Inveo Sp. z o.o.

# IQIO Sens

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 Sens is an advanced environmental monitoring and management system. It is dedicated to monitoring various environmental parameters such as temperature, humidity, pressure, air quality or presence of harmful substances. The main objective is to allow users to remotely monitor and manage these parameters in real time.

IQIO Sens offers a wide range of features, including configurable notifications, integration with various communication protocols and flexible configuration, allowing its versatile use in industry, agriculture, construction and urban infrastructure monitoring. Thanks to the configurable notification capabilities, users can react quickly to changes in environmental conditions or failures.
In addition, thanks to the LWT (Last Will and Testament) mechanism, the system can automatically send

notifications in the event of an MQTT broker connection loss, ensuring continuity of monitoring even in the event of network disruptions.

## 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
    - Sensors window
    - Display LED
  - Sensors configuration
    - All
      - Alarms configuration
    - Sensor handling
  - Notifications configuration
    - Sensors
    - Configuration
  - Logic functions
    - Conditions
    - Variables
  - System management
    - Access
      - API keys
    - Network
    - Time
    - System events
    - Backup
    - Restore

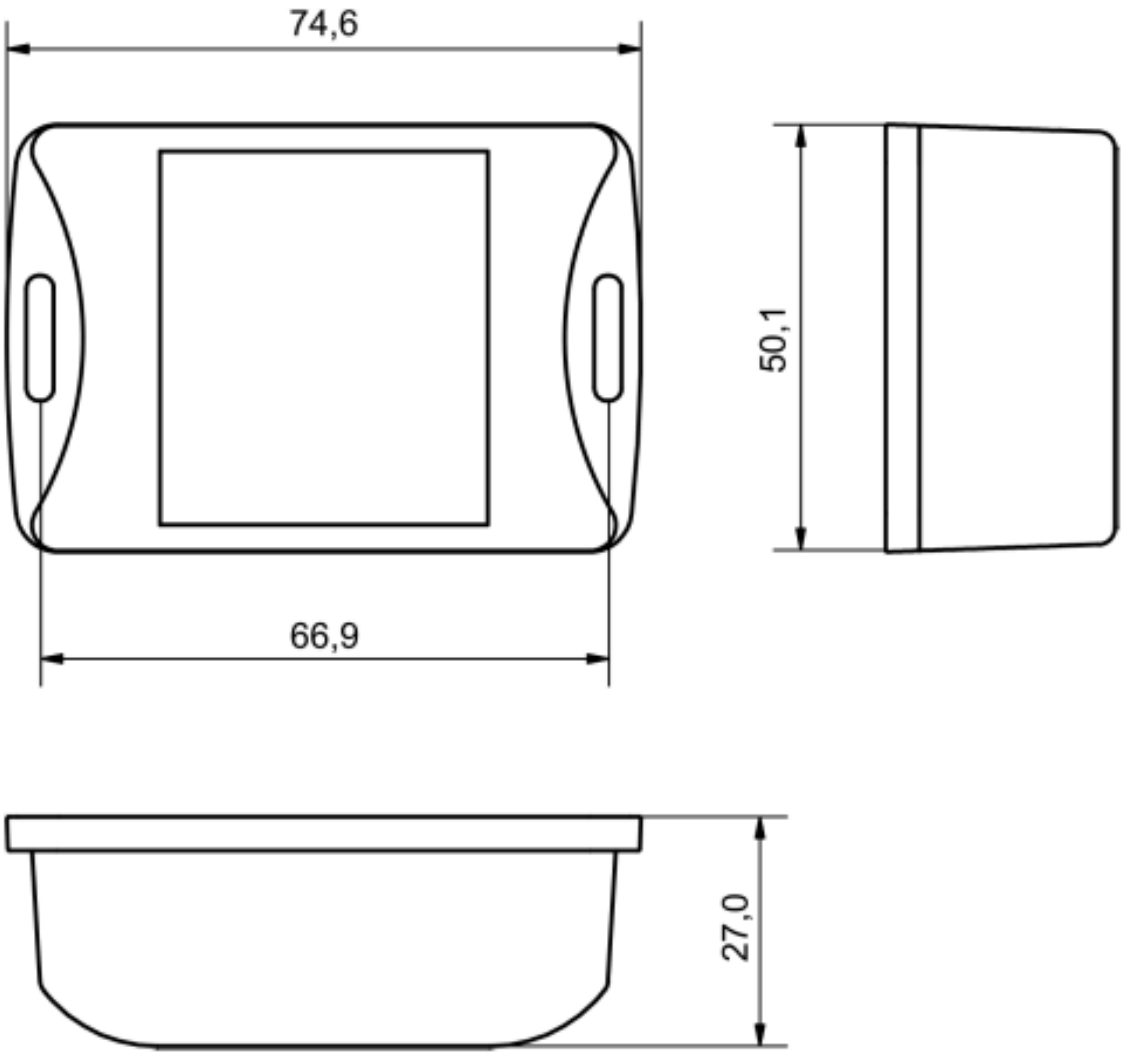
- Defining actions
  - All
  - Protocol configuration
    - UDP
    - TCP
    - MQTT
    - IO
    - E-mail
    - SNMP Trap
  - System
  - Periodic
- Communication protocols
  - Web
  - MQTT
  - E-mail
  - SNMP
    - SNMP v2c
  - TCP/UDP
  - iCluster
  - REST API
- Built-in variables
- Factory settings, 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<br>**PoE:** 33-57V PoE IEEE 802.3af *(IQIO Sens ETH)*<br>**USB-C** 5V |
| **Power consumption** | Max. 1,5W |
| **Bus** | **1-Wire** – Three-wire or flat RJ12 cable (adapter required)<br>Supports up to 2 sensors<br>Dedicated sensors: temperature, humidity, water pressure, air pressure, analogue voltage, analogue current, gases: CO, $CO_2$, $NO_x$ |
| **Communication** | Wi-Fi 2,4GHz *(IQIO Sens Wi-Fi)*<br>Ethernet 10/100Mbps Full Duplex, RJ45 port *(IQIO Sens ETH)* |
| **Enclosure ingress protection** | IP30 |
| **Weight** | ca. 60g (2,1oz) |

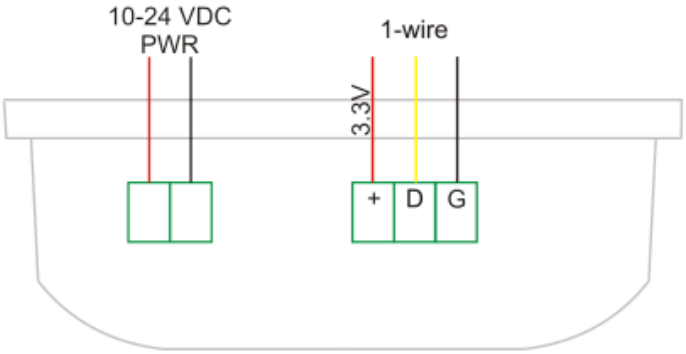
## Dimensions

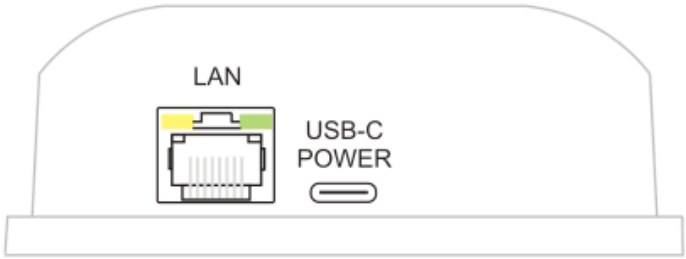



**Information**

**All dimensions are in millimeters.**

## Module connectors description



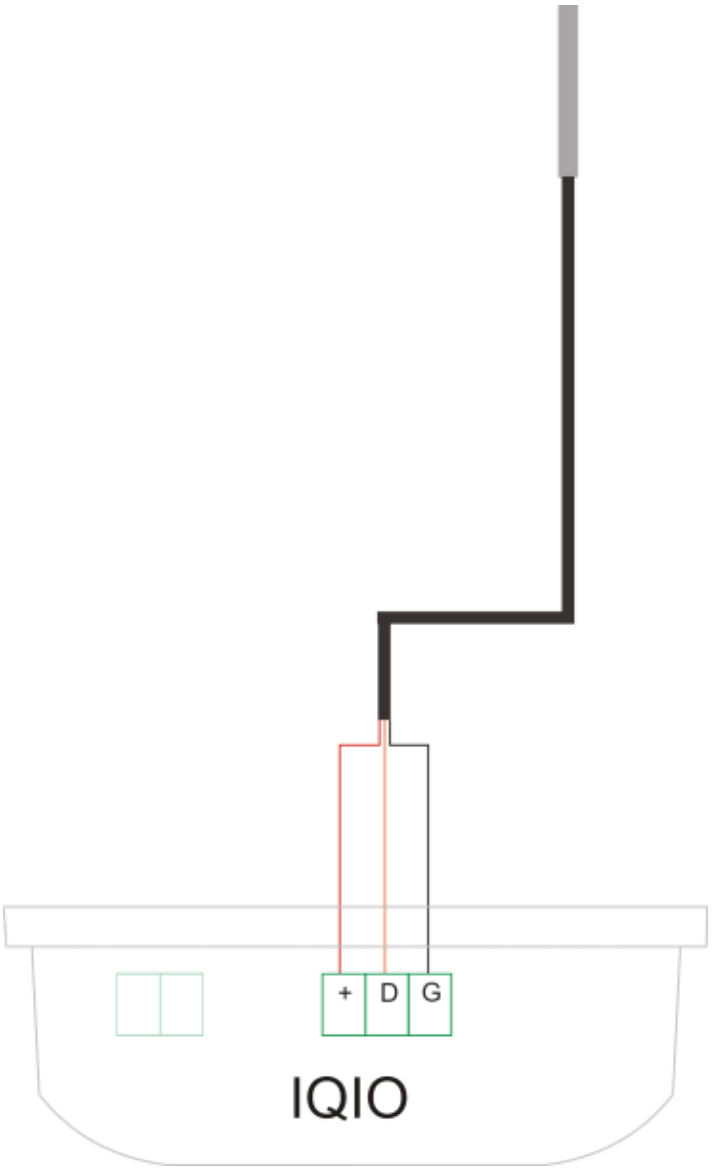




The IQIO Sens module has the following connectors:

- **BUS** – Sensor bus terminal block,
- **LAN** – LAN and PoE IEEE 802.3af,
- **PWR 5VDC** – 5V USB C power connector.

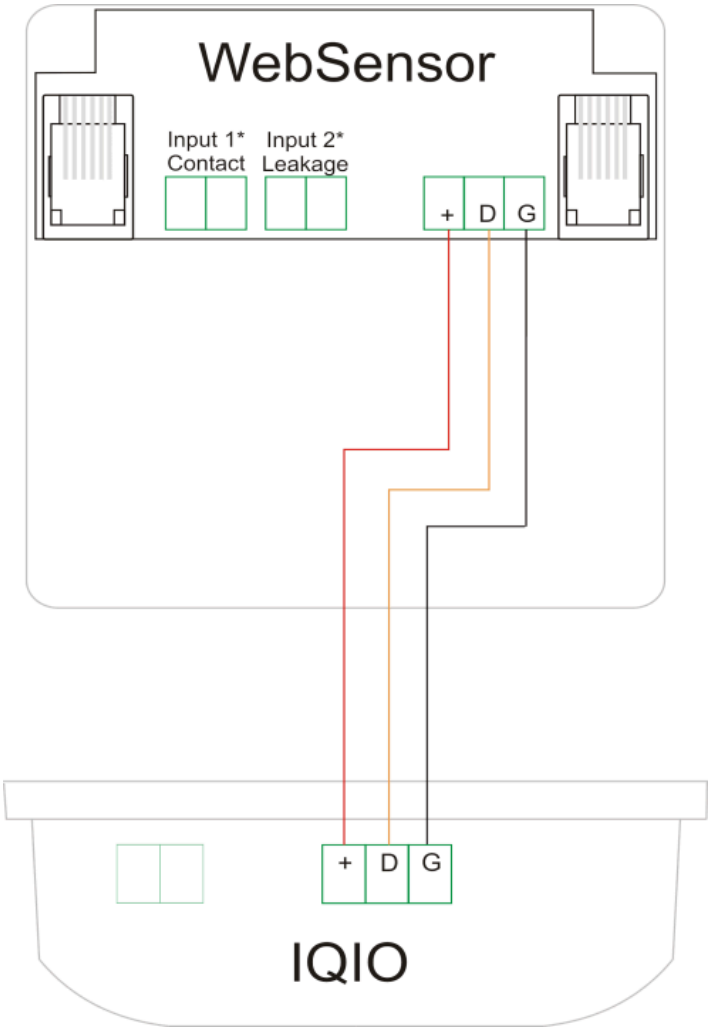
## Sensor connection diagram

**Connecting a sensor:**

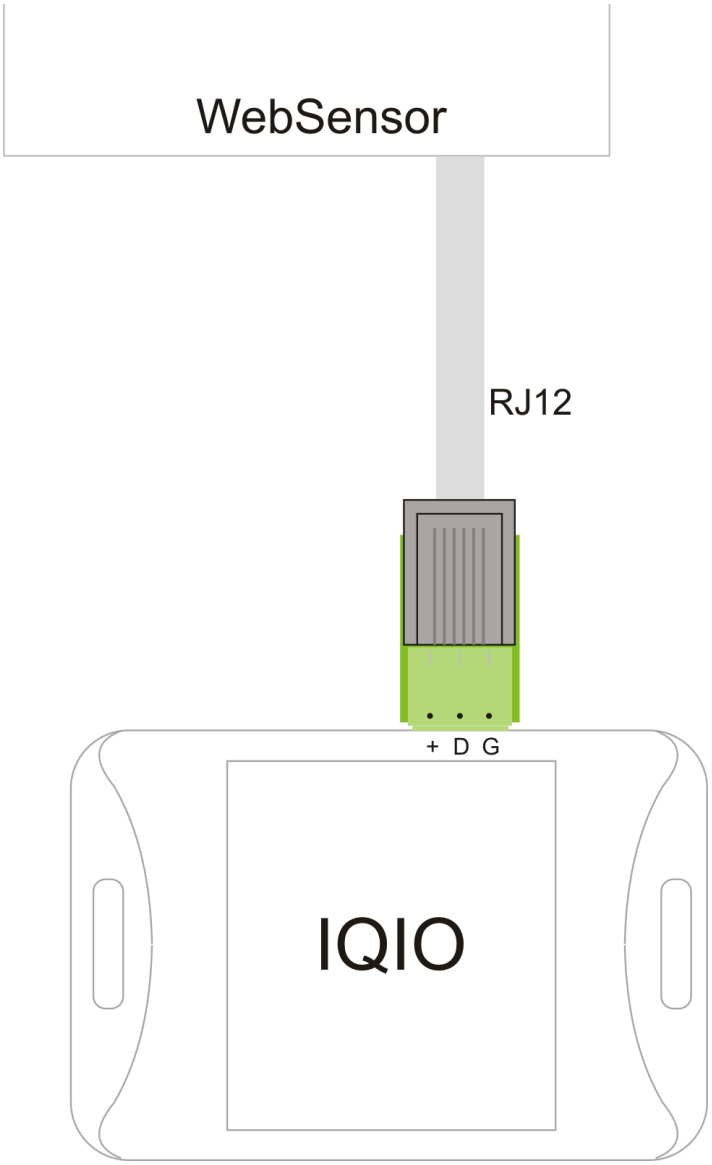


**Connecting a WebSensor:**

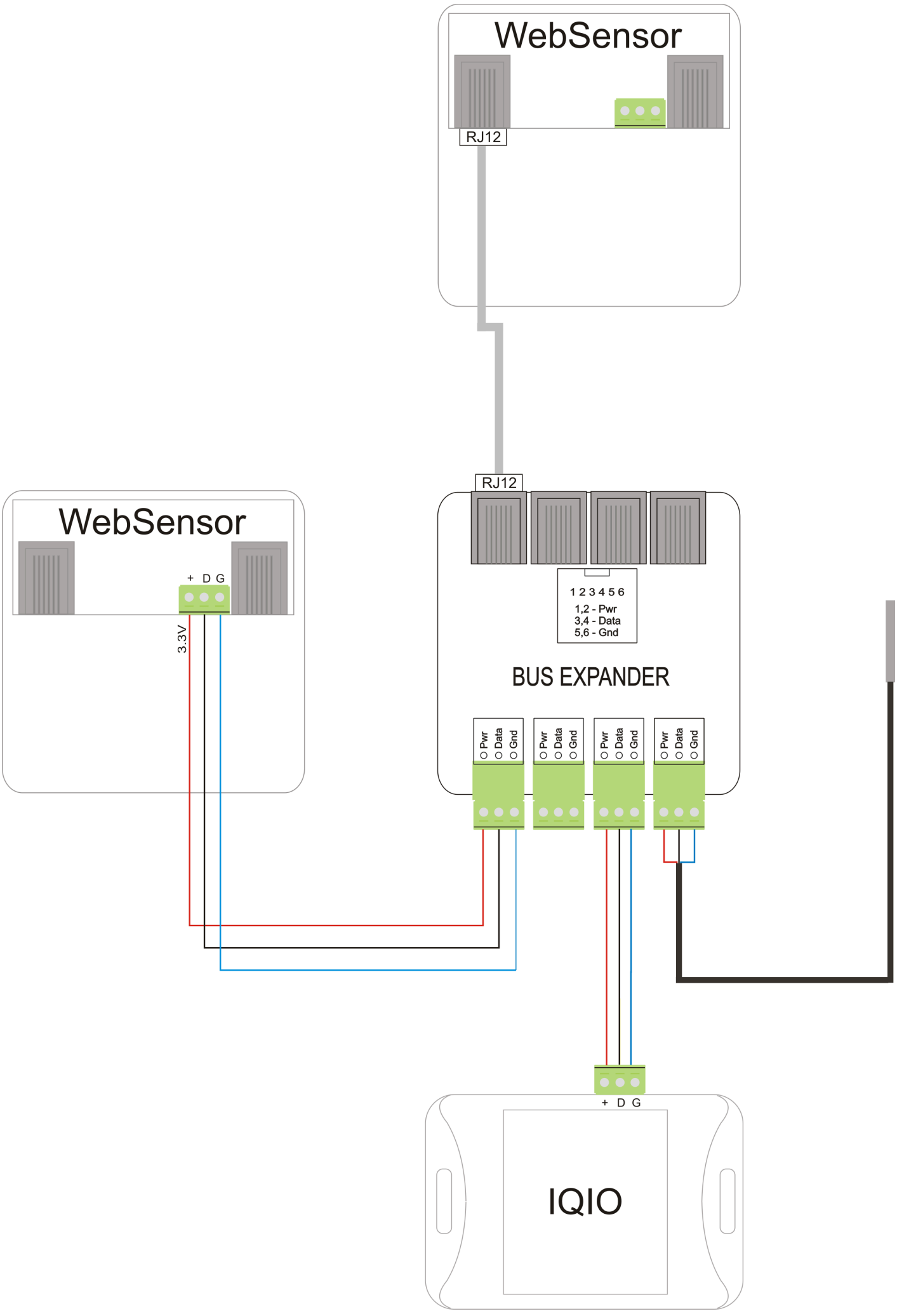
- 3-wire cable:



- RJ12 flat cable + adapter:



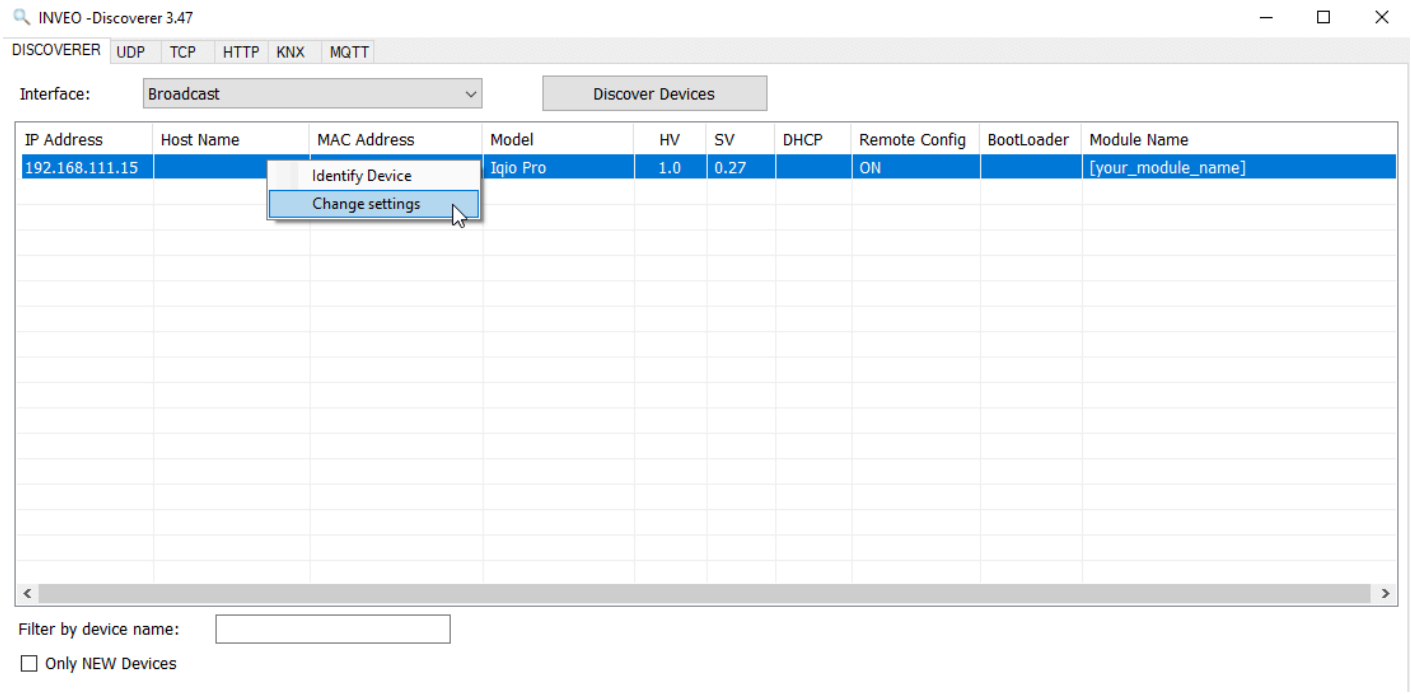

**Connecting sensors using the BUS Expander splitter:**


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

# Network configuration

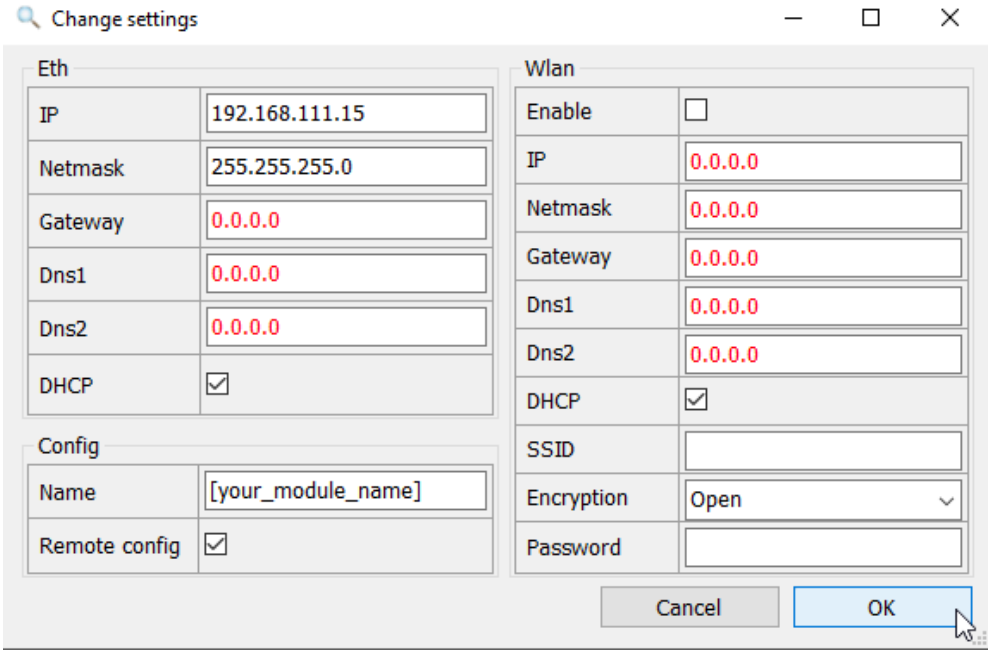
> **Warning**
>
> **After the initial power-up, it's needed to configure the device. It can be done in two ways, the simplest method is to use the Inveo Discoverer programme.**

## 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:

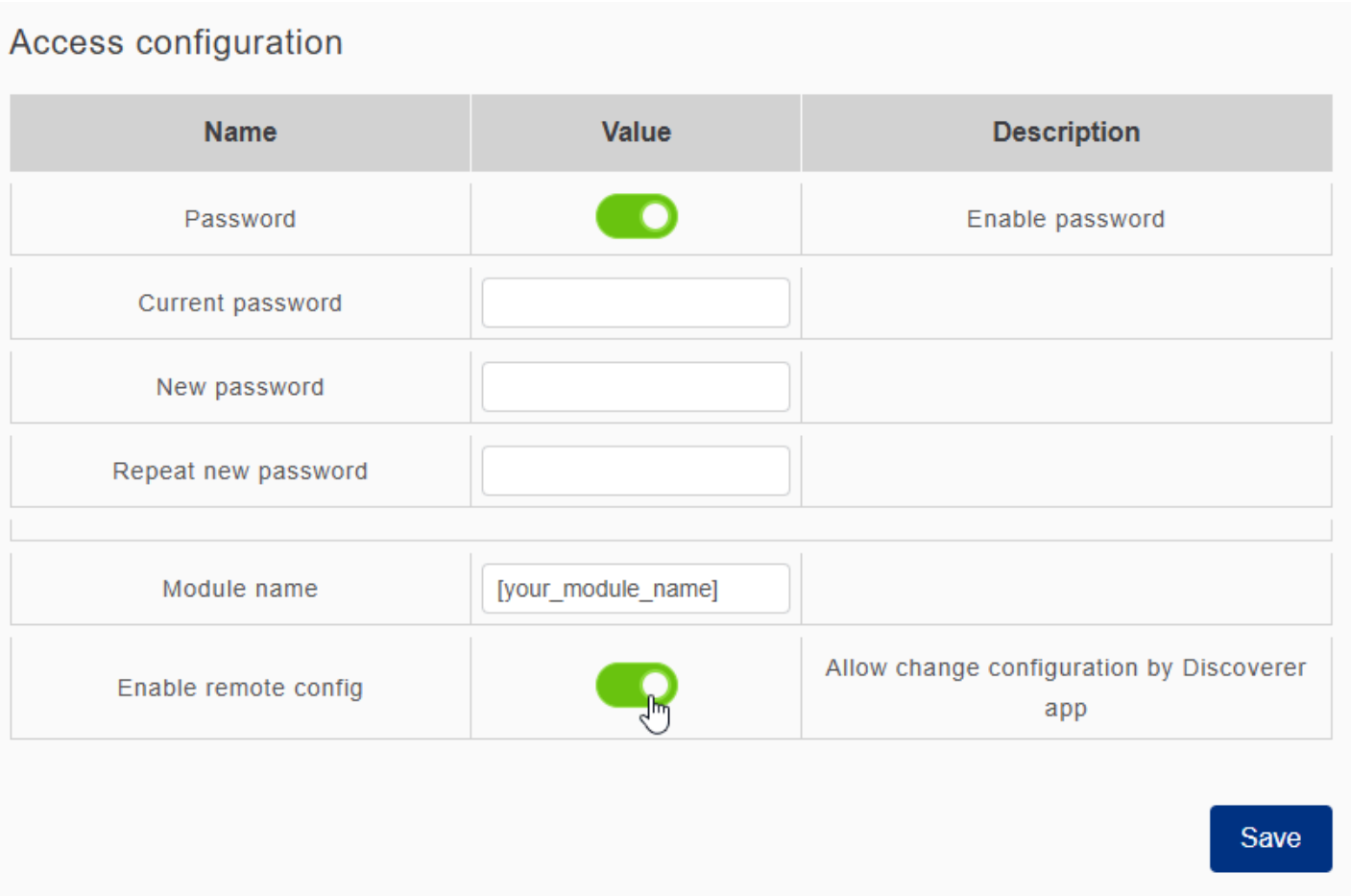
- Set the IP address, mask, gateway, DNS1/DNS2.
- Change the Host name.

> **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

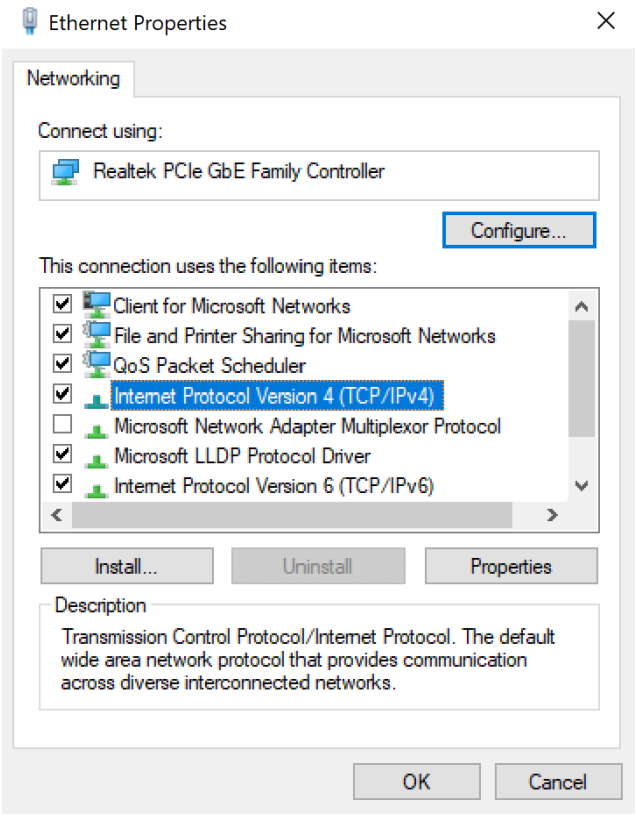
During configuration without **Discoverer** programme, it's needed to change the subnet address of the computer on the same network.

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

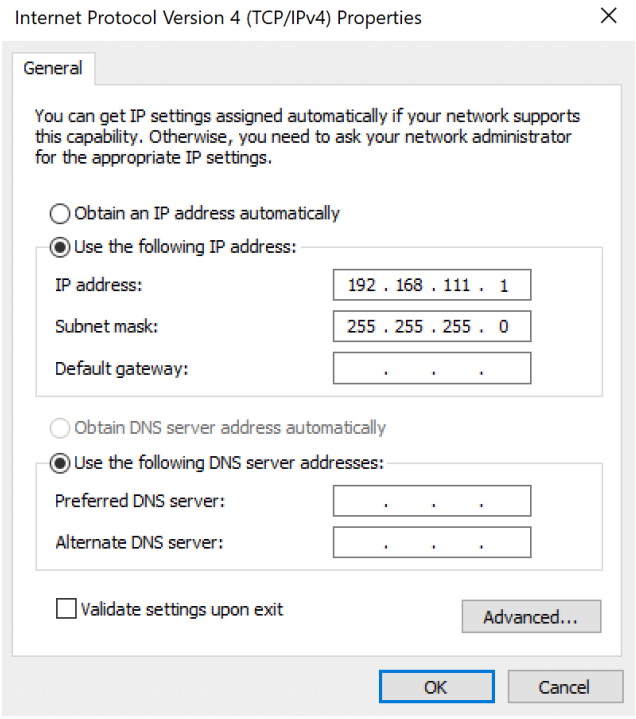
- Press **Win + R**, type in `ncpa.cpl`, and then press **Enter**.
- Alternatively, go to:
  **Start** → **Control Panel** → **Network and Internet** → **Network and sharing center** → **Change adapter settings**.

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:

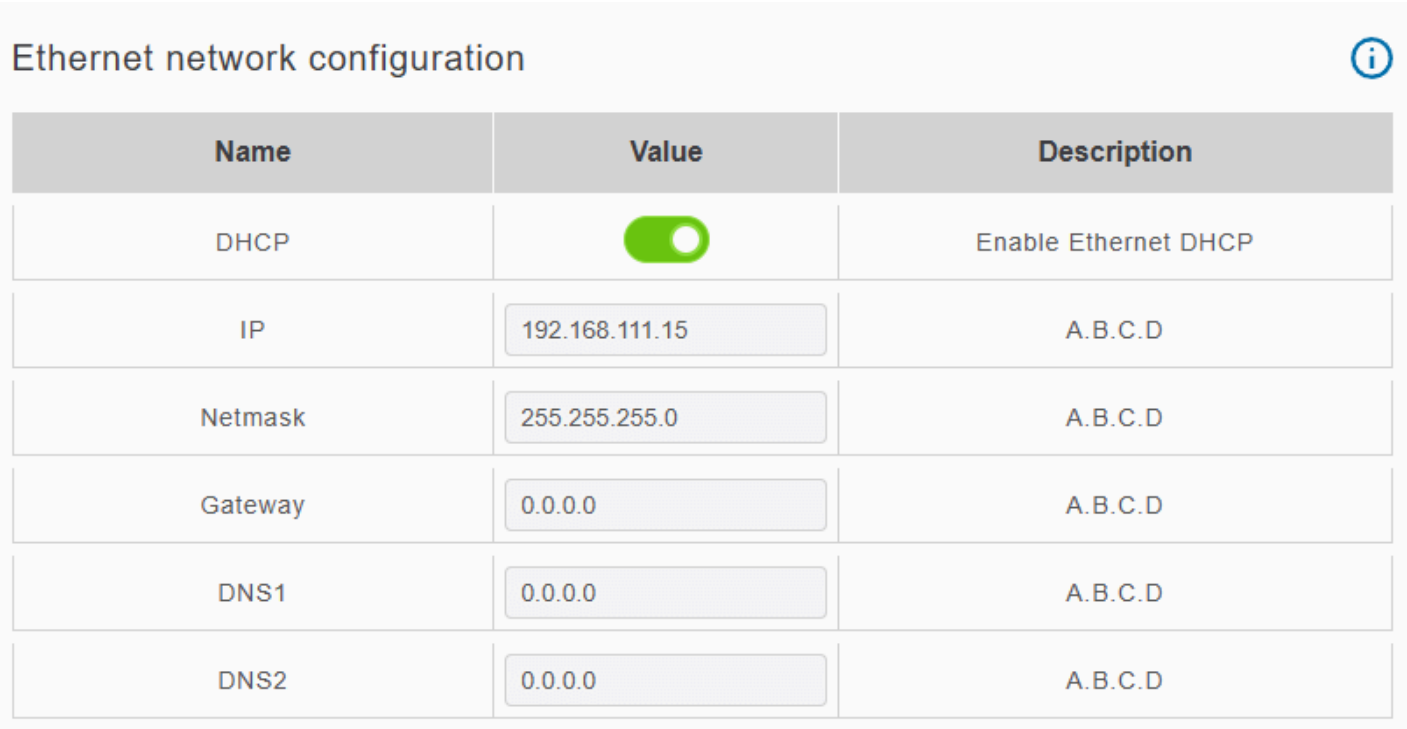



**Note**

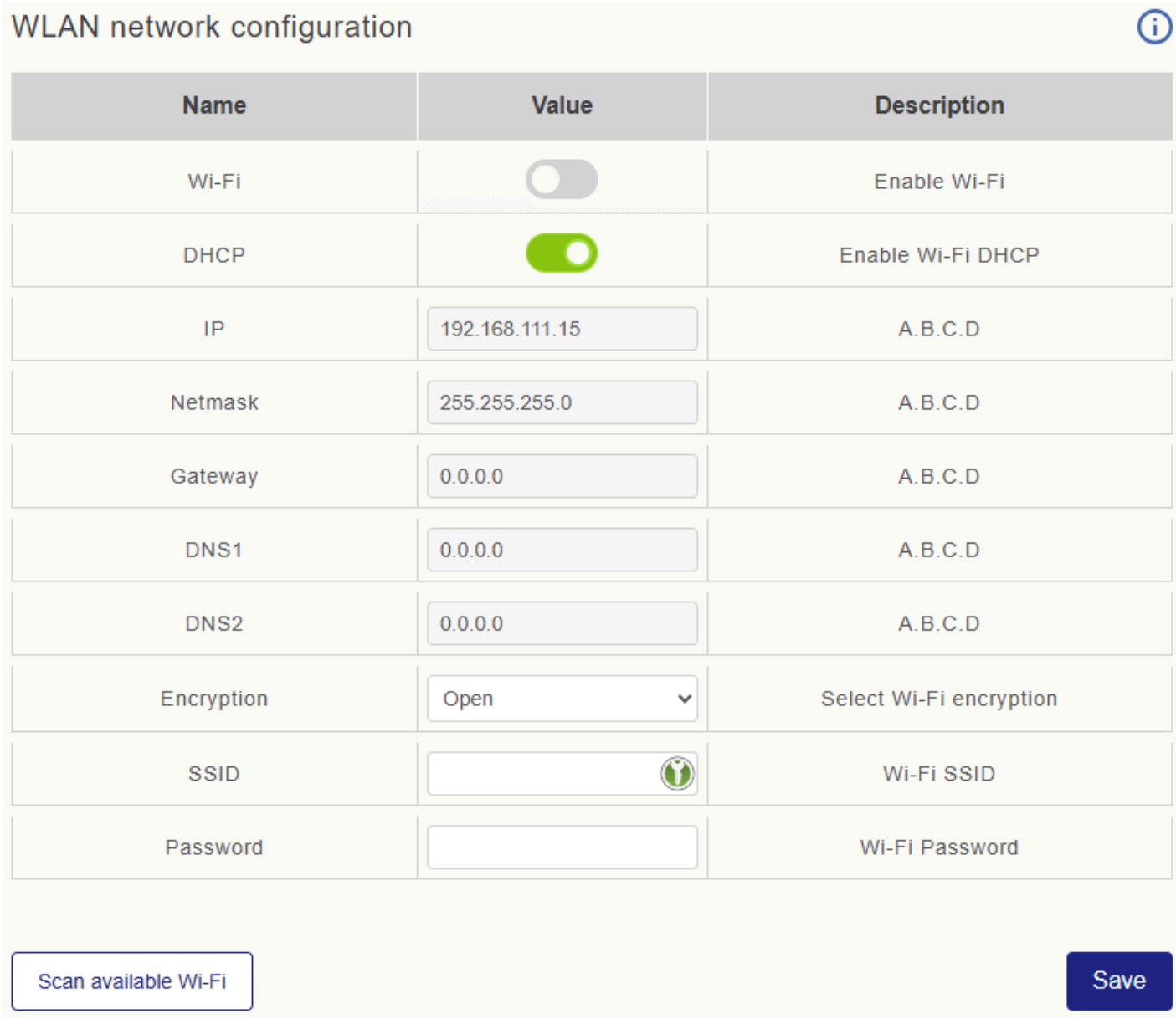
**After applying the configuration with OK, start a web browser and type in the following address: 192.168.111.15. (Default user and password: admin/admin)**

## 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

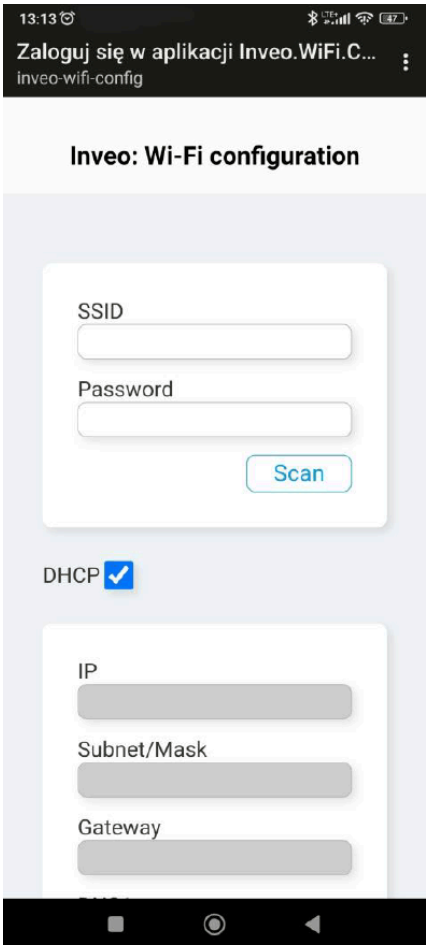
Pressing and holding the **RESET** button will display the IP address.

**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



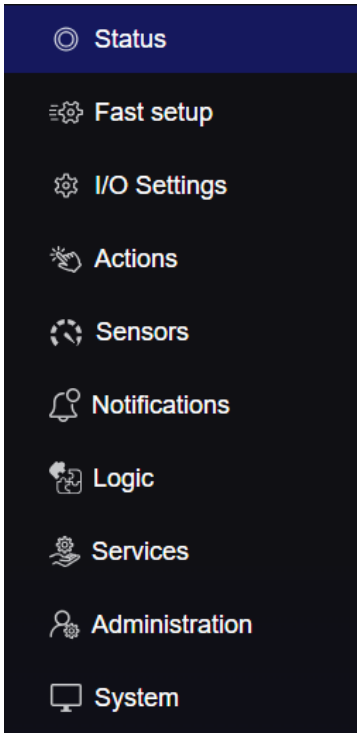

1. For 3 minutes after the power has been applied to the device (during **Configuration mode**), Wi-Fi connection can be configured. To do that, press and hold the **RESET** button until **AP** is displayed.
2. Activate Wi-Fi network search on your smartphone or other device. A network called "Inveo-wifi-config" 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

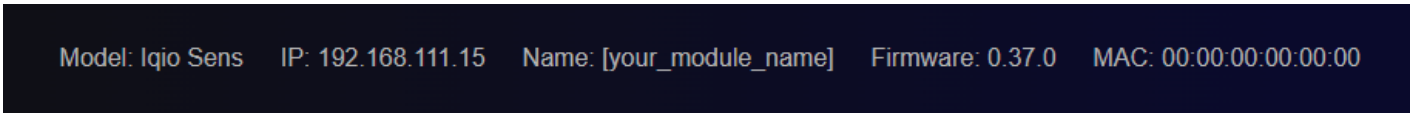
## Module's www interface

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.

**Sensors window**

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

Enable autorefresh

Sensors

| ID | Name | Type | State | Last value | Last read |
|---|---|---|---|---|---|
| 0 | s0 | | Normal | 0 | 3.3s |
| 1 | s1 | | Normal | 0 | 5.1s |

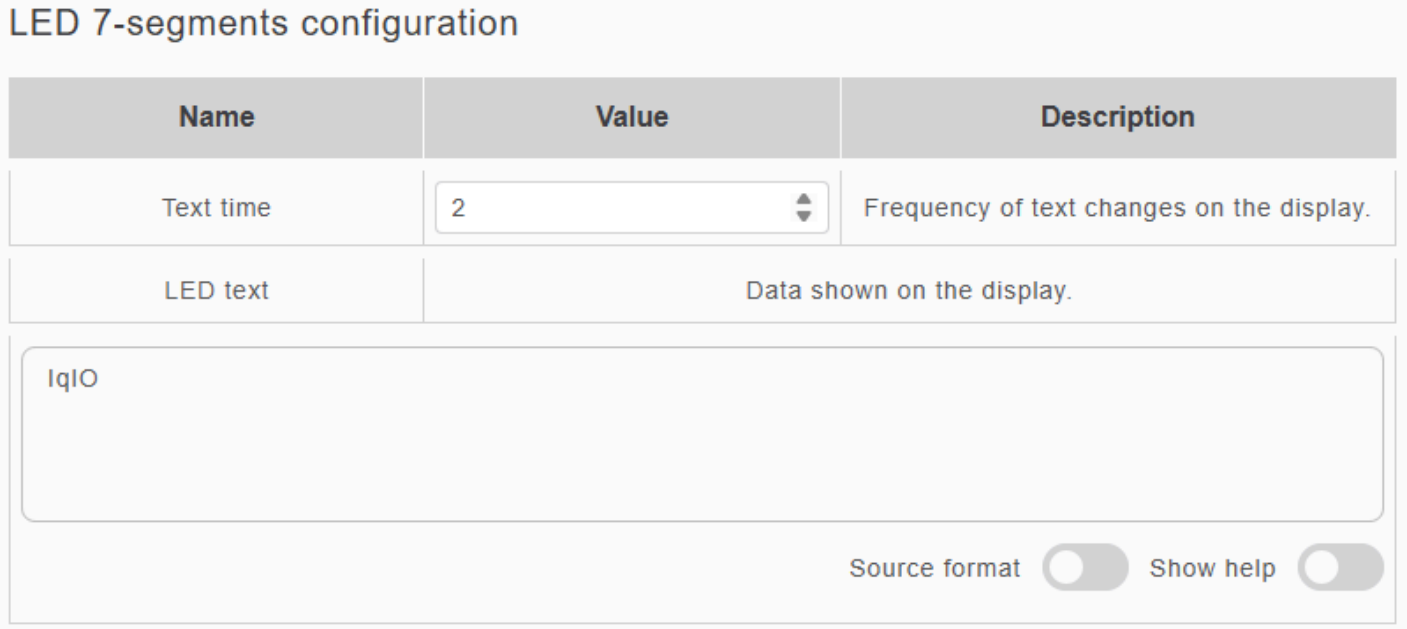
Using the **Enable autorefresh** button, the user can enable or disable automatic readout refreshing.

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).

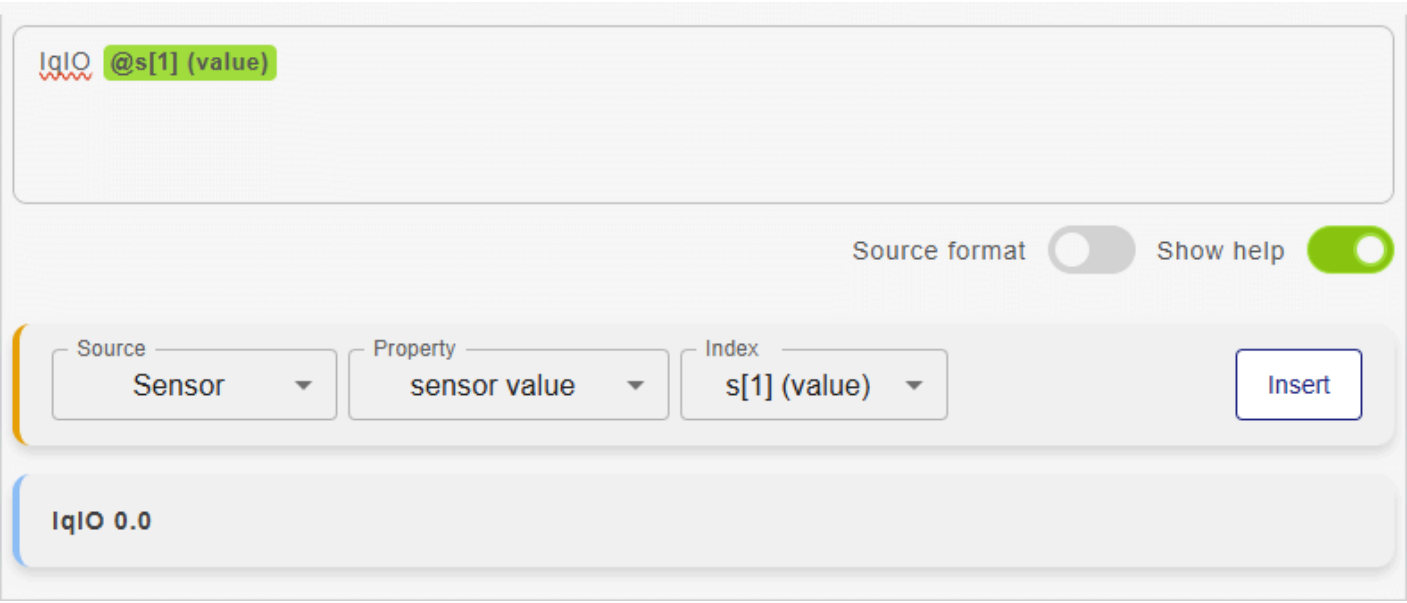
**Display LED**

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.

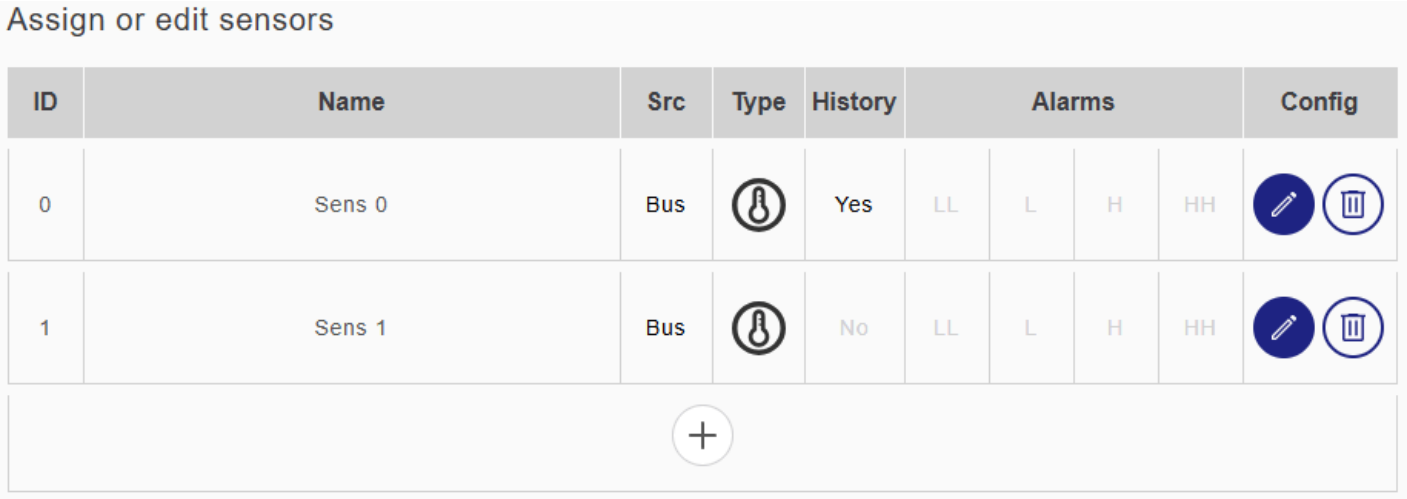


## Sensors configuration

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.



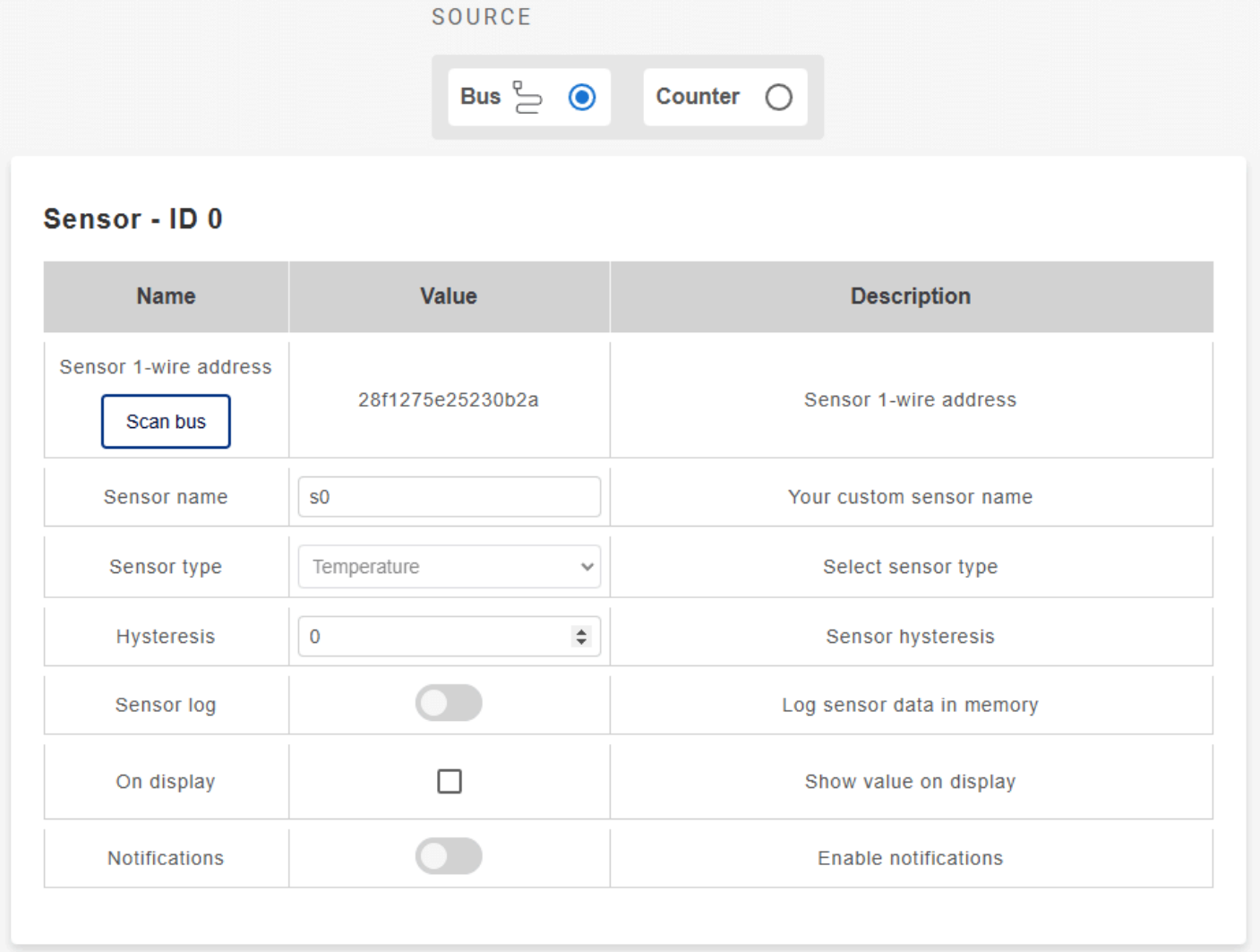

Each sensor table column contains the following information:

- **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:

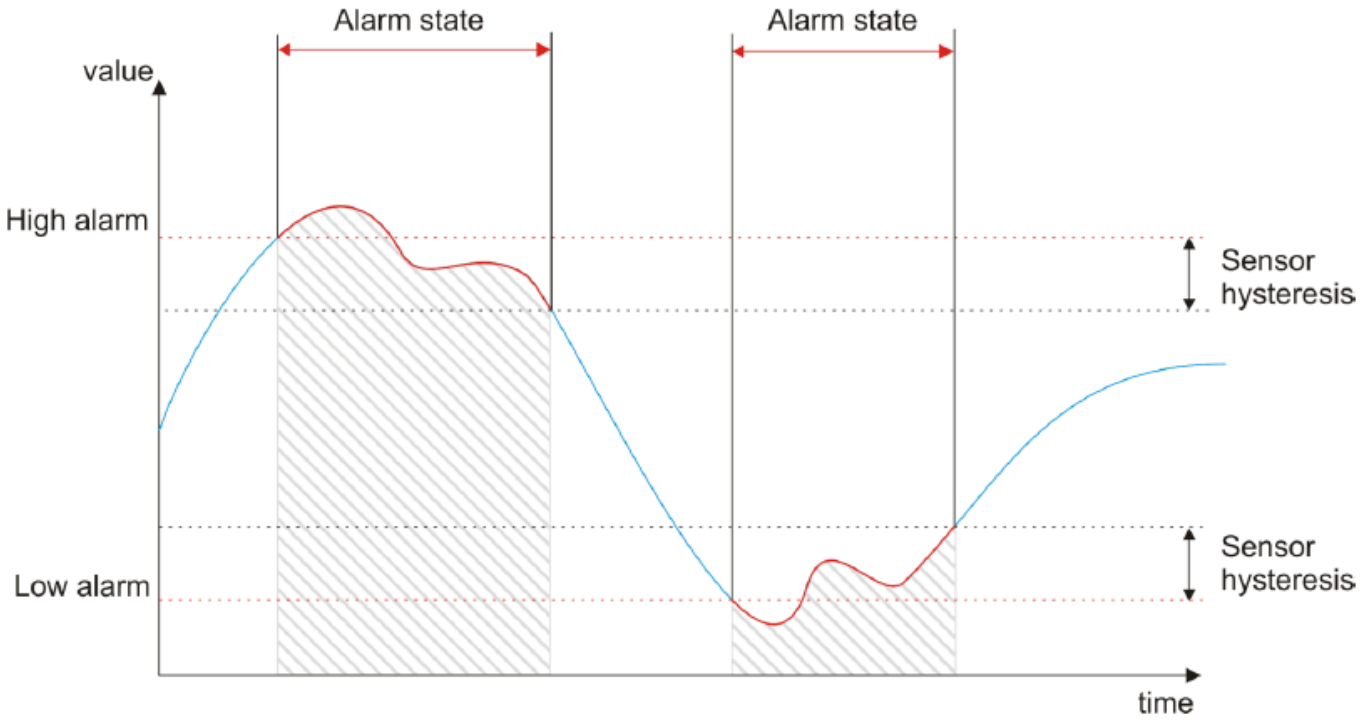



- **Source** – Sensor source *(version dependent)*:
  - **Bus** – Sensor bus,
  - **mbAgent** – Data read off Modbus,
  - **Inveo** – Data received from another device via iCluster,
  - **Counter** – Counter input.
- **Sensor bus address** – **Scan bus** makes it possible to locate and assign a sensor 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.**



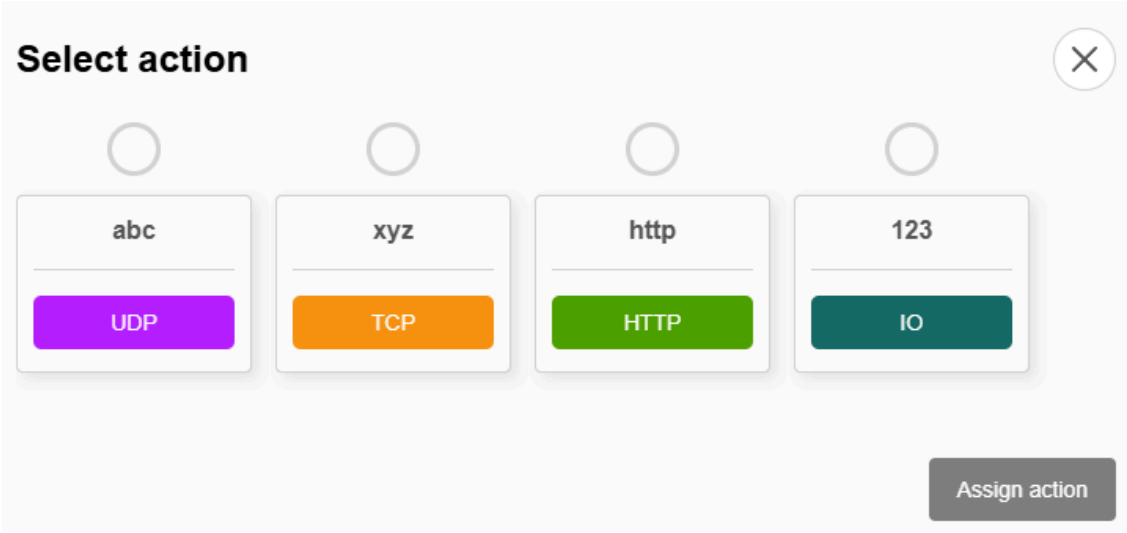

- **Channel** – Channel selection – active only if the sensor type is set to **Input**,
- **Sensor log** – Enable/disable sensor data logging to device memory *(version dependent)*,
- **On display** – Enable/disable display of measured value on the LED display *(IQIO series only)*,
- **Notifications**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

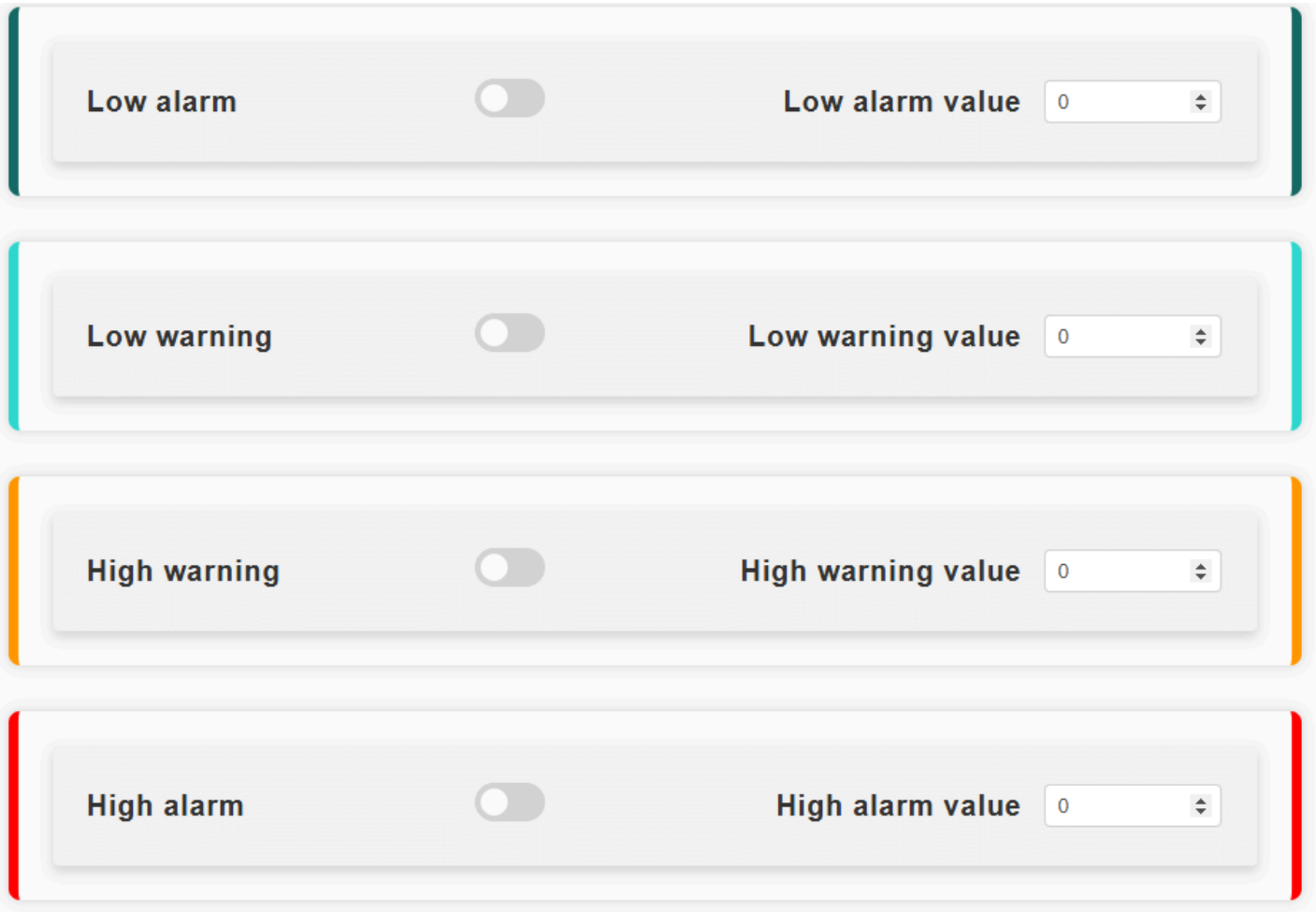
The user can select the type of a notification that will be sent in response to the above events. Appropriate settings in the **Services** tab must be configured first for the notifications to be sent.

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.

**Sensor handling**

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

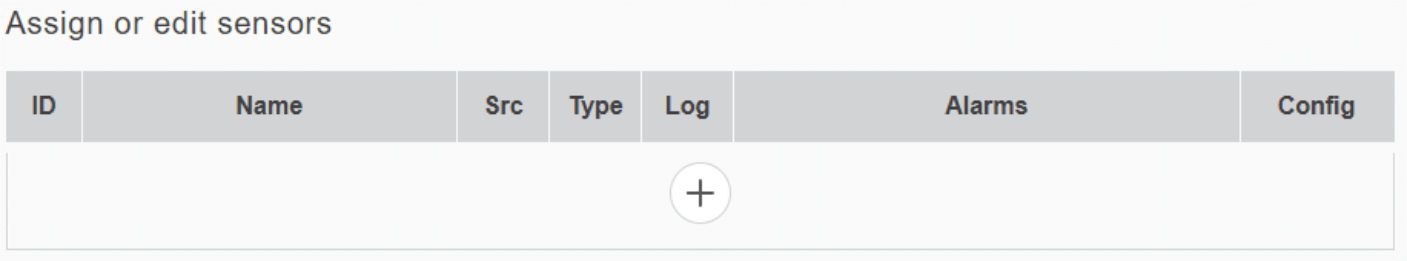
**Sensor assignment**

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

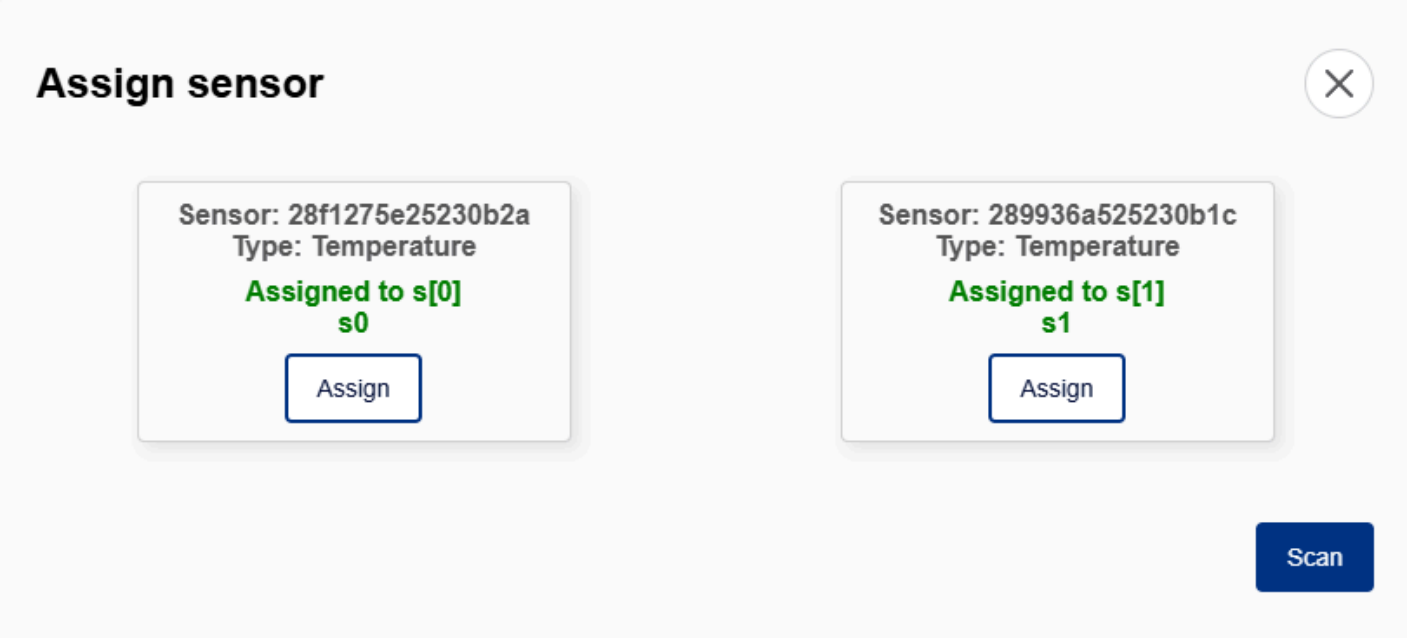
After that, using the device's webpage, locate and configure the sensor's basic parameters. If no sensors were connected to the device previously, the user can use the automatic sensor assignment option. Reset the device after the sensors have been connected – after the device restarts, it will automatically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



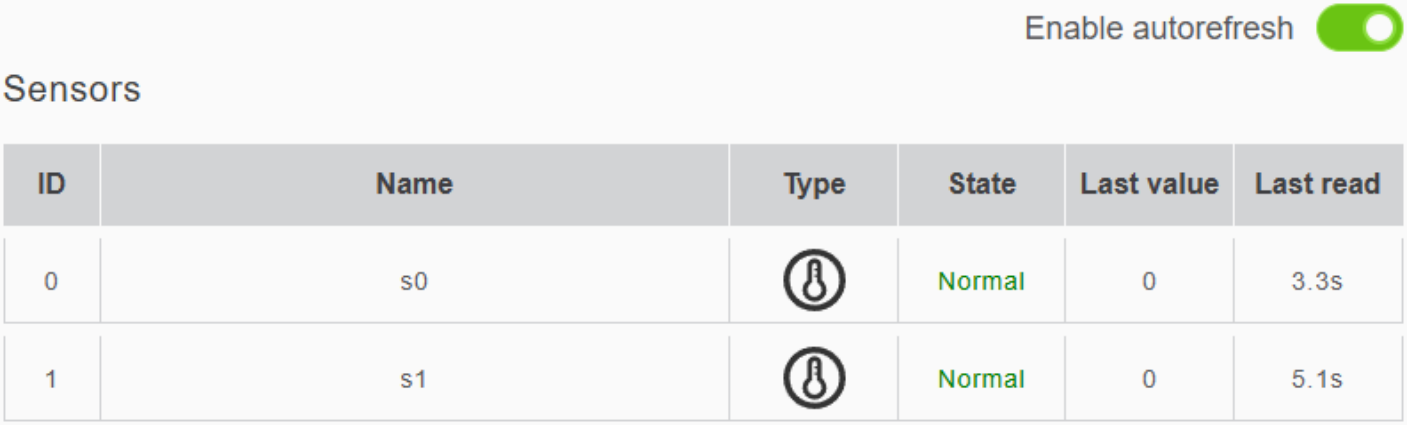

**Assign** the selected sensor.

**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**:



## 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:

| | Sens 0 (s0) | | |
|---|---|---|---|
| **State** | E-mail | SNMP Trap | MQTT |
| Info | ☐ | | |
| OK | ☐ | ☐ | |
| Error | ☐ | ☐ | |
| Alarm low (disabled) | ☐ | ☐ | ☐ |
| Warning low (disabled) | ☐ | ☐ | |
| Warning high (disabled) | ☐ | ☐ | |
| Alarm high (disabled) | ☐ | ☐ | |

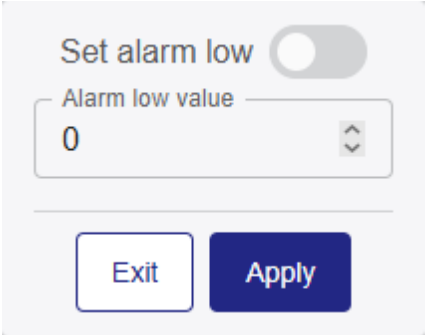
**Tip**

**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.**

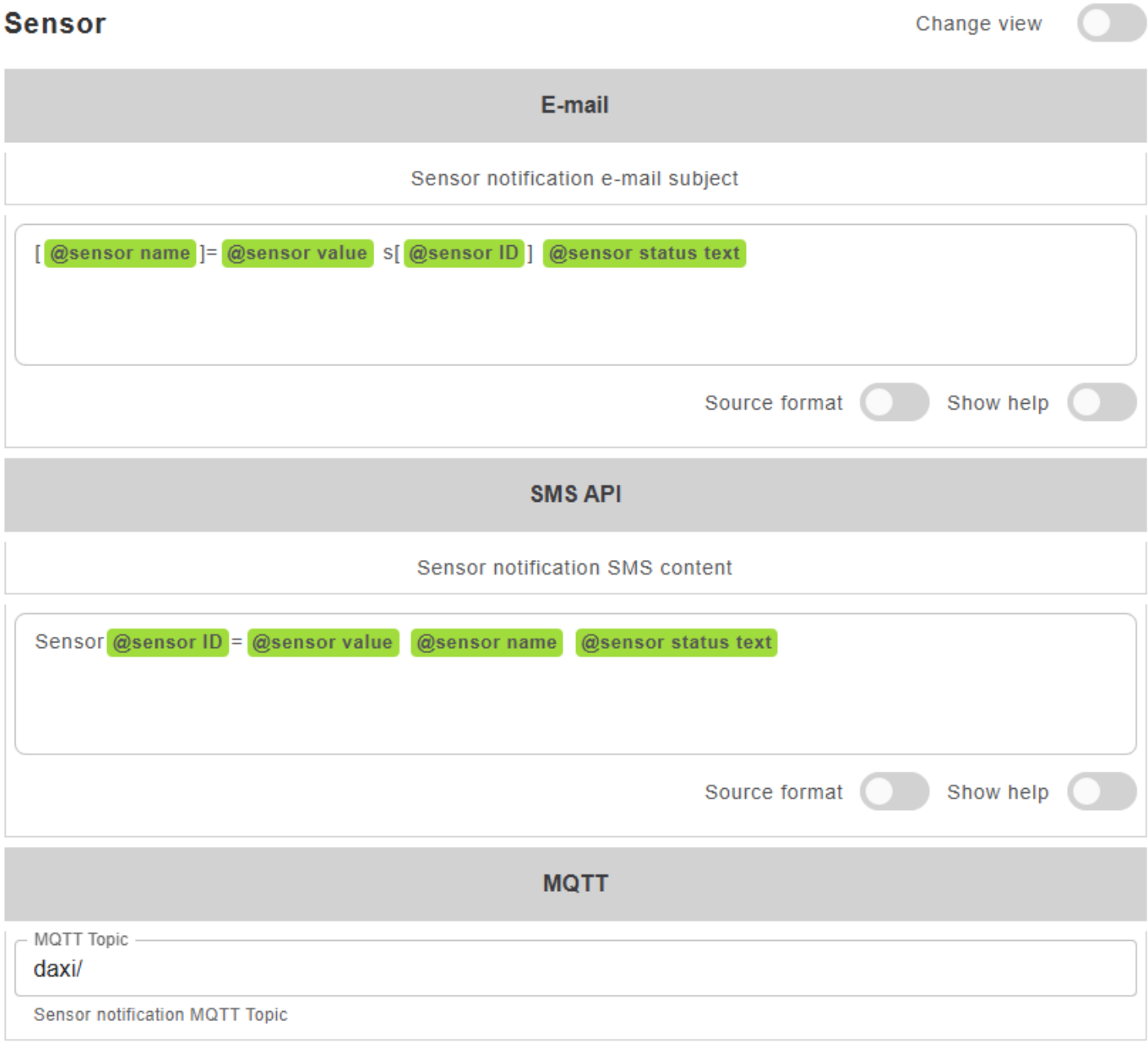
#### Configuration

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] |
| MQTT info | 60 | MQTT info time [s] |
| MQTT Retain |  | Set MQTT Retain flag |
| SNMP Trap | 0 | SNMP user trap |

- **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.

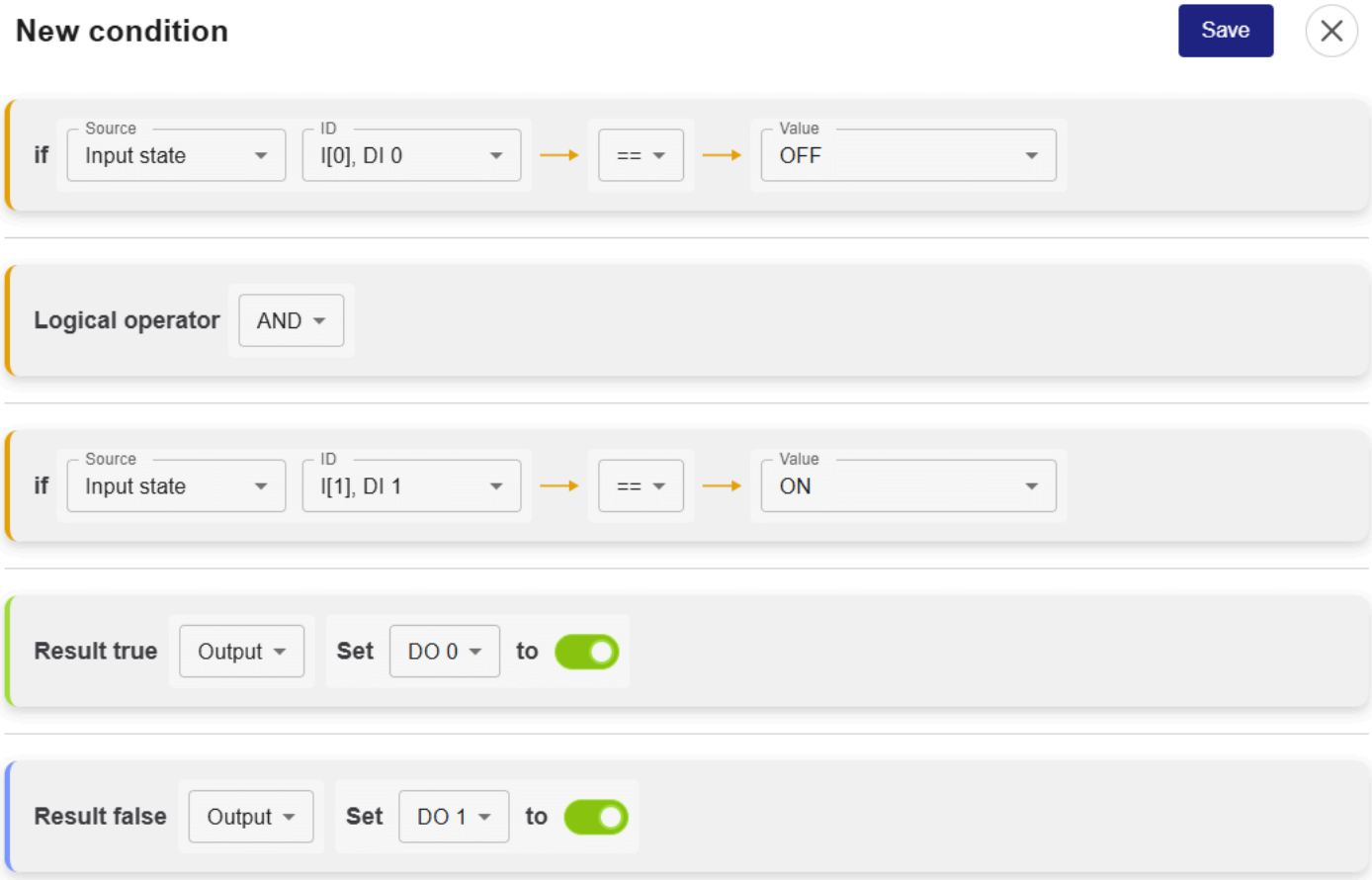



## Logic functions

This tab allows configuration of logic functions – afer certain conditions are met, a defined action is executed.

#### Conditions

To configure a new logical funtion, click **Add a condition**.




Available logical variables *(availability depends on the device version)*:

- **input** – Physical or virtual input state,
- **input cnt** – Input counter,
- **output** – Physical or virtual output state,
- **sensor** – Sensor reading,
- **sensor state**:
  - **0** – Sensor error,
  - **1** – Normal state,
  - **2** – Sensor low level warning,
  - **3** – Sensor high level warning,
  - **4** – Sensor low level alarm,
  - **5** – Sensor high level alarm.
- **constant**,
- **variable**,
- **active input action** – In **cnt** input mode,
- **schedule**.

Available logic operators:

- **AND** – Conjunction,

- **OR** – Disjunction (logical sum),
- **XOR** – Exclusive disjunction,
- **NAND** – Negation of conjunction,
- **NOR** – Negation of disjunction,
- **XNOR** – Negation of exclusive disjunction (logical equivalence).

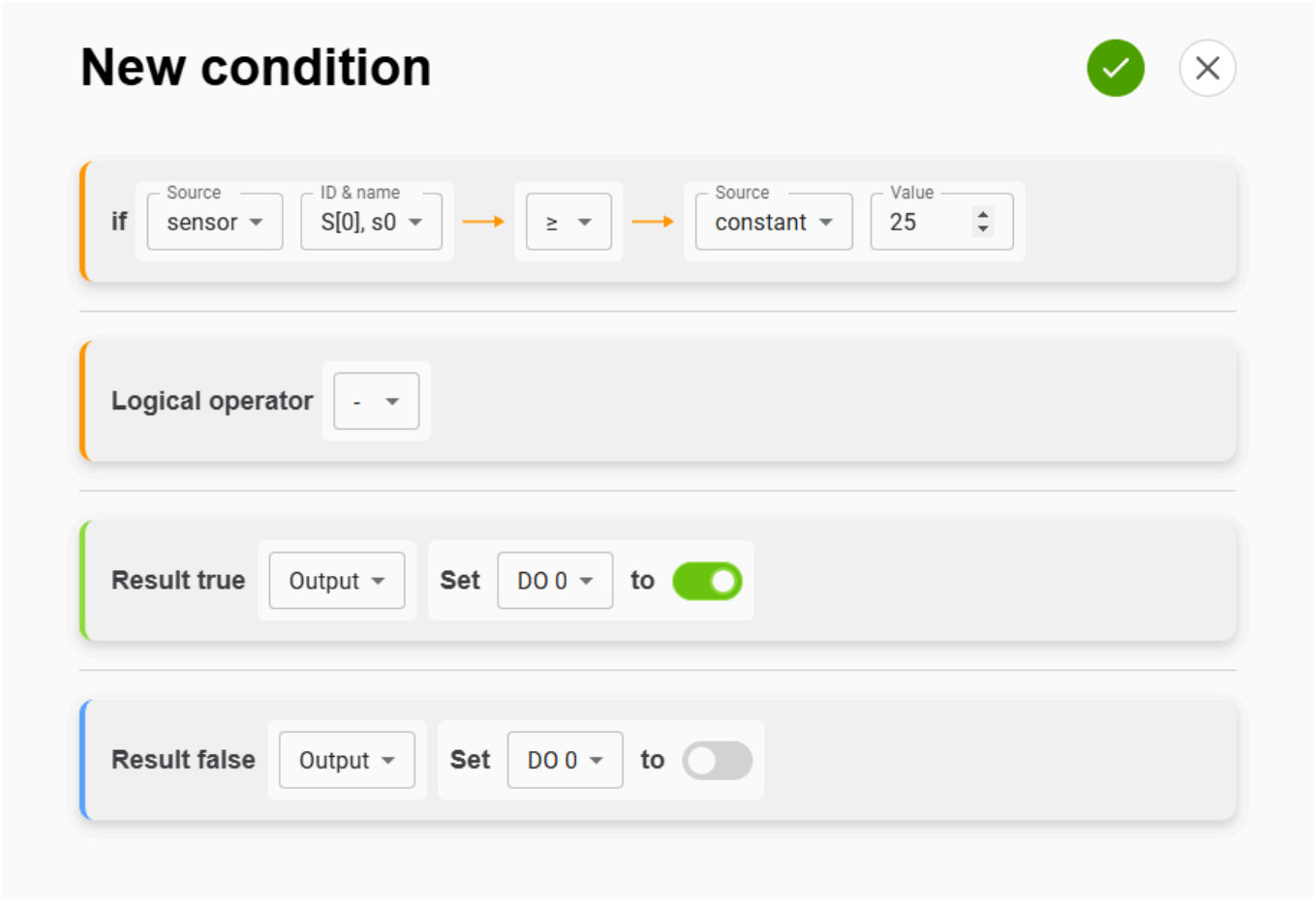
**Result True / Result False** – Reaction for meeting/not meeting the condition:

- **None**,
- **Output** – Output control,
- **Action** – Recall defined action,
- **Variable** – Virtual input/output control.

**Tip**

**All changes should be saved with**

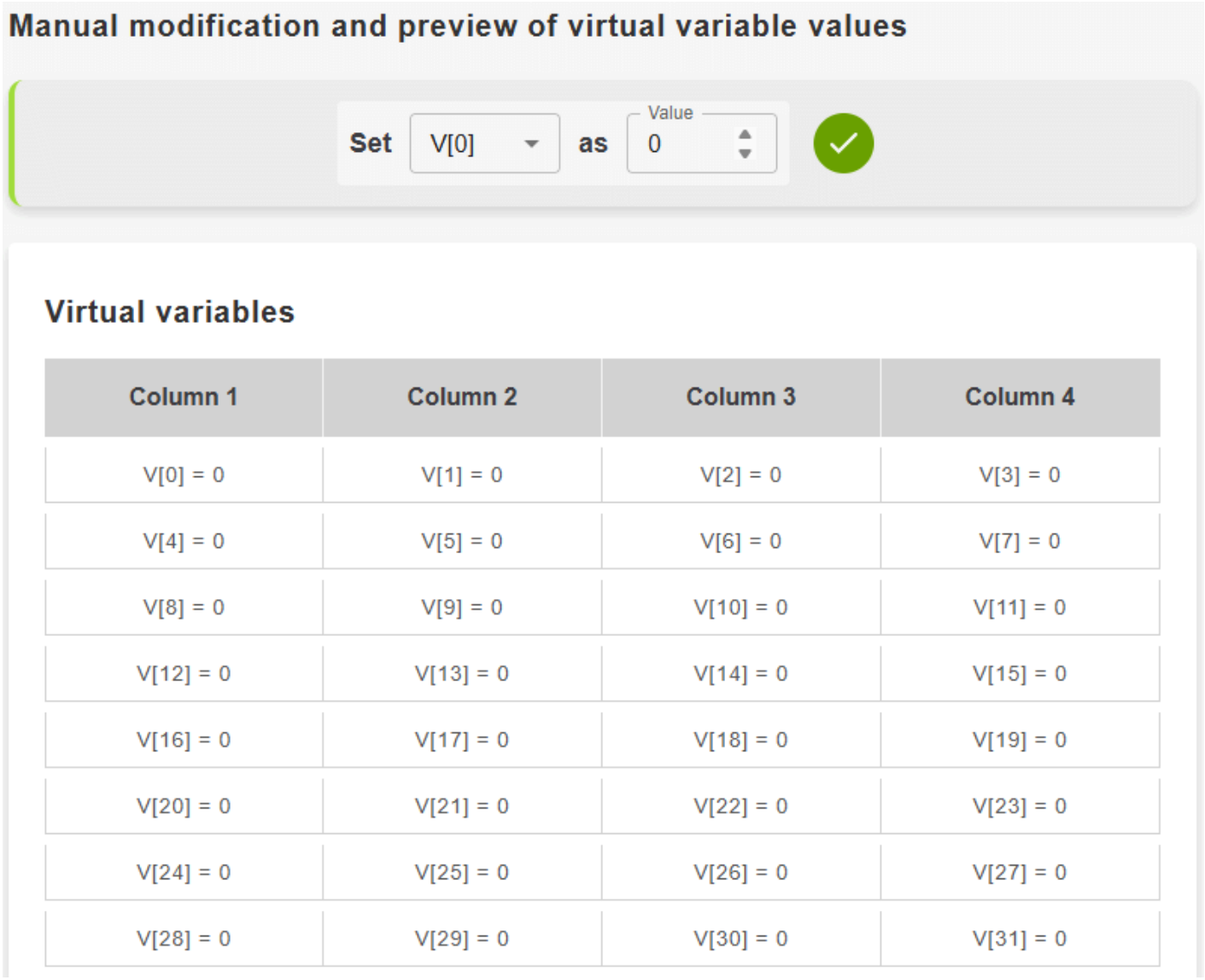
**Example**




**Output 1 will be activated as long as the sensor 0 temperature is greater than or equal to 25. If the temperature drops below this value, output 1 will be deactivated.**

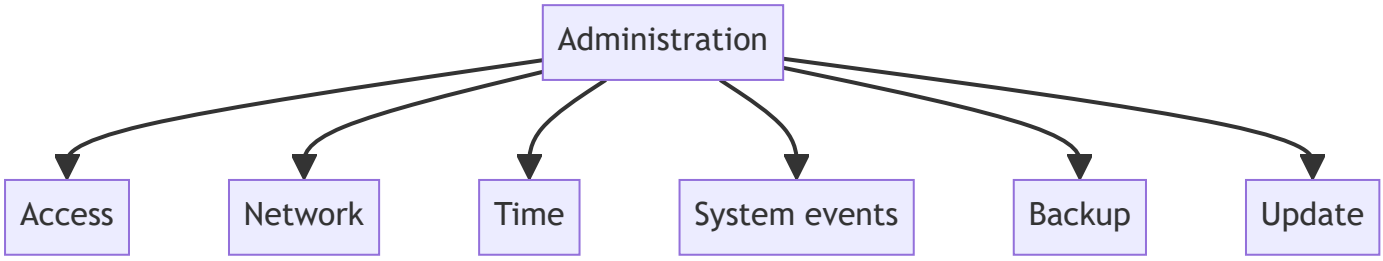
**Variables**

The **Variables** tab allows the user to define the values of internal variables.



## 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 |

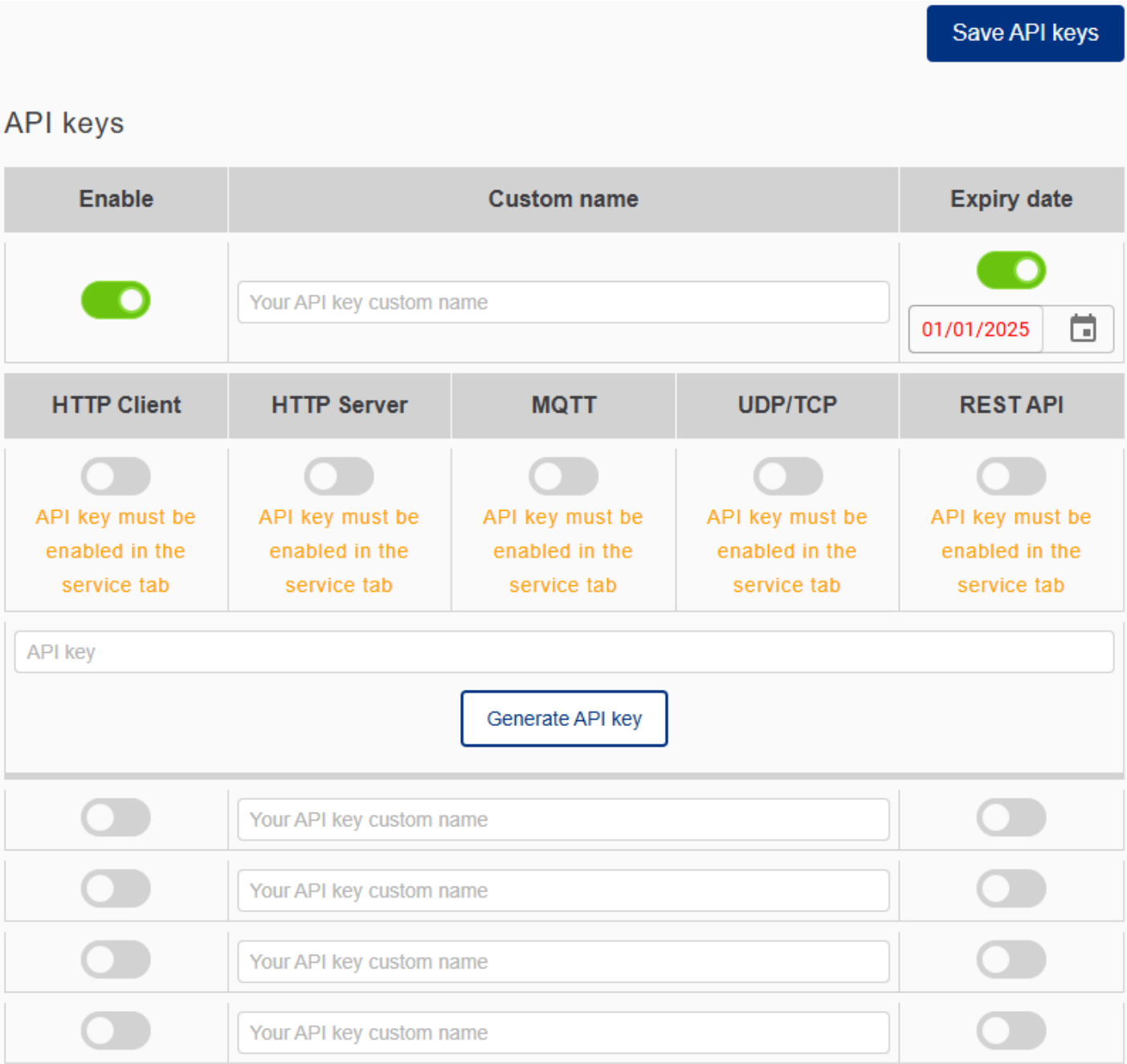
- **Password** – Enable/disable configuration password,
- **Current password**,
- **New password**,
- **Repeat new password**,
- **Module name** – Assigning an individual name to the module makes module identification in the system easier,
- **Enable remote config** – Enable/disable configuration via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

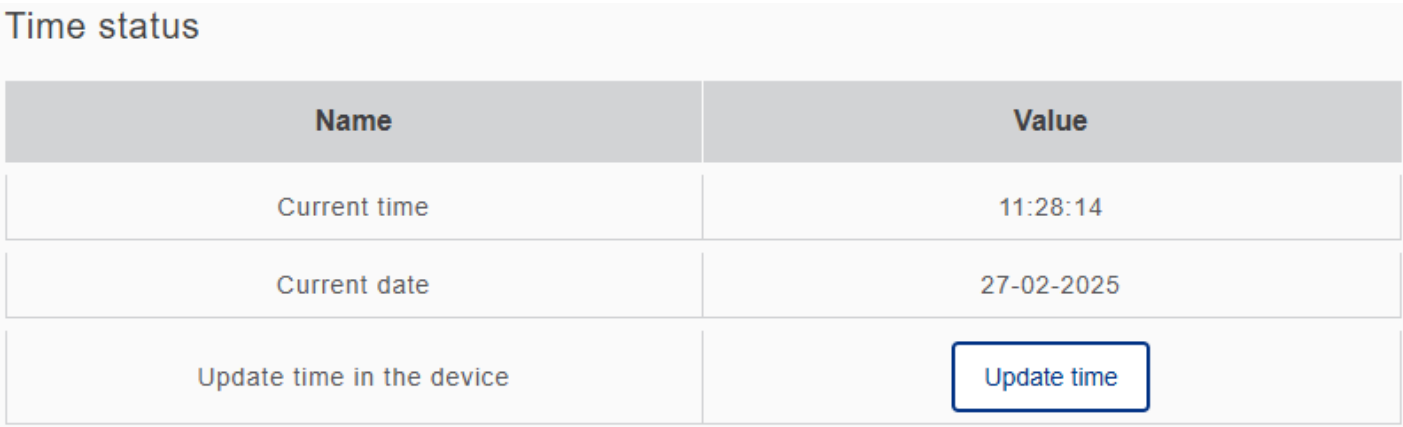
> **Tip**
>
> **Changes made in the API keys tab should be saved with Save API keys.**

**Network**

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

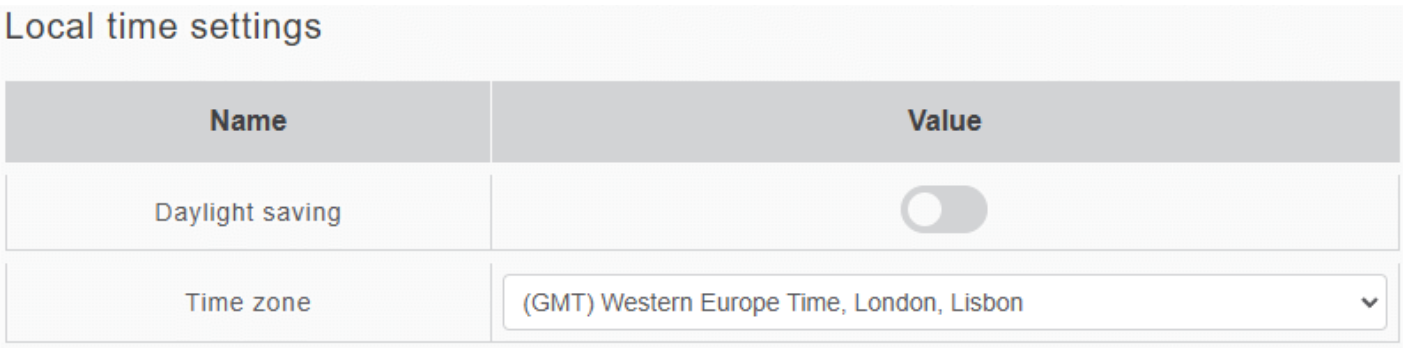
**Time**

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.

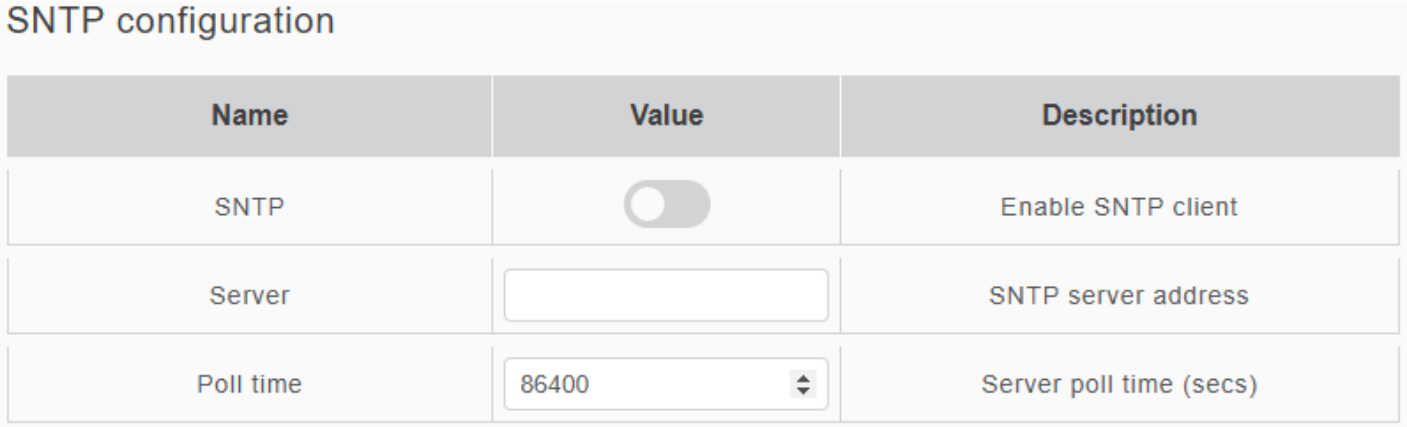



- **SNTP** – Enable/disable SNTP,

- **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**

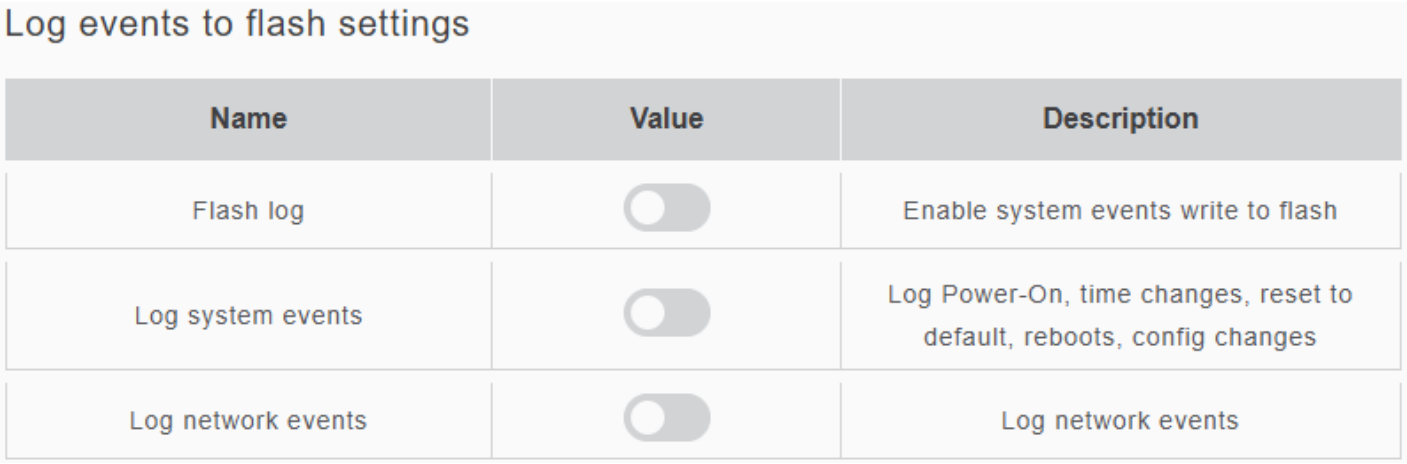
Additionally, the device is equipped with an internal RTC with battery backup. If the device does not have constant Internet access, it can use this clock to keep precise time.




- **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.

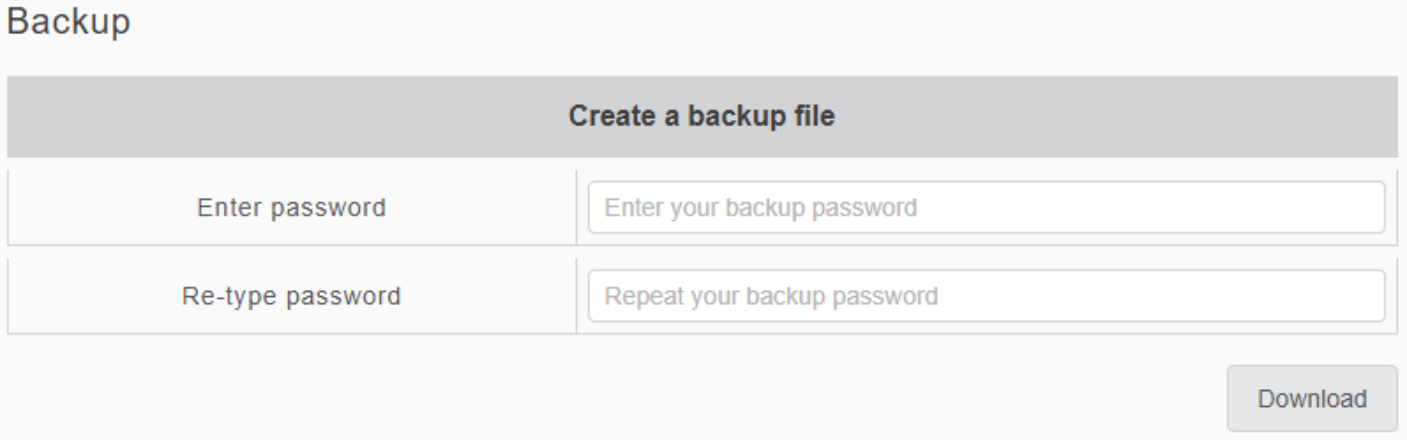



- **Flash log** – Enable/disable logging of events to flash memory,
- **Log system events** – Enable/disable logging of activations, time changes, factory settings restore, restarts, changes to configuration,
- **Log network events** – Enable/disable logging network events.

**Backup**

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

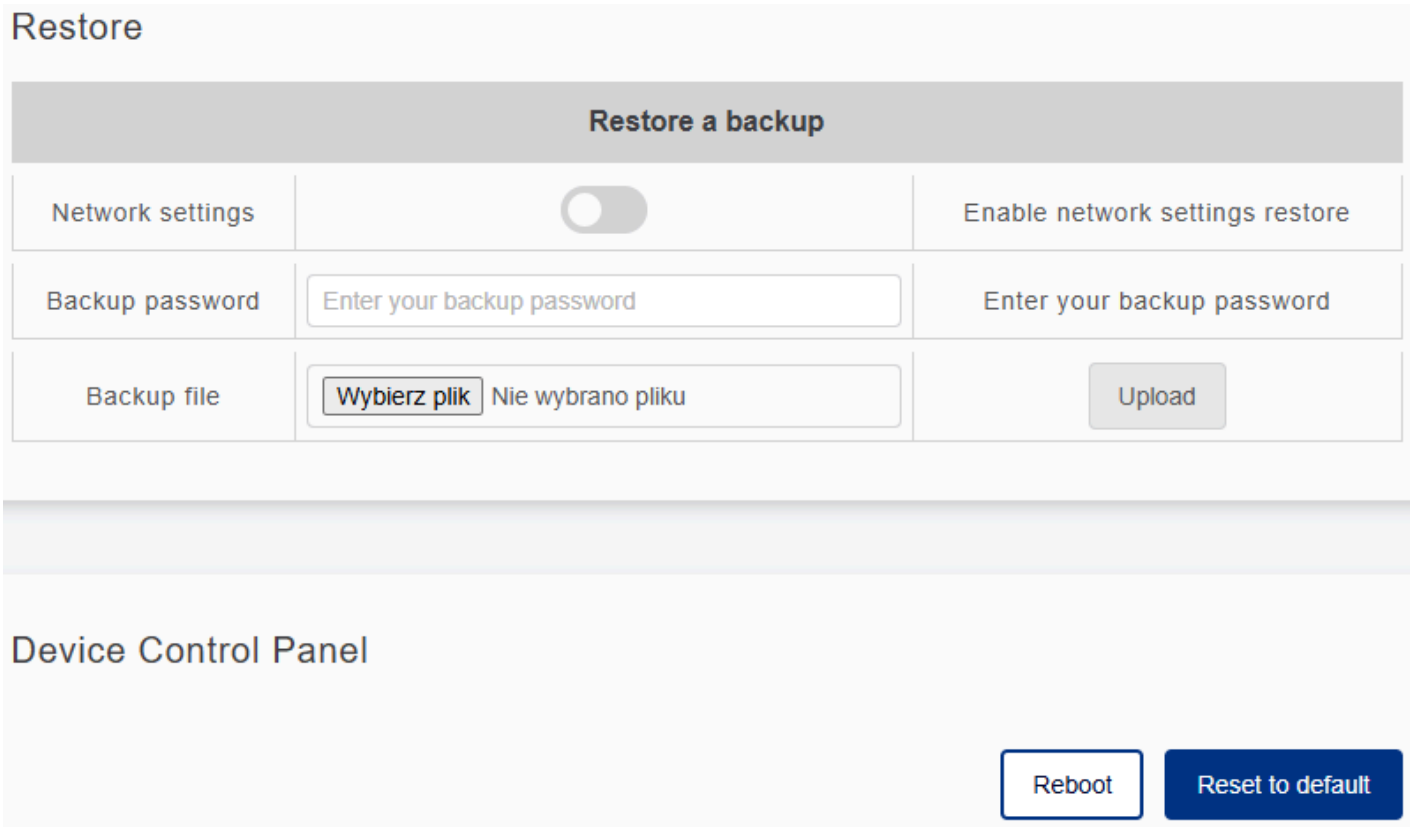
**Create a backup file**




- **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.

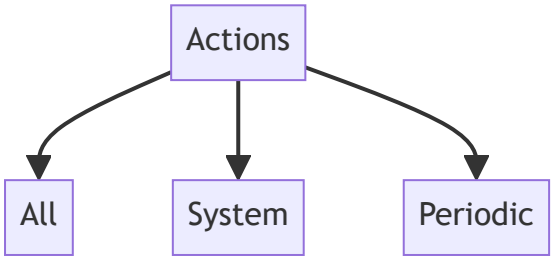
**Upload** – Uploads the selected backup to the device. **Reboot** – Allows the device to reboot. **Reset to default** – Allows the user to restore default settings.

# 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.

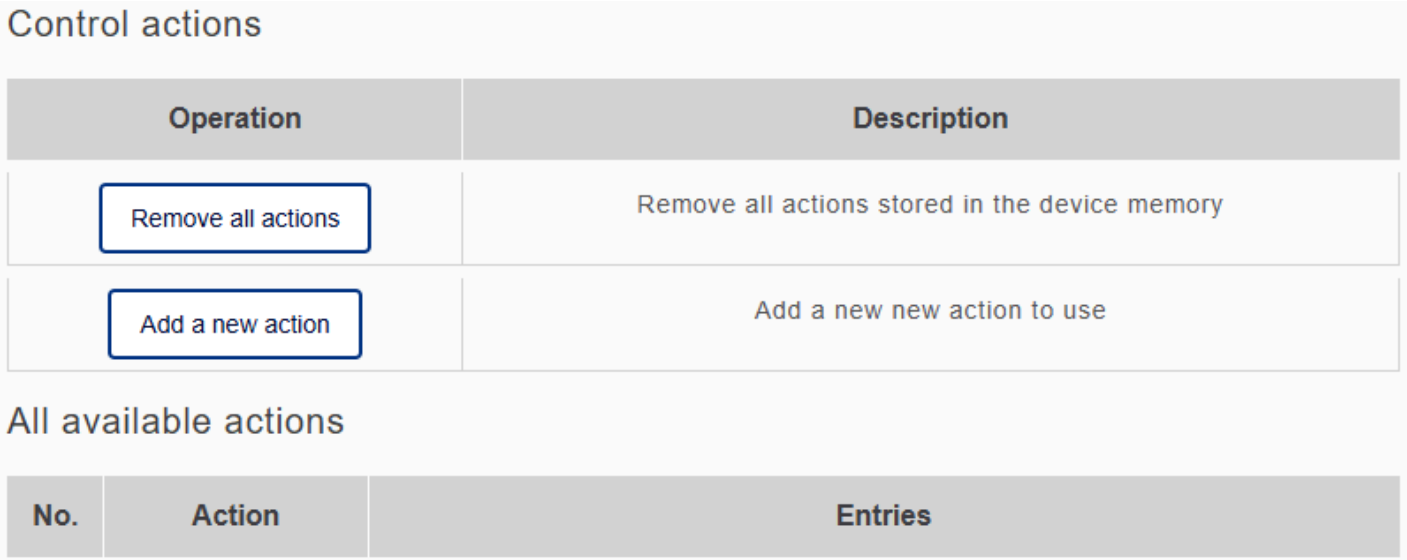
The actions are specific reactions of the module to received signals and input data, in accordance to the instructions set by the user. Many functions can be conducted by multiple methods depending on preferences and needs.



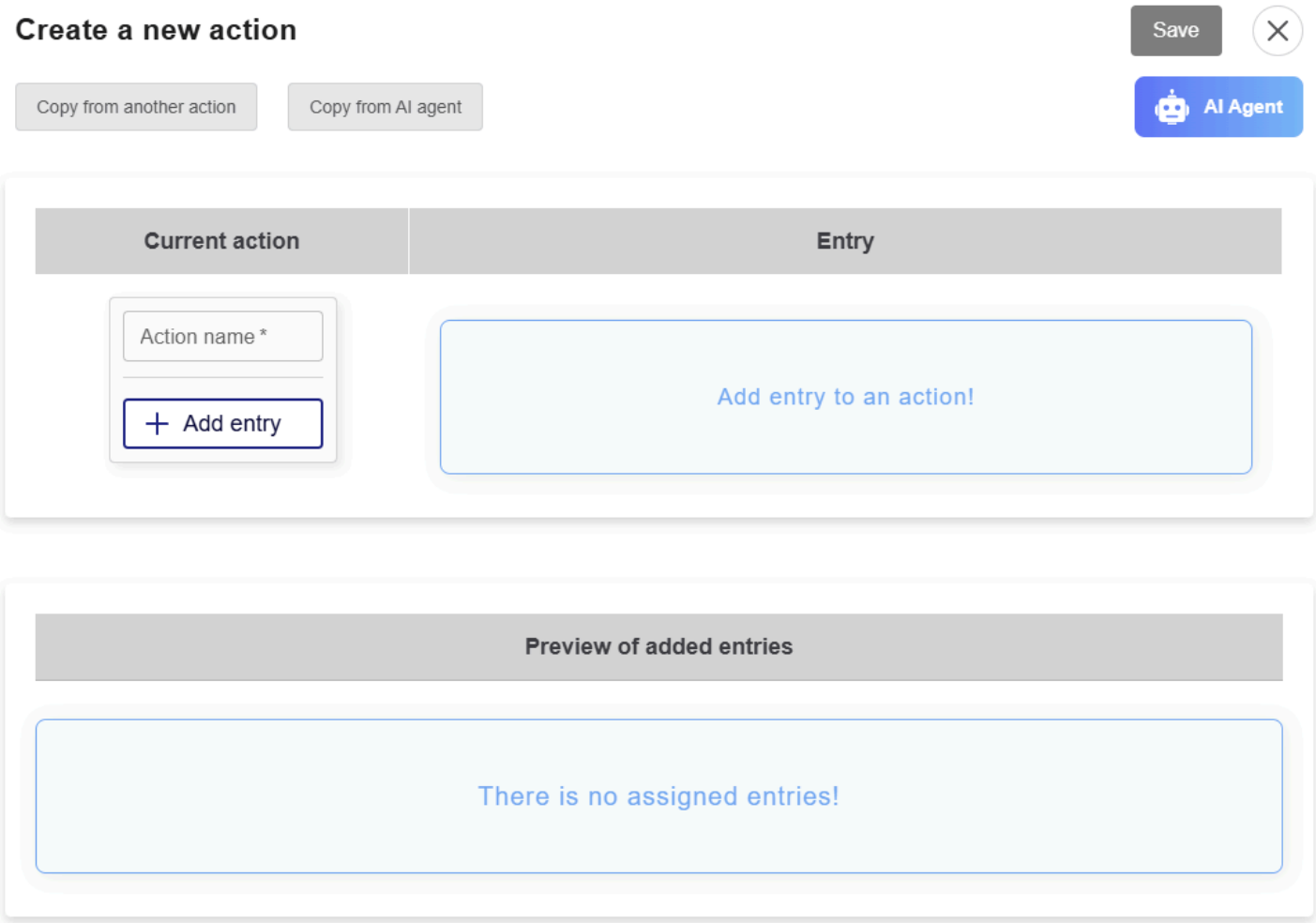

## All

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 –

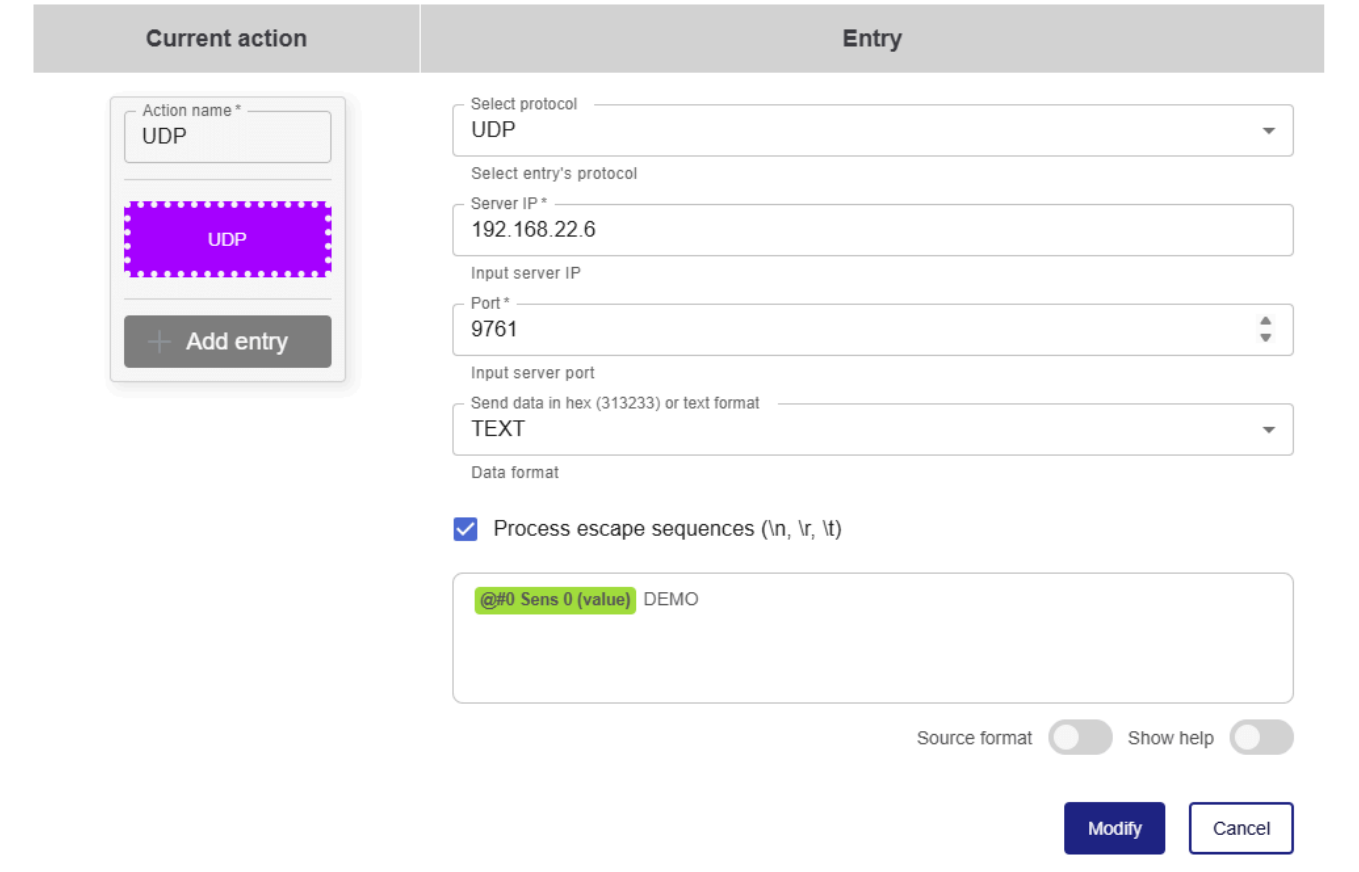
## Protocol configuration

**UDP**

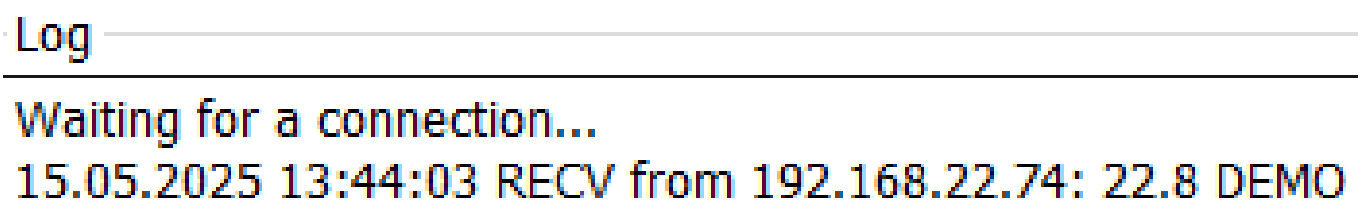
- **Server IP** – Target IP address,
- **Port** – Port, on which the target device is listening,
- **Format** – Data format: **TEXT** or **HEX**,
- **Input data** – Command sent to the target device.

**Example**

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




**Sent data:**

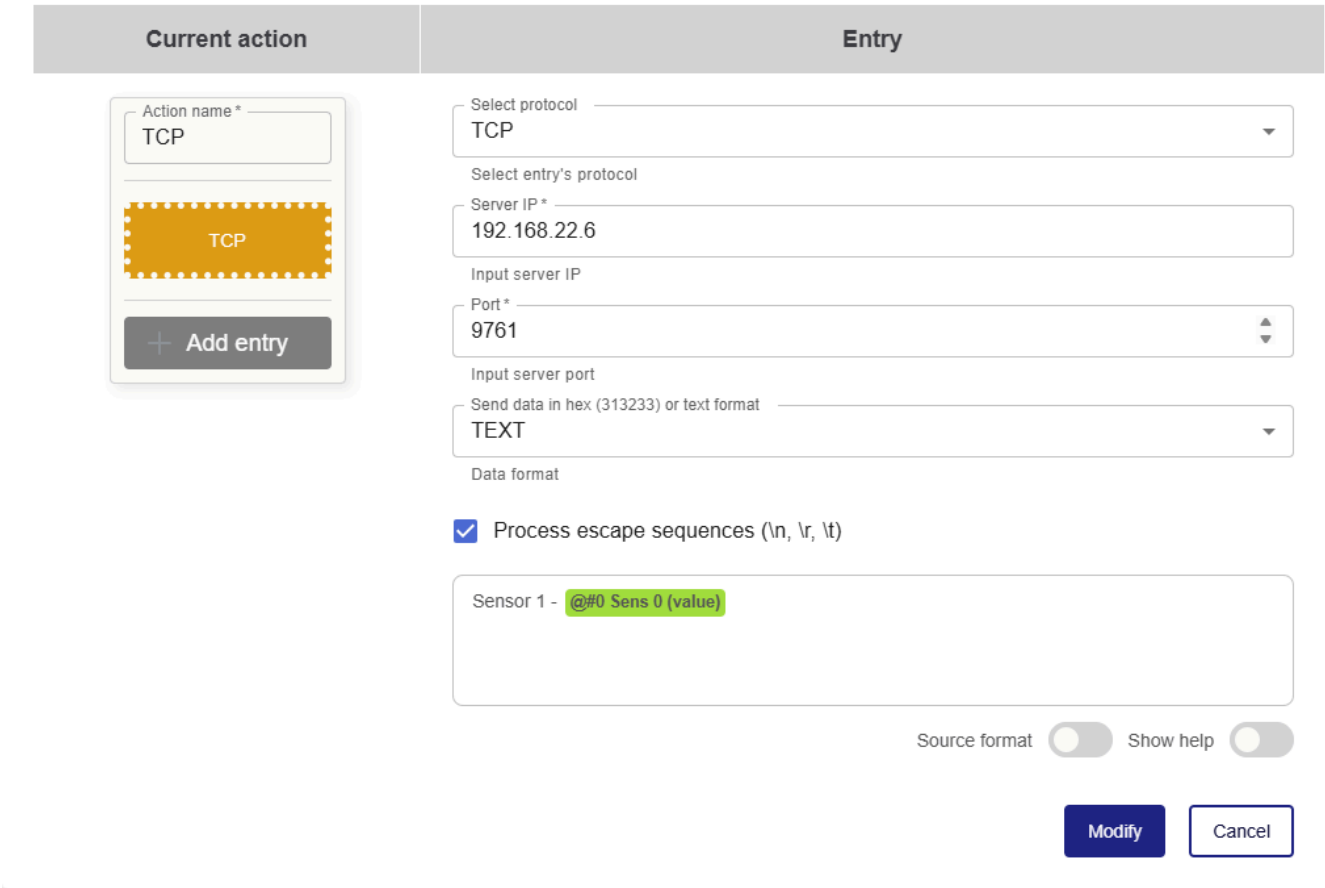


**TCP**

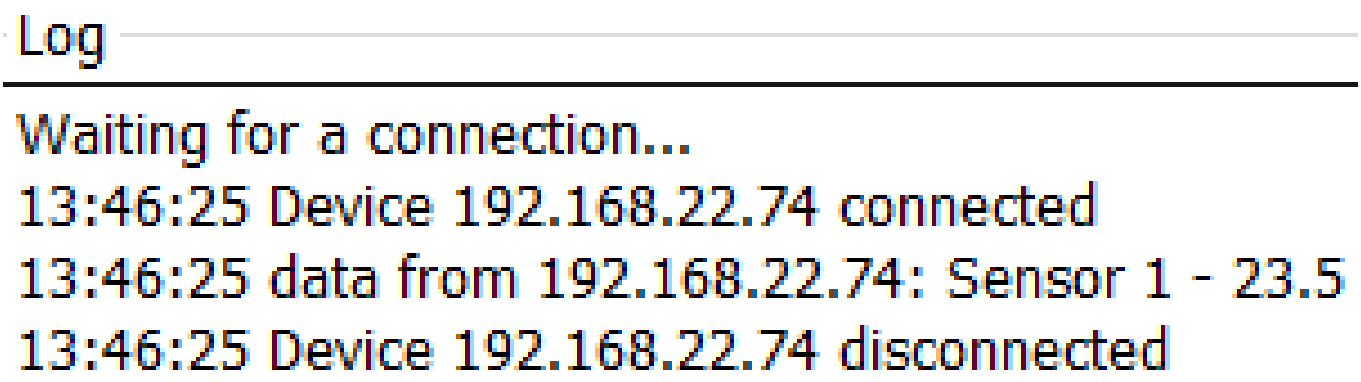
- **Server IP** – Target IP address,
- **Port** – Port, on which the target device is listening,
- **Format** – Data format: **TEXT** or **HEX**,
- **Input data** – Command sent to the target device.

**Example**

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




**Sent data:**



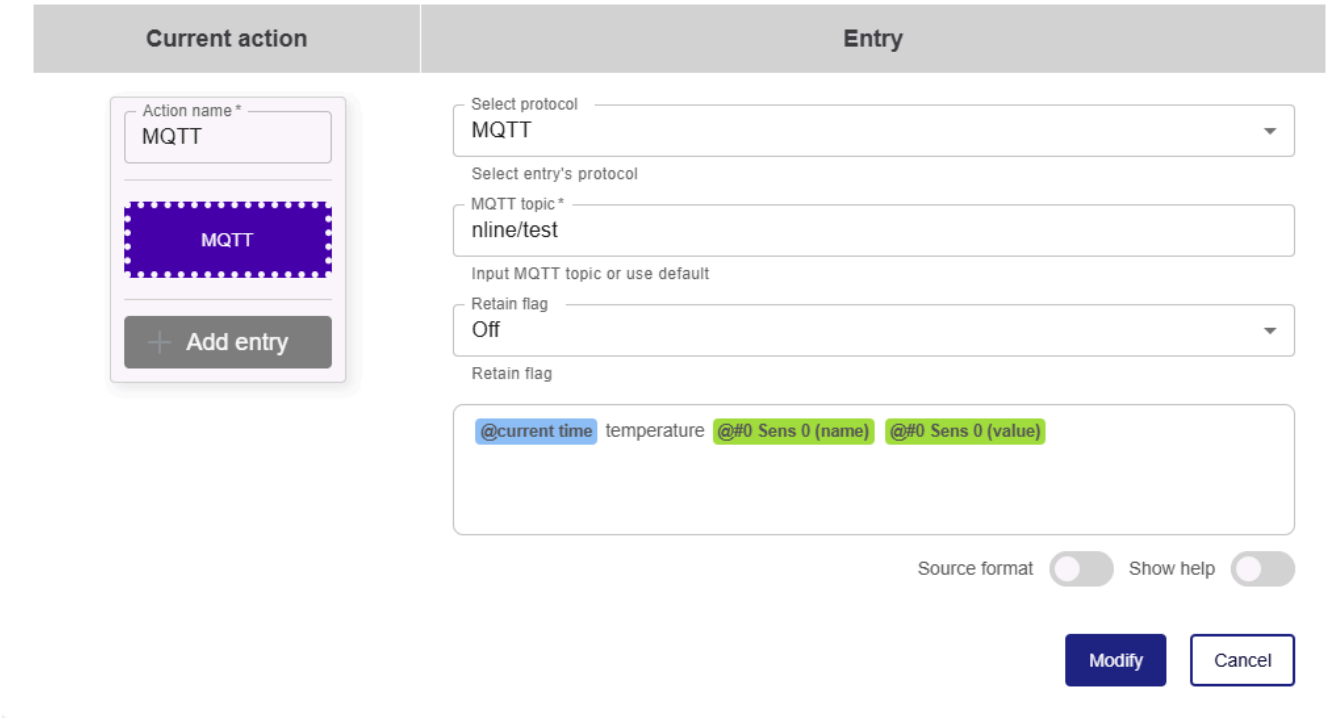
### MQTT

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

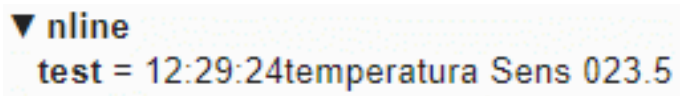
- **MQTT topic** – Topic, the device sends data to,
- **Retain flag** – Activated option causes the broker to retain last messages for topics the device sends data to,
- **Input data** – Message payload.

**Example**

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




**Sent data:**

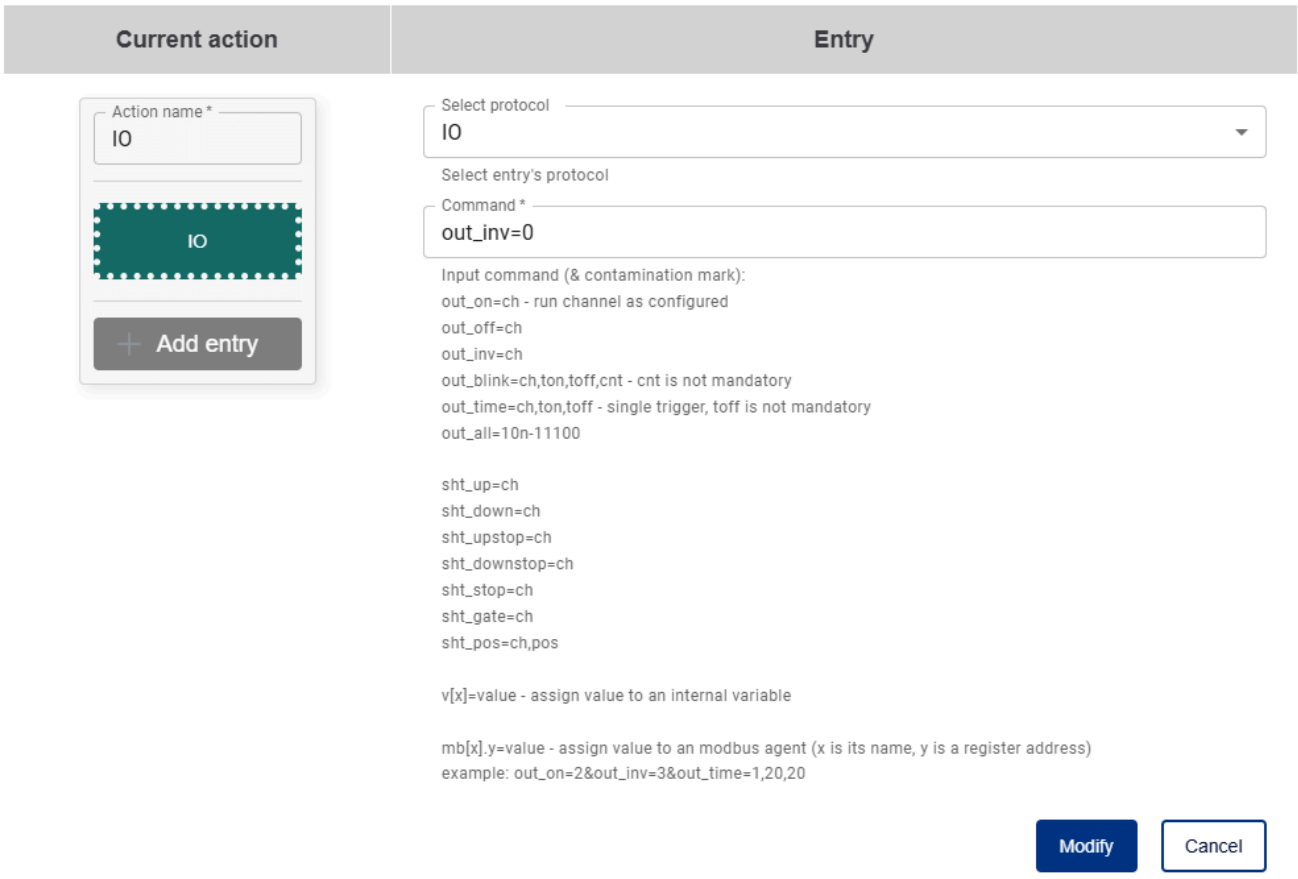


### IO

- **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.**

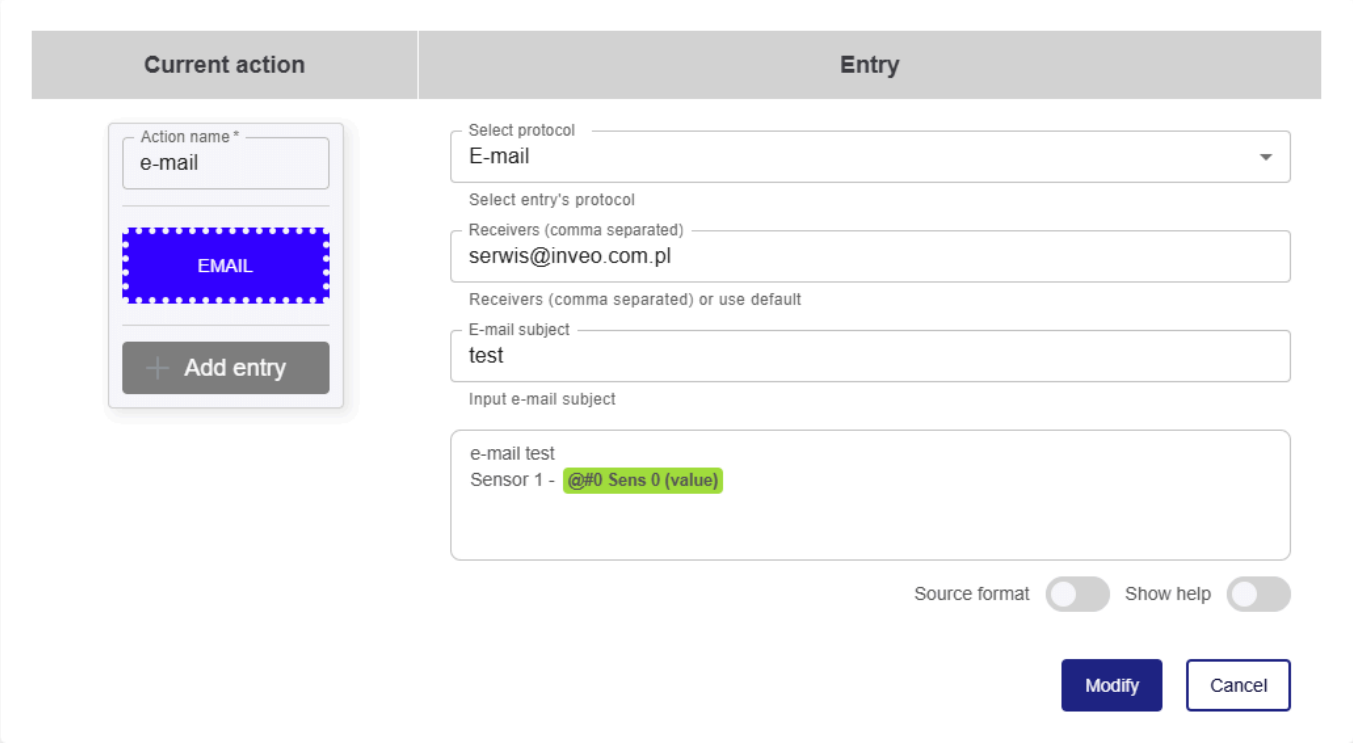
### E-mail

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]%`



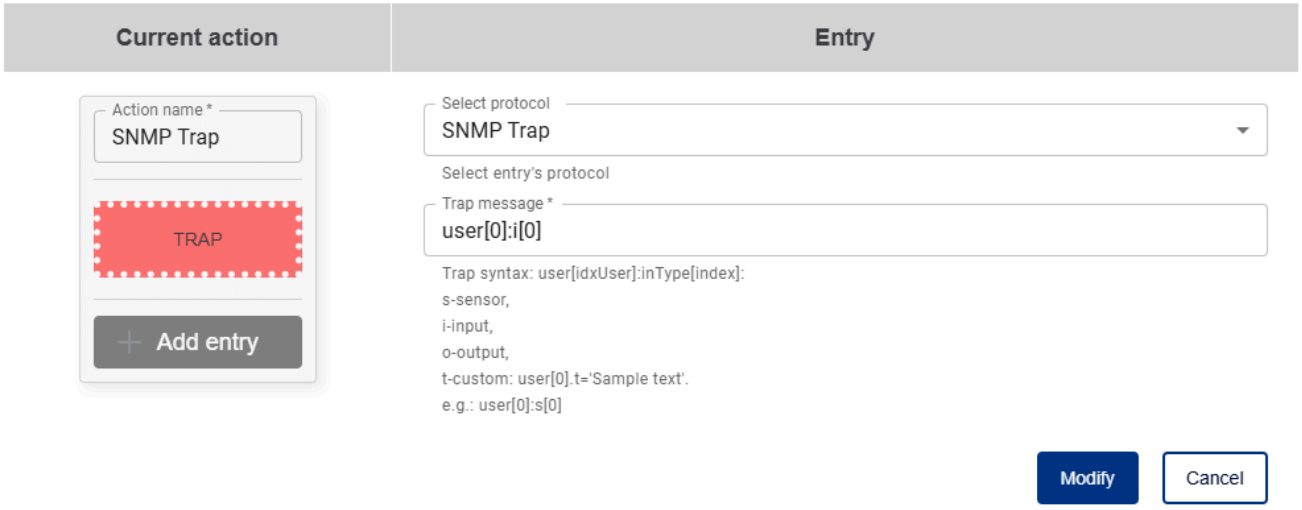

**Those settings will cause an e-mail with the topic of `test`, with the contents of `e-mail test Input 1 -` and current input state to be sent to test1@test.com.**

### SNMP Trap

- **Trap message** – Message syntax.

**Example**

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




**Sent data:**

| Description | Source | Time |
|---|---|---|
| .1.3.6.1.4.1.42814.10.1.1.100.0.5 | 192.168.22.74 | 2025-05-15 13:55:12 |

## System

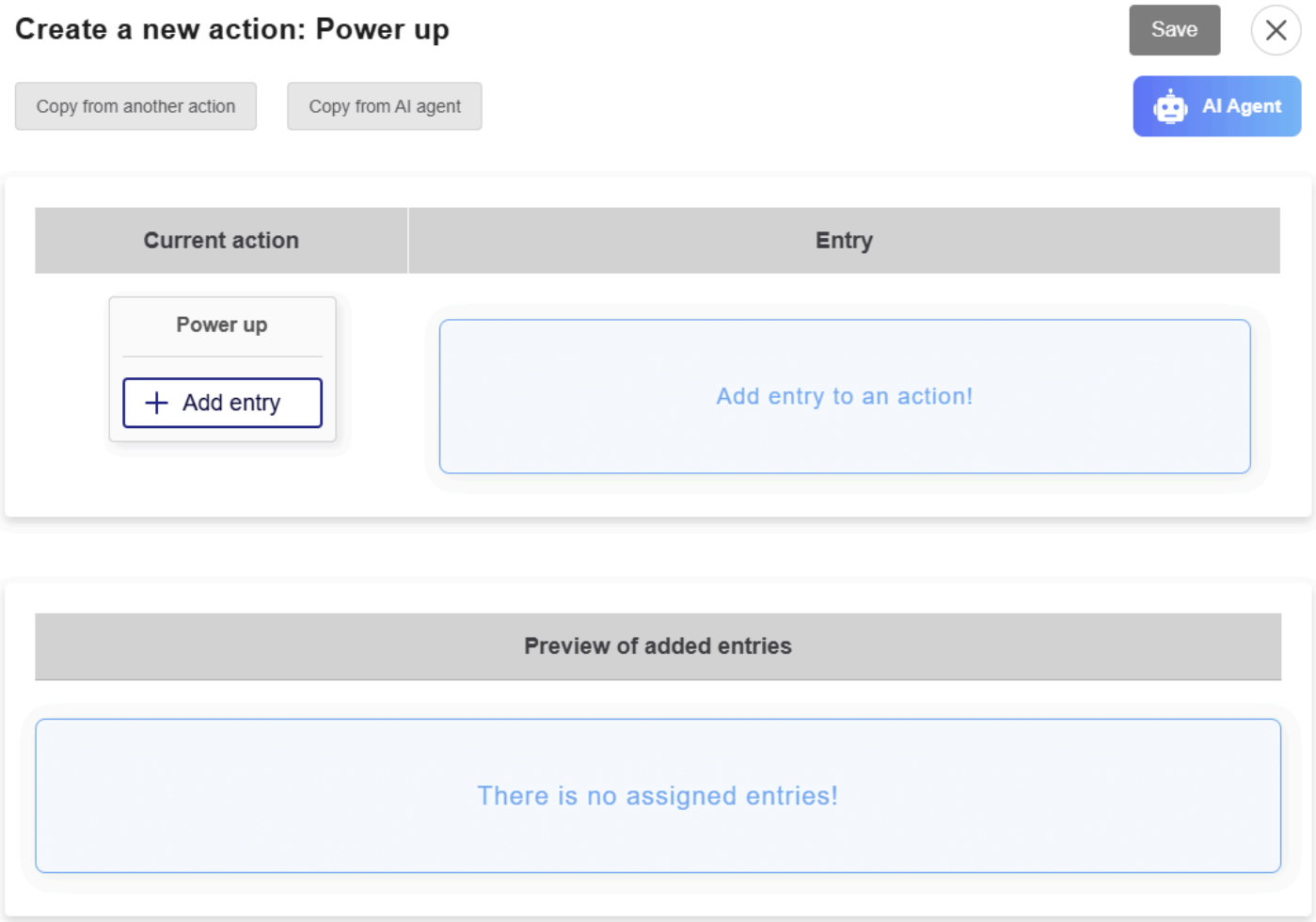
This tab allows the user to define system actions which the device will perform in the following events:

All constant actions

| Action type | Entries |
| --- | --- |
| Power up | |
| Ethernet up | |
| Ethernet down | |

- **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.

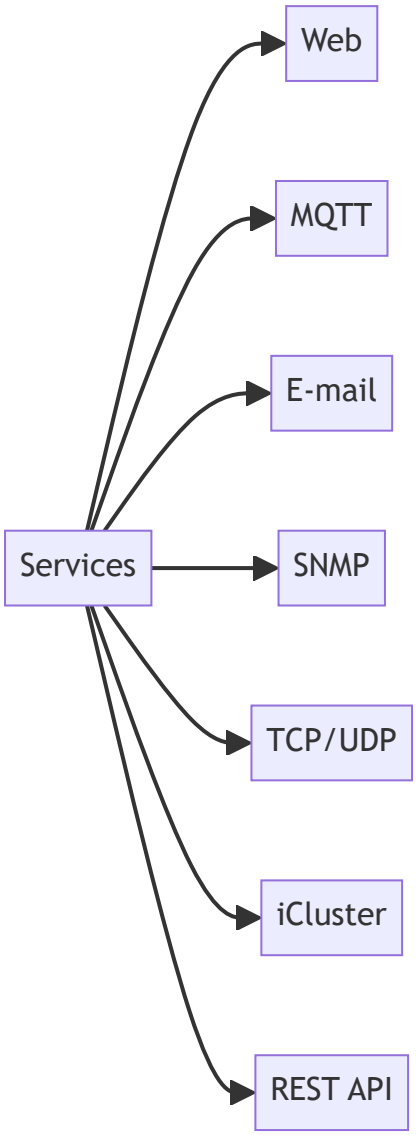
After defining all required settings, save the changes using .

## Periodic

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

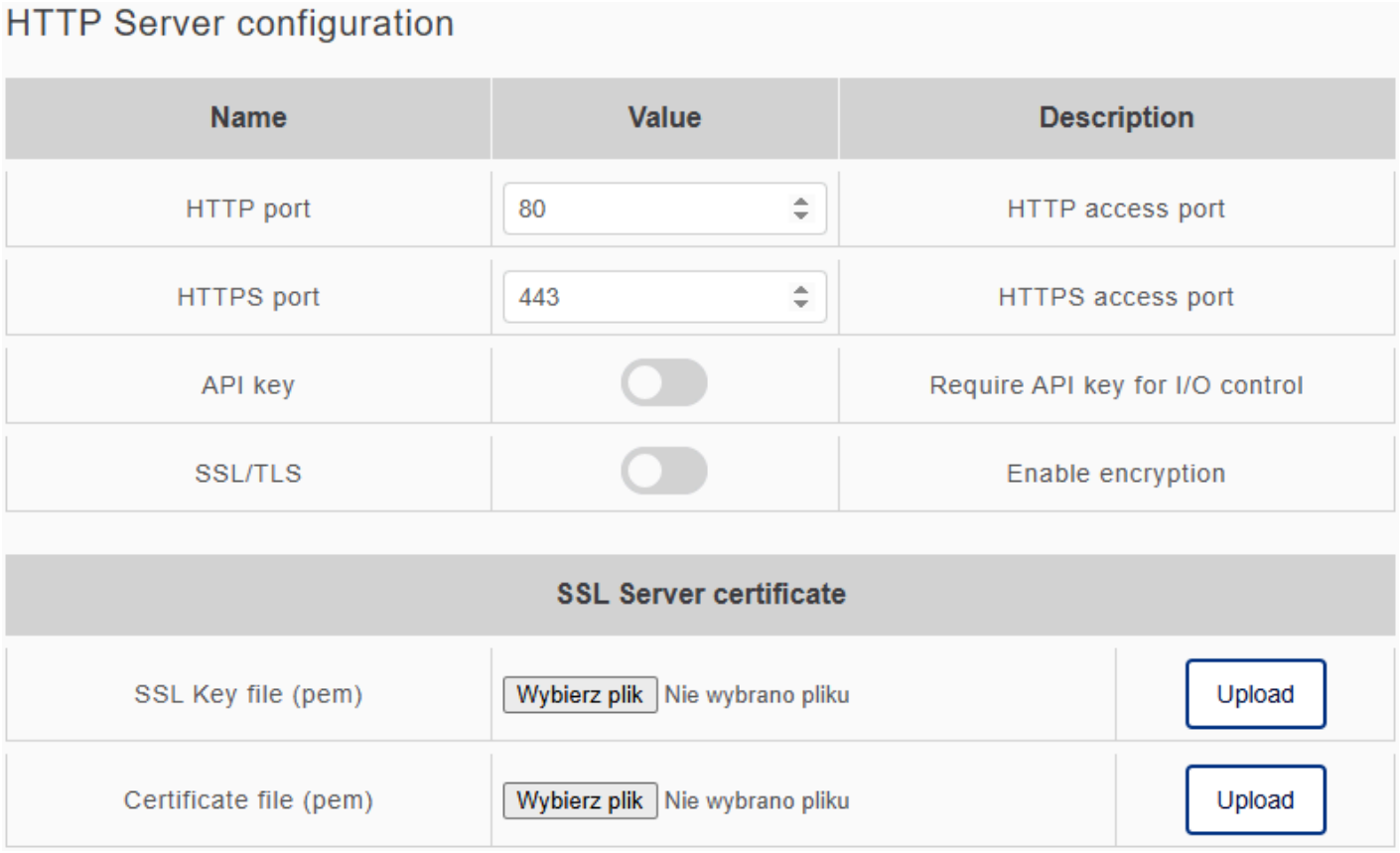
## Communication protocols

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



## Web

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



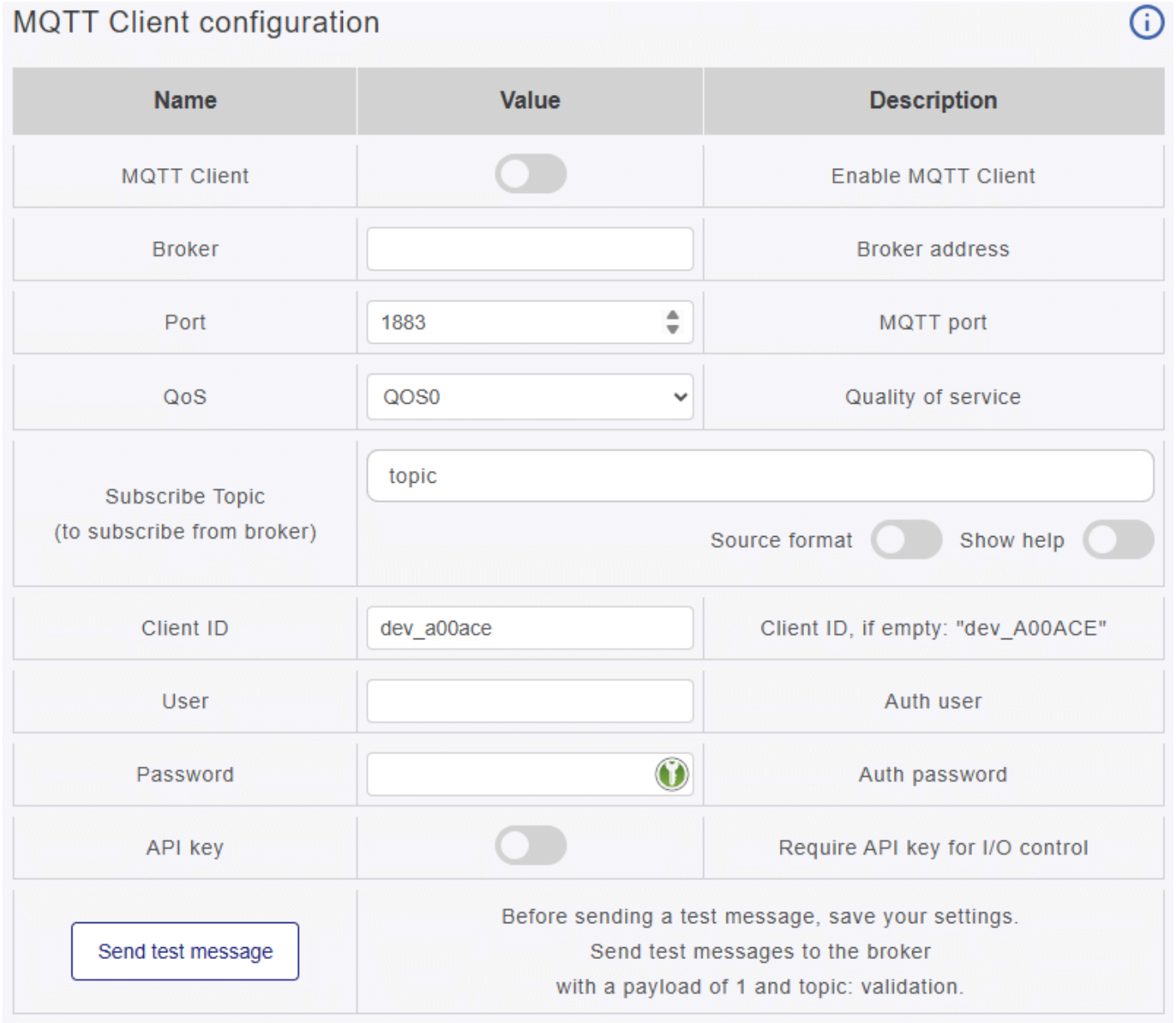

- **HTTP Port**,
- **HTTPS port**,
- **API key** – Enable/disable API key requirement for I/O control,
- **SSL/TLS** – Enable/disable encryption,
- **Select Key file (pem)** – Allows upload of SSL server key (pem format),
- **Select CSR file (pem)** – Allows upload of CSR server key (pem format).

## 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.

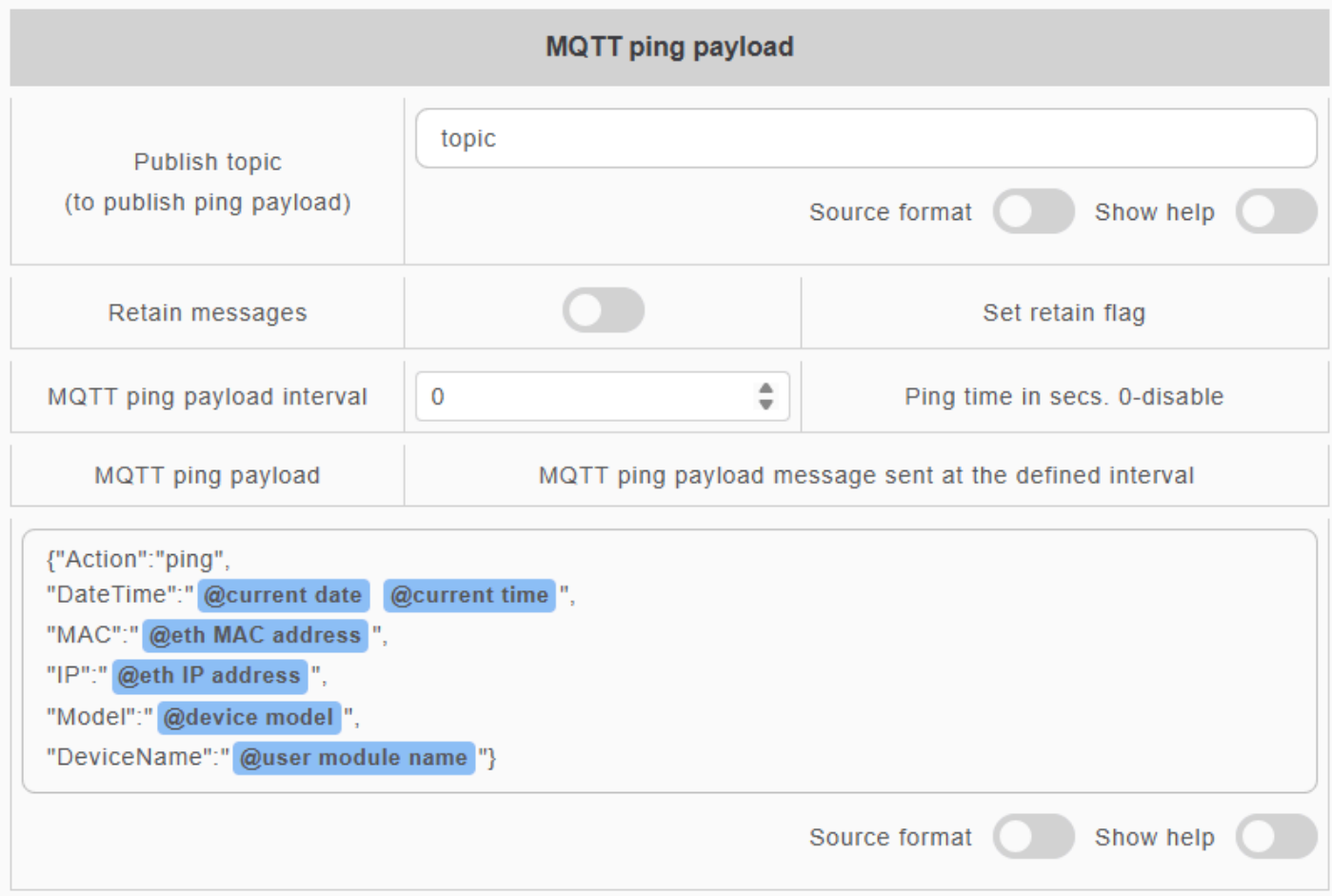
The data stream can be encrypted. After a connection with the MQTT broker is established, the users can subscribe to the data coming from the device.

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



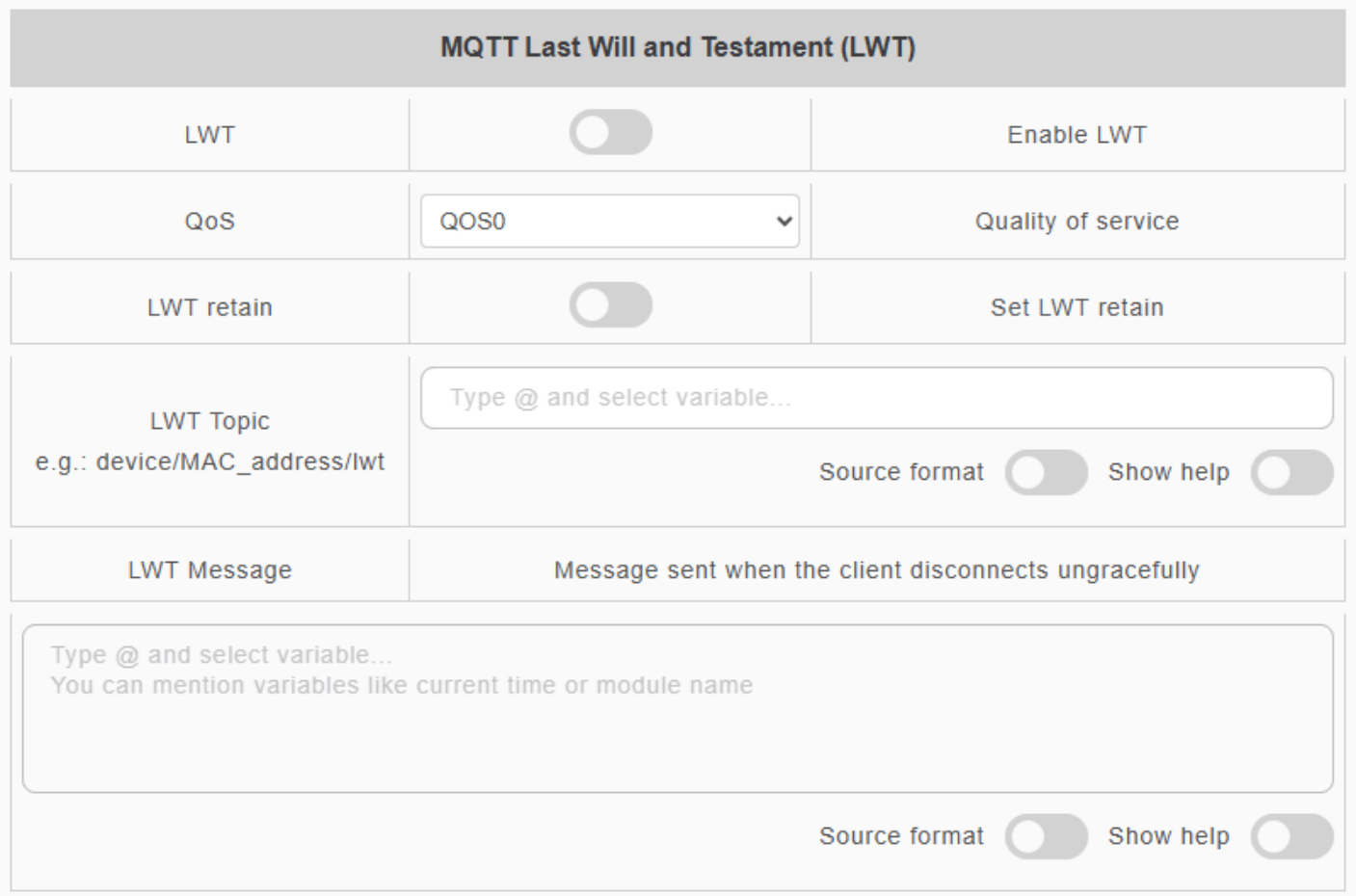

- **MQTT Client** – Enable MQTT service,
- **Broker** – MQTT broker address,
- **Port** – Port, on which the server listens (commonly 1883),
- **QoS** – Quality of Service level. Can assume one of three values: 0 (At most once), 1 (At least once), 2 (Exactly once),
- **Subsribe topic** – The topic must 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.

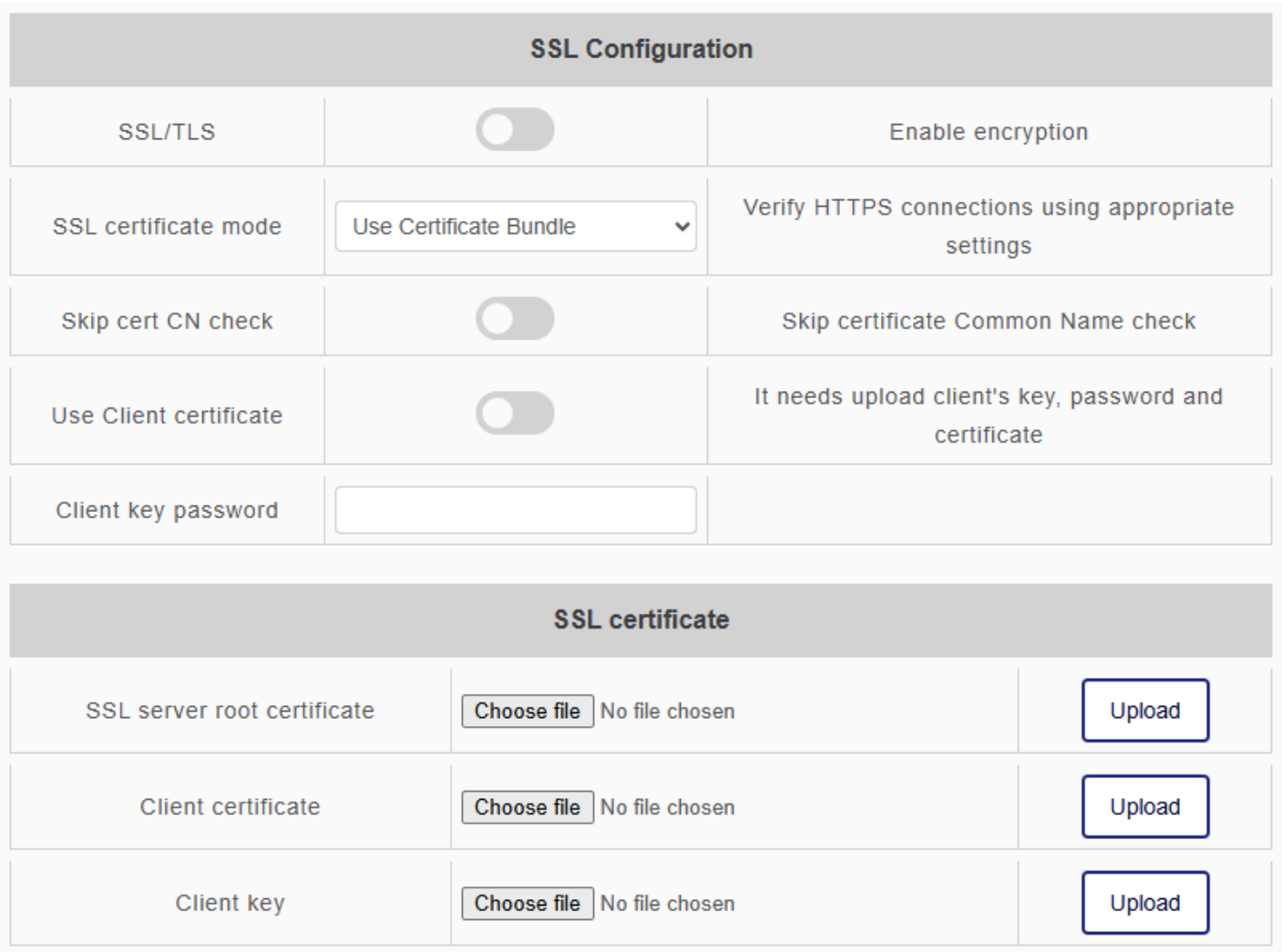



- **Publish topic** – Topic, to which data will be sent periodically,
- **Retain messages** – If enabled, the message will be saved on the broker an will be available for new topic subscribers,
- **MQTT ping payload interval** – Time interval between the data packets. Setting `0` disables the function,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

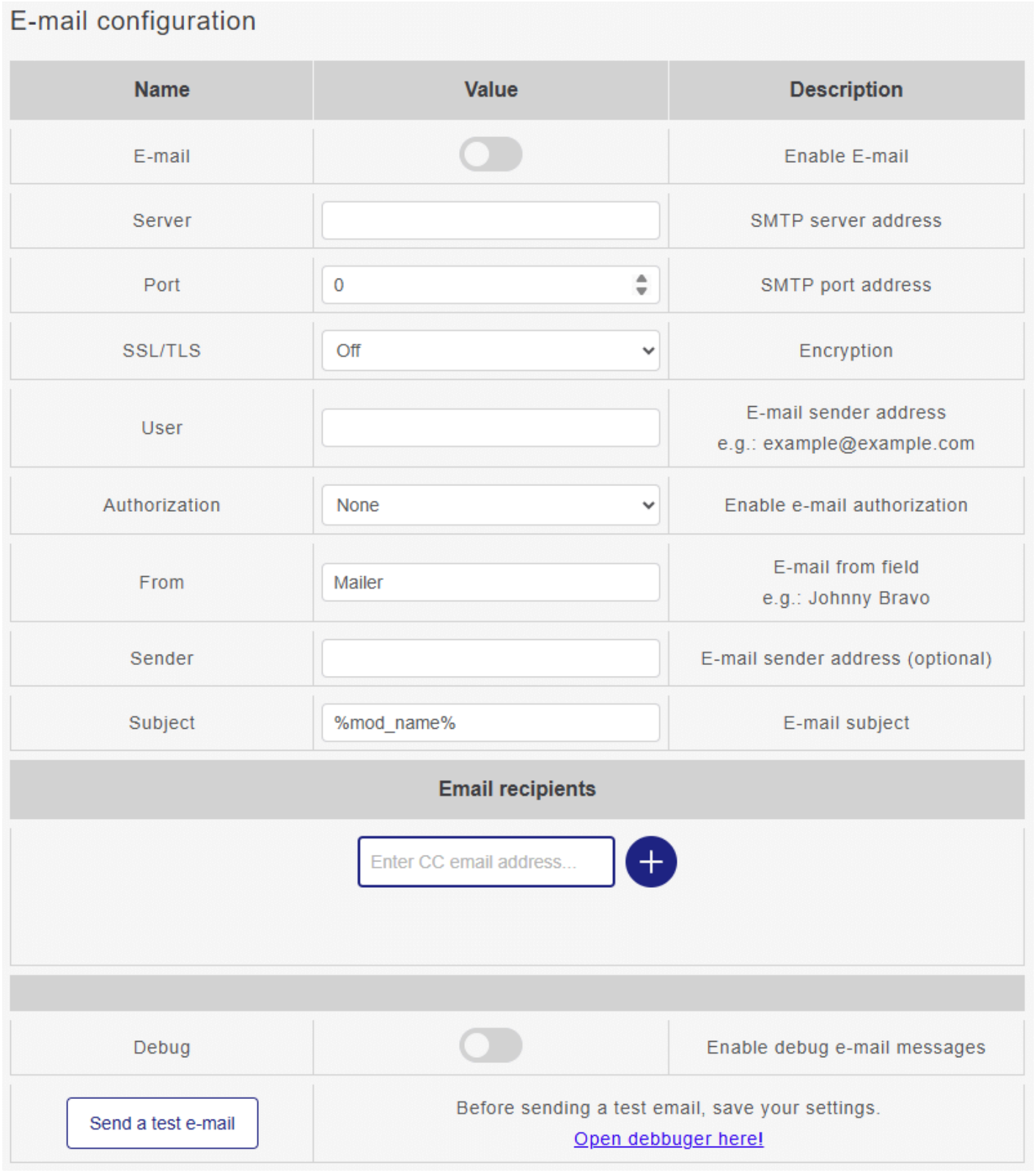
**For the Inveo broker, the settings should be as follows:**
- MQTT Address**: mqtt.inveo.com.pl**
- MQTT Port**: 1883**
**A computer with the Inveo Monitoring application installed can be used as a broker. To do that, type the PC's IP address into the MQTT Address field.**

**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.



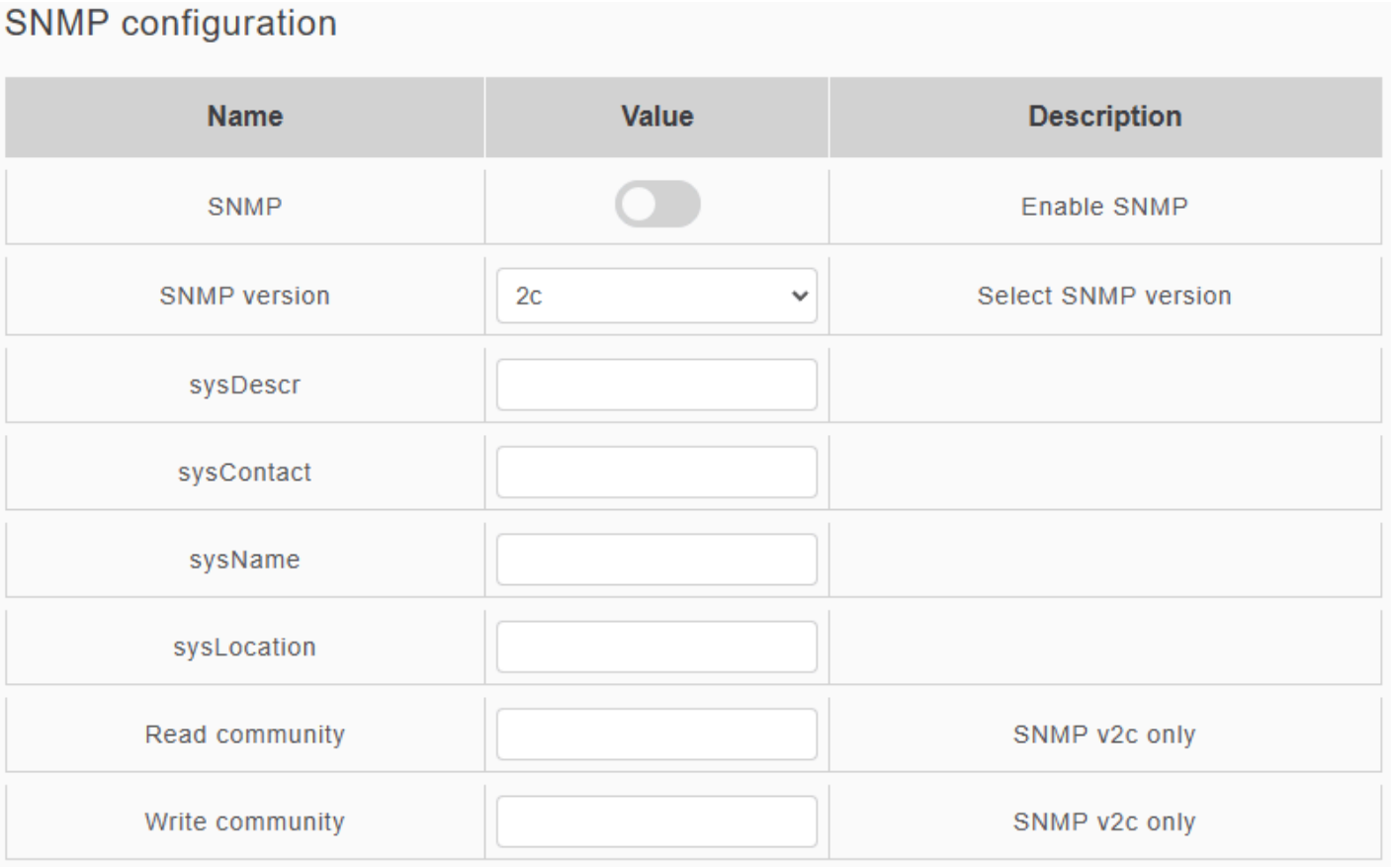

- **E-mail** – Enable/disable e-mail service,
- **Server** – SMTP server address,
- **Port**,
- **SSL/TLS** – Encryption:
  - **Off**,
  - **SSL**,
  - **STARTTLS**.

- **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**.

## SNMP

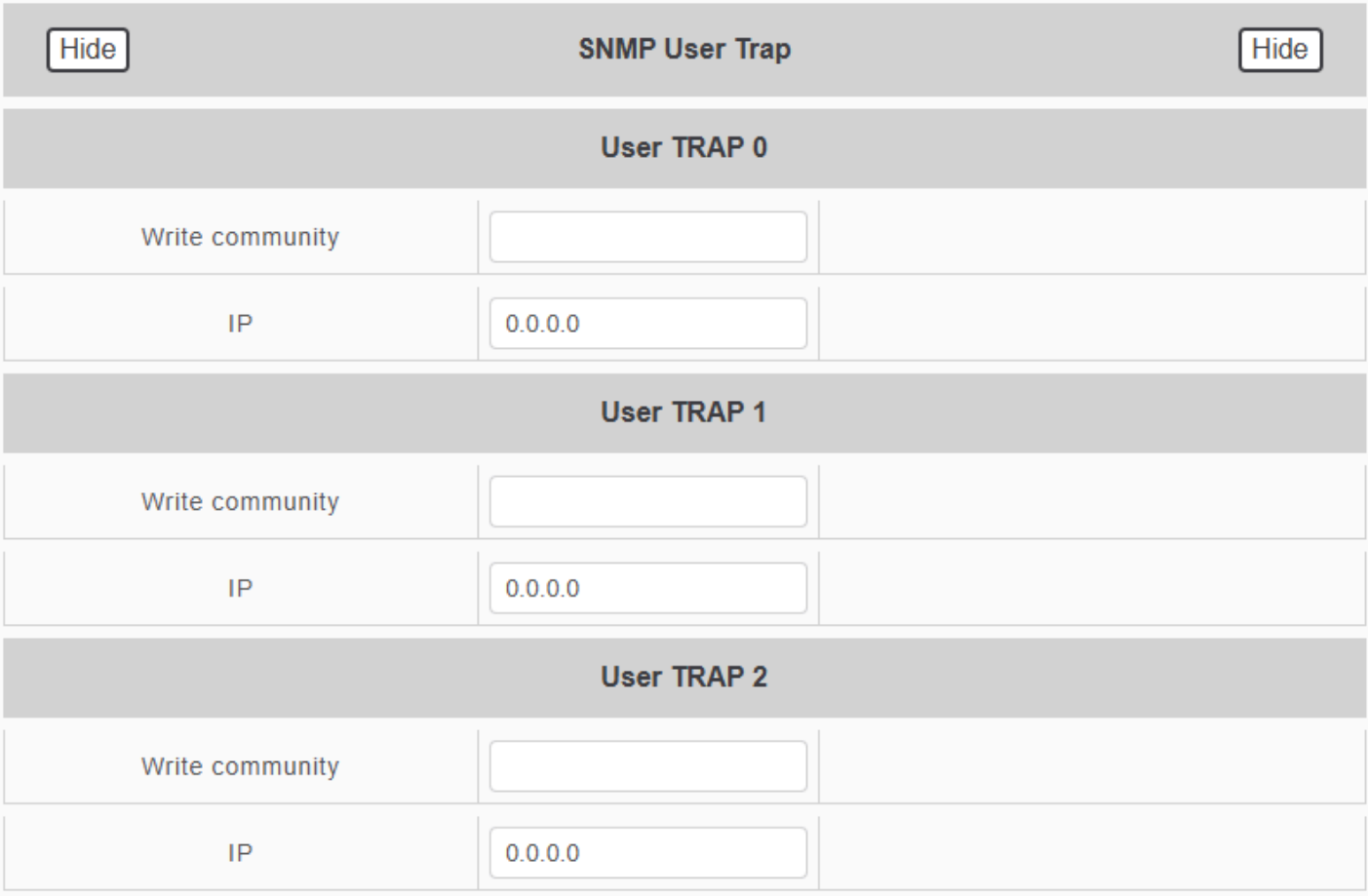
This section allows configuration of SNMP protocol settings, used for monitoring and network device management. The module is equipped with the v2c or v2c and v3 *(version dependent)* SNMP servers. Depending on the SNMP version selected, different parameters are available.

**SNMP v2c**




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

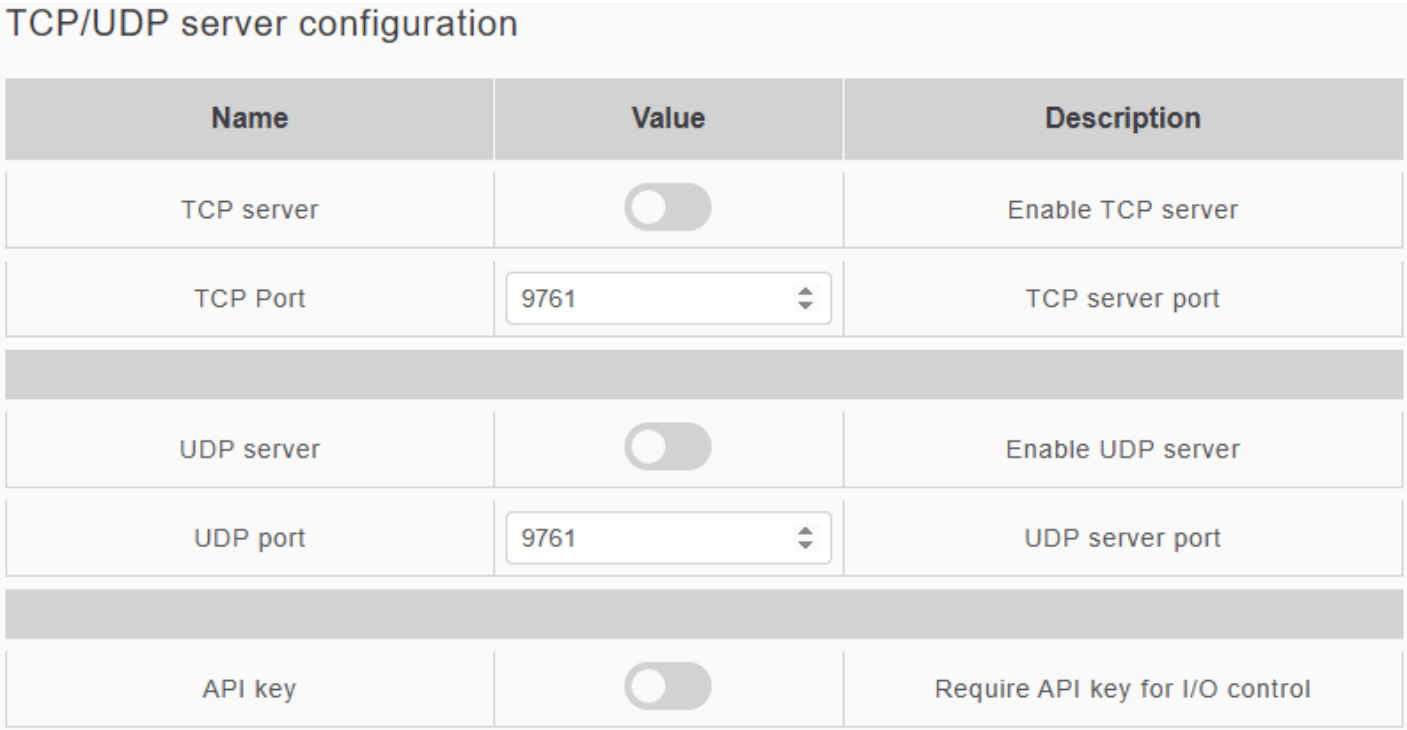
- **Read community** – Data read password,
- **Write community** – Data write password.




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

### TCP/UDP

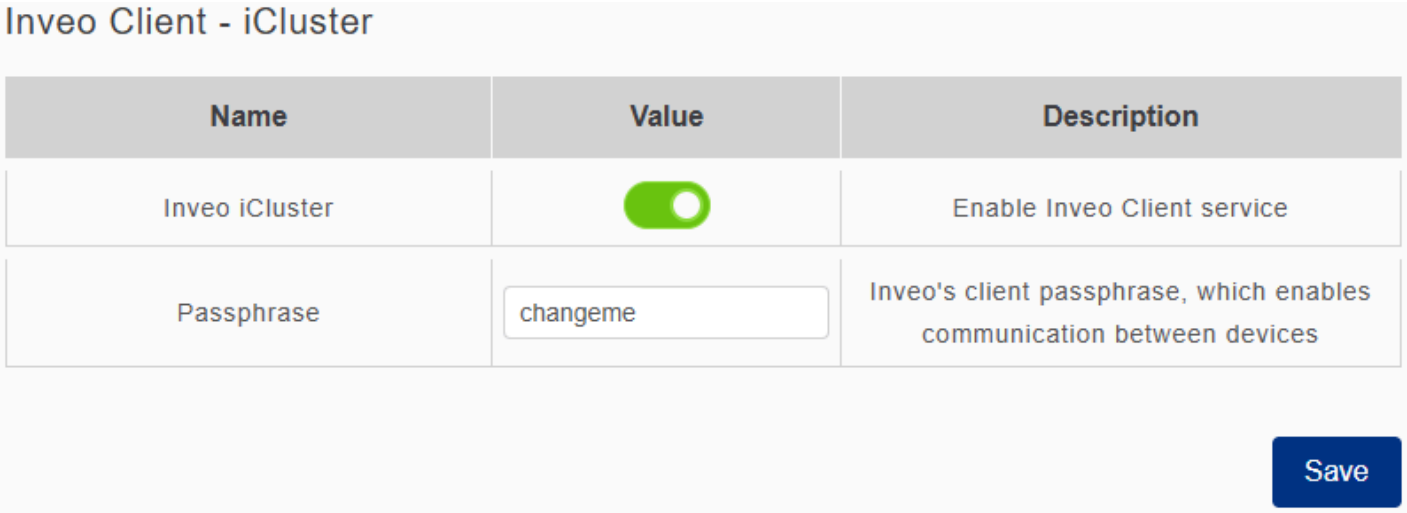
This tab allows the user to enable and configure TCP and UDP protocols support. The user can customize settings such as ports and communication parameters, providing flexibility in device configuration in compliance with network requirements. By sending commands to the device's IP address and port using 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.

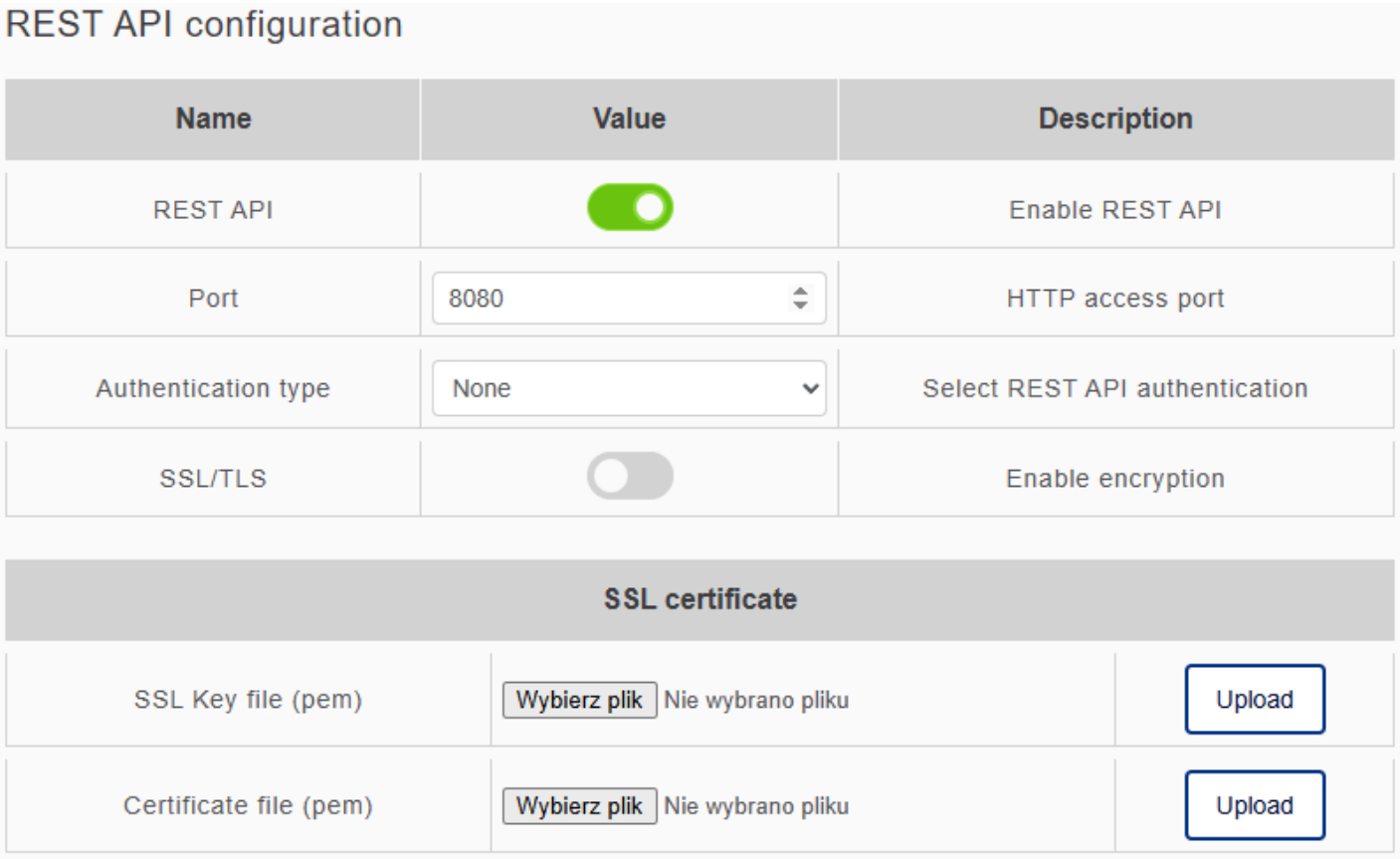
## iCluster

**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.

## 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`

## 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 |
|---|---|---|
| `%s[x]%` | `%s[1]%` | Sensor `x` measured value<br>Example: a value measured by sensor No. 1 will be returned |
| `%s[x].name%` | `%s[1].name%` | Sensor `x` name |
| `%s[x].idx%` | `%s[1].idx%` | Sensor `x` index |
| `%s[x].stat%` | `%s[1].stat%` | Sensor `x` status index |
| `%s[x].statTxt%` | `%s[1].statTxt%` | Sensor `x` status (słownie) |
| `%v[x]%` | `%v[1]%` | Virtual variable `x` state |
| `%time%` | | Current time |
| `%date%` | | Current date |
| `%timedate%` | | Current time and date |
| `%ts%` | | Current timestamp – number of seconds since the specified date: 1st of January 1970 |
| `%mod_name%` | | User-defined module name |
| `%mod_model%` | | Device model |
| `%eip%` | | Ethernet IP address *(IQIO Sens ETH)* |
| `%emac%` | | Ethernet MAC address *(IQIO Sens ETH)* |
| `%wip%` | | Wi-Fi IP address *(IQIO Sens Wi-Fi)* |
| `%wmac%` | | Wi-Fi MAC address *(IQIO Sens Wi-Fi)* |
| `%sunrise%` | | Calculated sunrise time |

| | | |
|---|---|---|
| `%sunset%` | | Calculated sunset time |

# Factory settings, backup

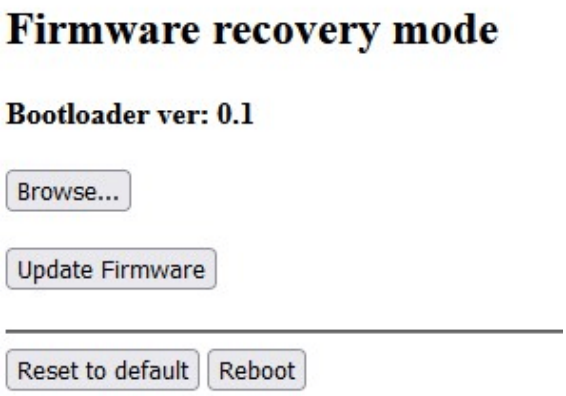
## Emergency firmware restore / restoring factory settings

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.