Apricancello GV17 GATOR – manuale di installazione e programmazione

Manuale di installazione e programmazione dell'apricancello Trikdis GV17 GATOR: collegamenti, scheda SIM e configurazione in TrikdisConfig, utenti e permessi, controllo con chiamata, SMS e dall'app Protegus 2.



Edizione: 2026-11-17
Versione web sempre aggiornata: https://trikdis.it/manuale-gv17

Indice

1. Panoramica

1.1 A cosa serve e come funziona
1.2 Varianti
1.3 Dati tecnici
1.4 Parti del dispositivo e morsetti
1.5 Segnalazioni dei LED
1.6 Contenuto della confezione e strumenti necessari

2. Messa in servizio rapida

2.1 Messa in servizio in tre passi
2.2 Apertura solo per le persone autorizzate
2.3 Configurazione dell'app e della centrale di vigilanza

3. Installazione e collegamenti

3.1 Fissaggio e inserimento della scheda SIM
3.2 Alimentazione
3.3 Ingressi
3.4 Collegamento di un relè all'uscita universale
3.5 Collegamento dell'automazione del cancello
3.6 Collegamento del lettore RFID (Wiegand 26/34)
3.7 Modulo WiFi W485
3.8 Modulo Ethernet E485
3.9 Moduli di espansione RF-LORA e iO-LORA con lettore RFID
3.10 Moduli di espansione iO8 e iO8-LORA

4. Controllo a distanza

4.1 Controllo con chiamata telefonica
4.2 Controllo con la tastiera del telefono (DTMF)
4.3 Controllo dall'app Protegus 2
A rendszer létrehozása a Protegus 2 alkalmazásban
4.4 Widget nella schermata iniziale del telefono
4.5 Gestione degli utenti nell'app
4.6 Controllo con messaggio SMS
4.7 Programmazione via SMS

5. Configurazione con il software TrikdisConfig

5.1 La barra di stato
5.2 Pagina „System Options”
5.3 Pagina „IN/OUT”
5.3.1 Scheda IN/OUT – ingressi e uscite
5.3.2 Scheda Scheduler – programmazione oraria delle uscite
5.3.3 Scheda Holidays – giorni festivi
5.4 Pagina „Modules”
5.4.1 Scheda Modules
5.4.2 Scheda Parameters – modulo WiFi W485
5.4.3 Scheda Parameters – modulo Ethernet E485
5.5 Pagina „IP Reporting”
5.6 Pagina „User list”

5.6.1 Scheda Users – gli utenti
5.6.2 Registrazione di una tessera RFID (portachiavi)
5.6.3 Scheda Scheduler – programmazione oraria degli utenti
5.6.4 Scheda Black list – lista nera
5.7 Pagina „System events”
5.8 Pagina „Events Log”
5.9 Ripristino delle impostazioni di fabbrica
5.10 Segnalazione dello stato del cancello
6. Programmazione a distanza
7. Verifica del funzionamento
8. Aggiornamento del firmware
9. Ricerca guasti e domande frequenti
10. Norme di sicurezza
Vedi anche

1. Panoramica

Il **GV17 GATOR** è l'apricancello su rete mobile di Trikdis: è progettato per il controllo a distanza di cancelli elettrici, barriere, porte da garage e altre apparecchiature. L'utente lo controlla con una **chiamata telefonica**, con un **messaggio SMS** o dall'app **Protegus 2**; il dispositivo gestisce i numeri di telefono (le tessere RFID, gli indirizzi e-mail) di fino a **7 amministratori** e **1000 utenti**, e per ogni utente si possono impostare un limite di tempo (programmazione oraria, periodo di validità) e un contatore separati. Il GATOR invia notifiche via SMS e nell'app sui cambiamenti di stato degli ingressi e delle uscite (attivazione e ripristino) – il testo degli SMS lo decidi tu – e trasmette gli eventi anche alla centrale di vigilanza in formato Contact ID. Con il modulo WiFi **W485** o il modulo Ethernet **E485** il controllo e la trasmissione funzionano anche via Internet, senza dati mobili; con il ricetrasmettitore **RF-LORA** si possono collegare fino a 8 moduli di espansione senza fili **iO-LORA** e un modulo di espansione **iO8-LORA**, così con un solo dispositivo si possono controllare fino a 8 cancelli o barriere lontani tra loro, ciascuno con il proprio lettore RFID (i lettori RFID collegati ai moduli iO-LORA possono comandare fino a 8 uscite – un lettore sempre e solo un'uscita del proprio modulo di espansione –; per questo serve il firmware 2.13 o successivo del GATOR). Le impostazioni si eseguono con il software **TrikdisConfig**, tramite cavo USB o a distanza.



Figura 1. L'apricancello GV17 GATOR: sul davanti i LED NETWORK, DATA, POWER e TROUBLE, in alto il connettore dell'antenna, in basso la morsettiera estraibile.

1.1 A cosa serve e come funziona

A cosa serve soprattutto

- **Apertura a distanza di cancelli, barriere e porte da garage** per la famiglia, per il condominio, per i dipendenti di un'azienda o per gli affittuari di un parcheggio: l'utente chiama il numero della scheda SIM del GATOR e il cancello si apre – il dispositivo rifiuta la chiamata, perciò la chiamata è gratuita. Lo stesso si può fare dall'app con un pulsante, con un widget messo nella schermata iniziale del telefono oppure con un SMS.
- **Controllo accessi con tessera RFID e codice**: con uno o due lettori Wiegand 26/34 (ingresso e uscita), pulsante di uscita, programmazione oraria per utente (chi può entrare e quando), periodo di validità e contatore degli accessi; dagli ingressi e dalle uscite si può ricavare anche una **rilevazione delle presenze** in Protegus 2 – ne parla un articolo a parte: GV17 come sistema di controllo accessi e/o rilevazione presenze.
- **Qualsiasi altra apparecchiatura** accesa e spenta a distanza, in modalità a impulso o bistabile, anche secondo una programmazione oraria: illuminazione, irrigazione, pompa, riscaldamento.
- **Più cancelli in un solo sistema**: con i moduli RF-LORA e iO-LORA, senza fili, fino a 8 siti, ciascuno con il proprio relè, ingresso e lettore RFID – Controllo accessi flessibile e senza fili con il sistema GATOR RF-LoRa.

Come funziona

- **Controllo**: con una chiamata telefonica (di fabbrica chiunque chiami; con l'elenco utenti solo le persone autorizzate), durante la chiamata con la tastiera del telefono (DTMF), con comando SMS, dall'app mobile e web Protegus 2, con il widget Android, con tessera RFID e codice.
- **Notifiche all'utente**: via SMS agli amministratori (sugli eventi degli ingressi e delle uscite, test, nuovo utente), con notifiche push nell'app Protegus 2.
- **Trasmissione alla centrale di vigilanza**: con codici evento Contact ID ai ricevitori IP software e hardware di Trikdis, che funzionano con qualsiasi software di centrale di vigilanza; ricevitore principale e di riserva (se la connessione con il ricevitore principale si interrompe, i messaggi vanno automaticamente al ricevitore di riserva), SMS di riserva; gli eventi possono andare contemporaneamente alla centrale di vigilanza e a Protegus 2.
- **Ingressi e uscite**: 2 ingressi (NO, NC o EOL 10 kΩ), 2 morsetti universali (ingresso o uscita a collettore aperto, 50 mA), 1 uscita a relè (1 A / 30 V DC, 0,5 A / 125 V AC). Ogni modulo di espansione iO-LORA aggiunge al sistema 1 ingresso e 1 uscita a relè (fino a 8 moduli, cioè in tutto 8 ingressi e 8 uscite in più), il modulo di espansione iO8 o iO8-LORA ulteriori ingressi e uscite (se ne può collegare uno al GATOR).
- **Installazione e configurazione**: pronto all'uso di fabbrica; gli utenti li aggiungi e li cancelli dall'app Protegus 2 (come amministratore), via SMS o con il software TrikdisConfig; la configurazione avviene con cavo USB Mini-B o a distanza; il firmware si può aggiornare anche a distanza; due livelli di accesso (installatore e amministratore).

1.2 Varianti

Il GATOR è disponibile in due varianti di rete mobile; i collegamenti, la configurazione e il controllo sono identici, cambia solo il modem. Nella barra di stato di TrikdisConfig vedi il tipo esatto nel formato **GV17_xxxx** (punto 5.1).

Variante	Modem	Bande
GV17-4G	4G (LTE)	in Europa LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28 (per l'America Latina esiste una variante con bande diverse)
GV17-2G	2G (GSM/GPRS)	850 / 900 / 1800 / 1900 MHz

Trikdis GV17 - GATOR controllore cancello intelligente 4G GSM / IP

Trikdis GV17 - GATOR controllore cancello intelligente 2G GSM / IP

A causa del graduale spegnimento delle reti 2G, per le nuove installazioni consigliamo la variante 4G. Sui dispositivi con codice tipo **GV17_2E70** e **GV17_2S70** il controllo con la tastiera durante la chiamata (DTMF) non funziona (punto 4.2); il controllo con chiamata, SMS e dall'app funziona anche su questi allo stesso modo.

1.3 Dati tecnici

Caratteristica	Valore
Bande del modem 2G (GSM)	850 / 900 / 1800 / 1900 MHz
Bande del modem 4G (LTE)	Europa: LTE-FDD B1 / B3 / B5 / B7 / B8 / B20 / B28; America Latina: LTE-FDD B2 / B3 / B4 / B5 / B7 / B8 / B28 / B66
Tensione di alimentazione	9–32 V DC oppure 12–24 V AC
Assorbimento	100 mA
Ingressi	2, tipo selezionabile: NC, NO, EOL = 10 kΩ
Ingressi/uscite universali	2; come ingresso NC, NO, EOL = 10 kΩ, come uscita a collettore aperto (OC), al massimo 50 mA
Uscita	1 relè, 1 A / 30 V DC, 0,5 A / 125 V AC
Memoria degli eventi non inviati	fino a 60 eventi
Registro eventi	fino a 5000 eventi
Utenti che ricevono messaggi e sono autorizzati al controllo (amministratori)	7
Utenti autorizzati al controllo	1000
Ambiente operativo	–20 … +50 °C, umidità relativa al massimo 80 % a +20 °C
Dimensioni	92 × 62 × 26 mm
Peso	80 g

1.4 Parti del dispositivo e morsetti

I numeri della figura indicano le parti del dispositivo; il significato dei morsetti è riportato nella tabella.

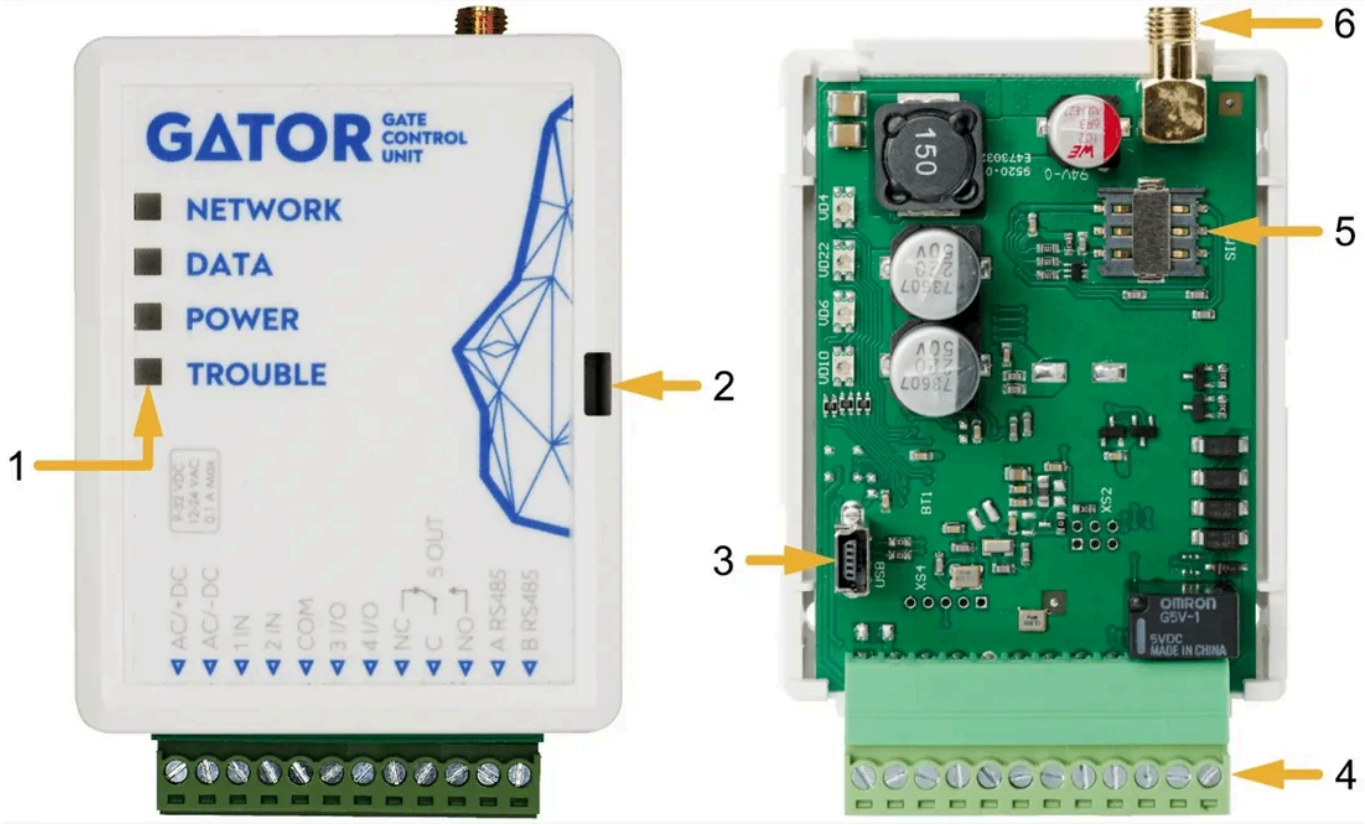


Figura 2. Le parti del GATOR.

- 1 LED di segnalazione
- 2 apertura per togliere il coperchio frontale
- 3 connettore USB Mini-B per la programmazione
- 4 morsettiera estraibile
- 5 alloggiamento della scheda nano SIM
- 6 connettore SMA dell'antenna di rete mobile

Morsetto	Funzione
AC/+DC	alimentazione: polo positivo 9–32 V DC oppure 12–24 V AC
AC/−DC	alimentazione: polo negativo 9–32 V DC oppure 12–24 V AC
1 IN	ingresso 1, tipo NO, NC o EOL (di fabbrica: ingresso NO)
2 IN	ingresso 2, tipo NO, NC o EOL (di fabbrica: disattivato)
COM	punto comune per gli ingressi
3 I/O	ingresso o uscita (di fabbrica: disattivato)
4 I/O	ingresso o uscita (di fabbrica: disattivato)
NC	contatto normalmente chiuso del relè
C	contatto comune del relè
NO	contatto normalmente aperto del relè
A RS485	filo A del bus RS485
B RS485	filo B del bus RS485

Il programma e i comandi SMS chiamano l'uscita a relè **5 OUT** (OUTPUT5) e i due morsetti universali, usati come uscite, **3 OUT** e **4 OUT**. La morsettiera a 12 poli si può sfilare dal dispositivo ed è disponibile anche separatamente:

1.5 Segnalazioni dei LED

LED	Luce	Significato
NETWORK	verde, fisso	connesso alla rete mobile
	giallo lampeggiante	intensità del segnale della rete mobile con 0–5 lampeggi; 3 sono già sufficienti
DATA	verde, fisso	invio di un messaggio in corso
	giallo, fisso	nella memoria ci sono eventi in attesa di invio
POWER	verde lampeggiante	la tensione di alimentazione è corretta
	giallo lampeggiante	la tensione di alimentazione non è corretta
	rosso e giallo lampeggiante	modalità di configurazione
TROUBLE	spento	nessun guasto di funzionamento
	1 lampeggio	manca la scheda SIM
	2 lampeggi	il codice PIN della scheda SIM è errato
	3 lampeggi	non riesce a connettersi alla rete mobile
	4 lampeggi	non riesce a connettersi al cloud Protegus o al ricevitore IP primario
	5 lampeggi	non riesce a connettersi al ricevitore IP di riserva
	6 lampeggi	l'orologio interno non è impostato
	7 lampeggi	la tensione di alimentazione non è corretta

Se nessun LED è acceso, controlla la tensione di alimentazione e i collegamenti.

Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

1.6 Contenuto della confezione e strumenti necessari

Nella confezione: 1 apricancello GV17 GATOR, 1 antenna di rete mobile, 3 resistenze da 10 kΩ, 1 nastro biadesivo (5 cm) e 2 viti.

Cosa ti servirà

Prima di iniziare l'installazione controlla di avere tutto a portata di mano: cavo USB Mini-B per la configurazione · cavo con almeno 4 conduttori per i collegamenti · cacciavite piatto da 2,5 mm · scheda nano SIM attivata (disattiva la richiesta del PIN) con servizio dati mobile, se usi anche l'app o la centrale di vigilanza · antenna esterna, se sul posto il segnale è debole · il manuale per l'installatore dell'apparecchiatura controllata (motore del cancello, barriera), con il collegamento dell'ingresso di comando e dell'uscita di stato del cancello. Gli accessori elencati vanno procurati separatamente – ordinali presso il tuo rivenditore.

Con segnale debole, in una scatola metallica o dietro un muro spesso, al posto dell'antenna della confezione usa un'antenna remotabile con cavo da 2,5 m:

Trikdis ME301M antenna GSM magnetica con cavo da 2,5m

Trikdis ANT04 antenna GSM adesiva con cavo da 2,5m

2. Messa in servizio rapida

Il GATOR è pronto all'uso di fabbrica

Se qualcuno chiama il numero di telefono della scheda SIM inserita nel dispositivo, il GATOR rifiuta la chiamata e attiva l'uscita a relè **5 OUT** per **3 secondi**. Se questo funzionamento ti va bene, il dispositivo può essere messo in servizio senza nessun'altra impostazione.

2.1 Messa in servizio in tre passi

1. **Inserisci la scheda nano SIM** nell'alloggiamento del GATOR (punto 3.1). Prima disattiva sulla scheda la richiesta del PIN in un telefono, altrimenti il dispositivo non si registra sulla rete (oppure devi inserire il PIN in TrikdisConfig, punto 5.2).
2. **Collega l'alimentazione e l'automazione del cancello** secondo gli schemi del capitolo 3: l'alimentazione ai morsetti **AC/+DC** e **AC/−DC**, l'ingresso di comando dell'automazione ai contatti **C** e **NO** del relè.
3. **Accendi l'alimentazione.** Con funzionamento corretto il LED **POWER** lampeggia in verde, il LED **NETWORK** è acceso in verde e intanto lampeggia in giallo in base all'intensità del segnale. Chiama il numero della scheda SIM: il dispositivo rifiuta la chiamata e il relè si eccita per 3 secondi.

2.2 Apertura solo per le persone autorizzate

Di fabbrica **chiunque** chiami il suo numero può controllare il GATOR. Se vuoi consentirlo solo a determinate persone, invia un SMS con il numero di telefono degli utenti (invia il comando dal tuo telefono, perché chi per primo chiama o invia un SMS al dispositivo ne diventa l'amministratore, punto 4.1):

```
SETU 123456 +CC123456789#Pietro#pietro@example.com
```

Dopo l'inserimento del primo numero il GATOR reagisce solo alle chiamate provenienti dai numeri presenti nell'elenco e ignora le altre. Puoi aggiungere altri utenti allo stesso modo, uno alla volta; l'insieme completo dei comandi SMS è descritto al punto 4.7, e l'elenco lo puoi gestire anche in TrikdisConfig e nell'app Protegus 2 (punti 5.6 e 4.5).

Cambia la password dell'amministratore

Con la password di fabbrica `123456` chiunque conosca il numero del dispositivo può riprogrammare il GATOR. Alla prima messa in servizio cambiala via SMS (`PSW 123456 nuovapassword`, 6 caratteri) oppure in TrikdisConfig (**System Options** → **Administrator Code**).

2.3 Configurazione dell'app e della centrale di vigilanza

- **App Protegus 2:** in TrikdisConfig, nella pagina **IP Reporting**, attiva il servizio cloud (**Enable cloud service**, punto 5.5) e cambia il codice di fabbrica `123456` del **Cloud Access Code**; lo stesso via SMS: `CONNECT 123456 PROTEGUS=ON`. Dopo di che il sistema si può aggiungere all'app come descritto al punto 4.3. Per questo sulla scheda SIM serve il servizio dati mobile (oppure un modulo W485 / E485).
- **Centrale di vigilanza:** nella pagina **IP Reporting** inserisci l'indirizzo, la porta e la chiave di crittografia del ricevitore, nella pagina **System Options** il codice oggetto (punti 5.2 e 5.5).
- **Ordine consigliato delle impostazioni in TrikdisConfig:** password dell'amministratore e dati della SIM (APN) → funzione degli ingressi e delle uscite, durata dell'impulso → utenti, tessere RFID, programmazione oraria → cloud e centrale di vigilanza → verifica secondo il capitolo 7.

Se vuoi modificare le impostazioni di fabbrica o attivare altre funzioni del dispositivo, il capitolo 5 descrive le impostazioni del software TrikdisConfig.

3. Installazione e collegamenti

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.

Il capitolo descrive il fissaggio del GATOR, l'alimentazione, il collegamento degli ingressi, del relè e dell'automazione del cancello, e poi il collegamento dei lettori RFID e dei moduli di espansione (W485, E485, RF-LORA + iO-LORA, iO8 / iO8-LORA). Negli schemi i nomi dei morsetti del GATOR corrispondono alle scritte sul dispositivo (punto 1.4).

3.1 Fissaggio e inserimento della scheda SIM

1. Togli il coperchio frontale (sgancialo inserendo il cacciavite nell'apertura laterale), poi sfila la morsettiera.
2. Estrai il circuito stampato dalla scatola: sollevalo premendo la linguetta di fissaggio.
3. Fissa il fondo della scatola nel punto desiderato con le viti (oppure con il nastro biadesivo in dotazione).
4. Rimetti al suo posto il circuito stampato e la morsettiera.
5. Avvita l'antenna di rete mobile sul connettore SMA.
6. Inserisci la scheda nano SIM nell'alloggiamento.
7. Rimetti il coperchio frontale.

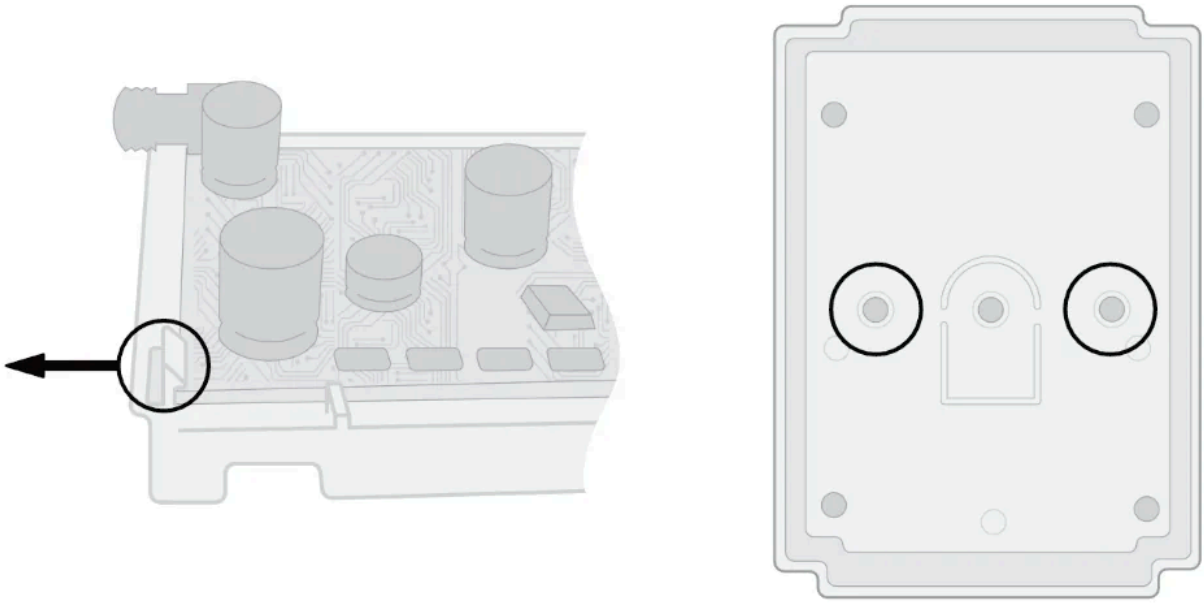


Figura 3. A sinistra la linguetta di fissaggio del circuito stampato (premendola nella direzione della freccia la scheda si libera), a destra i due fori per le viti del fondo.

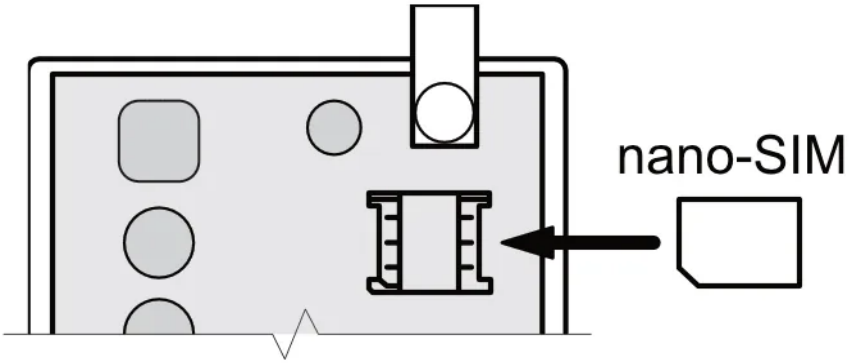


Figura 4. Inserimento della scheda nano SIM nella direzione della freccia, nell'alloggiamento sul circuito stampato.

La morsettiera è estraibile: così il dispositivo si può togliere dall'alimentazione o riavviare con un solo gesto, durante il collegamento è più comoda da maneggiare e, per la programmazione via USB, il dispositivo si può portare al computer.

3.2 Alimentazione

Il GATOR funziona con alimentazione **9–32 V DC** oppure **12–24 V AC**; i due morsetti di alimentazione (**AC/+DC**, **AC/−DC**) accettano entrambi i tipi. Nella maggior parte dei casi basta l'uscita di alimentazione per accessori della centralina del motore del cancello (di solito 24 V AC o DC), così non serve un alimentatore separato. Con un'alimentazione propria va bene un trasformatore ~230 V / 16 V da almeno 10 VA (con fusibile da 125 mA sul lato 230 V) oppure un alimentatore in corrente continua da 9–32 V e almeno 0,2 A. Il dispositivo non ha una batteria di riserva: se il cancello deve aprirsi anche durante un'interruzione di corrente, alimentalo da un gruppo di continuità. Collega i fili secondo lo schema seguente.

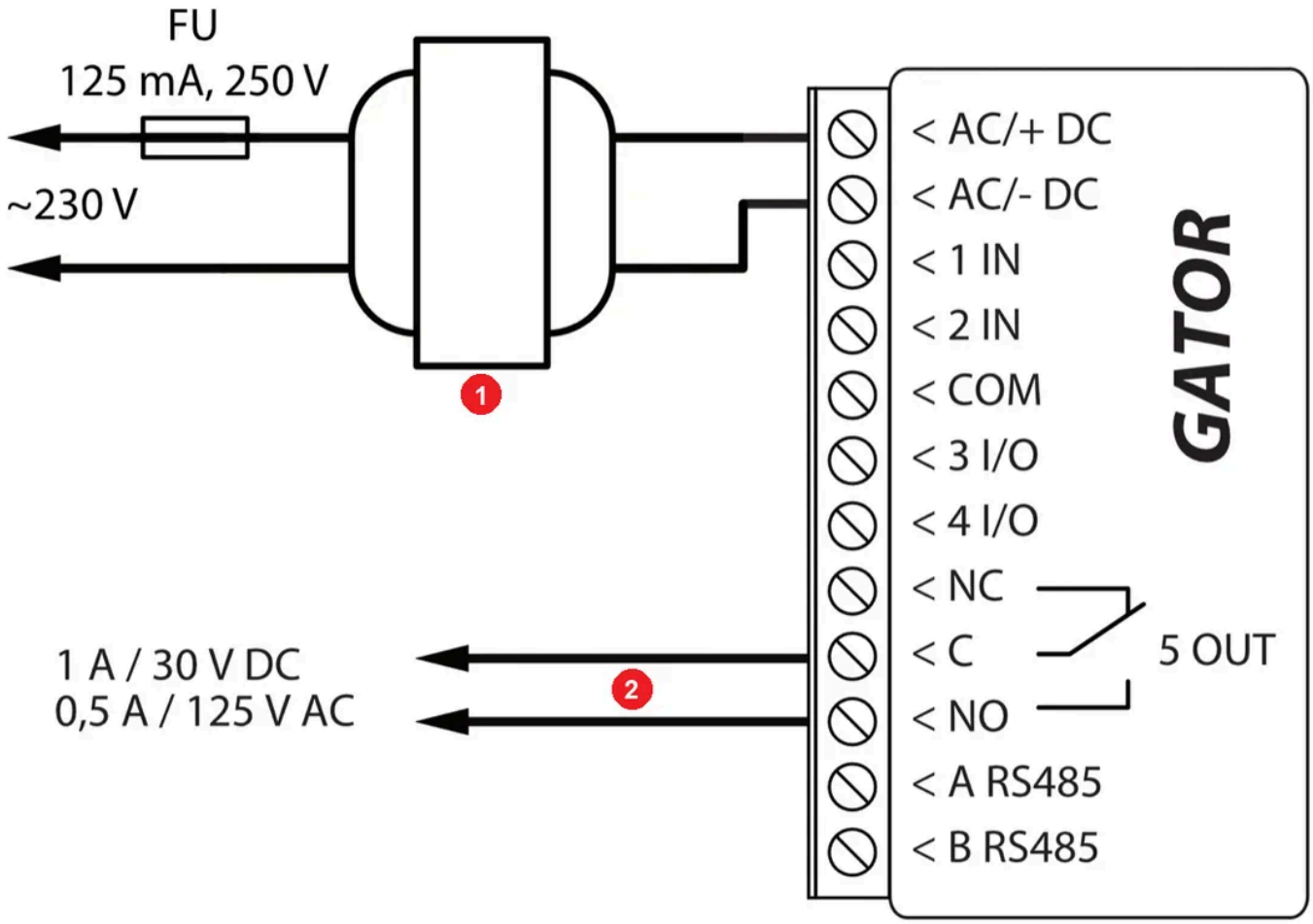


Figura 5. Collegamento dell'alimentazione e dell'automazione del cancello: alimentazione di rete da trasformatore ~230 V / 16 V, 10 VA, 50 Hz (fusibile 125 mA, 250 V) o da alimentatore in corrente continua 9–32 V, 0,2 A ai morsetti AC/+DC e AC/−DC; l'ingresso di comando dell'automazione ai contatti C e NO del relè; portata del relè 1 A / 30 V DC oppure 0,5 A / 125 V AC.

- 1 trasformatore, ~230 V / 16 V, 10 VA, 50 Hz („Transformer"), oppure alimentatore in corrente continua, 9–32 V, 0,2 A („or DC power supply source")
- 2 comando del cancello („Gate control") – l'ingresso di comando dell'automazione del cancello

Negli schemi l'alimentazione dei lettori RFID, dei relè e dei moduli di espansione è presa dal morsetto **AC/+DC**: questo è possibile solo con alimentazione in **corrente continua** (negli schemi 9–16 V DC, 0,5 A, per i moduli W485 / E485 e iO8 10–28 V DC). Con alimentazione in corrente alternata il lettore e il modulo hanno bisogno di un alimentatore DC separato.

3.3 Ingressi

Il GATOR ha **quattro ingressi**: **1 IN** e **2 IN** sono sempre ingressi, **3 I/O** e **4 I/O** sono morsetti universali che si possono impostare come ingresso o come uscita. Ognuno funziona rispetto al morsetto **COM** e può essere di tipo **NO**, **NC** o **EOL** (con resistenza di fine linea da 10 kΩ); tre resistenze di fine linea sono nella confezione. All'ingresso puoi collegare il finecorsa o l'uscita di stato del cancello (segnalazione dello stato del cancello, punti 3.5 e 5.10), un pulsante di uscita (punto 3.6), oppure qualsiasi sensore o contatto di cui vuoi ricevere un SMS o una notifica push quando cambia, o con cui vuoi comandare un'uscita (**CTRL by IN**, punto 5.3). Il tipo e il tempo di reazione si impostano nella pagina **IN/OUT** di TrikdisConfig; di fabbrica è attivo solo 1 IN (NO). Collega gli ingressi in base al tipo impostato (NC, NO, EOL), secondo lo schema seguente.

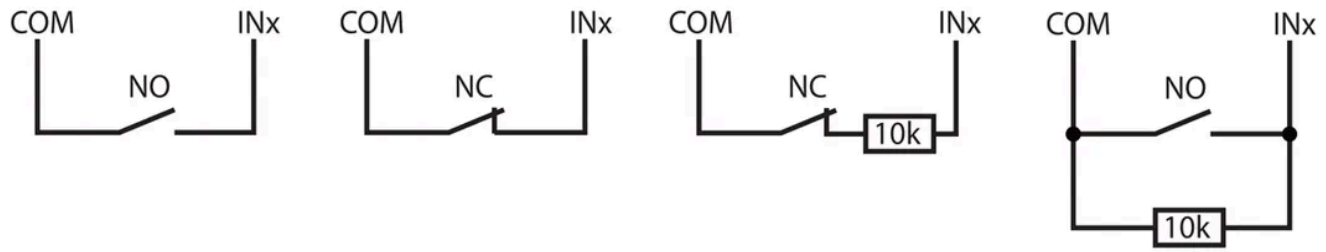


Figura 6. I quattro modi di collegare gli ingressi tra il morsetto COM e il morsetto IN. Da sinistra a destra: **NO** – contatto normalmente aperto – chiusura = allarme, apertura = ripristino; **NC** – contatto normalmente chiuso – apertura = allarme, chiusura = ripristino; **NC + EOL** – contatto normalmente chiuso con resistenza da 10 kΩ in serie – cortocircuito e interruzione = allarme, 10 kΩ = riposo; **NO + EOL** – contatto normalmente aperto con resistenza da 10 kΩ in parallelo – cortocircuito e interruzione = allarme, 10 kΩ = riposo.

3.4 Collegamento di un relè all'uscita universale

I morsetti **3 I/O** e **4 I/O**, come uscite, sono a collettore aperto con portata massima di **50 mA**: direttamente possono comandare solo la bobina di un piccolo relè. Con i contatti del relè si può accendere e spegnere a distanza qualsiasi apparecchiatura. Lo schema vale per l'alimentazione in corrente continua: un capo della bobina va al morsetto **AC/+DC**, l'altro all'uscita; in TrikdisConfig la funzione del morsetto va impostata su **Output** (punto 5.3).

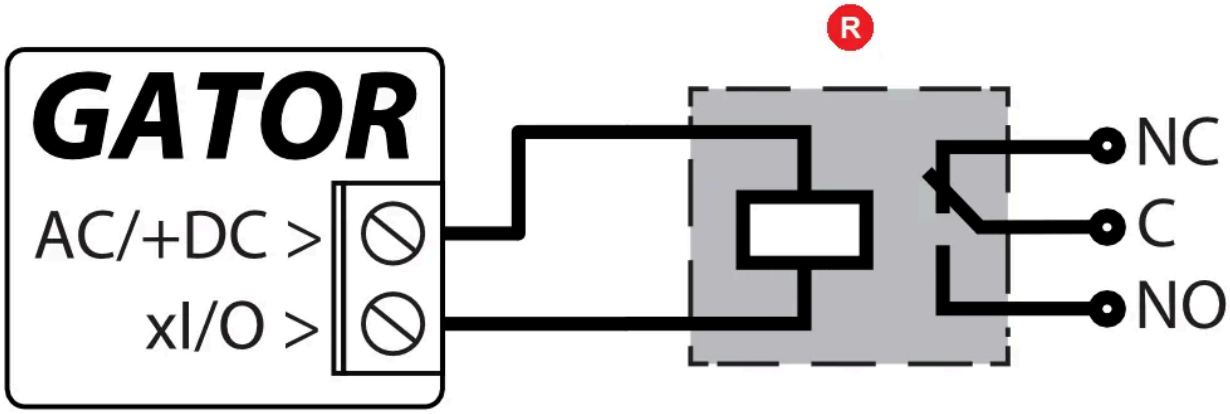


Figura 7. Relè esterno sull'uscita universale: la bobina tra AC/+DC e il morsetto 3 I/O o 4 I/O impostato come uscita; i contatti NC, C e NO del relè comandano l'apparecchiatura.

- R relè („Relay")

3.5 Collegamento dell'automazione del cancello

Esegui sempre il collegamento in assenza di tensione. I morsetti della centralina dell'automazione e la loro tensione nominale sono descritti nella documentazione del motore del cancello – lo schema mostra solo la disposizione tipica.

Il cancello viene aperto dai morsetti (di comando) **IN** e **COM** dell'automazione: qui vanno i contatti **C** e **NO** del relè del GATOR, e l'impulso del relè fa la stessa cosa del pulsante del telecomando. La maggior parte delle automazioni ha un'**uscita di stato del cancello** (OUT), che segnala se il cancello è aperto o chiuso; può essere un'uscita in tensione o un'uscita a relè. Nello schema il relè ausiliario K1 è collegato a un'automazione con uscita in tensione: con il cancello aperto tra i morsetti OUT e N dell'automazione si misurano ~230 V, il relè K1 si eccita e attiva l'ingresso **1 IN** del GATOR. Così lo stato di 1 IN segue esattamente la posizione del

cancello, che viene mostrata anche da Protegus 2 e dall'icona del widget – l'impostazione relativa si trova al punto 5.10. Con un'automazione con uscita a relè il K1 non serve, il contatto di stato si può collegare direttamente tra 1 IN e COM.

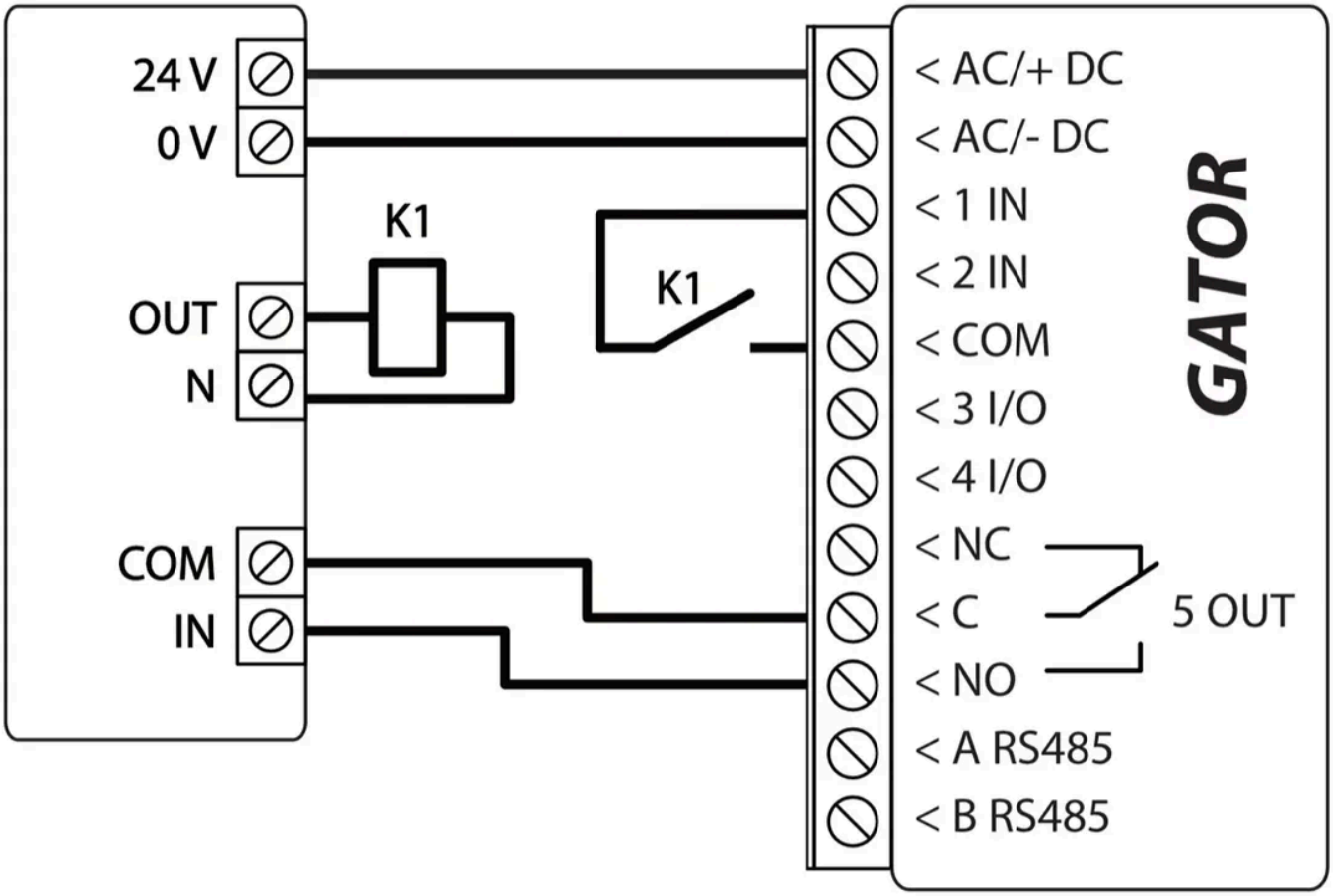


Figura 8. Collegamento tra la centralina dell'automazione del cancello („Gate control unit") e il GATOR con il relè ausiliario K1. Alimentazione („Power"): l'uscita di alimentazione a 24 V dell'automazione al morsetto AC/+DC del GATOR, lo 0 V al morsetto AC/−DC; stato del cancello („Gate status"): i morsetti OUT e N dell'automazione alla bobina del relè K1, il contatto del K1 tra i morsetti 1 IN e COM del GATOR; comando del cancello („Gate control"): il morsetto COM dell'automazione al contatto C di 5 OUT del GATOR, il morsetto IN al contatto NO di 5 OUT.

3.6 Collegamento del lettore RFID (Wiegand 26/34)

Il GATOR accetta uno o due lettori RFID con protocollo **Wiegand 26/34** (sia lettori a tessera sia lettori con tastiera a codice). Il lettore comanda l'uscita **5 OUT** con le tessere e i codici inseriti nell'elenco utenti (il permesso, la programmazione oraria e il contatore per utente valgono anche per il lettore). La configurazione del lettore si fa nella pagina **IN/OUT** di TrikdisConfig (punto 5.3), l'inserimento delle tessere nella pagina **User list** (punto 5.6); il codice colori dei fili segue lo standard Wiegand: rosso +U, nero GND, verde D0, bianco D1.

Un lettore: D0 va al morsetto **1 IN**, D1 al morsetto **2 IN**, il pulsante di uscita tra **COM** e **3 I/O**. Nel programma **Wiegand reader mode** deve essere **Single Reader** e, se c'è un pulsante di uscita, spunta la casella **IO3 as exit button (5 OUT)**: quando si preme il pulsante, 5 OUT si attiva per la durata dell'impulso impostata. Se non c'è il pulsante, la casella resta vuota.

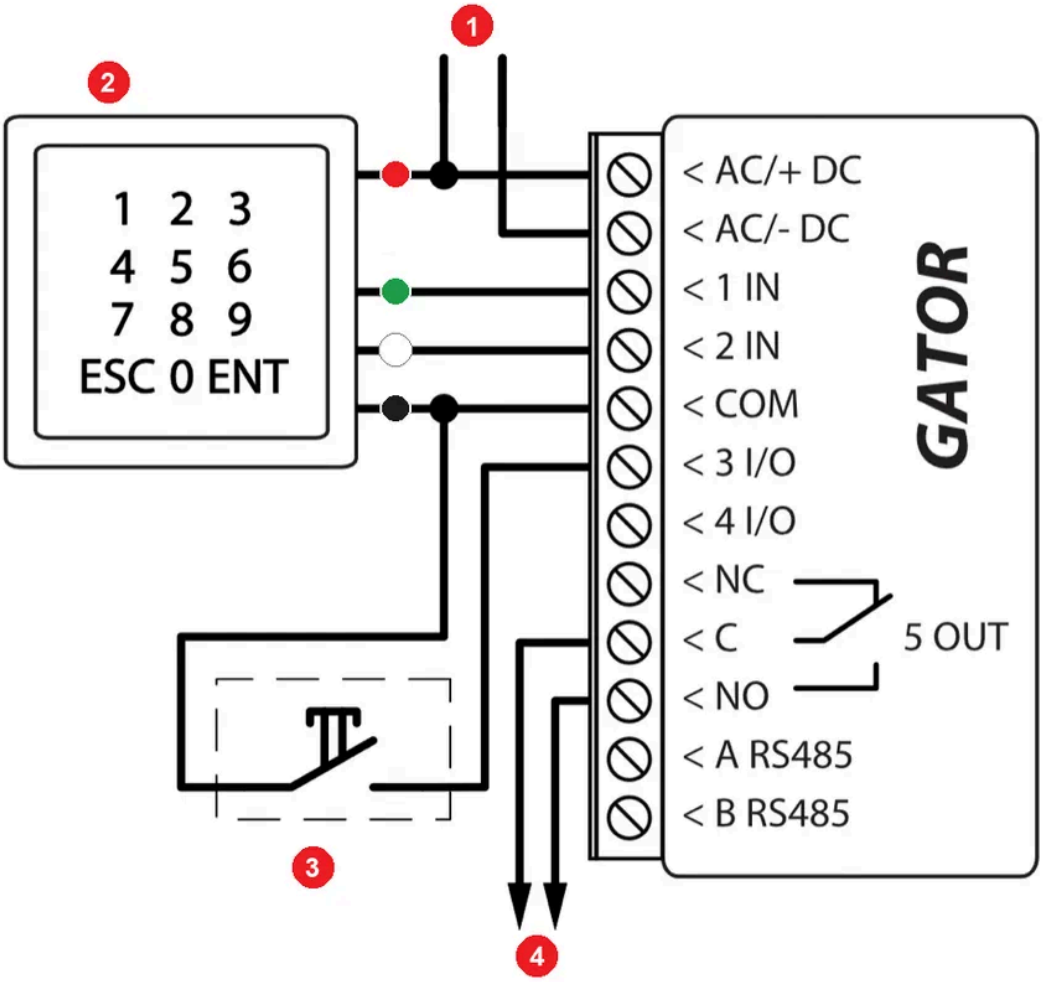


Figura 9. Collegamento di un lettore Wiegand 26/34 e del pulsante di uscita: alimentazione in corrente continua, 9–16 V, 0,5 A, ai morsetti AC/+DC e AC/−DC; del lettore di ingresso il filo rosso (+U) al morsetto AC/+DC, il verde (D0) a 1 IN, il bianco (D1) a 2 IN, il nero (GND) a COM; il pulsante di uscita tra i morsetti COM e 3 I/O; l'automazione del cancello sui contatti C e NO del relè (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 alimentatore in corrente continua („DC power supply"), 9–16 V, 0,5 A
- 2 lettore di ingresso („Entry reader") – lettore RFID con tastiera, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)")
- 3 pulsante di uscita („»Exit« button")
- 4 comando del cancello („Gate control") – l'ingresso di comando dell'automazione; portata del relè 1 A / 30 V DC, 0,5 A / 125 V AC
- filo rosso, +U („R - red (+U)")
- filo nero, GND („B - black (GND)")
- filo bianco, D1 („W - white (D1)")
- filo verde, D0 („G - green (D0)")

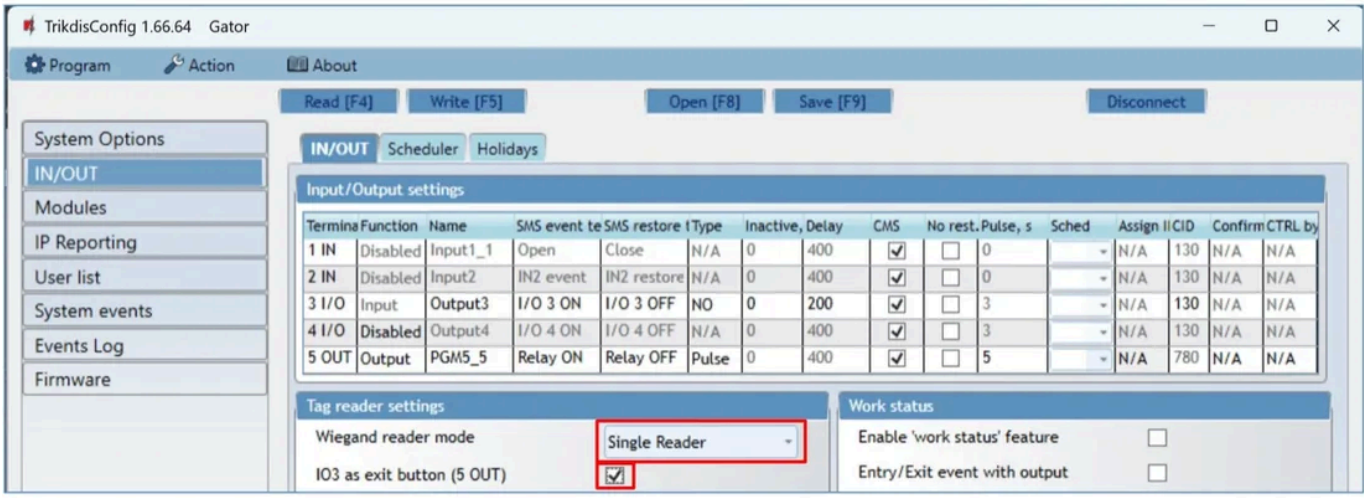


Figura 10. TrikdisConfig – IN/OUT, **Tag reader settings**: con un lettore **Wiegand reader mode = Single Reader**, con pulsante di uscita **IO3 as exit button (5 OUT)** spuntato.

Due lettori (ingresso e uscita): i fili D0 / D1 del primo lettore vanno ai morsetti **1 IN** / **2 IN**, quelli del secondo ai morsetti **3 I/O** / **4 I/O**; nel programma **Wiegand reader mode = Dual Reader**. Con due lettori il 3 I/O è occupato, il pulsante di uscita non vi si può collegare.

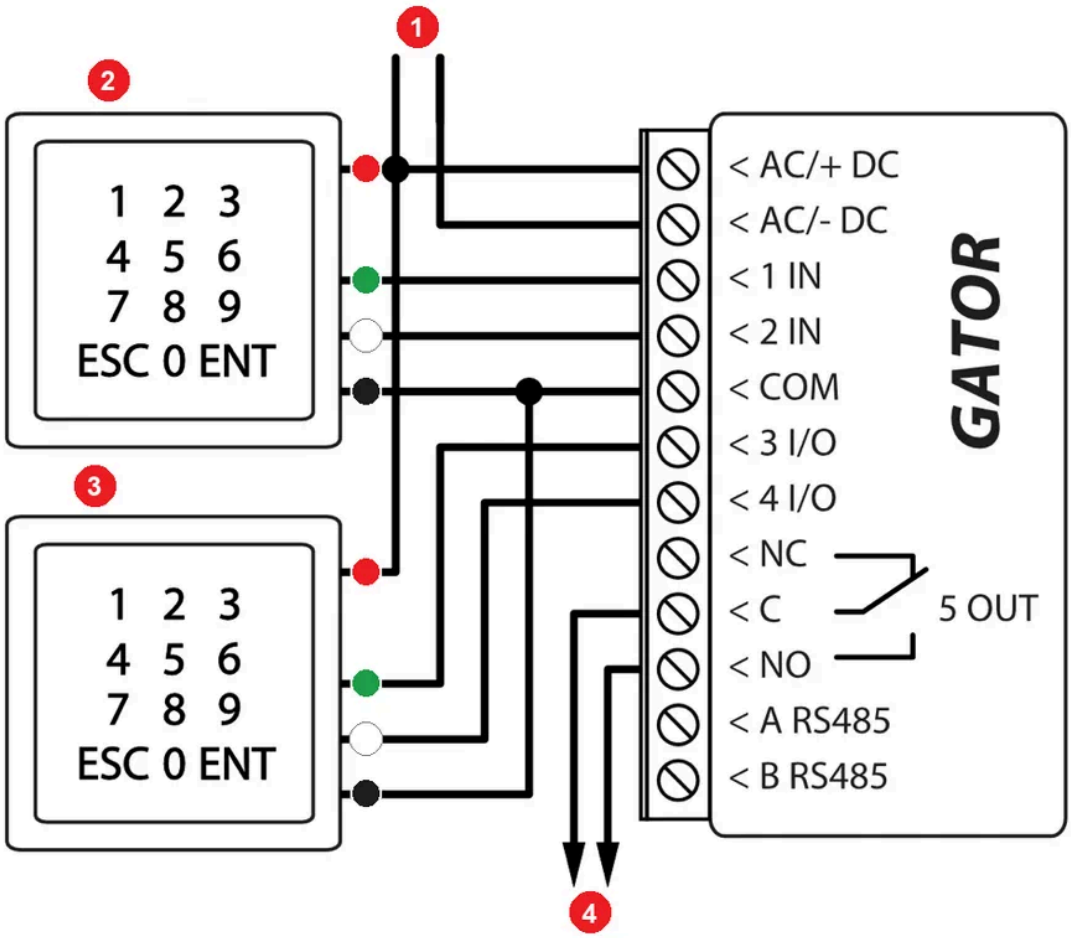


Figura 11. Collegamento di due lettori Wiegand 26/34, entrambi lettori RFID con tastiera („RFID reader with keypad (Wiegand 26/34)"): alimentazione in corrente continua, 9–16 V, 0,5 A; del lettore di ingresso il filo verde (D0) al morsetto 1 IN, il bianco (D1) a 2 IN; del lettore di uscita il filo verde (D0) al morsetto 3 I/O, il bianco (D1) a 4 I/O; di entrambi i lettori il filo rosso (+U) al morsetto AC/+DC, il nero (GND) a COM; l'automazione del cancello sui contatti C e NO del relè (1 A / 30 V DC, 0,5 A / 125 V AC).

- 1 alimentatore in corrente continua („DC power supply"), 9–16 V, 0,5 A
- 2 lettore di ingresso („Entry reader")
- 3 lettore di uscita („Exit reader")
- 4 comando del cancello („Gate control") – l'ingresso di comando dell'automazione; portata del relè 1 A / 30 V DC, 0,5 A / 125 V AC
- filo rosso, +U („R - red (+U)")
- filo nero, GND („B - black (GND)")
- filo bianco, D1 („W - white (D1)")
- filo verde, D0 („G - green (D0)")

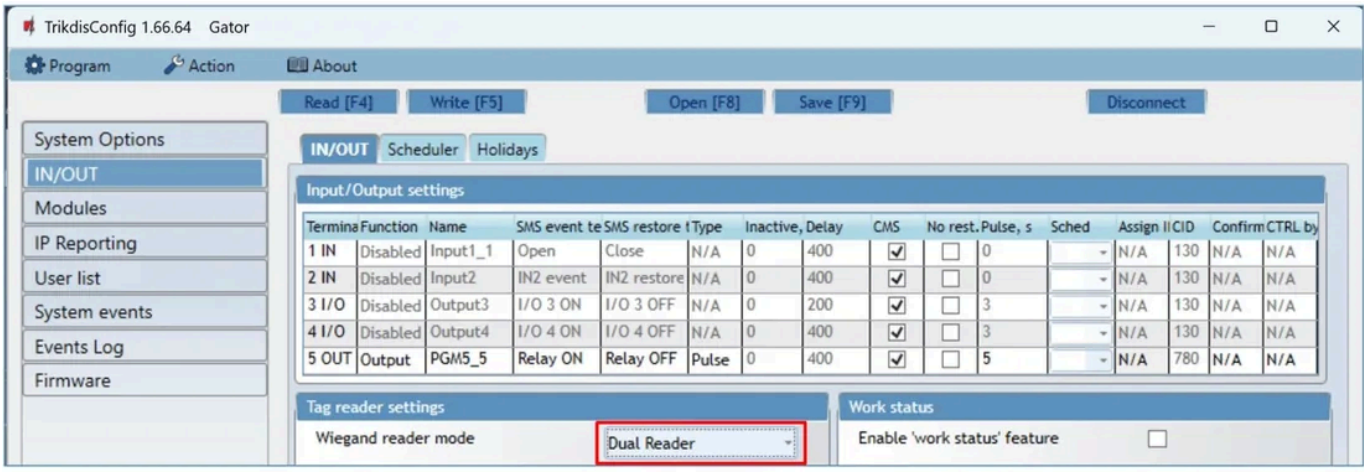


Figura 12. TrikdisConfig – IN/OUT, **Tag reader settings**: con due lettori **Wiegand reader mode = Dual Reader**.

Se il lettore ha un'uscita a 5 V (bassa tensione), spunta la casella **Low voltage reader**; se il lettore dà impulsi molto brevi e la tessera non viene riconosciuta, disattiva il filtro interno con la casella **Disable reader filter** (punto 5.3).

3.7 Modulo WiFi W485

Il modulo **W485** invia i messaggi del GATOR alla centrale di vigilanza e all'app Protegus 2 tramite la rete WiFi locale, attraverso il router Internet, così i dati mobili non si consumano. Se il WiFi si interrompe, il dispositivo passa da solo alla rete mobile e, al ritorno del WiFi, torna al W485. La funzione è disponibile dal firmware **1.06** del GATOR. Il modulo si collega al bus **RS485** (A–A, B–B), con cavo per allarme fino a **100 m al massimo**, e funziona con l'alimentazione 10–28 V DC comune con il GATOR. **Con il W485 il GATOR si può usare anche senza scheda SIM** – in questo caso si controlla solo dall'app, senza chiamate e SMS. La configurazione del modulo è al punto 5.4.

Trikdis W485 modulo WiFi (RS485)

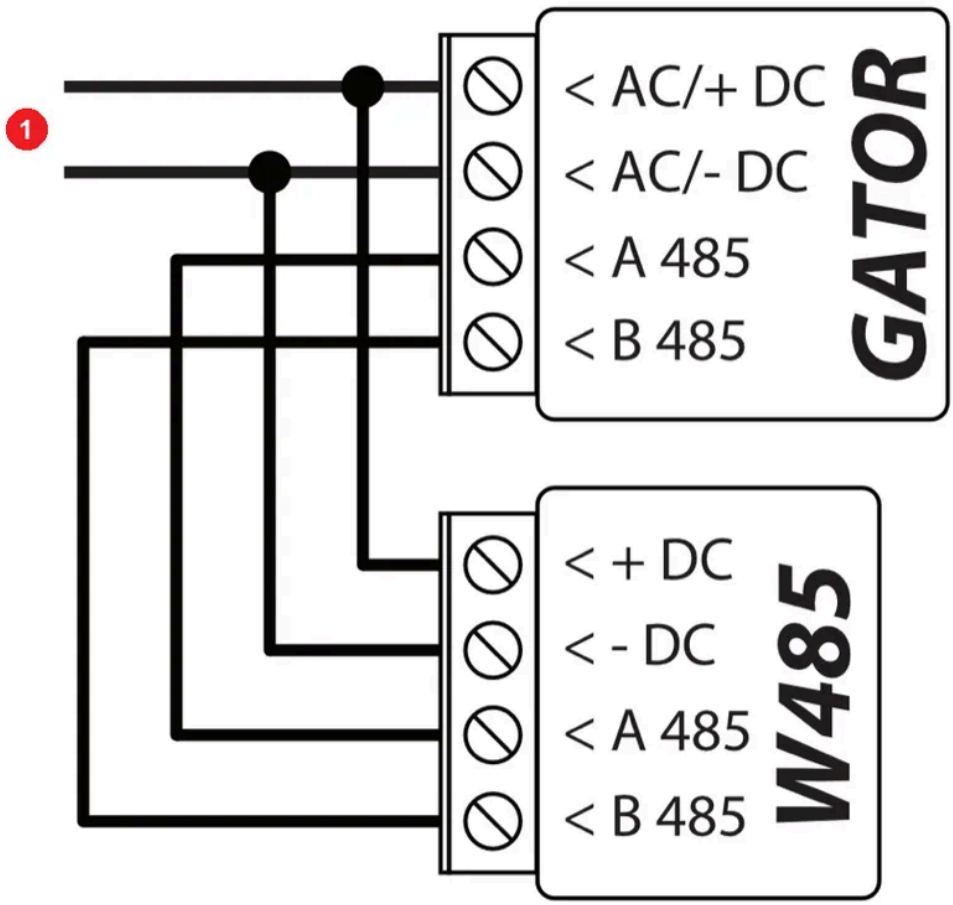


Figura 13. Collegamento del modulo W485: il polo positivo dell'alimentatore 10–28 V DC, 0,5 A ai morsetti AC/+DC del GATOR e +DC del W485, il negativo ai morsetti AC/−DC e −DC; collegamento RS485 („RS485 connection"), fino a 100 m („up to 100m"): A 485 – A 485, B 485 – B 485.

- 1 alimentatore („Power supply"), 10–28 V DC, 0,5 A

Le distanze «fino a … m» sono valori massimi teorici, raggiungibili in condizioni ideali. In pratica la qualità e il percorso del cavo, le fonti di disturbo e, nei collegamenti radio, i muri e il terreno danno una portata nettamente inferiore. Prevedi un margine e, sulle lunghe distanze, verifica il collegamento alla messa in servizio.

3.8 Modulo Ethernet E485

Il modulo **E485** fa la stessa cosa con Internet cablato: i messaggi del GATOR vanno alla centrale di vigilanza e all'app Protegus 2 attraverso il cavo Ethernet collegato al router, il dispositivo non usa Internet mobile e la rete mobile è solo di riserva: se Internet cablato si interrompe, invia i messaggi tramite Internet mobile e, al ritorno della connessione cablata, di nuovo tramite l'E485. Dal firmware **1.06**; bus RS485 fino a 100 m; alimentazione comune 10–28 V DC; si può usare anche senza scheda SIM. Configurazione al punto 5.4.

Trikdis E485 modulo Ethernet (RS485)

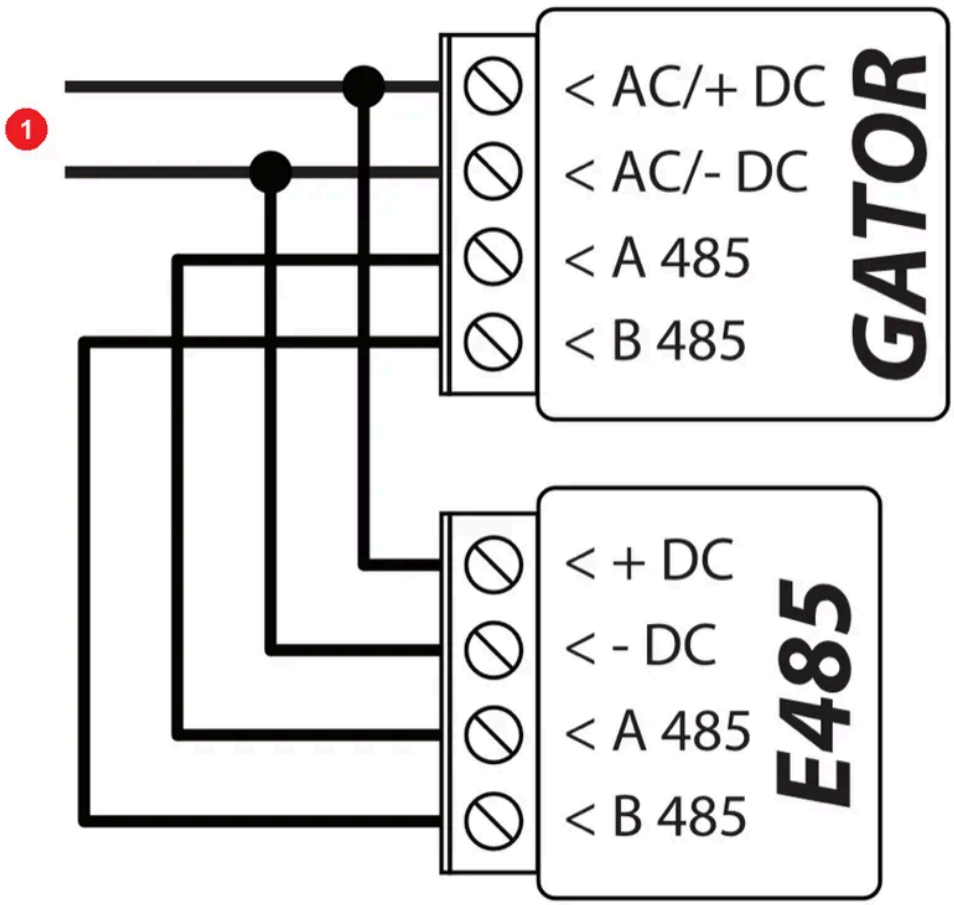


Figura 14. Collegamento del modulo E485: il polo positivo dell'alimentatore 10–28 V DC, 0,5 A ai morsetti AC/+DC del GATOR e +DC dell'E485, il negativo ai morsetti AC/−DC e −DC; collegamento RS485 („RS485 connection"), fino a 100 m („up to 100m"): A 485 – A 485, B 485 – B 485.

- 1 alimentatore („Power supply"), 10–28 V DC, 0,5 A

Le distanze «fino a … m» sono valori massimi teorici, raggiungibili in condizioni ideali. In pratica la qualità e il percorso del cavo, le fonti di disturbo e, nei collegamenti radio, i muri e il terreno danno una portata nettamente inferiore. Prevedi un margine e, sulle lunghe distanze, verifica il collegamento alla messa in servizio.

3.9 Moduli di espansione RF-LORA e iO-LORA con lettore RFID

Dal firmware **2.13** del GATOR il sistema si può espandere senza fili: il ricetrasmettitore **RF-LORA** si collega al bus RS485 e mantiene via radio la connessione con fino a **8 moduli di espansione iO-LORA** (in campo aperto fino a 5000 m). Ogni modulo iO-LORA aggiunge al GATOR un ingresso e un'uscita a relè, e vi si può collegare un proprio lettore RFID Wiegand 26/34: il lettore comanda **solo l'uscita a relè del proprio modulo**, non un'uscita remota. Così con un GATOR si possono controllare fino a 8 cancelli o barriere lontani tra loro, ciascuno con il proprio lettore di tessere e il proprio pulsante di uscita – i dettagli della soluzione: Controllo accessi flessibile e senza fili con il sistema GATOR RF-LoRa.

Trikdis RF-LORA modulo di espansione wireless

Trikdis IO-LORA modulo di espansione wireless

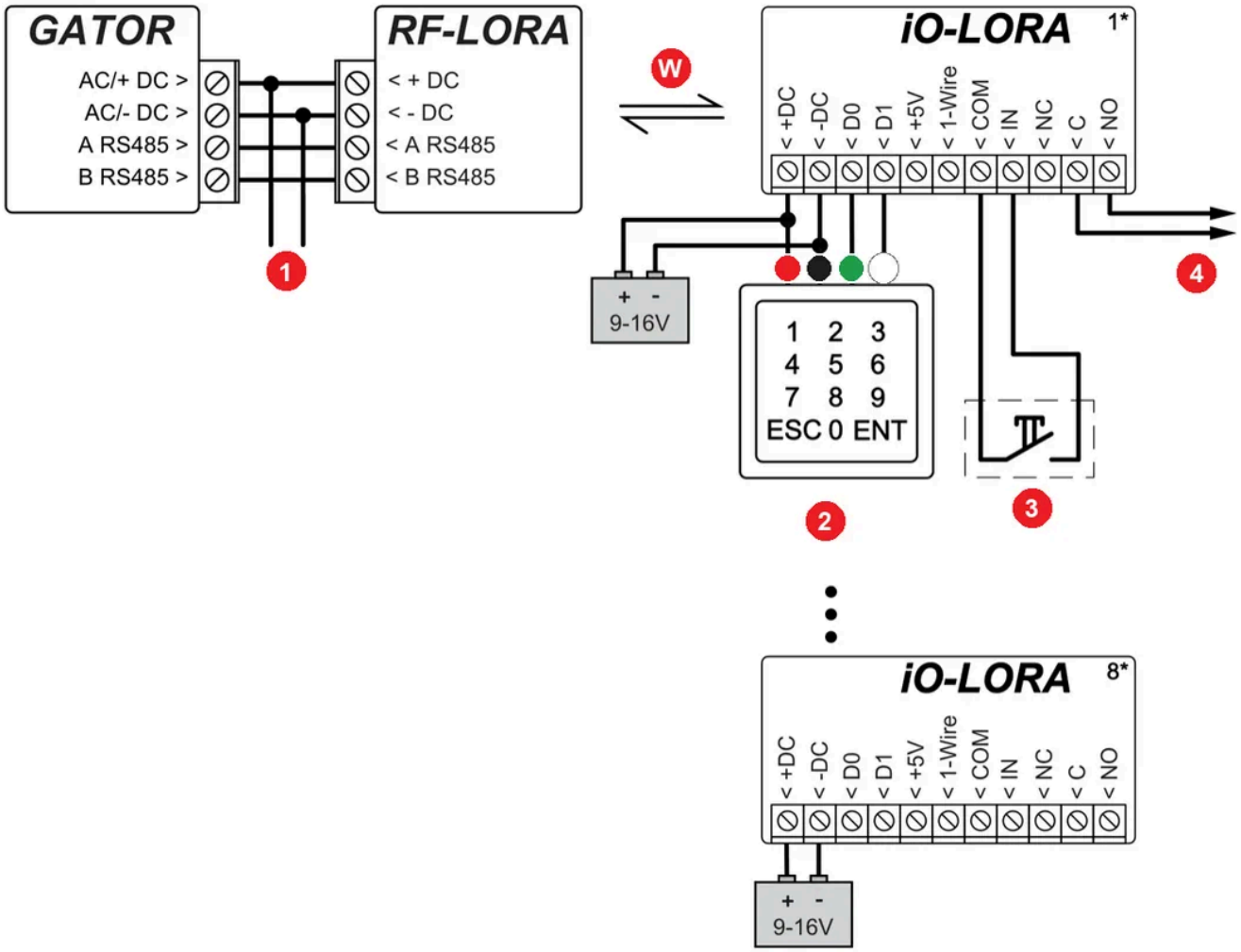


Figura 15. Ricetrasmettitore RF-LORA sul GATOR e moduli di espansione iO-LORA con lettore RFID: alimentazione comune 9–16 V DC, 0,5 A per il GATOR e l'RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A–A, B–B; collegamento radio tra l'RF-LORA e i moduli iO-LORA 1...8, fino a 5000 m; ogni iO-LORA riceve una propria alimentazione 9–16 V; il lettore sull'iO-LORA: rosso (+U) al morsetto +DC, nero (GND) a −DC, verde a D0, bianco a D1; pulsante di uscita tra i morsetti COM e IN dell'iO-LORA; l'automazione del cancello sui contatti C e NO del relè dell'iO-LORA (2 A / 230 V AC).

- 1 alimentatore in corrente continua („DC power supply"), 9–16 V, 0,5 A
- W collegamento senza fili („Wireless connection"), fino a 5000 m („up to 5000 m")
- 2 lettore RFID con tastiera, Wiegand 26/34 („RFID reader with keypad (Wiegand 26/34)")
- 3 pulsante di uscita („»Exit« button")
- 4 comando del cancello („Gate control") – l'ingresso di comando dell'automazione; portata del relè dell'iO-LORA 2 A / 230 V AC
- filo rosso, +U („R - red (+U)")
- filo nero, GND („B - black (GND)")
- filo verde, D0 („G - green (D0)")
- filo bianco, D1 („W - white (D1)")

Le distanze «fino a ... m» sono valori massimi teorici, raggiungibili in condizioni ideali. In pratica la qualità e il percorso del cavo, le fonti di disturbo e, nei collegamenti radio, i muri e il terreno danno una portata nettamente inferiore. Prevedi un margine e, sulle lunghe distanze, verifica il collegamento alla messa in servizio.

Configurazione in TrikdisConfig (la descrizione delle finestre è nel capitolo 5):

1. Avvia TrikdisConfig, collega il GATOR al computer con il cavo USB Mini-B oppure accedi a distanza, e leggi le impostazioni (**Read [F4]** – il programma mostra le impostazioni attuali del dispositivo). Se il programma lo chiede, inserisci nella finestra che compare il codice di 6 cifre dell'amministratore o

dell'installatore. Nella pagina **Modules** scegli dall'elenco la voce **iO-LORA controller** e nel campo **Serial No.** scrivi il numero di serie a sei cifre del modulo (sull'etichetta del modulo). L'RF-LORA non va aggiunto separatamente.



Figura 16. TrikdisConfig – Modules: il modulo iO-LORA selezionato, nel campo **Serial No.** va il numero di serie.

2. Per ogni modulo iO-LORA aggiunto compaiono nell'elenco della pagina **IN/OUT** un ingresso (per esempio **6 IN iO-LORA 1**) e un'uscita (**7 OUT iO-LORA 1**). La funzione dell'ingresso deve essere **Exit button** (qui i morsetti IN e COM del modulo collegano il pulsante di uscita): quando lo si preme, il relè del modulo (nell'esempio **7 OUT**) si attiva per la durata dell'impulso impostata. Il tipo dell'uscita è **Pulse**, la durata dell'impulso adatta all'automazione del cancello (nell'esempio 3 s).

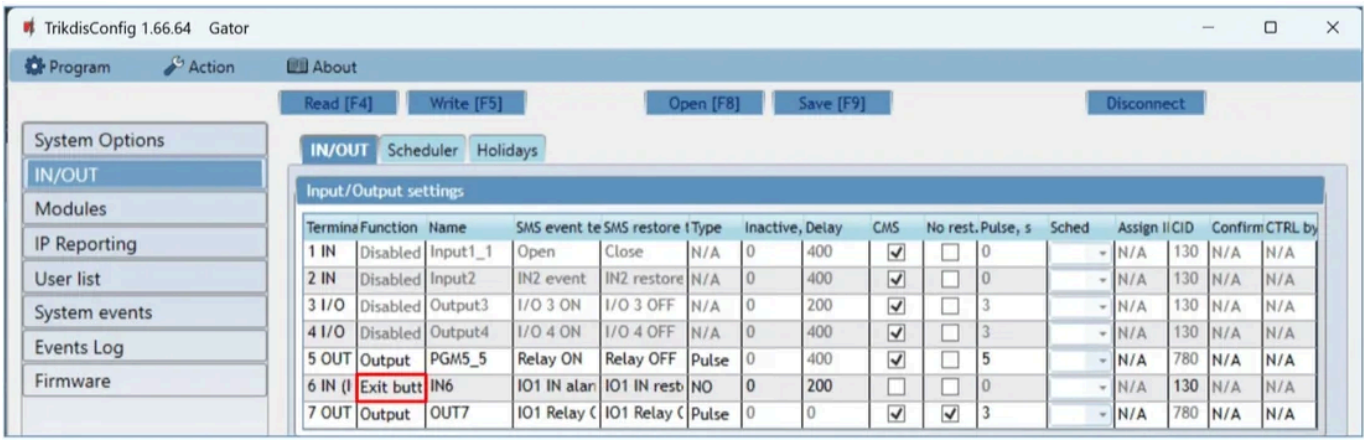


Figura 17. TrikdisConfig – IN/OUT: la funzione di **6 IN** è **Exit button**, l'uscita **7 OUT** è di tipo **Pulse**, con impulso di 3 s.

3. Nella pagina **User list** inserisci il nome dell'utente, il numero della tessera RFID (**Phone/RFID**), con un lettore a codice il codice, spunta la casella **En** e indica quale uscita può controllare (nell'esempio la 7). Scrivi le impostazioni (**Write [F5]**), attendi la fine dell'aggiornamento, poi **Disconnect** e scollega il cavo USB.

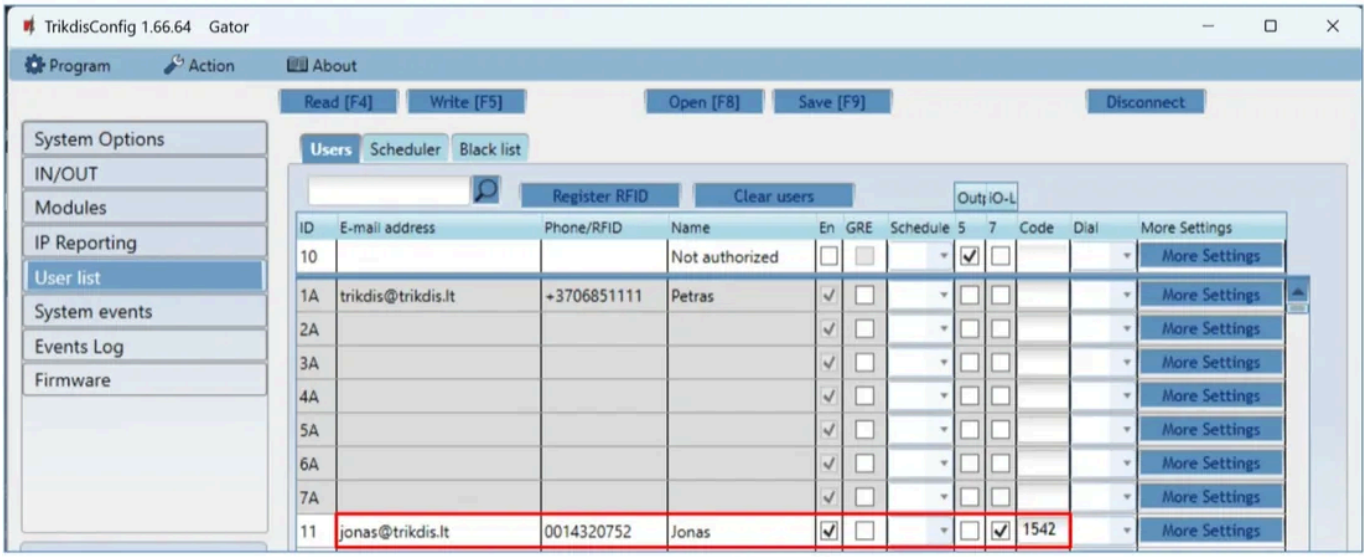


Figura 18. TrikdisConfig – User list: per l'utente sono compilati il numero RFID, il nome e il codice, **En** spuntato, l'uscita 7 contrassegnata.

4. **Verifica:** attiva l'uscita con la tessera o con il codice, poi premi il pulsante di uscita – entrambe le volte il relè deve eccitarsi per la durata dell'impulso impostata.

3.10 Moduli di espansione iO8 e iO8-LORA

Se in un punto ti servono più ingressi o uscite, al GATOR si può collegare **un** modulo di espansione **iO8** (cablato, RS485) oppure **iO8-LORA** (senza fili, tramite l'RF-LORA). Gli ingressi e le uscite del modulo compaiono nell'elenco della pagina **IN/OUT** e si gestiscono come quelli del GATOR; il modulo va aggiunto nella pagina **Modules** con il suo numero di serie (punto 5.4).

Trikdis iO8 modulo di espansione cablato | **Trikdis IO8-LORA modulo di espansione wireless**

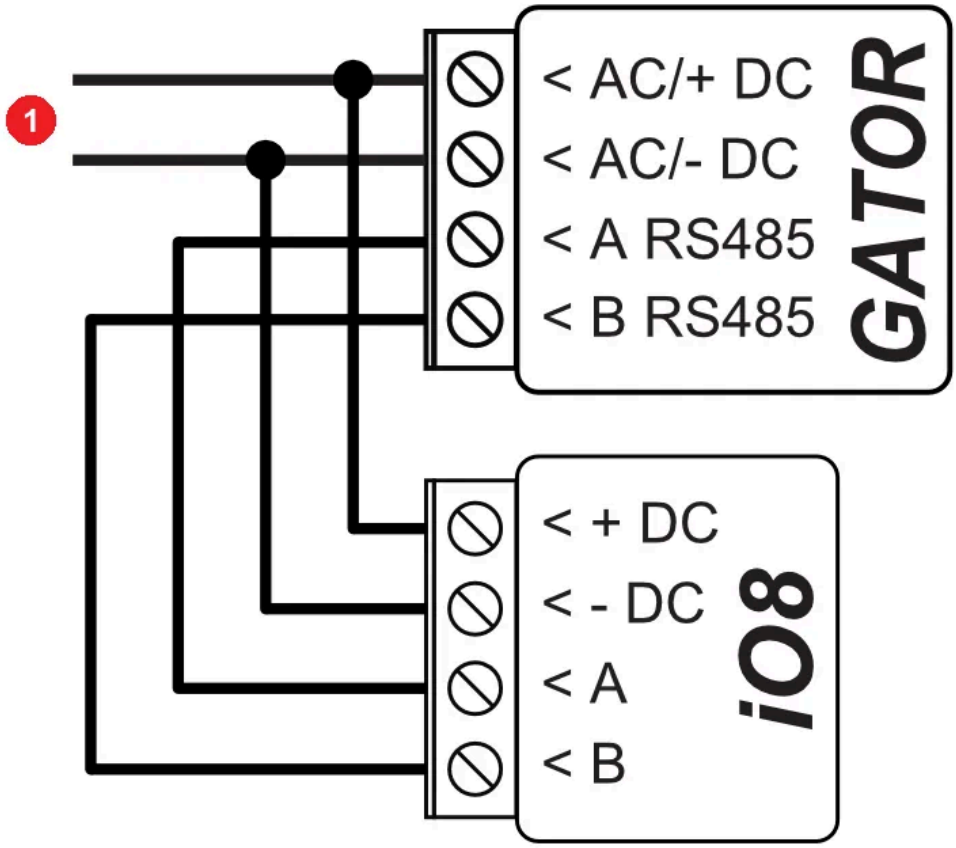


Figura 19. Collegamento del modulo di espansione iO8: il polo positivo dell'alimentatore 10–28 V DC, 0,5 A ai morsetti AC/+DC del GATOR e +DC dell'iO8, il negativo ai morsetti AC/−DC e −DC; collegamento RS485 („RS485 connection"), fino a 100 m („up to 100m"): il morsetto A RS485 del GATOR al morsetto A dell'iO8, B RS485 al morsetto B.

- 1 alimentatore („Power supply"), 10–28 V DC, 0,5 A

L'iO8 funziona a 10–26 V DC: se l'alimentatore fornisce una tensione superiore a 26 V, l'iO8 riceve un alimentatore separato, collegando tra loro i poli negativi delle due alimentazioni.

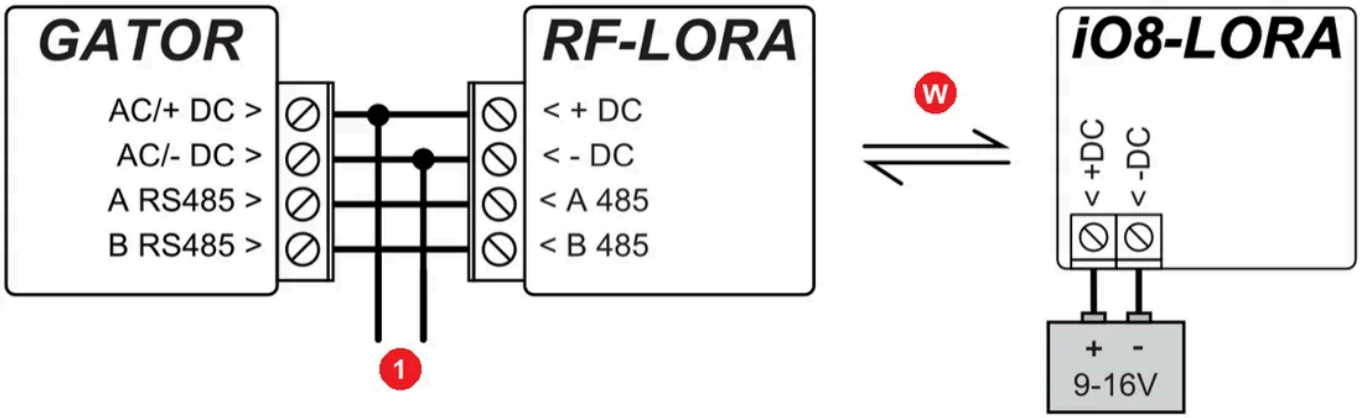


Figura 20. Il modulo di espansione iO8-LORA tramite il ricetrasmettitore RF-LORA: alimentazione 9–16 V DC, 0,5 A per il GATOR e l'RF-LORA (AC/+DC – +DC, AC/−DC – −DC); RS485: A RS485 – A 485, B RS485 – B 485; collegamento radio tra l'RF-LORA e l'iO8-LORA, fino a 5000 m; l'iO8-LORA riceve una propria alimentazione 9–16 V.

- 1 alimentatore in corrente continua („DC power supply"), 9–16 V, 0,5 A
- W collegamento senza fili („Wireless connection"), fino a 5000 m („up to 5000 m")

Le distanze «fino a … m» sono valori massimi teorici, raggiungibili in condizioni ideali. In pratica la qualità e il percorso del cavo, le fonti di disturbo e, nei collegamenti radio, i muri e il terreno danno una portata nettamente inferiore. Prevedi un margine e, sulle lunghe distanze, verifica il collegamento alla messa in

servizio.

4. Controllo a distanza

Puoi controllare il GATOR in quattro modi: con una **chiamata telefonica** (gratuita, perché il dispositivo non risponde alla chiamata), durante la chiamata con la **tastiera del telefono** (DTMF), dall'app **Protegus 2** o con un **widget** messo nella schermata iniziale del telefono, e con un **comando SMS**. In tutti e quattro i modi è l'elenco utenti (punto 5.6) a decidere chi può fare cosa; con i comandi SMS l'amministratore può anche modificare le impostazioni.

4.1 Controllo con chiamata telefonica

Chiama il numero della scheda SIM inserita nel GATOR. Il dispositivo **rifiuta automaticamente** la chiamata e attiva l'uscita a relè **5 OUT** per **3 secondi** – la chiamata non costa nulla. Di fabbrica chiunque conosca il suo numero può controllare il dispositivo in questo modo.

- **Solo le persone autorizzate**: se inserisci nell'elenco utenti anche un solo numero (via SMS: `SETU …`, punto 4.7; in TrikdisConfig o nell'app), il GATOR reagisce solo alle chiamate dai numeri presenti nell'elenco. In TrikdisConfig la stessa cosa è comandata dalla casella **En** della voce numero 10 della **User list**, chiamata **Not authorized** (punto 5.6): spuntata, può chiamare chiunque; vuota, solo i membri dell'elenco.
- **Quale uscita apre**: se un utente può controllare più uscite, alla chiamata si attivano le uscite contrassegnate nella colonna **Dial**, dopo di che il dispositivo chiude la chiamata.
- **Durata della chiamata**: con il valore **System Options** → **Hang-up after** a 0 il dispositivo rifiuta subito la chiamata; con un valore maggiore risponde e chiude dopo il tempo indicato – questo serve per il controllo con la tastiera (punto 4.2).

Chi **per primo** chiama il GATOR in stato di fabbrica, o per primo gli invia un SMS, diventa l'**amministratore** del dispositivo: da quel momento solo lui può gestirlo con i comandi SMS. Per questo fai la prima chiamata dal telefono del proprietario o dell'installatore.

4.2 Controllo con la tastiera del telefono (DTMF)

Se il GATOR risponde alla chiamata (**Hang-up after** maggiore di 0), l'utente può comandare più uscite con la tastiera del telefono:

1. Chiama il numero della scheda SIM del GATOR – il dispositivo risponde alla chiamata.
2. Digita il comando sulla tastiera del telefono secondo la tabella.

Codice DTMF	Funzione	Descrizione
`USCITA*STATO#`	controllo dell'uscita	**USCITA** – il numero dell'uscita. **STATO** – 0: spegnimento; 1: accensione; 2: spegnimento per la durata dell'impulso; 3: accensione per la durata dell'impulso (la durata dell'impulso si imposta nella tabella **IN/OUT** di TrikdisConfig). **#** – fine del comando. Esempio – accensione dell'uscita 5: `5*1#`; accensione dell'uscita 4 per la durata dell'impulso: `4*3#`
`#`	fine del comando	se hai sbagliato il comando, premi il tasto **#** e digitalo di nuovo

Il controllo con la tastiera (DTMF) non funziona sui dispositivi con codice tipo **GV17_2E70** e **GV17_2S70**. Il tipo esatto lo vedi nella barra di stato di TrikdisConfig (punto 5.1).

4.3 Controllo dall'app Protegus 2

In Protegus 2 l'utente apre il cancello da qualsiasi luogo, vede lo stato del sistema e lo stato del cancello (se lo stato del cancello è collegato, punti 3.5 e 5.10), riceve tutti gli eventi del sistema come notifiche push e, come amministratore, gestisce anche gli utenti. L'app è gratuita; sul telefono la scarichi dagli store, nel browser si apre all'indirizzo https://web.protegus.app.

Prima di aggiungere il sistema

In TrikdisConfig, nella pagina **IP Reporting**, deve essere spuntato **Enable cloud service** (punto 5.5; via SMS: `CONNECT 123456 PROTEGUS=ON`), l'alimentazione deve essere corretta (il LED **POWER** lampeggia in verde) e il dispositivo deve essere in rete (il LED **NETWORK** è acceso in verde e lampeggia in giallo). Sulla scheda SIM deve esserci il servizio dati mobile, oppure deve esserci un modulo W485 / E485.

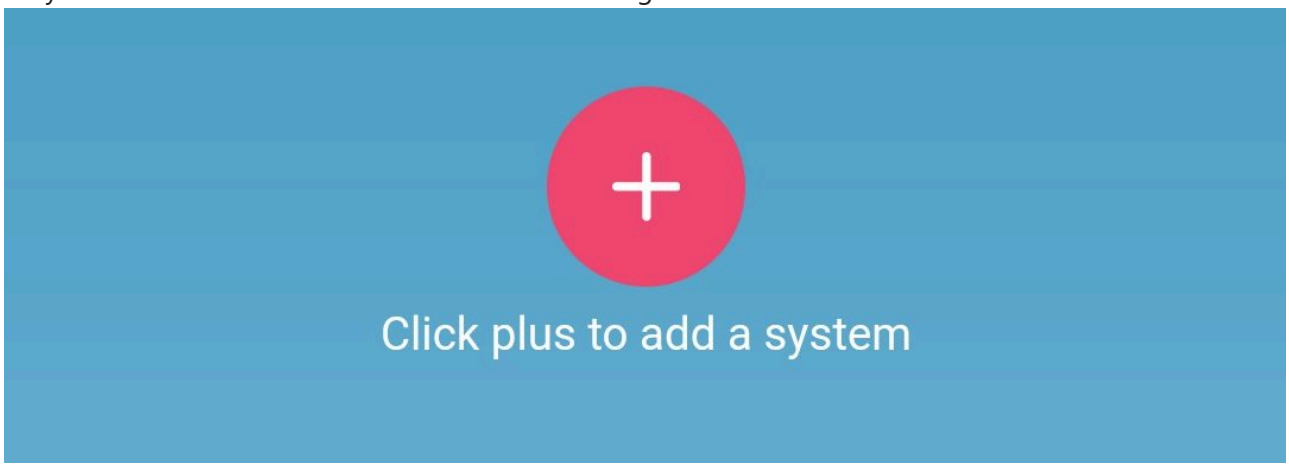
Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

A rendszer létrehozása a Protegus 2 alkalmazásban

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



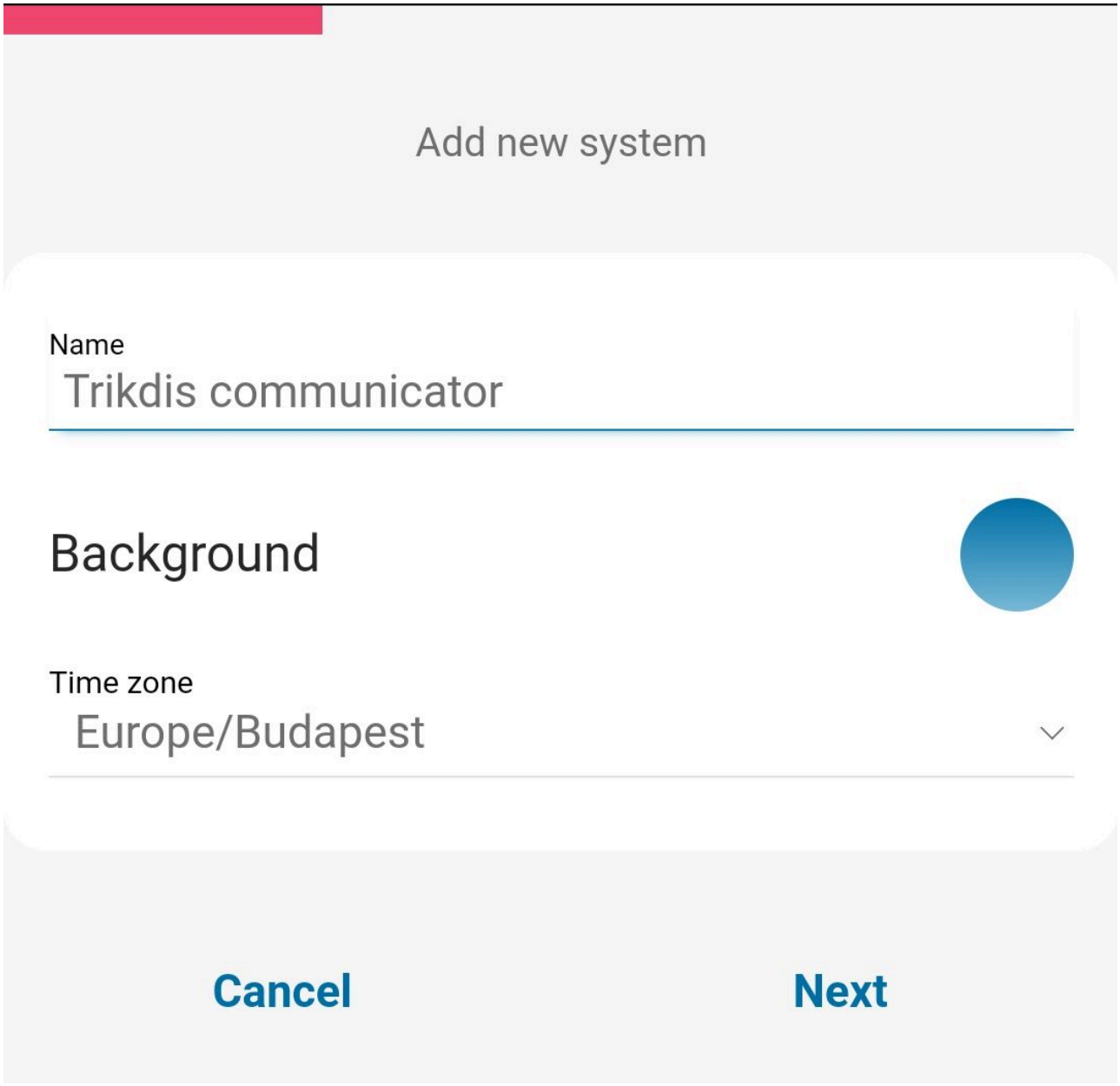
2. Regisztrálj egy fiókot, ha még nincs.
3. Lépj be a fiókba.
4. A nyitó oldalon kattints a "+" Rendszer létrehozása gombra



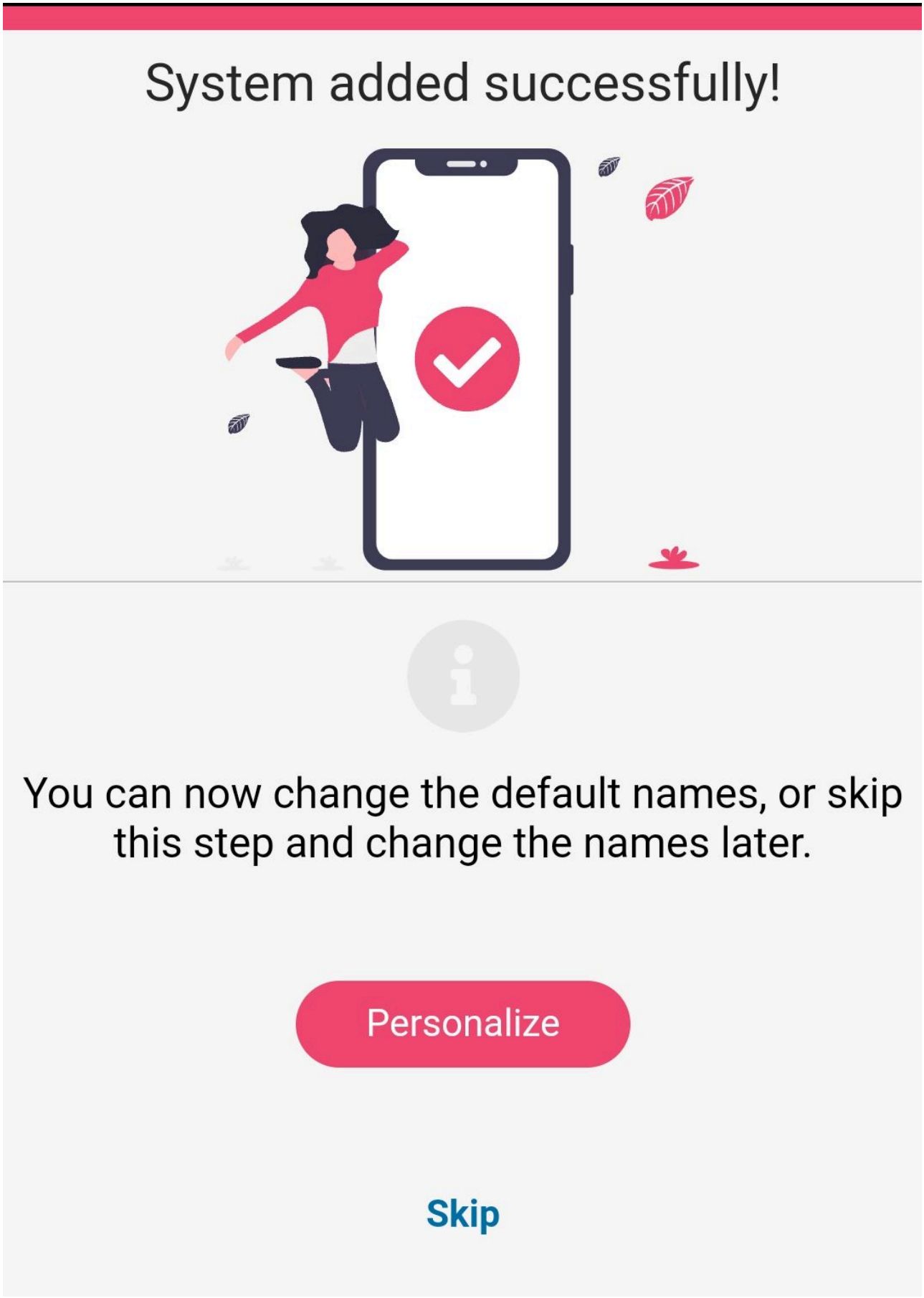
5. Add meg az egyedi azonosítóját a Trikdis eszköznek (telefonon a kamerával is beolvashatod a vonalkódot vagy QR kódot), amit megtalálsz
    - Az eszközön található matricán
    - Az eszköz papírdobozán
    - A TrikdisConfig bal alsó sarkában (kijelölhető és másolható formátumban)



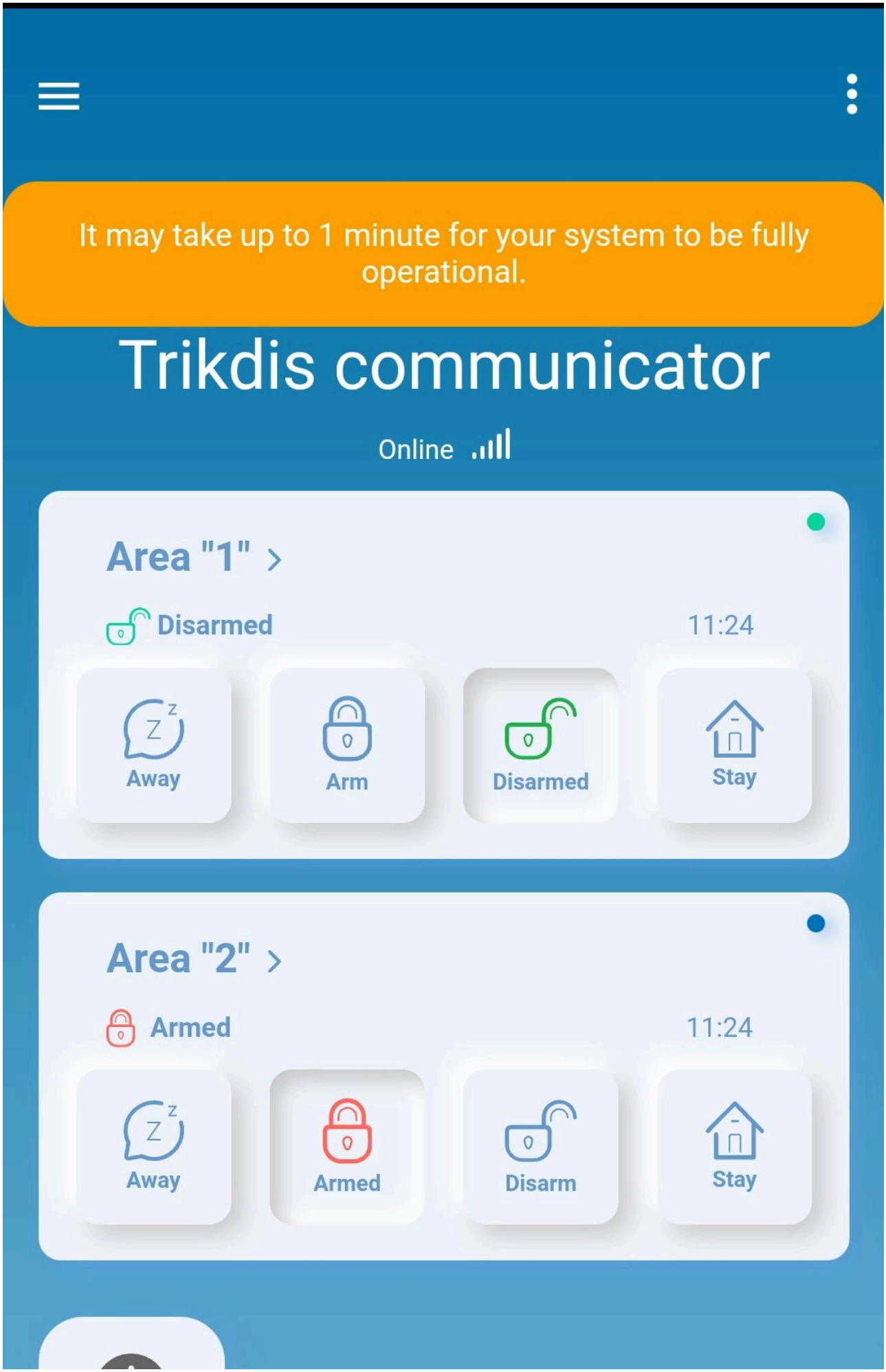
6. Add meg a rendszer nevét és válassz idozónát



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



Con il GATOR, durante l'aggiunta fai attenzione a questi punti:

1. L'identificativo univoco è il numero **IMEI** del GATOR: si trova sull'etichetta sul fondo del dispositivo e sulla scatola, e lo vedi anche nella barra di stato di TrikdisConfig; puoi leggere il codice QR dell'etichetta anche con la fotocamera del telefono. Se l'installatore ha cambiato il valore di fabbrica `123456` del **Cloud Access Code**, l'app chiede anche quello.
2. Dopo aver inserito il nome del sistema, puoi saltare il passo **Personalize** con il pulsante **Skip**: i nomi delle uscite e degli ingressi li puoi modificare anche in seguito.
3. Attendi che la scritta su sfondo giallo scompaia – il sistema diventa operativo entro 1 minuto al massimo.

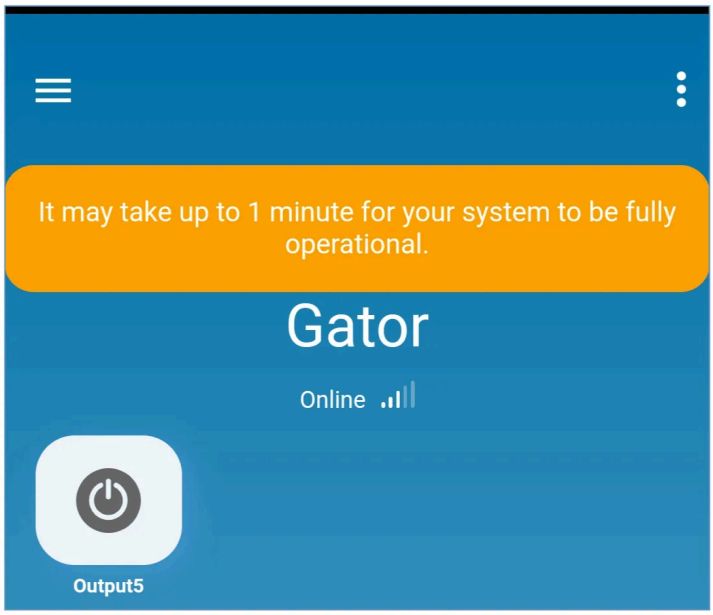


Figura 21. Il GATOR in Protegus 2 dopo l'aggiunta: il sistema è **Online**, la barra gialla indica che bisogna attendere al massimo 1 minuto prima del funzionamento completo.

4. Il cancello si apre con il pulsante **Output5**. **Suggerimento:** tieni premuto il pulsante, scegli la modifica, poi tocca l'icona e scegline una adatta all'uso (cancello, barriera, garage) e salva. Se lo stato del cancello è collegato, l'icona mostra anche lo stato aperto e chiuso del cancello.

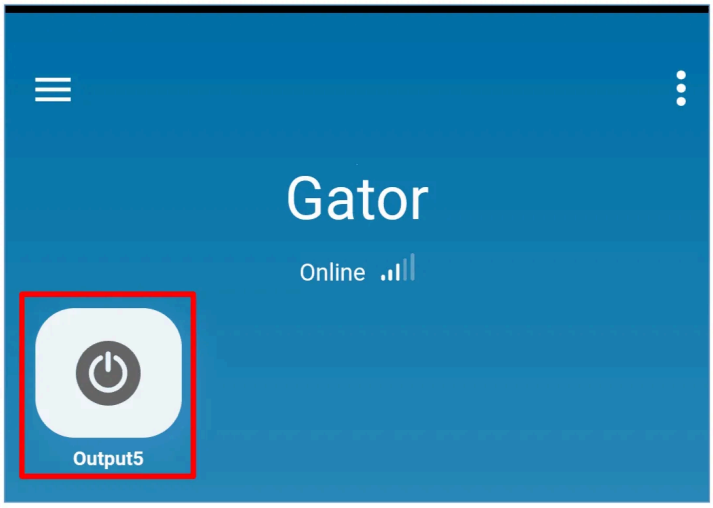


Figura 22. La schermata iniziale del sistema con il pulsante **Output5** – questo comanda il relè del GATOR.

Vedi anche

Il dispositivo per l'automazione dei cancelli GV17 si può usare con Protegus 2 · App Protegus per Android / iPhone e web · Notifiche push nel browser nell'app Protegus 2

4.4 Widget nella schermata iniziale del telefono

Il pulsante di apertura del cancello lo puoi mettere anche nella schermata iniziale del telefono, così apri con un solo tocco, senza aprire l'app. Funziona **solo su Android**; il modo di posizionare il widget può variare un po' da telefono a telefono. Il GATOR deve essere aggiunto a Protegus 2 e devi aver effettuato l'accesso all'app; poi chiudi la finestra dell'app.

1. Tieni premuta una parte vuota della schermata iniziale e, nella barra che compare, scegli la voce **Widget**.
2. Cerca nell'elenco **Protegus 2** e scegli il widget **Switch Protegus 2**.
3. Scegli l'uscita da controllare (per esempio **Gator Output5**) e premi il pulsante **ADD WIDGET**.
4. Il pulsante compare nella schermata iniziale. Provalo: torna alla schermata iniziale e premi il pulsante – dopo averlo premuto, un indicatore circolare mostra che l'uscita si è attivata; con lo stato del cancello collegato, il colore del pulsante mostra lo stato aperto e chiuso del cancello.



Figura 23. Passo 1 – dopo aver tenuto premuta la schermata iniziale, la voce di menu **Widget**.

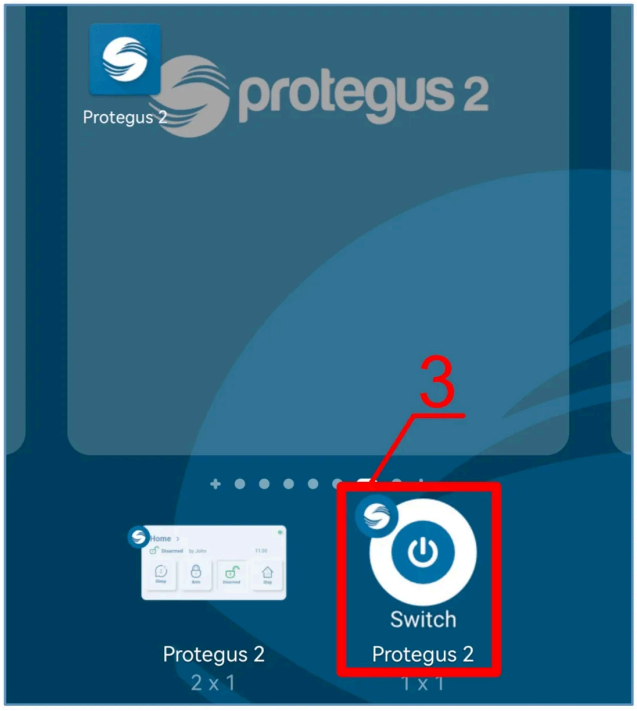


Figura 24. Passo 2 – tra i widget di Protegus 2, **Switch Protegus 2**.



Figura 25. Passo 3 – la scelta dell'uscita **Gator Output5** e il pulsante **ADD WIDGET**.



Figura 26. Passo 4 – il widget **Output5** nella schermata iniziale; il pulsante verde indica l'uscita attiva (cancello aperto).

4.5 Gestione degli utenti nell'app

Come amministratore puoi aggiungere e cancellare utenti anche in Protegus 2; l'utente aggiunto vede e apre il cancello dal proprio account, e può ricevere notifiche anche via SMS (se il messaggio di benvenuto **HELLO** è attivo, riceve un SMS sull'aggiunta).

1. Avvia l'app Protegus 2 sul telefono e accedi con il tuo nome utente e la tua password. Nella schermata del sistema apri il menu **Settings** (impostazioni), poi la voce **System configuration**.
2. Scegli l'elenco **Users** (utenti) e premi il pulsante **+** (**Add new user** – nuovo utente).
3. Inserisci l'**indirizzo e-mail**, il **nome** e il **numero di telefono** dell'utente (oppure il numero della tessera RFID, punto 5.6), con un lettore a codice il suo **codice** di 4 cifre, e indica quale uscita può controllare (**Output5**).
4. Premi il pulsante **Add user** (aggiungi utente): il nuovo utente compare nell'elenco. Con il pulsante **Back** torni alla finestra principale.

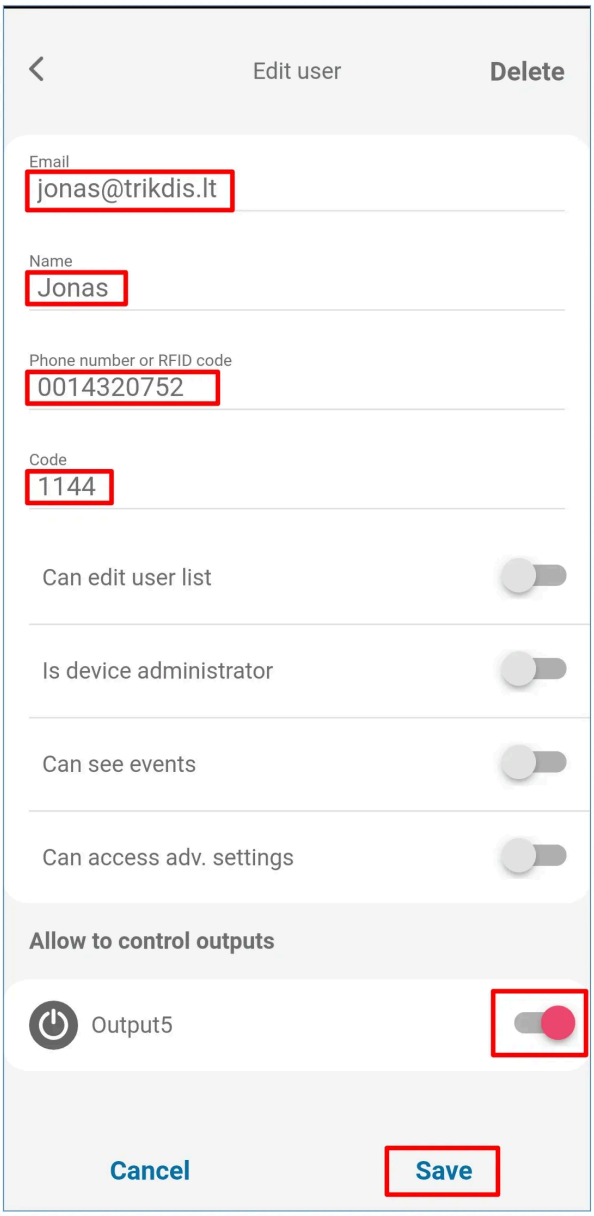


Figura 27. Modifica di un utente in Protegus 2: indirizzo e-mail, nome, numero di telefono o numero della tessera RFID, codice e autorizzazione al controllo di **Output5**.

4.6 Controllo con messaggio SMS

L'uscita a relè (**OUTPUT5**) la comandi con questi comandi SMS; `xxxxxx` è la password di 6 cifre dell'amministratore (di fabbrica `123456`). Via SMS puoi comandare anche altre uscite, ma prima vanno impostate come uscite in TrikdisConfig (punto 5.3).

Comando	Parametro	Descrizione
`OUTPUTx xxxxxx ON`	ON	accensione dell'uscita; **x** è il numero dell'uscita. Esempio: `OUTPUT5 123456 ON`
`OUTPUTx xxxxxx OFF`	OFF	spegnimento dell'uscita. Esempio: `OUTPUT5 123456 OFF`
`OUTPUTx xxxxxx PULSE=ttt`	PULSE=ttt	accensione dell'uscita per **ttt** secondi (1–999, con tre cifre). Esempio: `OUTPUT5 123456 PULSE=002`

4.7 Programmazione via SMS

Il dispositivo accetta i comandi SMS solo dai numeri degli **amministratori** (1A–7A); ogni comando contiene la password di 6 cifre dell'amministratore. Il dispositivo invia un SMS di risposta sull'esecuzione, se per l'amministratore è attivo **ACK for SMS message** (punto 5.6).

Cambio della password dell'amministratore – per motivi di sicurezza deve essere la prima cosa da fare:

```
PSW 123456 xxxxxx
```

`123456` – la password di fabbrica; `xxxxxx` – la nuova password di 6 caratteri.

Controllo solo per le persone autorizzate – dal telefono dell'amministratore invia i dati degli utenti:

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

`PHONENO` – il numero di telefono dell'utente in formato internazionale (+CC..., dove CC è il prefisso internazionale); `NAME` – il suo nome; `EMAIL` – il suo indirizzo e-mail (per Protegus 2). Dopo l'inserimento del primo numero il GATOR reagisce solo alle chiamate dai numeri presenti nell'elenco.

Diritti di amministratore a un'altra persona – gli altri amministratori ricevono i messaggi di sistema e possono aggiungere utenti:

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

`Nox` – la posizione dell'amministratore nell'elenco (1–7); se scrivi **1**, cedi il tuo diritto di amministratore.

Elenco dei comandi SMS (in ognuno la password segue la parola di comando, negli esempi quella di fabbrica `123456`):

Comando	Parametro	Descrizione
`INFO`	–	dati sul dispositivo: tipo, IMEI, intensità del segnale, tensione di alimentazione, versione del firmware, numero di serie, data e ora. Esempio: `INFO 123456`
`ASKI`	–	stato degli ingressi. Esempio: `ASKI 123456`
`ASKO`	–	stato delle uscite. Esempio: `ASKO 123456`
`SETA`	`NoX=numero di telefono#nome#e-mail`	inserimento di un amministratore nella posizione X (1A–7A); il numero deve iniziare con + e il prefisso internazionale, i campi sono separati da #. Esempio: `SETA 123456 No3=+CC123456789#Giovanni#giovanni@example.com`
`SETA`	`NoX=DEL`	cancellazione dell'amministratore X. Esempio: `SETA 123456 No2=DEL`
`SETU`	`numero di telefono#nome#e-mail`	inserimento di un nuovo utente (posizioni 11–1010); anche qui il numero deve iniziare con + e il prefisso internazionale, i campi sono separati da #. Esempio: `SETU 123456 +CC123456789#Pietro#pietro@example.com`
`DELU`	`numero di telefono` o `nome`	cancellazione di un utente in base al numero di telefono o al nome. Esempio: `DELU 123456 +CC123456789`, `DELU 123456 Pietro`
`SETB`	`e-mail` o `numero di telefono`	inserimento nella lista nera (indirizzo e-mail o numero di telefono). Esempio: `SETB 123456 giovanni@example.com`, `SETB 123456 +CC123456789`
`DELB`	`ALL`	cancellazione dell'intera lista nera. Esempio: `DELB 123456 ALL`

Comando	Parametro	Descrizione
`DELB`	`e-mail` o `numero di telefono`	cancellazione di una voce dalla lista nera (per l'indirizzo e-mail contano maiuscole e minuscole). Esempio: `DELB 123456 giovanni@example.com`, `DELB 123456 +CC123456789`
`RESET`	–	riavvio del dispositivo. Esempio: `RESET 123456`
`PSW`	`nuova password`	cambio della password dell'amministratore. Esempio: `PSW 123456 654123`
`TXTA`	`nome dell'oggetto`	impostazione del nome dell'oggetto. Esempio: `TXTA 123456 Casa`
`TXTE`	`N1=testo` … `N5=testo`	testo dell'SMS inviato all'attivazione dell'ingresso o dell'uscita; N1…N5 è il numero del morsetto. Esempio: `TXTE 123456 N1=Cancello aperto`
`TXTR`	`N1=testo` … `N5=testo`	testo dell'SMS inviato al ripristino. Esempio: `TXTR 123456 N5=Rele spento`
`SETD`	`IDx=yy`	tempo di inattività dell'ingresso x in minuti (0–2880): dopo l'attivazione il dispositivo invia la notifica e per questo tempo non reagisce ad altri cambiamenti dell'ingresso; 0 = disattivato. Esempio: `SETD 123456 ID1=30`
`RESD`	`IDx`	annullamento del tempo di inattività già in corso dell'ingresso x. Esempio: `RESD 123456 ID1`
`TIME`	`AAAA/MM/GG,hh:mm:ss`	impostazione di data e ora. Esempio: `TIME 123456 2026/10/30,12:23:00`
`RDR`	`numero di telefono#testo`	inoltro di un SMS al numero indicato (per esempio una ricarica del credito all'operatore). Esempio: `RDR 123456 +CC123456789#Ricarica 10 EUR`
`HELLO`	`ON` / `OFF`	notifica SMS al nuovo utente sull'aggiunta (per un utente aggiunto dall'app o via SMS) attiva / disattiva. Esempio: `HELLO 123456 ON`
`NATH`	`ON` / `OFF`	attivazione e disattivazione della modalità **Not authorized** (può chiamare chiunque) senza modificare le altre impostazioni; con più uscite, elencando le uscite attivate dalla chiamata (attiva la modalità **Not authorized** e le uscite elencate, disattiva le altre uscite). Esempio: `NATH 123456 ON`, `NATH 123456 ON=5,7,22`, `NATH 123456 OFF`
`UUSD`	`*codice#`	invio di un codice USSD all'operatore mobile (verifica del credito, ricarica). Esempio: `UUSD 123456 *245#`
`CONNECT`	`Protegus=ON` / `Protegus=OFF`	connessione al cloud Protegus o disconnessione. Esempio: `CONNECT 123456 PROTEGUS=ON`
`CONNECT`	`APN=nome`, `USER=nome`, `PSW=password`	nome APN, nome utente e password della connessione dati mobile. Esempio: `CONNECT 123456 APN=INTERNET`
`CONNECT`	`Code=password`	cambio del codice di accesso al cloud Protegus (**Cloud Access Code**). Esempio: `CONNECT 123456 Code=123456`

Al posto del prefisso internazionale (CC) e dell'indirizzo e-mail degli esempi vanno i tuoi dati. Nell'SMS evita le lettere accentate e i caratteri speciali, se l'impostazione **System Options** → **Text language** non è impostata sul set di caratteri adatto (punto 5.2). L'elenco degli APN: Impostazione dell'APN – elenco degli operatori mobili europei.

5. Configurazione con il software TrikdisConfig

Tutte le impostazioni del GATOR sono accessibili con il programma per Windows **TrikdisConfig** – tramite cavo USB o a distanza (capitolo 6). Con le impostazioni di fabbrica il dispositivo apre alla chiamata (capitolo 2); il programma serve quando configuri utenti, tessere RFID, programmazioni orarie, testi SMS, moduli, il cloud Protegus o la centrale di vigilanza.

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

TrikdisConfig Letöltés a trikdis.com oldalról.

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

1. Con un cacciavite piatto togli il coperchio frontale del GATOR come mostrato in figura.
2. Collega il GATOR al computer con un cavo **USB Mini-B**.
3. Avvia TrikdisConfig. Il programma riconosce il dispositivo e apre la finestra di programmazione del GATOR.
4. Fai clic sul pulsante **Read [F4]**: il programma legge le impostazioni attuali del dispositivo. Se lo chiede, inserisci nella finestra che compare il codice di 6 cifre dell'**amministratore** o dell'**installatore** (il codice dell'amministratore di fabbrica è `123456`).



Figura 28. Rimozione del coperchio frontale: inserendo il cacciavite nell'apertura laterale e spingendolo verso il basso, il coperchio si sgancia; sotto c'è il connettore USB Mini-B.

Avvertenza

Finché il dispositivo è collegato al computer con il cavo USB, è in modalità di programmazione: il funzionamento normale si interrompe, non sorveglia, non trasmette, non può essere comandato, è alimentato dalla porta USB e si riavvia quando il cavo viene scollegato. Per questo il dispositivo non deve essere liberamente accessibile: deve trovarsi in un contenitore metallico chiuso, con protezione antimanomissione (tamper) o con un rilevatore di movimento che sorveglia il contenitore. Dettagli nelle FAQ

Alle impostazioni di fabbrica riporta il pulsante **Restore** nella parte in basso a sinistra della finestra di programmazione (punto 5.9).

5.1 La barra di stato

Dopo aver collegato e letto il dispositivo (**Read [F4]**), in fondo alla finestra compaiono i dati principali del dispositivo:

Etichetta	Significato
IMEI / Unique ID, nei dispositivi Ethernet **MAC / Unique ID**	L'identificativo univoco del dispositivo: nei dispositivi con scheda SIM l'IMEI, nei dispositivi Ethernet l'indirizzo MAC. Lo stesso è riportato sulla scatola e sul retro del dispositivo.
Status	Lo stato di funzionamento attuale.
Device	Il tipo (la sigla) del dispositivo. Verifica che qui compaia il tipo del tuo dispositivo.
SN	Numero di serie.
BL	La versione del bootloader.
FW	La versione del firmware.
HW	La versione dell'hardware.
State	La modalità di connessione: USB o da remoto (remote).
Administrator / Installer	Il livello di accesso di chi esegue la programmazione (dopo l'inserimento della password).

Dopo aver eseguito le impostazioni, le scrivi nel dispositivo con il pulsante **Write [F5]**; con i pulsanti **Open [F8]** e **Save [F9]** puoi salvare l'intero set di impostazioni su file e caricarlo in un altro dispositivo. **Save [F9]** salva le impostazioni in un file di configurazione, **Open [F8]** apre il file salvato; le impostazioni salvate si possono caricare in seguito anche in altri dispositivi, così puoi configurare più dispositivi rapidamente con le stesse impostazioni.



Figura 29. La barra di stato del GATOR: nel campo a sinistra l'**IMEI/Unique ID**, in basso **Status: reading done**, **Device: GV17_2200** (il codice tipo), il numero di serie, la versione **BL** e **FW**, il modo di connessione (USB). Per il GATOR il campo **Device** deve avere la forma **GV17_xxxx**.

5.2 Pagina „System Options”

Le impostazioni generali del dispositivo: identificativo, ora, codice dell'amministratore, risposta alle chiamate, test, scheda SIM e fuso orario.

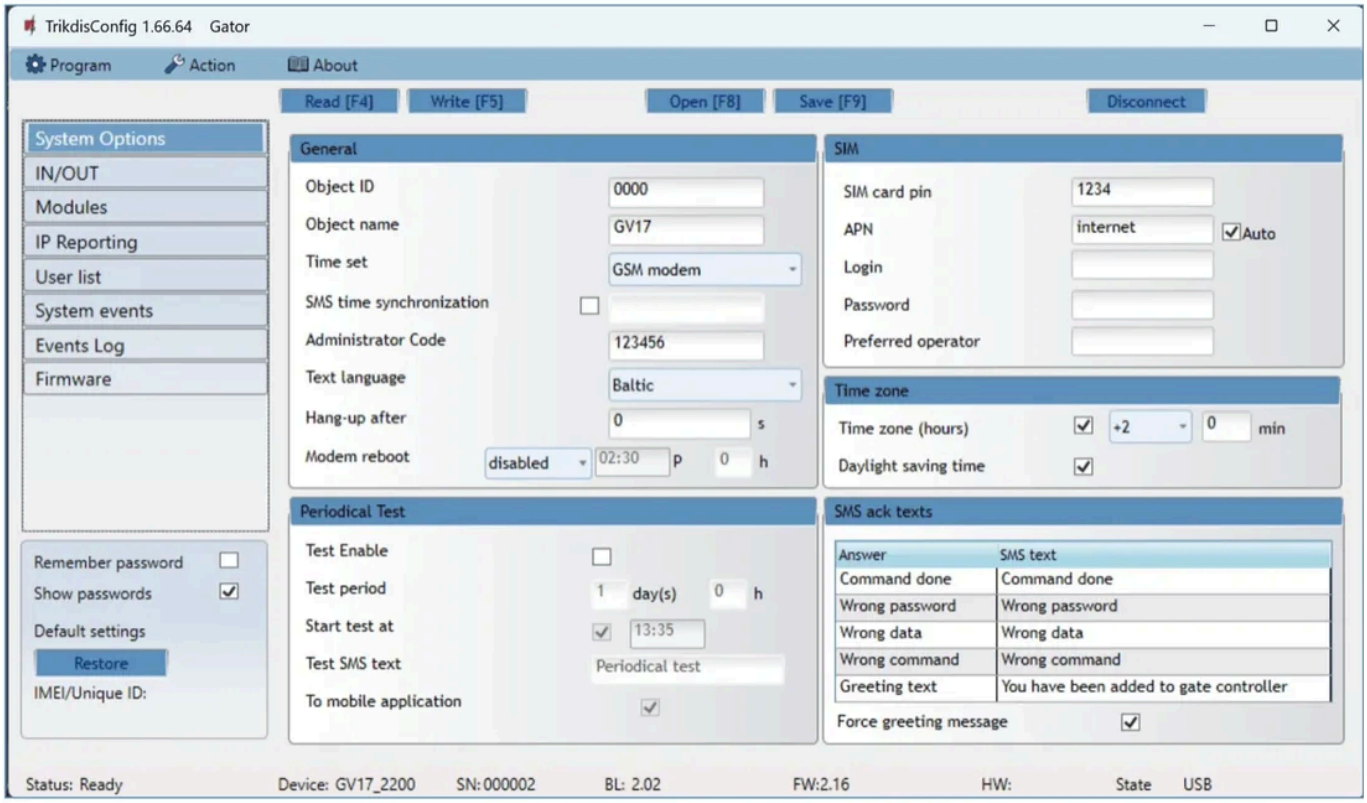


Figura 30. TrikdisConfig – **System Options**: i gruppi **General**, **Periodical test**, **SIM**, **Time zone** e **SMS ack texts**.

Gruppo General

- **Object ID** – il codice oggetto ricevuto dalla centrale di vigilanza (numero esadecimale di 4 cifre, 0–9, A–F). Non usare i valori FFFE e FFFF.
- **Object name** – il dispositivo invia ogni evento con questo nome.
- **Time set** – la fonte della sincronizzazione dell'ora (per esempio la rete mobile).
- **SMS time synchronization** – spunta la casella e inserisci il numero della scheda SIM del GATOR in formato internazionale (+CC…), se l'ora viene sincronizzata via SMS.
- **Administrator Code** – il codice dell'amministratore: con questo si possono modificare tutti i parametri del GATOR (di fabbrica `123456` – cambialo).
- **Text language** – il set di caratteri dei messaggi SMS.
- **Hang-up after** – con 0 il dispositivo rifiuta la chiamata (apre alla chiamata); con un altro valore risponde e chiude dopo i secondi indicati – per il controllo con la tastiera (DTMF) (punto 4.2).
- **Modem reboot** – riavvio giornaliero del modem a un orario indicato.

Gruppo Periodical test

- **Test Enable** – spuntato, il dispositivo invia un rapporto di test periodico.
- **Test period** – il tempo tra i rapporti di test.
- **Start test at** – l'orario del primo test.
- **Test SMS text** – il testo dell'SMS di test.
- **To mobile application** – spuntato, il rapporto di test va anche nell'app Protegus 2.

Gruppo SIM

- **SIM card PIN** – il codice PIN della scheda SIM, se non hai disattivato la richiesta.

- **APN** – il punto di accesso della connessione dati mobile. Con la casella **Auto** il dispositivo sceglie l'APN dall'elenco integrato (dati di diversi operatori internazionali e nazionali) e usa il valore scritto nel campo solo se non trova l'operatore. Se la connessione dati non si stabilisce, inserisci l'APN dell'operatore: Impostazione dell'APN – elenco degli operatori mobili europei.
- **Login**, **Password** – il nome utente e la password dell'APN, se l'operatore li richiede.
- **Preferred operator** – se inserisci un codice operatore (MCC + MNC), il GATOR si connette solo a quella rete; ha importanza con le schede SIM internazionali (roaming).

Gruppo Time zone – qui imposti l'ora esatta del paese: inserisci il fuso orario e indica se nel paese c'è l'ora legale.

- **Time zone (hours)** – spunta la casella e inserisci il fuso orario del paese (Italia: +1).
- **Daylight saving time** – spunta la casella se nel paese c'è l'ora legale.

Gruppo SMS ack texts – il testo degli SMS di risposta che l'utente riceve dopo i comandi SMS.

- **Force greeting message** – spuntato, il dispositivo invia un SMS di benvenuto al nuovo utente aggiunto via SMS o da Protegus 2 (via SMS lo disattiva `HELLO 123456 OFF`).

5.3 Pagina „IN/OUT"

Le impostazioni degli ingressi e delle uscite, dei lettori RFID e della rilevazione presenze, su tre schede: **IN/OUT**, **Scheduler**, **Holidays**.

5.3.1 Scheda IN/OUT – ingressi e uscite

Nella tabella ogni riga è un morsetto; qui decidi quale è un ingresso e quale un'uscita, e come deve segnalare.

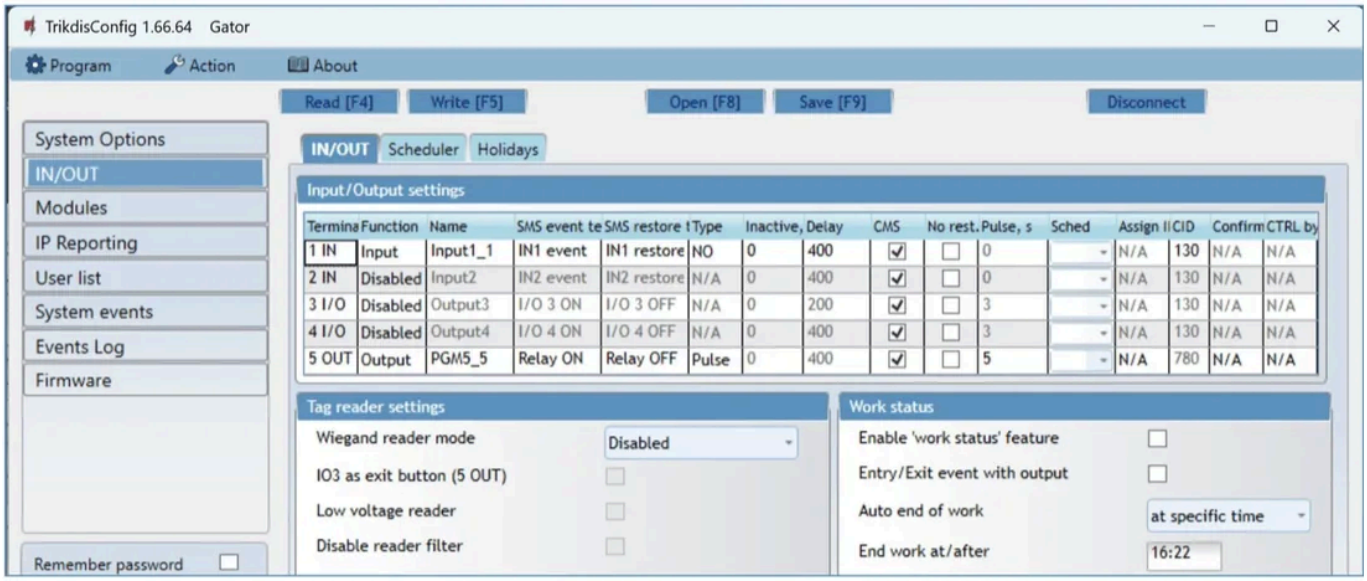


Figura 31. TrikdisConfig – **IN/OUT**: la tabella **Input/Output settings** (di fabbrica 1 IN ingresso, 2 IN, 3 I/O, 4 I/O disattivati, 5 OUT uscita di tipo **Pulse**), sotto i gruppi **Tag reader settings** e **Work status**.

Gruppo Input/Output settings

- **Terminal** – il numero dei morsetti del GATOR (1 IN … 5 OUT; i morsetti dei moduli di espansione sono in fondo all'elenco).
- **Function** – la funzione del morsetto: **Input** (ingresso), **Output** (uscita) o **Disabled** (disattivato).
- **Name** – il nome dell'ingresso o dell'uscita (così compare nell'app e negli SMS).

- **SMS event text** – il testo dell'SMS inviato all'attivazione.
- **SMS restore text** – il testo dell'SMS inviato al ripristino.
- **Type** – per un ingresso il tipo di circuito (**NC**, **NO**, **EOL = 10 kΩ**), per un'uscita il funzionamento: **Pulse** (impulso) o **Level** (bistabile).
- **Inactive** – dopo la prima attivazione l'ingresso non segnala di nuovo per questo tempo; 0 = disattivato.
- **Delay** – il tempo di reazione dell'ingresso in millisecondi (di fabbrica 400 ms).
- **CMS** – spuntato, l'evento va alla centrale di vigilanza e anche a Protegus 2.
- **No rest.** – non inviare l'evento di ripristino.
- **Pulse** – la durata dell'impulso in secondi, se l'uscita è di tipo **Pulse** (di fabbrica 3 s su 5 OUT; per l'automazione del cancello di solito bastano 1–3 s).
- **Sched** – il numero della programmazione oraria che comanda l'uscita (dalla scheda **Scheduler**).
- **Assign IN** – l'ingresso assegnato all'uscita: invece dello stato dell'uscita l'app mostra lo stato reale dell'ingresso (del cancello) (punto 5.10).
- **CID** – il codice Contact ID dell'evento.
- **Confirm** – il numero dell'ingresso il cui stato attivo è condizione per l'attivazione dell'uscita.
- **CTRL by IN** – l'attivazione dell'ingresso scelto comanda l'uscita (automatismo locale, funziona anche senza rete).

Gruppo Tag reader settings – le impostazioni dei lettori RFID (collegamento al punto 3.6)

- **Wiegand reader mode** – il numero dei lettori Wiegand collegati: **Single Reader** o **Dual Reader**.
- **IO3 as exit button (5 OUT)** – spuntalo se il pulsante di uscita è collegato al morsetto 3 I/O: quando lo si preme, 5 OUT si attiva per la durata dell'impulso impostata.
- **Low voltage reader** – per un lettore a bassa tensione (livello del segnale di 5 V).
- **Disable reader filter** – disattiva il filtro interno degli impulsi brevi, se il dispositivo non riconosce i segnali del lettore.

Gruppo Work status – rilevazione delle presenze in Protegus 2 (dettagli: GV17 – sistema di controllo accessi e/o rilevazione presenze)

- **Enable “work status” feature** – attiva la segnalazione dello stato di lavoro nell'app.
- **Entry/Exit event with output** – spuntato, anche l'attivazione a distanza dell'uscita genera un evento di ingresso / uscita.
- **Auto end of work** – il modo della chiusura automatica dell'orario di lavoro.
- **End work at/after** – l'orario della chiusura o il tempo fino alla chiusura, a seconda dell'impostazione precedente.

5.3.2 Scheda Scheduler – programmazione oraria delle uscite

Le uscite possono anche attivarsi da sole secondo una programmazione oraria (per esempio cancello aperto durante l'orario di lavoro, chiuso la sera). La programmazione si assegna nella colonna **Sched** dell'uscita.

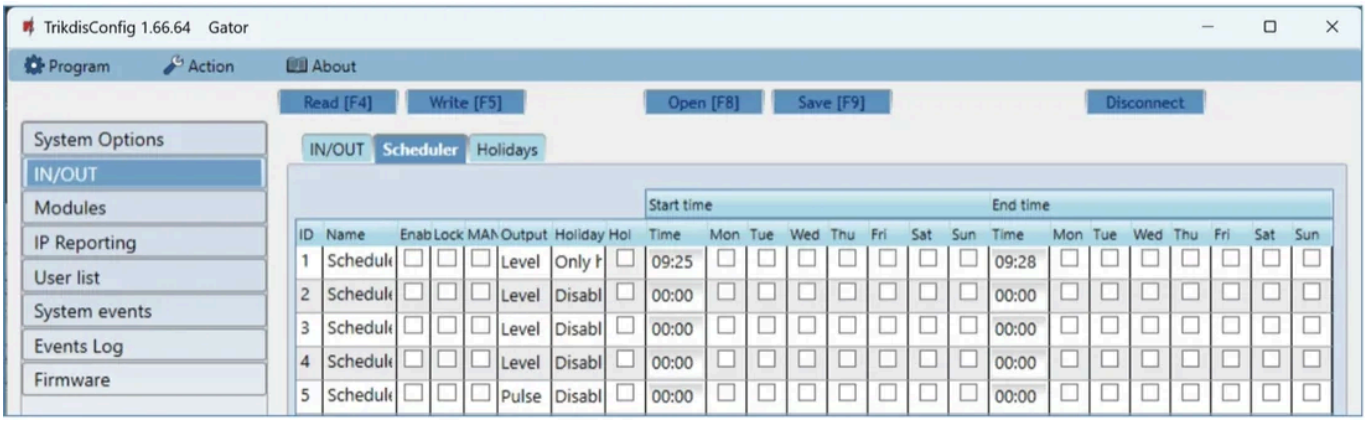


Figura 32. TrikdisConfig – IN/OUT, scheda **Scheduler**: per ogni programmazione abilitazione, blocco, modalità di uscita, modalità festiva, orario di inizio e di fine con i giorni della settimana.

- **Name** – il nome della programmazione.
- **Enable** – abilitazione della programmazione.
- **Lock** – spuntato, durante il periodo attivo della programmazione l'uscita non si può comandare in altro modo (con chiamata, dall'app).
- **MANUAL** – spuntato, all'avvio della programmazione l'uscita non si attiva da sola; la programmazione parte quando l'utente attiva l'uscita.
- **Output mode** – il funzionamento dell'uscita durante la programmazione: **Level** – l'uscita resta attiva per tutto il periodo indicato; **Pulse** – l'uscita si attiva all'inizio e alla fine della programmazione per la durata dell'impulso impostata.
- **Holiday mode** – come deve funzionare la programmazione nei giorni festivi; **Hol** – spuntalo se nei giorni festivi devono valere gli orari festivi.
- **Start time** – i giorni della settimana e l'orario da cui l'uscita si attiva.
- **End time** – i giorni della settimana e l'orario fino a cui l'uscita resta attiva.

Se la modalità dell'uscita è **Level** ed è indicato solo **End time**, l'uscita si disattiva all'orario indicato, se fino ad allora era attiva.

5.3.3 Scheda Holidays – giorni festivi

Qui indichi i giorni di calendario in cui la programmazione funziona con gli orari festivi.

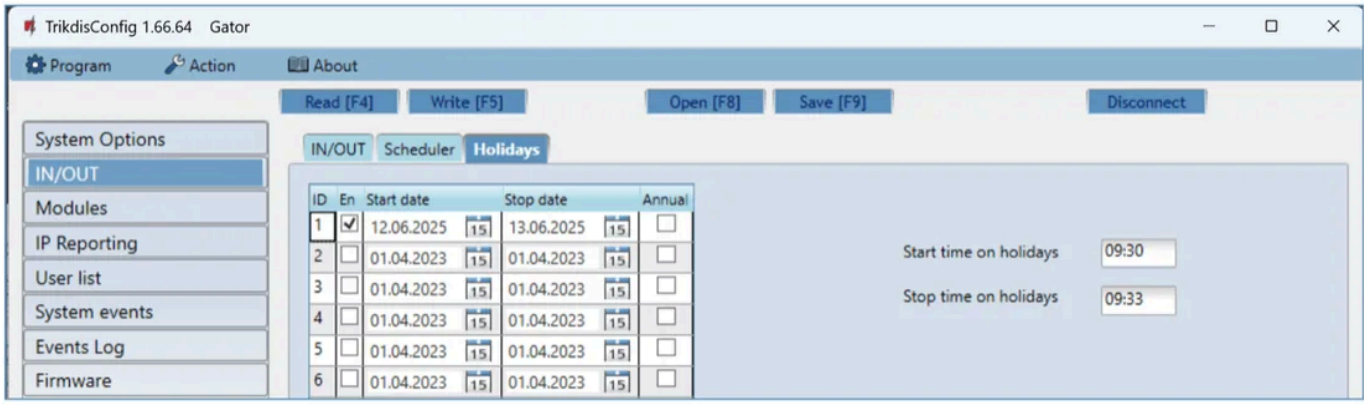


Figura 33. TrikdisConfig – IN/OUT, scheda **Holidays**: periodi festivi con data di inizio e di fine, con l'orario di inizio e di fine festivo.

- **En.** – abilitazione del periodo festivo.
- **Start date**, **Stop date** – il primo e l'ultimo giorno del periodo.
- **Annual** – festività che si ripete ogni anno: il dispositivo guarda solo il mese e il giorno.

- **Start time on holidays**, **Stop time on holidays** – l'orario di inizio e di fine nei giorni festivi.

5.4 Pagina „Modules”

5.4.1 Scheda Modules

Al GATOR, tramite il bus RS485 o via radio, si possono collegare questi moduli: modulo WiFi **W485**, modulo Ethernet **E485**, modulo di espansione senza fili **iO-LORA** (tramite il ricetrasmettitore RF-LORA, fino a 8; i lettori RFID collegati ai moduli iO-LORA possono così comandare fino a 8 uscite in più, un lettore sempre e solo un'uscita del proprio modulo di espansione – dal firmware 2.13 del GATOR, punto 3.9), modulo di espansione cablato **iO8** e senza fili **iO8-LORA** (tramite l'RF-LORA; dei due, uno in tutto). Il ricetrasmettitore RF-LORA non va aggiunto all'elenco. Se sul posto c'è il WiFi o Internet cablato, con il modulo W485 o E485 il GATOR invia i messaggi via Internet al cloud Protegus e alla centrale di vigilanza: i dati mobili non si consumano (il traffico dati della scheda SIM si può anche disattivare), anzi il GATOR si può usare anche senza scheda SIM, controllandolo solo dall'app.

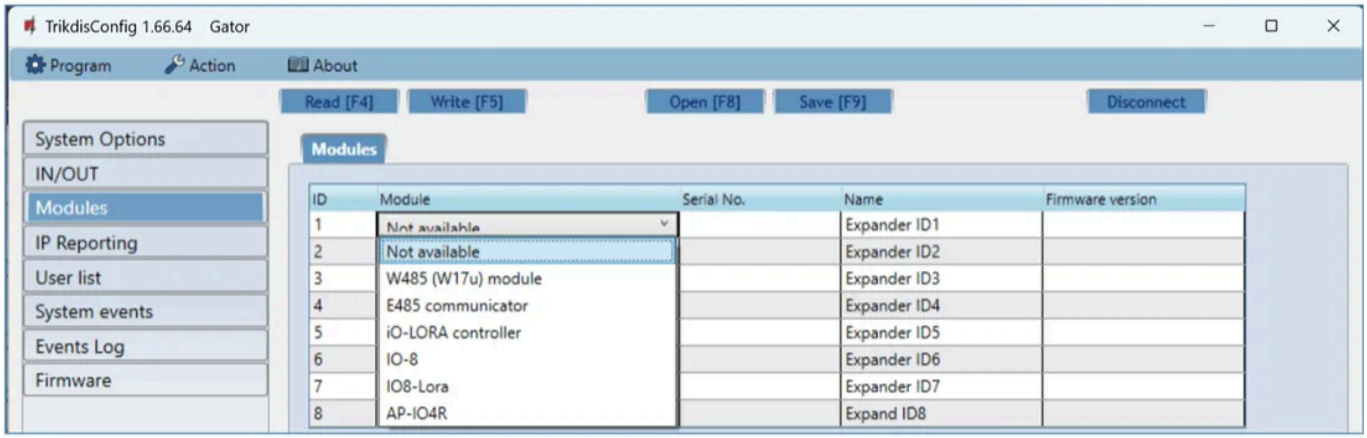


Figura 34. TrikdisConfig – **Modules**: nell'elenco a discesa **Module** i moduli W485, E485, iO-LORA, iO8, iO8-LORA e **AP-IO4R** (iO4R); accanto le colonne **Serial No.**, **Name** e **Firmware version**.

- **Module** – scegli dall'elenco il modulo collegato.
- **Serial No.** – il numero di serie di 6 cifre del modulo (sull'etichetta sul contenitore e sulla scatola del modulo).

Dopo aver scelto il modulo e inserito il numero di serie compare la scheda **Parameters** con le impostazioni proprie del modulo.

Modulo di espansione a relè iO4R

La voce **AP-IO4R** dell'elenco è il modulo di espansione a relè **iO4R**: serve per la supervisione e l'esclusione a distanza dei sensori di sicurezza dell'automazione del cancello, e per il conteggio dei cicli del cancello. La sua configurazione si esegue nell'app Protegus 2, nella modalità **Advanced Gator Monitoring** selezionabile quando si aggiunge l'apricancello – vedi il manuale dell'iO4R.

5.4.2 Scheda Parameters – modulo WiFi W485

Dopo aver scelto il W485, qui inserisci i dati della rete WiFi e il modo di uso della scheda SIM.

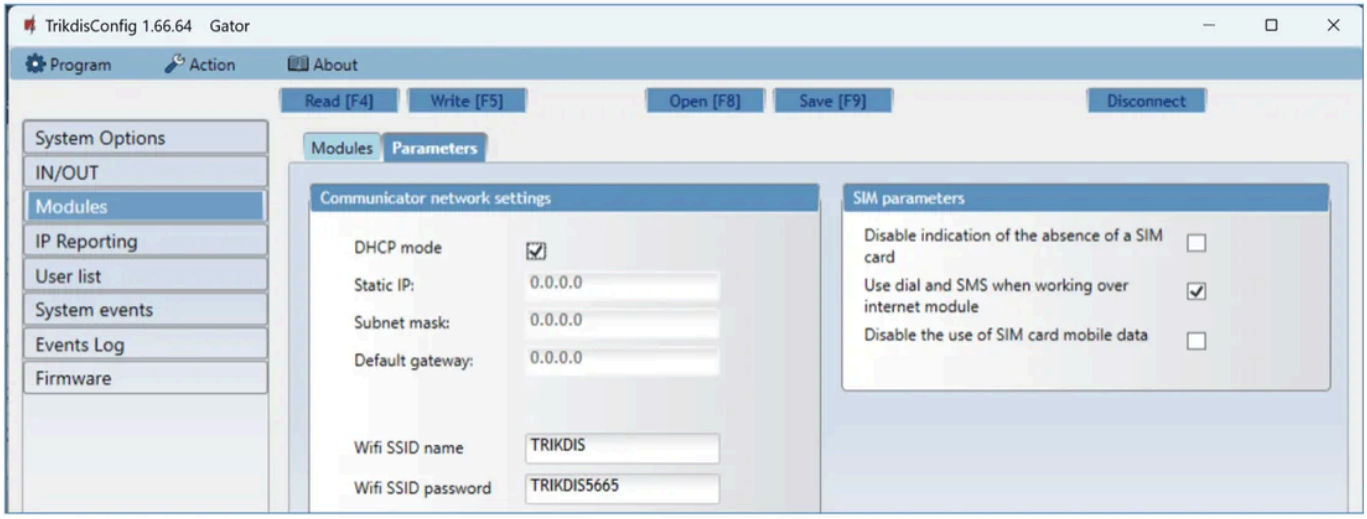


Figura 35. TrikdisConfig – Modules, scheda **Parameters** per il W485: **Communicator network settings** (DHCP, indirizzo IP, nome e password della rete WiFi) e **SIM parameters**.

Gruppo Communicator network settings

- **DHCP mode** – spuntato, il modulo riceve automaticamente dal router le impostazioni di rete (indirizzo IP, subnet mask, gateway); vuoto, le inserisci a mano.
- **Static IP**, **Subnet mask**, **Default gateway** – l'indirizzo IP fisso, la subnet mask e l'indirizzo del gateway con l'impostazione manuale.
- **Wifi SSID name** – il nome della rete WiFi a cui si connette il W485 (rete a 2,4 GHz).
- **Wifi SSID password** – la password della rete WiFi.

Gruppo SIM parameters

- **Disable indication of the absence of a SIM card** – spuntato, il dispositivo non segnala come guasto la mancanza della scheda SIM (per l'uso senza SIM, solo via Internet).
- **Use dial and SMS when working over internet module** – spuntato, il controllo con chiamata e SMS funziona anche insieme al modulo. Vuoto, finché la connessione Internet è attiva il dispositivo non usa chiamate e SMS; se Internet si interrompe, la chiamata e l'SMS funzionano di nuovo e il dispositivo invia un SMS agli utenti.
- **Disable the use of SIM card mobile data** – spuntato, il dispositivo non usa i dati mobili della scheda SIM, i dati passano solo tramite il W485. Se il WiFi si interrompe, il dispositivo memorizza gli eventi e li invia al ritorno della connessione.

5.4.3 Scheda Parameters – modulo Ethernet E485

Dopo aver scelto l'E485, qui inserisci i dati della rete cablata e il modo di uso della scheda SIM.

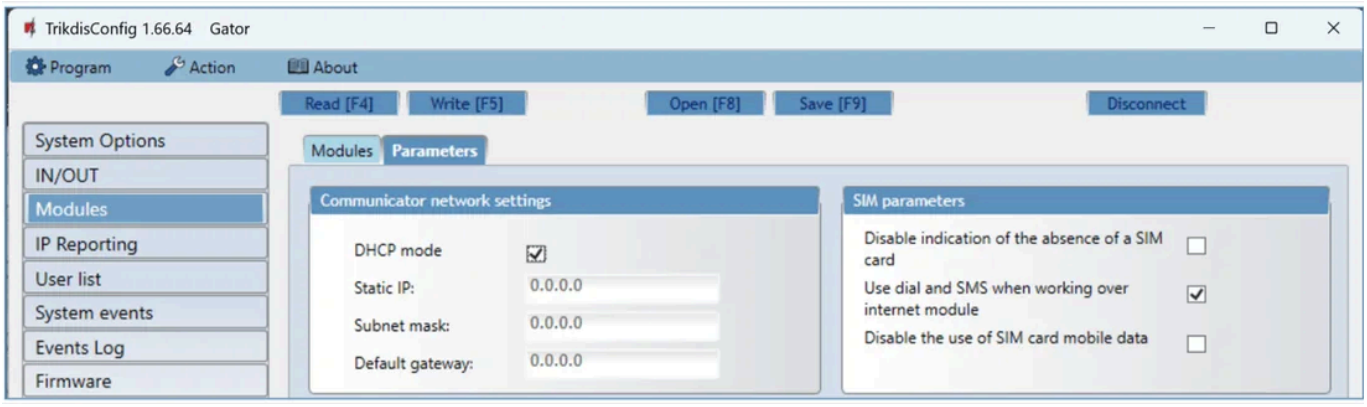


Figura 36. TrikdisConfig – Modules, scheda **Parameters** per l'E485: impostazioni di rete (DHCP o indirizzo IP fisso) e **SIM parameters**.

- **DHCP mode**, **Static IP**, **Subnet mask**, **Default gateway** – come per il W485: impostazione di rete automatica o manuale.
- **SIM parameters** – il significato delle tre caselle è identico a quanto descritto per il W485; con i dati mobili disattivati i dati passano solo tramite l'E485, durante l'assenza di Internet il dispositivo memorizza gli eventi.

5.5 Pagina „IP Reporting”

Il GATOR invia gli eventi al ricevitore IP della centrale di vigilanza e al cloud Protegus; il cloud lo attivi in questa pagina.

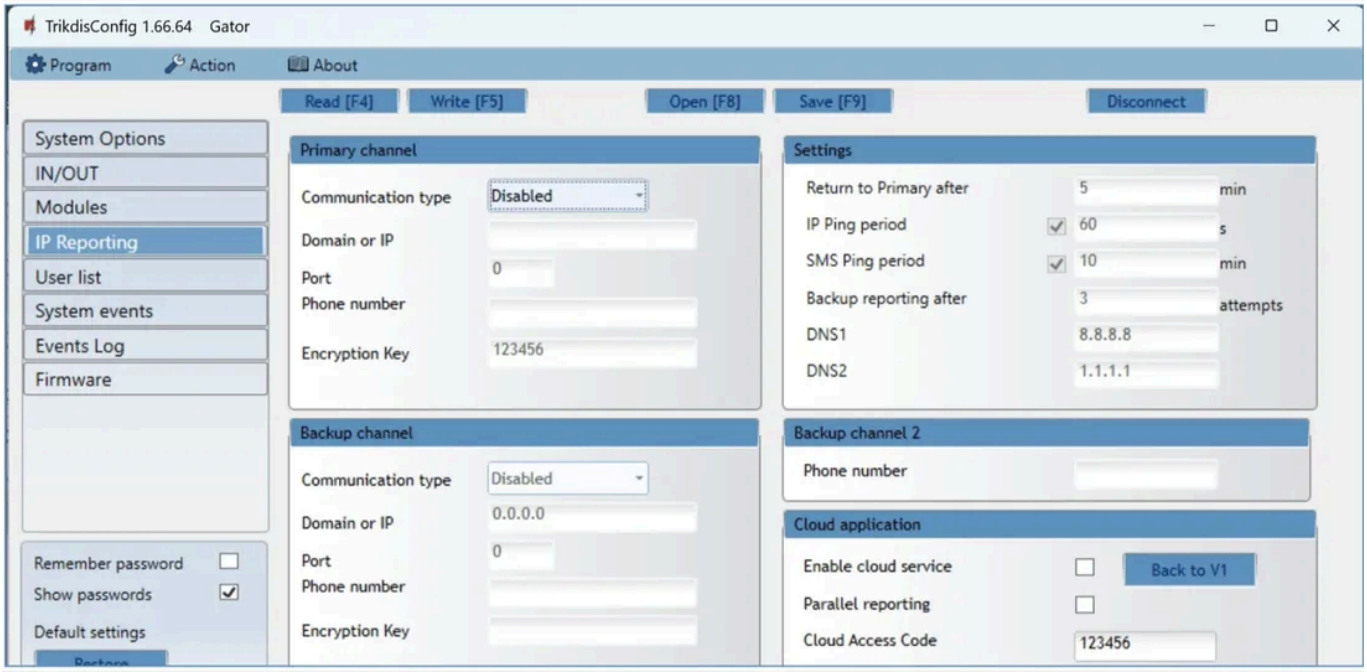


Figura 37. TrikdisConfig – **IP Reporting**: **Primary channel** e **Backup channel** (di fabbrica disattivati), **Settings**, il canale SMS di riserva e il gruppo **Cloud application** con la casella **Enable cloud service** e il codice **Cloud Access Code**.

Gruppo Primary channel

- **Communication type** – il tipo di connessione con il ricevitore della centrale di vigilanza: **IP** o **SMS**; **Disabled** = nessuna trasmissione.
- **Domain or IP** – il nome di dominio o l'indirizzo IP del ricevitore.
- **Port** – la porta di rete del ricevitore.

- **Phone number** – il numero di telefono del ricevitore SMS della centrale di vigilanza (+CC…), se il tipo è SMS.
- **Encryption Key** – chiave di crittografia di 6 cifre, che deve coincidere con quella impostata nel ricevitore.

Gruppo Backup channel – il ricevitore di riserva, con le stesse impostazioni del primario.

Gruppo Settings

- **Return to primary after** – dopo questo tempo il dispositivo prova a tornare dal canale di riserva al canale primario.
- **IP Ping period** – abilitazione e intervallo dei segnali PING che mantengono la connessione.
- **SMS Ping period** – lo stesso sul canale SMS.
- **Backup reporting after** – dopo questo numero di tentativi falliti il dispositivo passa al canale di riserva.
- **DNS1**, **DNS2** – l'indirizzo IP dei server dei nomi.

Gruppo Backup channel 2

- **Phone number** – il numero del ricevitore SMS della centrale di vigilanza. Il dispositivo invia qui un SMS se non riesce a inviare il messaggio né sul canale IP primario né su quello di riserva; funziona anche se nella rete dell'operatore mobile viene a mancare la connessione IP. È attivo solo se entrambi i canali IP sono su rete mobile; il ricevitore SMS riceve un messaggio alla prima accensione del dispositivo e alla perdita della connessione TCP/IP o UDP/IP.

Gruppo Cloud application

- **Enable cloud service** – attivazione del cloud Protegus: il GATOR comunica con l'app e si può programmare a distanza anche con TrikdisConfig (capitolo 6).
- **Parallel reporting** – spuntato, gli eventi vanno contemporaneamente alla centrale di vigilanza, a Protegus 2 e agli utenti; vuoto, l'app e gli utenti li ricevono solo dopo la conferma della centrale di vigilanza.
- **Cloud Access Code** – codice di 6 cifre per la connessione a Protegus 2 (di fabbrica `123456`); l'app lo chiede quando si aggiunge il sistema, se non è quello di fabbrica.

5.6 Pagina „User list”

L'elenco degli amministratori e degli utenti, la registrazione delle tessere RFID, le programmazioni orarie degli utenti e la lista nera – su quattro schede.

5.6.1 Scheda Users – gli utenti

Nella tabella ogni riga è un amministratore o un utente con i suoi permessi.

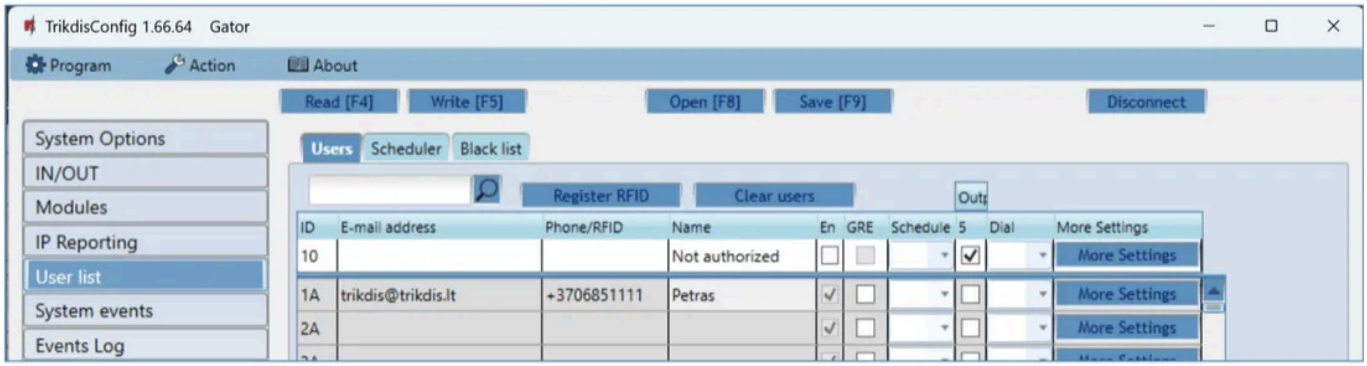


Figura 38. TrikdisConfig – **User list**, scheda **Users**: in alto i pulsanti **Register RFID** e **Clear users**; nella tabella le colonne **ID**, **E-mail address**, **Phone/RFID**, **Name**, **En**, **GRE**, **Schedule**, **Dial** e il pulsante **More settings**; la riga 10 è la voce **Not authorized**.

- **ID** – il numero dell'utente. Le righe con la lettera **A** (**1A–7A**) sono gli amministratori: possono configurare il dispositivo, comandare le uscite e ricevono i messaggi. Le righe con numero **11–1010** sono gli utenti: possono solo comandare le uscite.
- **E-mail address** – l'indirizzo e-mail dell'utente (per Protegus 2).
- **Phone/RFID** – il numero di telefono in formato internazionale (+CC…) o il numero identificativo della tessera RFID.
- **Name** – il nome dell'utente.
- **En** – abilitazione dell'utente: spuntato, l'utente può comandare le uscite.
- **GRE** – invio di un SMS di benvenuto all'utente.
- **Schedule** – il numero della programmazione oraria secondo cui l'utente può controllare (punto 5.6.3).
- **Output** – l'uscita o le uscite che l'utente può controllare.
- **Code** – con un lettore Wiegand a codice (con tastiera) il codice dell'utente.
- **Dial** – l'uscita o le uscite attivate dalla chiamata, se l'utente ha più uscite; dopo l'attivazione il dispositivo chiude la chiamata.
- **More settings** – la finestra delle altre impostazioni (sotto).

La riga 10, „Not authorized”

Se per l'utente numero 10, chiamato **Not authorized**, la casella **En** è **spuntata**, il GATOR si può controllare con una chiamata **da qualsiasi numero di telefono**. Se è vuota, possono chiamare solo le persone nell'elenco; ogni utente comanda l'uscita contrassegnata nella propria colonna **Dial**. Via SMS la stessa cosa si imposta con il comando `NATH` (punto 4.7).

L'apertura tramite chiamata e la notifica con chiamata telefonica funzionano su 2G o VoLTE. Dove l'operatore ha spento il 2G e non ha approvato il modem per la VoLTE, la chiamata non è garantita. Prima dell'ordine, verificalo con l'operatore della SIM.

Altre impostazioni – amministratore (1A–7A)

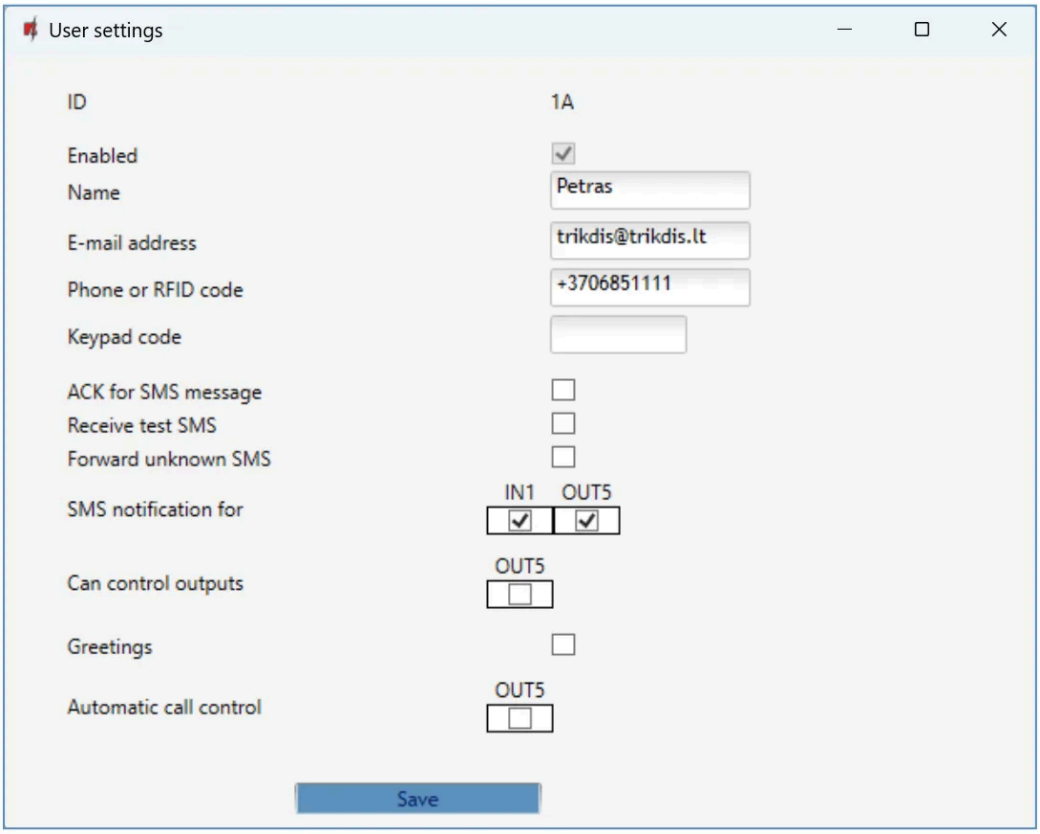


Figura 39. TrikdisConfig – **User settings** per un amministratore: **Enabled**, i dati, **ACK for SMS message**, **Receive test SMS**, **Forward unknown SMS**, **SMS notification for** (IN1, IN2, OUT3, OUT4, OUT5), **Can control output**, **Greetings** e **Automatic call control**.

- **ID**, **Enabled**, **Name**, **E-mail address**, **Phone or RFID code**, **Keypad code** – i dati corrispondenti alle colonne dell'elenco.
- **ACK for SMS message** – l'amministratore riceve un SMS di risposta sull'esecuzione dei comandi SMS.
- **Receive test SMS** – riceve l'SMS di test periodico.
- **Forward unknown SMS** – il dispositivo gli inoltra gli SMS che arrivano da numeri sconosciuti (per esempio l'avviso del credito dell'operatore).
- **SMS notification for** – di quali eventi (IN1, IN2, OUT3, OUT4, OUT5) riceve un SMS quando cambiano.
- **Can control output** – le uscite che può controllare.
- **Greetings** – invio di un SMS di benvenuto.
- **Automatic call control** – le uscite attivate dalla sua chiamata, dopo di che il dispositivo chiude la chiamata.

Altre impostazioni – utente (11–1010)

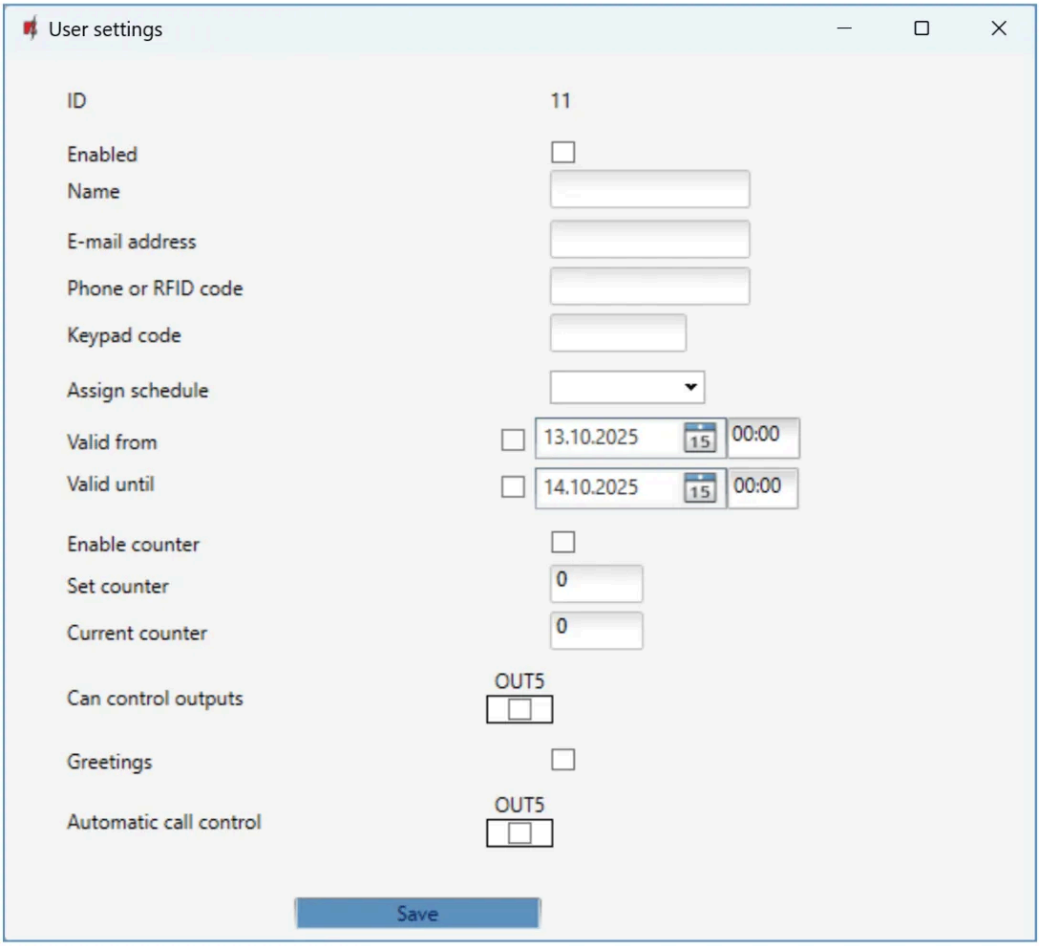


Figura 40. TrikdisConfig – **User settings** per un utente: **Assign schedule**, **Valid from** / **Valid until**, **Enable counter**, **Set counter**, **Current counter**, **Can control outputs**, **Greetings**, **Automatic call control**.

- **Assign schedule** – la programmazione o le programmazioni orarie durante le quali l'utente può controllare.
- **Valid from**, **Valid until** – inizio e fine del permesso (data e ora) – per esempio per un affittuario o un ospite.
- **Enable counter** – attivazione del contatore; **Set counter** – quante volte l'utente può controllare entro il tempo indicato; **Current counter** – il numero di attivazioni finora.
- **Can control outputs**, **Greetings**, **Automatic call control** – come per l'amministratore.

5.6.2 Registrazione di una tessera RFID (portachiavi)

1. Collega il lettore RFID (punto 3.6), accendi l'alimentazione del GATOR, avvia TrikdisConfig e connettiti con il cavo USB o a distanza. Nella pagina **IN/OUT** imposta il numero dei lettori (**Wiegand reader mode**).
2. Nella pagina **User list** fai clic sul pulsante **Register RFID**.

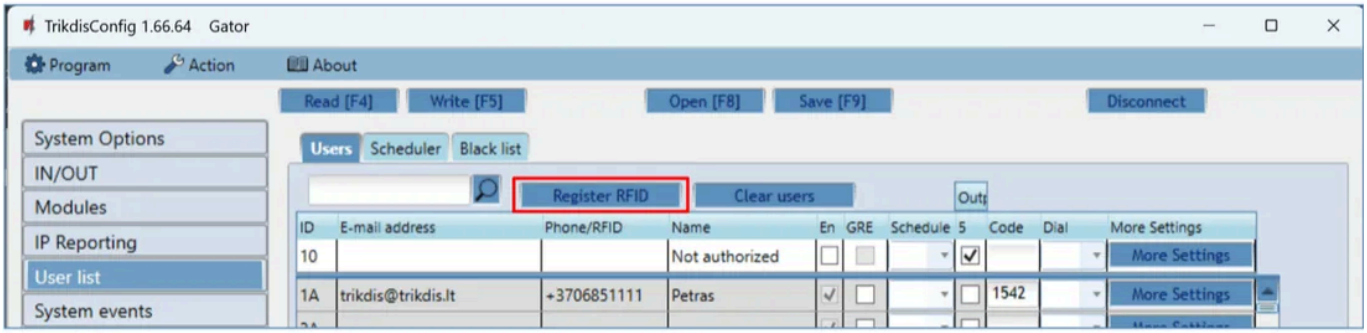


Figura 41. TrikdisConfig – User list: il pulsante **Register RFID** sopra la tabella degli utenti.

3. Si apre la finestra di registrazione (**Add RFID tag/card to reader**).

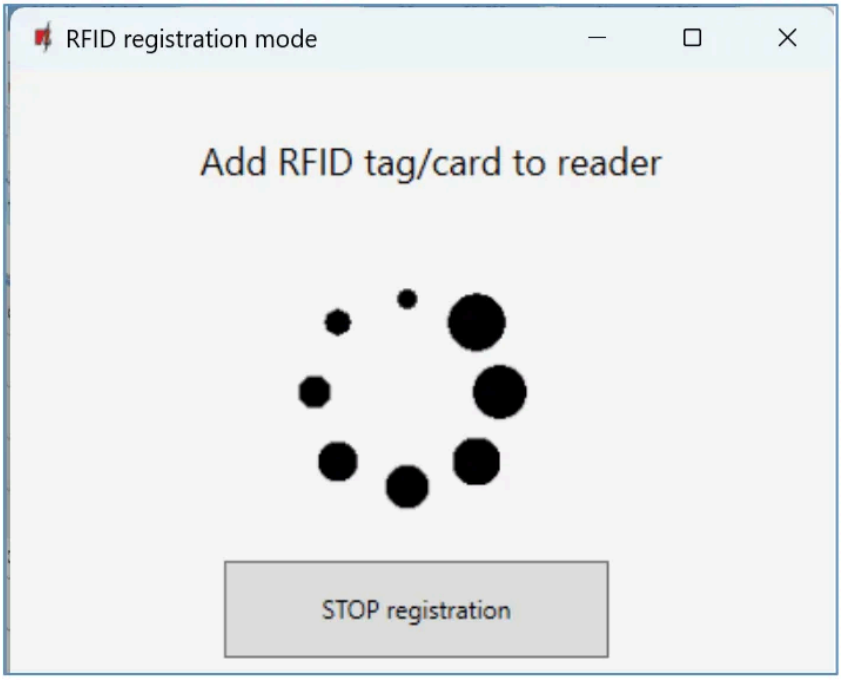


Figura 42. La finestra di registrazione RFID: la tessera va avvicinata al lettore; il pulsante **STOP registration** chiude la registrazione.

4. Avvicina la tessera al lettore. Quando il lettore l'ha letta, si apre una nuova finestra: scrivi il nome dell'utente (**Enter user name**), indica l'uscita che può controllare (**User can control PGM Output 5**; con la casella **Device administrator** diventa amministratore) e fai clic sul pulsante **ADD**. Ripeti con le altre tessere, poi premi il pulsante **STOP registration**.
5. Con il pulsante **Write [F5]** scrivi l'elenco delle tessere nel dispositivo.

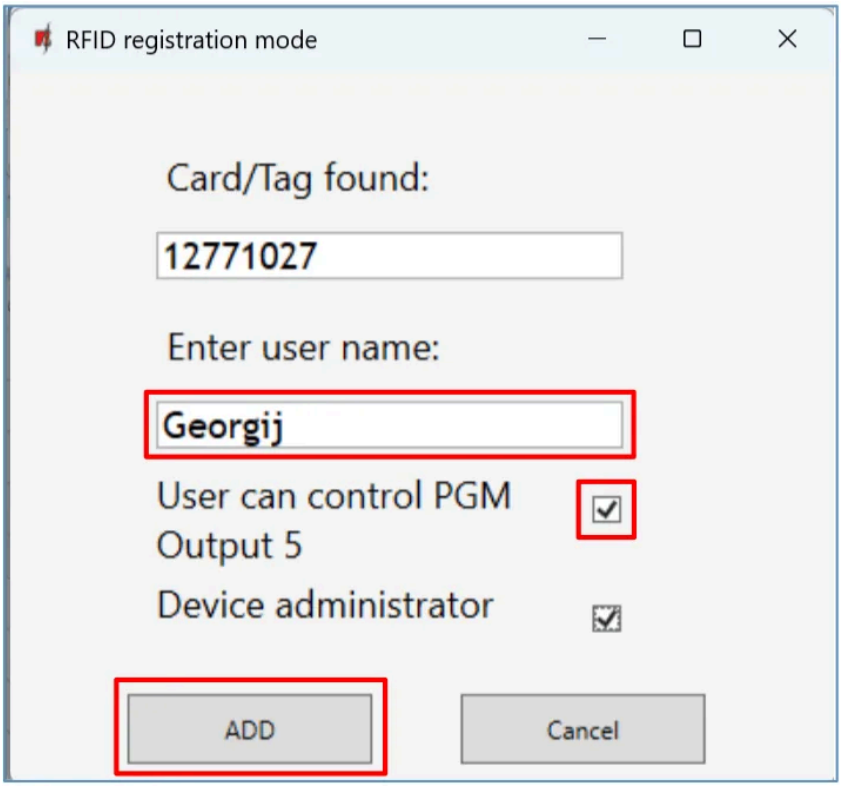


Figura 43. La finestra della tessera letta: nome, **User can control PGM Output 5**, **Device administrator**, poi **ADD**.

Aggiunta di una tessera in base al suo numero: il numero identificativo stampato sulla tessera lo puoi anche scrivere direttamente nel campo **Phone/RFID**; inserisci il nome, spunta la casella **En** e l'uscita controllabile, poi **Write [F5]**.

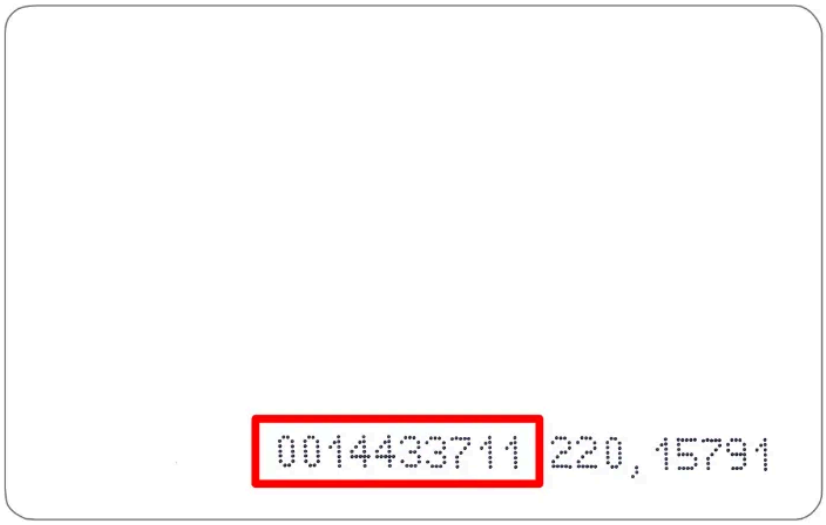


Figura 44. Il numero identificativo stampato sulla tessera RFID (sul bordo inferiore della tessera).

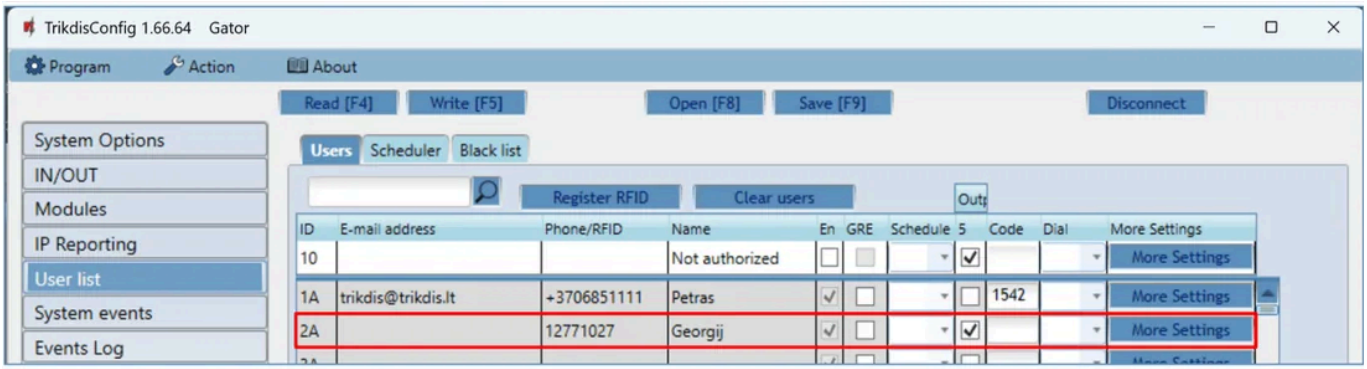


Figura 45. TrikdisConfig – User list: la riga del nuovo utente con il numero della tessera nel campo **Phone/RFID**, con il nome, **En** spuntato, l'uscita 5 contrassegnata.

Aggiunta di una tessera da Protegus 2: nell'elenco degli utenti scegli l'aggiunta di un nuovo utente, inserisci l'indirizzo e-mail, il nome, il numero identificativo della tessera (nel campo del numero di telefono), con un lettore a codice il codice di 4 cifre, indica l'uscita e salva (punto 4.5).

5.6.3 Scheda Scheduler – programmazione oraria degli utenti

L'utente può controllare solo durante la programmazione oraria assegnata (per esempio l'addetto alle pulizie nei giorni feriali tra le 6 e le 8). La programmazione si assegna nella colonna **Schedule** dell'utente o nel campo **More settings** → **Assign schedule**.

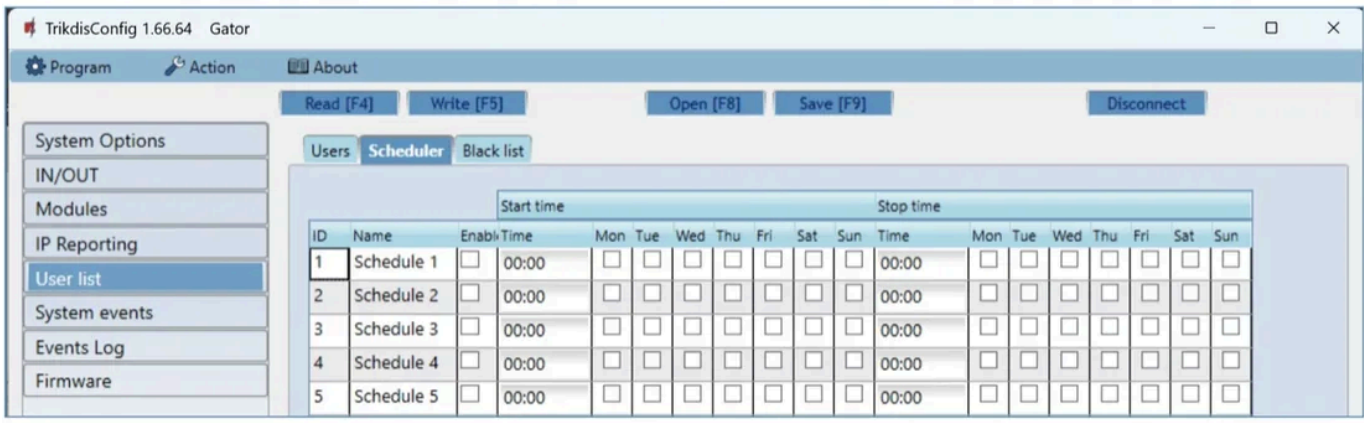


Figura 46. TrikdisConfig – User list, scheda **Scheduler**: cinque programmazioni, ognuna con **Enable**, orario di inizio e di fine con i giorni della settimana.

- **Name** – il nome della programmazione.
- **Enable** – abilitazione della programmazione.
- **Start time** – i giorni della settimana e l'orario da cui l'utente può controllare.
- **Stop time** – i giorni della settimana e l'orario fino a cui può controllare.

5.6.4 Scheda Black list – lista nera

Chi inserisci qui non può controllare il dispositivo in nessun modo.

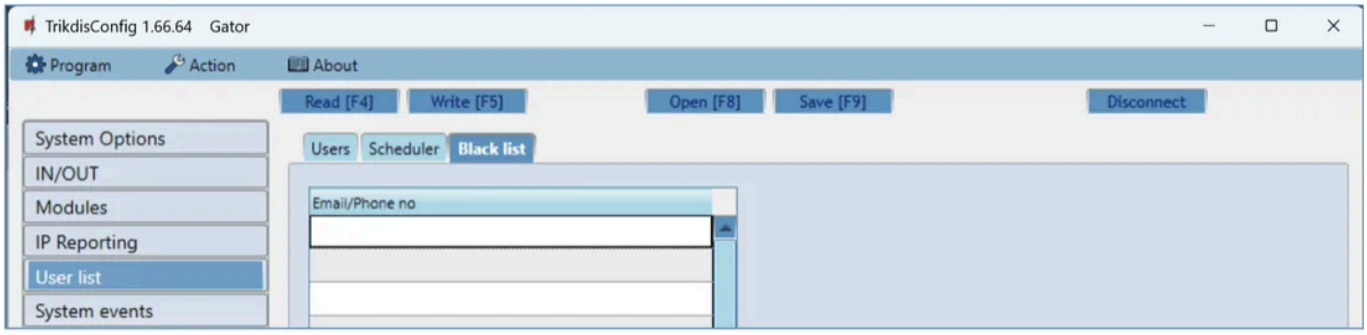


Figura 47. TrikdisConfig – User list, scheda **Black list**: la tabella degli indirizzi e-mail, dei numeri di telefono e dei numeri di tessera bloccati.

Nella lista nera ci sono gli indirizzi e-mail, i numeri di telefono e i numeri delle tessere RFID a cui è vietato controllare il GATOR. Puoi aggiungere una voce anche direttamente dal registro eventi: fai clic con il tasto destro sul numero di telefono, sull'indirizzo e-mail o sul numero della tessera e scegli la voce di menu **Add to black list**. Via SMS la lista si gestisce con i comandi `SETB` e `DELB` (punto 4.7).

5.7 Pagina „System events”

Qui imposti quali tra gli eventi di sistema del GATOR devono andare alla centrale di vigilanza e all'app Protegus 2.

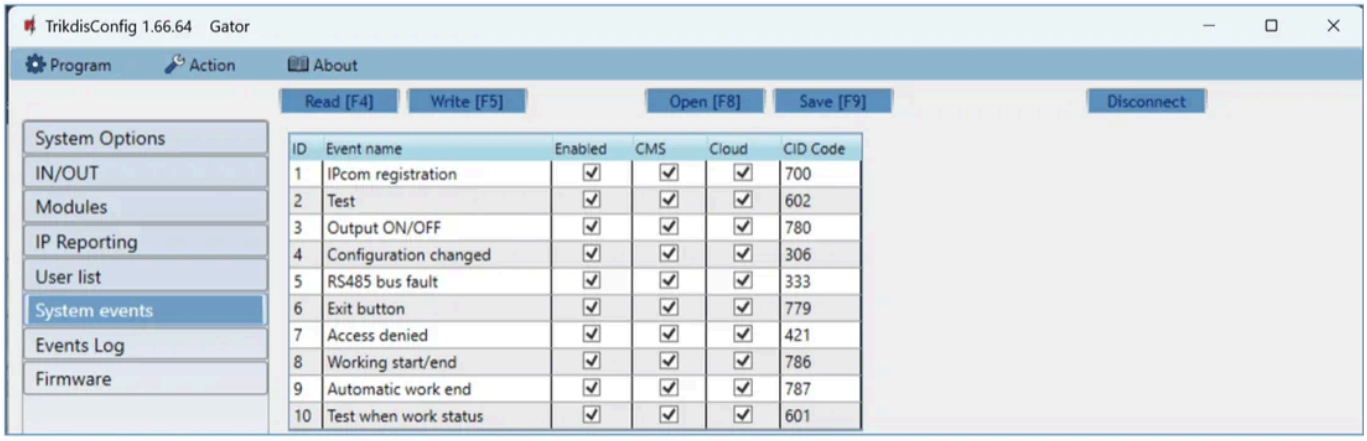


Figura 48. TrikdisConfig – **System events**: l'elenco degli eventi con il codice Contact ID (per esempio IPcom registration 700, Test 602, Output ON/OFF 780, Configuration changed 306, RS485 bus fault 333, Exit button 779, Access denied 421, Working start/end 786, Automatic work end 787), ognuno con le caselle **Enabled**, **CMS** e **Cloud**.

- **ID** – il numero dell'evento.
- **Event name** – il nome dell'evento.
- **Enabled** – monitoraggio dell'evento.
- **CMS** – l'evento va alla centrale di vigilanza.
- **Cloud** – l'evento va all'app Protegus 2.
- **CID Code** – il codice Contact ID dell'evento.

5.8 Pagina „Events Log”

Il registro eventi del dispositivo – per la ricerca guasti e per ricostruire gli accessi.

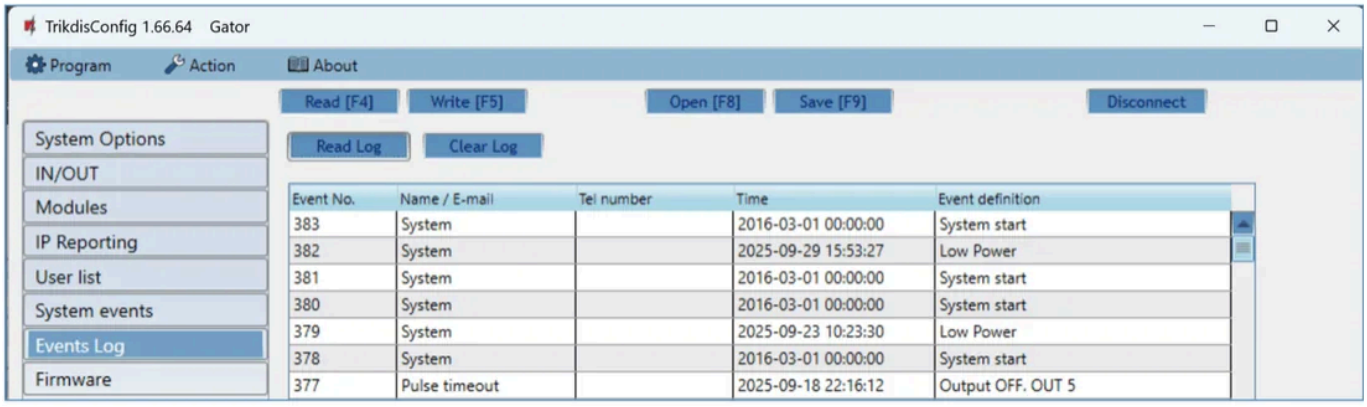


Figura 49. TrikdisConfig – **Events Log**: i pulsanti **Read Log** e **Clear Log**; per gli eventi il numero, il nome o l'indirizzo e-mail dell'utente, il numero di telefono, l'ora e la descrizione dell'evento.

Fai clic sul pulsante **Read Log**: il programma legge gli eventi dalla memoria del dispositivo (fino a 5000). Il registro mostra tutte le operazioni e gli eventi interni del GATOR con dati dettagliati: chi ha aperto il cancello, quando e con cosa (chiamata, SMS, app, tessera), e quali ingressi sono cambiati. Il pulsante **Clear Log** cancella il registro.

5.9 Ripristino delle impostazioni di fabbrica

Per ripristinare le impostazioni di fabbrica fai clic sul pulsante **Restore** nel gruppo **Default settings**, nella parte in basso a sinistra della finestra di programmazione. Il ripristino cancella tutte le impostazioni – anche l'elenco utenti e le password –, perciò prima conviene salvare le impostazioni in un file (**Save [F9]**).



Figura 50. TrikdisConfig – il pulsante **Restore** del gruppo **Default settings** sopra la barra di stato.

5.10 Segnalazione dello stato del cancello

L'app Protegus 2 e il widget possono mostrare lo stato reale del cancello (aperto o chiuso). Per questo l'ingresso **1 IN** del GATOR va collegato all'uscita di stato dell'automazione del cancello o al finecorsa del cancello (punto 3.5), e poi nel programma l'ingresso va assegnato all'uscita che comanda il cancello:

1. Nella pagina **IN/OUT** l'**1 IN** deve avere la funzione **Input**, con il tipo adatto al contatto (nell'esempio NO). Nella riga di **5 OUT**, nella colonna **Assign IN**, scegli l'ingresso **1 IN**.
2. Se vuoi ricevere anche un SMS sull'apertura e la chiusura del cancello, scrivi i testi **SMS event text** e **SMS restore text** di 1 IN (per esempio „Cancello aperto” / „Cancello chiuso”).

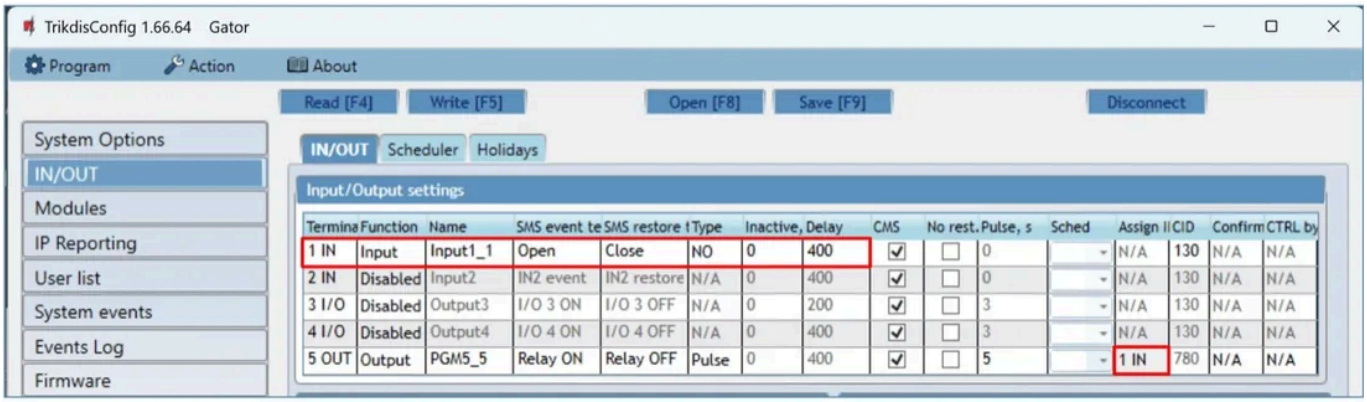


Figura 51. TrikdisConfig – IN/OUT: l'ingresso **1 IN** (NO, con testo SMS **Open** / **Close**), nella riga di **5 OUT**, nella colonna **Assign IN**, l'**1 IN**.

3. Nella pagina **User list**, nella riga dell'utente, fai clic sul pulsante **More settings** e nel gruppo **SMS notification for** spunta la casella **IN1**, così l'utente riceve un SMS sullo stato del cancello. Fai clic sul pulsante **Save**, poi scrivi le impostazioni (**Write [F5]**).



Figura 52. TrikdisConfig – User list: il pulsante **More settings** nella riga dell'utente.

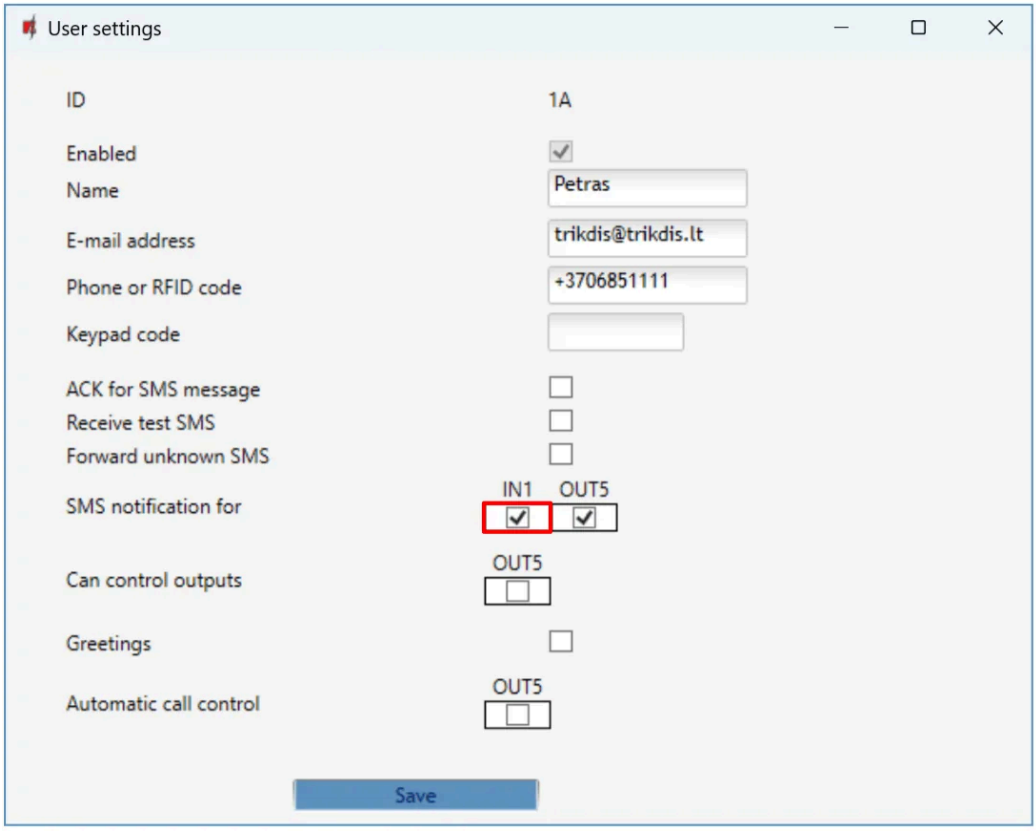


Figura 53. TrikdisConfig – User settings: nel gruppo **SMS notification for IN1** (e **OUT5**) spuntati, in basso il pulsante **Save**.

6. Programmazione a distanza

Le impostazioni del GATOR le puoi leggere e modificare anche a distanza, tramite il cloud Protegus – senza andare sul posto.

Condizioni per la programmazione a distanza

In TrikdisConfig, nella pagina **IP Reporting**, deve essere spuntato **Enable cloud service** (punto 5.5; via SMS: `CONNECT 123456 PROTEGUS=ON`), l'alimentazione deve essere corretta (il LED **POWER** lampeggia in verde) e il dispositivo deve essere in rete (il LED **NETWORK** è acceso in verde e lampeggia in giallo). Se queste condizioni non sono soddisfatte, il dispositivo non è raggiungibile a distanza.

1. Scarica e installa l'ultima versione di TrikdisConfig dal sito di Trikdis (https://www.trikdis.com), se non è ancora sul tuo computer.
2. Assicurati che il GATOR sia connesso a Internet e che il cloud Protegus sia attivo.
3. Avvia TrikdisConfig. Nella sezione **Remote access** della schermata iniziale, nel campo **Unique ID**, scrivi il numero **IMEI** del GATOR (si trova sull'etichetta sul fondo del dispositivo e sulla scatola; con la connessione USB lo vedi anche nella barra di stato).
4. Nel campo **System Name** scrivi un nome a piacere (per esempio il nome dell'oggetto) e fai clic sul pulsante **Configure**.

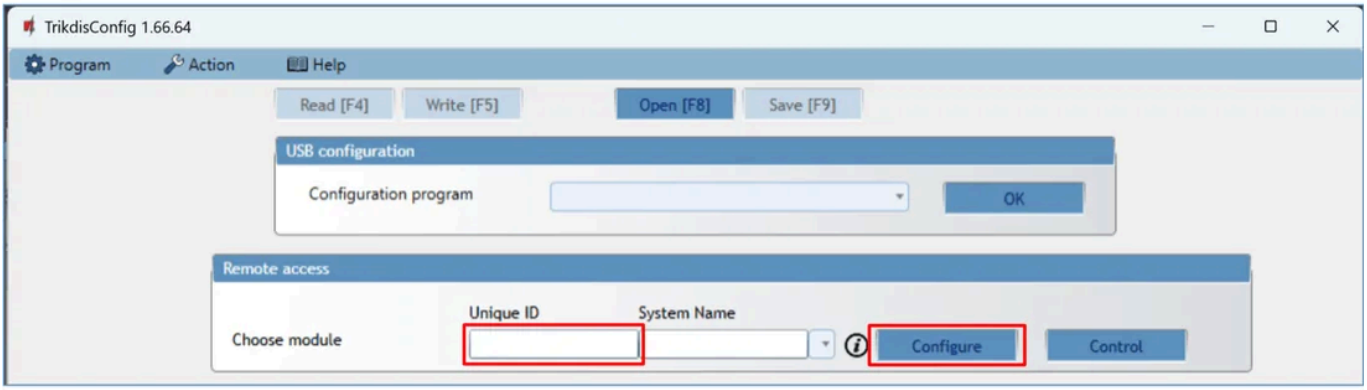


Figura 54. TrikdisConfig – la sezione **Remote access**: il campo **Unique ID**, il campo **System Name** e il pulsante **Configure**.

5. Si apre la finestra di programmazione del GATOR. Fai clic sul pulsante **Read [F4]**: il programma legge le impostazioni attuali del dispositivo. Se il programma chiede il codice di accesso, inserisci il codice di 6 cifre dell'**amministratore**. Se spunti la casella **Remember password** e fai clic sul pulsante **Write [F5]**, il programma memorizza il codice.
6. Esegui le impostazioni e scrivile con il pulsante **Write [F5]**. Alla fine chiudi la connessione con il pulsante **Disconnect** e chiudi il programma.

Per la programmazione a distanza non serve aiuto sul posto: il cliente controlla soltanto l'alimentazione e la rete dai LED. Per modificare l'elenco utenti non serve nemmeno TrikdisConfig – l'amministratore lo gestisce anche da Protegus 2 (punto 4.5) o via SMS (punto 4.7).

7. Verifica del funzionamento

Al termine dell'installazione e della configurazione prova tutto il sistema – sul posto, prima di consegnarlo:

1. **Alimentazione**: il LED **POWER** lampeggia in verde. Se lampeggia in giallo, la tensione di alimentazione non è corretta – misurala sui morsetti di alimentazione (9–32 V DC oppure 12–24 V AC).

2. **Rete**: il LED **NETWORK** è acceso in verde e lampeggia in giallo in base all'intensità del segnale (3 lampeggi sono già sufficienti). Se il LED **TROUBLE** lampeggia, il numero dei lampeggi indica il guasto (punto 1.5).
3. **Ingressi**: attiva uno dopo l'altro gli ingressi collegati (contatto di stato del cancello, pulsante di uscita) e controlla che i destinatari ricevano i messaggi corretti via SMS, in Protegus 2 e alla centrale di vigilanza.
4. **Uscite**: attiva le uscite a distanza – con chiamata, dall'app, via SMS e anche con la tessera, se c'è un lettore – e controlla che il cancello si apra, che i destinatari ricevano i messaggi e che anche nell'app lo stato del cancello segua la realtà (punto 5.10).

Il LED DATA è il modo più semplice per verificare la connessione Internet. Il LED DATA è acceso quando nella memoria del dispositivo c'è un messaggio in attesa di invio. Il verde del LED NETWORK dice soltanto che la connessione di rete è stabilita – nei dispositivi su rete mobile il dispositivo si è registrato sulla rete dell'operatore, in quelli Ethernet il collegamento funziona fino al router –, non che il dispositivo raggiunga anche Internet. Se il LED NETWORK è verde ma il LED DATA resta acceso fisso anche dopo un evento o un rapporto di test, la connessione Internet non funziona: il messaggio non riesce a partire. Su rete mobile la causa più frequente è l'APN o il servizio dati della SIM, su Ethernet il router, il firewall o il DNS. Se il LED DATA si spegne, il messaggio è stato inviato e la connessione dati è a posto.

Lo stato del dispositivo lo puoi chiedere anche via SMS dal telefono dell'amministratore: al comando `INFO 123456` il GATOR risponde con il suo tipo, l'intensità del segnale, la tensione di alimentazione, la versione del firmware, la data e l'ora (punto 4.7). Se l'SMS di risposta non arriva, controlla che per l'amministratore sia attivo **ACK for SMS message** (punto 5.6).

8. Aggiornamento del firmware

Se il GATOR è collegato a TrikdisConfig ed esiste un firmware più recente, il programma propone da solo l'aggiornamento – per questo il computer deve essere connesso a Internet. Se sul computer è attivo un antivirus, può bloccare l'aggiornamento automatico; in questo caso consenti TrikdisConfig nell'antivirus.

Puoi aggiornare il firmware anche da solo – a una versione più recente e, se necessario, anche a una precedente. Dopo l'aggiornamento tutte le impostazioni del dispositivo restano invariate.

1. Avvia il software TrikdisConfig e collega il dispositivo con il cavo USB, oppure accedi alla sua programmazione da remoto.
2. Se c'è un firmware più recente, il programma ne propone il download – accetta.
3. Scegli la pagina **Firmware** e fai clic sul pulsante **Open firmware**. Seleziona il file del firmware.
4. Premi il pulsante **Update [F12]**, attendi la fine dell'aggiornamento, poi nella finestra che compare fai clic su **OK**. Nel frattempo non scollegare il cavo e non interrompere la connessione.

I file del firmware si trovano nella cartella di installazione di TrikdisConfig, all'interno della sottocartella **Firmwares**, nella cartella con il nome del dispositivo. Se questa cartella non c'è, o non esiste un aggiornamento per il dispositivo, oppure va aggiornato il software TrikdisConfig stesso. I file più recenti si possono scaricare anche dal sito del produttore, dalla pagina del dispositivo, come utente registrato.

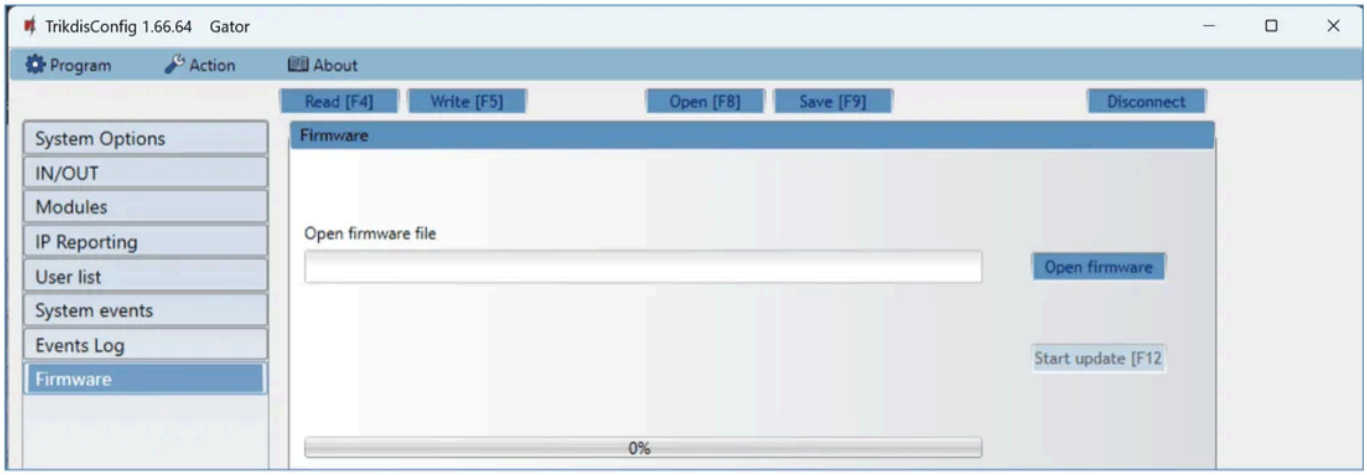


Figura 55. TrikdisConfig – GATOR, pagina **Firmware**: il pulsante **Open firmware**, il campo del file selezionato, il pulsante **Start update [F12]** e l'indicatore di avanzamento.

Per il GATOR la scritta del pulsante che avvia l'aggiornamento è **Start update [F12]**. Per usare i moduli RF-LORA e iO-LORA serve almeno il firmware **2.13**, per i moduli W485 ed E485 almeno l'**1.06**; la versione attuale la vedi nel campo **FW** della barra di stato (punto 5.1).

9. Ricerca guasti e domande frequenti

Se il dispositivo non fa quello che ti aspetti, guarda prima i LED (punto 1.5), poi i punti qui sotto.

Il LED TROUBLE lampeggia – che cosa significa il numero di lampeggi?

Il numero di lampeggi indica la causa del guasto: **1** – manca la scheda SIM (oppure non fa contatto: estraila e reinseriscila); **2** – il codice PIN della scheda SIM è errato (disattiva la richiesta del PIN in un telefono, oppure scrivi il PIN corretto nel campo **System Options** → **SIM card PIN**); **3** – non riesce a connettersi alla rete mobile (segnale, antenna, se la scheda SIM è attiva, scheda 2G in un dispositivo 4G); **4** – non riesce a connettersi al cloud Protegus o al ricevitore IP primario (dati mobili sulla SIM, APN, indirizzo e porta del ricevitore); **5** – non riesce a connettersi al ricevitore IP di riserva; **6** – l'orologio interno non è impostato (sincronizzazione dell'ora, comando `TIME`); **7** – la tensione di alimentazione non è corretta.

Lo chiamo, ma il GATOR non reagisce

- Se il LED **NETWORK** non è acceso in verde, il dispositivo non è in rete: controlla la scheda SIM (attiva, PIN disattivato, adatta a ricevere chiamate), l'antenna e il segnale (il numero dei lampeggi gialli).
- Se hai già inserito degli utenti, o se la casella **En** della riga **Not authorized** (10) è vuota, il dispositivo accetta chiamate solo dai numeri presenti nell'elenco – il numero di chi chiama deve essere nell'elenco, in formato internazionale (+CC…), abilitato (**En**), con programmazione oraria e periodo di validità validi (punto 5.6).
- Sul telefono di chi chiama il numero non deve essere nascosto, altrimenti il dispositivo non lo può identificare.
- Controlla che il numero non sia nella lista nera (punto 5.6.4).

Con la chiamata non apre, ma dall'app sì

Se al dispositivo è collegato un modulo W485 o E485, nella scheda **Modules** → **Parameters**, nel gruppo **SIM parameters**, controlla la casella **Use dial and SMS when working over internet module**: vuota, il dispositivo non usa la chiamata e l'SMS finché c'è la connessione Internet (punto 5.4). Spuntala se ti serve

anche il controllo con chiamata.

Durante la chiamata non riesco a controllare con la tastiera del telefono

Per il controllo con la tastiera (DTMF) il valore di **System Options** → **Hang-up after** deve essere maggiore di 0, altrimenti il dispositivo rifiuta subito la chiamata (punto 4.2). Sui dispositivi con codice tipo **GV17_2E70** e **GV17_2S70** il controllo DTMF non funziona – il tipo è mostrato dal campo **Device** della barra di stato.

Protegus 2 non trova il dispositivo, oppure il dispositivo non diventa Online

- Nella pagina **IP Reporting** deve essere spuntato **Enable cloud service** (via SMS: `CONNECT 123456 PROTEGUS=ON`), e il LED **TROUBLE** non deve fare 4 lampeggi.
- Sulla scheda SIM deve esserci il servizio dati mobile e l'APN deve essere corretto: nel campo **System Options** → **APN** la casella **Auto** sceglie dall'elenco integrato; se la connessione non si stabilisce, scrivi l'APN dell'operatore (elenco).
- Nell'app l'IMEI deve essere esatto e, se il **Cloud Access Code** non è quello di fabbrica `123456`, inserisci quello corretto.
- Se è tutto a posto, dopo l'aggiunta attendi al massimo 1 minuto (punto 4.3).

Il widget non funziona, oppure non lo trovo

Il widget è disponibile solo su telefoni **Android** (punto 4.4); su iPhone apri dalla schermata iniziale dell'app. Su Android il GATOR deve essere aggiunto ai sistemi e devi aver effettuato l'accesso; se il widget resta grigio, apri una volta l'app e controlla la connessione Internet.

Il lettore RFID non legge la tessera, oppure il GATOR non reagisce

- Controlla il collegamento secondo lo schema del punto 3.6 (con un lettore **D0** → **1 IN**, **D1** → **2 IN**; con il secondo lettore **D0** → **3 I/O**, **D1** → **4 I/O**; punto negativo comune) e l'alimentazione del lettore: con un lettore a 12 V il GATOR deve funzionare con **alimentazione DC**, con un lettore con livello del segnale di 5 V spunta la casella **Low voltage reader**.
- Nella pagina **IN/OUT** il **Wiegand reader mode** deve corrispondere al numero dei lettori (**Single** / **Dual**), e **3 I/O**, **4 I/O** non devono essere impostati su un'altra funzione.
- Se il dispositivo non riconosce i segnali del lettore, prova la casella **Disable reader filter**.
- La tessera deve essere nella tabella **User list** (registrata o inserita con il suo numero), abilitata, con l'uscita del lettore (punto 5.6.2). Il registro eventi (punto 5.8) mostra se la lettura è avvenuta e perché è stata rifiutata (**Access denied**).

Nell'app non si vede lo stato reale del cancello

Per la segnalazione dello stato del cancello l'uscita di stato dell'automazione o il finecorsa del cancello va collegato all'ingresso **1 IN** (punto 3.5), nella pagina **IN/OUT** va impostato il tipo dell'ingresso in base al contatto e, nella riga di **5 OUT**, nella colonna **Assign IN**, va scelto l'ingresso **1 IN** (punto 5.10). Dopo di che nell'app l'icona dell'uscita mostra lo stato dell'ingresso.

Il dispositivo non risponde ai comandi SMS

- Accetta comandi SMS solo dai numeri degli **amministratori** (1A–7A); il primo che chiama o invia un SMS diventa l'amministratore. Se non sai chi è, leggi la tabella **User list** in TrikdisConfig.
- Nel comando la password deve seguire la parola di comando, con uno spazio (`INFO 123456`); la nuova password è di 6 caratteri.
- L'SMS di risposta arriva solo se per l'amministratore è spuntato **ACK for SMS message** (punto 5.6).

- Se il dispositivo funziona con un modulo Internet (W485 / E485) e **Use dial and SMS when working over internet module** è vuoto, durante la connessione Internet non elabora gli SMS (punto 5.4).

Ho dimenticato la password dell'amministratore

La password non si può richiedere. Collegati al dispositivo con il cavo USB e ripristina le impostazioni di fabbrica con il pulsante **Restore** nella parte in basso a sinistra della finestra di programmazione (punto 5.9) – così l'elenco utenti e tutte le impostazioni vengono cancellati, perciò dopo il dispositivo va configurato di nuovo. Se in precedenza hai salvato le impostazioni in un file (**Save [F9]**), dopo il ripristino puoi caricarle con il pulsante **Open [F8]** e devi solo reinserire la password.

Serve una scheda SIM se uso un modulo W485 o E485?

No: con il modulo WiFi W485 o con il modulo Ethernet E485 il GATOR funziona anche senza scheda SIM; il controllo avviene allora dall'app (e con la tessera RFID), senza chiamate e SMS. Nella scheda **Modules** → **Parameters** spunta la casella **Disable indication of the absence of a SIM card**, così il dispositivo non segnala come guasto la mancanza della scheda (punto 5.4). Se vuoi anche la riserva su rete mobile, inserisci una scheda SIM e lascia vuota la casella **Disable the use of SIM card mobile data**.

Voglio controllare più cancelli da un solo dispositivo

Il relè del GATOR comanda un cancello; i morsetti **3 I/O** e **4 I/O**, come uscite a collettore aperto (50 mA), possono pilotare un relè esterno. Per cancelli lontani tra loro, con il ricetrasmettitore **RF-LORA** si possono collegare fino a 8 moduli di espansione senza fili **iO-LORA**, ciascuno con il proprio relè, ingresso e lettore RFID (punto 3.9); per più ingressi e uscite cablati, un modulo di espansione **iO8** o **iO8-LORA** (punto 3.10). Per gli utenti indichi nel campo **Can control output** quale uscita possono comandare.

10. Norme di sicurezza

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.

- Il GATOR può essere installato e sottoposto a manutenzione solo da personale qualificato.
- Prima dell'installazione leggi questo manuale, per evitare errori che possono causare malfunzionamenti o danni all'apparecchiatura.
- **Prima di ogni collegamento elettrico scollega l'alimentazione** – sia quella del GATOR sia quella dell'automazione del cancello.
- Cambiamenti, modifiche o riparazioni non autorizzati dal produttore comportano la perdita della garanzia.
- Rispetta le norme locali sullo smaltimento dei rifiuti: non gettare il dispositivo e i suoi componenti nei rifiuti domestici – consegna il dispositivo dismesso come rifiuto elettronico.

Vedi anche

- Il dispositivo per l'automazione dei cancelli GV17 si può usare con Protegus 2 – il GATOR e l'app insieme.
- GV17 come sistema di controllo accessi e/o rilevazione presenze – lettori RFID, ingresso e uscita, orario di lavoro in Protegus 2.
- Comunicazione dual-path ora anche per l'apricancello GV17 GATOR – modulo W485 / E485 per il GATOR.
- Controllo accessi flessibile e senza fili con il sistema GATOR RF-LoRa – moduli RF-LORA e iO-LORA, più cancelli in un solo sistema.
- Impostazione dell'APN – elenco degli operatori mobili europei – se la connessione dati mobile non si stabilisce.
- App Protegus per Android / iPhone e web – sull'app.
- Documentazione in inglese: docs.trikdis.com – Cellular gate controller GATOR – i manuali di docs.trikdis.com sono in inglese.

Prodotti correlati

Trikdis GV17 - GATOR controllore cancello intelligente 4G GSM / IP

Trikdis GV17 - GATOR controllore cancello intelligente 2G GSM / IP

Trikdis W485 modulo WiFi (RS485) **Trikdis E485 modulo Ethernet (RS485)**

Trikdis RF-LORA modulo di espansione wireless

Trikdis IO-LORA modulo di espansione wireless **Trikdis iO8 modulo di espansione cablato**

Trikdis IO8-LORA modulo di espansione wireless

Trikdis ANT04 antenna GSM adesiva con cavo da 2,5m

Trikdis ME301M antenna GSM magnetica con cavo da 2,5m

Diritti d'autore

Questo manuale è stato realizzato da trikdis.hu e mobilamb.eu. Il testo, la struttura, le nostre illustrazioni e le integrazioni sono di nostra proprietà intellettuale e sono protetti dal diritto d'autore. Senza il nostro consenso non può essere copiato, distribuito né pubblicato su un altro sito web, né in tutto né in parte. Puoi scaricarlo e stamparlo liberamente per installare e usare il prodotto.

I nomi e i loghi Trikdis e Protegus sono marchi di UAB Trikdis.

Versione sempre aggiornata di questo manuale: https://trikdis.it/manuale-gv17