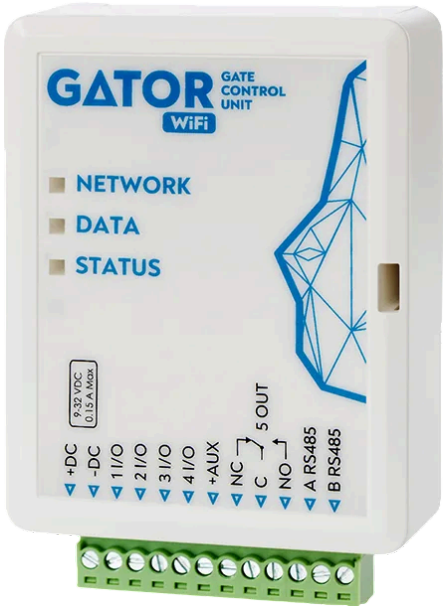
mobilamb
TRIKDIS Official Distributor

WP17 GATOR WiFi gate controller – installation and programming manual

Installation and programming manual for the Trikdis WP17 GATOR WiFi gate controller: wiring, Wi-Fi setup, users and permissions, control from the Protegus 2 app.



Edition: 2026-11-17
Always up-to-date web version: https://mobilamb.eu/wp17-manual

Contents

1. Overview

- 1.1 What it is for and how it works
- 1.2 Technical data
- 1.3 Parts and terminals of the device
- 1.4 LED indications
- 1.5 Package contents and required tools

2. Quick start

- 2.1 Commissioning in four steps
- 2.2 Only authorised people should be able to open
- 2.3 Monitoring station and further settings

3. Installation and wiring

- 3.1 Mounting and placement
- 3.2 Power supply and wiring the gate opener
- 3.3 Inputs
- 3.4 Wiring a relay to the universal output
- 3.5 Wiring an indicator LED
- 3.6 Wiring an RFID reader (Wiegand 26/34)
- 3.7 RF-LORA and iO-LORA expanders with RFID reader

4. Control

- 4.1 Wi-Fi pairing from Protegus 2
- 4.2 Widget on the phone's home screen
- 4.3 Managing users in the app

5. Setup with the TrikdisConfig software

- 5.1 The status bar
- 5.2 "System Options" page
- 5.3 "IN/OUT" page
  - 5.3.1 IN/OUT tab – the inputs and outputs
  - 5.3.2 Scheduler tab – scheduling the outputs
  - 5.3.3 Holidays tab – holidays
- 5.4 "Modules" page
- 5.5 "IP Reporting" page
- 5.6 "User list" page
  - 5.6.1 Users tab – the users
  - 5.6.2 Registering an RFID card (key fob)
  - 5.6.3 Scheduler tab – scheduling the users
  - 5.6.4 Black list tab – black list
- 5.7 "Events Log" page
- 5.8 Restoring the default settings
- 5.9 Indicating the gate's state

6. Remote programming

7. Checking operation

8. Firmware update

9. Troubleshooting and frequently asked questions

10. Safety instructions

See also

1. Overview

The **WP17 GATOR WiFi** is the Trikdis gate controller that works over a Wi-Fi network: it is designed for remote control of electric gates, barriers, garage doors and other equipment. The user controls it from the **Protegus 2** app – from a phone, a tablet or a browser –; the device handles up to **1000 users** (by e-mail address or RFID card – a user who controls it from the app is entered with their e-mail address), and a separate schedule, validity period and counter (how many times they may control the system) can be set for each user. It has no SIM card: it reaches the internet over the site's 2.4 GHz Wi-Fi network, so it works without a mobile subscription and without a monthly fee. It notifies about state changes of the inputs and outputs – activation and restore – in the app, and also forwards the events to the monitoring station in Contact ID format. With an **RF-LORA** transceiver, up to 8 wireless **iO-LORA** expanders can be connected to it, so one device can control up to 9 gates or barriers located far from each other, each with its own RFID reader. You make the settings with the **TrikdisConfig** software, over a USB cable or remotely.

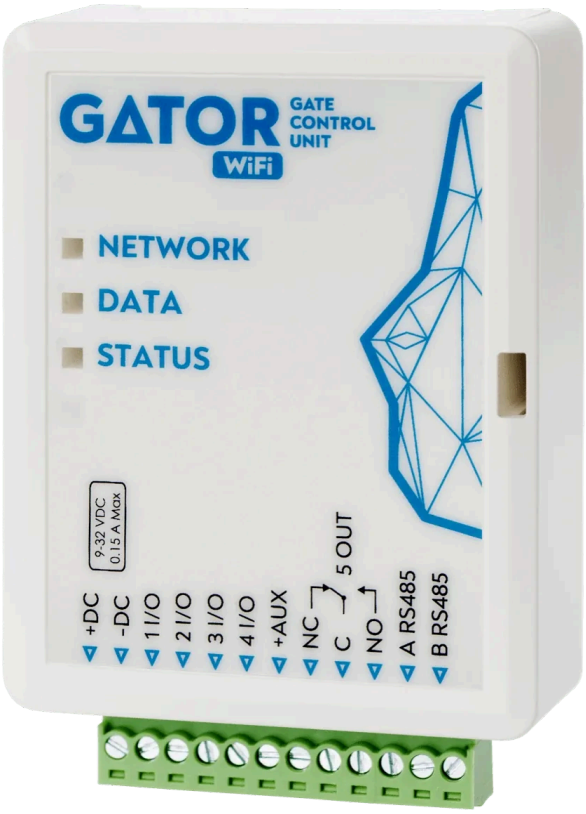


Figure 1. The WP17 GATOR WiFi gate controller: at the front the NETWORK, DATA and STATUS indicators, at the bottom the detachable terminal block (+DC, −DC, 1–4 I/O, +AUX, the relay's NC / C / NO contacts – 5 OUT – and the A / B terminals of the RS485 bus).

1.1 What it is for and how it works

What it is best for

- **Remote opening of gates, barriers and garage doors** for the family, the residents of a building, the employees of a company or the tenants of a car park – wherever there is Wi-Fi: a house, a block of flats, an office, a business site. The user opens with one button in the Protegus 2 app, and on an

Android phone also without opening the app, with a widget placed on the home screen. No SIM card, no mobile subscription, no monthly fee.
- **Access control with RFID card and code**: with one Wiegand 26/34 reader, an exit push button, and per-user scheduling (who may enter when), validity period and entry counter.
- **Any other equipment** switched on and off remotely, in pulse or two-state (level) mode, also on a schedule: lighting, irrigation, a pump, heating.
- **Several gates in one system**: wirelessly with the RF-LORA and iO-LORA modules, up to 8 additional locations, each with its own relay, input and RFID reader – Flexible wireless access control with the GATOR RF-LoRa system.

How it works

- **Control**: from the Protegus 2 mobile and web app, with an Android widget, on site with RFID card and code; as local automation with an input (**CTRL by IN**) or on a schedule. **It does not respond to phone calls or SMS** – it has no SIM card. If control by call or SMS is needed, or there is no Wi-Fi at the gate, the cellular GV17 GATOR is the right choice.
- **Notifications to the user**: push messages in the Protegus 2 app about events of the inputs and outputs and about the test.
- **Reporting to the monitoring station**: with Contact ID event codes to Trikdis software and hardware IP receivers (TCP/IP or UDP/IP over the Wi-Fi network), which work with any monitoring software; primary and backup receiver – if the connection to the primary receiver is lost, messages automatically go to the backup receiver; events can go to the monitoring station and to Protegus 2 at the same time.
- **Inputs and outputs**: 4 universal terminals (as inputs NO, NC or EOL 10 kΩ, as outputs open collector, 50 mA) and 1 relay output (1 A / 30 V DC, 0.5 A / 125 V AC). Each iO-LORA expander adds 1 input and 1 relay output to the system (up to 8 expanders, i.e. up to 8 additional inputs and 8 additional outputs in total).
- **Installation and setup**: you pair it with the Wi-Fi network from the Protegus 2 app using the device's **PAIR** button – there is no need to touch the router; you add and delete users from Protegus 2 (as administrator) or with the TrikdisConfig software; setup is done with a USB Mini-B cable or remotely; the firmware can also be updated remotely.

Trikdis WP17 Smart WiFi controller

1.2 Technical data

Property	Value
Supply voltage	9–32 V DC
Current consumption	150 mA
Universal inputs/outputs	4; as inputs NC, NO, EOL = 10 kΩ, as outputs open collector (OC), up to 50 mA
Output	1 relay, 1 A / 30 V DC, 0.5 A / 125 V AC
Connection to the monitoring station	TCP/IP or UDP/IP over the Wi-Fi network
Event transmission protocol	TRK_TCP or TRK_UDP
Encryption key	6 characters
Wi-Fi	2.4 GHz, 802.11 b/g/n; WPA, WPA2 or mixed (WPA mixed) encryption
Network settings	DHCP (automatic) or manual IP setup (from a phone or a computer)

Property	Value
Buffer for unsent events	up to 60 events
Event log	up to 5000 events
Users allowed to control	1000
Supported modules	iO-LORA expander (via the RF-LORA transceiver, up to 8; to use the iO-LORA, an RF-LORA transceiver must be connected to the WP17)
Operating environment	–10 … +50 °C, up to 80 % relative humidity at +20 °C
Dimensions	88 × 62 × 26 mm
Weight	80 g

2.4 GHz Wi-Fi only

The WP17 connects only to **2.4 GHz** Wi-Fi networks (802.11 b/g/n); it does not see 5 GHz networks. If your router broadcasts both bands under one name, pairing will also need the 2.4 GHz network.

1.3 Parts and terminals of the device

The numbers in the figure mark the parts of the device; the meaning of the terminals is given in the table.

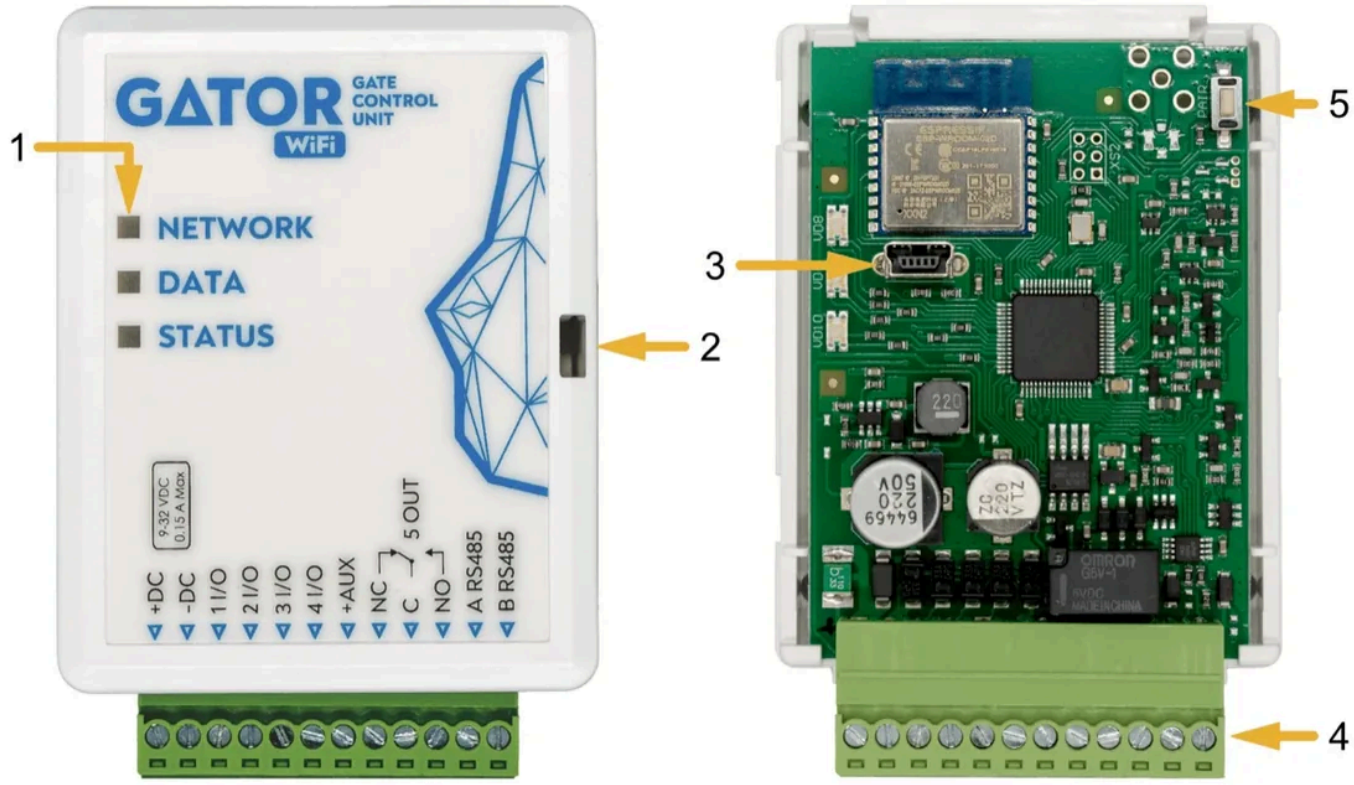


Figure 2. Parts of the WP17: on the left the front view, on the right the printed circuit board under the removed front cover.

- 1 LED indicators
- 2 opening for removing the front cover
- 3 USB Mini-B connector for programming
- 4 detachable terminal block
- 5 PAIR button – switches on the Wi-Fi pairing (configuration) mode

Terminal	Purpose
+DC	supply voltage 9–32 V DC, positive pole
–DC	negative pole of the supply voltage; common point of the inputs
1 I/O	universal terminal: input (NO, NC, EOL) or open-collector output
2 I/O	universal terminal: input or output
3 I/O	universal terminal: input or output
4 I/O	universal terminal: input or output
+AUX	positive power output for external devices (relay, LED)
NC	the relay's normally closed contact
C	the relay's common contact
NO	the relay's normally open contact
A RS485	wire A of the RS485 bus (RF-LORA transceiver)
B RS485	wire B of the RS485 bus

The software and the app handle the relay output as **5 OUT** (**Output5**); the four universal terminals appear in the software as **1 I/O … 4 I/O**. By default 1 I/O and 2 I/O are NO inputs, 3 I/O and 4 I/O are open-collector outputs; on the default TrikdisConfig screen all four terminals are **Disabled** – in every case you set the function on the **IN/OUT** page (section 5.3). The 12-pin terminal block can be pulled off the device.

1.4 LED indications

Indicator	Light	Meaning
NETWORK	green, steady	connected to the Wi-Fi network
	green flashing	connecting to the Wi-Fi network
	yellow flashing	Wi-Fi signal strength with 0–5 flashes
	fast green-yellow flashing	Wi-Fi pairing (configuration) mode
DATA	green, steady	sending a message
	yellow, steady	there are events in the buffer waiting to be sent
STATUS	green flashing	no operating fault
	1 red flash	cannot connect to the Wi-Fi network
	2 red flashes	weak Wi-Fi signal
	3 red flashes	cannot connect to the primary IP receiver
	4 red flashes	cannot connect to the Protegus 2 server
	5 red flashes	cannot connect to any receiver channel
	6 red flashes	the internal clock is not set
	7 red flashes	the supply voltage is low

If none of the LEDs is lit, check the supply voltage and the wiring. If STATUS indicates a weak signal with 2 red flashes, find a place for the device closer to the router, or put a Wi-Fi access point closer to it.

The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for an Ethernet device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network the most common culprit is the APN or the data service of the SIM card; on Ethernet, the router, the firewall or the DNS. When the DATA LED goes out, the message has been sent and the data connection is fine.

1.5 Package contents and required tools

In the box: 1 WP17 GATOR WiFi gate controller, 3 resistors of 10 kΩ, 1 piece of double-sided adhesive tape (5 cm) and 2 screws. There is no antenna in the package, and none is needed: the Wi-Fi antenna is on the printed circuit board.

What you will need

Before starting the installation, make sure you have all the necessary accessories: a USB Mini-B cable for setup · a cable with at least 4 wires for the wiring · a 2.5 mm flat screwdriver · a 9–32 V DC power supply of at least 0.2 A (or the gate opener's DC power output) · a **2.4 GHz Wi-Fi network** available on site and its password · the Protegus 2 app on your phone, with an account you are logged in to · the installer manual of the controlled device (gate motor, barrier), including the wiring of its control input and gate status output. These are not in the package: obtain the necessary accessories separately from your distributor.

2. Quick start

The WP17 has no SIM card – you pair it with the Wi-Fi network from the app

The device reaches the internet over the site's Wi-Fi network, so the first step is always pairing. There is no need to touch the router for this: using the WP17's **PAIR** button, the Protegus 2 app builds a temporary connection with the device and hands it the name and password of the Wi-Fi network. After that the device connects by itself, and you open the gate with the **Output5** button in the app.

2.1 Commissioning in four steps

1. **Mount and wire it** according to the drawings in chapter 3: the power supply (9–32 V DC) to the **+DC** and **–DC** terminals, the gate opener's control input to the relay's **C** and **NO** contacts. Put it where the Wi-Fi reception is good (section 3.1).
2. **Switch on the power.** The meaning of the LEDs is in section 1.4; without a Wi-Fi network the **STATUS** LED indicates with 1 red flash that it cannot connect yet – this is normal before pairing.
3. **Pair it with the Wi-Fi network from Protegus 2** (section 4.1 step by step, with pictures): **Add new system** → the device's **MAC** number from the sticker or from the QR code → **Start WiFi configuration WP17** → remove the WP17's cover and press the **PAIR** button for 3 seconds (the **NETWORK** LED flashes green-yellow quickly) → select the Wi-Fi network, enter its password → **Connect** → enter the system name → **Skip**.
4. **Try it.** After at most 1 minute the system is **Online**; on the **Output5** button the relay pulls in for 3 seconds and the gate opens. The **NETWORK** LED is steady green and flashes yellow according to the signal strength, **STATUS** flashes green.

2.2 Only authorised people should be able to open

Only someone who has access to the system in Protegus 2 can control the WP17: whoever added the system is its administrator, and they add the other users by e-mail address from the app (section 4.3) or on the TrikdisConfig **User list** page (section 5.6); RFID cards and codes are registered in the same place. A schedule, a validity period and a counter can be assigned to each user, and banned cards and addresses can be put on a black list.

Change the default codes

The device's two default codes are known (`123456`): the **administrator code** (**System Options** → **Administrator Code**), with which every setting of the WP17 can be changed, and the **cloud access code** (**IP Reporting** → **Cloud Access Code**), which Protegus 2 asks for when the system is added. At the first commissioning, change both in TrikdisConfig (sections 5.2 and 5.5).

2.3 Monitoring station and further settings

- **Protegus cloud:** enabled by default (**IP Reporting** → **Enable cloud service**, section 5.5) – that is why pairing and the app work without any further setting; do not switch it off.
- **Monitoring station:** on the **IP Reporting** page enter the receiver's address, port and encryption key (TCP/IP or UDP/IP), and on the **System Options** page the object ID (sections 5.2 and 5.5).
- **Wi-Fi without a phone:** you can also enter the name and password of the Wi-Fi network in TrikdisConfig, over a USB cable (**System Options** → **Communicator network settings**, section 5.2); a static IP address instead of DHCP can be set in the same place.
- **Recommended order of settings:** Wi-Fi pairing → administrator and cloud code → function of the inputs and outputs, pulse time → users, RFID cards, scheduling → monitoring station → testing according to chapter 7.

3. Installation and wiring

Figyelem!

Tilos a vezetékezést feszültség alatt álló eszközön elvégezni. A munka előtt a megfelelő áramtalanításról és érintésvédelemről (beleértve a szünetmentes működést biztosító akkumulátorokat) gondoskodni kell.

This chapter describes mounting the WP17, the power supply, wiring the gate opener, the inputs, the relay and the indicator LED, and then connecting the RFID reader and the RF-LORA + iO-LORA expanders. In the drawings the terminal names match the markings on the device (section 1.3).

3.1 Mounting and placement

1. Remove the front cover (insert the screwdriver into the side opening and snap it off), then pull off the terminal block.
2. Take the printed circuit board out of the case: press the retaining tab and lift it out.
3. Fix the back of the case in the desired place with screws (or with the supplied double-sided adhesive tape).
4. Put the printed circuit board and the terminal block back.
5. Put the front cover back.

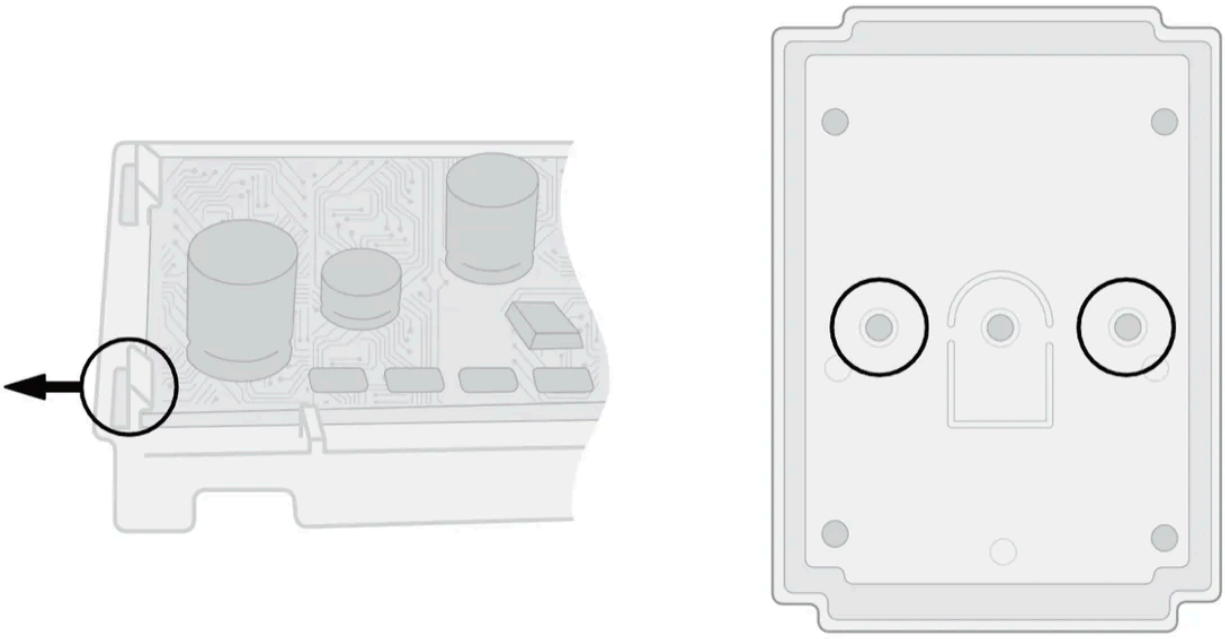


Figure 3. On the left the retaining tab of the printed circuit board (pressed in the direction of the arrow, the board comes free), on the right the two screw holes of the back plate.

The terminal block can be pulled off: this way the device can be powered down or restarted with one movement, it is easier to handle during wiring, and for USB programming the device can be taken to the computer.

Where should the device be?

The Wi-Fi antenna is on the board, so a metal enclosure and thick walls weaken reception: inside the gate opener's metal control box the Wi-Fi often does not reach. Choose a place where the number of yellow flashes of the **NETWORK** LED is as high as possible (section 1.4); if the **STATUS** LED indicates a weak signal with 2 red flashes, put the device outside the box, or place a Wi-Fi access point closer.

3.2 Power supply and wiring the gate opener

The WP17 works from a **9–32 V DC** supply (at least 0.2 A); **it does not accept alternating voltage**, so the 24 V AC accessory power output of gate openers is not suitable for it directly – in that case use the gate opener's DC output or a separate DC power supply. The device has no backup battery: if the gate must also open during a power cut, run it from an uninterruptible power supply. The gate opener's control input goes to the relay's **C** and **NO** contacts; the relay's pulse does the same as the button of the remote control. Wire the WP17 according to the drawing below.

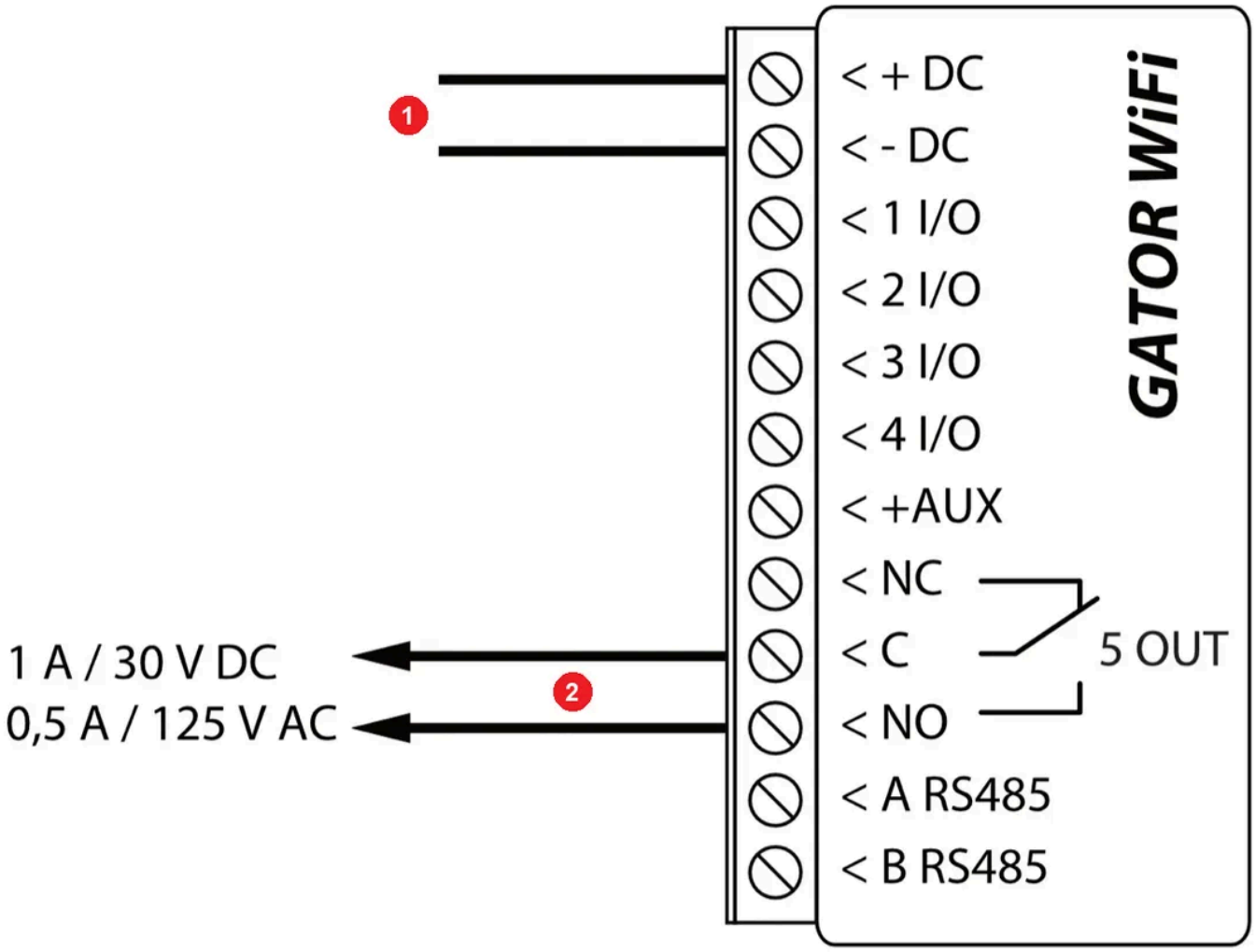


Figure 4. Wiring the power supply and the gate opener: 9–32 V, 0.2 A DC power supply, its positive pole to the +DC, its negative pole to the −DC terminal; the gate opener's control input to the C and NO contacts of the relay (5 OUT); the relay's rating is 1 A / 30 V DC or 0.5 A / 125 V AC.

- 1 DC power supply source, 9–32 V, 0.2 A
- 2 Door control – the gate opener's control input

Always do the wiring with the power off. The terminals of the gate opener's control unit and their rated voltage are described in the gate motor's documentation – the drawing only shows the typical arrangement.

Most gate openers have a **gate status output** (OUT), which indicates whether the gate is open or closed; this can be a voltage output or a relay output. In the drawing the auxiliary relay K1 is connected to a gate opener with a voltage output: with the gate open, ~230 V can be measured between the gate opener's OUT and N terminals, relay K1 pulls in and activates the WP17's **1 I/O** input. This way the state of 1 I/O follows the position of the gate exactly, which is also shown by Protegus 2 and by the widget icon – the related setting is in section 5.9. With a gate opener that has a relay output, K1 is not needed; the status contact can be wired directly between 1 I/O and −DC.

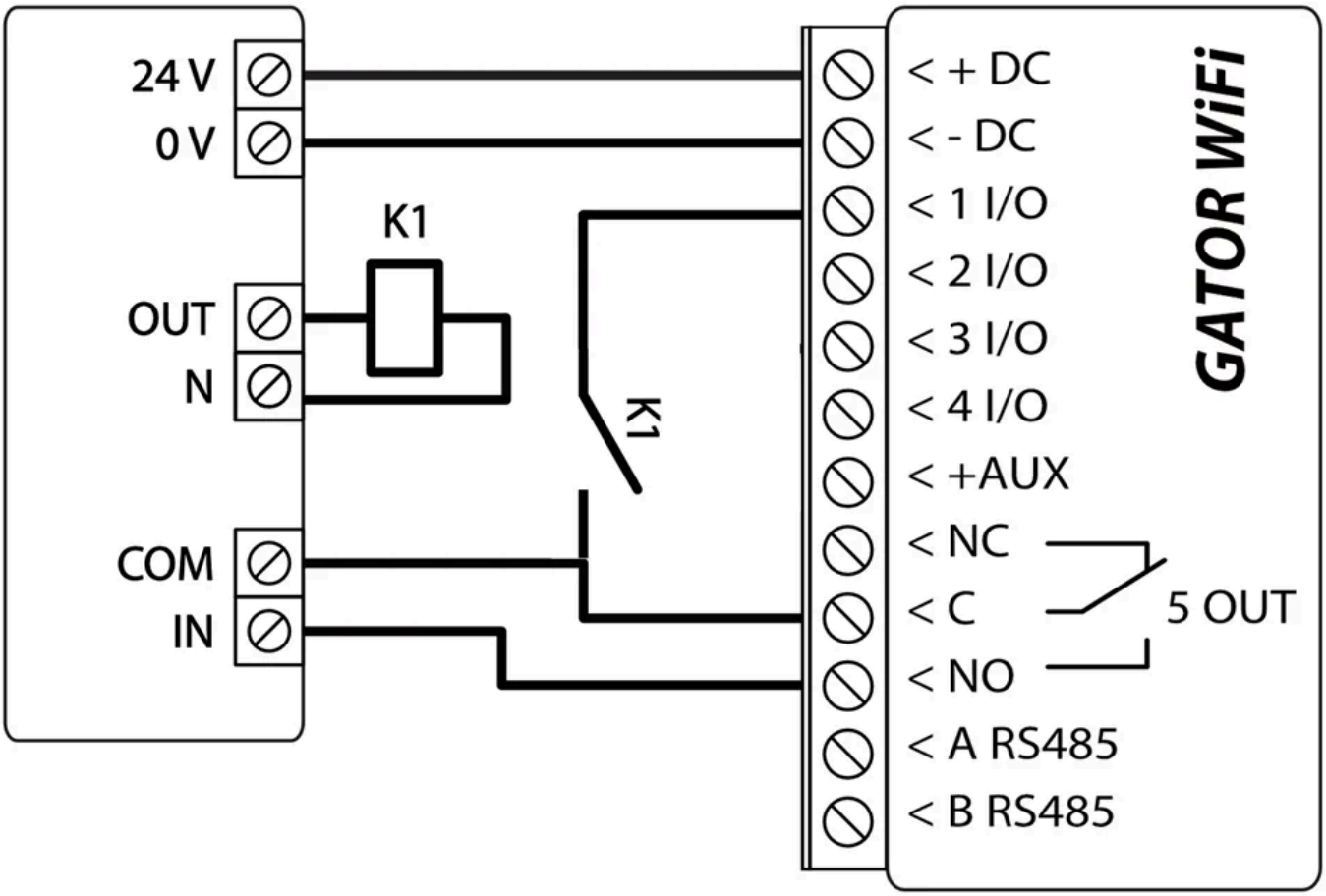


Figure 5. Connecting the gate opener control unit (the box on the left, "Gate control unit") and the WP17 with the auxiliary relay K1: the gate opener's 24 V power output to the WP17's +DC, 0 V to the −DC terminal; the gate opener's OUT and N terminals to the coil of relay K1, the contact of K1 between the WP17's 1 I/O and −DC terminals; the gate opener's COM terminal to the WP17's 5 OUT C contact, its IN terminal to the 5 OUT NO contact.

3.3 Inputs

The WP17's **four universal terminals** (1 I/O ... 4 I/O) can be set as inputs or outputs. As inputs they work relative to the **−DC** terminal, and their type can be **NO**, **NC** or **EOL** (with a 10 kΩ end-of-line resistor); three end-of-line resistors are in the package. To an input you can connect the gate's status output or limit switch (sections 3.2 and 5.9), the exit push button (section 3.6), or any sensor or contact about whose changes you want a push message, or with which you want to switch an output (**CTRL by IN**, section 5.3). The function, the type and the response time are set on the TrikdisConfig **IN/OUT** page. The wiring must match the set input type (NC, NO, EOL) – according to the drawings below.

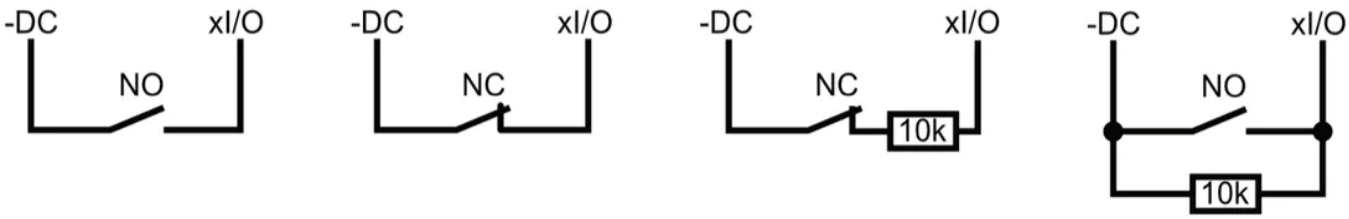


Figure 6. The four ways of wiring the inputs between the −DC and the I/O terminal. From left to right: **Normally open (NO)** – normally open contact: closing = activation, opening = restore; **Normally closed (NC)** – normally closed contact: opening = activation, closing = restore; **NC + 10 kΩ EOL** – normally closed contact with a 10 kΩ resistor in series: short circuit and open circuit = activation, 10 kΩ = rest; **NO + 10 kΩ EOL** – normally open contact with a 10 kΩ resistor in parallel: short circuit and open circuit = activation, 10 kΩ = rest.

3.4 Wiring a relay to the universal output

As an output the I/O terminal is open collector, with a load capacity of at most **50 mA**: directly it can only switch the coil of a small relay. With the relay's contacts any equipment can be switched on and off remotely. One end of the coil goes to the **+AUX** terminal, the other to the output; in TrikdisConfig the terminal's function must be set to **Output** (section 5.3).

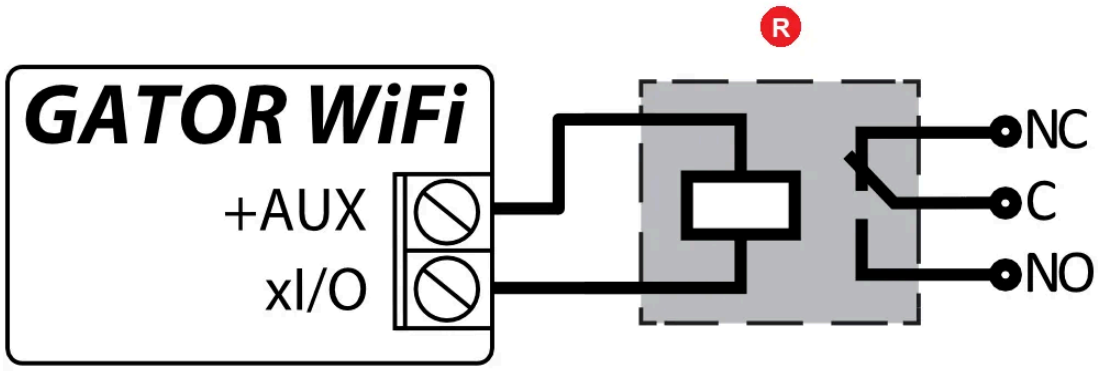


Figure 7. External relay on the universal output: the coil between +AUX and the I/O terminal set as output (xI/O); the relay's NC, C and NO contacts switch the equipment.

- R Relay

3.5 Wiring an indicator LED

For local indication of the output's state, an LED can also be connected to the universal output: from the **+AUX** terminal through a 2.2 kΩ (2k2) series resistor to the LED, and from there to the output; here too the terminal's function is **Output**.

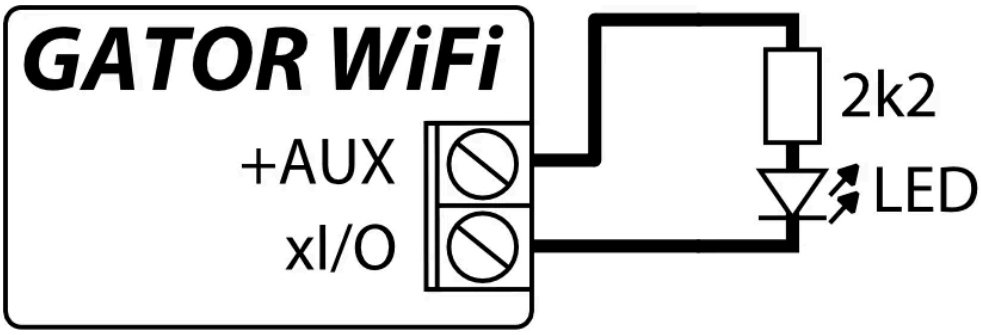


Figure 8. LED on the universal output: +AUX → 2k2 (2.2 kΩ) series resistor → LED → the I/O terminal set as output (xI/O).

3.6 Wiring an RFID reader (Wiegand 26/34)

The WP17 accepts **one Wiegand 26/34** RFID reader (a card reader or a reader with a code keypad). With the cards and codes entered in the user list the reader switches **only the 5 OUT** output; the per-user permission, schedule and counter also apply to the reader. The wire colour code follows the Wiegand standard: red +U, black GND, green D0, white D1. Wiring: red → **+DC**, black → **–DC**, green (D0) → **1 I/O**, white (D1) → **2 I/O**; the exit push button between **–DC** and **3 I/O**. The reader works from the 9–16 V DC, 0.5 A supply shared with the WP17.

On the TrikdisConfig **IN/OUT** page tick the **Wiegand reader mode** checkbox (section 5.3); after that, pressing the exit button wired to 3 I/O switches 5 OUT on for the set pulse time. Cards are added on the **User list** page (section 5.6.2).

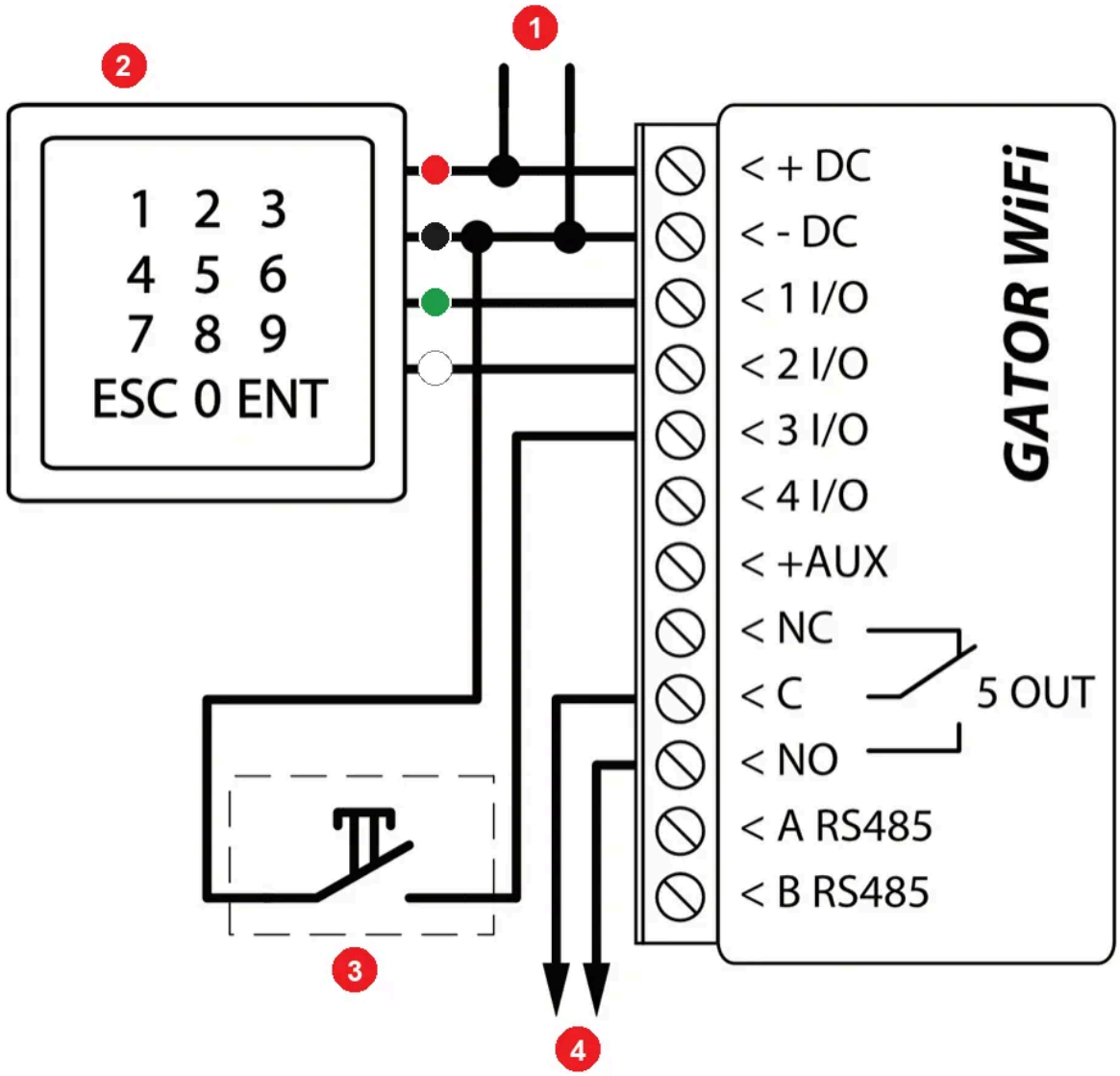


Figure 9. Wiring a Wiegand 26/34 reader and an exit button: DC power supply, 9–16 V, 0.5 A, to the +DC and −DC terminals; the reader's red wire (+U) to +DC, black (GND) to −DC, green (D0) to the 1 I/O, white (D1) to the 2 I/O terminal; the exit push button between the −DC and 3 I/O terminals; the gate opener on the relay's C and NO contacts (1 A / 30 V DC, 0.5 A / 125 V AC).

- 1 DC power supply, 9–16 V, 0.5 A
- 2 Entry reader – RFID reader with keypad (Wiegand 26/34)
- 3 "Exit" button
- 4 Gate control – the gate opener's control input; the relay's rating is 1 A / 30 V DC, 0.5 A / 125 V AC
- red wire, +U ("R - red (+U)")
- black wire, GND ("B - black (GND)")
- green wire, D0 ("G - green (D0)")
- white wire, D1 ("W - white (D1)")

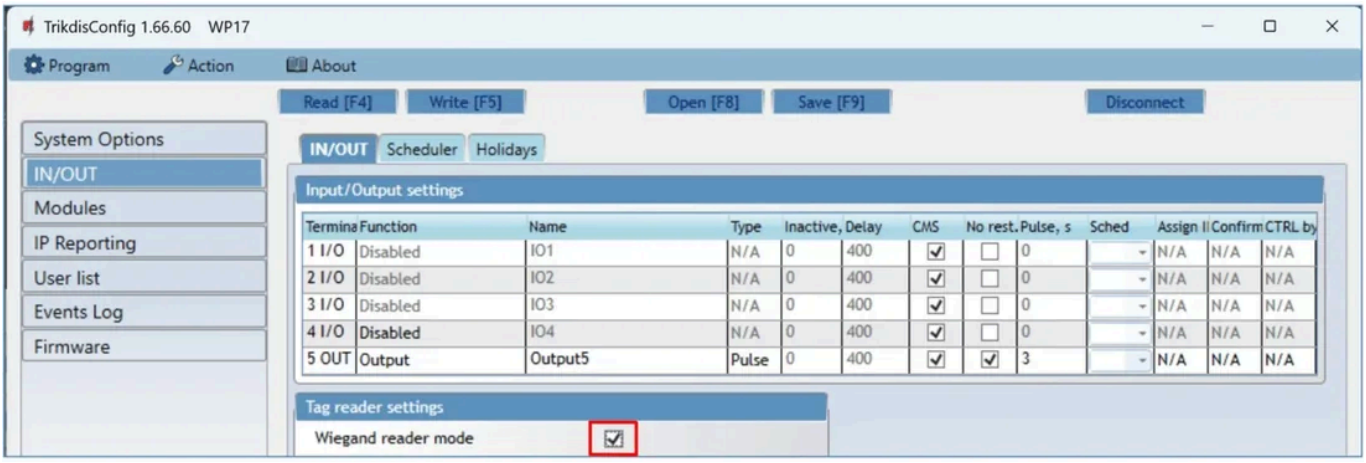


Figure 10. TrikdisConfig – IN/OUT, **Tag reader settings**: **Wiegand reader mode** ticked; the **5 OUT** row has the **Output** function, **Pulse** type, with a 3 s pulse.

If the reader has a 5 V (low-voltage) signal level, tick the **Low voltage reader** checkbox; if the reader gives very short pulses and the device does not recognise the card, switch off the internal filter with the **Disable reader filter** checkbox (section 5.3).

3.7 RF-LORA and iO-LORA expanders with RFID reader

From WP17 firmware **1.21** the system can be expanded wirelessly: the **RF-LORA** transceiver connects to the RS485 bus (A–A, B–B, shared 9–16 V DC supply) and keeps a radio connection with up to **8 iO-LORA** expanders. Each iO-LORA expander adds one input and one relay output to the system, and its own Wiegand 26/34 RFID reader can be connected to it: the reader switches **only the relay output of its own expander**, not a remote output. This way one WP17 can control up to **9 gates** (its own relay and 8 expanders), each with its own card reader and exit button – details of the solution: Flexible wireless access control with the GATOR RF-LoRa system.

Trikdis RF-LORA wireless expander module **Trikdis IO-LORA wireless expander module**

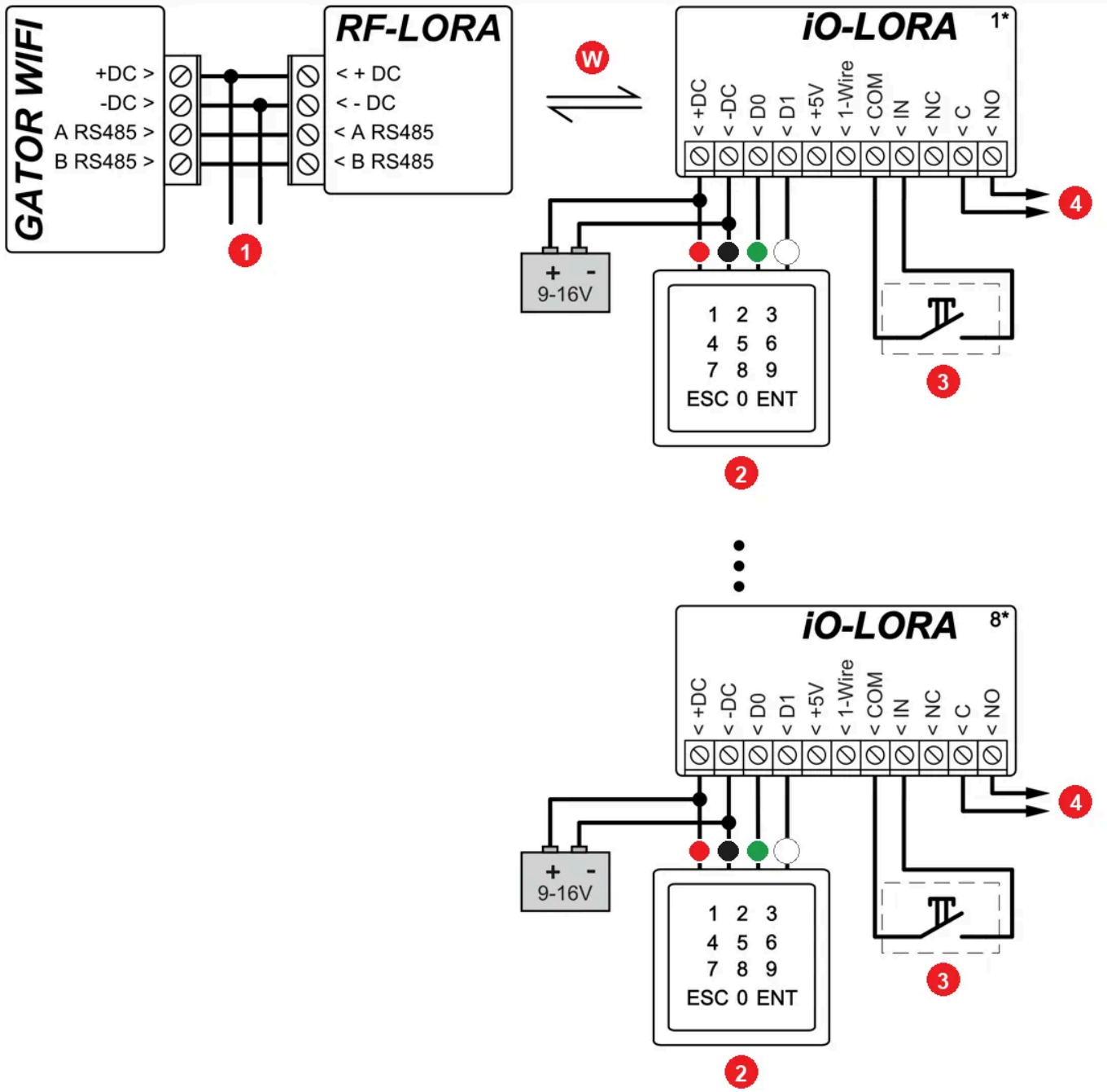


Figure 11. RF-LORA transceiver on the WP17 and iO-LORA expanders with RFID reader: a shared 9–16 V DC, 0.5 A supply for the WP17 and the RF-LORA (+DC – +DC, −DC – −DC); RS485: A RS485 – A RS485, B RS485 – B RS485; radio connection between the RF-LORA and the iO-LORA 1...8 expanders, up to 5000 m; each iO-LORA gets its own 9–16 V supply; the reader on the iO-LORA: red (+U) to the +DC, black (GND) to the −DC, green to the D0, white to the D1 terminal; exit push button between the iO-LORA's COM and IN terminals; the gate opener on the C and NO contacts of the iO-LORA's relay (2 A / 230 V AC).

- 1 DC power supply, 9–16 V, 0.5 A
- W Wireless connection, up to 5000 m
- 2 RFID reader with keypad (Wiegand 26/34)
- 3 "Exit" button
- 4 Gate control – the gate opener's control input; the rating of the iO-LORA's relay is 2 A / 230 V AC
- red wire, +U ("R - red (+U)")
- black wire, GND ("B - black (GND)")
- green wire, D0 ("G - green (D0)")
- white wire, D1 ("W - white (D1)")

The "up to … m" distances are theoretical maximums achievable under ideal conditions. In practice, the quality and routing of the cable, sources of interference and, for radio links, walls and terrain give a considerably shorter range. Plan with a margin, and on long runs check the connection during commissioning.

Setup in TrikdisConfig (the windows are described in chapter 5):

1. Start TrikdisConfig, connect the WP17 with a USB cable or log in remotely, and read the settings (**Read [F4]** – the program shows the device's current settings; if asked, enter the 6-digit administrator or installer code). On the **Modules** page select **iO-LORA controller** from the list, and enter the expander's six-digit serial number (on the expander's sticker) in the **Serial No.** field. The RF-LORA does not have to be added separately.



Figure 12. TrikdisConfig – Modules: in row 1 **iO-LORA controller** selected, the serial number goes into the **Serial No.** field.

2. For each added iO-LORA expander, one input (for example **6 IN**) and one output (**7 OUT**) appear in the list on the **IN/OUT** page. The input's function should be **Exit button** (the expander's IN and COM terminals connect the exit button here): when it is pressed, the expander's relay (in the example **7 OUT**) switches on for the set pulse time. The output type is **Pulse**, the pulse time matches the gate opener (3 s in the example); **Wiegand reader mode** must be ticked.

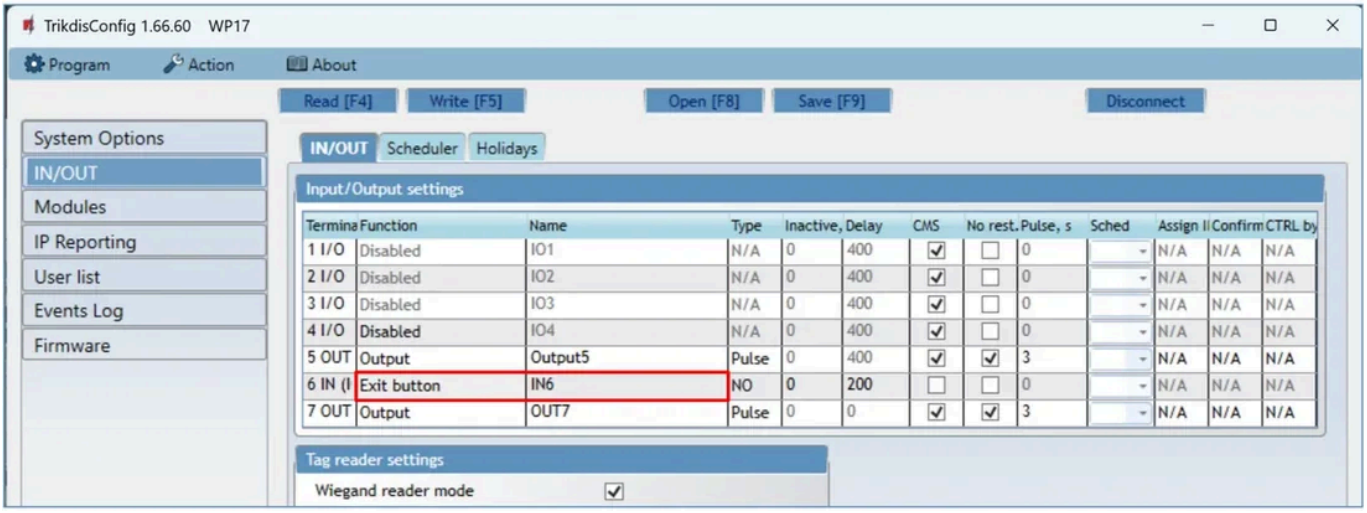


Figure 13. TrikdisConfig – IN/OUT: the function of **6 IN** is **Exit button** (NO), the **5 OUT** and **7 OUT** outputs are of **Pulse** type, with a 3 s pulse; **Wiegand reader mode** ticked.

3. On the **User list** page enter the user's name, the RFID card number (**RFID Code**), with a code reader the code, tick the **En** checkbox, and mark which output they may control. Write the settings (**Write [F5]**), wait for the update to finish, then **Disconnect** and unplug the USB cable.

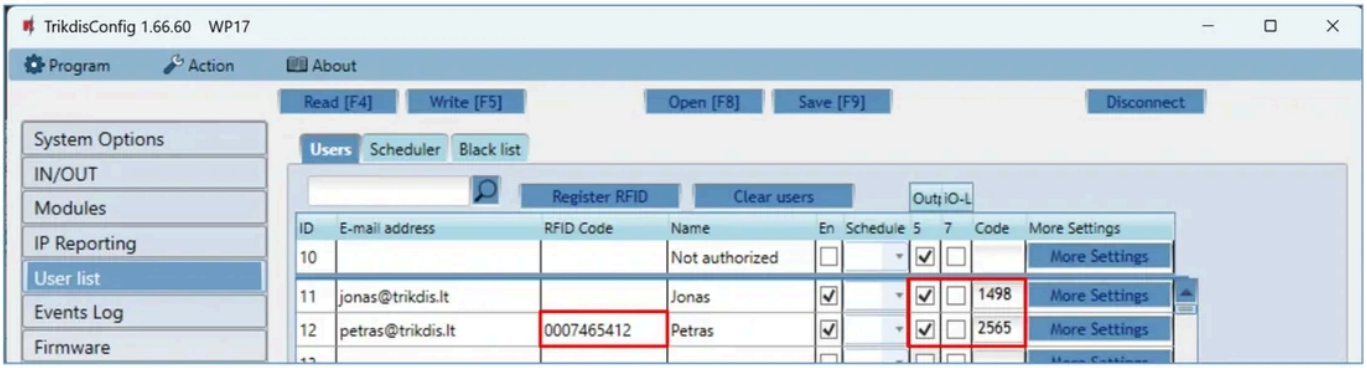


Figure 14. TrikdisConfig – User list: for the users the **RFID Code** filled in, output 5 marked, the code entered.

4. **Check:** switch on the output with the card or the code, then press the exit button – both times the relay must pull in for the set pulse time.

4. Control

You control the WP17 from the **Protegus 2** app – from a phone, a tablet or a browser –, on an Android phone also with a widget placed on the home screen; on site with an RFID card and a code (section 3.6). The device does not respond to phone calls or SMS: it has no SIM card.

4.1 Wi-Fi pairing from Protegus 2

In Protegus 2 the user opens the gate from anywhere, sees the state of the gate (if the gate status is wired, sections 3.2 and 5.9), receives the events as push messages, and as administrator also manages the users. The app is free; for phones you download it from the app stores, in a browser it opens at https://web.protegus.app. With the WP17, adding the system is also the **Wi-Fi pairing**: while adding, the app hands the device the name and password of the Wi-Fi network.

protegus 2
intelligent security & control

GET IT ON Google Play

Download on the App Store

Before you add the system

Formally, two conditions are given for adding: the power must be on (the **STATUS** LED flashes green), and the device must be on the network (the **NETWORK** LED is steady green and flashes yellow). In practice: the power must be in order (the **STATUS** LED flashes – red without a network, pairing can still be started), Wi-Fi must be switched on on your phone, and you should have the name and password of the **2.4 GHz** Wi-Fi network at hand. If the device has already been on the network (the **NETWORK** LED is steady green and flashes yellow), steps 3–9 are skipped: the system is added immediately after the ID is entered.

1. Log in to Protegus 2 (or register a new account), and in the menu choose **Add new system**.

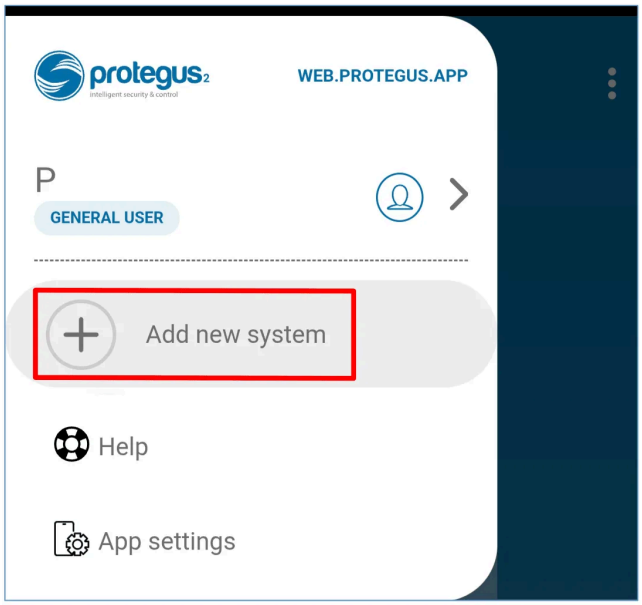


Figure 15. The Protegus 2 menu with the **Add new system** item.

2. Enter the device's unique ID, the **MAC** number (**Unique ID (MAC)**) – it is on the sticker on the bottom of the device and on the box –, or scan the sticker's QR code with the **Scan QR Code** button, then press **Next**. If the installer has changed the default `123456` value of the **Cloud Access Code**, the app asks for that too.



Figure 16. Entering the ID: the MAC number goes into the **Unique ID/IMEI** field, or the sticker's QR code can be scanned with the **Scan QR Code** button; then **Next**.

3. The app checks the device. Since the WP17 is not yet on the network, the **Device is offline** screen appears: here choose the **Start WiFi configuration WP17** line.

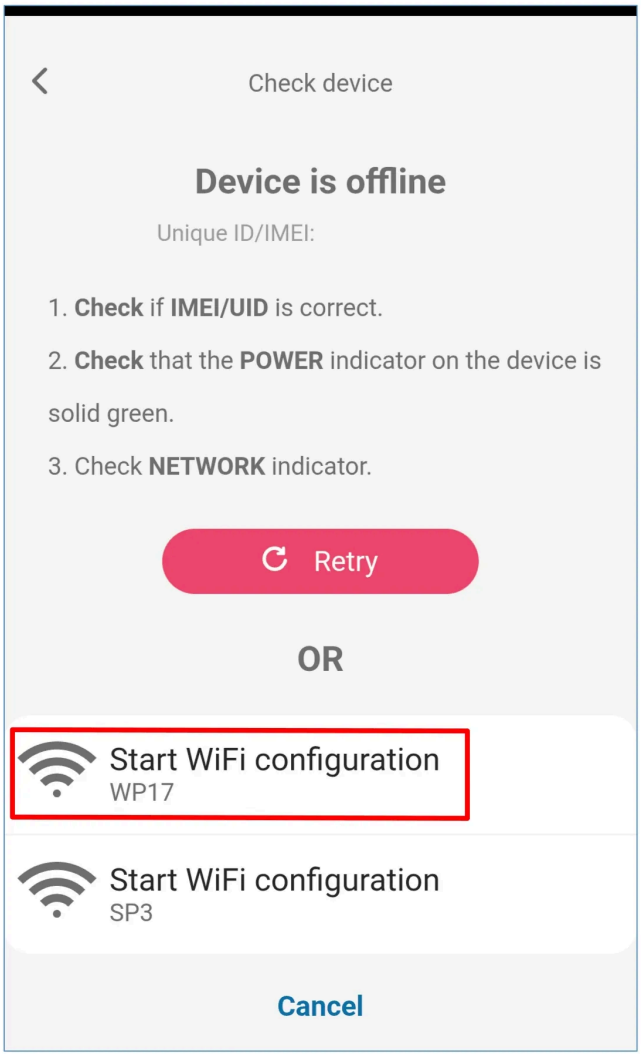


Figure 17. The **Check device** screen: the device is offline, at the bottom the **Start WiFi configuration WP17** option.

4. Remove the WP17's front cover with a flat screwdriver and press the **PAIR** button on the board for **3 seconds**, until the **NETWORK** LED starts flashing green-yellow quickly; then release it. The device is in pairing mode.



Figure 18. The **Scanning nearby WP17** screen: the app searches for the device and shows that the button must be held until the NETWORK LED flashes green-yellow.

5. Wait until the app finds the device (**Found WP17**), and press **OK**.

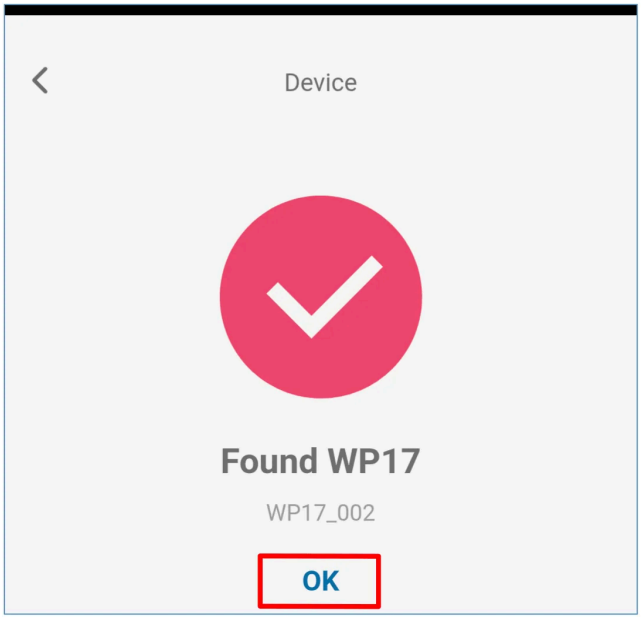


Figure 19. The **Found WP17** screen with the **OK** button.

6. Select from the list the Wi-Fi network the WP17 will connect to.

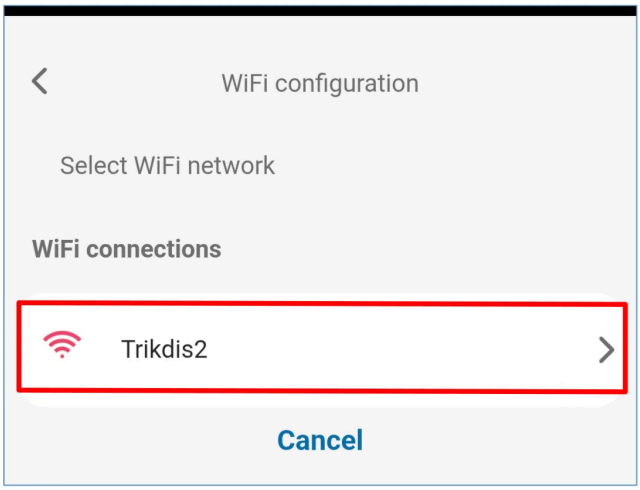


Figure 20. The **WiFi configuration** screen: the selected network from the list of nearby networks.

7. Enter the password of the Wi-Fi network and press **OK**.

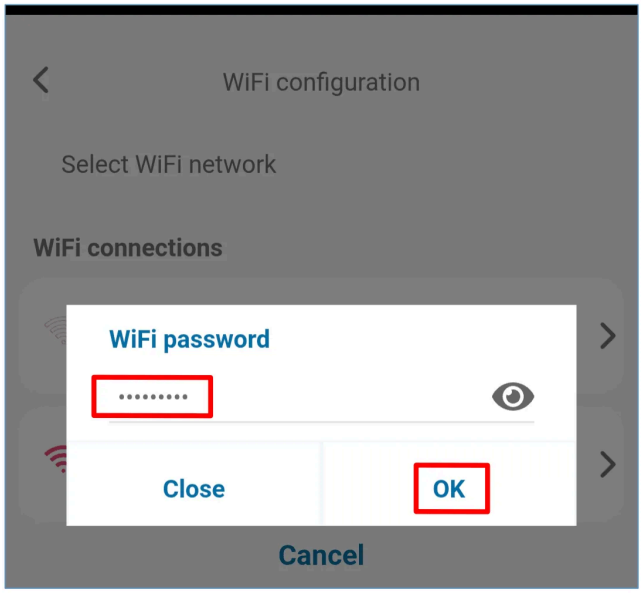


Figure 21. Entering the Wi-Fi password.

8. Press **Connect**: the app hands the network data to the device over a temporary Wi-Fi connection.

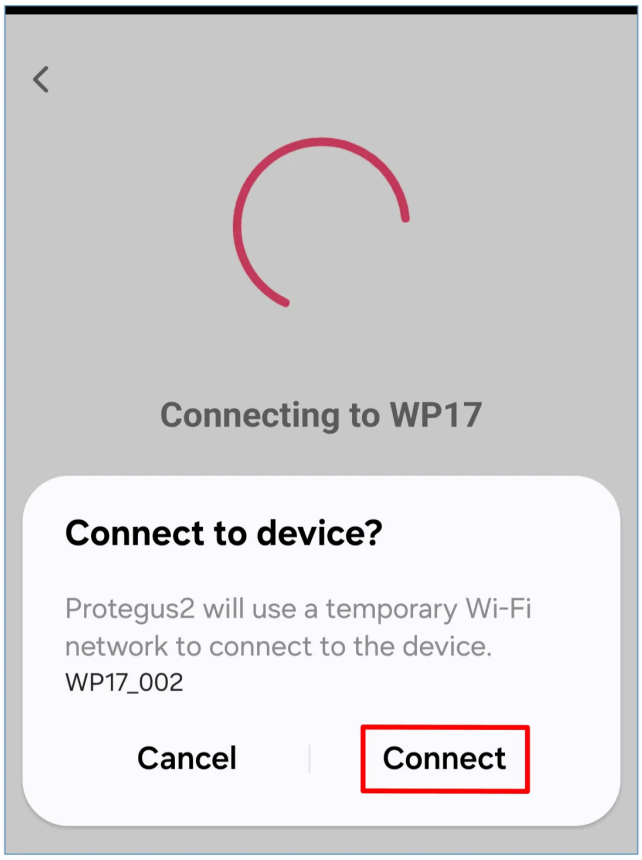


Figure 22. The **Connect to device?** question: Protegus 2 uses a temporary Wi-Fi network for the device; **Connect**.

9. Wait until the device connects to the network and the cloud (**Waiting for device to come online**).

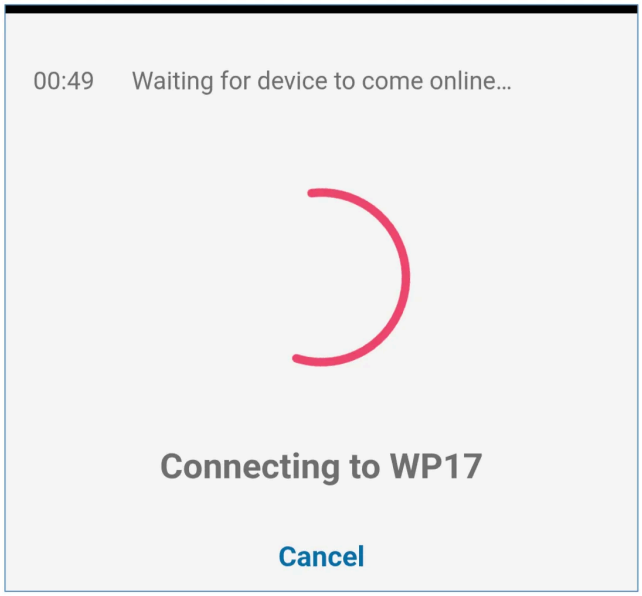


Figure 23. The connection screen with a countdown.

10. Enter the system name (and check the time zone), then **Next**.

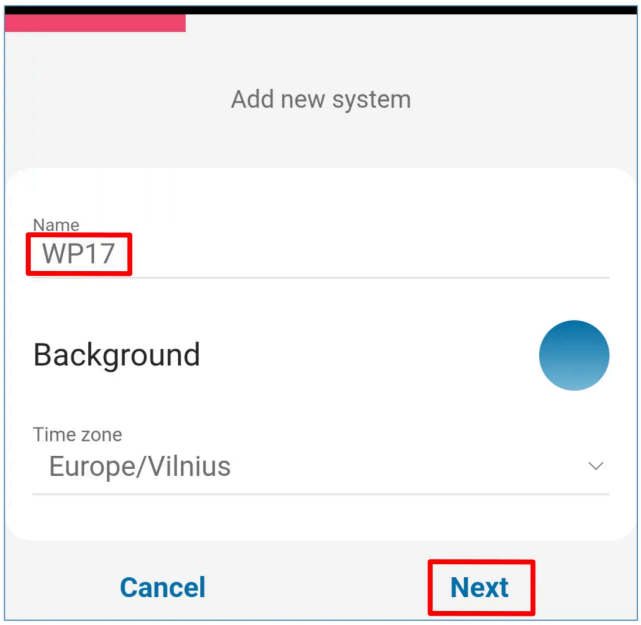


Figure 24. The **Add new system** screen: the system name and the time zone.

11. On the **System added successfully** screen you can skip the **Personalize** step with the **Skip** button: you can rename the outputs and inputs later too.

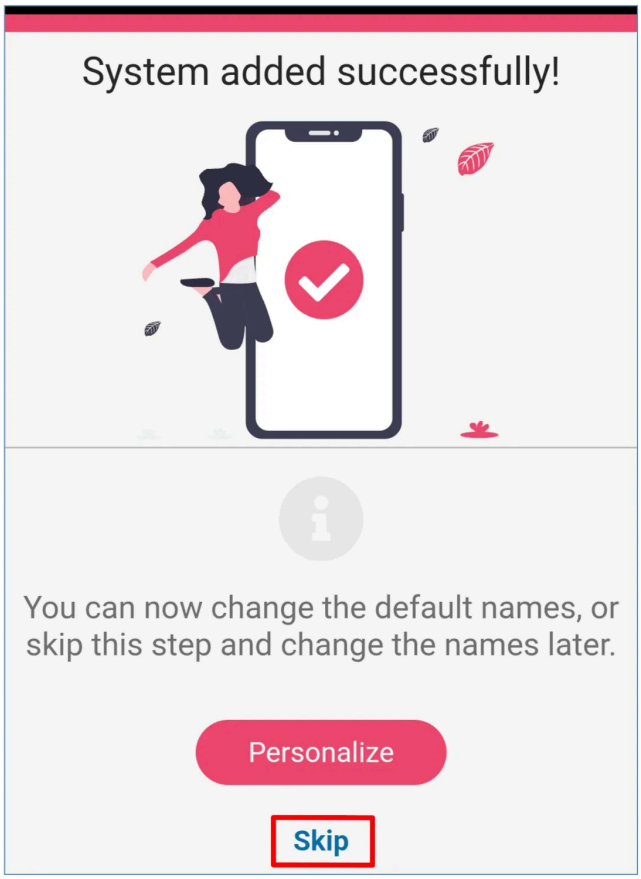


Figure 25. The system has been added; the **Skip** button.

12. Wait at most 1 minute until the text on the yellow background disappears. The WP17 leaves pairing mode by itself after a few minutes; if you do not want to wait, press the **PAIR** button again for 3 seconds, until the fast green-yellow flashing of the **NETWORK** LED stops. Put the front cover back.

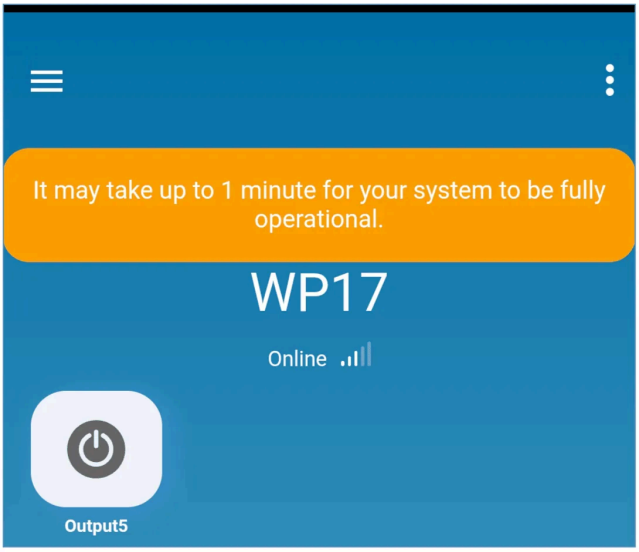


Figure 26. The WP17 in Protegus 2: the system is **Online**, the yellow bar indicates that you have to wait at most 1 minute for full operation.

13. You open the gate with the **Output5** button. **Tip:** press and hold the button, choose editing, then tap the icon to choose one that suits the use (gate, barrier, garage), and save it. If the gate status is wired, the icon also shows the open and closed state of the gate.



Figure 27. The system's home screen with the **Output5** button – this switches the WP17's relay.

See also

Protegus Android / iPhone and web app · Browser push notifications in the Protegus 2 app

4.2 Widget on the phone's home screen

You can also put the gate-opening button on the phone's home screen, so you open with one touch without opening the app. **It works only on Android**; the way of placing the widget may differ slightly from phone to phone. The WP17 must be added to Protegus 2 and you must be logged in to the app; then close the app window.

1. Touch and hold an empty part of the home screen, and in the bar that appears choose **Widgets**.
2. Find **Protegus 2** in the list, and choose the **Switch Protegus 2** widget.
3. Select the output to control (**WP17 Output5**), and press the **ADD WIDGET** button.

4. The button appears on the home screen. Go back to the home screen and press the icon. Try it: after pressing, a circular indicator shows that the output has switched on; with the gate status wired, the colour of the button shows the open and closed state of the gate.



Figure 28. Step 1 – the **Widgets** item after touching and holding the home screen.

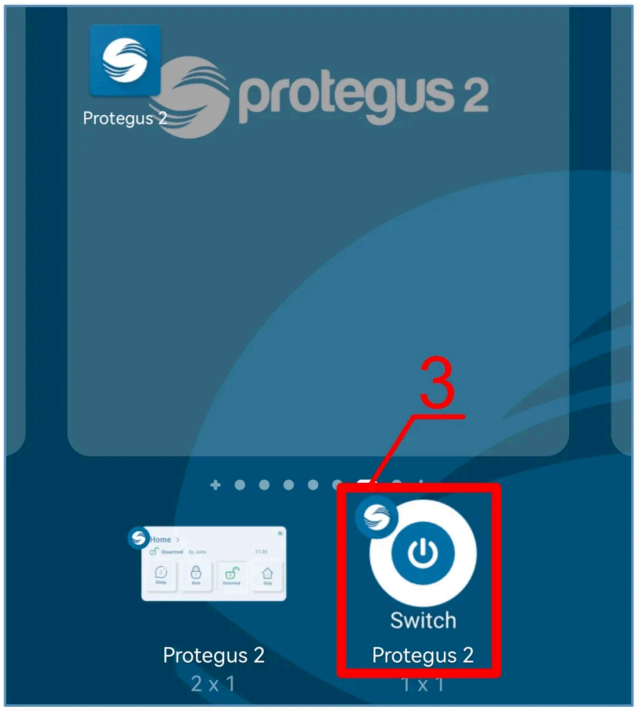


Figure 29. Step 2 – **Switch Protegus 2** among the Protegus 2 widgets.



Figure 30. Step 3 – selecting the **WP17 Output5** output and the **ADD WIDGET** button.



Figure 31. Step 4 – the **Output5** widget on the home screen; the green button shows the switched-on output (open gate).

4.3 Managing users in the app

As administrator you can also add and delete users in Protegus 2; an added user sees and opens the gate from their own account, and receives the events as push messages.

1. On the system's screen open the **Settings** menu, then the **System configuration** item.
2. Choose the **Users** list, and press the **+** (new user) button.
3. Enter the user's **e-mail address** and **name**, if there is a reader, the RFID card number, and with a code reader their code (section 5.6), and mark which output they may control (**Output5**).
4. Press the **Add user** button: the new user appears in the list. With the **Back** button you return to the main window.

The schedule, the validity period and the counter are set per user on the TrikdisConfig **User list** page (section 5.6); banned addresses and cards go on the black list (section 5.6.4).

5. Setup with the TrikdisConfig software

All settings of the WP17 are available with the Windows program called **TrikdisConfig** – over a USB cable or remotely (chapter 6). Wi-Fi pairing and opening the gate work from the app without the program (chapters 2 and 4); you need the program when you set up RFID cards, scheduling, the function of the inputs and outputs, expansion modules or the monitoring station, or when you change the default codes.

Az összes Trikdis eszköz egy közös szoftverrel programozható. A program neve TrikdisConfig és a gyártó honlapjáról letölthető.

TrikdisConfig Letöltés a trikdis.com oldalról.

Letöltést követően telepítsd a programot. Ha bármikor a TrikdisConfig indításakor a program azt jelzi, hogy új verzió jelent meg, töltsd le az ajánlott frissítést és telepítsd!

1. Remove the WP17's front cover with a flat screwdriver as shown in the figure.
2. Connect the WP17 to the computer with a **USB Mini-B** cable.
3. Start TrikdisConfig. The program recognises the device and opens the WP17 programming window.
4. Click the **Read [F4]** button: the program reads the device's current settings. If asked, enter the 6-digit **administrator** code in the pop-up window (`123456` by default).

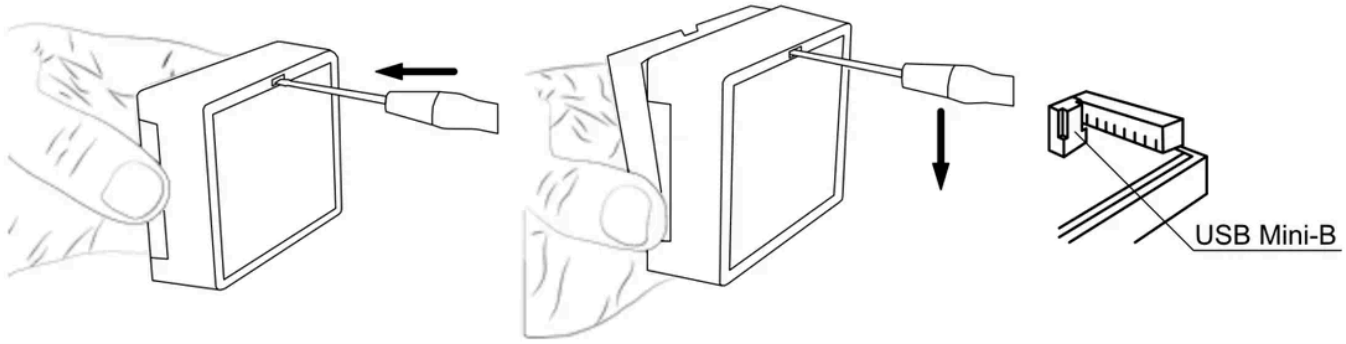


Figure 32. Removing the front cover: insert the screwdriver at the upper edge and move it downwards, and the cover snaps off; next to it the USB Mini-B connector.

Warning

While the device is connected to a computer via USB cable, it is in programming mode: its normal operation stops, it does not monitor, does not report, cannot be controlled, is powered from USB, and restarts once the cable is unplugged. Therefore the device must not be freely accessible: keep it in a closed metal enclosure with tamper protection or with a motion detector covering the enclosure. More in the FAQ

The **Restore** button at the bottom left of the programming window takes you back to the default settings (section 5.8).

5.1 The status bar

After connecting the device and reading it (**Read [F4]**), the most important device data are shown at the bottom of the window:

Label	Meaning
IMEI / Unique ID, on an Ethernet device **MAC / Unique ID**	The device's unique identifier: the IMEI on a device with a SIM card, the MAC address on an Ethernet device. The same is printed on the box and on the back of the device.
Status	The current operating status.
Device	The device type (model designation). Check that the type of your own device is shown here.
SN	Serial number.
BL	The bootloader version.

Label	Meaning
FW	The firmware version.
HW	The hardware version.
State	The connection mode: USB or remote.
Administrator / Installer	The access level of the person programming (after the password has been entered).

After making the settings, you write them to the device with the **Write [F5]** button; with the **Open [F8]** and **Save [F9]** buttons you can save the complete set of settings to a file and load it into another device. **Save [F9]** saves the settings to a settings file, and **Open [F8]** opens the saved file; you can later load the saved settings into other devices as well, so you can quickly set up several devices with identical settings.

The WP17's unique ID is the **MAC** number: it appears in the left field of the status bar as **MAC/Unique ID**, and Protegus 2 asks for the same when the system is added (section 4.1), as does remote programming (chapter 6).



Figure 33. The WP17 status bar: in the left field the **MAC/Unique ID**, at the bottom **Status: reading done**, **Device: WP17_3001** (the type code), the serial number, the **BL** and **FW** version, the connection mode (USB). The **Device** field must be of the form **WP17_xxxx**.

5.2 "System Options" page

The device's general settings: ID, time, administrator code, test and the data of the Wi-Fi network.

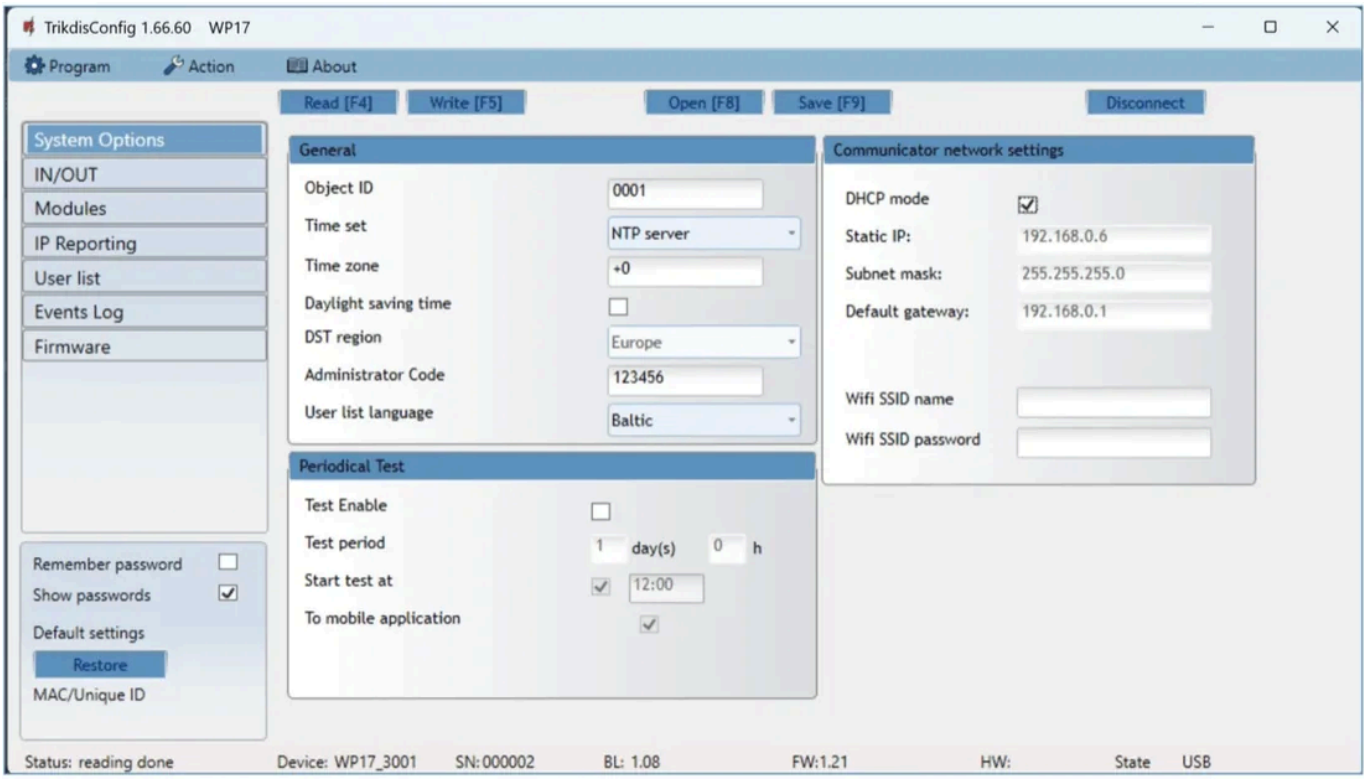


Figure 34. TrikdisConfig – **System Options**: the **General**, the **Periodical Test** and the **Communicator network settings** group.

General group

- **Object ID** – the object ID received from the monitoring station (a 4-digit hexadecimal number, 0–9, A–F). Do not use the values FFFE and FFFF.
- **Time set** – the source of time synchronisation (for example **NTP server**).
- **Time zone** – the time zone offset, if the time is taken from an NTP server (for example Central European Time: +1).
- **Daylight saving time** – tick it if the country has daylight saving time: the device changes the clock by itself in spring and autumn; **DST region** – the region whose rules it follows when changing (Europe).
- **Administrator Code** – the administrator code: with it every parameter of the WP17 can be changed (`123456` by default – change it).
- **User list language** – the character set of the user list (names can be entered with the letters of this language).

Periodical Test group

- **Test Enable** – when ticked, the device sends a periodic test report.
- **Test period** – the time between test reports (days and hours).
- **Start test at** – the time of the first test.
- **To mobile application** – when ticked, the test report also goes to the Protegus 2 app.

Communicator network settings group – the data of the Wi-Fi connection; pairing from the app (section 4.1) fills in the same fields, but you can also enter them manually over a USB cable.

- **DHCP mode** – when ticked, the device gets the network settings (IP address, subnet mask, gateway) automatically from the router; when empty, you enter them manually.
- **Static IP**, **Subnet mask**, **Default gateway** – the static IP address, the subnet mask and the gateway address for manual setup.
- **Wifi SSID name** – the name of the Wi-Fi network the WP17 connects to (2.4 GHz network).
- **Wifi SSID password** – the password of the Wi-Fi network.

5.3 "IN/OUT" page

Settings of the inputs and outputs, the RFID reader and the scheduling of the outputs, on three tabs: **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 IN/OUT tab – the inputs and outputs

The table has one terminal per row; here you decide which one is an input and which an output, and how it should report.

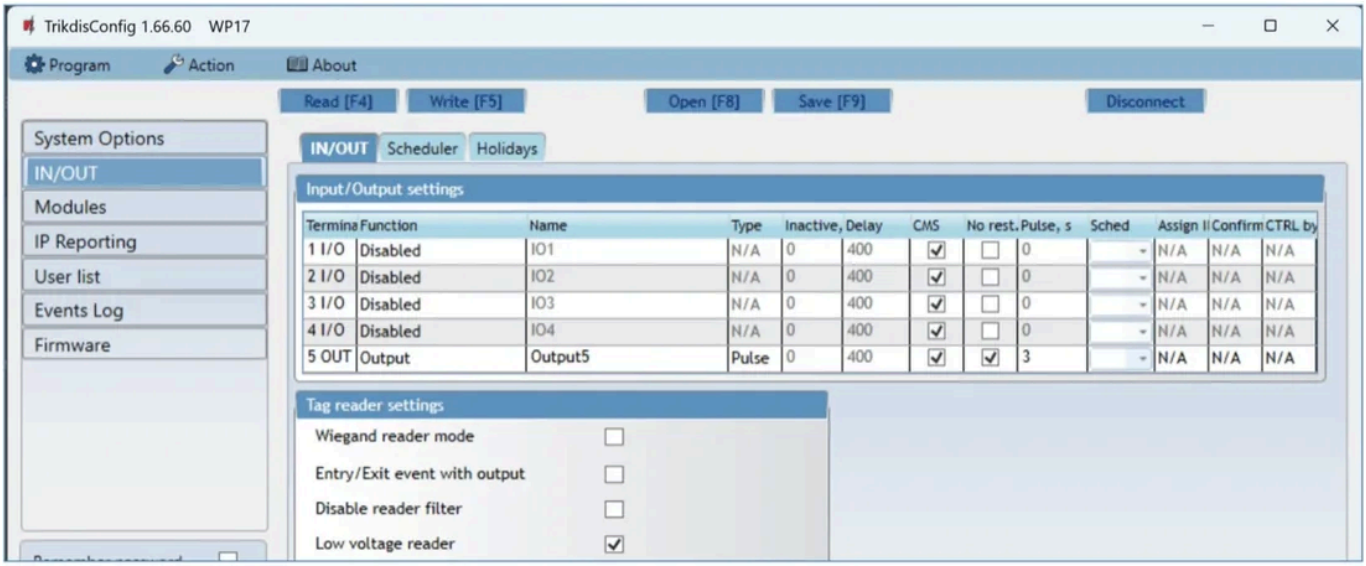


Figure 35. TrikdisConfig – **IN/OUT**: the **Input/Output settings** table (in the default picture 1–4 I/O are disabled, **5 OUT** is a **Pulse** type output with a 3 s pulse), below it the **Tag reader settings** group.

Input/Output settings group

- **Terminal** – the number of the WP17 terminal (1 I/O … 4 I/O, 5 OUT; the expanders' terminals at the end of the list).
- **Function** – the terminal's function: **Input**, **Output** or **Disabled**.
- **Name** – the name of the input or output (this is how it appears in the app).
- **Type** – for an input the circuit type (**NC**, **NO**, **EOL = 10 kΩ**), for an output the operation: **Pulse** or **Level** (two-state).
- **Inactive** – after the first activation the input does not report again for this time; 0 = off.
- **Delay** – the input's response time in milliseconds (400 ms by default).
- **CMS** – when ticked, the event also goes to the monitoring station and to Protegus 2.
- **No rest.** – do not send a restore event.
- **Pulse** – the length of the pulse in seconds, if the output is of **Pulse** type (3 s by default on 5 OUT; for a gate opener 1–3 s is usually enough).
- **Sched** – the number of the schedule controlling the output (from the **Scheduler** tab).
- **Assign IN** – the input assigned to the output: instead of the output's state, the app shows the actual state of the input (the gate) (section 5.9).
- **Confirm** – the number of the input whose active state is a condition for switching the output.
- **CTRL by IN** – activation of the selected input switches the output (local automation, also works without a network).

Tag reader settings group – settings of the RFID reader (wiring in section 3.6)

- **Wiegand reader mode** – tick it if a Wiegand 26/34 RFID reader is connected to the WP17.
- **Entry/Exit event with output** – when ticked, an entry / exit event is also generated when the output is switched from the app.
- **Disable reader filter** – switches off the internal filter for short pulses, if the device does not recognise the reader's signals.
- **Low voltage reader** – for a low-voltage reader (5 V signal level).

5.3.2 Scheduler tab – scheduling the outputs

The outputs can also switch by themselves on a schedule (for example the gate open during working hours, closed in the evening). Three things are needed for this: enter the time and the days of the week, enable the schedule (**Enable**), and assign it to the output. You assign the schedule in the output's **Sched** column.

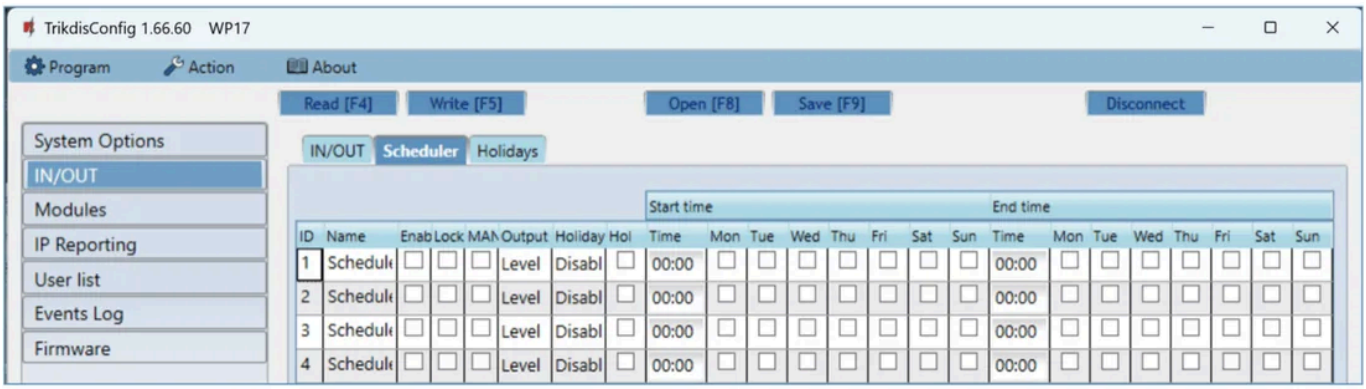


Figure 36. TrikdisConfig – IN/OUT, **Scheduler** tab: for each schedule enabling, locking, manual start, output mode, holiday mode, start and end time with the days of the week.

- **Name** – the name of the schedule.
- **Enable** – enabling the schedule.
- **Lock** – when ticked, the output cannot be switched in any other way (from the app, with a card) while the schedule is active.
- **MANUAL** – when ticked, the output does not switch by itself when the schedule starts; the schedule starts when the user switches the output on.
- **Output mode** – the operation of the output during the schedule: **Level** – the output stays on throughout the given period; **Pulse** – the output switches for the set pulse time at the beginning and at the end of the schedule.
- **Holiday mode** – how the schedule should work on holidays; **Hol** – tick it if on holidays the holiday times are used.
- **Start time** – the days of the week and the time from which the output switches on.
- **End time** – the days of the week and the time until which the output stays on.

If the output mode is **Level** and only **End time** is given, the output switches off at the given time if it was on until then. The schedule must be assigned to the output, otherwise it does not run.

5.3.3 Holidays tab – holidays

Here you enter the calendar days (holidays) on which the schedule works with the holiday times – that is, the days for which additional holiday switching of the output given in the **Scheduler** table can be set.

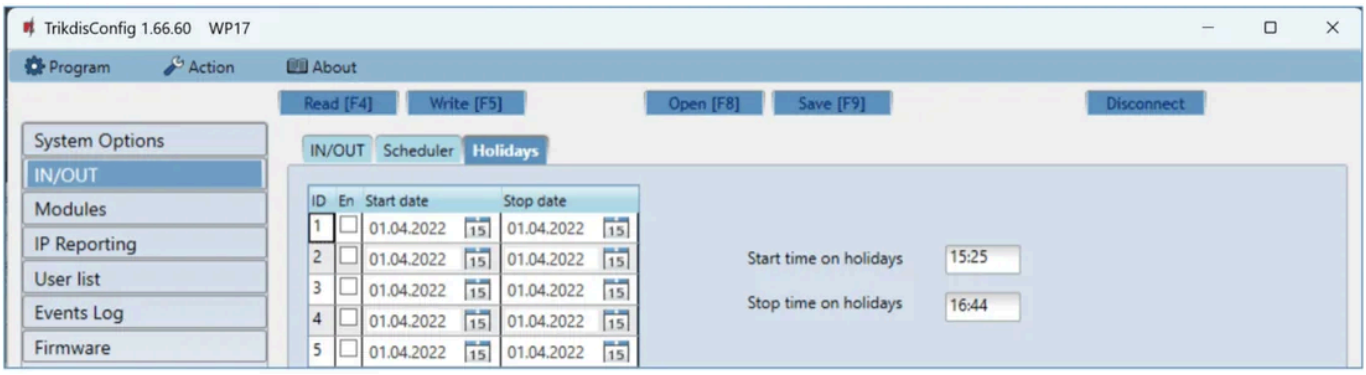


Figure 37. TrikdisConfig – IN/OUT, **Holidays** tab: holiday periods with start and end date, and the holiday start and end time.

- **En.** – enabling the holiday period.
- **Start date**, **Stop date** – the first and last day of the period.
- **Start time on holidays**, **Stop time on holidays** – the start and end time on holidays.

5.4 "Modules" page

Up to **8 iO-LORA** wireless expanders can be connected to the WP17 via the **RF-LORA** transceiver (from firmware 1.21); the RFID readers connected to the iO-LORA expanders can control 8 additional gates – one expander with one reader controls one gate. The RF-LORA transceiver does not have to be added to the list. The wiring and the complete setup procedure are in section 3.7.

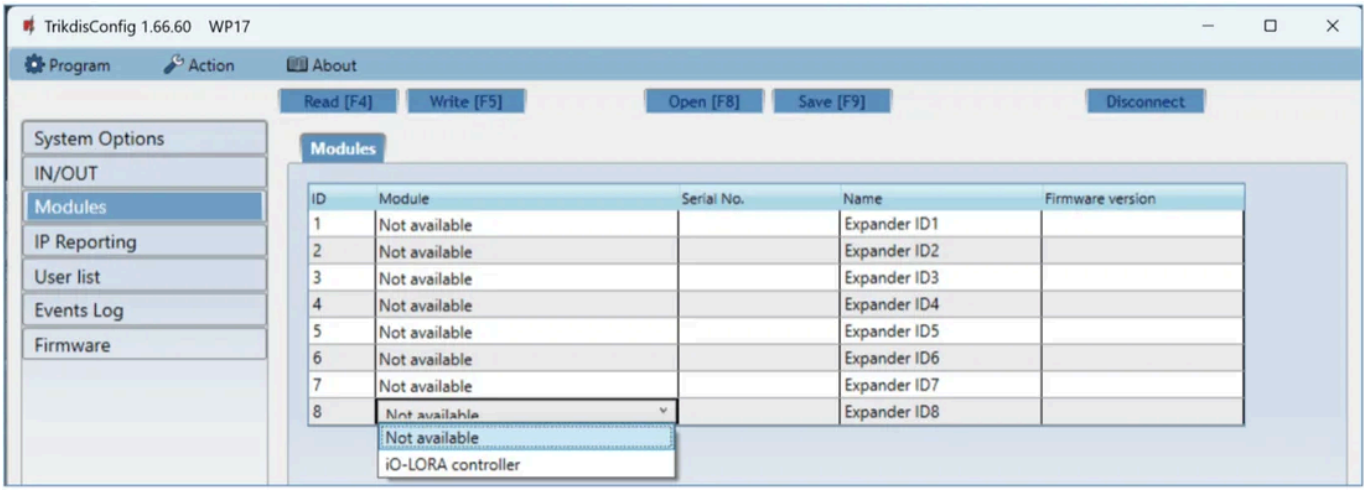


Figure 38. TrikdisConfig – **Modules**: eight expander slots (**Not available** by default); **iO-LORA controller** in the **Module** drop-down list; next to it the **Serial No.** field.

- **Module** – select the connected module from the list (**iO-LORA controller**).
- **Serial No.** – the module's 6-digit serial number (on the sticker on the module's housing and box).

The added expander's input and output appear in the list on the **IN/OUT** page (for example **6 IN** and **7 OUT** for expander 1), and can be handled just like the WP17's own.

iO4R relay expander

The **iO4R** relay expander can also be connected to the WP17 on the RS485 bus: it is used to supervise and remotely bypass the safety sensors of the gate automation, and to count gate cycles. It is set up in the Protegus 2 app, in the **Advanced Gator Monitoring** mode that can be chosen when the gate controller is added – see the iO4R manual.

5.5 "IP Reporting" page

The WP17 sends the events to the monitoring station's IP receiver and to the Protegus cloud; the cloud and the cloud access code are also on this page.

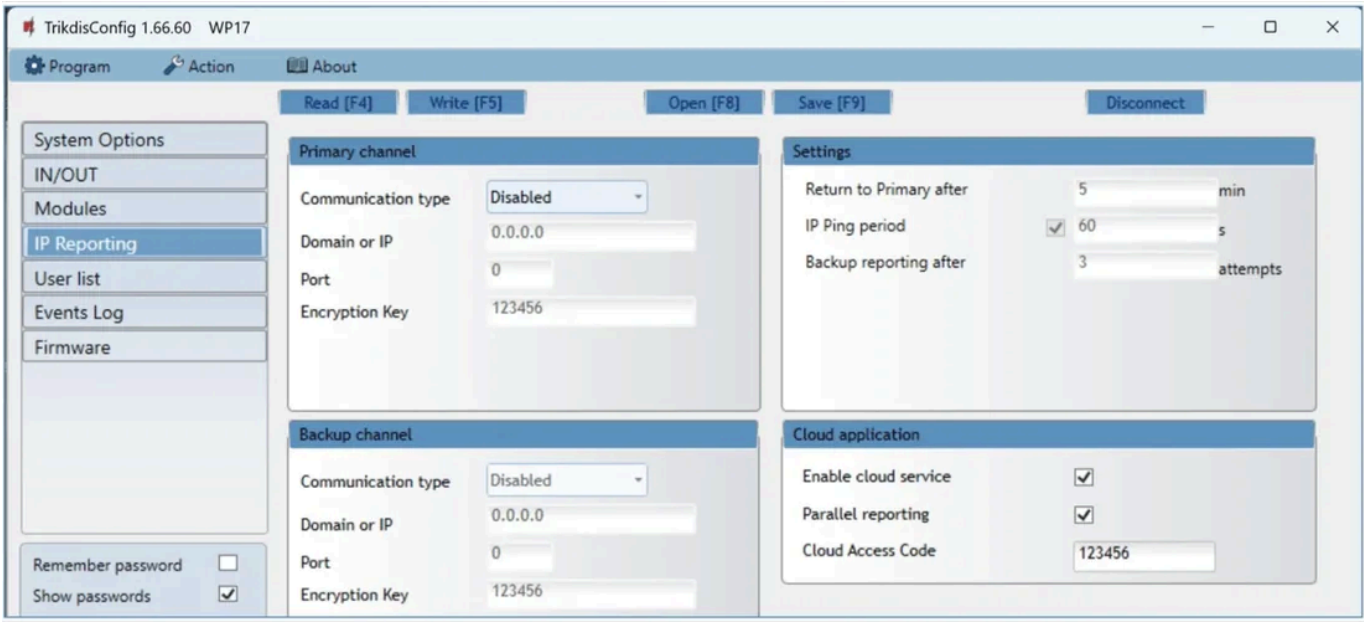


Figure 39. TrikdisConfig – **IP Reporting**: **Primary channel** and **Backup channel** (disabled by default), **Settings**, and the **Cloud application** group with the **Enable cloud service** and **Parallel reporting** checkboxes and the **Cloud Access Code**.

Primary channel group – you can send the WP17's messages to the monitoring station; for this the communication channels with the monitoring station's receiver must be set.

- **Communication type** – the type of connection with the monitoring station's receiver: **TCP/IP** or **UDP/IP**; **Disabled** = no reporting.
- **Domain or IP** – the receiver's domain name or IP address.
- **Port** – the receiver's network port.
- **Encryption Key** – the 6-digit encryption key, which must match the one set in the receiver.

Backup channel group – the backup receiver, with the same settings as the primary one.

Settings group

- **Return to primary after** – after this time the device tries to return from the backup to the primary channel.
- **IP Ping period** – enabling and interval of the PING signals that keep the connection alive.
- **Backup reporting after** – after this many failed attempts the device switches to the backup channel.

Cloud application group

- **Enable cloud service** – switching on the Protegus cloud (on by default): the WP17 communicates with the app and can also be programmed remotely with TrikdisConfig (chapter 6). If you switch it off, it cannot be controlled from the app.
- **Parallel reporting** – when ticked, events go to the monitoring station and to Protegus 2 at the same time; when empty, the app only receives them after the monitoring station's acknowledgement.
- **Cloud Access Code** – 6-digit code for connecting to Protegus 2 (`123456` by default); the app asks for it when the system is added, if it is not the default one.

5.6 "User list" page

The list of users, registration of RFID cards, user schedules and the black list – on three tabs.

5.6.1 Users tab – the users

The table has one user per row with their permissions; the WP17 handles up to 1000 users (numbers 11–1010).

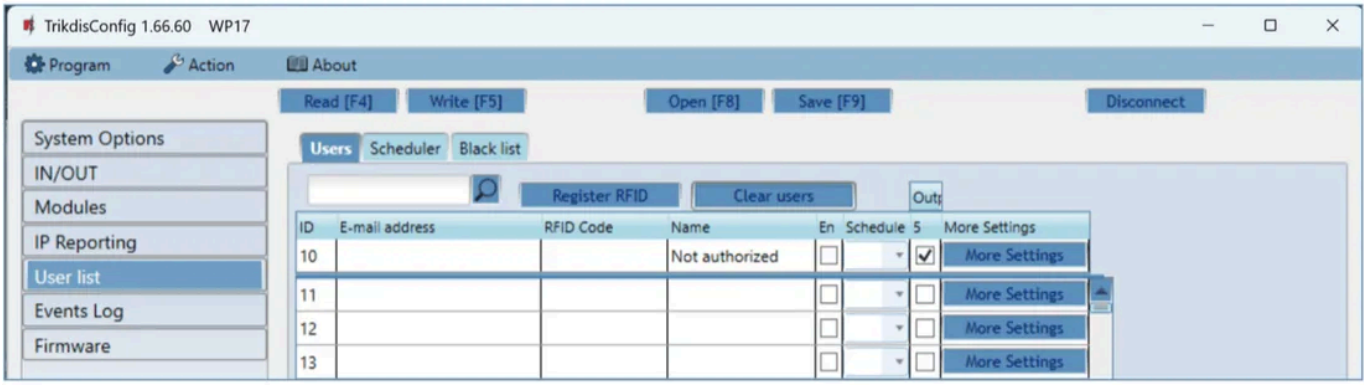


Figure 40. TrikdisConfig – **User list**, **Users** tab: at the top the search box, the **Register RFID** and the **Clear users** button; in the table the **ID**, **E-mail address**, **RFID Code**, **Name**, **En**, **Schedule**, the column of output **5** and the **More Settings** button; row 10 is the default **Not authorized** entry.

- **E-mail address** – the user's e-mail address (they log in to Protegus 2 with it).
- **RFID Code** – the ID number of the RFID card (key fob), if there is a reader and the user has a card.
- **Name** – the user's name.
- **En** – enabling the user: when ticked, they can switch the outputs.
- **Schedule** – the number of the schedule according to which the user can control (section 5.6.3).
- **Outputs** (in the example the **5** column) – the output(s) the user can control.
- **Code** – with a Wiegand 26/34 reader with code keypad, the user's four-digit code (**Keypad code** in the **More settings** window).
- **More Settings** – the window of further settings (below).

Row 10, **Not authorized**, is a default entry (on the cellular GV17 it means the permission of unknown caller numbers); for the WP17 the documentation says nothing about it – leave it as it is.

Further settings (More settings) – user (11–1010)

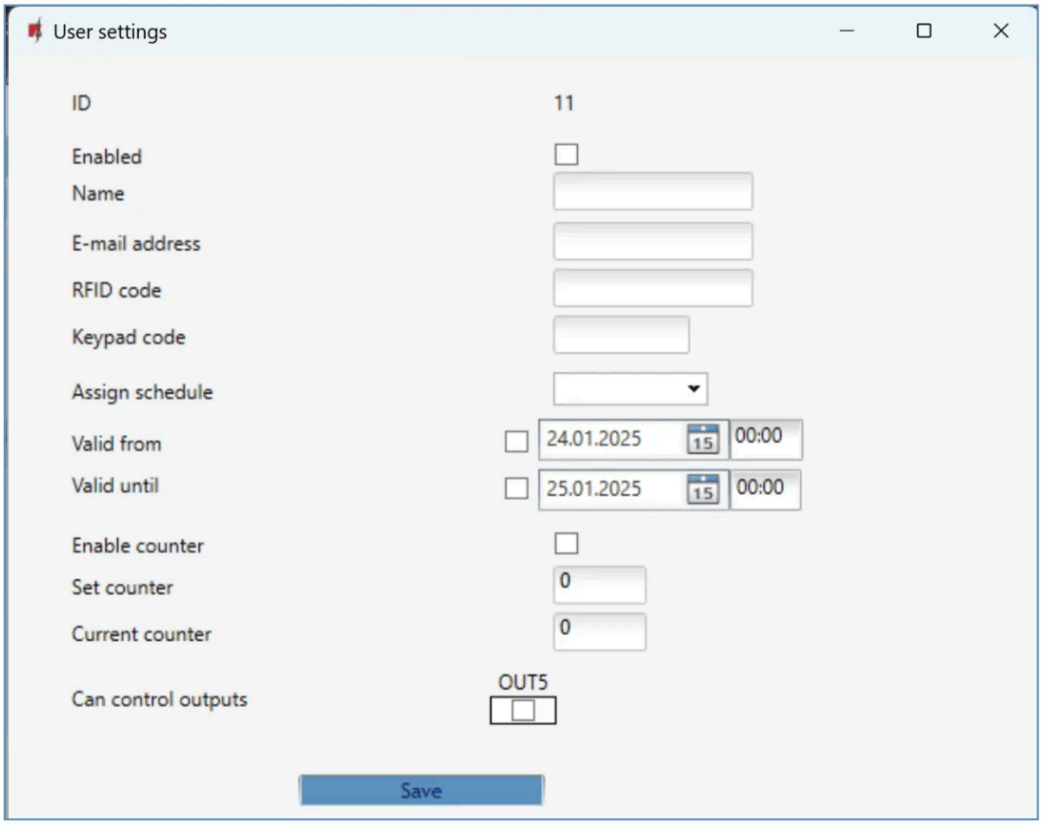


Figure 41. TrikdisConfig – **User settings** for one user: **Enabled**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs** (OUT5) and **Can control iO-LORA outputs**.

- **Enabled** – when ticked, the user can switch the outputs.
- **Name**, **E-mail address**, **RFID code**, **Keypad code** – the data corresponding to the columns of the list.
- **Assign scheduler** – the schedule(s) during which the user can control.
- **Valid from**, **Valid until** – the start and end of the permission (date and time) – for example for a tenant or a guest.
- **Enable counter** – switching on the counter; **Set counter** – how many times the user may control within the given time; **Current counter** – the number of switchings so far.
- **Can control outputs** – which of the WP17's own outputs can be controlled; **Can control iO-LORA outputs** – which of the iO-LORA expanders' outputs can be controlled (section 3.7).

5.6.2 Registering an RFID card (key fob)

1. Wire the RFID reader (section 3.6), switch on the WP17's power, start TrikdisConfig, and connect with a USB cable or remotely. On the **IN/OUT** page tick the **Wiegand reader mode** checkbox.
2. On the **User list** page click the **Register RFID** button.

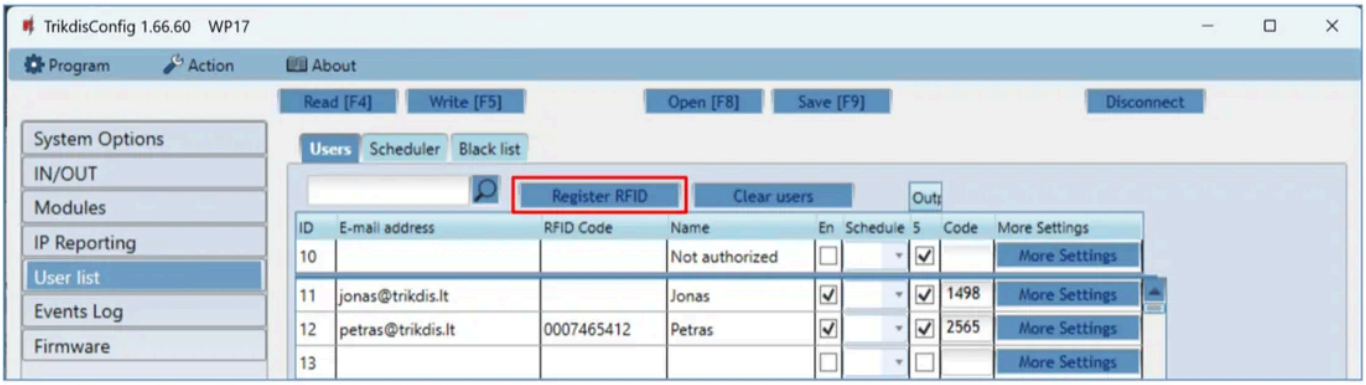


Figure 42. TrikdisConfig – User list: the **Register RFID** button above the user table.

3. The registration window opens (**Add RFID tag/card to reader**).

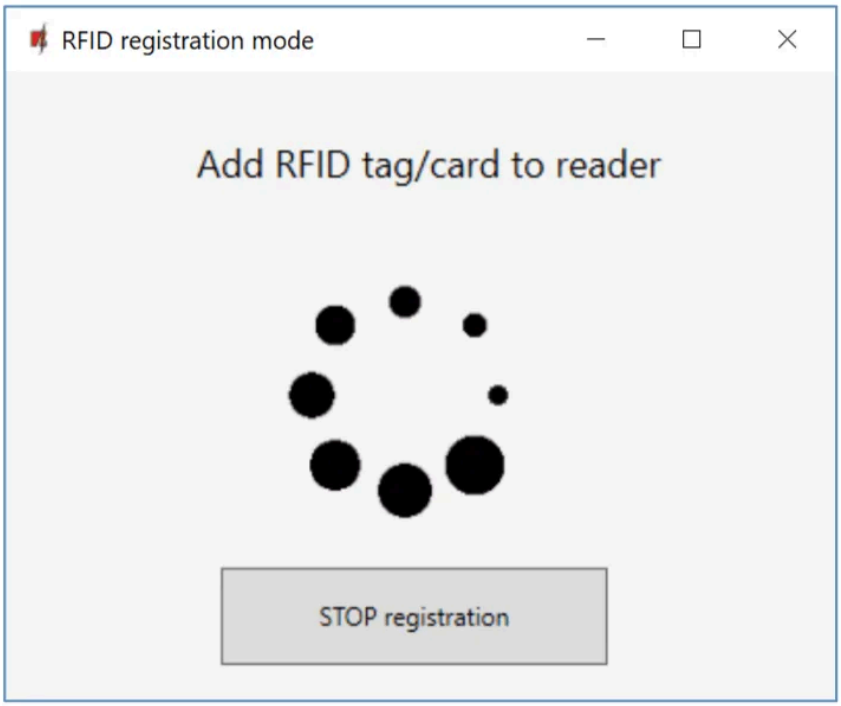


Figure 43. The RFID registration window: hold the card to the reader; the **STOP registration** button ends registration.

4. Hold the card to the reader. When the reader has read it, a new window opens: enter the user's name (**Enter user name**), tick the **User can control PGM Output 5** checkbox, and click **ADD**. Repeat with the other cards.

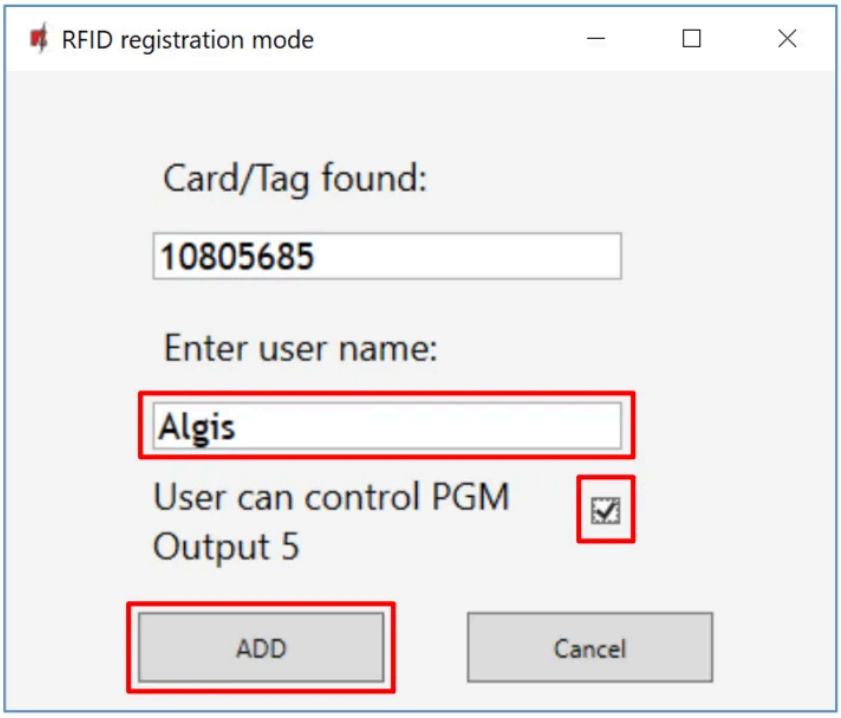


Figure 44. The window of the card that was read: the name, the **User can control PGM Output 5** checkbox and the **ADD** button.

5. When you have added all cards, press **STOP registration**, then write the card list to the device with the **Write [F5]** button.

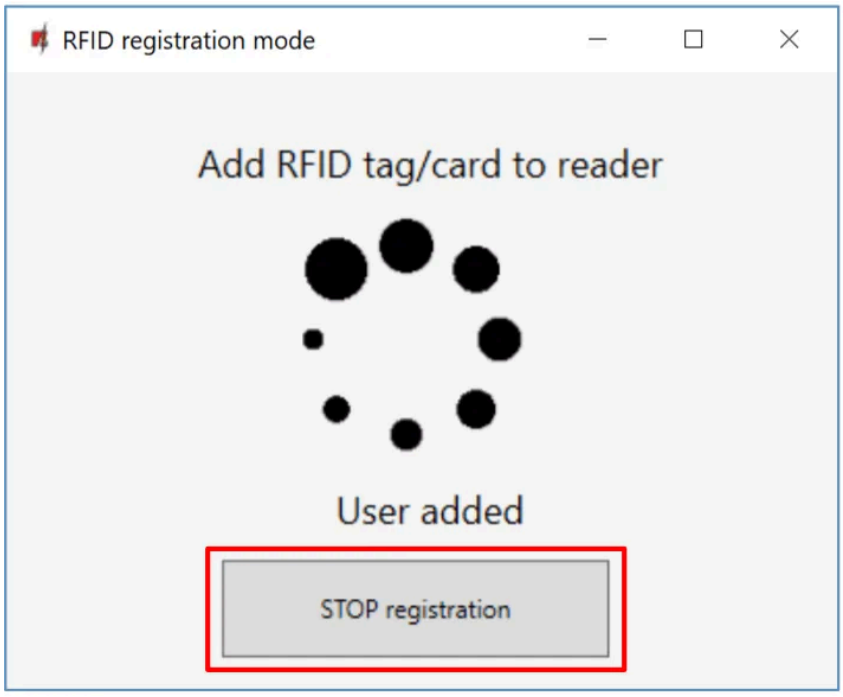


Figure 45. The **User added** confirmation and the **STOP registration** button.

Adding a card by its number: you can also type the ID number printed on the card directly into the **RFID Code** field; enter the name, tick the **En** checkbox and the output that can be controlled, then **Write [F5]**.

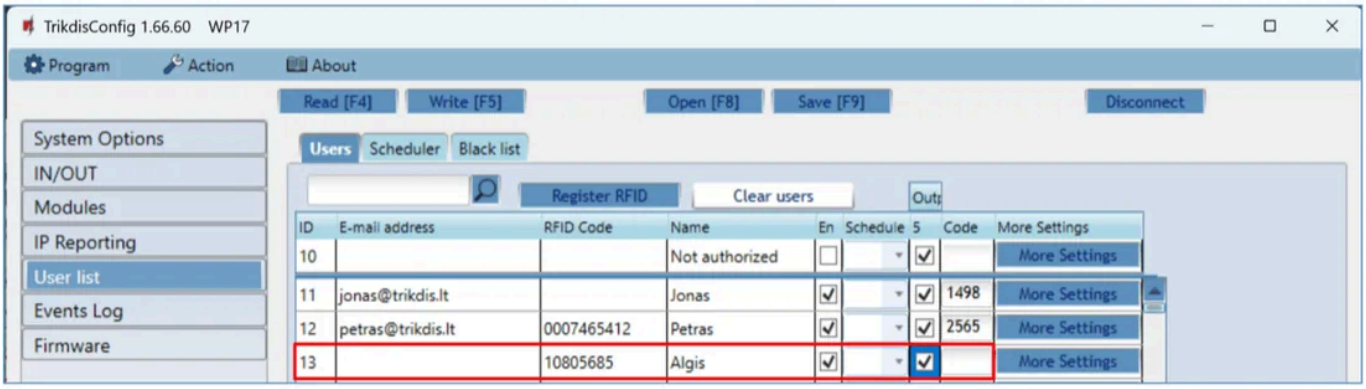


Figure 46. TrikdisConfig – User list: the user's row with the card number in the **RFID Code** field, the name, **En** ticked, output 5 marked; at the top the **Write [F5]** button.

Adding a card from Protegus 2: in the user list choose adding a new user, enter the e-mail address, the name, the card's ID number, with a code reader the code, mark the output, and save it (section 4.3).

5.6.3 Scheduler tab – scheduling the users

The user can only control during the assigned schedule (for example the cleaner on weekdays between 6 and 8 o'clock). You assign the schedule in the user's **Schedule** column or in the **More settings** → **Assign scheduler** field.

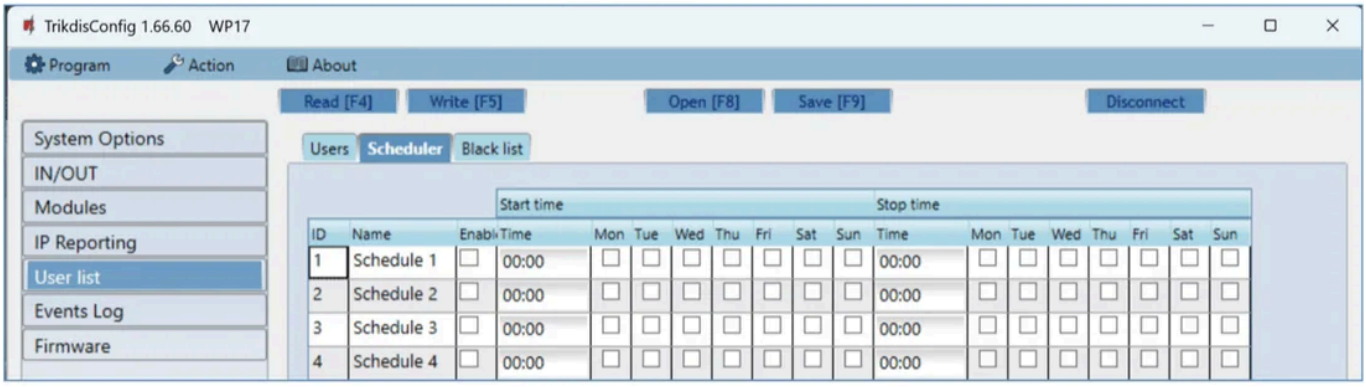


Figure 47. TrikdisConfig – User list, **Scheduler** tab: four schedules, each with **Enable**, start and end time with the days of the week.

- **Name** – the name of the schedule.
- **Enable** – enabling the schedule.
- **Start time** – the days of the week and the time from which the user can control.
- **Stop time** – the days of the week and the time until which they can control.

5.6.4 Black list tab – black list

Whoever you add here cannot control the device in any way.

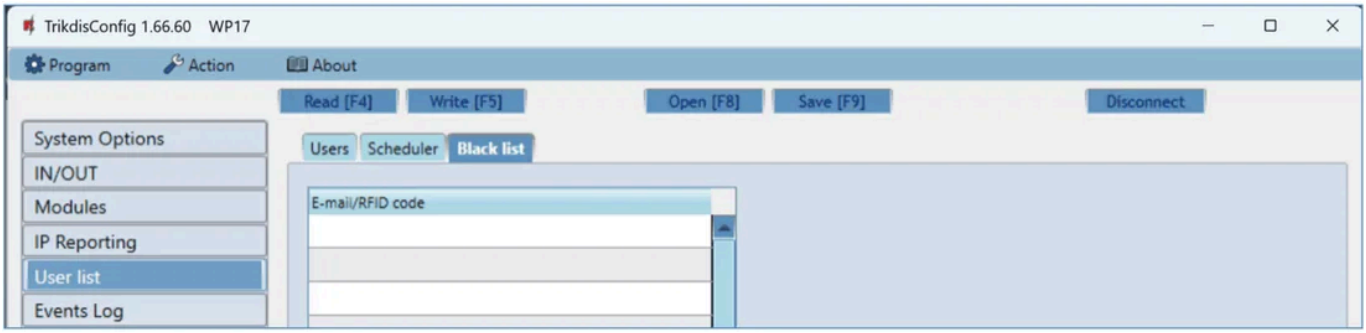


Figure 48. TrikdisConfig – User list, **Black list** tab: the table of banned e-mail addresses and card numbers.

The black list contains the e-mail addresses and RFID card numbers that are forbidden to control the WP17. You can also add an entry directly from the event log: right-click the name or the card number and choose **Add to Black List**.

5.7 "Events Log" page

The device's own event log – for troubleshooting and for looking back at who entered and when.

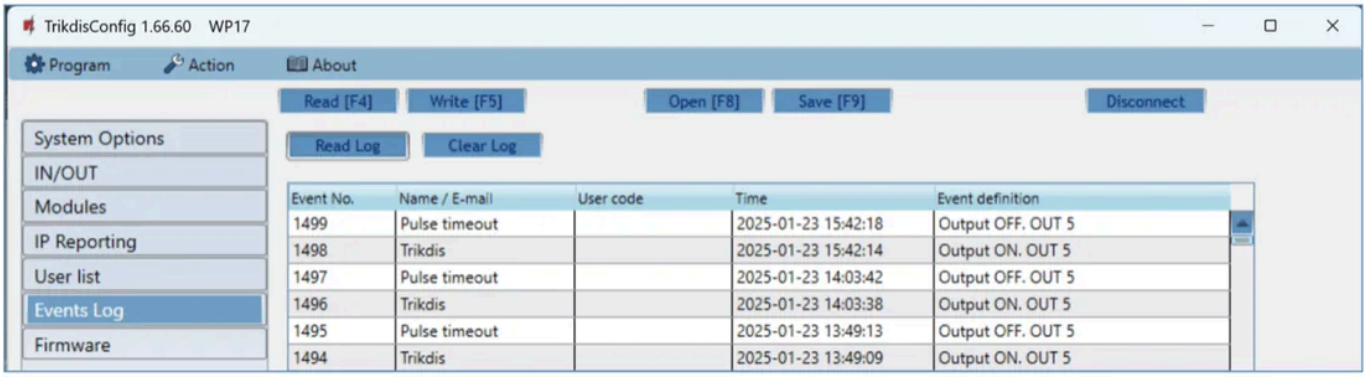


Figure 49. TrikdisConfig – **Events Log**: the **Read Log** and **Clear Log** buttons; for the events the number, the user's name or e-mail address, the code, the time and the description of the event (for example **Output ON** / **Output OFF**, OUT 5).

Click **Read Log**: the program reads the events from the device's memory (up to 5000). The log shows every operation and internal event of the WP17: who opened the gate, when and with what (app, card, code), and which inputs changed. The **Clear Log** button deletes the log.

5.8 Restoring the default settings

To restore the default settings, connect the WP17 with a USB cable and click the **Restore** button in the **Default settings** group at the bottom left of the programming window. Restoring deletes all settings – including the user list and the codes –, so it is worth saving the settings to a file first (**Save [F9]**). Expect to enter the data of the Wi-Fi network again as well (section 4.1 or 5.2).

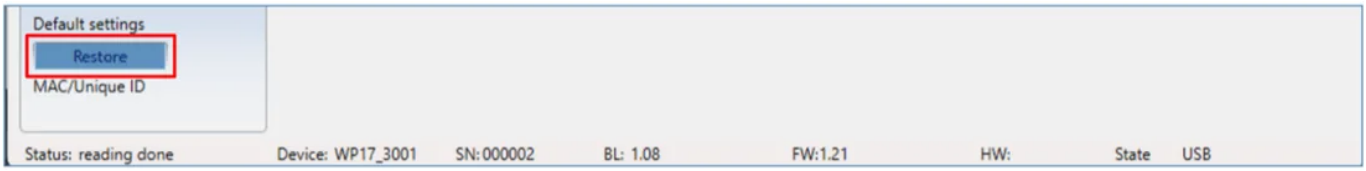


Figure 50. TrikdisConfig – the **Restore** button of the **Default settings** group above the **MAC/Unique ID** field.

5.9 Indicating the gate's state

The Protegus 2 app and the widget can show the actual state of the gate (open or closed). For this, one of the WP17's inputs – **1 I/O** in the drawings – must be wired to the gate opener's status output or to the gate's limit switch (section 3.2), and then in the program the input must be assigned to the output that switches the gate:

1. On the **IN/OUT** page **1 I/O** should have the **Input** function, with the type matching the contact (NO, NC or EOL), and give it a name (for example "Gate").
2. In the **5 OUT** row, in the **Assign IN** column, select the 1 I/O input, and write the settings (**Write [F5]**).

After that, in the app and on the widget the output's icon shows not the state of the relay but the actual state of the input – that is, of the gate.

6. Remote programming

You can also read and change the WP17's settings remotely through the Protegus cloud – there is no need to go to the site.

Conditions for remote programming

In TrikdisConfig, on the **IP Reporting** page, **Enable cloud service** must be ticked (it is on by default, section 5.5), the power must be in order (the **STATUS** LED flashes green), and the device must be on the Wi-Fi network (the **NETWORK** LED is steady green and flashes yellow). If these are not met, the device cannot be reached remotely.

1. Download and install the latest version of TrikdisConfig from the Trikdis website (https://www.trikdis.com), if it is not yet on your computer.
2. Make sure the WP17 is connected to the internet and the Protegus cloud is switched on.
3. Start TrikdisConfig. In the **Remote access** part of the start screen, enter the WP17's **MAC** number in the **Unique ID** field (it is on the sticker on the bottom of the device and on the box; with a USB connection you also see it in the **MAC/Unique ID** field of the status bar).
4. In the **System Name** field enter any name (for example the name of the object), and click **Configure**.

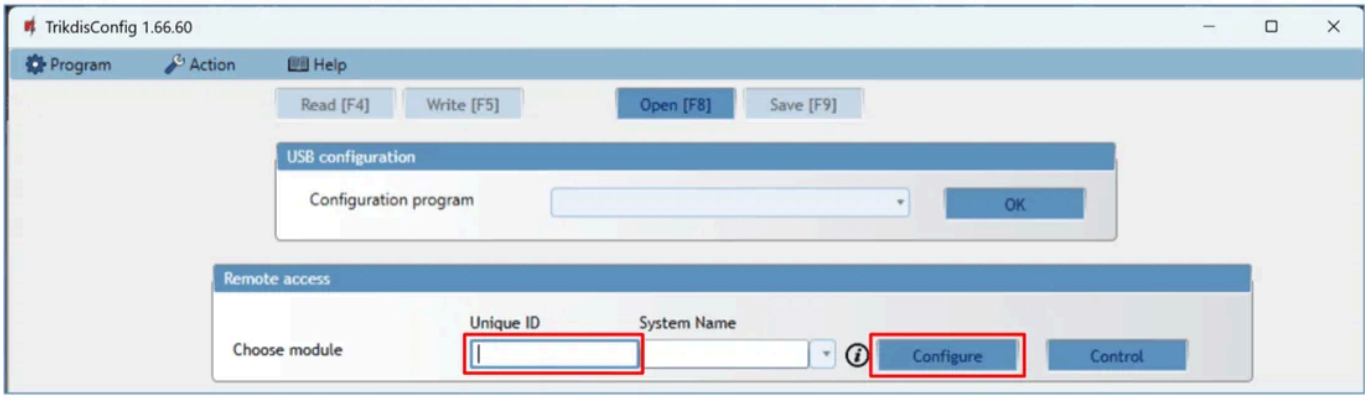


Figure 51. TrikdisConfig – the **Remote access** part: the **Unique ID** field, the **System Name** field and the **Configure** button.

5. The WP17 programming window opens. Click **Read [F4]**: the program reads the device's current settings. If the program asks for the access code, enter the 6-digit **administrator** code. If you tick **Remember password** and click **Write [F5]**, the program remembers the code.
6. Make the settings and write them with the **Write [F5]** button. At the end, disconnect with the **Disconnect** button and close the program.

Remote programming needs no help on site: the customer only checks the power and the network on the LEDs. To change the user list you do not even need TrikdisConfig – the administrator also manages it from Protegus 2 (section 4.3). The data of the Wi-Fi network, however, can only be changed on site (by pairing or over a USB cable): if the device is not on the network, you cannot reach it remotely.

7. Checking operation

At the end of installation and setup, test the whole system – on site, before you hand it over:

1. **Power**: the **STATUS** LED flashes green. If it gives 7 red flashes, the supply voltage is low – measure it on the power terminals (9–32 V DC).
2. **Network**: the **NETWORK** LED is steady green and flashes yellow according to the signal strength; **STATUS** flashes green. If STATUS flashes red, the number of flashes shows the fault (section 1.4): 1 – no Wi-Fi connection, 2 – weak signal, 4 – cannot reach the Protegus 2 server.
3. **Inputs**: activate the wired inputs one by one (gate status contact, exit push button), and check that the recipients receive the correct messages in Protegus 2 and at the monitoring station.
4. **Outputs**: switch the outputs on remotely – from the app, with the widget, and with the card or code too if there is a reader –, and check that the gate opens, the recipients receive the messages, and the gate status in the app also follows reality (section 5.9).

The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for an Ethernet device, that the connection up to the router is alive – but not that the device can also reach the internet. If the NETWORK LED is green but the DATA LED stays lit continuously even after an event or test report, the internet connection is not working: the message cannot be sent. On a mobile network the most common culprit is the APN or the data service of the SIM card; on Ethernet, the router, the firewall or the DNS. When the DATA LED goes out, the message has been sent and the data connection is fine.

If the Wi-Fi or the internet drops out, the device stores up to 60 unsent events and sends them when the connection returns; the yellow light of the **DATA** LED indicates that there are events waiting to be sent. The event log (**Events Log**, section 5.7) also shows afterwards what happened during the tests: who opened the gate, when and with what.

8. Firmware update

When the WP17 is connected to TrikdisConfig and newer firmware is available, the program offers the update by itself – for this the computer must be online. If antivirus software runs on the computer, it may block the automatic update; in that case allow TrikdisConfig in the antivirus software.

You can update the firmware yourself – to a newer version and, if necessary, to an older one as well. All device settings remain unchanged after the update.

1. Start the TrikdisConfig software and connect the device with a USB cable, or open its programming remotely.
2. If newer firmware is available, the software offers to download it – accept it.
3. Select the **Firmware** page and click the **Open firmware** button. Select the firmware file.

4. Press the **Update [F12]** button, wait for the update to finish, then click **OK** in the pop-up window. Do not unplug the cable or interrupt the connection in the meantime.

The firmware files are in the TrikdisConfig installation folder, inside the **Firmwares** subfolder, in the folder named after the device. If there is no such folder, either there is no update for it or the TrikdisConfig software itself needs to be updated. The latest files can also be downloaded as a registered user from the device's page on the manufacturer's website.

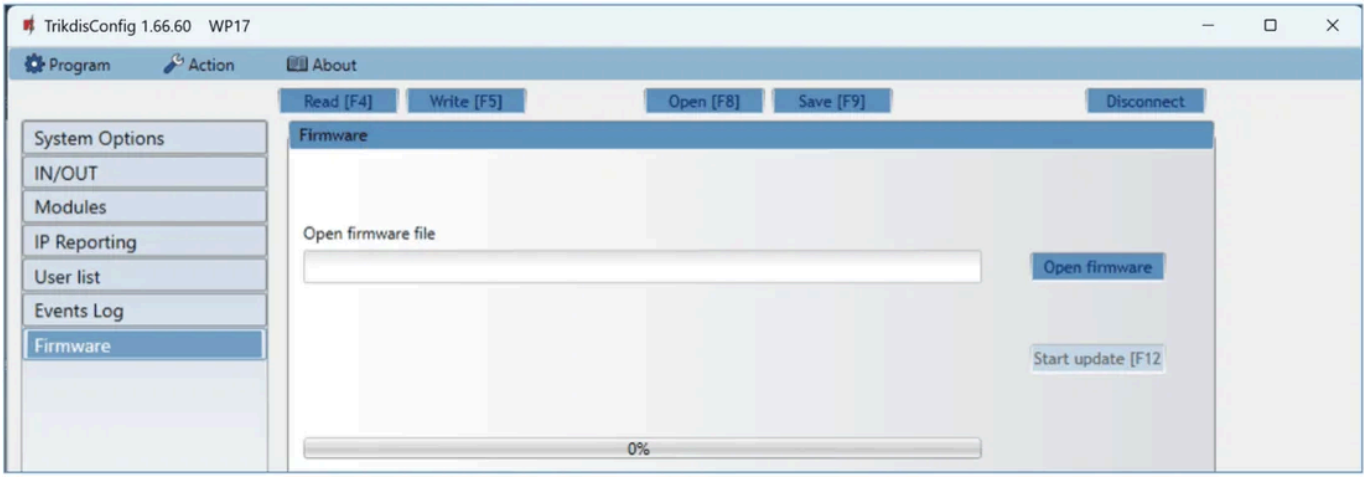


Figure 52. TrikdisConfig – WP17, **Firmware** page: the **Open firmware** button, the field of the selected file, the **Start update [F12]** button and the progress bar.

On the WP17 the button that starts the update is labelled **Start update [F12]**. After the update all previous settings are kept; with a manual update an older version can also be loaded back. To use the RF-LORA and iO-LORA modules, firmware **1.21** or later is required; you see the current version in the **FW** field of the status bar (section 5.1).

9. Troubleshooting and frequently asked questions

If the device does not do what you expect, first look at the LEDs (section 1.4), then at the points below.

The STATUS LED flashes red – what does the number of flashes mean?

The number of flashes is the cause of the fault: **1** – cannot connect to the Wi-Fi network (the network name or password is wrong, the network is not 2.4 GHz, or the router is switched off – pair again, or check the fields of **System Options** → **Communicator network settings**); **2** – the Wi-Fi signal is weak (move the device closer to the router, or place an access point closer); **3** – cannot connect to the primary IP receiver (the receiver's address, port and key on the **IP Reporting** page); **4** – cannot connect to the Protegus 2 server (the router has no internet connection, or **Enable cloud service** is switched off); **5** – cannot connect to any receiver channel; **6** – the internal clock is not set (**System Options** → **Time set**); **7** – the supply voltage is low (measure it on the power terminals: 9–32 V DC).

Wi-Fi pairing fails – the app does not find the WP17

- Hold the **PAIR** button for 3 seconds, until the **NETWORK** LED flashes green-yellow quickly; only then start the search in the app. If the flashing has stopped (the device leaves pairing mode by itself after a few minutes), press the button again.
- Wi-Fi must be switched on on the phone, and stay close to the device during pairing: the app talks to it over a temporary Wi-Fi connection.

- The device's power must be in order (the **STATUS** LED flashes), and the **MAC** number in the app must be exact (from the sticker or from the QR code).

Pairing succeeded, but the system does not become Online

- Look at the **STATUS** LED: **1** red flash – the network password is wrong, or the network is not 2.4 GHz; **2** – weak signal; **4** – the router has no internet connection, or **IP Reporting** → **Enable cloud service** is switched off.
- If MAC address filtering is on in the router, add the WP17's MAC number to the allowed devices.
- If the **Cloud Access Code** is not the default `123456`, enter the correct one in the app.
- If everything is in order, wait at most 1 minute after adding (section 4.1).

The name or password of the Wi-Fi network has changed – what should I do?

In this case the device does not reach the network (**STATUS** gives 1 red flash), and it cannot be reached remotely either. On site, enter the new data in TrikdisConfig over a USB cable (**System Options** → **Communicator network settings** → **Wifi SSID name / password**, section 5.2), or repeat the pairing from Protegus 2 with the **PAIR** button (section 4.1).

Does it work with a 5 GHz Wi-Fi network?

No: the WP17 connects only to **2.4 GHz** (802.11 b/g/n) networks, with WPA / WPA2 or mixed encryption. If your router broadcasts both bands under one name, the 2.4 GHz band must be switched on; if the device does not connect after pairing, it is worth setting up a separately named 2.4 GHz network on the router.

Is a SIM card or a mobile subscription needed?

No. The WP17 reaches the Protegus cloud and the monitoring station over the site's Wi-Fi network and the router's internet connection; there is no monthly fee. If there is no Wi-Fi at the gate, or control by call and SMS is also needed, the cellular GV17 GATOR is the right choice.

What happens if the internet or the Wi-Fi drops out?

Until then the device cannot be controlled from the app, but the local functions – the RFID card and code, the exit push button, scheduling and the **CTRL by IN** automation – keep working, because the user list and the settings are in the device. The device stores up to 60 unsent events (the **DATA** LED is yellow), and sends them when the connection returns.

The widget does not work, or I cannot find it

The widget is only available on an **Android** phone (section 4.2); on an iPhone you open from the app's home screen. On Android the WP17 must be added to the systems and you must be logged in; if the widget stays grey, open the app once and check the phone's internet connection.

The RFID reader does not read the card, or the WP17 does not respond to it

- Check the wiring according to the drawing in section 3.6 (green **D0** → **1 I/O**, white **D1** → **2 I/O**, black to −DC, red to the +DC terminal) and the reader's power; with a reader with 5 V signal level tick the **Low voltage reader** checkbox.
- On the **IN/OUT** page **Wiegand reader mode** must be ticked, and 1 I/O and 2 I/O must not be set to another function.
- If the device does not recognise the reader's signals, try the **Disable reader filter** checkbox.

- The card must be in the **User list** table (registered or entered by its number), enabled (**En**), with output 5, a valid schedule and a valid validity period (section 5.6); it must not be on the black list. The event log (section 5.7) shows whether the reading took place.

The app does not show the actual state of the gate

For gate status indication, the gate opener's status output or the gate's limit switch must be wired to an input (**1 I/O** in the drawings) (section 3.2), on the **IN/OUT** page the input type must be set to match the contact, and in the **5 OUT** row, in the **Assign IN** column, this input must be selected (section 5.9). After that, the output's icon in the app shows the state of the input.

I forgot the administrator code

The code cannot be retrieved. Connect to the device with a USB cable and restore the default settings with the **Restore** button at the bottom left of the programming window (section 5.8) – this deletes the user list and all settings, so afterwards the device has to be set up again, and it also has to be paired with the Wi-Fi network again. If you saved the settings to a file earlier (**Save [F9]**), after restoring you can load them with the **Open [F8]** button, and you only have to enter the code again.

I would like to control several gates from one device

The WP17's own relay switches one gate; the **I/O** terminals as open-collector outputs (50 mA) can drive an external relay (section 3.4). For gates far from each other, up to 8 **iO-LORA** wireless expanders can be connected with the **RF-LORA** transceiver, each with its own relay, input and RFID reader (section 3.7). For the users, you mark in the **Can control outputs** and **Can control iO-LORA outputs** fields which output they may switch (section 5.6).

10. Safety instructions

Figyelem!

Az elektromosság veszélyes! Személyi sérülést vagy HALÁLT, valamint anyagi kárt okozhat!

A telepítés során elektromos berendezéssel történik munkavégzés, amit az érvényes erős- és gyengeáramú rendelkezések betartásával kell kivitelezni!

A garancia (jótállás) érvényesítésének is feltétele, hogy az eszközt szakképzett személy telepítse az elektromos berendezések telepítésére vonatkozó előírások betartásával és az elektromos berendezések biztonságos üzemeltetésére vonatkozó hatályos előírásokat követve.

- The WP17 may only be installed and maintained by qualified persons.
- Before installation, read this manual to avoid mistakes that could lead to malfunction or damage to the equipment.
- **Disconnect the power supply before making any electrical connection** – both the WP17's and the gate opener's.
- Changes, modifications or repairs not authorised by the manufacturer void the warranty.
- Follow the local waste disposal rules: do not throw the device and its parts into household waste – hand in the discarded device as electronic waste.

See also

- Flexible wireless access control with the GATOR RF-LoRa system – RF-LORA and iO-LORA modules, several gates in one system.
- Protegus Android / iPhone and web app – about the app.
- Browser push notifications in the Protegus 2 app – notifications on a computer too.
- Trikdis GV17 GATOR – the cellular version, if there is no Wi-Fi at the gate, or control by call and SMS is needed.
- Documentation in English: docs.trikdis.com – GATOR WiFi Gate Controller – the manuals on docs.trikdis.com are in English.

Related products

Trikdis WP17 Smart WiFi controller **Trikdis RF-LORA wireless expander module**

Trikdis IO-LORA wireless expander module

Copyright

This manual was produced by trikdis.hu and mobilamb.eu. Its text, structure, our own illustrations and additions are our intellectual property and are protected by copyright. Without our permission it may not be copied, distributed or published on another website, in whole or in part. It may be freely downloaded and printed for installing and using the product.

Trikdis and Protegus names and logos are trademarks of UAB Trikdis.

Always up-to-date version of this manual: https://mobilamb.eu/wp17-manual