

User manual IQIO PRO




Dear Customer

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

Remember!

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

Table of contents

Table of contents	3
1 Introductory information	6
2 Guarantee and liability of the manufacturer	6
3 Safety in use	7
3.1 Storage, operating and transport conditions	7
3.2 Installation and use.....	7
3.3 Disposal and decommissioning	7
4 Purpose of the device.....	7
5 Assembly of the device	8
5.1 Technical data	8
5.1 Dimensions.....	8
5.2 Connection diagram	9
6 Device configuration	12
6.1 7.1 Changing the IP address via the Discoverer program.....	12
6.2 Changing the subnet of the computer to be configured	13
6.3 Configuring network settings	15
6.4 Configuration mode.....	17
6.5 Instructions for setting up the WiFi connection.....	18
7 Software update	19
8 Appliance website.....	20
9 Device status overview (Status)	21
9.1 Sensors window.....	21
9.2 Outputs window.....	22
9.3 Inputs window.....	23
10 Configuring inputs/outputs (I/O Settings)	23
10.1 Outputs.....	23
10.2 Inputs.....	25
10.2.1 Types of action: Standard.....	25
10.2.2 Action types: Hold.....	26
10.2.3 Action types: Cnt.....	26
10.2.4 Action types: Toggle.....	28
10.2.5 Action types: Freq.....	28
10.3 Display LED	29
10.4  IO control via various communication protocols.....	29
11 Defining tasks (Action)	30
11.1 All	31
11.1.1 Okno Control Actions	31

11.1.2	All available actions and All system actions window	32
11.2	Inputs.....	33
11.2.1	Assigning an action	34
11.3	System	36
11.4	Periodic.....	37
12	Configuration of sensors (Sensors)	38
12.1	All	38
12.1.1	Alarm configuration	42
12.2	History.....	44
12.3	Chart	45
12.4	➡ Operating the sensor	46
12.4.1	Assigning the sensor	46
12.4.2	Storing sensor readings and viewing the graph	48
12.4.3	Downloading stored sensor readings	52
13	Configuration of notifications	53
13.1	Sensors.....	53
13.2	Inputs.....	54
13.3	Outputs.....	55
13.4	Configuration	56
14	Binding	58
14.1	Poller	58
14.2	Outputs.....	61
14.3	Inputs.....	61
15	Ping of remote hosts (Watchdog).....	62
16	Logic functions (Logic).....	63
17	Network services (Services)	64
17.1	Web.....	65
17.2	HTTPc	66
17.3	MQTT	68
17.4	E-mail.....	71
17.5	SMS.....	73
17.6	Modbus	74
17.7	SNMP.....	76
17.7.1	SNMP v2c	76
17.7.2	SNMP v3.....	78
17.8	SNTP	81
17.9	TCP/UDP	82
18	System administration (Administration).....	82
18.1	Access	83
18.2	Network	83

18.3	Time.....	84
18.4	System events	85
18.5	Backup.....	85
18.6	Update.....	86
19	Emergency software upload / factory reset	87
20	Built-in variables.....	88
21	IO commands	90

1 Introductory information

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

Description of symbols used in this manual:



Warning

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



Tip

Important instructions and information.

Observing the texts marked with this sign will facilitate operation.

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

2 Guarantee and liability of the manufacturer



Warning

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

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

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

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



Warning

There are no user-serviceable parts inside the appliance.

3 Safety in use

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

3.1 Storage, operating and transport conditions

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

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

The unit is designed to operate under the following conditions:

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

Recommended transport conditions:

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

3.2 Installation and use

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

3.3 Disposal and decommissioning

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

4 Purpose of the device

The IQIO device is an advanced tool for monitoring parameters such as temperature, humidity or digital inputs. It can handle up to six different sensors. The user can access all readings via an embedded web page, where current changes can be tracked, measurement history can be viewed and graphs can be analysed.

The IQIO supports a variety of communication protocols, including HTTP, HTTPS, MQTT, SNMP v2/v3, SMSApi, e-mail. This enables it to work with a wide range of devices and systems. There is also the functionality to send notifications, both email (encrypted) and SMS, informing of the current status of the sensors or when set alarm values are exceeded. The device is Wi-Fi enabled.

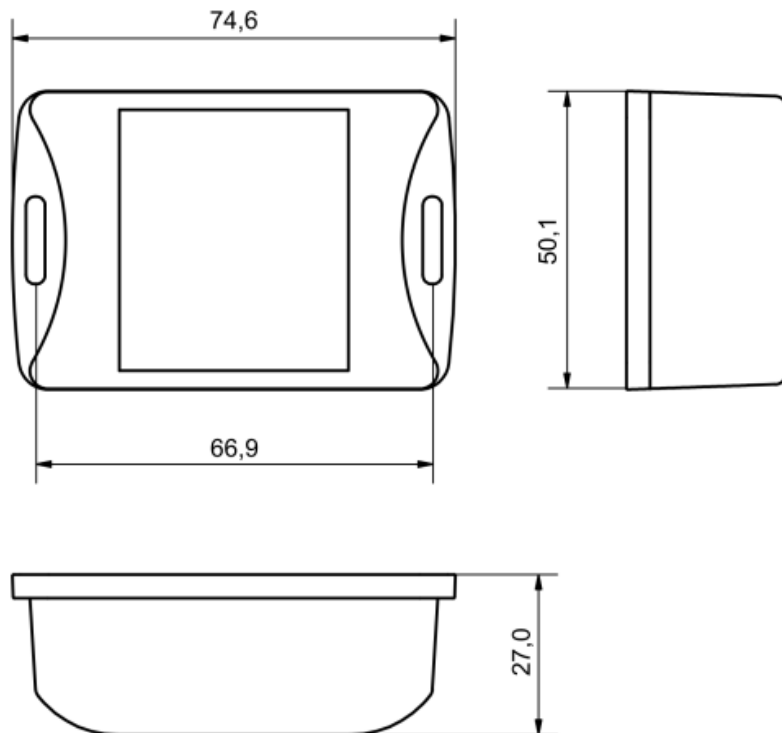
The device also offers an independent output to control various system components. Thanks to built-in mechanisms, the IQIO can automatically respond to signals and readings, and the user can programme specific actions, such as controlling a particular output or generating notifications.

5 Assembly of the device

5.1 Technical data

Power supply	PoE: 33-57V PoE IEEE 802.3af DC: 12-24VDC (3.5mm screw connector) USB: 5VDC USB C cable
Power consumption	max 1,5W
Bus	1-wire - 3-wire cable or RJ12 flat cable using adapter*. support for up to 6 sensors dedicated sensors: temperature, humidity, water pressure, air pressure, analogue voltage, analogue current, CO, CO ₂ , NO _x gases
Inputs	1 digital input pre-polarised, NO
Outputs	1 relay output potential-free NO max. operating voltage 30VDC max load current 1A NO output (normally open) ON/OFF time 1ms/5ms operating modes: bistable, astable, monostable, timed
Communication	Wi-Fi optional 10/100 Mbps Ethernet port
Display	LED 7-segment, red
Operating temperature	from -10°C to +55°C
Enclosure	Enclosure class: IP30

5.1 Dimensions



5.2 Connection diagram

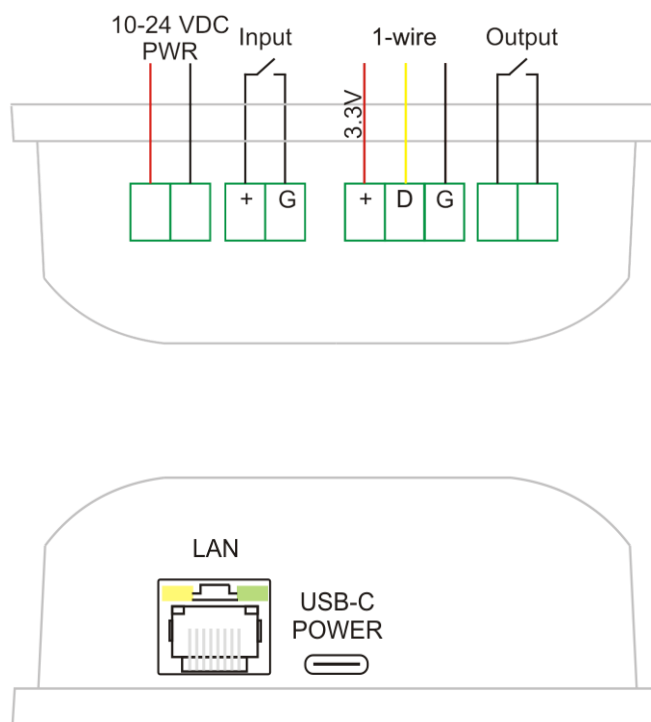
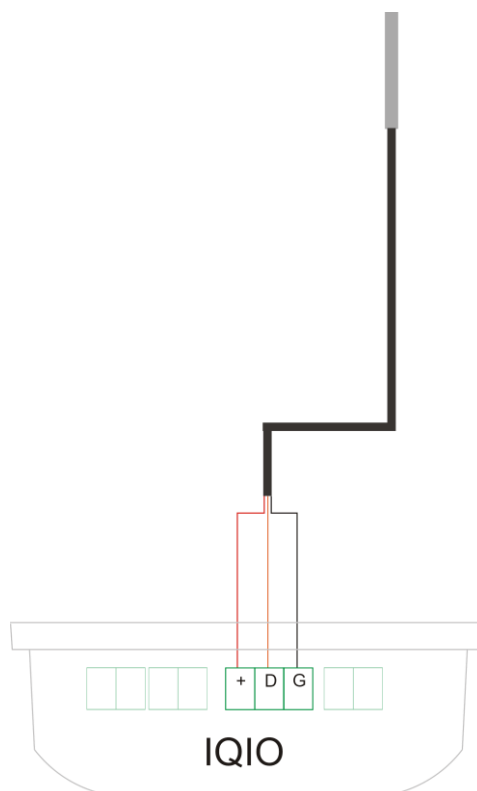
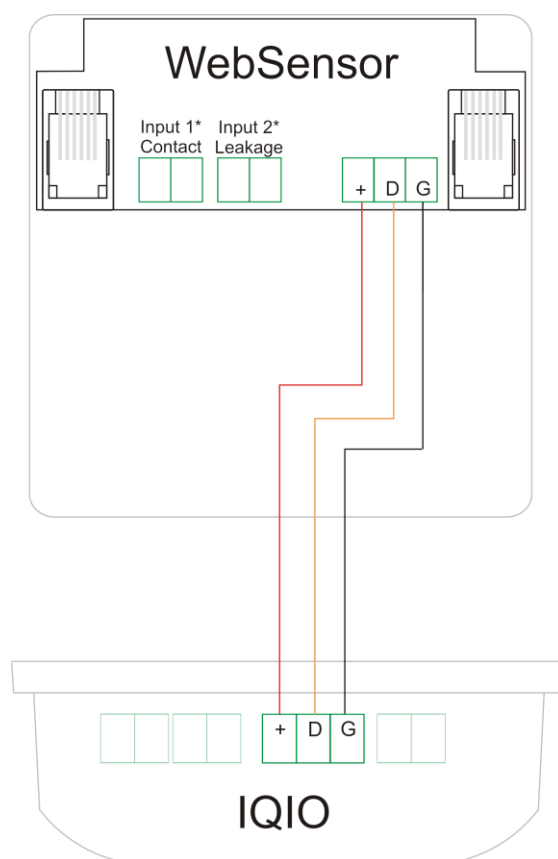


Diagram of the connection of the sensor to the IQIO device:

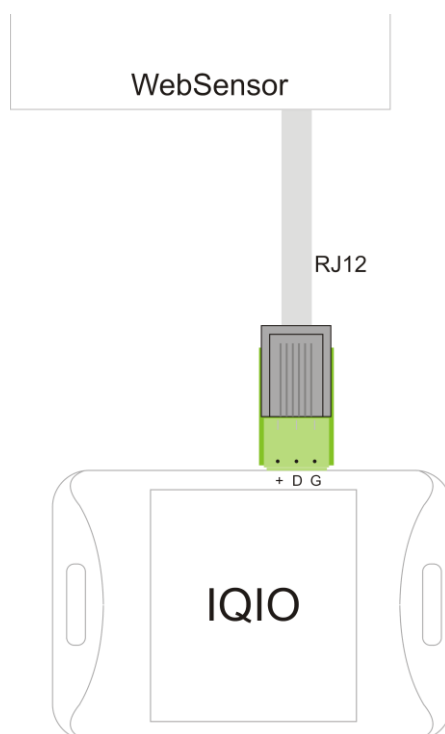


Ways to connect WebSensor devices with IQIO:

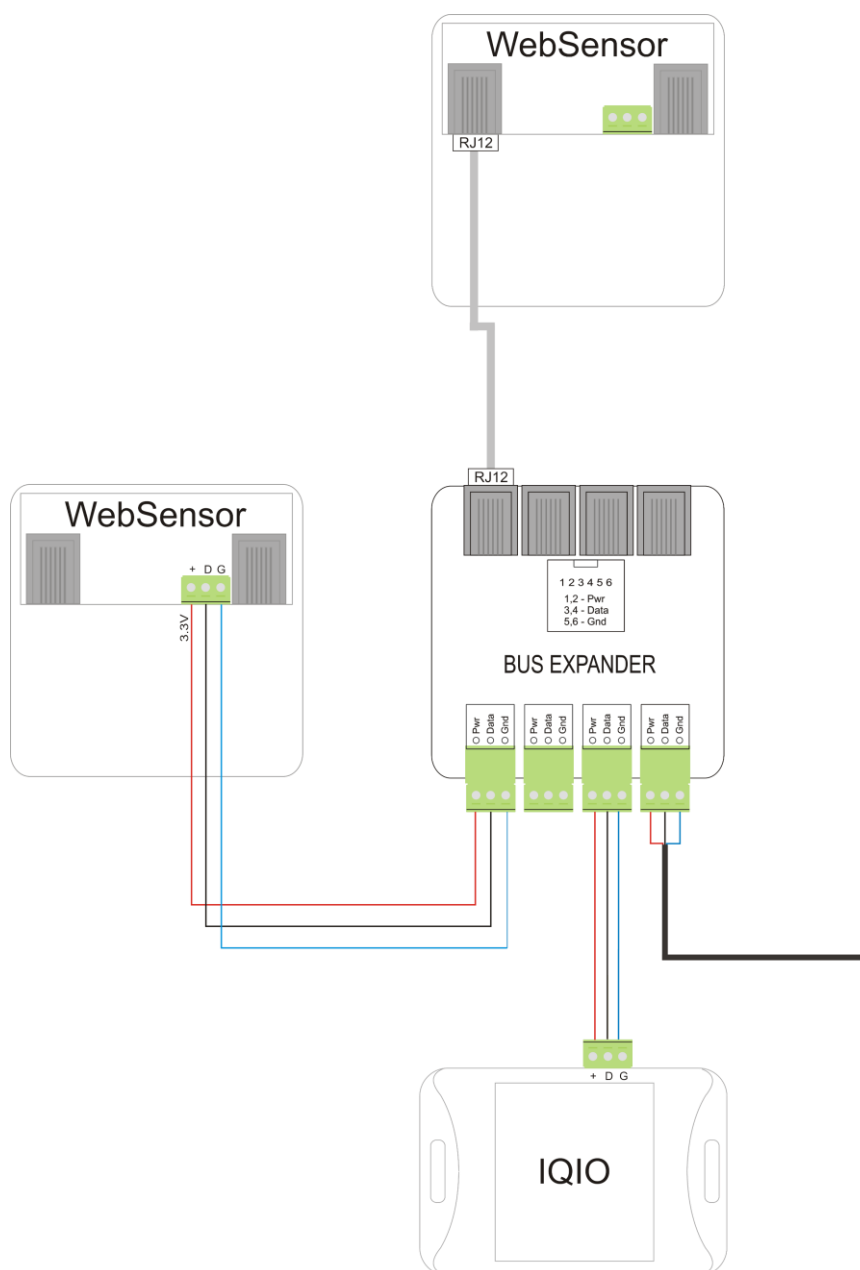
- 3-wire cable:



- RJ12 cable + adapter:



- Connection of multiple WebSensors:

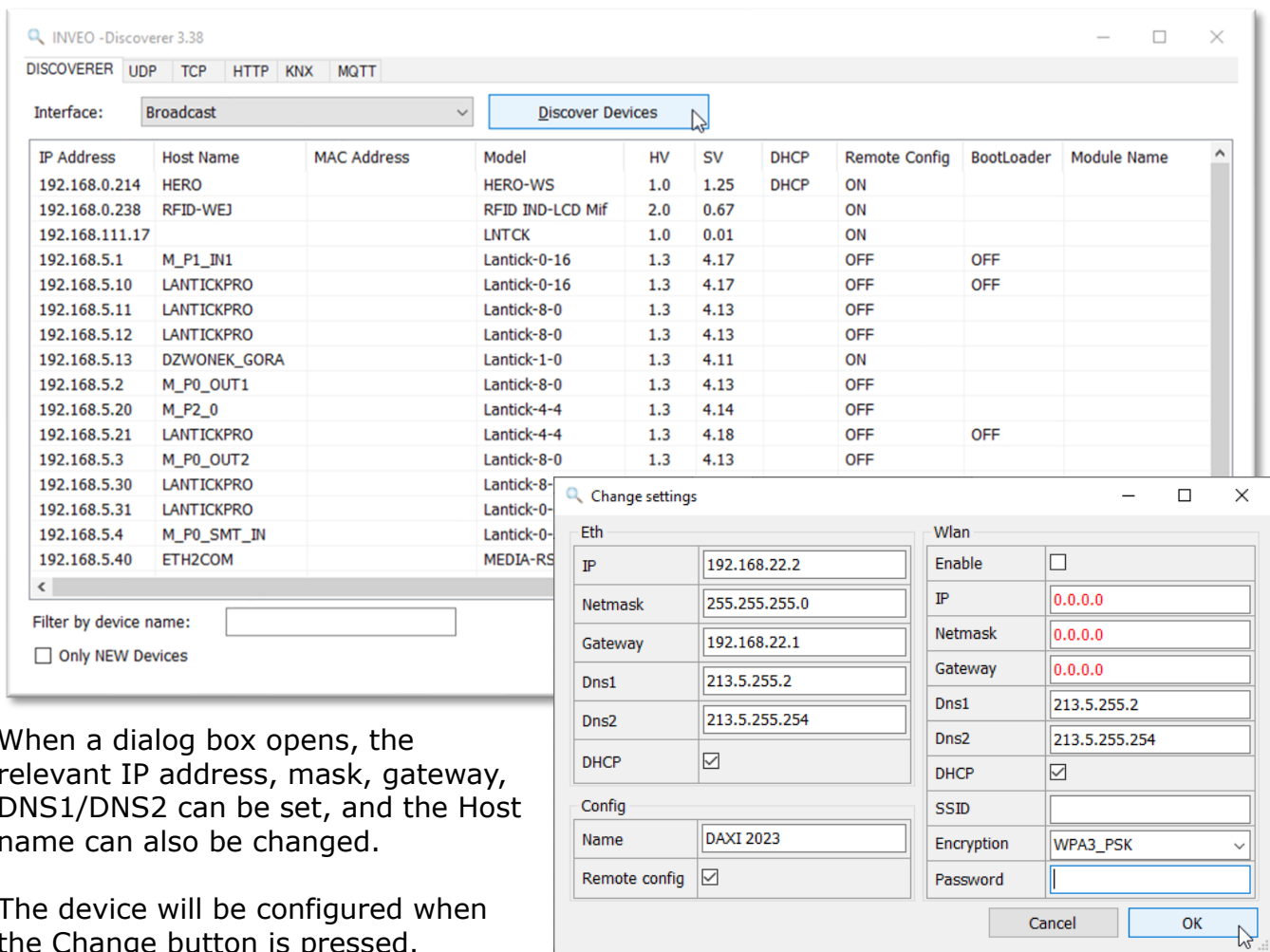


6 Device configuration

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

6.1 7.1 Changing the IP address via the Discoverer program

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





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

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

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

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

Access configuration

Name	Value	Description
Password		Enable password
Current password	<input type="text"/>	
New password	<input type="text"/>	
Repeat new password	<input type="text"/>	
Module name	<input type="text"/>	
Enable remote config		Allow change configuration by Discoverer app

Save

Then click Save to save the settings.

6.2 Changing the subnet of the computer to be configured

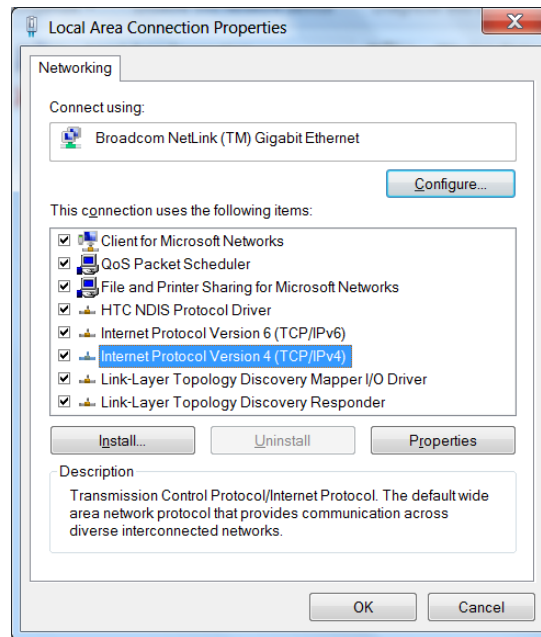
When configuring the device bypassing the Discoverer application, you must first change the subnet address of the computer connected to the same network.

To do this, go to the network configuration of the computer:

- Press Win + R, type `ncpa.cpl` and press Enter,
OR
- Start → Control Panel → Network and Internet → Network and Sharing Centre → Change network adapter settings.

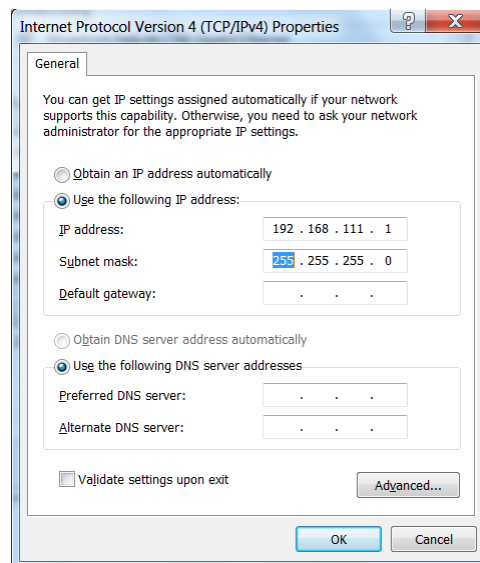
Select your network connection, press the right mouse button and click Properties.

Once selected, the configuration screen will appear:



Changing the network configuration in WINDOWS

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




Examples of TCP/IP protocol settings

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

6.3 Configuring network settings

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



Ethernet network configuration

Name	Value	Description
DHCP		Enable Ethernet DHCP
IP	<input type="text" value="192.168.111.15"/>	A.B.C.D
Netmask	<input type="text" value="255.255.255.0"/>	A.B.C.D
Gateway	<input type="text" value="0.0.0.0"/>	A.B.C.D
DNS1	<input type="text" value="0.0.0.0"/>	A.B.C.D
DNS2	<input type="text" value="0.0.0.0"/>	A.B.C.D

[Save](#)

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

WLAN network configuration

Name	Value	Description
Wi-Fi		Enable Wi-Fi
DHCP		Enable Wi-Fi DHCP
IP	<input type="text" value="192.168.111.15"/>	A.B.C.D
Netmask	<input type="text" value="255.255.255.0"/>	A.B.C.D
Gateway	<input type="text" value="0.0.0.0"/>	A.B.C.D
DNS1	<input type="text" value="0.0.0.0"/>	A.B.C.D
DNS2	<input type="text" value="0.0.0.0"/>	A.B.C.D
Encryption	<input type="text" value="Open"/> ▾	Select Wi-Fi encryption
SSID	<input type="text"/>	Wi-Fi SSID
Password	<input type="text"/>	Wi-Fi password

Scan available Wi-Fi

Save

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

Scan available Wi-Fi

The button

Scan available Wi-Fi

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

6.4 Configuration mode



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

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

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

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

6.5 Instructions for setting up the WiFi connection

- Step 1.** For three minutes after the device has been powered up (during Configuration Mode, see section [6.4 Configuration mode](#)) it is possible to configure the WiFi connection. To do this, press and hold the "RESET" button until "AP" appears on the device display.
- Step 2.** Turn on the search for available Wi-Fi networks on your phone or other device. A network named "Inveo-wifi-config" should appear.
- Step 3.** A network named "Inveo-wifi-config" will appear - connect to it.
- Step 4.** When the connection is established, press the 'scan' button in the configuration interface or enter the WiFi SSID name in the SSID field.

13:13

Zaloguj się w aplikacji Inveo.WiFi.C...
inveo-wifi-config

Inveo: Wi-Fi configuration

SSID

Password

Scan

DHCP ☒

IP

Subnet/Mask

Gateway

- Step 5.** Select the network from the list of available ones to which the device is to be connected.
- Step 6.** Enter the appropriate password for the selected network.
- Step 7.** If the DHCP server is not available, you can configure the network settings manually after unchecking the "DHCP" option.
- Step 8.** If the settings are successfully saved, this "SUCCESS" message will appear.

7 Software update

The DAXI device is equipped with a software update facility. The software is supplied as a file with the extension .bin.

To update the software, please follow the following steps:

Step 1. Go to the device's web page to the Administration/Update tab.

Step 2. Using the "Browse" button, locate the previously saved software file on your device.

Firmware update

	File name	File size (bytes)
<input type="button" value="Browse"/>	IQIO PRO.bin	2101268

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

Firmware update

	File name	File size (bytes)
<input type="button" value="Browse"/>	IQIO PRO.bin	2101268

Loading, please wait...

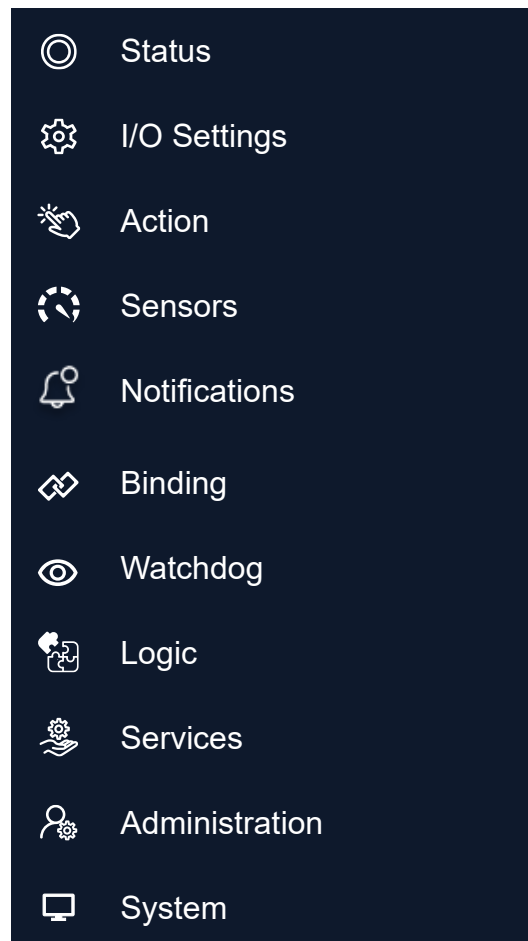
Step 4. Step 4. Once the update is complete, the screen will display the message "Firmware updated, rebooting...". (Firmware has been updated, rebooting takes place). The device will automatically reboot.



8 Appliance website

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

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



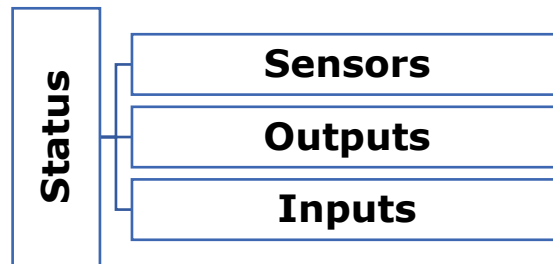
An information bar at the top of the page presents itself, providing key data about the device, such as the name, unique name given by the user, model, IP address, software number and MAC address.

Model: IQIO PRO	IP: 192.168.111.15	Name: IQIO PRO test	Firmware: 0.07	MAC: 00:00:00:00:00:00
-----------------	--------------------	------------------------	----------------	------------------------

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

9 Device status overview (Status)

In the Status tab you can find all information about the currently operated outputs, inputs, sensor readings etc.



9.1 Sensors window


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

Enable autorefresh



Sensors

ID	Name	State	Last value	Last read
0	s0	Normal	0	8.1s
1	s1	Normal	0	8.1s
2	s2	Normal	0	8.1s

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

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



Tips

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

9.2 Outputs window

The window displays the current status of the outputs supported by the DAXI device, as defined in the I/O Settings tab. The individual columns of the table with the outputs data can be found:

- **Name** - the name of the output (assigned by the user on the I/O Settings tab). If the output status depends on other factors, the relevant information is displayed under its name:
 - **output unavailable** - assigned to the shutter - output is assigned to the shutter control,
 - **output unavailable** - output is routed - output reflecting the state of e.g.: an input, another output, etc., see [Binding](#)
- **Off/On** - current state of the output, pressing the left mouse button in this area will change the state of the output - this option enables manual control of the output,
- **Coil state** - current status of the relay coil - green colour means the relay is on.

The activation of the output (visible in the Off/On column in the table) is not always the same as the coil state (visible in the Coil state column in the table).

Example:


If the output is configured in astable mode, with Time on and Time off parameters, switching the output on in the Status tab will result in a change of state in the Off/On column. On the other hand, the state of the coil will be reflected in the Coil state column. In this case, we can observe the coil state of the relay being alternately signalled as on / off, according to the Time on / Time off parameters set.



Tips

If an output is configured to control roller shutters or is programmed to reflect the status of another output or input - it cannot be tested in the Off/On column.


Outputs

Name	Off/On	Coil state
DO 0		

9.3 Inputs window

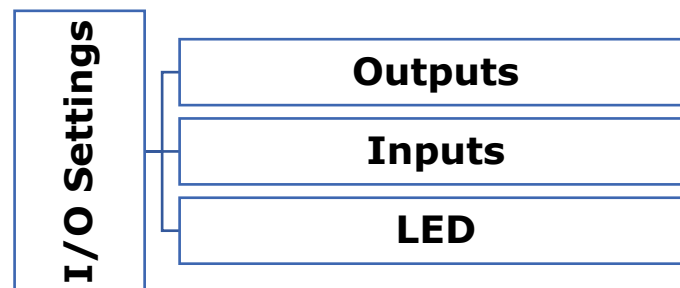
The window displays the current status of the inputs supported by the DAXI device, as defined in the I/O Settings tab. The individual columns of the table with the output data can be found:

- **Name** – name of the input (editable on the I/O Settings tab)
- **In state** – the state of the input
- **Counter** – counter, displaying information on the number of inputs activated since the last reset,
- **Action** – RESET button enables the counter to be reset.

Inputs			
Name	In state	Counter	Action
DI 0		0	RESET

10 Configuring inputs/outputs (I/O Settings)

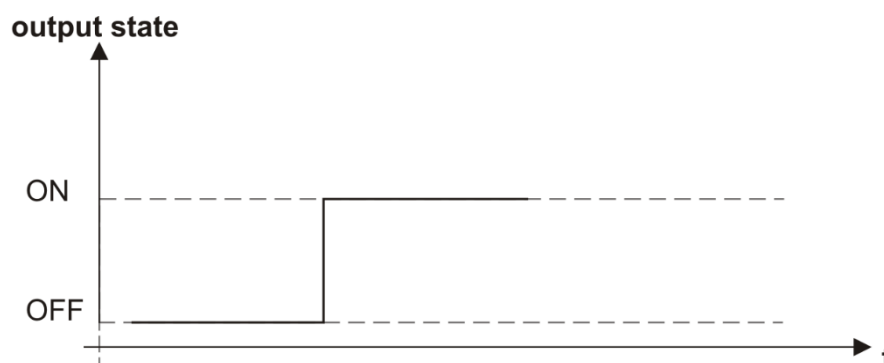
In the I/O Settings tab, you have access to advanced configuration options that allow you to define the exact operation of the device. Here you can specify precisely how the individual inputs and outputs will behave. In addition, for those who wish to customise the way data is presented, this tab also gives you the option to configure the display.



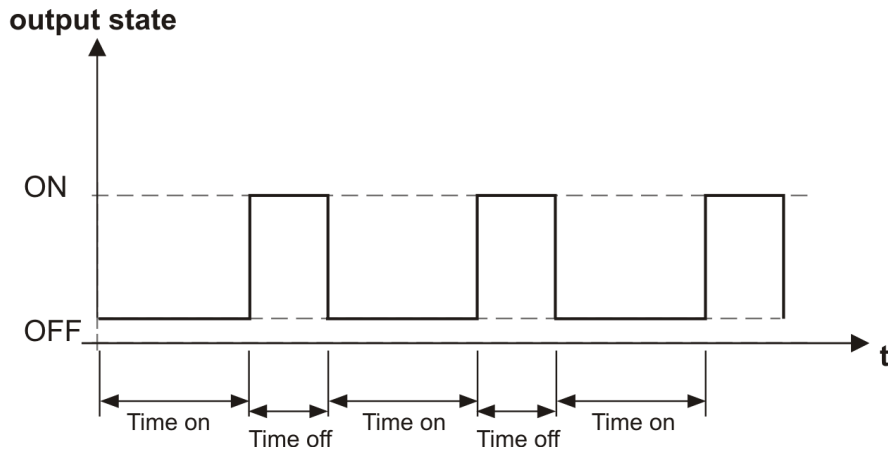
10.1 Outputs

This tab allows the configuration of the outputs supported by the DAXI device - both physical and virtual. The following settings can be changed in the individual columns:

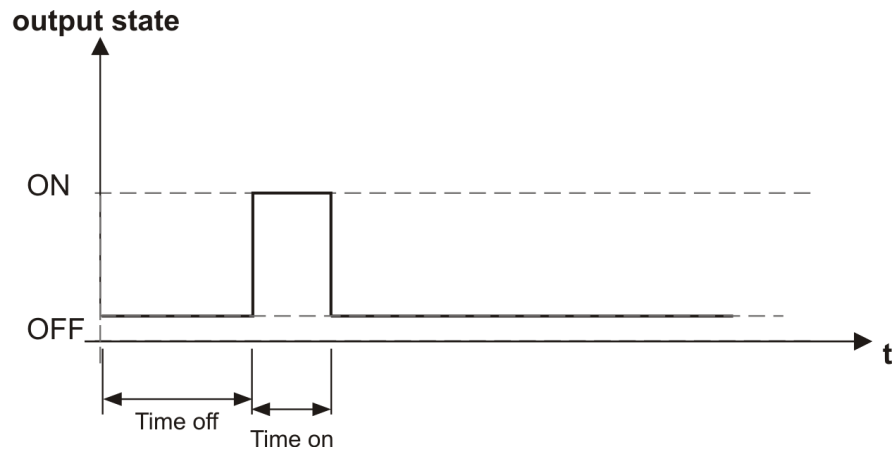
- **Name** – the field allows you to change the name of the output,
- **Mode** – operation mode of the output:
 - **Disable** – disable operation of the output,
 - **Bistable** – bistable mode,



- **Astable** – cyclic mode - the output is switched on at defined intervals (parameter Time on) for a defined period of time (parameter Time off),



- **One-pulse** – the output is switched on once for a defined period of time (parameter Time on) after a defined time (parameter Time off),



- **Invert** – changing the base state of the output channel,
- **Time on** – time of switching on the output (parameter used in Astable and One-pulse mode),
- **Time off** – output switching off time (parameter used in Astable and One-pulse mode),

Physical outputs configuration

No.	Name	Mode	Invert	Time on	Time off
0	DO 0	Bistable ▾	Standard ▾	0 ▴▾	0 ▴▾

Save

10.2 Inputs

This tab allows the configuration of the inputs supported by the DAXI device - both physical and virtual. The following settings can be changed in the individual columns:

- **Name** - a field allows the name of the input to be changed,
- **Invert** - changing the base state of the input channel,
- **Action type** - mode of triggering the action assigned to the input:
 - **Standard**,
 - **Hold**,
 - **Cnt**,
 - **Toggle**,
 - **Freq**,
- **Parameter** - the value used in the various action activation schemes. When the mouse cursor is placed over the input field, the unit in which the parameter is represented appears, for example Hz for the Freq type.

The button [Go to the input actions](#) in the top right-hand corner allows quick access to the Action/Inputs tab, see section [11.2 Inputs](#).

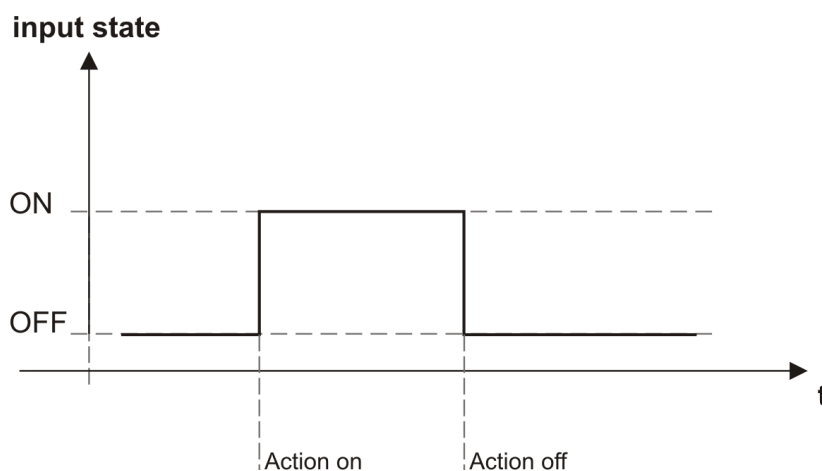
Physical inputs configuration

No.	Name	Invert	Action type	Parameter
0	DI 0	Standard ▾	Hold ▾	600 ▴ ▾

Save

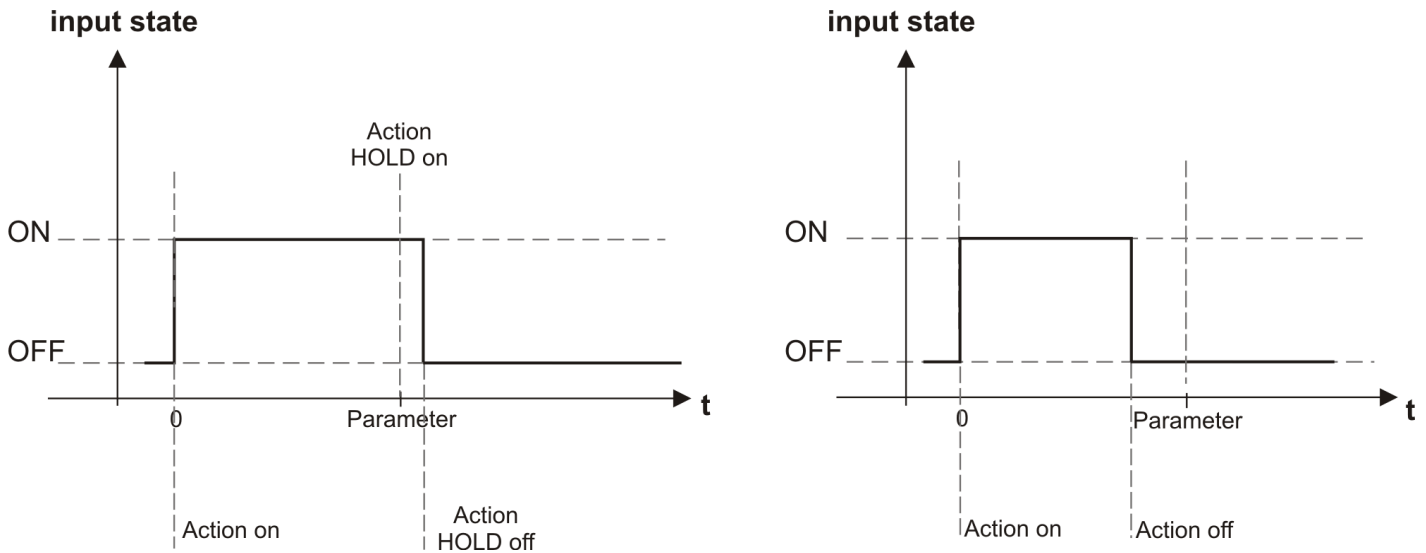
10.2.1 Types of action: Standard

The action is triggered by switching the input on/off.



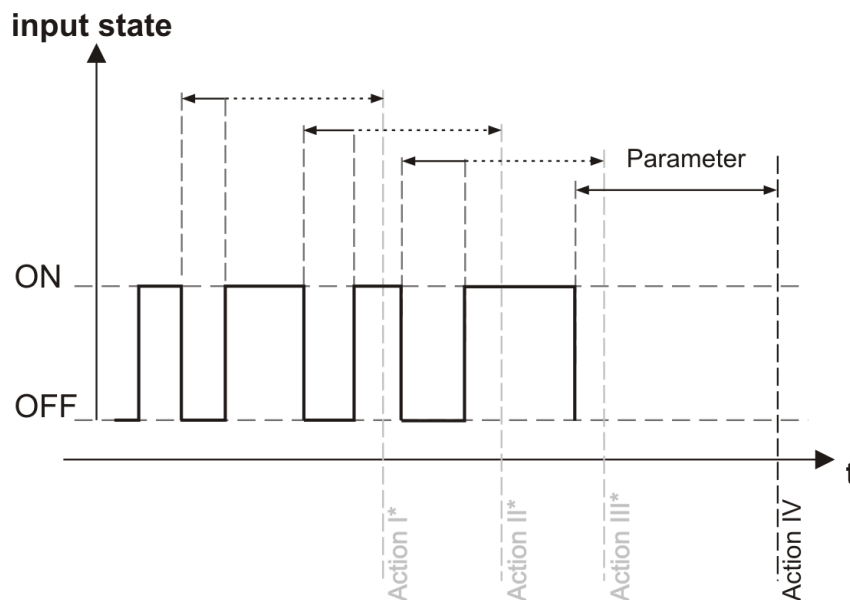
10.2.2 Action types: Hold

The triggering of a specific action depends on the length of the input pulse. A pulse at the input triggers an event described as Action on. If the pulse continues and exceeds the time specified in the Parameter field - the action described as Action Hold on is triggered. If the pulse is interrupted before the time specified in the Parameter field expires - Action off is triggered. If the pulse is interrupted after the time specified in the Parameter field - the action described as Action hold off is called.



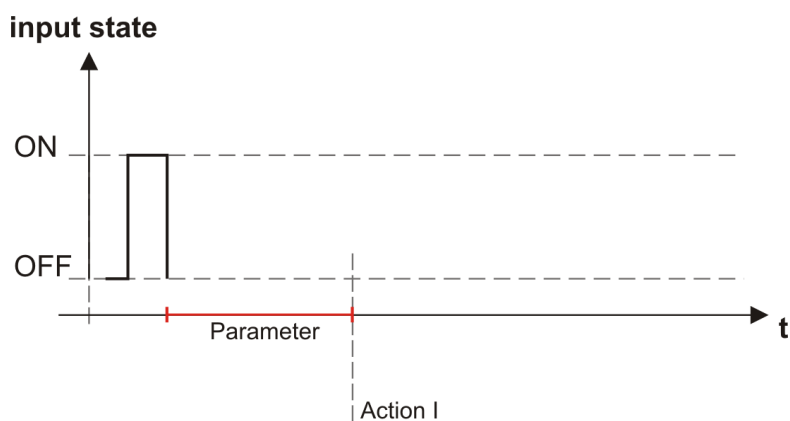
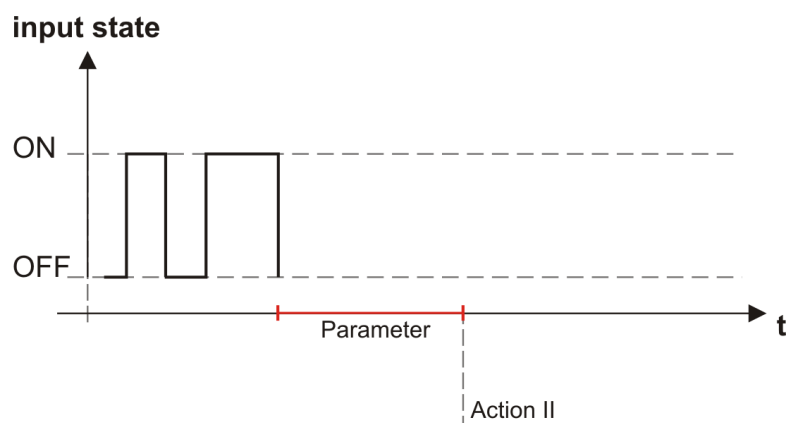
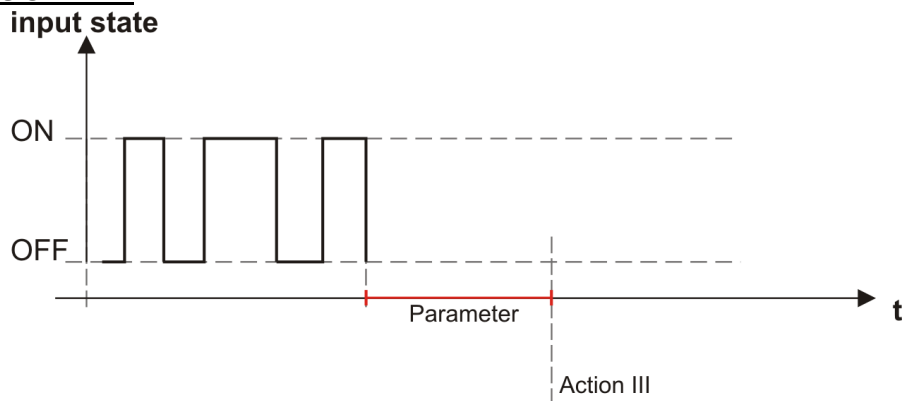
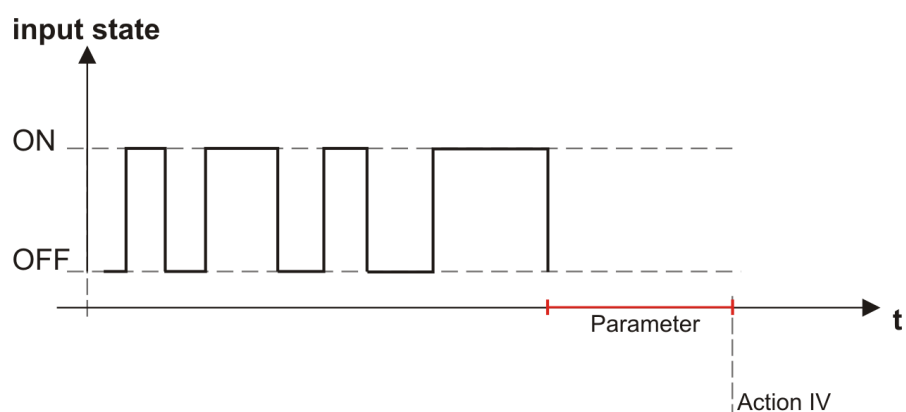
10.2.3 Action types: Cnt

Pulse counter in a specific time interval - the action is triggered by a specific number of activations occurring within the time interval defined in the Parameter field,



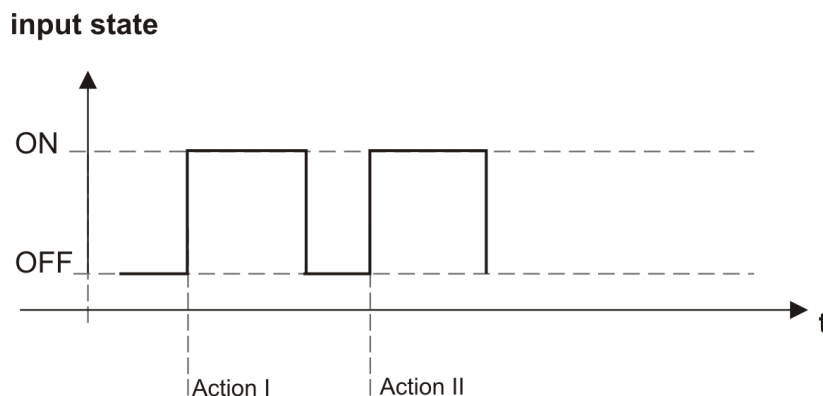
*the action is triggered only if no further impulses occur within the defined time interval (value entered in the Parameter field) (input is not switched on again).

The specified action is triggered when the time - the delay time from the end of the input pulse (e.g.: release of the switch) - has elapsed. If a new event (another pulse) occurs during this delay, the countdown of the delay is interrupted.

Call to action I:**Call to action II:****Call to action III:****Call to action IV:**

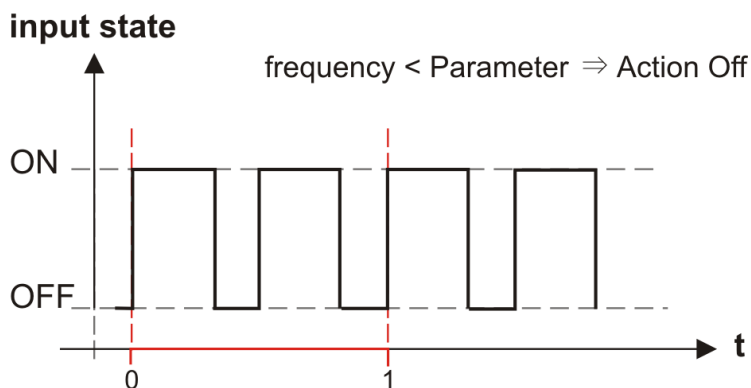
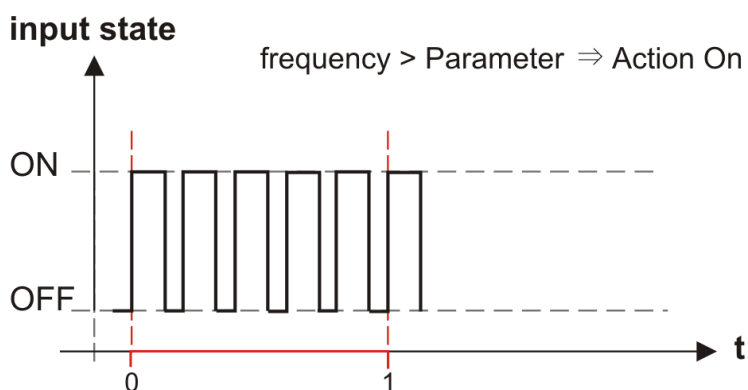
10.2.4 Action types: Toggle

Successive pulses on the input trigger Action I / Action II alternately.



10.2.5 Action types: Freq

The triggering of an action depends on the frequency of the input pulses. The value of the desired frequency must be entered in the Parameter field - expressed in Hz.



10.3 Display LED

In this tab, the display settings can be configured.

- Test time – frequency of text changes on the display - expressed in seconds,
- LED text – data displayed on the main screen, you can use the built-in variables described in detail in chapter [20 Built-in variables](#).

LED 7-segments configuration

Name	Value	Description
Text time	2	Frequency of text changes on the display.
LED text	SEnS %sens0%	Data shown on the display.

Save

Save

Confirm the settings using the .

10.4 —> IO control via various communication protocols

The user has the possibility to control the outputs of the DAXI device using different protocols such as HTTP, TCP, UDP and MQTT.

The following commands are available for the outputs from the different protocols (HTTP, UDP/TCP, MQTT):

- out_on=ch - enable output numbered "ch".
- out_off=ch - switch off the output with the number "ch".
- out_inv=ch - changing the state of the output numbered 'ch' to the opposite.
- out_blink=ch,tone,toff,cnt - programming cyclic control of the output numbered "ch".

Parameters:

- ton - on time (expressed in seconds).
- toff - off time (expressed in seconds).
- cnt - number of switch-on cycles (optional parameter).
- out_time=ch,tone,toff - switch on the output number "ch" for the time specified in the tone parameter, after the time specified in the toff parameter. The toff parameter is not mandatory - omitting this parameter will switch on the output without delay.
- out_all=10n-11100 - command defining the status of all available outputs. Each digit represents another output:
 - 1 - on.
 - 0 - off.
 - n - change of state to the opposite.
 - - - no change of state.

Example: out_all=10n-1110 will switch on outputs number 0, 4,5,6; switch off outputs 1 and 7; change the state to the opposite of output 2; leave the state of output number 3 unchanged.

Commands can be combined with the & sign.

Example:

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

Controlling the outputs via the HTTP protocol

In order to control the outputs using the listed commands, the io resource must be referenced. Example:

http://192.168.111.14/io?out_inv=2&out_inv=3.

The address contains: the IP of the device, the "io" resource and the selected commands, combined using "&".

Attachment of HTTP support and detailed configuration is available under Services / HTTPc - see section [17.2 HTTPc](#).

Output control via UDP, TCP protocols

Commands can also be used in the TCP and UDP protocols.

Server services and ports for TCP/UDP can be enabled under Services / TCP/UDP - see chapter [17.9 TCP/UDP](#).

Output control via MQTT protocol

It is possible to use the above commands in communications using the MQTT protocol. After enabling the MQTT service on the device, it is necessary to specify the address of the broker, the port on which the broker listens and to specify the subscribe topic on which the device will listen.

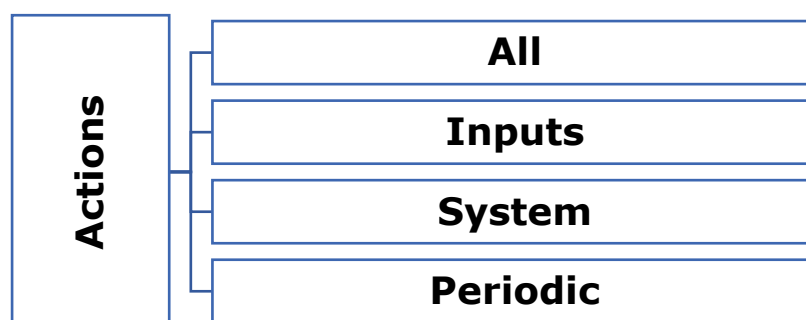
Enabling MQTT support and detailed configuration is available under Services / MQTT - see section [17.3 MQTT](#).

11 Defining tasks (Action)

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

- Output control: activating or deactivating a specific output based on a sensor reading. For example, activating a fan when the temperature value exceeds a certain threshold.
- Sending notifications in the form of SMS, e-mail, MQTT frame, HTTP, TCP, UDP, or SNMP trap and others. More specifically: automatic sending of an alert or message to the user or another system in response to specific conditions.
- Other user-defined actions: actions specific to a particular system or need, such as writing data to a database, activating an alarm, changing the settings of other devices, etc.

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





11.1 All

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

11.1.1 Okno Control Actions


Control actions

Operation	Description
	Remove all actions stored in the device memory
	Add a new new action to use

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




Create a new action

Current action	Entry
<div> <input type="text" value="Action name*"/> </div> <div>  </div>	<div> <p>Add entry to an action!</p> </div>

Preview of added entries
<div> <p>There is no assigned entries!</p> <div>Add some</div> </div>


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


 Add entry

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

Protocol	Available options	Description
KNX	Input KNX destination group	KNX target group
	Input KNX frame	Content of the KNX frame
UDP	Input server IP	target IP address
	Input server port	port on which the target device listens
	Input data	command sent to target device
TCP	Input server IP	target IP address
	Input server port	port on which the target device is listening on
	Input data	command sent to target device
HTTP*	Input server IP/URL address	target IP address/URL
	Select method	choice of communication method: GET, POST, PUT or DELETE
	Select content-type	choice of content type: Text/plain, application/json, application/xml
	Input data	command to be sent to the target device
MQTT*	Input MQTT topic	topic to which device sends data
	Input data	
IO	Input command	command field, list of supported commands - see chapter 21 IO commands
Internal log	Input log message	message body
E-mail*	Input e-mail receiver	target e-mail address
	Input e-mail message	content of e-mail message
SMS*	SMS sender	sender of the SMS message
	Receivers (comma separated)	recipients of the SMS message
	Input SMS message	content of the SMS message
SNMP Trap	Trap syntax	syntax of the notification sent




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

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

the settings with the button .



11.1.2 All available actions and All system actions window

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

- edit by clicking the button: ,
- try it out by clicking the button: ,
- delete it, using the button: .

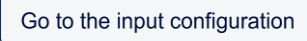
11.2 Inputs


In this tab, defined actions can be assigned and configured to specific inputs.

No.	Name	Actions	
0	DI 0	Action Off 	Action On 

Depending on the type of input action (this parameter is defined in the I/O Settings / Inputs tab - see section [10.2 Inputs](#)) different forms of action are available to trigger the assigned action.

Selected type of action	Available forms of action	Action which will trigger the assigned action
Standard	Action Off	Action is triggered by switching off the input
	Action On	Action triggers input switching on
Hold	Action Off	Action triggers deactivation of the input - input has been ON for a shorter time than specified by the user (in the Parameter field - see chapter 10.2 Inputs)
	Action On	Action triggers switching on of the output
	Action Hold On	Action triggers activation of the input for a time longer than specified by the user (in the Parameter field - see chapter 10.2 Inputs)
	Action Hold Off	Action triggers deactivation of the input - the input has been switched on for a longer time than specified by the user (in the Parameter field - see section 10.2 Inputs)
Cnt	Action I	Action is triggered by the specified number of activations occurring in the user-defined time interval (in the Parameter field - see chapter 10.2 Inputs)
	Action II	Action is triggered by the defined number of activations occurring in the user-defined time interval (in the Parameter field - see chapter 10.2 Inputs)
	Action III	Action is triggered by the defined number of activations occurring in the user-defined time interval (in the Parameter field - see chapter 10.2 Inputs)
	Action IV	An action is triggered by a specific number of activations occurring within a user-defined time interval (in the Parameter field - see section 10.2 Inputs)
Toggle	Action I	Consecutive pulses at the input trigger Action I and Action II alternately.
	Action II	
Freq	Action Off	The action calls for switching on the input with a frequency lower than the one specified by the user (in the Parameter field - see section 10.2 Inputs)
	Action On	The action calls for switching on an input with a frequency higher than the one indicated by the user (in the Parameter field - see chapter 10.2 Inputs)

The button  allows quick access to the I/O Settings/Inputs tab.

The icon  allows you to go to the configuration step by step.

11.2.1 Assigning an action

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

Select action ✕

☐

abc

UDP

☐

xyz

TCP

☒

HTTP

HTTP

☐

xyz

IO

Show additional settings

Assign action

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

Select action ✕

☒

HTTP

UDP

Number of executions (-1 = infinity)	<input type="text" value="Number of executions"/> <div style="text-align: right;">⬆ ⬇ ⬆</div>
Action execution interval [s]	<input type="text" value="5"/> <div style="text-align: right;">⬆ ⬇ ⬆</div>
Delay of action execution [s] Regardless of the state of the trigger <input checked="" type="checkbox"/>	<input type="text" value="Delay of action execution"/> <div style="text-align: right;">⬆ ⬇ ⬆</div>
Delay of action execution [s] The trigger has to be active <input checked="" type="checkbox"/>	<input type="text" value="Delay of action execution"/> <div style="text-align: right;">⬆ ⬇ ⬆</div>

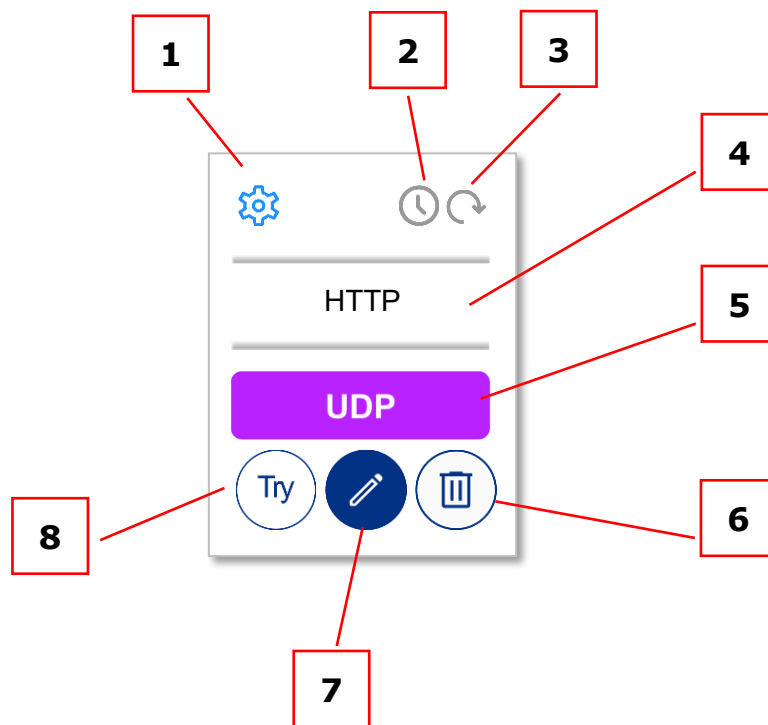
Show additional settings

Assign action

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

Assign action

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



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

11.3 System

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

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

All constant actions

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

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

Create a new action: Power up




Current action	Entry
<div>Power up</div> <div>+ Add entry</div>	<div>Add entry to an action!</div>

Preview of added entries


There is no assigned entries!

Add some



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

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

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

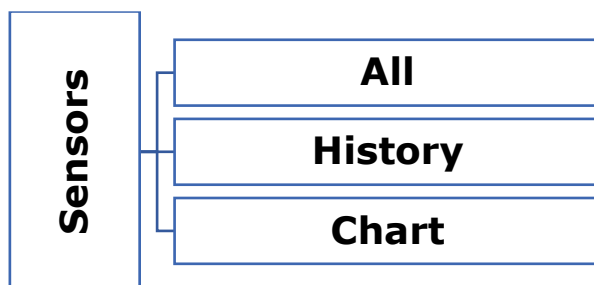
After defining all required entries, confirm the settings with the button .

11.4 Periodic

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

12 Configuration of sensors (Sensors)








This tab allows individual sensors to be assigned to dedicated memory slots and their parameters to be configured in detail. It allows individual management of each sensor, setting specific parameters and modes of operation. In addition, it provides the possibility to view the history of previous readings and download them in JSON or CSV formats.



12.1 All









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

Assign or edit sensors

ID	Name	Src	Type	Log	Alarms				Config
0	s0	1W	1	0	LL	L	H	HH	 
1	s1	1W	3	0	LL	L	H	HH	 
2	s2	1W	2	0	LL	L	H	HH	 
									

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

- **ID** – sensor identification number,
- **Name** – sensor name,
- **Src** – source from which the sensor readings are taken (1-Wire or Modbus poller)
- **Type** – type of connected sensor:








-  – temperature sensor,
-  – humidity sensor,
-  – input,
-  – analogue current sensor 4-20mA,
-  – pressure sensor,
-  – 0-10VDC analogue voltage sensor,
- **Log** – information whether the sensor has active (value 1) or inactive (value 0) readings stored in the device memory
- **Alarms** – activated alarms:
 - **LL** – low level alarm threshold activated,
 - **L** – low level warning alarm threshold activated,
 - **H** – high level warning alarm threshold activated,
 - **HH** – high level warning alarm threshold activated
- **Config** – sensor configuration buttons:
 -  – button for editing sensor parameters,
 -  – delete sensor

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

Go back!

Save

Sensor - ID 0

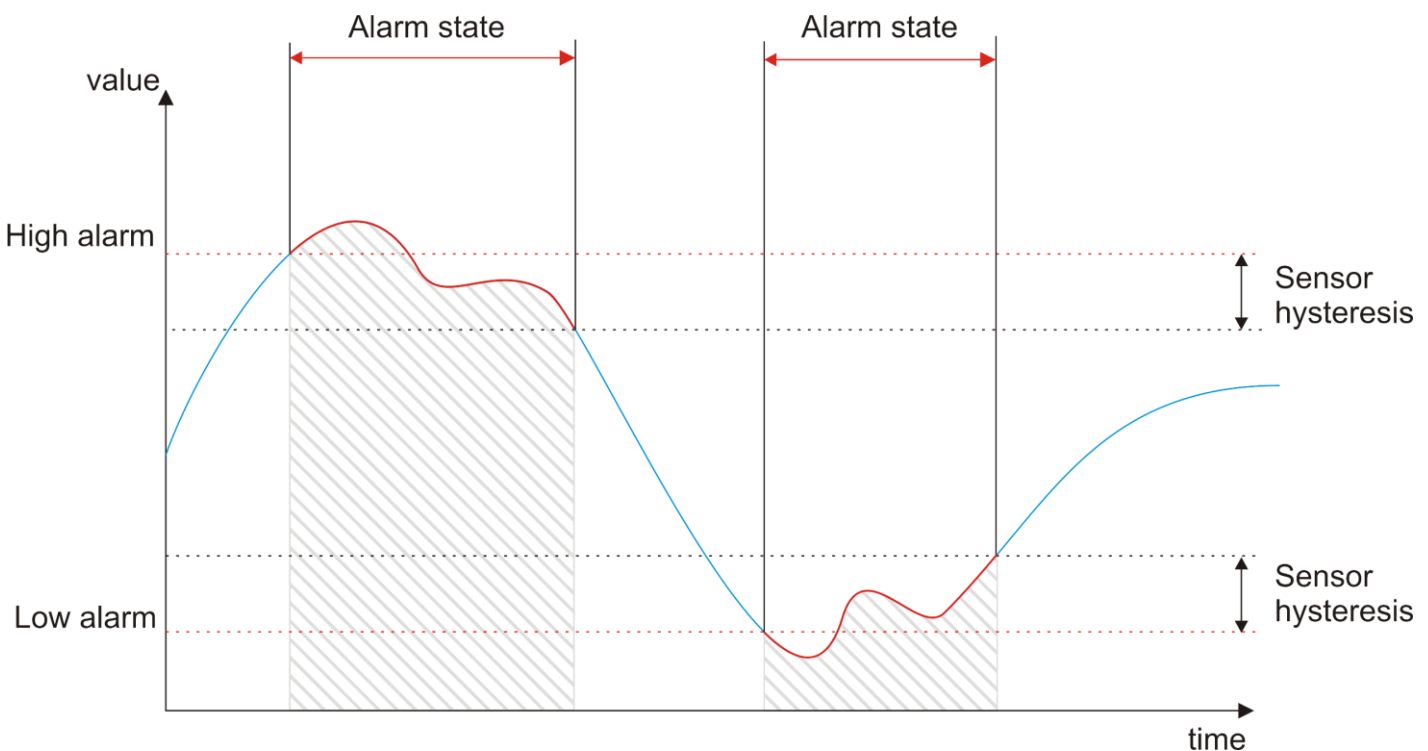
Name	Value	Description
Source	One-wire 	Select sensor value source
Sensor 1-wire address <div>Scan bus</div>		Sensor 1-wire address
Sensor name	Sens 0	Your custom sensor name
Sensor type	Not defined 	Select sensor type
Sensor hysteresis	0 	Sensor hysteresis
Sensor log	Distable 	Log sensor data in memory
Notifications	 	Enable notifications
MQTT notifications		Enable MQTT notifications

- **Source** – the source of the sensor:
 - **One-wire** – physically connected to the sensor bus on the Daxi device,
 - **Poller** – sensors using the Modbus protocol that are queried by Daxi via the Poller function - see section [14.1 Poller](#),
- **Sensor 1-wire address** – the Assign button is used to find and assign the sensor connected to the device,
- **Sensor name** – name of the sensor,
- **Sensor type** – type of sensor: temperature sensor, humidity sensor, input, raw value, pressure sensor, voltage detection sensor,
- **Sensor hysteresis** – (parameter not active when sensor type Input is selected) - applies to alarm and warning states. The hysteresis defines the maximum permissible difference between the alarm/warning value and the return to normal state.

Example:

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

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



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

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

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

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

Action triggered in error-free and alarm-free state

Action on normal



Notification

E-mail ☐

SMS ☐

SNMP Trap ☐

Action triggered on error state

Action on error



Notification

E-mail ☐

SMS ☐

SNMP Trap ☐

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

Select action



☐

abc

☐

xyz

☒

HTTP

UDP

☐

xyz

TCP

Show additional settings

Assign action

The procedure for assigning an action is described in detail in chapter [11.2 Inputs](#)

12.1.1 Alarm configuration

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

Low alarm

☐

Low alarm value

0

Low warning

☐

Low warning value

0

High warning

☐

High warning value

0

High alarm

☐

High alarm value

0

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

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



Sensor corrections final = a * (x + preoffset) + b		
Sensor preoffset	<input type="text" value="0"/>	Sensor preoffset correction
Sensor multiplication 'a'	<input type="text" value="1"/>	Multiplying sensor value
Sensor offset 'b'	<input type="text" value="0"/>	Constant value correction

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

12.2 History

This tab enables you to activate and configure the recording of the history of sensor readings:

History configuration

Name	Value	Description
History		Enable measurement recording
Wait for SNTP		Records data only when SNTP time is active Go to the SNTP configuration
Period	<input type="text" value="60"/>	Save data from sensors every defined time [s]
Remove	<input type="text" value="30"/>	Remove logs older than (days)

- **History** – enable/disable recording of sensor readings,
- **Wait for SNTP** – enabling this option will cause data from sensors to be recorded only when the device downloads time from SNTP server after restart,
[Go to the SNTP configuration](#) - allows access to the tab for SNTP configuration - see chapter [17.8 SNTP](#)
- **Period** – frequency of sensor data recording,
- **Remove** – enables you to activate the clearing from memory of records older than a specified number of days.

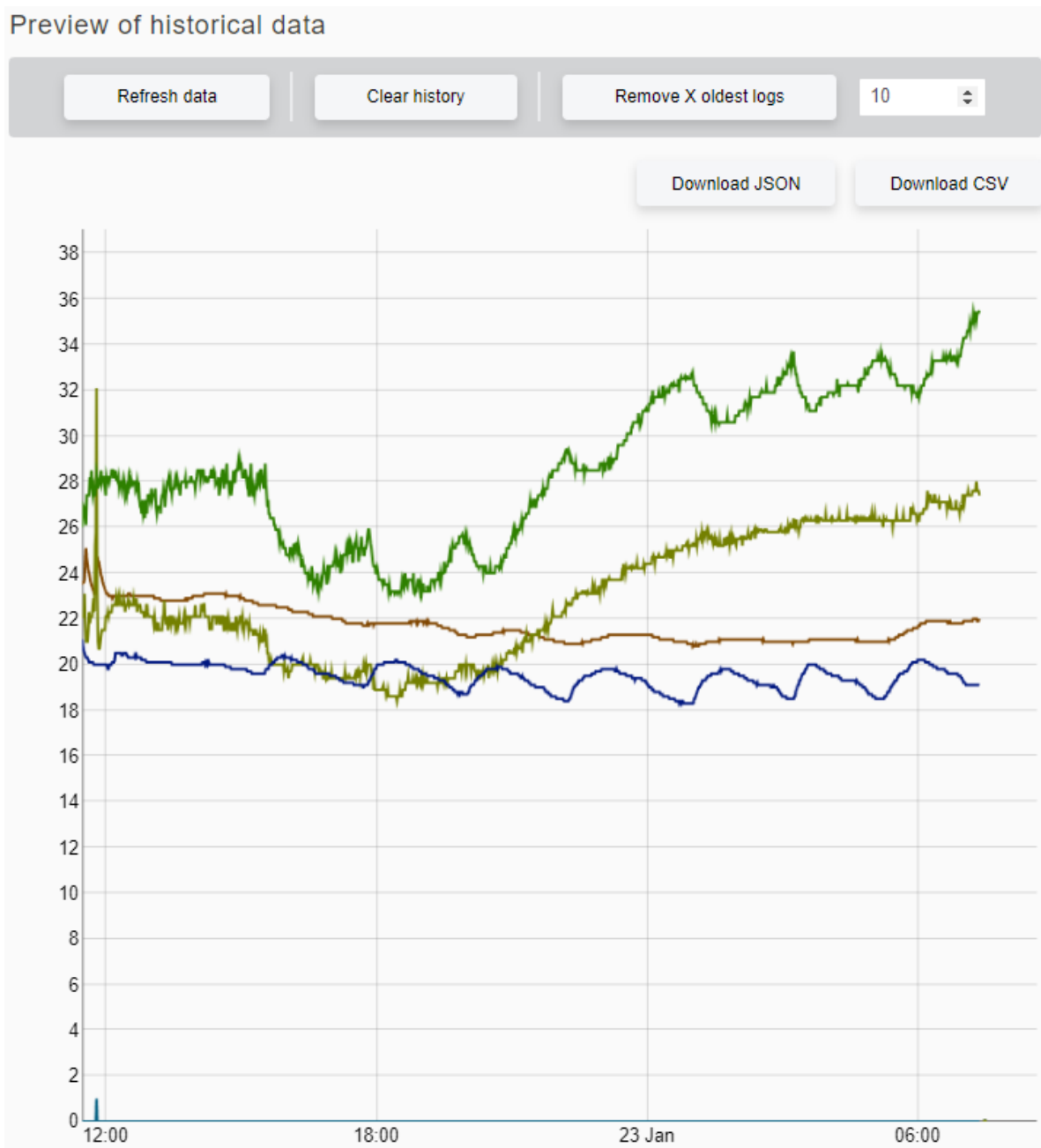


Tip

In order for the sensor data to be stored in the device memory, the data logging function must be activated - Sensors / All tab, Sensor log parameter (available in the sensor editing mode).

12.3 Chart

The tab shows the reading graphs of all sensors that have data logging attached (Sensors / All tab, Sensor log parameter).



- **Refresh data** – download the current sensor readings,
- **Download JSON** – download stored readings in JSON format,
- **Download CSV** – download stored readings in CSV format,
- **Remove X oldest logs** – remove X oldest recorded sensor measurements from the device memory.
- **Clear history** – clearing the device memory of all recorded measurements from the sensor.

12.4 —→ Operating the sensor

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

12.4.1 Assigning the sensor


First connect the sensor to the device - see section [5.2 Connection diagram](#)

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






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

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

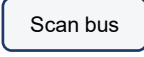
Assign or edit sensors

ID	Name	Src	Type	Log	Alarms	Config
<div style="text-align: right;">  </div>						

Sensor - ID 0

Name	Value	Description
Source	One-wire 	Select sensor value source
Sensor 1-wire address <div>Scan bus</div>		Sensor 1-wire address
Sensor name	Sens 0	Your custom sensor name
Sensor type	Not defined 	Select sensor type
Sensor hysteresis	0 	Sensor hysteresis
Sensor log	Enable 	Log sensor data in memory
Notifications		Enable notifications

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

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

Assign sensor

Sensor: 28fd4224322307b4
Type: Temperature

Assigned

Assign

Sensor: 3a862a59000000c9
Type: Input

Assigned

Assign

Sensor: 2647b989010000cc
Type: Humidity


Assigned

Assign

Scan

Assign the selected sensor by clicking on the Assign button.

Step 2: Configure the basic parameters.

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

Step 3: Preview in the Status tab

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

Enable autorefresh



Sensors

ID	Name	State	Last value	Last read
0	s0	Normal	0	8.1s
1	s1	Normal	0	8.1s
2	s2	Normal	0	8.1s











12.4.2 Storing sensor readings and viewing the graph

Performing the sensor configuration according to the instructions in the previous chapter does not guarantee that the readings are automatically stored in the device's memory. They only allow a current view of the values. To ensure that the sensor data is periodically recorded, follow the next steps:

Step 1: Enable automatic recording of sensor readings


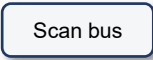




- Sensors / All tab, click on the edit sensor parameters button ,

Assign or edit sensors

ID	Name	Src	Type	Log	Alarms				Config
0	s0	1W		0	LL	L	H	HH	 
1	s1	1W		0	LL	L	H	HH	 
2	s2	1W		0	LL	L	H	HH	 
									

- Sensor configuration screen is displayed:

Sensor - ID 0

Name	Value	Description
Source	One-wire 	Select sensor value source
Sensor 1-wire address 		Sensor 1-wire address
Sensor name	Sens 0	Your custom sensor name
Sensor type	Not defined 	Select sensor type
Sensor hysteresis	0 	Sensor hysteresis
Sensor log		Log sensor data in memory
Notifications		Enable notifications





Go to Sensor log and select the Enable parameter. Confirm all settings with the button

Save

Step 2: Enable automatic logging of readings

- Sensors / History tab,

History configuration

Name	Value	Description
History		Enable measurement recording
Wait for SNTP		Records data only when SNTP time is active Go to the SNTP configuration
Period	60 	Save data from sensors every defined time [s]
Remove	30 	Remove logs older than (days)

Go to History and activate it using the slider.

When the device is rebooted or the internet connection fails, it will automatically switch to recording sensor readings using the internal real-time clock (RTC). The Wait for SNTP option allows the unit to wait for the current time to be downloaded from the network time server (SNTP) before starting to record sensor data. This ensures the time accuracy of the measurements, even if there is no internet connection.

Save

All settings should be confirmed with the button

Step 3: Setting the current time on the device

The Daxi device is equipped with an internal RTC clock with battery backup. If the device has permanent access to the Internet, the SNTP service can be switched on (see chapter [0](#)

- **Enable** – enable/disable SNMP support,
- **SNMP version** – SNMP version: v2c or v3,
- **sysDescr**
- **sysContact**
- **sysName**
- **sysLocation**
- **EngineId** – unique identifier of the device (only applies to SNMP v3),

SNMP User:

SNMP User		
User 0		
Username	<input type="text"/>	
Secure Level	<input type="text" value="noAuthnoPriv"/>	
Auth Protocol	<input type="text" value="no"/>	
Authorization Key	<input type="text"/>	
Priv Protocol	<input type="text" value="no"/>	
Private Key	<input type="text"/>	
Writable	<input type="text" value="Disable"/>	Writable

The parameters that can be set in this window allow authentication and privacy mechanisms to be defined for different users.

- **Username** – the name of the user,
- **Secure Level** – selection of the security level:
 - **noAuthnoPriv** – SNMPv3 communication takes place without any security,
 - **authNoPriv** – SNMPv3 communication authenticated but unencrypted,
 - **authPriv** – SNMPv3 communication authenticated and encrypted,
- **Auth Protocol** - choice of protocol for message authentication:
 - **no**
 - **md5**
 - **sha**
- **Authorization Key** – authorization key,
- **Priv Protocol:**
 - **no**
 - **des**
 - **aes**
- **Private Key**
- **Writable** – giving the user permission to send messages to the device.

SNMP User Trap

SNMP User Trap		
User TRAP 0		
IP	<input type="text" value="0.0.0.0"/>	
Username	<input type="text"/>	
Secure Level	<input type="text" value="noAuthnoPriv"/>	
Auth Protocol	<input type="text" value="no"/>	
Priv Protocol	<input type="text" value="no"/>	
Authorization Key	<input type="text"/>	
Private Key	<input type="text"/>	
Engine ID	<input type="text"/>	

The parameters that can be set in this window relate to the specific trap messages generated for or by a particular user.

- **IP** – the IP address of the device or system that generates the trap message,
- **Username** – the name of the SNMPv3 user,
- **Secure Level** – the security level used for SNMPv3 communication:
 - **noAuthnoPriv** - SNMPv3 communication takes place without any security,
 - **authNoPriv** – SNMPv3 communication authenticated but unencrypted,
 - **authPriv** – SNMPv3 communication authenticated and encrypted,
- **Auth Protocol** – authentication algorithm used to verify user identity:
 - **no**
 - **md5**
 - **sha**
- **Priv Protocol** – encryption algorithm used to ensure privacy of the message:
 - **no**
 - **des**
 - **aes**
- **Authorization Key** – the key used in the authentication process,
- **Private Key** – a private key,
- **Engine ID** – a unique identifier used to represent the SNMP engine instance on the device.

Download MIB file – link to download the MIB file.
SNTP).

- Services / SNTP - Enable tab, the tab allows you to set the SNTP time server, which ensures that the current time of the device is maintained despite a power failure

SNTP configuration

Name	Value	Description
SNTP	<input type="checkbox"/>	Enable SNTP client
Server	<input type="text"/>	SNTP server address
Poll time	<input type="text" value="86400"/>	Server poll time (secs)

Save

Save

All settings should be confirmed with the button

Once the unit has been configured according to the above instructions, the unit will start to save the sensor data to the internal memory. The module also allows you to view a graph of how the values read from the sensor have changed over time. You can also download the stored readings in JSON or CSV form.

12.4.3 Downloading stored sensor readings

Stored sensor readings (see previous section) can be downloaded from the device in JSON or CSV format by referring to the device's internal memory resource. Use the following command for this purpose: `http://adres_IP_urządzenia/data/log.json`.

Sensor readings can also be downloaded directly from the device page in JSON or CSV format.

To do this, use the corresponding buttons: or in the Sensors / Chart tab.

13 Configuration of notifications

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

In order for notifications to be sent effectively you must:






- Step 1.** Enable the notifications option in the tab of the selected system elements: sensors inputs or outputs, see section [13.1 Sensors](#), [13.2 Inputs](#) and [13.3 Outputs](#) to determine the type of notifications
- Step 2.** Depending on the selected notification type - SMS, e-mail, SNMP Trap, MQTT - make the configuration in the Services tab - see chapter [17 Network services](#) (Services).
- Step 3.** Enable the notification option in the Configuration tab - see chapter [13.4 Configuration](#)

13.1 Sensors

In the Sensors tab, it is possible to adjust the notification settings related to the operation of individual sensors. Notifications for the selected sensor can be activated in two ways: in the Sensors tab, during the configuration of the sensor (see chapter [12 Configuration of sensors](#)

([Sensors](#))) or by clicking on the icon  in the Notifications / Sensors tab.

Full personalisation is possible in the configuration window that appears when the notifications function is activated:

s0					
State		E-mail	SMS	SNMP Trap	MQTT
Info		<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
OK		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Error		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
 Alarm low (disabled)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
 Warning low (disabled)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
 Warning high (disabled)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
 Alarm high (disabled)		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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




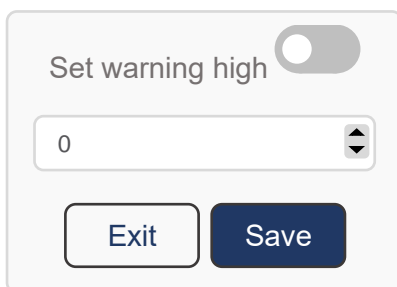
Tip


In order for E-mail, SMS, SNMP Trap and MQTT notifications to function correctly, these options must be configured in the Services tab - see chapter [17 Network services](#) (Services).

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

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

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




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




Tip

In order to activate the notification function, it is important that, in addition to the settings made here, this option is also activated on the Configuration tab - see section [13.4 Configuration](#)

13.2 Inputs

In the Inputs tab, you can configure the settings for notifications regarding the operation of the inputs connected to the device. When the icon  is pressed, notifications are activated for the selected input, leaving only its details to be configured. Full personalisation is possible in the configuration window that appears when the notifications function is activated:

DI 0 				
State	E-mail	SMS	SNMP Trap	MQTT
On change action	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Info	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

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



Tip

In order for E-mail, SMS, SNMP Trap and MQTT notifications to function correctly, these options must be configured in the Services tab - see chapter [17 Network services \(Services\)](#).

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


- **On change action** – change of the input status (on - off),
- **Info** – information about the input status.




Tip

In order to activate the notification function, it is important that, in addition to the settings made here, this option is also activated on the Configuration tab - see section [13.4 Configuration](#)

13.3 Outputs

In the Outputs tab, you can configure the settings for notifications regarding the operation of the outputs connected to the device. By pressing the icon , notifications are activated for the selected output, leaving only the details to be configured. Full personalisation is possible in the configuration window that appears when the notifications function is activated:

DO 0 				
State	E-mail	SMS	SNMP Trap	MQTT
On change action	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Info	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

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



Tip

In order for E-mail, SMS, SNMP Trap and MQTT notifications to function correctly, these options must be configured in detail under the Services tab - see chapter [17 Network services \(Services\)](#).

In the table displayed, the user has the option of selecting which types of notifications are to be sent in response to the occurrence of specific events:

- **On change action** – change of the output status (on - off),
- **Info** – information on the output status.





Tip

In order to activate the notification function, it is important that, in addition to the settings made here, this option is also activated on the Configuration tab - see section [13.4 Configuration](#)

13.4 Configuration

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

Protocol	Value	Description
Notification		Enable notification
E-mail info	<input type="text" value="86400"/>	E-mail info time [s]
SMS info	<input type="text" value="86400"/>	SMS info time [s]
MQTT info	<input type="text" value="60"/>	MQTT info time [s]
MQTT Retain		Set MQTT Retain flag
SNMP Trap	<input type="text" value="0"/>	SNMP user trap
IO time	<input type="text" value="100"/>	Minimum time before sending another state change for inputs and outputs [ms]

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

The tabs also include: Sensor, Inputs and Outputs.

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

Sensor		
E-mail	<input "[%s[?].name%]="%s[?].val%" %s[?].stattxt%"="" s[%s[?].idx%]="" type="text" value=""/>	E-mail sens subject
SMS	<input "sensor%s[?].idx%="%s[?].val%" %s[?].name%="" %s[?].stattxt%"="" type="text" value=""/>	SMS sens message
MQTT	<input "iqio="" c09bf4a003a2"="" pro="" type="text" value=""/>	MQTT sens topic

Inputs		
E-mail	<input "[%i[?].name%]="%i[?]%" i[%s[?].idx%]"="" type="text" value=""/>	E-mail input subject
SMS	<input "input%i[?].idx%="%i[?]%" %i[?].name%"="" type="text" value=""/>	SMS input message
MQTT	<input "iqio="" c09bf4a003a2"="" pro="" type="text" value=""/>	MQTT input topic

Outputs		
E-mail	<input "[%o[?].name%]="%o[?]%" o[%s[?].idx%]"="" type="text" value=""/>	E-mail output subject
SMS	<input "output%o[?].idx%="%o[?]%" %o[?].name%"="" type="text" value=""/>	SMS output message
MQTT	<input "iqio="" c09bf4a003a2"="" pro="" type="text" value=""/>	MQTT output topic

14 Binding

The Binding tab allows you to configure binding - poller settings, transferring input/output states, assigning outputs/inputs to KNX groups, etc.

14.1 Poller

Poller is a software function that regularly retrieves data of another system, device or application using the Modbus TCP or Modbus RTU protocol. The principle of the poller is to send a request to a specific target and wait for a response.

Create a poller instance

Clicking on the button will bring up further dialogues with detailed settings:

Device settings:

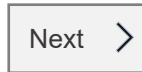
Create a new poller instance



Device settings		Next >
Poller name	<input type="text" value="name"/>	
Protocol	<input type="text" value="Modbus TCP"/> ▼	
Layer	<input type="text" value="TCP"/> ▼	
Device PDU	<input type="text" value="1"/> ▲▼	
Connection timeout [ms]	<input type="text" value="1000"/>	
Response timeout [ms]	<input type="text" value="200"/>	
IP address	<input type="text" value="e.g. 192.168.0.90"/>	
Port	<input type="text" value="502"/> ▲▼	

- **Poller name**
- **Protocol** – communication protocol for poller:
 - **Modbus TCP**
 - **Modbus RTU**
- **Layer**
 - **TCP** (optional for Modbus TCP protocol),
 - **UDP** (optional for Modbus TCP protocol),
 - **RS485/RS232** (optional for Modbus RTU protocol),

- **Device PDU** – number of the device being checked,
- **Connection timeout [ms]** (option for Modbus TCP protocol only), - connection timeout [ms],
- **Response timeout [ms]** - response timeout [ms],
- **IP address** (option only for Modbus TCP protocol) - IP address of the examined device,
- **Port** (option only for Modbus TCP protocol) - port for communication with the device being checked.



Clicking the button will take you to the next parameter window.

Data:



Create a new poller instance

Data	
Start register address	0
Number of registers	10
Register type	Coils
Refresh interval [s]	5
Writable	0

- **Start register address** - the address of the initial register,
- **Number of registers** – the number of registers,
- **Register type** – the type of register:
 - **Coils**
 - **Input Register 16-bits**
 - **Holding Register 16-bits**
 - **Discrete Inputs**
- **Refresh interval [s]** - refresh interval [s],
- **Writable** – recordable.

Mappers**Create a new poller instance**

Mappers		
Mapper name	<input type="text"/>	Mapper name to reference
Offset	<input type="text" value="0"/>	Register offset in the poller
Format	<input type="text" value="Convert to signed integer 16 bits"/>	Select variable format
Multiplication	<input type="text" value="1"/>	Scal your sensol value
Mappers		<button>Add mapper</button>

- **Mapper name** - the name of the mapper,
- **Offset** – the offset of the register,
- **Format** - selection of the format of the variable:
 - **Convert to signed integer 16 bits**
 - **Convert to unsigned integer 16 bits**
 - **Convert to signed integer 32 bits**
 - **Convert to unsigned integer 32 bits**
 - **Swap registers and convert to signed integer 32 bits**
 - **Swap registers and convert to unsigned integer 32 bits**
 - **Convert to floating-point 32 bits**
 - **Swap registers and convert to floating-point 32 bits**
- **Multiplication** - scaling of sensol values.

The button [Go to the sensor configuration](#) allows quick access to the Sensors/All tab.

14.2 Outputs

This tab enables you to assign outputs (both physical and virtual) to specific KNX groups and to redirect status from other components:

Physical outputs configuration

No.	Name	KNX read	Route to
0	DO 0	0/0/0	0[2]

- **Name** - allows the output to be renamed,
- **KNX read** - allows the output to be assigned to a KNX group - a change of state of the output will cause the data frame to be sent to the entered KNX group,
- **Route to** - indicates the source that is to influence the output state - a change of state on the channel indicated in this field will result in a corresponding change of the output state.

List of possible sources of the output state:

- **i[x]** - state of the input channel,
- **o[x]** - state of the output channel coil,
- **o[x].on** - state of the output channel,
- **v[x]** - state of virtual variable,
- **s[x].aHi** - sensor high alarm,
- **s[x].aLo** - sensor low alarm,
- **s[x].wHi** - sensor high warning state,
- **s[x].wLo** - sensor warning low state,
- **s[x].err** - sensor error,
- **s[x].ok** - sensor OK,
- **ping[x]** - ping status: 0 - error, 1- success,
- **poll[x].y** - poll value.

If the source indication is preceded by the characters "!", the state of the output relay coil will be opposite to the source state. For example: !"io[3] means that the output will have a state opposite to output 3.

14.3 Inputs

The tab allows inputs (both physical and virtual) to be assigned to specific KNX groups:

Physical inputs configuration

No.	Name	KNX read
0	DI 0	0/0/0

- **Name** - enables the input to be renamed,
- **KNX read** - allows the input to be assigned to a KNX group - - changing the state of the output will send a data frame to the KNX group entered,
- **Route from**

15 Ping of remote hosts (Watchdog)

The DAXI device has a "pinging" function. - can ping remote hosts (other network devices, servers...) and respond to their availability.

All ping pong actions

Ping pong	Actions ping OK	Actions ping Error
+		


To add a new device to the availability check, click on the + sign in the All ping pong actions table - a new Create a new ping feature dialog box will be displayed:

- **Name** - ping name
- **IP address** - IP address of the pinged device,
- **Interval** - frequency of sending ping expressed in seconds
- **Timeout** - time limit for a ping response,
- **Error tolerance** - maximum acceptable number of ping response errors before transition to error state

Create a new ping feature



Name	Value	Description
Name	<input type="text" value="ping name"/>	Input ping component name
IP Address	<input type="text" value="IP address"/>	Input the IP address of the pinged device
Interval	<input type="text" value="5"/>	Input period between pings in seconds
Timeout	<input type="text" value="1"/>	Input timeout for ping response
Error tolerance	<input type="text" value="max acceptable errors"/>	Input max acceptable errors response for ping before changing to error state

After entering all settings, confirm them with the button  - the newly created ping will appear in the table and in the columns Actions ping OK and Actions ping Error the + buttons will appear for assigning selected actions to be performed in case of a correct ping response and in case of an error - the process of assigning actions see section [11.2.1 Assigning an action](#).

16 Logic functions (Logic)

The Logic tab allows you to configure logical functions - when certain conditions are met, a specific reaction will be triggered.

To configure a new logical function, use the button

Add a condition

New condition



if

A Source
 IN
 0

 =

B Source
 IN
 0

Logical operator
 AND

if

C Source
 IN
 0

 =

D Source
 IN
 0

Result True
 None

Result False
 None

Available logical variables:

- **IN** – input
- **IN_cnt** – input counter
- **OUT** – output
- **Sens** – sensor
- **Sens_stat** – sensor value
- **Constant** – constant
- **Virt** – virtual
- **IN_active_action**

Result True / Result False - reaction to condition fulfilled / condition not fulfilled:

- **None** – no reaction,
- **Output** – activation of the output,
- **Action** – calling the defined action - see chapter [11 Defining tasks \(Action\)](#),
- **Virtual** – driving a virtual output / input.

Example:

New condition



if **A Source** Sens **B Source** Constant

Logical operator -

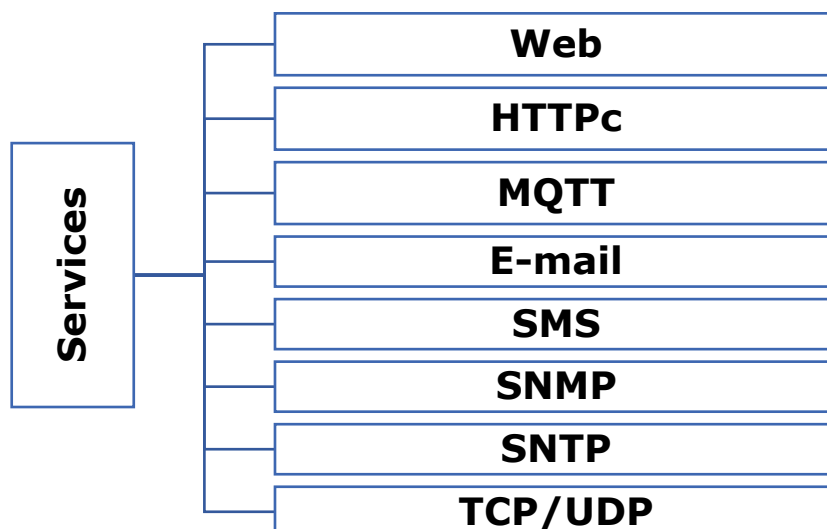
Result True Output **id** **value**

Result False Output **id** **value**

Output 7 will be switched on whenever the temperature at sensor 0 is greater than or equal to 25. If the temperature falls below this value output 7 will be switched off.

17 Network services (Services)

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



17.1 Web

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

HTTP Server configuration

Name	Value	Description
HTTP port	<input type="text" value="80"/>	HTTP access port
HTTPS port	<input type="text" value="443"/>	HTTPS access port
SSL/TLS	<input type="checkbox"/>	Enable encryption






SSL Server certificate		
SSL Key file (pem)	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>
Certificate file (pem)	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>

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





17.2 HTTPc

In this section, it is possible to configure the device to initiate HTTP connections to specific servers or services. URLs, request parameters and other connection details can be defined here. The DAXI device can send HTTP/HTTPS event information via GET or POST.

HTTP Client configuration

Name	Value	Description
HTTP Client		Enable HTTP Client
Server	<input type="text"/>	Remote server address
HTTP port	<input type="text" value="0"/> 	HTTP access port
HTTP Method	<input type="text" value="GET"/> 	HTTP request default method
Content type	<input type="text" value="text/plain"/> 	Content-type header
Resource	<input type="text" value="/"/>	Http resource i.e. /rfid.php
User	<input type="text"/>	Auth user
Password	<input type="text"/>	Auth password
HTTP ping server interval	<input type="text" value="0"/> 	Ping time in secs. 0-disable
HTTP ping server	<input type="text" value="HTTP request payload. i.e. ping=1&mac=%emac%"/>	

- **Enable** – Enable the HTTP Client service,
- **Server** – address of the HTTP server to which information will be sent,
- **HTTP Port** – the port the HTTP server is listening on,
- **HTTP Method** – the method of sending GET / POST / PUT / DELETE messages.
- **Content type** – the type of content:
 - **text/plain**
 - **json**
 - **xml**
- **Resource** – the resource that the module will refer to,
- **User** – user name,
- **Password** – password,
- **HTTP ping server** – the frequency of the ping request,
- **HTTP ping server** – content of the ping request.

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

- **SSL/TLS** – enable/disable encryption,
- **Skip cert CN check** – skip the certificate common name check
- **Use Client certificate** – require client key, password and certificate to be sent,
- **Client key password** – password for the client key.

SSL Server certificate		
SSL server root certificate	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>
Client certificate	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>
Client key	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>

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





17.3 MQTT

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

MQTT Client configuration

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



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

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

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

The device is equipped with the LWT mechanism, which stands for 'Last Will and Testament'. LWT is a mechanism that allows an MQTT client to send a message automatically in the event that the client fails or loses connection to the MQTT broker.

The LWT mechanism allows you to define the subject (topic) and content of the message that will be published when the client loses connection.

MQTT Last Will and Testament (LWT)		
LWT		Enable LWT
QoS	<input type="text" value="QOSO"/>	Quality of service
LWT retain		Set LWT retain
LWT Topic	<input type="text"/>	LWT Topic e.g.: /device/MAC_address/lwt
LWT Message	<input type="text"/>	LWT Message

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

SSL Server certificate		
SSL server root certificate	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>
Client certificate	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>
Client key	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>

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

Confirm the settings with the Save button.



Tip

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

- MQTT Address: mqtt.inveo.com.pl
- MQTT Port: 1883

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

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







Tip

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


17.4 E-mail

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

E-mail configuration

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

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

Debug		Enable debug e-mail messages
Subject	<input type="text" value="%mod_name%"/>	E-mail subject
Recipients (comma separated)	<div>E-mail recipient for a test</div>	
<div>Send test e-mail</div>	<div>Before sending a test email, save your settings. Open debbuger here!</div>	

Save

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

17.5 SMS

The DAXI device can be configured to send SMS messages in response to specific events or with information on e.g.: an alarm.

SMS API configuration

Name	Value	Description
SMS service	<input type="checkbox"/>	Enable SMS service
Provider	<input type="text" value="SMSAPI.pl"/>	Select SMS API provider
Token API	<input type="text" value=""/>	Token API (OAuth)
Limit	<input type="text" value="0"/>	Daily limit of requests to SMS service. 0 to disable
From	<input type="text" value=""/>	
Recipients (comma separated)	<input type="text" value=""/>	
<input type="button" value="Send test SMS"/>	Before sending a test SMS, save your settings. Open debugger here!	

- **Provider** – This parameter specifies the SMS service provider with which the API is integrated:
 - **SMSAPI.pl**
- **Token API** – a unique authorization key which is used to verify access and communication with API of SMS service provider
- **Limit** – daily limit of SMS messages, entering 0 will disable the SMS sending option,
- **From** – defines the sender of the SMS message; this can be a predefined name, phone number or other identifier that will be visible to the recipient of the message,
- **Recipients (comma separated)** – a list of recipients' phone numbers to which messages are to be sent; numbers should be separated by commas,
- **Send a test SMS** – this option allows you to send a test SMS message in order to verify the correctness of the configuration and operation of the service.

17.6 Modbus

Data from the device can be read and written via the MODBUS TCP protocol. The DAXI 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 configuration

Name	Value	Description
Modbus TCP	<input type="checkbox"/>	Enable modbus TCP
TCP Port	<input type="text" value="502"/>	Modbus TCP Port (default 502)
Modbus RTU	<input type="checkbox"/>	Enable modbus RTU
PDU	<input type="text" value="1"/>	
RTU Baudrate	<input type="text" value="9600"/>	
RTU Parity	<input type="text" value="None"/>	
RTU Stop bit	<input type="text" value="1"/>	
Block RFID read	<input type="text" value="Continuous"/>	Block next RFID read until unlock

Save

- **Enable TCP** - enable/disable Modbus TCP protocol support,
- **TCP Port** – Modbus TCP port (default 502),
- **Enable RTU** – enable/disable Modbus RTU protocol support,
- **PDU**
- **RTU Baudrate** – RTU baud rate,
- **RTU Parity** – RTU parity,
- **RTU Stop bit** – “stop bit”,
- **Block RFID read** - Blocking the next RFID read until it is unlocked.

The contents of the registers are shown in the following tables:

Read Coils		
Address	R/W	Description
1	R/W	Output status 0, switching on (in user-defined mode) / switching off output 0:0-off,1-on
2	R	Output status 0

Read Discrete Inputs		
Address	Name	Description
1	input0 state	Input status 0

Read Holding Registers		
Address	R/W	Description
1	R	Input 0 activation counter
2...	R	Counter for consecutive inputs
.		
.		
200		
201	R/W	Output status 0, switching on (in user-defined mode) / switching off output 0:0-off,1-on
202	R	Output operation mode 0: 0 - disable 1 - bistabile 2 - astabile 3 - one pulse
203	R	value Time on
204	R	value Time off

Read Input Registers		
concerns the sensor:	Address	
Sensor 0	1	0 - reading error (damaged sensor, incorrectly connected, etc.), 1 - sensor is providing correct readings that are within normal limits, 2 - warning of approaching low level, 3 - warning of approaching high level alarm, 4 - low level alarm condition, 5 - high level alarm condition,
	2	sensor value*10
	3	sensor value float
	4	
	5	time of last sensor reading
	6	time of last sensor reading
Sensor 1	7-12	i.e. applies to sensor 1
Sensor 2...	13...	as above for the following sensors

17.7 SNMP

This section allows the configuration of parameters for the SNMP protocol, used to monitor and manage devices on the network. The module is equipped with an SNMP v2c and v3 server. Depending on the choice of SNMP version, different setting parameters are available.

17.7.1 SNMP v2c

SNMP configuration

Name	Value	Description
SNMP	<input type="checkbox"/>	Enable SNMP
SNMP version	2c <input type="button" value="v"/>	Select SNMP version
sysDescr	<input type="text"/>	
sysContact	<input type="text"/>	
sysName	<input type="text"/>	
sysLocation	<input type="text"/>	
Read community	<input type="text"/>	SNMP v2c only
Write community	<input type="text"/>	SNMP v2c only

SNMP User Trap

- **Enable** – enable/disable SNMP support,
- **SNMP version** – SNMP version: v2c or v3,
- **sysDescr**
- **sysContact**
- **sysName**
- **sysLocation**
- **Read community** – password for reading data (only applies to SNMP v2c),
- **Write community** – password for writing data (only applies to SNMP v2c),

SNMP User Trap (window only visible for SNMP v2):

<div>Hide</div> <div>SNMP User Trap</div> <div>Hide</div>		
User TRAP 0		
Write community	<input type="text"/>	
IP	<input type="text" value="0.0.0.0"/>	
User TRAP 1		
Write community	<input type="text"/>	
IP	<input type="text" value="0.0.0.0"/>	
User TRAP 2		
Write community	<input type="text"/>	
IP	<input type="text" value="0.0.0.0"/>	

[MIB file](#)

Save

- **Write community** – password for writing data,
- **Trap IP** – address to which trap messages will be sent.

17.7.2 SNMP v3

SNMP configuration

Name	Value	Description
SNMP	<input type="checkbox"/>	Enable SNMP
SNMP version	3 <input type="button" value="v"/>	Select SNMP version
sysDescr	<input type="text"/>	
sysContact	<input type="text"/>	
sysName	<input type="text"/>	
sysLocation	<input type="text"/>	
EngineId	<input type="text"/>	

SNMP User

SNMP User Trap

[MIB file](#)

- **Enable** – enable/disable SNMP support,
- **SNMP version** – SNMP version: v2c or v3,
- **sysDescr**
- **sysContact**
- **sysName**
- **sysLocation**
- **EngineId** – unique identifier of the device (only applies to SNMP v3),

SNMP User:

SNMP User		
User 0		
Username	<input type="text"/>	
Secure Level	noAuthnoPriv ▼	
Auth Protocol	no ▼	
Authorization Key	<input type="text"/>	
Priv Protocol	no ▼	
Private Key	<input type="text"/>	
Writable	Disable	Writable

The parameters that can be set in this window allow authentication and privacy mechanisms to be defined for different users.

- **Username** – the name of the user,
- **Secure Level** – selection of the security level:
 - **noAuthnoPriv** – SNMPv3 communication takes place without any security,
 - **authNoPriv** – SNMPv3 communication authenticated but unencrypted,
 - **authPriv** – SNMPv3 communication authenticated and encrypted,
- **Auth Protocol** - choice of protocol for message authentication:
 - **no**
 - **md5**
 - **sha**
- **Authorization Key** – authorization key,
- **Priv Protocol:**
 - **no**
 - **des**
 - **aes**
- **Private Key**
- **Writable** – giving the user permission to send messages to the device.

SNMP User Trap

SNMP User Trap		
User TRAP 0		
IP	<input type="text" value="0.0.0.0"/>	
Username	<input type="text"/>	
Secure Level	<input type="text" value="noAuthnoPriv"/>	
Auth Protocol	<input type="text" value="no"/>	
Priv Protocol	<input type="text" value="no"/>	
Authorization Key	<input type="text"/>	
Private Key	<input type="text"/>	
Engine ID	<input type="text"/>	

The parameters that can be set in this window relate to the specific trap messages generated for or by a particular user.

- **IP** – the IP address of the device or system that generates the trap message,
- **Username** – the name of the SNMPv3 user,
- **Secure Level** – the security level used for SNMPv3 communication:
 - **noAuthnoPriv** - SNMPv3 communication takes place without any security,
 - **authNoPriv** – SNMPv3 communication authenticated but unencrypted,
 - **authPriv** – SNMPv3 communication authenticated and encrypted,
- **Auth Protocol** – authentication algorithm used to verify user identity:
 - **no**
 - **md5**
 - **sha**
- **Priv Protocol** – encryption algorithm used to ensure privacy of the message:
 - **no**
 - **des**
 - **aes**
- **Authorization Key** – the key used in the authentication process,
- **Private Key** – a private key,
- **Engine ID** – a unique identifier used to represent the SNMP engine instance on the device.


Download MIB file – link to download the MIB file.

17.8 SNTP

The DAXI device is equipped with SNTP protocol support, which is responsible for synchronising the device's time with the SNTP server. This is crucial for correct data logging and time tasks.

The options available under Services / SNTP allow you to configure the SNTP time server.

SNTP configuration

Name	Value	Description
SNTP		Enable SNTP client
Server	<input type="text" value="194.146.251.100"/>	SNTP server address
Poll time	<input type="text" value="1"/>	Server poll time (secs)

Save

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



Tip

Examples of SNTP servers:

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

In addition, the DAXI device is equipped with an internal RTC clock with battery backup. When the device does not have permanent access to the Internet, it can use this clock to maintain accurate time - see section [18.3 Time](#).

17.9 TCP/UDP

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

TCP/UDP server configuration

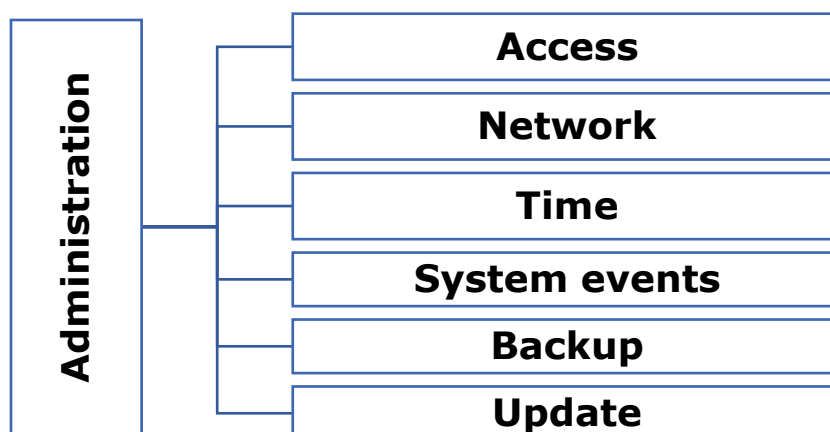
Name	Value	Description
TCP server	<input type="checkbox"/>	Enable TCP server
TCP Port	<input type="text" value="502"/>	TCP server port
UDP server	<input type="checkbox"/>	Enable UDP server
UDP Port	<input type="text" value="502"/>	UDP server port

Save

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

18 System administration (Administration)



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



18.1 Access

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

Access configuration

Name	Value	Description
Password		Enable password
Current password	<input type="password"/>	
New password	<input type="password"/>	
Repeat new password	<input type="password"/>	
Module name	<input type="text"/>	
Enable remote config		Allow change configuration by Discoverer app

Save

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



Tip

Default settings on the device:

- login: admin
- hasło: admin

18.2 Network

The network settings of the device are configured on this tab - see chapter 7.3 Configuring network settings [Błąd! Nie można odnaleźć źródła odwołania. Configuring network settings.](#)

18.3 Time

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

Time status

Name	Value
Current time	13:58:17
Current date	30-11-2023
Update time in the device	<button>Update time</button>

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

Time zone

Name	Value
Daylight saving	<input type="checkbox"/>
Time zone	(GMT) Western Europe Time. London. Lisbon ▼

Save




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

The DAXI device is equipped with an internal RTC clock with battery backup. When the device has permanent access to the Internet, the SNTP service can be used to ensure precise time synchronisation (see chapter [17.8 SNTP](#)).

18.4 System events

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

Log events to flash settings

Name	Value	Description
Flash log		Enable system events write to flash
Log system events		Log Power-On, time changes, reset to default, reboots, config changes
Log network events		Log network events

Save

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

18.5 Backup

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

Create a backup file

Enter password	<input type="password"/>
Re-type password	<input type="password"/>

Download

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

Download

The button allows you to save the backup to your computer.

Restore

Backup password	<input type="text" value="Repeat your backup password"/>	Enter your backup password
Backup file	<input type="button" value="Wybierz plik"/> Nie wybrano pliku	<input type="button" value="Upload"/>

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

The button will upload the selected backup to the device.

Button enables rebooting the device.

Button restores the factory settings of the device.

18.6 Update

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

Firmware update

<input type="button" value="Browse"/>	File name	File size (bytes)
	iqio.bin	2101264



Warning

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

19 Emergency software upload / factory reset

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

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



Tip

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

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

Firmware recovery mode

Bootloader ver: 0.1

Browse...

Update Firmware

Reset to default

Reboot

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

20 Built-in variables

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

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

%s[x]%	%s[3]%	Sensor value Example: the value for sensor no. 3 will be shown.
%s[x].statTxt	%s[2].statTxt	Sensor status Example: the value for sensor no. 2 will be shown
%o[x]%	%o[4]%	Output status Example: the status of output 4 will be shown
%i[x]%	%i[1]%	Input status Example: the status of input 1 will be shown
%v[x]%		Value of virtual variable
%cntx%		Input counter value

21 IO commands

Below is a summary of the commands used to create actions based on IO commands (see section [11.1 All](#)). It is worth noting that the following commands are also effective using various protocols such as HTTP, MQTT, UDP and TCP.

Syntax	Description	Values
out_all=10n-11100	command that controls all outputs	1 - on
		0 - switch off
		n - change state to opposite
		- do not change state
out_on=ch	switch the output on	ch = output number
out_off=ch	switch the output off	ch = output number
out_inv=ch	change of state to the opposite	ch = output number
out_blink=ch,ton,toff,cnt	command to switch an output on or off	ch - output number
		ton - output activation time, measured from the moment the action is activated, expressed in 0.1 second, e.g: 10=1second
		toff - output switch-off time measured from the time defined in the tone parameter, expressed in 0.1 second
		cnt - parameter specifying how many times the output is to be activated during a single action; if the field is left blank the output will be activated an infinite number of times
out_time=ch,ton,toff	command to turn the output on for a specified period	ch - output number
		ton - output switch-off time measured from the time defined in the tone parameter, expressed in 0.1 seconds
		toff - output cut-off time measured from the time defined in the tone parameter, expressed in 0.1 second, entering the value of single will switch the output on permanently



www.inveo.com.pl



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



ul. Rzemieślnicza 21
43-340 Kozy



serwis@inveo.com.pl