GET communicator – installer and user manual

Installer and user manual for the Trikdis GET Ethernet + 4G communicator: connection to the alarm control panel, LAN and SIM setup in TrikdisConfig, reporting to the monitoring station, the Protegus 2 app.



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

Contents

1. Overview

1.1 What it is for and how it works
1.2 Versions: GET, GT and GT+
1.3 Compatible alarm control panels
1.4 Parts of the communicator
1.5 Terminals
1.6 LED indications
1.7 Technical specifications

2. Quick start

2.1 Preparation
2.2 Connection to the Protegus 2 app
2.3 Connection to the monitoring station

3. Installation and wiring

3.1 Installation steps
3.2 Placement in the control panel's enclosure, antenna
3.3 Connection to the alarm control panel
3.3.1 DSC – data bus (Keybus)
3.3.2 Paradox – serial port
3.3.3 Paradox SP/MG – Keybus and TIP/RING
3.3.4 UTC Interlogix (Caddx) – data bus
3.3.5 Texecom – serial port
3.3.6 InnerRange Inception
3.3.7 InnerRange Integriti
3.3.8 Honeywell Vista – data bus
3.3.9 Any control panel – TIP/RING
3.4 Wiring a keyswitch zone
3.5 Wiring inputs
3.6 Wiring an output with a relay
3.7 Power-up and first check
A TRIKDIS átjelző elindítása

4. Programming the alarm control panel

4.1 Data bus or serial connection
4.1.1 DSC
4.1.2 Paradox
4.1.3 Texecom
4.1.4 UTC Interlogix (Caddx)
4.1.5 InnerRange
4.1.6 Honeywell Ademco Vista
4.2 Telephone line (TIP/RING) connection
4.2.1 Programming the Honeywell Vista dialer
4.2.2 The dialer of the UTC Interlogix (Caddx) NX

5. Remote control with the Protegus 2 app

5.1 Adding the device
A rendszer létrehozása a Protegus 2 alkalmazásban
5.2 Arming and disarming with an output

5.3 Arming and disarming from the app

6. The settings in detail

6.1 Connecting to the communicator

6.2 System settings (System options)

6.3 Panel settings

6.4 CMS reporting (Reporting to CMS)

6.4.1 Receiver channels (CMS settings)

6.4.2 Test, PING and the order of connections

6.5 User reporting (Protegus Cloud)

6.6 Network settings

6.6.1 LAN (Ethernet)

6.6.2 SIM1 and SIM2

6.7 IN/OUT

6.8 Event summary (System events)

6.9 Restoring the factory settings

7. Remote programming

8. Checking that the communicator works

9. Firmware update

10. Troubleshooting and frequently asked questions

11. Safety instructions

See also

1. Overview

The GET is Trikdis's **Ethernet + 4G communicator**: it forwards the events of the alarm control panel to the monitoring station and to the Protegus 2 app over the wired local network (LAN) or over the mobile network. It can be connected to the control panel in two ways: **directly**, to the panel's data bus or serial port (with DSC, Paradox, UTC Interlogix (Caddx), Texecom, InnerRange and Honeywell control panels), or to the **telephone line dialer (TIP/RING) of any control panel** that sends its events in Contact ID format with DTMF tones. The communicator forwards the complete event information (code, partition, zone or user) to the monitoring station. With the Protegus 2 app the user controls the system remotely and receives notifications about the events; the app works with every control panel the communicator supports, regardless of the panel's manufacturer. Reporting to the monitoring station and Protegus 2 can be used at the same time. This manual was written for the GET communicator with an LTE (4G) modem; the differences between the GET, the GT and the GT+ are summarized in section 1.2.

1.1 What it is for and how it works

- **It reports to the monitoring station.** It sends the events over an IP connection, via the wired network or the mobile network, to a Trikdis software or hardware receiver (TRK8 protocol) – these work with any monitoring software –, to a SIA DC-09 receiver or to a SUR-GARD receiver (TL150). Towards a SUR-GARD receiver it converts the Contact ID codes received from the control panel into SIA codes; the conversion table is in the appendix of the English documentation on docs.trikdis.com. It checks the connection with the receiver every 30 seconds (or at the interval you set) with a PING message; if the primary channel fails, it switches to the backup channel. With a parallel channel the events go to two receivers at the same time. You can put the connection paths – LAN, SIM1, SIM2 – in order: if the main path does not work, the communicator switches to the backup path (section 6.4.2). If the Protegus service is also switched on, the monitoring station receives the event first, and only then the users' app.
- **It notifies the user.** The Protegus 2 app shows the events in a push notification with a separate sound; from the app the user can arm and disarm, and switch the devices connected to it (lighting, gate, ventilation, heating, irrigation, etc.). In the app the administrator, the installer and the user have different rights. The GET does not send SMS or call notifications: notifications arrive through the Protegus 2 app.
- **It controls the control panel directly.** When connected to the data bus or serial port, the communicator also sees the panel's partition and zone states, and the user arms and disarms from Protegus 2 with their own keypad code – no keyswitch zone is needed for this.
- **It has its own inputs and outputs.** Two dual-function I/O terminals can be used as an input (IN) or as a controllable output (OUT); by default both are outputs. The outputs can be switched from the Protegus 2 app. The **A 485** and **B 485** terminals are not used on the GET; no RS485 expansion module can be connected to the GET.
- **It can be set up with two tools.** The settings can be made with the TrikdisConfig software running on Windows (over a USB-C cable or remotely) and – with firmware 1.08 or newer – also from the Protegus 2 app (Settings → Advanced settings). The settings can be saved to a file and written into other communicators. There are two access levels: the monitoring station's administrator and the installer. The communicator can also be set up remotely, and its firmware can also be updated remotely.

The diagram below shows the structure of the system: the alarm control panel connects to the communicator, the communicator reaches the internet in two ways – over the mobile network (LTE) or through the router (LAN) –, and from there the monitoring station's receiver (and its software) and the Protegus server; the user

sees the system in the Protegus 2 app.

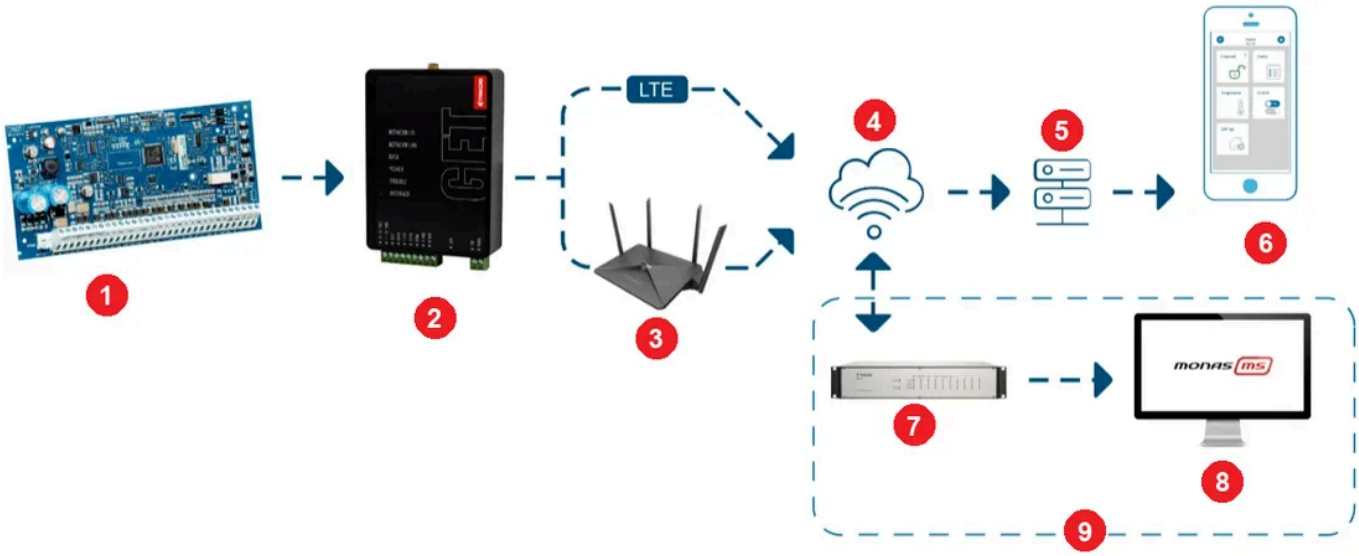


Figure 1. The communicator's place in the system: alarm control panel → GET → mobile network (LTE) or router (LAN) → internet → monitoring station receiver and Protegus server → Protegus 2 app.

- 1 alarm control panel ("Alarm panel")
- 2 GET LTE communicator ("LTE communicator")
- 3 router ("Router")
- 4 internet ("Internet")
- 5 Protegus server ("Protegus server")
- 6 phone with the Protegus app ("Phone with Protegus software")
- 7 monitoring station receiver ("Receiver")
- 8 monitoring software ("Monitoring software")
- 9 the security company's monitoring station ("Monitoring station in security company") – in the dashed frame

1.2 Versions: GET, GT and GT+

The GET is the Ethernet-port sibling of the GT and GT+ communicators: wiring and programming of the alarm control panel, the range of compatible control panels, the modem, the transmission protocols and the use of Protegus 2 are the same, so the chapter structure of the three communicators' manuals is also the same. The differences are summarized in the table below.

	GET	**GT**	**GT+**
Network connection	**LTE (4G) and Ethernet (LAN, RJ45)**; the order of the connection paths can be set (Main / Backup / Backup 2: LAN, SIM1, SIM2; section 6.4.2)	LTE (4G)	LTE (4G)
SIM card	**2 nano SIM holders** (SIM1, SIM2); one or two cards can be inserted	1 nano SIM	1 nano SIM
Supply voltage	10–18 V DC	10–18 V DC	10–32 V DC
Current consumption	up to 100 mA in standby, 300 mA while sending data	up to 100 / 200 mA	up to 100 / 200 mA
Size, weight	113 × 70 × 25 mm, 110 g	92 × 62 × 26 mm, 80 g	92 × 62 × 26 mm, 80 g

	GET	GT	GT+
Terminals	+12 VDC, −12 VDC, CLK, DATA, 1 I/O, 2 I/O, **COM**, A 485, B 485; separate **LAN** (RJ45) socket and TIP, RING	+12 VDC, −12 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485	+12 / 24 VDC, −12 / 24 VDC, TIP, RING, CLK, DATA, 1 I/O, 2 I/O, A 485, B 485
Default setting of the I/O terminals	output (OUT)	input (IN, NO)	input (IN, NO)
RS485 bus, iO-8 expander	the A 485 / B 485 terminals are **not used**; no expander can be connected	up to 4 iO-8	up to 4 iO-8
LEDs	NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE (not used)	NETWORK, DATA, POWER, TROUBLE, BAND	NETWORK, DATA, POWER, TROUBLE, BAND
TROUBLE LED flashes	1 = LAN physical connection (cable), 2 = SIM1 fault, 3 = SIM2 fault, 7 = control panel	1–8 (SIM, PIN, APN, network, receiver, control panel, ICCID)	1–8
SMS and calls	no SMS notification, SMS commands or calls: notification and control are done from Protegus 2	SMS and call notification, SMS commands	SMS and call notification, SMS commands
DSC control panel on the data bus and the TIP/RING terminals together	no	no	yes
TIP/RING connection setting (Panel settings → Communication protocol)	**2. AUTO**	**2. Dual tone**	**2. AUTO** (**3. MANUAL** can also be selected)
Setup from the Protegus 2 app	yes (Advanced settings, from firmware 1.08)	TrikdisConfig	TrikdisConfig
Event buffer	60 events	no data	no data
Internal messages (Event summary)	COMMUNICATION, LAN_FAILURE, POWER, REMOTE_STARTED, REMOTE_FINISHED, SIM1_FAILURE, SIM2_FAILURE, TEST	COMMUNICATION, POWER, REMOTE_STARTED, REMOTE_FINISHED, START, TEST	as the GT
Modem, transmission protocols (TRK8, DC-09, TL150), encryption, compatible control panels, wiring diagrams, Protegus 2	same	same	same

All three communicators are made with the same three kinds of modem; for the European market the European (EU) version is the right one. You can find the modem type and the hardware version in the TrikdisConfig status bar (**Device**, **HW**) and on the device's label.

Modem	Network and frequency bands
EG915U-EU (Europe)	LTE FDD: B1 / B3 / B5 / B7 / B8 / B20 / B28; GSM: B2 / B3 / B5 / B8

Modem	Network and frequency bands
EG915U-LA (Latin America)	LTE FDD: B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66; GSM: B2 / B3 / B5 / B8
BG95-M5 (LTE Cat M1)	LTE FDD: B1 / B2 / B3 / B4 / B5 / B8 / B12 / B13 / B18 / B19 / B20 / B25 / B26 / B27 / B28 / B66 / B85; EGPRS: 850 / 900 / 1800 / 1900 MHz

1.3 Compatible alarm control panels

The control panels below can be connected to the communicator directly, over the data bus or the serial port. The "Direct control" column shows whether the user can arm and disarm from Protegus 2 with their own keypad code without any further wiring; where this is not possible, the communicator reads the events from the bus, and a keyswitch zone is needed for control (section 3.4).

Manufacturer	Model	Connection	Direct control
DSC	PC585, PC1404, PC1565, PC1616, PC1832, PC1864, PC5020	data bus (Keybus)	yes
Paradox	Spectra SP4000, SP5500, SP6000, SP7000, SP65, SP5500+, SP6000+, SP7000+	serial port (EX-CRP2.4 cable), or Keybus + TIP/RING	yes
Paradox	Magellan MG5000, MG5050, MG5050E, MG5075, MG5050+	serial port (EX-CRP2.4 cable), or Keybus + TIP/RING	yes
Paradox	Digiplex EVO192, EVOHD, EVOHD+	serial port (EX-CRP2.4 cable)	yes
Paradox	Digiplex EVO48	serial port (EX-CRP2.4 cable)	no
Paradox	Spectra 1727, 1728, 1738; Esprit E55	serial port (EX-CRP2.4 cable)	no
UTC Interlogix	NetworX (Caddx) NX-4v2, NX-6v2, NX-8v2, NX-8e	data bus	yes
Texecom	Premier 24, 48, 88, 168, 640; Premier Elite 12, 24, 48, 64, 88, 168, 640	serial port (EX-CRP4 cable)	yes
InnerRange	Inception, Integriti	serial port (with the panel manufacturer's cable)	no
Honeywell	Ademco Vista-15, Vista-20, Vista-48	data bus	yes

- The firmware of directly controlled **Paradox** control panels must be at least **V.4**. On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2. The Spectra SP / SP+ and Magellan MG / MG+ control panels can also be connected to the data bus (Keybus) and the TIP/RING terminals together instead of the serial port – this does not require the paid unlocking, but the communicator's firmware must be at least 1.21 (section 3.3.3).
- The control panels of **all other manufacturers** connect through their telephone line dialer (TIP/RING), if it sends the events in Contact ID format with DTMF dialing; in that case a keyswitch zone is needed for control.
- You can check which Trikdis communicator and which connection suits your control panel in the Compatibility finder.

1.4 Parts of the communicator

The communicator's printed circuit board sits in a black plastic case; the front cover snaps off, and the terminal block can be pulled off. The LAN socket and the TIP/RING terminals are accessible on the side of the case, through a separate opening.

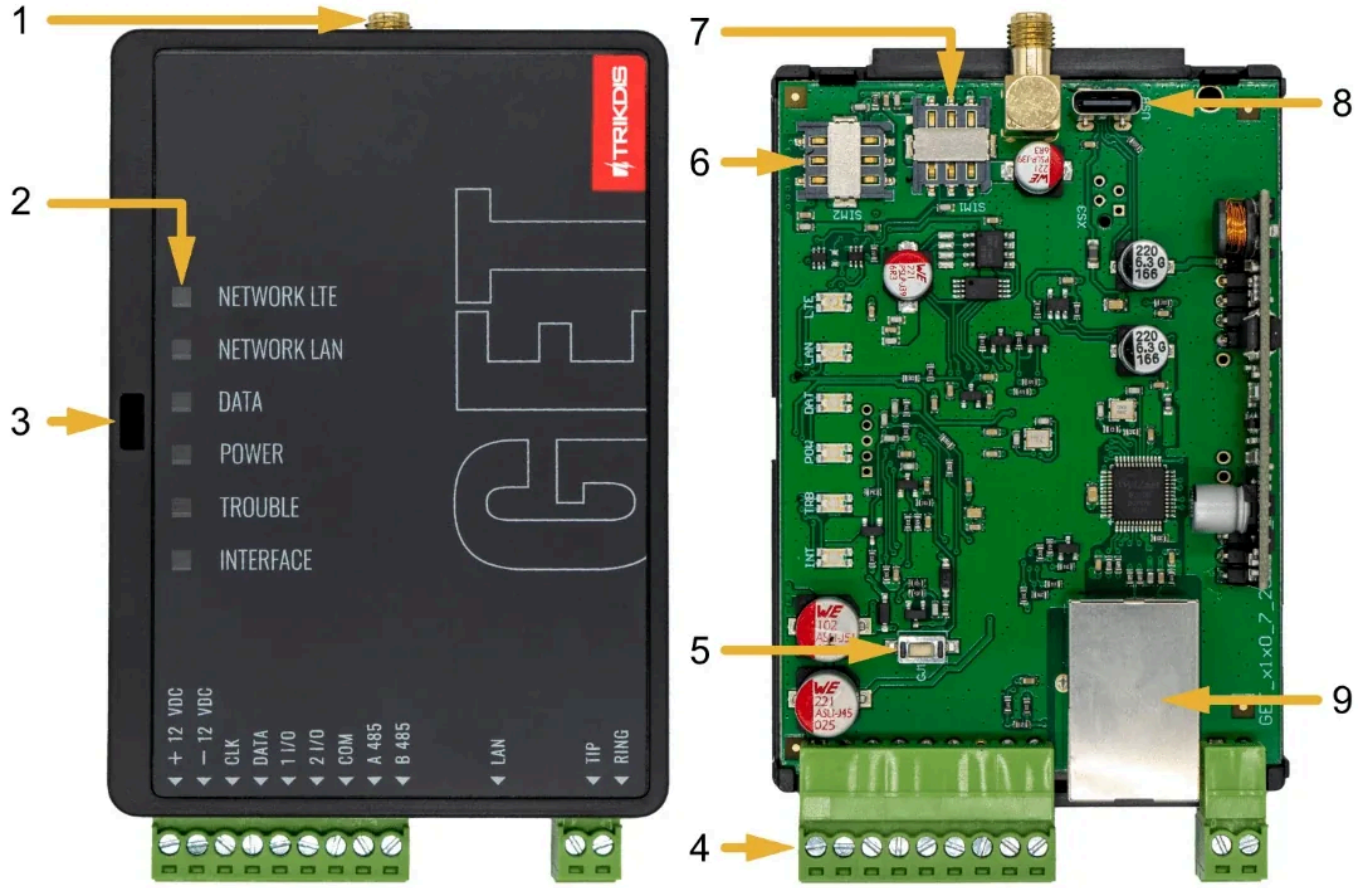


Figure 2. Parts of the communicator from the front (left) and with the case open (right).

- 1 SMA connector of the mobile antenna
- 2 LED indicators (NETWORK LTE, NETWORK LAN, DATA, POWER, TROUBLE, INTERFACE)
- 3 Slot for snapping off the front cover
- 4 Removable terminal block for the external connections
- 5 RESET button
- 6 SIM2 card holder
- 7 SIM1 card holder
- 8 USB-C socket for programming
- 9 Ethernet (LAN) RJ45 socket

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

1.5 Terminals

Terminal	Function
+12 VDC	Power, positive: +10–18 V DC
–12 VDC	Power, 0 V
CLK	Serial bus or data bus (clock) for direct connection of the control panel
DATA	Serial bus or data bus (data) for direct connection of the control panel

Terminal	Function
1 I/O	Input/output 1 (default setting: output, OUT)
2 I/O	Input/output 2 (default setting: output, OUT)
COM	Common (negative) point for the inputs and outputs
A 485	Not used
B 485	Not used (the pair of A 485)
LAN	Ethernet (local network) RJ45 socket
TIP	TIP terminal of the alarm control panel's telephone line dialer
RING	RING terminal of the alarm control panel's telephone line dialer

On the wiring diagrams the power terminals are marked **+DC** and **–DC** (on the device +12 VDC / −12 VDC), and the RS485 terminals **A RS485** / **B RS485** (on the device A 485 / B 485). The terminal labels are also printed on the front cover.

1.6 LED indications

The LEDs on the front cover are the most important tools for commissioning and troubleshooting. Read them together: POWER shows the power supply, NETWORK LTE the mobile network, NETWORK LAN the wired network, TROUBLE a fault; the INTERFACE LED has no function on the GET.

NETWORK LTE – mobile network connection

Indication	Meaning
off	No connection to the mobile network
flashing yellow	Connecting to the mobile network
steady green, flashing yellow	Connected to the mobile network; the number of yellow flashes is the **signal level**: on 4G, 3 flashes mean an adequate signal

NETWORK LAN – wired network connection

Indication	Meaning
off	No connection to the computer network
steady green	Connected to the computer network

DATA – data traffic

Indication	Meaning
off	No events waiting to be sent
steady green	There are events waiting to be sent in the buffer
flashing green	Data transfer between the communicator and the computer (during programming)

Quick check

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.

POWER – power supply

Indication	Meaning
off	No power, or the power supply is disconnected
steady green	Switched on, the supply voltage is adequate
steady yellow	Inadequate supply voltage (11.5 V or less)
steady green, flashing yellow	Ready for programming (during programming)
steady yellow (during programming)	No connection to the computer

TROUBLE – fault

Indication	Meaning
off	No fault
1 red flash	Fault in the physical connection of the wired network (PHY Link) – check the LAN cable
2 red flashes	SIM1 card fault
3 red flashes	SIM2 card fault
7 red flashes	The connection to the alarm control panel has been lost (serial bus)

INTERFACE – not used on the GET.

1.7 Technical specifications

Parameter	Value
Network connection	LTE (4G) and Ethernet (LAN)
Connection to the alarm control panel	serial bus, data bus (Keybus) or telephone line (TIP/RING, Contact ID, DTMF)
Inputs/outputs	2 dual-function I/Os: as an input NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (2.2 kΩ end-of-line resistor); as an output open collector (OC), max. 0.15 A / 30 V DC
Modem	EG915U-EU (Europe), EG915U-LA (Latin America) or BG95-M5 (LTE Cat M1) – the frequency bands are listed in the table of section 1.2
SIM card	2 nano SIM holders (SIM1, SIM2)
Supply voltage	10–18 V DC
Current consumption	up to 100 mA in standby; up to 300 mA while sending data
Transmission protocols	TRK8, DC-09_2007, DC-09_2012, TL150
Encryption	AES-128

Parameter	Value
Event buffer	60 events
Programming	TrikdisConfig (Windows) over a USB-C cable or remotely; Protegus 2 app (from firmware 1.08)
Operating environment	−10 … +50 °C, max. 80 % relative humidity (at +20 °C)
Size	113 × 70 × 25 mm
Weight	110 g

2. Quick start

The communicator can be set up with two tools: the Windows software called **TrikdisConfig** – over a USB-C cable or remotely – and the **Protegus 2 app** (Settings → Advanced settings). This chapter describes the shortest route: which settings are needed for the communicator to send events to the monitoring station, and for the system to be controllable from the Protegus 2 app. For every step we give both the app path and the TrikdisConfig path; the settings are explained in detail in chapter 6.

2.1 Preparation

What you will need

USB-C cable for programming · cable with at least 4 cores between the communicator and the control panel · CRP2.4 cable for the Paradox serial port · 2.5 mm flat screwdriver · a mobile antenna with suitable gain if coverage is weak at the site · an active SIM card (one or two; the PIN request can be switched off) if you use the mobile network · an Ethernet cable to the router or switch if you use the wired network · the installer manual of the alarm control panel.

Order the required accessories separately from the distributor.

Setup with TrikdisConfig. You set the device up on the desk, before wiring; afterwards, at the site, you only need to wire it in.

1. Download and install the TrikdisConfig software. On the Trikdis website (www.trikdis.com), type "TrikdisConfig" in the search field.

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!

2. Open the communicator's case with a flat screwdriver: insert the screwdriver into the slot at the top, next to the antenna, and lever outwards, then at the bottom, at the opening, downwards. The figure also shows the location of the USB-C socket on the edge of the printed circuit board.

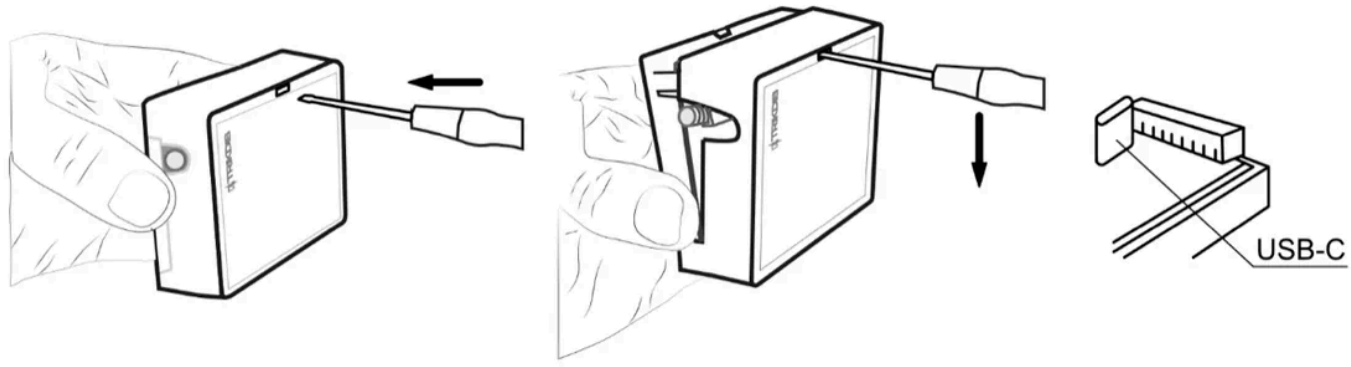


Figure 3. Snapping off the front cover with a flat screwdriver; the enlarged detail shows the location of the USB-C socket.

3. Insert the nano SIM card (or cards) into the holder, in the orientation shown in the figure: the SIM1 holder is in the middle of the printed circuit board, SIM2 is at the edge. The card must be active and have mobile data service, and if possible, switch off its PIN request in a phone (so you do not have to enter a PIN in the device). If you use the communicator on the wired network only, no SIM card is needed.

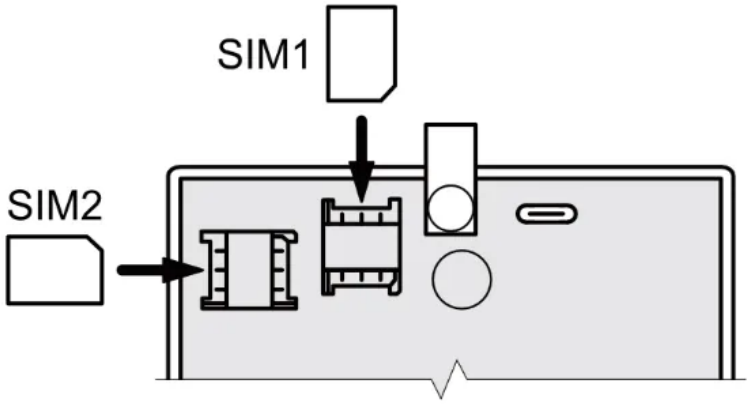


Figure 4. Location of the SIM1 and SIM2 holders on the printed circuit board; the arrows show the direction for inserting the card.

4. Connect the communicator to the computer with a USB-C cable.

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

5. Start TrikdisConfig. The program recognizes the device and opens the programming window. Click the **Read [F4]** button: the program reads the device's current settings. If it asks for a password, enter the 6-digit administrator code (default `123456`) or installer code (default `654321`).

Setup from the Protegus 2 app. You can make settings from the app if the communicator is already online and you have added it to your Protegus account (section 5.1). If the communicator cannot connect yet – for example because the SIM card asks for a PIN code, or the operator requires a different APN –, do the first setup with TrikdisConfig.

1. In the app, open the system and go to the **Settings** → **Advanced settings** menu.

2. The first time, the app warns you (**Proceed with Caution**): these settings are meant for professionals. Tap the **Accept the risk and continue** button; with the **Do not show this again** tick the warning will not appear next time.
3. The app reads the communicator's settings. If it asks for a **Service Access code**, enter the communicator's Protegus Cloud access code (default `123456`).
4. Make the settings described below, then tap the **Write** button: the app writes them into the communicator.

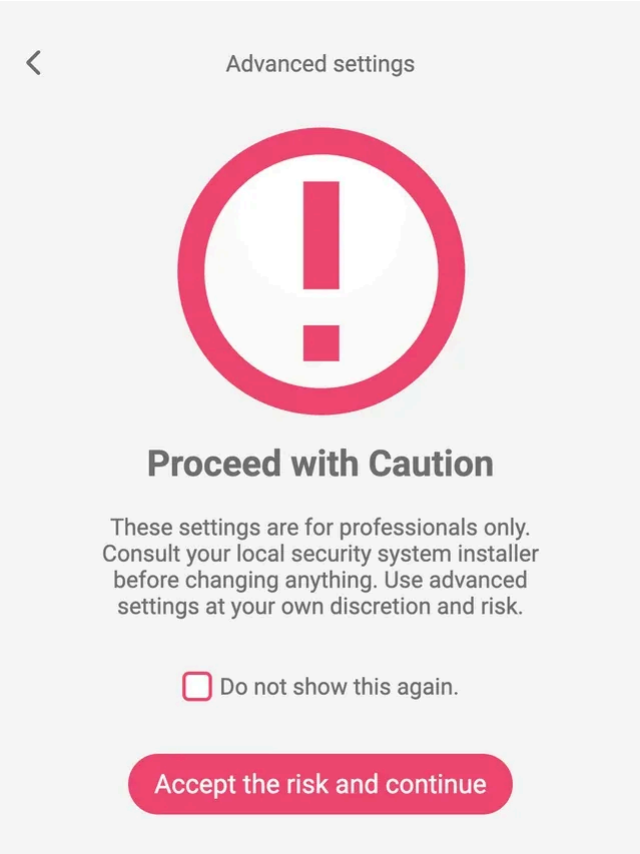


Figure 5. Protegus 2 – the warning shown when Advanced settings is opened for the first time (Proceed with Caution) and the Accept the risk and continue button.

The GET can be set up from the Protegus 2 app with **firmware 1.08 or newer** (updating is described in chapter 9).

2.2 Connection to the Protegus 2 app

In the app (Settings → Advanced settings):

1. **Panel settings** → **TLF** – if the communicator is connected to the control panel's TIP/RING terminals: set **Security panel model** to **AUTO**.
2. **Panel settings** → **Serial Bus** – if the communicator is connected to the control panel's data bus or serial port: in the **Security panel model** field, select the type of the connected control panel.
3. In the same place, switch on the **Remote Arm/Disarm** option if the users want to control the control panel from Protegus 2 with their own keypad code. It only appears for directly controllable control panels.
4. For direct control of a Paradox control panel, enter the **PC download password**, for a Texecom control panel the **UDL passcode**; it must match the password set in the control panel.

5. **User reporting** → **Cloud**: switch on the **Enabled** option, and change the **Cloud access code** if you want the user to have to enter it when the system is added to the app (default `123456`).
6. **Network settings** → **LAN** – if the communicator is connected to the wired network: switch on the **Use DHCP** option.
7. **Network settings** → **SIM** and **SIM2** – for every inserted SIM card: enter the **SIM card PIN** and the **APN**, and check that **DNS1** and **DNS2** work with your operator.
8. **Reporting to CMS** → **CMS settings** → **Reporting mode**: in the **Main type**, **Backup type** and **Backup type 2** fields, set the order in which the communicator uses the **LAN**, **SIM** (SIM1) and **SIM2** connections.
9. Tap the **Write** button.

In TrikdisConfig. First, on the **Panel settings** page, set how the communicator connects to the control panel.

If you connect it to the control panel's telephone line output (TIP/RING): in the **Communication protocol** field, select **AUTO**.

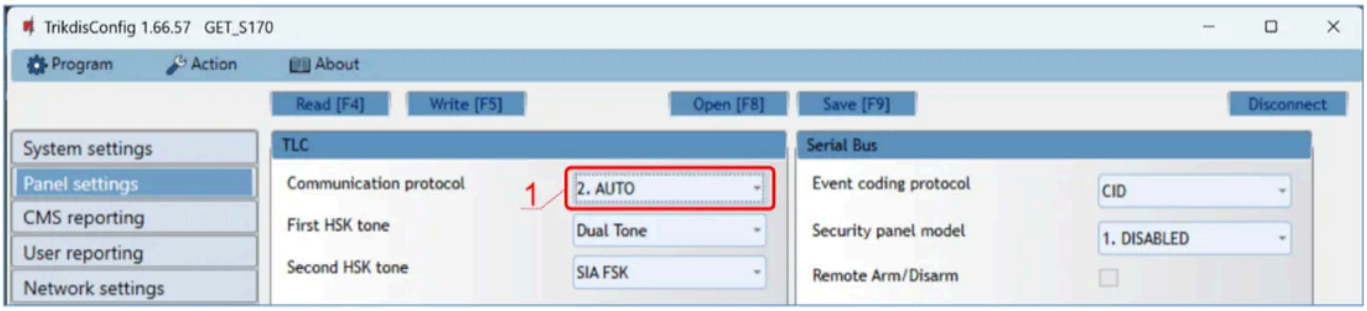


Figure 6. TrikdisConfig – Panel settings, TLC group.

- 1 **Communication protocol** – **2. AUTO** for TIP/RING connection.

If you connect it to the control panel's data bus or serial port: set up the control panel in the **Serial bus** group.



Figure 7. TrikdisConfig – Panel settings, Serial bus group.

- 2 **Security panel model** – the type of the connected control panel.
- 3 **Remote Arm/Disarm** – tick it if the users want to control the control panel from Protegus 2 with their own keypad code. It only appears for directly controllable control panels.
- 4 **Security panel PC download password** – for direct control of a Paradox or Texecom control panel, the PC or UDL password set in the control panel; the two must match.

For direct control the alarm control panel must also be set up – this is described in chapter 4, where you will also find how to enter the PC or UDL password.

Then, on the **User reporting** page, on the **PROTEGUS Cloud** tab, enable the cloud connection.

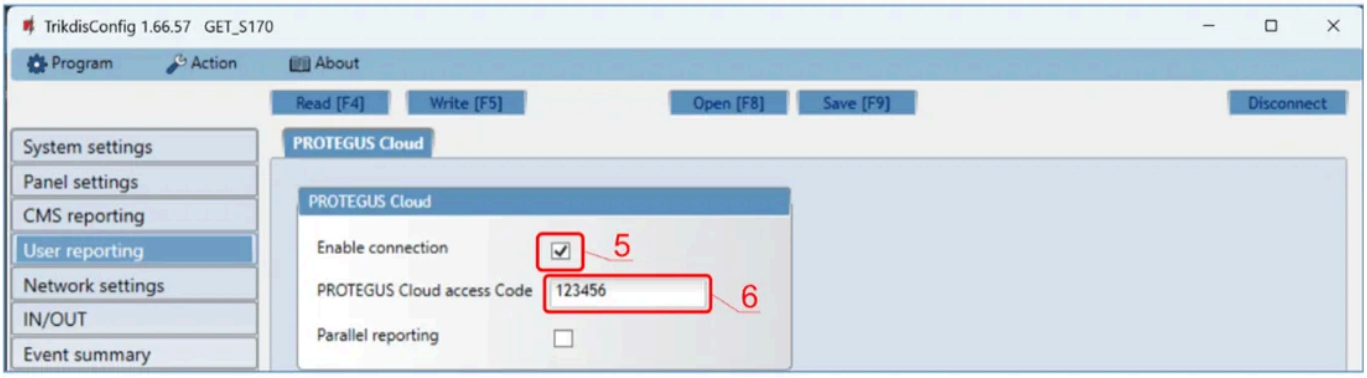


Figure 8. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- 5 **Enable connection** – tick it: it enables the connection to the Protegus cloud.
- 6 **PROTEGUS Cloud access Code** – the access code for Protegus 2 (default `123456`). Change it if you want the user to have to enter it when the system is added to the app. If you change the code later, it must also be changed in the Protegus 2 app.

If the communicator is connected to the wired network, on the **Network settings** page, on the **LAN** tab, tick the **Use DHCP** option: the communicator automatically receives the network settings (subnet mask, gateway) and gets an IP address.

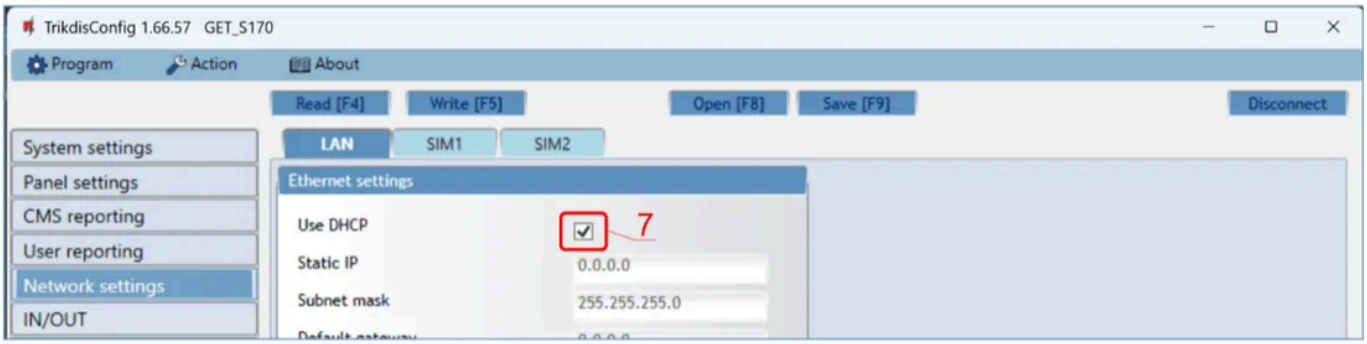


Figure 9. TrikdisConfig – Network settings, LAN tab (Ethernet settings).

- 7 **Use DHCP** – when ticked, the communicator automatically gets an IP address and network settings from the router.

If there is a SIM card (one or two cards) in the communicator, enter the card's data on the **SIM1** (and **SIM2**) tab.

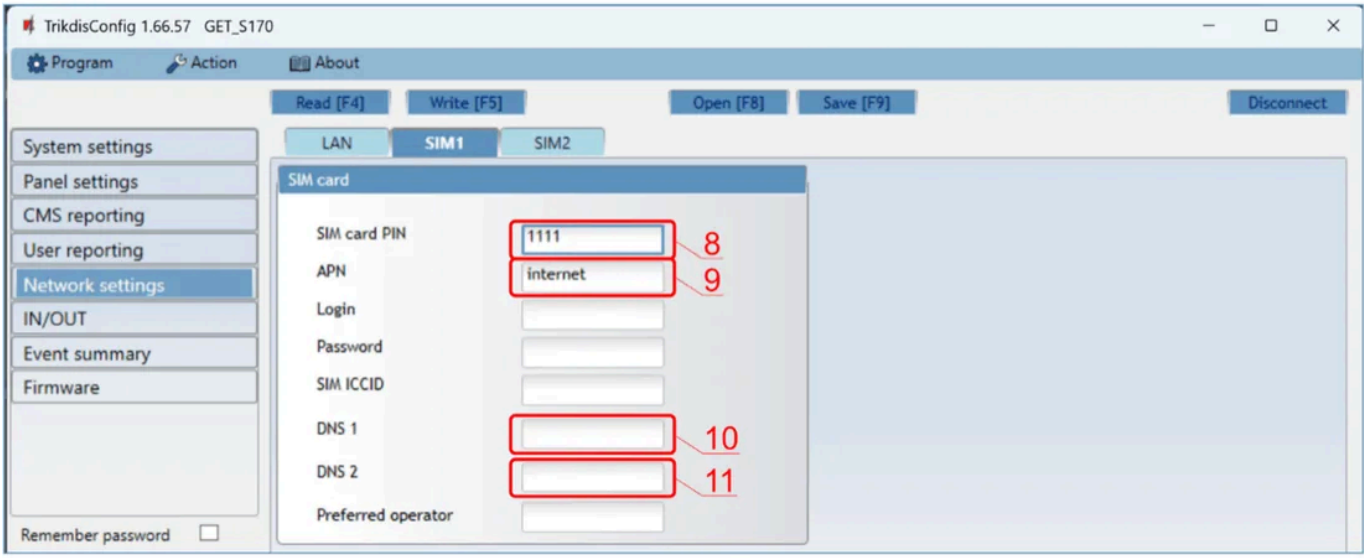


Figure 10. TrikdisConfig – Network settings, SIM1 tab.

- 8 **SIM card PIN** – the card's PIN code (if the PIN request is switched off, the default value can stay).
- 9 **APN** – the operator's data access point (see below).
- 10 **DNS 1** – primary name server; by default Google's DNS. Regardless of the IP settings, check that the DNS addresses work with your operator.
- 11 **DNS 2** – secondary name server (by default also Google's).

The APN (Access Point Name) is the mobile operator's data access point; without it the device cannot connect to the internet over the mobile network. You can find the exact value on the website of the SIM card's operator. We keep the known APNs of European operators in a separate article: APN settings – list of European mobile operators. If you have no other data from the operator, try the APN `internet`: it is generic and works in many operators' networks.

For IoT / M2M (machine-to-machine) data cards, the operator usually gives **a different APN than for consumer cards** – with the consumer APN the device does not connect. You can also find this value in the APN article, or ask the operator for it; if the operator also gives a user name and password, enter those as well.

Finally, on the **CMS reporting** page, on the **Settings** tab, in the **Reporting mode** group, set the order of the connections: this is the path on which the communicator sends the messages to the monitoring station and to Protegus 2.

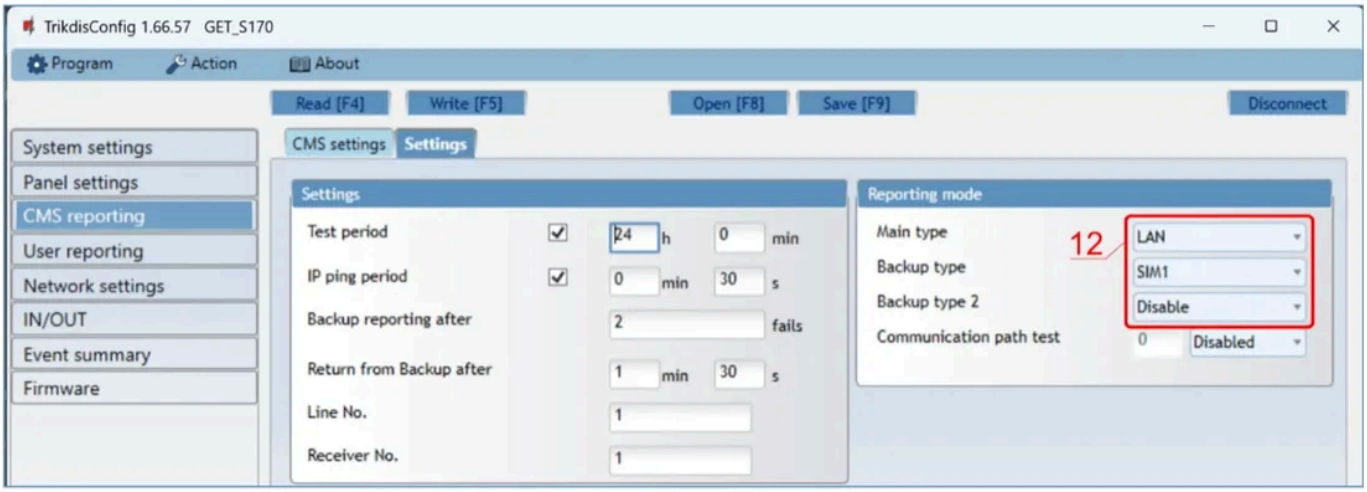


Figure 11. TrikdisConfig – CMS reporting, Settings tab, Reporting mode group (default: Main type LAN, Backup type SIM1, Backup type 2 Disable).

- 12 **Reporting mode** – **Main type**: the main connection (LAN, SIM1 or SIM2); **Backup type**: the backup; **Backup type 2**: the second backup.

You enter the connection types in order. If the communicator cannot connect with the **Main type** connection, it switches to the **Backup type**, and so on. If the backup connection has successfully delivered the message to the monitoring station, the communicator tries to return to the main connection after the set time (section 6.4.2).

If the device does not report to a monitoring station, the setup is now complete: press the **Write [F5]** button, wait for the confirmation, and unplug the USB cable.

With a telephone line (TIP/RING) connection, do not forget to switch on and set up the alarm control panel's dialer, otherwise the control panel sends no events; for direct control, the Paradox, Texecom, Caddx, InnerRange and Honeywell control panels must also be set up. Setting up the control panel is described in chapter 4.

2.3 Connection to the monitoring station

In the app (Settings → Advanced settings):

1. **System options** → **System general**: enter the account number received from the monitoring station (**Account No.**; 0–9, A–F; `FFFE` and `FFFF` cannot be used). On hardware version **x1x1**, with firmware **1.31** or newer, you enter the account number per channel: **Reporting to CMS** → **CMS settings** → **Primary channel** → **Primary Account no.** You can recognize this on the screen: if System general only shows the **Time set** field, use the channel setting.
2. **Panel settings** → **TLF** (TIP/RING connection): set **Security panel model** to **AUTO**; or **Panel settings** → **Serial Bus** (data bus or serial connection): select the **Security panel model**.
3. **Reporting to CMS** → **CMS settings** → **Primary channel**: switch on the **Enabled** option, then enter: **Communication type**: **IP**; the receiver's **Domain or IP** address and **Port**; **TCP or UDP**; **Protocol**: **TRK8** for a Trikdis receiver, **DC-09_2007** or **DC-09_2012** for a universal receiver, **TL150** for a SUR-GARD receiver; and the encryption key set in the receiver: with the TRK protocol in the **TRK encryption key** field, with DC-09 switch on the **Enable encryption key** option and enter the **DC-09 encryption key**.
4. (Recommended) Set up the **Backup channel** in the same way.
5. **Reporting to CMS** → **CMS settings** → **Reporting mode**: **Main type**, **Backup type**, **Backup type 2**.

6. **Network settings** → **LAN** (wired network): switch on the **Use DHCP** option. **Network settings** → **SIM** and **SIM2** (for every SIM card): **SIM card PIN**, **APN**, and check the **DNS1**, **DNS2** fields.
7. Tap the **Write** button.

In TrikdisConfig. First, on the **System settings** page, enter the account number.



Figure 12. TrikdisConfig – System settings page, General group.

- 1 **Object ID** – the account number received from the monitoring station (6 hexadecimal characters, 0–9, A–F). `FFFE` and `FFFF` cannot be used.

On the **Panel settings** page, set the control panel connection if you have not done so in section 2.2: for a TIP/RING connection set **Communication protocol** to **AUTO**; for a data bus or serial connection select the type of the connected control panel in the **Security panel model** field (the figures in section 2.2).

Then, on the **CMS reporting** page, on the **CMS settings** tab, in the **Primary channel** section, set the receiver's data. The picture shows the window before setup: the **Communication type** field of the primary channel is still **Disable**.

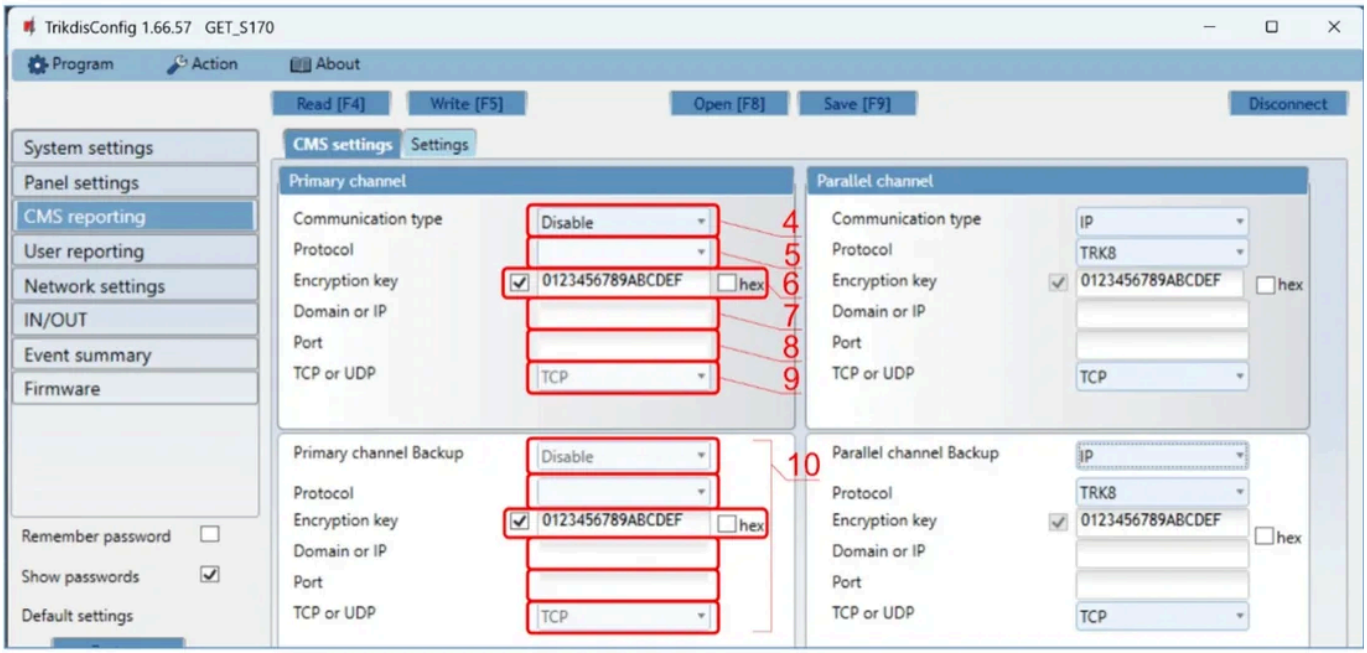


Figure 13. TrikdisConfig – CMS reporting, CMS settings tab.

- 4 **Communication type** – select the **IP** connection.
- 5 **Protocol** – **TRK8** for a Trikdis receiver, **DC-09_2007** or **DC-09_2012** for a universal receiver, **TL150** for a SUR-GARD receiver.
- 6 **Encryption key** – the encryption key set in the receiver.
- 7 **Domain or IP** – the receiver's domain name or IP address.
- 8 **Port** – the receiver's port number.
- 9 **TCP or UDP** – the transmission protocol; it follows the receiver's setting.
- 10 **Primary channel Backup** – backup channel for a failure of the primary; fill it in the same way, it is recommended.

On the **Settings** tab, in the **Reporting mode** group, set the order of the connections (**Main type**, **Backup type**, **Backup type 2**) if you have not done so in section 2.2 – you will find the figure and the description of how it works there as well.

Finally, on the **Network settings** page, enter the network data if you have not done so in section 2.2: on the **LAN** tab the **Use DHCP** tick, on the **SIM1** (and **SIM2**) tab the card's data (**SIM card PIN**, **APN**, **DNS 1, DNS 2**).

With the **DC-09** protocol, also enter the line and receiver number on the **Settings** tab (**Line No.**, **Receiver No.**, section 6.4.2). The GET reports to the monitoring station only over an IP connection – the wired network or the mobile internet –; it has no SMS backup channel.

At the end of the settings, press the **Write [F5]** button, wait for the confirmation, and unplug the USB cable. The device is now ready to be wired in. With a telephone line connection, the alarm control panel's dialer must also be switched on and set up here, otherwise the control panel sends no events (chapter 4).

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.

3.1 Installation steps

1. Remove the front cover (see section 2.1), and pull off the terminal block.
2. Insert the nano SIM card – or both – into its holder, if you have not done so during commissioning.
3. Take the printed circuit board out of the back cover: open the latch next to the antenna connector, and lift the board out (see the figure).
4. Fix the back cover with screws in the chosen place (the screw holes are circled in the figure), or, as described in section 3.2, with the supplied double-sided adhesive tape.
5. Put the printed circuit board back into the back cover, and plug the terminal block back in.
6. Screw on the mobile antenna.
7. Put the front cover back.
8. If you also send the events to the monitoring station over the wired network (LAN), plug the network cable into the communicator's LAN socket.

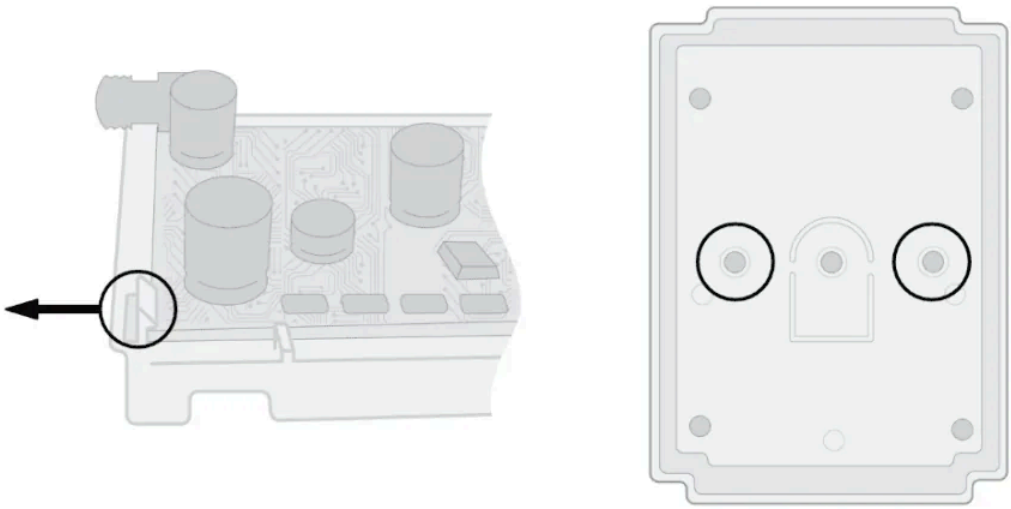


Figure 14. Lifting the printed circuit board out of the back cover (left: the latch and the lifting direction) and the screw holes of the back cover (right).

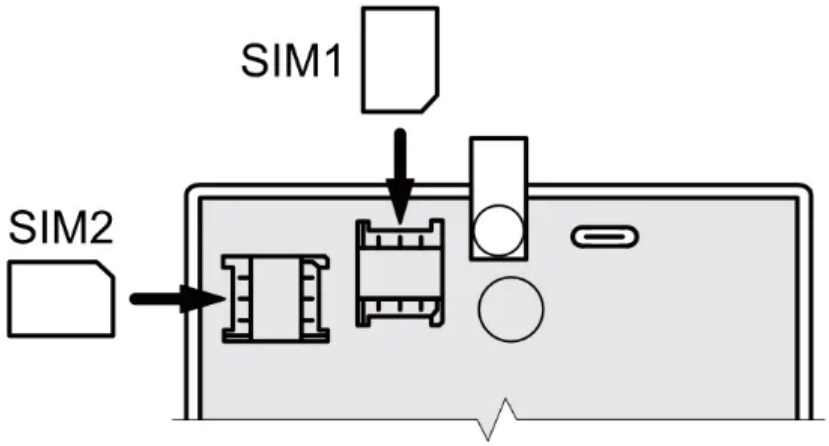


Figure 15. Location of the two SIM holders on the printed circuit board: SIM1 in the middle of the board, SIM2 at its left edge; the arrows show the direction for inserting the card.

One or two SIM cards can be inserted into the communicator. The card must be active, and for IP-based use the mobile data connection must work on it. If you do not want TrikdisConfig to ask for a PIN code, put the card into a mobile phone and switch off the PIN request there.

3.2 Placement in the control panel's enclosure, antenna

The communicator must be placed in the alarm control panel's **enclosure protected by a cover tamper switch**. Fix it to the inner back wall of the enclosure with the supplied industrial-grade double-sided acrylic foam tape: stick the tape on a clean, dry surface with firm pressure so that it holds securely. If the control panel's enclosure does not allow this secure fixing, the communicator can also be mounted in a separate, tamper-protected enclosure.

- In a **metal enclosure** the mobile signal is strongly attenuated. If the communicator goes into the control panel's metal housing, lead the antenna outside the enclosure, or use an antenna with a longer cable.
- Before final fixing, **check the signal level**: the number of yellow flashes of the NETWORK LTE LED must be at least 3 on 4G (section 1.6). If it is less, find a better place for the antenna, or switch to a more sensitive antenna that can be placed further away.

- Keep the antenna and the communicator away from the control panel's transformer and from mains wiring.
- Lead the LAN cable through the enclosure's cable entry into the RJ45 socket on the side of the communicator; the cable must not pull on the terminals.



A mobilhálózatos átjelzőhöz gyári tartozékként egy alap ANT01S GSM antenna jár. Ha a telepítés helyén gyenge jelszint várható, vagy ha az eszközt fémdoboz vagy vastag fal árnyékolja, javasolt nagyobb teljesítményű, például 2,5 m-es vezetékkel rendelkező ME301M mágneses vagy ANT04 felragasztható antenna használata.

3.3 Connection to the alarm control panel

Follow the diagram below that matches your control panel. On the diagrams **+DC** and **–DC** are the communicator's **+12 VDC** / **–12 VDC** power terminals, and **A RS485** / **B RS485** are the **A 485** / **B 485** terminals (these do not need to be connected on the GET). The communicator gets its power from the control panel's auxiliary power output (AUX), so during a power cut the control panel's battery also powers the communicator.

3.3.1 DSC – data bus (Keybus)

Connect the DSC control panel's Keybus to the communicator with four wires: **RED** → **+DC**, **BLK** → **–DC**, **YEL** → **CLK**, **GRN** → **DATA**.

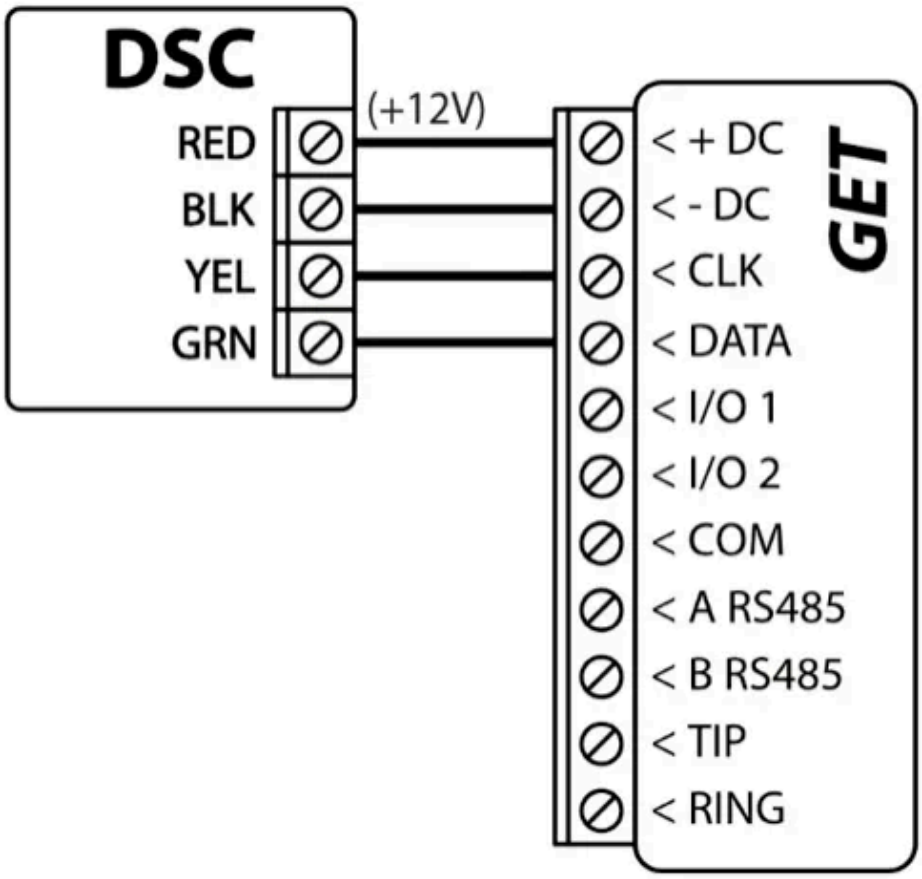


Figure 16. Connecting a DSC control panel on the data bus (Keybus, "Keypad bus"): RED → +DC, BLK → −DC, YEL → CLK, GRN → DATA.

The GET handles the DSC control panel on the data bus only; connecting the Keybus and the TIP/RING terminals together is only available on the GT+ communicator. When connected to the Keybus only, the communicator receives the general state of the zones from the control panel, but not the zone type (fire, burglary, water leak, etc.), so it reports every alarm as a **general alarm, with the Contact ID code E130**. If the monitoring station needs the control panel's own codes (for example fire alarm: E110), you can send the events with the control panel's telephone line dialer, with a TIP/RING connection (sections 3.3.9 and 4.2); in that case there is no direct control.

3.3.2 Paradox – serial port

The communicator connects to the Paradox control panel's serial port with the **EX-CRP2.4** cable, ordered separately: **red → +DC**, **black → −DC**, **yellow → CLK**, **green → DATA**.

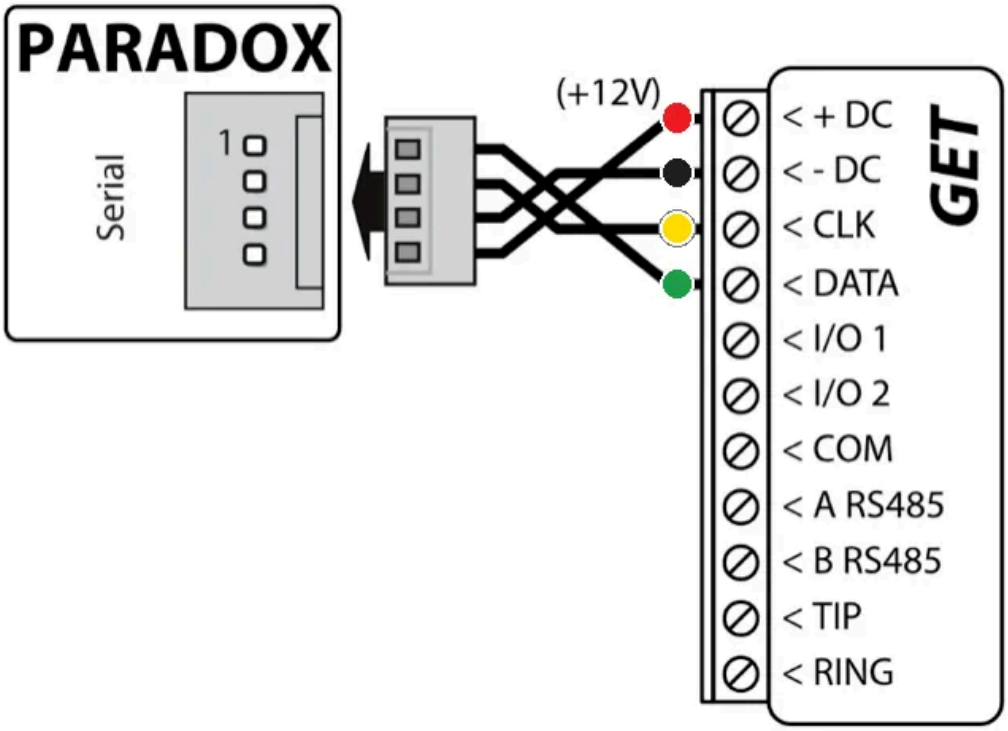


Figure 17. Connecting a Paradox control panel on the serial port with the EX-CRP2.4 cable (to be ordered separately; "Use the EX-CRP2.4 cable (ordered separately)"): red → +DC, black → −DC, yellow → CLK, green → DATA.

- red wire ("R - red")
- black wire ("B - black")
- yellow wire ("Y - yellow")
- green wire ("G - green")

On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2. With the Spectra SP / SP+ and Magellan MG / MG+ control panels, the connection described in the next section can also be used instead of the serial port.

3.3.3 Paradox SP/MG – Keybus and TIP/RING

The Paradox Spectra SP, SP+ and Magellan MG, MG+ control panels can also be connected to their data bus (Keybus) and TIP/RING terminals together instead of the serial port: **+AUX** → **+DC**, **−AUX** → **−DC**, **GRN** → **DATA**, **YEL** → **CLK**, and **TIP** → **TIP**, **RING** → **RING**. This connection uses the control panel's Keybus instead of the serial port, so the paid Paradox serial port unlocking is not needed for it.

For this connection the communicator's firmware must be at least **1.21** (updating is described in chapter 9).

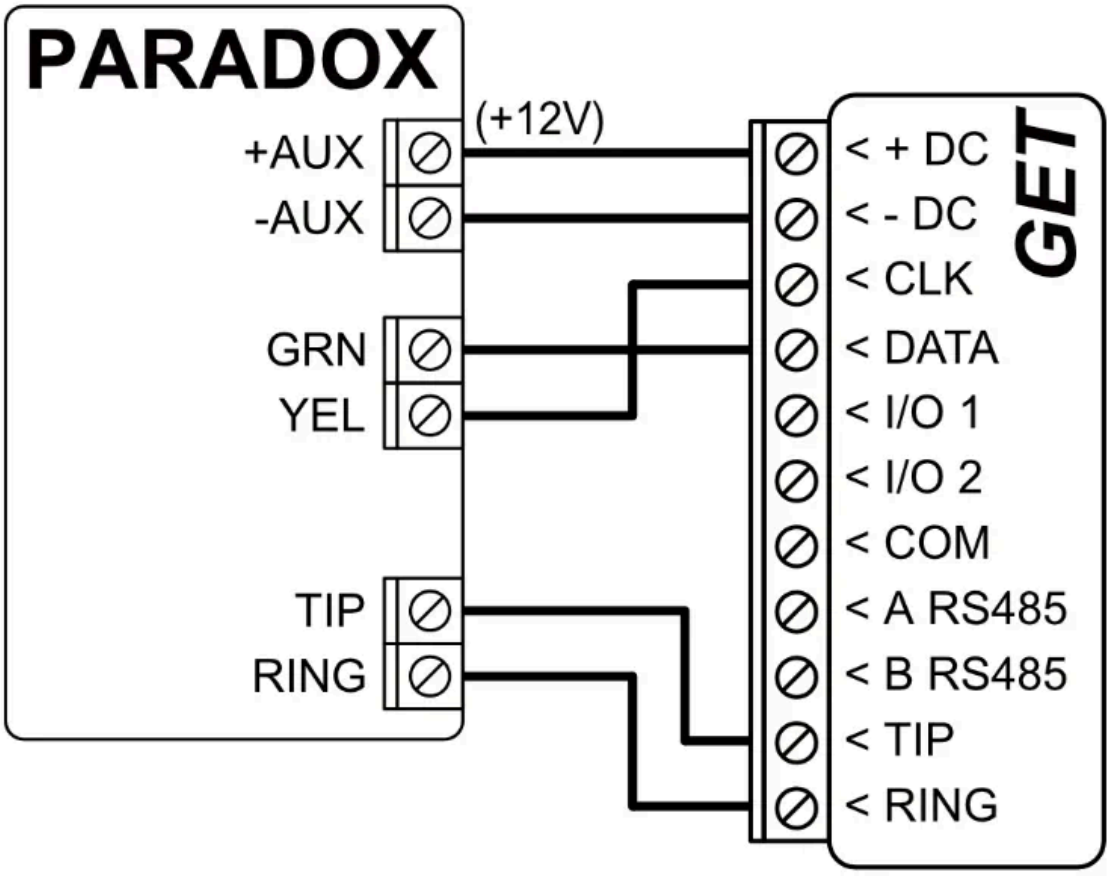


Figure 18. Connecting a Paradox SP / SP+ / MG / MG+ control panel on the Keybus (data bus, "Keypad bus") and the TIP/RING terminals together: +AUX → +DC, −AUX → −DC, GRN → DATA, YEL → CLK, TIP → TIP, RING → RING.

For this connection, set the following on the TrikdisConfig **Panel settings** page:

1. **Communication protocol**: **2. AUTO**.
2. **Security panel model**: select **Paradox SP+/MG+ series KeyBus** from the list (in the picture 7. PARADOX SP+/MG+).
3. **Remote Arm/Disarm**: tick it if the users want to control the control panel from the Protegus 2 app with their own keypad code.
4. **Security panel PC download password**: for direct control, enter the PC password set in the control panel; the two must match.

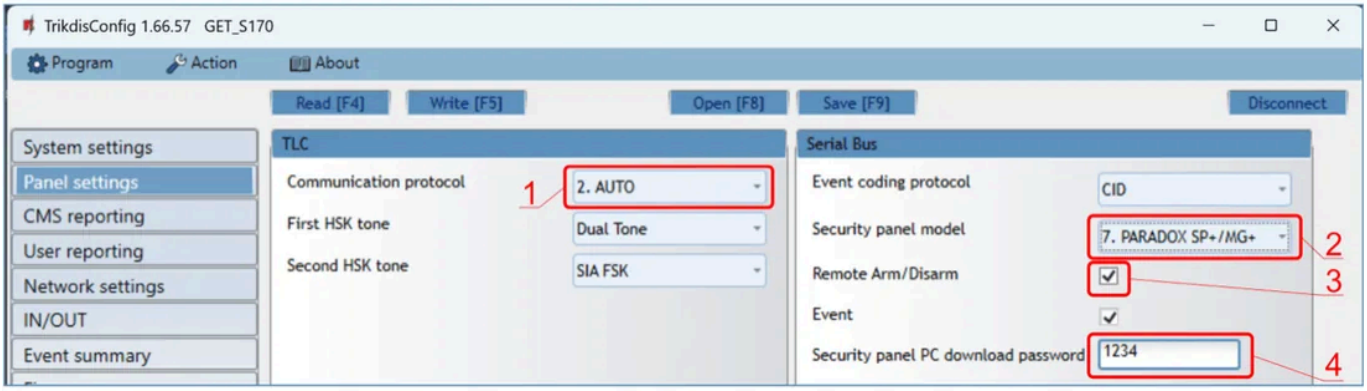


Figure 19. TrikdisConfig – Panel settings for the Keybus + TIP/RING connection: Communication protocol 2. AUTO (1), Security panel model 7. Paradox SP+/MG+ (2), Remote Arm/Disarm ticked (3), Security panel PC download password entered (4).

In the Protegus 2 app the same settings are on the **Panel settings** → **TLF** (Security panel model = Communication protocol) and **Panel settings** → **Serial Bus** pages (section 6.3).

The Paradox control panel must also be programmed so that it sends the events to the monitoring station and can be controlled from Protegus 2 – on the keypad connected to the control panel, set the following sections:

Section	Value	Section	Value
801	`********`	**815**	`123456`
811	`1111`	**911**	`1234`
812	`2222`		

The PC password entered in section **911** must match the communicator's **Security panel PC download password** field (section 4.1.2).

3.3.4 UTC Interlogix (Caddx) – data bus

Connect the Caddx NetworX control panel's data bus to the communicator with three wires: **POS** → **+DC**, **COM** → **–DC**, **DATA** → **DATA**. The CLK, TIP and RING terminals are not needed.

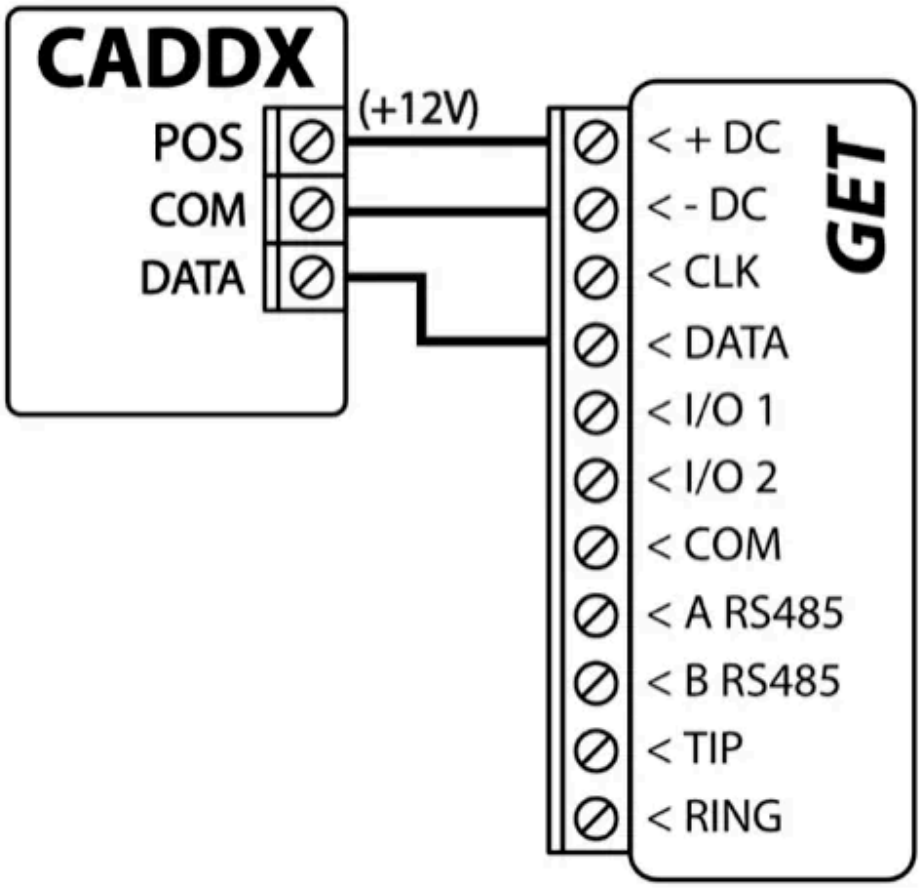


Figure 20. Connecting a UTC Interlogix (Caddx) NetworX control panel on the data bus ("Keypad bus"): POS → +DC, COM → –DC, DATA → DATA.

3.3.5 Texecom – serial port

The communicator connects to the Texecom Premier / Premier Elite control panel's serial port with the **EX-CRP4** cable, ordered separately: **red** → **+DC**, **black** → **–DC**, **blue** → **CLK**, **white** → **DATA**.

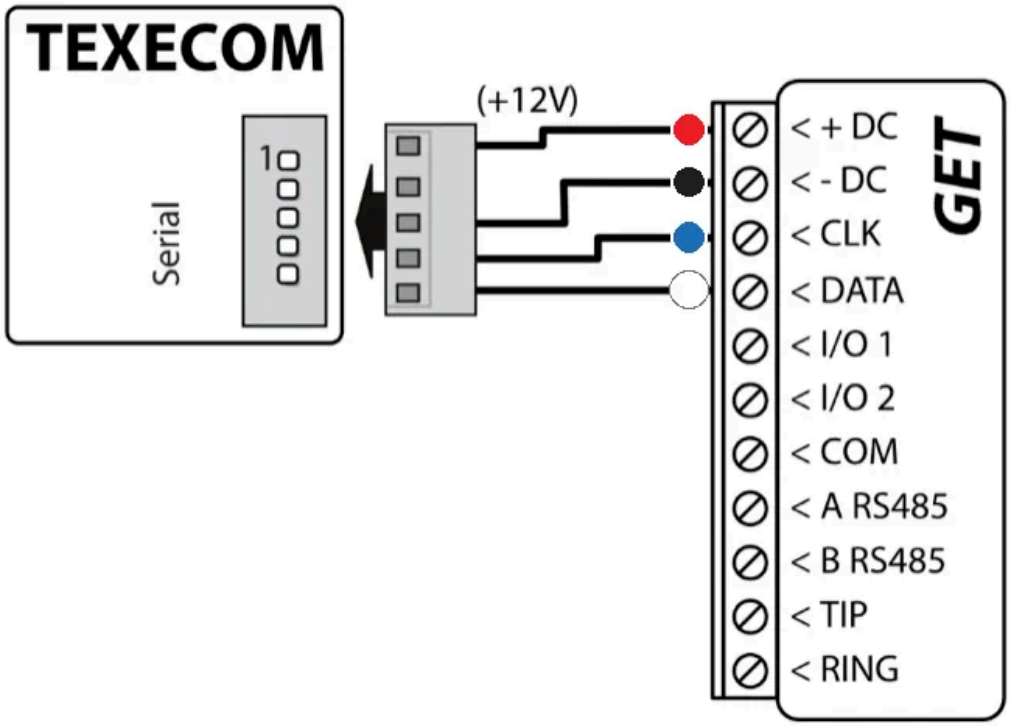


Figure 21. Connecting a Texecom control panel on the serial port with the EX-CRP4 cable (to be ordered separately; "Use the EX-CRP4 cable (ordered separately)"): red → +DC, black → −DC, blue → CLK, white → DATA.

- red wire ("R - red")
- black wire ("B - black")
- blue wire ("BL - blue")
- white wire ("W - white")

3.3.6 InnerRange Inception

The communicator gets its power from the Inception control panel's power output (**VOUT + → +DC**, **VOUT 0V → −DC**), and the data connection comes from the control panel's USB port, with Inner Range's **993030USB** cable: **black → 0V / −DC**, **green → CLK**, **white → DATA**.

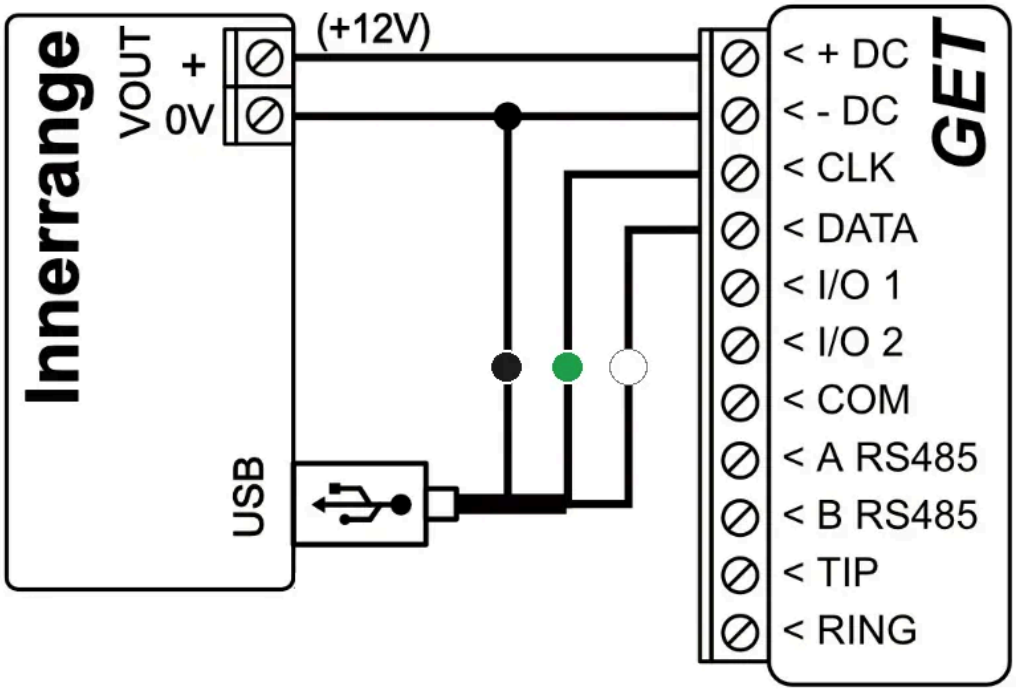


Figure 22. Connecting an InnerRange Inception: VOUT + → +DC, VOUT 0V → −DC; from the USB port with the 993030USB cable ("Cable, Inner Range part number 993030USB") black → −DC, green → CLK, white → DATA.

- black wire ("Black wire")
- green wire ("Green wire")
- white wire ("White wire")

3.3.7 InnerRange Integriti

The communicator connects to the **Port 0** serial port of the Integriti control panel with Inner Range's **INTG-996795** cable: **+DET (+13 V)** → **+DC**, **GND (5)** → **−DC**, **Rx (3)** → **CLK**, **Tx (2)** → **DATA**.

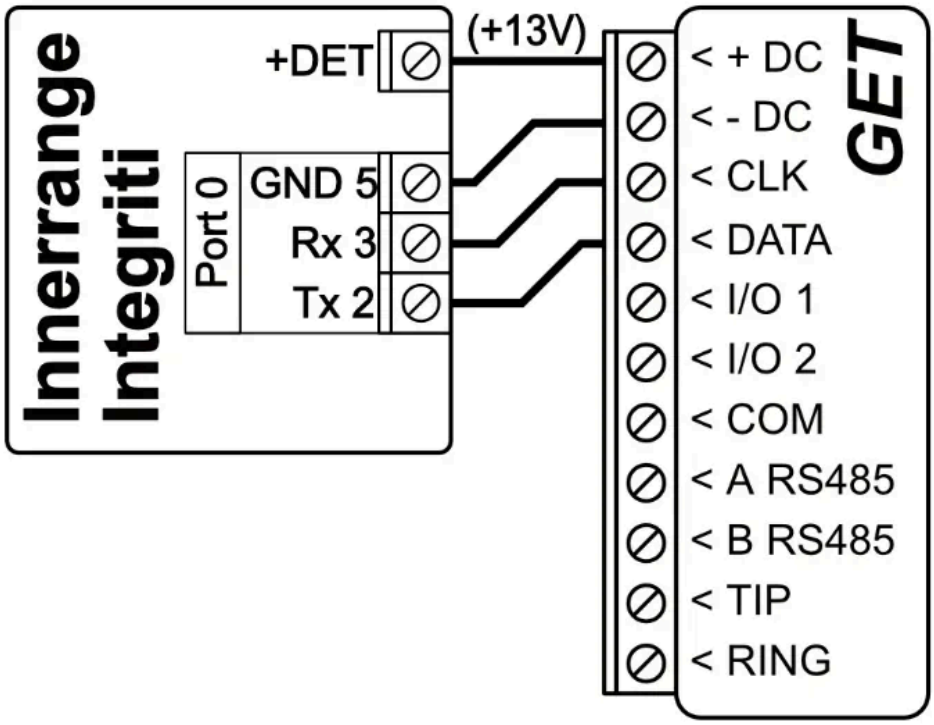


Figure 23. Connecting an InnerRange Integriti to Port 0 with the INTG-996795 cable ("Cable, Inner Range part number INTG-996795"): +DET → +DC, GND 5 → −DC, Rx 3 → CLK, Tx 2 → DATA.

3.3.8 Honeywell Vista – data bus

Connect the keypad bus of the Honeywell Ademco Vista-15, Vista-20 and Vista-48 control panels from the control panel's terminals to the communicator: **5** → **+DC** (+12 V), **4** → **−DC**, **7** → **CLK**, **6** → **DATA**.

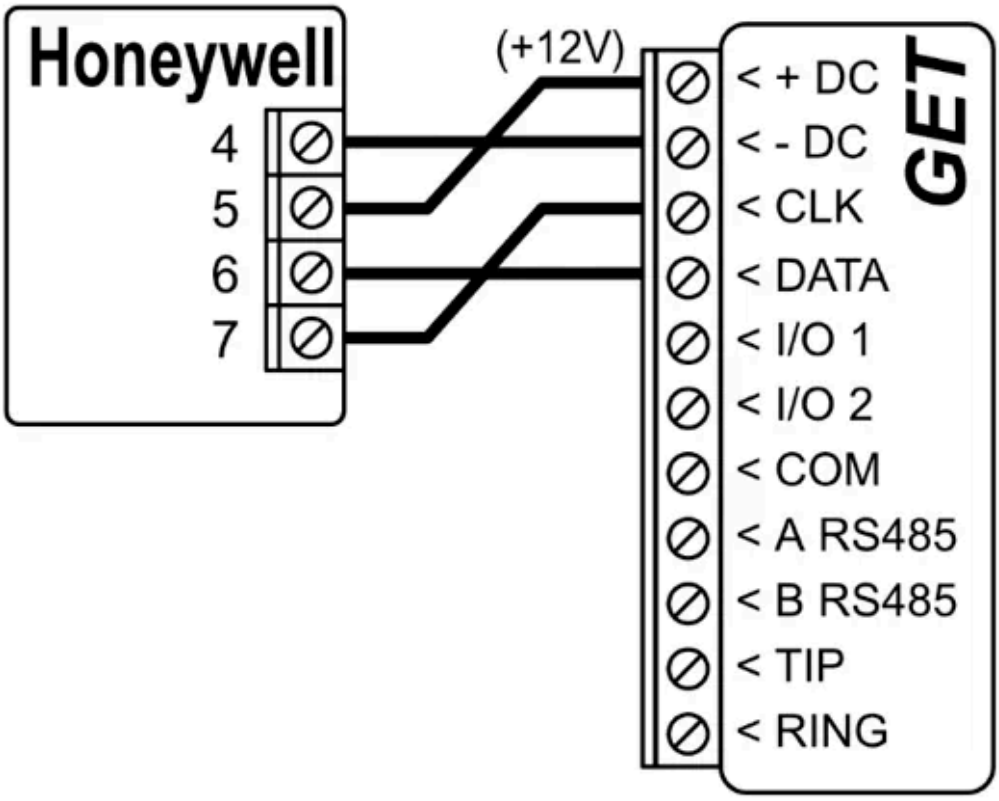


Figure 24. Connecting a Honeywell Vista-15 / -20 / -48 control panel on the data bus ("Keypad bus"): terminal 5 → +DC, 4 → −DC, 7 → CLK, 6 → DATA.

3.3.9 Any control panel – TIP/RING

Any other control panel can be connected through its telephone line communicator: power from the control panel's auxiliary power output (**+AUX** → **+DC**, **–AUX** → **–DC**), the telephone line output to the communicator's **TIP** and **RING** terminals (**TIP** → **TIP**, **RING** → **RING**). The control panel's dialer must be set up (section 4.2).

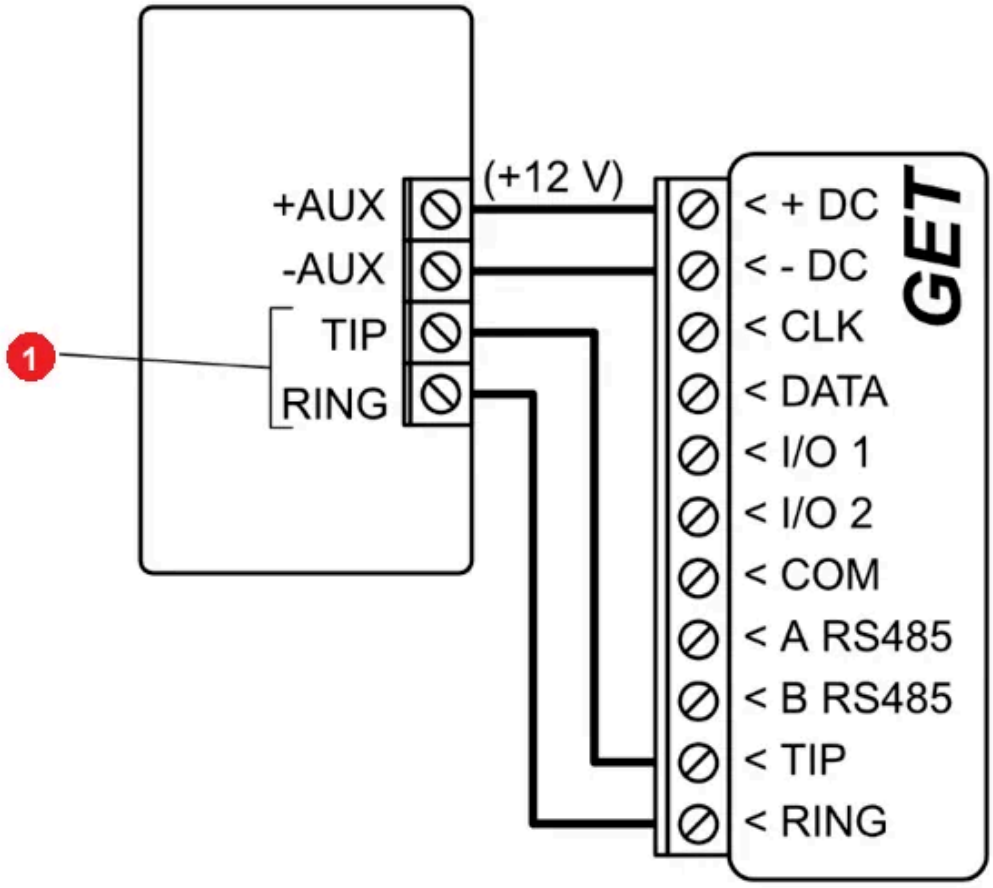


Figure 25. Connection to the telephone line communicator of the control panel ("Control panel"): +AUX → +DC, –AUX → –DC, TIP → TIP, RING → RING.

- 1 terminals of the control panel's telephone line communicator ("Telephone line communicator terminals")

3.4 Wiring a keyswitch zone

Follow this wiring if you want to arm and disarm the control panel from the Protegus 2 app with the communicator's output (PGM) switching the control panel's **keyswitch zone**. The communicator's two dual-function I/O terminals work as outputs (OUT, PGM) – on the GET both are outputs by default –, so the two outputs can control two partitions of the system: connect the keyswitch zone of partition 1 to the **1 I/O** terminal, and that of partition 2 to the **2 I/O** terminal. With this wiring, untick **Remote Arm/Disarm** on the TrikdisConfig **Panel settings** page, set the terminals to the **OUT** function on the **IN/OUT** page (section 6.7), and in the Protegus 2 app assign the outputs to the partitions as described in section 5.2.

With a data bus or serial connection, the data connection between the control panel and the communicator remains (the communicator reads the events from the bus), and arming and disarming are done through the keyswitch zone:

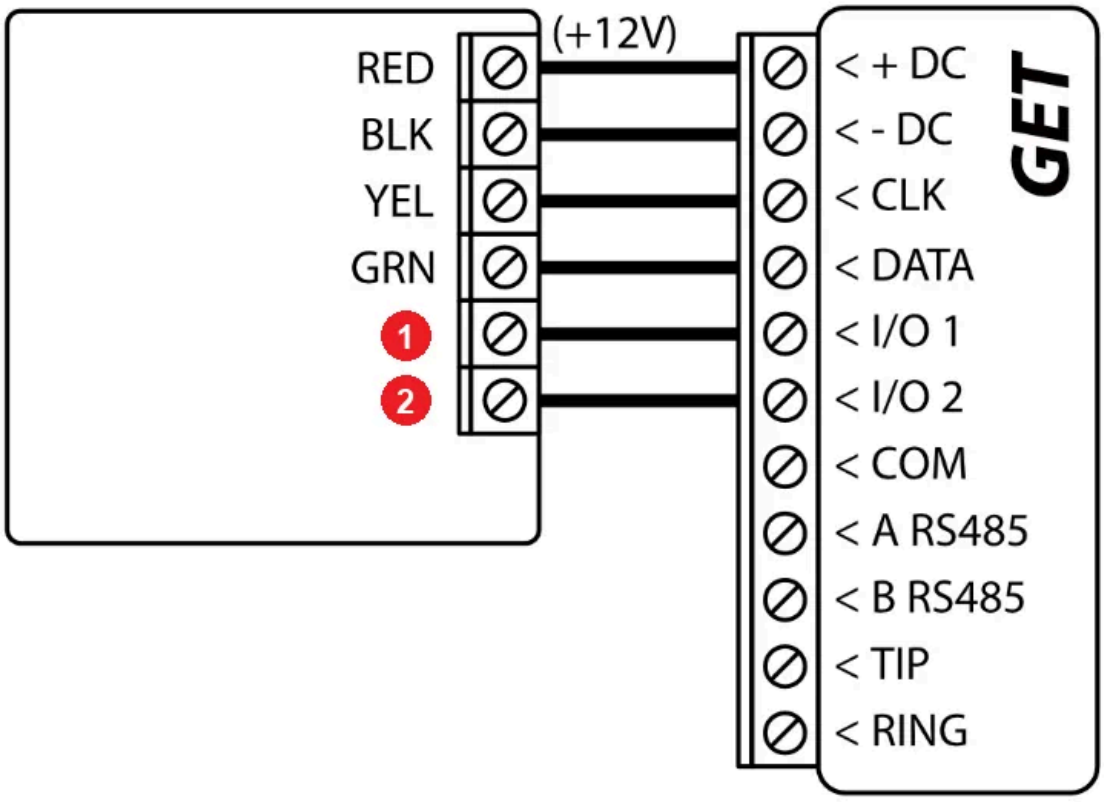


Figure 26. Arming and disarming with a keyswitch zone ("Zone (keyswitch)"), with a data bus or serial connection ("Keypad bus or Serial port"): the alarm control panel's ("Control panel") RED terminal → +DC, BLK → −DC, YEL → CLK, GRN → DATA; the zone of partition 1 → 1 I/O, that of partition 2 → 2 I/O.

- 1 keyswitch zone of partition 1 ("1-st Area")
- 2 keyswitch zone of partition 2 ("2-nd Area")

With a telephone line (TIP/RING) connection, the control panel sends the events with its dialer, and arming and disarming are done through the keyswitch zone in the same way:

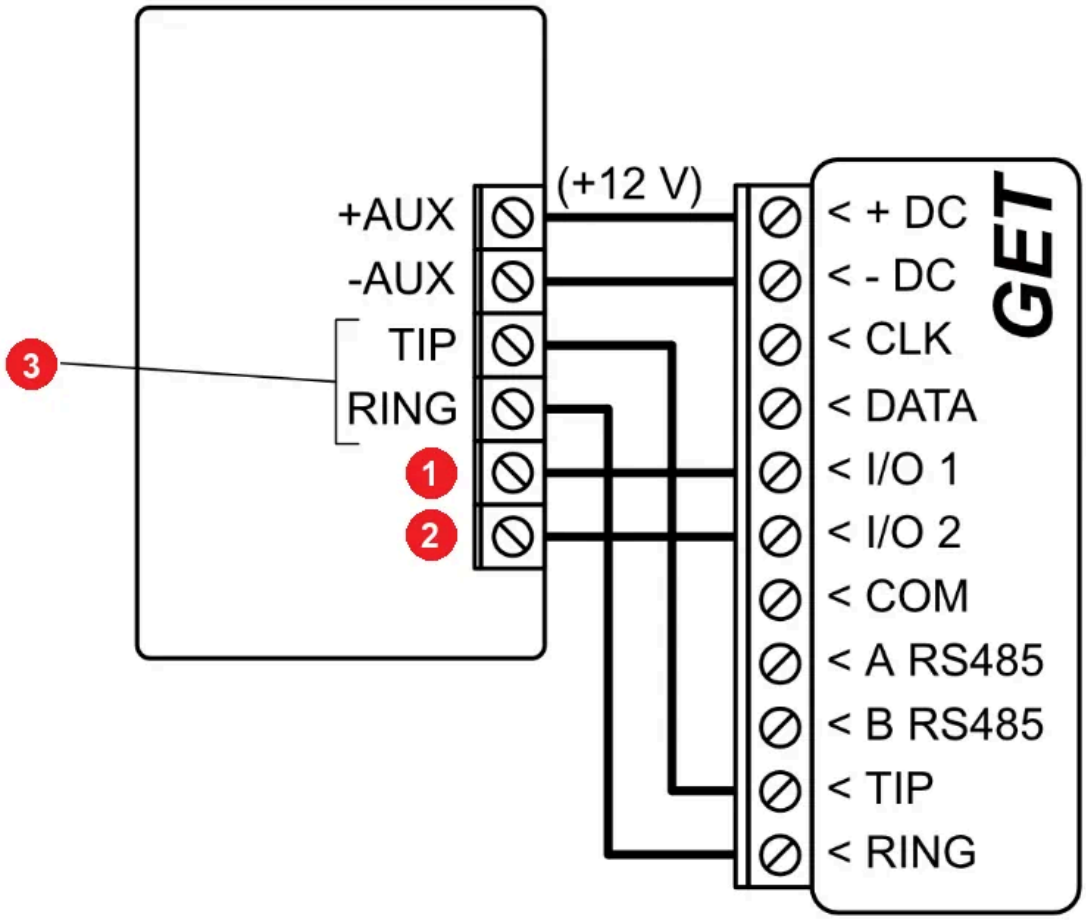


Figure 27. Arming and disarming with a keyswitch zone ("Zone (keyswitch)"), with a telephone line connection: the alarm control panel's ("Control panel") +AUX terminal → +DC, −AUX → −DC, TIP → TIP, RING → RING; the zone of partition 1 → 1 I/O, that of partition 2 → 2 I/O.

- 1 keyswitch zone of partition 1 ("1-st Area")
- 2 keyswitch zone of partition 2 ("2-nd Area")
- 3 terminals of the control panel's telephone line communicator ("Telephone line communicator terminals")

The keyswitch zone can be pulsed or two-state (latched) – the same mode must be set in the Protegus 2 app (section 5.2). The details and pitfalls of keyswitch arming are covered in a separate article: Remote arming with a keyswitch from the Protegus 2 app.

3.5 Wiring inputs

The communicator's two dual-function I/O terminals can also be used as inputs (IN) for additional detectors (e.g. tamper switch, panic button), independently of the alarm control panel. An NO, NC, NO/EOL, NC/EOL, NO/DEOL or NC/DEOL circuit can be connected to the input. On the GET the terminals are outputs by default: set the terminal you use to the **IN** function on the TrikdisConfig **IN/OUT** page, and enter the type of the connected circuit in the **Type** field; in the Protegus 2 app the same is on the **Advanced settings → IN/OUT** page, in the **Type** field of terminal 1 or 2 (section 6.7). The input must be connected between the selected I/O and the **COM** terminal, according to the selected type.

The inputs accept the following circuit types: **NC**, **NO**, **NC/EOL**, **NO/EOL**, **NC/DEOL**, **NO/DEOL**. The end-of-line resistor is **2.2 kΩ**. With a single end-of-line resistor (EOL), both a short circuit and an open circuit count as an alarm; with double end-of-line resistors (DEOL), the two resistors allow the alarm and the tamper (short or

open circuit) to be recognised separately. The factory setting is NO (normally open); you set the input type on the **IN/OUT** page of TrikdisConfig, according to the wiring.

Type	Normal state	Alarm	Tamper
NC	closed	open	–
NO	open	closed	–
NC/EOL	2.2 kΩ	open or short circuit	–
NO/EOL	2.2 kΩ	short or open circuit	–
NC/DEOL	2.2 kΩ	3.3–5.5 kΩ (2 × 2.2 kΩ)	open or short circuit
NO/DEOL	3.3–5.5 kΩ (2 × 2.2 kΩ)	2.2 kΩ	open or short circuit

When the input is triggered, the communicator sends its own event to the monitoring station and to Protegus 2; you can set the event's Contact ID code, partition and zone number on the **IN/OUT** page.

Wiring the input circuits between the COM and INx points: NO, NC, NC/EOL, NO/EOL, and with tamper detection NO/DEOL and NC/DEOL, with 2.2 kΩ end-of-line resistors; the individual states (short circuit, open circuit, 2.2 kΩ, 3.3–5.5 kΩ) are explained in the table of section 3.5.

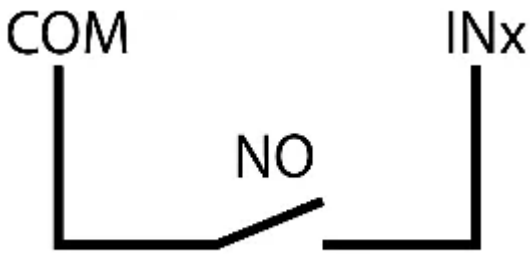


Figure 28. NO – normally open circuit: closed – alarm, open – normal state.

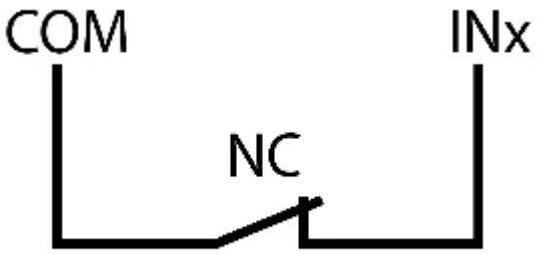


Figure 29. NC – normally closed circuit: open – alarm, closed – normal state.

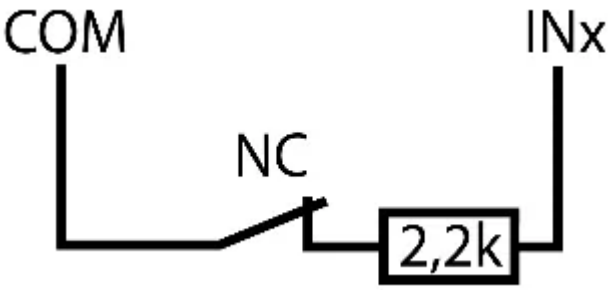


Figure 30. NC/EOL – normally closed circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

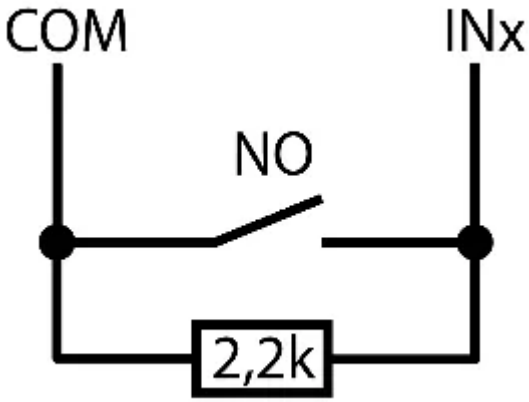


Figure 31. NO/EOL – normally open circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

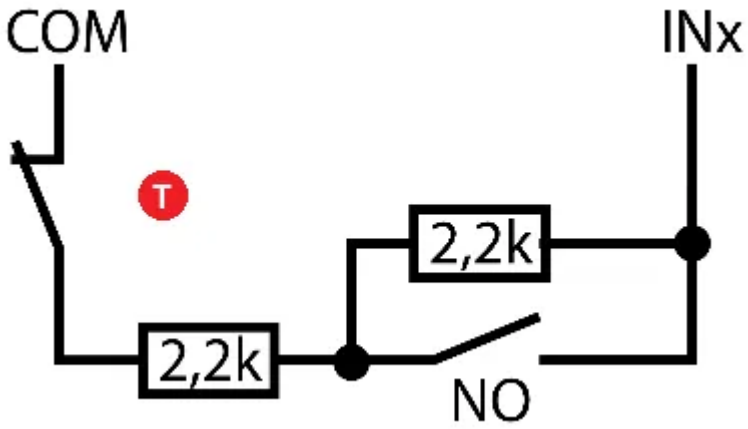


Figure 32. NO/DEOL – normally open circuit with 2.2 kΩ end-of-line resistors and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – alarm, 3.3–5.5 kΩ – normal state.

- T tamper contact ("Tamper"), it signals opening of the detector's cover

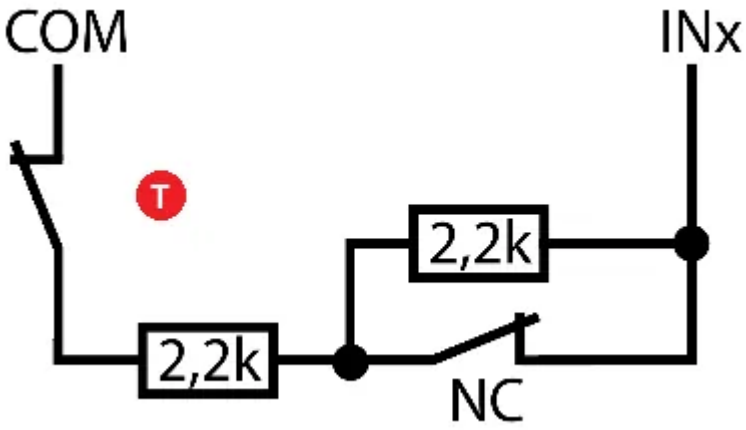


Figure 33. NC/DEOL – normally closed circuit with 2.2 kΩ end-of-line resistors and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – normal state, 3.3–5.5 kΩ – alarm.

- T tamper contact ("Tamper"), it signals opening of the detector's cover

3.6 Wiring an output with a relay

As outputs, the I/O terminals are open collector (OC) outputs: in the active state they pull the connected load to negative, with at most 0.15 A, up to 30 V DC. With the contacts of a relay you can switch various electrical devices on and off: one end of the relay coil goes to **+DC**, the other to the **x I/O** terminal, and the load is switched by the relay contacts (NC, C, NO). The I/O terminal you use must be an output (**OUT**) on the TrikdisConfig **IN/OUT** page (or on the app's IN/OUT page) – on the GET this is the default setting.

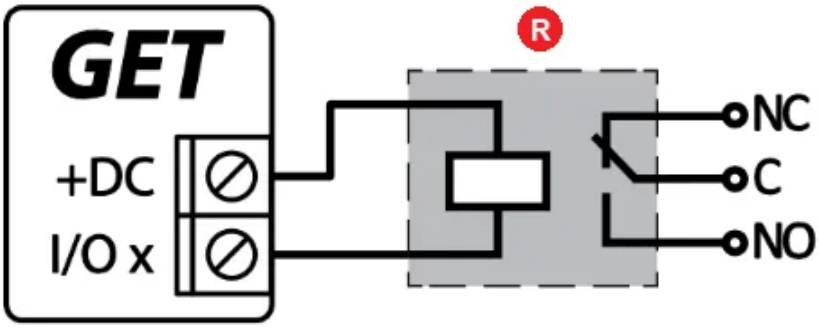


Figure 34. Connecting a relay to the communicator's output: the coil goes between +DC and the x I/O terminal, the contacts (NC, C, NO) switch the load.

- R relay ("Relay")

You can switch the outputs from the Protegus 2 app (chapter 5).

3.7 Power-up and first check

A TRIKDIS átjelző elindítása

1. SIM kártyás átjelző esetén a SIM kártyát az elindítás előtt helyezd be a készülékbe.
2. Ethernetes eszköz esetén az Ethernet kábelt elindítás előtt vagy utána is csatlakoztathatod
3. Az indításhoz húzd ki az USB kábelt és csatlakoztasd a lehúzott sorkapcsot

Akkor léphetsz tovább a következő fejezetre, ha az eszköz megfelelően elindul és nem jelez hibát.

- A Power LED zölden világít
- A Trouble LED nem villog pirosan
- A Network LED zölden világít (ha közben sárgán villog az rendben van)
- Ha Data LED nem alszik ki, az azt jelenti, hogy az eszköz nem tud elküldeni valamilyen eseményt. Ez internet / adat kapcsolat hibára utal.

After wiring, the communicator also starts when the alarm control panel's power is switched on. On the front cover you should see:

- **POWER** steady green – the power supply is adequate;
- **NETWORK LTE** steady green and flashing yellow – connected to the mobile network; the number of yellow flashes is the signal level: on 4G, 3 flashes are adequate; if you count fewer, the signal is weak: find another place for the communicator or the antenna, or use a more sensitive antenna (section 3.2);
- **NETWORK LAN** steady green if you have also plugged in a network cable – connected to the wired network;
- **TROUBLE** off.

If TROUBLE flashes, the number of flashes tells you the cause (section 1.6); any other LED indication also signals some fault, look up its cause in the tables of section 1.6. If none of the LEDs light up, check the power supply and the wiring.

4. Programming the alarm control panel

How the control panel is set up depends on how you connected it: over the data bus or serial port (section 4.1), or through its telephone line communicator, on the TIP/RING terminals (section 4.2). For the Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING connection, the settings of the control panel's sections are given in the table of section 3.3.3.

4.1 Data bus or serial connection

This section describes how to set up the control panel so that the communicator reads its events and can control it remotely. For remote control, the **Remote Arm/Disarm** option must be ticked on the TrikdisConfig **Panel settings** page (in the app: **Panel settings** → **Serial Bus**) (sections 2.2 and 6.3).

4.1.1 DSC

DSC PowerSeries panels (the list of supported models is in section 1.2) do not require any special settings: the communicator connected to the Keybus reads the events immediately, and once **Remote Arm/Disarm** is ticked, the user arms and disarms from the app with their own keypad code. The details of direct control – zone states, zone bypassing, automatic detection of partitions – are covered in a separate article: Direct control for DSC PowerSeries alarm panels.

The communicator does not work with **DSC PowerSeries NEO** panels: the manufacturer does not allow external devices on the NEO bus. For NEO, use a telephone-line (TIP/RING) communicator – see DSC Power Series NEO and Trikdis communicators: compatibility and solutions.

4.1.2 Paradox

Paradox panels only need to be programmed for direct control; nothing needs to be set for reading the events. The panel's firmware must be at least **V.4**.

On newer Paradox panels (for example the SP+, MG+ and EVOHD+ series), the serial port may be **locked from the factory**: the communicator receives no data until the port is unlocked. How to unlock it: Unlocking the locked serial port on Paradox alarm panels.

For control, the panel's **PC password** must be set, and the same must be entered in the **System settings → Security panel PC download password** field of TrikdisConfig – the two must match.

1. Enter the panel's installer programming on the keypad.
2. Open the PC password section: section **911** for the **MAGELLAN and SPECTRA** series, section **3012** for the **DIGIPLEX EVO** series.
3. Enter a **4-character** password. The password cannot be 0000 and **must not start with zero**.
4. Exit programming and **restart the panel** – a change of the PC password takes effect after a restart. Then enter the same password in TrikdisConfig.

Typical problems and their solutions

- The **keypad code assigned to the partition cannot be the master code**: give the user another code, and with that, arming / disarming from Protegus 2 will work.
- **Restart the communicator after any keypad code change** (power cycle or `RESET` SMS command): it reads the codes at start-up and does not see later changes.

On the GET communicator, the **Security panel PC download password** field is on the TrikdisConfig **Panel settings** page, in the **Serial bus** group; in the Protegus 2 app it is **Panel settings → Serial Bus → PC download password** (sections 2.2 and 6.3).

Keybus and TIP/RING connection (SP / SP+ / MG / MG+, section 3.3.3): in addition, the control panel must be programmed to send the events to the monitoring station and to be controllable from Protegus 2 – the values of the sections (801, 811, 812, 815, 911) are given in the table of section 3.3.3.

4.1.3 Texecom

Texecom Premier / Premier Elite panels must be programmed both for reading events and for control: you need to set the panel's 4-character password called **UDL passcode**, and enter the same in the **System settings → Security panel PC download password** field of TrikdisConfig – the two must match.

With Texecom's Wintex software: the UDL passcode is on the **Options** tab of the **Communication Options** window.

From the keypad:

1. Enter the 4-digit installer code and press **[Menu]** to enter the programming menu.
2. Immediately afterwards, press **[9]**.
3. Press **[7][6]**, then **[2]**, and enter the 4-digit UDL passcode.
4. Press **[Yes]**, then exit programming with the **[Menu]** button.

On the GET communicator, the **Security panel PC download password** field is on the TrikdisConfig **Panel settings** page, in the **Serial bus** group (in the app **Panel settings → Serial Bus → PC download password**); the UDL passcode must match it.

4.1.4 UTC Interlogix (Caddx)

The firmware of the **UTC Interlogix (Caddx) NetworX** panel must be at least **V2**. The following must be set on the panel's keypad:

1. Press **[*][8]** and enter the installer code (default **9713**).
2. Enter the **device number** (device address) assigned to the communicator (default **0**).
3. Program the rows of the table below one after the other: enter the location, the segment number and then the setting. You can go back to the previous field with the **[*]** button. `12345678` means that all eight switches of the segment are on (all digits are visible on the display).

Location	Segment	Setting
23	3	12345678
37 (not strictly necessary)	3	12345678
37 (not strictly necessary)	4	1234567*
90	3	12345678
93	3	12345678
96	3	12345678
99	3	12345678
102	3	12345678
105	3	12345678
108	3	12345678

4. When you have programmed all rows, press **[Exit]** twice to leave programming.

4.1.5 InnerRange

The firmware of the **InnerRange Inception** panel must be at least **2.3.0.3507-r0**, and the panel needs an internet connection. The settings are made in the panel's web interface:

1. Open `https://skytunnel.com.au/inception/SERIALNUMBER` in a browser, where SERIALNUMBER is the serial number on the panel's box. Log in with the installer account.
2. Open the **Configuration** → **General** → **Alarm Reporting** page.
3. In the **3rd Party Device Configuration** group: - tick **Enable 3rd Party Device Reporting**; - in the **3rd Party Device Type** field, select **Trikdis**; - in the **Serial Port** field, select **Serial Port 1 (Plugged In, In Use By 3rd Party Device)**.
4. Save the settings and log out of the interface.

The firmware of the **InnerRange Integriti** panel must be at least **19.1.0.36608**, and its programming software (Integriti Professional) at least **19.1.0.15396**. The settings are made in the panel's programming software:

1. For the serial port (**TTL Port-0**) to which the communicator is connected, select the **Trikdis** communication protocol.
2. The data format must be **Contact ID**.
3. Port settings: **19200, 8, N, 1**.
4. Save the settings and exit the program.

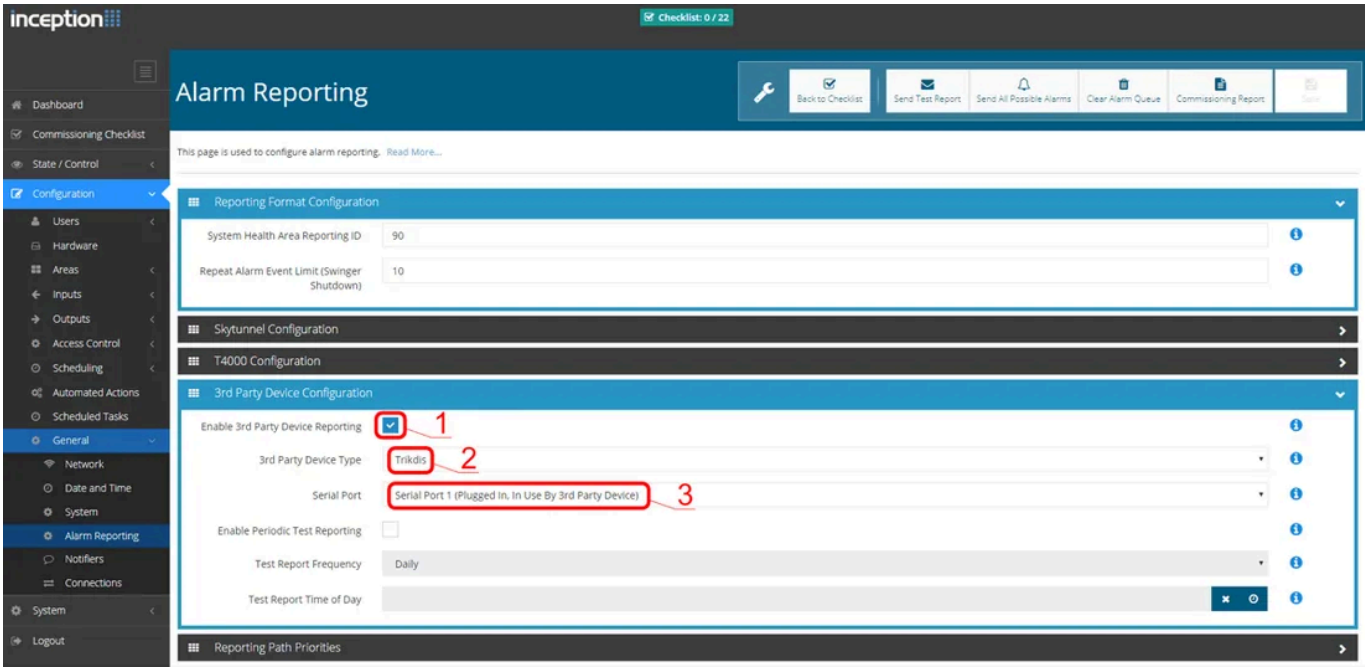


Figure 35. InnerRange Inception – Configuration → General → Alarm Reporting, 3rd Party Device Configuration group: Enable 3rd Party Device Reporting ticked, 3rd Party Device Type: Trikdis, Serial Port: Serial Port 1.

4.1.6 Honeywell Ademco Vista

The firmware of the **Honeywell Ademco Vista-20** and **Vista-48** panels must be at least **V5.3**. The settings are made on the panel's keypad.

Entering programming – in two ways:

- enter the installer code (default **4112**), then press **[8][0][0]**; or
- power up the panel and **within 50 seconds** press the **[*]** and **[#]** buttons at the same time (this only works if programming was previously exited with [*][9][8]).

Settings:

1. Enable sending Contact ID events on the long range radio (LRR) output: press **[*][2][9][1][#]**.
2. For remote control, enable the use of the **2nd AUI address**: press **[*][1][8][9][1][1][#]**.

Exiting programming: press **[*][9][9]**.

4.2 Telephone line (TIP/RING) connection

For the alarm panel to send events on its telephone-line output, the panel's dialler must be enabled and configured. You will find the exact program addresses in the panel's installation manual; the essence of the setting is the same for every manufacturer:

1. **Enable the telephone-line (PSTN) communicator** in the panel.
2. **Enter `1234` as the telephone number** of the monitoring receiver – whether the communicator is connected to the panel's RING/TIP terminals or to the telephone line. With another number it can happen that the panel dials but the communicator still does not receive the events: with a DSC PowerSeries NEO panel, too, reporting only started after the number was changed to `1234`.
3. **Dialling mode:** DTMF (tone), not pulse.
4. **Protocol:** Contact ID.

If you want to arm and disarm the panel remotely with the communicator's output, the zone wired to the output must be set as a **keyswitch zone** in the panel.

The keyswitch zone can be pulsed or latched (two-state). By default, the communicator's output gives a 3-second pulse; you can change the pulse length or switch to latched mode in the settings of the Protegus 2 app.

The DSC, Paradox, Caddx, Texecom, InnerRange and Honeywell control panels can also be connected to the communicator through their telephone line output (section 3.3.9) – in that case the dialer must be set up for these as well, and direct control is not available.

4.2.1 Programming the Honeywell Vista dialer

Enter programming mode on the keypad and set the following program addresses:

Program address	Setting
`*41`	the telephone number of the monitoring receiver: `1234`
`*43`	the panel's account number
`*47`	Tone dial = `1`, and the number of dialling attempts
`*48`	`7` (default)
`*49`	`5` (Split/Dual message)
`*50`	delay before sending a burglary alarm – default `2,0` (30 s); for immediate sending `0,0`

For a **Honeywell Vista 48** panel, also set the following program addresses:

Program address	Value	Program address	Value	Program address	Value
`*41`	1234 (receiver telephone number)	`*60`	1	`*69`	1
`*42`	1234	`*61`	1	`*70`	1
`*43`	1234 (account number)	`*62`	1	`*71`	1
`*44`	1234	`*63`	1	`*72`	1
`*45`	1111	`*64`	1	`*73`	1
`*47`	1	`*65`	1	`*74`	1
`*48`	7	`*66`	1	`*75`	1
`*50`	1	`*67`	1	`*76`	1
`*59`	0	`*68`	1		

At the end of programming, exit programming mode with the `*99` command.

4.2.2 The dialer of the UTC Interlogix (Caddx) NX

Programming the Interlogix NX-4V2 (NX-6V2, NX-8V2) control panel when the communicator is connected to the control panel's TIP/RING terminals. On the keypad, enter the following one after the other:

Location	Keys	Note
	`*89713`	Enter programming (`9713` is the default installer code)

Location	Keys	Note
	`0#`	
Location 0	`0#`	
Location 0	`1 2 3 4 #`	
Location 1	`1#`	
Location 1	`1 2 3 4 #`	
Location 2	`2#`	
Location 2	`1*#`	
Location 4	`4#`	All zone LEDs lit (segment 1)
Location 4	`12345678*`	All zone LEDs lit (segment 2)
Location 4	`12345678*#`	
Location 23	`23#`	All zone LEDs lit (segment 3)
Location 23	`**`	All zone LEDs lit (segment 3)
Location 23	`12345678*#`	All zone LEDs lit (segment 3)
Location 37	`37#`	All zone LEDs lit (segment 3)
Location 37	`**`	All zone LEDs lit (segment 4)
Location 37	`12345678*`	
Location 37	`12345678*#`	
	`EXIT` `EXIT`	Exit programming

5. Remote control with the Protegus 2 app

With the Protegus 2 mobile and web app the user sees the state of the system remotely, receives notifications about the events, can arm and disarm, and can switch the communicator's outputs. The app can be downloaded for Android and iOS (Google Play, App Store), or used in a browser: web.protegus.app. Log in with your user name and password, or register a new account. The GET does not notify by SMS or phone call, and does not accept SMS commands either: remote control and notification are done through the app; the communicator's settings are also available from the app (**Settings** → **Advanced settings**, chapter 6).

5.1 Adding the device

Before adding the device, check:

1. The SIM card is active, and its PIN code is entered in the device, or the PIN request is switched off – **or** the communicator is connected to the local network with a network (LAN) cable.
2. On the TrikdisConfig **User reporting** → **PROTEGUS Cloud** page, **Enable connection** is ticked (section 6.5).
3. The **POWER** LED is steady green.
4. The **NETWORK LTE** LED is steady green and flashing yellow (the device is on the mobile network); with a wired connection only, the **NETWORK LAN** LED is steady green.

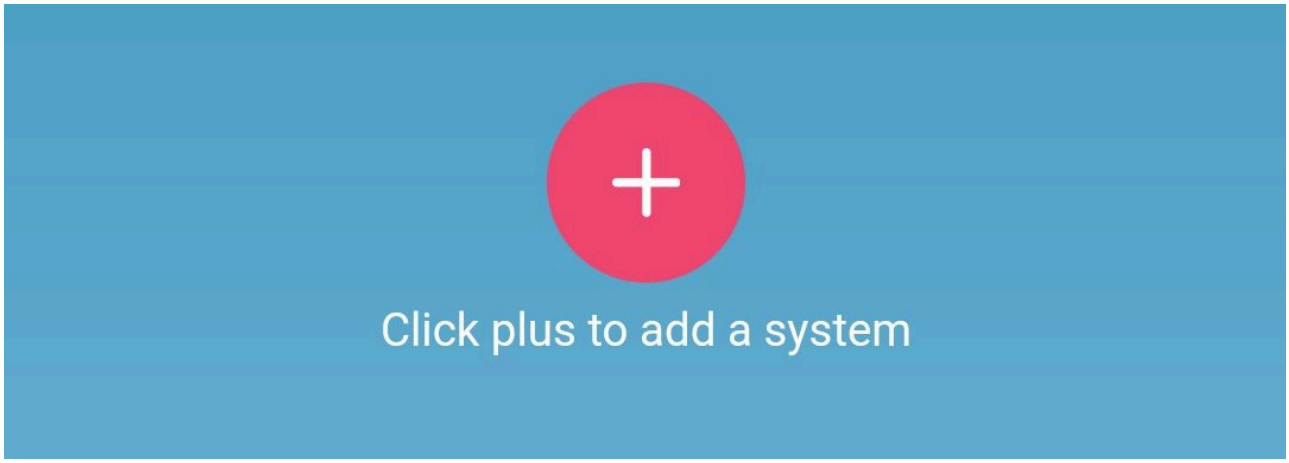
The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for 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



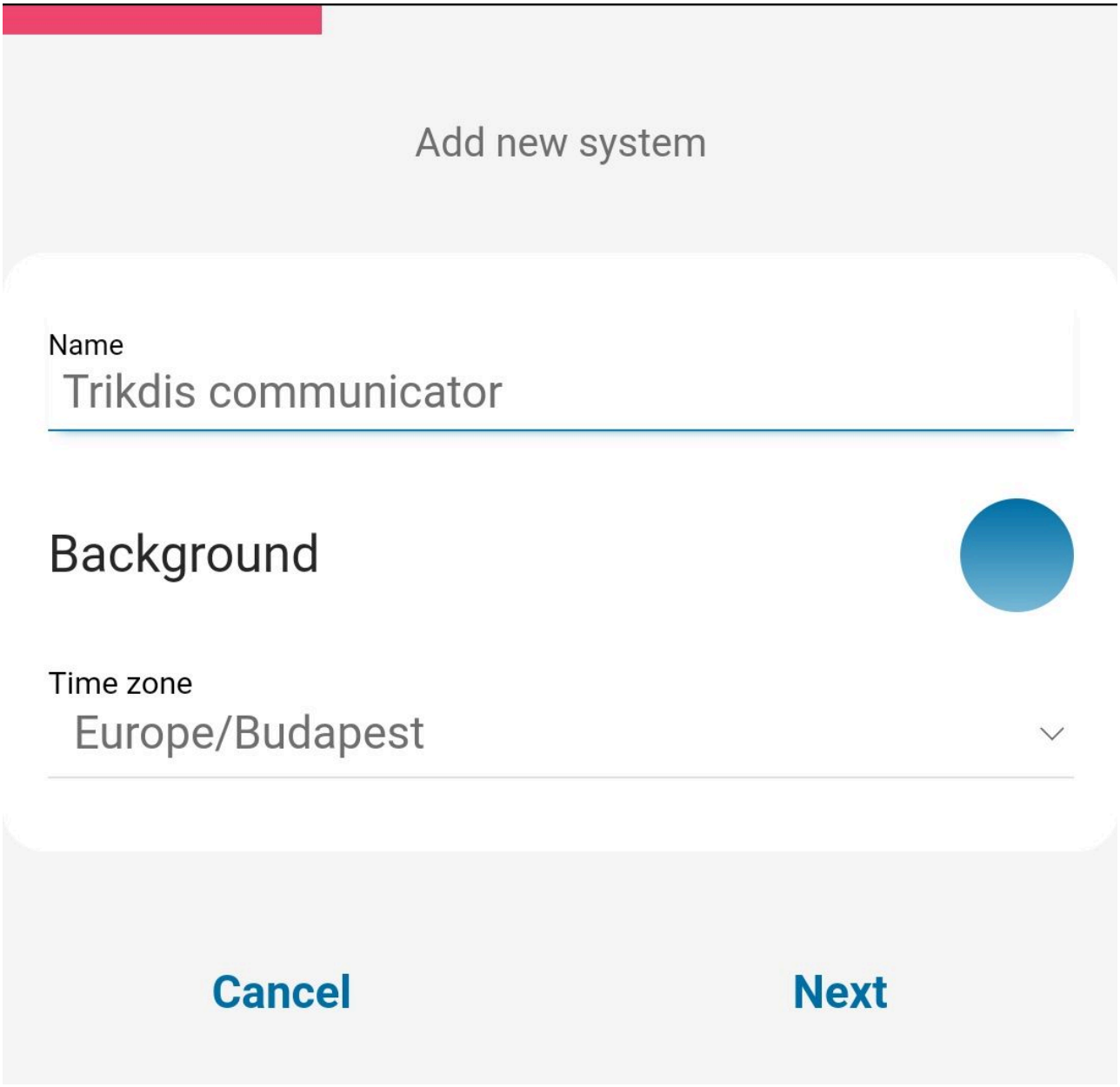
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



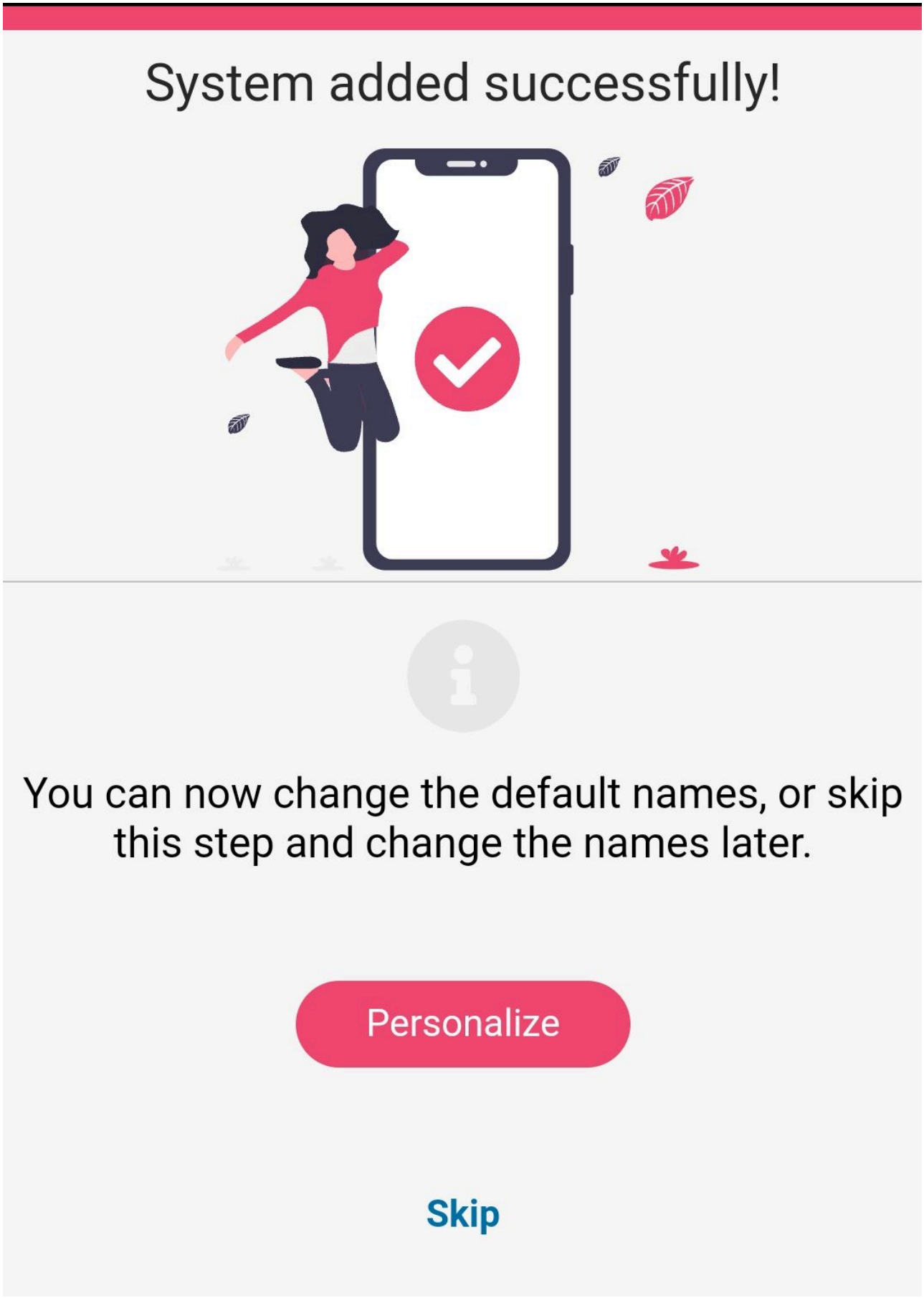
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



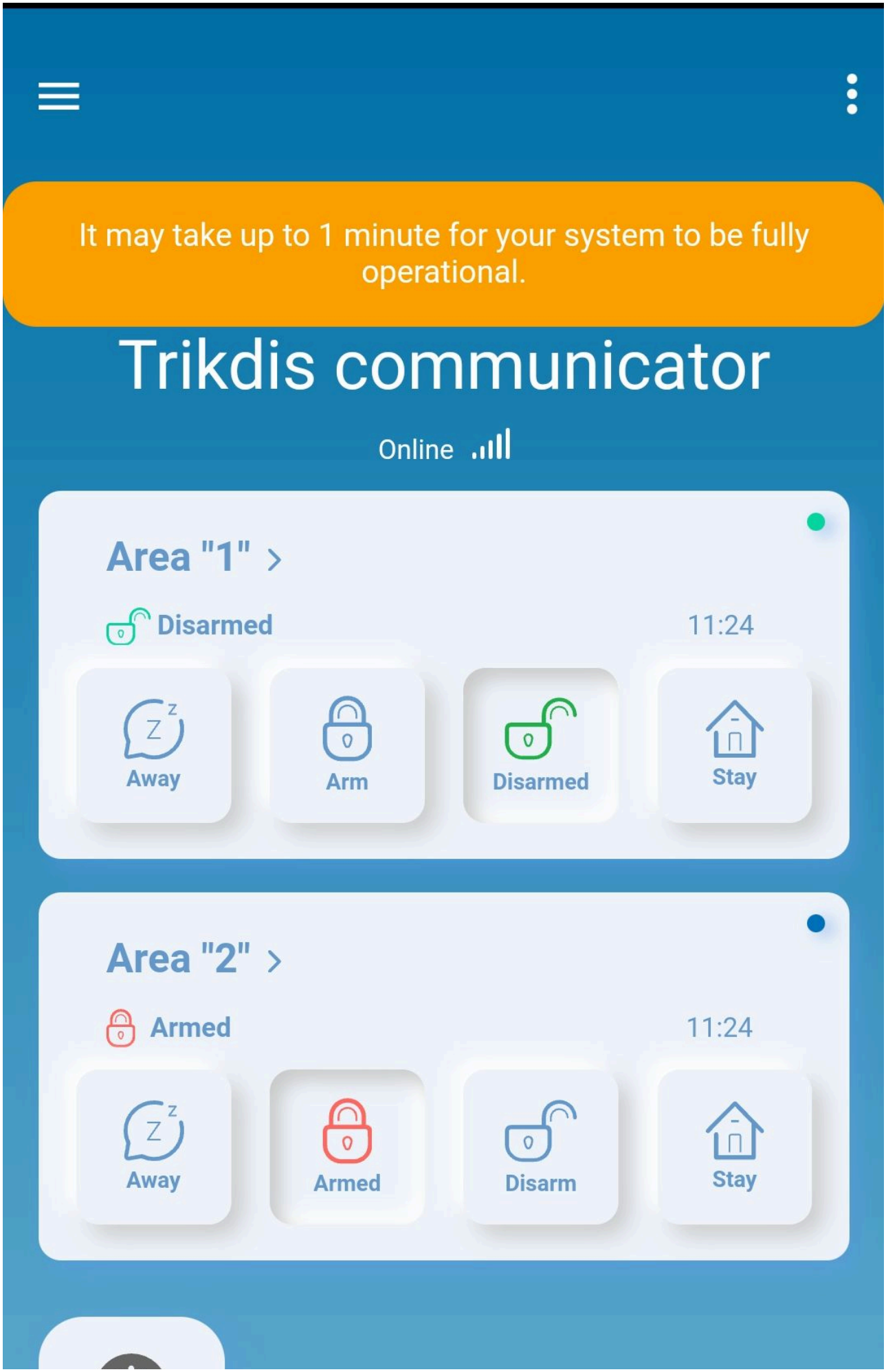
6. Add meg a rendszer nevét és válassz idozónát



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

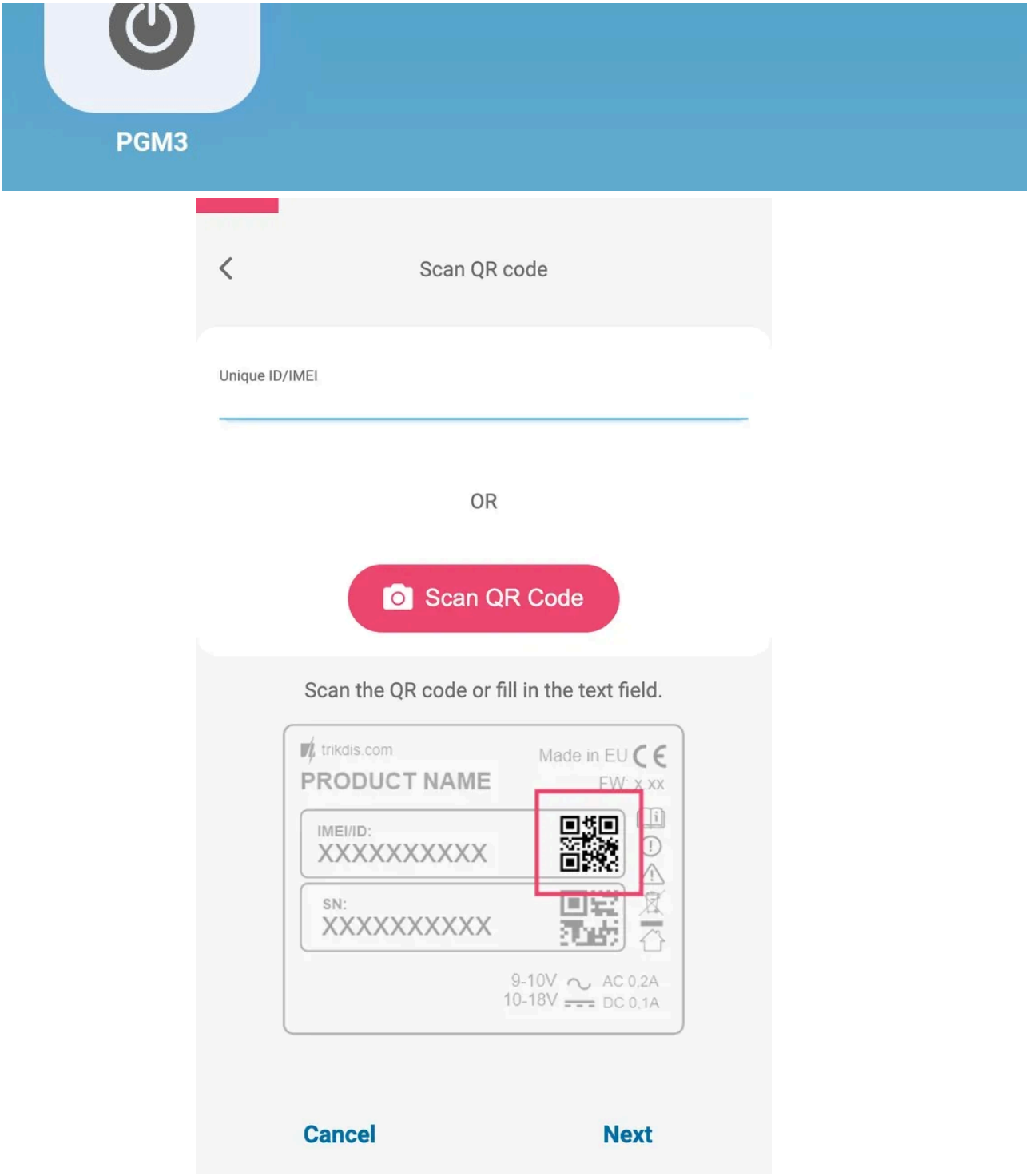


Figure 36. Protegus 2 – adding a new system: enter the IMEI / Unique ID or scan the QR code on the label, then Next.

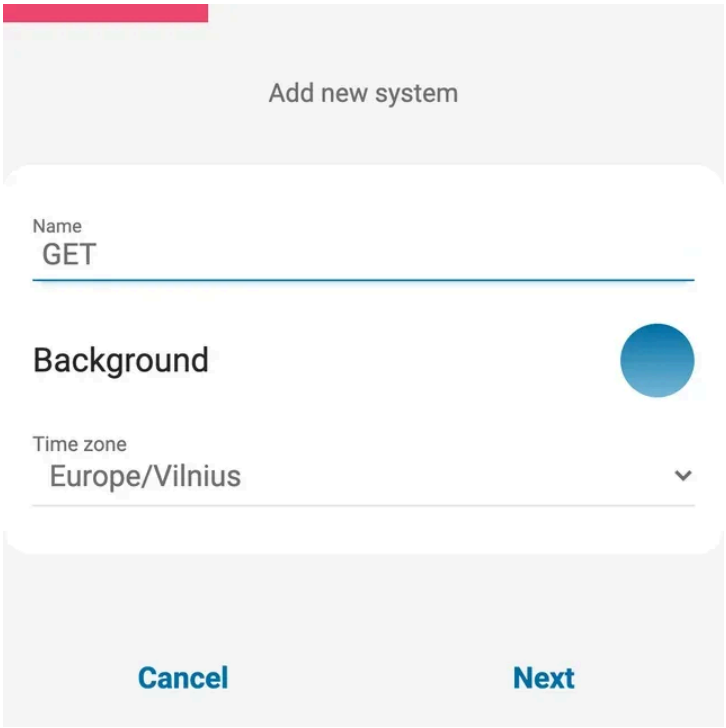


Figure 37. Protegus 2 – enter the system's name (Name), then Next.

The device's unique identifier (**IMEI / Unique ID**) can be read on the device's label and on the sticker on the box, and the TrikdisConfig status bar also shows it. If the **PROTEGUS Cloud access Code** in the device is not the default one, the app asks for it when adding.

5.2 Arming and disarming with an output

If you want to arm and disarm the alarm panel with the communicator's output, through the panel's keyswitch zone, specify in the Protegus 2 app for the partition which output controls it.

The panel zone to which the communicator's output is connected must be programmed as a **keyswitch zone** in the panel, and the panel must report the arming and disarming events – Protegus 2 shows the partition state based on these.

You can make the setting when creating the system, while adding the partitions, or later in the system settings, when editing the partition. When creating the system, the Protegus 2 wizard guides you through: click **Continue**, enter the partition name (**Area name**) and enable control of the PGM output from the Protegus 2 app – this is done with the following steps:

1. Select (or add) the partition you want to control. The partition number must match the one the panel sends in its events (partition 1 as 1, partition 2 as 2).
2. Switch on **Control with Protegus2** (control with PGM), and in the **Assigned Output** field select the communicator output (PGM1, PGM2 …). One output can control only one partition.
3. Select the operating mode: **Pulse** or **Level** (latched) – the same one you set for the keyswitch zone in the panel. Typically we use pulse; the pulse length can also be set (default 3 s).
4. Save the setting (**Save**). With several partitions, repeat this for each one with its own output: in the wizard you add a further partition with the **Click to add an area** button and set its PGM output in the same way. When you have set up all partitions, move on in the wizard with the **Skip** button.

Protegus 2 can only show the state of the partitions correctly if the panel sends the arming and disarming events with the correct partition number. The details and pitfalls of keyswitch arming are covered in a separate article: Remote arming with a keyswitch from the Protegus 2 app.



Figure 38. Protegus 2 – the "The system is not controlled remotely" page when creating the system: with the Continue button you go on to setting up the partition and the PGM output.

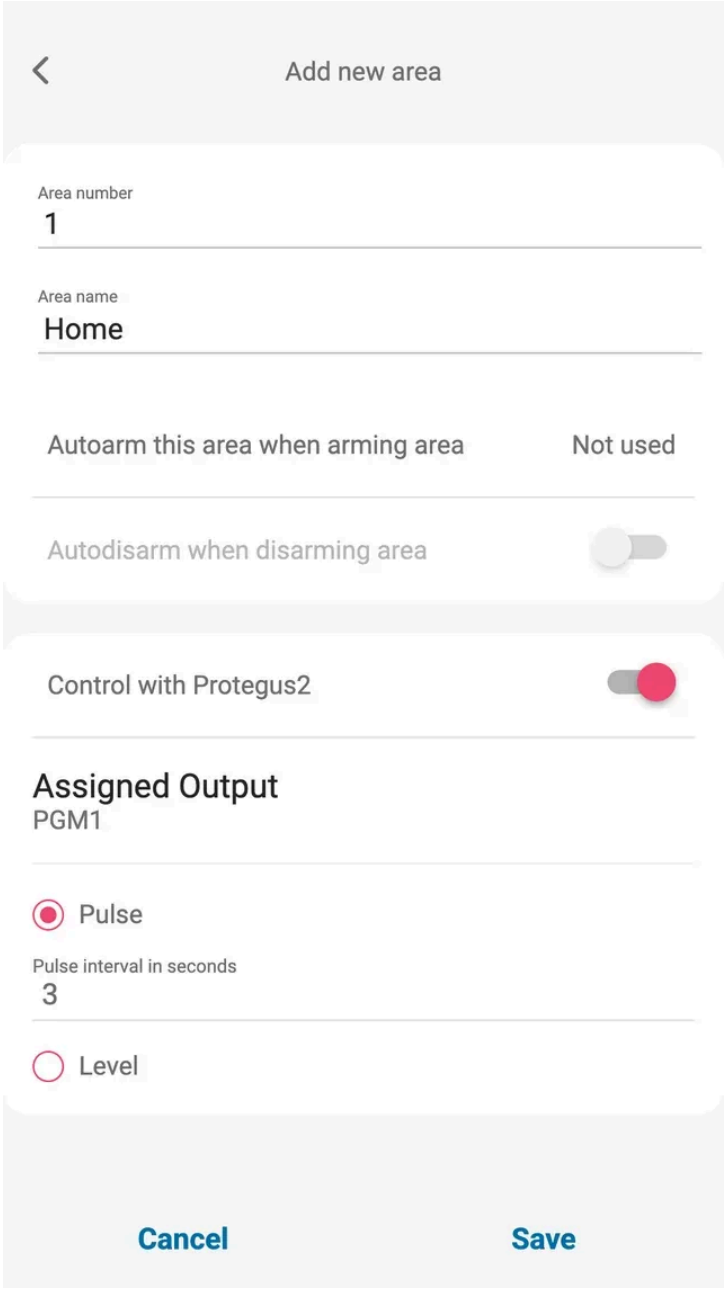


Figure 39. Protegus 2 – adding a partition (Add new area): Area number, Area name, Control with Protegus2 switched on, Assigned Output PGM1, Pulse (3 s) or Level, then Save.

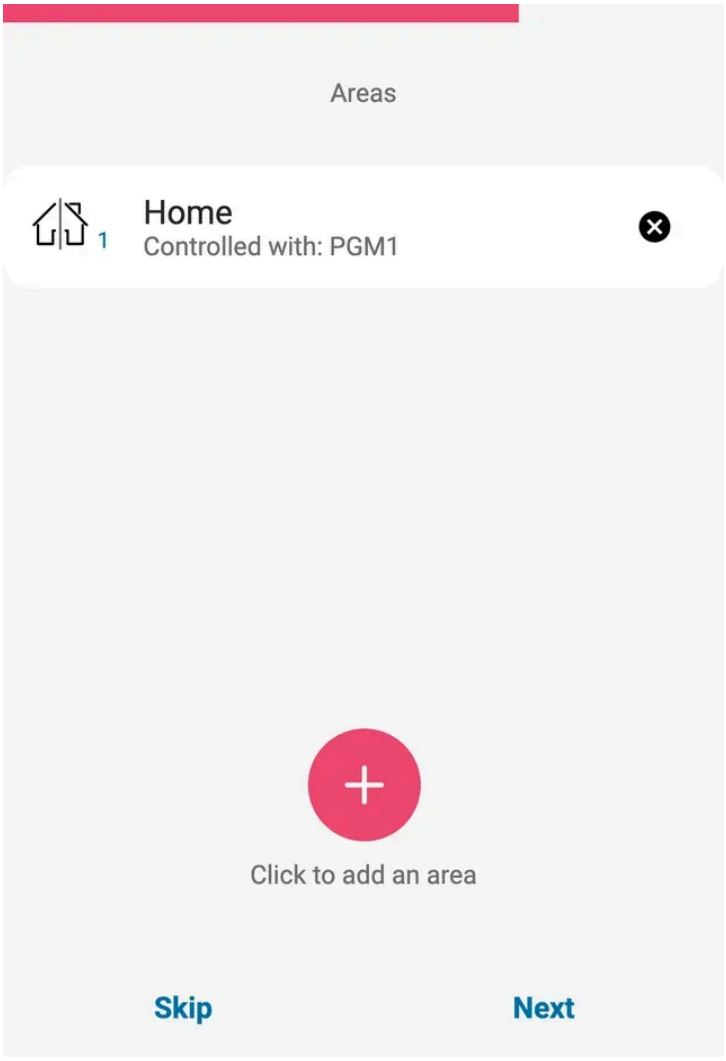


Figure 40. Protegus 2 – the list of partitions (Areas): the Home partition is controlled by PGM1; add further partitions with the Click to add an area button, close the wizard with the Skip button.

5.3 Arming and disarming from the app

1. Open the system in the Protegus 2 app. On the home screen every partition has its own card and padlock: a **closed, red padlock** means an armed partition, an **open, green padlock** a disarmed one.
2. Tap the partition's padlock and select the required action: arm or disarm.
3. If the app asks for it, enter the PIN code.

The padlock takes on the actual state in response to the event received from the alarm panel; the app also confirms in the event list and in a notification whether the panel has carried out the action.

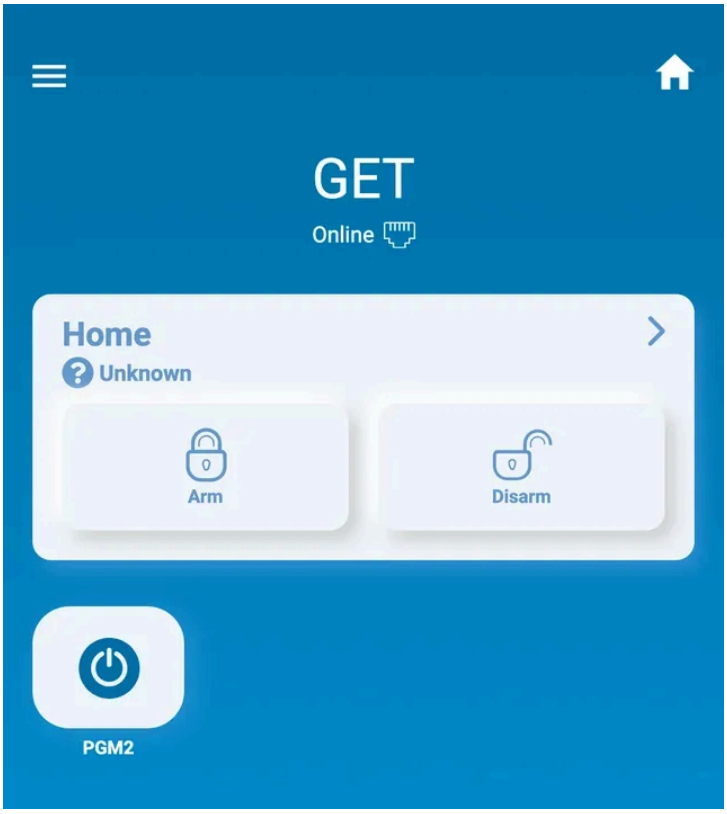


Figure 41. Protegus 2 – the system's home screen: the state of the partition, the Arm and Disarm buttons, below them the switchable PGM output.

6. The settings in detail

Most settings of the GET are available both in the **TrikdisConfig** software running on Windows and in the **Protegus 2** app (**Settings** → **Advanced settings**, section 2.2); where something is only in one of them, we say so. Every setting is described once, and for each section we give where you find it in the two tools; the app's label is in brackets if it differs from TrikdisConfig's. On the left side of the TrikdisConfig window you see the list of pages (System settings, Panel settings, CMS reporting, User reporting, Network settings, IN/OUT, Event summary, Firmware), at the top the button bar (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), and at the bottom the status bar.

6.1 Connecting to the communicator

Protegus 2 app. Open the system and go to the **Settings** → **Advanced settings** menu. At the top of every screen you see the data of the connected device: **Unique ID** (IMEI), **Serial** (serial number), **Firmware** and **Boot** version. The groups of settings in the menu: **System options**, **Panel settings**, **Reporting to CMS**, **User reporting**, **Network settings**, **IN/OUT** and **System events**. After making changes, you write the settings into the device with the **Write** button; **Read** reads the current values from the device again.

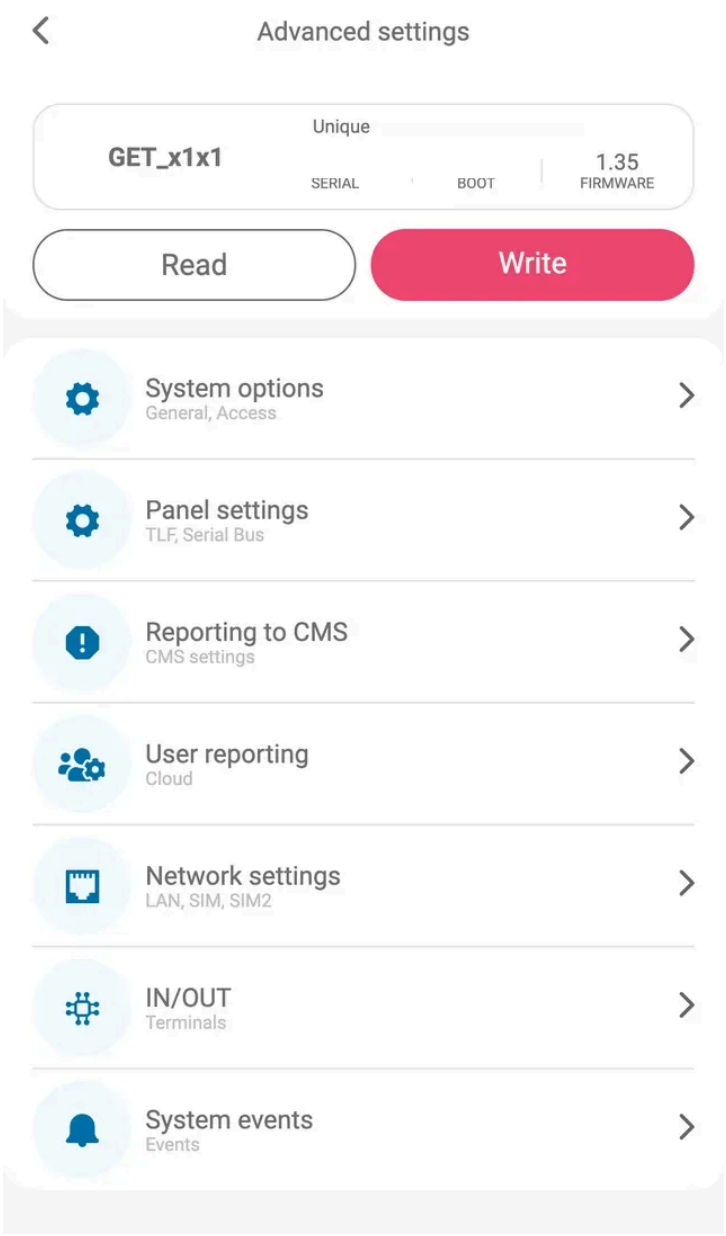


Figure 42. Protegus 2 – Advanced settings menu: at the top the device's data (type, Unique ID, serial number, boot and firmware version), the Read and Write buttons, below them the groups of settings.

TrikdisConfig. After connecting the communicator and pressing **Read [F4]**, the program shows the device's data in 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.

Label	Meaning
Device	The device type (model designation). Check that the type of your own device is shown here.
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 43. The TrikdisConfig status bar with a GET read out: identifier, status, type (Device: GET_S170), serial number, BL (bootloader), FW and HW version, connection mode and access level.

The **Device** field must show a GET type code (in the picture GET_S170; the letter-number suffix indicates the hardware version), **BL** is the bootloader version. After **Read [F4]** the program reads out and shows the values set in the device; make the necessary settings according to the page descriptions below.

6.2 System settings (System options)

In the app: Advanced settings → System options → System general (identifiers, time synchronization) and **System options → Access** (codes and installer rights). Where the **Account No.** and the **Device account No.** are depends on the hardware version and the firmware: on **x1x1** hardware, with firmware **1.31** or newer, you find them on the **Reporting to CMS → CMS settings → Primary channel** page (**Primary Account no.**; on the parallel channel **Parallel Account no.**) and on the **Reporting to CMS → Settings** page (**Device account No.**), and only **Time set** remains on the System general page; otherwise both are on the System general page.

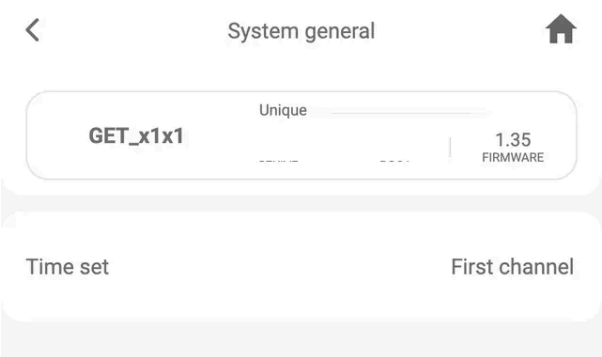


Figure 44. Protegus 2 – System options → System general on x1x1 hardware (firmware 1.35): only Time set is visible, the identifiers are among the CMS settings.

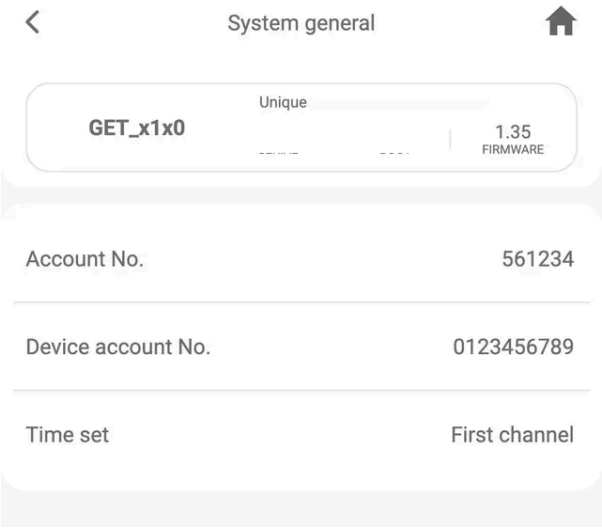


Figure 45. Protegus 2 – System options → System general on x1x0 hardware: Account No., Device account No. and Time set.

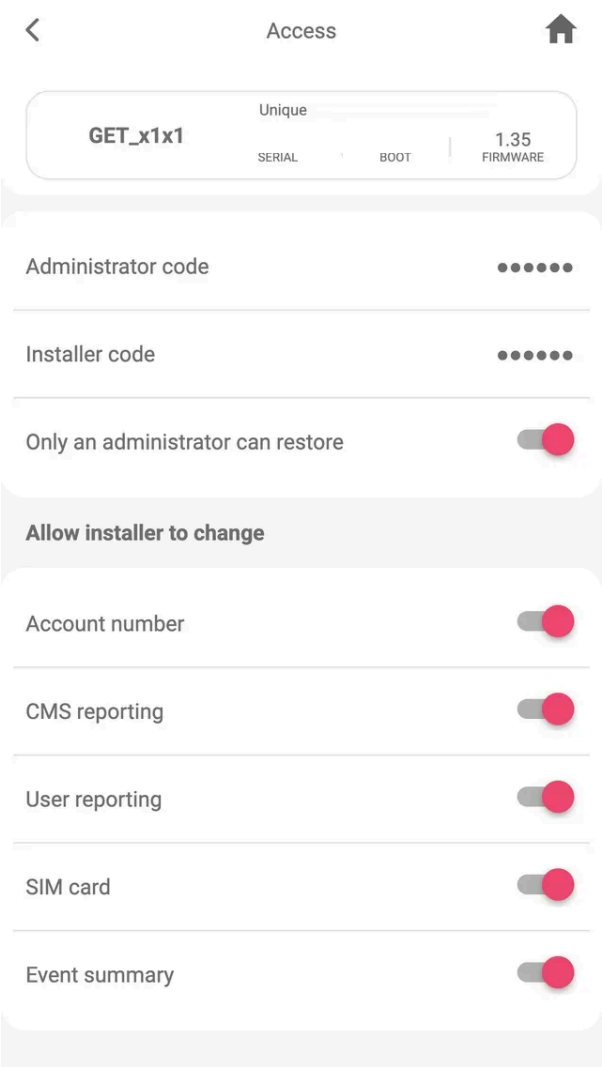


Figure 46. Protegus 2 – System options → Access: Administrator code, Installer code, Only an administrator can restore, and the Allow installer to change list (Account number, CMS reporting, User reporting, SIM card, Event summary).

In TrikdisConfig: the **System settings** page consists of two groups: in the **General** group you set the device's identifiers, in the **Access** group the access levels.

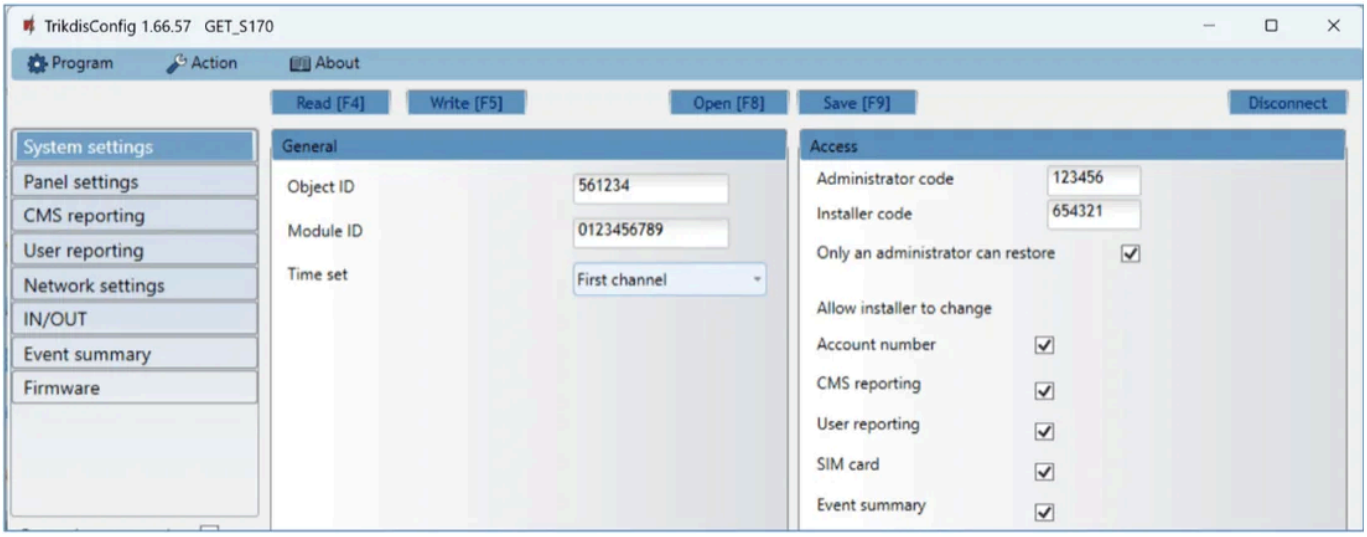


Figure 47. TrikdisConfig – System settings page: General group (Object ID, Module ID, Time set) and Access group (Administrator code, Installer code, Only an administrator can restore, Allow installer to change).

- **Object ID** (Account No.) – the account number received from the monitoring station (6 hexadecimal characters: 0–9, A–F; `FFFE` and `FFFF` cannot be used). Mandatory if the device also reports to a monitoring station.
- **Module ID** (Device account No.) – the module's identification number.
- **Time set** – the server from which the device synchronizes its clock.

In the **Access** group you manage the access levels and passwords.

There are two access levels for the device settings: **administrator** and **installer**.

- **Administrator code** – access to all settings (default password: `123456`; the password is 6 characters: digits or Latin letters).
- **Installer code** – access that can be restricted (default password: `654321`).
- **Only an administrator can restore** – when ticked, only the administrator can start restoring the factory settings.
- **Allow installer to change** – here you can select which groups of settings the installer may change: **Account number**, **CMS reporting**, **User reporting**, **SIM card** (on a mobile network device) or **Ethernet settings** (on an Ethernet device), **Event summary**.

Do not leave the default passwords in the device!

During commissioning, change at least the administrator password and note it down in a safe place. A forgotten password cannot be cleared by restoring the factory settings either, because that also requires a password: only the manufacturer or the distributor can reset it, once the device has been sent to them. The exception is a device with a hardware RESET button: holding the button for 10 seconds restores the factory settings without a password.

Installer login in the app. If you open the communicator with the installer code, Protegus 2 hides the **Administrator code** and **Only an administrator can restore** fields, and shows the settings not allowed by the administrator as read-only. In the app the **SIM card** right also covers the LAN settings; where the identifiers are among the CMS settings (see above), the **CMS reporting** right applies to them.

6.3 Panel settings

On this page you set how the communicator connects to the alarm control panel: the **TLC** group (in the app **TLF**) contains the settings of the telephone line (TIP/RING) connection, the **Serial bus** group (**Serial Bus**) those of the data bus or serial connection. In the app: **Advanced settings → Panel settings → TLF** or **Panel settings → Serial Bus**.

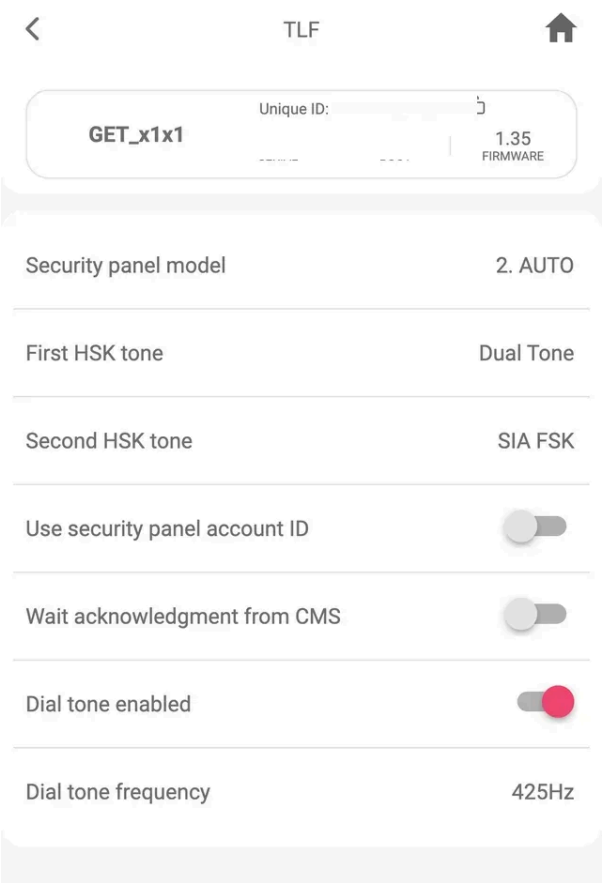


Figure 48. Protegus 2 – Panel settings → TLF: Security panel model 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone enabled, Dial tone frequency 425 Hz.

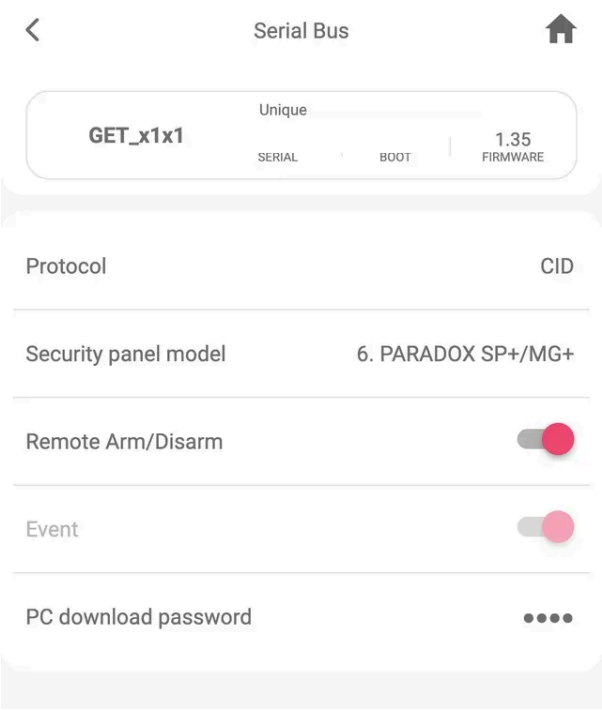


Figure 49. Protegus 2 – Panel settings → Serial Bus: Protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm switched on, Event (read-only), PC download password.

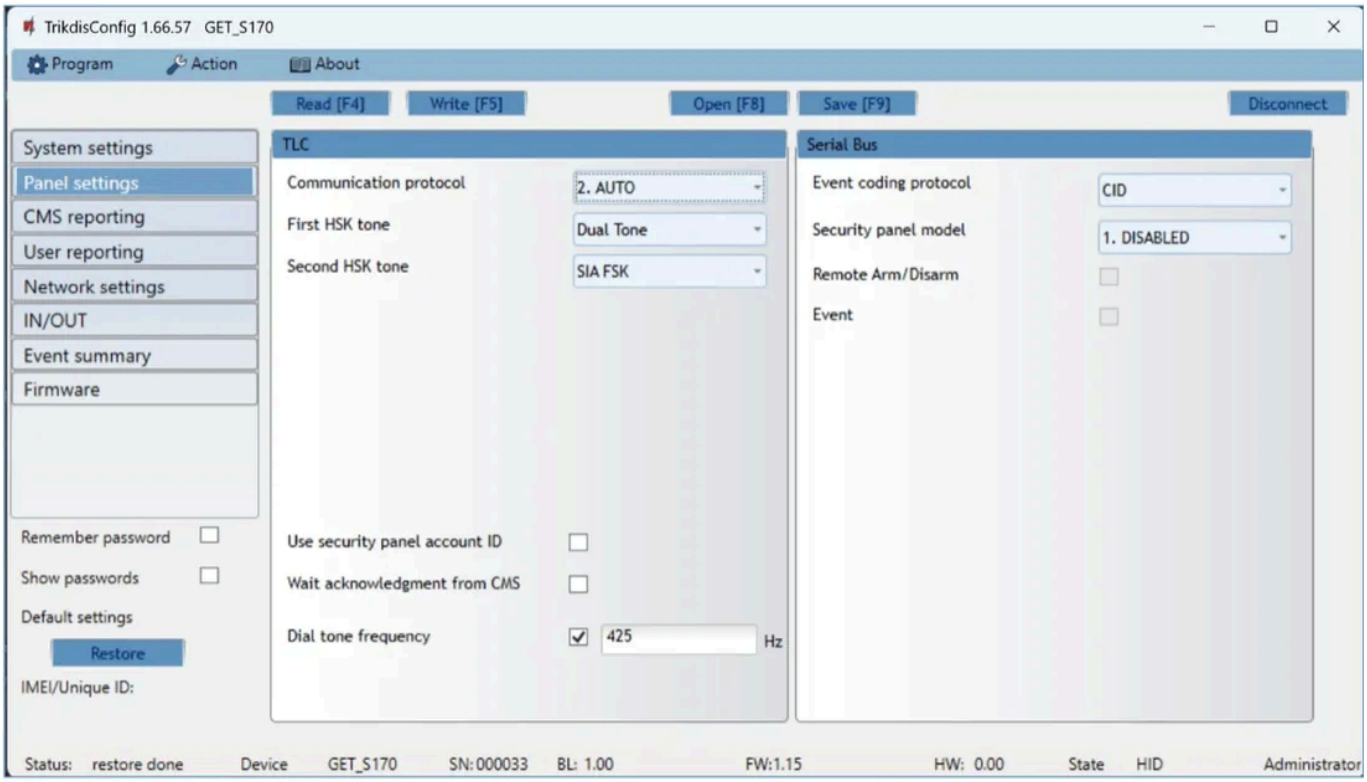


Figure 50. TrikdisConfig – Panel settings with a TIP/RING connection: in the TLC group Communication protocol 2. AUTO, First HSK tone Dual Tone, Second HSK tone SIA FSK, Use security panel account ID, Wait acknowledgment from CMS, Dial tone frequency 425 Hz; the Serial bus group is greyed out in this case.

TLC group – if the communicator is connected to the TIP/RING terminals of the control panel's telephone line communicator:

- **Communication protocol** (Security panel model) – switches the communicator's DTMF telephone line interface on (**2. AUTO**) or disables it (**1. DISABLED**). For a TIP/RING connection, select AUTO.
- **First HSK tone**, **Second HSK tone** – the handshake tone with which the communicator answers the control panel's dialer (in the picture Dual Tone and SIA FSK).
- **Use security panel account ID** – when ticked, the communicator does not send the value of its own **Object ID** field, but the account number set in the control panel and sent by the control panel.
- **Wait acknowledgment from CMS** – when ticked, after sending each event the communicator waits for the IP receiver's acknowledgment that the message has arrived; if the acknowledgment does not come, it does not give the "kiss-off" signal to the control panel, and the control panel's telephone line communicator repeats the message.
- **Dial tone frequency** – the frequency of the dial tone with which the communicator communicates with the control panel's dialer (default 425 Hz, the dial tone used in most European countries). On the app's TLF page there is also the **Dial tone enabled** switch: it switches the dial tone on or off; the frequency can only be changed when the dial tone is switched on.

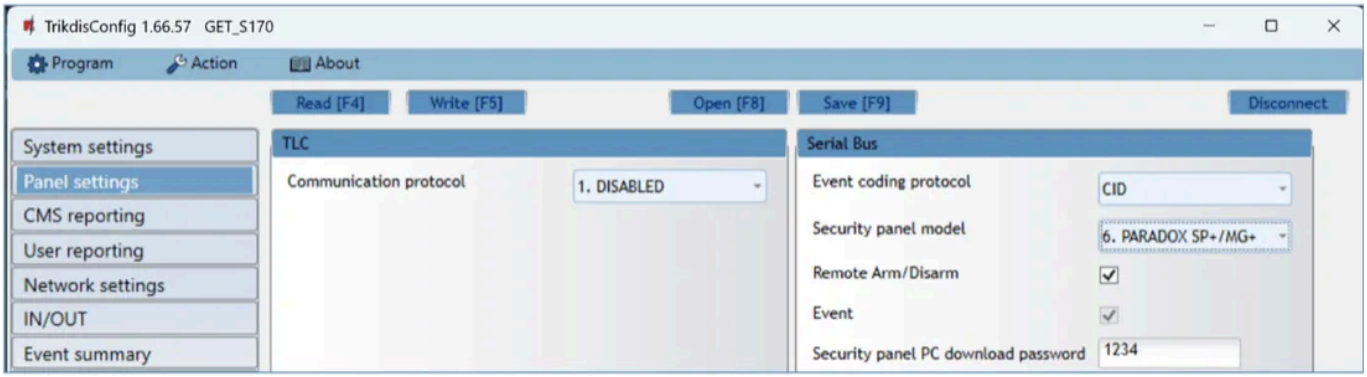


Figure 51. TrikdisConfig – Panel settings with a data bus or serial connection: Communication protocol 1. DISABLED; in the Serial bus group Event coding protocol CID, Security panel model PARADOX SP+/MG+, Remote Arm/Disarm and Event ticked, Security panel PC download password entered.

Serial bus group – if the communicator is connected to the control panel's data bus or serial port:

- **Event coding protocol** (Protocol) – the event reporting protocol: **CID** or **SIA**.
- **Security panel model** – the type of the connected alarm control panel from the list (for the Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING connection, select **Paradox SP+/MG+ series KeyBus**, section 3.3.3).
- **Remote Arm/Disarm** – when ticked, the communicator controls the control panel directly (arming and disarming from Protegus 2). Only visible for directly controllable control panels. For direct control the control panel must also be set up as described in section 4.1.
- **Event** – when ticked, the communicator sends the control panel's events to the monitoring station and to Protegus 2. The app shows this switch, but it cannot be changed there.
- **Security panel PC download password** (PC download password; for Texecom the UDL passcode) – for direct control of a Paradox or Texecom control panel, the PC or UDL password; it must match the password set in the control panel, which is described in section 4.1.

6.4 CMS reporting (Reporting to CMS)

The communicator sends the events to the monitoring station over an IP connection – over the wired network (LAN) or the mobile network (SIM1, SIM2), in the order set in section 6.4.2. The events can go over several channels: the **primary** and the **parallel** channel work at the same time (to two receivers at once), and each has a **backup** channel that takes effect if the given channel fails. Communication is encrypted and password-protected. The TRK protocols require a Trikdis receiver that receives the events and forwards them to the

monitoring software: for an IP connection the IPcom software receiver (Windows or Linux), the RL14 IP/SMS receiver or the RM14 multi-channel receiver; the DC-09 and TL150 protocols are for universal and SUR-GARD receivers respectively (see below, **Protocol**).

6.4.1 Receiver channels (CMS settings)

In the app: Advanced settings → Reporting to CMS → CMS settings, then **Primary channel**, **Backup channel** or **Parallel channel** (within it **Parallel primary channel** and **Parallel backup channel**). The channel's settings appear when you switch on the **Enabled** switch.

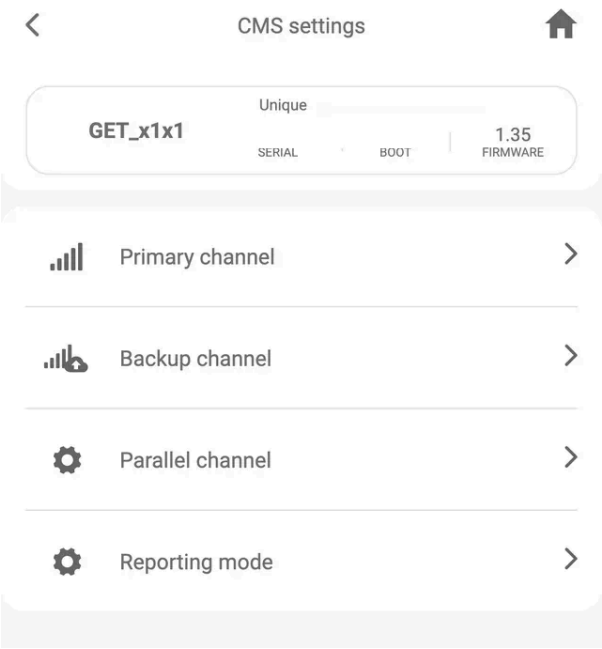


Figure 52. Protegus 2 – Reporting to CMS → CMS settings: Primary channel, Backup channel, Parallel channel and Reporting mode.

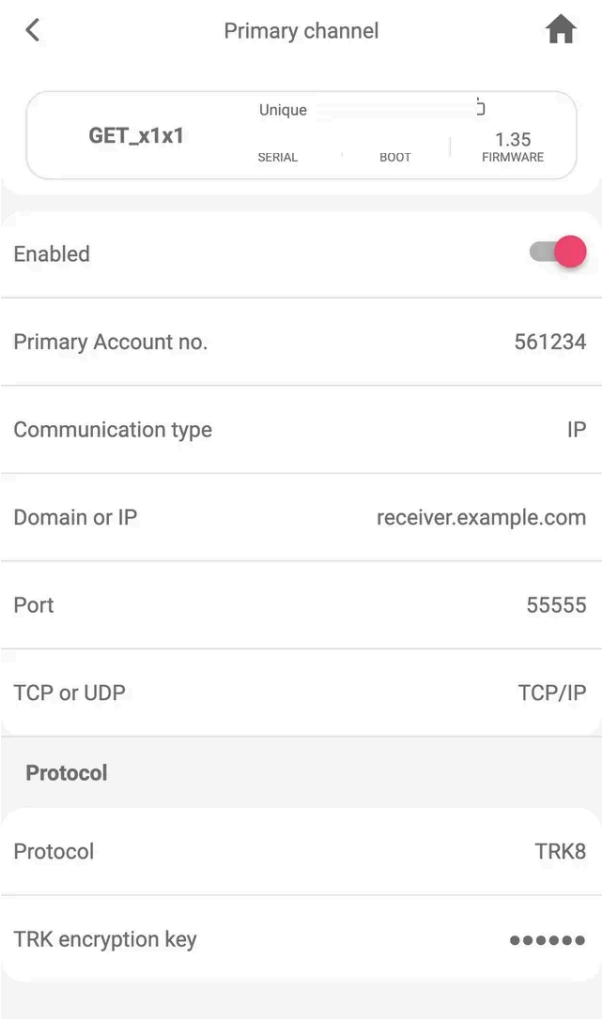


Figure 53. Protegus 2 – Primary channel on x1x1 hardware: Enabled, Primary Account no., Communication type IP, Domain or IP, Port, TCP or UDP, Protocol TRK8 and the TRK encryption key.

In TrikdisConfig: the **CMS settings** tab of the **CMS reporting** page.

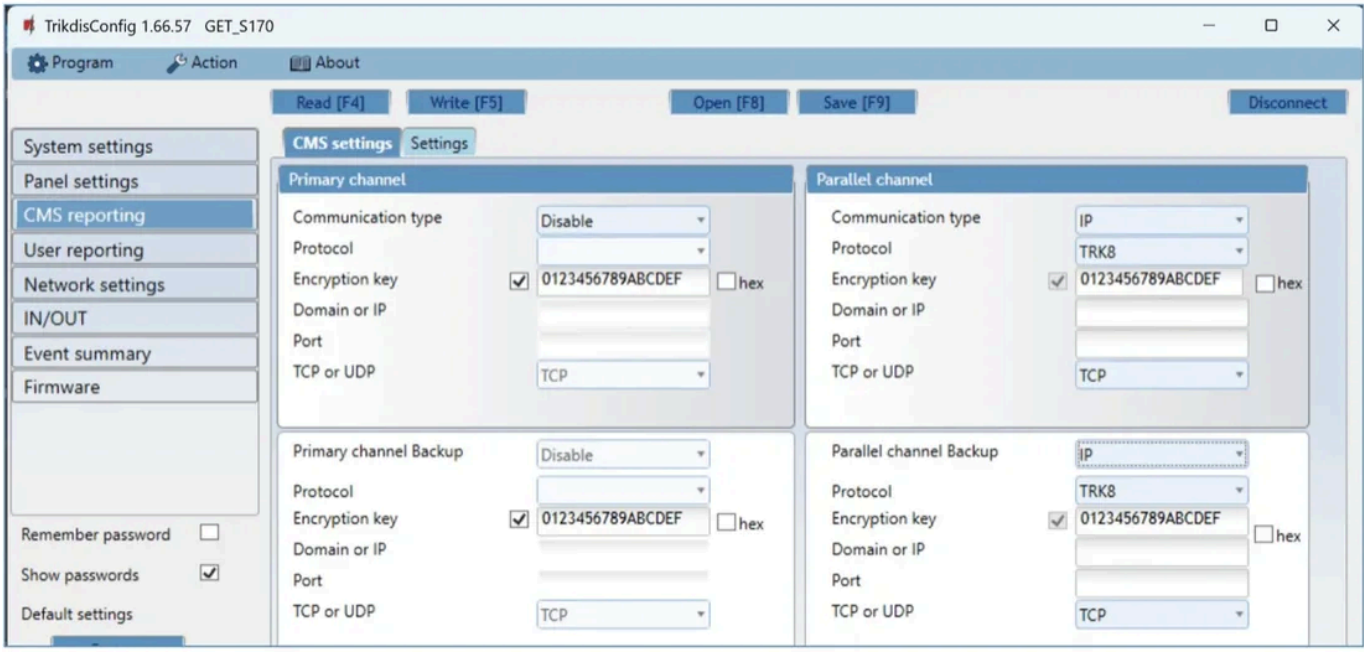


Figure 54. TrikdisConfig – CMS reporting, CMS settings tab: primary channel and its backup, parallel channel and its backup (in the picture the parallel channel with the IP / TRK8 / TCP setting).

Primary channel

- **Communication type** – the mode of connection with the receiver: **IP**.
- **Protocol** – **TRK8** (Trikdis receivers), **DC-09_2007** or **DC-09_2012** (universal receivers), **TL150** (SURGARD receivers).
- **Encryption key** (TRK encryption key; with the DC-09 protocols **Enable encryption key** and **DC-09 encryption key**, with the **HEX** switch for a hexadecimal key) – the encryption key of the messages; it must be the same in the communicator and in the receiver. In the app the TRK encryption key is at most 6, the DC-09 encryption key at most 16 characters (32 in HEX).
- **Domain or IP**, **Port** – the receiver's domain name or IP address and network port.
- **TCP or UDP** – the transmission protocol.

Primary channel Backup – backup channel. When switched on, it takes over communication if the primary channel does not work; its settings are the same as above.

Parallel channel. Alongside the primary, it sends to a second receiver at the same time (for example to the local and the central monitoring station). Its settings are the same as those of the primary channel.

6.4.2 Test, PING and the order of connections

In the app: Advanced settings → Reporting to CMS → Settings (test, PING, backup channel timings, receiver and line number) and **Reporting to CMS → CMS settings → Reporting mode** (the order of the connection paths). In the app there is a switch next to every interval: **Enable test** for the Test period, **Enable ping** for the IP ping period and **Test enabled** for the Communication path test; on the Reporting mode page the connection types are called **LAN**, **SIM** (SIM1) and **SIM2**.

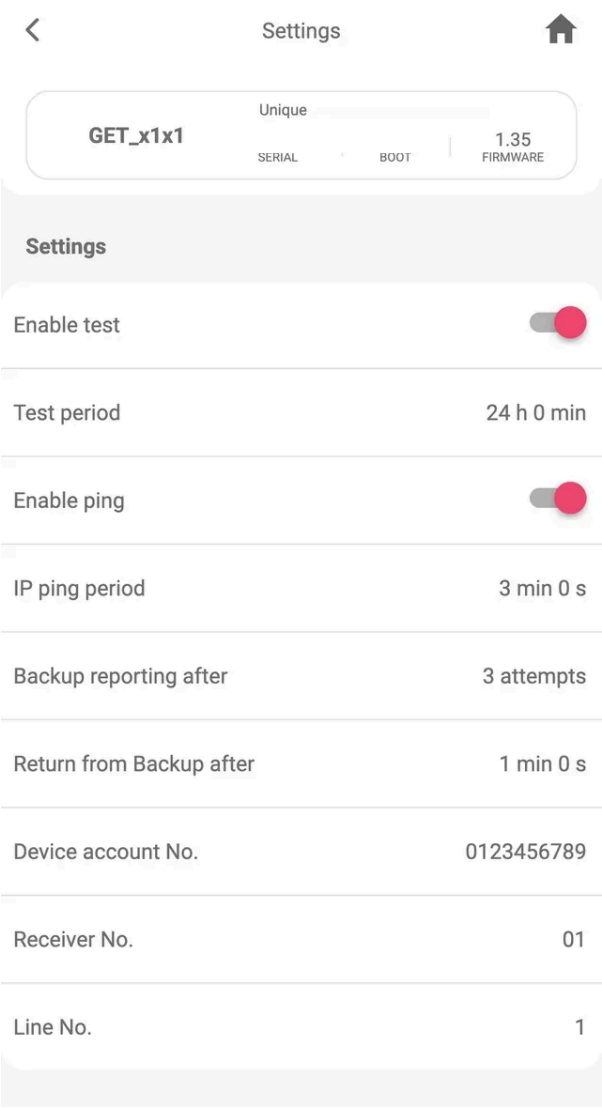


Figure 55. Protegus 2 – Reporting to CMS → Settings on x1x1 hardware: Enable test and Test period, Enable ping and IP ping period, Backup reporting after, Return from Backup after, Device account No., Receiver No., Line No.

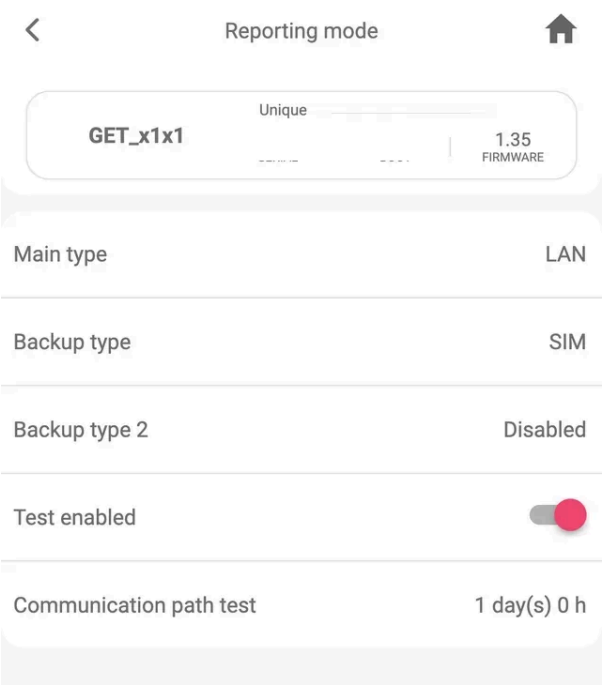


Figure 56. Protegus 2 – CMS settings → Reporting mode: Main type LAN, Backup type SIM, Backup type 2 Disabled, Test enabled and Communication path test.

In TrikdisConfig: the **Settings** tab of the **CMS reporting** page.

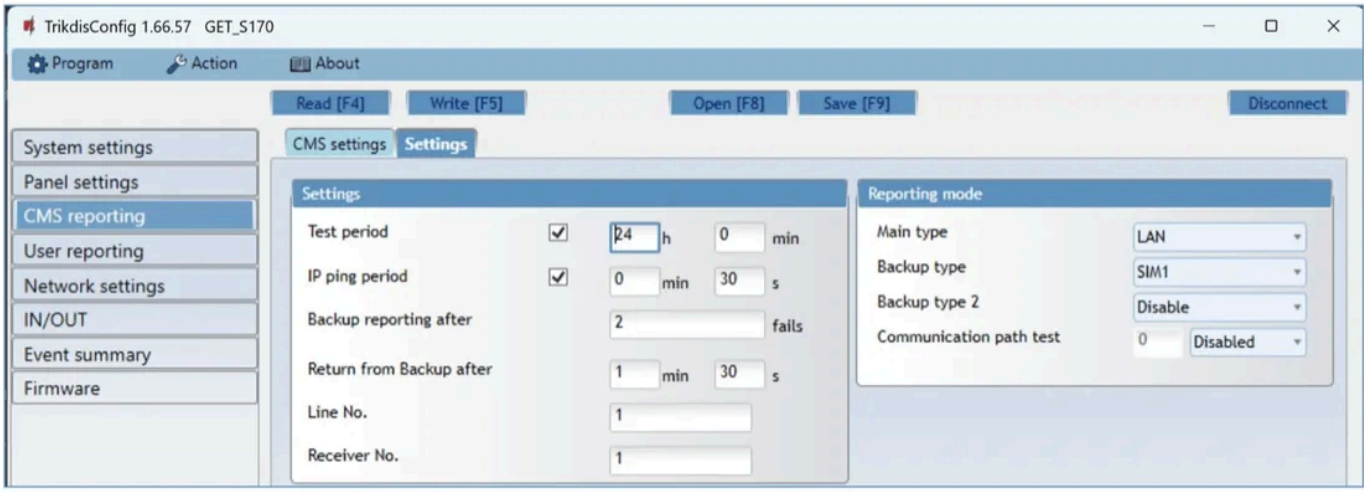


Figure 57. TrikdisConfig – CMS reporting, Settings tab: Test period, IP ping period, Backup reporting after, Return from Backup after, Line No., Receiver No.; in the Reporting mode group Main type LAN, Backup type SIM1, Backup type 2 Disable, Communication path test.

- **Test period** – the interval of the periodic test report (default 24 hours). The test report is sent as a Contact ID message to the monitoring station and to Protegus 2.
- **IP ping period** – the interval of the keep-alive signal (PING) on the IP channel (default 30 s). You enable it with the tick box and enter the time in the minutes (**min**) and seconds (**s**) fields; it is required for connection supervision. The receiver does not forward PINGs to the monitoring software so as not to overload it; the software only receives a message if the receiver gets no PING for three times the set period. For example, if the PING period is 3 minutes, the loss of connection is reported after the 9th minute.
- **Backup reporting after** – after this many failed sending attempts the device switches to the backup channel (default 2).

- **Return from Backup after** – after this time it returns to the primary channel (default 1 min 30 s).

The PING keeps the live connection between the device and the receiver, and remote access, control and programming also depend on it. That is why **we do not recommend a PING period longer than 5 minutes**.

DC-09 Settings (on the right side of the tab) – only needs to be filled in if you send with the DC-09_2007 or DC-09_2012 protocol on any channel; the group appears when DC-09_2007 or DC-09_2012 is selected in the **Protocol** field of any channel:

- **Object ID in DC-09** – a 3–16 character hexadecimal identifier, provided by the monitoring station.
- **DC-09 line No** – the line number.
- **DC-09 receiver No.** – the receiver number.

On the GET's Settings tab, the **Line No.** (the receiver's line number) and **Receiver No.** (receiver number) fields are also here; there is no separate "Object ID in DC-09" field on the GET.

Reporting mode group – here you set the path on which the communicator communicates with the monitoring station channels and with Protegus 2. You enter the connection types in order: if the connection set in **Main type** cannot be established, the communicator switches to the one set in **Backup type**, and so on; if the message was sent successfully on the backup path, after the set time (Return from backup after) it tries the main path again.

- **Main type** – the type of the main connection with the receiver and with Protegus 2: **LAN**, **SIM1** or **SIM2**.
- **Backup type** – the type of the backup connection (LAN, SIM1, SIM2).
- **Backup type 2** – the type of the second backup connection (LAN, SIM1, SIM2).
- **Communication path test** – the interval at which the communicator tests the selected connection types (LAN, SIM1, SIM2).

6.5 User reporting (Protegus Cloud)

With the Protegus 2 service the user monitors and controls the communicator and the system connected to it remotely; details: web.protegus.app. In the app: **Advanced settings** → **User reporting** → **Cloud**; in TrikdisConfig the **PROTEGUS Cloud** tab of the **User reporting** page.

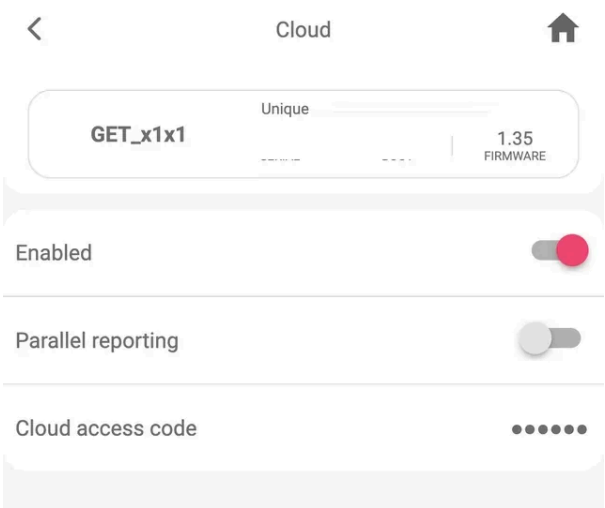


Figure 58. Protegus 2 – User reporting → Cloud: Enabled, Parallel reporting, Cloud access code.

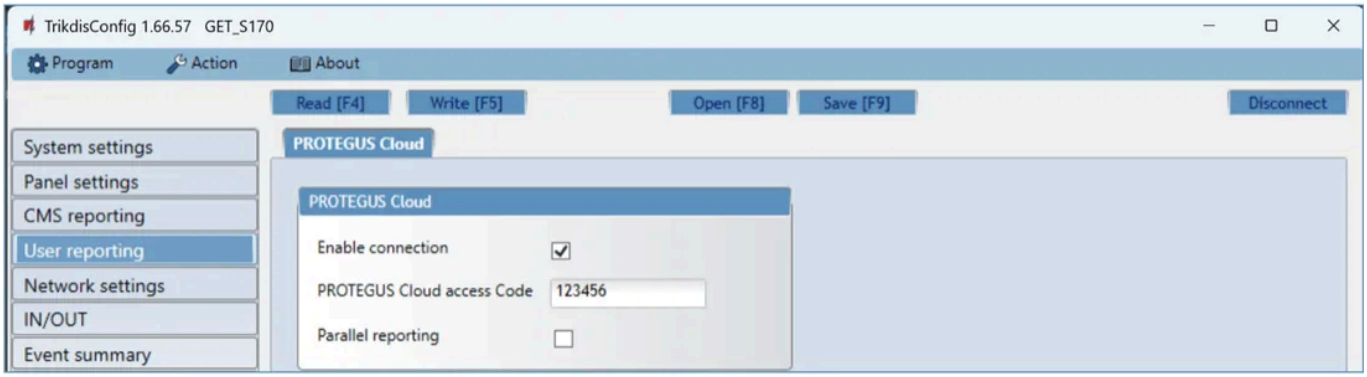


Figure 59. TrikdisConfig – User reporting, PROTEGUS Cloud tab: Enable connection, PROTEGUS Cloud access Code, Parallel reporting.

- **Enable connection** (Enabled) – enables the Protegus 2 service: the device exchanges data with the Protegus 2 app, and TrikdisConfig can also reach it remotely.
- **PROTEGUS Cloud access Code** (Cloud access code) – 6-digit code for connecting to Protegus 2 (default `123456`). If you change it in TrikdisConfig, it must also be changed in the Protegus 2 app.
- **Parallel reporting** (in the app only visible if the firmware supports it) – when ticked, the messages go on the primary channel (to the monitoring station) and to Protegus 2 at the same time; Protegus 2 and the users only receive the message after it has been sent to the monitoring station.

6.6 Network settings

6.6.1 LAN (Ethernet)

These settings must be entered if the communicator is connected to the wired local network (LAN). In the app: **Advanced settings** → **Network settings** → **LAN**; **Static IP**, **Subnet mask**, **Default gateway**, **DNS1** and **DNS2** can only be changed with **Use DHCP** switched off. In TrikdisConfig the **LAN** tab of the **Network settings** page, **Ethernet settings** group.

What does the network need? The communicator itself initiates the outgoing connection to the monitoring receiver and the Protegus cloud, so **no port needs to be opened or forwarded** on the router, and neither a public static IP address nor dynamic DNS is needed. What you do need:

- a free Ethernet port on the router or switch;
- DHCP (factory setting), or a static IP address, subnet mask, gateway and DNS provided by the network administrator;
- outgoing traffic allowed to the receiver's address and port (TCP or UDP, depending on the receiver setting), as well as to the Protegus cloud.

On a filtered – corporate or institutional – network, agree on this with the network administrator in advance: home routers allow all outgoing connections by default, but a firewall-protected network may need a separate rule.

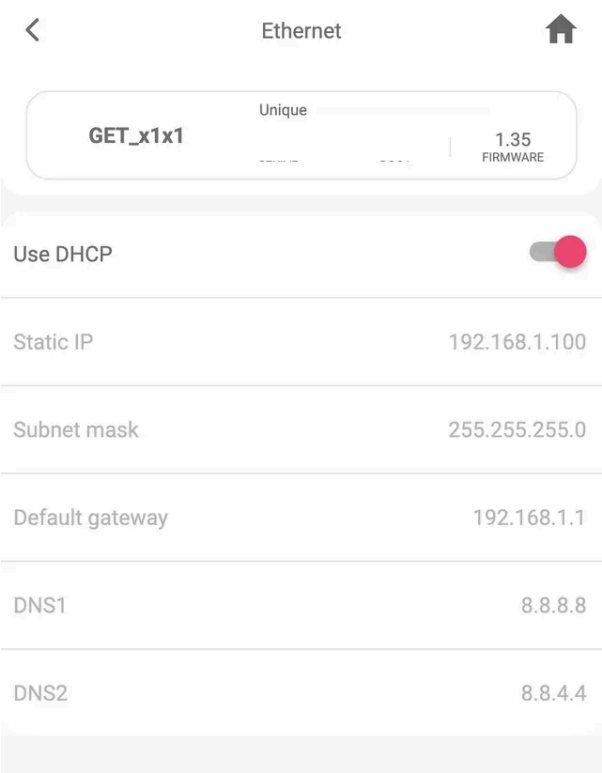


Figure 60. Protegus 2 – Network settings → LAN: Use DHCP switched on; the Static IP, Subnet mask, Default gateway, DNS1 and DNS2 fields are greyed out in this case.



Figure 61. TrikdisConfig – Network settings, LAN tab, Ethernet settings group: Use DHCP, Static IP, Subnet mask, Default gateway, DNS 1, DNS 2.

- **Use DHCP** – when ticked, the communicator logs on to the network automatically (it gets an address from the router's DHCP server). If automatic logon fails, the addresses must be entered manually:
- **Static IP** – the communicator's fixed IP address with manual setup.
- **Subnet mask** – subnet mask with manual setup.
- **Default gateway** – the address of the gateway (router) with manual setup.
- **DNS1, DNS2** – name servers (DNS, Domain Name System: it gives the IP address belonging to a domain name); they are needed if you entered the receiver in the channel's **Domain or IP** field with a domain name and not an IP address. The default is Google's public DNS. Regardless of the IP settings, check that the DNS addresses work with your internet service provider.

6.6.2 SIM1 and SIM2

These settings must be entered separately for every inserted SIM card; the settings of the SIM1 and SIM2 holders are the same.

Before use, make sure that the SIM card is active and working, and that the mobile data service is also enabled on the card.

In the app: **Advanced settings** → **Network settings** → **SIM** (SIM1) or **SIM2**. In TrikdisConfig the **SIM1** or **SIM2** tab of the **Network settings** page, **SIM card** group.

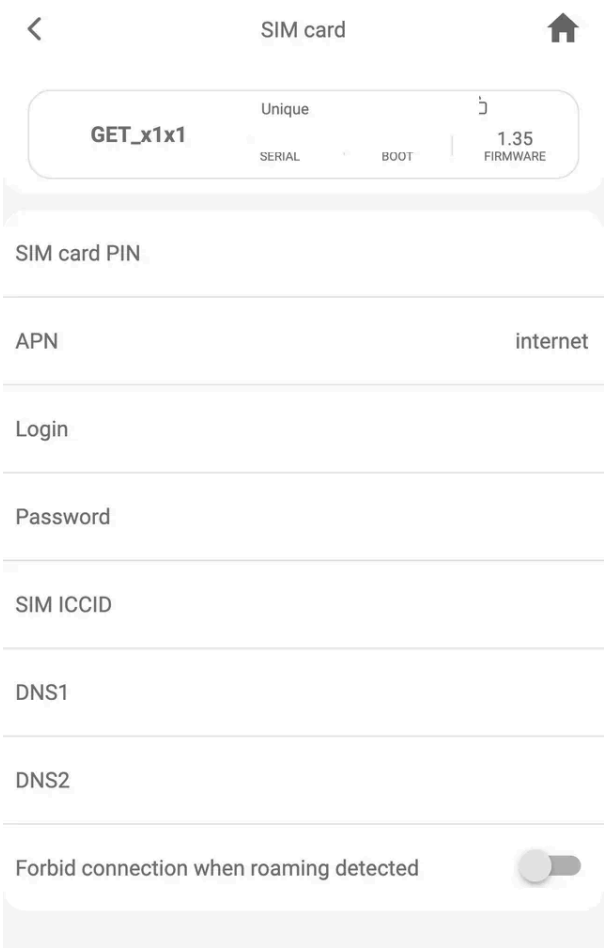


Figure 62. Protegus 2 – Network settings → SIM: SIM card PIN, APN, Login, Password, SIM ICCID, DNS1, DNS2 and the Forbid connection when roaming detected switch.

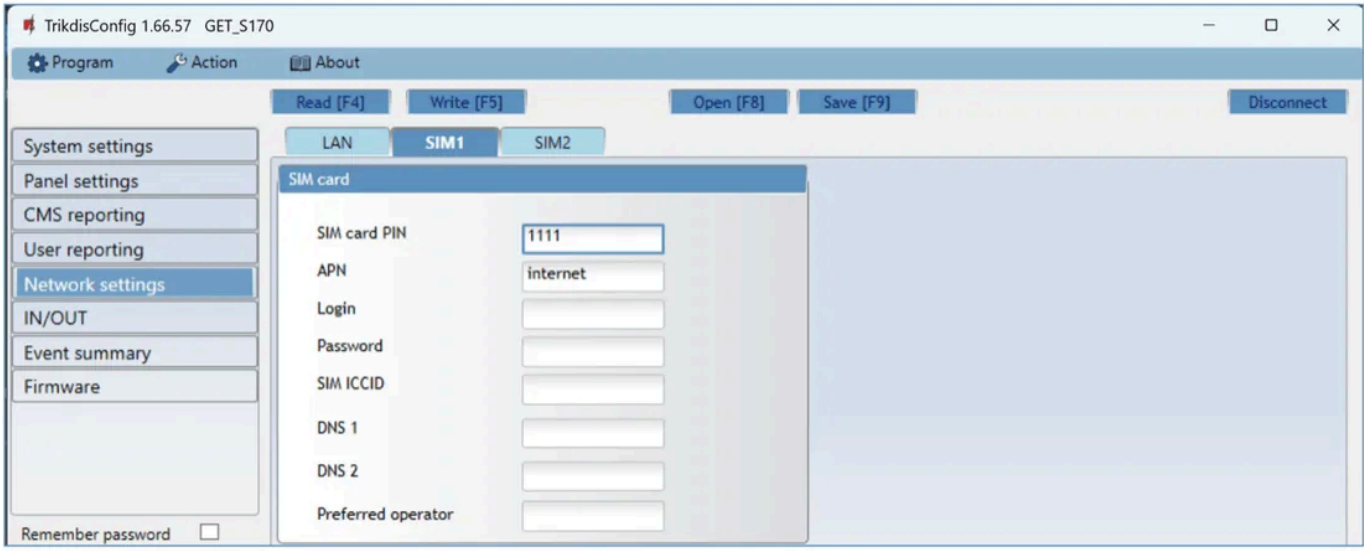


Figure 63. TrikdisConfig – Network settings, SIM1 tab, SIM card group: SIM card PIN, APN, Login, Password, SIM ICCID, DNS 1, DNS 2, Preferred operator (the SIM2 tab is the same).

- **SIM card PIN** – the card's PIN code. You can switch off the PIN request by putting the card into a mobile phone and disabling it there; in that case the field's default value can stay.
- **APN** – the operator's access point (Access Point Name); without it the device does not connect to the internet. You can find the value on the website of the SIM card's operator; `internet` is generic and works in many operators' networks. The known APNs of operators are listed in the APN article (for an IoT / M2M card the operator gives a separate APN, see section 2.3).
- **Login, Password** – user name and password for the internet connection, if the operator requires them.
- **SIM ICCID** – the SIM card's ICCID number, if you want the device to work only with this card.
- **DNS1, DNS2** – name servers; they are needed if you entered the receiver in the channel's **Domain or IP** field with a domain name. The default is Google's public DNS; check that the DNS addresses work with your operator.
- **Preferred operator** – the mobile operator's code (MCC + MNC); if you enter it, the device only connects to the selected operator's network. **Only in TrikdisConfig**.

On the app's SIM page, instead of Preferred operator there is the **Forbid connection when roaming detected** switch: when switched on, the communicator does not connect if it detects roaming. On hardware version **M15**, with firmware **1.17** or newer, the **Generation** and **Bands** settings also appear on the SIM page: with these you can restrict which mobile network technology and frequency bands the communicator uses.

6.7 IN/OUT

Here you set the role of the communicator's two dual-function I/O terminals: **Disabled** (not used), **IN** (input) or **OUT** (output; on the GET this is the default setting). For an input, the type of the connected circuit must also be set in the **Type** field (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL). Additional detectors can be connected to the inputs: when the detector is triggered, the communicator sends its own event with the Contact ID (SIA) code assigned to the input to the monitoring station and to Protegus 2.

In the app: **Advanced settings** → **IN/OUT**, then terminal **1** or **2**: the **Function** (Disabled, IN, OUT) and for an input the **Type**; in the **Alarm** and **Tamper** sections the event and restore messages sent when the input is triggered. In TrikdisConfig the **IN/OUT** page.

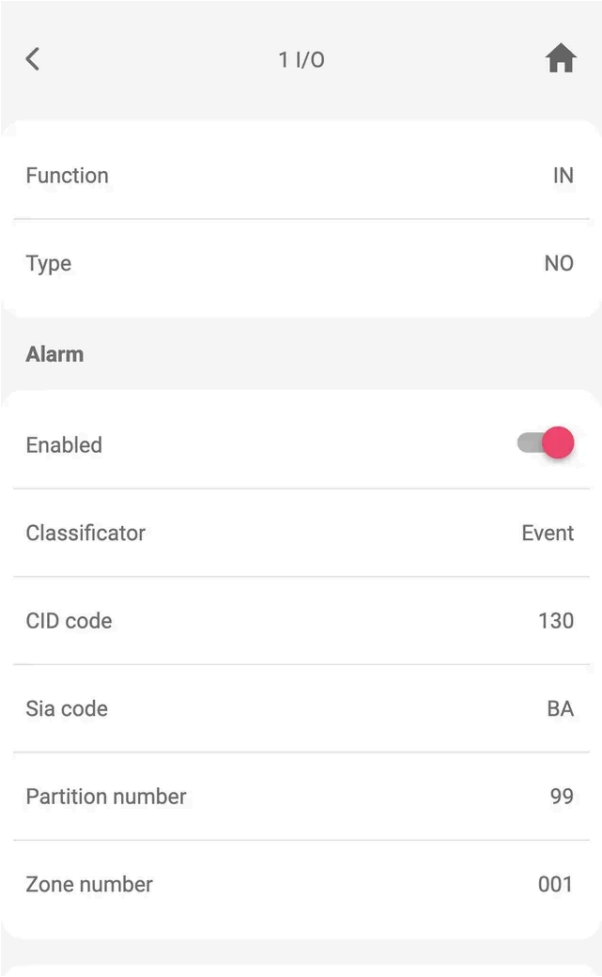


Figure 64. Protegus 2 – IN/OUT, terminal 1: Function IN, Type NO; the Alarm event Enabled, Classificator Event, CID code 130, Sia code BA, Partition number 99, Zone number 001.

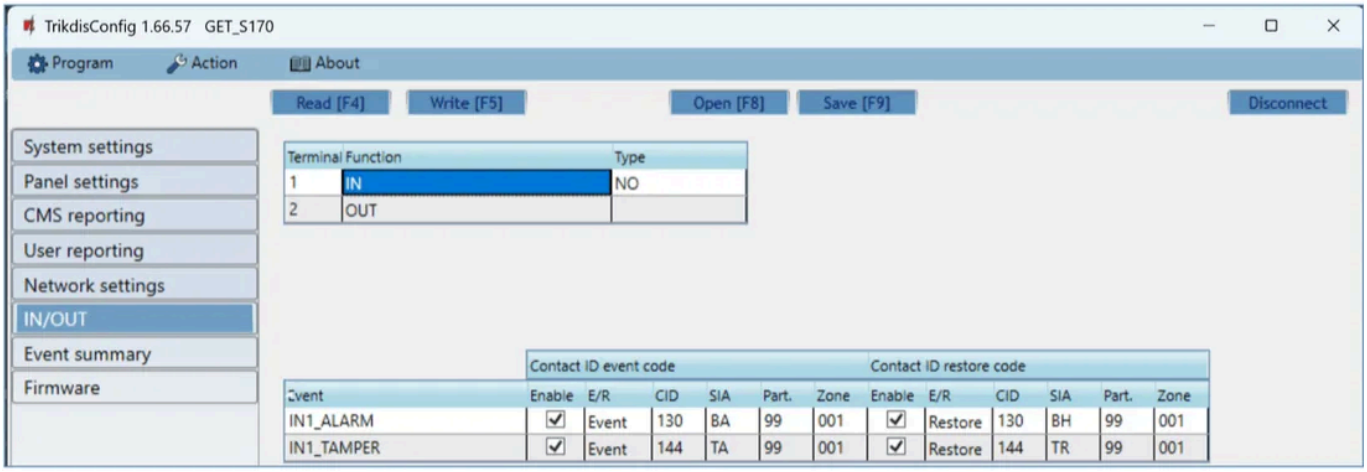


Figure 65. TrikdisConfig – IN/OUT page: terminal 1 is an input (IN, NO), terminal 2 an output (OUT); below, the alarm and tamper events of input 1 with CID and SIA codes.

When the detector connected to the input is triggered, the communicator sends an alarm (**INx_ALARM**, Contact ID 130, SIA BA; restore BH), and when the tamper circuit is violated, a tamper event (**INx_TAMPER**, 144, SIA TA; restore TR); the events of every terminal set as an input appear in the table. The columns of the table:

- **Enable** (Enabled) – enables sending the message to the monitoring station and to Protegus 2.

- **E/R** (Classificator) – the type of the message: Event or Restore.
- **CID** (CID code) – the Contact ID code (it can be changed, or the default can stay); when the input is triggered, the message goes to Protegus 2 and to the monitoring station with this code.
- **SIA** (Sia code) – the SIA code (it can be changed, or the default can stay).
- **Part.** (Partition number) – the partition number in the message (for the event and the restore as well).
- **Zone** (Zone number) – the zone number in the message.

6.8 Event summary (System events)

Here you can enable, disable and change the device's own internal messages. A message disabled here is not sent, regardless of any other setting. In the app: **Advanced settings** → **System events**, the messages are in the **Event** and **Restore** lists; to change one, select the message. In TrikdisConfig the **Event summary** page.

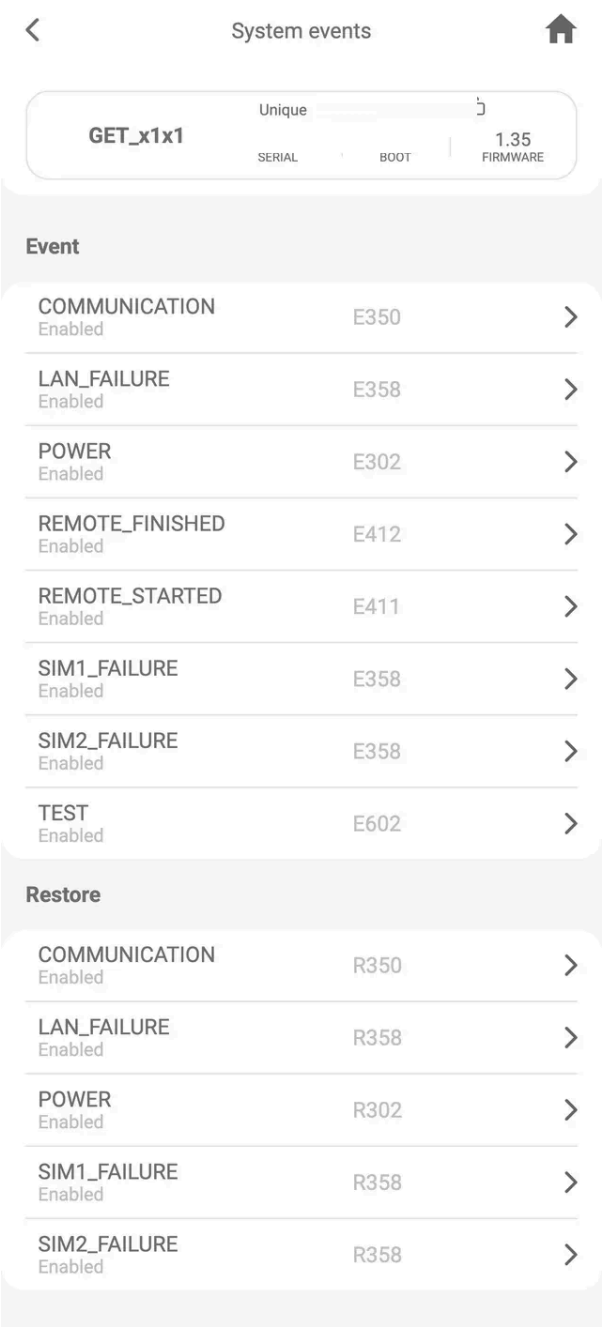


Figure 66. Protegus 2 – System events: the Event list (COMMUNICATION E350, LAN_FAILURE E358, POWER E302, REMOTE_FINISHED E412, REMOTE_STARTED E411, SIM1_FAILURE E358, SIM2_FAILURE E358, TEST E602) and the Restore list.

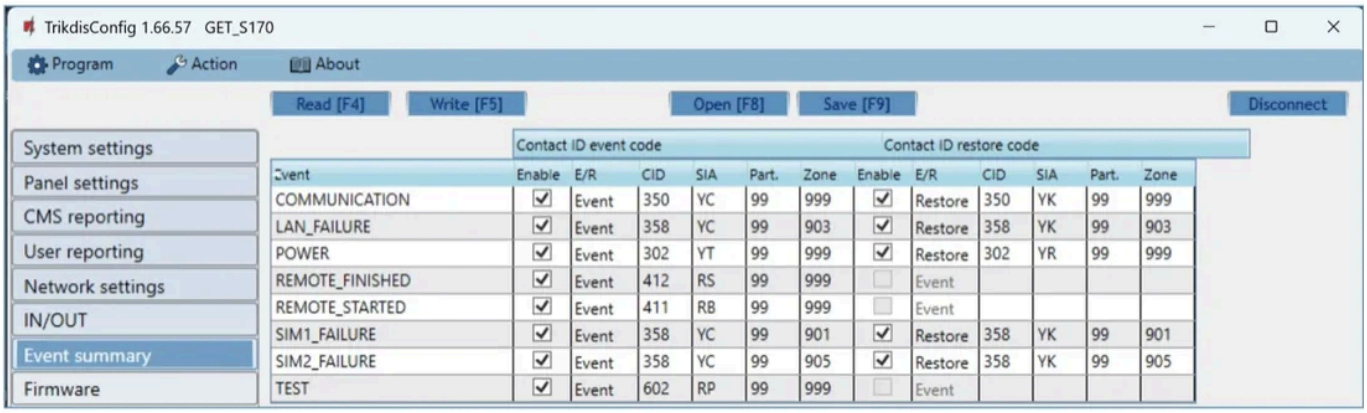


Figure 67. TrikdisConfig – Event summary page: the device's internal messages with CID and SIA codes, with partition 99.

The GET's internal messages (in brackets the default Contact ID code and zone):

- **COMMUNICATION** (350, zone 999) – fault of the connection between the control panel and the communicator; its restore is a separate message.
- **LAN_FAILURE** (358, zone 903) – fault of the wired network (LAN) connection; its restore is a separate message.
- **POWER** (302, zone 999) – low supply voltage; its restore is a separate message.
- **REMOTE_FINISHED** (412) – end of remote programming with TrikdisConfig (disconnection).
- **REMOTE_STARTED** (411) – remote connection for programming the GET with TrikdisConfig.
- **SIM1_FAILURE** (358, zone 901) – fault of the mobile network connection on SIM1; its restore is a separate message.
- **SIM2_FAILURE** (358, zone 905) – fault of the mobile network connection on SIM2; its restore is a separate message.
- **TEST** (602) – periodic test report.

You switch on the periodic TEST message and set its interval in the **Test period** field (section 6.4.2).

- **Enable** (Enabled) – when ticked, sending the message is enabled.
- For every message, the Contact ID (SIA) code, and the zone and partition number can be changed.

6.9 Restoring the factory settings

The factory settings can **not** be restored from the Protegus 2 app: this requires the TrikdisConfig **Restore** button or the device's **RESET** button.

To restore the factory settings, click the **Restore** button in the **Default settings** group at the bottom left of the TrikdisConfig window. Restoring deletes all settings – including the passwords – so it is worth saving the settings to a file first (**Save [F9]**).

With the installer password this is only possible if the administrator has not disabled it on the **System settings** → **Access** page.



Figure 68. TrikdisConfig – the Restore button of the Default settings group.

The factory settings can also be restored on the device, without a computer: with the power on, press and hold the **RESET** button on the printed circuit board (section 1.4) for **10 seconds**, until the NETWORK, POWER and TROUBLE LEDs go out and then the POWER LED lights up. Then release the button: the factory settings have been restored.

7. Remote programming

TrikdisConfig reaches Trikdis devices not only over a USB cable but also **remotely, via the Protegus cloud**. This way you can change the settings of an already installed device without going to the site.

Remote access requires:

1. The device must be switched on and have a network connection (the **POWER** and **NETWORK** LEDs are lit green; on a mobile network device the NETWORK LED also flashes yellow). On a mobile network device, the inserted SIM card must be active and its PIN code must be entered in the device, or the PIN request must be disabled; on an Ethernet device, the network (LAN) cable must be plugged in and the device must be able to reach the internet.
2. On the **User reporting** → **PROTEGUS Cloud** page of TrikdisConfig, **Enable connection** must be ticked (set this over USB during the first commissioning).
3. You need to know the device's **unique identifier** (IMEI or MAC – printed on the box and on the back of the device) and the administrator or installer password.

Steps:

1. Start the TrikdisConfig software.
2. In the **Remote access** section, enter the device's unique identifier (IMEI or MAC) in the **Unique ID** field.
3. Optionally, give the system a name in the **System name** field – the software remembers it, and next time you can choose it from the drop-down list.
4. Press the **Configure** button.
5. In the window that opens, click the **Read [F4]** button and enter the password. With the **Remember password** tick box, the software remembers it for this session.
6. Make the changes, then send them to the device with the **Write [F5]** button.

The software saves the named systems you have programmed remotely before; you can list them with the arrow next to the **System name** field. To delete one, select the identifier in the list, press the **Delete** key and confirm.

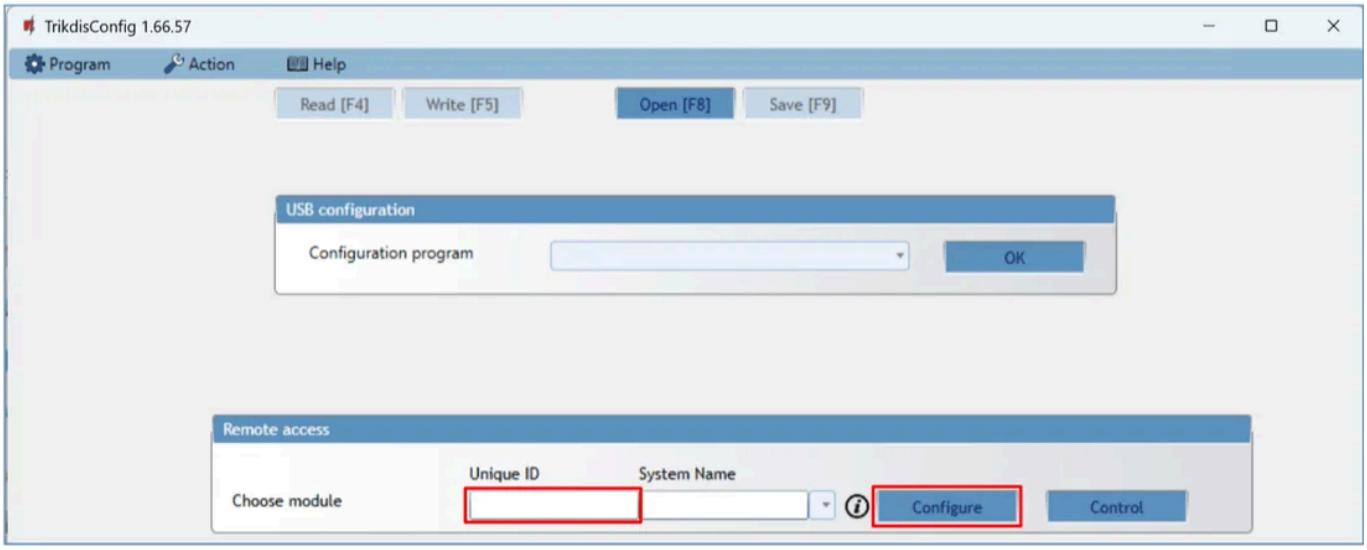


Figure 69. TrikdisConfig – the Remote access group: the Unique ID field, the System name list and the Configure button.

The GET's unique identifier is the **IMEI / Unique ID**; it can be read on the device's label and on the sticker on the box. Remote access only works if the SIM card is active, and its PIN code is entered or the PIN request is switched off – **or** the communicator is connected with a network (LAN) cable –; **Enable connection** is ticked on the **User reporting** → **PROTEGUS Cloud** page (section 6.5); the **POWER** LED is steady green; the **NETWORK LTE** LED is steady green and flashing yellow (with a wired connection only, the **NETWORK LAN** LED is steady green). The communicator reports the start and the end of remote programming with the REMOTE_STARTED and REMOTE_FINISHED messages (section 6.8).

8. Checking that the communicator works

After programming and wiring, always check the whole chain: alarm panel → communicator → monitoring station and/or Protegus 2.

Before that, check that there is power (the **POWER** LED is lit green) and a network connection (the **NETWORK** LED is lit green).

1. **Trigger an event.** Arm and then disarm the system on the keypad, or violate a zone while the system is armed so that an alarm is generated.
2. **Check that it arrives.** See whether the event has appeared in the monitoring software and/or in the event list of the Protegus 2 app – with the correct partition and zone number.
3. **Inputs.** Trigger the detector wired to the communicator's own input and check the corresponding event.
4. **Outputs.** Switch the output from the Protegus 2 app and check that the connected device (relay, keyswitch zone) actually operates.
5. **Remote arming.** If the panel can be controlled remotely, also arm and disarm it from the Protegus 2 app.

If the communicator reports both over the wired network and over the mobile network (section 6.4.2, Reporting mode), it is worth doing the test on both paths: unplug the LAN cable, trigger an event, and check that it also reaches the monitoring station through the SIM card; then plug the cable back in.

9. Firmware update

Ha bármikor az USB bedugásakor a program azt jelzi, hogy új firmware verzió jelent meg a Trikdis eszközhöz, fogadd el a frissítést és telepítsd!

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.

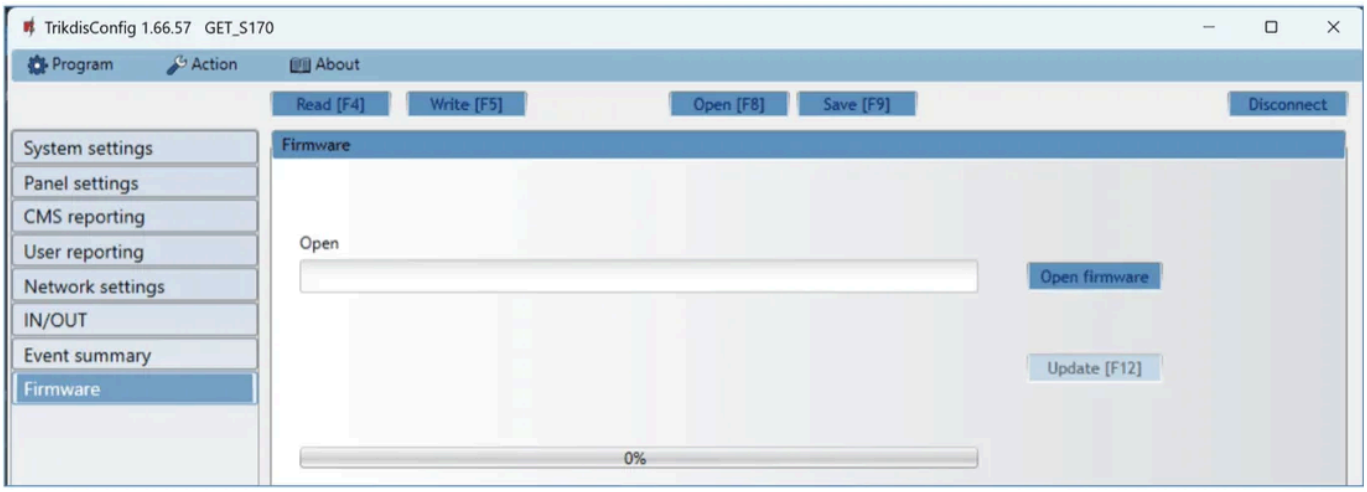


Figure 70. TrikdisConfig – Firmware page: Open firmware button, Update [F12] button and the progress bar.

The update requires an internet connection. Antivirus software, a firewall or strict internet access settings can prevent the automatic firmware update; in that case the antivirus settings must be changed.

Some functions of the GET require a specific firmware version:

- **1.08** or newer: setup from the Protegus 2 app (Advanced settings, section 2.2 and chapter 6);
- **1.17** or newer, on hardware version **M15**: the **Generation** and **Bands** settings on the app's SIM page (section 6.6.2);
- **1.21** or newer: the Paradox SP / SP+ / MG / MG+ Keybus + TIP/RING connection (section 3.3.3);
- **1.31** or newer, on hardware version **x1x1**: in the app the identifiers (Account No., Device account No.) are among the CMS settings (section 6.2).

10. Troubleshooting and frequently asked questions

The most common questions and faults, starting from the LED indications. Where the answer refers to a detailed chapter, you will find the exact location of the setting there.

The NETWORK LTE LED is off – no mobile network

1. Look at the flashes of the **TROUBLE** LED: 2 = SIM1 card fault, 3 = SIM2 card fault (section 1.6).
2. Check that the SIM card is active, has data service, and sits properly in its holder (SIM1 in the middle of the board, SIM2 at its left edge; section 3.1).
3. If the PIN request is switched on for the card, enter the PIN on the **Network settings** → **SIM1** (or **SIM2**) tab, or switch off the PIN request in a phone.
4. Check the APN (section 2.3): for an IoT / M2M card the operator gives a separate APN.
5. Check the antenna: it is screwed on, it is not in a metal enclosure, and the signal level is adequate (the NETWORK LTE LED flashes yellow at least 3 times; sections 1.6 and 3.2).
6. If the communicator reports over the wired network, the lack of the mobile network does not stop it by itself: it sends on the next available path according to the **Reporting mode** order (section 6.4.2) – but the backup path is then missing, so it is worth fixing.

The NETWORK LAN LED is off – no wired network

1. 1 flash of the **TROUBLE** LED indicates a fault in the physical connection of the wired network: check the LAN cable at both ends, and whether the router or switch port is live (section 1.6).
2. If the cable is fine, look at the **Network settings** → **LAN** tab: with DHCP the router must give an address; with a fixed address the Static IP, the Subnet mask and the Default gateway must match the local network (section 6.6.1).
3. If you entered the receiver with a domain name, the DNS addresses must also work in the network (DNS1, DNS2).

There is a network, but the monitoring station gets no events

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. Check the receiver's address, port, the TCP/UDP setting, the protocol and the encryption key (**CMS reporting** → **CMS settings**, section 6.4.1); the key must be the same in the communicator and in the receiver.
2. Look at the **Reporting mode** setting (section 6.4.2): the **Main type** must be a path that is actually available at the site (there is a LAN cable, or there is a SIM card in the given holder), and there must be a backup path too.
3. If the receiver is entered with a domain name, check the DNS setting on the path on which the communicator reports (**Network settings** → **LAN**, or **SIM1 / SIM2** → **DNS1, DNS2**).
4. On the mobile network, check that the SIM card's data plan does not block the required port (some M2M cards only allow certain addresses); on the wired network, the local firewall must allow the receiver's port outbound.
5. If the control panel sends no events (the DATA LED does not light up), the cause is on the control panel side: see the next item.

The TROUBLE LED flashes seven times – no connection to the control panel

1. With a data bus or serial connection, check the CLK and DATA wires, and that the type of the connected control panel is selected in the **Panel settings** → **Security panel model** field (section 6.3).
2. With a Paradox control panel, check that the serial port is not locked (section 4.1.2); with Texecom and Paradox control panels the **Security panel PC download password** must match the one set in the control panel.
3. With a telephone line connection, the control panel's dialer must be switched on, in DTMF mode, with Contact ID format and a phone number entered (section 4.2), and **Communication protocol** must be **2. AUTO** (section 6.3).

Which path does the event take: LAN or SIM?

The one given by the **Reporting mode** order (section 6.4.2): the path set in **Main type**; if that does not work, the one in **Backup type**, then in **Backup type 2**. If the message was sent on the backup path, the communicator tries the main path again after the **Return from backup after** time, and tests every path at the **Communication path test** interval. The Protegus 2 connection uses the same path. On the wired network no mobile data is used.

What are the two SIM holders for?

With cards from two different operators, the mobile network also becomes dual-path: in Reporting mode SIM1 and SIM2 are separate connection types, and either can be the main or the backup path (section 6.4.2). The two cards must be set up separately (**Network settings** → **SIM1**, **SIM2**: PIN, APN; section 6.6.2); a SIM2 fault is indicated by 3 flashes of the TROUBLE LED and the SIM2_FAILURE message (sections 1.6 and 6.8). The communicator also works with one card.

DSC: every alarm arrives as an E130 general alarm

When connected to the Keybus only, the communicator receives the state of the zones from the control panel, but not the zone type, so it reports every alarm with the E130 code (section 3.3.1). Connecting the Keybus and TIP/RING together is not available on the GET (it is a function of the GT+). If the monitoring station expects the code matching the zone type (for example fire: E110), connect the GET only to the control panel's TIP/RING terminals and program the dialer (sections 3.3.9 and 4.2): this way the control panel's own Contact ID codes are sent, but there is no direct control – arming requires a keyswitch zone (section 3.4).

Paradox: the serial port is locked, or there is no connection

On the newer Paradox control panels (SP+, MG+, EVOHD+) the serial port may be locked at the factory; unlocking is covered in section 4.1.2 and in the article Unlocking a locked serial port on Paradox alarm control panels. With the Spectra SP / SP+ and Magellan MG / MG+ control panels, the Keybus + TIP/RING connection can also be used instead of the serial port (section 3.3.3); it does not require unlocking, but the communicator's firmware must be at least 1.21 (chapter 9).

I cannot arm from Protegus 2

1. With direct control, **Panel settings** → **Remote Arm/Disarm** must be ticked, and the control panel must be set up as described in section 4.1 (Paradox: PC password, firmware V.4+; Texecom: UDL passcode; Caddx, InnerRange, Honeywell: the settings described). Check in the table of section 1.3 whether the control panel can be controlled directly at all.
2. With keyswitch arming (section 3.4), the terminal must be **OUT** on the **IN/OUT** page (the GET's default setting), the control panel's zone must be a keyswitch zone, and in Protegus 2 the output must be assigned to the partition, in the same mode as the control panel's (pulsed or two-state; section 5.2).

3. Protegus 2 shows the partition's state from the control panel's arming and disarming events: the control panel must report these (Opening/Closing).

Protegus 2 does not see the device

1. **Enable connection** must be ticked on the **User reporting** → **PROTEGUS Cloud** page (section 6.5).
2. When adding, you must enter the **PROTEGUS Cloud access Code** set in the device; if you changed the code in TrikdisConfig, change it in the app as well.
3. Enter the IMEI exactly, from the device's label or the sticker on the box (or scan the QR code).
4. There must be a working internet connection on at least one path: the NETWORK LTE LED is green and flashing yellow (SIM card with data service and a correct APN), or the NETWORK LAN LED is green (LAN cable). The DATA LED must go out after an event.

I cannot log in remotely with TrikdisConfig

1. The device must be online (NETWORK LTE green, flashing yellow, or NETWORK LAN green), and the Protegus connection must be enabled (**Enable connection**).
2. **CMS reporting** → **Settings** → **IP ping period** must not be longer than 5 minutes: the PING keeps up the connection needed for remote access.
3. Check the administrator or installer password.

Can I set up the communicator from the app?

Yes: with firmware 1.08 or newer, most settings are available in the Protegus 2 **Settings** → **Advanced settings** menu (section 2.2 and chapter 6). What is only in TrikdisConfig: restoring the factory settings (section 6.9), **Preferred operator** (section 6.6.2) and manual firmware update (chapter 9); the app shows the Serial bus **Event** switch, but does not change it. When logged in with the installer code, you can only change the groups the administrator has allowed (section 6.2).

I have forgotten the password

It cannot be reset with TrikdisConfig, because the restore also requires a password. It can be reset with the device's **RESET** button, though (section 6.9): with the power on, hold it pressed for 10 seconds. All settings are deleted. Restoring cannot be started from the app.

How much data traffic does the device use?

The event messages and the PINGs are very small; the traffic mainly depends on the PING period and on the frequency of the test reports. For an average household system the monthly traffic typically stays below 10 MB. The exact value depends on the settings and on the operator's billing unit, so with a data-limited card it is worth checking the traffic of the first month. As long as the communicator reports over the wired network, the SIM card's data is not used.

11. 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.

- Security equipment may only be installed and maintained by a qualified installer.
- Read the manual before installation; ignoring the instructions can lead to malfunction or failure of the equipment.
- Disconnect the equipment from the power supply before wiring, before every electrical connection and before servicing.
- Modifications, alterations and repairs not authorized by the manufacturer void the warranty.
- Follow local waste disposal regulations: do not throw the unusable device or its parts in household waste. The crossed-out wheeled bin symbol (WEEE) on the device indicates that it must be handed in separately as electronic waste.

See also

- Compatibility finder – which Trikdis communicator and which connection suits your alarm control panel.
- Trikdis communicator + DSC alarm control panel: short installer guide – the steps of the DSC connection in brief.
- Trikdis communicator + Paradox alarm control panel: short installer guide – the steps of the Paradox connection in brief.
- DSC Power Series NEO and Trikdis communicators: compatibility and solutions – why the NEO cannot be connected to the data bus, and what the solution is.
- Unlocking a locked serial port on Paradox alarm control panels – unlocking the serial port of the SP+, MG+ and EVOHD+ control panels.
- Remote arming with a keyswitch from the Protegus 2 app – the details and pitfalls of keyswitch arming.
- APN settings – list of European mobile operators – the operators' APNs, also for IoT / M2M cards.
- Documentation in English: docs.trikdis.com – GET – the Contact ID → SIA code conversion table is also here (appendix). The manuals on docs.trikdis.com are in English.

Related products

Trikdis GET Ethernet + 4G smart communicator

Trikdis CRP2 serial port connecting cable for Paradox alarm panels

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/get-manual