an additional window appears that allows the user to customise the device's response to the alarm situation. Here, the user can configure notifications and assign the execution of a specific action (see section 11.1 All)

Sensor corrections final = a * (x + preoffset) + b		
Sensor preoffset	0	Sensor preoffset correction
Sensor multiplication 'a'	1	Multiplying sensor value
Sensor offset 'b'	0	Constant value correction

- **Sensor preoffset** – this field is used for sensor preoffset correction, according to the formula of the linear function f(x)=ax*b,
- **Sensor multiplication 'a'** – multiplying sensor value,
- **Sensor offset 'b'** – correction of a constant value.

12.2 ⟶ Operating the sensor

To be sure of accurate and reliable sensor readings, it is recommended to follow the detailed step-by-step guide below, covering connection, assignment and configuration of the sensor.

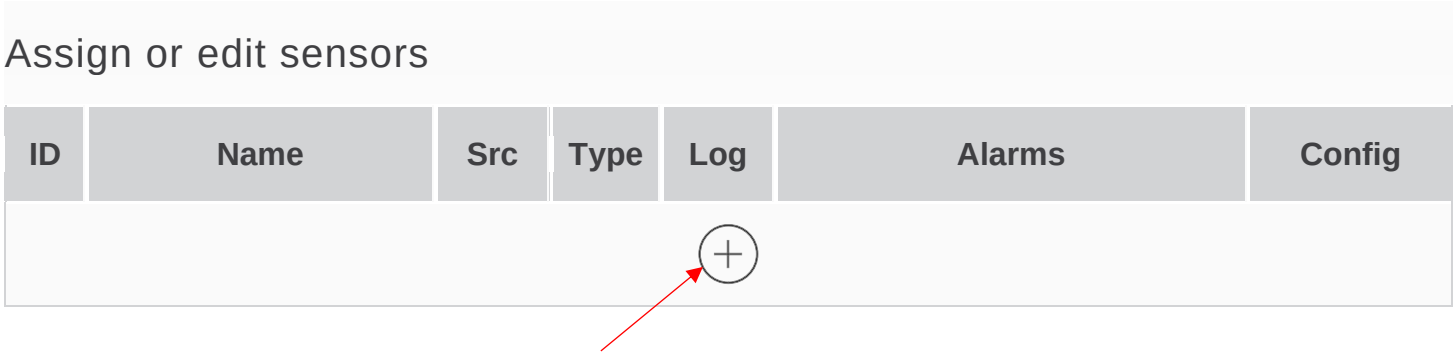
12.2.1 Assigning the sensor

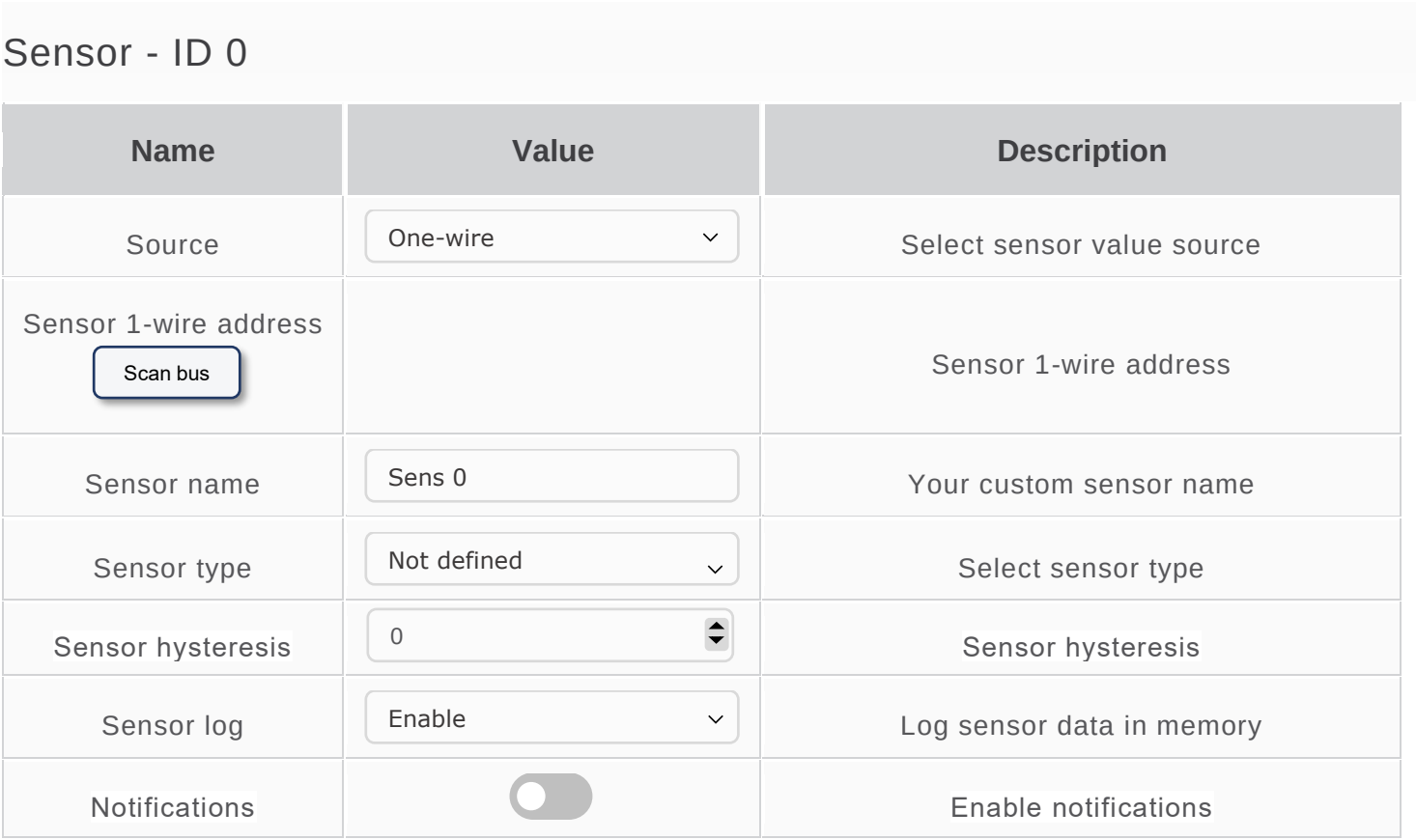
First connect the sensor to the device - see section 5.2 Connection diagram.

Then, using the device's website, you must locate, assign and configure the sensor's basic parameters. If no sensors have been connected to the DAXI device before, you can use the option to automatically assign them. Simply reset the device after connecting the sensors. When DAXI restarts, it will automatically recognise and assign the available sensors, also specifying their type.

The step-by-step process of manually configuring the sensors is described below.

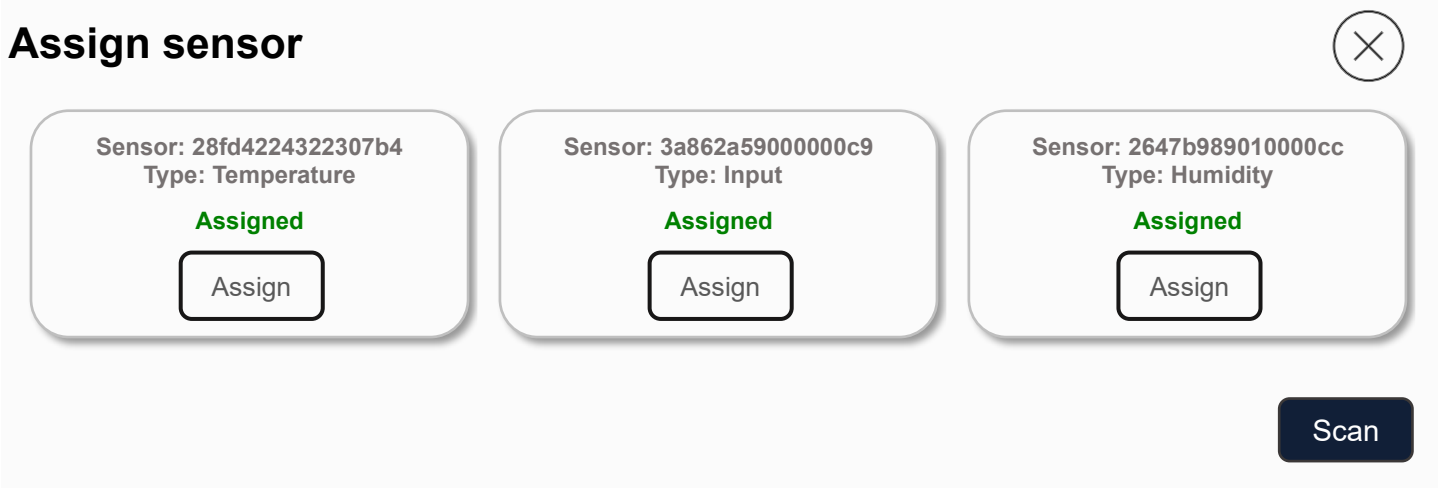
Step 1: Under Sensors / All - click the + buton:





In the dialog box that appears, the first step is to select the source of the sensor - the Source parameter. In this case, select One-wire (sensor physically connected to the Daxi bus).

Assign a sensor by starting with the icon Scan bus, which brings up a window showing the sensors detected by DAXI that are connected:

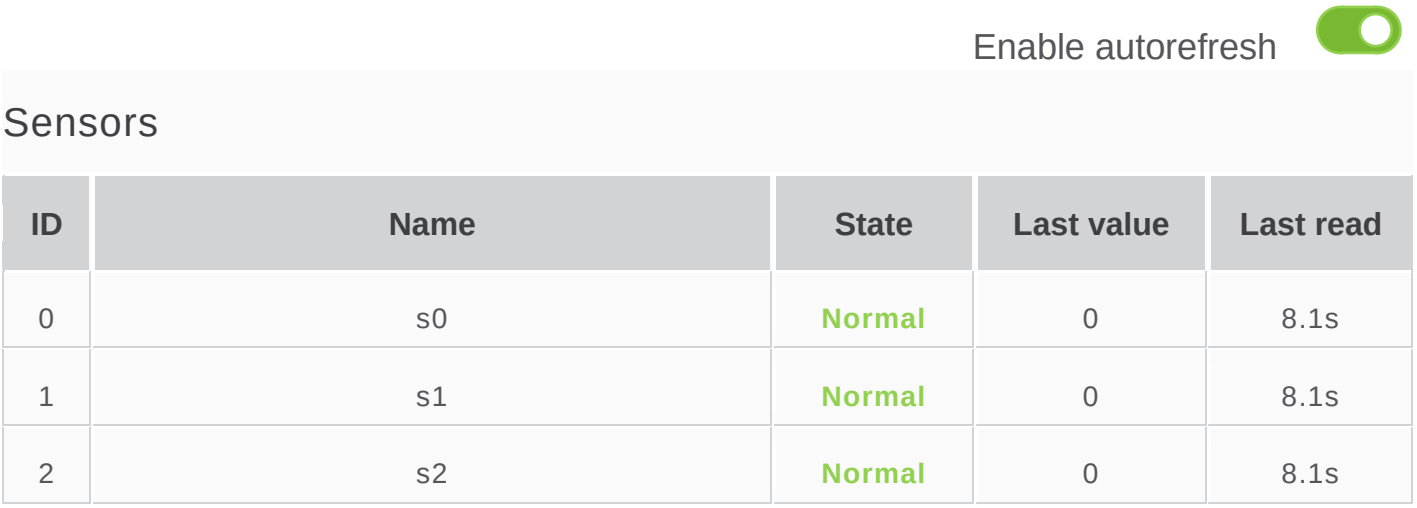


Assign the selected sensor by clicking on the Assign button.

Step 2: Configure the basic parameters.

In the sensor configuration window, the correct sensor type must be set, a name can be given, etc. All settings should be confirmed with the button Save.

Step 3: Preview in the Status tab
A correctly configured sensor will result in the readings being displayed in the Status tab of the Sensors window:



13 Configuration of notifications

The Notifications tab allows the configuration of various notifications - enabling, disabling and assigning notifications, including E-mail, SMS, SNMP Trap, MQTT, concerning the operation of sensors, inputs and outputs.

In order for notifications to be sent effectively you must:

Step 1. Enable the notification option in the Sensors tab, see section 13.1 Sensors, for the type of notification,

Step 2. Depending on the selected notification type - SMS, e-mail, SNMP Trap, MQTT - make the configuration in the Services tab - see chapter 14 Network services (Services.

Step 3. Enable the notification option in the Configuration tab - see chapter 13.2 Configuration

13.1 Sensors

In the Sensors tab, it is possible to adjust the notification settings related to the operation of individual sensors. Notifications for the selected sensor can be activated in two ways: in the Sensors tab, during the configuration of the sensor (see chapter 12 Configuration of sensors (Sensors)) or by clicking on the icon  in the Notifications / Sensors tab.
Full personalisation is possible in the configuration window that appears when the notifications function is activated:

s0				
State	E-mail	SMS	SNMP Trap	MQTT
Info	☐	☐		
OK	☐	☐	☐	
Error	☐	☐	☐	
Alarm low (disabled)	☐	☐	☐	☐
Warning low (disabled)	☐	☐	☐	
Warning high (disabled)	☐	☐	☐	
Alarm high (disabled)	☐	☐	☐	

It is possible to attach E-mail, SMS, SNMP Trap and MQTT notifications.

> **Tip** In order for E-mail, SMS, SNMP Trap and MQTT notifications to function correctly, these options must be configured in the Services tab - see chapter 14 Network services (Services).

In the table displayed, the user has the option to select what type of notifications are to be sent in response to the occurrence of specific events:

- **Info** - periodic information about the state of the sensor,
- **OK** - state of sensor's return to normal operation in a previous error or alarm state,
- **Error** - state of sensor error,
- **Alarm low** - state of low level alarm value,
- **Warning low** - state of warning value by approaching low level alarm,
- **Warning high** - state of warning value by approaching high level alarm,
- **Alarm high** - sensor reaching a high level alarm value.

If alarm limits have not been previously set for the sensor, this can be done here using the icon ⚙, which opens a window that allows you to enter the desired value:

After entering the desired value, activate the function by clicking the icon . The settings made here will also be visible in the Sensors tab.

Tip

In order to activate the notification function, it is important that, in addition to the settings made here, this option is also activated on the Configuration tab - see section 13.2 Configuration

13.2 Configuration

In the Configuration section, there is an option to activate the notification function necessary for sending messages. In addition, the user has the option to adjust general parameters related to the sending of notifications.

Protocol	Value	Description
Notifcation		Enable notification
E-mail info	86400	E-mail info time [s]
SMS info	86400	SMS info time [s]
MQTT info	60	MQTT info time [s]
MQTT Retain		Set MQTT Retain flag

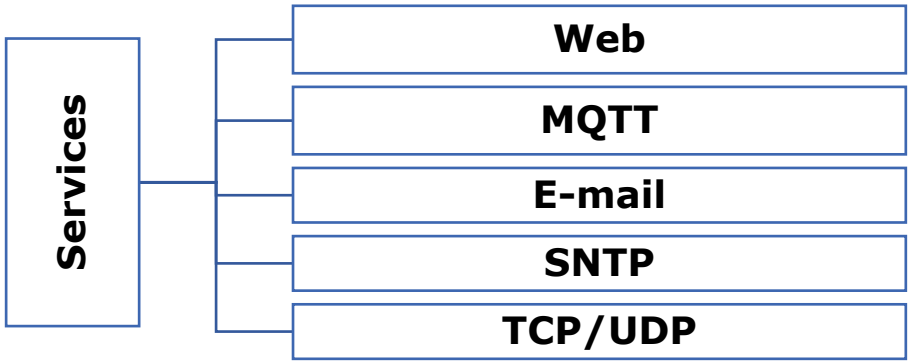
- **Notification** - activation / deactivation of notifications
- **E-mail info** - frequency of sending e-mail messages with information on the status of the sensor,
- **SMS info** - frequency of sending SMS messages with information on state of a sensor,
- **MQTT info** - frequency of MQTT messages with information about the state of the sensor,
- **MQTT Retain** - enable/disable MQTT Retain - enabled means that brokers will retain recent messages for subjects to which the device sends notifications,
- **SNMP Trap** - SNMP Trap selected
- **IO time** - the minimum time that must elapse between successive changes of state on the inputs/outputs to avoid excessive sending of notifications, especially when testing or experimenting with the device's inputs/outputs.

The tabs also include: Sensor, Inputs and Outputs.
Each table contains predefined commands to send email and SMS notifications containing the current states of the device. In addition, the user can edit these commands, allowing them to be customised according to personal preferences, for example by adding a device name. Each table also contains a topic, the use of which is necessary when sending notifications via the MQTT protocol.

Sensor		
E-mail	[%s[?].name%]=%s[?].val% s[%s[?].idx%] %s[?].statTxt%	E-mail sens subject
MQTT	IQIO SENS/c09bf4a003a2	MQTT sens topic

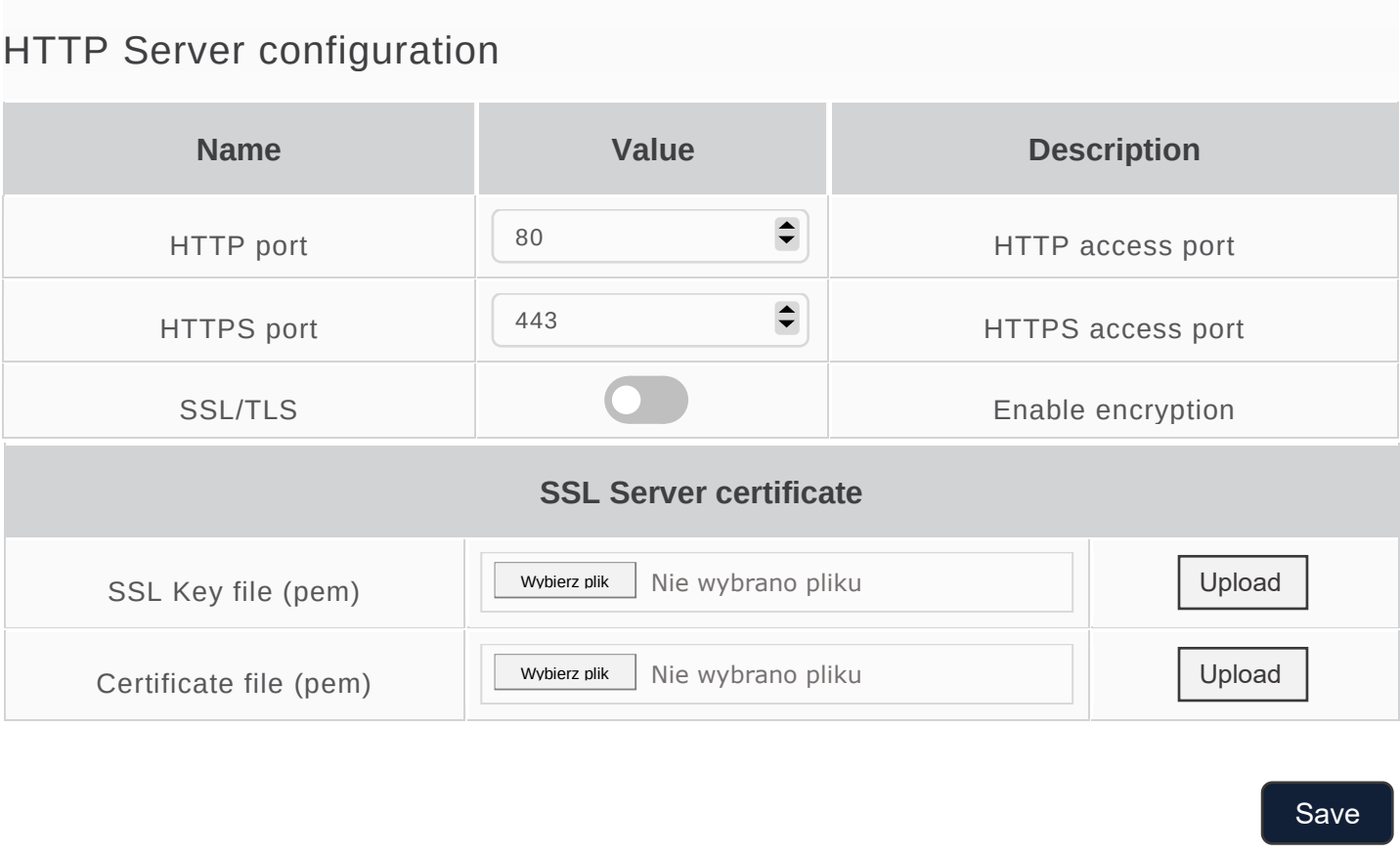
14 Network services (Services)

This tab presents options for the detailed configuration of support for various communication protocols, which is a key element of the device's functionality:



14.1 Web

In this section, the user can adjust the settings for the device's web interface, manage access to resources or modify parameters for connection to the network.



- **HTTP Port** – the HTTP port from which requests are sent,
- **HTTPS port** – the HTTPS port from which requests are sent,
- **SSL/TLS** – enable/disable encryption
- **Select Key file (pem)** – allows loading the SSL server key (in pem format)
- **Select CSR file (pem)** – loads the server CSR key (in pem format)

14.2 MQTT

This tab is used to configure the communication parameters with the MQTT broker, enabling data exchange in a publish-subscribe model. It allows key aspects such as topics, server address, port and other relevant connection parameters to be defined. The device sends information to the server every 1 minute and every time there is a change in value. The transmission of this data can be secured by encryption. Once the connection to the MQTT broker is established, users can subscribe to the data coming out of the device. There is no limit to the number of subscribers who can simultaneously receive information from a single device.

MQTT Client configuration

Name	Value	Description
MQTT Client		Enable MQTT Client
Server		Remote server address
MQTT port	1883	port
QoS	QOS0	Quality of service
Subscribe Topic	/	Topic to subscribe
Client ID	dev a002a4	Client ID
User		Auth user
Password		Auth password
Send test message	Before sending a test message, save your settings. Send test messages to the broker with a payload of 1 and topic of \validation.	

- **MQTT Client** – attachment of the MQTT service,
- **Server** – address of the MQTT server,
- **MQTT port** – the port on which the server is listening (usually 1883),
- **QoS**
- **Subsribe Topic** – the topic to which the message will be sent (the topic must be in the format e.g. /sensor/home - without the "/" at the end of the line),
- **Client ID**
- **User** – (optional) mqtt username,
- **Password** – (optionally) password of the mqtt user,
- **Send test message**

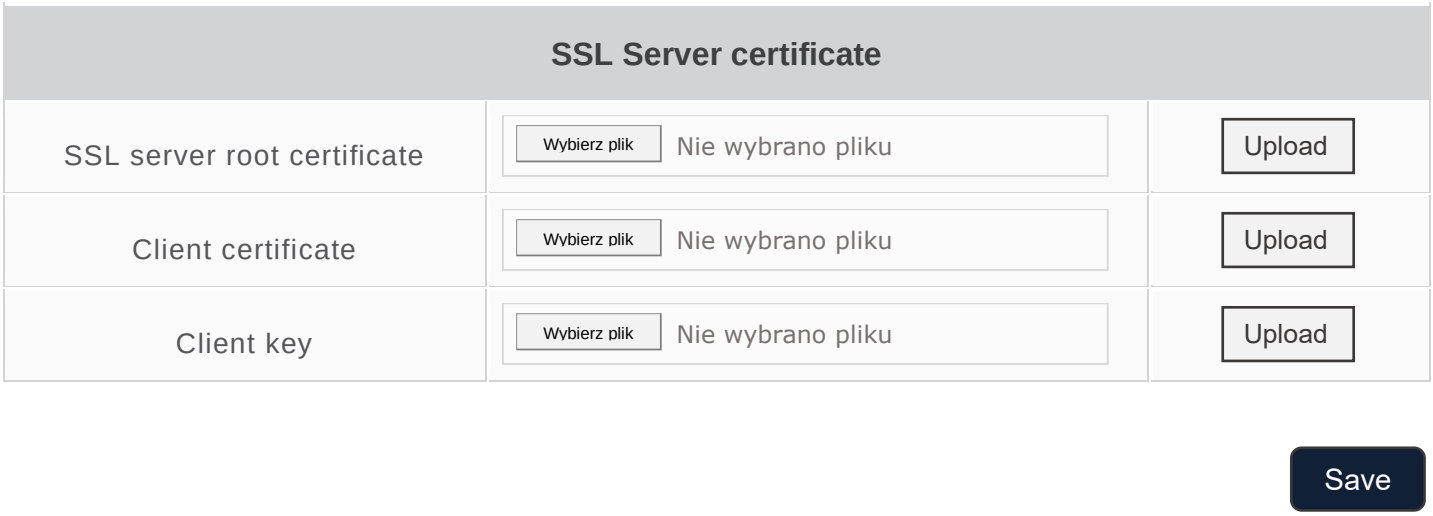
SSL/TLS		Enable encryption
Root certificate		Use CA ROOT certificate
Skip cert CN check		Skip certificate Common Name check
Use Client certificate		It needs upload client's key, password and certificate
Client key password		

- **SSL/TLS** – Enable/disable encryption,
- **Root certificate**
- **Skip cert CN check** – skip the certificate common name check
- **Use Client certificate** – require uploading client key, password and certificate
- **Client key password** – password for the client key

The device is equipped with the LWT mechanism, which stands for 'Last Will and Testament'. LWT is a mechanism that allows an MQTT client to send a message automatically in the event that the client fails or loses connection to the MQTT broker.
The LWT mechanism allows you to define the subject (topic) and content of the message that will be published when the client loses connection.

MQTT Last Will and Testament (LWT)		
LWT		Enable LWT
QoS	QOSO	Quality of service
LWT retain		Set LWT reatain
LWT Topic		LWT Topic e.g.: /device/MAC_address/lwt
LWT Message		LWT Message

- **LWT** – enable/disable the LWT mechanism,
- **QoS -** quality level of message delivery - refers to how the LWT message will be delivered if the client loses connection. It can take one of three values: 0 (At most once), 1 (At least once), 2 (Exactly once),
- **LWT retain** - a flag informing the MQTT broker whether to retain the last LWT message for clients who register with it after the client's LWT connection is lost,
- **LWT Topic** – the topic that will be used to publish the LWT message,
- **LWT Message –** the content of the message that will be published in the LWT topic after the loss of the client connection.



- **SSL server root certificate** – allows loading the SSL server certificate,
- **Client certificate** – allows to load SSL client certificate,
- **Client key** – enables loading SSL client key.

Confirm the settings with the Save button.

Tip

If using the Inveo broker, the values will be as follows:

- MQTT Address: mqtt.inveo.com.pl

- MQTT Port: 1883

You can use the computer on which the Inveo Monitoring application is installed in the broker function.

To do this, enter the IP address of the computer in the MQTT Address field.

Tip

Please ensure that the topic you assign is unique, e.g.: /IQIO/ MAC address.

14.3 E-mail

This section configures the parameters for the connection to the e-mail server, allowing e-mails to be sent automatically in response to specific events or alarms.

E-mail configuration

Name	Value	Description
E-mail		Enable E-mail
Server		SMTP server address
Port	0	Port
SSL/TLS	Off	Encryption
User		E-mail sender address e.g.: example@example.com
Authorization	None	Enable e-mail authorization
From	Mailer	E-mail from field e.g.: Johnny Bravo

- **Enable** – enable/disable e-mail service,
- **Server** – address of the SMTP server,
- **Port** – port of the mail service,
- **SSL/TLS** – enable/disable encryption,
- **User** – user name,
- **Password** – password,
- **From** - sender's e-mail address,

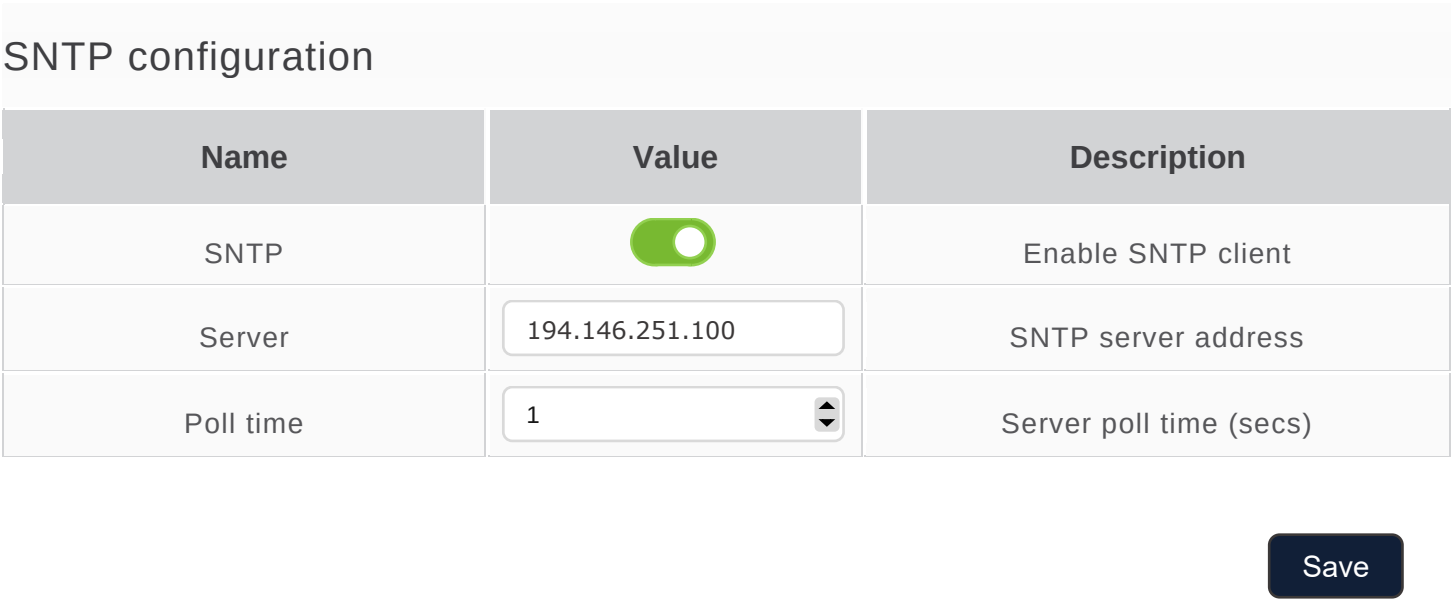
Debug		Enable debug e-mail messages
Subject	%mod_name%	E-mail subject
Recipients (comma separated)	E-mail recipient for a test	
Send test e-mail	Before sending a test email, save your settings. Open debbuger here!	

Save

- **Recipients (comma separated)** – list of recipients of emails (separated by commas),
- **Subject** – subject of the email to be sent,
- **Debug** – enable the message debugging function,
- **Send a test e-mail** – send a test e-mail.

14.4 SNTP

The DAXI device is equipped with SNTP protocol support, which is responsible for synchronising the device's time with the SNTP server. This is crucial for correct data logging and time tasks.
The options available under Services / SNTP allow you to configure the SNTP time server.



- **Enable –** enable/disable SNTP support
- **Server –** SNTP server address
- **Poll time** – server poll time (secs)

Tip

Examples of SNTP servers:

- tempus1.gum.gov.pl – new address: 194.146.251.100
- tempus2.gum.gov.pl – new address: 194.146.251.101

In addition, the DAXI device is equipped with an internal RTC clock with battery backup. When the device does not have permanent access to the Internet, it can use this clock to maintain accurate time - see section15.3 Time.

14.5 TCP/UDP

The TCP/UDP tab on the DAXI website allows TCP and UDP communication protocol support to be included and configured. The user can customise settings such as ports and communication parameters, providing flexibility in configuring the device according to network requirements.

TCP/UDP server configuration

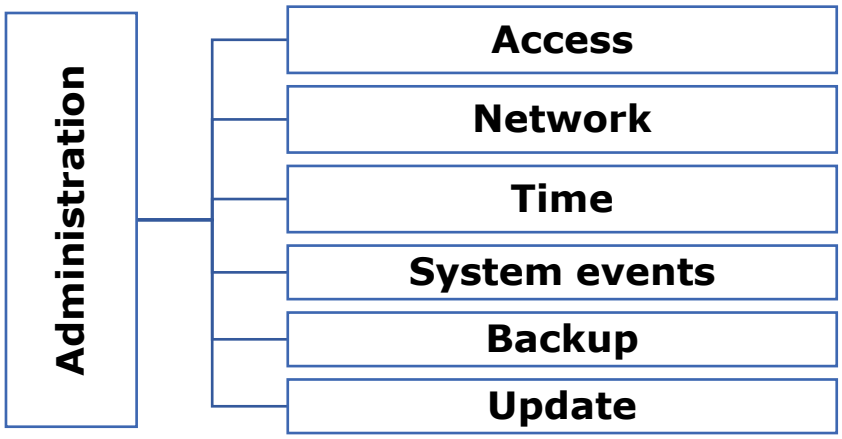
Name	Value	Description
TCP server		Enable TCP server
TCP Port	502	TCP server port
UDP server		Enable UDP server
UDP Port	502	UDP server port

Save

- **TCP server** - a location that listens for connections using the TCP protocol,
- **TCP port** - port number used to identify services and applications on target devices,
- **UDP server** - a place that listens for data sent using the UDP protocol,
- **UDP port** - port number used to identify services and applications in the UDP protocol.

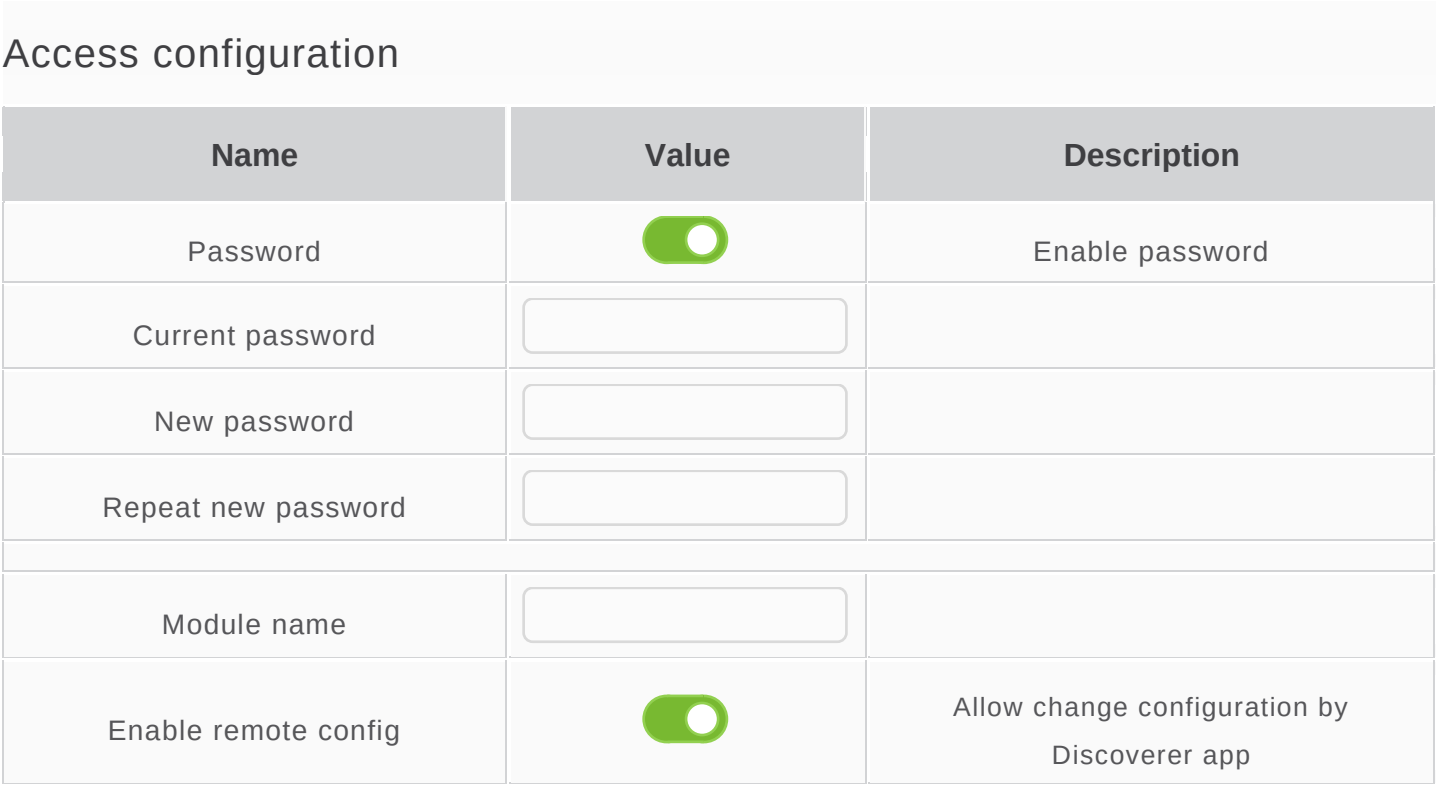
15 System administration (Administration)

The Administration tab allows you to manage aspects of the device that affect the operation, security and configuration of the system.



15.1 Access

In this section, the user can manage access to the device webserver. This includes authentication, name and access from Discoverer.



- **Enable** – enable/disable password,
- **Current password** – current password,
- **New password** – new password,
- **Repeat password** – repeat new password,
- **Module name** – module name (displayed, e.g. in Discoverer programme) - giving an individual name facilitates identification of a device in the system,
- **Enable remote config** – enabling/disabling permission to change configuration via Discoverer program.

Tip

Default settings on the device:

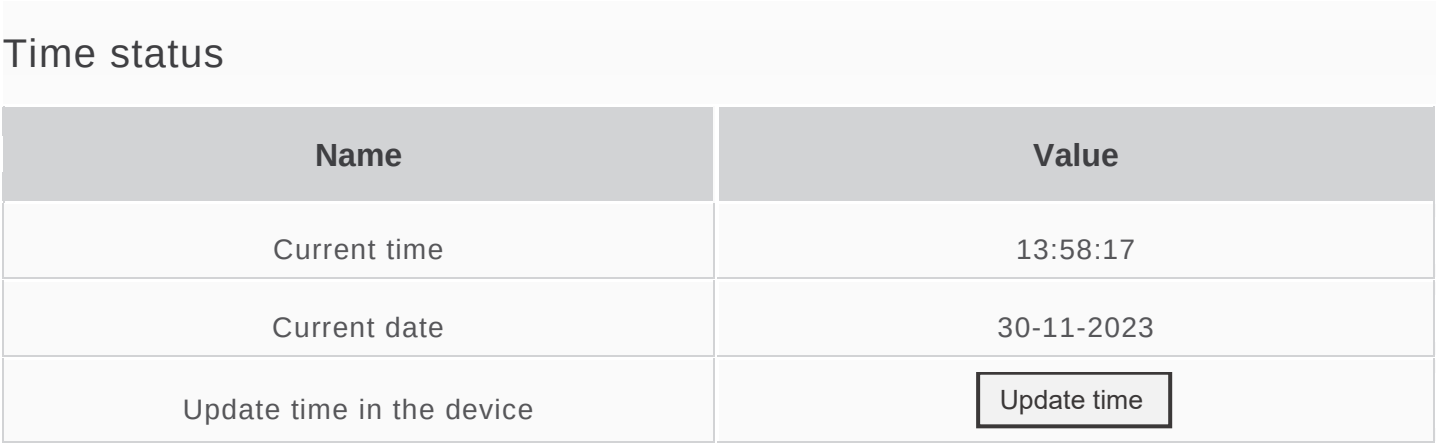
- login: admin
- hasło: admin

15.2 Network

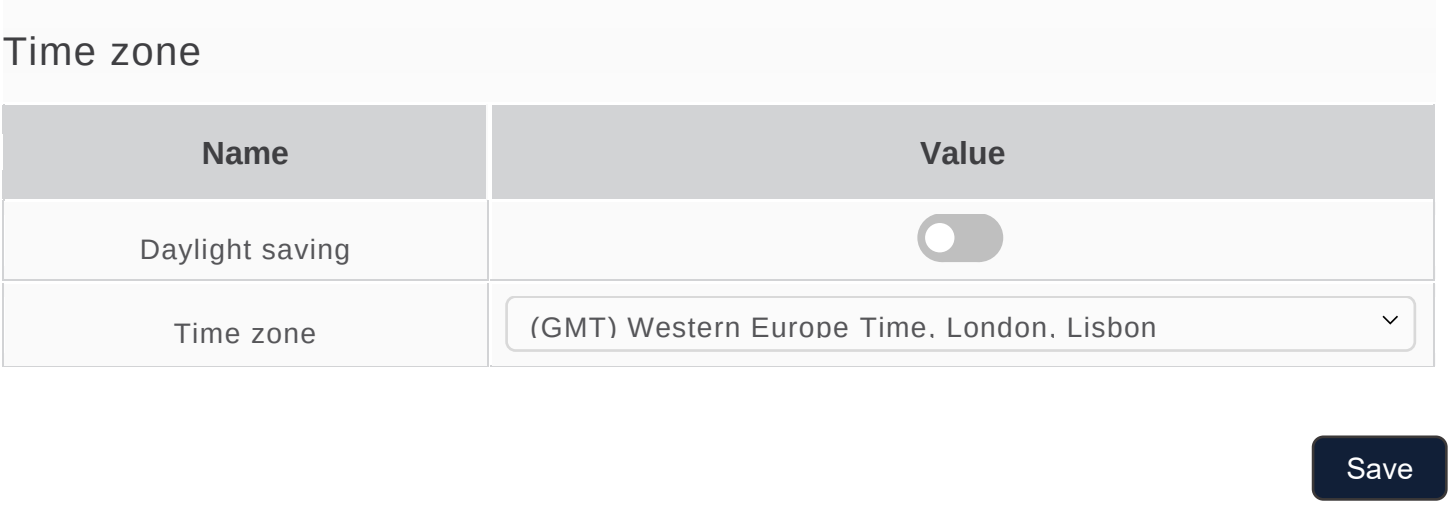
The network settings of the device are configured on this tab - see chapter 7.3 Configuring network settings 6.3 Configuring network settings.

15.3 Time

This section allows you to manually configure the time settings and time zone and download the current time from your computer.



- **Current time** – preview of the current time in the device,
- **Current date** – preview of the current date in the device,
- **Update time in the device** – allows the time in the device to be set the same as the time in the computer,

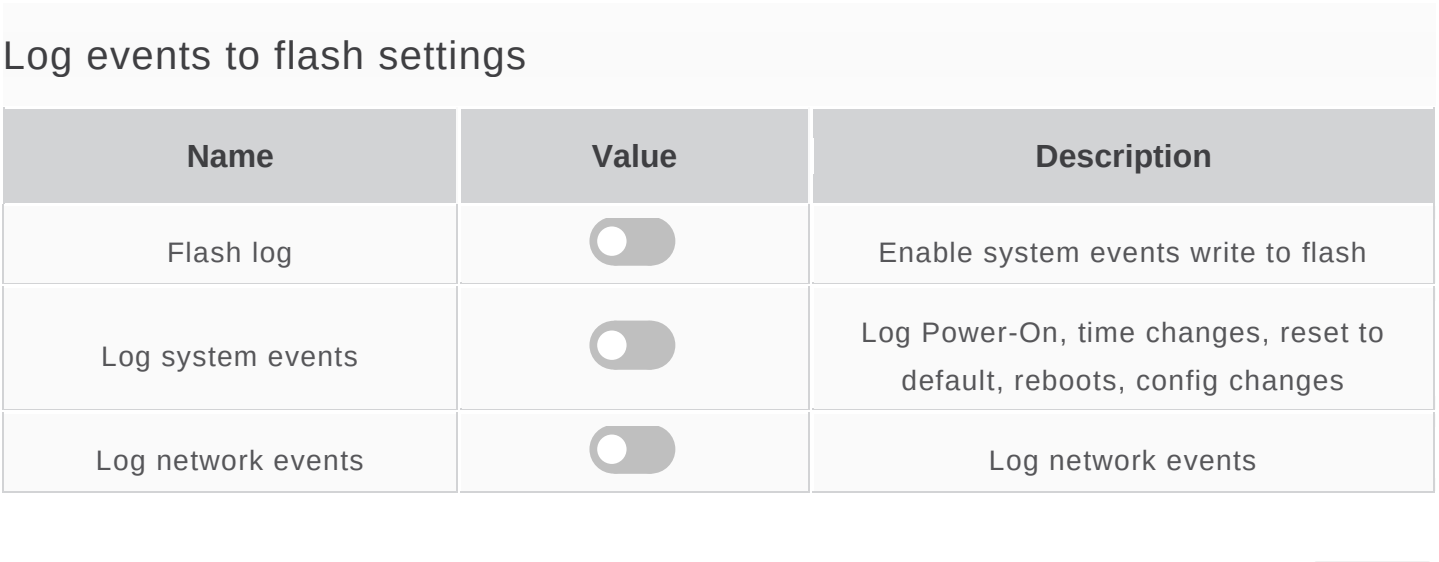


- **Daylight saving** – switching on/off daylight saving time,
- **Time zone** – selection of time zone.

The DAXI device is equipped with an internal RTC clock with battery backup. When the device has permanent access to the Internet, the SNTP service can be used to ensure precise time synchronisation (see chapter 14.4 SNTP).

15.4 System events

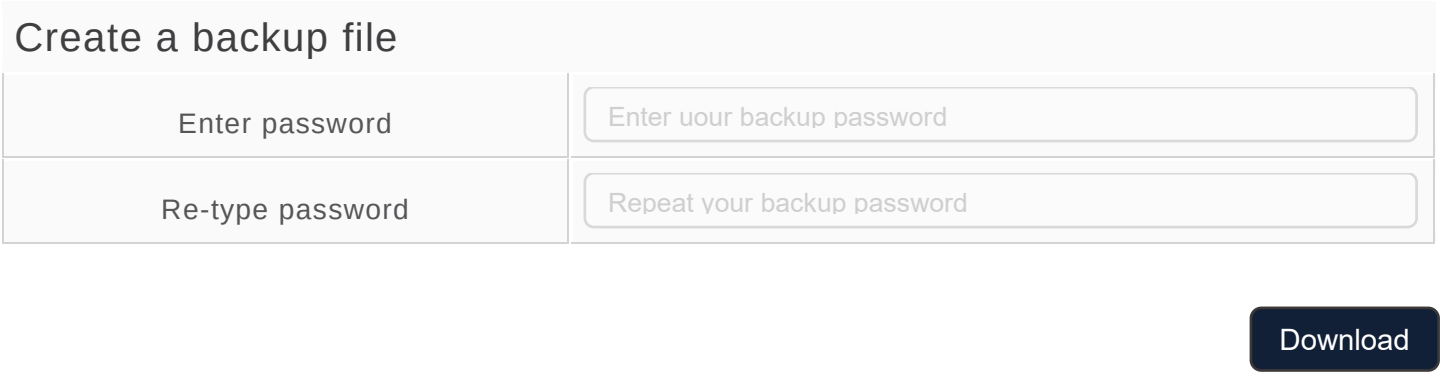
The tab allows system events to be recorded in flash memory, enabling users to view and analyse a variety of system events. This process helps to monitor system performance and diagnose potential problems.



- **Enable** – enable / disable logging of system events to flash memory,
- **Log system events** – enable / disable logging of power-ups, time changes, resetting to default settings, reboots, configuration changes,
- **Log network events** – enable / disable logging of network events.

15.5 Backup

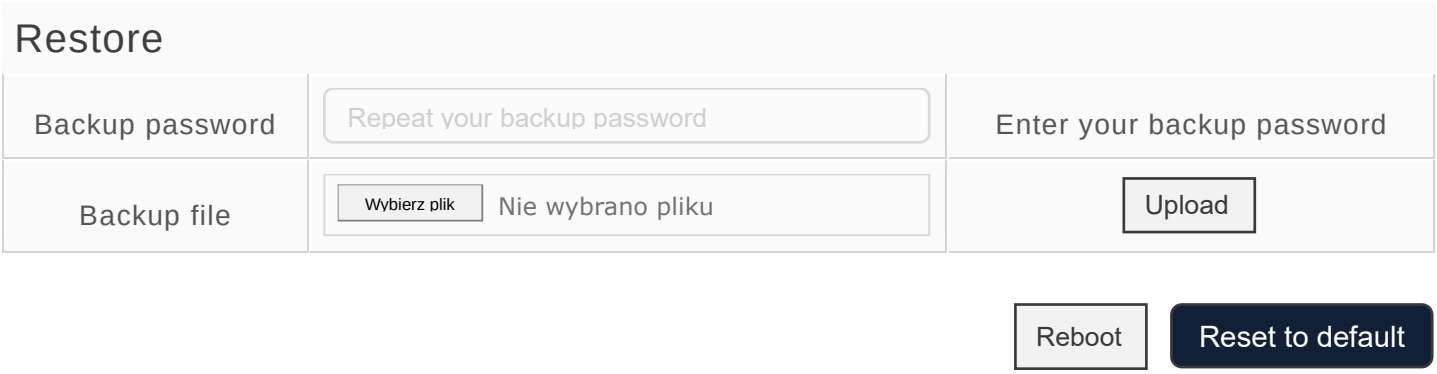
In this section, users can create backups of the current system configuration and restore the system from previous backups.



- **Enter password** – allows you to enter a password to protect the backup being created,
- **Re-type password** – retype the password.

The button 

allows you to save the backup to your computer.



- **Backup password** – password for the backup to be uploaded
- **Backup file** – button for searching the backup file

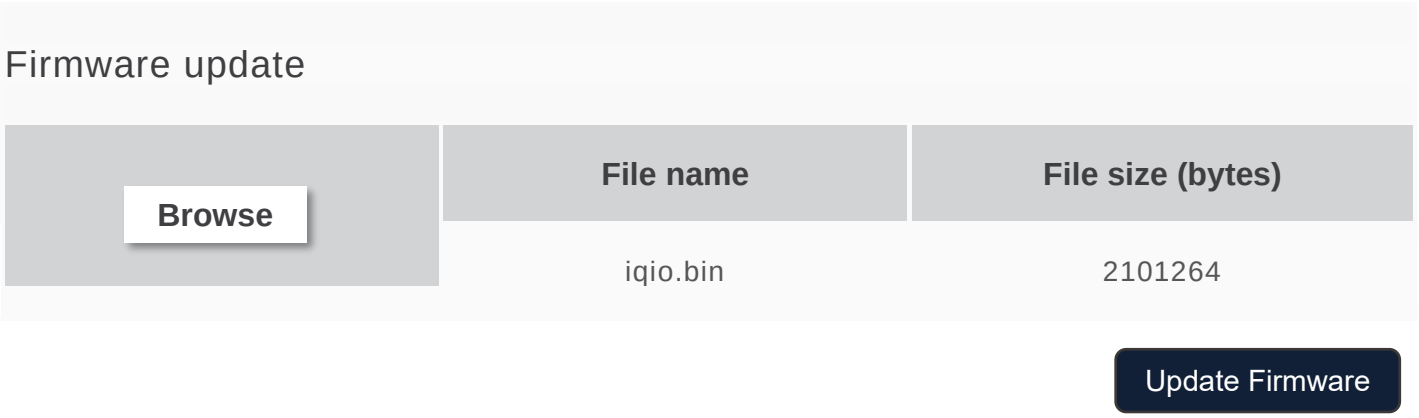
The button Upload will upload the selected backup to the device.

Button Reboot enables rebooting the device.

Button Reset to default restores the factory settings of the device.

15.6 Update

This tab enables the system or device to be updated to the latest software version. Users can upload new firmware or software versions here to provide bug fixes, updated functions and other improvements.



Warning Incorrect use of the firmware update function may damage the module.

16 Emergency software upload / factory reset

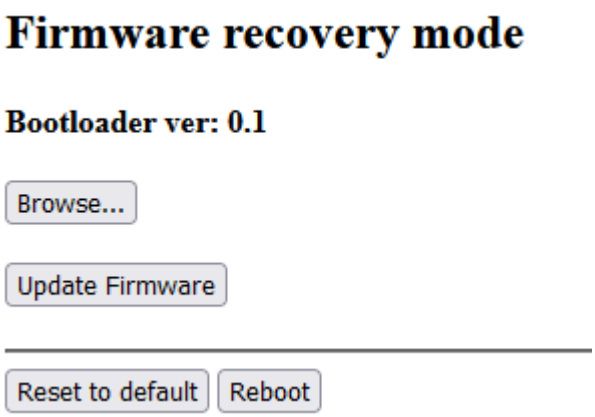
In the event of a device failure preventing normal access to the website, use the emergency procedure:

- Disconnect the device from the power supply
- Press the RESET button
- Power up the device and connect it to the LAN
- Without releasing the RESET button, open the device web page:
  - Adres IP: 192.168.111.15
  - Maska IP: 255.255.255.0

Tip

To access the address 192.168.111.15, the IP address of the computer must be in the same subnet (example IP address for the computer: 192.168.111.1.) Changing the subnet of the computer is described in section 6.2 Changing the subnet of the computer to be configured.

Referring to the given IP address will access the bootloader of the device. The RESET button can only be released after the page has been opened:



Here we have the possibility to upload firmware, reset the device to factory settings and restart it.

17 Built-in variables

This chapter presents a table with examples of internal variables that enable the precise transmission of data related to the reader's operation. These variables are a key part of the configuration, use in email notifications, SMS, HTTP Client, etc.

Syntax	Example	Description
%out[range],[off],[on]%	%out[0-5],0,1%	state of outputs [range] means the range of outputs to be shown [off] means the value for the inactive state [on] means the value for the active state Example: the state for OUT 0-5 will be shown inactive value is 0 and active value is 1
%in[range],[off],[on]%	%in[0-7],i,I%	Input status [range] means the range of inputs to be displayed [off] means the value for the inactive state [on] means the value for the active state Example: the state for IN 0-7 will be shown inactive value is i and active value is I
%cnt[number]%	%cnt5%	input counter value [number] means the number of inputs Example: the counter value for input 5 will be shown
%sens[number]%	%sens10%	sensor value [number] means the sensor number Example: the value for sensor no. 10 will be shown
%sunrise%	%sunrise%	sunrise time
%sunset%	%sunset%	sunset time
%time%	%time%	current time
%date%	%date%	Current date
%timedate%	%timedate%	Current time and date
%ts%		Current timestamp - the number of seconds since a specific time: 1 January 1970
%mod_name%		User-defined module name
%mod_model%		Device model
%eip%		IP address of the device
%emac%		MAC address

%s[x]%	%s[3]%	Sensor value Example: the value for sensor no. 3 will be shown.
%s[x].statTxt	%s[2].statTxt	Sensor status Example: the value for sensor no. 2 will be shown
%v[x]%		Value of virtual variable
%cntx%		Input counter value

www.inveo.com.pl

tel.: +48 33 444 65 87
kom.: +48 785 552 252

ul. Rzemieślnicza 21
43-340 Kozy

serwis@inveo.com.pl