Inveo Sp. z o.o.

IQIO PRO

Instruction Manual

Overview

Warning

This manual applies only to the firmware version v0.37.0 onwards. Inveo does not guarantee that the information contained in this document applies to previous firmware revisions.



Purpose of the device

IQIO PRO is an advanced tool to monitor a variety of parameters, such as temperature, humidity or digital inputs. Up to six different sensors can be connected at the same time. The user has access to all readouts via the built-in website, where parameter changes, readout history and graphs can be reviewed.

IQIO PRO supports various communication protocols such as HTTP, HTTPS, MQTT, SNMP v2/v3, and e-mail, making integration with different monitoring and control systems easy. Additionally, the functionality to send e-mail and SMS notifications informing about the current sensor state or exceeded alarm thresholds can be implemented. The device is equipped with Wi-Fi.

The device also provides an independent output that can be used to control various system elements. Thanks to built-in mechanisms, IQIO can automatically react to signals and readouts, and the user has the option to program actions, such as output control or notifications generation.

Changelog

Table of contents

- Overview
  - Purpose of the device
  - Changelog
- Device construction
  - Technical characteristics
  - Module connectors description
  - Sensor connection diagram
- Network configuration
  - Changing the device's IP address - Discoverer programme
  - Changing the computer's subnet address for configuration
  - Network settings configuration
  - Configuration mode
  - Wi-Fi connection configuration
- Device configuration
  - Module's www interface
  - Device status preview
    - Sensors window
    - Sensor charts
    - Outputs window
    - Inputs window
    - Watchdog status window
  - Inputs/outputs configuration
    - Outputs
      - Last output state or counter retention
    - Inputs
    - Display LED
  - Sensors configuration
    - All
      - Alarms configuration
    - History
    - Chart
    - Sensor handling
      - Sensor readings logging and graph preview
      - Download of stored sensor readings

- Notifications configuration
  - Sensors
  - Inputs
  - Outputs
  - Configuration
- Binding
  - Outputs
- Schedule
  - Weekly
  - Cron action
  - Cron standard
  - Configuration
  - Twilight
- Remote hosts ping (Watchdog)
- System management
  - Access
    - API keys
  - Network
  - Time
  - System events
  - Backup
  - Restore

- Defining actions
  - All
  - Protocol configuration
    - UDP
    - TCP
    - HTTP
    - MQTT
    - IO
    - E-mail
    - SMS
    - SNMP Trap
  - Inputs
  - System
  - Periodic

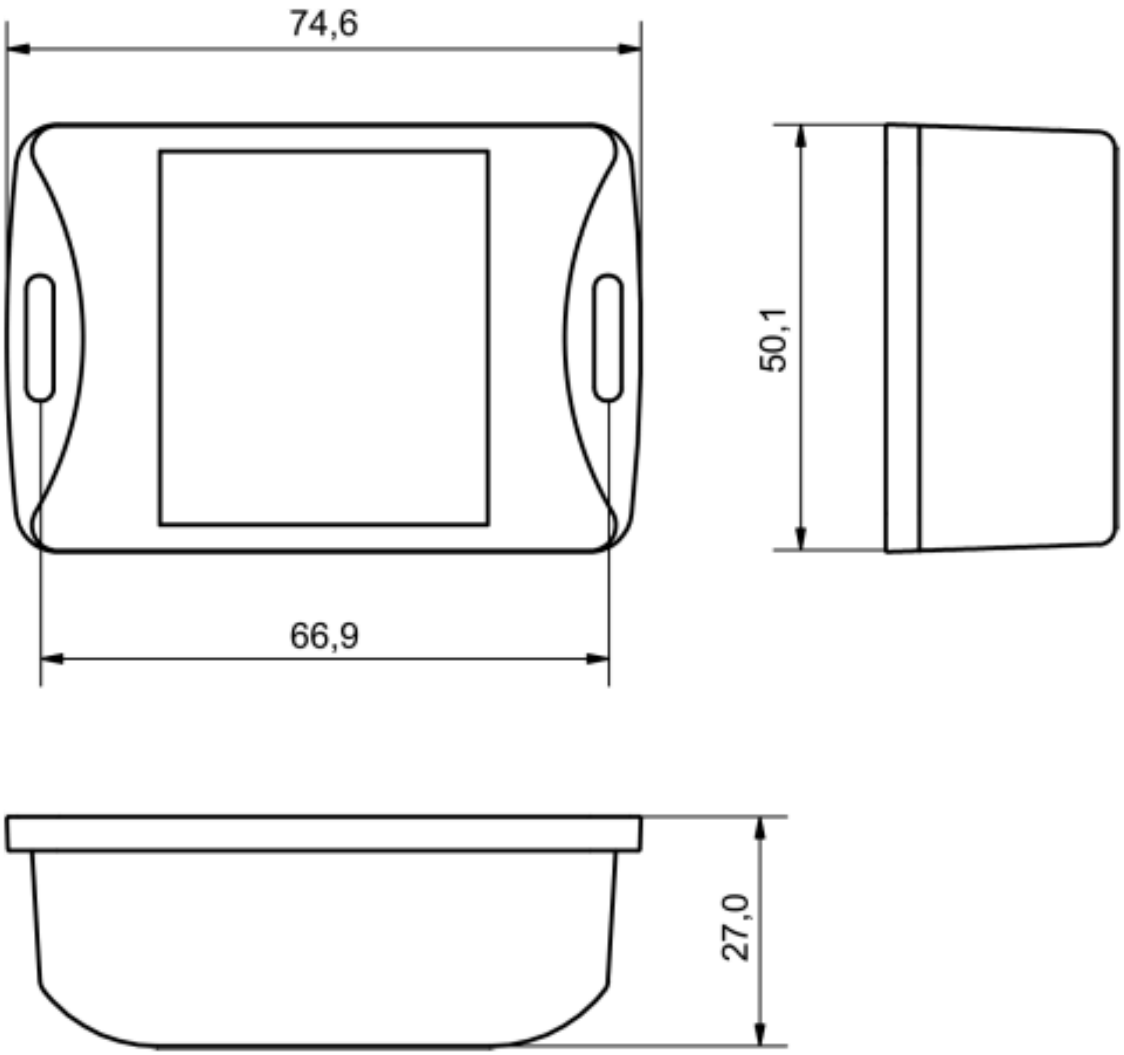
- Communication protocols
  - Web
  - HTTPc
  - MQTT
  - E-mail
  - SMS API
  - Modbus
    - Coils addressing
    - Discrete Inputs addressing
    - Holding Registers addressing
    - Input Registers addressing
  - SNMP
    - SNMP v2c
    - SNMP v3
  - Syslog
  - TCP/UDP
  - iCluster
  - IO commands
  - Built-in variables
  - REST API
- Application examples
  - Example 1: Notifying about sensor, input, and system state
  - Example 2: Notifying about sensor state via e-mail
  - Example 3: Advanced MQTT notifications configuration
- Factory settings, backup
- Emergency firmware restore / restoring factory settings
- Warranty and manufacturer's liability
  - Storage, operation and transport conditions
  - Disposal and decommissioning

Device construction

Technical characteristics

Parameter	Description
Power supply	**10-24V DC** with a 3,5mm pluggable terminal block **PoE:** 33-57V PoE IEEE 802.3af *(IQIO PRO ETH Wi-Fi)* **USB-C** 5V
Power consumption	Max. 1,5W
Bus	**1-Wire** – Three-wire or flat RJ12 cable (adapter required) Supports up to 6 sensors Dedicated sensors: temperature, humidity, water pressure, air pressure, analogue voltage, analogue current, gases: CO, CO_2, NO_x
Inputs	**Input type:** digital, normally open, pre-polarized
Outputs	**Output type:** potential-free NO relay output **Maximum operating voltage:** 30V DC **Maximum relay load:** 1A NO output (normally open) **Activation time:** 1ms **Deactivation time:** 5ms **Operating mode:** bistable, astable, monostable, timed
Communication	Wi-Fi 2,4GHz *(IQIO PRO ETH Wi-Fi)* Ethernet 10/100Mbps Full Duplex, RJ45 port *(IQIO PRO ETH)*
Enclosure ingress protection	IP30
Weight	ca. 74g (2,6oz)

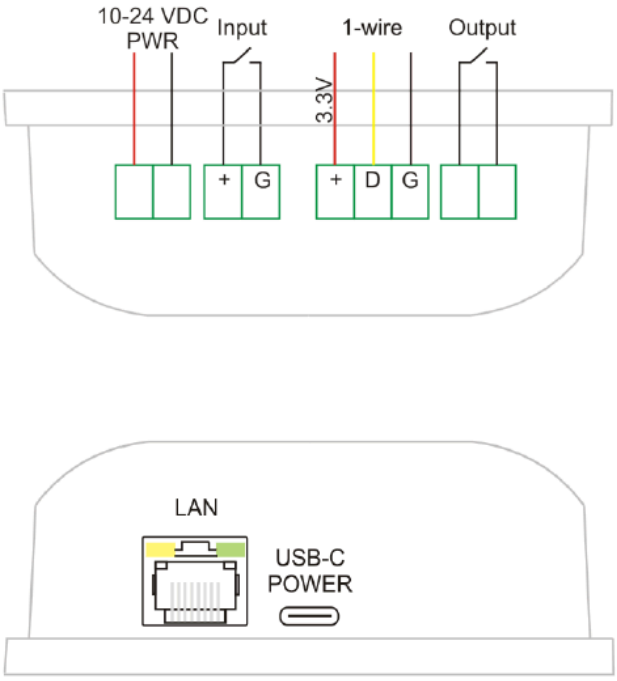
Dimensions



Information

All dimensions are in millimeters.

Module connectors description

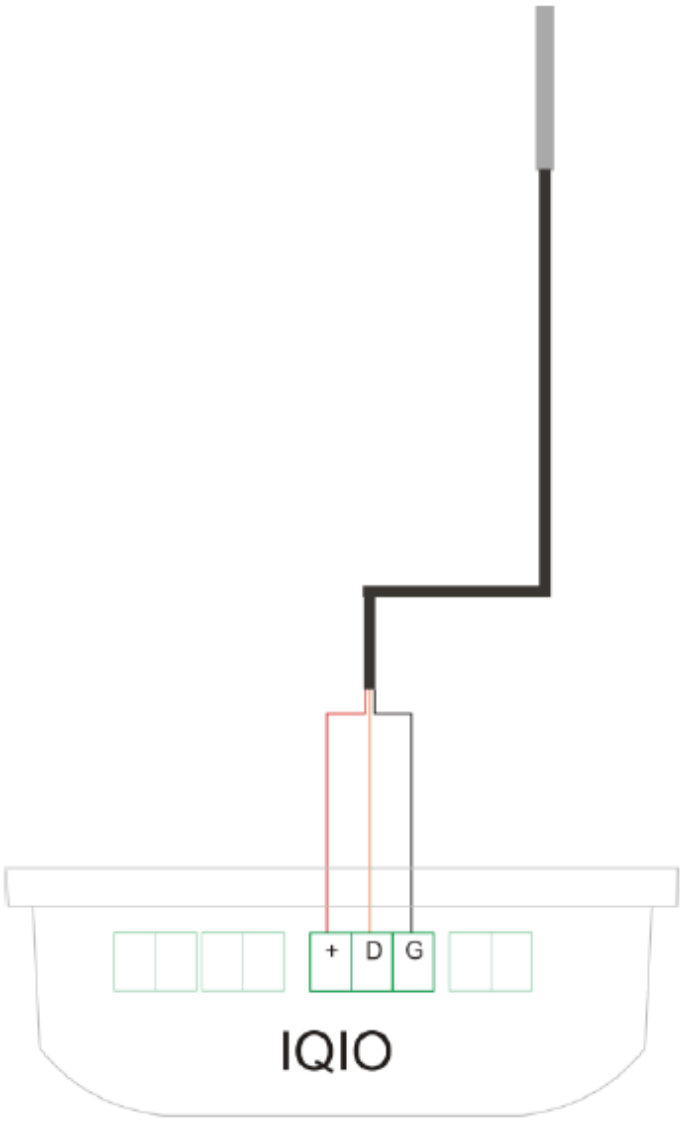


The IQIO Pro module has the following connectors:

- **RELAY OUT** – Relay's pluggable terminal block,
- **BUS** – 1-Wire bus,
- **IN** – Digital input,
- **LAN** – LAN and PoE IEEE 802.3af,
- **PWR 5VDC** – 5V USB-C power connector.

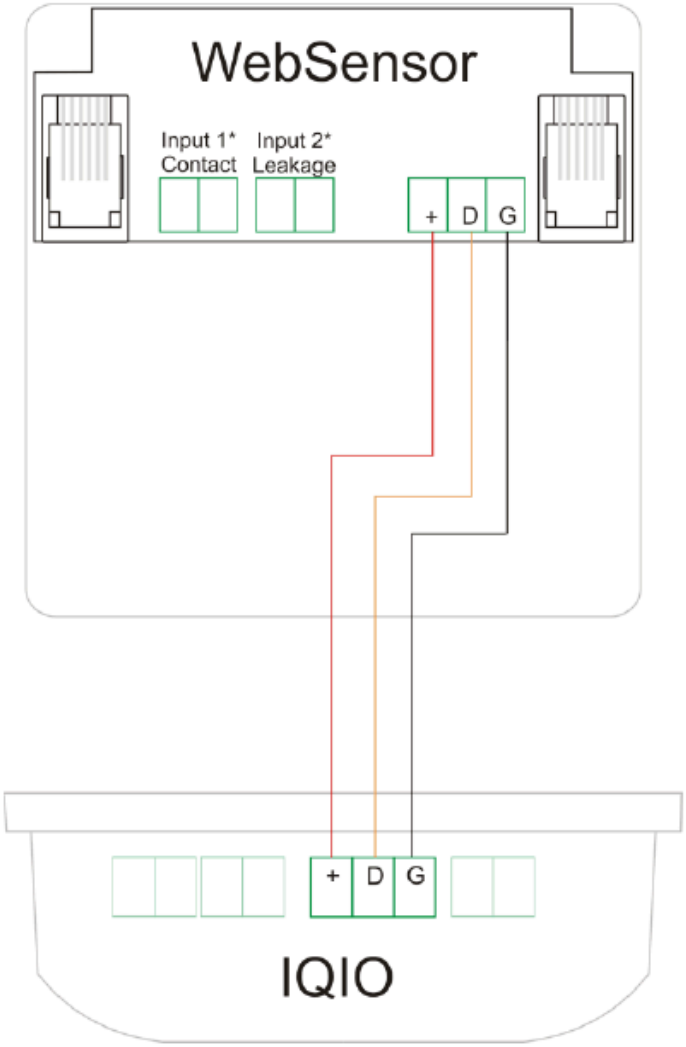
Sensor connection diagram

Connecting a sensor

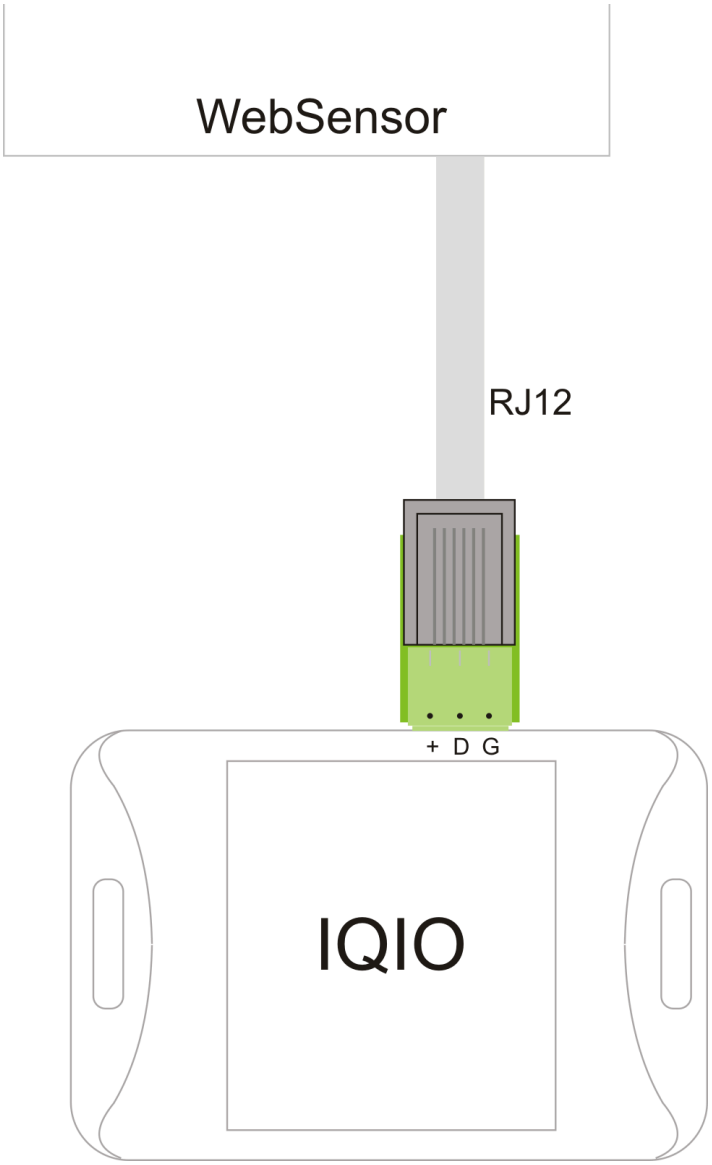


Connecting a WebSensor

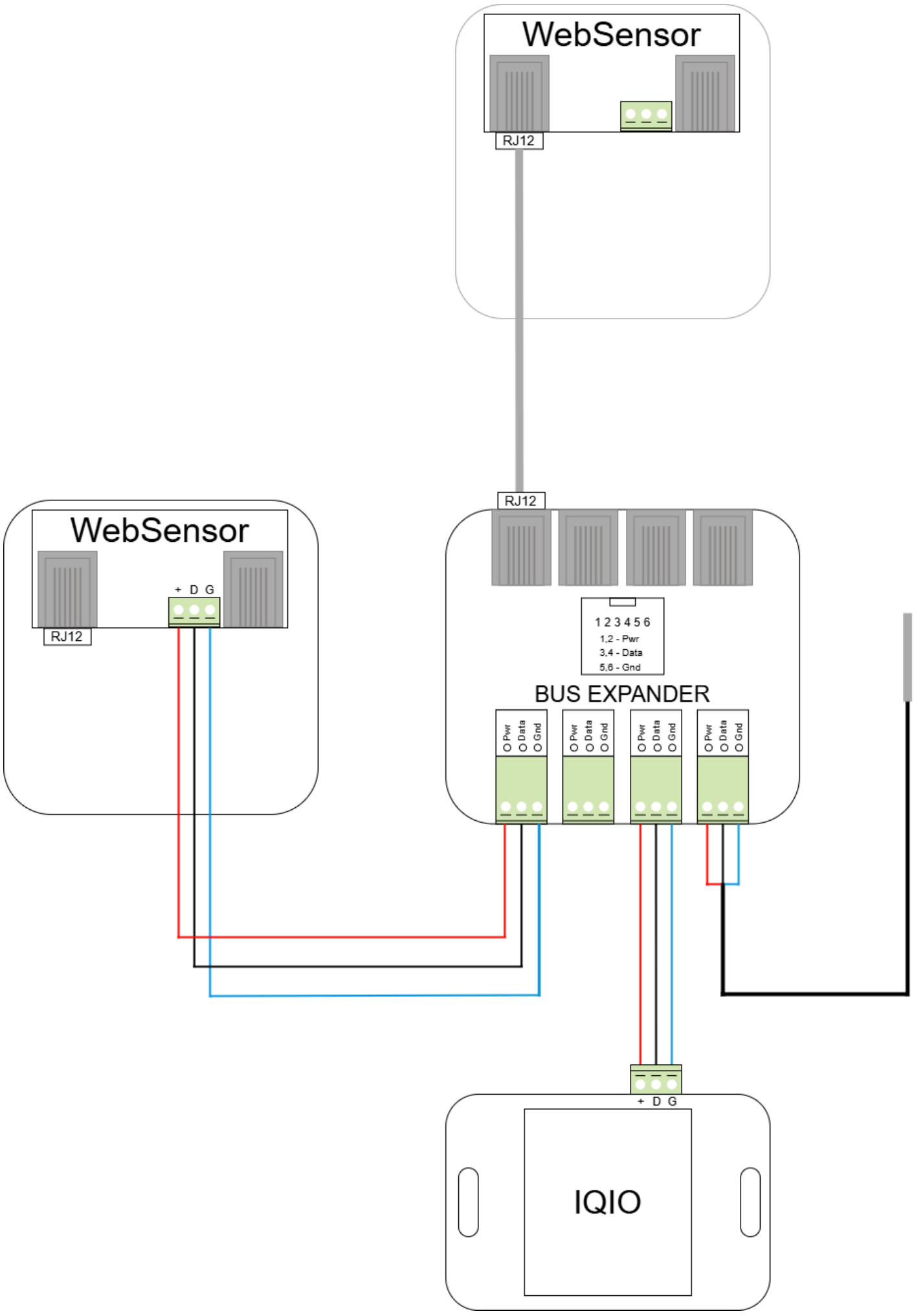
- 3-wire cable:



- RJ12 flat cable + adapter:



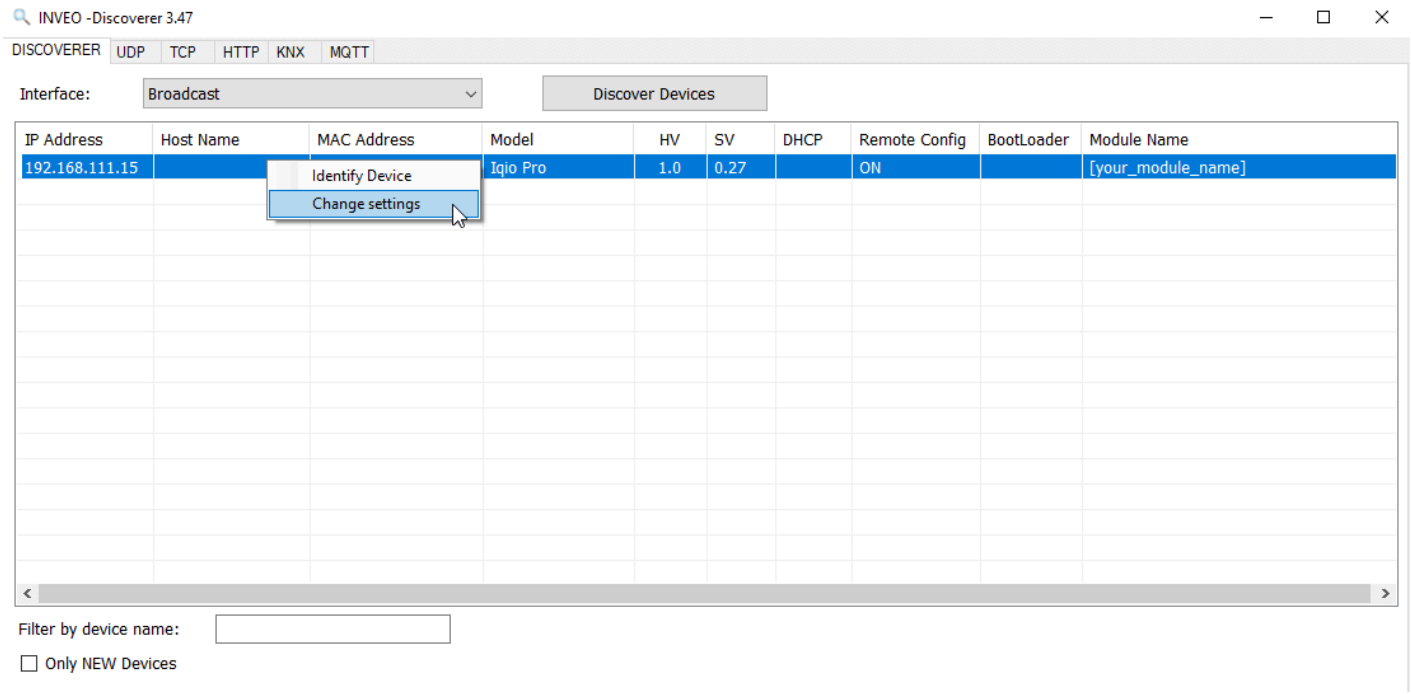
Connecting sensors using the BUS Expander splitter


WebSensor
RJ12
WebSensor
+ D G
RJ12
RJ12
1 2 3 4 5 6
1,2 - Pwr
3,4 - Data
5,6 - Gnd
BUS EXPANDER
Pwr
Data
Gnd
Pwr
Data
Gnd
Pwr
Data
Gnd
Pwr
Data
Gnd
+ D G
IQIO

Network configuration

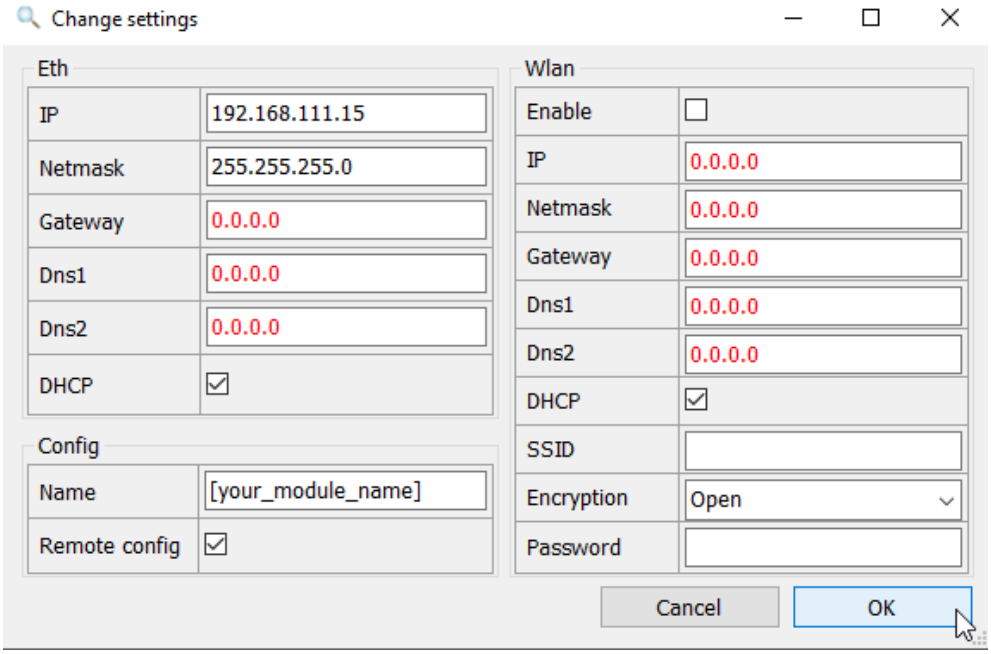
> **Warning**
>
> **After the initial power-up, it's needed to configure the device. It can be done in two ways, the simplest method is to use the Inveo Discoverer programme.**

Changing the device's IP address - Discoverer programme



After running the **Discoverer** programme and searching for the appropriate device:

1. Right-click the device,
2. Click the **Change** button.



After the dialogue window is opened you can:

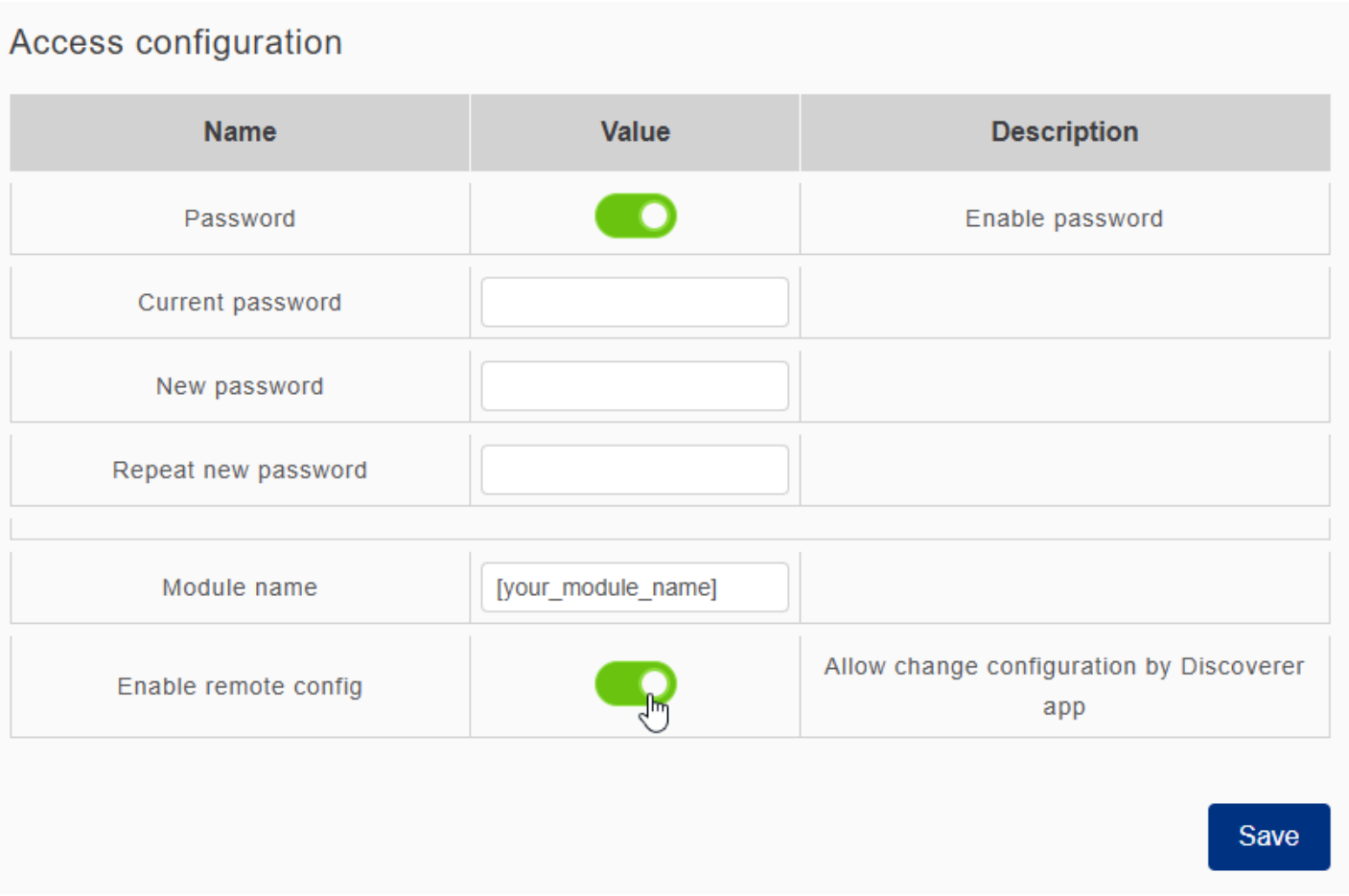
- Set the IP address, mask, gateway, DNS1/DNS2.
- Change the Host name.

> **Note**
>
> **The device will be configured after the Change button is pressed.**

If **Remote Config** is disabled (enabled by default), the device needs to be configured by changing the computer's subnet:

To enable remote configuration:

1. Go to the **Administration** tab,
2. In the **Access configuration** window, select **Enable Remote Config**.



> **Tip**
>
> **After making changes, apply them using the Save button**

Changing the computer's subnet address for configuration

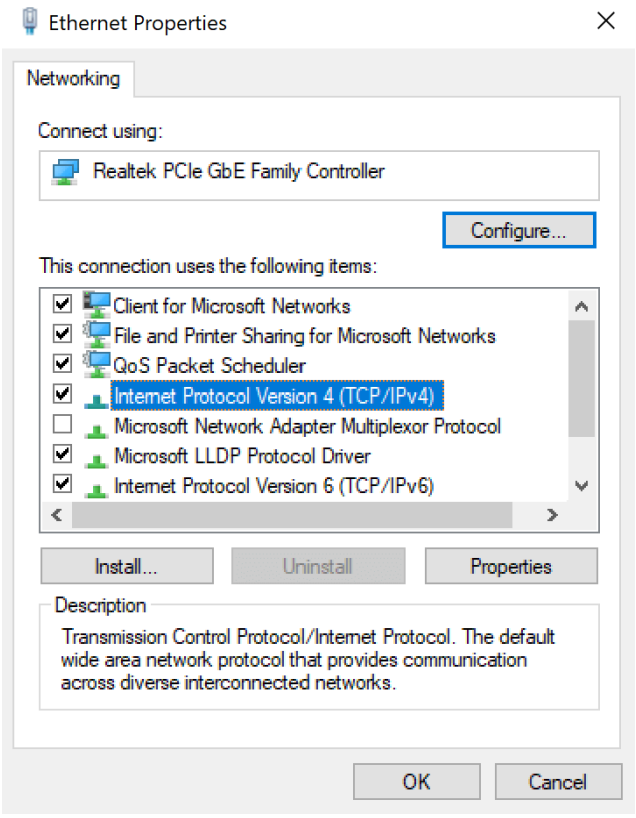
During configuration without **Discoverer** programme, it's needed to change the subnet address of the computer on the same network.

To access the computer's network configuration, do one of the following:

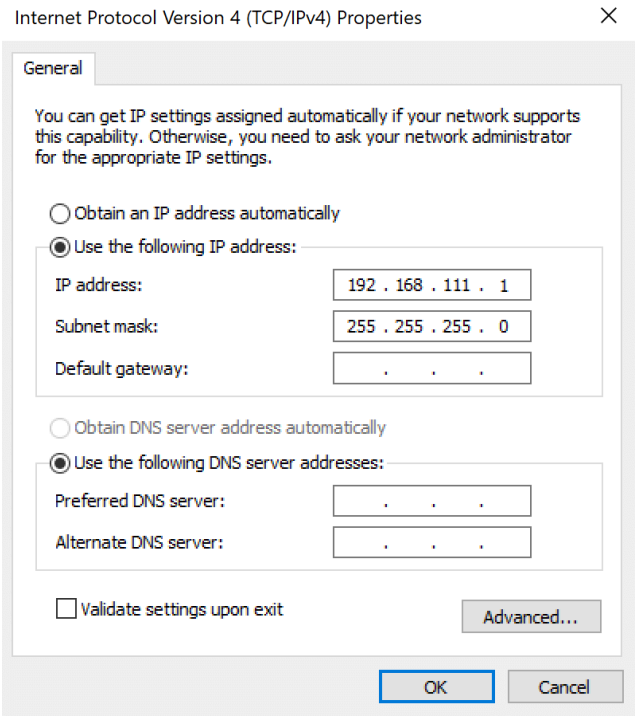
- Press **Win + R**, type in `ncpa.cpl`, and then press **Enter**.
- Alternatively, go to:
  Start → **Control Panel** → **Network and Internet** → **Network and sharing center** → **Change adapter settings**.

Then:

1. Select the network connection.
2. Right-click it and select **Properties**.
3. After selecting this option, network connection configuration screen will appear.



Select **Internet protocol version 4 (TCP/IPv4)** and type in the following parameters:

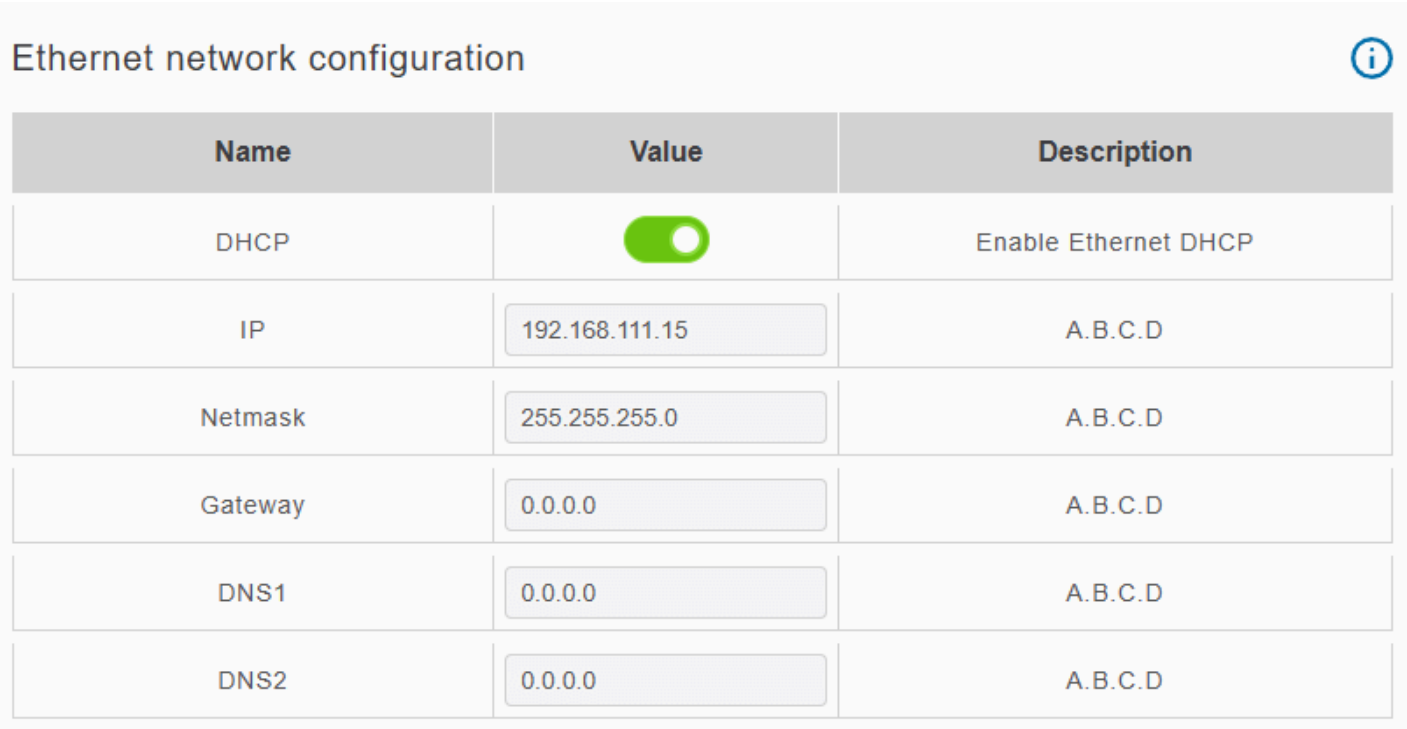


Note

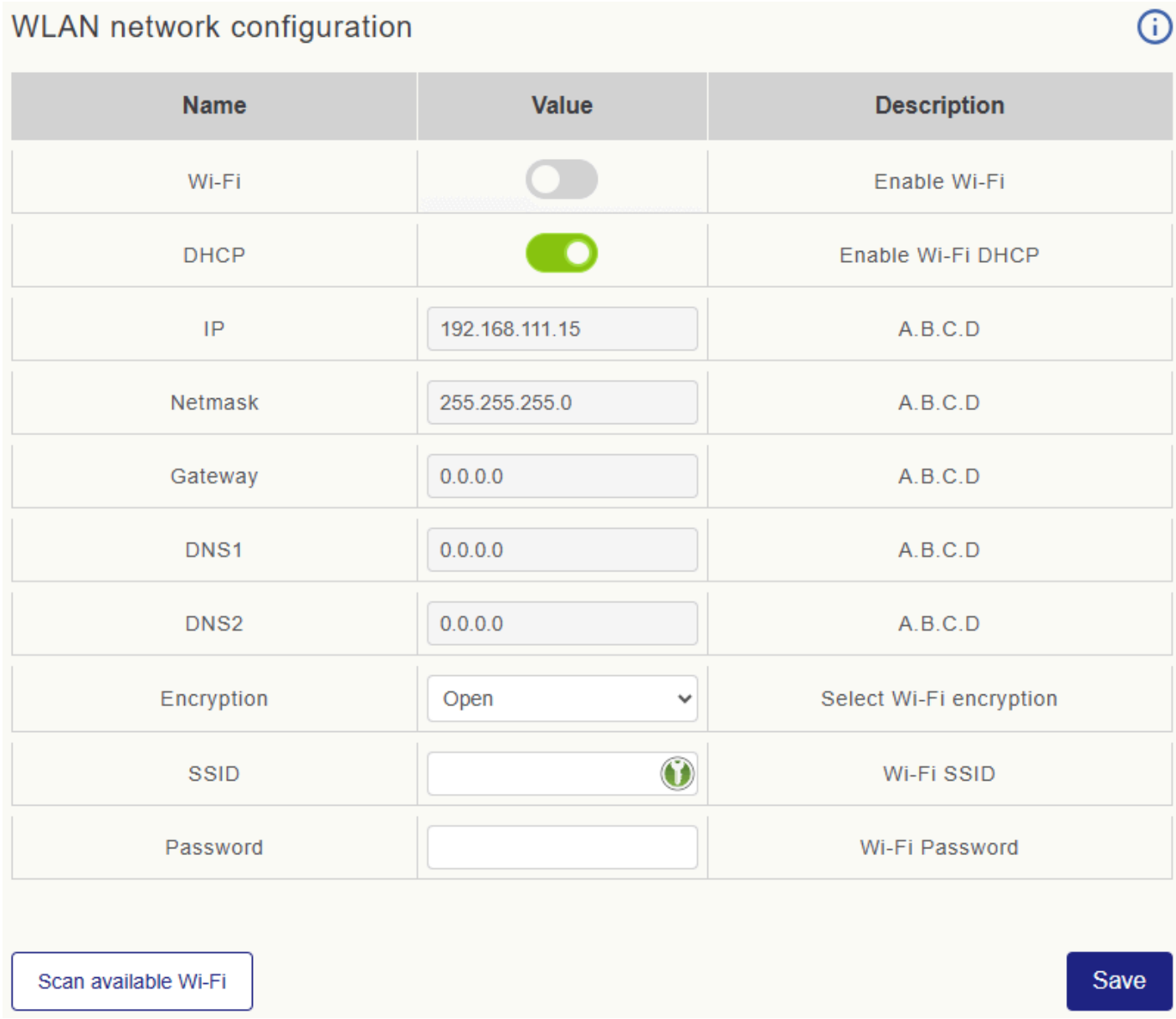
After applying the configuration with OK, start a web browser and type in the following address: 192.168.111.15. (Default user and password: admin/admin)

Network settings configuration

To customise the device's network settings, go to the **Administration / Network** tab. Parameters such as the IP address, subnet mask, gateway, DNS, and other network-specific options can be configured here. This tab allows the user to configure both the wired (**Ethernet network configuration**) and wireless (**WLAN network configuration**) connections.



- **DHCP** – Enable/disable DHCP server,
- **IP** – Device IP address,
- **Netmask** – IP subnet mask,
- **Gateway** – Network gateway,
- **DNS1, DNS2** – DNS server addresses.



- **Wi-Fi** – Enable/disable Wi-Fi service,
- **DHCP** – Enable/disable DHCP server in Wi-Fi,
- **IP** – Device IP address,
- **Netmask** – IP subnet mask,
- **Gateway** – Network gateway,
- **DNS1, DNS2** – DNS server addresses,
- **Encryption** – Wi-Fi encryption type:
  - Open,
  - WEP,
  - WPA-PSK,
  - WPA2_PSK,
  - WPA_WPA2_PSK,
  - WPA3_PSK,

- **SSID** – Network name,
- **Password** – Wi-Fi access password.

Scan available Wi-Fi allows the device to search and display a list of available Wi-Fi networks in range of the device.

Configuration mode



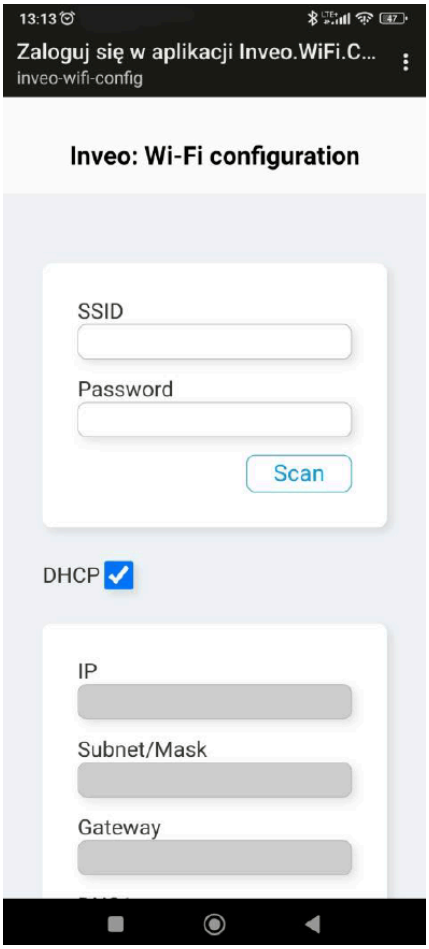
Pressing and holding the **RESET** button will display the IP address.

Configuration mode – After the power supply is connected to the device, changing and preview o certain settings is available for 3 minutes. Press and hold the **RESET** button to display the following information sequentially:

- **IP** – Device IP address,
- **dhcp eth** – If the **RESET** button is released while this prompt is displayed, DHCP will be enabled/disabled,
- **AP** – Release of **RESET** will allow the device's Wi-Fi to be configured,
- **rst def** – Release of the button will cause the device to reset to factory settings.

No changes will be made if the **RESET** button is released in the pause between prompts or after the last prompt has been displayed.

Wi-Fi connection configuration



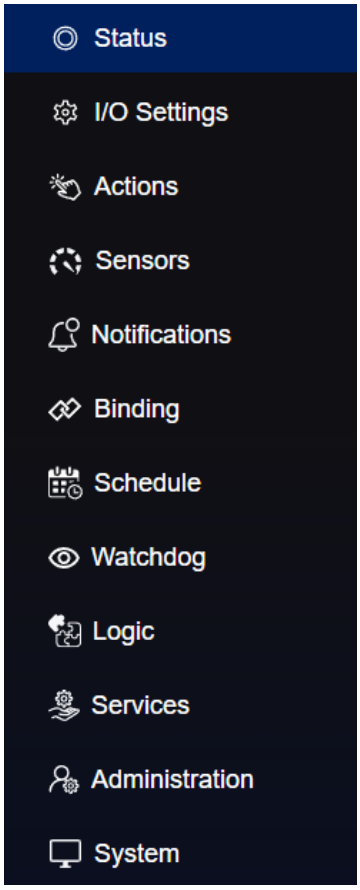
1. For 3 minutes after the power has been applied to the device (during **Configuration mode**), Wi-Fi connection can be configured. To do that, press and hold the **RESET** button until **AP** is displayed.
2. Activate Wi-Fi network search on your smartphone or other device. A network called "Inveo-wifi-config" should appear on the list.
3. Connect with the network.
4. After connection is established, click **scan** in the configuration interface or enter the Wi-Fi SSID into the correct field.
5. Select the network the device should connect to from the list of available options.
6. Enter the correct password to the selected network.
7. If the DHCP server is unavailable, manual configuration can be conducted after de-selecting **DHCP**.
8. **SUCCESS** will appear if the settings are saved successfully. The device will restart and resume normal operation.

Device configuration

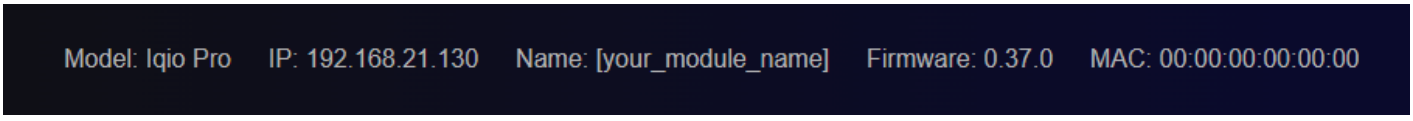
Module's www interface

The web interface allows for intuitive and advanced device management. After typing in the device's IP address into the browser's search bar, a webpage opens allowing full configuration and customisation of the device's operating parameters according to the individual user needs. On the left-hand side of the screen, a list of tabs is located, allowing for quick access to various functions and settings. Available tabs:

> **Note**
>
> **Some tabs are only visible after activationg the Advanced view.**



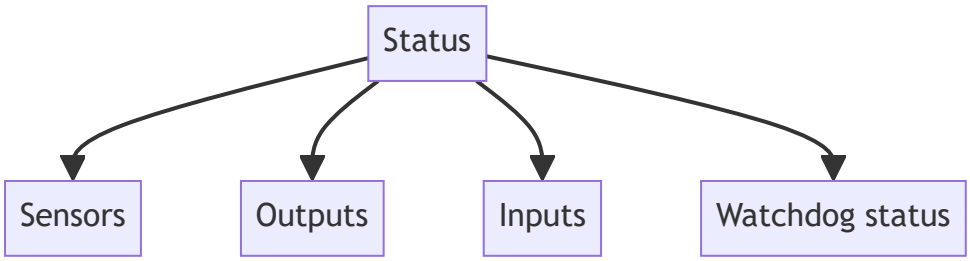
In the upper portion of the website, an information ribbon is located, informing the user about key device data, such as: model, IP address, unique user-assigned name, firmware version, and MAC address.



Thanks to the website, the user can modify settings, configure parameters, and monitor device operation in real-time. The webpage is the central control point, allowing for effective management and customization according to the changing user needs.

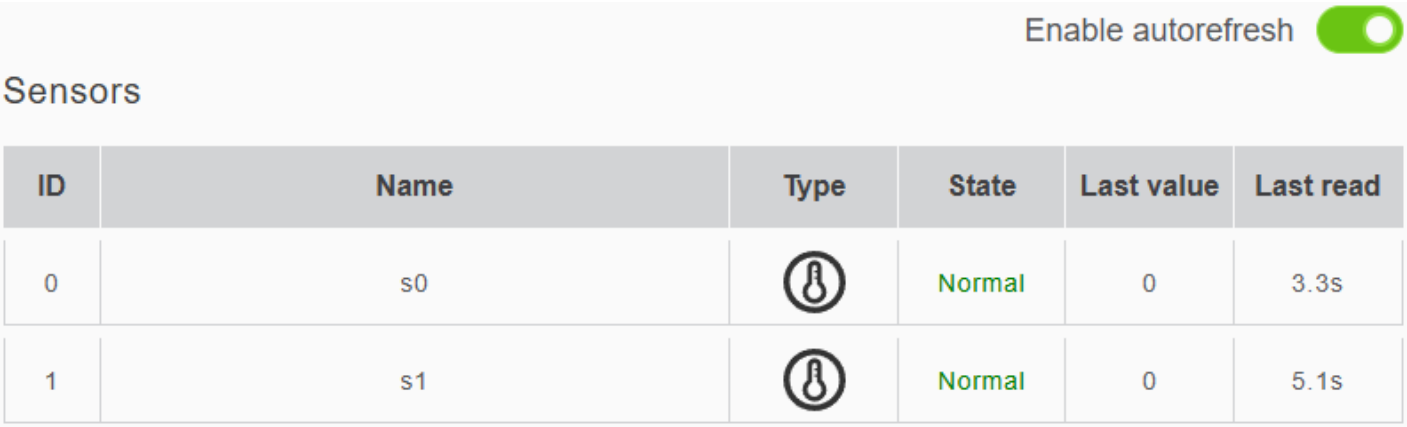
Device status preview

In the **Status** tab, all information about currently used outputs, inputs and sensor readings can be found.



Sensors window

In this window, current sensor readings are displayed. Sensors can be configured in the **Sensors** tab.



Using the **Enable autorefresh** button, the user can enable or disable automatic readout refreshing.

Individual table columns contain the following data:

- **Name** – Sensor name defined in the **Sensors** tab,
- **Type** – Graphic representation of the sensor type:
  - – Temperature sensor,
  - – Humidity sensor,
  - – Input,
  - – Analogue current sensor 4-20mA,
  - – Pressure sensor,
  - – Analogue voltage sensor 0-10V DC,

-  – Carbon monoxide presence sensor (CO),
-  – Carbon dioxide presence sensor (CO2).

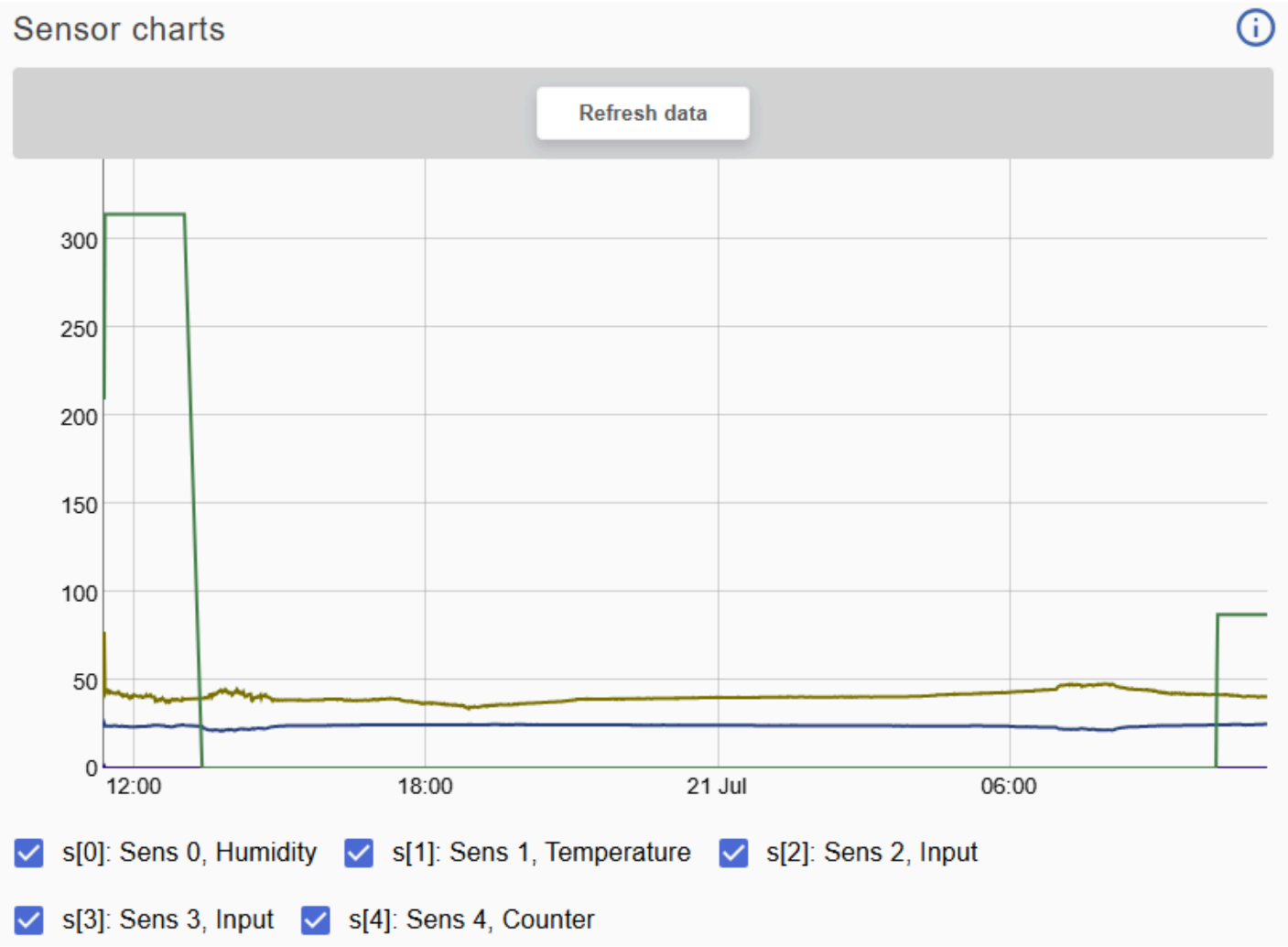
- **State** – Sensor state:
  - **Error** – Reading error (sensor damaged or connected incorrectly),
  - **Normal** – Sensor gives correct readings that are within normal limits,
  - **Warn L** – Lower threshold warning,
  - **Warn H** – Upper threshold warning,
  - **Alert L** – Lower alarm threshold,
  - **Alert H** – Upper alarm threshold.
- **Last value** – Last read value,
- **Last read** – Time that has passed from the last reading (value is refreshed constantly when autorefresh is on).

> **Tip**
>
> **The Sensors window is visible only after a sensor has been configured in the Sensors tab.**

Sensor charts

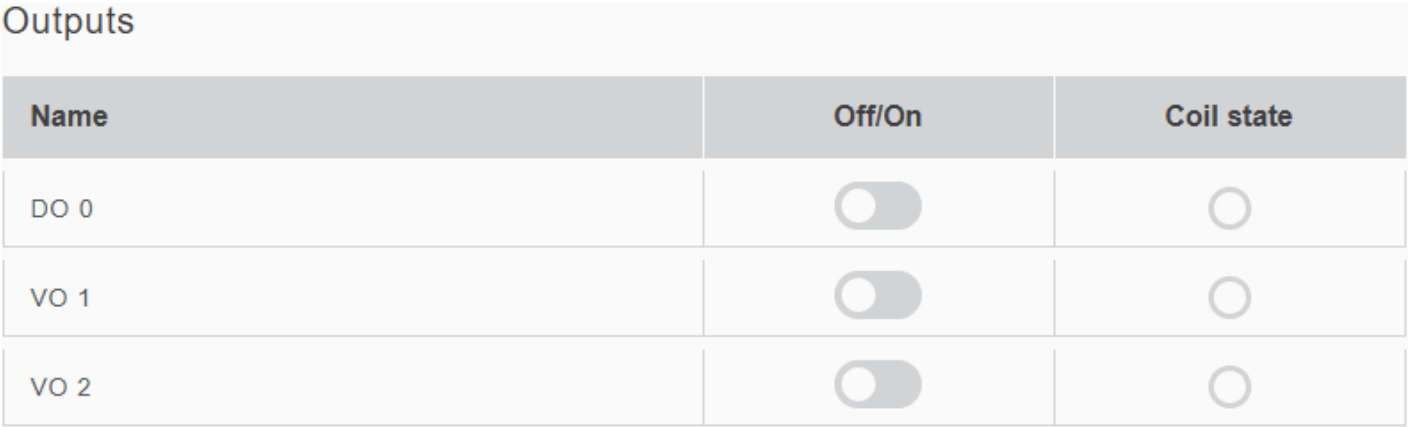
This window allows quick preview of all available sensor graphs.

The **Refresh data** button allows the user to manually refresh the data, while the blue **i** icon indicates the amount of records present in the device's memory.



Outputs window

In this window, current output state is displayed. Outputs can be defined in the **I/O Settings** tab.



Individual table columns contain the following data:

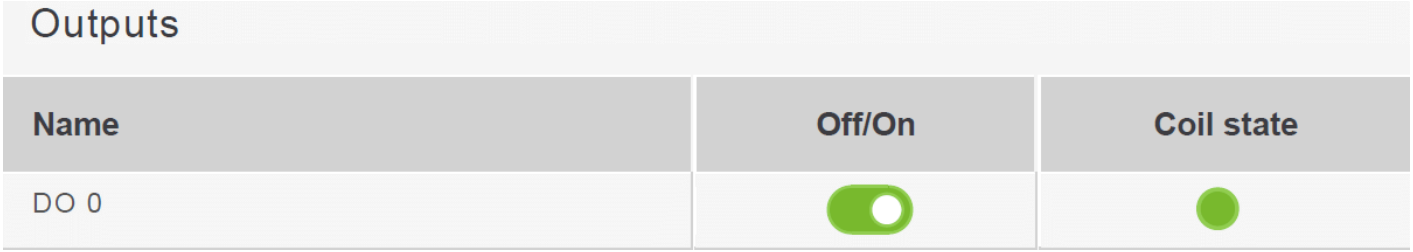
- **Name** – Output name defined in the **I/O Settings** tab.

The following input types are available:

- **Digital – DO** – Physical module outputs,
- **Virtual – VO** – Virtual outputs used for binding and relations configuration.

If the output state is dependent upon different factors, appropriate information is shown under its name:

- **output unavailable – assigned to the shutter**,
- **output unavailable – output is routed** – See section **Binding**.
- **Off/On** – Current output state, clicking the left mouse button in this area will change the output state - this option enables manual output control,
- **Coil state** – Current relay coil state - green colour means that the relay is activated.



Output activation (**Off/On** column in the table) is not always identical as the **Coil state**.

Example

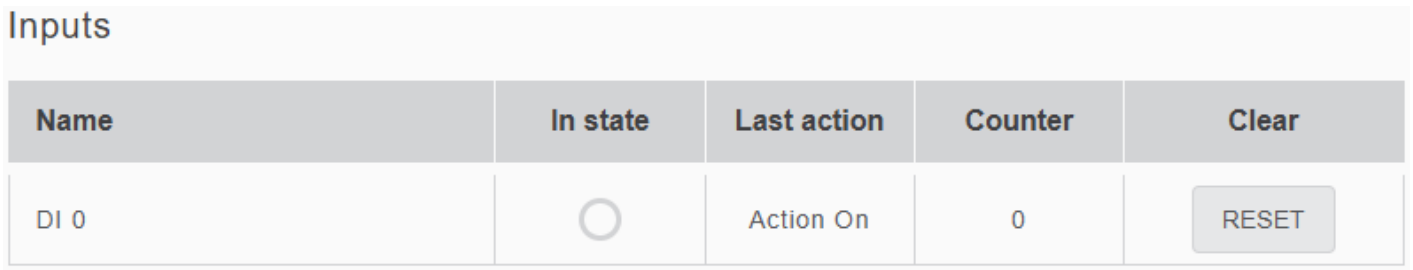
If the output is configured in astable mode, with Time on and Time off parameters defined, enabling the output in the Status tab changes the state in the Off/On column. In this case we can observe the coil state is alternately activated/deactivated, according to the parameters defined in Time on / Time off.

Tip

If the output is configured for shutter control or other input/output state has been bound to it, testing its operation in the Off/On column will not be possible.

Inputs window

In this window, current input state is displayed. Inputs can be defined in the **I/O Settings** tab.



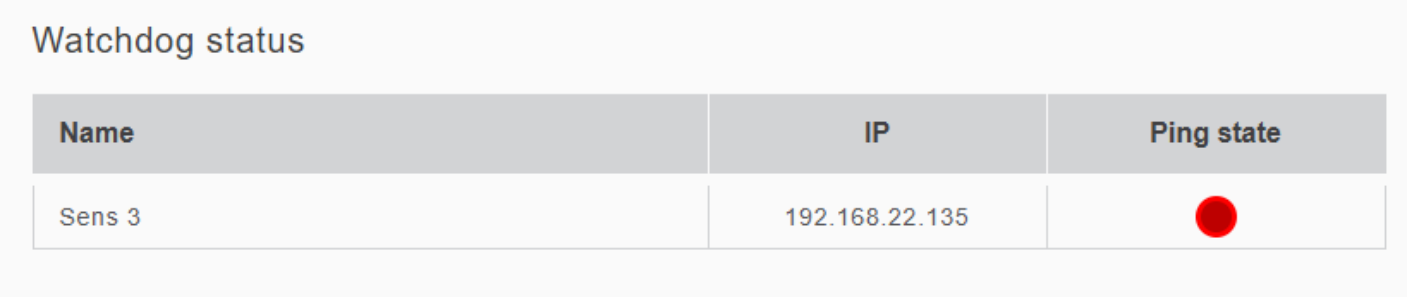
Individual table columns contain the following data:

- **Name** – Input name defined in the **I/O Settings** tab,
- **In state** – Input state,
- **Last action** – Last registered action (eg. Action On),
- **Counter** – Displays the amount of times the input has been activated since last reset,

- **Clear** – Resets the counter.

Watchdog status window

In this window, current state of the remote hosts ping (Watchdog) function is displayed.

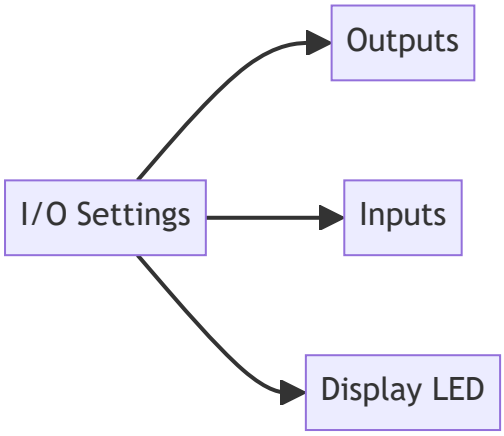


- **Name** – Ping name,
- **IP** – IP address of the pinged device,
- **Ping state** – Status indicator:
  - **Green colour** – Correct ping response,
  - **Red colour** – Response error.

The **Watchdog** function is described in the **Watchdog** section of this manual.

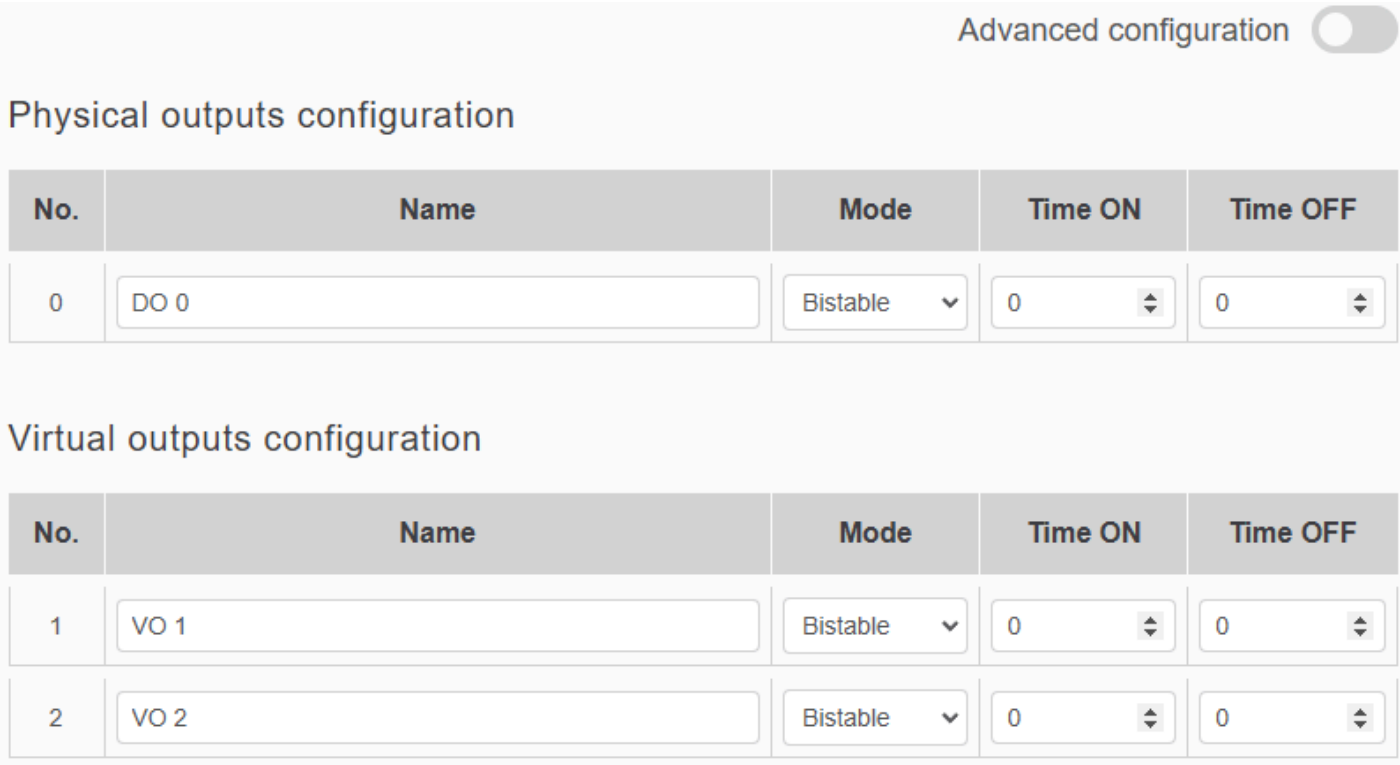
Inputs/outputs configuration

In the **I/O Settings** tab, advanced configuration options can be accessed, allowing the user to define device operation. Here, behaviour of inputs and outputs can be configured. Additionally, this tab gives users the option to configure the display.

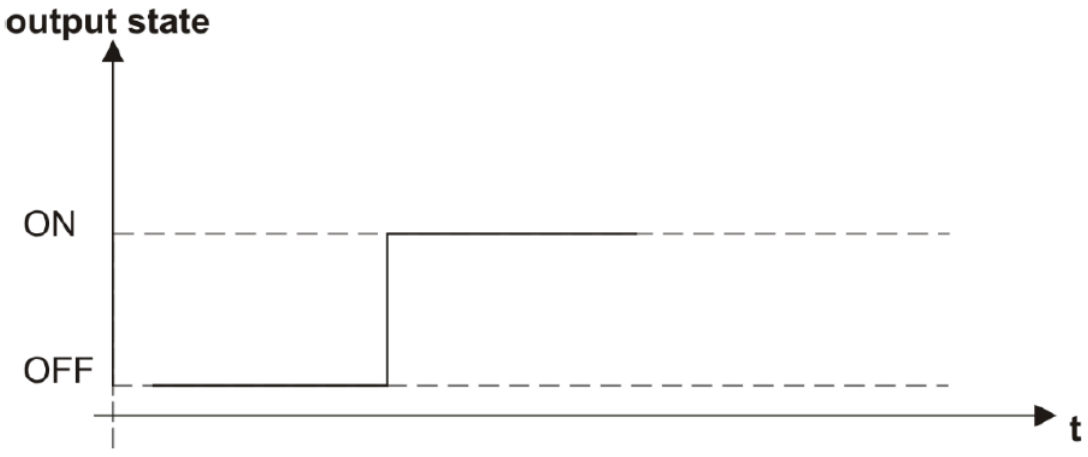


Outputs

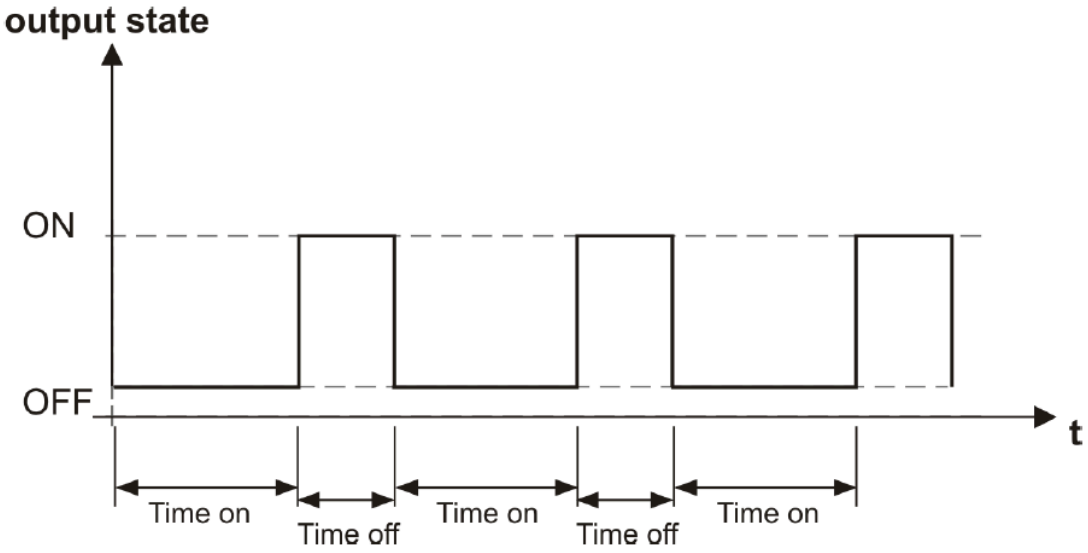
This tab allows configuration of outputs – both physical and virtual *(option)*. The following settings can be changed in individual columns:



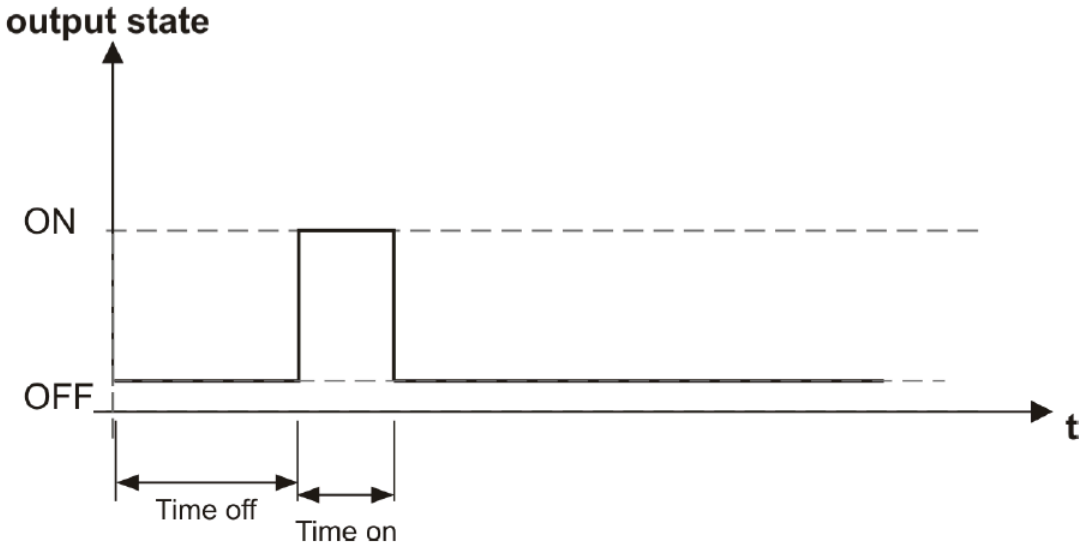
- **Name** – This field allows the output name to be changed,
- **Mode** – Output operation mode:
  - **Disable**,
  - **Bistable**,



  - **Astable** – Periodic mode - output is activated and deactivated periodically. The activation and deactivation times are defined by the parameters **Time on** and **Time off**,

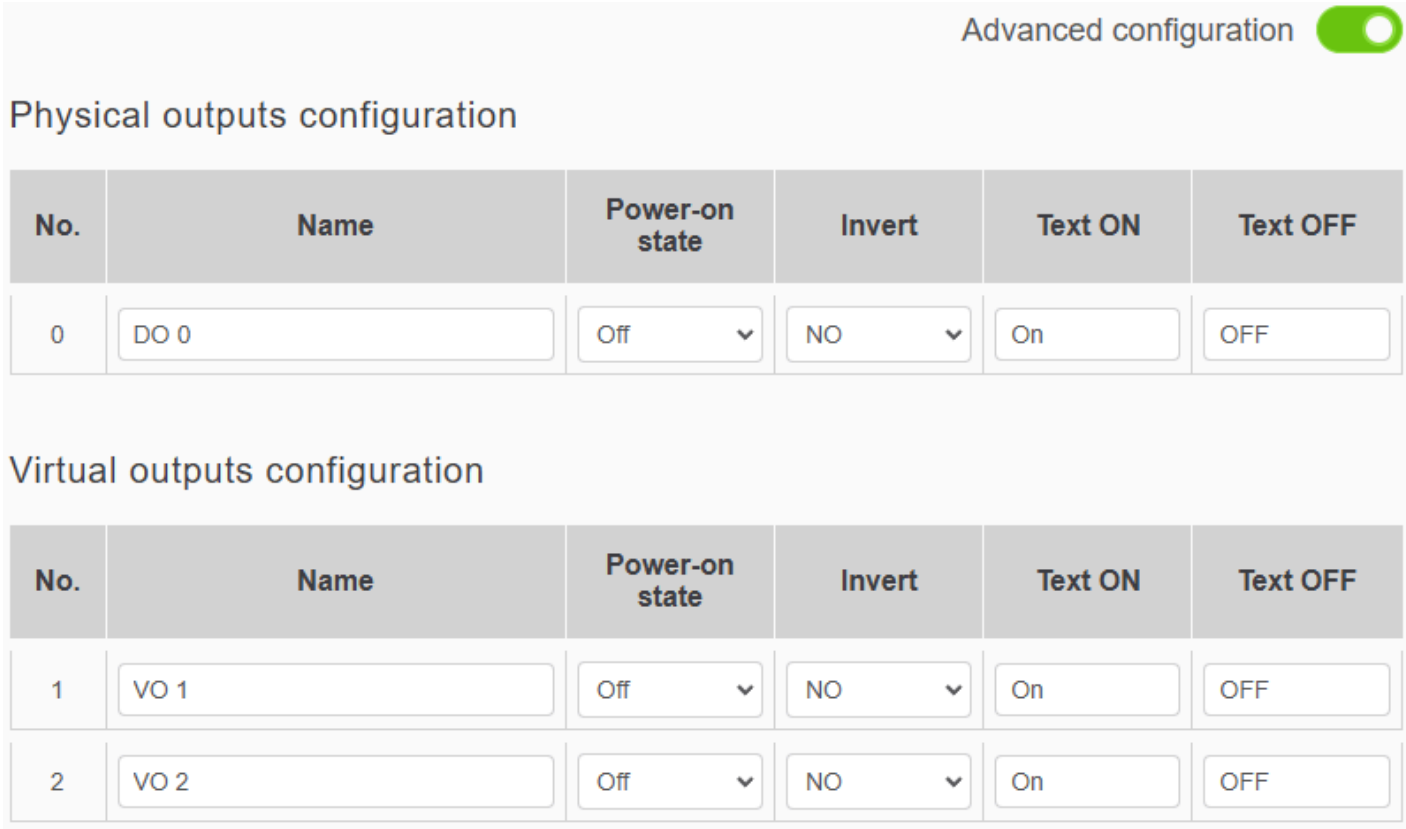


- **One-pulse** – Single output trigger mode - output is activated for a time defined in **Time on** after time defined in **Time off** passes,



- **Time on** – (parameter used in **Astable** and **One-pulse** mode),
- **Time off** – (parameter used in **Astable** and **One-pulse** mode).

Clicking **Advanced configuration** enables changing of advanced output settings:

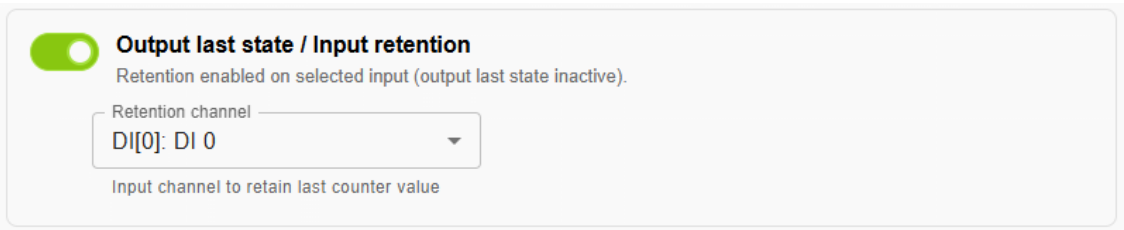


- **Name** – This field allows the output name to be changed,
- **Power-on state** – State that the device should reach after power is connected to the module:
  - **Off**,
  - **On**,
  - **Last** – State before the power was disconnected.
- **Invert** – Output channel inversion:
  - **NO** – Normally open,
  - **NC** – Normally closed.
- **Text ON** – Text dispayed on the LED display when the output is activated,
- **Text OFF** – Text dispayed on the LED display when the output is deactivated.

LAST OUTPUT STATE OR COUNTER RETENTION

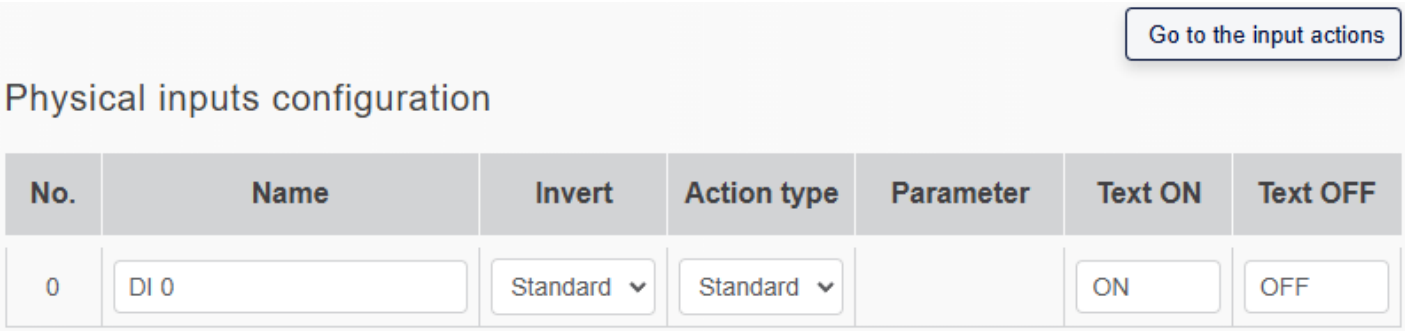
The module offers the possibility to store the last output or specified input counter state in non-volatile memory.

The **Ouptut last state / Input retention** slider enables selection of the desired setting.

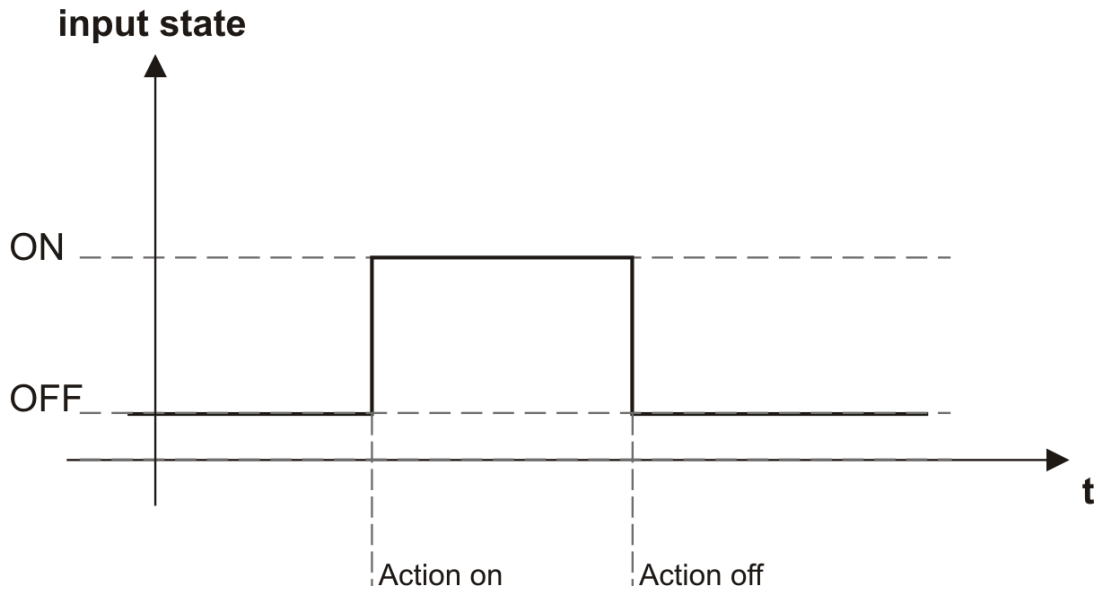


Inputs

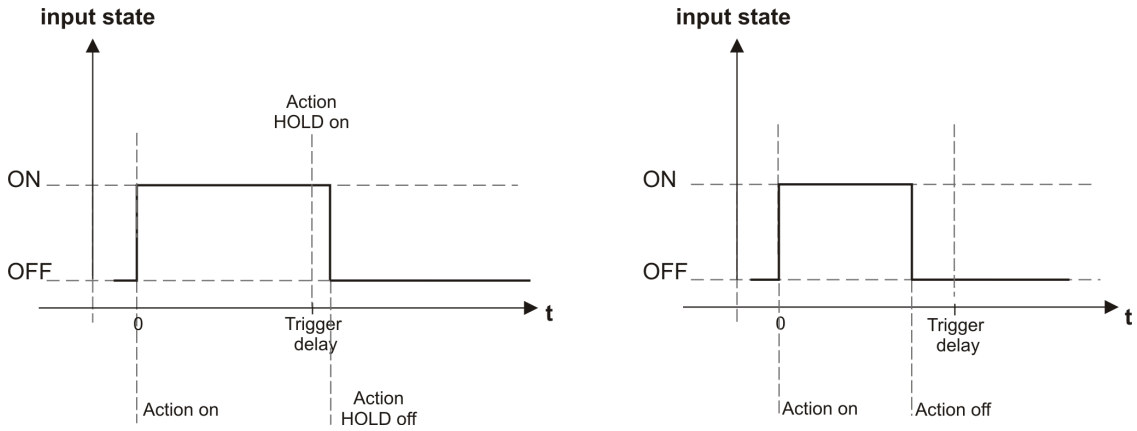
This tab allows configuration of inputs supported by the device. The following settings can be changed in individual columns:



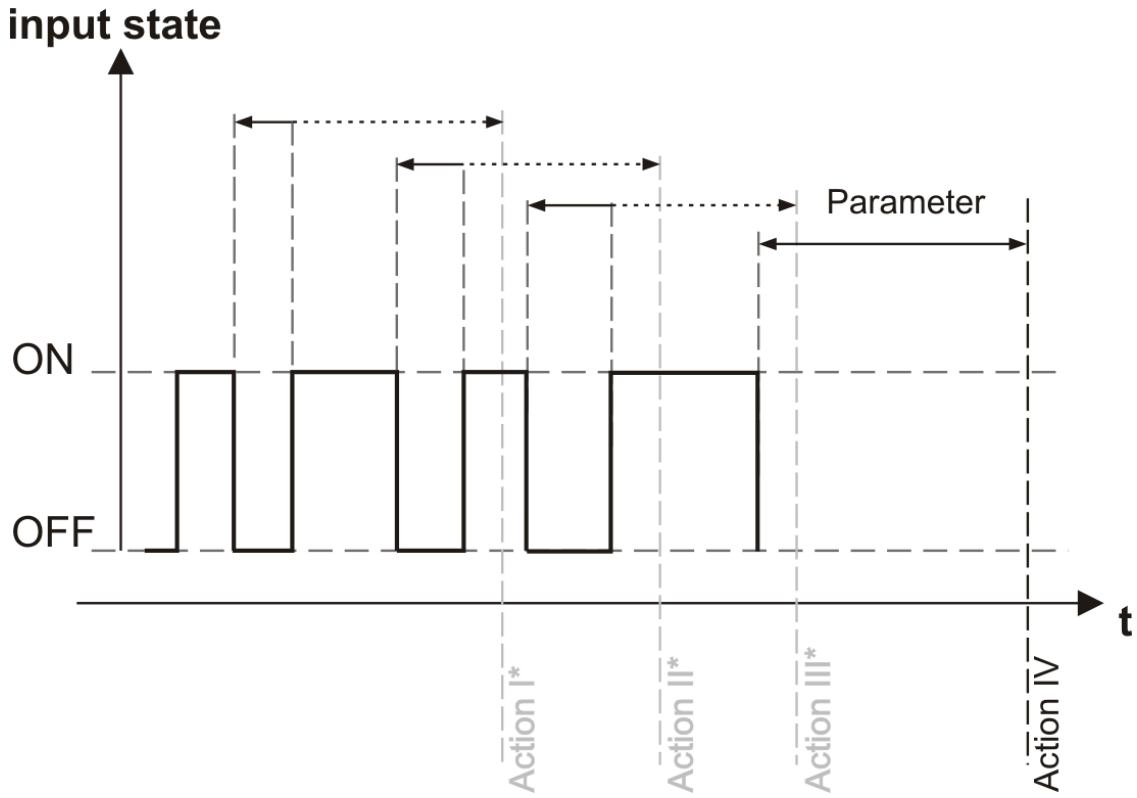
- **Name** – This field allows the input name to be changed,
- **Invert** – Input channel inversion,
- **Action type**:
  - **Standard** – Action is triggered by input activation/deactivation,



- **Hold** – Triggering of a defined action is dependent upon the pulse length on the input. The pulse recalls the action defined as **Action on**. If the pulse persists and exceeds the time in the **Parameter** field - action defined as **Action hold on** is recalled. If the pulse ceases before the time defined in **Parameter** - **Action off** is recalled. If the pulse ceases after the time defined in **Parameter** field - **Action hold off** is recalled,

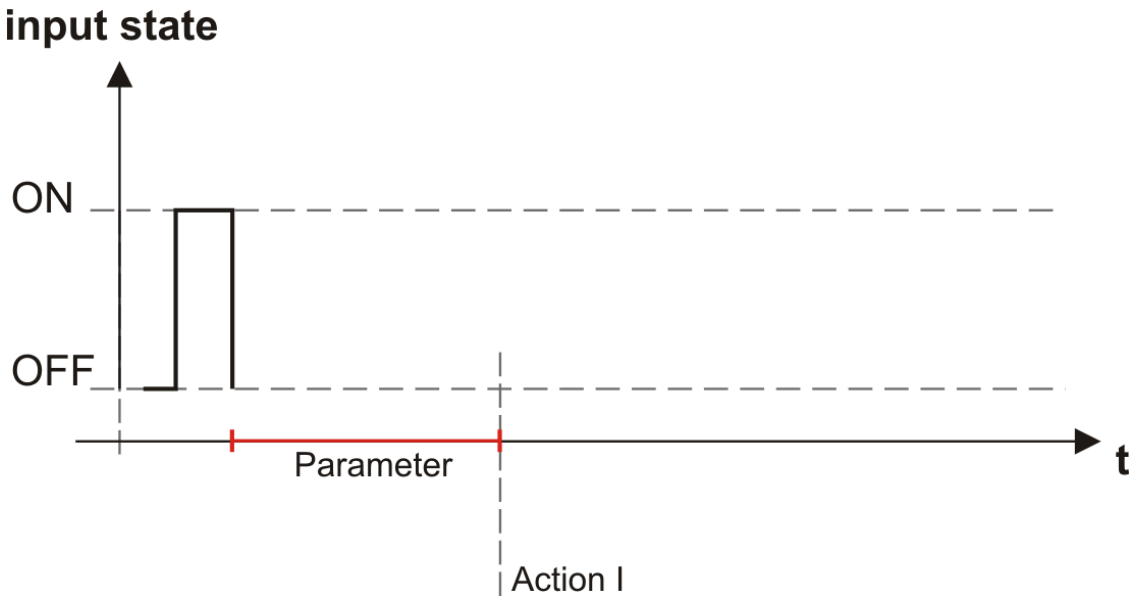


- **Cnt** – Pulse counter during specified time period - the action is recalled by the defined amount of activations in the time period specified by **Parameter**,

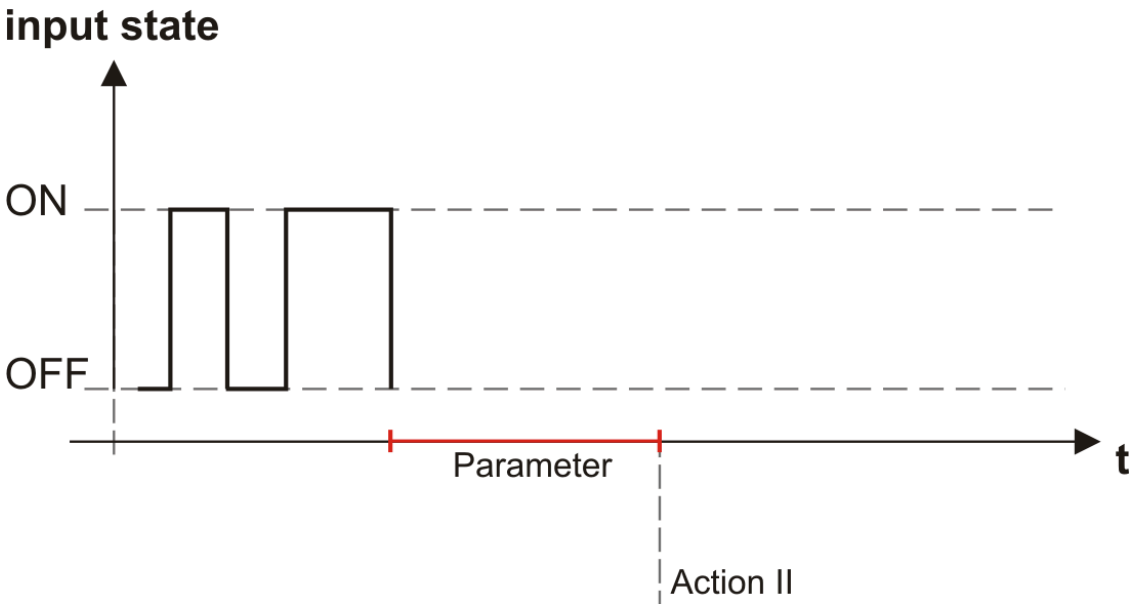


Action will be recalled only when no subsequent pulse occurs (input is not activated again). The defined action is recalled after the pulse absence delay time passes (i.e. a button is released). If another pulse occurs during this delay time, the countdown is stopped.

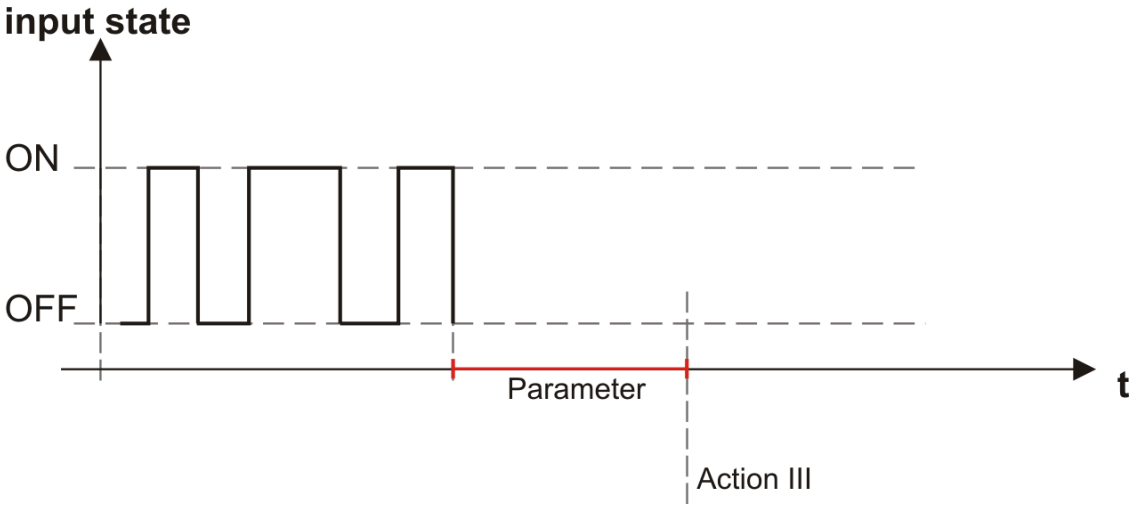
Recalling action I:



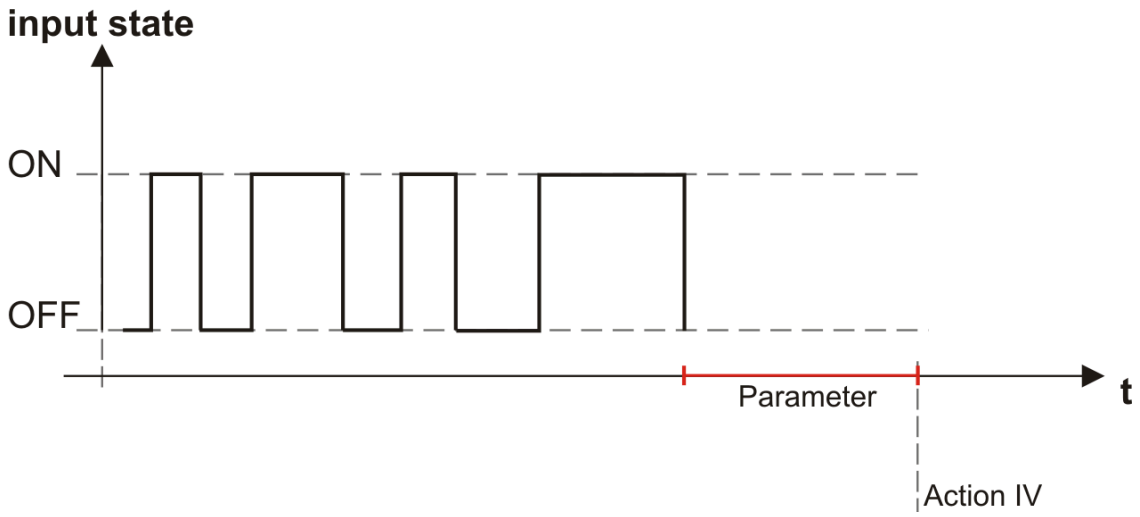
Recalling action II:



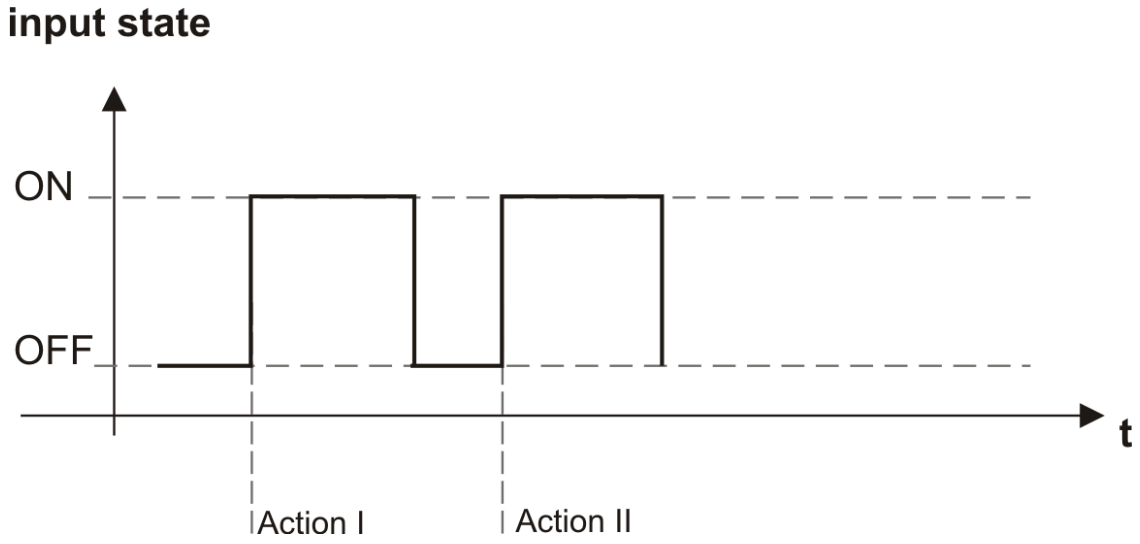
Recalling action III:



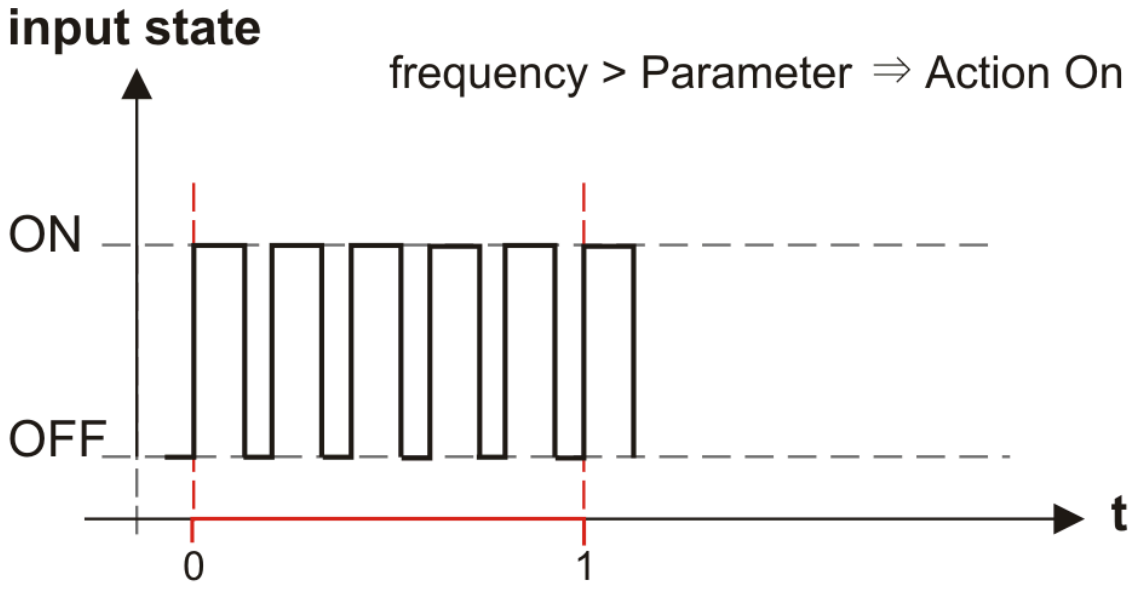
Recalling action IV:

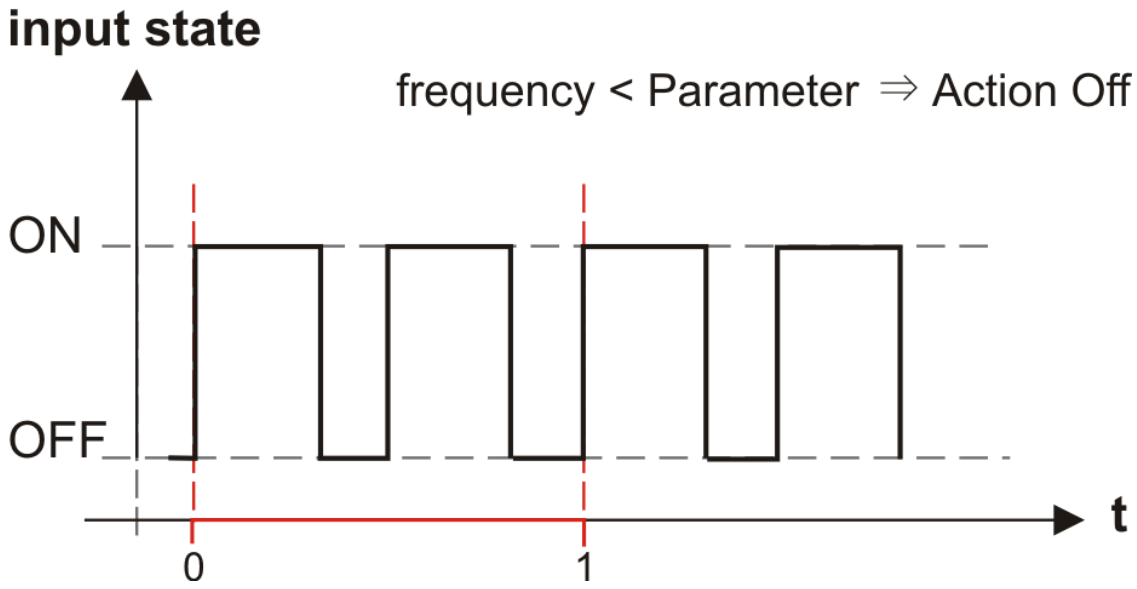


- **Toggle** – Subsequent pulses on the input recall **Action I** / **Action II** alternately,



- **Freq** – Action recall is dependent upon the frequency of pulses on the input. The desired frequency is inputted into the **Parameter** field in **Hz**,



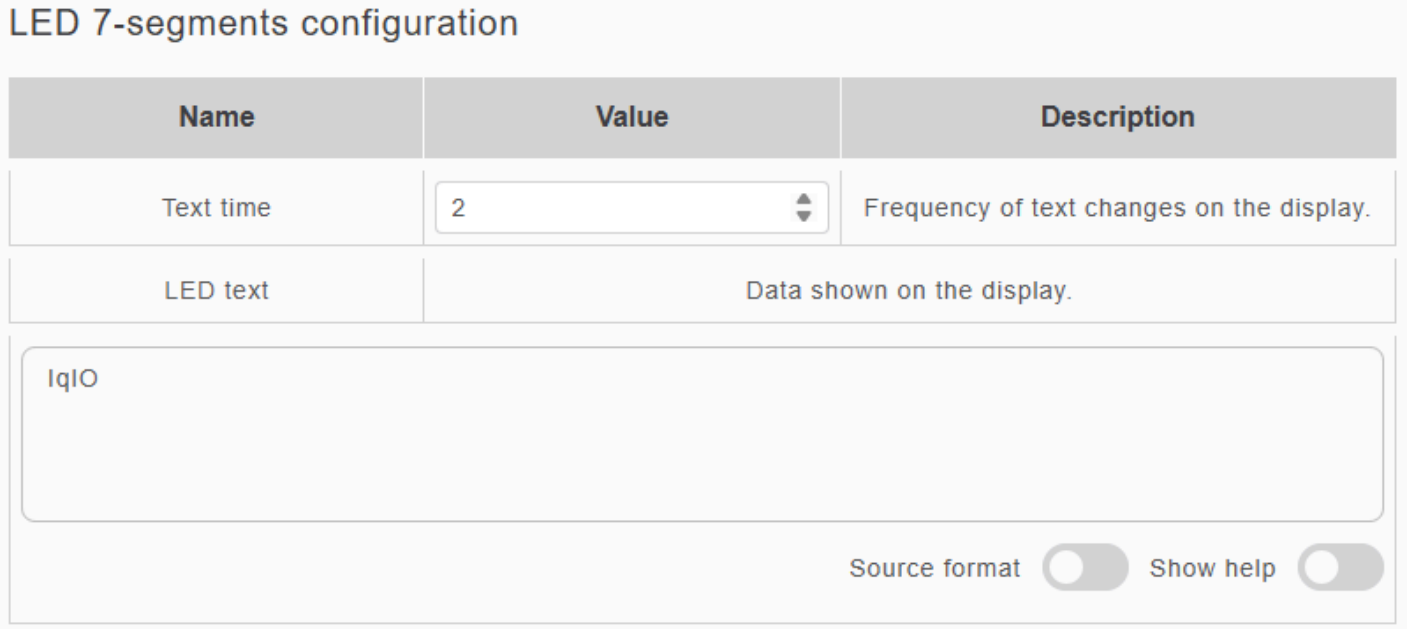


- **Parameter** – Value used in various action activation methods. When the cursor is placed over the input field, a parameter unit is displayed - eg. **Hz** for **Freq**,
- **Text ON** – Text dispayed on the LED display when the input is activated,
- **Text OFF** – Text dispayed on the LED display when the input is deactivated.

The **Go to the input actions** button located in the upper-right corner allows quick access to the **Action/Inputs** tab.

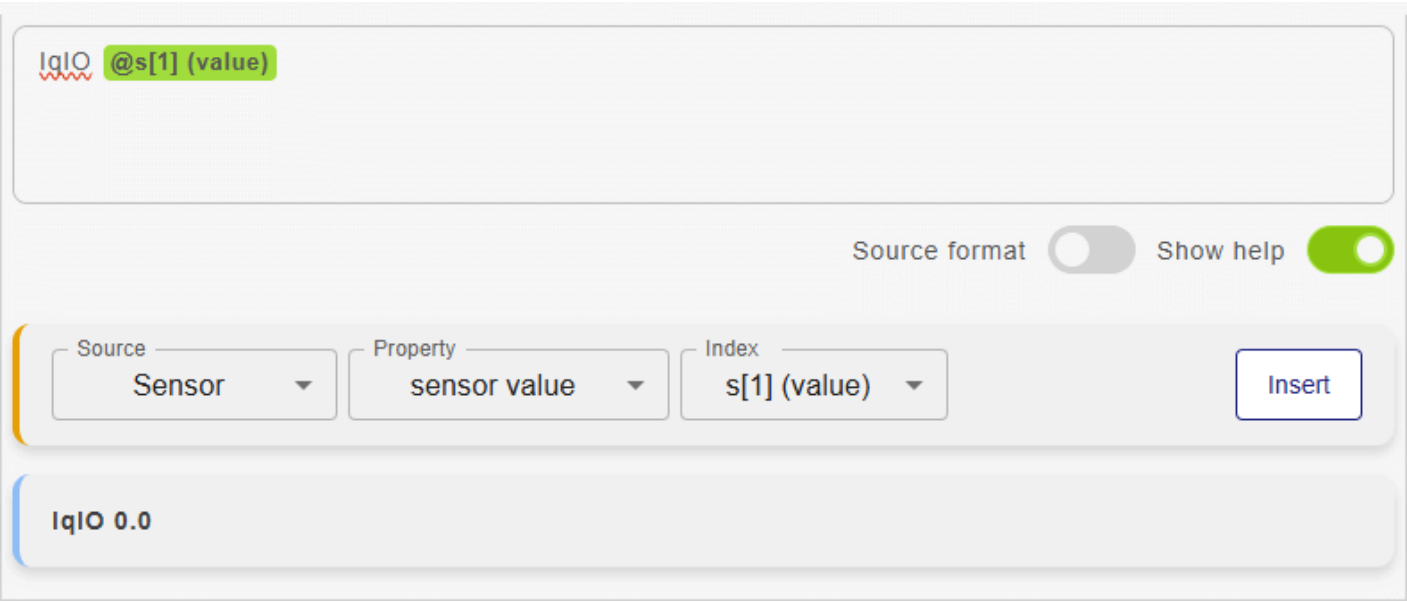
Display LED

The display settings can be configured in this tab:



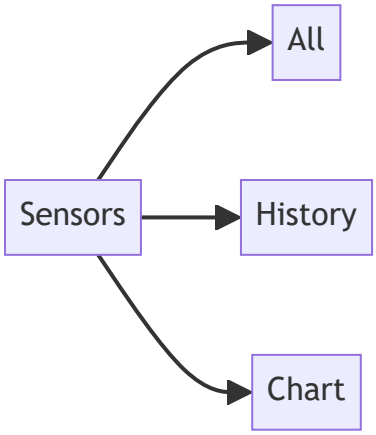
- **Text time** – Frequency of display text changes – in seconds,
- **LED text** – Data displayed on the main screen. Predefined variables can be used.

Clicking **Show help** opens a tool that allows easy input of variables into the **LED text** field. Displayed text preview is available in the bottom part.



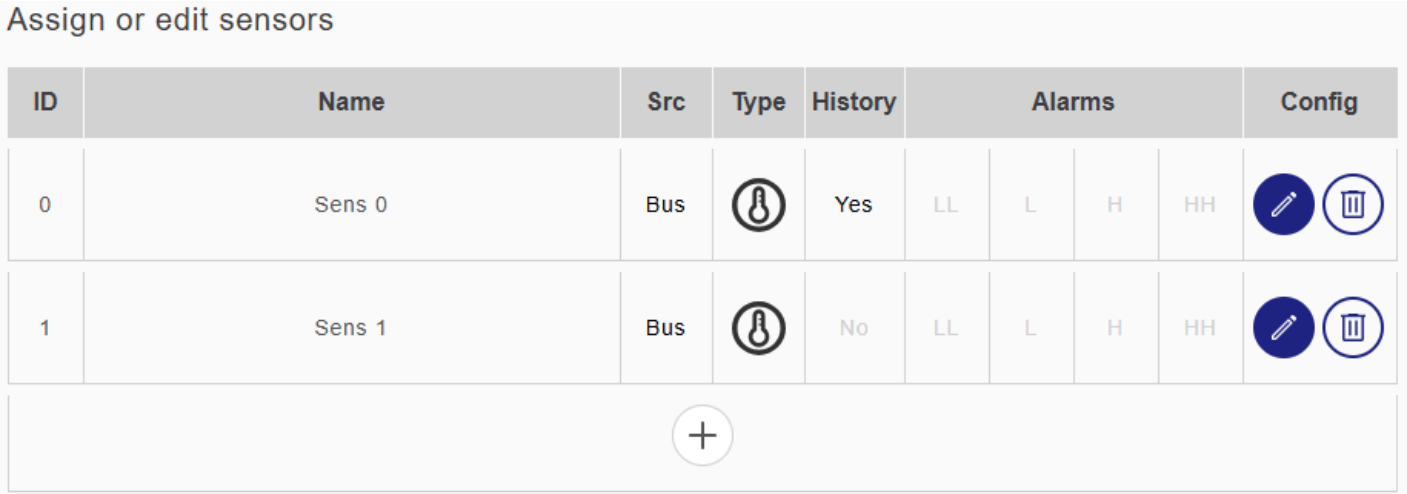
Sensors configuration

This tab allows the user to assign specific sensors to dedicated memory slots and to configure their parameters. It allows individual control over each sensor, setting specific parameters and modes of operation. Additionally, it enables the preview of historical readings, which can be downloaded in the form of JSON or CSV files.



All

Thanks to this tab, the user has full control over sensors configuration, readings correction and notifications. New sensors that integrate with the system automatically can be added. The user can define parameters for each sensor, customizing them to own needs and operation conditions. Additionally, this tab shares the tools to edit existing sensors, allowing them to be constantly adaptable to the changing conditions or user needs.



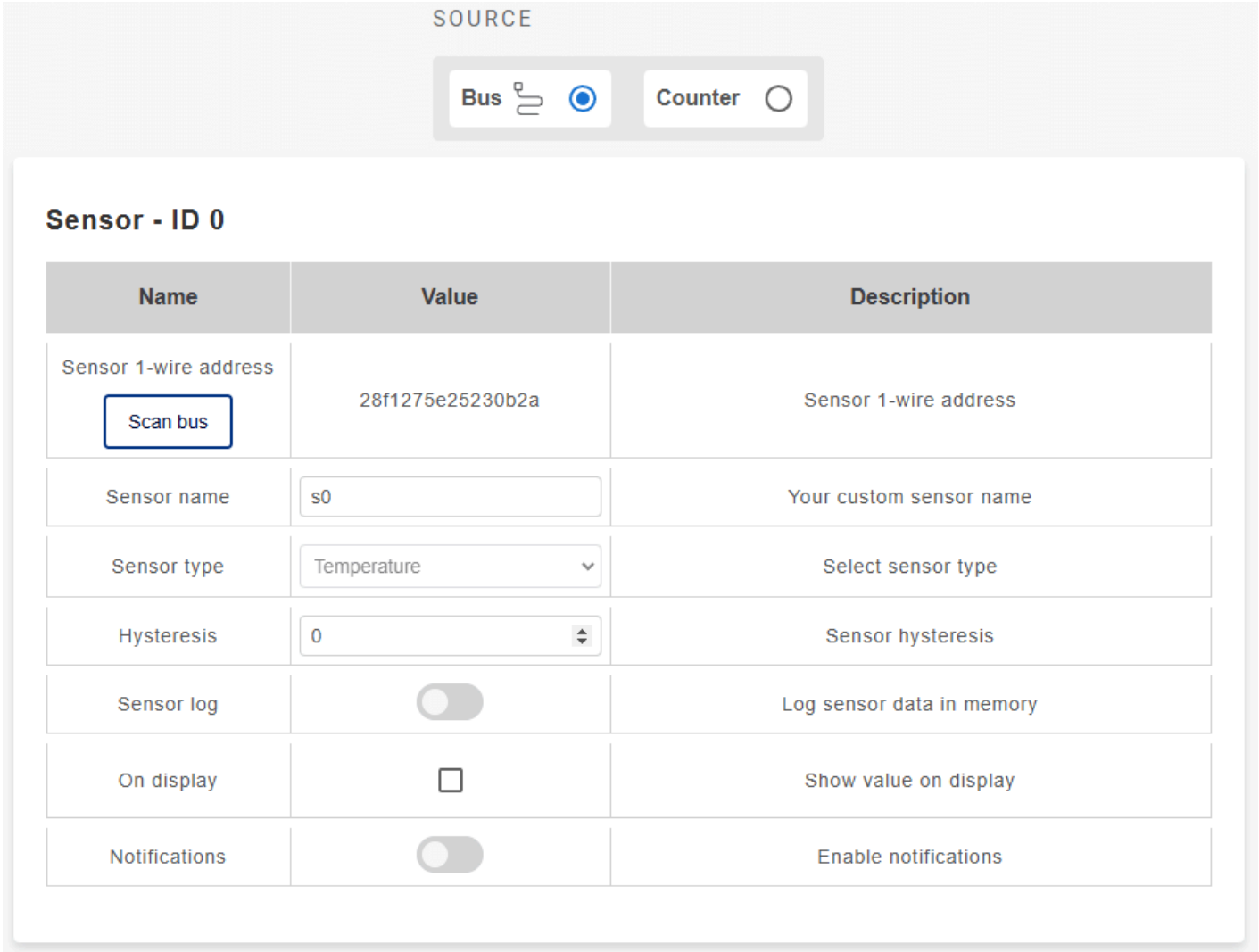
Each sensor table column contains the following information:

- **ID** – Sensor identification number,
- **Name** – Sensor name,
- **Src** – Source, from which the sensor readings are taken (1-Wire or counter),
- **Type** – Connected sensor type:
  - – Temperature sensor,

-  – Humidity sensor,
-  – Input,
-  – Pressure sensor,
-  – Analogue 0-10V DC voltage sensor,
-  – Analogue 4-20mA current sensor,
-  – Carbon monoxide presence sensor (CO),
-  – Carbon dioxide presence sensor (CO2).

- **Log** – Informs if the sensor has an active (Yes) or inactive (No) readout logging function,
- **Alarms** – Activated warnings/alarms:
  - **LL** – Lower alarm threshold,
  - **L** – Lower warning threshold,
  - **H** – Upper warning threshold,
  - **HH** – Upper alarm threshold.
- **Config** – Sensor configuration buttons:  – Edit sensor parameters,  – Delete sensor.

The following dialogue window is displayed afer clicking the edit button:



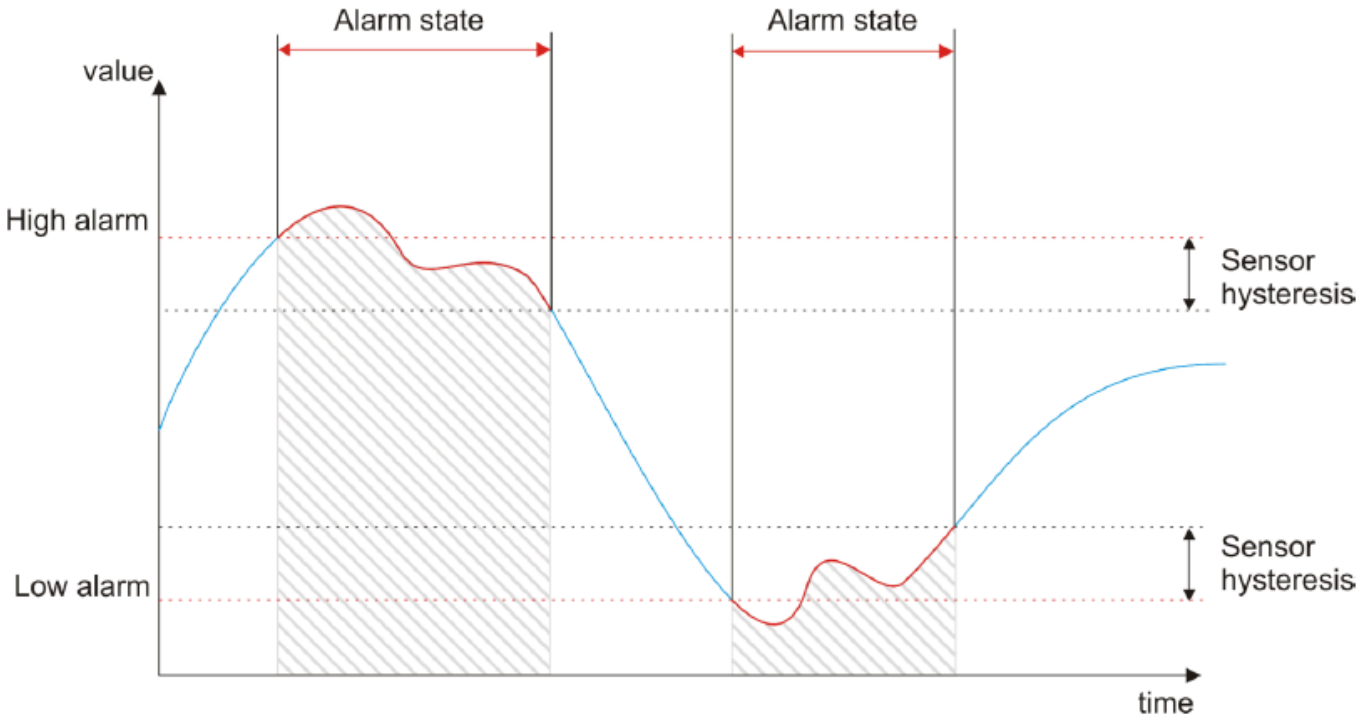
- **Source** – Sensor source *(version dependent)*:
  - **Bus** – Sensor bus,
  - **mbAgent** – Data read off Modbus,
  - **Inveo** – Data received from another device via iCluster,
  - **Counter** – Counter input.
- **Sensor bus address** – **Scan bus** makes it possible to locate and assign a sensor connected to the device,
- **Sensor name**,
- **Sensor type**:
  - **Temperature**,
  - **Humidity**,
  - **Input**,
  - **Current**,
  - **Pressure**,
  - **Voltage**,
  - **CO** – Carbon monoxide,

- **CO2** – Carbon dioxide.

- **Hysteresis** – Sensor hysteresis (inactive if the sensor type is set to **Input**) – applies to the warning and alarm states. The hysteresis defines the maximum acceptable difference between the warning/alarm threshold and normalization value.

Example

High warning is set to 30 degrees, hysteresis is 2 degrees. After the sensor reaches 30°C, the device will reach the alarm state that will presist until the sensor value drops to 28°C (30-2=28). Hysteresis is the offset between warning/alarm activation or deactivation, preventing the alarm states from being triggered too often during small measurement fluctuations.

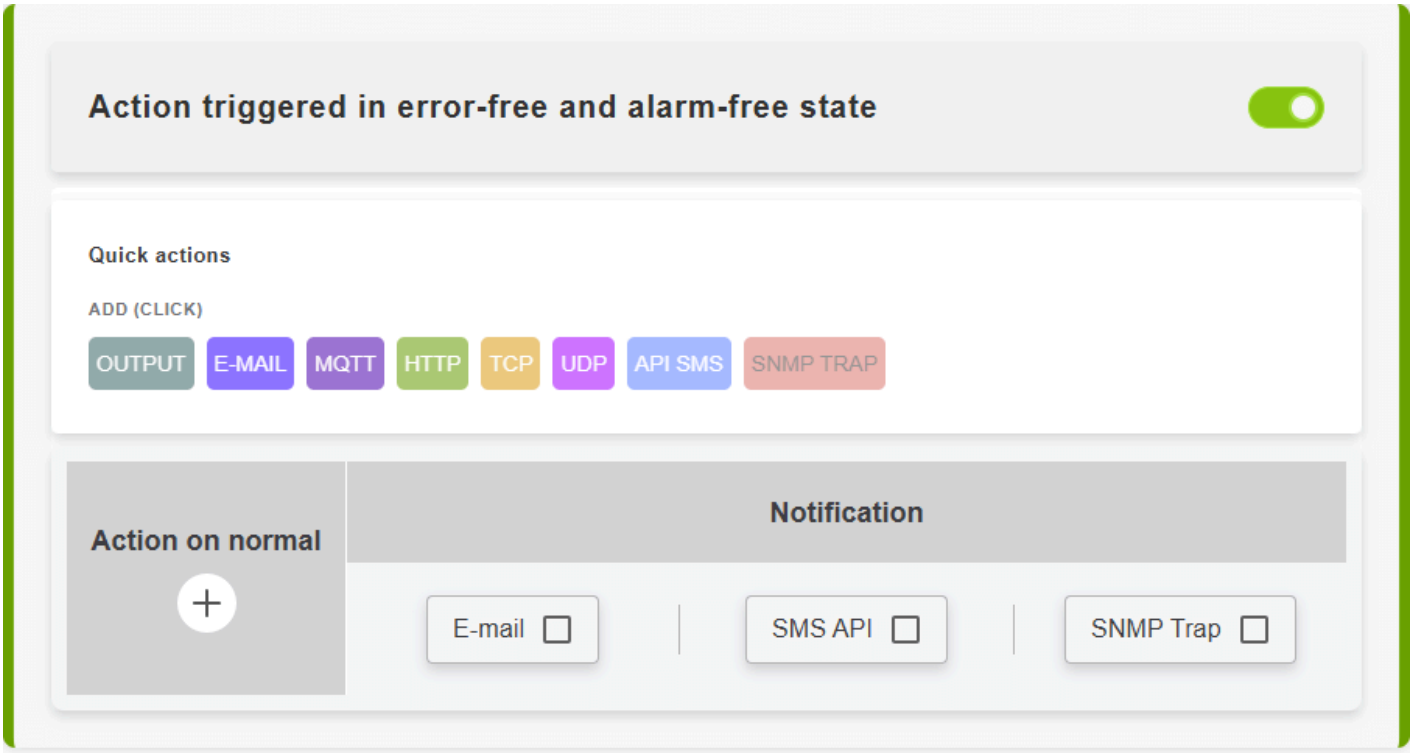


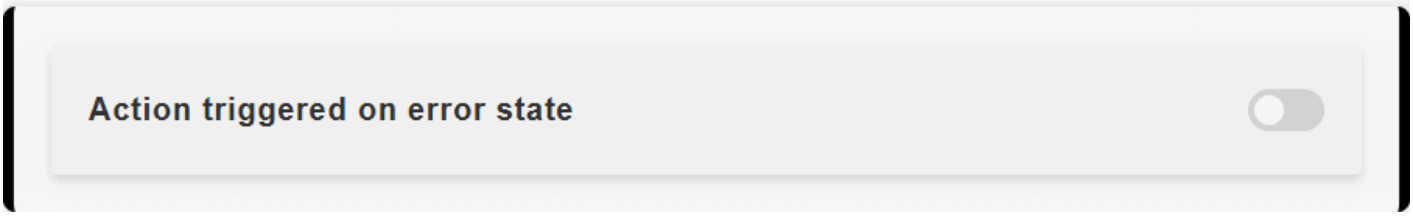
- **Channel** – Channel selection – active only if the sensor type is set to **Input**,
- **Sensor log** – Enable/disable sensor data logging to device memory *(version dependent)*,
- **On display** – Enable/disable display of measured value on the LED display *(IQIO series only)*,
- **Notifications** – Enable/disable notifications,
  - **MQTT notification** – Enable/disable MQTT notifications.

Enabling **Notifications** allows to change the device's reaction to:

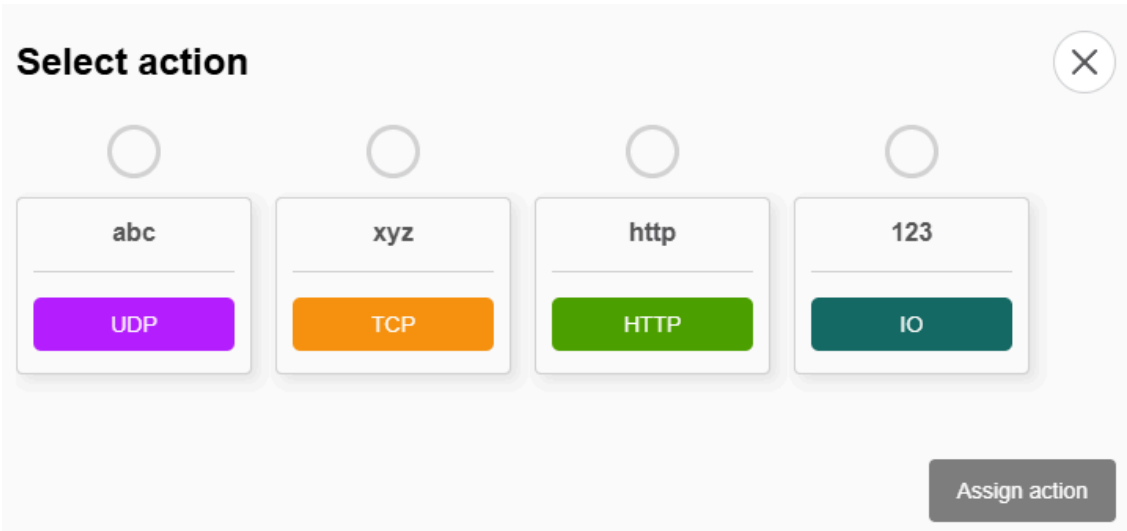
- Transition of sensor to an alarm- and error-free state,
- Transition of sensor to the error state.

The user can select the type of a notification that will be sent in response to the above events. Appropriate settings in the **Services** tab must be configured first for the notifications to be sent.



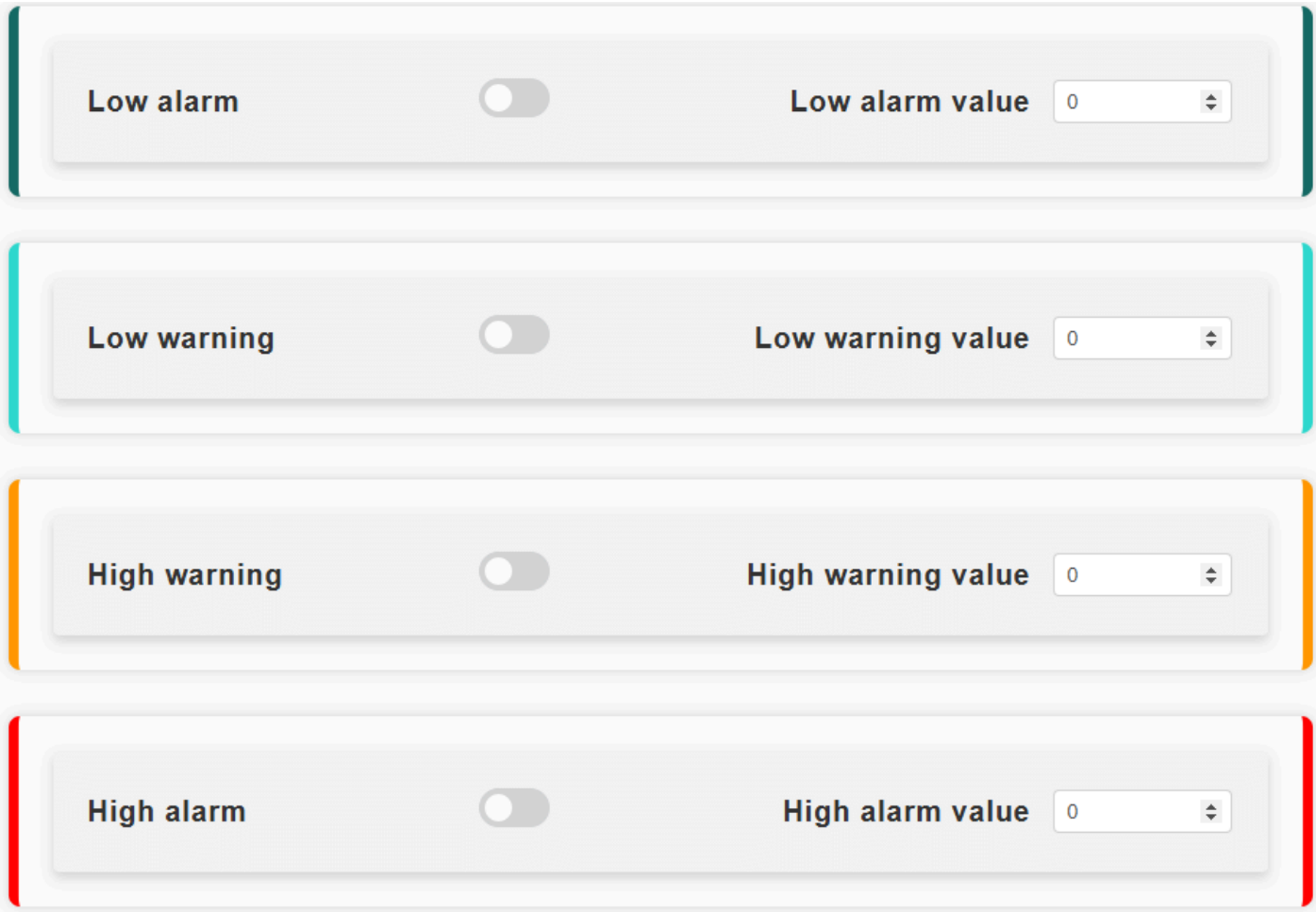


To assign an action, click **+**. A dialogue window will be displayed, where the desired action (defined previously in **All**) can be selected.



ALARMS CONFIGURATION

In the settings section dedicated to sensor alarm configuration, the user gains full control over customization of alarm parameters to his own needs. This allows configuration of alerts and reactions to important sensor operation events.



- **Low alarm** – Enable low level alarm,
  - **Low alarm value** – Value that will make the sensor reach the state of low level alarm.
- **Low warning** – Enable low level warning,
  - **Low warning value** – Value that will make the sensor reach the state of low level warning.
- **High warning** – Enable high level warning,
  - **High warning value** – Value that will make the sensor reach the state of high level warning.
- **High alarm** – Enable high level alarm,
  - **High alarm value** – Value that will make the sensor reach the state of high level alarm.

After the alarm is activated, additional window that allows customization of device reaction for alarm situation appears. Here, the user can configure notifications and assign specific actions.

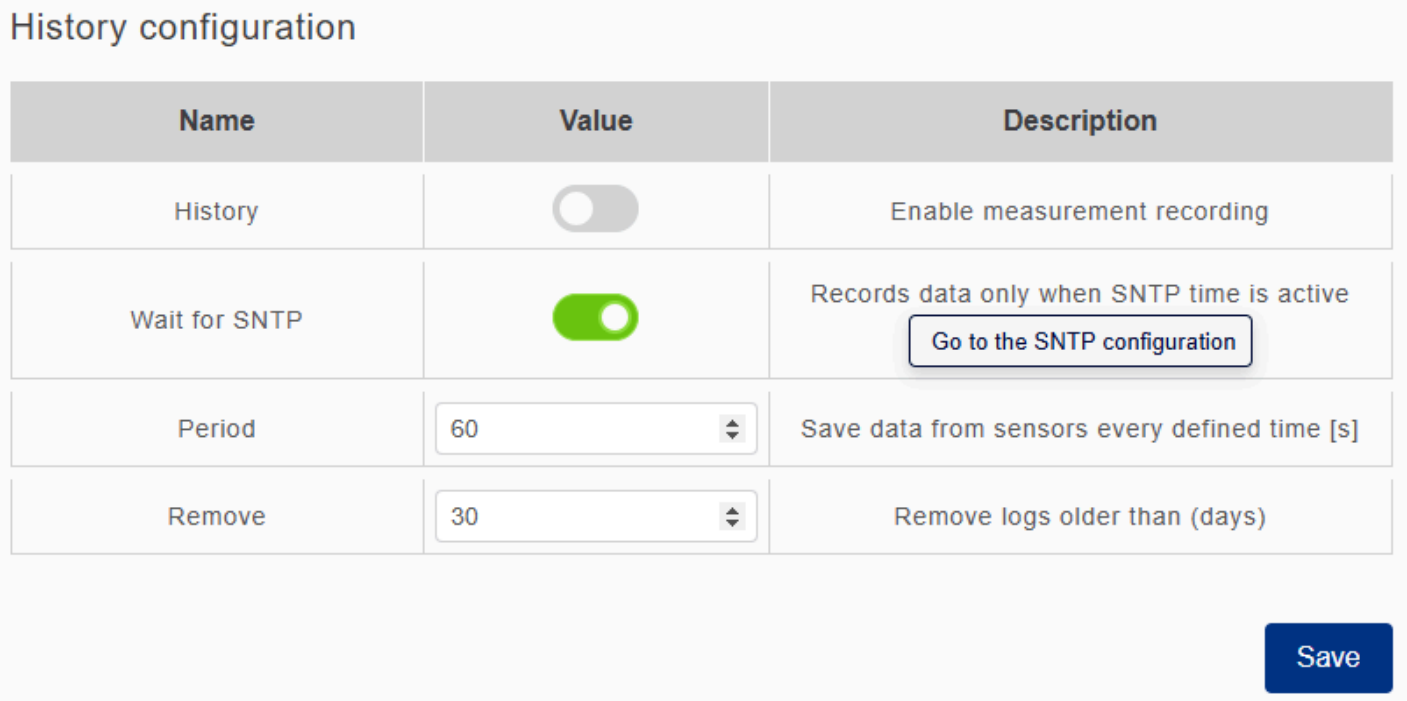
Sensor corrections final = a * (x + preoffset) + b		
Sensor preoffset	0	Sensor preoffset correction
Sensor multiplication: a	1	Multiplying sensor value
Sensor offset: b	0	Fixed correction value

- **Sensor preoffset** – Sensor correction field, according to the linear function formula f(x)=ax*b,

- **Sensor multiplication 'a'**,
- **Sensor offset 'b'** – Constant value correction.

History

This tab allows for activation and configuration of historical sensor readout logging:

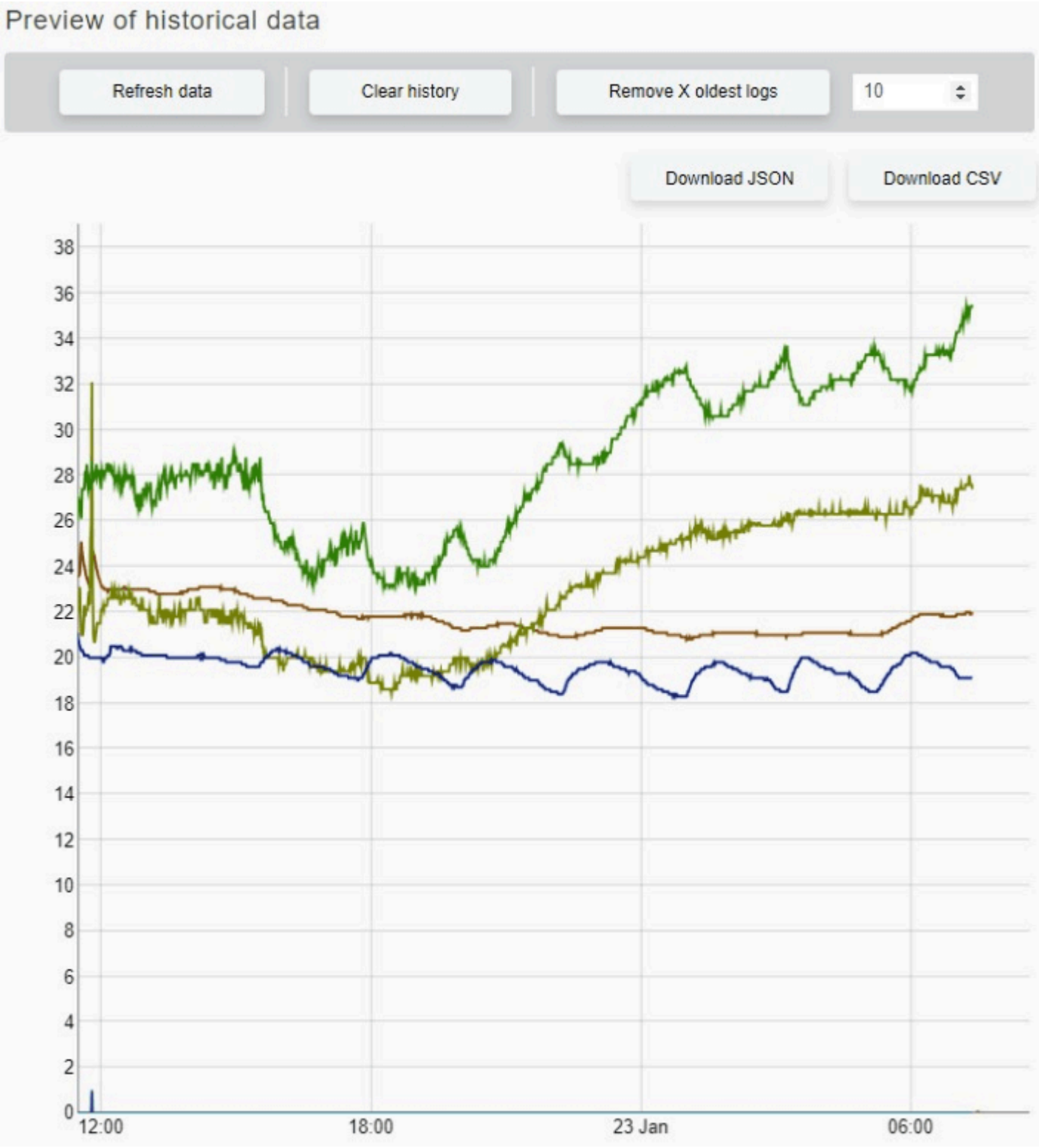


- **History** – Enable/disable sensor readout logging,
- **Wait for SNTP** – When enabled, data from the sensors will be logged only when the device downloads time from the SNTP server after a restart,
- **Go to SNTP configuration button** – Enables quick access to the SNTP configuration tab,
- **Remove** – Allows clearing memory of records older than the specified number of days.

> **Tip**
>
> **In order to log the sensor data into the device's memory, the Sensor log function must be activated in Sensors / All (available in sensor configuration mode).**

Chart

In this tab, all sensors (with **Sensor log** enabled in **Sensors / All**) readings are presented on graphs.



- **Refresh data**,
- **Download JSON**,
- **Download CSV**,
- **Remove X oldest logs** – Remove x oldest sensor readings from memory,
- **Clear history** – Remove all readings from device memory.

Sensor handling

To make sure that the sensor readings are precise and reliable, it is recommended to follow the configuration steps below:

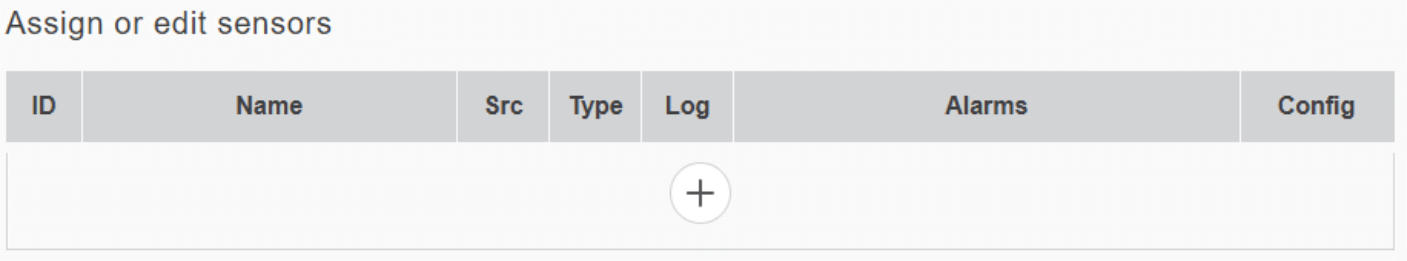
Sensor assignment

First, connect the sensor to the device – consult **Sensor connection diagram**.

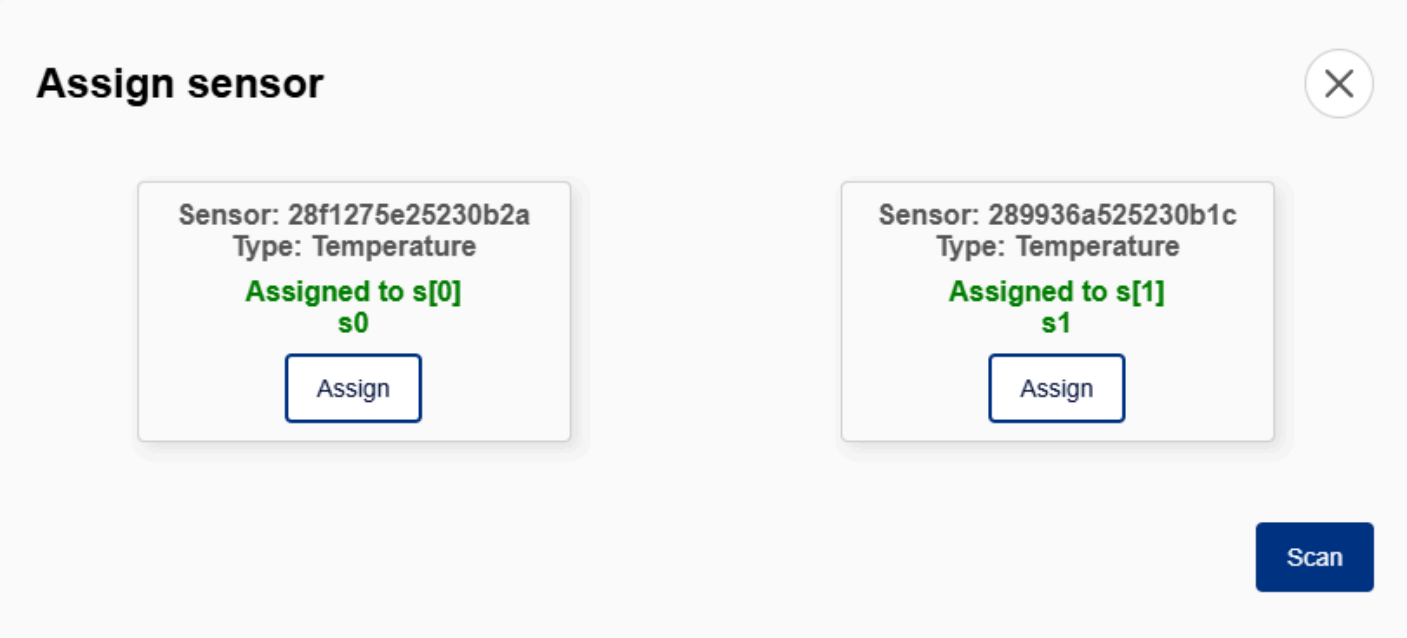
After that, using the device's webpage, locate and configure the sensor's basic parameters. If no sensors were connected to the device previously, the user can use the automatic sensor assignment option. Reset the device after the sensors have been connected – after the device restarts, it will automatically recognize and assign available sensors, specifying their type too.

Manual sensor configurations steps are described below.

Step 1: In **Sensors / All**, click **+**:



In the displayed dialogue window, select the sensor **Source** first. In this case, select **One-wire** (sensor physically connected to the device's bus).
Sensor assignment should begin with clicking **Scan bus**, that will display a window with detected sensors:



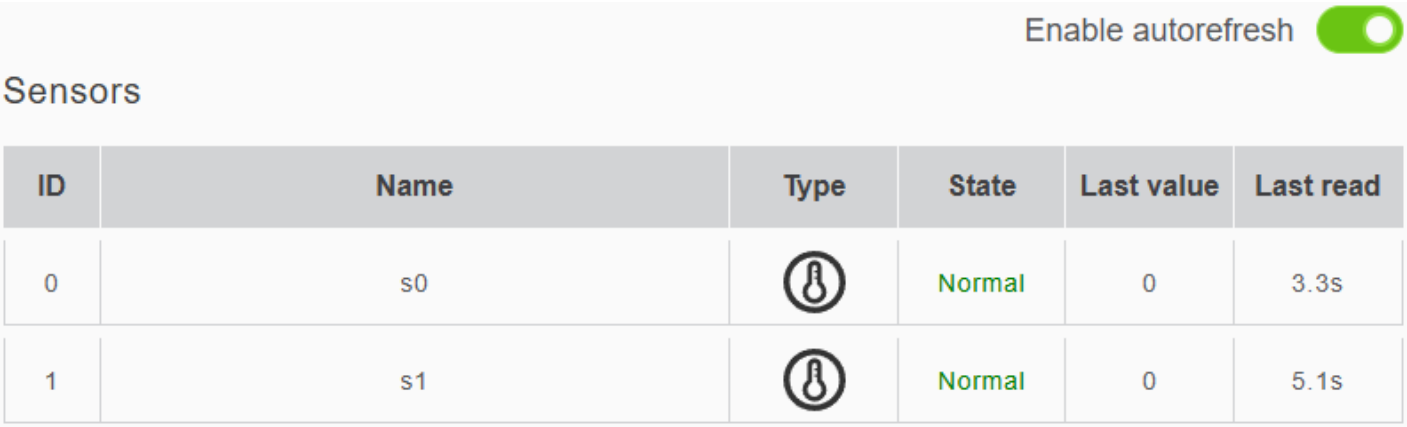
Assign the selected sensor.

Step 2: Basic parameters configuration:

In the sensor's configuration window, set the correct sensor type, assign a name etc. All settings should be applied using the **Save** button.

Step 3: Status tab preview:

A sensor that is configured correctly will display its readings in **Status / Sensors**:



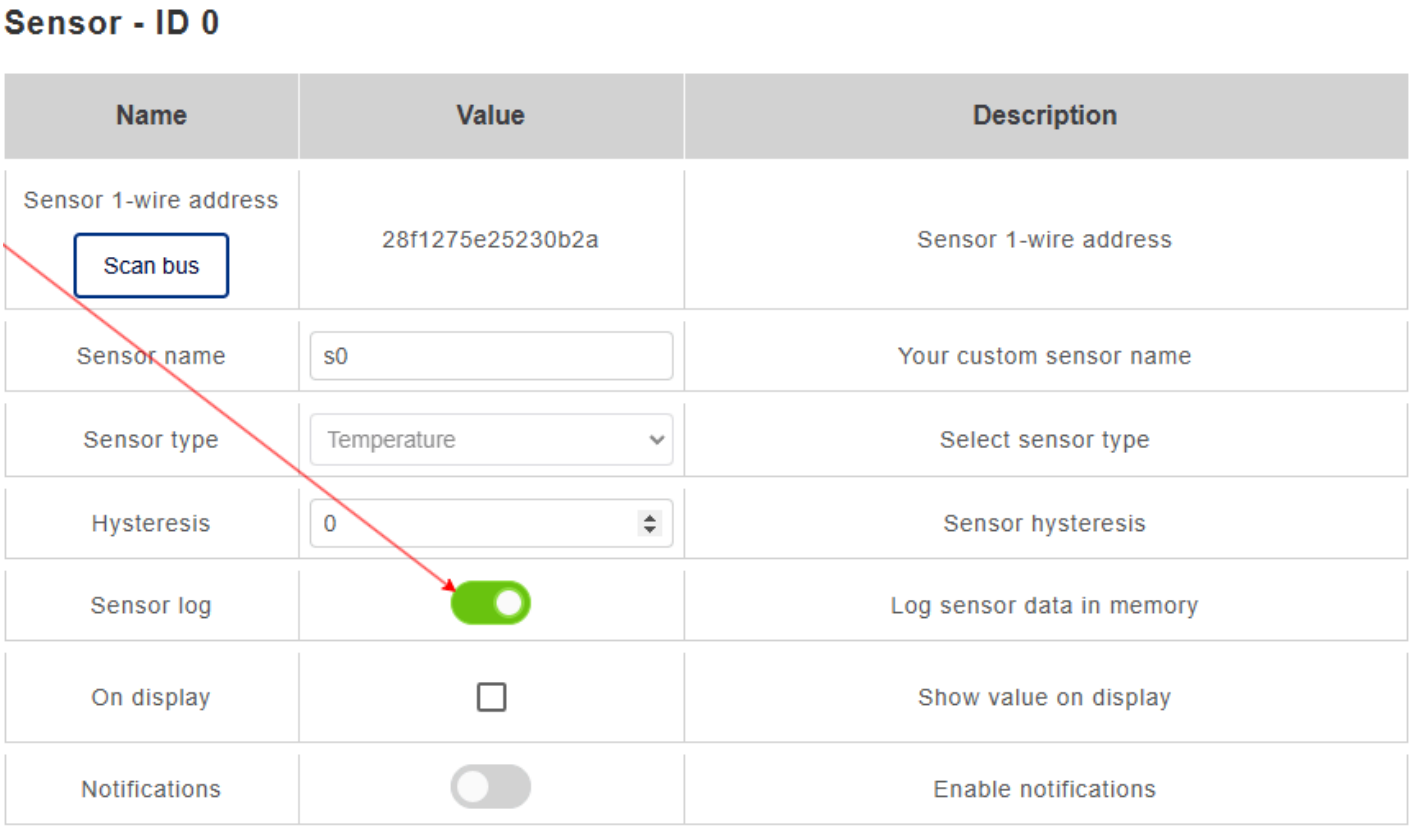
SENSOR READINGS LOGGING AND GRAPH PREVIEW

Conducting the configuration as per above instructions does not guarantee automatic sensor readings logging to the device memory. It only allows current value preview. To log the sensor data periodically, follow those directions:

Step 1: Enable automatic sensor readings logging:

In **Sensors / All**, click 

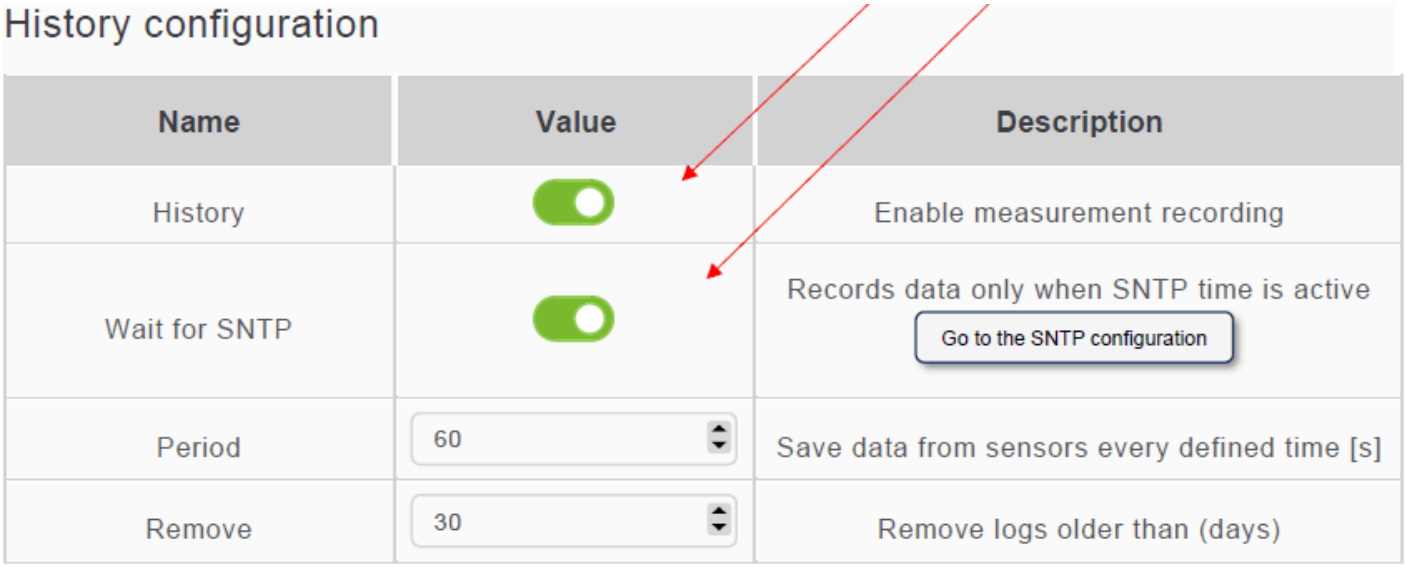
A sensor configuration window will be displayed:



Go to **Sensor log** and **Enable** it. All settings should be applied using the **Save** button.

Step 2: Enable automatic reading logging:

Sensors / History tab:

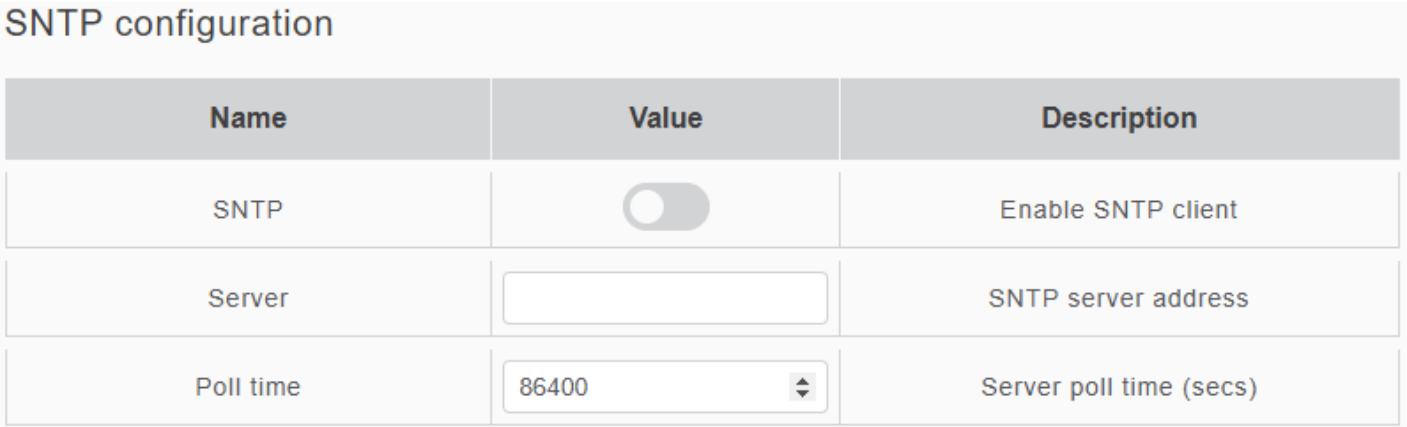


Go to **History** and select it using the slider.
After the device restarts or an Internet connection error occurs, it will automatically switch to logging using the built-in Real Time Clock (RTC). **Wait for SNTP** allows the device to wait for SNTP time before it begins logging data. Thanks to this, reading time precision is provided, even when no Internet connection is available.

> **Tip**
>
> **After making changes, apply them using the Save button.**

Step 3: Set the current time:

The device is equipped with an internal RTC with battery backup. If the device has constant Internet access, **SNTP** can be enabled.
Administration / Time - SNTP allows for SNTP configuration – guaranteeing that the current time will be kept even when no power is connected to the device.



> **Tip**
>
> **After making changes, apply them using the Save button.**

Once the unit has been configured according to the above instructions, the device will start saving sensor data to internal memory. The module also allows preview of graph of sensor readings over time.

DOWNLOAD OF STORED SENSOR READINGS

Saved sensor readings can be downloaded in the form of JSON or CSV files by recalling the internal memory resource. To do this, use the following command: `http://<IP_address>/data/log.json`.

Sensor readings can also be downloaded from the device's webpage. To do that, in **Sensors / Chart**, click the appropriate button: **Download JSON** or **Download CSV**.

Notifications configuration

This tab enables configuration of various notifications – activation, deactivation and notifications assignment involving E-mail, SMS, SNMP Trap, MQTT, related to sensors, inputs and outputs *(version dependent)*.

For the notifications to be effective:

Step 1: Enable notifications in the selected system elements tab: sensors, inputs or outputs, define the type of notifications,

Step 2: Depending on the notification type selected - SMS, e-mail, SNMP Trap, MQTT – configure the settings in **Services** – consult **Network services**

Step 3: Enable notifications in the **Configuration** tab.

Sensors

In this tab, notifications settings regarding operation of particular sensors can be configured. Notifications for the selected sensor can be enabled in two ways: in the **Sensors** tab during sensor configuration or by clicking an icon in **Notifications / Sensors**.

The configuration window that appears after notifications are activated, allows for full customization:

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

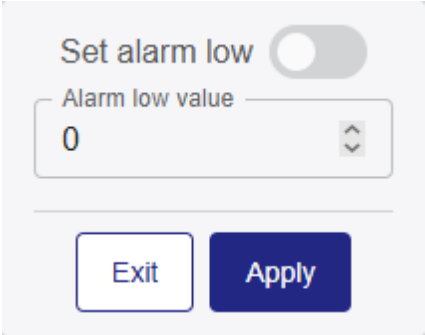
Tip

In order for the E-mail, SMS, SNMP Trap and MQTT notifications to operate correctly, configure them in the Services tab – consult Network services.

In the table, the user has the ability to select the type of notifications that are to be sent in response to defined events:

- **Info** – Periodic sensor state information,
- **OK** – Sensor normalization state after a previous error or alarm state,
- **Error** – Sensor error state,
- **Alarm low** – Low level alarm state,
- **Warning low** – Low level warning state,
- **Warning high** – High level warning state,
- **Alarm high** – High level alarm state.

If no alarm values have been previously defined, it can be done using the icon which opens a window to input the required value:



After inputting the required value, enable the function by clicking .
The settings will also be visible in the **Sensors** tab.

> **Tip**
>
> **To activate the notifications function, it is important to enable it in the Configuration tab, in addition to the settings configured here.**

Inputs

In this tab, notifications settings regarding operation of device inputs can be configured. After clicking , notifications for the selected input will be activated, leaving only their details to be configured. The configuration window that appears after the notifications have been activated, enables full customization.

DI 0 (DI0)				
State	E-mail	SMS	SNMP Trap	MQTT
On change action	☐	☐	☐	☐
Info	☐	☐		☐

It's possible to activate MQTT and SMS, SNMP Trap and notifications.

> **Tip**
>
> **In order for the E-mail, SMS, SNMP Trap and MQTT notifications to operate correctly, configure them in the Services tab – consult Network services.**

In the table, the user can select the type of notifications that are to be sent in response to defined events:

- **On change action** – Input state change (activated – deactivated),
- **Info** – Input state information.

> **Tip**
>
> **To activate the notifications function, it is important to enable it in the Configuration tab, in addition to the settings configured here.**

Outputs

In this tab, notifications settings regarding operation of devices connected to the device's outputs can be configured.

After clicking , notifications for the selected output will be activated, leaving only their details to be configured. The configuration window that appears after the notifications have been activated, enables full customization.

DO 0 (DO0)				
State	E-mail	SMS	SNMP Trap	MQTT
On change action	☐	☐	☐	☐
Info	☐	☐		☐

It's possible to activate E-mail, SMS, SNMP Trap and MQTT notifications.

> **Tip**
>
> **In order for the E-mail, SMS, SNMP Trap and MQTT notifications to operate correctly, configure them in the** Services **tab - consult** Network services**.**

In the table, the user has the ability to select the type of notifications that are to be sent in response to defined events:

- **On change action** – Output state change (activated – deactivated),
- **Info** – Output state information.

> **Tip**
>
> **To activate the notifications function, it is important to enable it in the** Configuration **tab, in addition to the settings configured here.**

Configuration

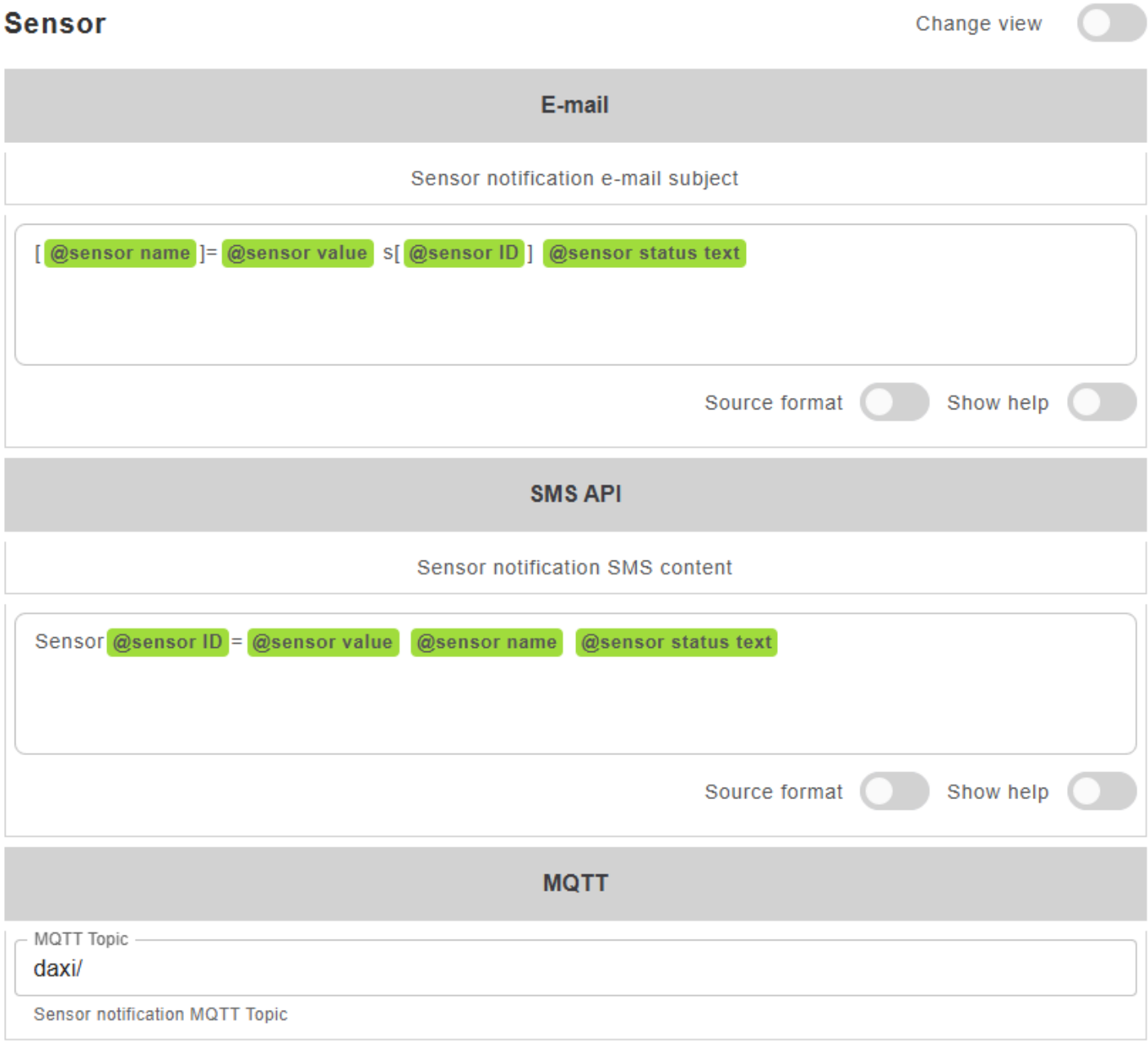
In this section, there is an option to activate the notification functions required to send notifications. Additionally, the user has the ability to adjust general parameters related to notifications.

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
SNMP Trap	0	SNMP user trap
IO time	100	Minimum time before sending another state change for inputs and outputs [ms]

- **Notification** – Enable/disable notifications,
- **E-mail info** – Frequency of e-mail messages containing the sensor/input/output state sending *(only modules with SMTP support)*,
- **SMS info** – Frequency of SMS messages containing the sensor/input/output state sending *(only modules with SMS API support)*,
- **MQTT info** – Frequency of MQTT messages containing the sensor/input/output state sending,

- **MQTT Retain** – Activated option causes the broker to retain last messages for topics the device sends data to,
- **SNMP Trap** – Selected SNMP Trap,
- **IO time** – Minimum time that must pass between subsequent input/output state changes to prevent multiple notifications to be sent, especially during testing or experiments with device's inputs/outputs.

The tables **Sensor**, **Input** and **Output** are located in this tab.
Each table contains predefined commands that allow sending of e-mail and SMS messages containing the current device states. Additionally, the user has the ability to edit those commands, which makes customization to own preferences possible, eg. by assigning a name to the device. Each table contains a topic, use of which is required if using MQTT to send notifications.



Input	
E-mail	Input notification e-mail subject

[@input name]= @input state i[@input ID]

Show help

SMS	Input notification SMS content}

Input @input ID = @input state @input name

Show help

MQTT	MQTT Topic iqio/c09bf4a00490 Input notification MQTT Topic

Output	
E-mail	Output notification e-mail subject

[@output name]= @output state o[@output ID]

Show help

SMS	Output notification SMS content}

Output @output ID = @output state @output name

Show help

MQTT	MQTT Topic iqio/c09bf4a00490 Output notification MQTT Topic

Binding

This tab enables configuration of relations between inputs and outputs.

Outputs

This tab allows routing of state from other components:



- **Name**,
- **Route from** – Source that will have influence over the output state – change of state of the channel in this field will cause the output state to change accordingly.

Available output state sources:

- `i[x]` – Input channel state,
- `i[x].act` – Last input action,
- `o[x]` – Output channel coil state,
- `o[x].on` – Output channel state,
- `v[x]` – Virtual variable state,
- `s[x].aHi` – Sensor high level alarm,
- `s[x].aLo` – Sensor low level alarm,
- `s[x].wHi` – Sensor high level warning,
- `s[x].wLo` – Sensor low level warning,
- `s[x].err` – Sensor error,
- `s[x].ok` – Sensor operates correctly,
- `ping[x]` – Ping status: `0` - error, `1` - success,
- `mb[x].y` – mbAgent value,
- External device:
  - `dev[x].err` – Connection lost,
  - `dev[x].o[y]` – External output,
  - `dev[x].i[y]` – External input,
  - `dev[x].s[y].err` – External sensor error.
- Negation and logic operations (|/&/^) e.g.:
  - `!s[0].err`
  - `!o[0]&v[1]`
- **Route to** – Variable, the output state will have influence on. Available variables:

- `v[x]` – Internal variable,
- `mb[x].y` – mbAgent value,
- External device:
  - `dev[x].o[y]` – External output.
- Negation and logic operations (|/&/^) e.g.:
  - `!s[0].err`
  - `!o[0]&v[1]`

> **Tip**
>
> **If the source is preceeded by "!i", the coil state will be opposite to the state of source channel. For example: !io[3] means that the output will have the state opposite to input 3.**

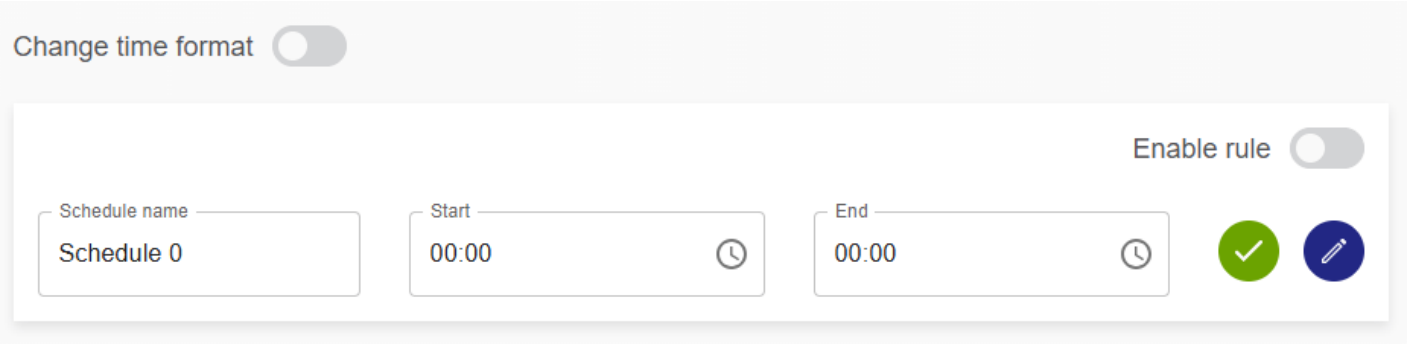
The  icon opens the step-by-step configuration window.

Schedule

This tab allows the user to control system operation using defined schedules or cron expressions. This advanced function allows for flexible programming of various actions, such as turning devices on and off, defining latitude and longitude for precise synchronization with sunrises and sunsets. Additionally, it's possible to assign specified actions to cron expressions, creating a personalized system operation schedule.

Weekly

It's possible to define up to four weekly schedules – activation of device outputs during specified hours of a weekday.



Change time format – Change time format from 24h to 12h.

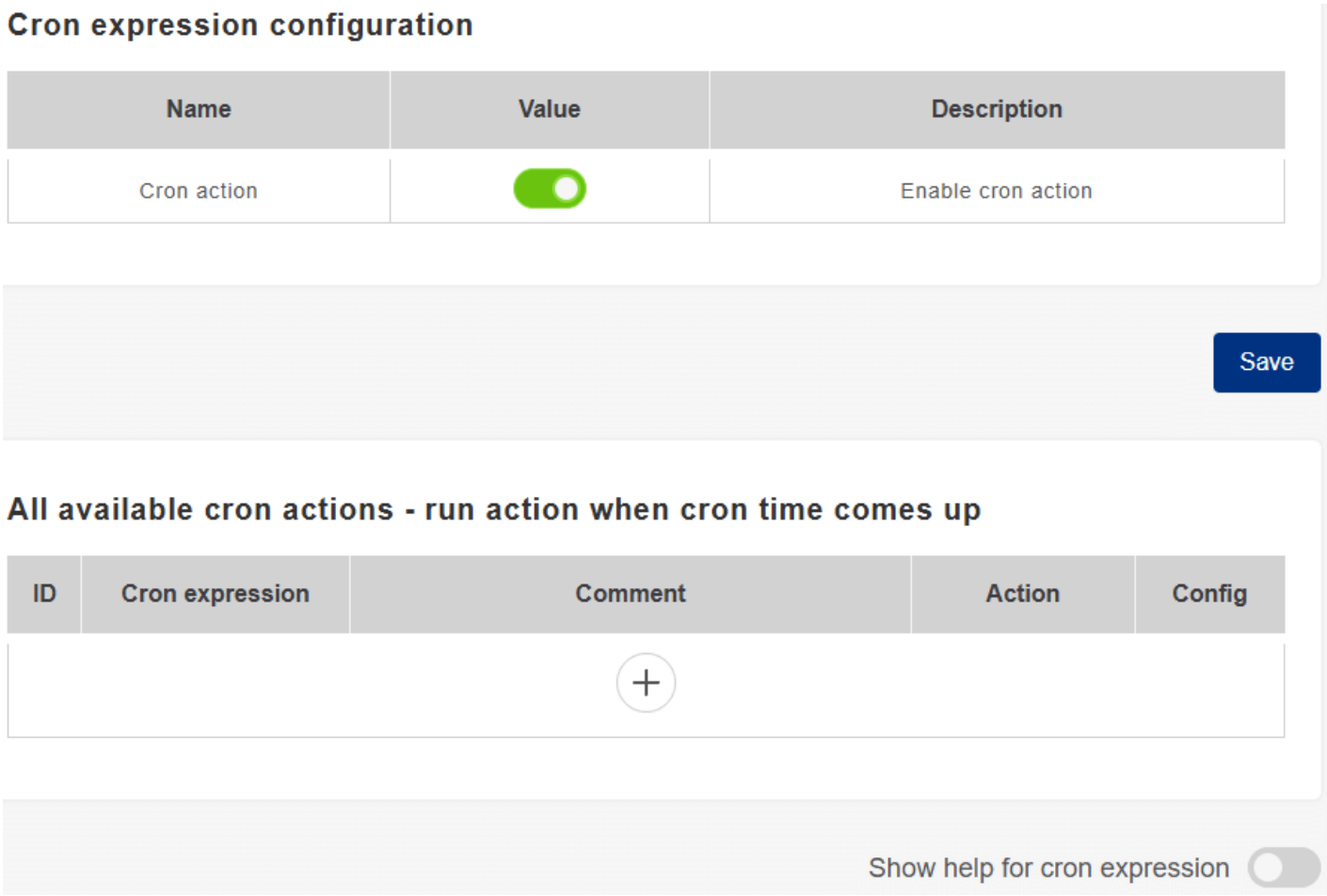
Programming of the schedule should begin with defining the start and end times. Next, using the  button, go to weekday selection, and define the outputs that the schedule will aplly to. Save all changes using .

Enable rule – Enables/disables the selected schedule.

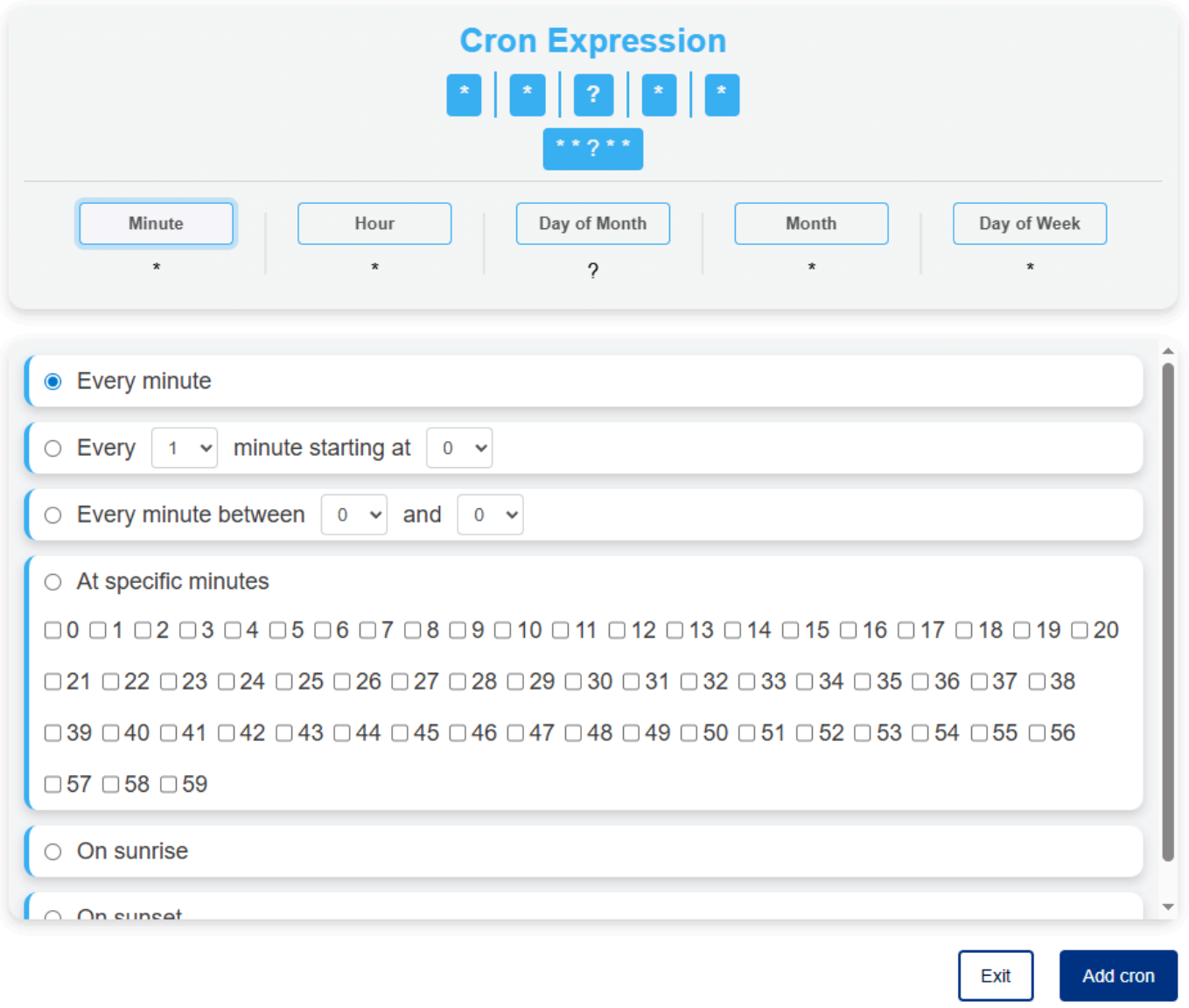
Cron action

The tab allows the user to activate previously defined actions, according to a schedule utilizing a cron expression.

Firstly, enable cron operation:



Clicking **+** will start a step-by-step cron configuration.



After applying the cron time settings, go to the next configuration step:

All available cron actions - run action when cron time comes up



- **Cron expression** – Defined cron expression.  returns to cron configuration,
- **Comment** – User comments,
- **Action** – Assign actions defined previously – consult **Defining actions**,
- **Config** – Allows the user to accept the configuration or leave the editor.

Cron standard

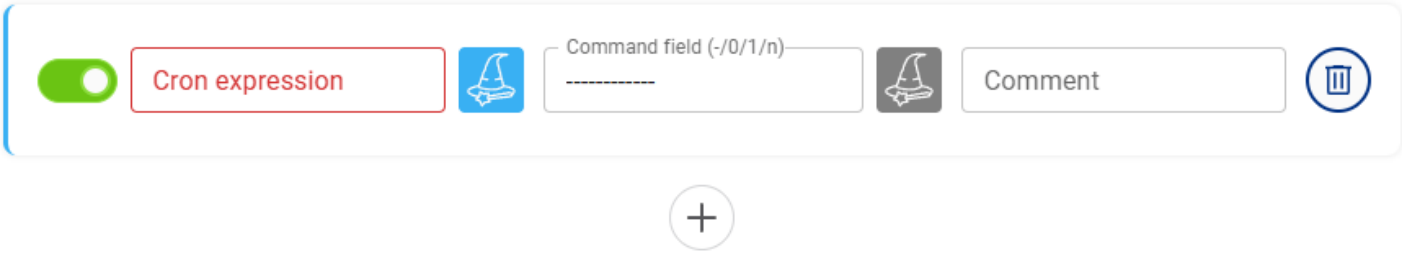
This tab allows for programming of output operation according to the cron expressions:

Cron expression

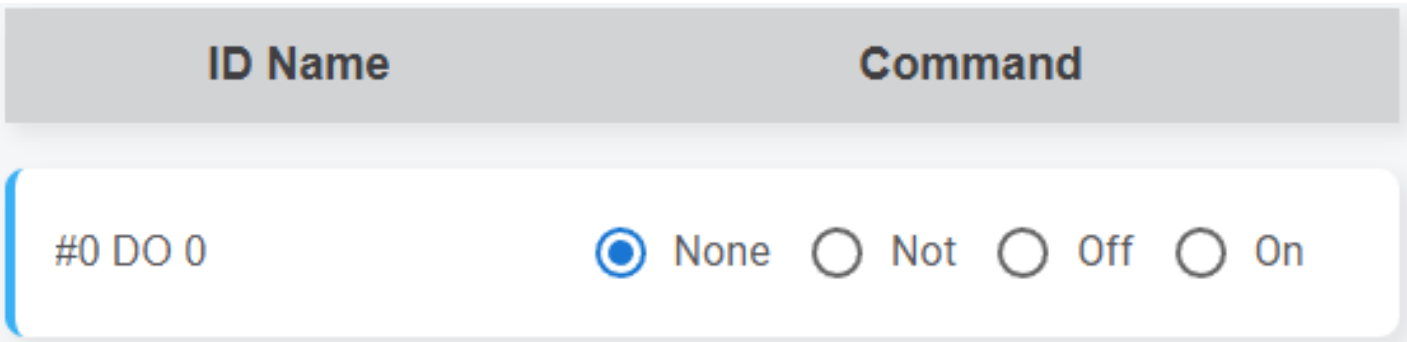
Name	Value	Description
Cron standard		Enable cron standard
Missed Cron Replay		Execute cron commands that were missed due to power loss Max recovery time: 7 days of power loss

- **Cron standard** – Enable/disable Cron,
- **Missed Cron Replay** – Execution of cron orders that have been missed because of a power failure. Maximum restore time: 7 days since power loss.

Step-by-step cron configuration:



Clicking will go to the cron expression configuration. After a cron expression is added, command configuration is possible - program how particular outputs should operate during the set cron expression. The following options are available to each output:



- **None** – No state change,
- **Not** – State inversion,
- **Off**,
- **On**.

Apply the configuration by clicking **Add command**.

Click **+** to add additional commands.

Advanced cron configuration:

Advanced configuration allows the user to access advanced cron configuration.

The drawing describes the meaning of columns:

```
* * * * * Control command
| | | | |
| | | | ---------- Day of the week (0-7) (0 and 7 sunday)
| | | -------------- Month (1-12)
| | ----------------- Day of the month (1-31)
| --------------------- Hour (0-23)
------------------------ Minute (0-59)
```

The control command consists of 8 fields representing the state of outputs.

Each field can assume the values:
- 1 – Output activation,
- 0 – Output deactivation,

- n – Negation (state inversion),
- - – Leave the output with no changes.

Example

Wyjście	1	2	3	4	5	6	7	8
Stan	1	1	0	1	n	1	-	0

- Activate outputs 1, 2, 4, 6,
- Deactivate outputs 3, 8,
- Invert output 5,
- Output 7 - no changes.

The controller recognizes the following entries:

- Sunday can be represented by 0 or 7
- The day of command execution can be inputted in two ways: day of the month or day of the week. If two fields are filled, the command will be executed both on the day of the month and day of the week!
- Numerical values can be saved in various formats:
  - 1-3 – Values 1, 2, 3,
  - 0-10/2 – Values 0, 2, 4, 6, 8 i 10 (every 2nd value in the range from 0 to 10),
  - 1,2,5 – Values 1, 2, 5,
  - */2 – Every 2nd allowed value (np. in the first collumn it will be 0, 2, 4, 6...56, 58),
  - 1-3,5,6 – 1, 2, 3 and 5, 6,
- SR – time of the sunrise,
- SS – time of the sunset.

Tip

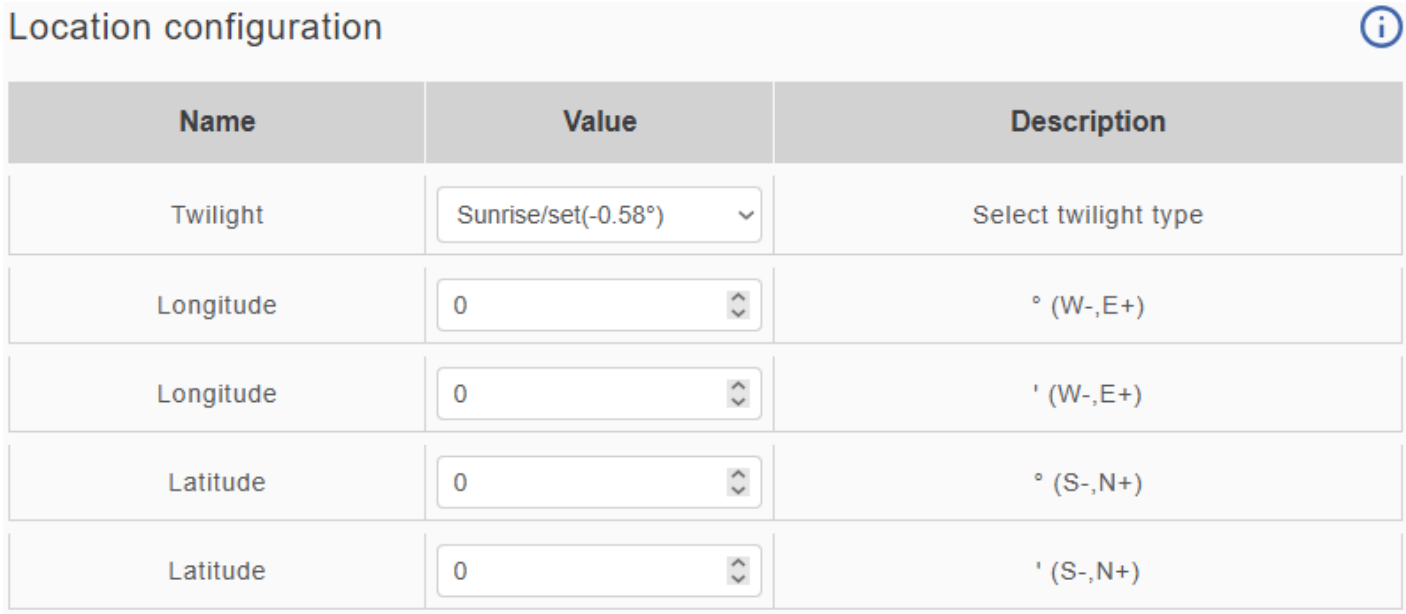
Because of Daylight Savings Time, avoid tasks that should happen between 2:00 and 3:00 on a Sunday. During automatic change from winter to summer time, the action will not complete, while during change from summer to winter time, it will be completed twice.

Example

- Activate relay No. 3 at 12:45: `45 12 * * * --1------`
- Activate relay No. 5 at 17:30 on the 16th of October: `30 17 16 10 * ----1---`
- Activate relay No. 2 at 8:00 form Monday til Friday: `00 8 * * 1-5 -1--------`
- Activate relay No. 1 and 5 from Monday til Friday at sunrise: `SR SR * * 1-5 1---0---`
- Activate relay No. 1 at dusk and deactivate at dawn: `SS SS * * * 1---------  SR SR * * * 0---------`
- Activate relay No. 3 10 minutes after dawn: `SR+10 SR * * * --1-----`

Configuration

This tab allows output control configuration using cron expressions. The device can calculate the sunrise and sunset times automatically depending on the specified location – to do that, geographical coordinates should be entered in the degree and minute format.



- **Twilight** – Twilight type selection – see **Twilight**,
- **Longitude** – Degrees (positive value for the eastern longitude, negative for western longitude),
- **Longitude** – Minutes (positive value for the eastern longitude, negative for western longitude),
- **Latitude** – Degrees (positive value for the northern latitude, negative for southern latitude),
- **Latitude** – Minutes (positive value for the northern latitude, negative for southern latitude).

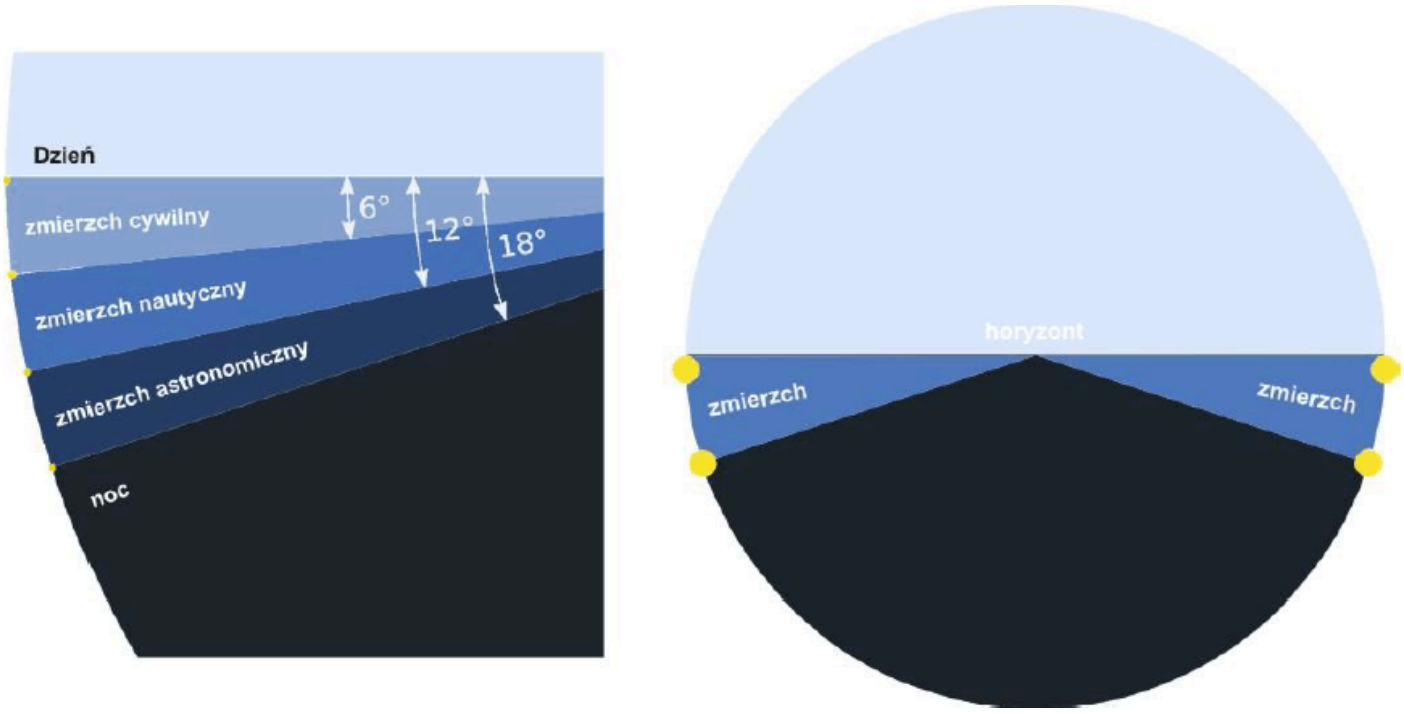
Tip

The blue "i" icon in the upper-right corner of the tab enables preview of the calculated sunrise and sunset times.

Twilight

- **Civil (-6º)** – Civil twilight - the phase of sunset when the centre of the solar disc is no more than 6 angular degrees below the horizon. During this period, the brightest stars and planets appear in the sky, retaining enough natural light for normal outdoor activities.
- **Nautical (-12º)** – Nautical twilight (also known as dusk) - the time after sunset when the centre of the solar disc is less than 6 angular degrees below the horizon, but still above 12°. This phase allows the horizon line to be clearly observed, which is important in astronavigation, enabling simultaneous navigation based on terrestrial and celestial objects.
- **Astromical (-18º)** – Astronomical twilight - the period when the centre of the solar disc is between 12 and 18 angular degrees below the horizon. It ends with the beginning of astronomical night. Astronomical dawn - the time before sunrise when the sun's rays light up the sky, making the faintest stars no longer visible. Astronomical dawn lasts from the time the centre of the Sun's disc is more than 18° below the horizon line until it is more than 12° below the horizon line. The astronomical dawn ends the astronomical night and then the nautical dawn begins.
- **Nautical dawn** – The time before sunrise when the horizon and landscape become visible, allowing navigation based on illuminated objects on land or sea. During this time, the brightest stars are still visible in the sky. Nautical dawn lasts from the moment when the centre of the Sun's disc is more than 12° below the horizon line, but still less than 6° below the horizon line.

- **Civil dawn** – The time before sunrise when the centre of the sun's disc is already more than 6° below the horizon line.

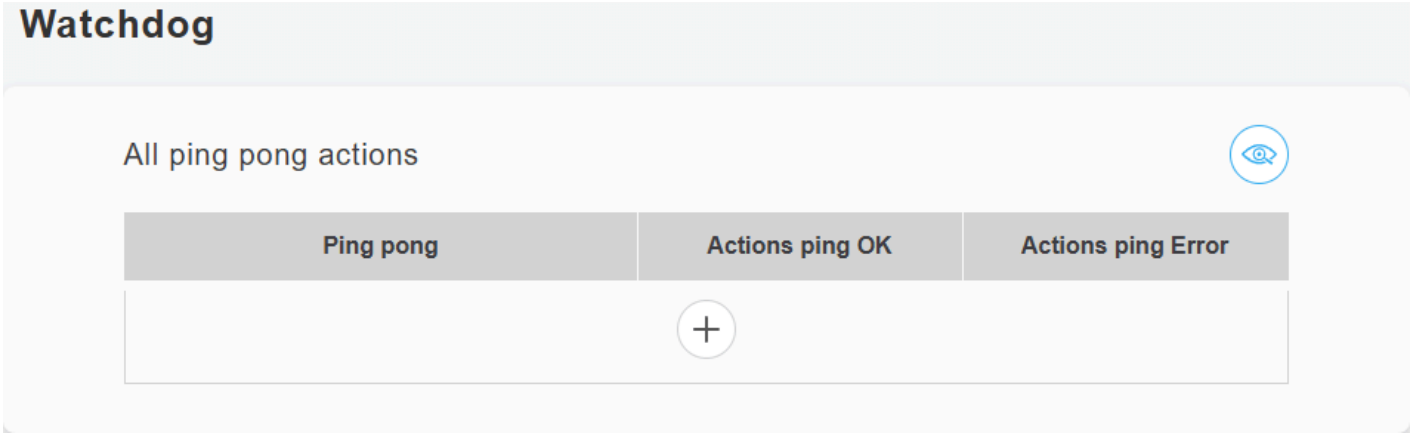


Virtus calculates the hour of the sunrise and sunset - to do that, input of geographical coordinates is needed (longitude and latitude in the degrees/minutes format).

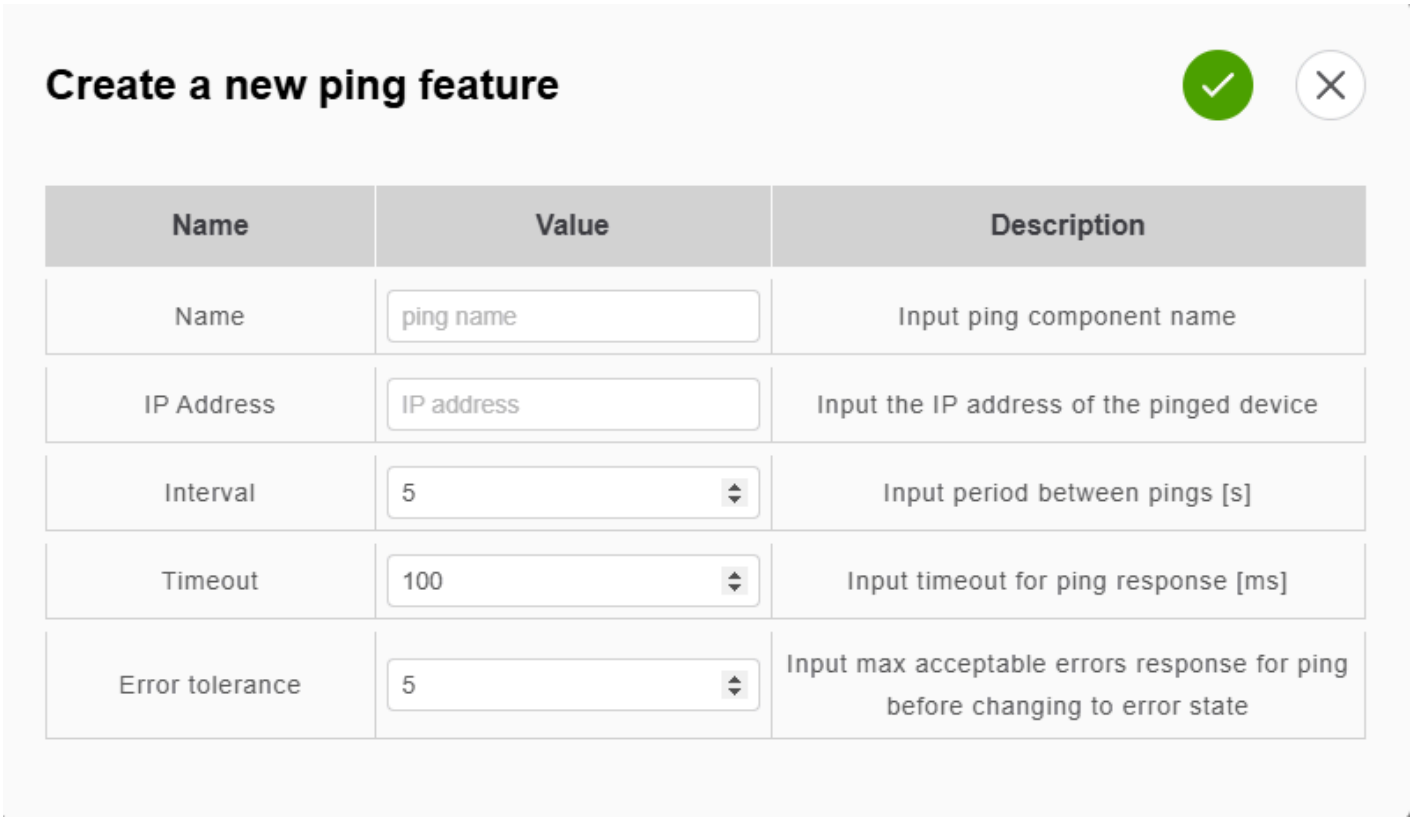
- **Twilight** – Select the astronomical clock mode:
  - **Sunrise/set (-0,58°)**,
  - **Civil (-6°)**,
  - **Nautical (-12°)**,
  - **Astronomical (-18°)**.

Remote hosts ping (Watchdog)

The device is equipped with the function of "pinging" – it can interrogate remote hosts (other network devices, servers etc.) and react to their availability.



To add a new device to check the availability of, click **+** in the **All ping pong actions** table – a **Create a new ping feature** dialogue window will appear:



- **Name** – Ping name,
- **IP address** – IP address of the pinged device,
- **Interval** – Ping interval (in seconds),
- **Timeout** – Ping response time limit,
- **Error tolerance** – Maximum permissible amount of ping response errors before error state occurs.

Tip

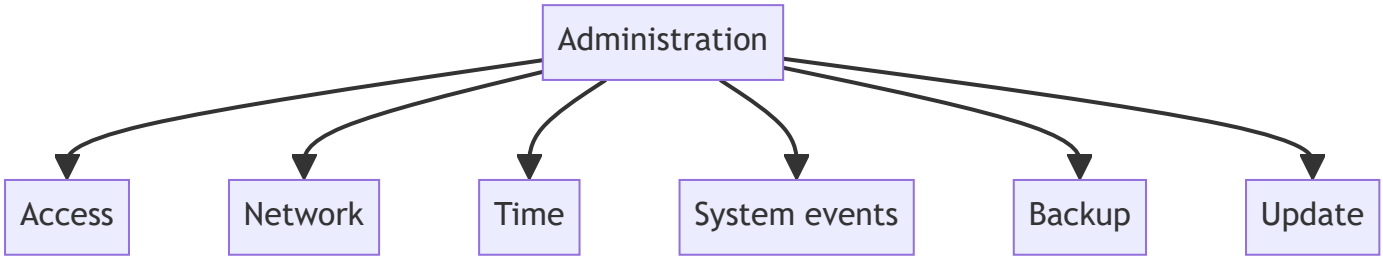
All changes should be saved with

A new ping will show up in the table, **Actions ping OK** and **Actions ping Error** columns will be populated with **+** buttons, that allow assignment of selected actions that are to be executed in the event of correct and erroneous ping response. The process of assigning actions is described in the **Defining actions** chapter.

Clicking will activate an additional indicator next to the request name - assuming **green** colour for a correct ping response or **red** if a response error occurs.

System management

The **Administration** tab allows control over device aspects that influence the operation, security and system configuration.



Access

The user can manage webserver access. This involves authentication, device name and access from the Discoverer programme.

Access configuration

Name	Value	Description
Password		Enable password
Current password		
New password		
Repeat new password		
Module name	[your_module_name]	Your custom module name
Enable remote config		Allow change configuration by Discoverer app

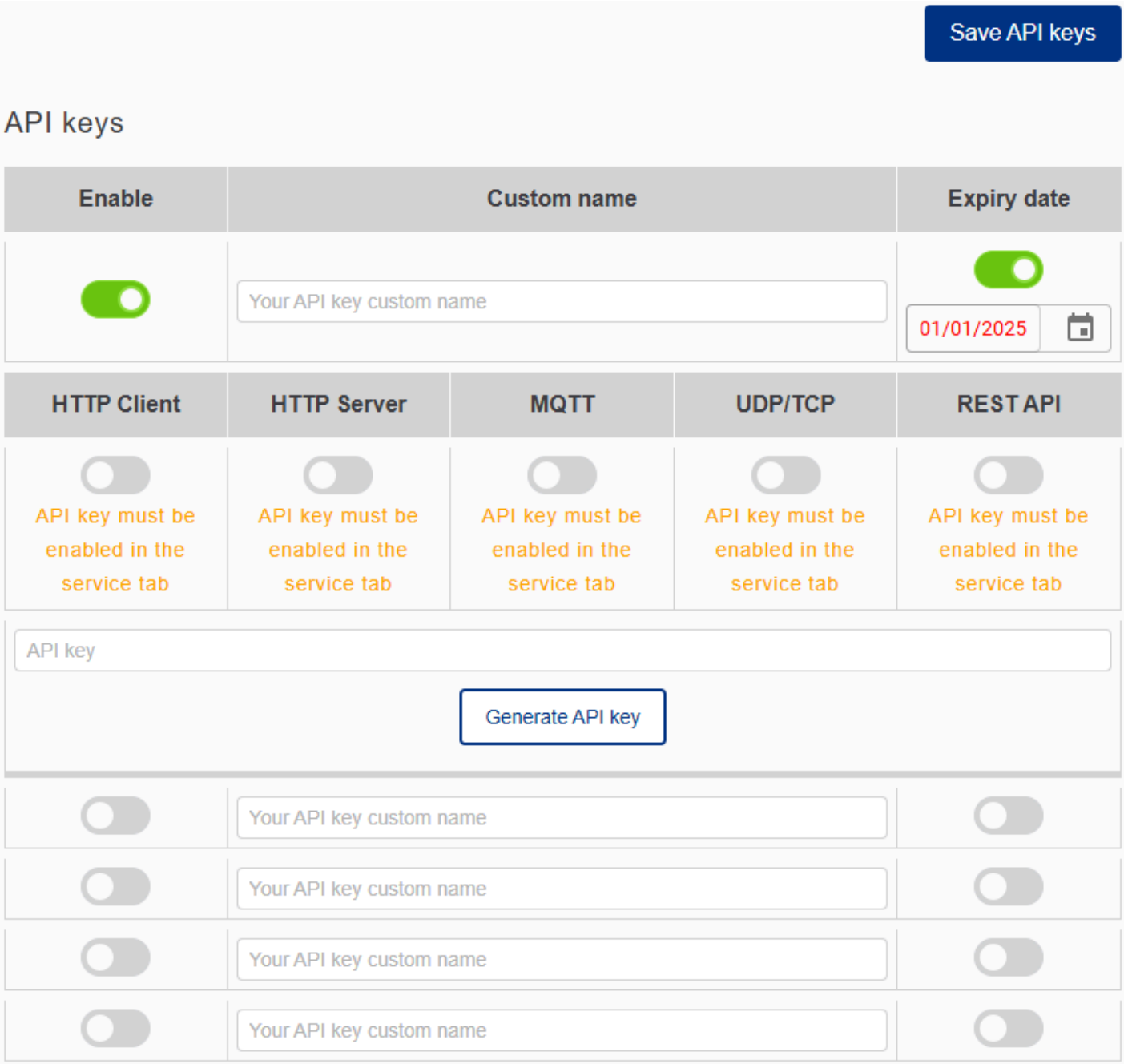
- **Password** – Enable/disable configuration password,
- **Current password**,
- **New password**,
- **Repeat new password**,
- **Module name** – Assigning an individual name to the module makes module identification in the system easier,
- **Enable remote config** – Enable/disable configuration via the Discoverer programme.

Information

Default device settings:
- username: admin
- password: admin

API KEYS

The device allows the user to configure a set of five unique API keys, used for authentication and identification of users or processes that initiate communications with the device.



- **Enable** – Enable/disable the selected API key,
- **Custom name** – Key name assigned by the user,
- **Expiry date** – API key expiry date,

- **HTTP Client, HTTP Server, MQTT, UDP/TCP, REST API** – Selection of the communication protocol that will use the specified API key,
- **API key** – Key value entry field,
- **Generate API key** – This button generates a random API key that will automatically be inputted into the **API key** field.

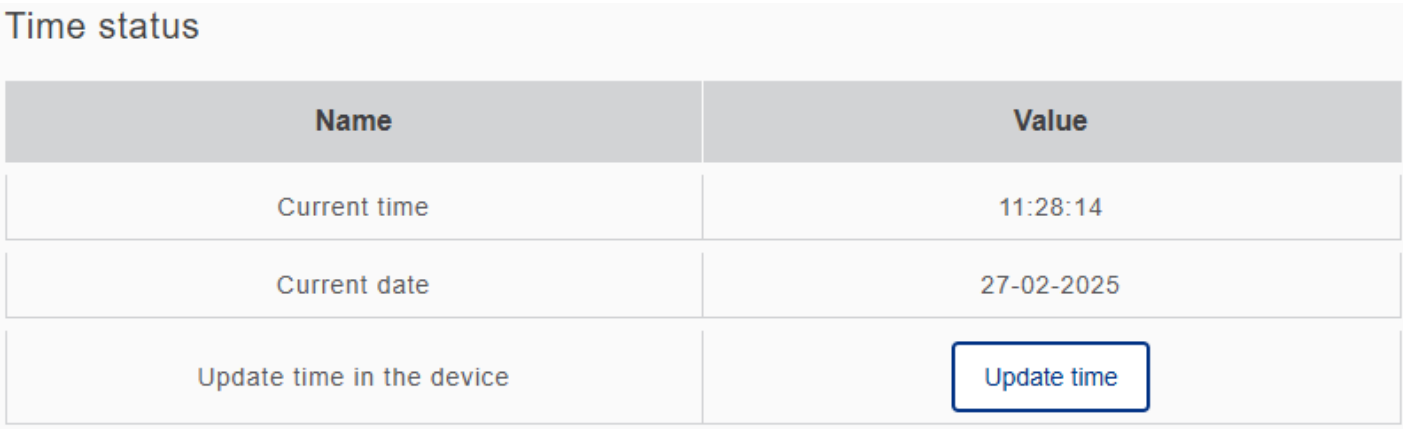
> **Tip**
>
> **Changes made in the API keys tab should be saved with Save API keys.**

Network

In this tab, the device's network settings can be changed. Configuration is described in the **Network configuration** chapter.

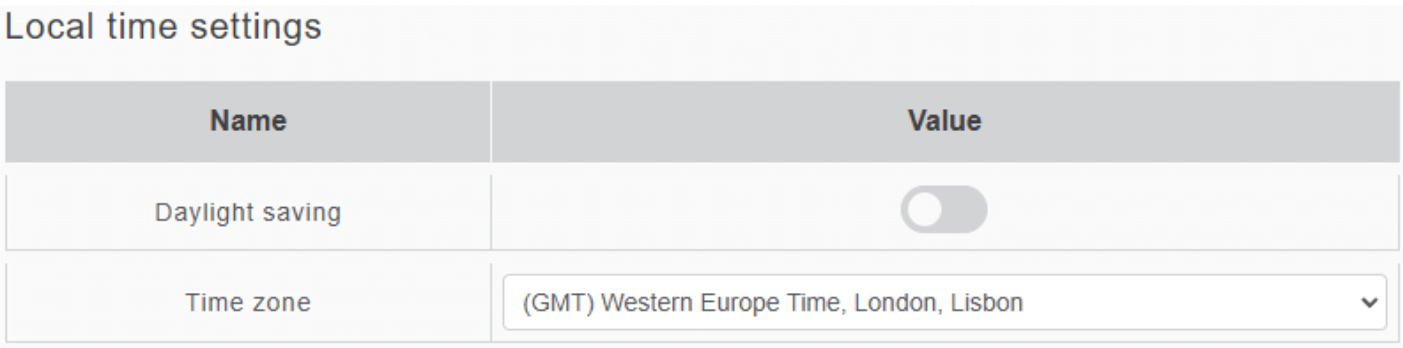
Time

This section allows the user to control time, time zone settings, and download of curerrent time from the computer.



- **Current time** – Preview of current time in the device,
- **Current date** – Preview of current date in the device,
- **Update time in the device** – Allows to set the device time to the same time as the computer.

The device is equipped with SNTP support, that is responsible for synchronizing device time with a SNTP server. It's crucial for correct data logging and performing timed tasks.

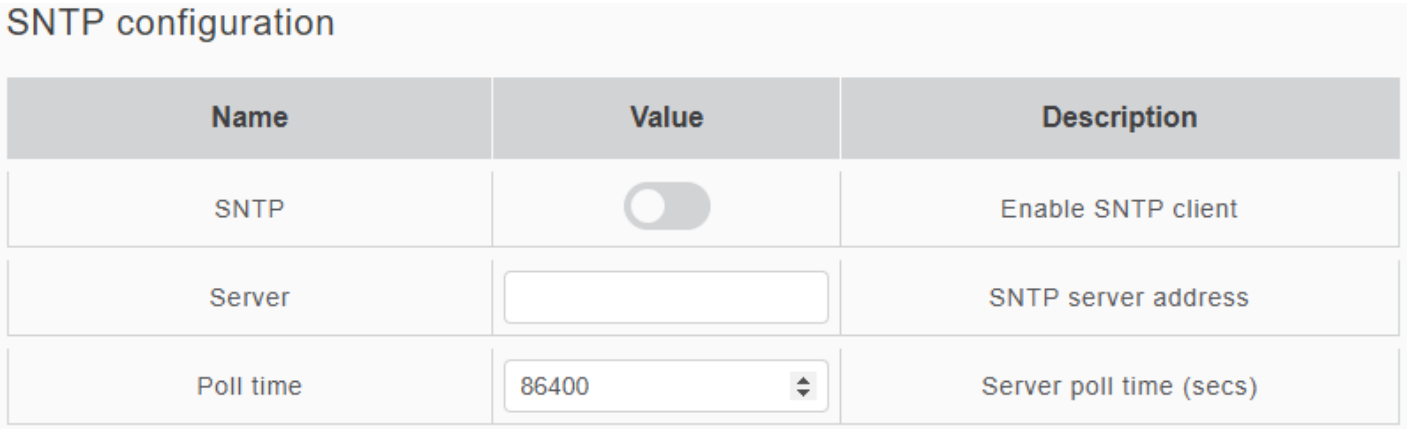


- **SNTP** – Enable/disable SNTP,

- **Server** – SNTP server address,
- **Poll time** – Server poll time (in seconds).

> **Tip**
>
> **Example SNTP servers:**
> **- tempus1.gum.gov.pl – IP address: 194.146.251.100**
> **- tempus2.gum.gov.pl – IP address: 194.146.251.101**

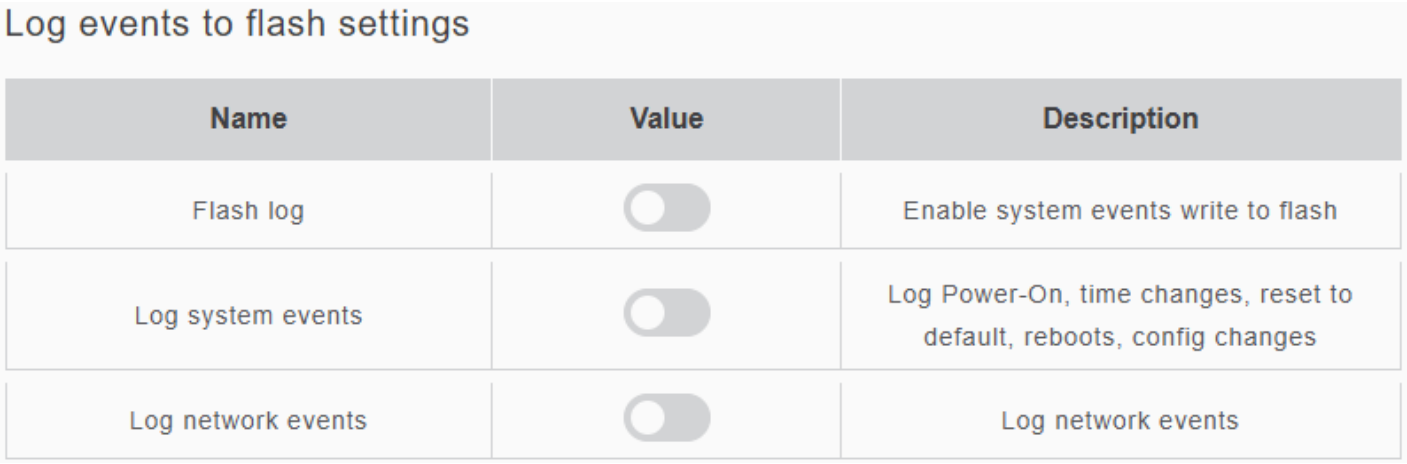
Additionally, the device is equipped with an internal RTC with battery backup. If the device does not have constant Internet access, it can use this clock to keep precise time.



- **Daylight saving** – Enable/disable daylight savings time,
- **Time zone** – Time zone selection.

System events

This tab enables logging of system events to the flash memory, giving users the option to preview and analyze different system events. This process helps with system operation monitoring and diagnosing possible problems.

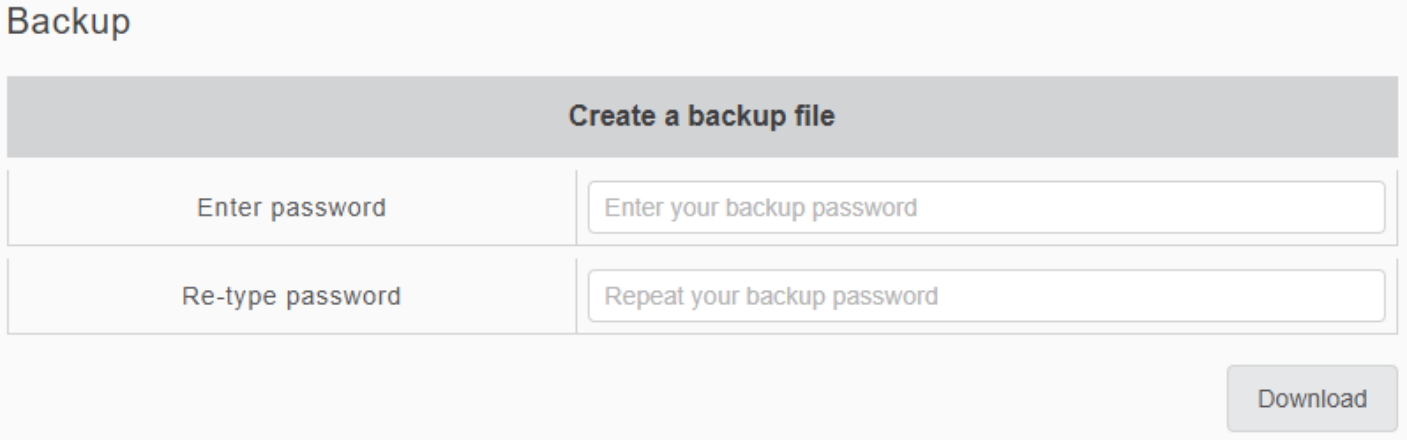


- **Flash log** – Enable/disable logging of events to flash memory,
- **Log system events** – Enable/disable logging of activations, time changes, factory settings restore, restarts, changes to configuration,
- **Log network events** – Enable/disable logging network events.

Backup

Users can create configuration backups and restore the system from previous backups in this tab.

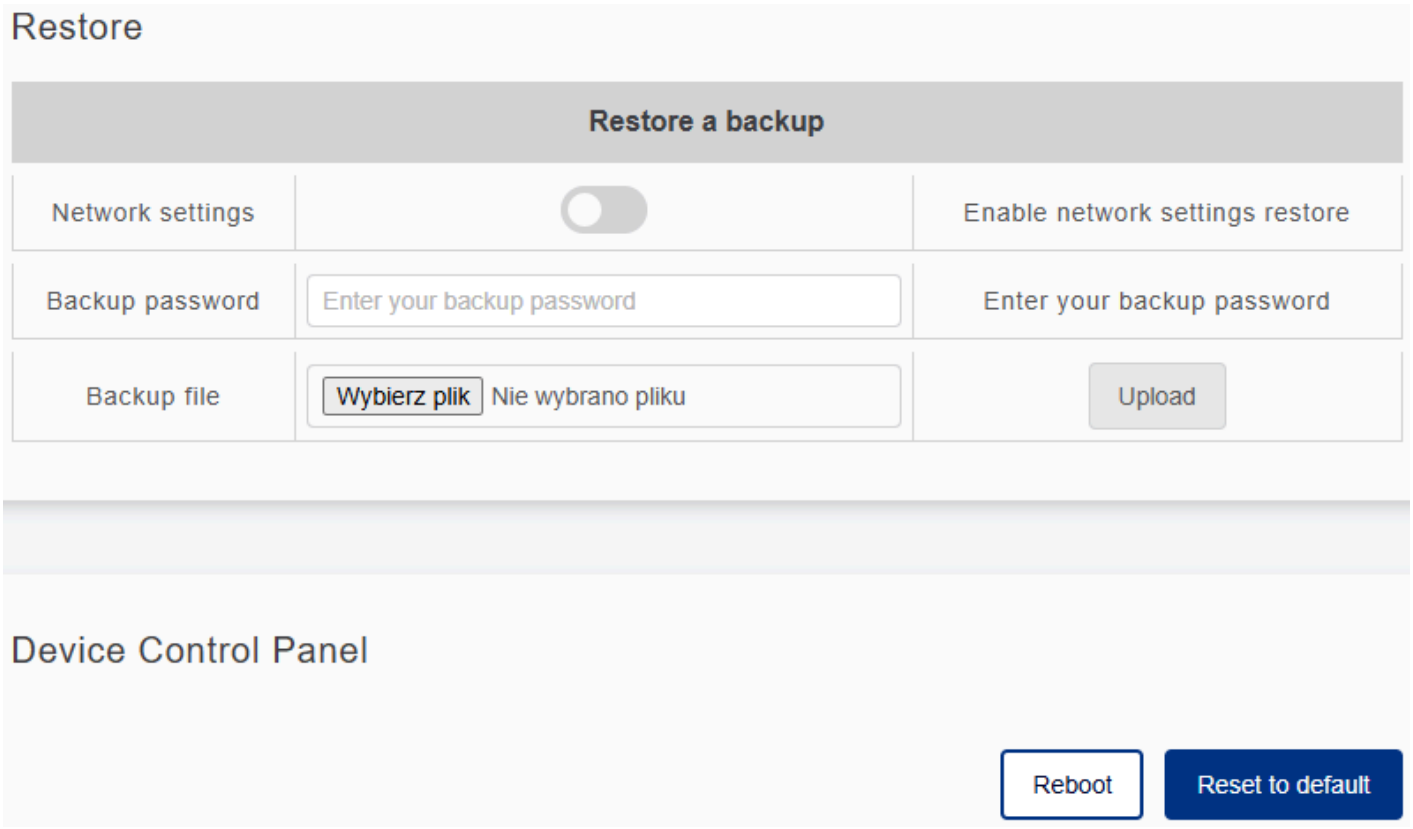
Create a backup file



- **Enter password** – Password protecting the backup,
- **Re-type password**.

Download enables download of configuration data to the PC.

Restore



- **Backup password** – Backup access password,
- **Backup file** – Browse the backup file.

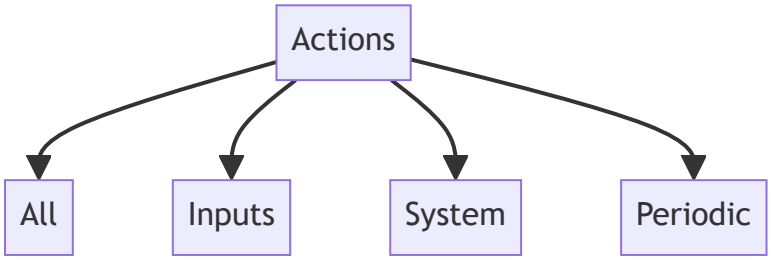
Upload – Uploads the selected backup to the device. **Reboot** – Allows the device to reboot. **Reset to default** – Allows the user to restore default settings.

Defining actions

The device undertakes user-defined actions in response to specific signals or sensor readings. Those may include:

- **Output control:** Activation or deactivation of a selected output based on sensor readings. (eg. turning a fan on after temperature exceeds a certain threshold),
- **Sending notifications in the form of SMS, e-mail, MQTT frame, HTTP, TCP, UDP, SNMP trap, and other:** Automatic sending of alert/notification to the user or another system in response to defined conditions,
- **Other actions defined by the user:** Actions specific to a particular system or needs such as saving data to a database, alarm activation, change to other device settings etc.

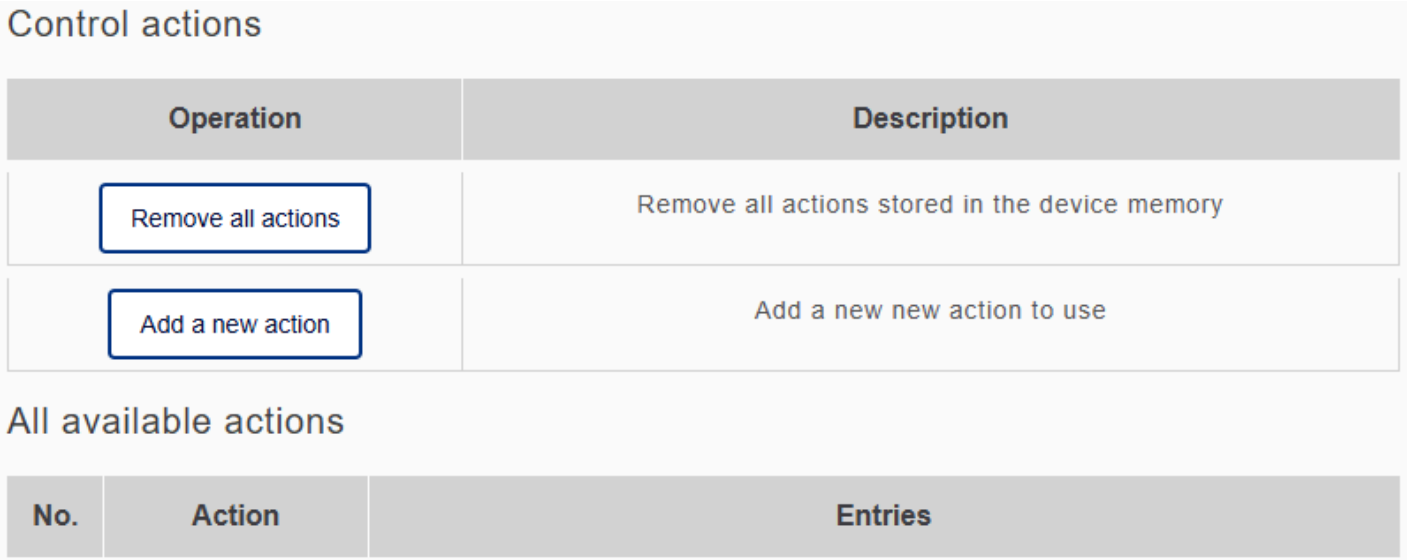
The actions are specific reactions of the module to received signals and input data, in accordance to the instructions set by the user. Many functions can be conducted by multiple methods depending on preferences and needs.



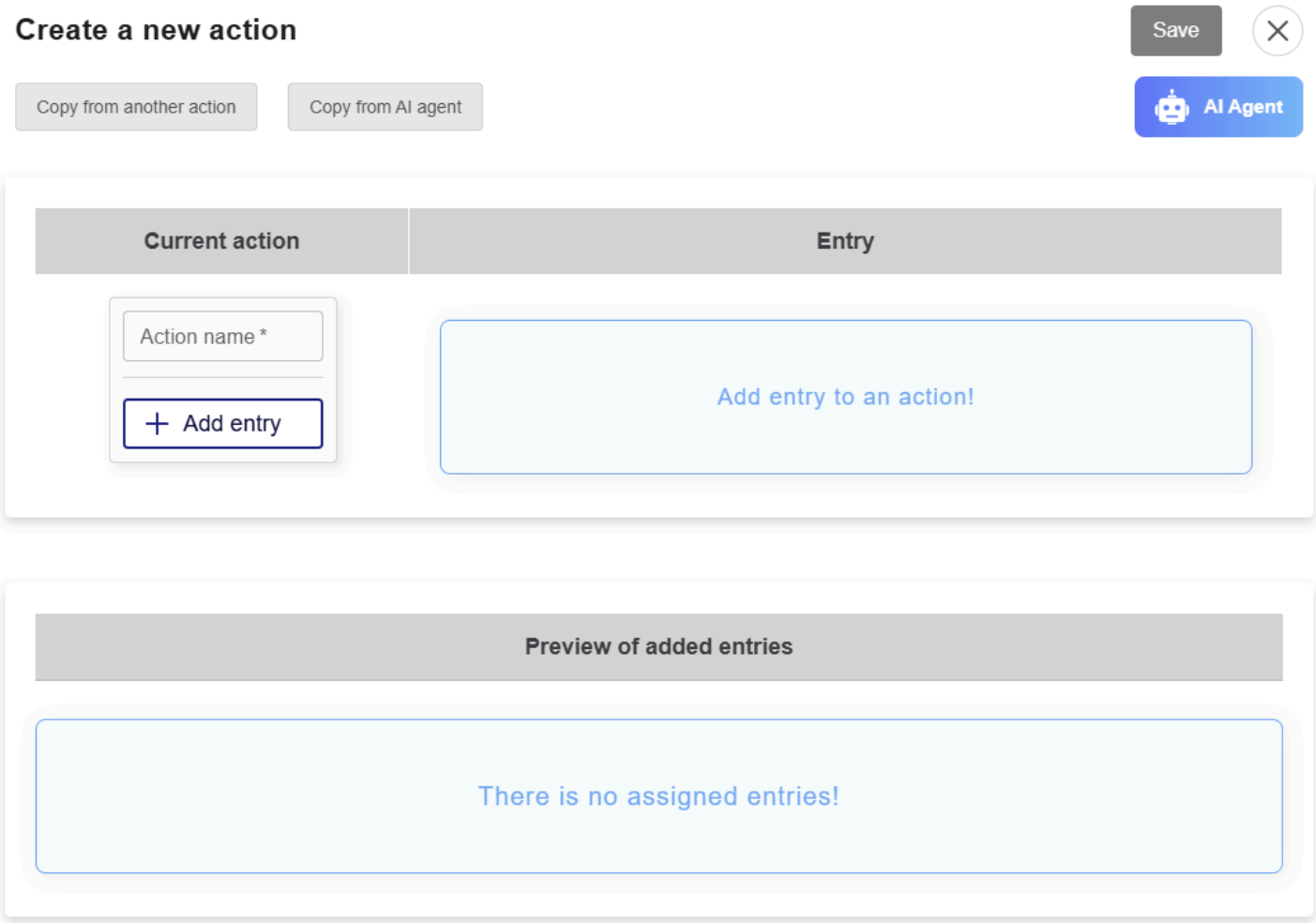
All

This tab allows preview and management of defined actions supported by the device.

Control Actions window



- **Remove all actions** – Removes all actions defined in the device,
- **Add a new action** – A window displayed after clicking this button allows the user to define each parameter of the added action:



- **Copy from another action**,
- **Copy from AI agent** – Opens a new window, to which the Inveo AI - generated string can be entered,
- **Action name**.

Clicking **Add entry** allows for communication protocol selection and further configuration.

After the programmed action's details are configured, click **Add**. It's possible to configure multiple actions for one event. After defining all required settings, save the changes using .

All available actions window

All defined and system actions are visible in this window. Each of them can be:

- Amended –
- Tested – Try
- Deleted –

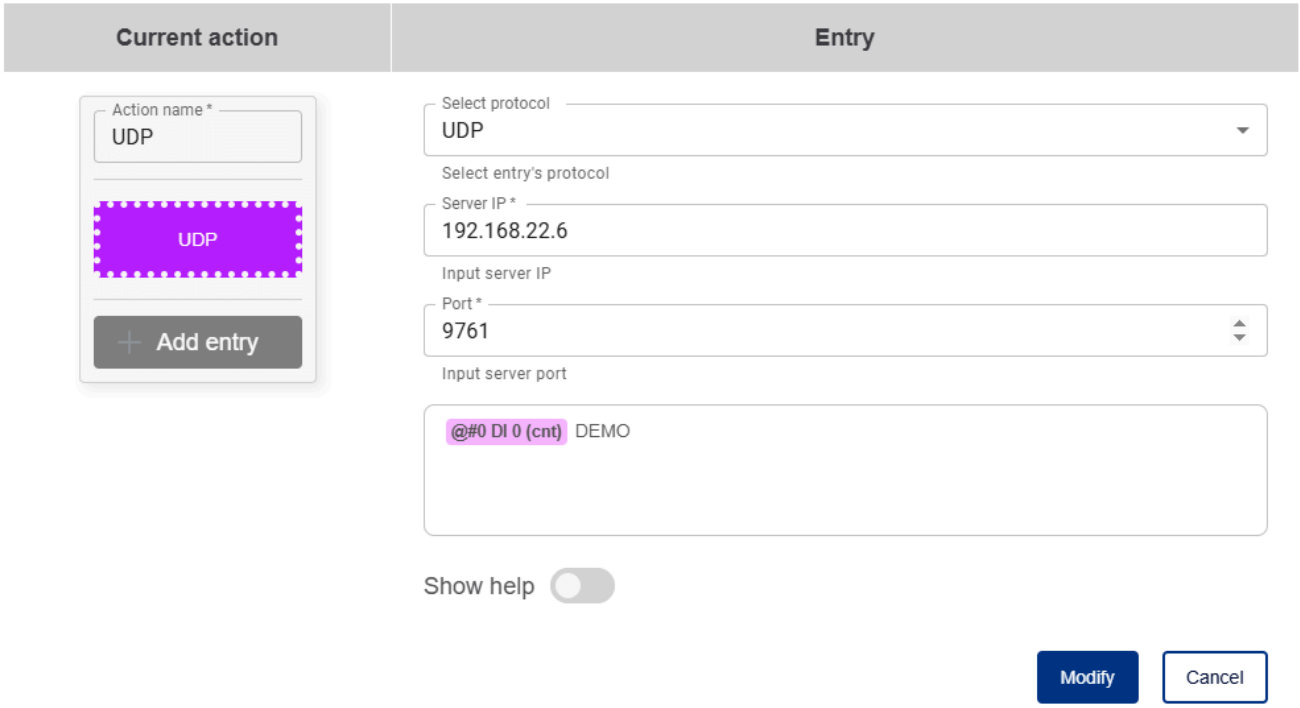
Protocol configuration

UDP

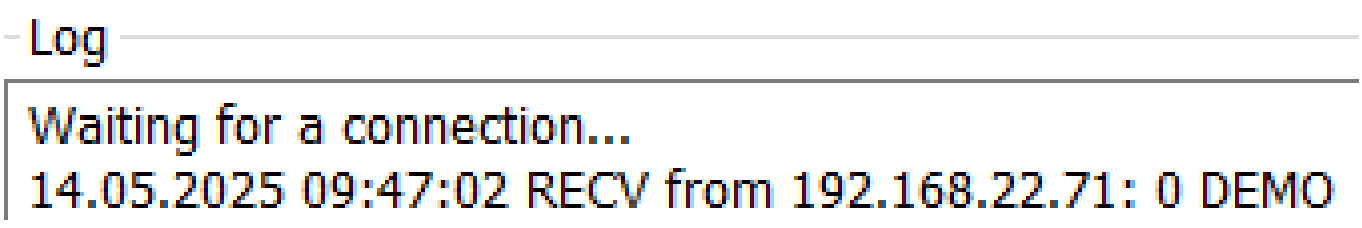
- **Server IP** – Target IP address,
- **Port** – Port, on which the target device is listening,
- **Format** – Data format: **TEXT** or **HEX**,
- **Input data** – Command sent to the target device.

Example

- **Server IP: 192.168.22.6**
- **Port: 9761**
- **Format: TEXT**
- **Input data:** `%i[0].cnt% DEMO`



Sent data:

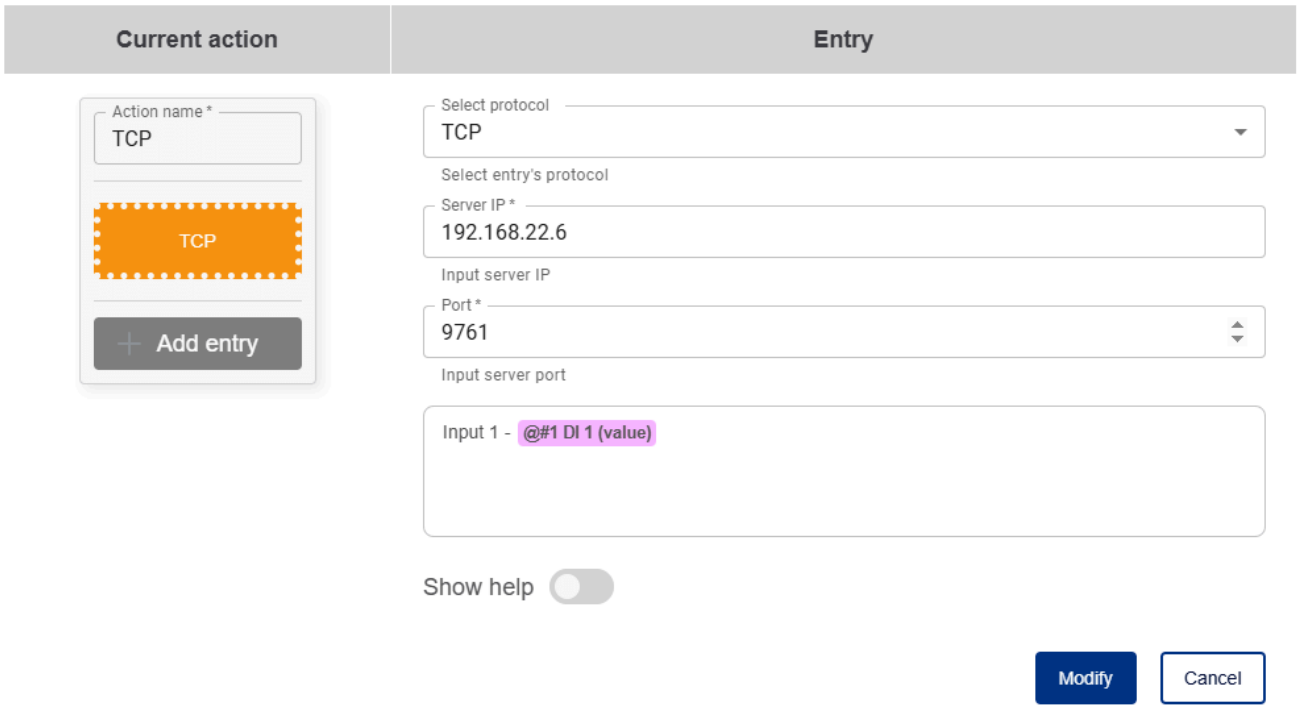


TCP

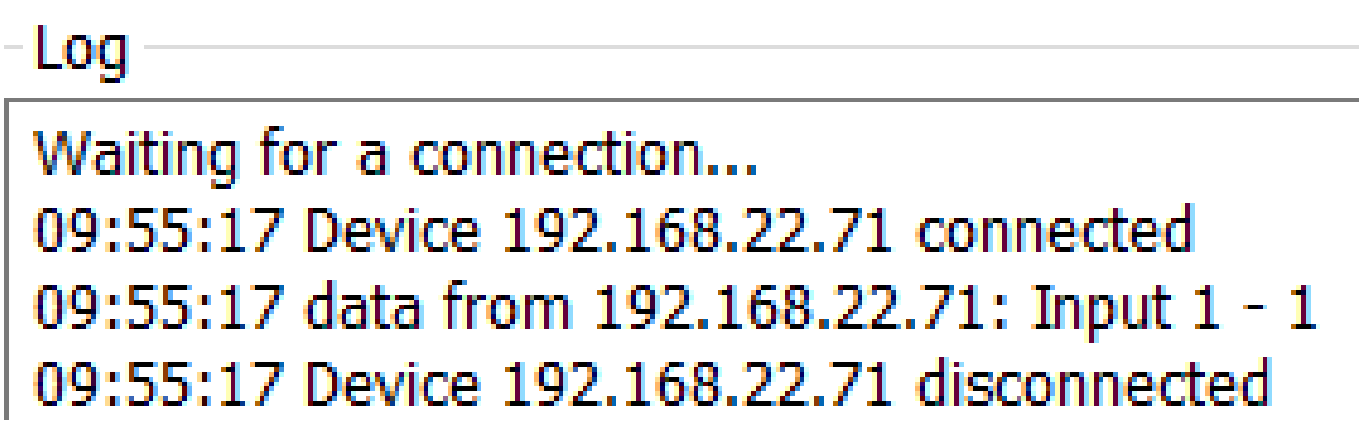
- **Server IP** – Target IP address,
- **Port** – Port, on which the target device is listening,
- **Format** – Data format: **TEXT** or **HEX**,
- **Input data** – Command sent to the target device.

Example

- **Server IP: 192.168.22.6**
- **Port: 9761**
- **Format: TEXT**
- **Input data:** `Input 1 - %i[1]%`



Sent data:



HTTP

Detailed protocol configuration is located in the **Services** tab.

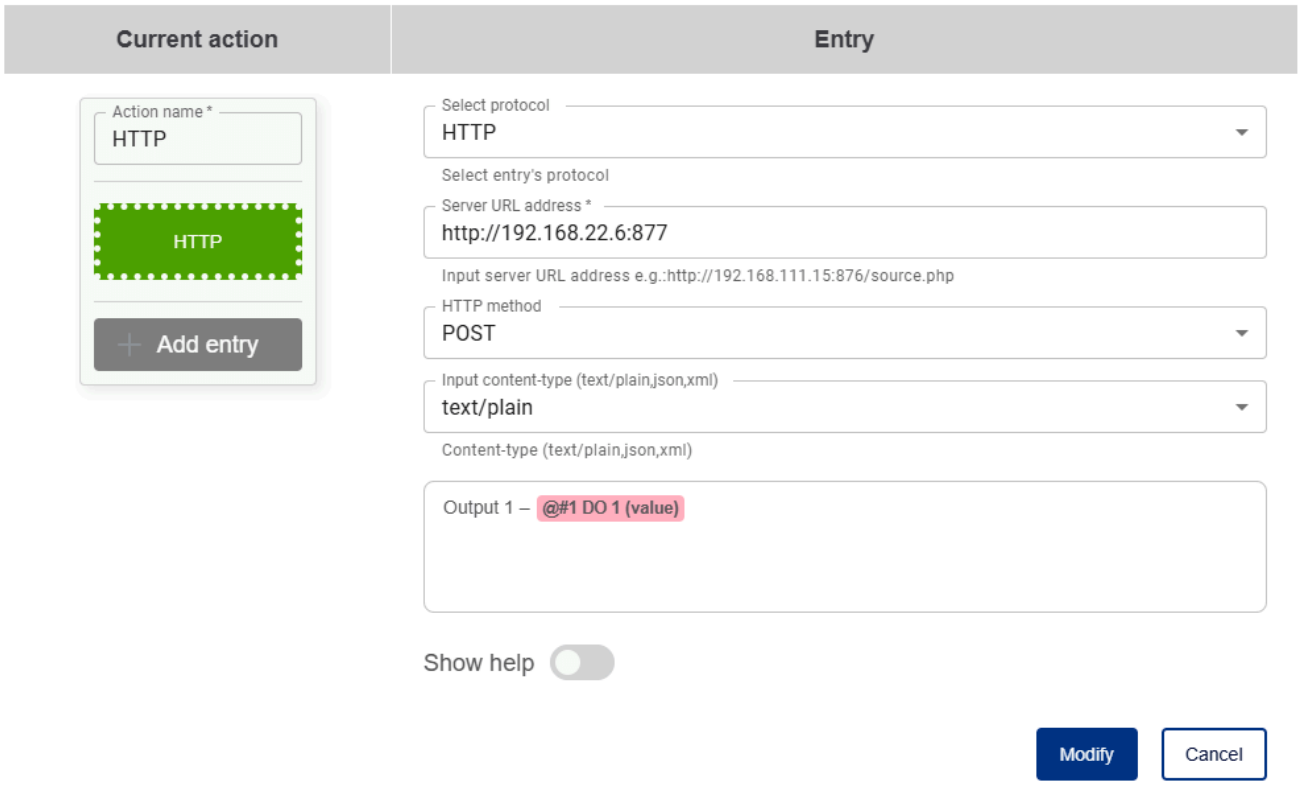
- **Server URL address** – Target URL address,

> **Warning**
>
> **The target URL must match the following convention:** `http://<IP_address>:<port>/<resource>`

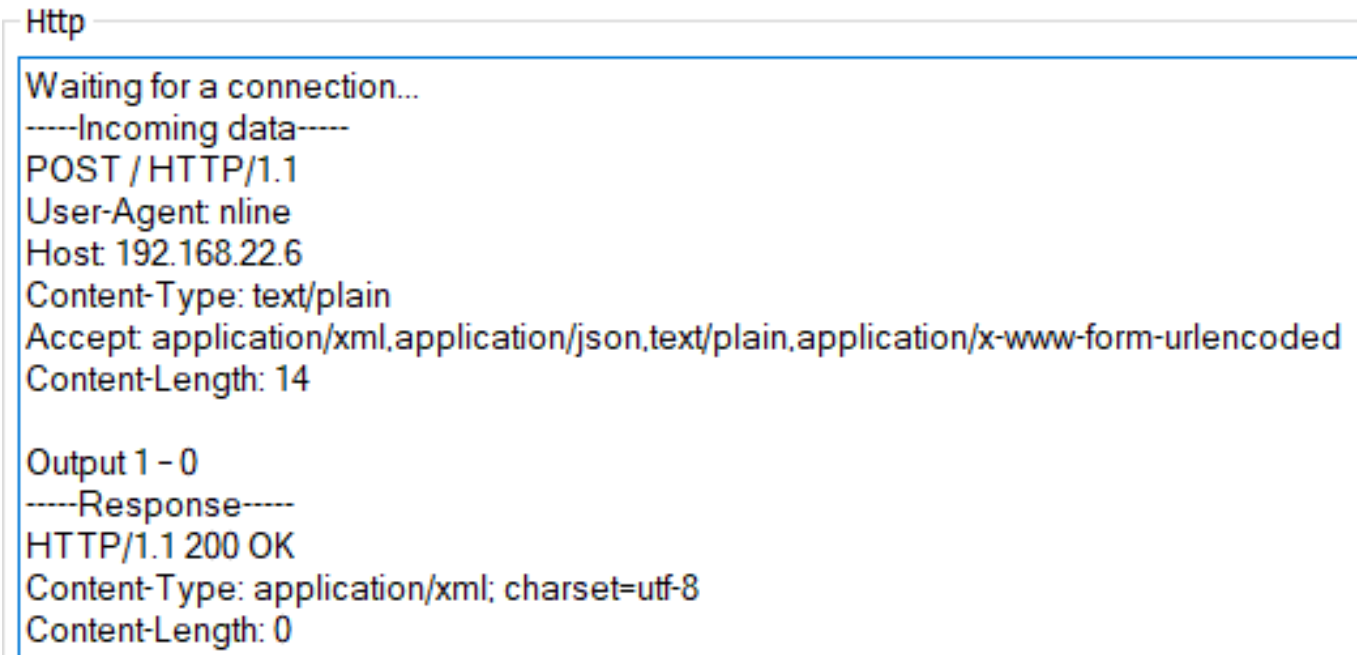
- **HTTP method:**
  - GET
  - POST
  - PUT
  - DELETE
- **Content-type:**
  - text/plain
  - application/x-www-form-urlencoded
  - application/json
  - application/xml
- **Input data** – Command sent to the target device.

Example 1

- **Server URL address:** `http://192.168.22.6:877`
- **HTTP method: POST**
- **Content-type: text/plain**
- **Input data:** `Output 1 – %o[1]%`



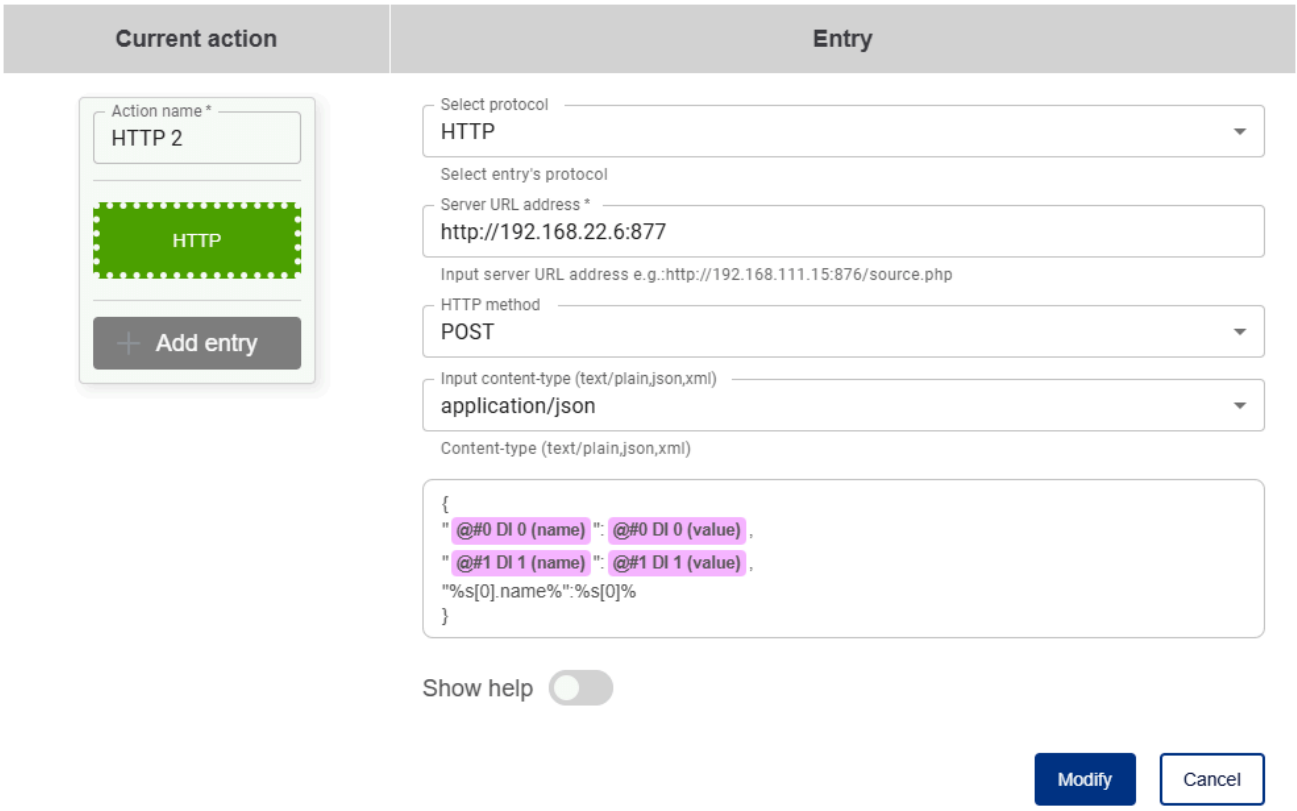
Sent data:



Example 2

- **Server URL address:** `http://192.168.22.6:877`
- **HTTP method: POST**
- **Content-type: application/json**
- **Input data:**

```
{
"%i[0].name%":%i[0]%,
"%i[1].name%":%i[1]%,
"%s[0].name%":%s[0]%
}
```



Sent data:

Http

```
Waiting for a connection...
-----Incoming data-----
POST / HTTP/1.1
User-Agent: nline
Host: 192.168.22.6
Content-Type: application/json
Accept: application/xml,application/json,text/plain,application/x-www-form-urlencoded
Content-Length: 30

{"DI 0":0,"DI 1":1,"s0":0}
-----Response-----
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 0
```

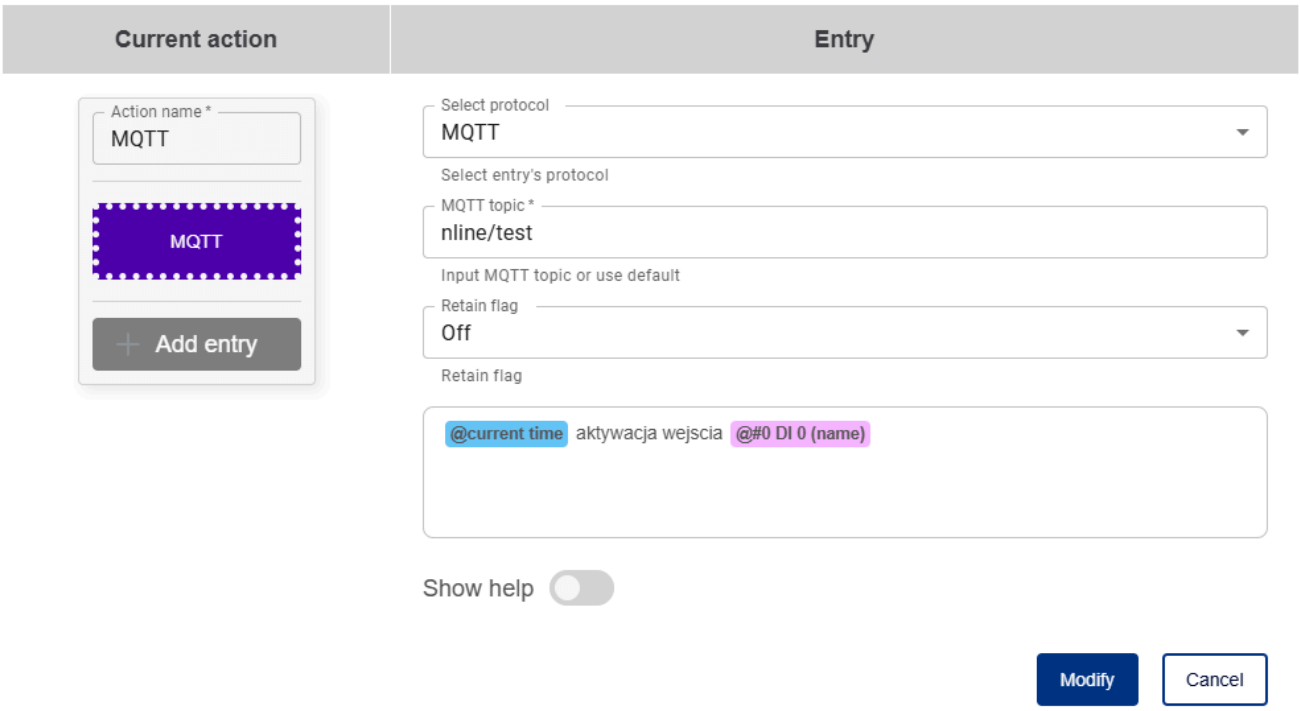
MQTT

Detailed protocol configuration is located in the **Services** tab.

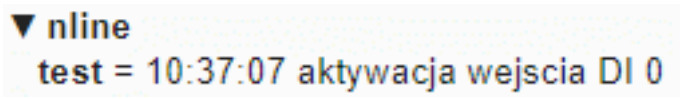
- **MQTT topic** – Topic, the device sends data to,
- **Retain flag** – Activated option causes the broker to retain last messages for topics the device sends data to,
- **Input data** – Message payload.

Example

- **MQTT topic:** `nline/test`
- **Retain flag: Off**
- **Input data:** `%time% input %i[0].name% activation`



Sent data:

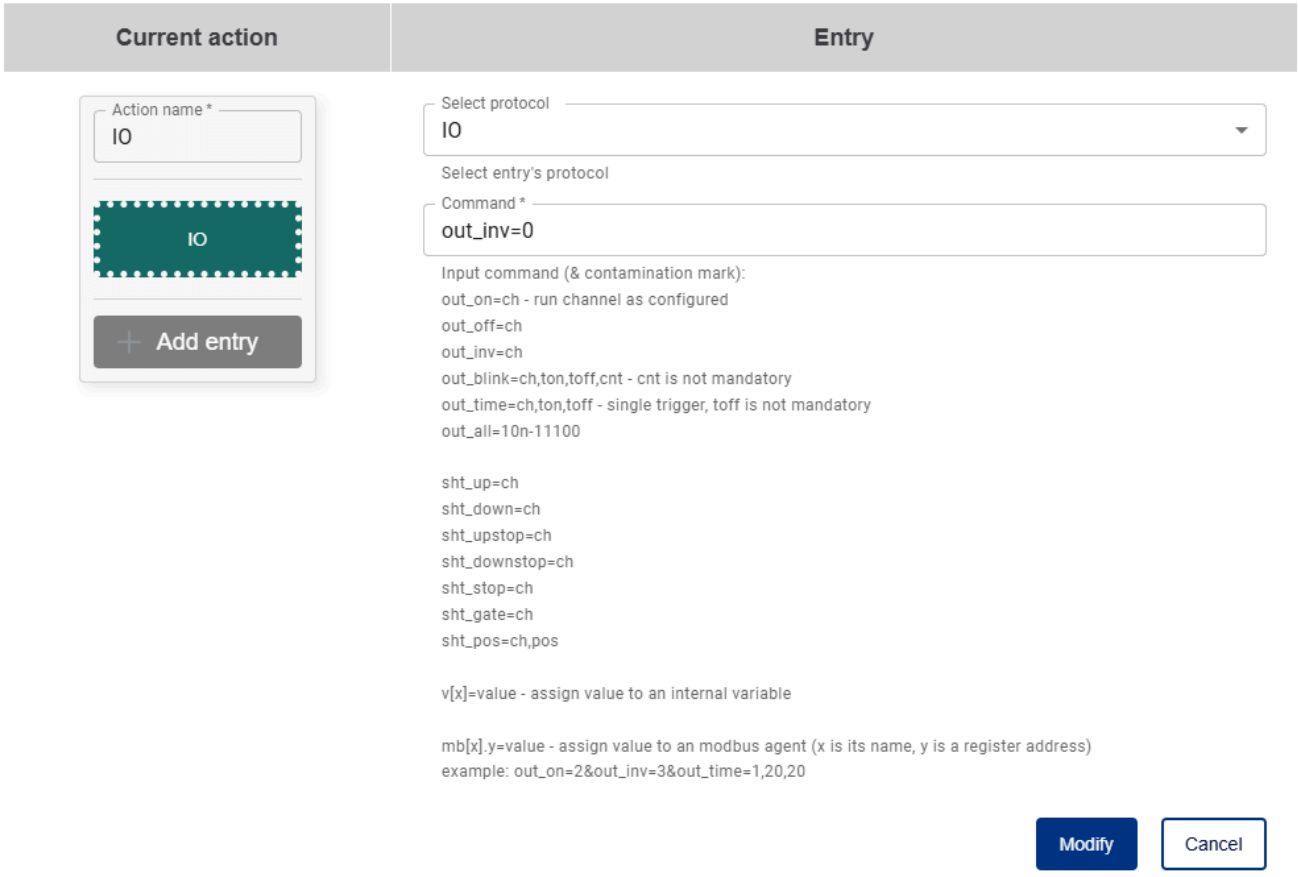


IO

- **Input command** – Command field:
  - `in_cnt=ch,val` – Set the `ch` channel counter value to `val`,
  - `out_on=ch` – Activate output channel `ch`,
  - `out_off=ch` – Deactivate output `ch`,
  - `out_inv=ch` – Output `ch` state invert,
  - `out_blink=ch,ton,toff,cnt` – Periodic output `ch` control. Parameters:
    - `ton` – Activation time (in seconds),
    - `toff` – Deactivation time (in seconds),
    - `cnt` – Number of activation cycles (not required).
  - `out_time=ch,ton,toff` – Activate output `ch` for the time defined in `ton`, after `toff` time passes. The `toff` parameter is not required – omitting it will activate the output without a delay,
  - `out_all=10n-11100` – Command defining the state of all available outputs. Each digit represents a subsequent output:
    - `1` – Activated,
    - `0` – Deactivated,
    - `n` – State invert,
    - `-` – No state change.
  - `sht_up=ch` – Open the shutter,
  - `sht_down=ch` – Close the shutter,
  - `sht_upstop=ch` – Open the shutter and stop,
  - `sht_downstop=ch` – Close the shutter and stop,
  - `sht_stop=ch` – Shutter stop,
  - `sht_gate=ch` – ,
  - `sht_pos=ch,pos` – Move shutter to the specified position,
  - `v[x]=value` – Assign a `value` to the variable `x`,
  - `mb[x].y=value` – Write the `value` to the Modbus register `y`, of the agent `x`,
  - `dev[x].o[y]=0|1` – Assign 0 or 1 to the external output `y` in device `x`.

Example

- **Input command:** `out_inv=0`



This setting will invert the state of output 0.

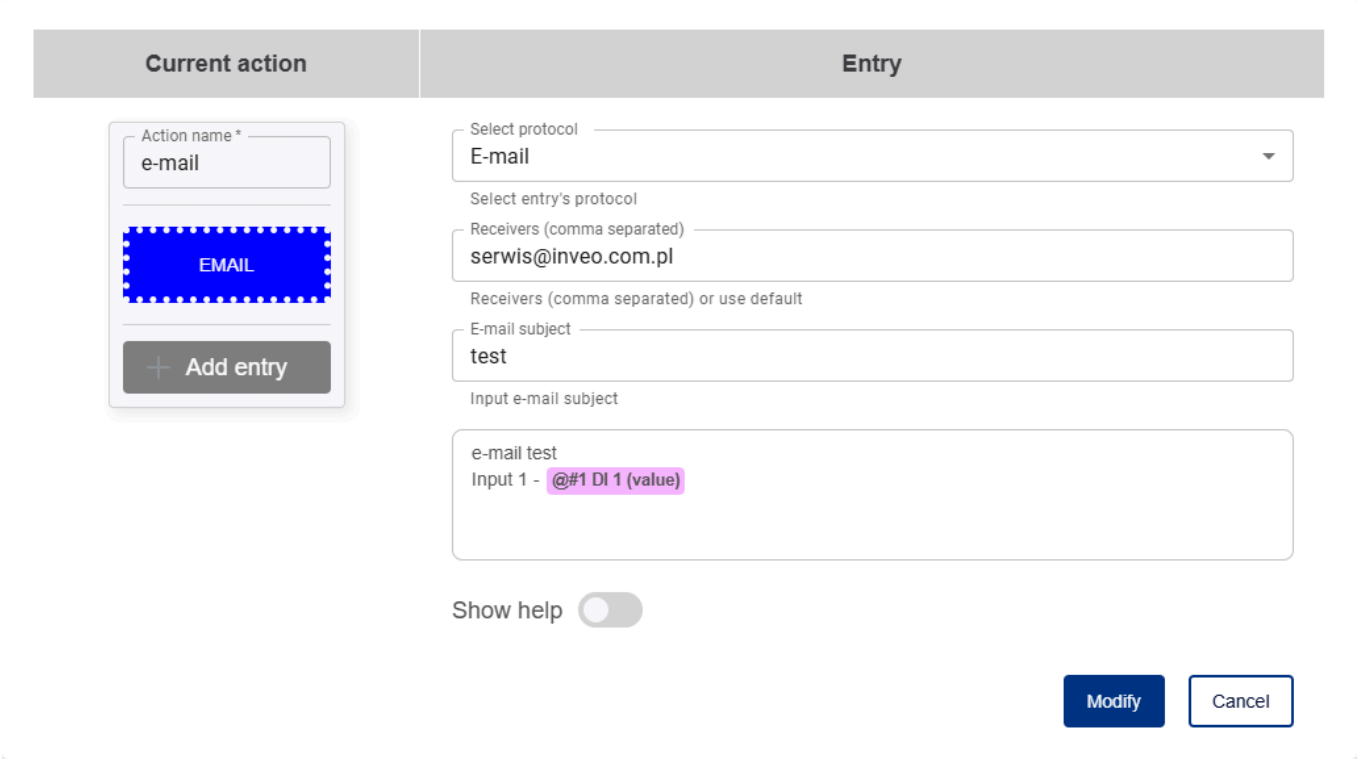
E-mail

Detailed protocol configuration is located in the **Services** tab.

- **Receivers (comma separated)** – E-mail recipients (comma separated),
- **E-mail subject** – E-mail message subject,
- **E-mail message** – E-mail message contents.

Example

- **Receivers (comma separated):** `test1@test.com`
- **E-mail subject:** `test`
- **E-mail message:** `e-mail test Input 1 - %i[0]%`



Those settings will cause an e-mail with the topic of `test`, with the contents of `e-mail test Input 1 -` and current input state to be sent to test1@test.com.

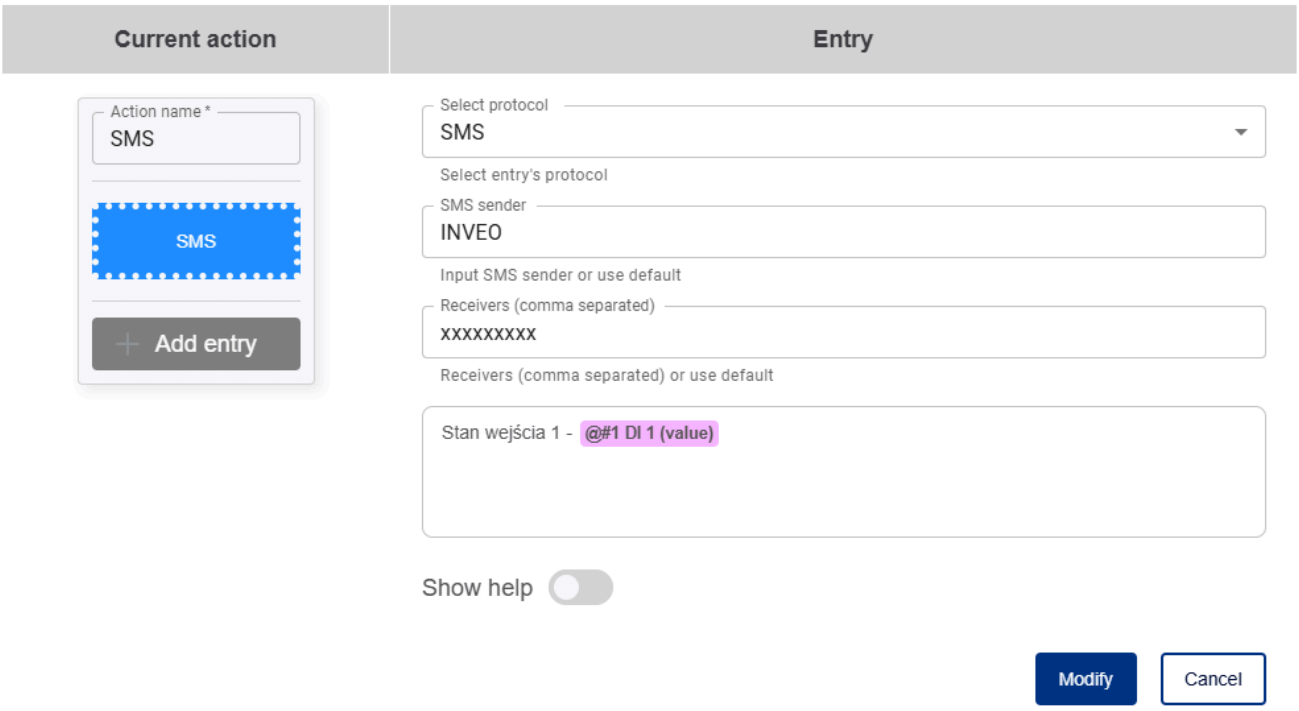
SMS

Detailed protocol configuration is located in the **Services** tab.

- **SMS sender**,
- **Receivers (comma separated)** – SMS recipients (comma separated),
- **SMS message** – SMS message contents.

Example

- **SMS sender: INVEO**
- **Receivers (comma separated): xxx xxx xxx**
- **SMS message:** `Output 1 state - %i[1]%`



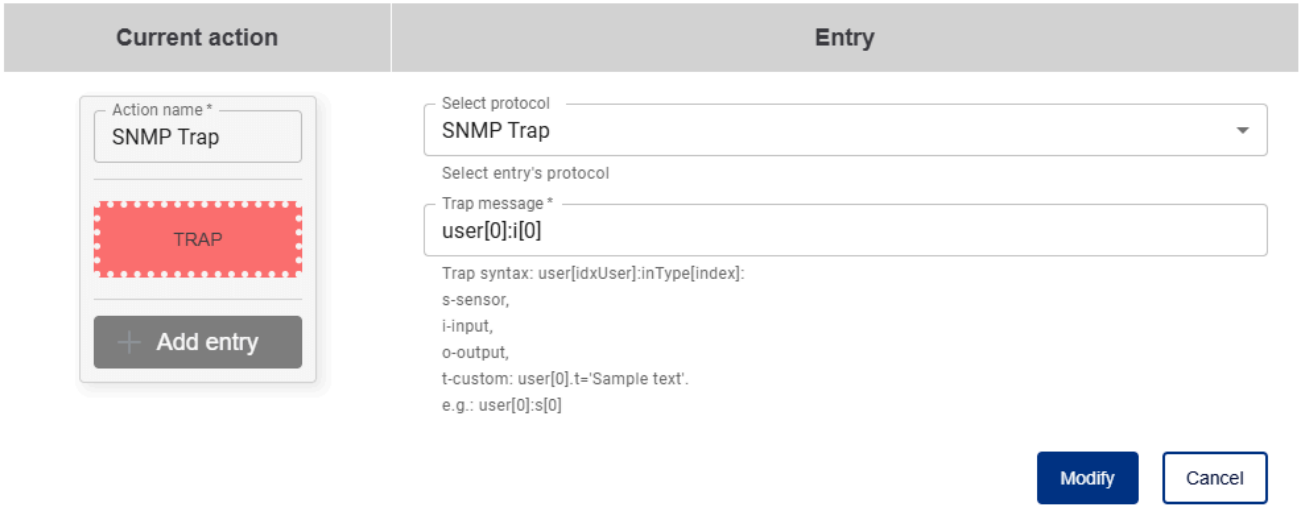
Those settings will cause an SMS from INVEO**, with the contents of** `Output 1 state - (output state)` **to be sent to the phone number xxx xxx xxx.**

SNMP Trap

- **Trap message** – Message syntax.

Example

- **Trap message:** `user[0]:i[0]`

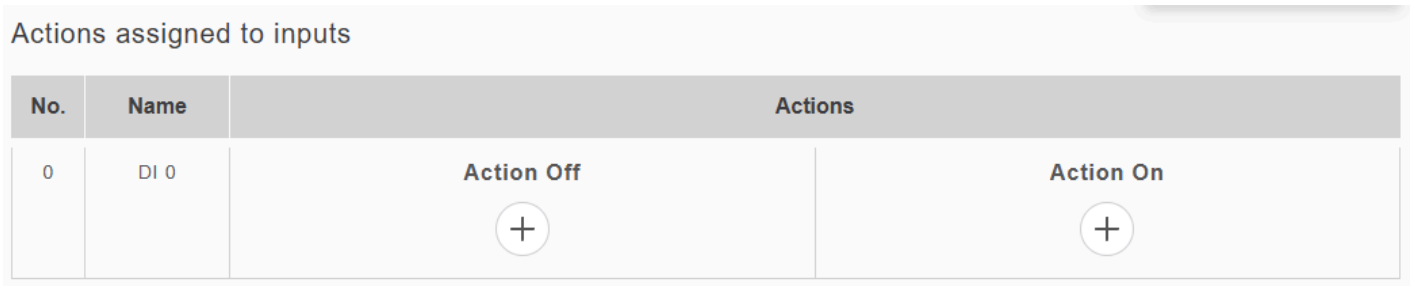


Sent data:

Description	Source	Time	Severity
.1.3.6.1.4.1.42814.10.1.1.100.0.5	192.168.22.71	2025-05-14 10:41:34	

Inputs

Defined actions can be configured and assigned to specific inputs in this tab.



Depending on the input operation mode (defined in **I/O Settings / Inputs**), various forms of actions triggering the assigned action are available.

Selected action mode	Available action forms	Action that will trigger the assigned action
Standard	Action Off	Action is triggered by input deactivation
	Action On	Action is triggered by input activation
Hold	Action Off	Action is triggered by input deactivation - input was activated for a time shorter than defined by the user in **Parameter**
	Action On	Action is triggered by input activation
	Action Hold On	Action is triggered by input activation for a time longer than defined by the user in **Parameter**
	Action Hold Off	Action is triggered by input deactivation – input was activated for a time longer than defined by the user in **Parameter**
Cnt	Action I	Action is triggered by the specified number of activations in a time period defined by the user in **Parameter**
	Action II	Action is triggered by the specified number of activations in a time period defined by the user in **Parameter**
	Action III	Action is triggered by the specified number of activations in a time period defined by the user in **Parameter**
	Action IV	Action is triggered by the specified number of activations in a time period defined by the user in **Parameter**
Toggle	Action I	Subsequent pulses on the input recall **Action I** and **Action II** alternately

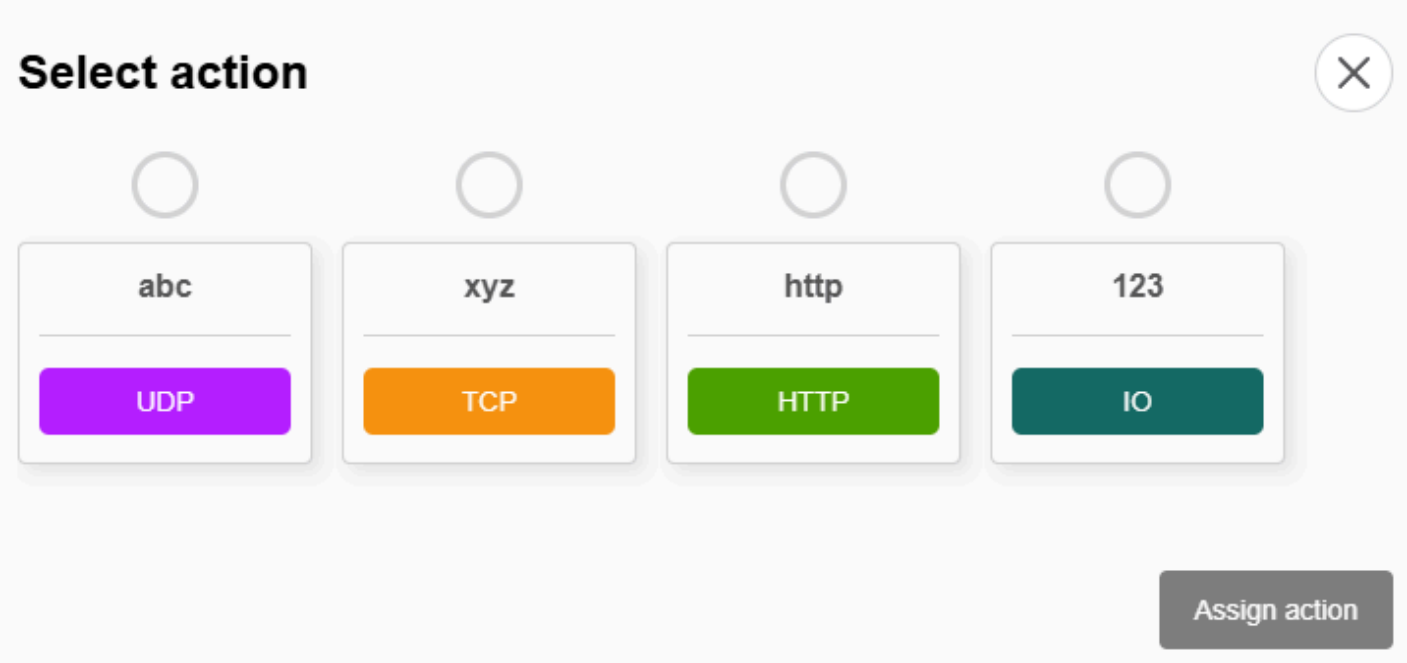
	Action II	
Freq	Action Off	Action is triggered by input activation with a frequency lower than defined by the user in **Parameter**
	Action On	Action is triggered by input activation with a frequency higher than defined by the user in **Parameter**

The **Go to the input actions** allows quick access to the **I/O Settings / Inputs** tab.

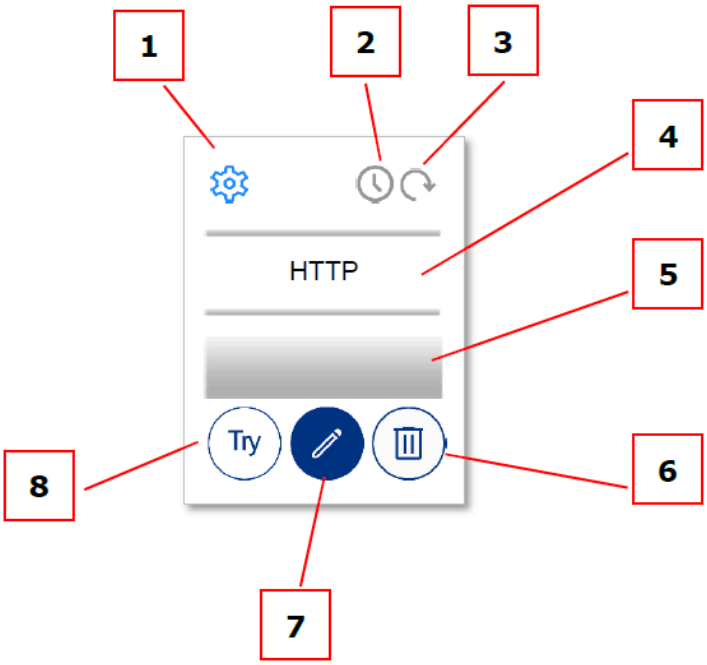
The  icon allows for step-by-step configuration.

Assigning actions

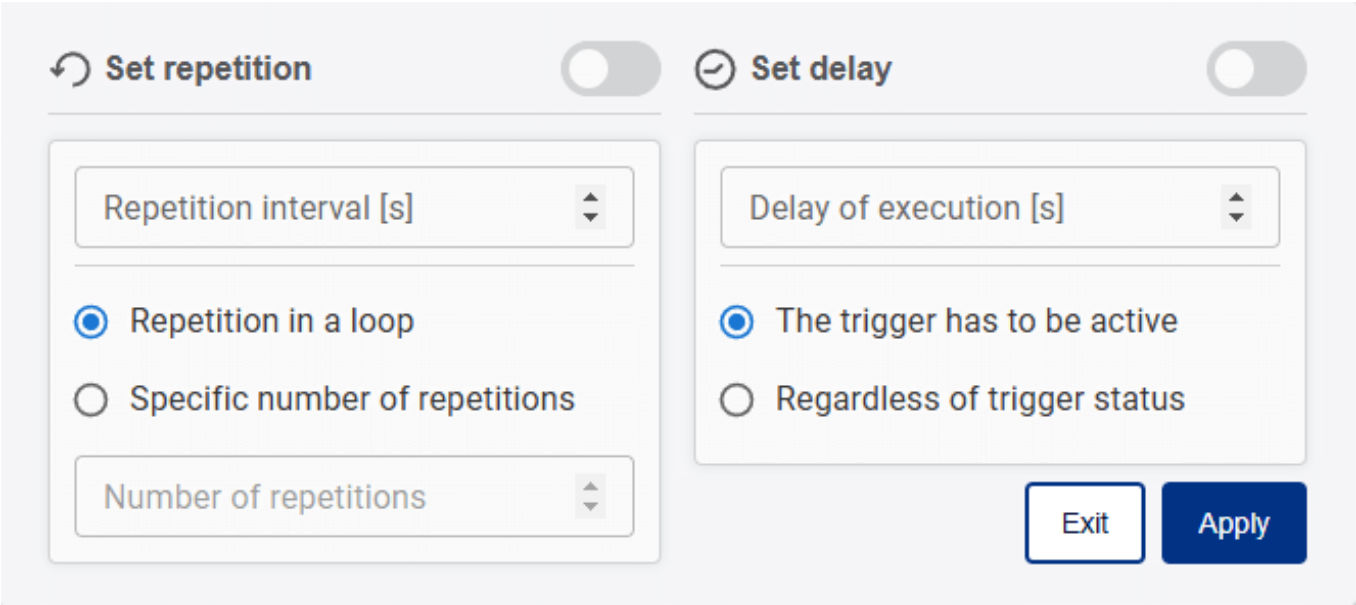
To assign an action to a chosen event, click **+**. A dialogue window will be displayed, where the desired action (defined previously in **All**) can be selected.



After an action is assigned, a window appears in the table:



1. Additional settings (repetition and delay) icon:



- **Repetition interval [s]** – Interval between executed actions. If this field is empty, the action will be executed only once,
  - **Repetiton in a loop** – Actions will be executed in a loop,
  - **Specific number of repetitions** – Actions will be repeated for a specified number of times,
    - **Number of repetitions**,
- **Delay of action execution [s]**:
  - The trigger has to be active – The action will be delayed only when the trigger is active,
  - Regardless of trigger status – The action will be delayed regardless of the trigger state, Save the changes using **Apply**.

2. Action delay icon: **grey** – delay disabled, **green** – delay enabled,

3. Action repetition icon: **grey** – repetition disabled, **green** – repetition enabled,
4. Action name – defined by the user during addition or amendment of action settings,
5. Utilized communication protocol,
6. Bin icon – clicking it will remove action assignment,
7. Edit icon – clicking it will edit the action settings,
8. Try icon – clicking it will execute the action.

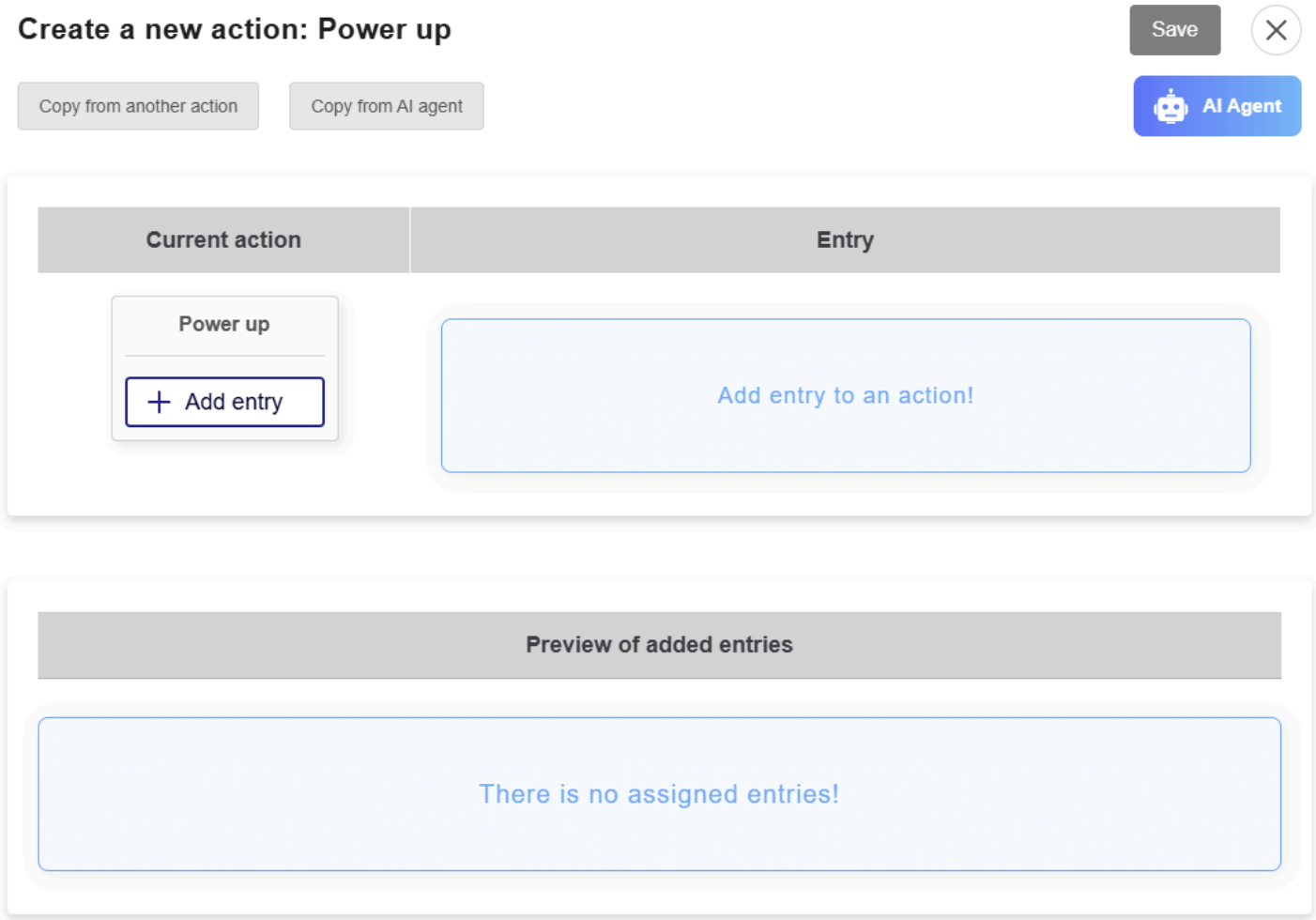
System

This tab allows the user to define system actions which the device will perform in the following events:



- **Power up** – Device power supply restore,
- **Ethernet up** – Ethernet access gained,
- **Ethernet down** – Ethernet access lost,
- **Wi-Fi up** – Wi-Fi access gained,
- **Wi-Fi down** – Wi-Fi access lost,
- **Modbus safe mode**.

Click **+** to assign the action to a desired event. A new dialogue window will appear:



Clicking **Add entry** will enable communication protocol selection and further configuration.

- **Select protocol** – The parameters of each protocol have been described in detail in the **Control Actions window** section.

After the programmed action's details are configured, click **Add**. It's possible to configure multiple actions for one event.

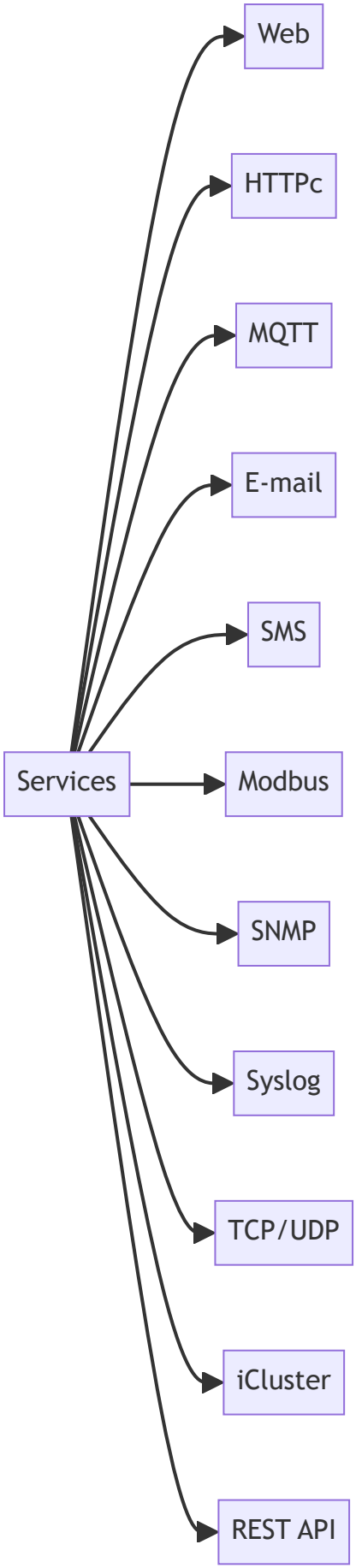
After defining all required settings, save the changes using .

Periodic

This tab allows the user to define periodic actions - performed in specified time intervals.

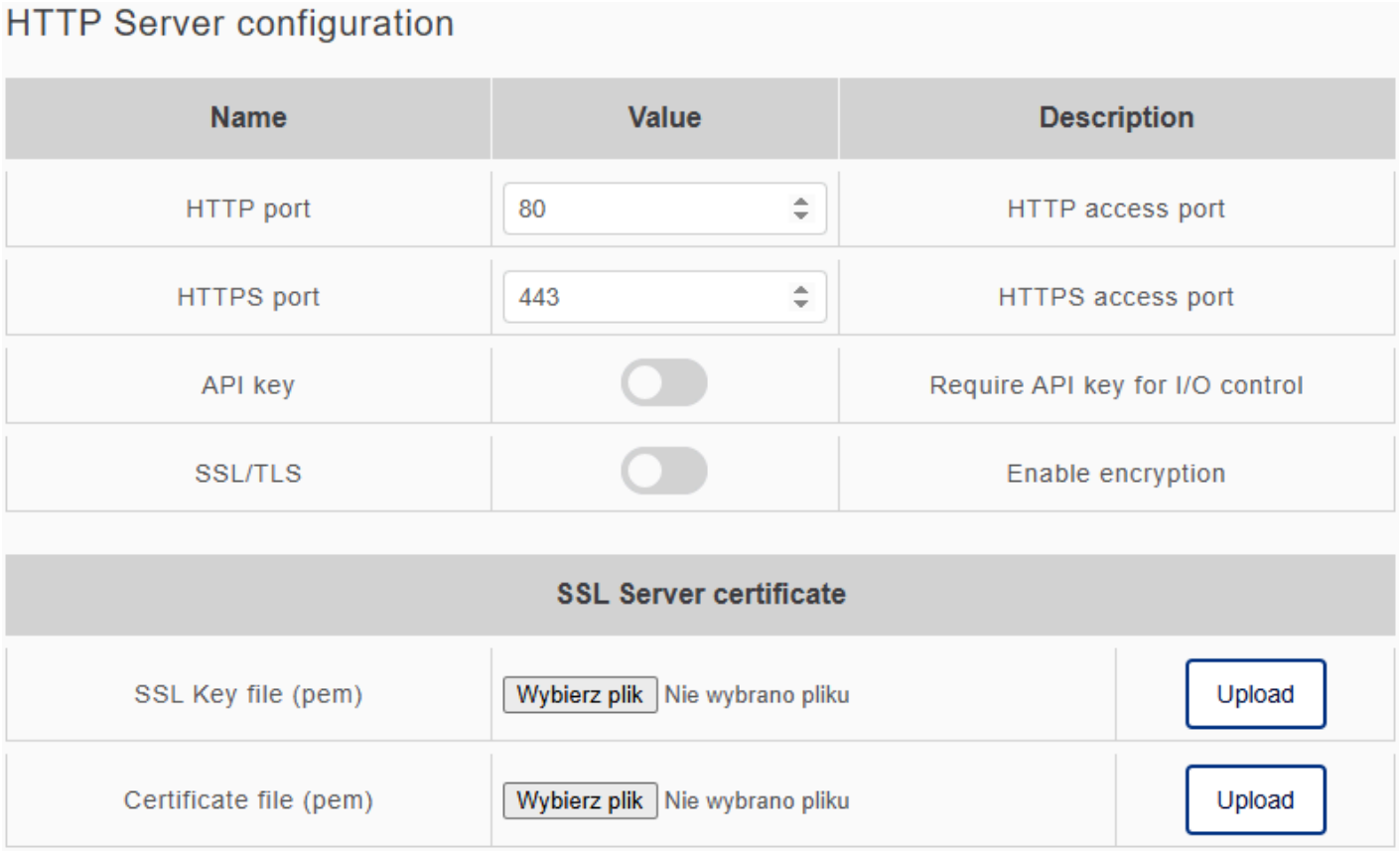
Communication protocols

In the **Services** tab, options enabling detailed communication protocol configuration options are located:


Web
HTTPc
MQTT
E-mail
SMS
Services
Modbus
SNMP
Syslog
TCP/UDP
iCluster
REST API

Web

In this section, the user can customize the device's network interface settings, manage resource access or modify network connection parameters.



- **HTTP Port**,
- **HTTPS port**,
- **API key** – Enable/disable API key requirement for I/O control,
- **SSL/TLS** – Enable/disable encryption,
- **Select Key file (pem)** – Allows upload of SSL server key (pem format),
- **Select CSR file (pem)** – Allows upload of CSR server key (pem format).

HTTPc

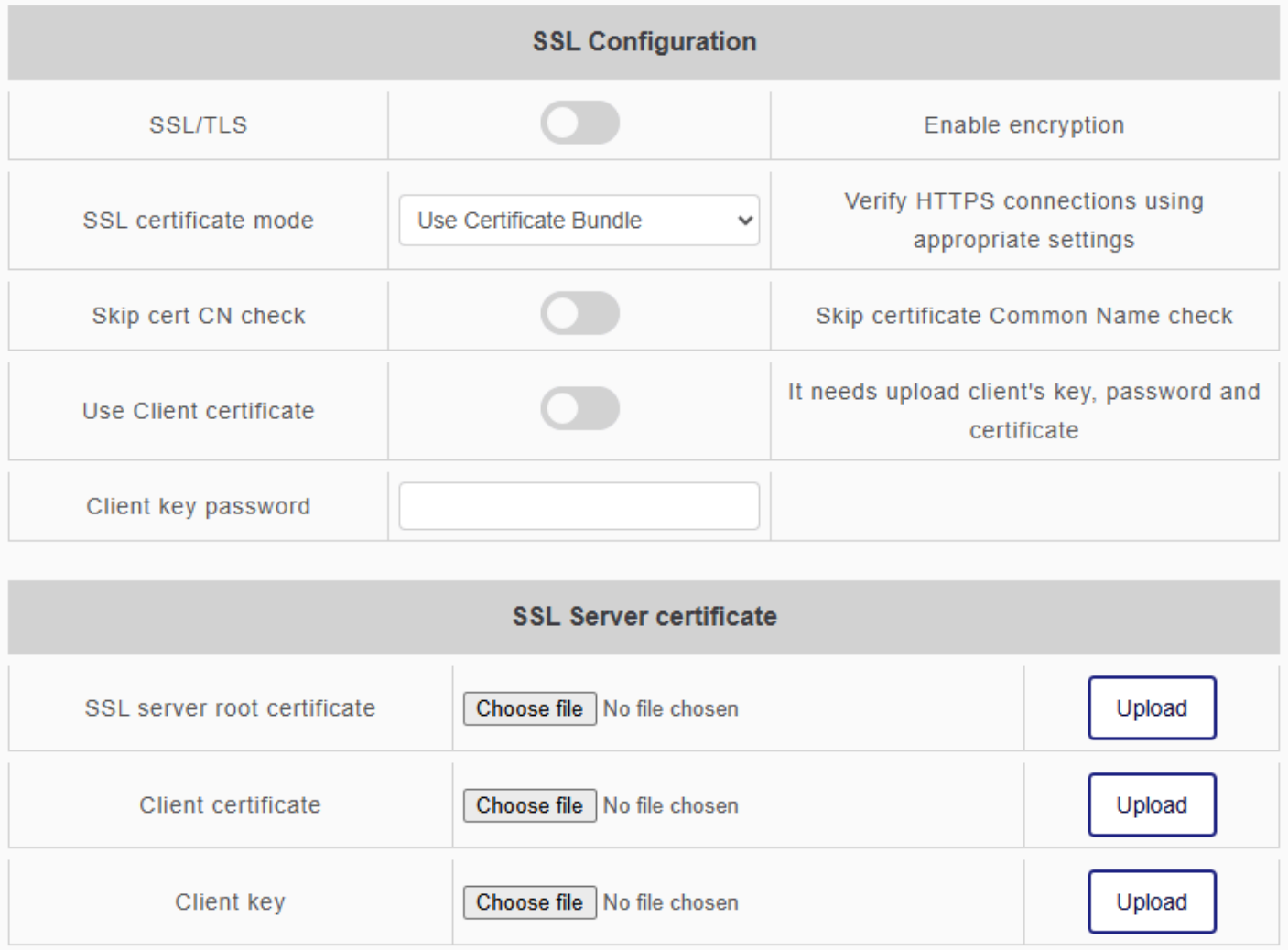
In this section, the device can be configured so it initiates HTTP connections with defined servers or services. URL addresses, request parameters and other connection details can be defined here. The device can send event data via HTTP/HTTPS, using GET or POST.

HTTP Client configuration

Name	Value	Description
HTTP Client		Enable HTTP Client
Server		Remote server address: IP or DNS-registered name
HTTP port	0	HTTP access port
HTTP Method	GET	HTTP request default method
Content type	text/plain	Content-type header
Resource	/	HTTP resource i.e. /resource.php
API key		Require API key for I/O control
Authentication to Server		
Authentication type	None	Select the authentication method for server communication
HTTP ping request		
HTTP ping request interval	0	Ping time in secs. 0-disable
HTTP ping request	HTTP ping requests to test the availability of web servers and APIs. These can be used in health testing or monitoring systems.	

Type @ and select variable...
You can mention variables like current time or module name

Source format Show help



- **HTTP Client** – Enable **HTTP Client** service,
- **Server** – HTTP server address, to which information will be sent,
- **HTTP Port** – Port, on which the HTTP server listens,
- **HTTP Method** – Message sending method: GET / POST / PUT / DELETE,
- **Content type**:
  - text/plain,
  - json,
  - xml,
  - form.
- **Resource** – Resource the module will refer to,
- **API key** – Enable/disable API key requirement for I/O control,
- **Authentication type** – Server authentication type,
  - **None**,
  - **Basic Authentication** – Username and password authorization:
    - **User**,
    - **Password**.

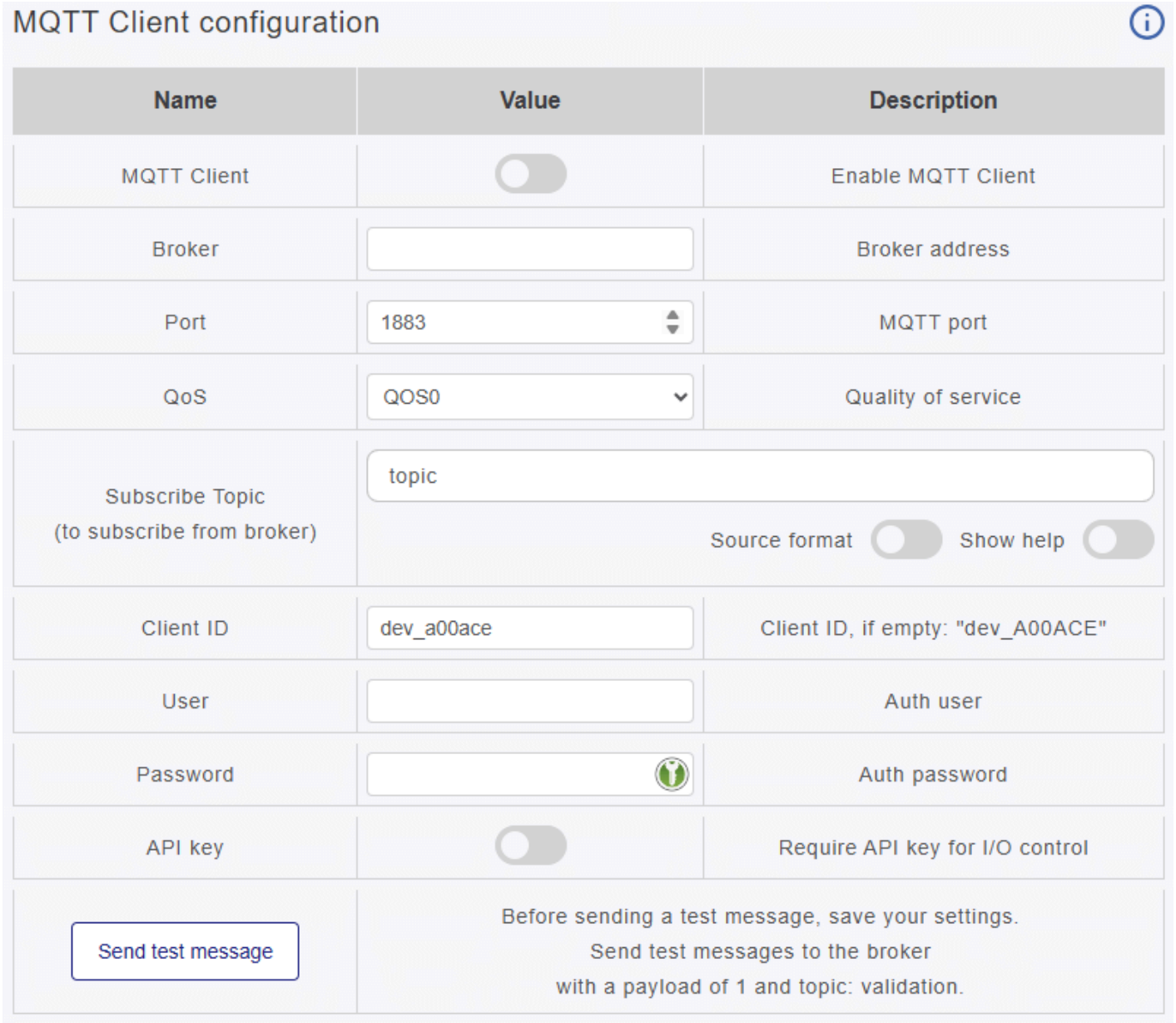
    - **X-API-KEY** – API key authorization:
        - **API Key**.
    - **Bearer Token**
        - **API Key**.
- **HTTP ping request interval**,
- **HTTP ping request** – Ping request syntax,
- **SSL/TLS** – Enable/disable encryption,
- **SSL certificate mode**:
    - **Use Certificate Bundle**,
    - **Use Uploaded Certificate**,
    - **Insecure! Disable SSL verification**,
- **Skip cert CN check** – Skip certificate common name check,
- **Use Client certificate**,
- **Client key password**,
- **SSL server root certificate**,
- **Client certificate**,
- **Client key**.

MQTT

This tab is used to configure MQTT broker communication parameters, allowing for data exchange with the publish-subscribe model. This allows the user to define key aspects such as topics, server address, port, and other connection parameters.
The device sends data to the server every minute and every time a value change occurs.

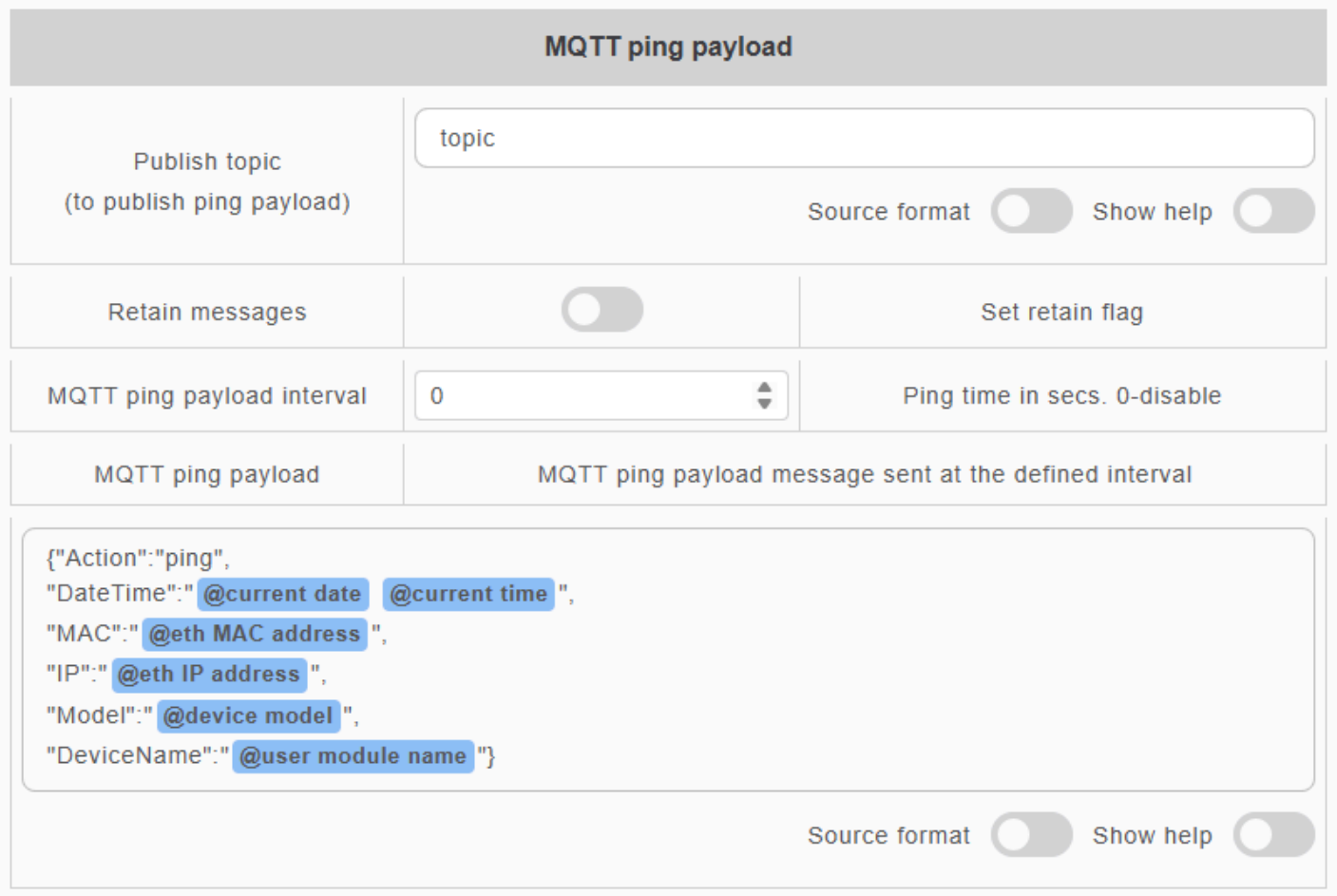
The data stream can be encrypted. After a connection with the MQTT broker is established, the users can subscribe to the data coming from the device.

There is no limit in the amount of subscribers that can receive data from a single device.



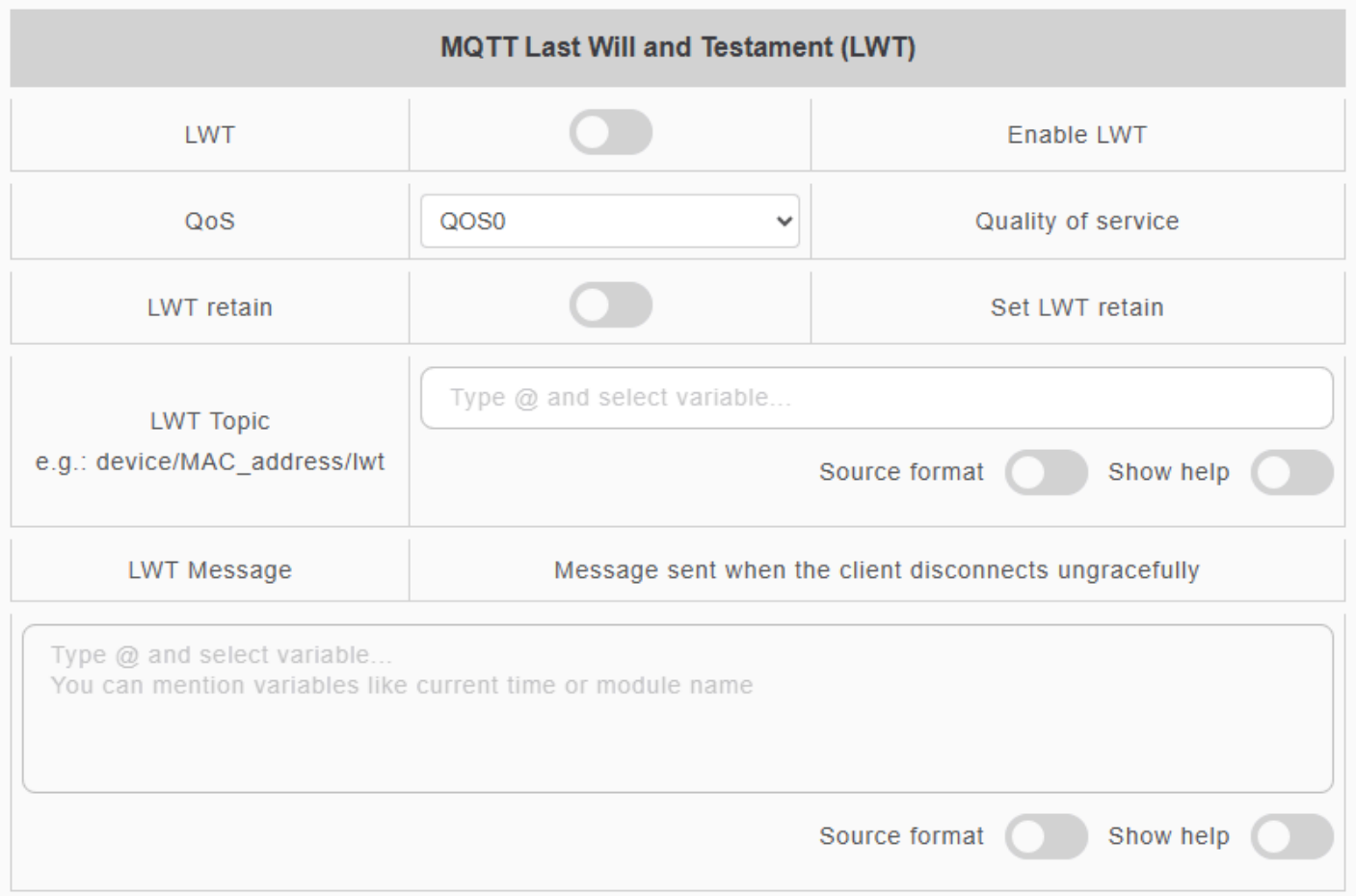
- **MQTT Client** – Enable MQTT service,
- **Broker** – MQTT broker address,
- **Port** – Port, on which the server listens (commonly 1883),
- **QoS** – Quality of Service level. Can assume one of three values: 0 (At most once), 1 (At least once), 2 (Exactly once),
- **Subsribe topic** – The topic must be in the format (eg. /sensor/home – without „/” at the end),
- **Client ID**,
- **User** – (optional) MQTT user name,
- **Password** – (optional),
- **API key** – Enable/disable API key requirement for I/O control,
- **Send test message** - Send a test message to the broker - topic **validation**, payload **1**.

The module can periodically send its data to the Broker. This functionality can be used to verify the integrity of notifications or for periodic data reading.

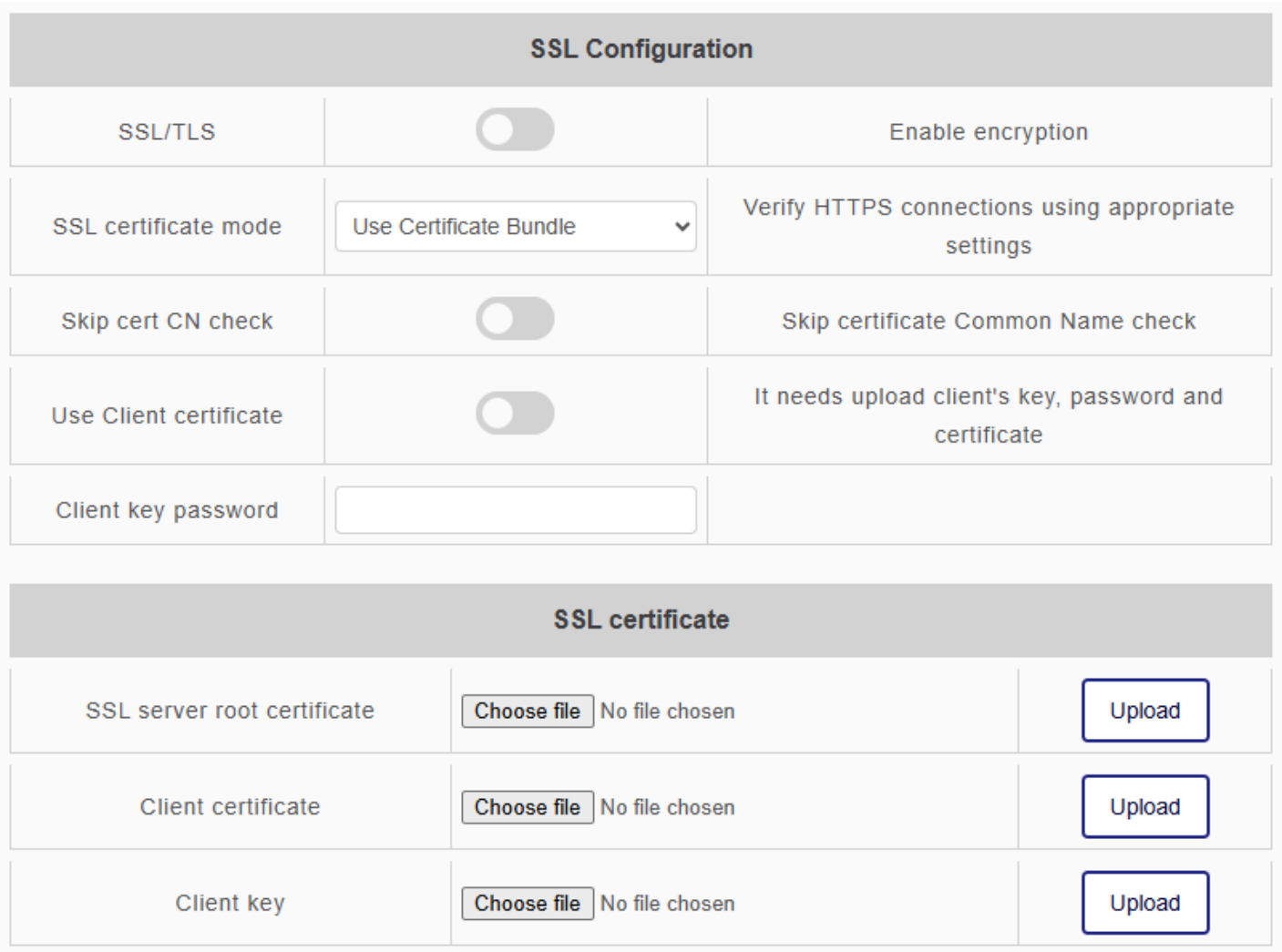


- **Publish topic** – Topic, to which data will be sent periodically,
- **Retain messages** – If enabled, the message will be saved on the broker an will be available for new topic subscribers,
- **MQTT ping payload interval** – Time interval between the data packets. Setting `0` disables the function,
- **MQTT ping paylaod**.

The device is equipped with the LWT mechanism, meaning **Last Will and Testament**. LWT is a mechanism that allows the MQTT client to send a message automatically in the event of a client error or MQTT broker connection loss.
The LWT mechanism allows the user to define a topic and message that will be published if the client looses connection.



- **LWT** – Enable/disable LWT,
- **QoS** – Quality of Service level. Can assume one of three values: 0 (At most once), 1 (At least once), 2 (Exactly once),
- **LWT retain** – If enabled, the LWT message will be saved on the broker an will be available for new topic subscribers,
- **LWT Topic** – Topic that the LWT message will be published at,
- **LWT Message** – LWT message contents.



- **SSL/TLS** – Enable/disable encryption,
- **SSL certificate mode**:
  - **Use Certificate Bundle**,
  - **Use Uploaded Certificate**,
  - **Insecure! Disable SSL verification**,
- **Skip cert CN check** – Skip certificate common name check,
- **Use Client certificate**,
- **Client key password**.
- **SSL server root certificate**,
- **Client certificate**,
- **Client key**.

Tip

After making changes, apply them using the Save button.

Tip

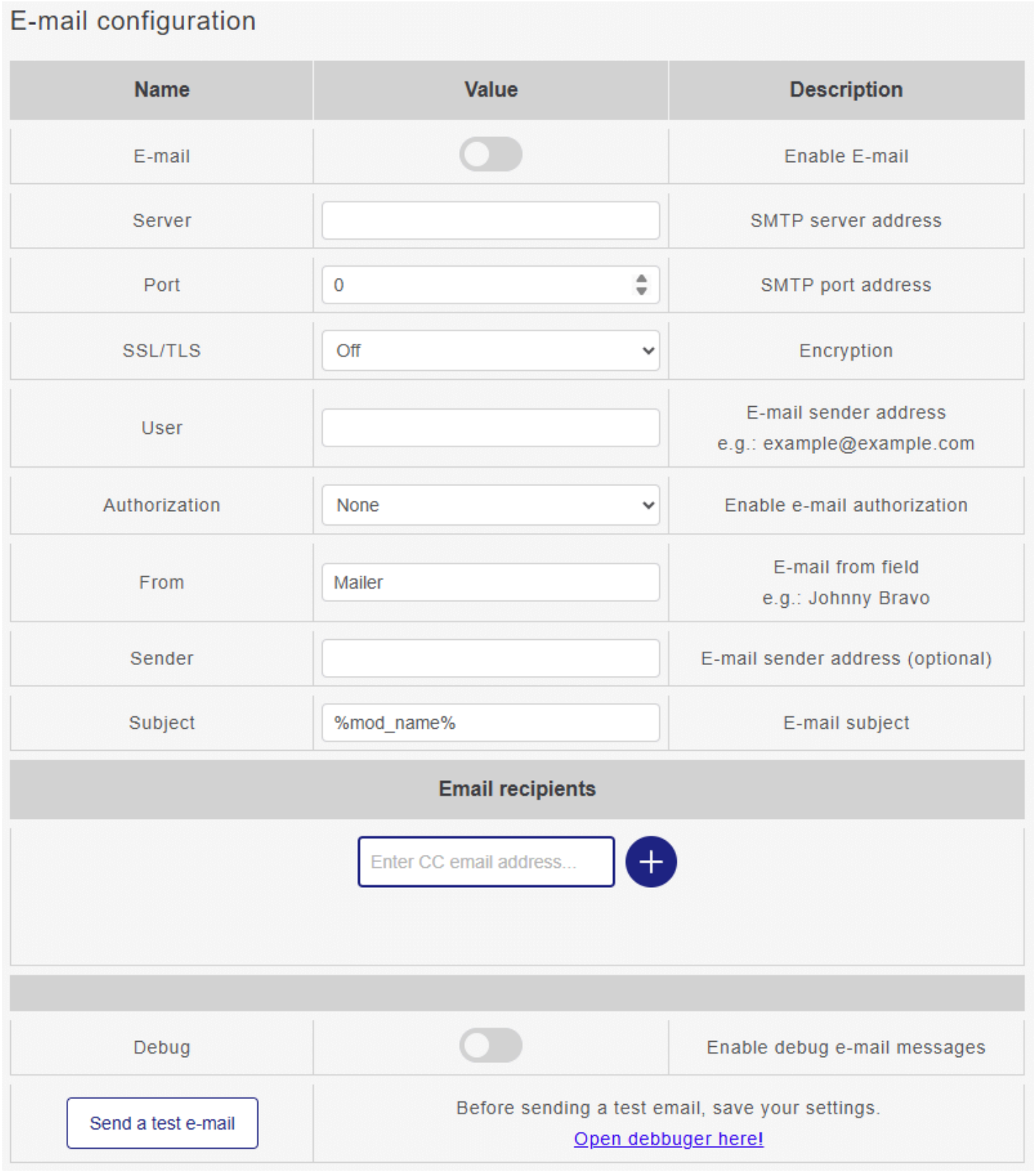
For the Inveo broker, the settings should be as follows:
- MQTT Address**: mqtt.inveo.com.pl**
- MQTT Port**: 1883**
A computer with the Inveo Monitoring application installed can be used as a broker. To do that, type the PC's IP address into the MQTT Address field.

Tip

Make sure that the selected Topic is unique, eg. /daxi/MAC address.

E-mail

In this section, e-mail server connection parameters can be configured. This makes it possible to send e-mails automatically in response to defined actions or alarms.

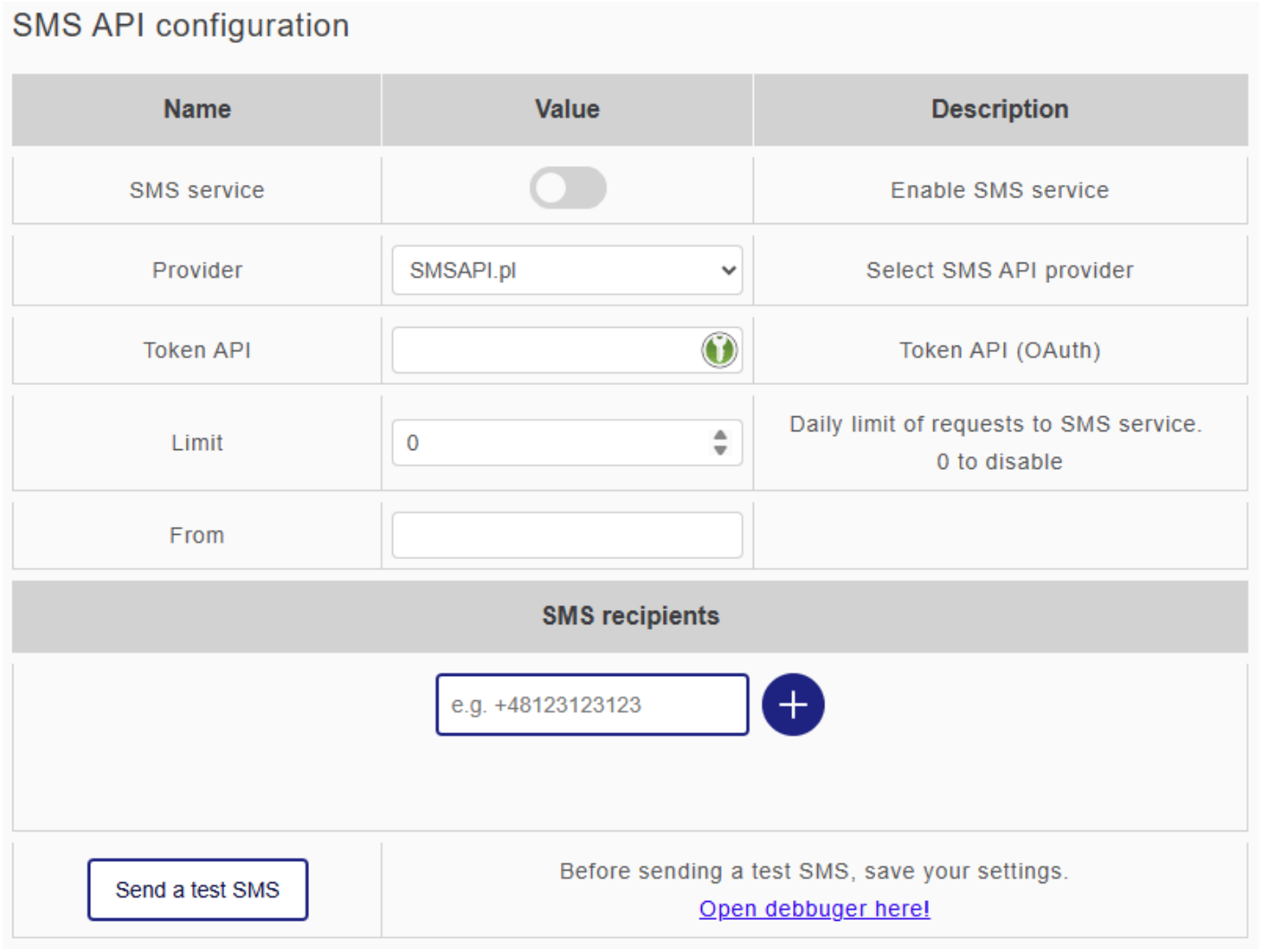


- **E-mail** – Enable/disable e-mail service,
- **Server** – SMTP server address,
- **Port**,
- **SSL/TLS** – Encryption:
  - **Off**,
  - **SSL**,
  - **STARTTLS**.

- **User** – E-mail address,
- **Authorization** – Authorization method:
  - **None**,
  - **Plain** – Password:
    - **Password**.
- **From** – Message sender,
- **Sender** – Sender's e-mail address (if different from the user),
- **Subject**,
- **Recipients**,
- **Debug** – Message debugging function,
- **Send a test e-mail**.

SMS API

The module can be configured to send SMS messages in respondse to defined events or with an information eg. about an alarm.

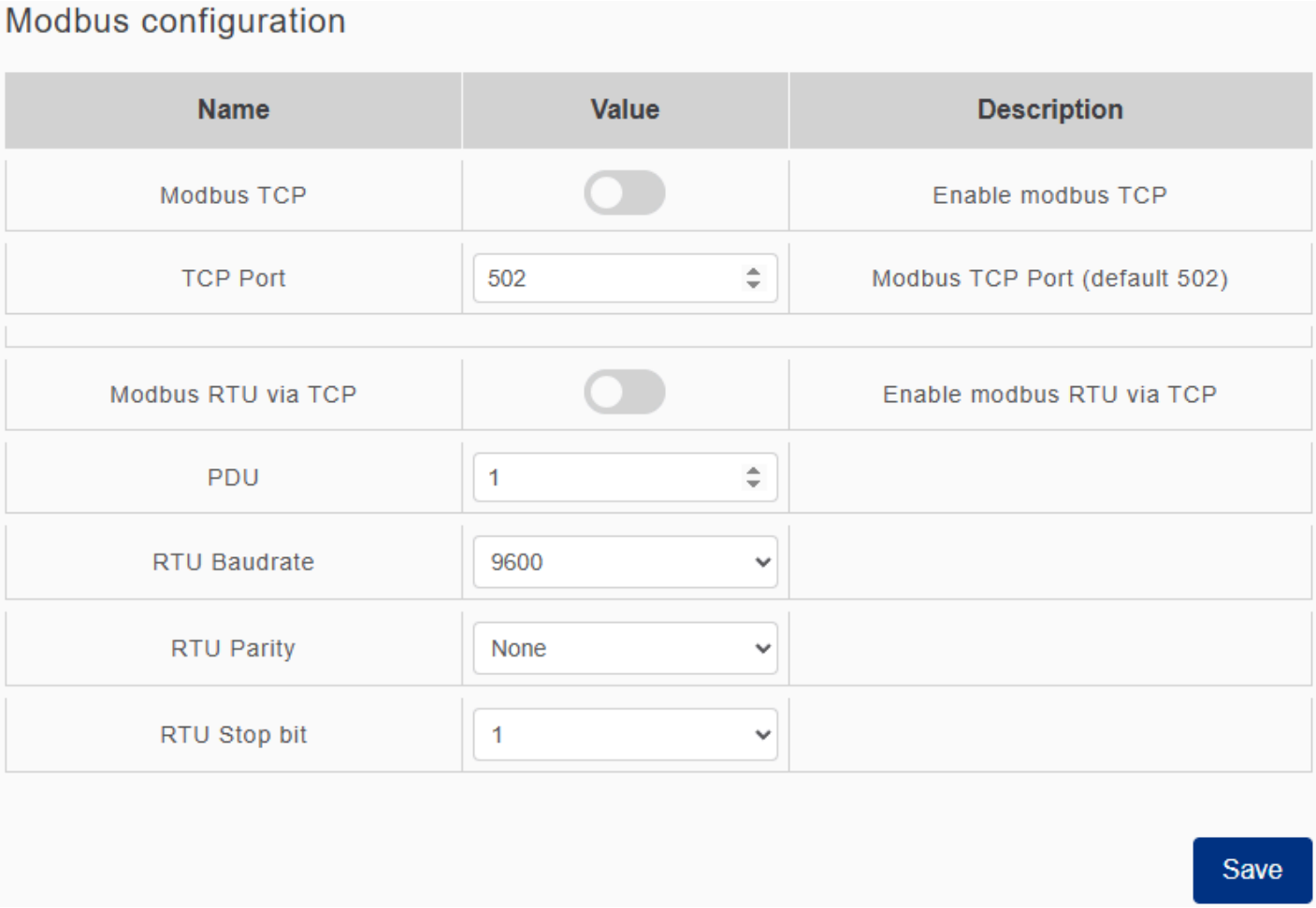


- **SMS service** – Enable/disable SMS service,
- **Provider** – Defines the SMS service provider, with whom the API is integrated:
  - **SMSAPI.pl**
- **Token API** – Unique authorization key used for access authentication and communication with the SMS service provider's API,
- **Limit** – Daily limit of SMS messages, value of 0 will disable the SMS sending service,
- **From** – Defines the message sender: this can be a predefined name, phone number or other identifier that will be visible to the message's recipient,
- **Recipients** – List of recipients phone numbers,
- **Send a test SMS**.

Modbus

Device data can be read and written using Modbus TCP. The device supports the following Modbus functions:

- 0x01 Read Coils
- 0x02 Read Discrete Inputs
- 0x03 Read Holding Register
- 0x04 Read Input Register
- 0x05 Write Single Coil
- 0x06 Write Single Register
- 0x0F Write Multiple Coils
- 0x10 Write Multiple Registers



- **Modbus TCP** – Enable/disable Modbus TCP service,
- **TCP Port** – Modbus TCP port (default 502),
- **Modbus RTU via TCP** – Enable/disable Modbus RTU via TCP service,
- **PDU**,
- **RTU Baudrate**,
- **RTU Parity**,

- **RTU Stop bit**.

Content of the registers is shown in the following tables:

Coils addressing

Address	R/W	Description
1	R/W	Output 0 state, enable/disable output 0: **0** – OFF, **1** – ON
2	R	Output 0 state
3		As shown above – applies to subsequent outputs

Discrete Inputs addressing

Address	R/W	Description
1	R	Input 0 state
2...	R	State of subsequent inputs

Holding Registers addressing

Address	R/W	Description
1	R	Input 0 counter – MSB
2	R	Input 0 counter – LSB
3-200	R	As shown above – applies to subsequent inputs
201	R/W	Output 0 state, enable/disable output 0: **0** – OFF, **1** – ON
202	R/W	Output 0 operating mode: **0** – disable **1** – bistabile **2** – astabile **3** – one pulse
203	R/W	**Time On** value
204	R/W	**Time off** value

205...		As shown above – applies to subsequent outputs
1001		Sensor 0 Low Alarm: **0** – OFF, **1** – ON
1002-1003	R/W	Sensor 0 Low Alarm value (FLOAT32, little endian)
1004	R/W	Sensor 0 Low Warning: **0** – OFF, **1** – ON
1005-1006	R/W	Sensor 0 Low Warning value (FLOAT32, little endian)
1007	R/W	Sensor 0 High Warning: **0** – OFF, **1** – ON
1008-1009	R/W	Sensor 0 High Warning value (FLOAT32, little endian)
1010	R/W	Sensor 0 High Alarm: **0** – OFF, **1** – ON
1011-1012	R/W	Sensor 0 High Alarm value (FLOAT32, little endian)
1013...	R/W	As shown above – applies to subsequent sensors

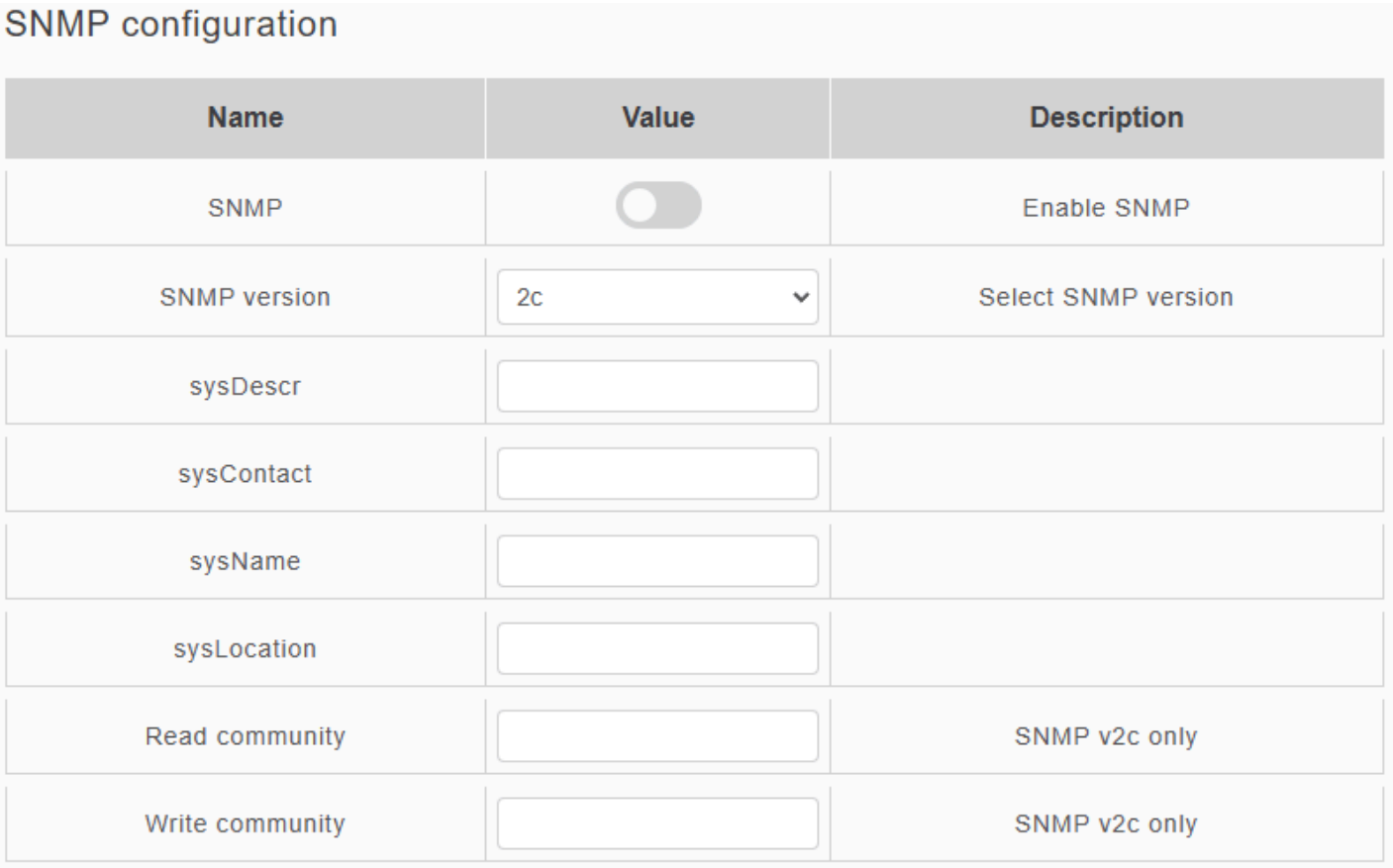
Input Registers addressing

Address	R/W	Description
1	R	**0** – read error (sensor damaged or miswired), **1** – the sensor is giving readings that are within set limits, **2** – low level warning, **3** – high level warning, **4** – low level alarm, **5** – high level alarm, **6** – sensor initializing.
2	R	Sensor value x10 (SINT16)
3-4	R	Sensor value (FLOAT32, little endian)
5	R	Sensor's last read time – MSB
6	R	Sensor's last read time – LSB
7...	R	As shown above – applies to subsequent sensors

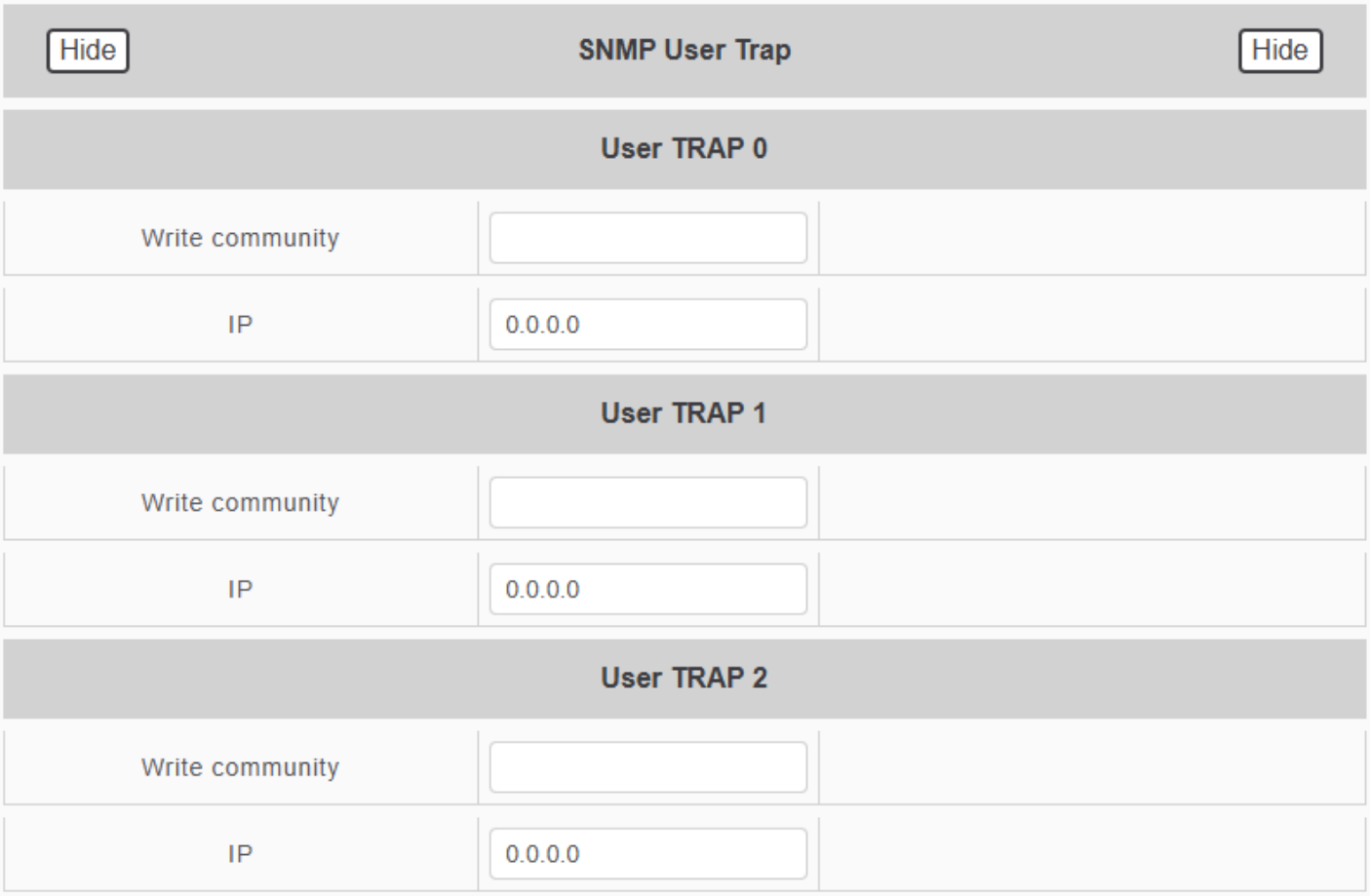
SNMP

This section allows configuration of SNMP protocol settings, used for monitoring and network device management. The module is equipped with the v2c or v2c and v3 *(version dependent)* SNMP servers. Depending on the SNMP version selected, different parameters are available.

SNMP v2c

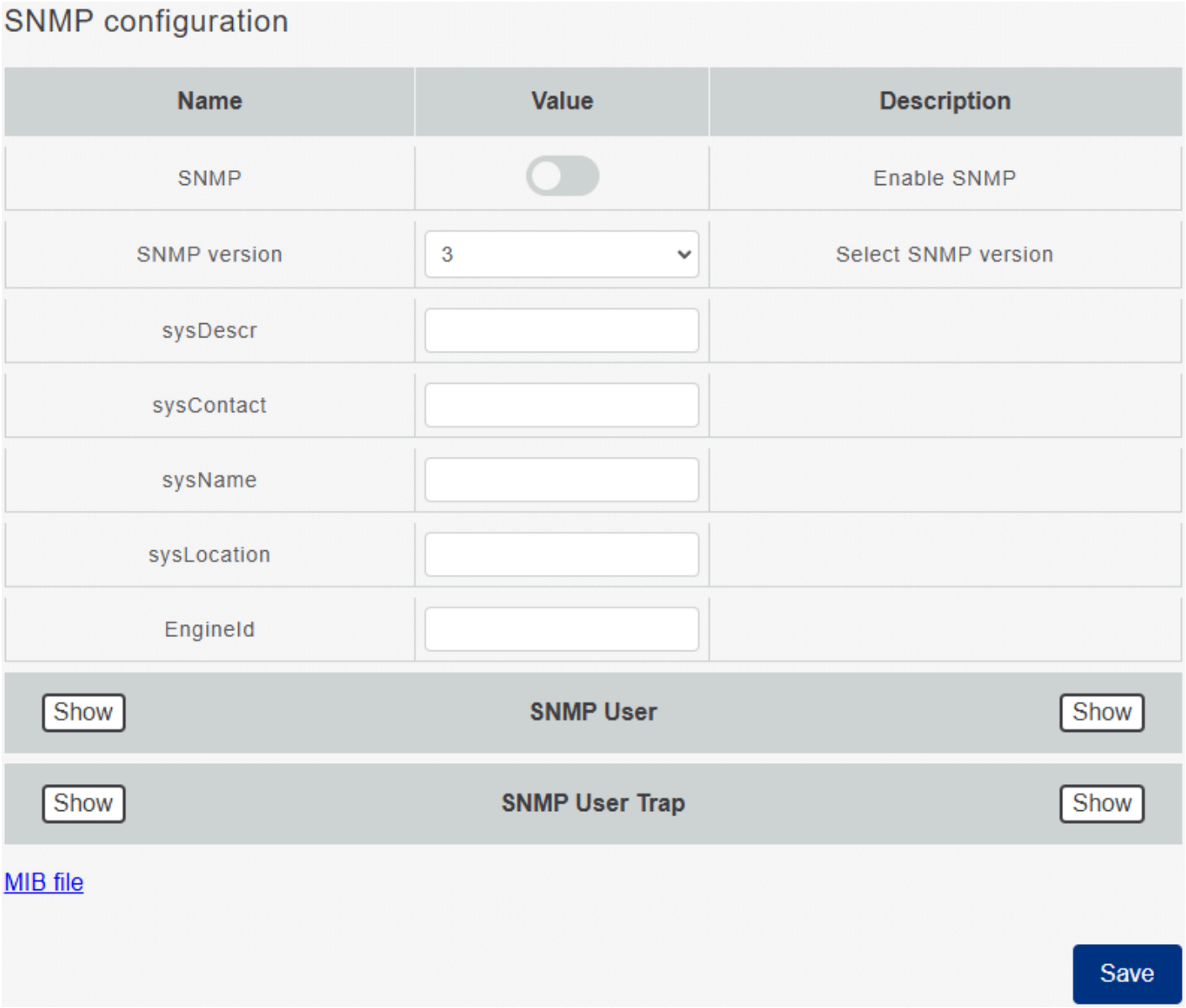


- **SNMP** – Enable/disable SNMP service,
- **SNMP version** – **v2c** or **v3**,
- **sysDescr**, **sysContact**, **sysName**, **sysLocation** – Optional system identification fields,
- **Read community** – Data read password,
- **Write community** – Data write password.

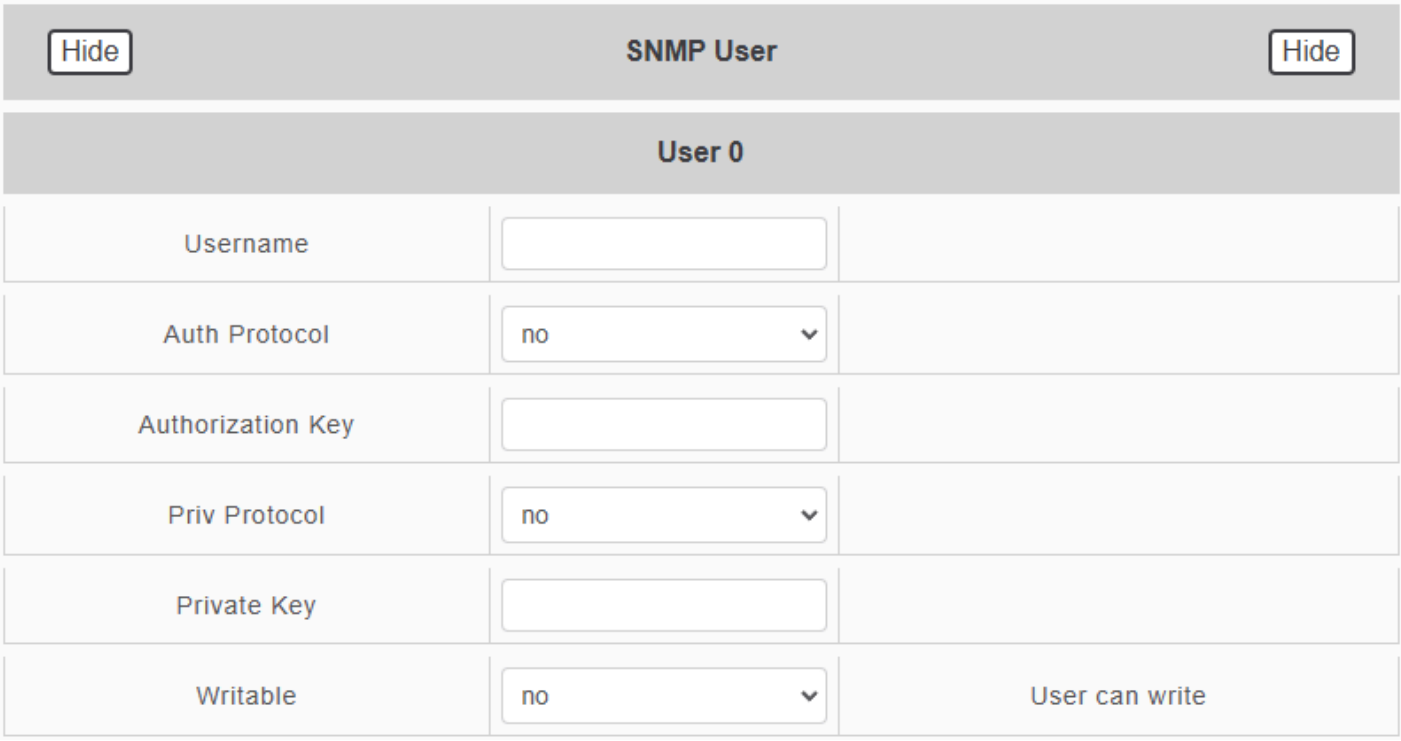


- **Write community** – Data write password,
- **Trap IP** – Address, to which trap messages will be sent.

SNMP v3

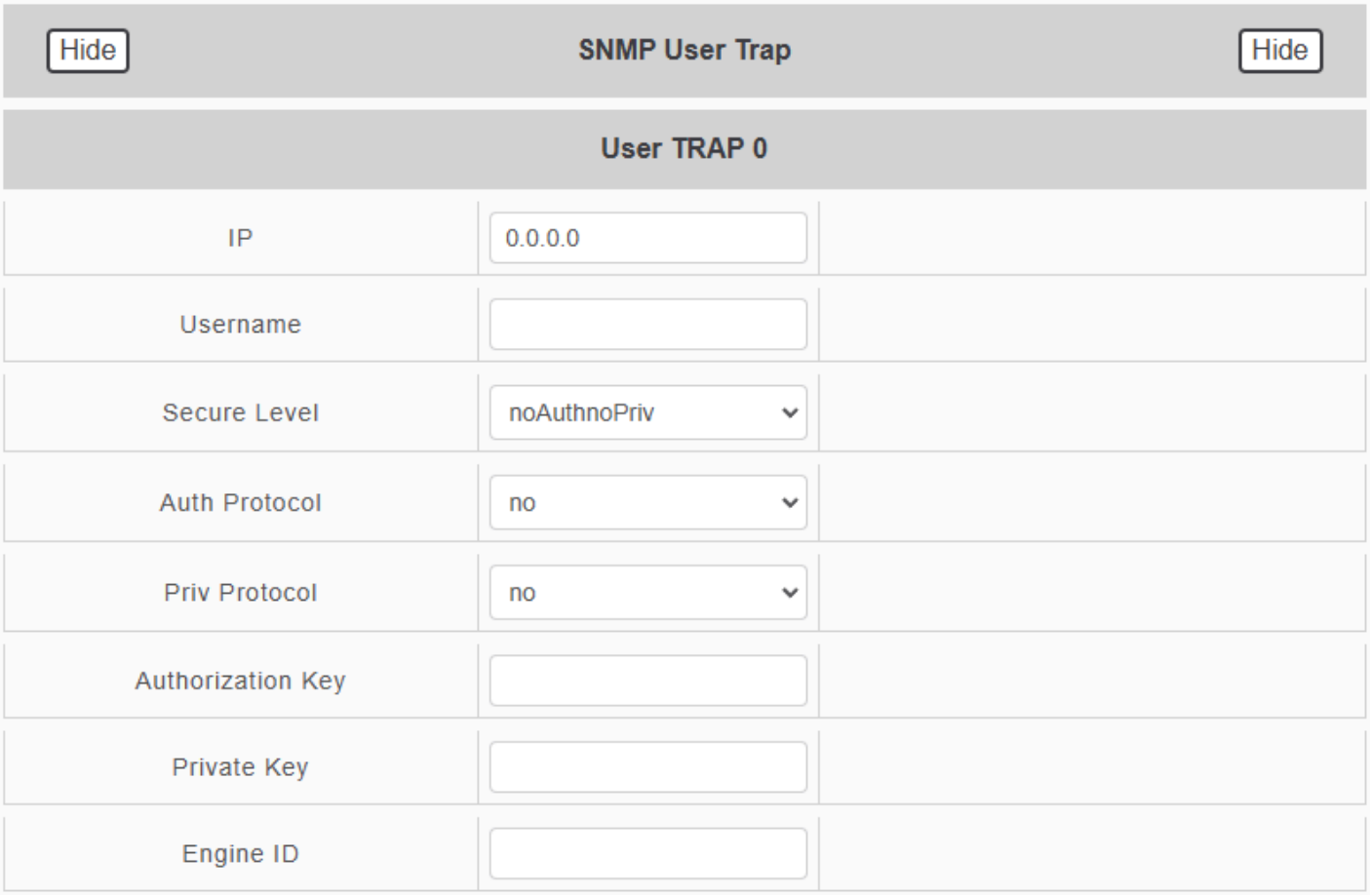


- **Enable** – Enable/disable SNMP service,
- **SNMP version** – **v2c** or **v3**,
- **sysDescr**, **sysContact**, **sysName**, **sysLocation** – Optional system identification fields,
- **EngineId** – Unique device identifier.



Parameters that can be set in this window allow defining of authentication and privacy mechanism for different users.

- **Username**,
- **Secure level** – SNMP v3 security level:
  - **noAuthnoPriv** – SNMPv3 communication is carried out with no security,
  - **authNoPriv** – SNMPv3 communication is authenticated but not encrypted,
  - **authPriv** – SNMPv3 communication is authenticated and encrypted,
- **Auth Protocol**:
  - MD5,
  - SHA.
- **Authorization Key**,
- **Priv Protocol**:
  - DES,
  - AES.
- **Private Key**,
- **Writable** – Assign the user with privilege to send messages to the device.



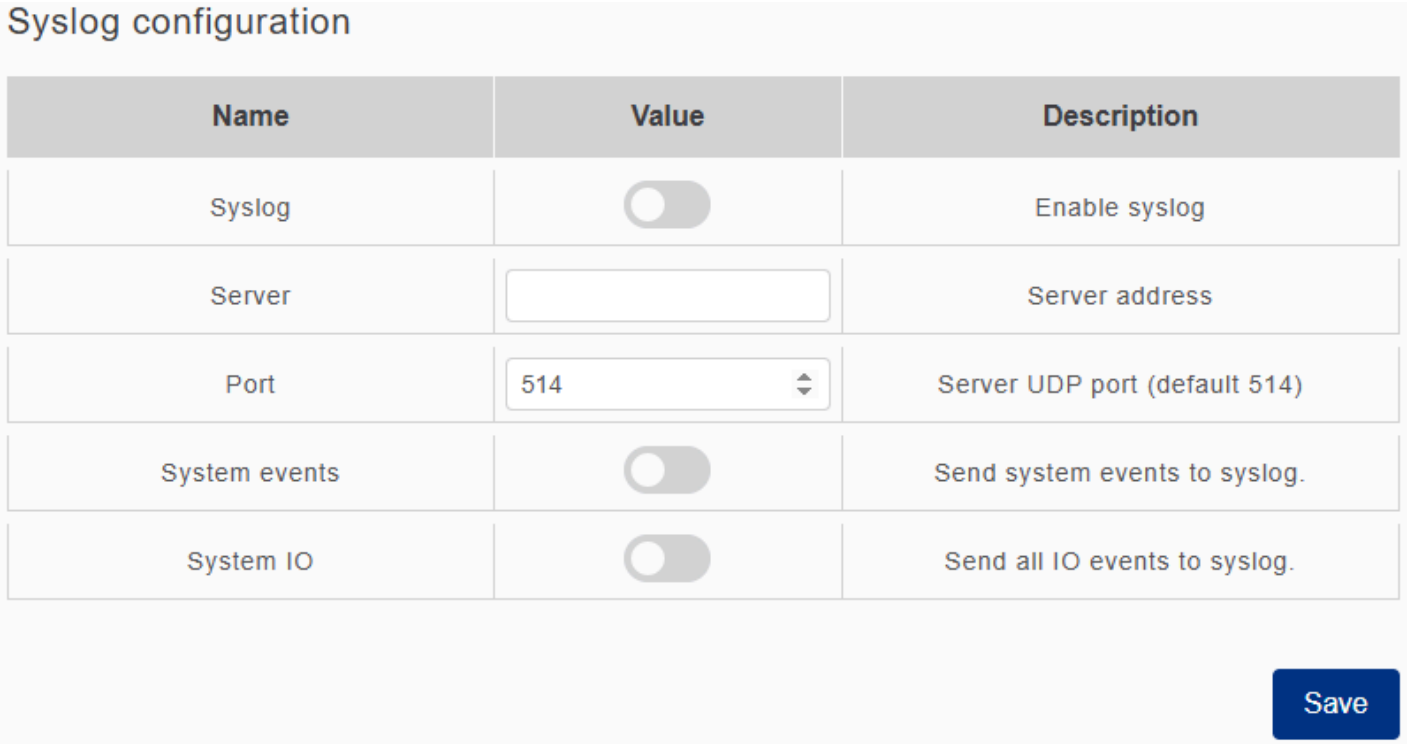
Parameters that can be set in this window apply to specific trap notifications generated for or by the user concerned.

- **IP** – IP address of the device or system generating the trap notification,
- **Username** – SNMPv3 user name,
- **Secure Level** used with SNMPv3:
  - **noAuthnoPriv** – SNMPv3 communication is carried out with no security,
  - **authNoPriv** – SNMPv3 communication is authenticated but not encrypted,
  - **authPriv** – SNMPv3 communication is authenticated and encrypted,
- **Auth Protocol**:
  - MD5,
  - SHA.
- **Authorization Key**,
- **Priv Protocol**:
  - MD5,
  - SHA.
- **Private Key**,
- **Engine ID** – Unique identifier used to represent the SNMPw engine in the device.

Download MIB file – Link to download the MIB file.

Syslog

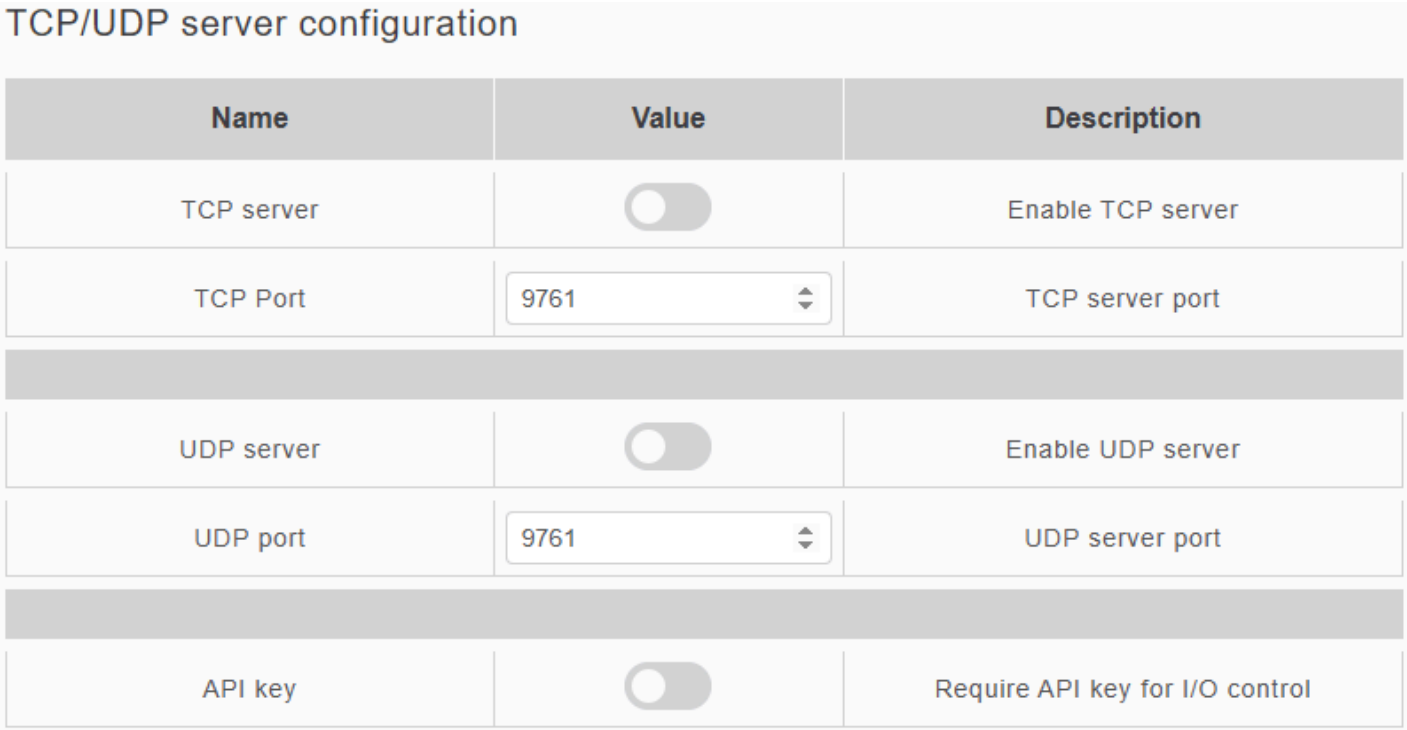
In this section, sending of system logs to a remote syslog server can be configured, making remote diagnostics and device monitoring easier.



- **Enable** – Enable syslog client service,
- **Server** – Syslog server address in the form of IP address or domain name (maximum of 24 characters),
- **Port** – Port number, the syslog server is listening to,
- **System events** – Events related to system operation,
- **Syslog IO**.

TCP/UDP

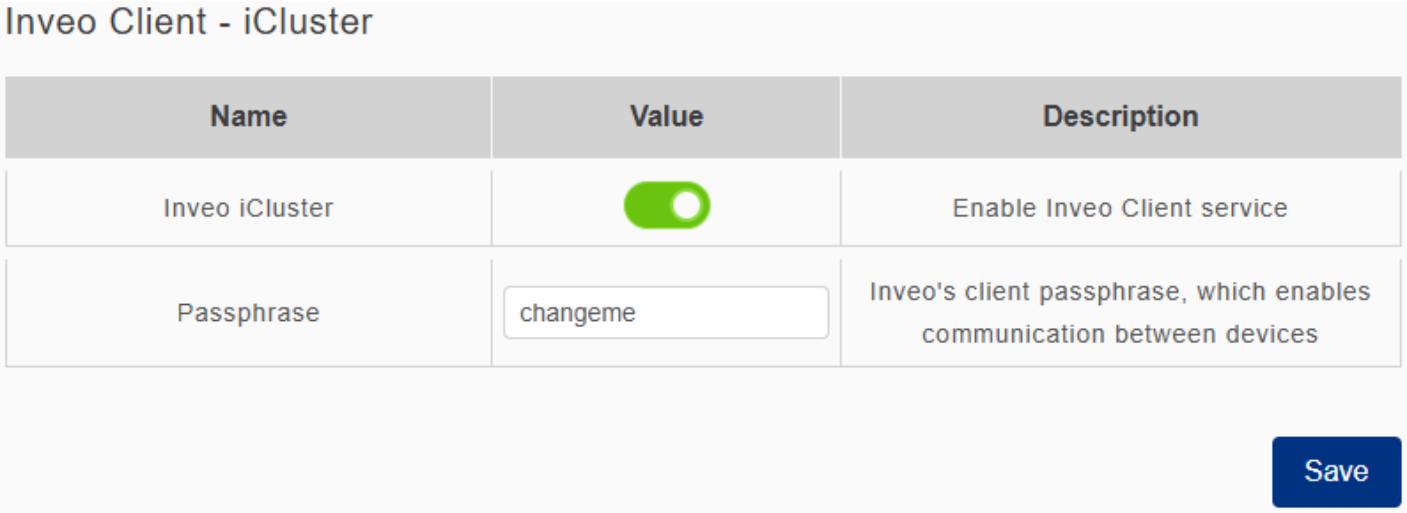
This tab allows the user to enable and configure TCP and UDP protocols support. The user can customize settings such as ports and communication parameters, providing flexibility in device configuration in compliance with network requirements. By sending commands to the device's IP address and port using an appropriate protocol, the user can control the outputs state. Available commands – see **IO commands**.



- **TCP server**,
- **TCP port**,
- **UDP server**,
- **UDP port**,
- **API key** – Enable/disable API key requirement for I/O control.

iCluster

iCluster allows multiple Inveo devices to interconnect within a single LAN. IQIO can operate as an iCluster client, allowing the device to oversee its parameters such as: sensor readings, input/output state, output control etc.



- **Inveo iCluster** – Enable/disable **iCluster** service,
- **Passphrase** – Password used by the Inveo client that allows communication between devices. The password set here will be required in the device that would like to establish a connection with a Daxi device.

IO commands

Shown below is the summary of commands used to create actions based upon IO commands. It is worth noting that those commands are useful when using different protocols such as HTTP, MQTT, UDP and TCP too.

- `in_cnt=ch,val` – set the `ch` channel counter value to `val`,
- `out_on=ch` – activate output channel `ch`,
- `out_off=ch` – deactivate output `ch`,
- `out_inv=ch` – output `ch` state invert,
- `out_blink=ch,ton,toff,cnt` – periodic output `ch` control. Parameters:
  - `ton` – activation time (in seconds),
  - `toff` – deactivation time (in seconds),
  - `cnt` – number of activation cycles (not required).
- `out_time=ch,ton,toff` – activate output `ch` for the time defined in `ton`, after `toff` time passes. The `toff` parameter is not required – omitting it will activate the output without a delay,
- `out_all=10n-11100` – command defining the state of all available outputs. Each digit represents a subsequent output:
  - `1` – activated,
  - `0` – deactivated,
  - `n` – state invert,
  - `-` – no state change.

Example

`out_all=10n-1110` will activate outputs No. 0, 4, 5, 6; deactivate outputs 1 and 7; invert the state of 2; leave output No. 3 with no changes.

The commands can be joined together using **&**.

Example

```
out_on=2&out_inv=3&out_time=1,20,20
```

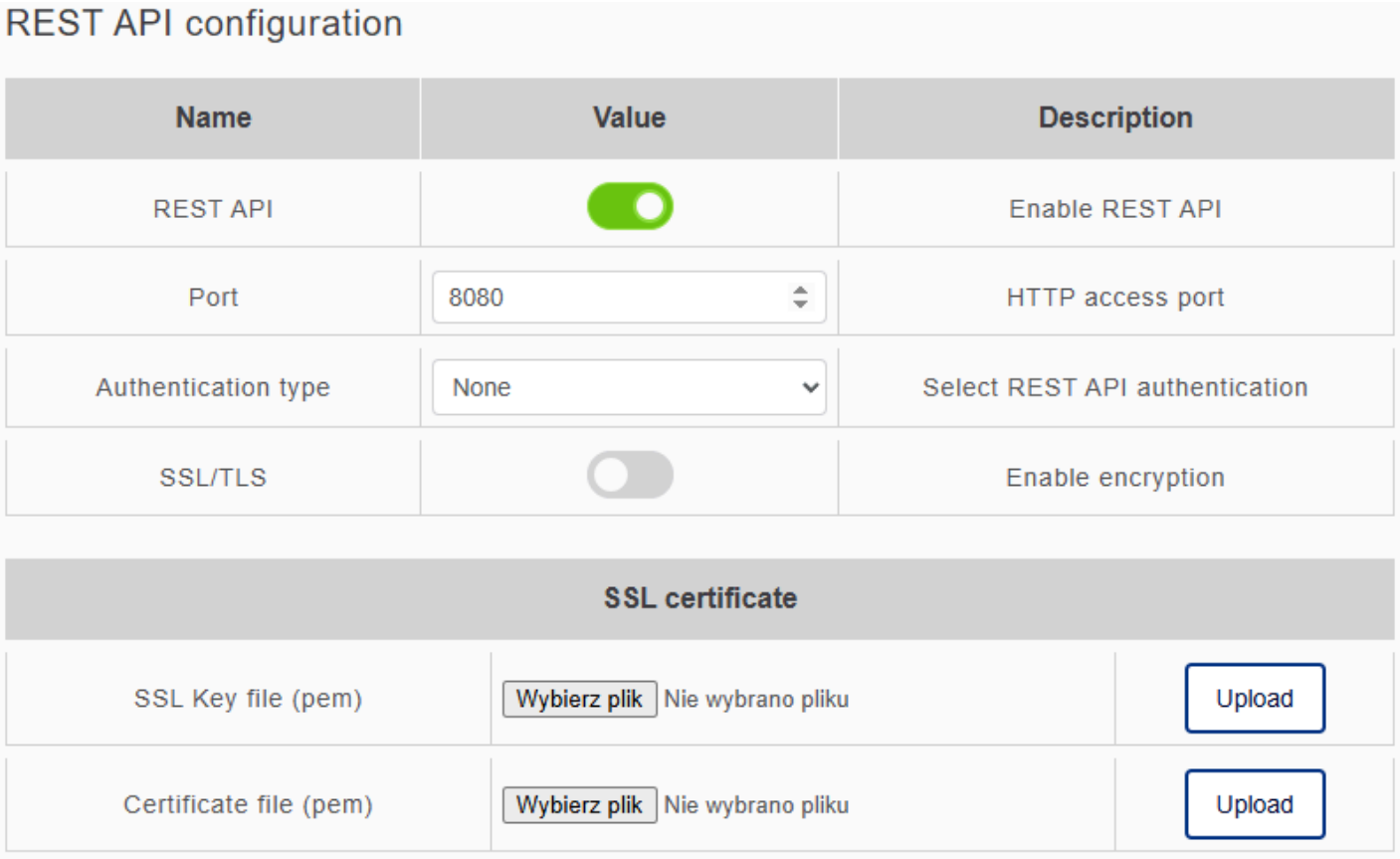
Built-in variables

The following table contains example internal variables that allow for precise transfer of module operation data. Those variables are key elements in configuration, e-mail and SMS notifications, HTTP Client etc.

Syntax	Example	Description
`%out[range],[off],[on]%`	`%out[0-5],0,1%`	Outputs state [range] is the range of outputs to be displayed [off] is the value for inactive state [on] is the value for active state Example: state of OUT 0-5 will be displayed. 0 - inactive 1 - active
`%in[range],[off],[on]%`	`%in[0-7],i,I%`	Inputs state [range] is the range of inputs to be displayed [off] is the value for inactive state [on] is the value for active state Example: state of IN 0-7 will be displayed. 0 - inactive 1 - active
`%cnt[number]%`	`%cnt5%`	Input counter value [number] is the input number Example: counter value of input No. 5 will be displayed
`%sens[number]%`	`%sens10%`	Sensor value [number] is the sensor number Example: sensor No. 10 value will be displayed
`%sunrise%`	`%sunrise%`	Sunrise hour
`%sunset%`	`%sunset%`	Sunset hour
`%time%`	`%time%`	Current time
`%date%`	`%date%`	Current date
`%timedate%`	`%timedate%`	Current time and date
`%ts%`		Current timestamp – number of seconds since the specified date: 1st of January 1970
`%mod_name%`		Module name defined by the user
`%mod_model%`		Device model
`%eip%`		Device's IP address
`%emac%`		Device's MAC address

`%s[x]%`	`%s[3]%`	Sensor value Example: sensor No. 3 value will be displayed
`%s[x].statTxt`	`%s[2].statTxt`	Sensor status Example: sensor No. 2 status will be displayed
`%o[x]%`	`%o[4]%`	Output state Example: state of output No. 4 will be displayed
`%i[x]%`	`%i[1]%`	Input state Example: state of input No. 1 will be displayed
`%v[x]%`	`%v1%`	Virtual variable value
`%cnt[x]%`	`%cnt1%`	Input counter value

REST API



- **REST API** – Enable REST API,
- **Port**,
- **Authentication type**:
  - **None**,
  - **Basic authentication** – User name and password authentication,

    - **API KEY** – API key authentication, utilizing a key generated in **Administration / Access**. The key should be entered as a parameter, preceded with `apikey=`.
- **User** – User name used with Basic authentication,
- **Password** – Password used with Basic authentication,
- **SSL/TLS** – Enable/disable encryption.
- **SSL Key file (pem)** – Allows upload of SSL key (pem format),
- **Certificate file (pem)** – Allows upload of certificate file (pem format).

Example

API key value: `12345678901234567890`
REST API request syntax: `http://<IP_address>:<port>/io/outputs/1?apikey=12345678901234567890`

Application examples

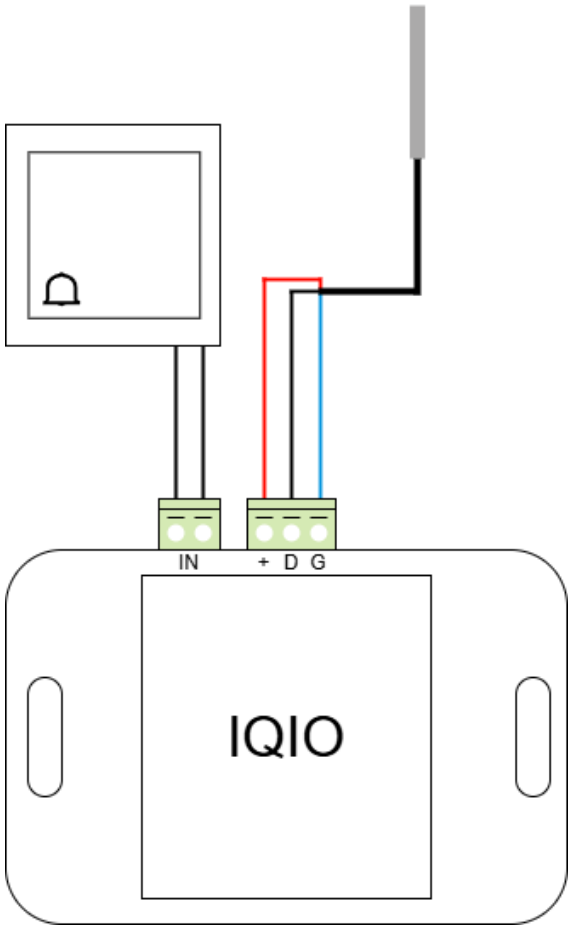
Example 1: Notifying about sensor, input, and system state

Objective: Sending sensor and input status, system messages to the MQTT broker in the form of notifications.

Implementation instructions:

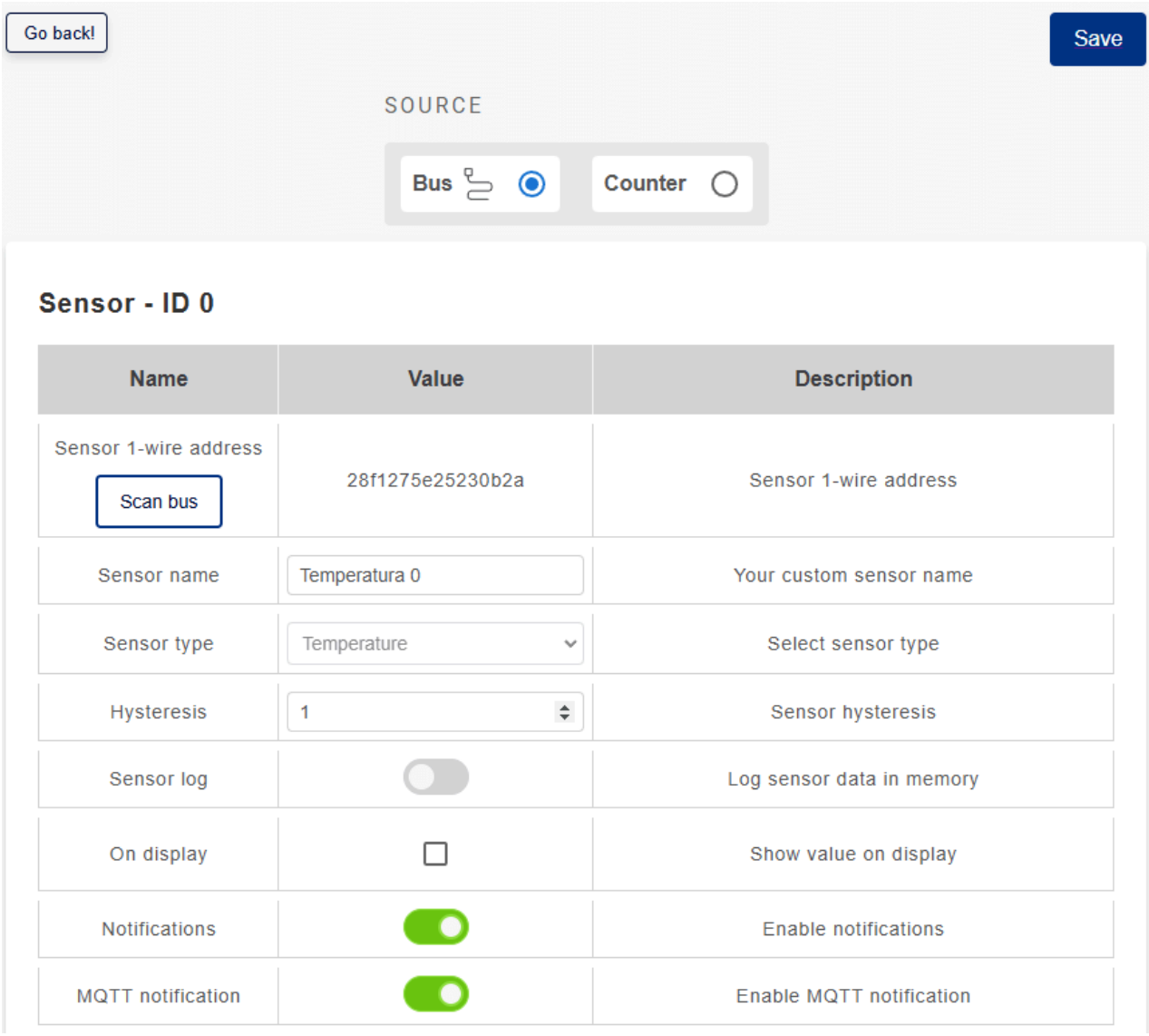
1. Connect the sensors and input devices

- Make sure that all sensors and inputs are connected to IQIO correctly.
- For the purpose of this demonstration, we will connect a temperature sensor and a momentary switch to the device:



2. Sensor configuration

- In the IQIO PRO control panel go to the **Sensors / All** tab,
- Click **+**,
- In the sensor's configuration window, click **Scan bus**, then select the appropriate sensor with **Assign**,
- Change the sensor's name, set a hysteresis, data logging, and content display if needed,
- Make sure that **Notifications** and **MQTT notification** are enabled.

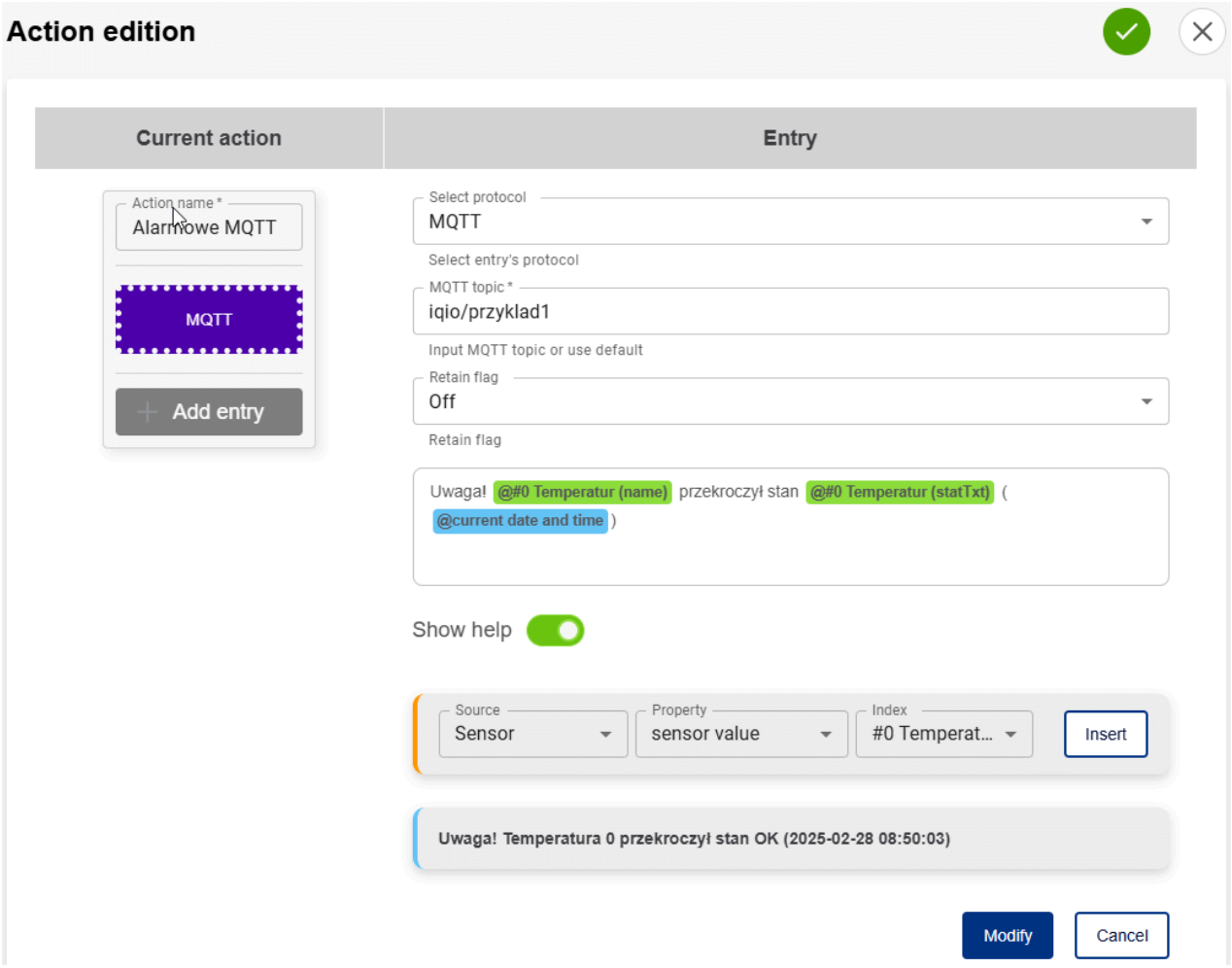


Tip

After making changes, apply them using the Save button.

3. Warning and alarm thresholds configuration

- In **Actions / All**, click **Add a new action**,
- In the **Create a new action** window, enter the action name and click **Add entry**,
- Select a communication protocol (**MQTT** in this case),
- In the **MQTT topic** field, input the topic that the notifications will be sent to,
- In the syntax field, enter the command that will be sent to the broker.



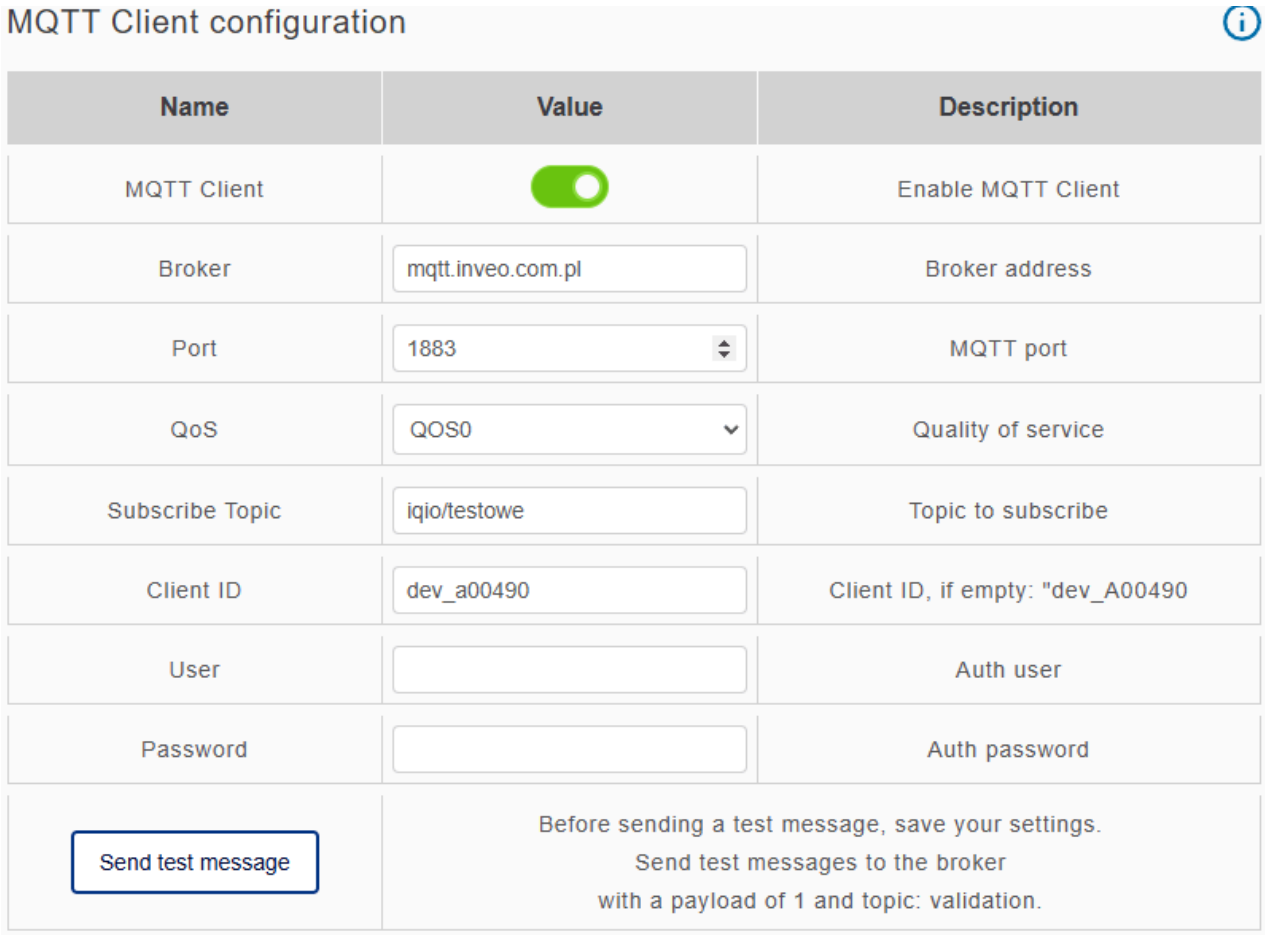
- In the **Actions / System** tab, assign the **Power up** action, that will send device power-up information to the broker.
  In the message contents, the following can be included: `Module power connected @current date and time.`

Tip

After making changes, apply them using the Save button.

4. MQTT client configuration

- Select **MQTT Client** in the **Services / MQTT** tab,
- Input the broker's address (for the Inveo broker - `mqtt.inveo.com.pl`), port, set **QOS**,
- Enter the topic IQIO will subscribe to,
- If needed, input the access data: **User** name and **Password**, set the encryption parameters and/or LWT message parameters,
- Send a test message using **Send test message** to verify the data and test the connection. A message with a payload of **1** will be sent to the **validation** topic.



Tip

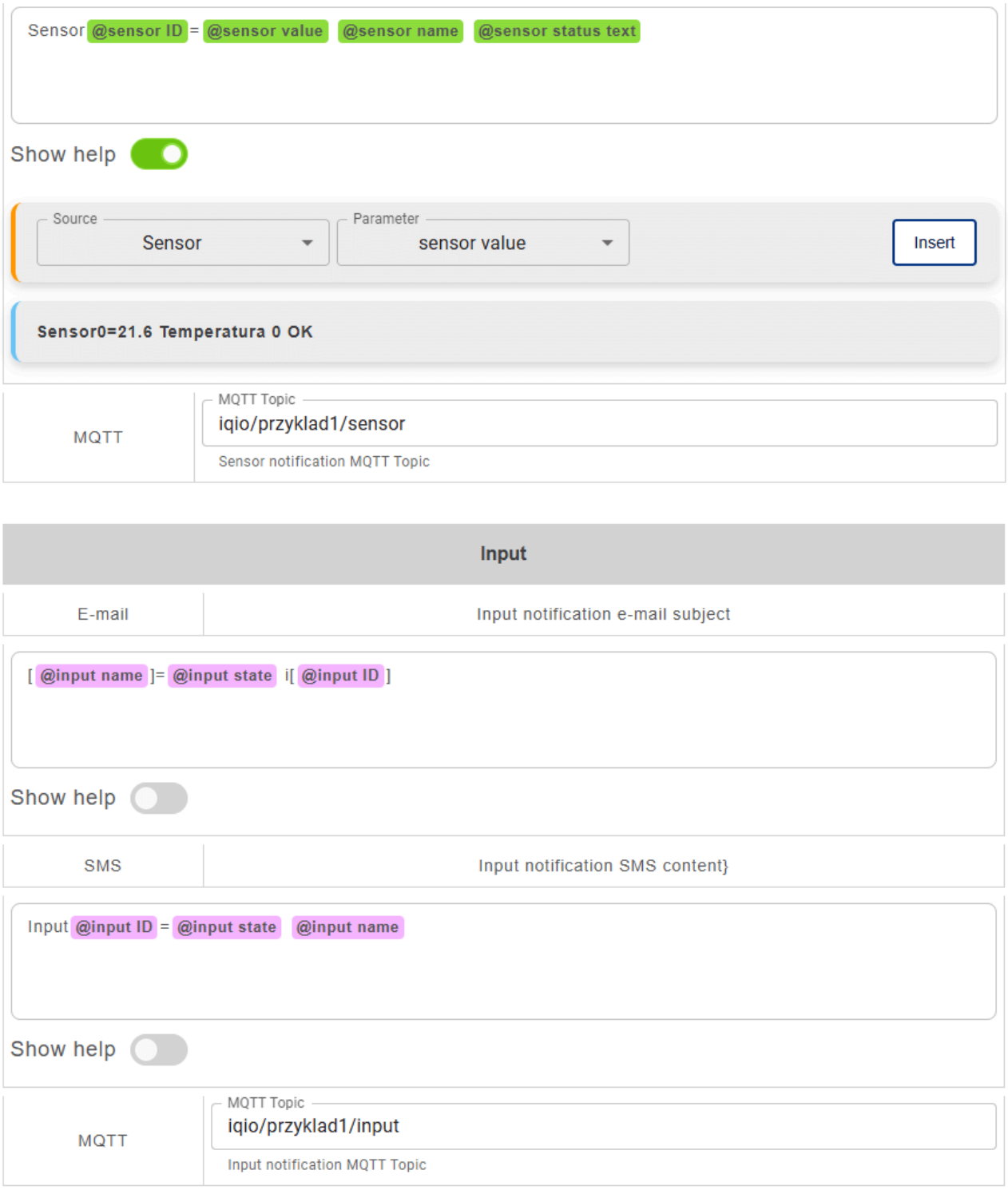
After moving the cursor over the i icon in the upper-right part of the window, a broker connection status will be displayed. Successful connection is indicated by MQTT Broker connection state: Connected.

Tip

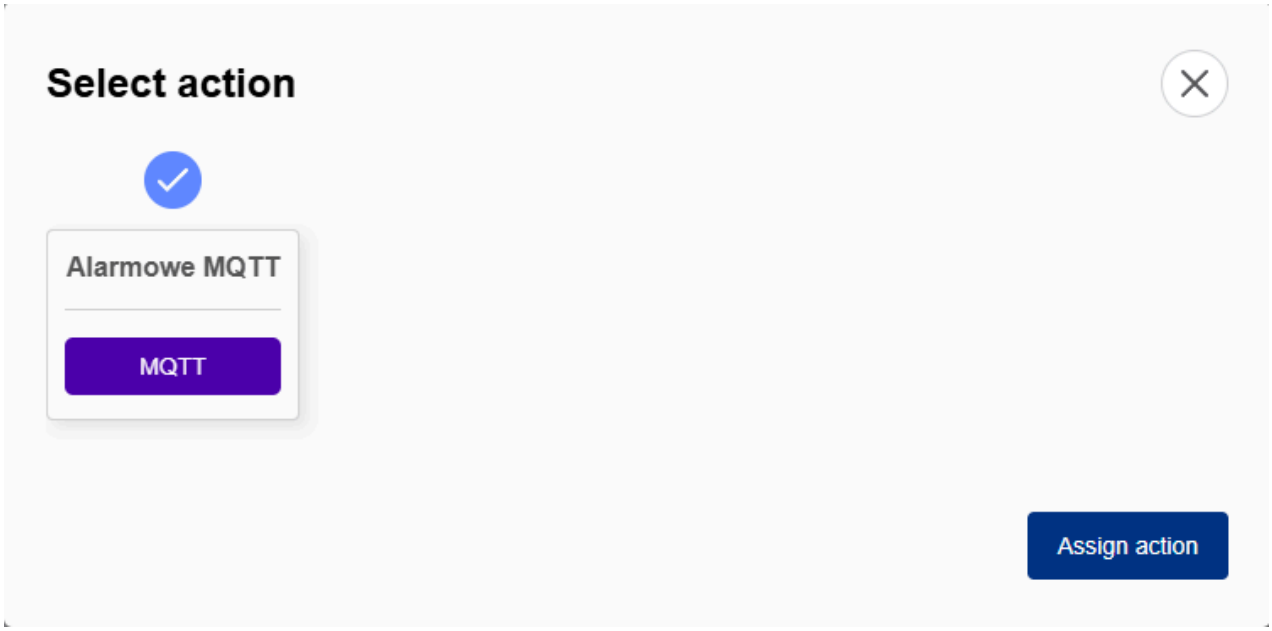
After making changes, apply them using the Save button.

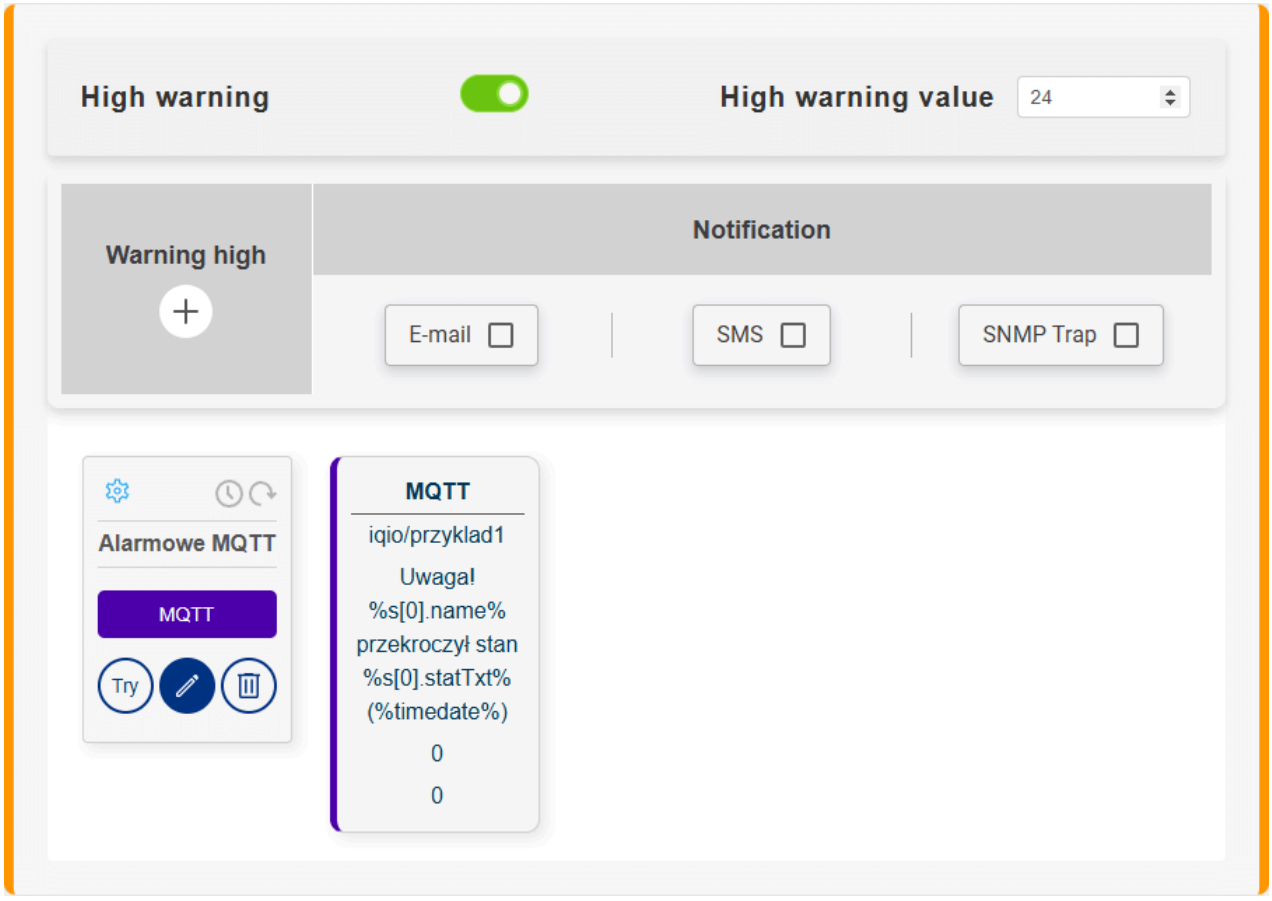
5. Notifications configuration

- In the **Notifications / Configuration** tab, enable **Notification**. Change the **MQTT info** and/or **MQTT Retain** fields if required,
- In the **Sensor** and **Input** sections, notification contents and topic can be defined.

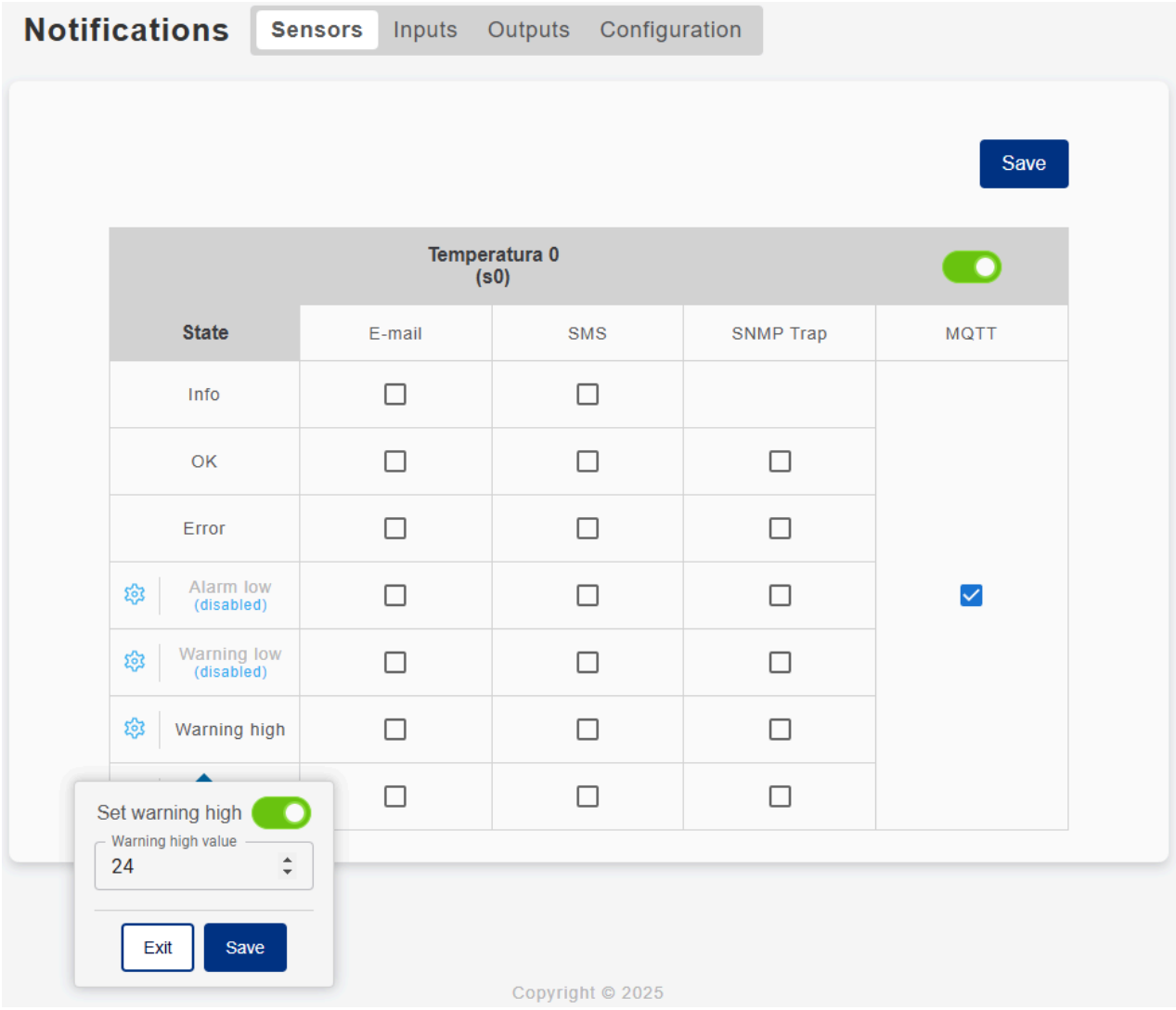


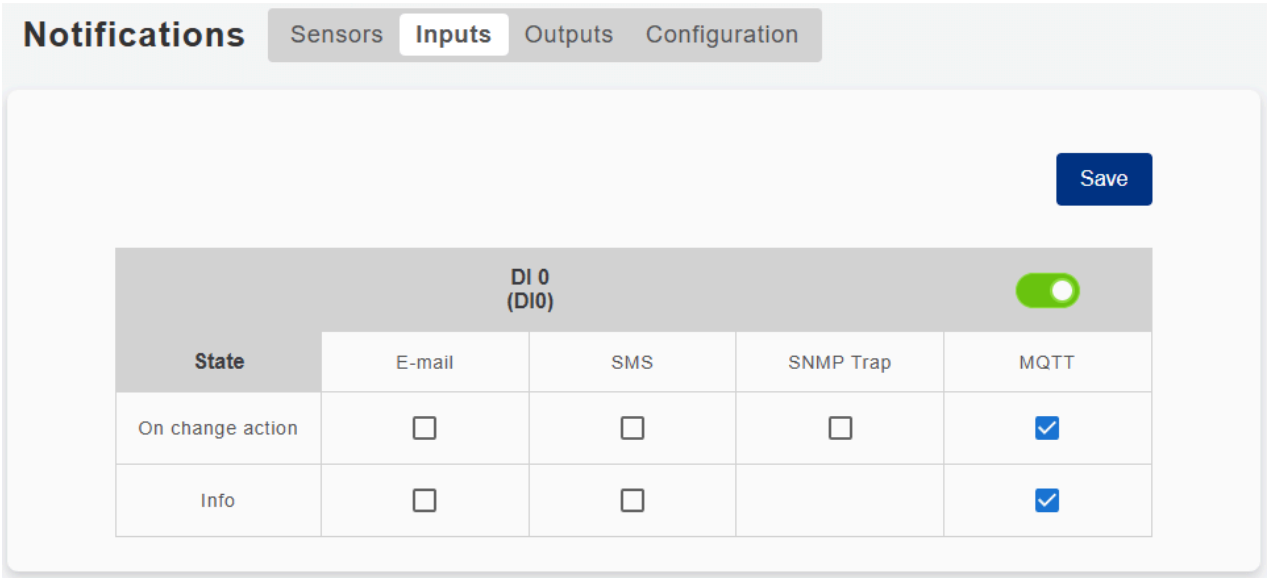
- After selecting the sensor in **Sensors / All**, activate the chosen notification options (eg. high warning and high alarm), assign an action and enter a value that will trigger it.





- In **Notifications / Sensors/Inputs**, enable selected sensors/inputs and enable **MQTT** next to the reqired fields in the table,
- Set the selected warnings/alarms by clicking the gear icon and activating them with a slider control.





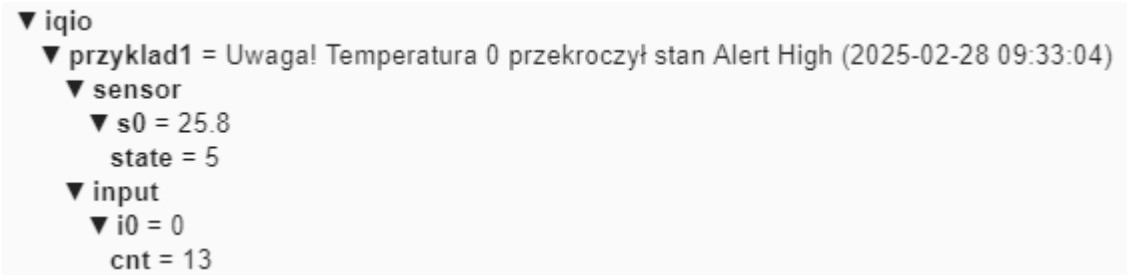
Tip

After making changes, apply them using the Save button.

Test the configuration:

Using an appropriate programme (eg. MQTT Explorer) make sure that the defined notifications are reaching the broker.

If configuration was successful, the following data should be displayed in the window:



- **example1** = ... – In this topic, system messages regarding exceeded warning/alarm thresholds and device's power status will be published with the date and time of the event,
- **sensor > s0** = ... – Value read from the s0 sensor, temperature in this case,
- **input > i0** = ... – Input i0 state: **0** - deactivated, **1** - activated,
- **cnt** = ... – Input counter, in this configuration, each press of the button will increment the counter's value by 1.

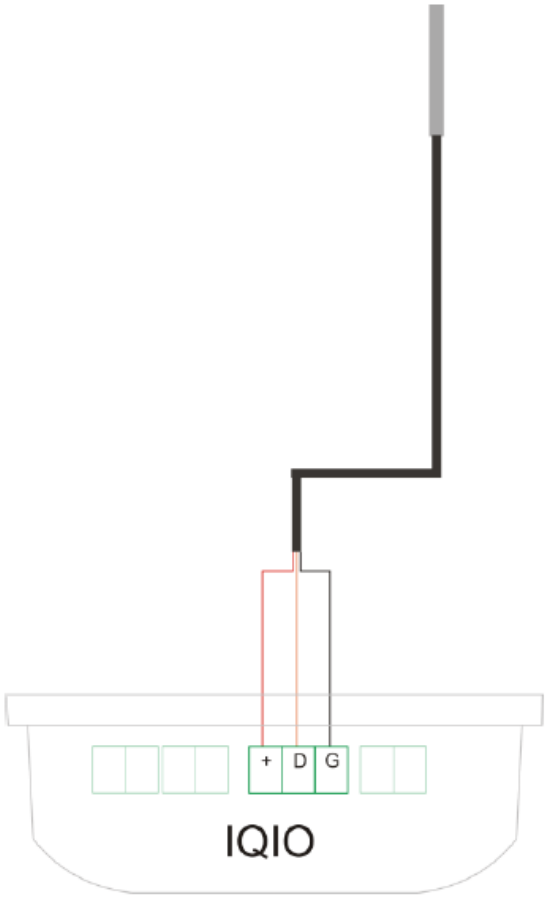
Example 2: Notifying about sensor state via e-mail

Objective: Sending information about exceeded warning/alarm thresholds, normal and sensor error states in the form of e-mail messages.

Implementation instructions:

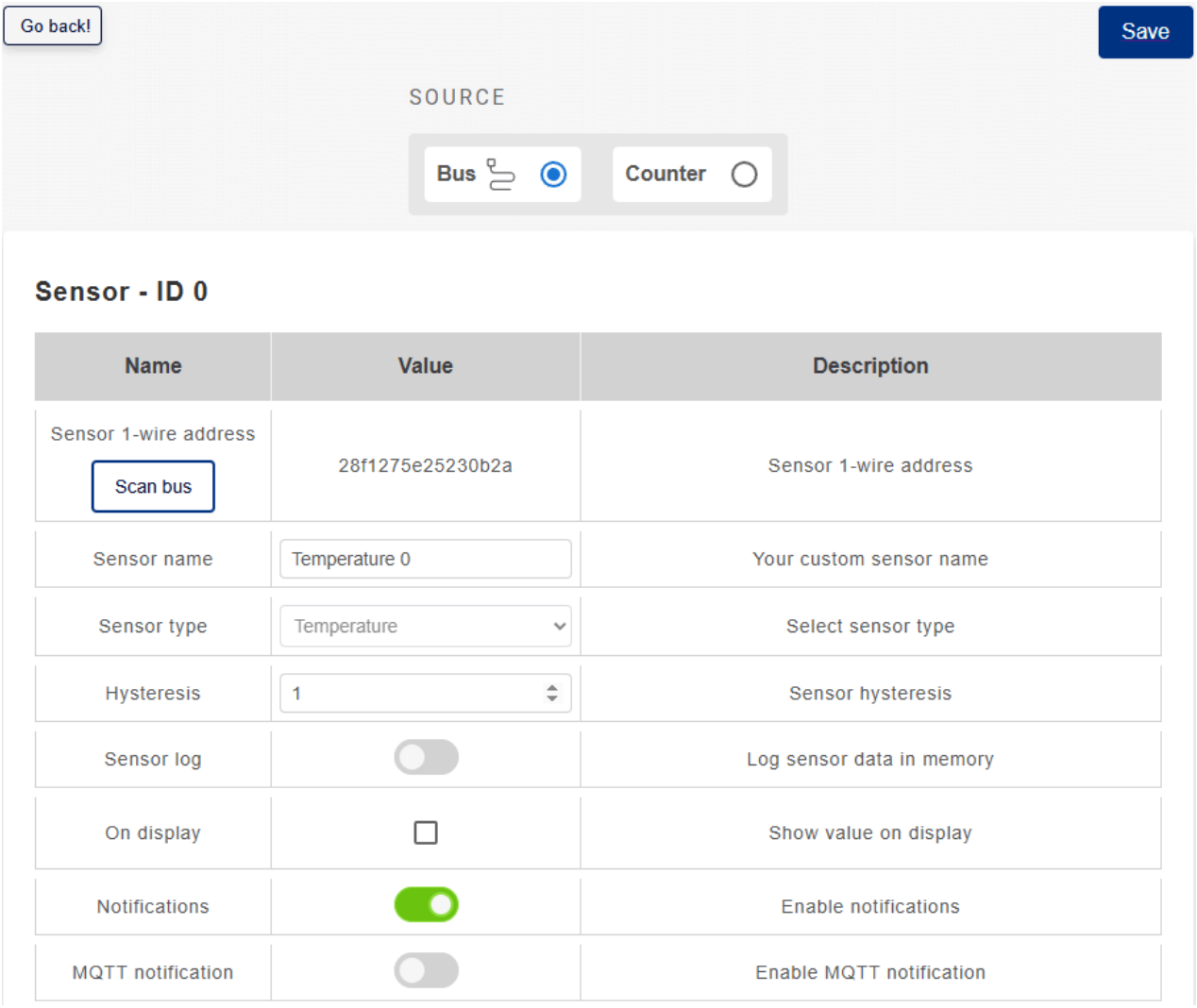
1. Connect the sensors and input devices

- Make sure that all sensors and inputs are connected to IQIO correctly,
- For the purpose of this demonstration, we will connect a temperature sensor to the device:



2. Sensors configuration

- In the IQIO PRO control panel go to the **Sensors / All** tab,
- Click **+**,
- In the sensor's configuration window, click **Scan bus**, then select the appropriate sensor with **Assign**,
- Change the sensor's name, set a hysteresis, data logging, and content display if needed,
- Make sure that **Notifications** is enabled.

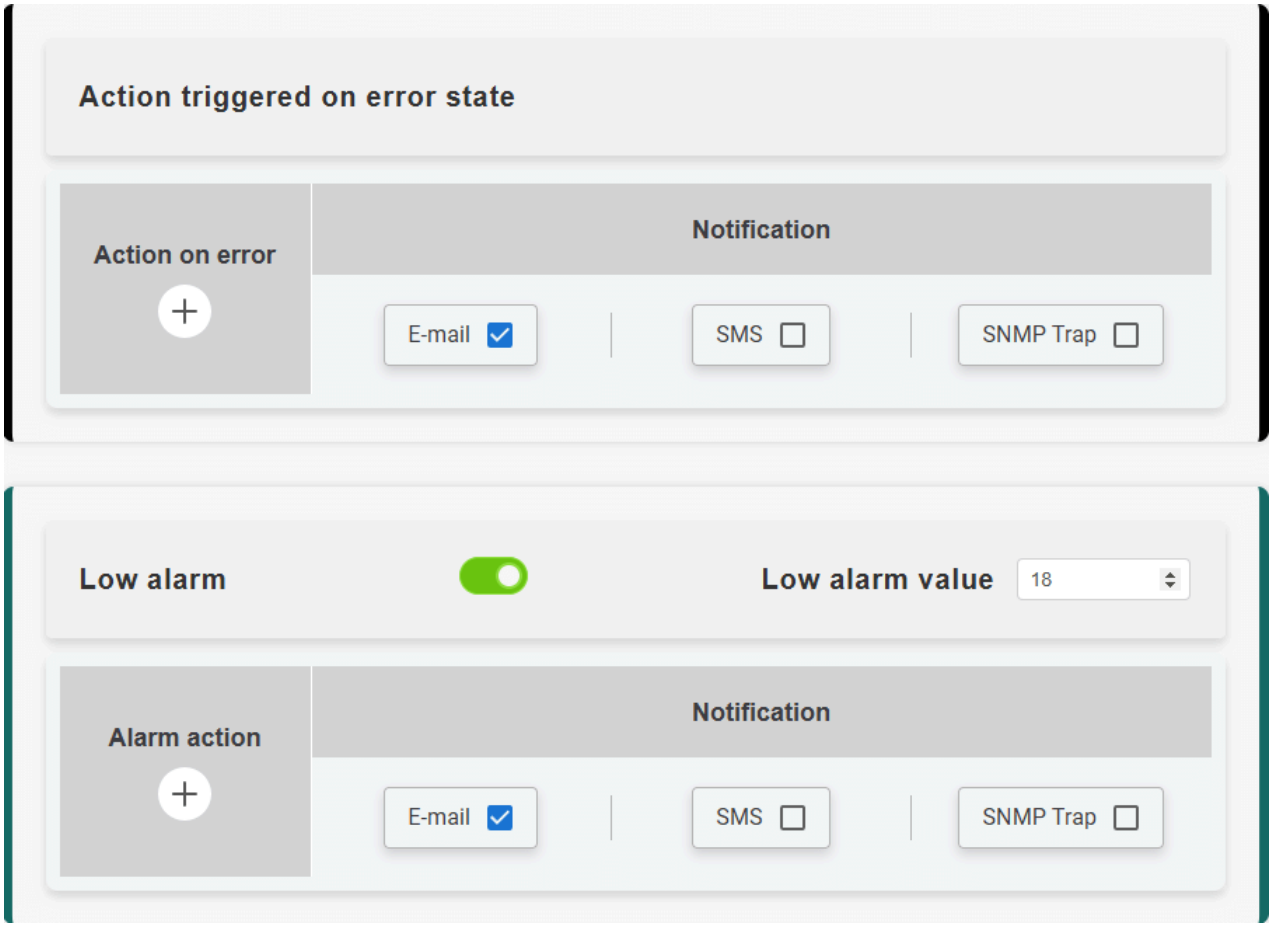


Tip

After making changes, apply them using the Save button.

3. Warning and alarm thresholds configuration

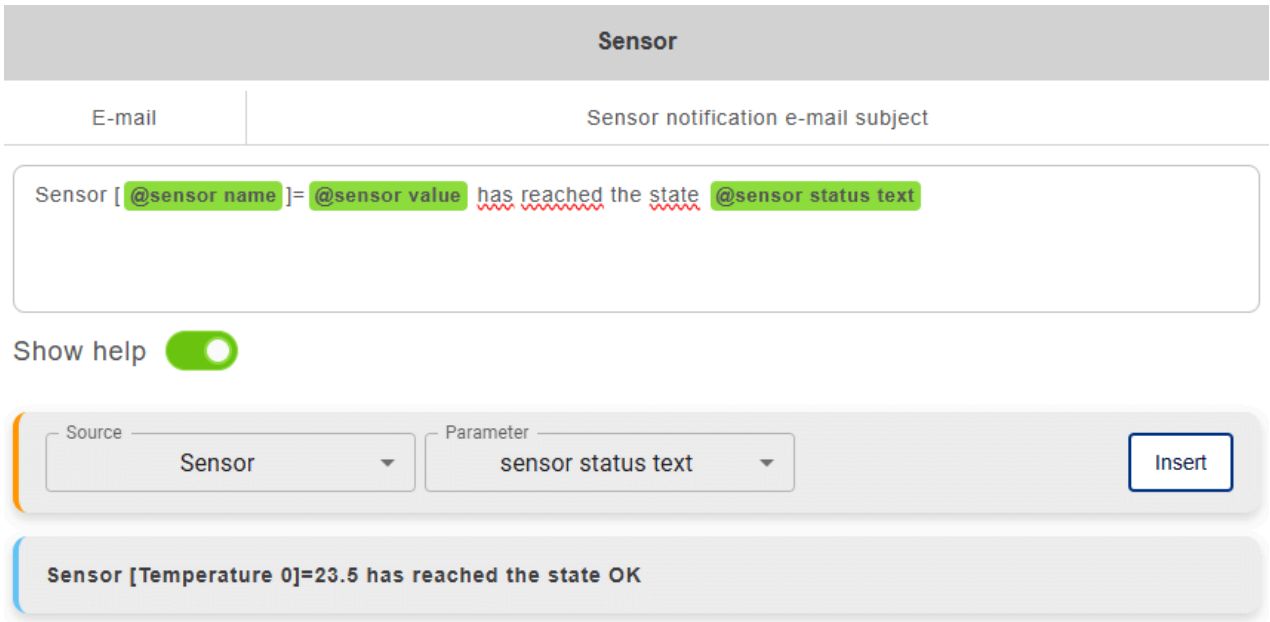
- In the sensor's configuration window, activate the chosen notification options (eg. high warning and high alarm), assign an action and enter a value that will trigger it,
- Select **E-mail** next to the action that will send the e-mail message. For the purpose of this demonstration, we will select **E-mail** next to all available actions.



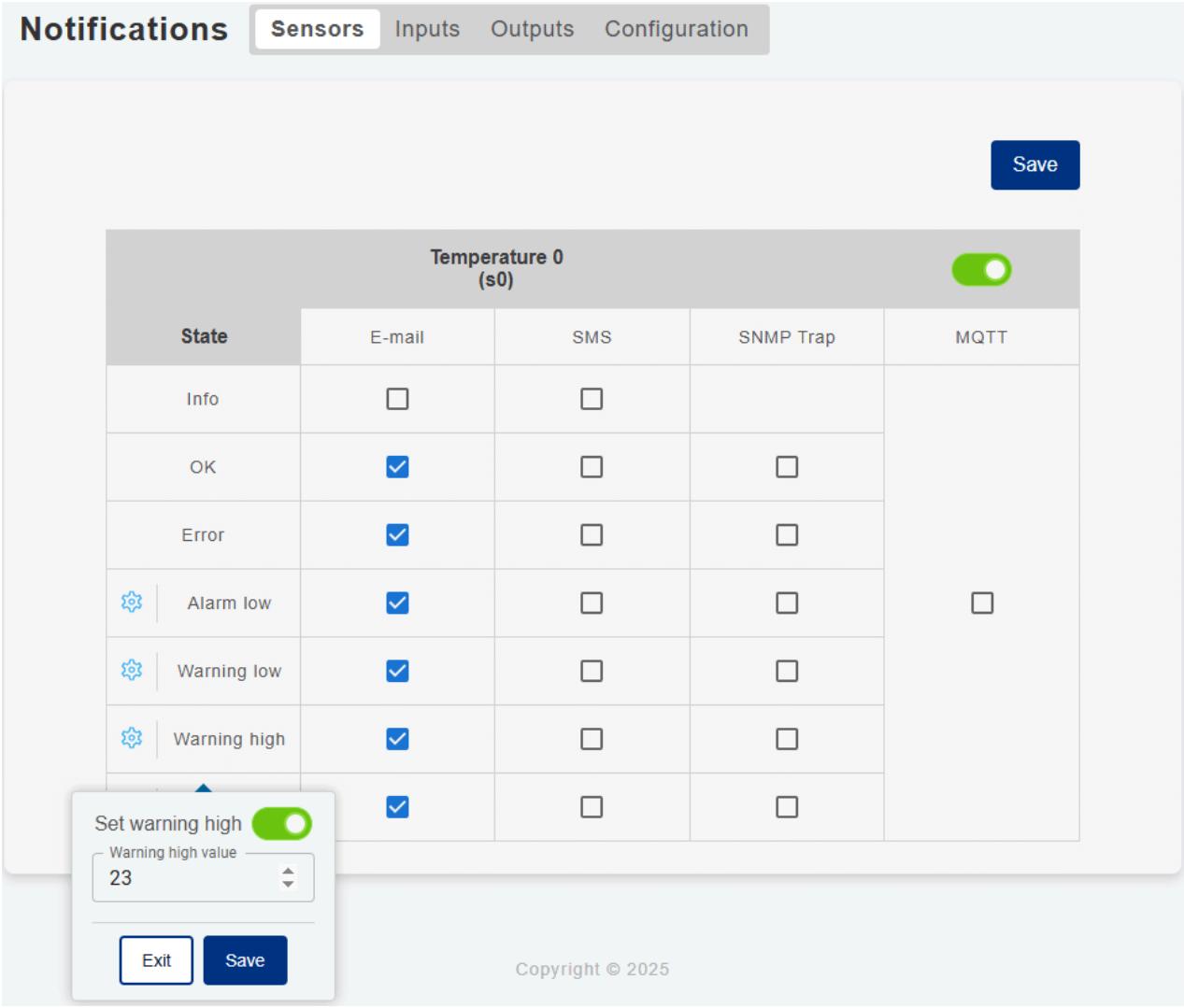
> **Tip**
>
> **After making changes, apply them using the Save button.**

4. Notifications configuration

- In the **Notifications / Configuration** tab, enable the **Notification** option. Change **E-mail info** if needed,
- In the **Sensor** section, message contents can be defined:



- In **Notifications / Sensors**, enable the selected sensors and select **E-mail** next to the reqired fields in the table,
- Set the selected warnings/alarms by clicking the gear icon and activating them with a slider control.



Tip

After making changes, apply them using the Save button.

4. E-mail client configuration

Information

The configuration options shown in this demonstration apply to the SMTP server provided by Gmail. Configuration can differ depending on the e-mail service provider.

- In **Services / E-mail**, select **E-mail**,
- Type the SMTP server address into the **Server** field (`smtp.gmail.com`), port (**465**),
- Set the **SSL** encryption method in the **SSL/TLS** field,
- Enter the username or e-mail address, the messages will be sent from, into the **User** field,

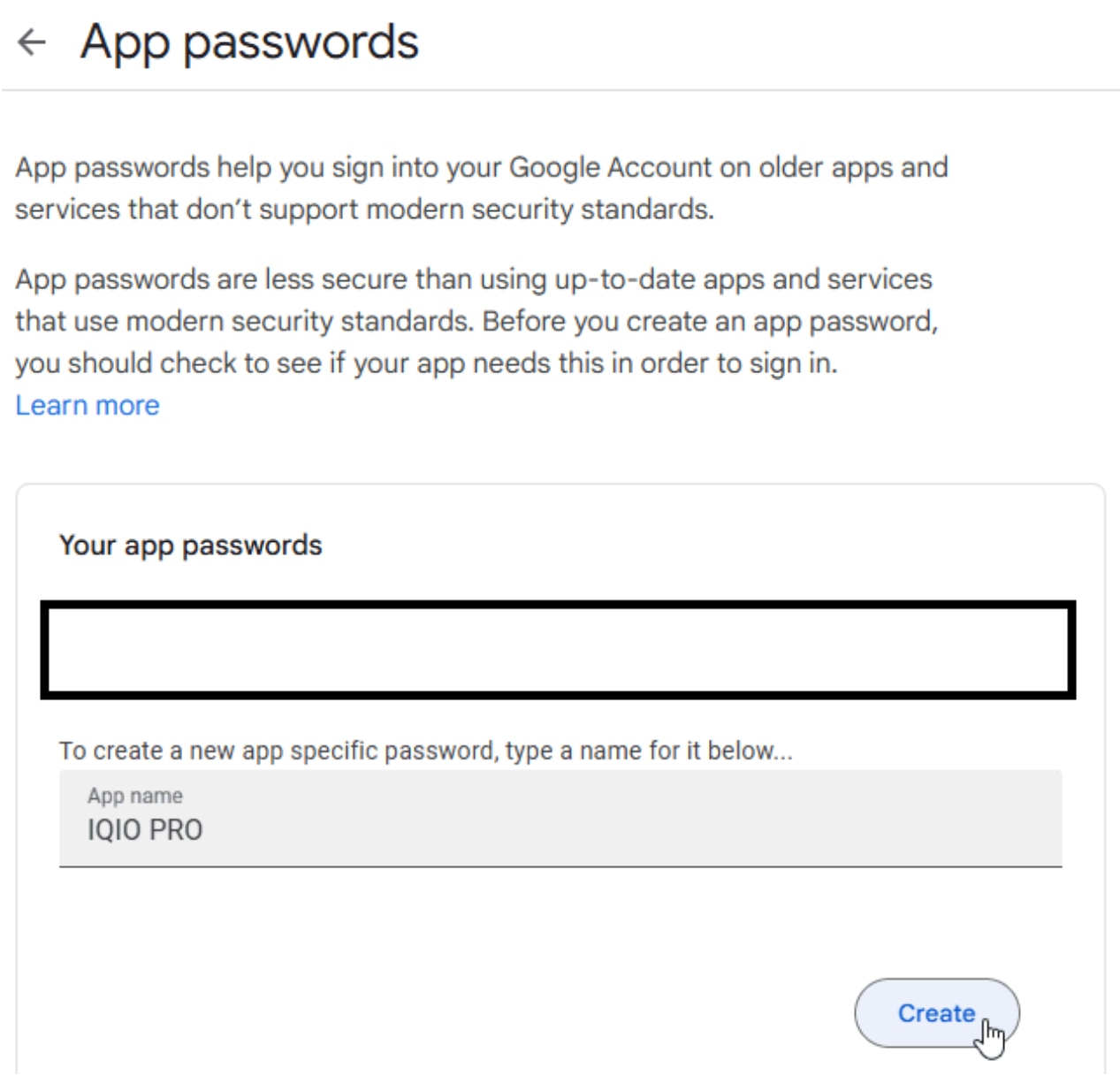
- Choose the authorization method **None** or **Plain**,
- Enter the **Password**, that can be obtained as follows:
- Log in to your Gmail account,
- Clicking your profile picture, select **Manage your Google Account**:



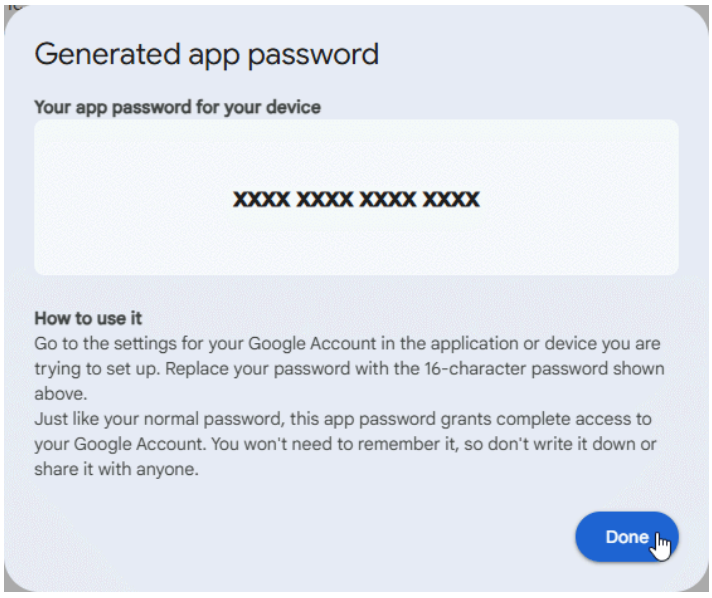
- Go to the **Security** section,
- In the **Search Google Account**, type **app passwords** and click the first link:



- Enter your account's password and confirm,
- Type a name (eg. **IQIO PRO**) into the **App name** field and click **Create**



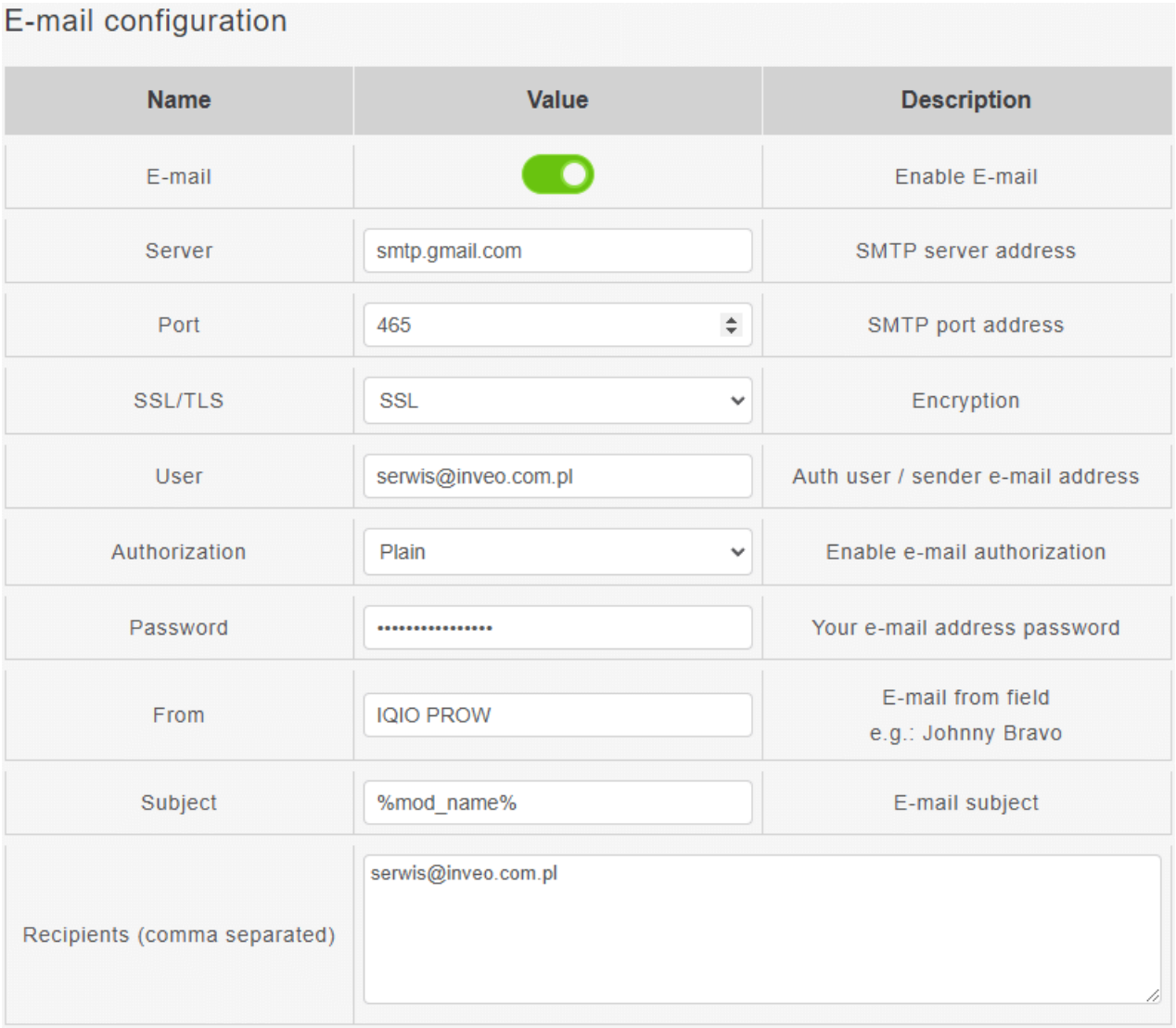
- A window will be shown containing the generated application password. Copy, and paste it into the **Password** field in the IQIO configuration panel:



- A name that will display as the message sender can be entered into the **From** field,

- **Subject** allows the user to change the message subject,
- Enter the message recipients into the **Recipients (comma separated)** field. Consecutive addresses should be separated with commas.

After all required data is inputted, a test e-mail message can be sent using **Send a test e-mail**.
If configuration was successful, all addresses from the **Recipients** field should receive a message titled **Test e-mail topic**.



Tip

Save all changes before sending the test message.

Test the configuration:

If configuration was successful, all declared recipients should receive the e-mail message when any warning/alarm threshold is exceeded or after the normal or error state has been reached.

Sensor [Temperature 0]=24.9 has reached the state Warning High Odebrane ×

Utwórz podsumowanie tego e-maila

IQIO PRO <serwis@inveo.com.pl>
do mnie

Notification sent from IQIO device [your_module_name].
Designed and developed by Inveo (www.inveo.com.pl).

Odpowiedz Przekaż dalej

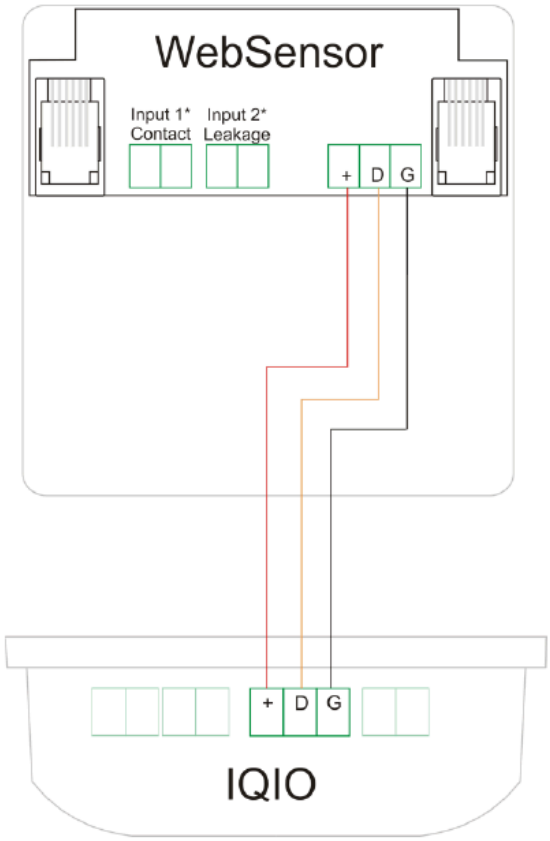
Example 3: Advanced MQTT notifications configuration

Objective: Send the measured value from multiple sensors to different topics via MQTT protocol. Notify about exceeded warning/alarm thresholds to a common topic.

Implementation instructions:

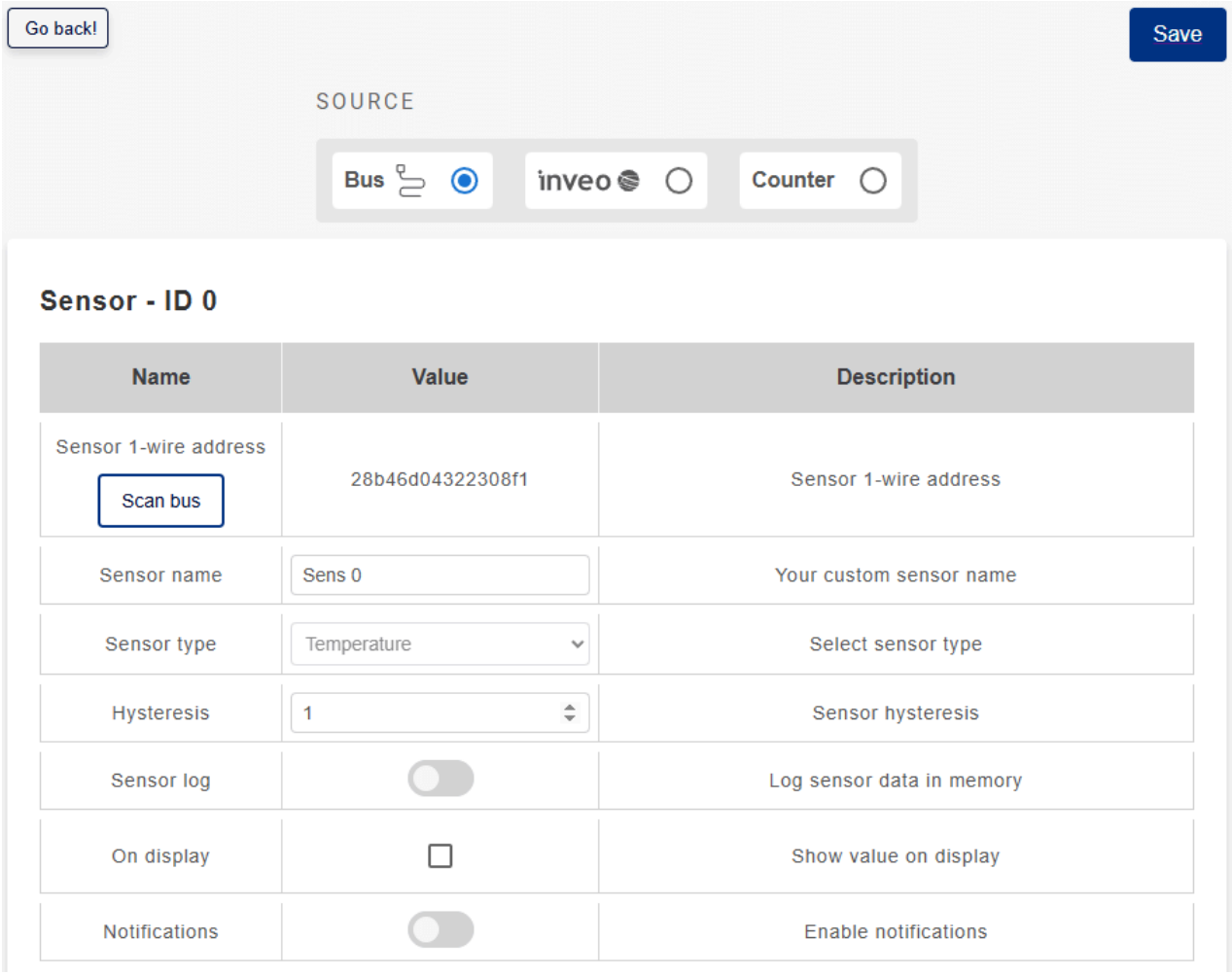
1. Connect the sensors and input devices

- Make sure that all sensors and inputs are connected to IQIO correctly,
- For the purpose of this demonstration, we will connect a WebSensor Combo (temperature and humidity measurement, Contact and Leakage digital inputs):



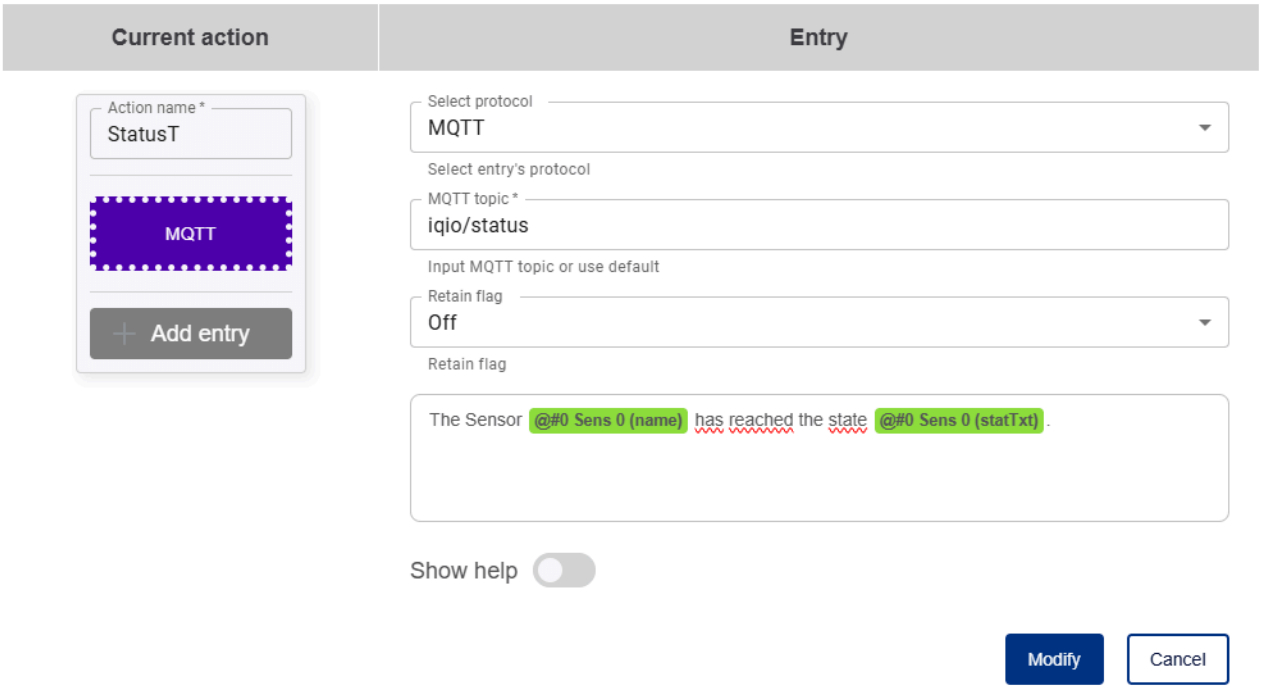
2. Sensors configuration

- Go to the **Sensors / All** tab in the IQIO's control panel,
- Click **+**,
- In the sensor's configuration window, click **Scan bus**, then select the appropriate sensor with **Assign**,
- Change the sensor's name, set a hysteresis, data logging, and content display if needed,
- Repeat the instructions for every sensor. In this example, we assign temperature and humidity sensors.

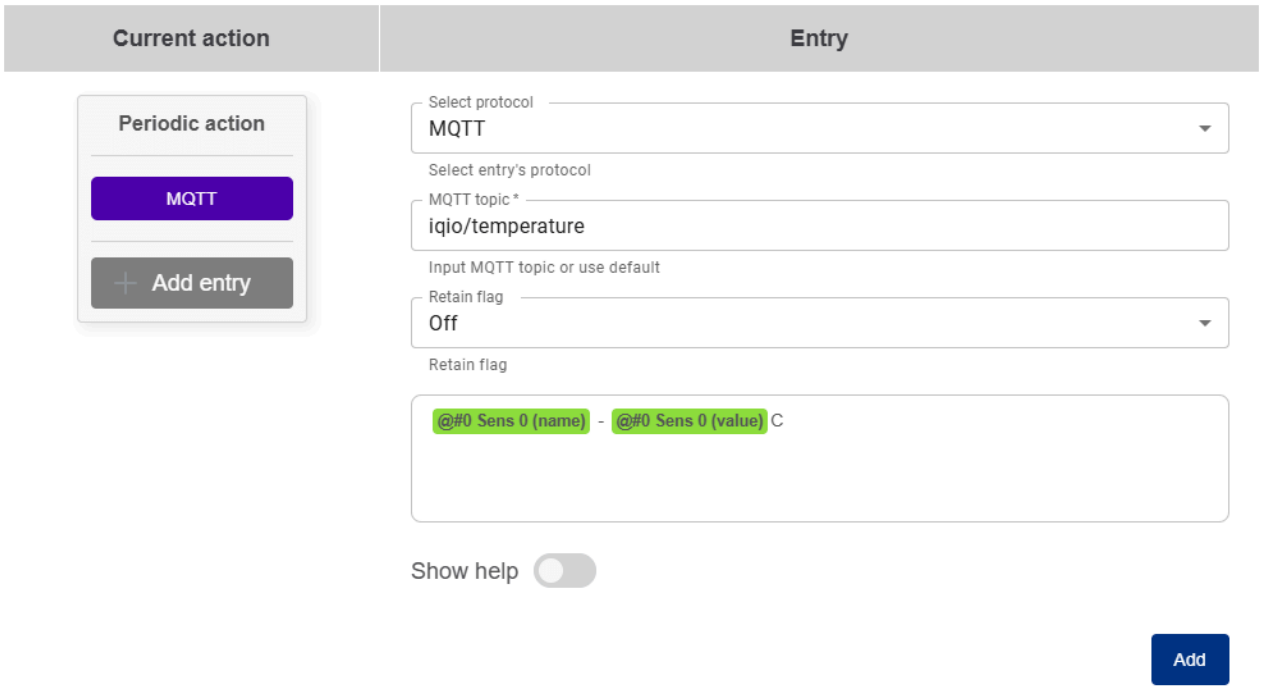


3. Creating actions

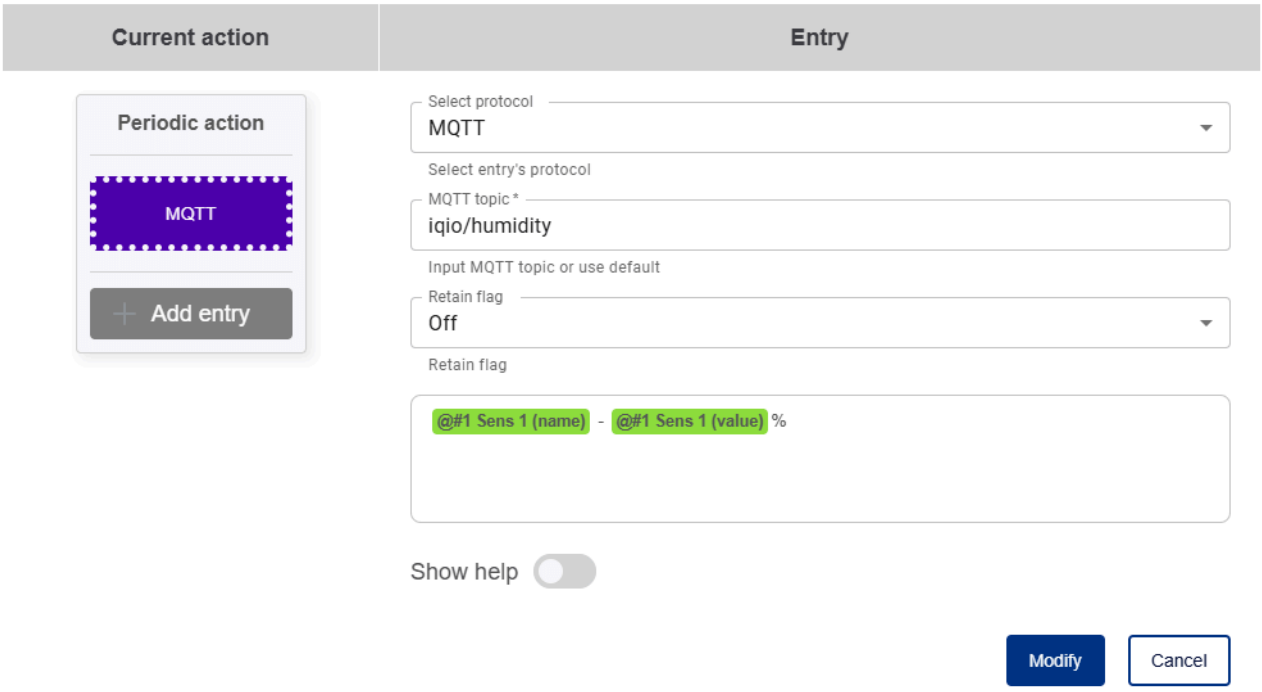
- In the **Actions / All** tab, **Add a new action**. This action will be used to notify about the status of sensor No. 1,
- In the **Create a new action** window, type in the action's name and confirm by clicking **Add entry**,
- Select the communication protocol (**MQTT** in this case),
- Input the **MQTT topic** that notifications will be sent to,
- In the syntax field, enter the command that will be sent to the broker.
- In **Create a new action**, add another action for sensor No. 2 (humidity):



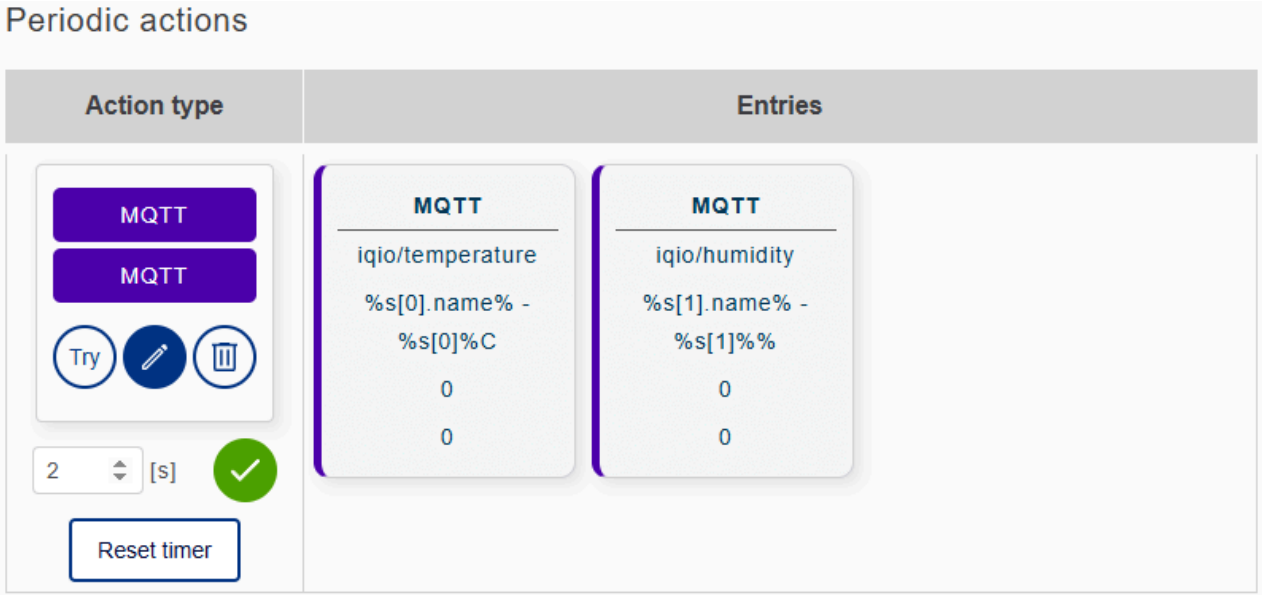
- In **Actions / Periodic**, create an action that will inform about the sensor's 1 measured value (temperature):
- In **Create a new action**, click **Add entry**,
- Select the communication protocol (**MQTT** in this case),
- Input the **MQTT topic** that notifications will be sent to. For the temperature sensor, we'll define `iqio/temperature`,
- In the syntax field, enter the command that will be sent to the broker.



- **Create a new action** for sensor No. 2 (Humidity):



- After leaving to **Actions / Periodic**, set the notifications interval and confirm it with .



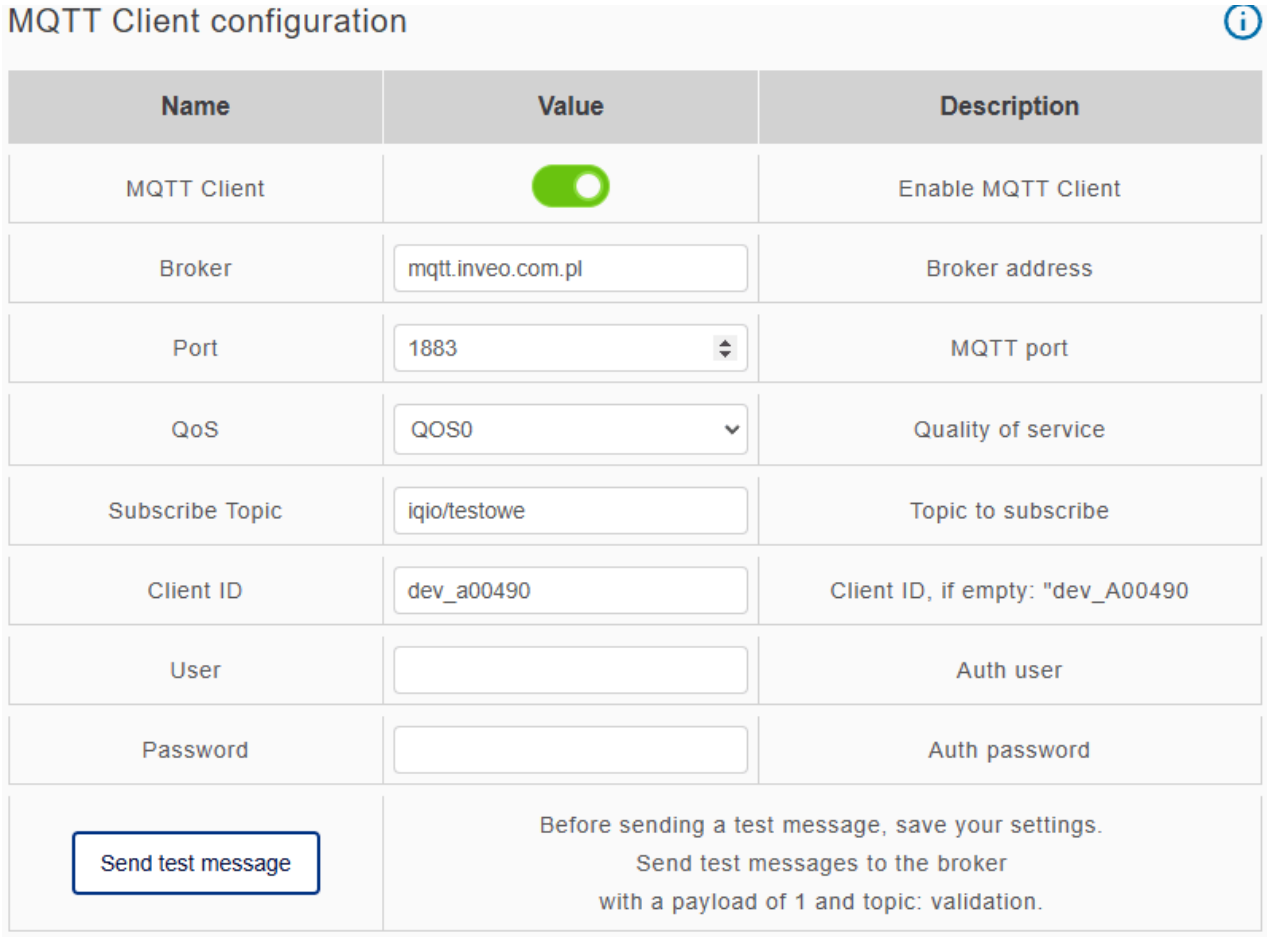
Tip

After making changes, apply them using the Save button.

4. MQTT client configuration

- Select **MQTT Client** in the **Services / MQTT** tab,
- Enter the broker's address (for the Inveo broker - `mqtt.inveo.com.pl`), port, set **QOS**,
- Enter the topic IQIO will subscribe to,
- If needed, enter the access data: **User** name and Password, set the encryption parameters and/or LWT message parameters,

- Send a test message using **Send test message** to verify the data and test the connection. A message with a payload of **1** will be sent to the **validation** topic.



Tip

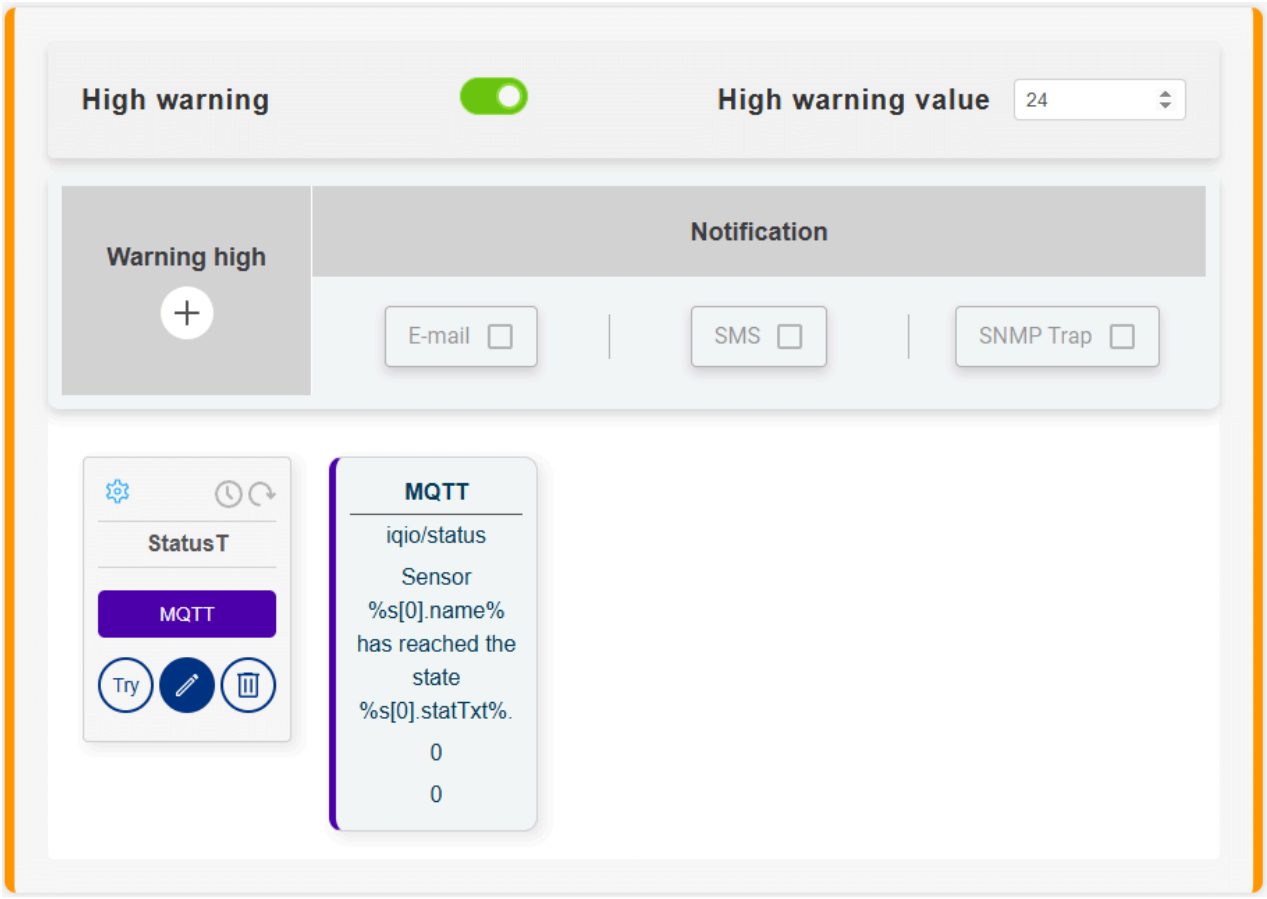
After moving the cursor over the i icon in the upper-right part of the window, a broker connection status will be displayed. Successful connection is indicated by MQTT Broker connection state: Connected.

Tip

After making changes, apply them using the Save button.

4. Warning and alarm thresholds configuration

- In the sensor's configuration window, activate the chosen notification options (eg. high warning and high alarm), assign an action and enter a value that will trigger it.



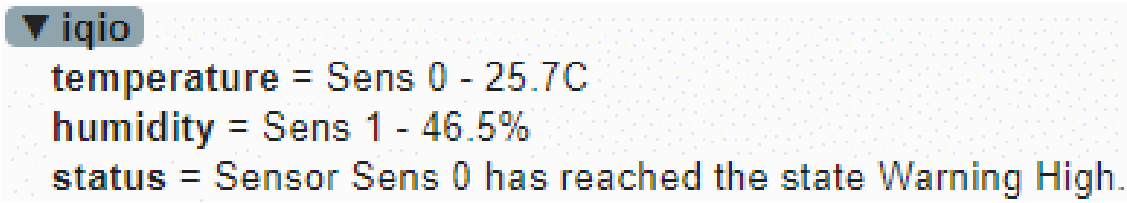
Tip

After making changes, apply them using the Save button.

Test the configuration:

Using an appropriate programme (eg. MQTT Explorer) make sure that the defined notifications are reaching the broker.

If configuration was successful, the following data should be displayed in the window:



- **iqio/status** = ... – In this topic, system messages regarding exceeded warning/alarm thresholds will be published,
- **iqio/temperatura** = ... – Value read from Sens 0; temperature in this case,
- **iqio/wilgotnosc** = ... – Value read from Sens 1; humidity in this case.

Factory settings, backup

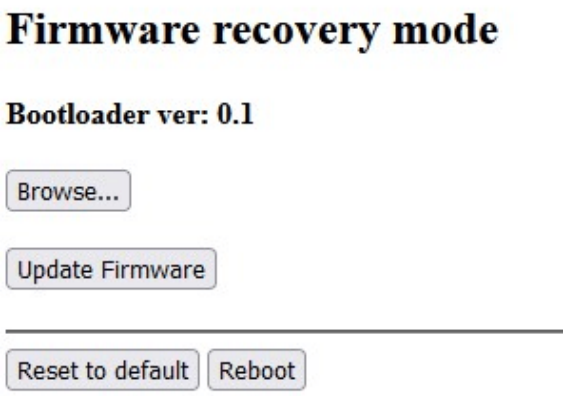
Emergency firmware restore / restoring factory settings

If device failure occurs, preventing normal access to the webpage, the emergency procedure should be put into effect:

1. Disconnect the power supply,
2. Depress the **RESET** button,
3. Power up the device and connect it to LAN,
4. Without releasing the **RESET** button, open the device's webpage:
    - **IP address:** 192.168.111.15
    - **IP mask:** 255.255.255.0

> **Tip**
>
> **In order to access the 192.168.111.15 address, computer's IP address must be in the same subnet (example computer address: 192.168.111.1).**

Referring to the specified IP address will give access to the device's bootloader. The **RESET** button can be released after the following webpage opens:



In this window, the following options are available:

- Firmware upload,
- Default settings reset,
- Device restart.

Warranty and manufacturer's liability

> **Warning**
>
> **The manufacturer provides a two-year warranty for the device and post-warranty service for a period of 10 years from the date of introduction of the device to the market. The warranty covers all material and production defects.**

The manufacturer undertakes to respect the warranty agreement, if the following conditions are met:

- All repairs, changes, expansions and device calibrations are carried out by the manufacturer or an authorized service center,
- The power supply system meets the applicable standards,
- The device is operated in accordance with the suggestions presented in this manual,
- The device is operated in accordance with its intended purpose.

The manufacturer assumes no responsibility for consequences resulting from improper installation, improper use of the device, failure to comply with the instruction manual, and repairs made by unauthorized personnel.

> **Warning**
>
> **The device contains no user serviceable parts inside.**

Storage, operation and transport conditions

The device should be stored in enclosed rooms, where the atmosphere is free from vapours and corrosive substances:

- Environment temperature from -30°C to +60°C (-22°F - 140°F),
- Humidity from 25% to 90% (condensation unacceptable),
- Atmospheric pressure from 700 to 1060 hPa.

The device is intended to operate in the following conditions:

- Environment temperature from -10°C do +55°C (14°F - 131°F),
- Humidity from 30% to 75%,
- Atmospheric pressure from 700 to 1060 hPa.

Recommended transport conditions:

- Environment temperature from -40°C do +85°C (-40°F - 185°F),
- Humidity from 5% to 95%,
- Atmospheric pressure from 700 to 1060 hPa.

Installation and device operation:

- The module should be operated in accordance with recommendations provided later in this manual.

Disposal and decommissioning

In an event the device needs to be decommissioned (eg. after its intended life period is surpassed), it is recommended to contact the manufacturer or his representative, who are responsible to respond appropriately, i.e., to collect the device from the user. The user can alternatively contact companies specializing in electronic device or computer equipment disposal and/or decommissioning. Under no condition should the device be placed with other waste.