mobilamb
TRIKDIS Official Distributor

GV17 GATOR gate controller – installation and programming manual

Installation and programming manual for the Trikdis GV17 GATOR gate controller: wiring, SIM and setup in TrikdisConfig, users and permissions, control by phone call, SMS and from the Protegus 2 app.



Edition: 2026-11-18
Always up-to-date web version: https://mobilamb.eu/gv17-manual

Contents

1. Overview

1.1 What it is for and how it works
1.2 Versions
1.3 Technical specifications
1.4 Parts and terminals of the device
1.5 LED indications
1.6 Package contents and the tools you need

2. Quick start

2.1 Putting it into service in three steps
2.2 Only authorized people should be able to open
2.3 Setting up the app and the monitoring station

3. Installation and wiring

3.1 Mounting and inserting the SIM card
3.2 Power supply
3.3 Inputs
3.4 Connecting a relay to the universal output
3.5 Wiring the gate opener
3.6 Wiring the RFID reader (Wiegand 26/34)
3.7 W485 Wi-Fi module
3.8 E485 Ethernet module
3.9 RF-LORA and iO-LORA expanders with an RFID reader
3.10 iO8 and iO8-LORA expander

4. Remote control

4.1 Control by phone call
4.2 Control with the phone's keypad (DTMF)
4.3 Control from the Protegus 2 app
A rendszer létrehozása a Protegus 2 alkalmazásban
4.4 Widget on the phone's home screen
4.5 Managing users in the app
4.6 Control by SMS message
4.7 Programming by SMS

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
5.4.1 Modules tab
5.4.2 Parameters tab – W485 Wi-Fi module
5.4.3 Parameters tab – E485 Ethernet module
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 – blacklist
5.7 “System events” page
5.8 “Events Log” page
5.9 Restoring the default settings
5.10 Indicating the state of the gate
6. Remote programming
7. Testing the operation
8. Firmware update
9. Troubleshooting and frequently asked questions
10. Safety instructions
See also

1. Overview

The **GV17 GATOR** is Trikdis's cellular gate controller: it is designed for the remote control of electric gates, barriers, garage doors and other equipment. The user controls it by **phone call**, by **SMS message** or from the **Protegus 2** app; the device handles the phone numbers (RFID cards, e-mail addresses) of up to **7 administrators** and **1000 users**, and a separate time restriction (schedule, validity period) and counter can be set for each user. The GATOR notifies about state changes of the inputs and outputs (activation and restore) by SMS and in the app – you set the text of the SMS messages yourself –, and it also forwards the events to the monitoring station in Contact ID format. With a **W485** Wi-Fi or an **E485** Ethernet module, control and reporting also work over the internet, without mobile data; with an **RF-LORA** transceiver, up to 8 wireless **iO-LORA** expanders and one **iO8-LORA** expander can be connected to it, so up to 8 gates or barriers far from each other can be controlled with one device, each with its own RFID reader (the RFID readers connected to the iO-LORA expanders can switch up to 8 outputs – a reader always switches only one output of its own expander –, this requires GATOR firmware 2.13 or newer). You make the settings with the **TrikdisConfig** software over a USB cable or remotely.



Figure 1. The GV17 GATOR gate controller: the NETWORK, DATA, POWER and TROUBLE indicators on the front, the antenna connector at the top, the removable terminal block at the bottom.

1.1 What it is for and how it works

What it is mostly used for

- **Remote opening of a gate, barrier or garage door** for the family, the residents of a building, a company's employees or the tenants of a car park: the user calls the number of the GATOR's SIM card, and the gate opens – the device rejects the call, so the call is free of charge. The same can be done from the app with one button, with a widget placed on the phone's home screen, or by SMS.
- **Access control with an RFID card and code**: with one or two Wiegand 26/34 readers (entry and exit), exit with a push button, with a schedule per user (who may enter when), a validity period and an entry counter; from the entries and exits a **time and attendance record** can also be made in Protegus 2 – there is a separate article about this: GV17 access control and/or time and attendance system.
- **Any other equipment** switched on and off remotely, in pulse or two-state (latching) mode, also on a schedule: lighting, irrigation, pump, heating.
- **Several gates in one system**: with the RF-LORA and iO-LORA modules, wirelessly, up to 8 sites, each with its own relay, input and RFID reader – Flexible wireless access control with the GATOR RF-LoRa system.

How it works

- **Control**: by phone call (by default anyone who calls; with a user list, only the authorized users), during a call with the phone's keypad (DTMF), by SMS command, from the Protegus 2 mobile and web app, with an Android widget, with an RFID card and code.
- **Notifying the user**: by SMS to the administrators (about events of the inputs and outputs, test, new user), by push notification in the Protegus 2 app.
- **Reporting to the monitoring station**: with Contact ID event codes to the Trikdis software and hardware IP receivers, which work with any monitoring software; primary and backup receiver (if the connection with the primary receiver is lost, the messages automatically go to the backup receiver), SMS backup; the events can go to the monitoring station and to Protegus 2 at the same time.
- **Inputs and outputs**: 2 inputs (NO, NC or EOL 10 kΩ), 2 universal terminals (input or open-collector output, 50 mA), 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. 8 more inputs and 8 outputs in total), the iO8 or iO8-LORA expander adds further inputs and outputs (one of them can be connected to the GATOR).
- **Installation and setup**: ready to work out of the box; you add and delete users from the Protegus 2 app (as administrator), by SMS or with the TrikdisConfig software; setup is done with a USB Mini-B cable or remotely; the firmware can also be updated remotely; two access levels (installer and administrator).

1.2 Versions

The GATOR is available in two cellular versions; the wiring, setup and control of the two are the same, only the modem differs. In the TrikdisConfig status bar you see the exact type in the form **GV17_xxxx** (section 5.1).

Version	Modem	Bands
GV17-4G	4G (LTE)	In Europe LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 (for Latin America a version with a different band allocation is made)
GV17-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis GV17 - GATOR smart 4G GSM / IP gate controller

Trikdis GV17 - GATOR smart 2G GSM / IP gate controller

Because 2G networks are being gradually switched off, we recommend the 4G version for new installations. On devices with the type code **GV17_2E70** and **GV17_2S70**, control with the keypad during a call (DTMF) does not work (section 4.2); control by call, by SMS and from the app works the same way on these too.

1.3 Technical specifications

Parameter	Value
2G (GSM) modem bands	850 / 900 / 1800 / 1900 MHz
4G (LTE) modem bands	Europe: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28; Latin America: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Supply voltage	9–32 V DC or 12–24 V AC
Current consumption	100 mA
Inputs	2, selectable type: NC, NO, EOL = 10 kΩ
Universal inputs/outputs	2; as input NC, NO, EOL = 10 kΩ, as output open collector (OC), up to 50 mA
Output	1 relay, 1 A / 30 V DC, 0.5 A / 125 V AC
Memory for unsent events	up to 60 events
Event log	up to 5000 events
Users receiving messages and authorized to control (administrators)	7
Users authorized to control	1000
Operating environment	–20 … +50 °C, up to 80 % relative humidity at +20 °C
Dimensions	92 × 62 × 26 mm
Weight	80 g

1.4 Parts and terminals of the device

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

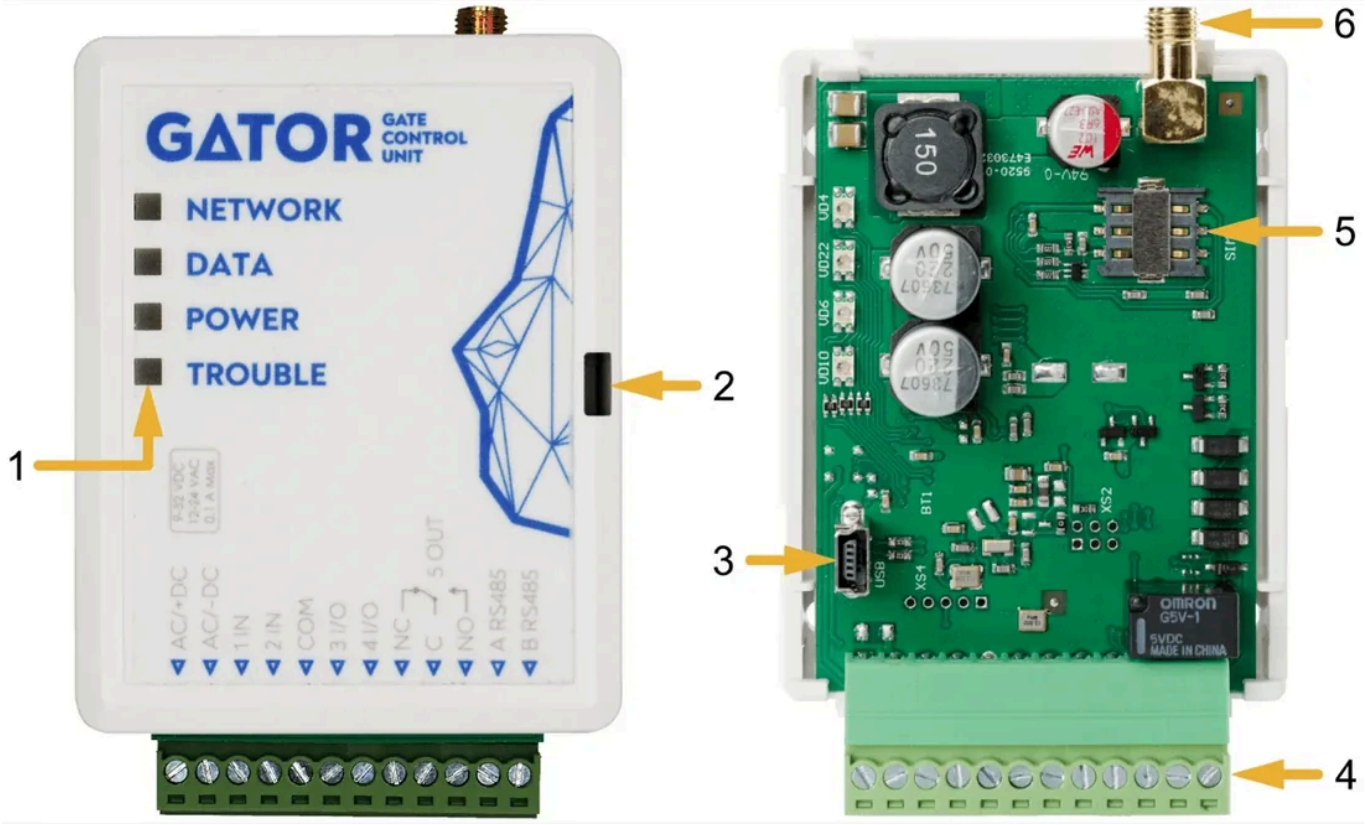


Figure 2. Parts of the GATOR.

- 1 LED indicators
- 2 opening for removing the front cover
- 3 USB Mini-B connector for programming
- 4 removable terminal block
- 5 nano-SIM card holder
- 6 SMA connector of the cellular antenna

Terminal	Purpose
AC/+DC	supply voltage: positive pole of 9–32 V DC or 12–24 V AC
AC/–DC	supply voltage: negative pole of 9–32 V DC or 12–24 V AC
1 IN	input 1, NO, NC or EOL type (default: NO input)
2 IN	input 2, NO, NC or EOL type (default: disabled)
COM	common point for the inputs
3 I/O	input or output (default: disabled)
4 I/O	input or output (default: disabled)
NC	normally closed contact of the relay
C	common contact of the relay
NO	normally open contact of the relay
A RS485	A wire of the RS485 bus
B RS485	B wire of the RS485 bus

The software and the SMS commands handle the relay output as **5 OUT** (OUTPUT5), and the two universal terminals, when used as outputs, as **3 OUT** and **4 OUT**. The 12-pin terminal block can be pulled off the device and is also available separately:

1.5 LED indications

Indicator	Light	Meaning
NETWORK	green, steady	connected to the mobile network
	yellow blinking	mobile network signal strength with 0–5 blinks; 3 is already enough
DATA	green, steady	message being sent
	yellow, steady	there are events waiting to be sent in the memory
POWER	green blinking	the supply voltage is correct
	yellow blinking	the supply voltage is not correct
	red and yellow blinking	configuration mode
TROUBLE	off	no operating fault
	1 blink	no SIM card
	2 blinks	the PIN code of the SIM card is wrong
	3 blinks	cannot connect to the mobile network
	4 blinks	cannot connect to the Protegus cloud or to the primary IP receiver
	5 blinks	cannot connect to the backup IP receiver
	6 blinks	the internal clock is not set
	7 blinks	the supply voltage is not correct

If none of the LEDs is lit, check the supply voltage and the wiring.

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.

1.6 Package contents and the tools you need

In the box: 1 GV17 GATOR gate controller, 1 cellular antenna, 3 resistors of 10 kΩ, 1 piece of double-sided adhesive tape (5 cm) and 2 screws.

What you will need

Before you start the installation, check that you have everything at hand: a USB Mini-B cable for the setup · a cable with at least 4 wires for the wiring · a 2.5 mm flat screwdriver · an activated nano-SIM card (switch off the PIN request) with mobile data service, if you also use the app or the monitoring station · an external antenna, if the signal is weak at the site · the installer manual of the controlled device (gate motor, barrier), including the wiring of its control input and gate state output. The listed accessories must be obtained separately – order them from your dealer.

With a weak signal, in a metal box or behind a thick wall, use an antenna with a 2.5 m cable that can be mounted away from the device instead of the antenna in the package:

Trikdis ME301M magnetic antenna with 2,5m wire

Trikdis ANT04 GSM stick-on antenna with 2,5m wire

2. Quick start

The GATOR is ready to work out of the box

If anyone calls the phone number of the SIM card inserted in the device, the GATOR rejects the call and switches on the **5 OUT** relay output for **3 seconds**. If this operation suits you, the device can be put into service without any further setup.

2.1 Putting it into service in three steps

1. **Insert the nano-SIM card** into the GATOR's holder (section 3.1). Before that, switch off the PIN request on the card in a phone, otherwise the device will not register on the network (or you must enter the PIN in TrikdisConfig, section 5.2).
2. **Connect the power supply and the gate opener** according to the drawings in chapter 3: the power supply to the **AC/+DC** and **AC/−DC** terminals, the control input of the gate opener to the **C** and **NO** contacts of the relay.
3. **Switch on the power.** When it works correctly, the **POWER** LED blinks green, the **NETWORK** LED is lit green and in between blinks yellow according to the signal strength. Call the number of the SIM card: the device rejects the call and the relay pulls in for 3 seconds.

2.2 Only authorized people should be able to open

By default **anyone** who calls its number can control the GATOR. If you want to allow it only for specific people, send an SMS with the users' phone numbers (send the command from your own phone, because whoever calls or sends an SMS to the device first becomes its administrator, section 4.1):

```
SETU 123456 +CC123456789#Peter#peter@example.com
```

(CC is the country code.) After the first number has been added, the GATOR only reacts to calls from numbers on the list and ignores the others. You can add more users the same way, one by one; the full set of SMS commands is described in section 4.7, and you can also manage the list in TrikdisConfig and in the Protegus 2 app (sections 5.6 and 4.5).

Change the administrator password

With the default `123456` password, anyone who knows the device's number can reprogram the GATOR. At the first start-up, change it by SMS (`PSW 123456 newpassword`, 6 characters) or in TrikdisConfig (**System Options** → **Administrator Code**).

2.3 Setting up the app and the monitoring station

- **Protegus 2 app:** in TrikdisConfig, on the **IP Reporting** page, switch on the cloud service (**Enable cloud service**, section 5.5), and change the default `123456` code of the **Cloud Access Code**; the same by SMS: `CONNECT 123456 PROTEGUS=ON`. After this, the system can be added to the app as described in section 4.3. This requires mobile data service on the SIM card (or a W485 / E485 module).

- **Monitoring station:** on the **IP Reporting** page enter the receiver's address, port and encryption key, and on the **System Options** page the object ID (sections 5.2 and 5.5).
- **Recommended order of the settings in TrikdisConfig:** administrator password and SIM data (APN) → function of the inputs and outputs, pulse time → users, RFID cards, schedule → cloud and monitoring station → testing as described in chapter 7.

If you want to change the default settings or switch on further functions of the device, chapter 5 describes the settings of the TrikdisConfig software.

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 GATOR, the power supply, wiring the inputs, the relay and the gate opener, and then connecting the RFID readers and the expansion modules (W485, E485, RF-LORA + iO-LORA, iO8 / iO8-LORA). In the drawings the GATOR's terminal names match the labels on the device (section 1.4).

3.1 Mounting and inserting the SIM card

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 box: press the holding tab and lift it out.
3. Fix the back of the box in the desired place with screws (or with the supplied double-sided adhesive tape).
4. Put back the printed circuit board and the terminal block.
5. Screw the cellular antenna onto the SMA connector.
6. Insert the nano-SIM card into the holder.
7. Put back the front cover.

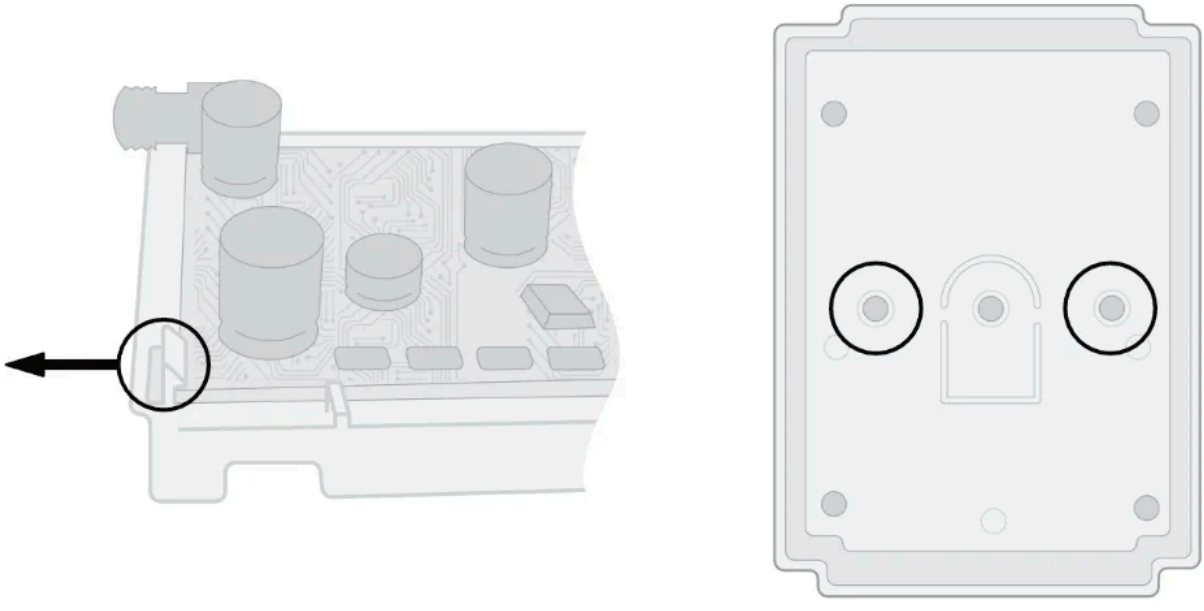


Figure 3. On the left, the holding tab of the printed circuit board (pressed in the direction of the arrow, the board is released), on the right, the two screw holes of the back panel.

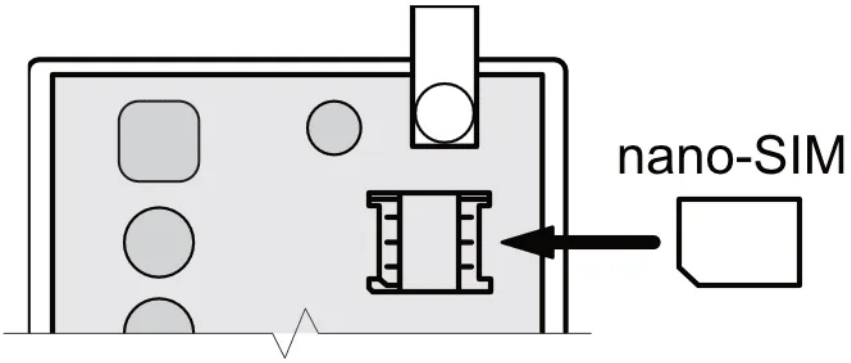


Figure 4. Inserting the nano-SIM card in the direction of the arrow into the holder on the printed circuit board.

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

3.2 Power supply

The GATOR works from a **9–32 V DC** or **12–24 V AC** power supply; the two power terminals (**AC/+DC**, **AC/−DC**) accept both supply types. In most cases the accessory power output of the gate motor's control unit (typically 24 V AC or DC) is sufficient, so no separate power supply is needed. For a separate power supply, a ~230 V / 16 V transformer of at least 10 VA (with a 125 mA fuse on the 230 V side) or a 9–32 V DC power supply of at least 0.2 A is suitable. The device has no backup battery: if the gate must also open during a power outage, run it from an uninterruptible power supply. Connect the wires according to the drawing below.

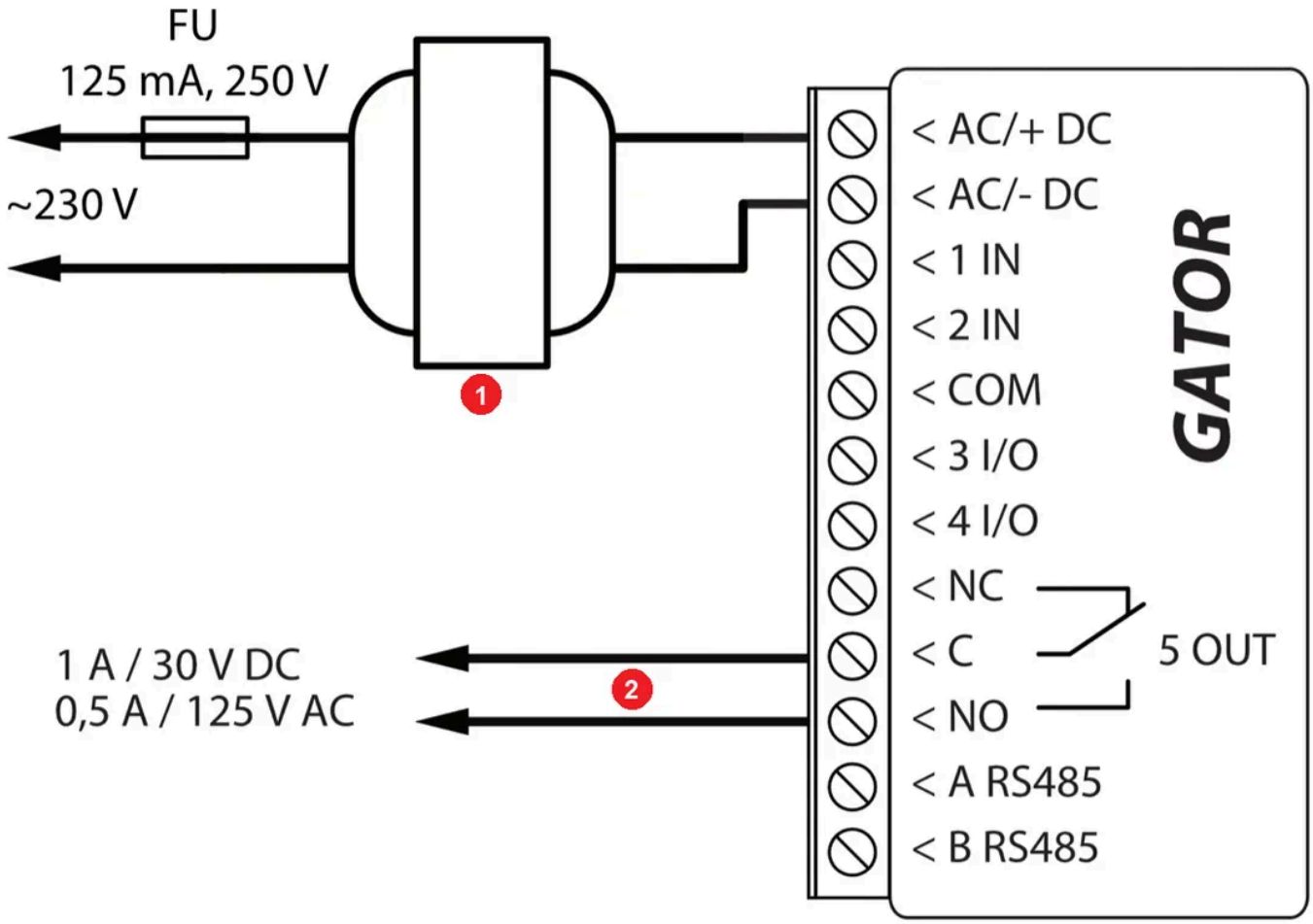


Figure 5. Wiring the power supply and the gate opener: mains power from a ~230 V / 16 V, 10 VA, 50 Hz transformer (fuse 125 mA, 250 V) or from a 9–32 V, 0.2 A DC power supply to the AC/+DC and AC/−DC terminals; the control input of the gate opener to the C and NO contacts of the relay; the relay's load capacity is 1 A / 30 V DC or 0.5 A / 125 V AC.

- 1 transformer, ~230 V / 16 V, 10 VA, 50 Hz (“Transformer”), or DC power supply, 9–32 V, 0.2 A (“or DC power supply source”)
- 2 gate control (“Gate control”) – the control input of the gate opener

In the drawings the RFID readers, the relays and the expansion modules take their power from the **AC/+DC** terminal: this is only possible with a **DC** power supply (in the drawings 9–16 V DC, 0.5 A, for the W485 / E485 and iO8 module 10–28 V DC). With an AC power supply, the reader and the module need a separate DC power supply.

3.3 Inputs

The GATOR has **four inputs**: **1 IN** and **2 IN** are always inputs, **3 I/O** and **4 I/O** are universal terminals that can be set as input or as output. Each works relative to the **COM** terminal and can be of **NO**, **NC** or **EOL** type (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 limit switch or state output (gate state indication, sections 3.5 and 5.10), an exit push button (section 3.6), or any detector or contact about whose change you want an SMS or push notification, or with which you want to switch an output (**CTRL by IN**, section 5.3). You set the type and the reaction time on the **IN/OUT** page of TrikdisConfig; by default only 1 IN is active (NO). Connect the inputs according to the set type (NC, NO, EOL), as shown in the drawing below.

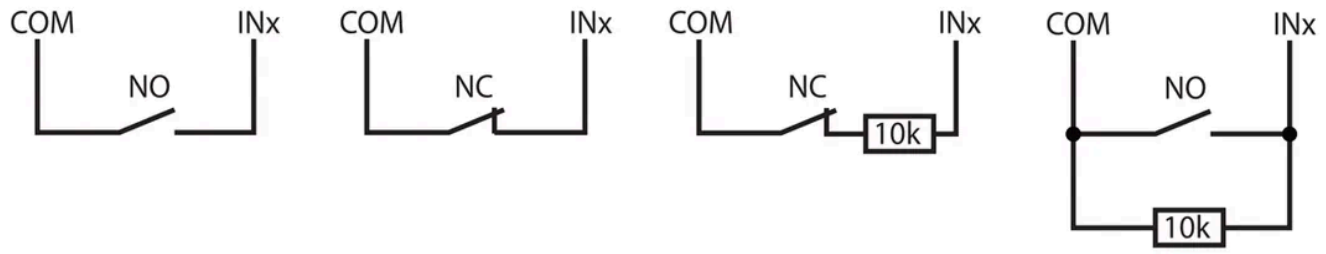


Figure 6. The four ways of wiring the inputs between the COM and the IN terminal. From left to right: **NO** – normally open contact – closing = alarm, opening = restore; **NC** – normally closed contact – opening = alarm, closing = restore; **NC + EOL** – normally closed contact with a 10 kΩ resistor in series – short circuit and open circuit = alarm, 10 kΩ = normal state; **NO + EOL** – normally open contact with a 10 kΩ resistor in parallel – short circuit and open circuit = alarm, 10 kΩ = normal state.

3.4 Connecting a relay to the universal output

As outputs, the **3 I/O** and **4 I/O** terminals are open collector with a load capacity of up to **50 mA**: directly they can only switch the coil of a small relay. With the relay's contacts any equipment can be switched on and off remotely. The drawing applies to a DC power supply: one end of the coil goes to the **AC/+DC** terminal, the other to the output; in TrikdisConfig the function of the terminal must be set to **Output** (section 5.3).

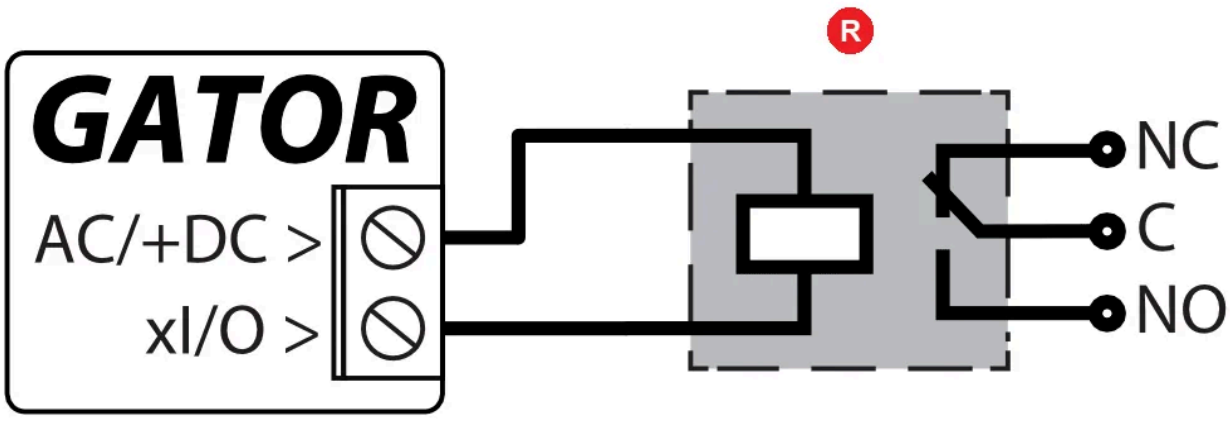


Figure 7. External relay on the universal output: the coil between AC/+DC and the 3 I/O or 4 I/O terminal set as output; the relay's NC, C and NO contacts switch the equipment.

- R relay (“Relay”)

3.5 Wiring the gate opener

Always do the wiring with the power disconnected. 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.

The gate is opened by the **IN** and **COM** (control) terminals of the gate opener: the **C** and **NO** contacts of the GATOR's relay go here, and the relay's pulse does the same as the button of the remote control. Most gate openers have a **gate state 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 K1 auxiliary relay 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, the K1 relay pulls in and activates the GATOR's **1 IN** input. This way the state of 1 IN follows exactly the position of the gate, which the Protegus 2 app and the widget icon also show – the related setting is in section 5.10. With a gate opener with a relay output, K1 is not needed; the state contact can be connected directly between 1 IN and COM.

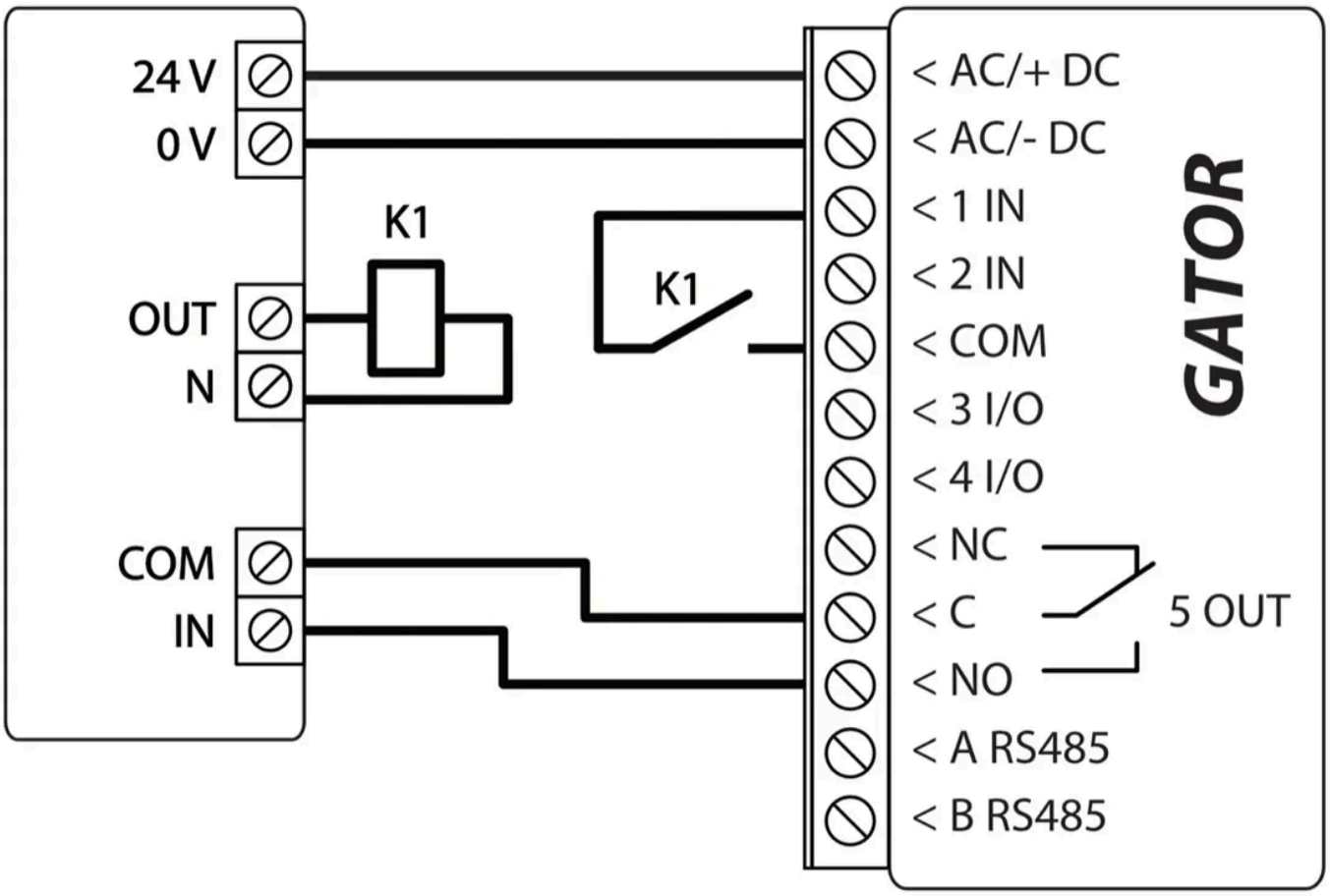


Figure 8. Connecting the gate opener's control unit ("Gate control unit") and the GATOR with the K1 auxiliary relay. Power supply ("Power"): the gate opener's 24 V power output to the GATOR's AC/+DC terminal, 0 V to its AC/−DC terminal; gate state ("Gate status"): the gate opener's OUT and N terminals to the coil of the K1 relay, the K1 contact between the GATOR's 1 IN and COM terminals; gate control ("Gate control"): the gate opener's COM terminal to the GATOR's 5 OUT C contact, its IN terminal to the 5 OUT NO contact.

3.6 Wiring the RFID reader (Wiegand 26/34)

The GATOR accepts one or two RFID readers with the **Wiegand 26/34** protocol (card readers and code keypad readers as well). With the cards and codes added to the user list, the reader switches the **5 OUT** output (the per-user permission, schedule and counter also apply to the reader). The reader is set up on the **IN/OUT** page of TrikdisConfig (section 5.3), and the cards are added on the **User list** page (section 5.6); the colour code of the wires follows the Wiegand standard: red +U, black GND, green D0, white D1.

One reader: D0 goes to the **1 IN** terminal, D1 to the **2 IN** terminal, the exit push button between **COM** and **3 I/O**. In the software, set **Wiegand reader mode** to **Single Reader**, and if there is an exit button, tick the **IO3 as exit button (5 OUT)** checkbox: when the button is pressed, 5 OUT switches on for the set pulse time. If there is no button, leave the checkbox empty.

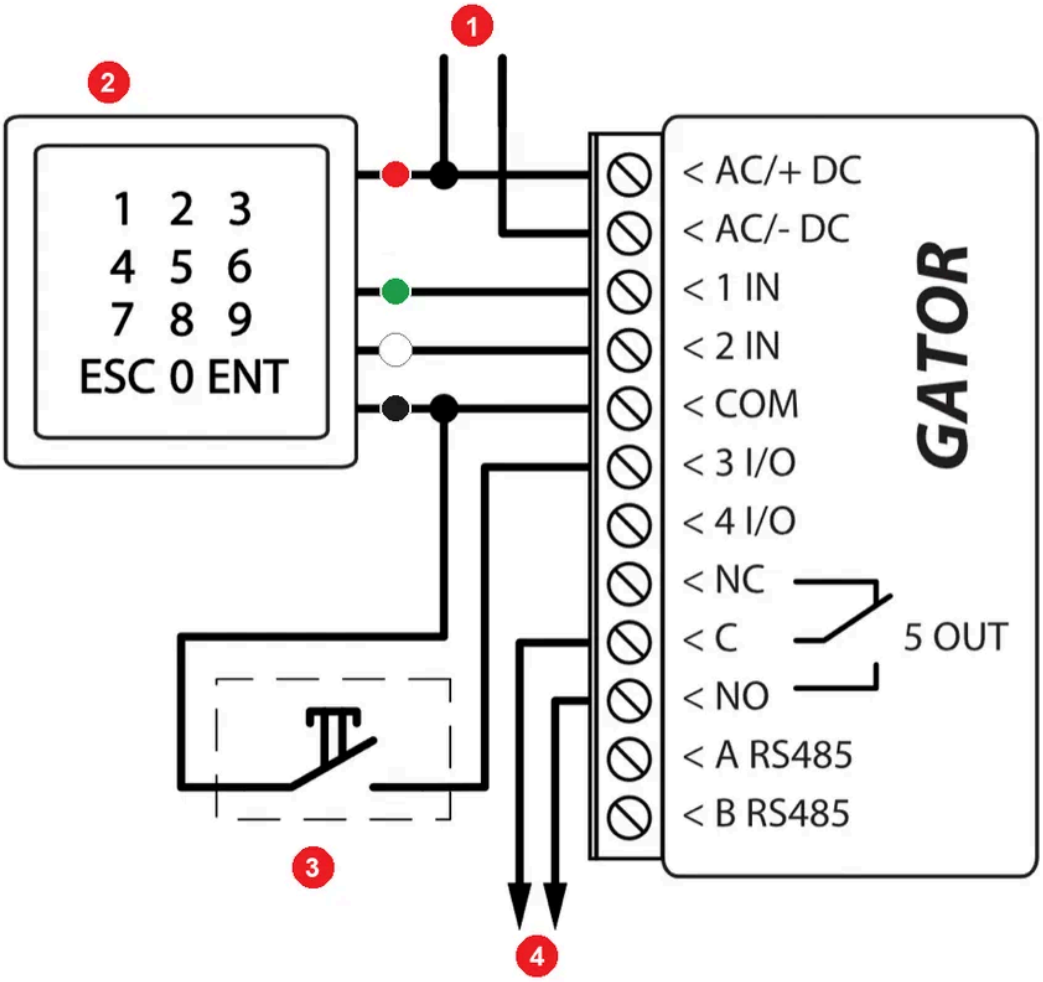


Figure 9. Wiring one Wiegand 26/34 reader and an exit button: DC power supply, 9–16 V, 0.5 A, to the AC/+DC and AC/−DC terminals; the entry reader's red wire (+U) to AC/+DC, the green (D0) to 1 IN, the white (D1) to 2 IN, the black (GND) to the COM terminal; the exit push button between the COM and the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

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

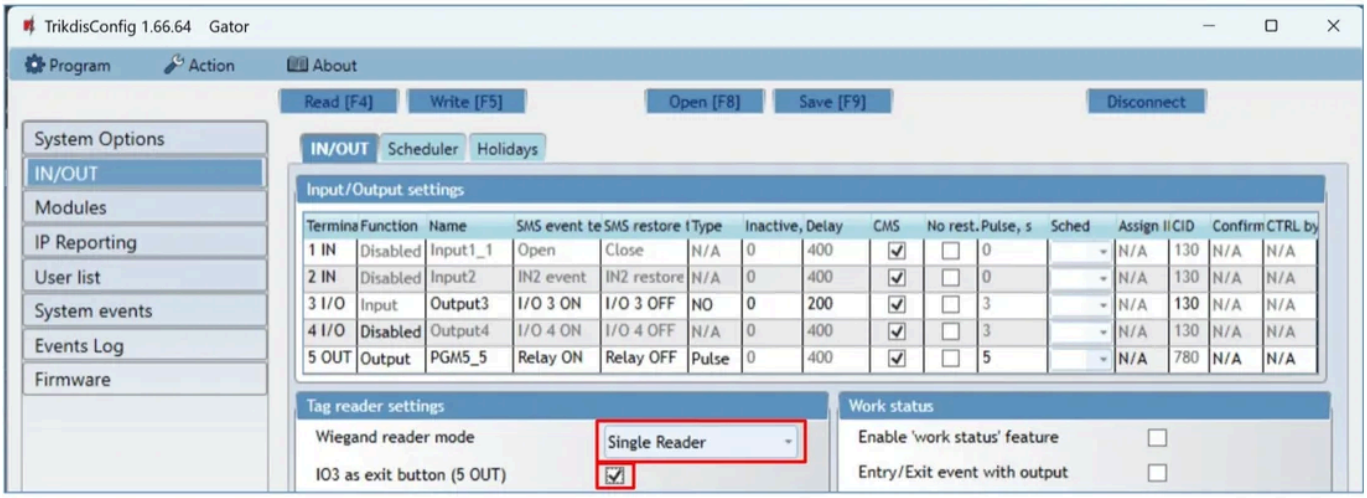


Figure 10. TrikdisConfig – IN/OUT, **Tag reader settings**: with one reader **Wiegand reader mode = Single Reader**, with an exit button **IO3 as exit button (5 OUT)** ticked.

Two readers (entry and exit): the D0 / D1 wires of the first reader go to the **1 IN** / **2 IN** terminals, those of the second to the **3 I/O** / **4 I/O** terminals; in the software **Wiegand reader mode = Dual Reader**. With two readers 3 I/O is in use, so no exit button can be connected to it.

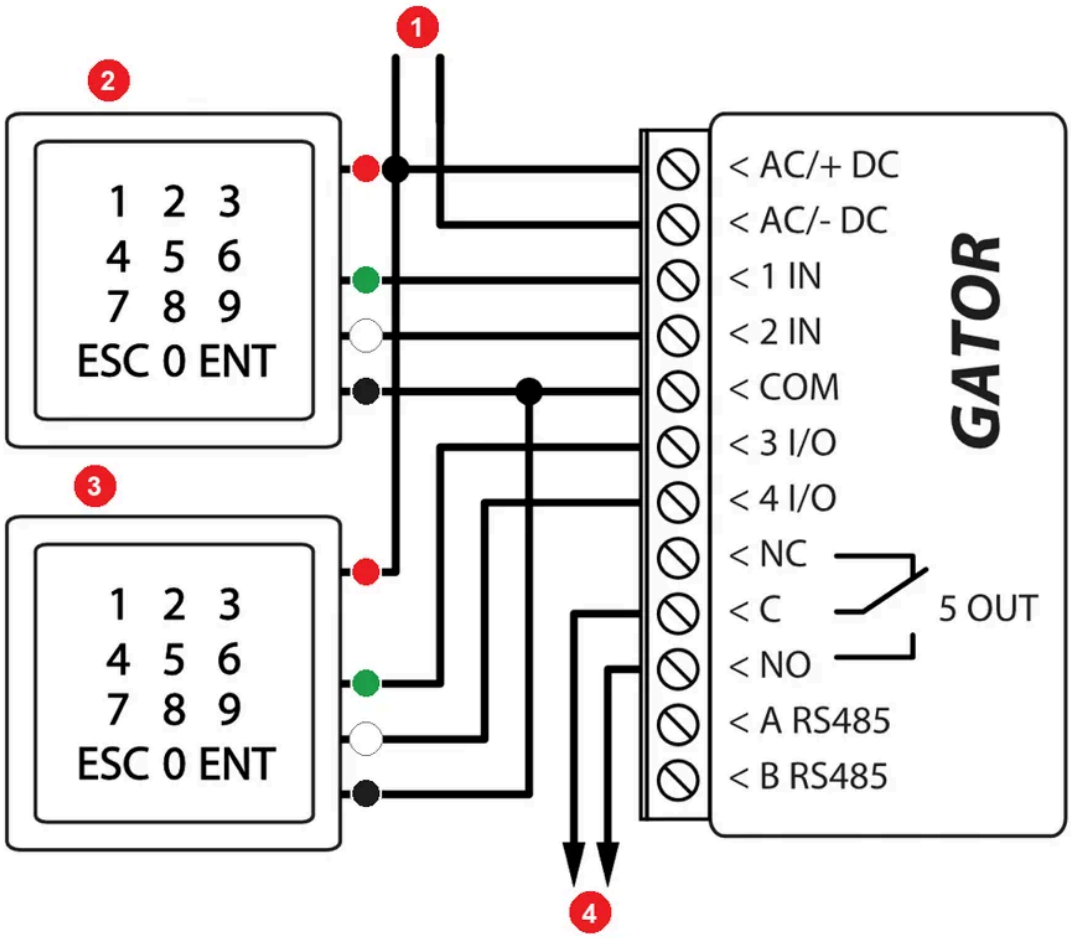


Figure 11. Wiring two Wiegand 26/34 readers, both RFID readers with keypad (“RFID reader with keypad (Wiegand 26/34)”): DC power supply, 9–16 V, 0.5 A; the entry reader's green wire (D0) to 1 IN, the white (D1) to the 2 IN terminal; the exit reader's green wire (D0) to 3 I/O, the white (D1) to the 4 I/O terminal; the red wire (+U) of both readers to AC/+DC, the black (GND) to the COM terminal; the gate opener on the C and NO contacts of the relay (1 A / 30 V DC, 0.5 A / 125 V AC).

- 1 DC power supply (“DC power supply”), 9–16 V, 0.5 A
- 2 entry reader (“Entry reader”)
- 3 exit reader (“Exit reader”)
- 4 gate control (“Gate control”) – the control input of the gate opener; the relay's load capacity is 1 A / 30 V DC, 0.5 A / 125 V AC
- red wire, +U (“R - red (+U)”)
- black wire, GND (“B - black (GND)”)
- white wire, D1 (“W - white (D1)”)
- green wire, D0 (“G - green (D0)”)

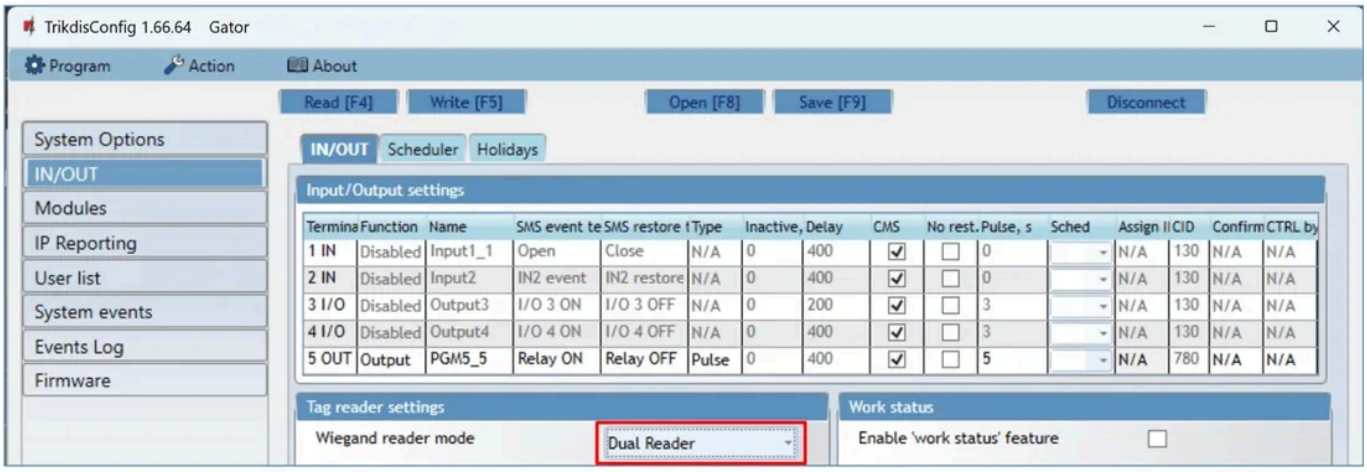


Figure 12. TrikdisConfig – IN/OUT, **Tag reader settings**: with two readers **Wiegand reader mode = Dual Reader**.

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

3.7 W485 Wi-Fi module

The **W485** module sends the GATOR's messages over the local Wi-Fi network, through the internet router, to the monitoring station and the Protegus 2 app, so no mobile data is used. If the Wi-Fi connection is lost, the device switches to the mobile network by itself, and when the Wi-Fi returns, it goes back to the W485. The function works from GATOR firmware **1.06**. The module connects to the **RS485** bus (A–A, B–B), with alarm cable **up to 100 m** away, and works from a 10–28 V DC power supply shared with the GATOR. **With the W485 the GATOR can also be used without a SIM card** – in that case it can only be controlled from the app; there are no calls and SMS. The module's setup is in section 5.4.

Trikdis W485 Wifi module (RS485)

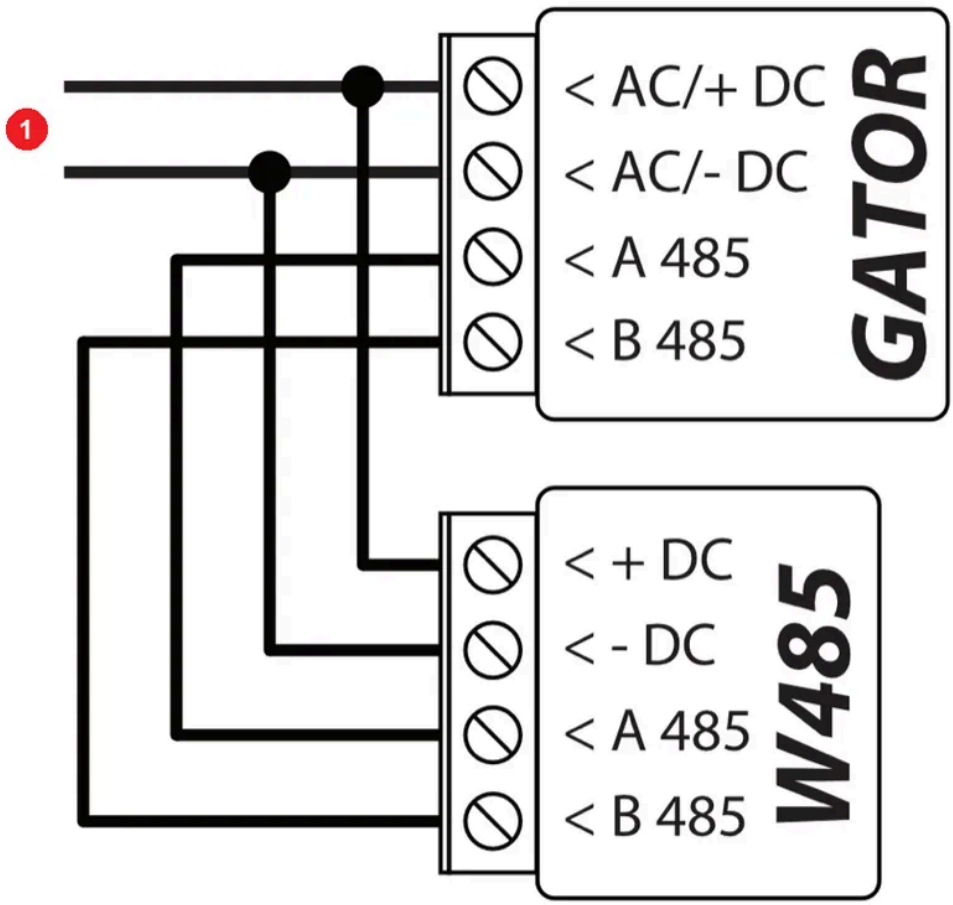


Figure 13. Wiring the W485 module: the positive pole of the 10–28 V DC, 0.5 A power supply to the GATOR's AC/+DC and the W485's +DC terminal, the negative to the AC/−DC and −DC terminals; RS485 connection (“RS485 connection”), up to 100 m (“up to 100m”): A 485 – A 485, B 485 – B 485.

- 1 power supply (“Power supply”), 10–28 V DC, 0.5 A

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.

3.8 E485 Ethernet module

The **E485** module does the same with wired internet: the GATOR's messages go to the monitoring station and the Protegus 2 app over the Ethernet cable plugged into the router, the device does not use mobile internet, and the mobile network is only a backup: if the wired internet is lost, it sends the messages over mobile internet, and when the wired connection returns, over the E485 again. From firmware **1.06**; RS485 bus up to 100 m; shared 10–28 V DC power supply; can also be used without a SIM card. Setup is in section 5.4.

Trikdis E485 Ethernet module (RS485)

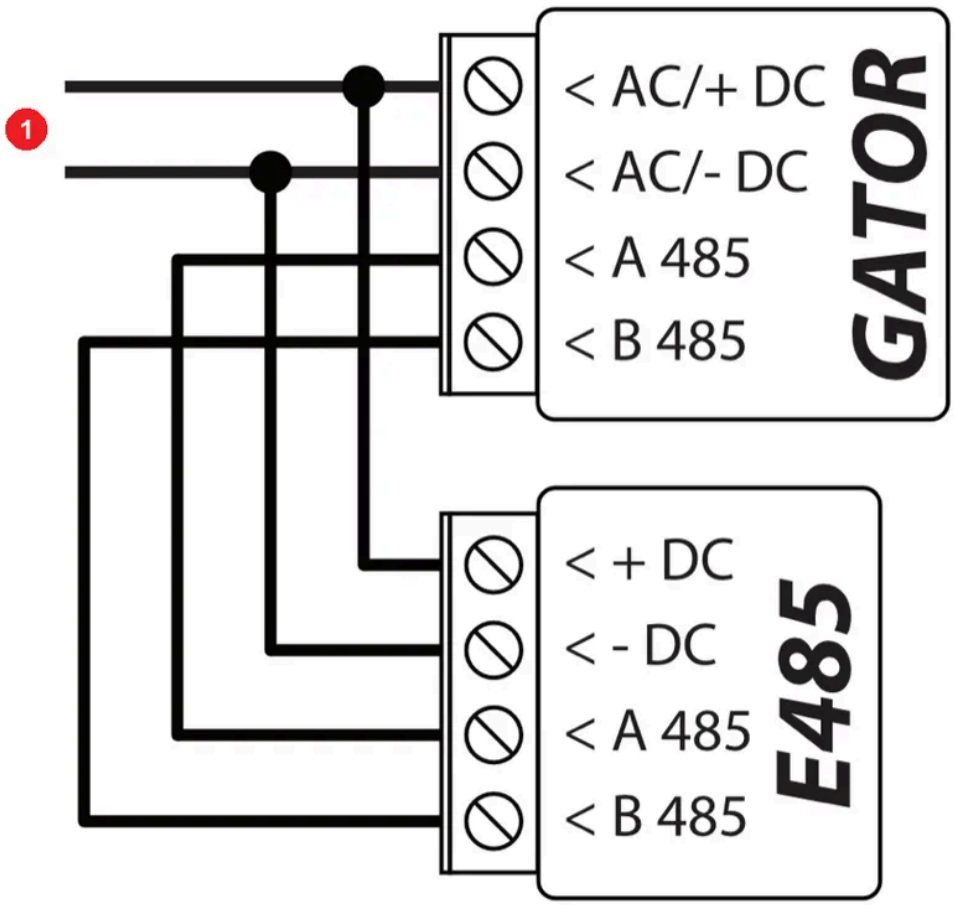


Figure 14. Wiring the E485 module: the positive pole of the 10–28 V DC, 0.5 A power supply to the GATOR's AC/+DC and the E485's +DC terminal, the negative to the AC/−DC and −DC terminals; RS485 connection ("RS485 connection"), up to 100 m ("up to 100m"): A 485 – A 485, B 485 – B 485.

- 1 power supply ("Power supply"), 10–28 V DC, 0.5 A

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.

3.9 RF-LORA and iO-LORA expanders with an RFID reader

From GATOR firmware **2.13** the system can be expanded wirelessly: the **RF-LORA** transceiver connects to the RS485 bus and keeps radio contact with up to **8 iO-LORA** expanders (up to 5000 m in open space). Each iO-LORA expander adds one input and one relay output to the GATOR, 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 up to 8 gates or barriers far from each other can be controlled with one GATOR, 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**

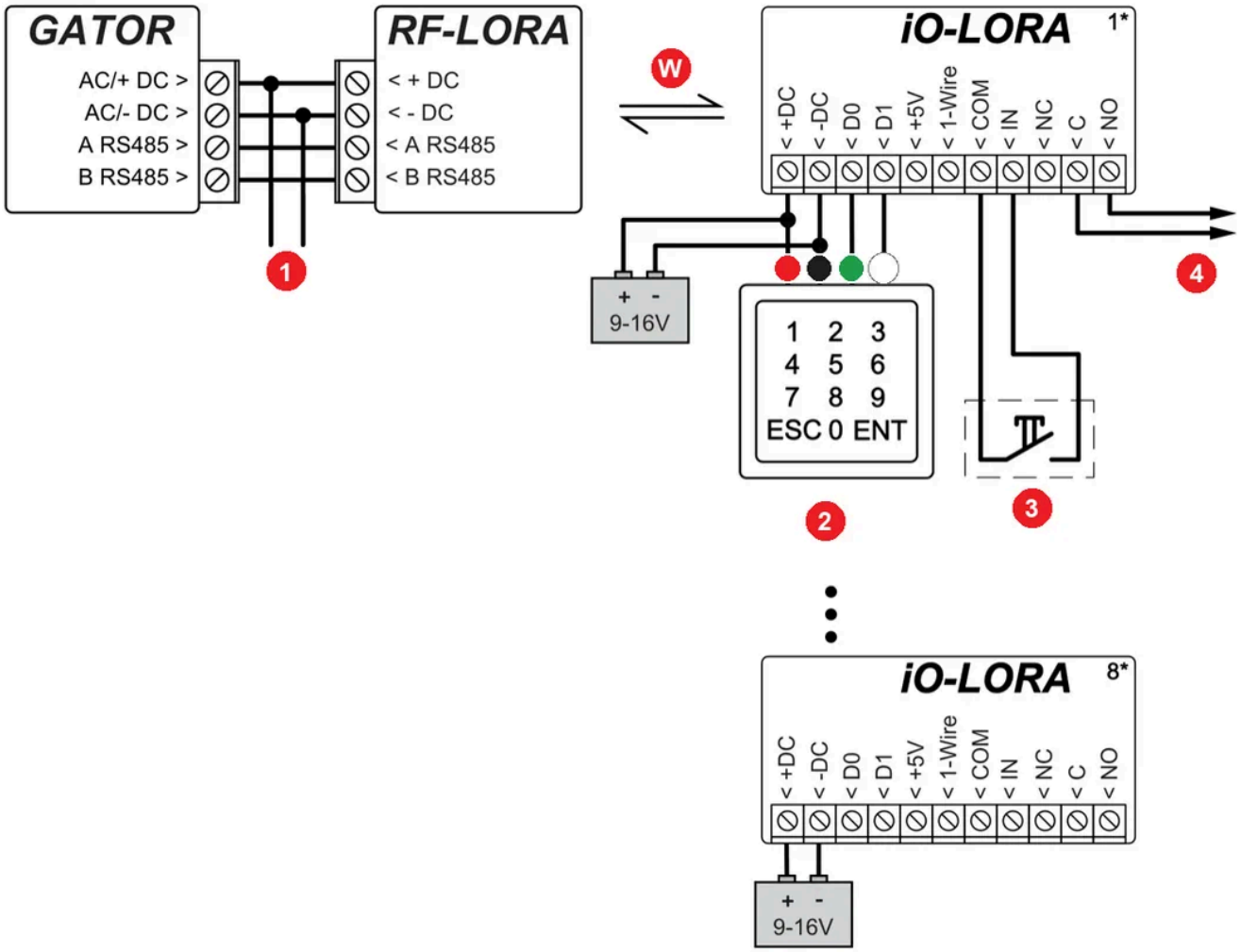


Figure 15. RF-LORA transceiver on the GATOR and iO-LORA expanders with an RFID reader: shared 9–16 V DC, 0.5 A power supply for the GATOR and the RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A–A, B–B; radio connection between the RF-LORA and the iO-LORA 1…8 expanders, up to 5000 m; each iO-LORA gets its own 9–16 V power supply; the reader on the iO-LORA: red (+U) to +DC, black (GND) to −DC, green to 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 (“DC power supply”), 9–16 V, 0.5 A
- W wireless connection (“Wireless connection”), up to 5000 m (“up to 5000 m”)
- 2 RFID reader with keypad, Wiegand 26/34 (“RFID reader with keypad (Wiegand 26/34)”)
- 3 exit push button (“»Exit« button”)
- 4 gate control (“Gate control”) – the control input of the gate opener; the load capacity 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 GATOR to the computer with a USB Mini-B cable or log in remotely, and read the settings (**Read [F4]** – the software shows the device's current settings). If the software asks for it, enter the 6-digit administrator or installer code in the pop-up window. On the **Modules** page select

the **iO-LORA controller** item from the list, and in the **Serial No.** field enter the expander's six-digit serial number (on the expander's sticker). The RF-LORA does not need to be added separately.



Figure 16. TrikdisConfig – Modules: the iO-LORA expander selected, the serial number goes into the **Serial No.** field.

2. For each added iO-LORA expander, an input (for example **6 IN iO-LORA 1**) and an output (**7 OUT iO-LORA 1**) appear in the list on the **IN/OUT** page. Set the input's function to **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 (in the example 3 s).

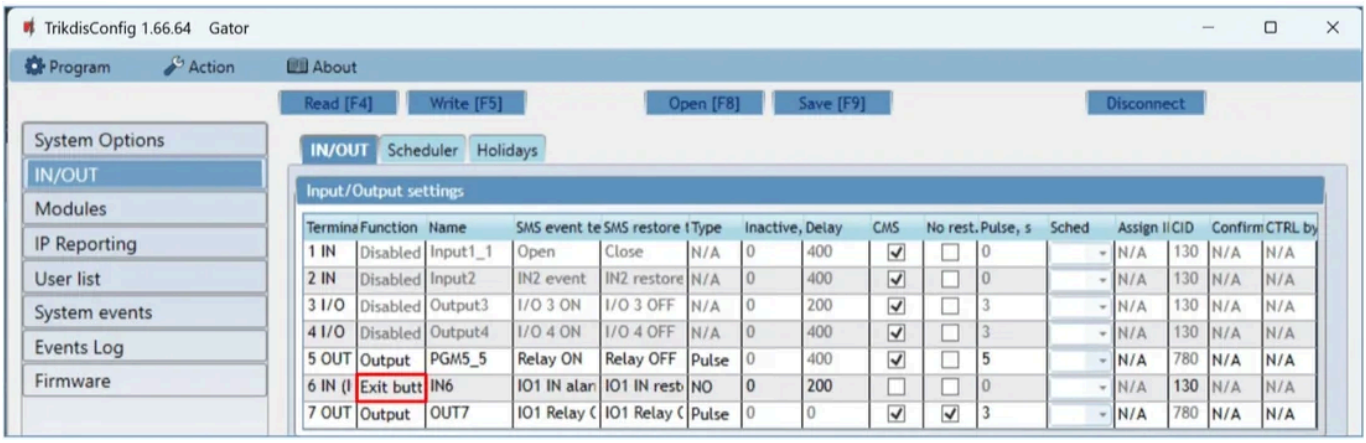


Figure 17. TrikdisConfig – IN/OUT: the function of **6 IN** is **Exit button**, the **7 OUT** output is of **Pulse** type, with a 3 s pulse.

3. On the **User list** page enter the user's name, the RFID card number (**Phone/RFID**), for a code reader the code, tick the **En** checkbox, and mark which output the user may control (in the example output 7). Write the settings (**Write [F5]**), wait until the update finishes, then **Disconnect** and unplug the USB cable.

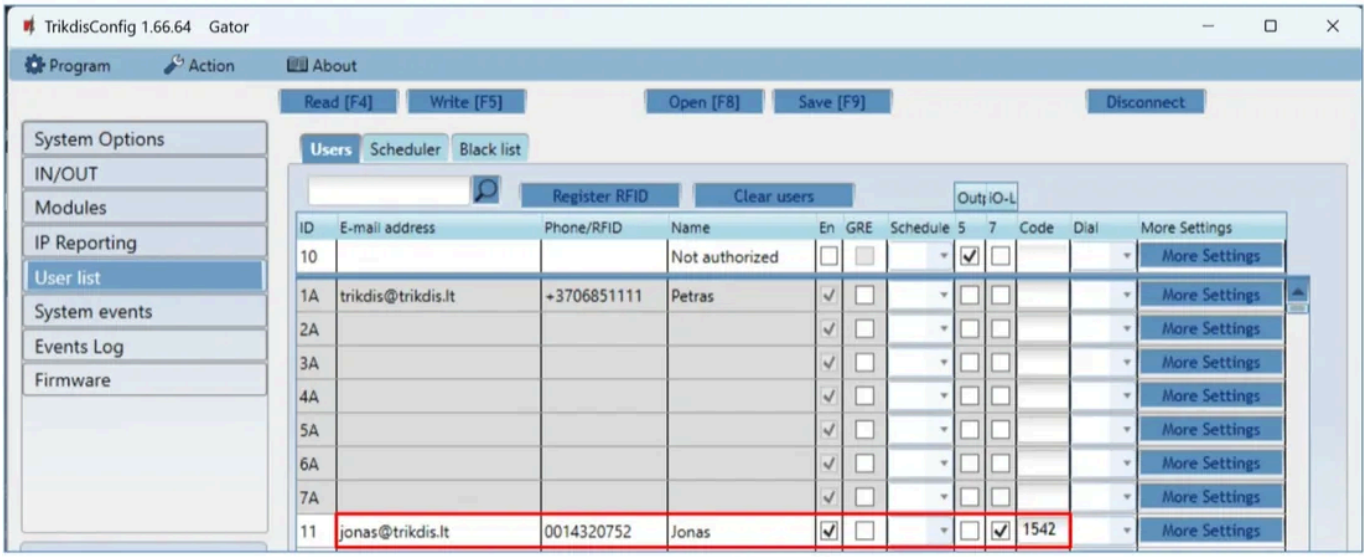


Figure 18. TrikdisConfig – User list: for the user the RFID number, the name and the code are filled in, **En** is ticked, output 7 is marked.

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

3.10 iO8 and iO8-LORA expander

If you need more inputs or outputs in one place, **one iO8** (wired, RS485) or **iO8-LORA** (wireless, through the RF-LORA) expander can be connected to the GATOR. The expander's inputs and outputs appear in the list on the **IN/OUT** page and can be handled in the same way as the GATOR's own; the module must be added on the **Modules** page with its serial number (section 5.4).

Trikdis iO8 wired expander module **Trikdis IO8-LORA wireless expander module**

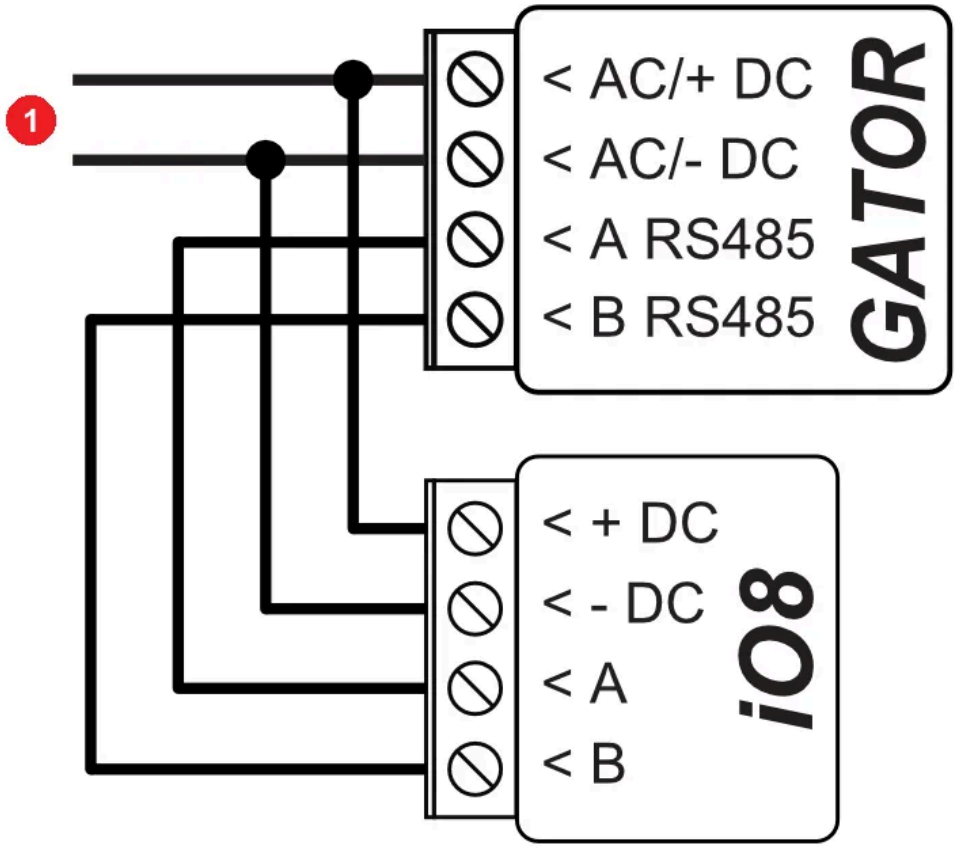


Figure 19. Wiring the iO8 expander: the positive pole of the 10–28 V DC, 0.5 A power supply to the GATOR's AC/+DC and the iO8's +DC terminal, the negative to the AC/−DC and −DC terminals; RS485 connection (“RS485 connection”), up to 100 m (“up to 100m”): the GATOR's A RS485 terminal to the iO8's A terminal, B RS485 to the B terminal.

- 1 power supply (“Power supply”), 10–28 V DC, 0.5 A

The iO8 runs on 10–26 V DC: if the power supply gives more than 26 V, the iO8 gets a separate power supply, with the negative poles of the two power supplies connected together.

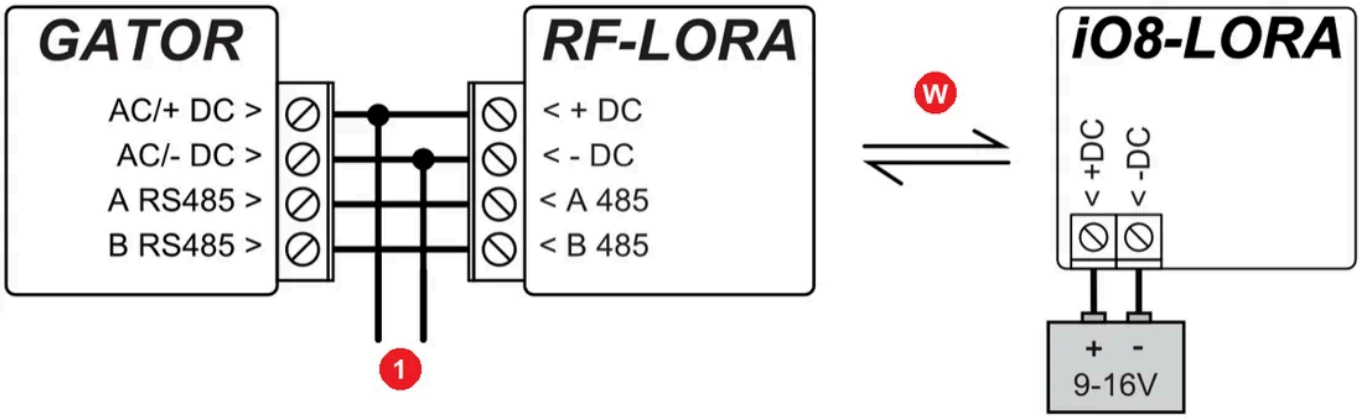


Figure 20. The iO8-LORA expander through the RF-LORA transceiver: 9–16 V DC, 0.5 A power supply for the GATOR and the RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A RS485 – A 485, B RS485 – B 485; radio connection between the RF-LORA and the iO8-LORA, up to 5000 m; the iO8-LORA gets its own 9–16 V power supply.

- 1 DC power supply (“DC power supply”), 9–16 V, 0.5 A
- W wireless connection (“Wireless connection”), up to 5000 m (“up to 5000 m”)

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.

4. Remote control

You can control the GATOR in four ways: by **phone call** (free of charge, because the device does not answer the call), during a call with the **phone's keypad** (DTMF), from the **Protegus 2** app or with a **widget** placed on the phone's home screen, and by **SMS command**. In all four modes the user list (section 5.6) decides who may do what; with SMS commands the administrator can also change the settings.

4.1 Control by phone call

Call the number of the SIM card inserted in the GATOR. The device **automatically rejects** the call and switches on the **5 OUT** relay output for **3 seconds** – the call costs nothing. By default anyone who knows its number can control the device this way.

- **Only authorized users**: if you add even a single number to the user list (by SMS: `SETU …`, section 4.7; in TrikdisConfig or in the app), the GATOR only reacts to calls from numbers on the list. In TrikdisConfig the same is switched by the **En** checkbox of the entry no. 10 called **Not authorized** in the **User list** (section 5.6): ticked, anyone can call; empty, only the members of the list.
- **Which output opens**: if a user may control several outputs, the outputs marked in the **Dial** column switch on a call, after which the device ends the call.
- **Length of the call**: with the **System Options** → **Hang-up after** value at 0, the device rejects the call immediately; with a higher value it answers the call and ends it after the set time – this is needed for keypad control (section 4.2).

Whoever **first** calls the GATOR in its factory state, or first sends it an SMS, becomes the device's **administrator**: from then on only this person can manage it with SMS commands. So make the first call from the owner's or the installer's phone.

4.2 Control with the phone's keypad (DTMF)

If the GATOR answers the call (**Hang-up after** greater than 0), the user can switch several outputs with the phone's keypad:

1. Call the number of the GATOR's SIM card – the device answers the call.
2. Type the control command on the phone's keypad according to the table.

DTMF code	Function	Description
`OUTPUT*STATE#`	output control	**OUTPUT** – the number of the output. **STATE** – 0: switch off; 1: switch on; 2: switch off for the pulse time; 3: switch on for the pulse time (the pulse time can be set in the **IN/OUT** table of TrikdisConfig). **#** – end of the command. Example – switching on output 5: `5*1#`; switching on output 4 for the pulse time: `4*3#`
`#`	end of the command	if you made a mistake in the command, press the **#** key and type it again

Keypad (DTMF) control does not work on devices with the type code **GV17_2E70** and **GV17_2S70**. You see the exact type in the TrikdisConfig status bar (section 5.1).

4.3 Control from the Protegus 2 app

In Protegus 2 the user opens the gate from anywhere, sees the state of the system and the state of the gate (if the gate state is wired, sections 3.5 and 5.10), receives all system events as push notifications, and as administrator also manages the users. The app is free of charge; for the phone you download it from the app stores, in a browser it opens at https://web.protegus.app.

Before you add the system

In TrikdisConfig, on the **IP Reporting** page, **Enable cloud service** must be ticked (section 5.5; by SMS: `CONNECT 123456 PROTEGUS=ON`), the power supply must be in order (the **POWER** LED blinks green), and the device must be on the network (the **NETWORK** LED is lit green and blinks yellow). The SIM card must have mobile data service, or there must be a W485 / E485 module.

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.

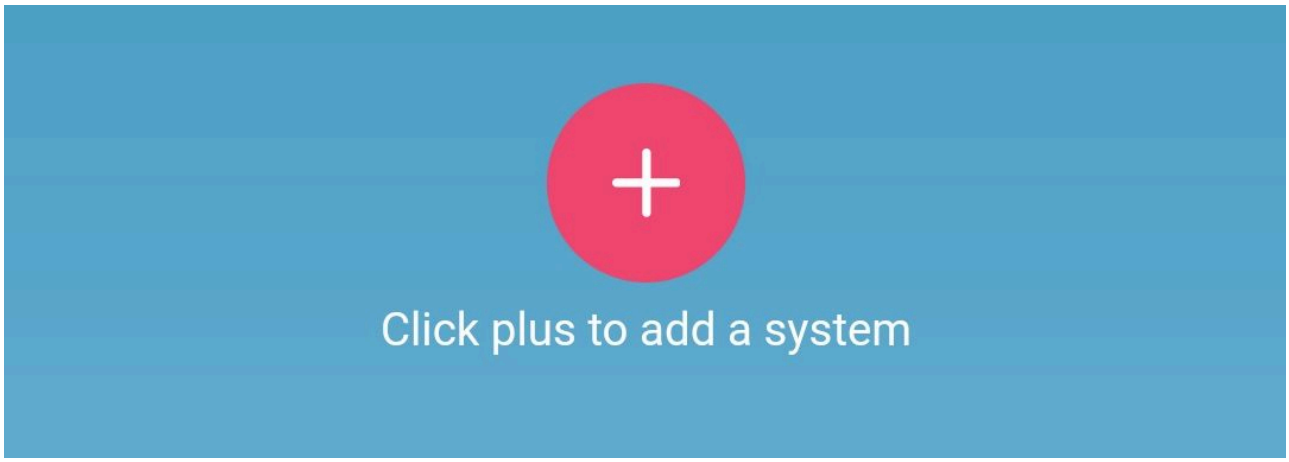
A rendszer létrehozása a Protegus 2 alkalmazásban

1. Töltsd le a Protegus 2 alkalmazást a telefonodra vagy nyisd meg egy böngészőben



2. Regisztrálj egy fiókot, ha még nincs.

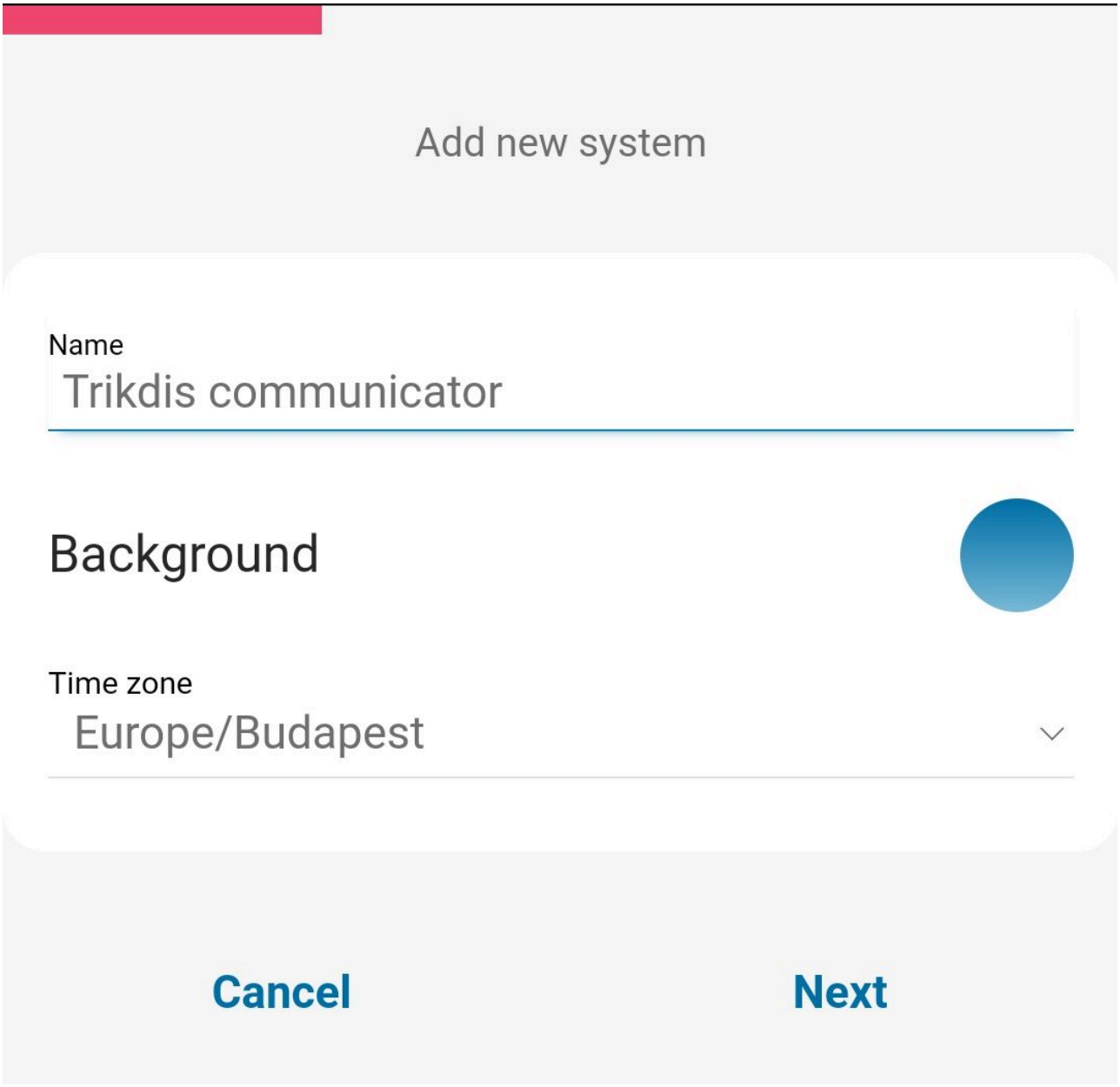
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



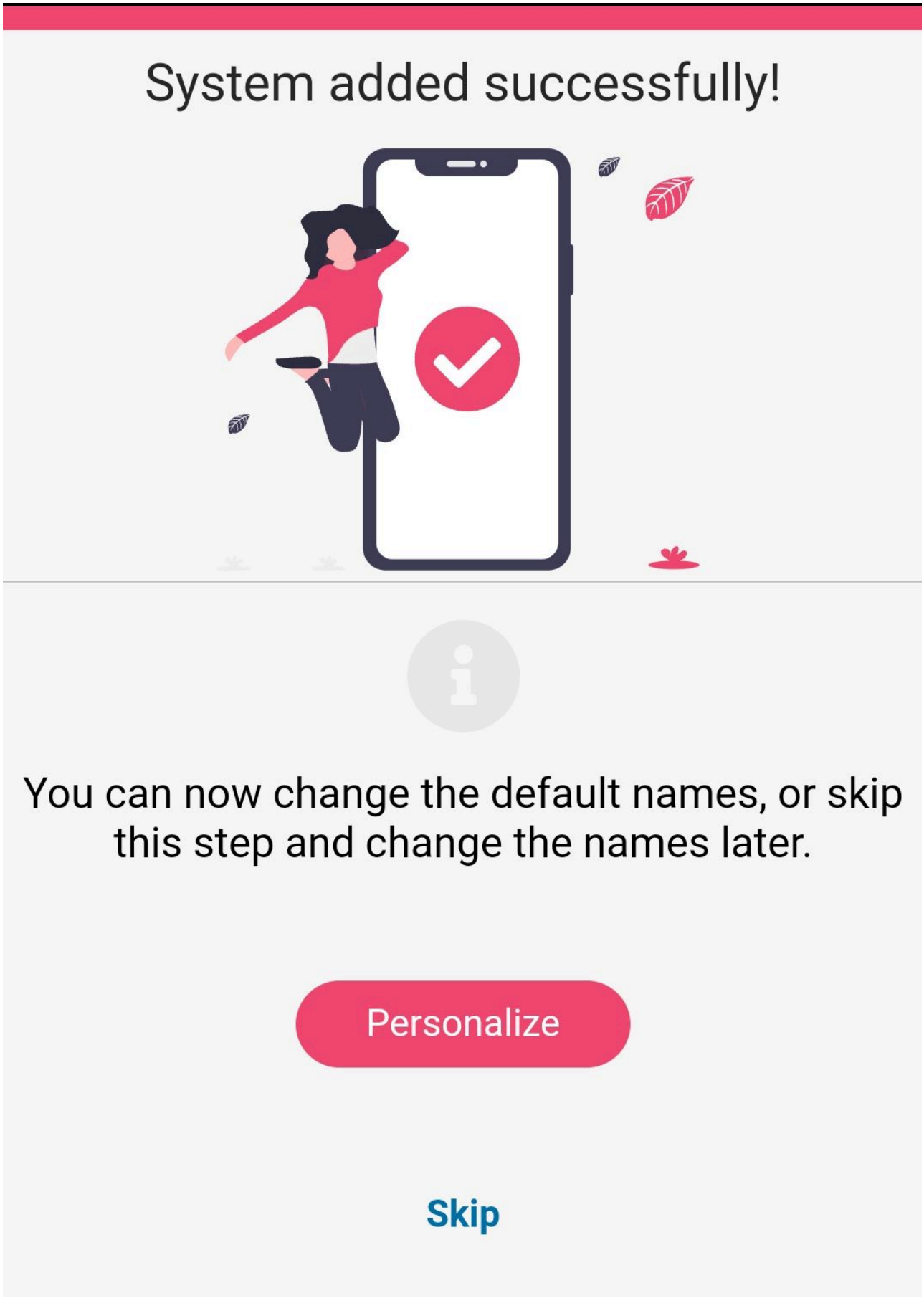
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



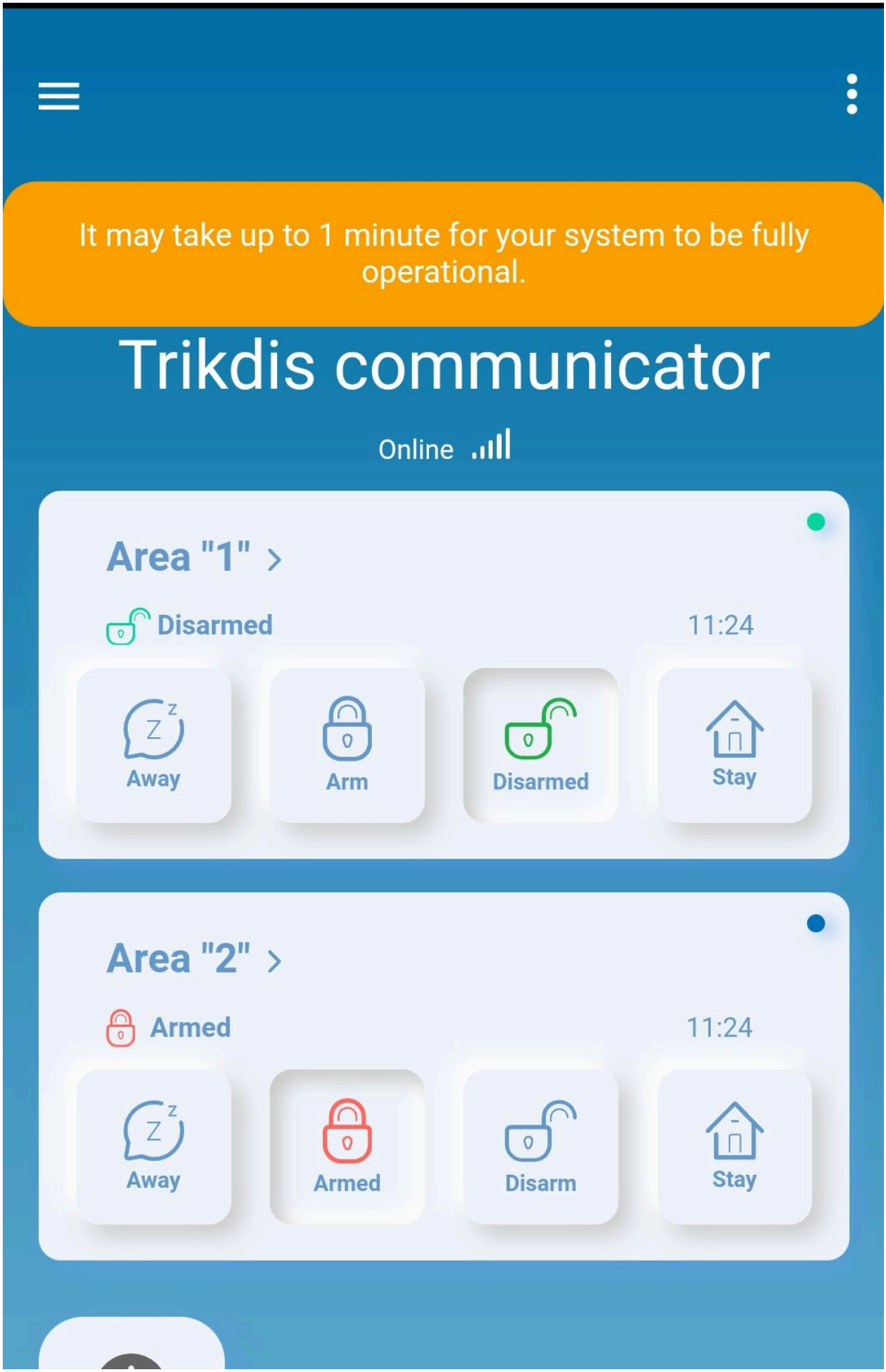
6. Add meg a rendszer nevét és válassz idozónát



7. A rendszered elkészült, a következő lépésnél még elnevezheted a partíciókat és zónákat, de ezt később bármikor megteheted.



8. Az utolsó lépésben megjelenik a rendszered kezdőképernyője. Várd meg, amíg eltűnik a sárga csík és a rendszered elkészült.


It may take up to 1 minute for your system to be fully operational.
Trikdis communicator
Online
Area "1" >
Disarmed
11:24
Away
Arm
Disarmed
Stay
Area "2" >
Armed
11:24
Away
Armed
Disarm
Stay



With the GATOR, pay attention to these when adding it:

1. The unique ID is the GATOR's **IMEI** number: it is on the sticker on the bottom of the device and on the box, and you also see it in the TrikdisConfig status bar; you can also scan the QR code of the sticker with the phone's camera. If the installer has changed the default `123456` value of the **Cloud Access Code**, the app asks for it too.
2. After entering the name of the system, you can skip the **Personalize** step with the **Skip** button: you can rename the outputs and inputs later as well.
3. Wait until the text with the yellow background disappears – the system becomes operational within 1 minute at most.

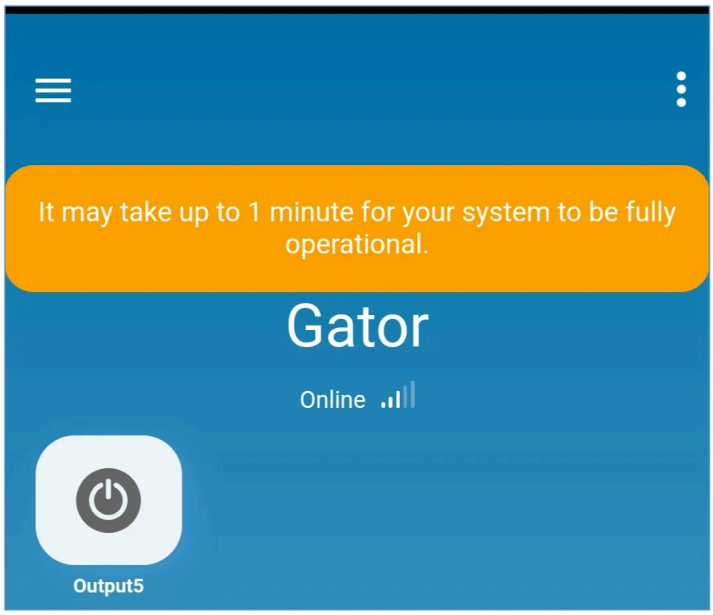


Figure 21. The GATOR in Protegus 2 after adding it: the system is **Online**, the yellow bar indicates that you have to wait up to 1 minute until full operation.

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

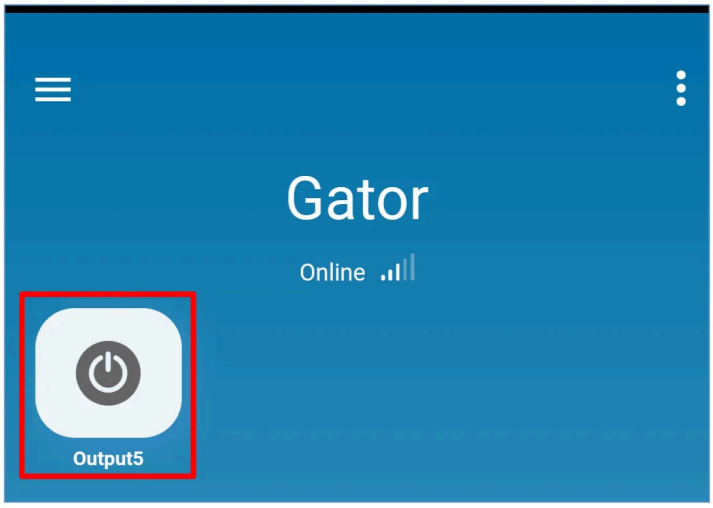


Figure 22. The home screen of the system with the **Output5** button – this switches the GATOR's relay.

See also

The GV17 gate automation device can be used with Protegus 2 · Protegus Android / iPhone and web app · Browser push notifications in the Protegus 2 app

4.4 Widget on the phone's home screen

You can also put the gate opener button on the phone's home screen, so you open with one touch, without opening the app. It **only works on Android**; the way of placing the widget may differ slightly from phone to phone. The GATOR 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 be controlled (for example **Gator Output5**) and press the **ADD WIDGET** button.
4. The button appears on the home screen. Try it: go back to the home screen and press the button – after pressing it, a round indicator shows that the output has switched on; with the gate state wired, the colour of the button shows the open and closed state of the gate.



Figure 23. Step 1 – the **Widgets** menu item after touching and holding the home screen.

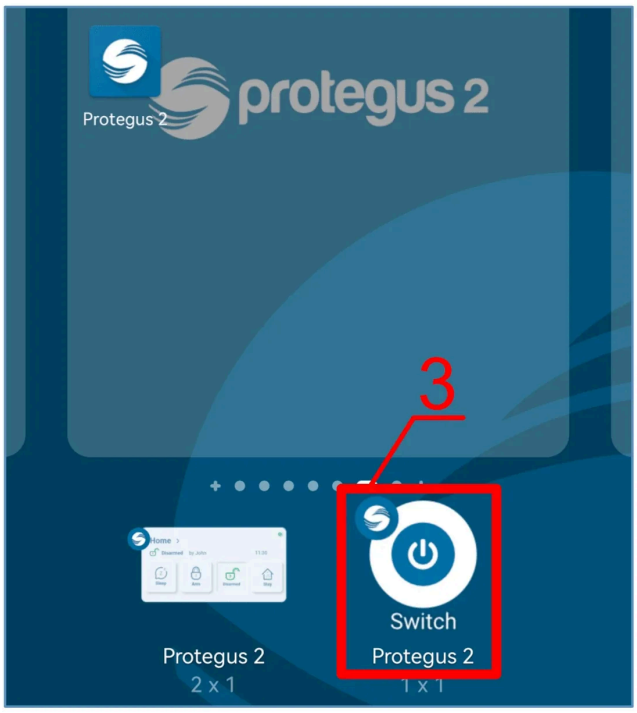


Figure 24. Step 2 – **Switch Protegus 2** among the Protegus 2 widgets.



Figure 25. Step 3 – selecting the **Gator Output5** output and the **ADD WIDGET** button.



Figure 26. Step 4 – the **Output5** widget on the home screen; the green button shows the switched-on output (open gate).

4.5 Managing users in the app

As administrator you can also add and delete users in Protegus 2; the added user sees and opens the gate from their own account, and can also receive notifications by SMS (if the **HELLO** welcome message is switched on, they get an SMS about being added).

1. Start the Protegus 2 app on your phone and log in with your username and password. On the system's screen open the **Settings** menu, then **System configuration**.
2. Choose the **Users** list and press the **+** (**Add new user**) button.
3. Enter the user's **e-mail address**, **name** and **phone number** (or the RFID card number, section 5.6), for a code reader their 4-digit **code**, 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.

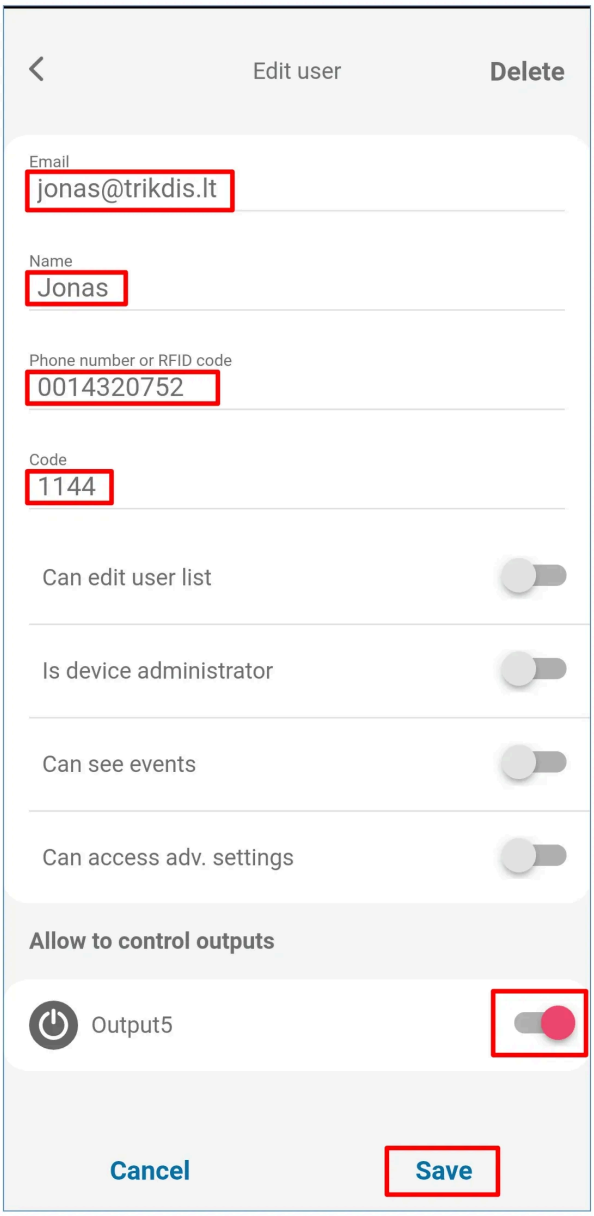


Figure 27. Editing a user in Protegus 2: e-mail address, name, phone number or RFID card number, code, and permission to control **Output5**.

4.6 Control by SMS message

You switch the relay output (**OUTPUT5**) with these SMS commands; `xxxxxx` is the 6-digit administrator password (default `123456`). You can also switch other outputs by SMS, but they must first be set as outputs in TrikdisConfig (section 5.3).

Command	Parameter	Description
`OUTPUTx xxxxxx ON`	ON	switching on the output; **x** is the number of the output. Example: `OUTPUT5 123456 ON`
`OUTPUTx xxxxxx OFF`	OFF	switching off the output. Example: `OUTPUT5 123456 OFF`
`OUTPUTx xxxxxx PULSE=ttt`	PULSE=ttt	switching on the output for **ttt** seconds (1–999, with three digits). Example: `OUTPUT5 123456 PULSE=002`

4.7 Programming by SMS

The device only accepts SMS commands from the **administrator** numbers (1A–7A); every command contains the 6-digit administrator password. The device sends a reply SMS about the execution if **ACK for SMS message** is switched on for the administrator (section 5.6).

Changing the administrator password – for security reasons this should be the first thing you do:

```
PSW 123456 xxxxxx
```

`123456` – the default password; `xxxxxx` – the new, 6-character password.

Only authorized users may control – send the users' data from the administrator's phone:

```
SETU xxxxxx +PHONENO#NAME#EMAIL
```

`PHONENO` – the user's phone number in international format (+CC…, where CC is the country code); `NAME` – their name; `EMAIL` – their e-mail address (for Protegus 2). After the first number has been added, the GATOR only reacts to calls from numbers on the list.

Administrator rights for someone else – the additional administrators receive the system messages and can add users:

```
SETA xxxxxx Nox=+PHONENO#NAME#EMAIL
```

`Nox` – the administrator's position in the list (1–7); if you write **1**, you hand over your own administrator rights.

List of SMS commands (in each of them the password follows the command word; in the examples the default `123456`):

Command	Parameter	Description
`INFO`	–	data about the device: type, IMEI, signal strength, supply voltage, firmware version, serial number, date and time. Example: `INFO 123456`
`ASKI`	–	state of the inputs. Example: `ASKI 123456`
`ASKO`	–	state of the outputs. Example: `ASKO 123456`
`SETA`	`NoX=phone number#name#e-mail`	adding an administrator in position X (1A–7A); the number must start with + and the country code, the fields are separated by #. Example: `SETA 123456 No3=+CC123456789#John#john@example.com`
`SETA`	`NoX=DEL`	deleting administrator X. Example: `SETA 123456 No2=DEL`
`SETU`	`phone number#name#e-mail`	adding a new user (positions 11–1010); here too the number must start with + and the country code, the fields are separated by #. Example: `SETU 123456 +CC123456789#Peter#peter@example.com`
`DELU`	`phone number` or `name`	deleting a user by phone number or name. Example: `DELU 123456 +CC123456789`, `DELU 123456 Peter`
`SETB`	`e-mail` or `phone number`	adding to the blacklist (e-mail address or phone number). Example: `SETB 123456 john@example.com`, `SETB 123456 +CC123456789`
`DELB`	`ALL`	deleting the whole blacklist. Example: `DELB 123456 ALL`

Command	Parameter	Description
`DELB`	`e-mail` or `phone number`	deleting one entry from the blacklist (for an e-mail address upper and lower case matter). Example: `DELB 123456 john@example.com`, `DELB 123456 +CC123456789`
`RESET`	–	restarting the device. Example: `RESET 123456`
`PSW`	`new password`	changing the administrator password. Example: `PSW 123456 654123`
`TXTA`	`object name`	setting the name of the object. Example: `TXTA 123456 Home`
`TXTE`	`N1=text` … `N5=text`	text of the SMS sent when the input or output is activated; N1…N5 is the number of the terminal. Example: `TXTE 123456 N1=Gate open`
`TXTR`	`N1=text` … `N5=text`	text of the SMS sent on restore. Example: `TXTR 123456 N5=Relay off`
`SETD`	`IDx=yy`	inactivity time of input x in minutes (0–2880): after activation the device notifies and does not react to further changes of the input for this time; 0 = disabled. Example: `SETD 123456 ID1=30`
`RESD`	`IDx`	clearing the already running inactivity time of input x. Example: `RESD 123456 ID1`
`TIME`	`YYYY/MM/DD,HH:MM:SS`	setting the date and time. Example: `TIME 123456 2026/10/30,12:23:00`
`RDR`	`phone number#text`	forwarding an SMS to the given number (for example a balance top-up to the operator). Example: `RDR 123456 +CC123456789#Topup 10 EUR`
`HELLO`	`ON` / `OFF`	SMS notification of the new user about being added (for a user added from the app or by SMS) on / off. Example: `HELLO 123456 ON`
`NATH`	`ON` / `OFF`	switching the **Not authorized** mode (anyone can call) on and off without changing the other settings; with several outputs, by listing the outputs switched on a call (it switches on the **Not authorized** mode and the listed outputs, and switches off the other outputs). Example: `NATH 123456 ON`, `NATH 123456 ON=5,7,22`, `NATH 123456 OFF`
`UUSD`	`*code#`	sending a USSD code to the mobile operator (balance query, top-up). Example: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON` / `Protegus=OFF`	connecting to the Protegus cloud, or disconnecting from it. Example: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`APN=name`, `USER=name`, `PSW=password`	APN name, username and password of the mobile data connection. Example: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`Code=password`	changing the access code of the Protegus cloud (**Cloud Access Code**). Example: `CONNECT 123456 Code=123456`

Replace the country code (CC) and the e-mail address in the examples with your own data. In the SMS, avoid accented and special letters if the **System Options** → **Text language** setting is not set to the matching character set (section 5.2). The list of APNs: APN settings – list of European mobile operators.

5. Setup with the TrikdisConfig software

All settings of the GATOR are available with the Windows program called **TrikdisConfig** – over a USB cable or remotely (chapter 6). With the default settings the device opens on a call (chapter 2); you need the software when you set up users, RFID cards, schedules, SMS texts, modules, the Protegus cloud or the monitoring

station.

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 GATOR's front cover with a flat screwdriver as shown in the figure.
2. Connect the GATOR to the computer with a **USB Mini-B** cable.
3. Start TrikdisConfig. The software recognizes the device and opens the GATOR's programming window.
4. Click the **Read [F4]** button: the software reads the device's current settings. If it asks for it, enter the 6-digit **administrator** or **installer** code in the pop-up window (the default administrator code is `123456`).



Figure 28. Removing the front cover: insert the screwdriver into the side opening and move it downwards, and the cover snaps off; underneath is 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 in the lower left part of the programming window takes you back to the default settings (section 5.9).

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.

Label	Meaning
SN	Serial number.
BL	The bootloader version.
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.



Figure 29. The GATOR's status bar: in the left field the **IMEI/Unique ID**, at the bottom **Status: reading done**, **Device: GV17_2200** (the type code), the serial number, the **BL** and **FW** version, the connection mode (USB). For the GATOR the **Device** field must be in the form **GV17_xxxx**.

5.2 “System Options” page

The general settings of the device: ID, time, administrator code, call handling, test, SIM card and time zone.

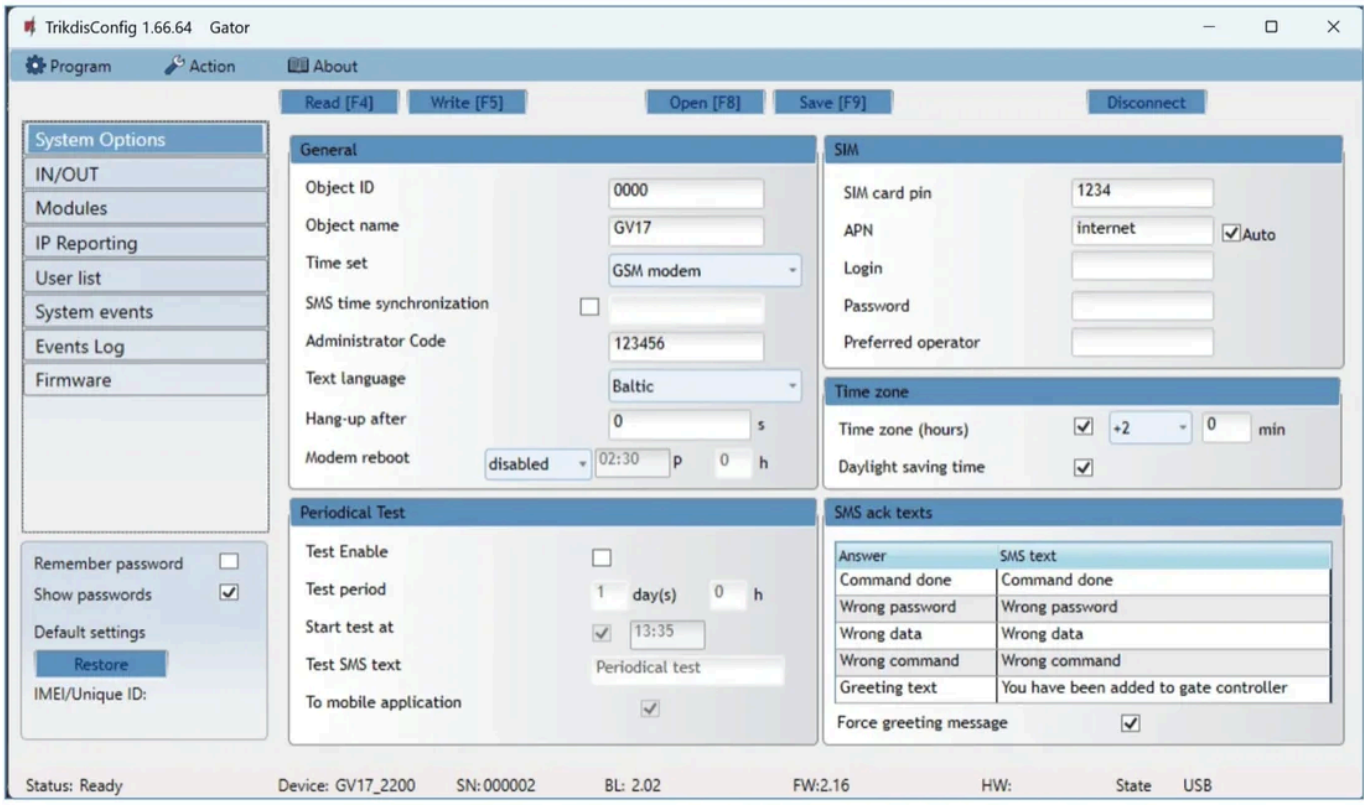


Figure 30. TrikdisConfig – **System Options**: the **General**, **Periodical test**, **SIM**, **Time zone** and **SMS ack texts** groups.

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.
- **Object name** – the device sends every event with this name.
- **Time set** – the source of time synchronization (for example the mobile network).
- **SMS time synchronization** – tick it and enter the number of the GATOR's SIM card in international format (+CC..., where CC is the country code) if it synchronizes the time by SMS.
- **Administrator Code** – the administrator code: with it every parameter of the GATOR can be changed (default `123456` – change it).
- **Text language** – the character set of the SMS messages.
- **Hang-up after** – at 0 the device rejects the call (opens on a call); at any other value it answers the call and ends it after the given number of seconds – for keypad (DTMF) control (section 4.2).
- **Modem reboot** – daily restart of the modem at a set time.

Periodical test group

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

SIM group

- **SIM card PIN** – the PIN code of the SIM card, if you have not switched off the PIN request.
- **APN** – the access point of the mobile data connection. With the **Auto** checkbox the device chooses an APN from the built-in list (data of several international and national operators), and only uses the value written in the field if it does not find the operator. If the data connection is not established, enter the operator's APN: APN settings – list of European mobile operators.
- **Login**, **Password** – the username and password of the APN, if the operator requires them.
- **Preferred operator** – if you enter an operator code (MCC + MNC), the GATOR only connects to that network; this matters for international (roaming) SIM cards.

Time zone group – here you set the exact time of the country: enter the time zone and mark whether the country uses daylight saving time.

- **Time zone (hours)** – tick it and enter the country's time zone (for example Central European Time: +1).
- **Daylight saving time** – tick it if the country uses daylight saving time.

SMS ack texts group – the texts of the reply SMS messages that the user receives after the SMS commands.

- **Force greeting message** – when ticked, the device sends a greeting SMS to a new user added by SMS or from Protegus 2 (by SMS, `HELLO 123456 OFF` switches it off).

5.3 “IN/OUT” page

The settings of the inputs and outputs, the RFID readers and the time and attendance record, on three tabs: **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 IN/OUT tab – the inputs and outputs

In the table each row is one terminal; here you decide which is an input and which an output, and how it should report.

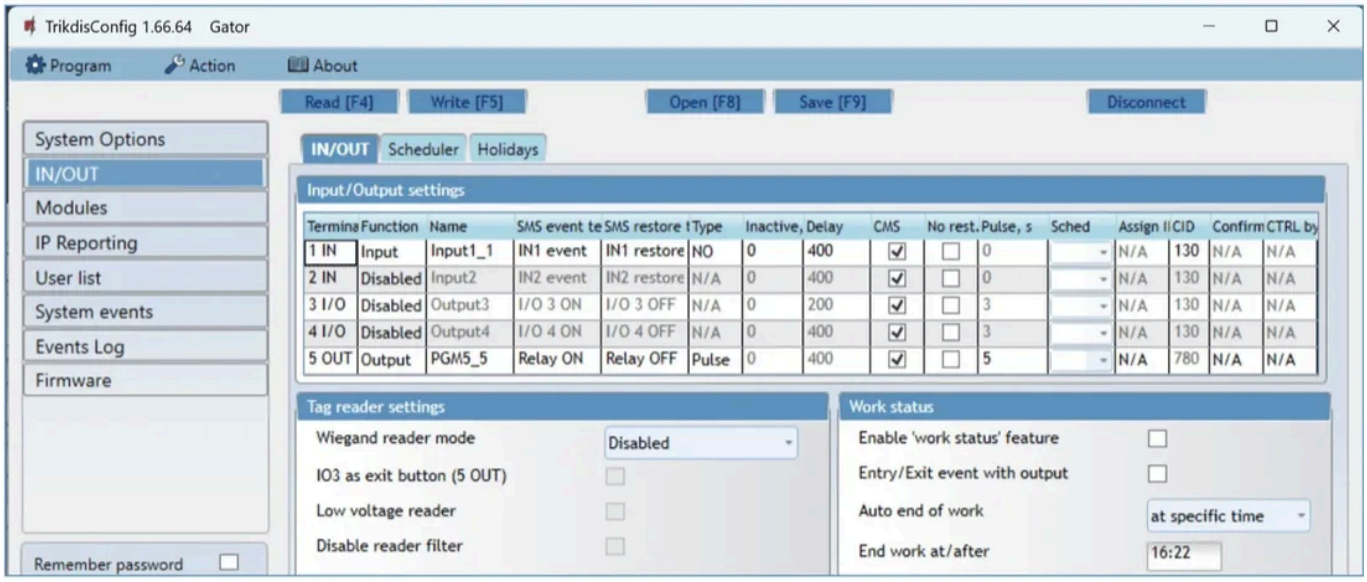


Figure 31. TrikdisConfig – **IN/OUT**: the **Input/Output settings** table (by default the 1 IN input, 2 IN, 3 I/O, 4 I/O disabled, 5 OUT an output of **Pulse** type), below it the **Tag reader settings** and **Work status** groups.

Input/Output settings group

- **Terminal** – the number of the GATOR's terminals (1 IN … 5 OUT; the expanders' terminals at the end of the list).
- **Function** – the function of the terminal: **Input**, **Output** or **Disabled**.
- **Name** – the name of the input or output (this is how it appears in the app and in the SMS messages).
- **SMS event text** – the text of the SMS sent on activation.
- **SMS restore text** – the text of the SMS sent on restore.
- **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 = disabled.
- **Delay** – the reaction time of the input in milliseconds (default 400 ms).
- **CMS** – when ticked, the event goes to the monitoring station and also 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 (default 3 s on 5 OUT; for the 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 state of the output, the app shows the actual state of the input (the gate) (section 5.10).
- **CID** – the Contact ID code of the event.
- **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 – the settings of the RFID readers (wiring in section 3.6)

- **Wiegand reader mode** – the number of connected Wiegand readers: **Single Reader** or **Dual Reader**.

- **IO3 as exit button (5 OUT)** – tick it if the exit push button is connected to the 3 I/O terminal: when it is pressed, 5 OUT switches on for the set pulse time.
- **Low voltage reader** – for a low-voltage reader (5 V signal level).
- **Disable reader filter** – switches off the internal filter of short pulses if the device does not recognize the reader's signals.

Work status group – time and attendance record in Protegus 2 (details: GV17 – access control and/or time and attendance system)

- **Enable "work status" feature** – switches on the indication of the work status in the app.
- **Entry/Exit event with output** – when ticked, an entry / exit event is also created when the output is switched remotely.
- **Auto end of work** – the mode of automatically closing the working time.
- **End work at/after** – the time of closing or the time until closing, depending on the previous setting.

5.3.2 Scheduler tab – scheduling the outputs

The outputs can also switch by themselves according to a schedule (for example the gate open during working hours, closed in the evening). You assign the schedule in the **Sched** column of the output.

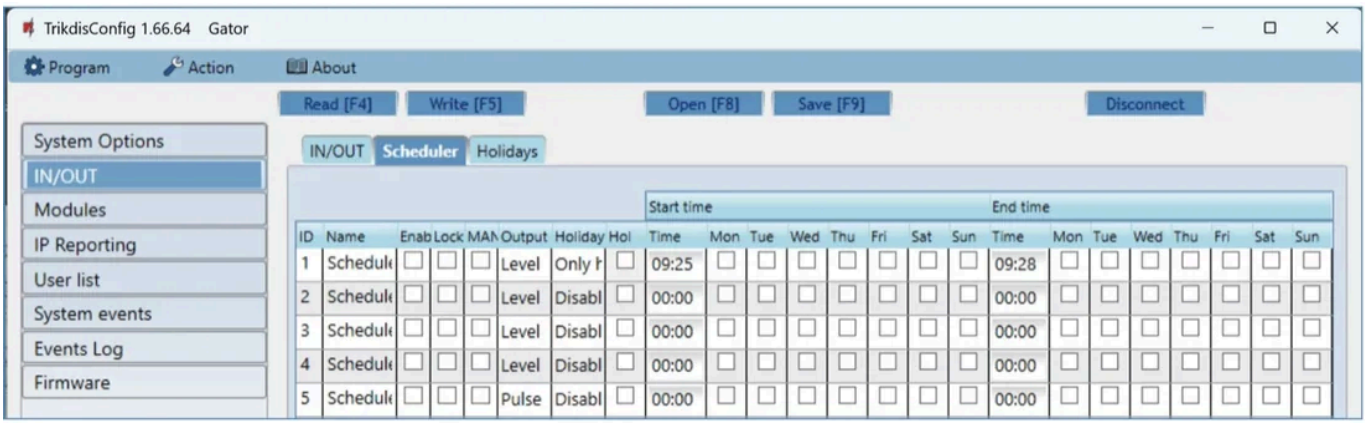


Figure 32. TrikdisConfig – IN/OUT, **Scheduler** tab: for each schedule enabling, locking, output mode, holiday mode, start and end time with the days of the week.

- **Name** – the name of the schedule.
- **Enable** – enabling the schedule.
- **Lock** – when ticked, the output cannot be switched in any other way (by call, from the app) 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 on the output.
- **Output mode** – the operation of the output during the schedule: **Level** – the output is on during the whole set period; **Pulse** – the output switches for the set pulse time at the start and at the end of the schedule.
- **Holiday mode** – how the schedule should work on a holiday; **Hol** – tick it if on holidays it uses the holiday times.
- **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 set, the output switches off at the set time if it was on until then.

5.3.3 Holidays tab – holidays

Here you enter the calendar days on which the schedule works with the holiday times.

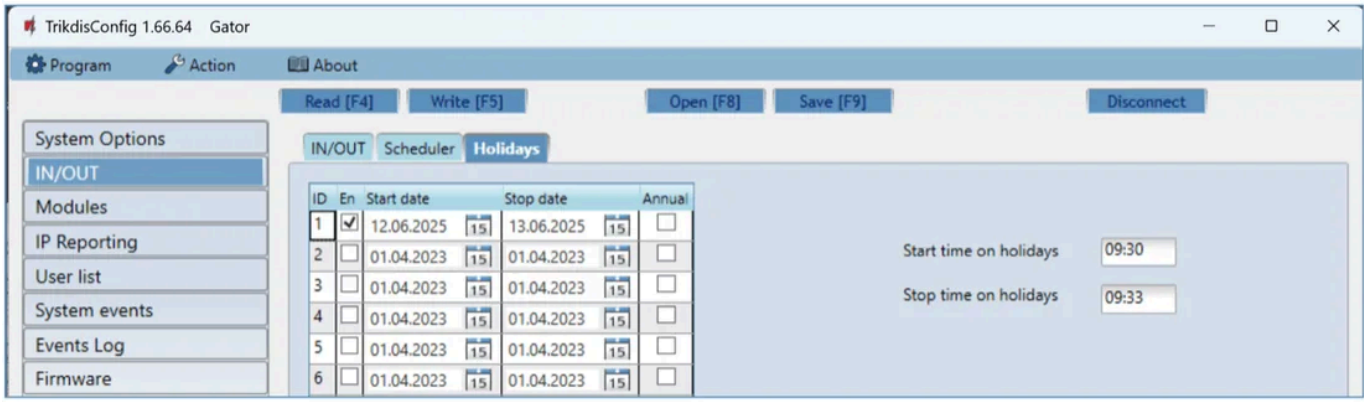


Figure 33. TrikdisConfig – IN/OUT, **Holidays** tab: holiday periods with start and end date, with the holiday start and end time.

- **En.** – enabling the holiday period.
- **Start date**, **Stop date** – the first and last day of the period.
- **Annual** – a holiday repeated every year: the device only looks at the month and the day.
- **Start time on holidays**, **Stop time on holidays** – the holiday start and end time.

5.4 “Modules” page

5.4.1 Modules tab

These modules can be connected to the GATOR on the RS485 bus or by radio: **W485** Wi-Fi module, **E485** Ethernet module, **iO-LORA** wireless expander (through the RF-LORA transceiver, up to 8; the RFID readers connected to the iO-LORA expanders can thus switch up to 8 more outputs, a reader always switches only one output of its own expander – from GATOR firmware 2.13, section 3.9), **iO8** wired and **iO8-LORA** wireless expander (through the RF-LORA; one of the two in total). The RF-LORA transceiver does not need to be added to the list. If there is Wi-Fi or wired internet at the site, with the W485 or E485 module the GATOR sends the messages over the internet to the Protegus cloud and the monitoring station: no mobile data is used (the SIM card's data traffic can even be disabled), and the GATOR can even be used without a SIM card, controlled only from the app.

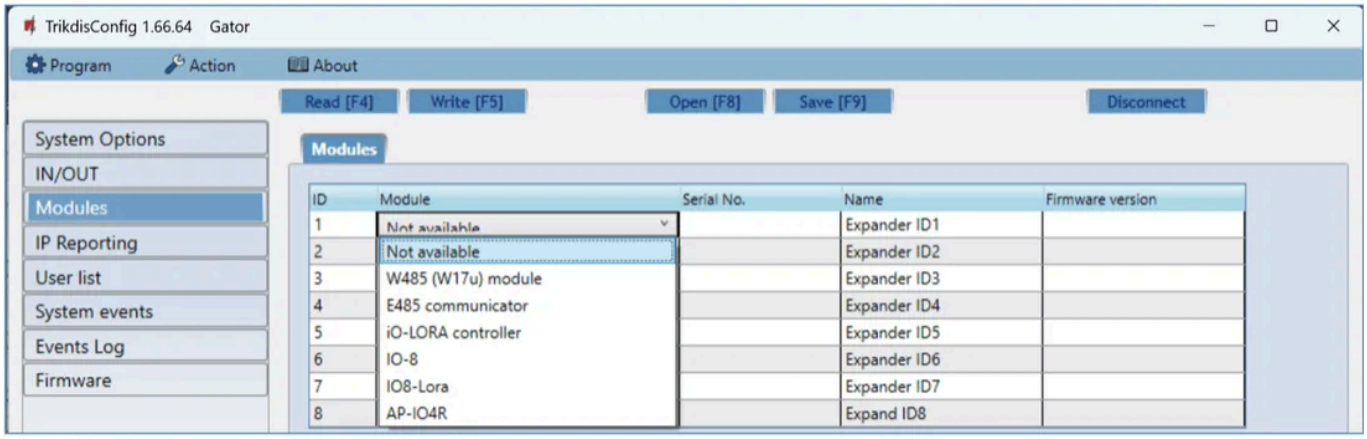


Figure 34. TrikdisConfig – **Modules**: in the **Module** drop-down list the W485, E485, iO-LORA, iO8, iO8-LORA and **AP-IO4R** (iO4R) modules; next to it the **Serial No.**, **Name** and **Firmware version** columns.

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

After selecting the module and entering the serial number, the **Parameters** tab with the module's own settings appears.

iO4R relay expander

The **AP-IO4R** in the list is the **iO4R** relay expander: it is used for monitoring and remotely bypassing the safety sensors of the gate automation, and for counting the gate cycles. It is set up in the Protegus 2 app, in the **Advanced Gator Monitoring** mode that can be selected when the gate controller is added – see the iO4R manual.

5.4.2 Parameters tab – W485 Wi-Fi module

After selecting the W485, here you enter the data of the Wi-Fi network and the way the SIM card is used.

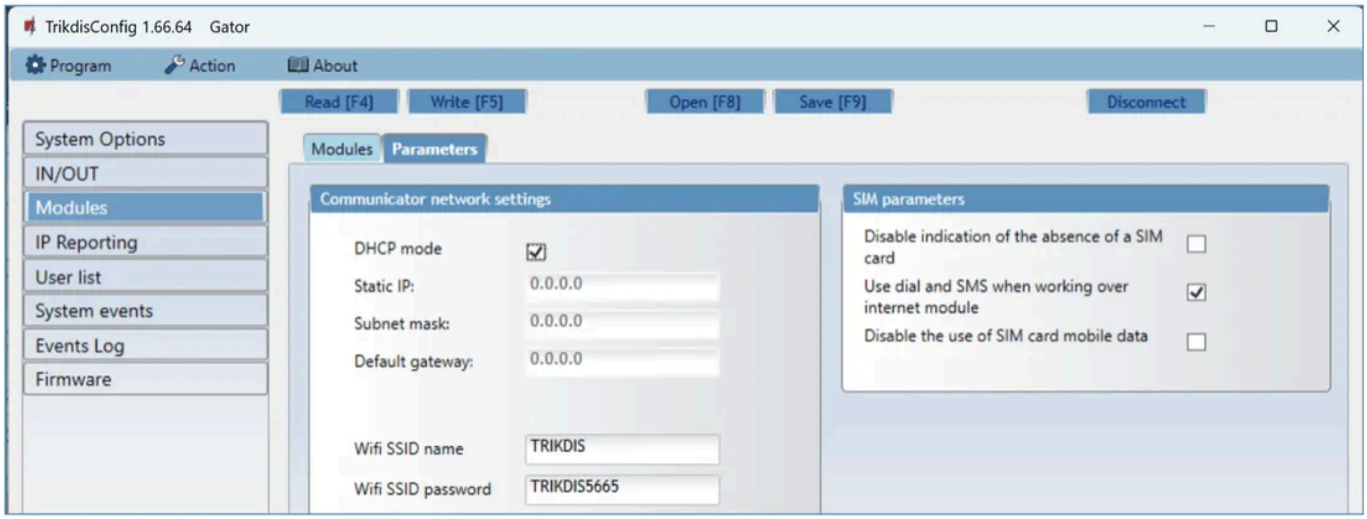


Figure 35. TrikdisConfig – Modules, **Parameters** tab for the W485: **Communicator network settings** (DHCP, IP address, Wi-Fi network name and password) and **SIM parameters**.

Communicator network settings group

- **DHCP mode** – when ticked, the module automatically gets the network settings (IP address, subnet mask, gateway) from the router; when empty, you enter them manually.
- **Static IP**, **Subnet mask**, **Default gateway** – the fixed IP address, the subnet mask and the gateway address for manual setup.
- **Wifi SSID name** – the name of the Wi-Fi network the W485 connects to (2.4 GHz network).
- **Wifi SSID password** – the password of the Wi-Fi network.

SIM parameters group

- **Disable indication of the absence of a SIM card** – when ticked, the device does not indicate a missing SIM card as a fault (for use without a SIM, over the internet only).
- **Use dial and SMS when working over internet module** – when ticked, control by call and SMS also works alongside the module. When empty, as long as the internet connection is alive, the device does not use calls and SMS; if the internet is lost, calls and SMS work again, and the device sends an SMS to the users.
- **Disable the use of SIM card mobile data** – when ticked, the device does not use the SIM card's mobile data; the data only goes through the W485. If the Wi-Fi is lost, the device stores the events and sends them when the connection returns.

5.4.3 Parameters tab – E485 Ethernet module

After selecting the E485, here you enter the data of the wired network and the way the SIM card is used.

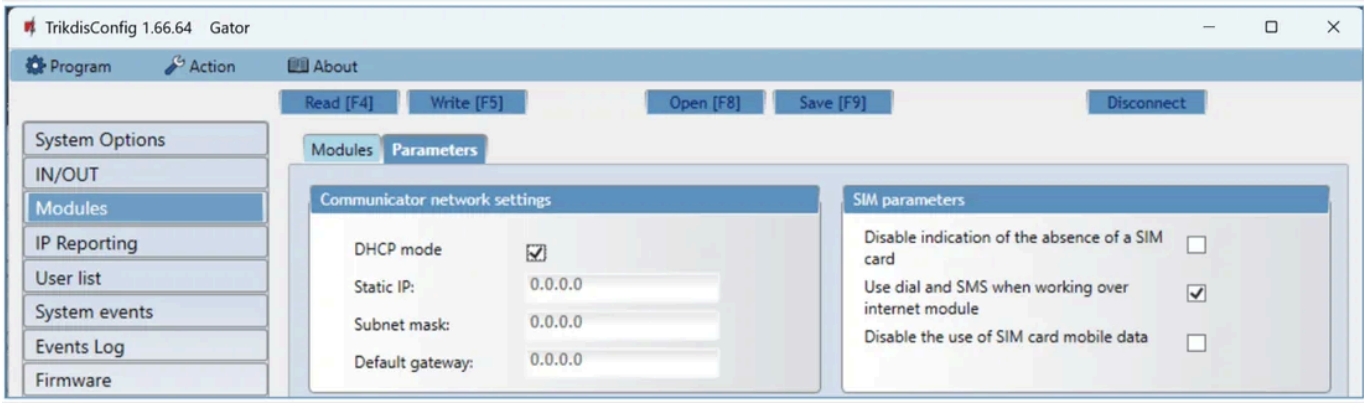


Figure 36. TrikdisConfig – Modules, **Parameters** tab for the E485: network settings (DHCP or fixed IP address) and **SIM parameters**.

- **DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway** – the same as for the W485: automatic or manual network setup.
- **SIM parameters** – the three checkboxes mean the same as described for the W485; with mobile data disabled, the data only goes through the E485, and while the internet is down the device stores the events.

5.5 “IP Reporting” page

The GATOR sends the events to the monitoring station's IP receiver and to the Protegus cloud; you switch on the cloud on this page.

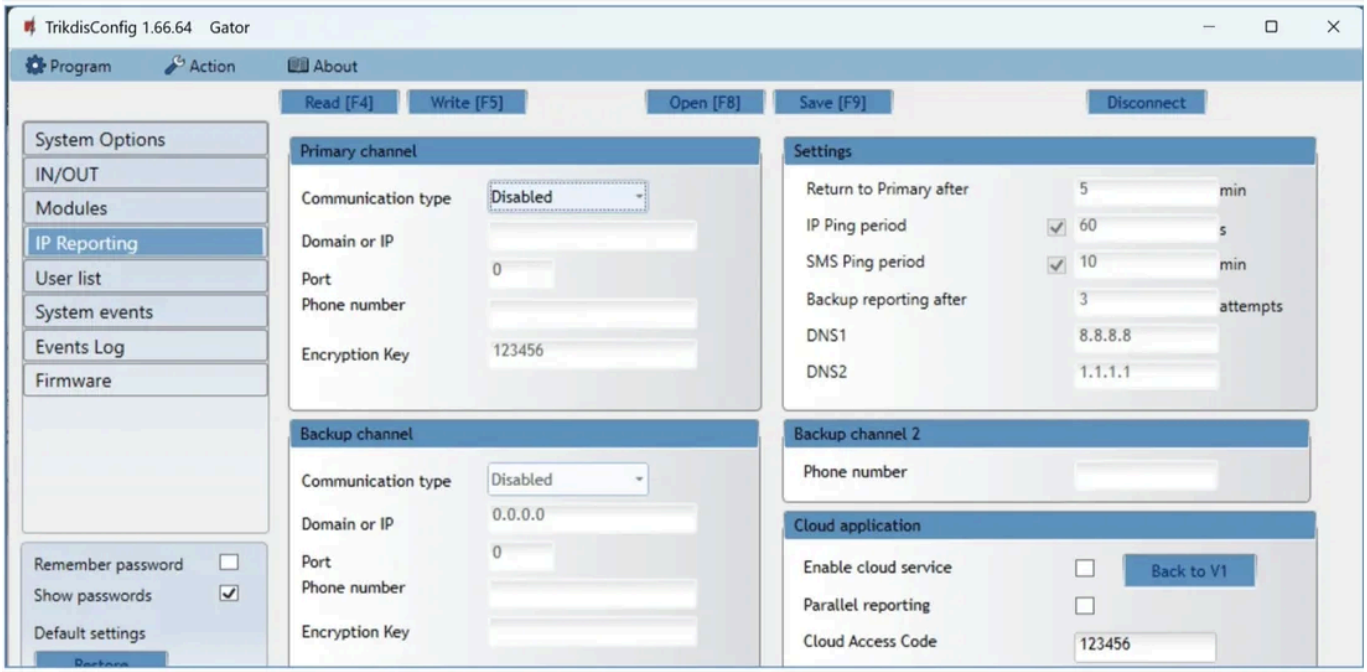


Figure 37. TrikdisConfig – **IP Reporting**: **Primary channel** and **Backup channel** (disabled by default), **Settings**, the backup SMS channel and the **Cloud application** group with the **Enable cloud service** checkbox and the **Cloud Access Code**.

Primary channel group

- **Communication type** – the type of connection with the monitoring station's receiver: **IP** or **SMS**; **Disabled** = no reporting.
- **Domain or IP** – the domain name or IP address of the receiver.
- **Port** – the network port of the receiver.
- **Phone number** – the phone number of the monitoring station's SMS receiver (+CC…), if the type is SMS.
- **Encryption Key** – 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.

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.
- **SMS Ping period** – the same on the SMS channel.
- **Backup reporting after** – after this number of unsuccessful attempts the device switches to the backup channel.
- **DNS1**, **DNS2** – the IP addresses of the name servers.

Backup channel 2 group

- **Phone number** – the number of the monitoring station's SMS receiver. The device sends an SMS here if the message cannot be sent on either the primary or the backup IP channel; it also works if the IP connection drops in the mobile operator's network. It is only active if both IP channels are on the mobile network; the SMS receiver gets a message when the device is first switched on and when the TCP/IP or UDP/IP connection is lost.

Cloud application group

- **Enable cloud service** – switching on the Protegus cloud: the GATOR communicates with the app and can also be programmed remotely with TrikdisConfig (chapter 6).
- **Parallel reporting** – when ticked, the events go to the monitoring station, to Protegus 2 and to the users at the same time; when empty, the app and the users only receive them after the monitoring station's acknowledgement.
- **Cloud Access Code** – 6-digit code for connecting to Protegus 2 (default `123456`); 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 administrators and users, registration of RFID cards, the user schedules and the blacklist – on four tabs.

5.6.1 Users tab – the users

In the table each row is one administrator or user with their permissions.

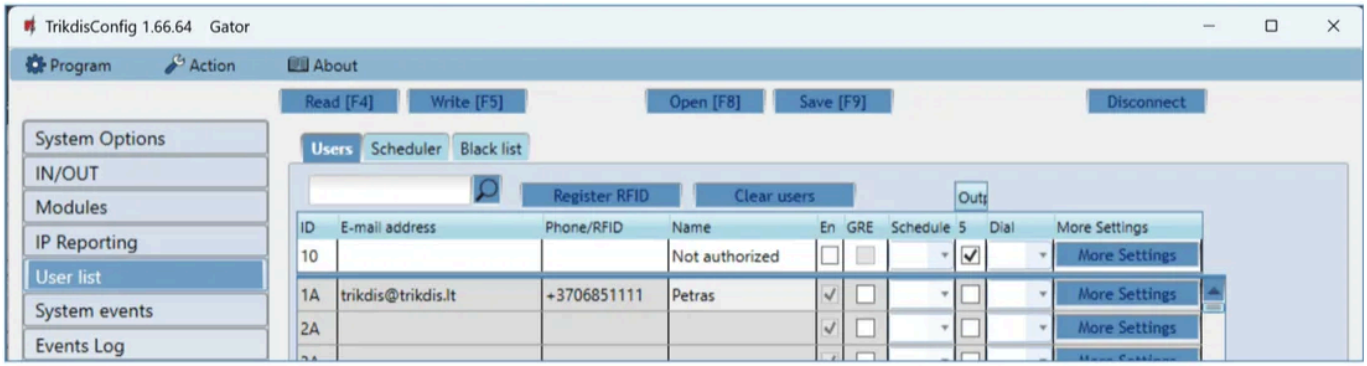


Figure 38. TrikdisConfig – **User list**, **Users** tab: at the top the **Register RFID** and **Clear users** buttons; in the table the **ID**, **E-mail address**, **Phone/RFID**, **Name**, **En**, **GRE**, **Schedule**, **Dial** columns and the **More settings** button; row 10 is the **Not authorized** entry.

- **ID** – the user's position number. The rows with the letter **A** (**1A–7A**) are the administrators: they can set up the device, switch the outputs, and they receive the messages. The rows numbered **11–1010** are the users: they can only switch the outputs.
- **E-mail address** – the user's e-mail address (for Protegus 2).
- **Phone/RFID** – the phone number in international format (+CC…) or the ID number of the RFID card.
- **Name** – the user's name.
- **En** – enabling the user: when ticked, the user can switch the outputs.
- **GRE** – sending a greeting SMS to the user.
- **Schedule** – the number of the schedule according to which the user may control (section 5.6.3).
- **Output** – the output(s) the user can control.
- **Code** – for a code (keypad) Wiegand reader, the user's code.
- **Dial** – the output(s) switched on a call, if the user has several outputs; after switching, the device ends the call.
- **More settings** – the window of further settings (below).

Row 10, “Not authorized”

If the **En** checkbox **is ticked** for the user no. 10 called **Not authorized**, the GATOR can be controlled by call **from any phone number**. If it is empty, only those on the list can call; each user switches the output marked in their own **Dial** column. By SMS the same is set by the `NATH` command (section 4.7).

After the 2G network is shut down, some mobile operators may not allow 4G voice calls (VoLTE) for the Quectel EG915U-EU modem we use. In that case, opening the gate by phone call and call notifications do not work. SMS and the data connection (Protegus 2 app) are not affected by this restriction and keep working.

More settings – administrator (1A–7A)

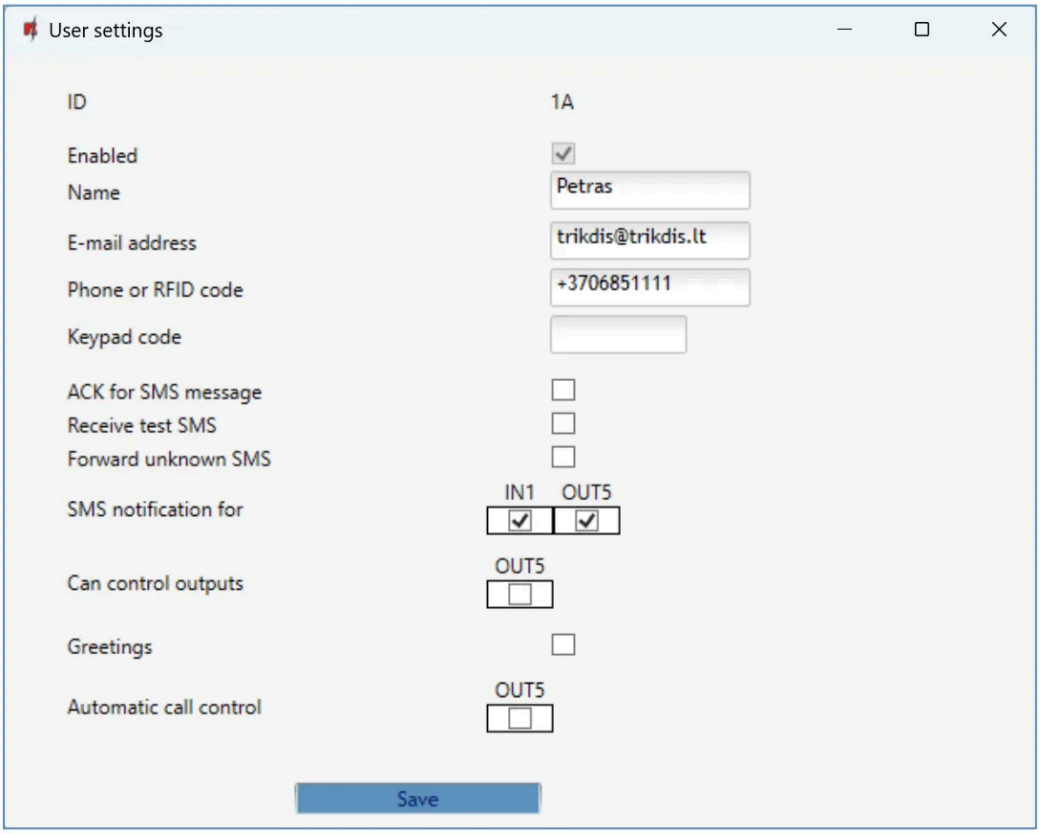


Figure 39. TrikdisConfig – **User settings** for an administrator: **Enabled**, the data, **ACK for SMS message**, **Receive test SMS**, **Forward unknown SMS**, **SMS notification for** (IN1, IN2, OUT3, OUT4, OUT5), **Can control output**, **Greetings** and **Automatic call control**.

- **ID**, **Enabled**, **Name**, **E-mail address**, **Phone or RFID code**, **Keypad code** – the data corresponding to the columns of the list.
- **ACK for SMS message** – the administrator receives a reply SMS about the execution of the SMS commands.
- **Receive test SMS** – receives the periodic test SMS.
- **Forward unknown SMS** – the device forwards to them the SMS messages arriving from an unknown number (for example the operator's balance notification).
- **SMS notification for** – about the changes of which events (IN1, IN2, OUT3, OUT4, OUT5) they receive an SMS.
- **Can control output** – the outputs they can control.
- **Greetings** – sending a greeting SMS.
- **Automatic call control** – the outputs switched on their call, after which the device ends the call.

More settings – user (11–1010)

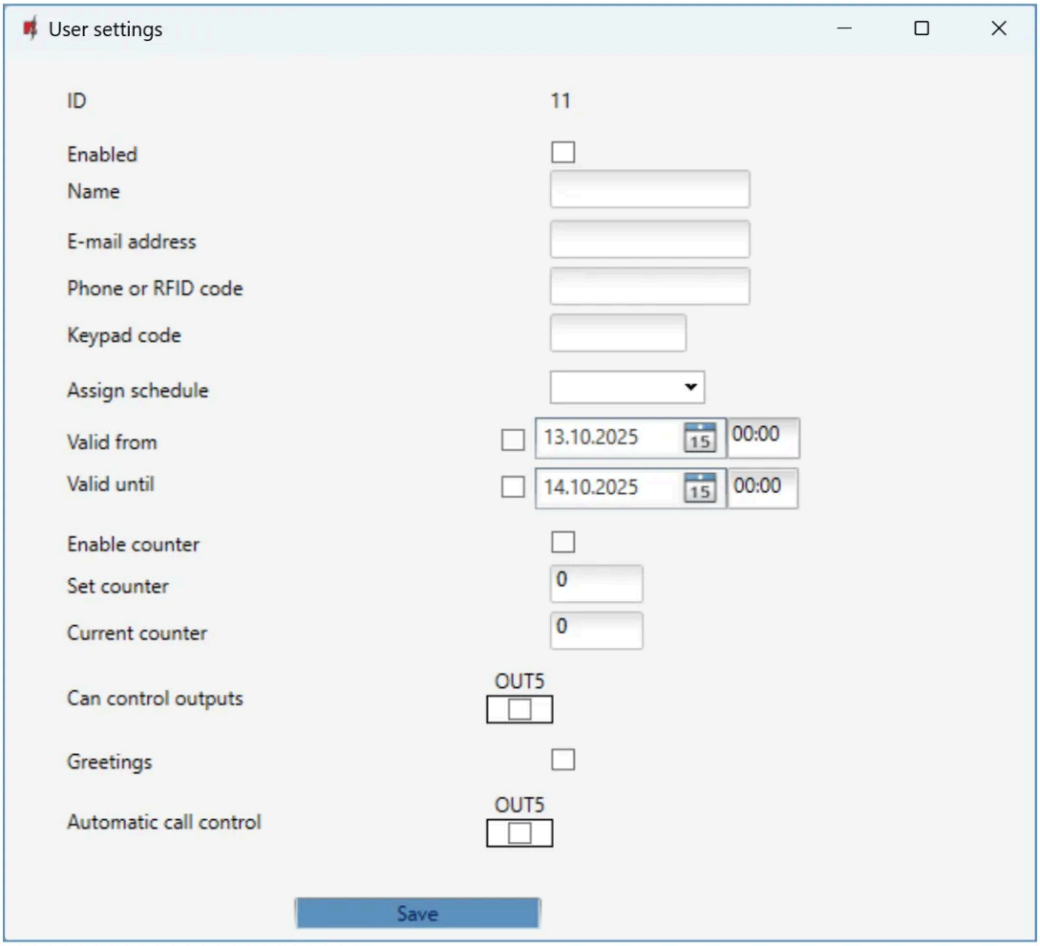


Figure 40. TrikdisConfig – **User settings** for a user: **Assign schedule**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs**, **Greetings**, **Automatic call control**.

- **Assign schedule** – the schedule(s) during which the user may 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 set time; **Current counter** – the number of switchings so far.
- **Can control outputs**, **Greetings**, **Automatic call control** – as for the administrator.

5.6.2 Registering an RFID card (key fob)

1. Connect the RFID reader (section 3.6), switch on the GATOR's power, start TrikdisConfig and connect over a USB cable or remotely. On the **IN/OUT** page set the number of readers (**Wiegand reader mode**).
2. On the **User list** page click the **Register RFID** button.

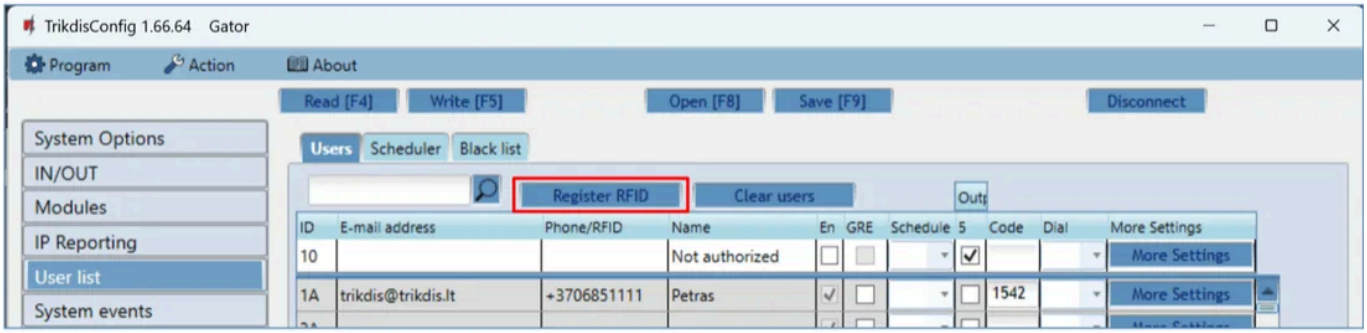


Figure 41. TrikdisConfig – User list: the **Register RFID** button above the user table.

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

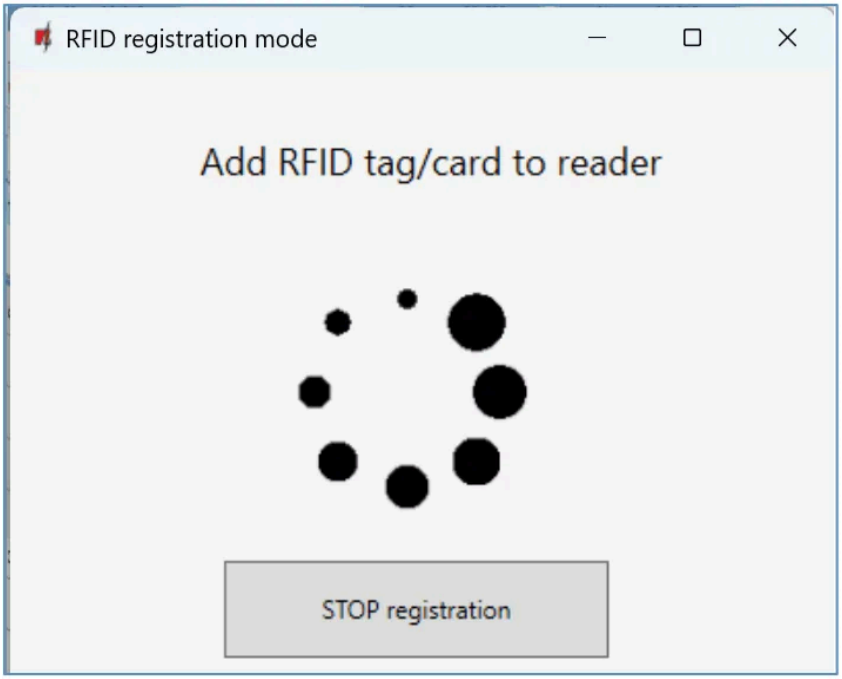


Figure 42. The RFID registration window: the card must be held to the reader; the **STOP registration** button closes the registration.

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**), mark the output that can be controlled (**User can control PGM Output 5**; with the **Device administrator** checkbox the user becomes an administrator), and click the **ADD** button. Repeat with the other cards, then press the **STOP registration** button.
5. With the **Write [F5]** button write the card list to the device.

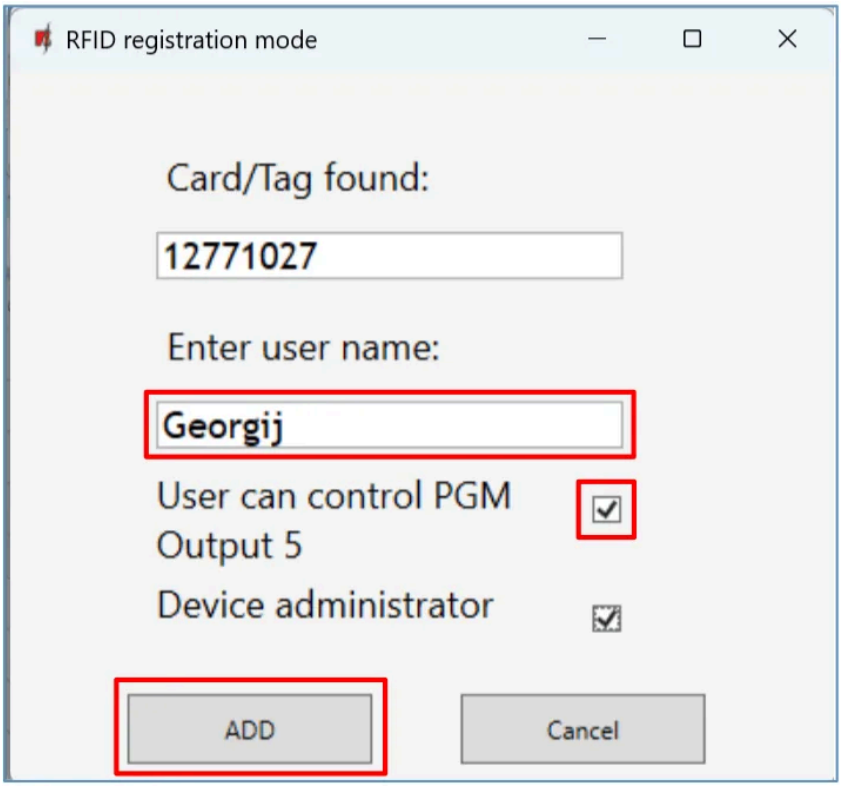


Figure 43. The window of the card that has been read: name, **User can control PGM Output 5**, **Device administrator**, then **ADD**.

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

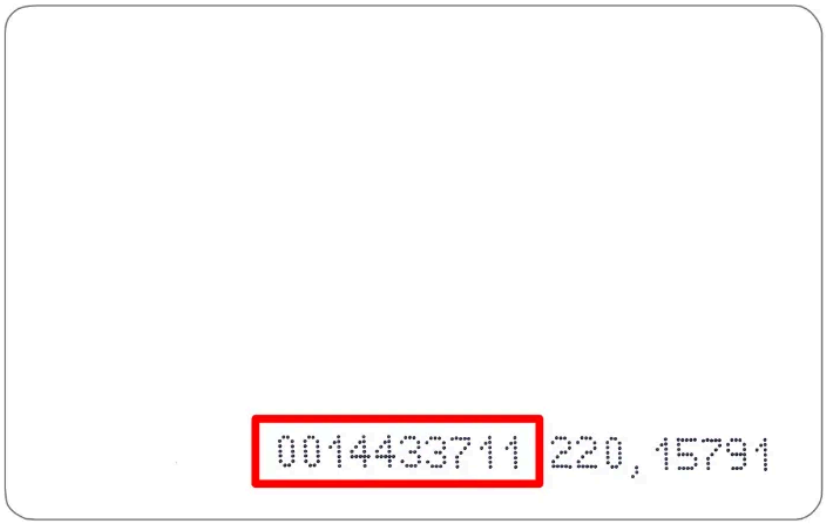


Figure 44. The ID number printed on the RFID card (on the bottom edge of the card).

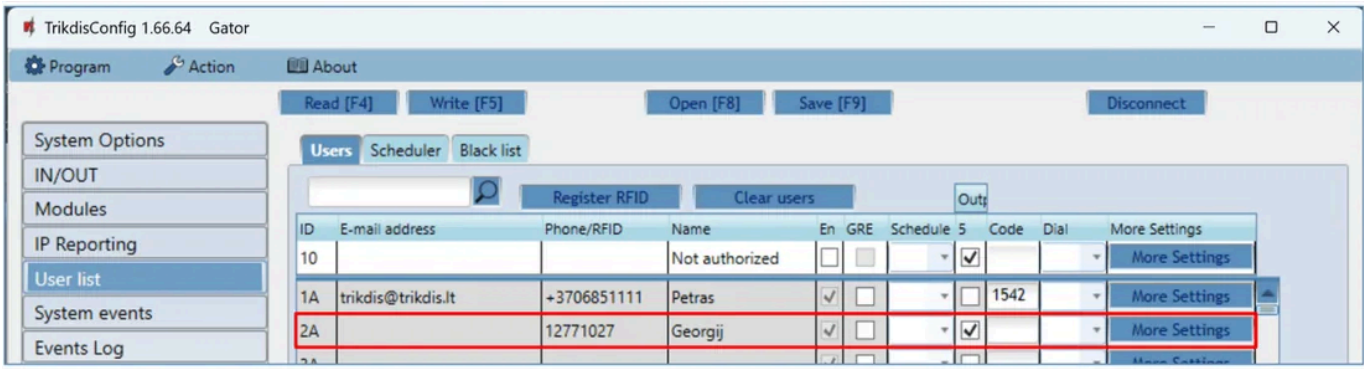


Figure 45. TrikdisConfig – User list: the row of the new user with the card number in the **Phone/RFID** field, with name, **En** ticked, output 5 marked.

Adding a card from Protegus 2: in the list of users choose adding a new user, enter the e-mail address, the name, the card's ID number (in the phone number field), for a code reader the 4-digit code, mark the output and save it (section 4.5).

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 schedule** field.

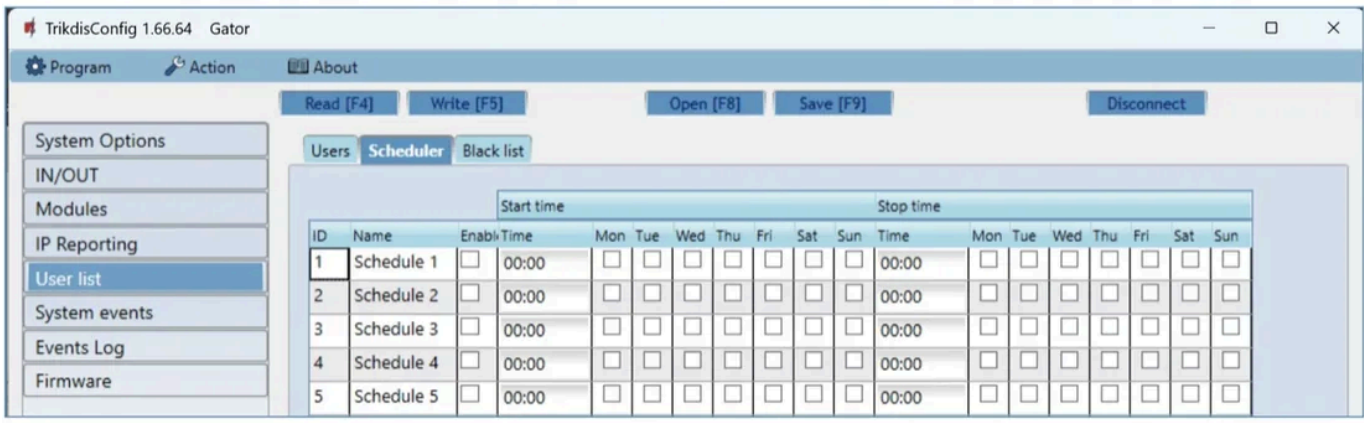


Figure 46. TrikdisConfig – User list, **Scheduler** tab: five schedules, each with **Enable**, start and end time with the days of the week.

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

5.6.4 Black list tab – blacklist

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

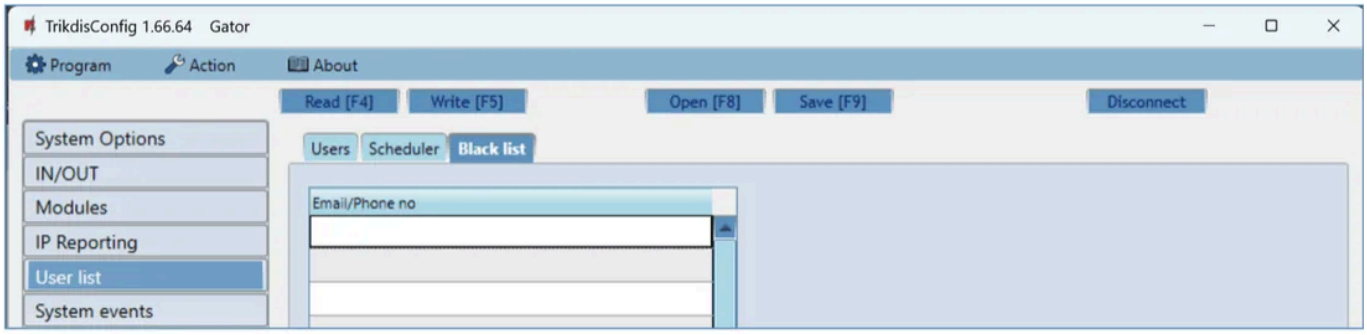


Figure 47. TrikdisConfig – User list, **Black list** tab: the table of the blocked e-mail addresses, phone numbers and card numbers.

The blacklist contains the e-mail addresses, phone numbers and RFID card numbers that are not allowed to control the GATOR. You can also add an entry directly from the event log: right-click the phone number, e-mail address or card number, and choose the **Add to black list** menu item. By SMS the `SETB` and `DELB` commands manage the list (section 4.7).

5.7 “System events” page

Here you set which of the GATOR's own system events go to the monitoring station and to the Protegus 2 app.

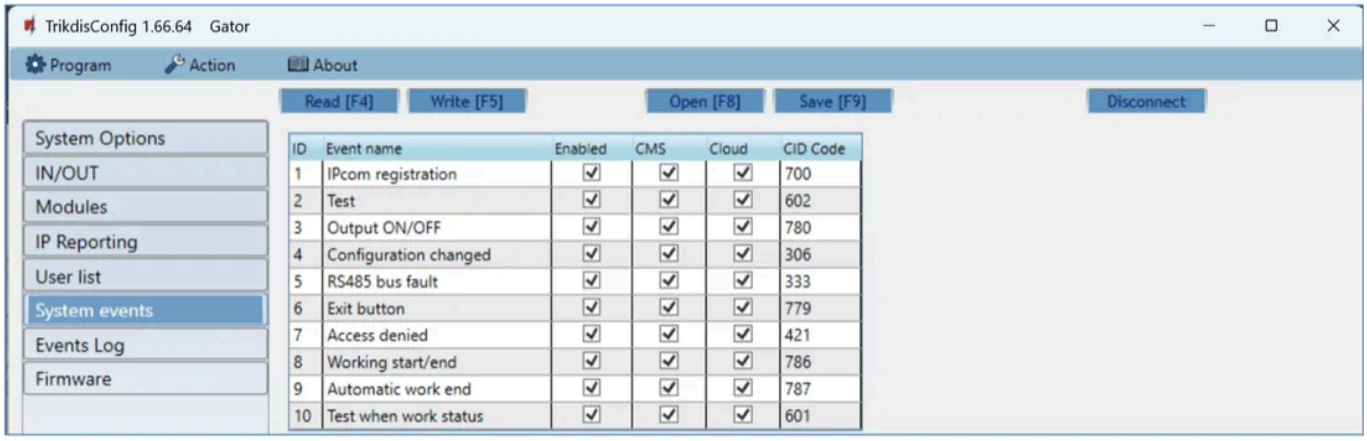


Figure 48. TrikdisConfig – **System events**: the list of events with the Contact ID code (for example IPcom registration 700, Test 602, Output ON/OFF 780, Configuration changed 306, RS485 bus fault 333, Exit button 779, Access denied 421, Working start/end 786, Automatic work end 787), each with the **Enabled**, **CMS** and **Cloud** checkboxes.

- **ID** – the number of the event.
- **Event name** – the name of the event.
- **Enabled** – monitoring of the event.
- **CMS** – the event goes to the monitoring station.
- **Cloud** – the event goes to the Protegus 2 app.
- **CID Code** – the Contact ID code of the event.

5.8 “Events Log” page

The device's own event log – for troubleshooting and for looking up the entries.

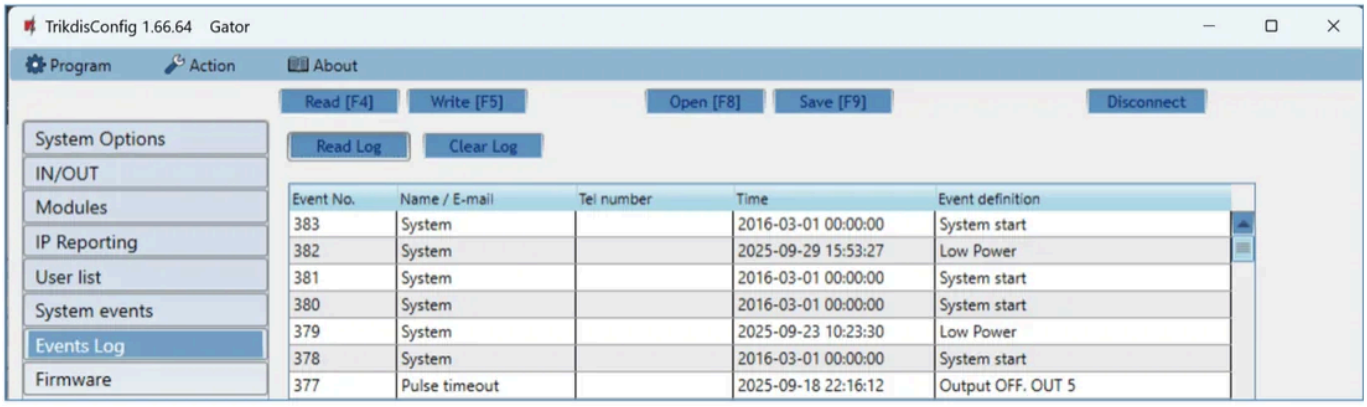


Figure 49. TrikdisConfig – **Events Log**: the **Read Log** and **Clear Log** buttons; for the events the number, the user's name or e-mail address, the phone number, the time and the description of the event.

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

5.9 Restoring the default settings

To restore the default settings, click the **Restore** button in the **Default settings** group in the lower left part of the programming window. Restoring deletes all settings – the user list and the passwords as well –, so it is worth saving the settings to a file beforehand (**Save [F9]**).



Figure 50. TrikdisConfig – the **Restore** button of the **Default settings** group above the status bar.

5.10 Indicating the state of the gate

The Protegus 2 app and the widget can show the actual state of the gate (open or closed). For this, the GATOR's **1 IN** input must be connected to the gate opener's state output or to the gate's limit switch (section 3.5), and then in the software the input must be assigned to the output that switches the gate:

1. On the **IN/OUT** page, **1 IN** must have the **Input** function, with the type matching the contact (in the example NO). In the row of **5 OUT**, in the **Assign IN** column, choose the **1 IN** input.
2. If you also want an SMS about the opening and closing of the gate, enter the **SMS event text** and **SMS restore text** of 1 IN (for example “Gate open” / “Gate closed”).

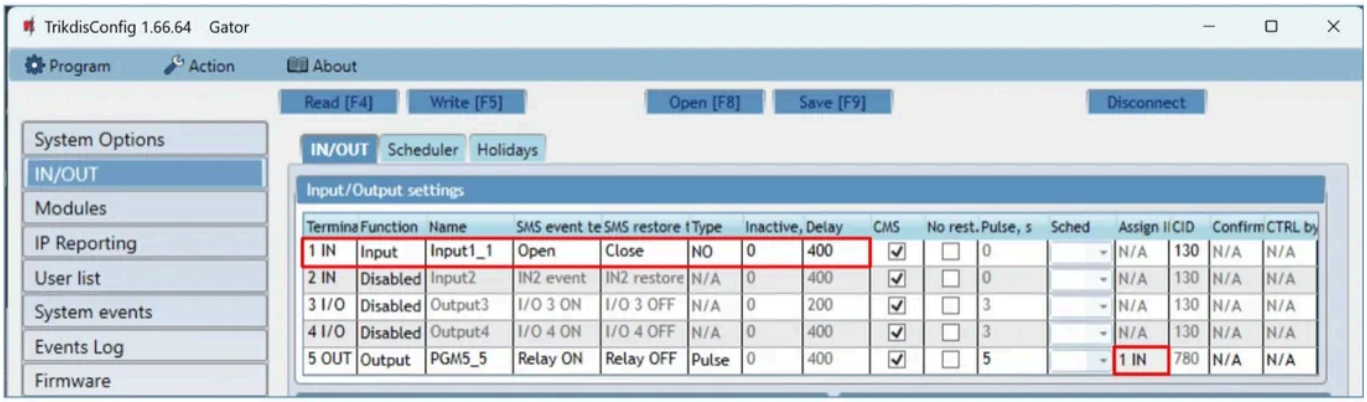


Figure 51. TrikdisConfig – IN/OUT: the **1 IN** input (NO, with **Open** / **Close** SMS text), in the row of **5 OUT** in the **Assign IN** column **1 IN**.

3. On the **User list** page, in the user's row, click the **More settings** button, and in the **SMS notification for** group tick the **IN1** checkbox so that the user receives an SMS about the state of the gate. Click the **Save** button, then write the settings (**Write [F5]**).



Figure 52. TrikdisConfig – User list: the **More settings** button in the user's row.

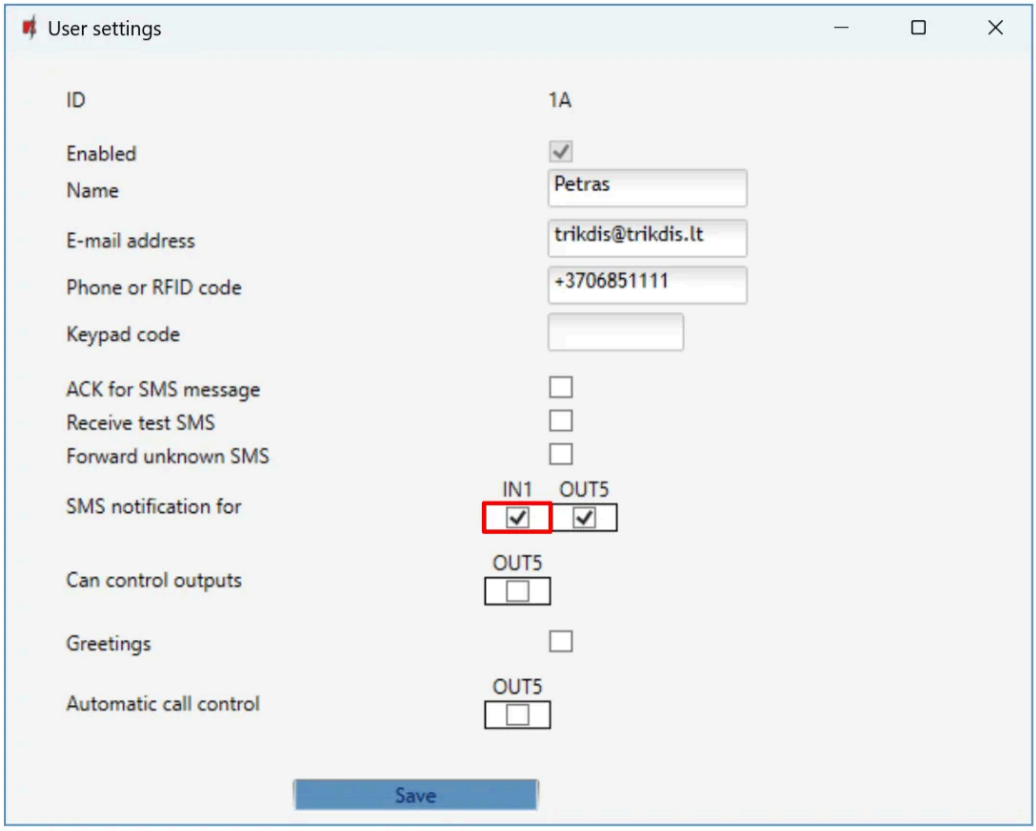


Figure 53. TrikdisConfig – User settings: in the **SMS notification for** group **IN1** (and **OUT5**) ticked, at the bottom the **Save** button.

6. Remote programming

You can also read and change the GATOR's settings remotely through the Protegus cloud – you do not need to go to the site.

Conditions for remote programming

In TrikdisConfig, on the **IP Reporting** page, **Enable cloud service** must be ticked (section 5.5; by SMS: `CONNECT 123456 PROTEGUS=ON`), the power supply must be in order (the **POWER** LED blinks green), and the device must be on the network (the **NETWORK** LED is lit green and blinks 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 that the GATOR 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 GATOR's **IMEI** 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 status bar).
4. In the **System Name** field write any name (for example the name of the object), and click the **Configure** button.

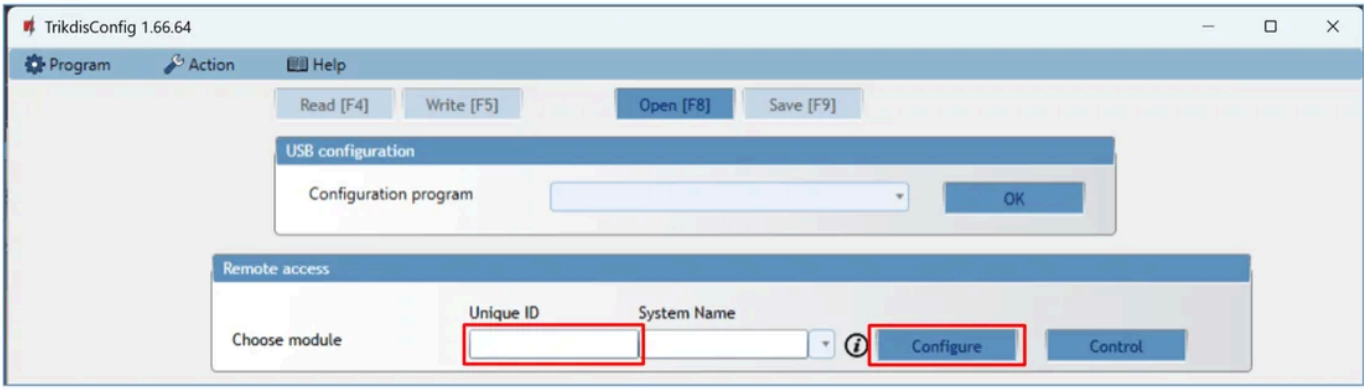


Figure 54. TrikdisConfig – the **Remote access** part: the **Unique ID** field, the **System Name** field and the **Configure** button.

5. The GATOR's programming window opens. Click the **Read [F4]** button: the software reads the device's current settings. If the software asks for the access code, enter the 6-digit **administrator** code. If you tick the **Remember password** checkbox and click the **Write [F5]** button, the software 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 software.

Remote programming needs no help on site: the customer only checks the power supply 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 4.5) or by SMS (section 4.7).

7. Testing the operation

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

1. **Power supply**: the **POWER** LED blinks green. If it blinks yellow, the supply voltage is not correct – measure it on the power terminals (9–32 V DC or 12–24 V AC).

2. **Network**: the **NETWORK** LED is lit green and blinks yellow according to the signal strength (3 blinks are already enough). If the **TROUBLE** LED blinks, the number of blinks shows the fault (section 1.5).
3. **Inputs**: activate the wired inputs one after the other (gate state contact, exit push button), and check that the recipients receive the correct messages by SMS, in Protegus 2 and at the monitoring station.
4. **Outputs**: switch on the outputs remotely – by call, from the app, by SMS and with the card too, if there is a reader –, and check that the gate opens, the recipients receive the messages, and the gate state in the app also follows reality (section 5.10).

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.

You can also query the state of the device by SMS from the administrator's phone: to the `INFO 123456` command the GATOR sends back its type, the signal strength, the supply voltage, the firmware version, the date and the time (section 4.7). If the reply SMS does not arrive, check that **ACK for SMS message** is switched on for the administrator (section 5.6).

8. Firmware update

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

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.

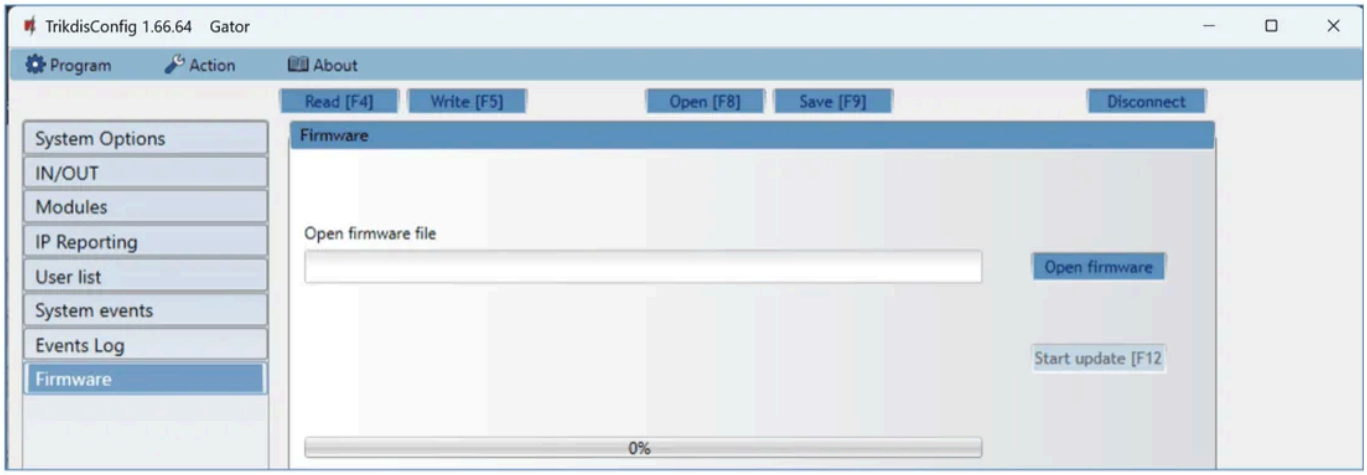


Figure 55. TrikdisConfig – GATOR, **Firmware** page: the **Open firmware** button, the field of the selected file, the **Start update [F12]** button and the progress indicator.

On the GATOR the label of the button that starts the update is **Start update [F12]**. Using the RF-LORA and iO-LORA modules requires firmware **2.13** or newer, the W485 and E485 modules require firmware **1.06** or newer; 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 1.5), then at the points below.

The TROUBLE LED blinks – what does the number of blinks mean?

The number of blinks is the cause of the fault: **1** – no SIM card (or it does not make contact: take it out and put it back); **2** – the PIN code of the SIM card is wrong (switch off the PIN request in a phone, or enter the correct PIN in the **System Options** → **SIM card PIN** field); **3** – cannot connect to the mobile network (signal strength, antenna, whether the SIM card is active, a 2G card in a 4G device); **4** – cannot connect to the Protegus cloud or to the primary IP receiver (mobile data on the SIM, APN, the receiver's address and port); **5** – cannot connect to the backup IP receiver; **6** – the internal clock is not set (time synchronization, `TIME` command); **7** – the supply voltage is not correct.

I call it, but the GATOR does not react

- If the **NETWORK** LED is not lit green, the device is not on the network: check the SIM card (active, PIN switched off, suitable for receiving calls), the antenna and the signal strength (the number of yellow blinks).
- If you have already added users, or the **En** checkbox of the **Not authorized** row (no. 10) is empty, the device only accepts calls from numbers on the list – the caller's number must be on the list, in international format (+CC..., where CC is the country code), enabled (**En**), with a valid schedule and validity period (section 5.6).
- The caller's phone must not hide its caller ID, otherwise the device cannot identify it.
- Check that the number is not on the blacklist (section 5.6.4).

It does not open on a call, but it does from the app

If a W485 or E485 module is connected to the device, on the **Modules** → **Parameters** tab, in the **SIM parameters** group, look at the **Use dial and SMS when working over internet module** checkbox: when it is empty, the device does not use calls and SMS while the internet connection is up (section 5.4). Tick it if you

also need control by call.

I cannot control it with the phone's keypad during a call

For keypad (DTMF) control, the value of **System Options** → **Hang-up after** must be greater than 0, otherwise the device rejects the call immediately (section 4.2). On devices with the type code **GV17_2E70** and **GV17_2S70** DTMF control does not work – the type is shown in the **Device** field of the status bar.

Protegus 2 does not find the device, or it does not become Online

- On the **IP Reporting** page **Enable cloud service** must be ticked (by SMS: `CONNECT 123456 PROTEGUS=ON`), and the **TROUBLE** LED must not blink 4 times.
- The SIM card must have mobile data service, and the APN must be correct: in the **System Options** → **APN** field the **Auto** checkbox chooses from the built-in list; if the connection is not established, enter the operator's APN (list).
- In the app the IMEI must be exact, and if the **Cloud Access Code** is not the default `123456`, enter the correct one.
- If everything is in order, wait up to 1 minute after adding it (section 4.3).

The widget does not work, or I cannot find it

The widget is only available on an **Android** phone (section 4.4); on an iPhone you open from the app's home screen. On Android the GATOR must be added to the systems and you must be logged in; if the widget stays grey, open the app once and check the internet connection.

The RFID reader does not read the card, or the GATOR does not react to it

- Check the wiring according to the drawing in section 3.6 (with one reader **D0** → **1 IN**, **D1** → **2 IN**; with the second reader **D0** → **3 I/O**, **D1** → **4 I/O**; common negative point), and the reader's power supply: with a 12 V reader the GATOR must run from a **DC power supply**, with a reader with a 5 V signal level tick the **Low voltage reader** checkbox.
- On the **IN/OUT** page **Wiegand reader mode** must match the number of readers (**Single** / **Dual**), and **3 I/O**, **4 I/O** must not be set to another function.
- If the device does not recognize 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, with the reader's output (section 5.6.2). The event log (section 5.8) shows whether the reading took place and why it was rejected (**Access denied**).

The app does not show the actual state of the gate

For gate state indication, the gate opener's state output or the gate's limit switch must be connected to the **1 IN** input (section 3.5), on the **IN/OUT** page the input's type must be set to match the contact, and in the row of **5 OUT**, in the **Assign IN** column, the **1 IN** input must be selected (section 5.10). After that, in the app the output's icon shows the state of the input.

The device does not reply to the SMS commands

- It only accepts SMS commands from the **administrator** numbers (1A–7A); the first caller or SMS sender becomes the administrator. If you do not know who that is, read the **User list** table in TrikdisConfig.
- In the command the password must follow the command word, with a space (`INFO 123456`); the new password is 6 characters.

- The reply SMS only arrives if **ACK for SMS message** is ticked for the administrator (section 5.6).
- If the device runs with an internet module (W485 / E485) and **Use dial and SMS when working over internet module** is empty, it does not process the SMS messages while the internet connection is up (section 5.4).

I have forgotten the administrator password

The password cannot be queried. Connect to the device with a USB cable and restore the default settings with the **Restore** button in the lower left part of the programming window (section 5.9) – this deletes the user list and all settings, so afterwards the device must be set up 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 need to enter the password again.

Do I need a SIM card if I use a W485 or E485 module?

No: with the W485 Wi-Fi or the E485 Ethernet module the GATOR also works without a SIM card; control then takes place from the app (and with an RFID card), without calls and SMS. On the **Modules** → **Parameters** tab tick the **Disable indication of the absence of a SIM card** checkbox so that the device does not indicate the missing card as a fault (section 5.4). If you also want the mobile network backup, insert a SIM card and leave the **Disable the use of SIM card mobile data** checkbox empty.

I want to control several gates from one device

The GATOR's own relay switches one gate; the **3 I/O** and **4 I/O** terminals as open-collector outputs (50 mA) can drive an external relay. 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 3.9); for more wired inputs and outputs, one **iO8** or **iO8-LORA** expander (section 3.10). For the users you mark in the **Can control output** field which output they may switch.

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 GATOR may only be installed and maintained by qualified persons.
- Before installation, read this manual to avoid mistakes that can lead to malfunction or damage to the equipment.
- **Disconnect the power before making any electrical connection** – of the GATOR and of the gate opener as well.
- Changes, modifications or repairs not authorized by the manufacturer void the warranty.
- Follow local waste disposal regulations: do not throw the device and its parts in household waste – hand in the discarded device as electronic waste.

See also

- The GV17 gate automation device can be used with Protegus 2 – the GATOR and the app together.
- GV17 access control and/or time and attendance system – RFID readers, entry and exit, working time in Protegus 2.
- Dual-path communication now for the GV17 GATOR gate opener too – W485 / E485 module for the GATOR.
- Flexible wireless access control with the GATOR RF-LoRa system – RF-LORA and iO-LORA modules, several gates in one system.
- APN settings – list of European mobile operators – if the mobile data connection is not established.
- Protegus Android / iPhone and web app – about the app.
- Documentation in English: docs.trikdis.com – Cellular gate controller GATOR – the manuals on docs.trikdis.com are in English.

Related products

Trikdis GV17 - GATOR smart 4G GSM / IP gate controller

Trikdis GV17 - GATOR smart 2G GSM / IP gate controller **Trikdis W485 Wifi module (RS485)**

Trikdis E485 Ethernet module (RS485) **Trikdis RF-LORA wireless expander module**

Trikdis IO-LORA wireless expander module **Trikdis iO8 wired expander module**

Trikdis IO8-LORA wireless expander module

Trikdis ANT04 GSM stick-on antenna with 2,5m wire

Trikdis ME301M magnetic antenna with 2,5m wire

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/gv17-manual