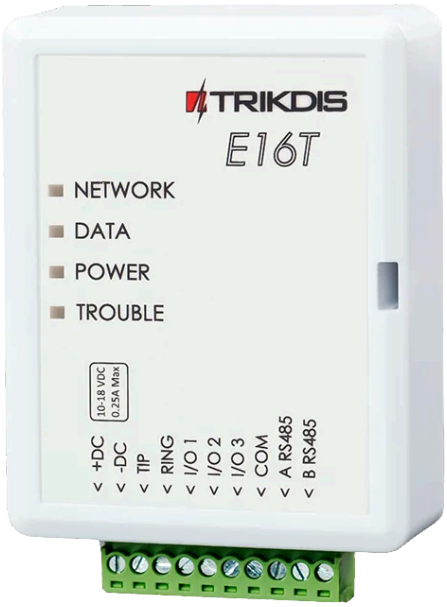
mobilamb
TRIKDIS Official Distributor

E16T communicator – installer and user manual

Installer and user manual for the Trikdis E16T Ethernet communicator: connection to the alarm control panel, network setup in TrikdisConfig, reporting to the monitoring station, Protegus 2 app, testing and troubleshooting.



Edition: 2026-11-17
Always up-to-date web version: https://mobilamb.eu/e16t-manual

Contents

1. Overview

1.1 What it is for and how it works
1.2 Versions
1.3 Main features
1.4 Parts of the communicator
1.5 Terminals
1.6 LED indications
1.7 Technical data

2. Quick setup with TrikdisConfig

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 Location and network
3.3 Connection to the alarm control panel
3.3.1 If needed: line supervision
3.4 Wiring a keyswitch zone
3.5 Wiring the inputs
3.6 Connecting the Ethernet cable
3.7 Wiring an output with a relay
3.8 Connecting an iO-8 expander
3.9 Switching on and first check
A TRIKDIS átjelző elindítása

4. Programming the alarm control panel

4.1 Programming the Honeywell Vista dialer
4.2 Panels of other makes

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. TrikdisConfig – the settings in detail

6.1 The status bar
6.2 System settings
6.3 CMS reporting
6.4 User reporting
6.5 Ethernet settings
6.6 IN/OUT
6.7 RS485 modules
6.8 Event summary
6.9 Restoring the factory settings

7. Remote programming

8. Testing the communicator

9. Firmware update

10. Troubleshooting and frequently asked questions

11. Safety instructions

See also

1. Overview

The E16T is Trikdis's **universal Ethernet communicator**: it connects to the telephone line output (TIP/RING) of the alarm control panel and behaves like a telephone exchange. The panel "dials", sends the Contact ID message with DTMF tones, and the E16T picks up the line, decodes the message and forwards it over the local network and the wired internet connection to the monitoring receiver, as well as to the Protegus cloud and the user's app. This way **a panel of any make** that has a Contact ID dialer can be used with it – the panel does not need to be replaced, only its dialer has to be set up. The E16T works over wired internet, without a SIM card or subscription.

1.1 What it is for and how it works

- **It reports to the monitoring station.** It sends the events over an IP connection to a Trikdis software or hardware receiver (TRK protocol; these receivers work with any monitoring software) or to any universal receiver (SIA DC-09 2007/2012, SUR-GARD TL150). By default it checks the connection every 30 seconds (it sends a heartbeat, a PING, to the receiver; the interval can be changed), and if there is a fault it switches to the backup channel.
- **It notifies the user.** The Protegus 2 app shows what happened with push notifications (with a separate sound alert) and an event list; from the app the user can arm and disarm, and switch the connected devices (lighting, gate, ventilation, heating, irrigation, etc.). The app works with the alarm control panel of any make that the E16T is connected to.
- **It works with the monitoring station and the user together or separately:** it can be used with Protegus 2 only (without a monitoring station), with a monitoring station only, or with both. If both are set up, the event is sent to the monitoring station first, then to the user.
- **It has its own inputs and outputs.** Three dual-function I/O terminals can be used as inputs (detector, tamper) or as controllable outputs (keyswitch zone, relay). With an iO-8 expander connected to the RS485 bus, 8 more I/Os can be added to the system.
- **No subscription.** The E16T uses the site's existing internet connection: no SIM card, mobile subscription or antenna is needed, and the mobile signal strength does not matter either.

The figure below shows how the system is built up: the telephone line output of the alarm control panel connects to the E16T, the E16T reaches the internet through the local router, and from there the monitoring receiver and the Protegus cloud, while the user sees the system in the Protegus 2 app.

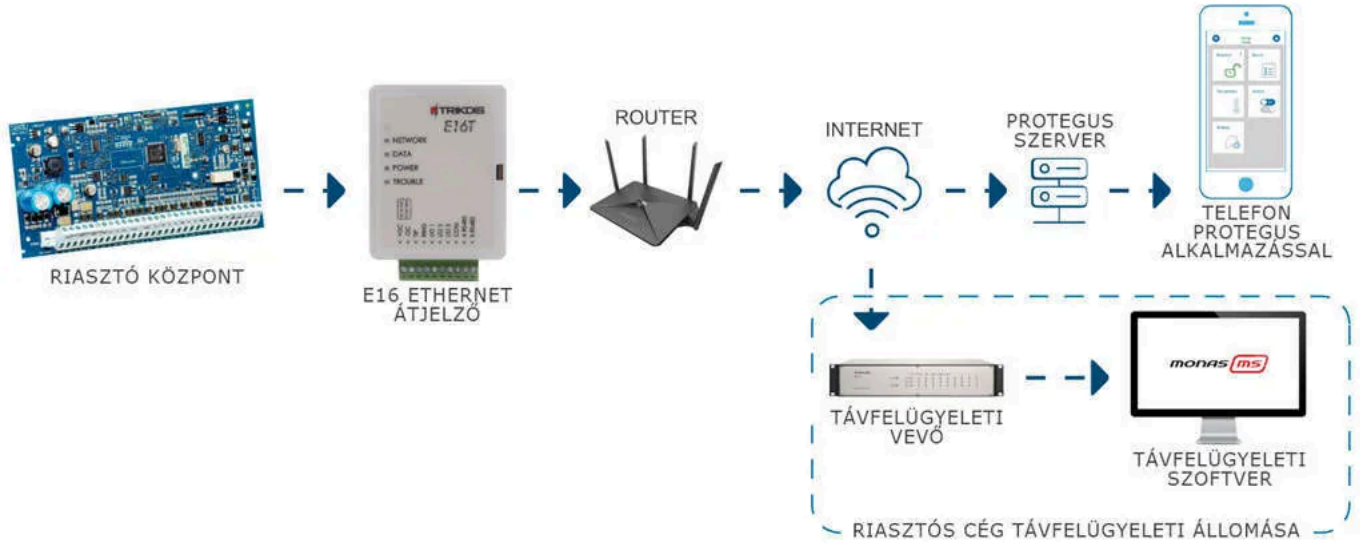


Figure 1. The place of the E16T in the system: alarm control panel → E16T → router → internet → monitoring receiver and Protegus cloud → Protegus 2 app.

1.2 Versions

This manual was written for the **current, v2 hardware version** of the E16T (TrikdisConfig shows it as **E16T_2000**), but it **can also be used for the earlier E16T**: wiring, setup and operation are largely the same. The differences are summarised in the table below; where the text gives the v2 value, take these into account for the earlier version.

	Earlier E16T	**E16T v2 (current)**
Inputs/outputs	2 inputs of selectable type (T-1/IN1, R-1/IN2 – NC, NO, EOL; they can also be used to supervise the telephone line) + 1 open-collector output (OUT, max. 0.15 A, up to 30 V; can be controlled from the Protegus app)	3 dual-function I/O terminals (I/O 1, I/O 2, I/O 3), each usable as an input (types NC, NO, EOL, DEOL) or as an open-collector output (max. 0.15 A)
Current consumption	up to 0.5 A	100 mA nominal, up to 250 mA while sending
LEDs	NETWORK, DATA, POWER, TROUBLE, LINE (LINE is steady green while the panel has "picked up the receiver", i.e. is dialing; the different indications of the other LEDs are listed in the note at the end of section 1.6)	NETWORK, DATA, POWER, TROUBLE
Event buffer	100 messages	60 messages
Dimensions	88 × 62 × 25 mm	88 × 65 × 26 mm

You will find the hardware version in the TrikdisConfig status bar (**HW**) and on the label on the back of the device.

1.3 Main features

Connection to the alarm control panel

- Standard connection to the panel's telephone line output: DC+, DC−, TIP and RING. If needed, it can also be connected with line supervision (with the T-1 and R-1 wires): then the connection between the panel and the communicator is **supervised**, the communicator signals a broken wire.

- The panel sends the events in Contact ID format with DTMF dialing; the E16T forwards the full event information (code, partition, zone or user).

Communication with the monitoring station

- IP connection to Trikdis receivers (IPcom software receiver, RL14, RM14) and universal receivers (SIA DC-09, TL150).
- Primary, backup and parallel channel: it can send to two receivers at the same time, with a separate backup channel for each.
- Encrypted, password-protected communication; event buffer of 60 messages.

User functions

- Protegus 2 mobile and web app: notifications, event list, arming and disarming, switching outputs.
- Multi-level user rights in the app (administrator, installer, user).

Installation and setup

- The settings can be saved to a file and loaded into another communicator.
- Two access levels: administrator and installer – for setting up the device, for the administrator of the monitoring station and for the installer.
- Can be set up and updated remotely with the TrikdisConfig software.

1.4 Parts of the communicator

The E16T has its printed circuit board in a white plastic case; the front cover is removable and the terminal block can be pulled off. The network (RJ45) connector is on the upper edge of the printed circuit board and can be reached through the opening in the case.

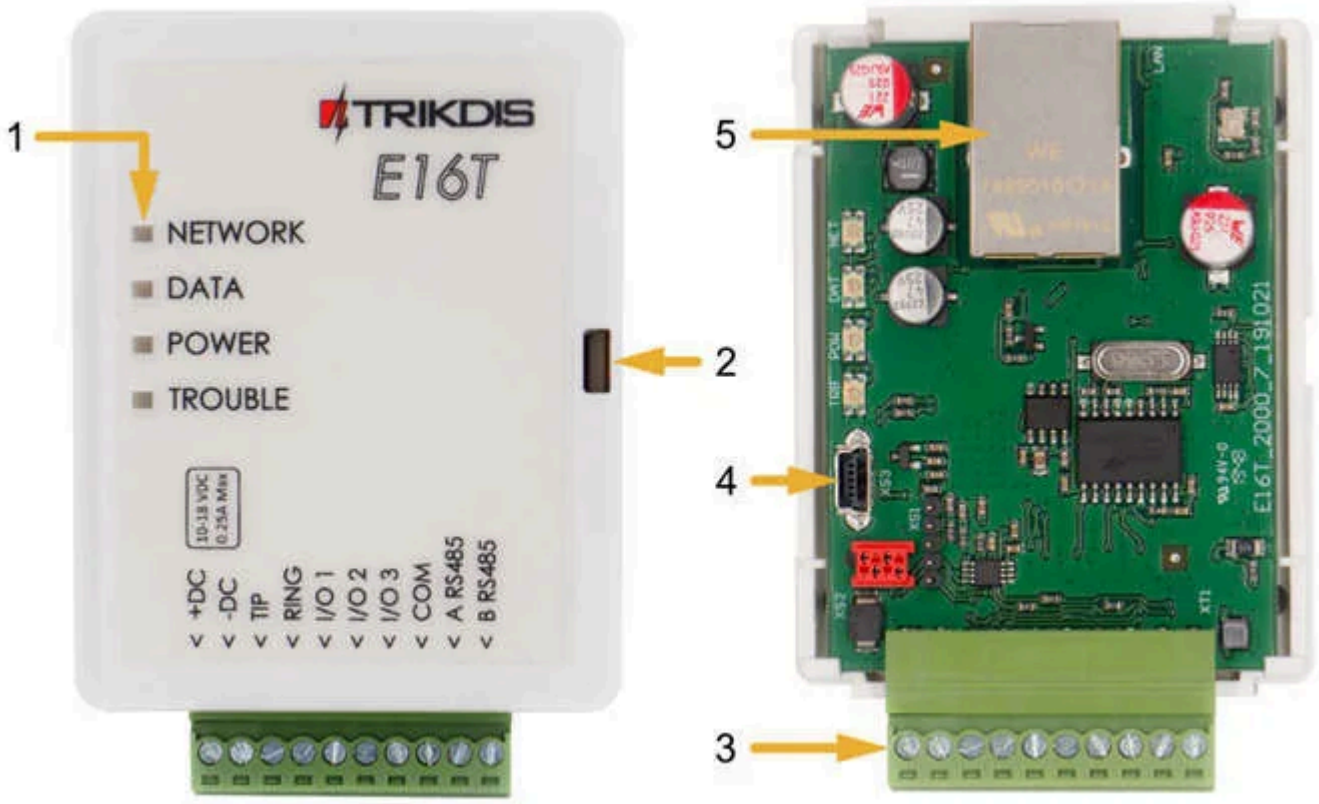


Figure 2. Parts of the E16T, from the front and with the case open.

- 1 LED indicators (NETWORK, DATA, POWER, TROUBLE)
- 2 Slot to help remove the front cover (on the upper edge of the cover)
- 3 Detachable terminal block
- 4 USB Mini-B socket for programming
- 5 Ethernet connector (RJ45)

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
+DC	Power, +10–18 V DC
–DC	Power, negative
TIP	TIP terminal of the alarm control panel
RING	RING terminal of the alarm control panel
I/O 1 (T-1)	Input/output 1, or the T-1 point of the telephone line supervision
I/O 2 (R-1)	Input/output 2, or the R-1 point of the telephone line supervision
I/O 3	Input/output 3
COM	Common (negative) point for the inputs and outputs
A 485	RS485 bus wire A (iO-8 and other iO-series expanders)
B 485	RS485 bus wire B

The terminal labels are also printed on the front cover, so you do not need to remove the cover for wiring.

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 the network connection, DATA the messages waiting to be sent and TROUBLE the fault.

NETWORK – network connection

Indication	Meaning
off	No network connection (no cable, the port is not live, or it did not get an IP address)
steady green	Connected to the local network – the connection is live up to the router. Whether the internet can also be reached is shown by the DATA LED (see below).

DATA – data traffic

Indication	Meaning
off	No messages waiting to be sent
steady green	There are messages waiting to be sent in the buffer
flashing green	Data is being sent or received (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 – supply voltage

Indication	Meaning
off	No power, or the power is disconnected
steady green	Switched on, the supply voltage is correct
steady yellow	Incorrect supply voltage (11.5 V or less)
steady green, flashing yellow	Ready for programming (USB cable plugged in)
steady yellow (during programming)	No connection to the computer

TROUBLE – fault

Indication	Meaning
off	No fault
1 red flash	No physical network connection (PHY link): the cable, the connector or the router / switch port

Indication	Meaning
2 red flashes	DHCP error: the device did not get an IP address
3 red flashes	DNS error: name resolution is not working
6 red flashes	No connection to the monitoring receiver
7 red flashes	The connection to the alarm control panel has been lost
flashing red (during programming)	Memory error
steady red (during programming)	Corrupted firmware

Earlier E16T

Some of the LEDs of the earlier E16T show different things: **DATA** is steady yellow if there is an event waiting to be sent in the buffer, and flashes green while the alarm control panel is passing a message to the communicator; **POWER** flashes green if the power is on and the voltage is correct, and flashes yellow if the supply voltage is not sufficient (11.5 V or less); a steady red **TROUBLE** light indicates a network (LAN) connection fault, off means no fault; **LINE** is steady green while the panel has "picked up the receiver" (section 1.2).

1.7 Technical data

Parameter	Value
Connection to the alarm control panel	wired telephone line (TIP/RING), Contact ID, DTMF
Inputs/outputs	3 dual-function I/Os (I/O 1, I/O 2, I/O 3): as inputs NC, NO, NC/EOL, NO/EOL, NC/DEOL, NO/DEOL (2.2 kΩ end-of-line resistor); as outputs open collector (OC), max. 0.15 A / 30 V DC
Expansion	on the RS485 bus: iO-8 expander (+8 I/Os) and other iO-series expanders, up to 4 modules
Network connection	Ethernet, IEEE 802.3, 10Base-T, RJ45 socket
Network settings	DHCP (default) or fixed IP address
Supply voltage	10–18 V DC
Current consumption	100 mA nominal; up to 250 mA while sending
Transmission protocols	TRK, DC-09_2007, DC-09_2012, TL150
Event buffer	60 messages
Programming	TrikdisConfig (Windows) over a USB Mini-B cable or remotely
Operating environment	−10 … +50 °C, max. 80 % relative humidity (at +20 °C)
Dimensions	88 × 65 × 26 mm
Weight	80 g

2. Quick setup with TrikdisConfig

All settings of the E16T are made with the **TrikdisConfig** program, which runs on Windows – over a USB cable or remotely. In this chapter we describe the shortest route: you set up the device on the desk, before wiring, and on site you then only need to wire it. The settings are explained in detail in chapter 6.

2.1 Preparation

What you will need

USB Mini-B cable (for the setup) · a cable with at least 4 cores to the panel · 2.5 mm flat-blade screwdriver · Ethernet cable (CAT-5 or better, up to 100 m) to the router or switch · a free network port · if there is no DHCP on the network: the fixed IP address, mask, gateway and DNS from the network administrator · the installer manual of the alarm control panel. Anything missing can be ordered separately from the local distributor.

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 front cover of the E16T and connect it to the computer. Insert a flat-blade screwdriver into the slot on the top edge of the cover and, levering downwards, gently snap off the front cover, then plug in the USB Mini-B cable. The USB provides enough power for programming; no separate power supply is needed.

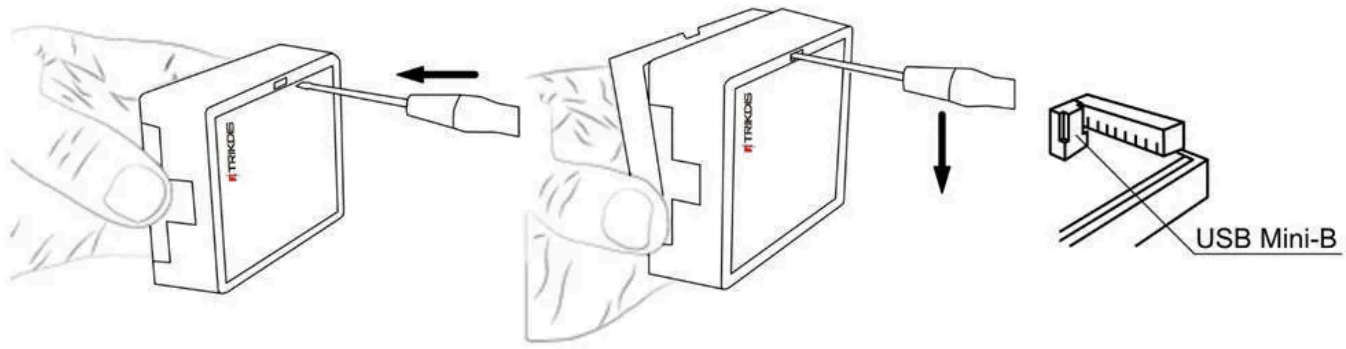


Figure 3. Snapping off the front cover and connecting to the computer with a USB Mini-B cable.

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

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

The next two sections describe what needs to be set so that the alarm control panel can be controlled from the Protegus 2 app (2.2), and so that the communicator sends events to the monitoring station (2.3).

2.2 Connection to the Protegus 2 app

If the user wants to see and control the system from the Protegus 2 app, set the following on the **User reporting** page, on the **PROTEGUS Cloud** tab.



Figure 4. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- 1 **Enable connection** – tick it: enables the connection to the Protegus cloud.
- 2 **Protegus Cloud access code** – change the default password `123456`. This is what has to be entered in the app when the system is created; **it cannot be changed after the system has been created.**

Then check the type of the alarm control panel interface on the **System settings** page.

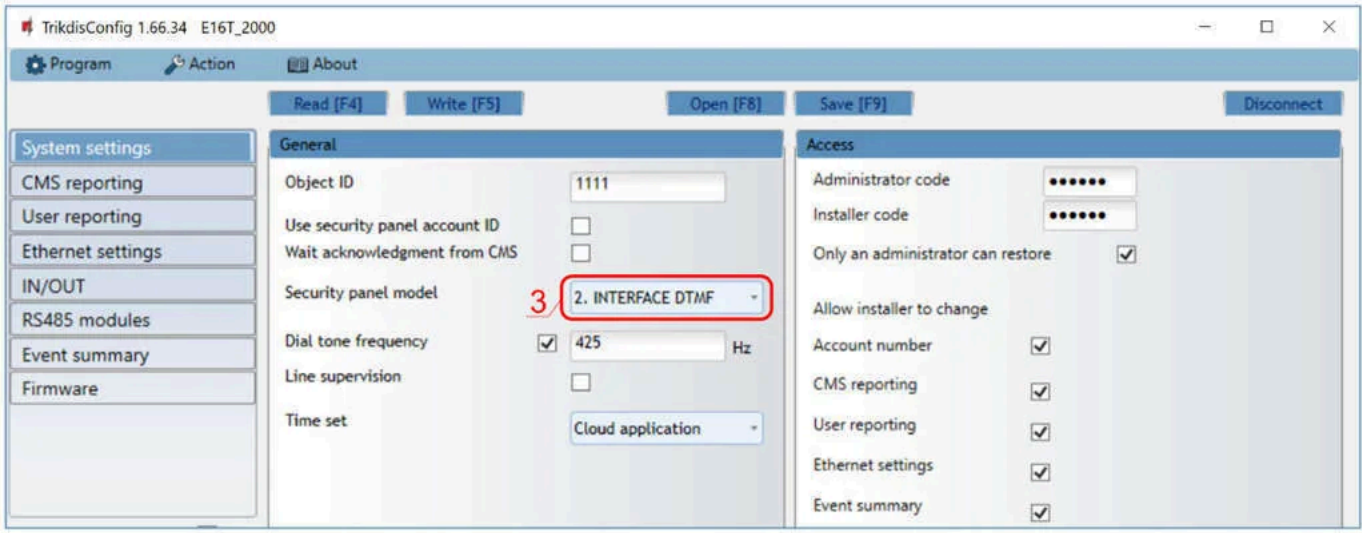


Figure 5. TrikdisConfig – System settings page, General group.

- 3 **Security panel model** – leave it at **2. INTERFACE DTMF** (the telephone line connection with DTMF dialing).

For the network settings, **Use DHCP** is ticked by default on the **Ethernet settings** page: the device gets its IP address from the router automatically, and in most places nothing more needs to be done. If there is no DHCP on the network, or a fixed address has to be used, enter the manual settings here (section 6.5).

If you use the device with Protegus 2 only, without a monitoring station, the setup is now complete: press the **Write [F5]** button, wait for the confirmation and unplug the USB cable.

Do not forget to enable and set up the telephone line dialer of the alarm control panel, otherwise the panel will not send any events. Setting up the panel is described in chapter 4.

2.3 Connection to the monitoring station

If the device also reports to a monitoring receiver, first enter the object ID on the **System settings** page.

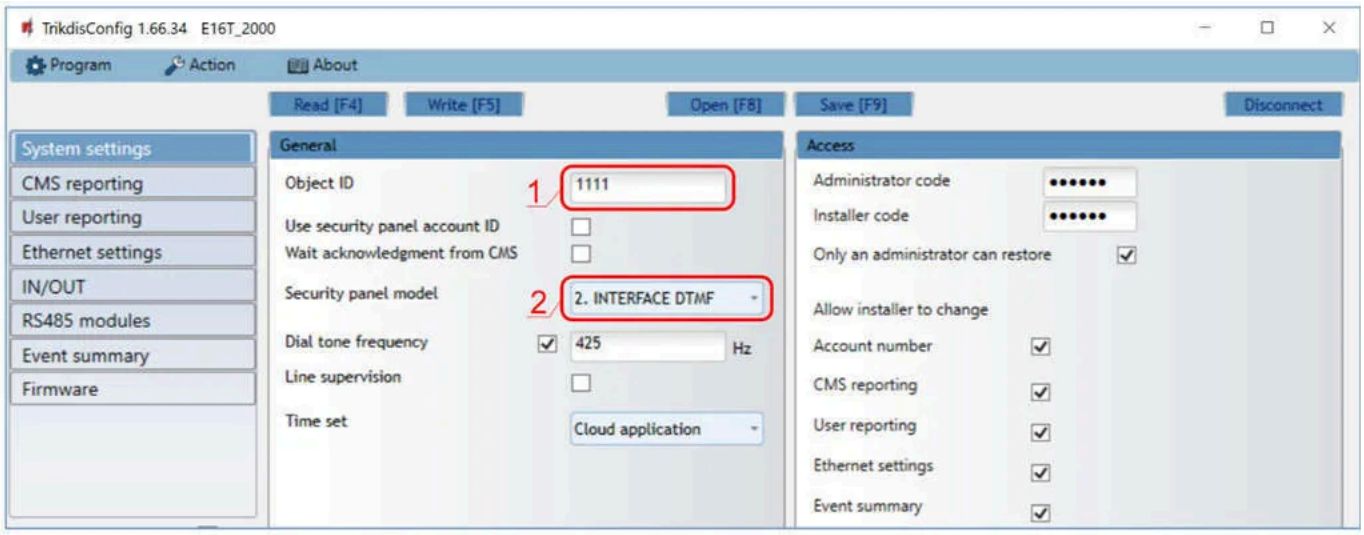


Figure 6. TrikdisConfig – System settings page, General group.

- 1 **Object ID** – the object ID received from the monitoring station (4 hexadecimal characters, 0–9, A–F). `FFFE` and `FFFF` cannot be used.
- 2 **Security panel model** – leave it at **2. INTERFACE DTMF**.

Then, on the **CMS reporting** page, set the receiver details in the **Primary channel** section.

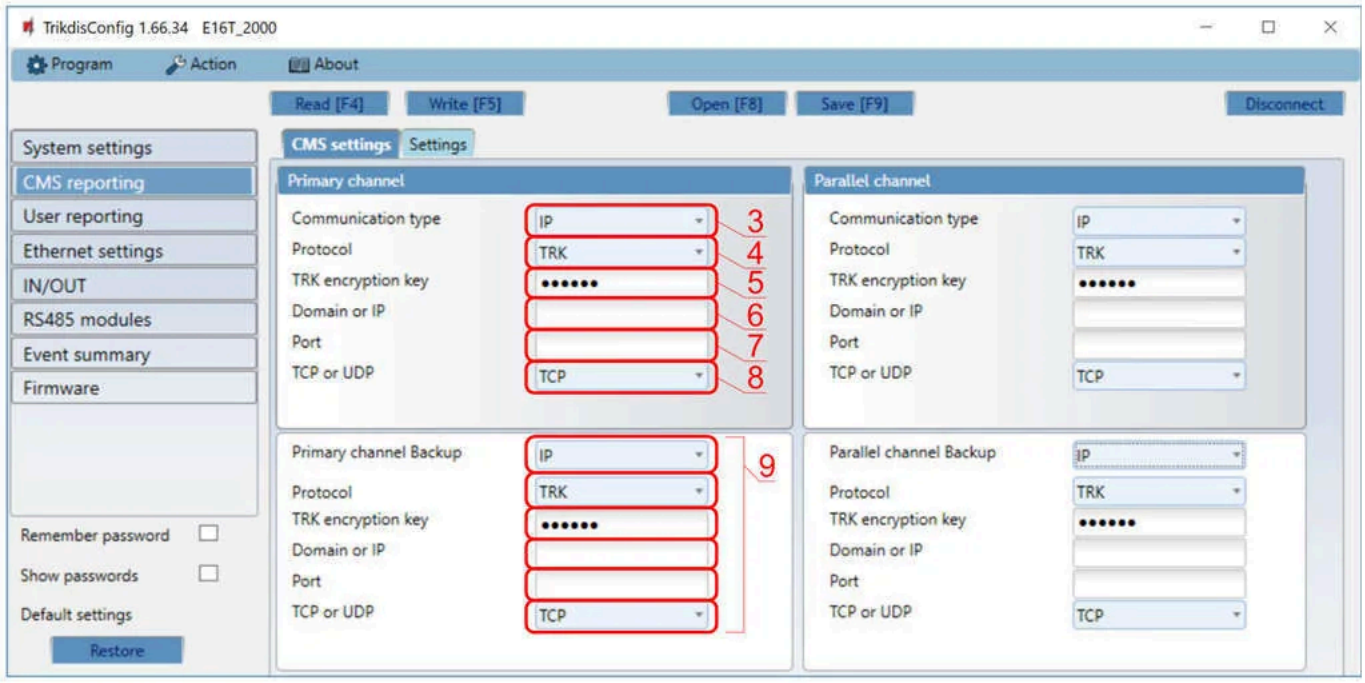


Figure 7. TrikdisConfig – CMS reporting, CMS settings tab.

- 3 **Communication type** – **IP** (this is the only option on the E16T).
- 4 **Protocol** – **TRK** for a Trikdis receiver, **DC-09_2007** or **DC-09_2012** for a universal receiver, **TL150** for a SUR-GARD receiver.
- 5 **TRK encryption key** – the 6-digit encryption key set in the receiver.
- 6 **Domain or IP** – the domain name or IP address of the receiver.
- 7 **Port** – the port number of the receiver.
- 8 **TCP or UDP** – the transmission protocol; it follows the receiver's setting.
- 9 **Primary channel Backup** – backup channel in case the primary one fails; fill it in the same way, it is recommended.

With the **DC-09** protocol, also enter the DC-09 object, line and receiver numbers on the **Settings** tab (section 6.3); with DC-09_2012, encryption can also be switched on with the DC-09 key set in the receiver (note in section 6.3). To check the connection, you set the heartbeat (PING) interval on the same **Settings** tab (**IP ping period**, default 30 s). If you entered the receiver with a domain name, the DNS setting on the **Ethernet settings** page is also needed for name resolution (by default it contains Google's public DNS). On the earlier E16T the fields have different names (**Enable**, **Remote Host**, **Remote Port**, **PING Time**, **Encryption key**); the note in section 6.3 gives the mapping.

If the user also uses the Protegus 2 app, make the settings of section 2.2 as well (**User reporting** → **PROTEGUS Cloud**). At the end of the setup, press the **Write [F5]** button, wait for the confirmation and unplug the USB cable. The device is now ready for wiring.

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. Take the printed circuit board out of the back cover: open the latch in the corner.

3. Fix the back cover with screws in the chosen place.
4. Put the printed circuit board back into the back cover and plug the terminal block back in.
5. Plug the Ethernet cable into the RJ45 socket (section 3.6).
6. Put the front cover back on.

3.2 Location and network

- Put the communicator in a **dry, indoor** place, preferably near the alarm control panel's enclosure, so that the wiring is short. A metal enclosure does not interfere with it: the E16T has no antenna.
- The Ethernet cable (CAT-5 or better) to the router or switch can be **up to 100 m** long.
- Keep the communicator and the cables away from the panel's transformer and from mains wiring.

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

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.

Power failure

The E16T is powered by the alarm control panel, so during a power failure it keeps working from the panel's battery – the router and the modem, however, typically do not, and without them there is no internet. If this is not acceptable for the system, run the network devices from an uninterruptible power supply as well, or choose a cellular communicator (G16T).

3.3 Connection to the alarm control panel

The E16T has to be connected to the panel's telephone line output (TIP/RING), and it gets its power from the panel's 12 V auxiliary power output (AUX).

Recommended, standard wiring: DC+, DC−, TIP and RING. In this case the communicator does not detect if the wire is broken.

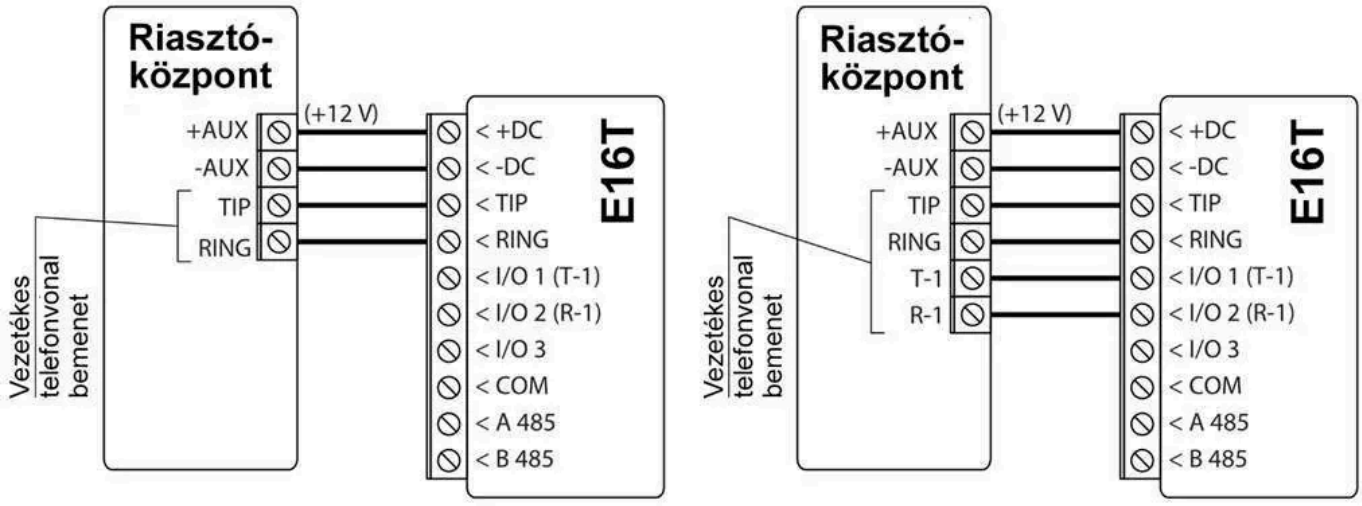


Figure 8. Connection to the panel's telephone line output: on the left the standard wiring, on the right the wiring with line supervision.

The E16T draws up to 250 mA while sending. Check that the panel's AUX output can supply this together with the other devices connected to it. As the power comes from the panel, during a power failure the panel's battery also powers the communicator.

3.3.1 If needed: line supervision

Only needed if line supervision is required: the communicator then signals if the connection between it and the alarm control panel is broken.

1. In addition to the standard wiring, connect these two wires as well: the panel's **T-1** terminal to the communicator's **I/O 1 (T-1)** terminal, and the panel's **R-1** terminal to the communicator's **I/O 2 (R-1)** terminal.
2. On the **System settings** page of TrikdisConfig, switch on the **Line supervision** option.
3. Check the settings required on the alarm control panel side in the panel's installation manual.

In this case I/O 1 and I/O 2 cannot be used for anything else.

3.4 Wiring a keyswitch zone

If you want to arm and disarm the panel remotely, from the Protegus 2 app, set one of the communicator's I/O terminals as an **output** and connect it to a **keyswitch zone** of the panel. When activated, the output pulls the zone to COM (negative); connect the zone's end-of-line resistor according to the panel's zone type. As the E16T has three I/O terminals, even three partitions can be handled with separate outputs.

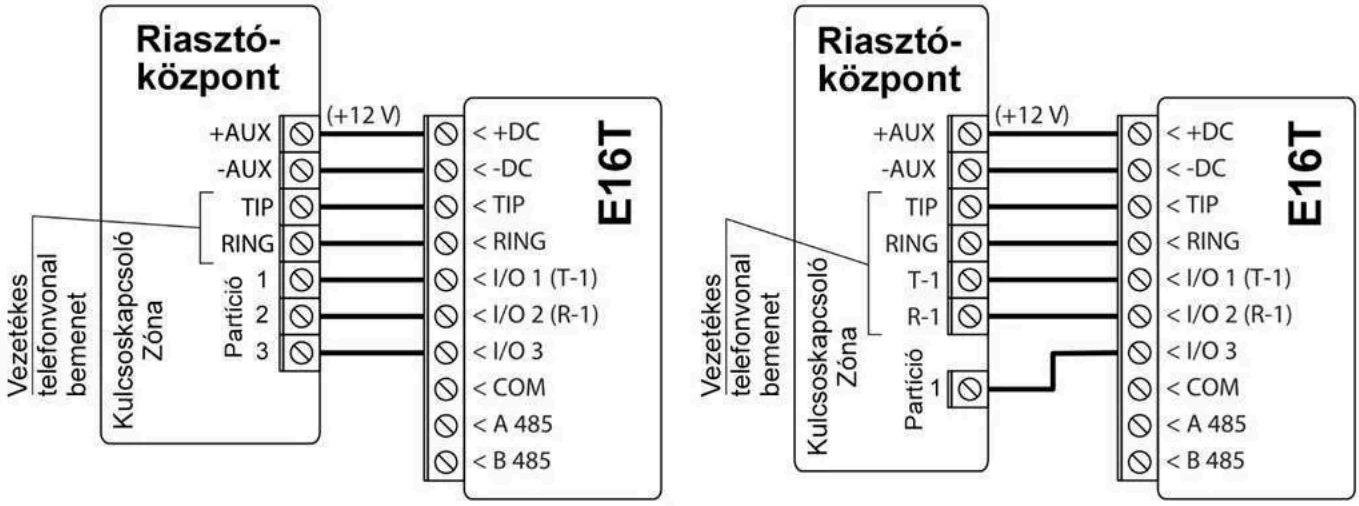


Figure 9. Arming and disarming with a keyswitch zone: on the left the standard wiring, on the right the wiring with line supervision (in this case I/O 3 remains for the keyswitch).

The keyswitch zone can be pulse or latching (two-state) – the same mode has to be set in the Protegus 2 app (section 5.2). A separate article covers the details and pitfalls of keyswitch arming: Remote arming with a keyswitch from the Protegus 2 app.

Earlier E16T

On the earlier E16T (2 inputs + OUT), the type and mode of the output have to be set in the **System settings** → **Output** group of TrikdisConfig: for keyswitch arming, **OUT type** should be **Remote Control**, and **OUT mode** should be **Pulse** (with a pulse length) or **Level** – according to the panel's zone type.

3.5 Wiring the inputs

As inputs, the communicator's I/O terminals can also take additional detectors (e.g. tamper switch, panic button, temperature switch), independently of the alarm control panel. The input has to be connected between the selected I/O and the COM terminal.

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: NC, NO, EOL and DEOL types with a 2.2 kΩ end-of-line resistor, with a tamper loop for the DEOL types.

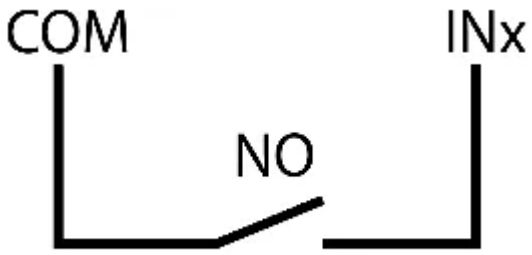


Figure 10. NO – normally open circuit: closed – alarm, open – normal state.

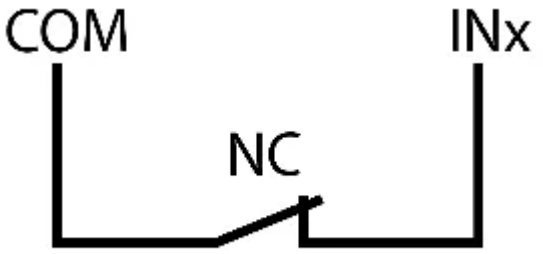


Figure 11. NC – normally closed circuit: open – alarm, closed – normal state.

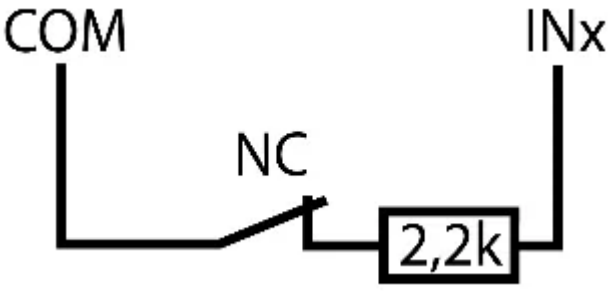


Figure 12. NC/EOL – normally closed circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

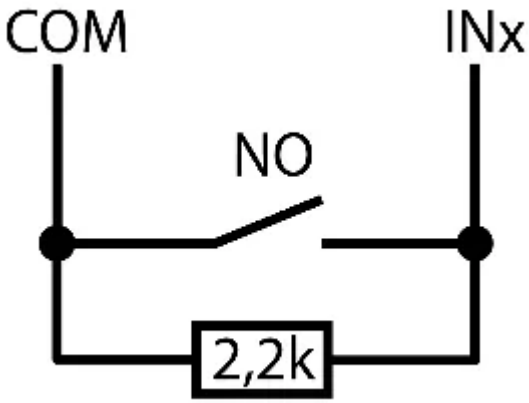


Figure 13. NO/EOL – normally open circuit with a 2.2 kΩ end-of-line resistor: short circuit or open circuit – alarm, 2.2 kΩ – normal state.

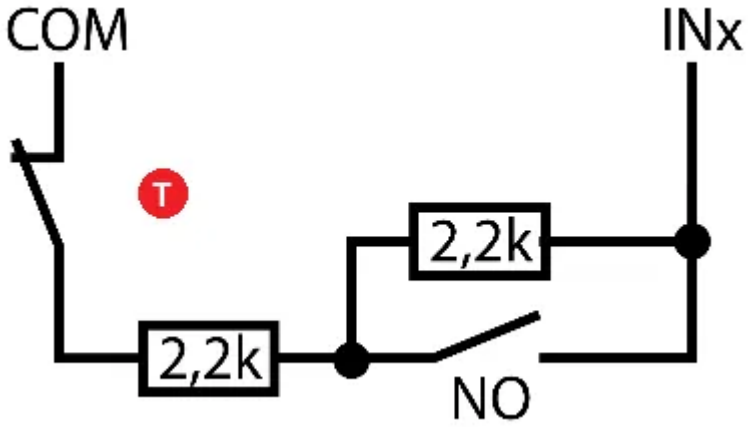


Figure 14. NO/DEOL – normally open circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – alarm, 3.3–5.5 kΩ – normal state.

- T tamper contact (“Tamper”), signals that the detector's housing has been opened

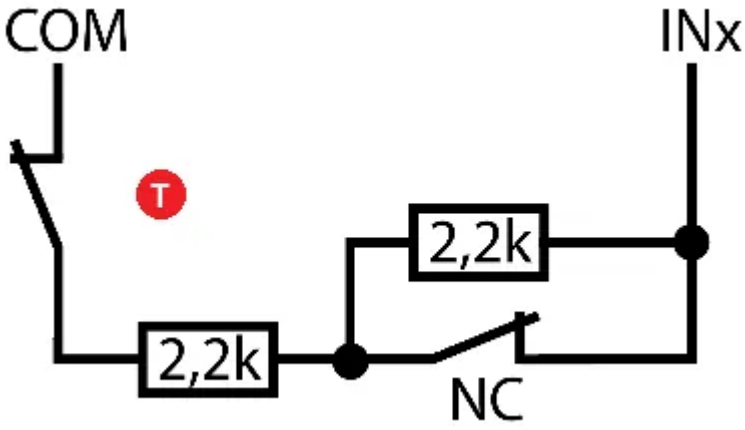


Figure 15. NC/DEOL – normally closed circuit with a 2.2 kΩ end-of-line resistor and tamper detection: short circuit or open circuit – tamper, 2.2 kΩ – normal state, 3.3–5.5 kΩ – alarm.

- T tamper contact (“Tamper”), signals that the detector's housing has been opened

Earlier E16T

The two inputs (IN1, IN2) of the earlier E16T (2 inputs + OUT) take NO, NC or EOL type circuits; the default is NO. There, the input type is not set on the IN/OUT page but on the **Event summary** page of TrikdisConfig (note in section 6.6). The wiring is the same: connect the input according to the selected type (NO, NC, EOL).

3.6 Connecting the Ethernet cable

Plug one end of the Ethernet cable into the RJ45 socket on the E16T's printed circuit board, and the other into a free port of the router or switch. A standard straight-through (patch) cable is needed; the cable enters through the upper opening of the case. After switching on, the green light of the **NETWORK** LED shows that the network connection has been established.

3.7 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 up to 0.15 A, up to 30 V DC. Switch a larger load or a mains-voltage device **through a relay**: one end of the relay coil goes to +DC, the other to the I/O terminal. An indicator LED can also be connected directly to the output: from +DC through a 2.2 kΩ series resistor to the LED, and the other leg of the LED to the I/O terminal (on the earlier E16T, to the OUT terminal).

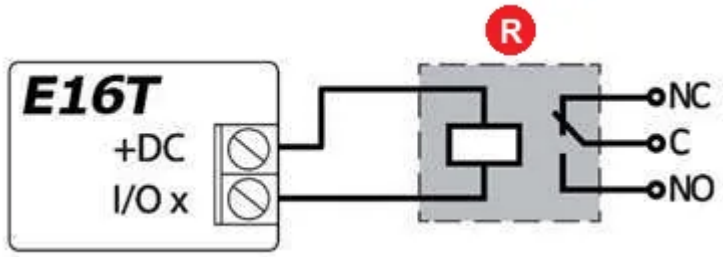


Figure 16. Connecting a relay to the communicator's output: the coil goes between +DC and the I/O x terminal, the contacts (NC, C, NO) switch the load.

- R relay (“Relay”)

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

3.8 Connecting an iO-8 expander

If more inputs or outputs are needed, up to four **iO-8** expanders can be connected to the E16T's RS485 bus; each adds 8 more dual-function I/Os. Connect the A 485 and B 485 terminals to the A and B terminals of the module, and take the module's power from the panel's 12 V. The RS485 bus can be up to 100 m long – this is a theoretical maximum, see the note in section 3.2. The module has to be added on the **RS485 modules** page of TrikdisConfig (section 6.7). The other members of the iO series (iO, iO-WL, iO-LO, LO-MOD) can also be connected here; W485 and E485 modules do not go with the E16T, since the E16T itself is a wired internet device.

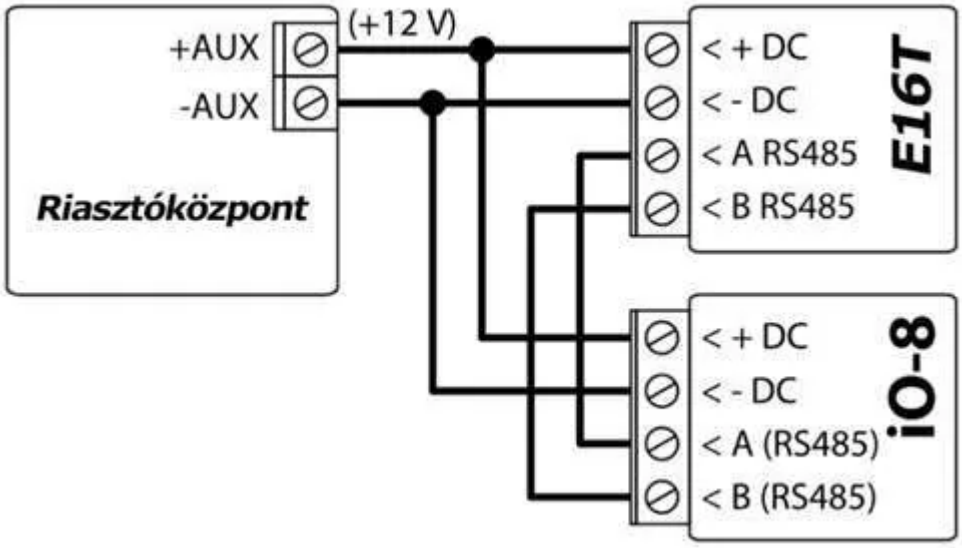


Figure 17. Connecting an iO-8 expander to the E16T's RS485 bus; power from the alarm control panel's AUX output.

3.9 Switching on 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 starts when the alarm control panel is switched on. On the front cover you should see:

- **POWER** steady green – the power supply is correct;
- **NETWORK** steady green – connected to the local network;
- **TROUBLE** off.

If TROUBLE is flashing, the number of flashes tells you the cause (section 1.6): 1 = no physical connection (cable, port), 2 = no IP address received (DHCP), 3 = DNS error, 6 = it cannot reach the receiver. If none of the LEDs is lit, check the power supply and the wiring.

4. Programming the alarm control panel

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.

4.1 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 Panels of other makes

In the installer manual of every panel, look for the same four settings: enabling the telephone line communicator, the receiver's telephone number, the dialing mode (DTMF) and the communication format (Contact ID). If the panel expects a dial tone before dialing, the E16T provides it; if the call still does not start, switch off dial tone detection in the panel ("dial without dial tone" or a similar option).

If the panel signals a fault at the end of the call although the event has arrived, check the **Wait acknowledgment from CMS** setting on the **System settings** page of TrikdisConfig: when it is on, the communicator only ends the call after the acknowledgement of the monitoring receiver (kiss-off). In a system without a monitoring station, with Protegus 2 only, leave it off (this is the default), because there is no receiver to acknowledge.

5. Remote control with the Protegus 2 app

With the Protegus 2 mobile and web app, the user can see the state of the system remotely, receives notifications about the events, can arm and disarm, and can switch the communicator's outputs.

5.1 Adding the device

Before adding the device, check that:

1. The E16T is connected to the network and can reach the internet: the **NETWORK** LED is steady green, and the **DATA** LED goes off after an event or a test report.
2. On the **User reporting** → **PROTEGUS Cloud** tab of TrikdisConfig (section 6.4), **Enable connection** is ticked – i.e. the Protegus cloud is enabled – and the **Protegus Cloud access code** is set (it cannot be changed after the system has been created).
3. The **POWER** LED is steady green.

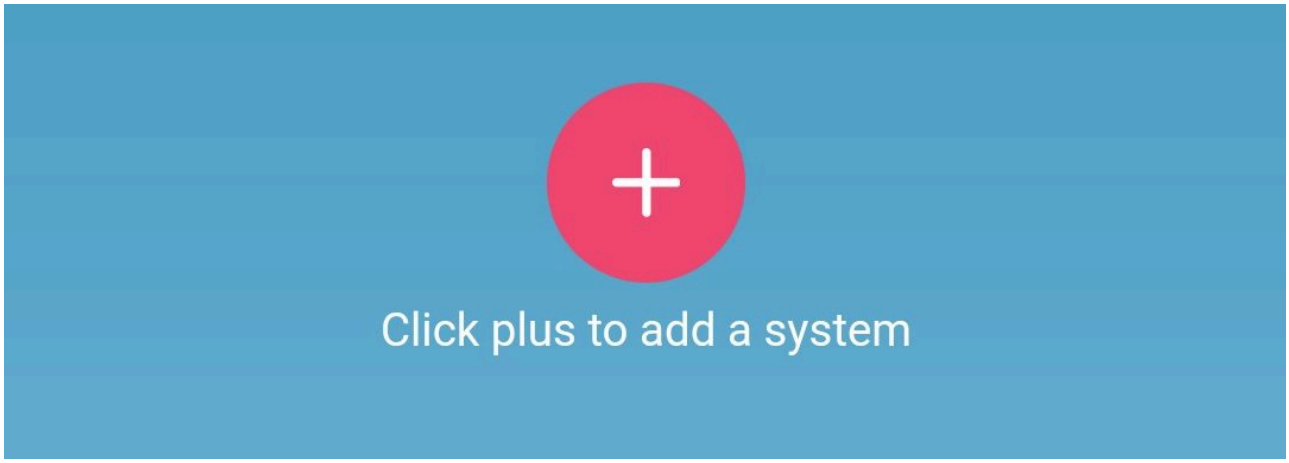
The DATA LED is the simplest internet check. The DATA LED is lit when there is a message waiting to be sent in the device's memory. A green NETWORK LED only tells you that the network connection has been established – for a mobile network device, that it has registered on the operator's network; for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



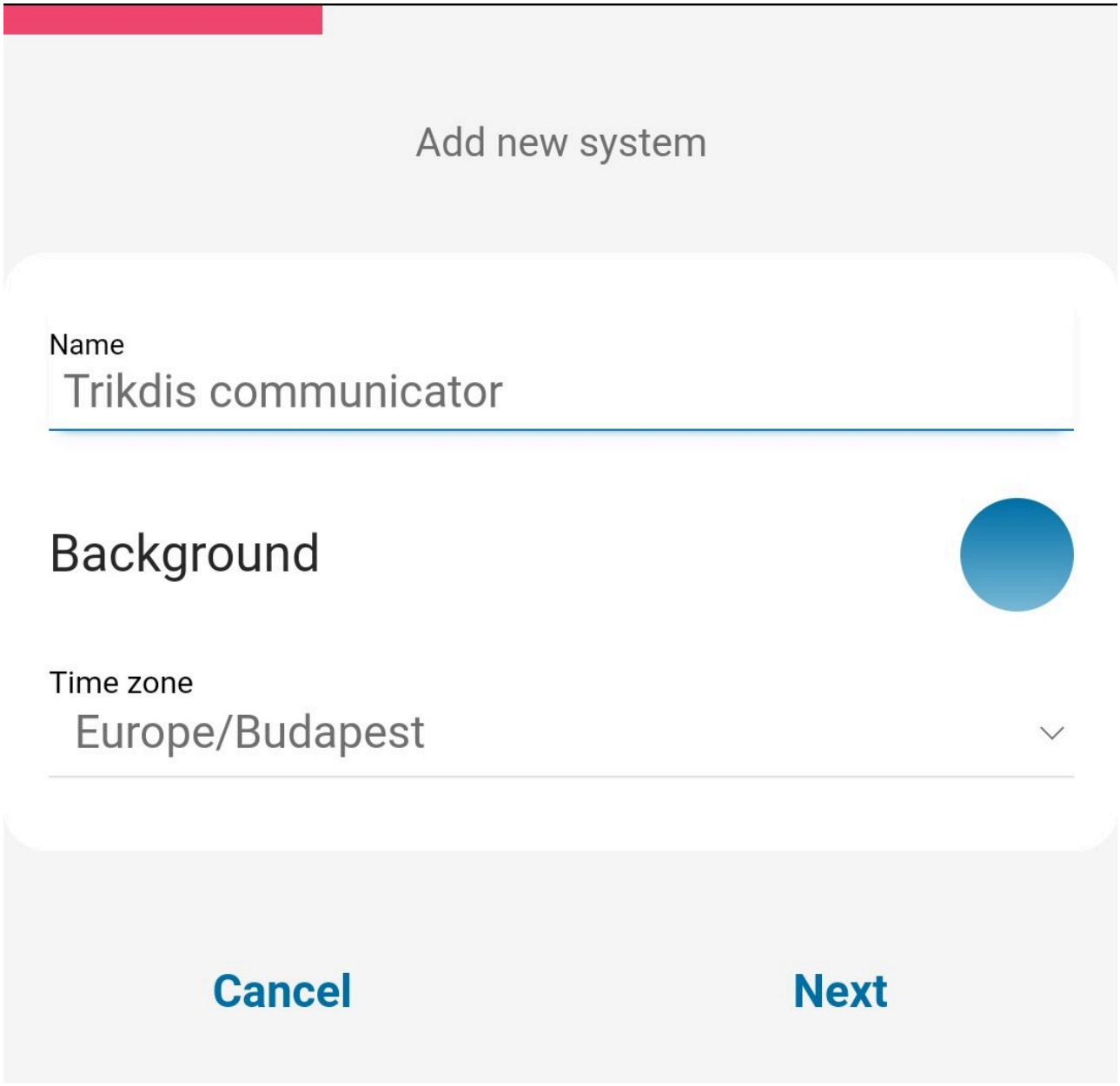
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



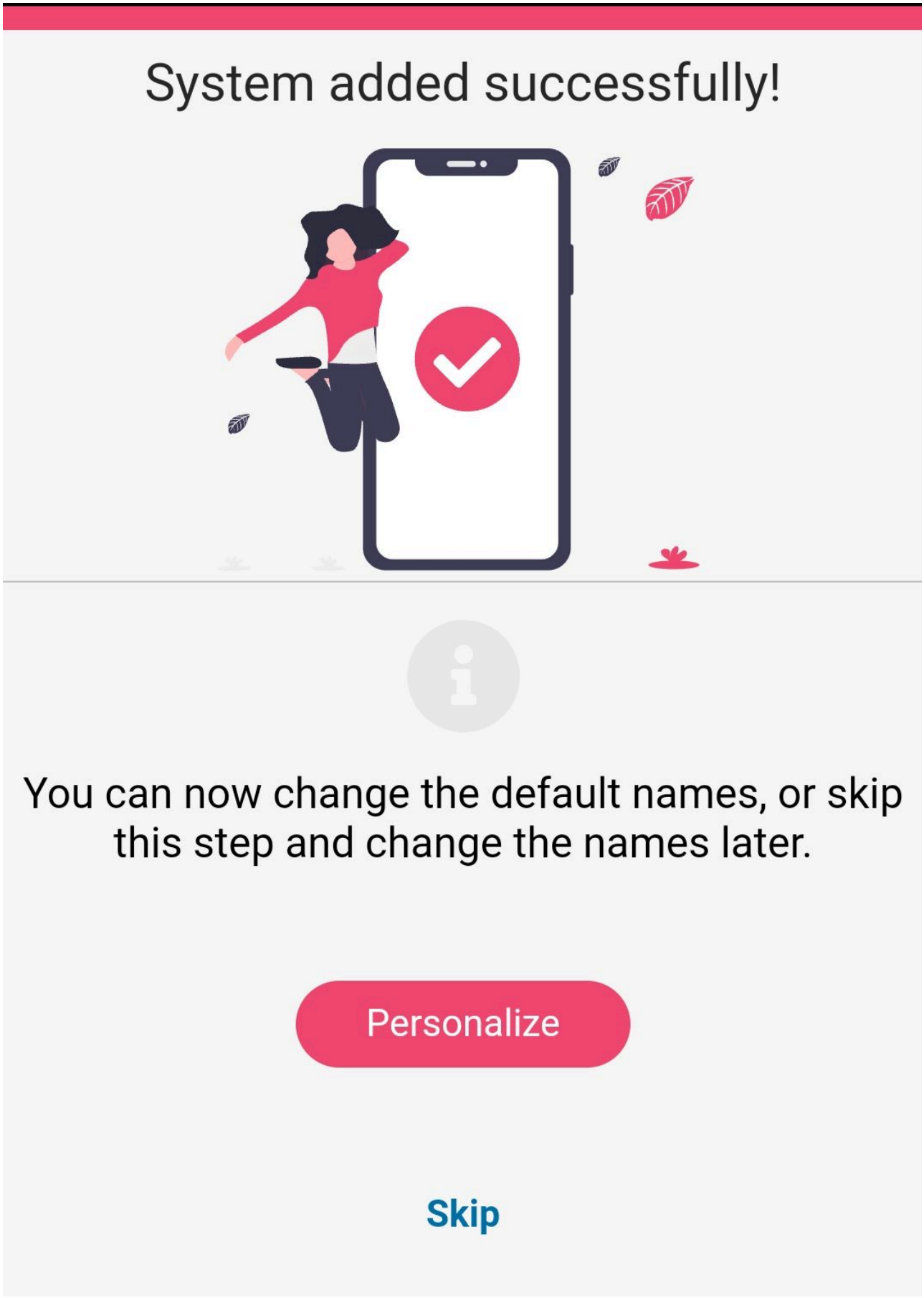
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



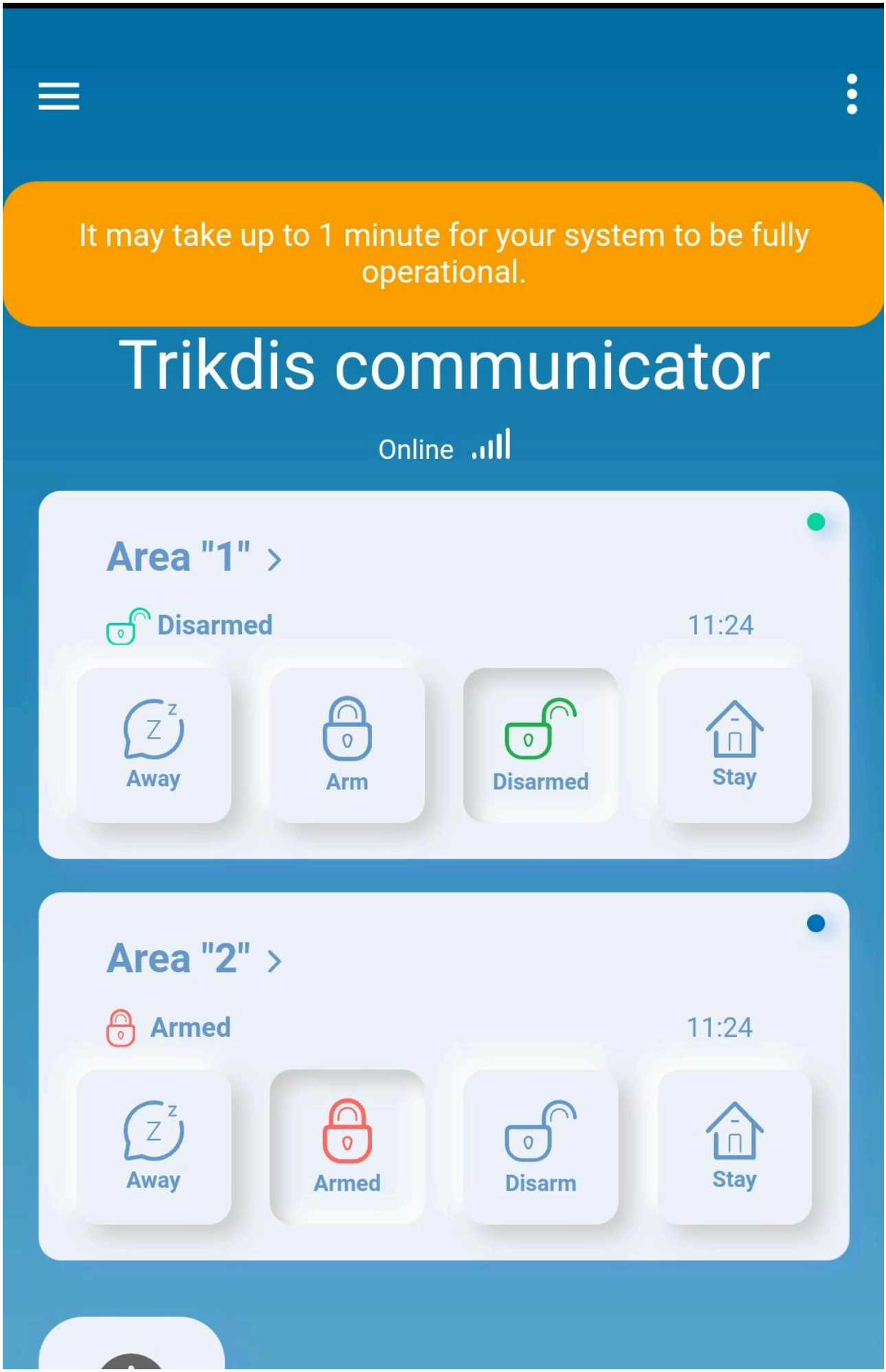
6. Add meg a rendszer nevét és válassz idozónát



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



The unique identifier of the device on the E16T is the **MAC address**: it can be read on the box and on the back of the device, and TrikdisConfig also shows it (**MAC / Unique ID**).

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.

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.

6. TrikdisConfig – the settings in detail

On the left side of the TrikdisConfig window you see the list of pages (System settings, CMS reporting, User reporting, Ethernet settings, IN/OUT, RS485 modules, Event summary, Firmware), at the top the button bar (**Read [F4]**, **Write [F5]**, **Open [F8]**, **Save [F9]**), and at the bottom the status bar. This chapter goes through the settings of the E16T page by page.

6.1 The status bar

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

Label	Meaning
IMEI / Unique ID, on an Ethernet device **MAC / Unique ID**	The device's unique identifier: the IMEI on a device with a SIM card, the MAC address on an Ethernet device. The same is printed on the box and on the back of the device.
Status	The current operating status.
Device	The device type (model designation). Check that the type of your own device is shown here.
SN	Serial number.
BL	The bootloader version.
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 18. The TrikdisConfig status bar with an E16T that has been read: on the left the factory reset button and the MAC / Unique ID, at the bottom the state, type, serial number, versions, connection mode and access level.

After **Read [F4]**, the program reads and shows the settings stored in the device; the **Device** field should show the device type (E16T; for v2, **E16T_2000**). Make the settings according to the page descriptions below.

6.2 System settings

The page consists of two groups: in the **General** group you set the basic operation of the device, in the **Access** group the access levels.

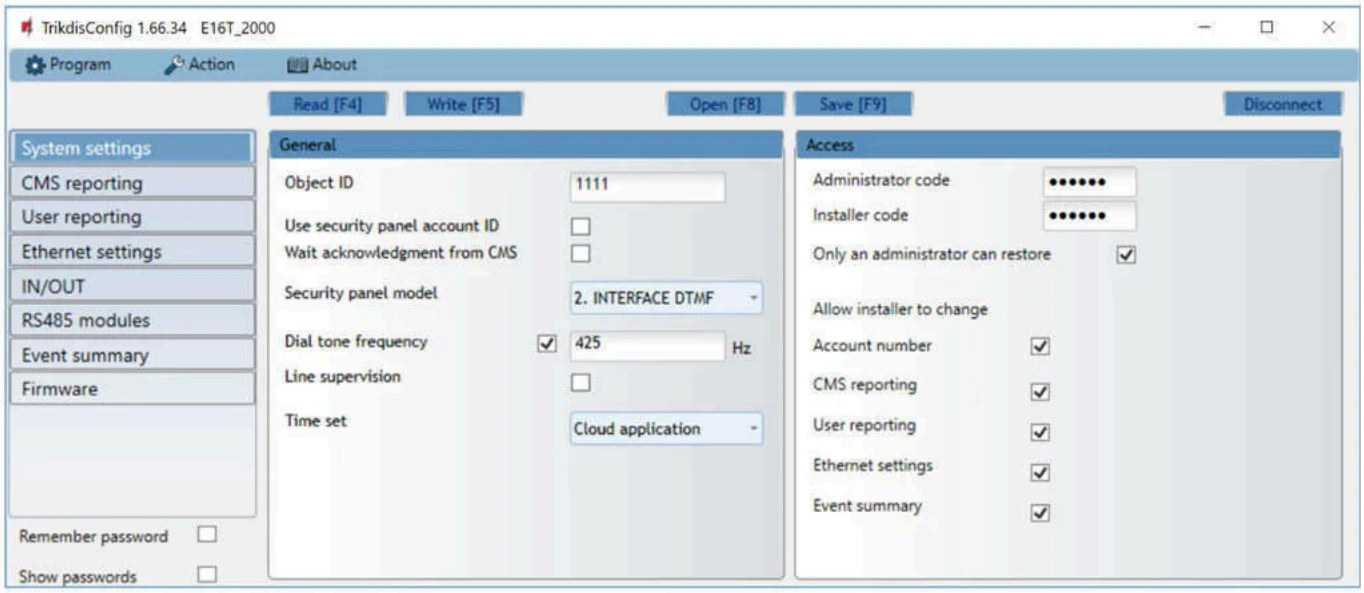


Figure 19. TrikdisConfig – System settings page: General and Access groups.

- **Object ID** – the object ID received from the monitoring station (4 hexadecimal characters: 0–9, A–F; `FFFE` and `FFFF` cannot be used). Mandatory if the device also reports to a monitoring station.
- **Use security panel account ID** – when ticked, the communicator does not use its own Object ID but the ID sent by the panel in the Contact ID message. Useful if several partitions report with separate IDs.
- **Wait acknowledgment from CMS** – when ticked, after each event the communicator waits for the receiver's acknowledgement and only then sends the closing (kiss-off) signal to the panel. If there is no acknowledgement, the panel sends the event again. In a system without a monitoring station, with Protegus 2 only, leave it off (default).
- **Security panel model** – the type of the telephone line interface; default **2. INTERFACE DTMF**. With this you switch the communicator's DTMF telephone line interface on or off.
- **Dial tone frequency** – the frequency of the dial tone that the E16T gives to the panel (default 425 Hz, the standard dial tone in most European countries).
- **Line supervision** – supervision of the wire between the panel and the communicator; the T-1 and R-1 wires must also be connected (section 3.3.1).
- **Time set** – the source of the device's clock (default **Cloud application**, the Protegus cloud).

Earlier E16T

On the earlier E16T, the System settings page also has further groups:

- **General** → **Test period** – the periodic test report is sent at the interval given here (on v2 this is on the **CMS reporting** → **Settings** tab).
- **Ethernet settings** group (on v2 a separate page, section 6.5): **Internal MAC** – the unique identifier of the device, the MAC address; **Use DHCP** – when ticked, the device registers on the network automatically; if automatic registration fails, fill in the **Internal IP address**, **Mask** (subnet mask), **Gateway** and **DNS** fields manually.
- **Output** group (on v2 the IN/OUT page, section 6.6): **OUT type** – the operation of the output, from the list: Disabled, LAN OK (the network is OK), Communication Trouble, Remote Control (remote control from the Protegus app); **Inverted** – when ticked, the output works inversely; **OUT mode**: **Pulse** – the output stays in the new state for the time given in the **Pulse Time** field (seconds), **Level** – the state is kept until the next command; **Pulse time** – the length of the pulse in seconds; in Pulse mode the output switches for this long.

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.

6.3 CMS reporting

The communicator sends the events to the monitoring station over an IP connection. 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 over if that channel is interrupted. The communication is encrypted and password-protected; for receiving and forwarding to the monitoring software, a Trikdis receiver (IPcom software receiver for Windows or Linux, RL14 hardware IP/SMS receiver, RM14 multi-channel receiver) or a universal receiver that knows the DC-09 / TL150 protocol is needed.

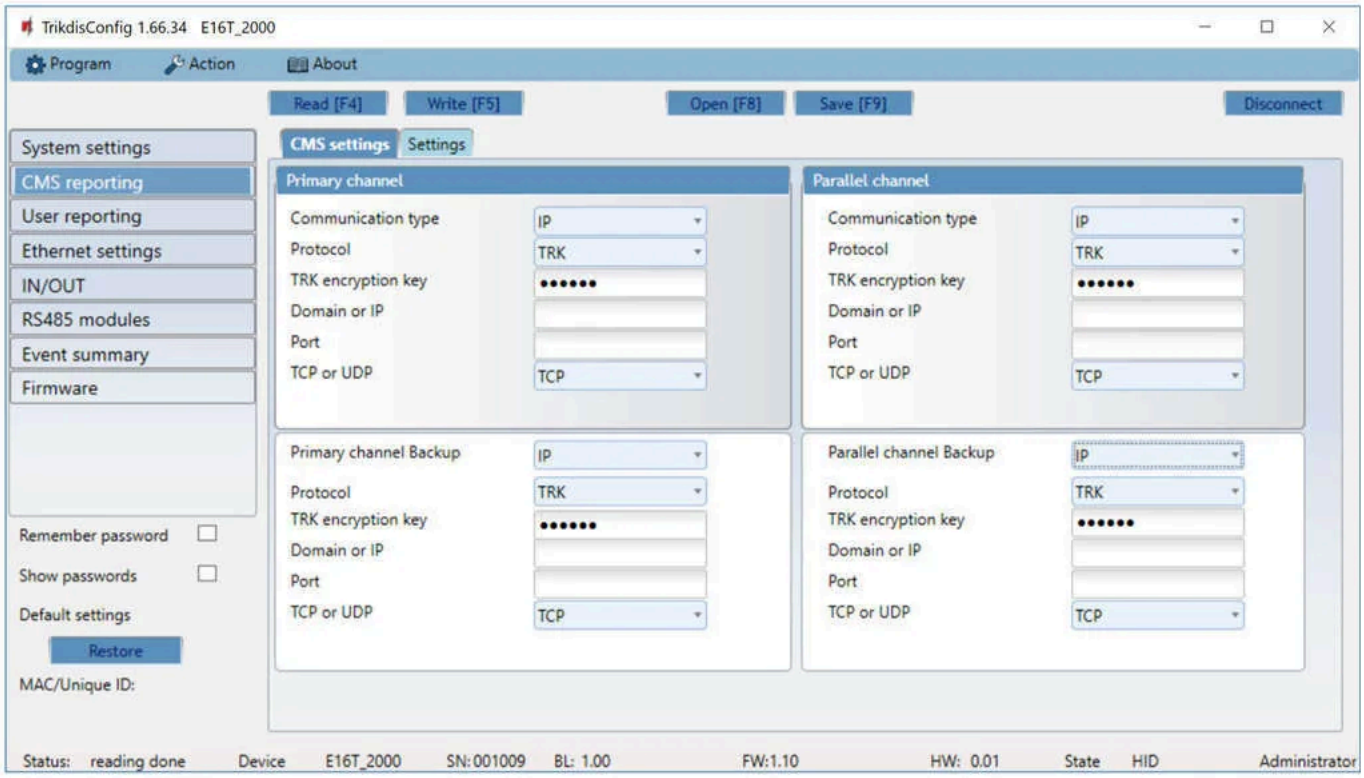


Figure 20. TrikdisConfig – CMS reporting, CMS settings tab: primary, backup and parallel channel.

Primary channel

- **Communication type** – on the E16T only **IP** can be selected.
- **Protocol** – TRK (Trikdis receivers), DC-09_2007 or DC-09_2012 (universal receivers), TL150 (SUR-GARD).
- **TRK encryption key** – 6-digit encryption key; it must be the same in the communicator and in the receiver.
- **Domain or IP**, **Port** – the address of the receiver (domain name or IP address) and its network port number.
- **TCP or UDP** – the transmission protocol: the events are sent with this (according to the receiver's setting).

Primary channel Backup – backup channel. It takes over communication if the primary channel is not working; its settings are the same as above. It is worth setting it up on a wired device too – for example with the receiver's second address or port – because the backup channel also bridges a fault on the receiver side.

Parallel channel. Alongside the primary channel, it sends to a second receiver at the same time (for example to the local and the central monitoring station). It has its own backup channel.

Earlier E16T

On the earlier E16T, TrikdisConfig shows the same on the **CMS Reporting** tab of the **Reporting** window, with different field names:

- **Primary** group: **Enable** – when ticked, the primary channel to the monitoring station is active; **Remote Host** – the domain name or IP address of the receiver; **Remote Port** – the network port number of the receiver; **TCP or UDP** – the transmission protocol; **PING Time** – switch it on and enter the time between heartbeats (default 30) – it is needed for supervising the connection; **Encryption key** – 6-digit encryption key, the same in the communicator and in the receiver.
- **Backup** group: **Enable** – switches on the backup channel, which sends if the primary connection is interrupted; the other fields are the same as for the primary.
- **Settings** group: **TCP protocol** – the encoding of the transmission: TRK (for a Trikdis receiver), DC-09_2007 or DC-09_2012 (for a universal receiver).
- **SIA IP parameter** group – can only be changed if the **TCP protocol** field is set to DC-09_2007 or DC-09_2012: **Encryption enabled** – with DC-09_2012, encryption can be switched on; **DC09-2012 encryption key** – the encryption key set in the receiver; **DC09-2012 receiver No.** – the number of the receiver; **DC-09 line No.** – the number of the receiver's line; **Use time stamp** – when ticked, the message also contains the time (time stamp).

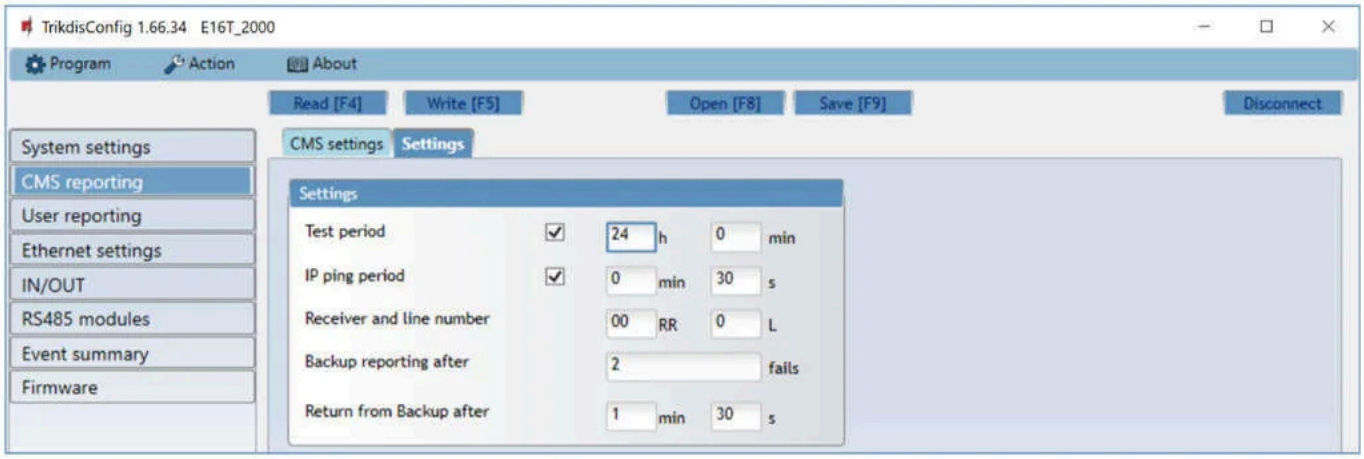


Figure 21. TrikdisConfig – CMS reporting, Settings tab: test report, PING, the receiver and line number (Receiver and line number: RR = receiver number, L = line number) and the timings of the backup channel.

On the **Settings** tab you set the timings and the receiver and line number; the DC-09 group is only needed if you send with the DC-09 protocol (it is not yet visible in the 2022 screenshot).

- **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.

6.4 User reporting

On the **PROTEGUS Cloud** tab you enable the Protegus service. The E16T has no SMS notification or SMS control, so this page has only this one tab.

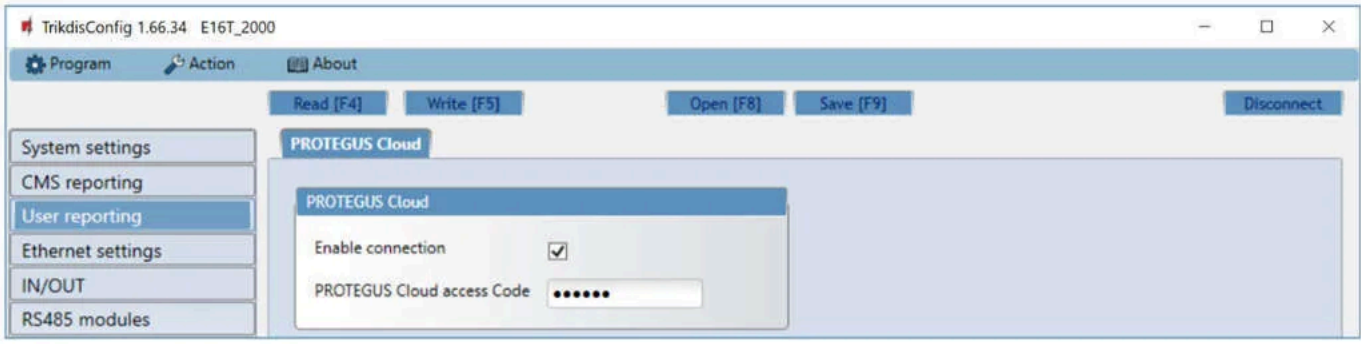


Figure 22. TrikdisConfig – User reporting, PROTEGUS Cloud tab.

- **Enable connection** – enables the connection to the Protegus cloud and remote access with TrikdisConfig.
- **Protegus Cloud access code** – 6-digit code for the Protegus connection (default `123456`). If you have changed it, this is what has to be entered when the system is added in Protegus 2. It can only be set before the system is created in Protegus 2; it cannot be changed afterwards.

6.5 Ethernet settings

Here you set how the E16T connects to the local network.



Figure 23. TrikdisConfig – Ethernet settings page; DHCP is switched on by default.

- **Use DHCP** – when ticked, the device automatically gets its IP address, subnet mask and gateway from the router's DHCP server. This is the factory setting, and in most places nothing more needs to be done. If there is no DHCP on the network, if automatic login to the network fails, or if the network administrator asks for a static address, untick it and fill in the fields below and the name servers manually:
- **Static IP** – the device's static IP address on the local network (an address not used by any other device and outside the DHCP range).
- **Subnet mask** – the subnet mask of the network.
- **Default gateway** – the default gateway, usually the router's address. With a wrong gateway the device reaches the local network but not the internet.
- **DNS 1, DNS 2** – name servers; through these the device finds the Protegus cloud and a receiver specified by domain name. Google's public DNS is set by default; if the network only allows its own name server towards the outside, enter the address of the local DNS here. 3 flashes of the TROUBLE LED indicate a DNS error.

The device's unique identifier, the MAC address (**Internal MAC** in the software), is shown in the newer TrikdisConfig window not on this page but at the bottom of the window, in the **MAC / Unique ID** field of the status bar.

The device only builds **outgoing** connections to the receiver and the Protegus cloud, so no port needs to be opened or forwarded on the router, and no public static IP address is needed either.

On the earlier E16T, the MAC address is shown in the **Internal MAC** field of the Ethernet settings group on the **System settings** page (note in section 6.2).

6.6 IN/OUT

Here you set the role of the communicator's three dual-function I/O terminals: **Disabled** (not used), **IN** (input) or **OUT** (output). For an input, the type also has to be set (NC, NO, NO/EOL, NC/EOL, NO/DEOL, NC/DEOL).

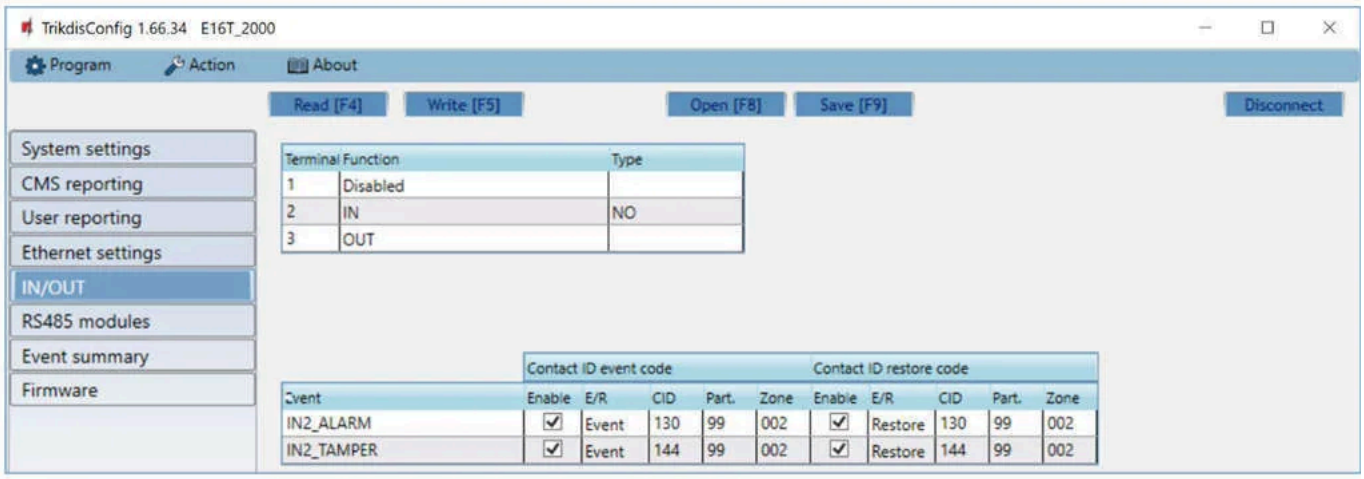


Figure 24. TrikdisConfig – IN/OUT page: the function of the I/O terminals and the events of the inputs.

When a detector connected to an input is violated, the communicator sends its own event (**INx_ALARM**, Contact ID 130), and when the tamper loop is violated, a tamper event (**INx_TAMPER**, 144), to the monitoring station and to Protegus 2; the events of every terminal set as an input appear in the table. The columns of the table:

- **Enable** – enables sending the message.
- **E/R** – the type of the event: Event (alarm) or Restore.
- **CID** – the Contact ID code.
- **Part.** – the partition number in the message.
- **Zone** – the zone number in the message.

Earlier E16T

The earlier E16T has no IN/OUT page: you set the type and events of the two inputs in the **Input description** group of the **Event summary** page. **Partition** – the partition number; **Contact ID** – the event code (the default value can stay), this is the code sent to Protegus and to the monitoring station when the input is violated; **Zone No.** – the zone number, this goes in the messages; **Type** – the input type (NO, NC, EOL); **Enable / Alarm** – when ticked, it reports when the input is violated (event); **Enable / Restore** – when ticked, it reports when the input is restored. The output is set in the **System settings** → **Output** group (note in section 6.2).

6.7 RS485 modules

The iO-8 and other iO-series expanders connected to the RS485 bus have to be added on the **Modules list** tab.

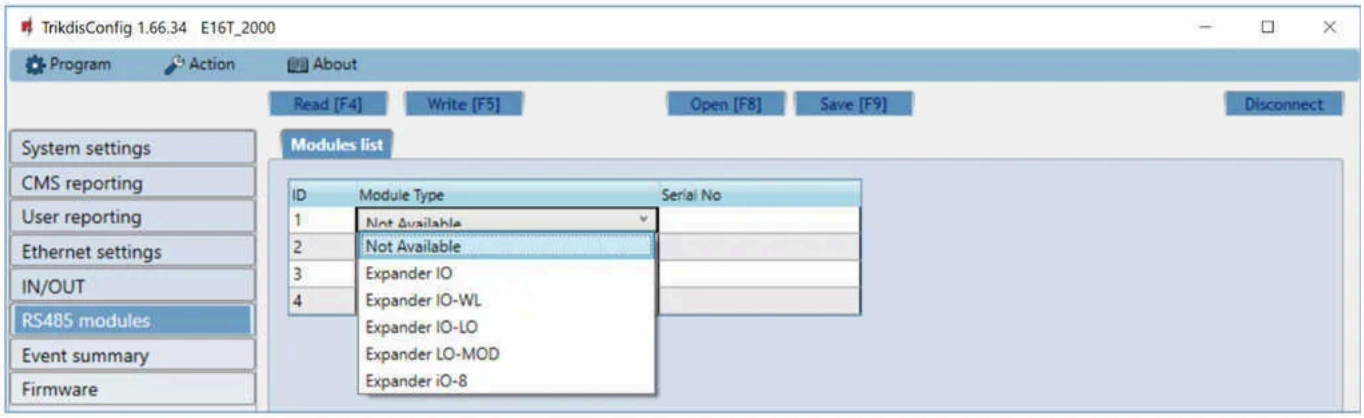


Figure 25. TrikdisConfig – RS485 modules, Modules list tab: the selectable module types.

- **Module Type** – the type of the connected module, from the list (Expander iO-8, IO, IO-WL, IO-LO, LO-MOD).
- **Serial No** – the 6-digit serial number of the module (on the module and its box, SN).

After selecting the module and entering the serial number, press the **Write [F5]** button, unplug the USB cable and wait a minute while the communicator registers the module. Then plug the cable back in, read the device (**Read [F4]**), and the module's own numbered tab appears on the RS485 modules page.

iO-8 expander – 8 dual-function I/Os; up to 4 modules can be connected to the communicator.

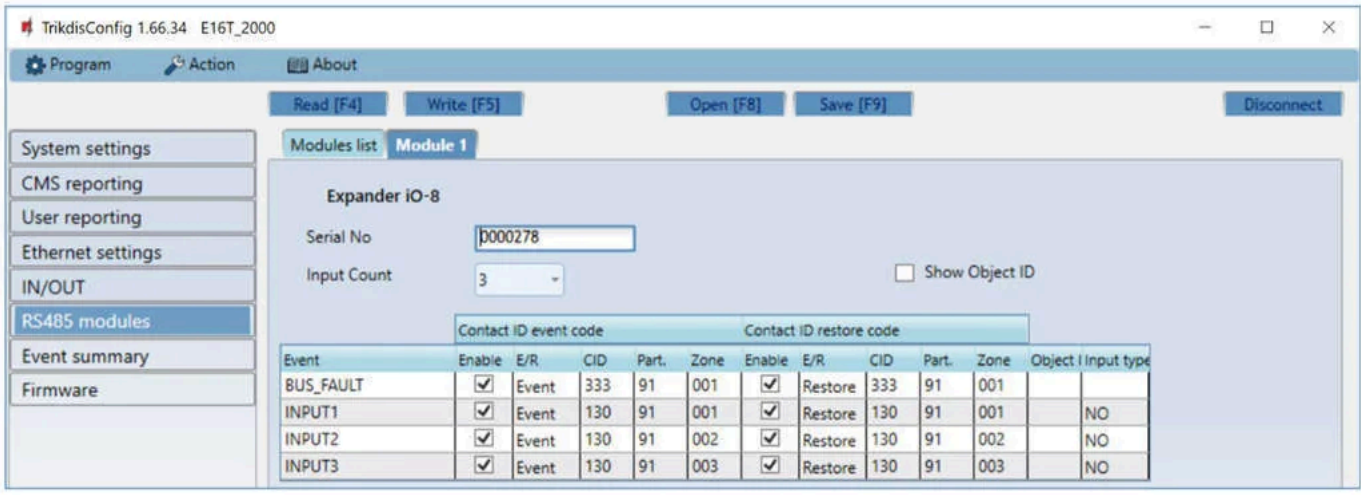


Figure 26. TrikdisConfig – RS485 modules, tab of the iO-8 module.

- **Input Count** – how many terminals should be inputs; the rest will be outputs. The input type (**Input type**: NO or NC) can be set in the table. The role of the outputs (arming / disarming or switching a device) is set in the Protegus 2 app.
- In the table you can assign Contact ID codes to the bus fault (**BUS_FAULT**, Contact ID 333) and to the violation and restore events of the inputs (**INPUTx**, 130) (**Enable**, **E/R**, **CID**, **Part.**, **Zone**). By default, module 1 reports with partition 91 and module 4 with partition 94. By ticking **Show Object ID**, an object ID different from the communicator's can also be set for the inputs.

6.8 Event summary

On this page you can enable or disable the device's **own internal messages** and change their Contact ID code, partition and zone number. A message disabled here is not sent by the device on any channel. By default the messages are sent with partition 99 and zone 999.

Message	Contact ID	When it is generated
COMMUNICATION	350	Communication between the communicator and the alarm panel has been lost (disabled by default). A communicator connected to the bus or serial port detects this directly; a telephone-line communicator only with **Line supervision** enabled.
POWER	302	Inadequate (low) supply voltage; its restore is a separate message.
REMOTE_STARTED	411	Remote programming with TrikdisConfig has started.
REMOTE_FINISHED	412	Remote programming has finished.
START	700	The device has connected to the network (start-up).
TEST	602	Periodic test report.
PING	760	The PING keep-alive message. It is not in every device's list: it appears on the screen of the earlier hardware version, while the Event summary page of the newer versions has no such row. Its interval is set in the **CMS reporting** → **Settings** → **IP ping period** field.

- **Enable** – enables sending the message to the monitoring station and to Protegus 2.
- **E/R** – the message type: Event or Restore – the row stands for the occurrence of the event or its restore.
- **Part.** – the partition (area) number the device sends with the internal event and its restore.
- **Zone** – the zone number the device sends with the internal event and its restore.
- The **CID** code, the **partition** and the **zone** can be changed for any event; where there is a restore (Restore), its code can be set separately.

The events of the device's own inputs (**INx_ALARM**, **INx_TAMPER**) are set on the **IN/OUT** page, and the events of the expansion modules (**BUS_FAULT**, **INPUTx**) on the **RS485 modules** page, on the module's tab. Enabling the test report and its interval are set in the **CMS reporting** → **Settings** → **Test period** field.

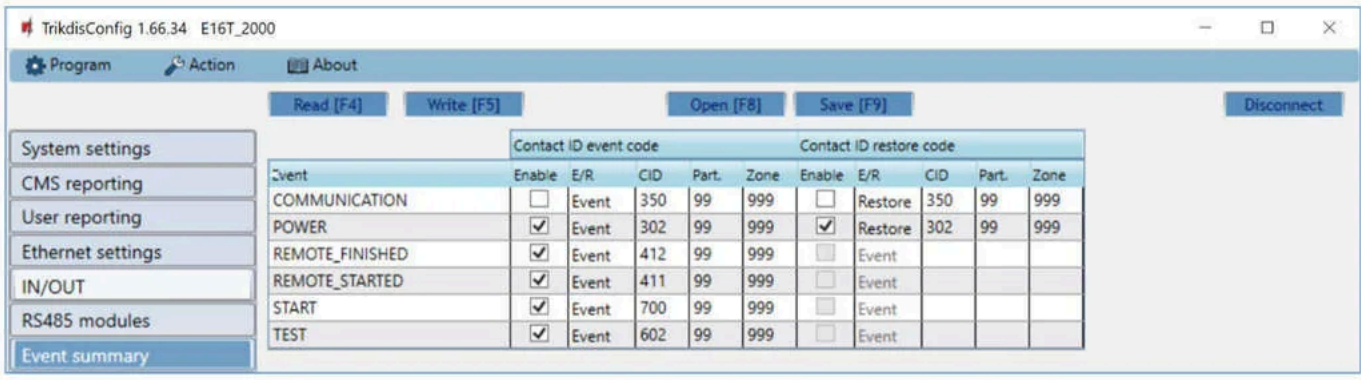


Figure 27. TrikdisConfig – Event summary page: the internal messages of the device.

On the earlier E16T, the inputs are also set on this page (note in section 6.6).

6.9 Restoring the factory settings

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.

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.

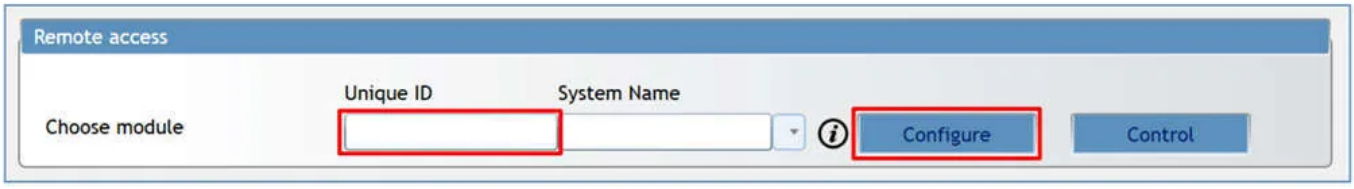


Figure 28. TrikdisConfig – Remote access: the device identifier (with the E16T the MAC address), the system name and the Configure button.

Enabling the Protegus service is described in section 6.4, downloading TrikdisConfig in section 2.1.

8. Testing the communicator

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.

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.

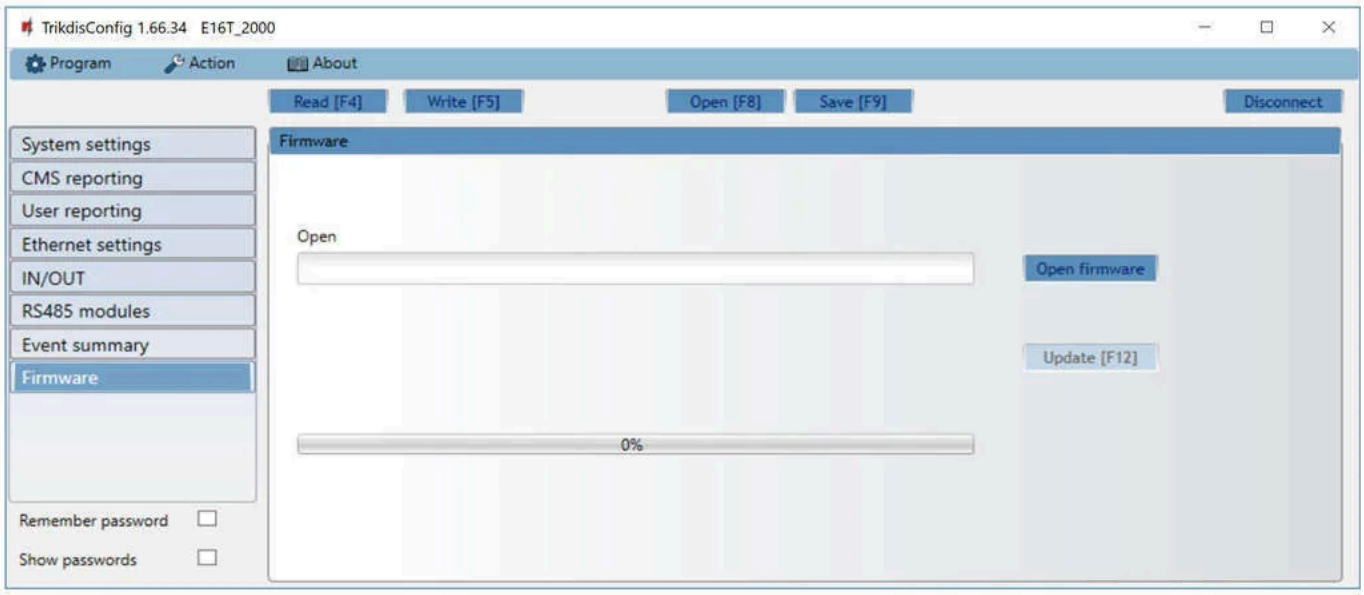


Figure 29. TrikdisConfig – Firmware page: Open firmware and Update [F12].

The update requires an internet connection. An antivirus program, a firewall or strict network settings can prevent the automatic firmware download; in that case download the file manually and open it on the Firmware page.

10. Troubleshooting and frequently asked questions

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

The NETWORK LED is off – no network

1. Look at the flashes of the **TROUBLE** LED: 1 = no physical connection, 2 = no IP address received (DHCP), 3 = DNS error.
2. **With 1 flash**, check the cable and the connectors (whether the RJ45 is plugged in until it clicks), the port of the router or switch (whether it is live, whether it is disabled), and try another cable or port.
3. **With 2 flashes**, there is no DHCP server on the network or it does not respond: switch it on in the router, or give the device a fixed IP address, mask and gateway on the **Ethernet settings** page (section 6.5).
4. **With 3 flashes**, name resolution is not working: check the DNS 1 / DNS 2 fields (by default Google's public DNS), and whether the network allows outgoing DNS traffic.

There is a network, but the monitoring station does not receive 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. 6 flashes of the **TROUBLE** LED indicate that there is no connection to the receiver: check the receiver's address, port, the TCP/UDP setting and the encryption key (**CMS reporting**).
2. If the receiver is entered with a domain name, check the DNS setting (**Ethernet settings**).
3. With a fixed IP address, check the gateway (**Default gateway**): with a wrong gateway the device reaches the local network, but not the internet.
4. On a company or filtered network, the firewall may block the outgoing connection to the receiver's port – check with the network administrator (section 3.2).

The panel does not send the events to the communicator

1. The panel's dialer must be switched on, in DTMF mode, with Contact ID format and a telephone number entered (chapter 4).
2. Check the TIP/RING wiring; 7 flashes of the **TROUBLE** LED indicate a missing connection to the panel (when wired with line supervision).
3. If the panel expects a dial tone and does not start the call, switch off dial tone detection in it.
4. If the panel signals a "communication fault" although the event has arrived, check the **Wait acknowledgment from CMS** setting (section 6.2).

Protegus 2 does not see the device

1. **Enable connection** must be ticked on the **User reporting** → **PROTEGUS Cloud** tab.
2. When creating the system, the **Protegus Cloud access code** set in the device has to be entered; it cannot be changed in the device after the system has been created.
3. Enter the MAC address exactly, from the box or the back of the device – or scan the QR code on the label with the app, so it cannot be mistyped.
4. The internet connection must be working: the NETWORK LED is green, and the DATA LED goes off after an event. Reaching the Protegus cloud also requires a working DNS (**Ethernet settings**).

I cannot log in remotely with TrikdisConfig

1. The device must be online (NETWORK LED green, the DATA LED goes off after an event), and the Protegus connection must be enabled.
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.

I have forgotten the password

A forgotten password cannot be retrieved, and it cannot be cleared by restoring the factory settings either, because the restore also requires a password. In this case only the manufacturer or the distributor can reset it: the device has to be sent to them. So note down the passwords you set in a safe place.

Do I need a fixed IP address or port forwarding on the router?

No. The E16T itself initiates the outgoing connection to the receiver and to the Protegus cloud, so neither a fixed public IP address, nor dynamic DNS, nor port forwarding is needed. On the local network, the address received via DHCP is also fine; only give it a fixed local address if there is no DHCP on the network or the network administrator asks for it (section 6.5).

Does it work over Wi-Fi?

No: the E16T only supports a wired (RJ45) network connection. If there is no network cable near the panel, a Wi-Fi bridge to the router can be set up, or choose the G16T cellular communicator.

What happens during a power failure?

The communicator is powered by the panel's battery, but if the router and the modem are left without power, there is no internet, and the events wait in the buffer (the DATA LED is lit). The device sends them once the internet is back. If the outage is not acceptable, an uninterruptible power supply for the network devices or a cellular communicator is the solution (section 3.2).

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 carefully before installation; ignoring the instructions can lead to malfunction or failure.
- Disconnect the equipment from the power supply before wiring, before every electrical connection and before servicing.
- Faults resulting from improper installation or use, as well as modifications and repairs not authorized by the manufacturer, void the warranty.
- Follow local waste disposal regulations: do not throw the faulty device or its parts in household waste.

See also

- Remote arming with a keyswitch from the Protegus 2 app – the details and pitfalls of keyswitch arming.
- Documentation in English: docs.trikdis.com.

Related products

Trikdis E16T Ethernet universal communicator - IP module

Trikdis iO8 wired expander module

Copyright

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

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

Always up-to-date version of this manual: https://mobilamb.eu/e16t-manual