

Gate Control PRO – DIN rail

INSTALLATION AND APPLICATION MANUAL

for device version v10.01

Document version: 1.0 11.04.2025



Product models:

- Gate Control PRO 20 DIN rail – 4G.IN4.R2
- Gate Control PRO 1000 DIN rail – 4G.IN4.R2
- Gate Control PRO 1000 Monitoring DIN rail – ETH.4G.IN4.R2

Table of contents

1	General operation of the <i>Gate Control PRO</i>	5
1.1	Emergency control by SMS	6
1.2	Data traffic	6
1.3	Operation of the contact inputs	7
1.3.1	Dedicated input functions	7
2	Processing of personal data	8
2.1	Responsibility of the Manufacturer.....	8
3	Connecting the terminals and putting into operation	9
3.1	Under Voltage Lock Out (UVLO) function	9
3.2	Input wiring	9
3.3	Output wiring.....	9
3.4	Connections.....	10
3.4.1	Wiring diagrams according to output control modes.....	10
3.5	Preparing and installing the SIM card	14
3.6	Connecting the antenna.....	14
3.7	Installation.....	14
3.8	Putting into operation	15
3.9	STATUS and GSM LED signals.....	16
3.10	Technical specification	17
4	Configuring the <i>Gate Control PRO</i> device.....	18
4.1	The user interface and configuration options of the software:.....	18
4.2	Methods of connecting to the device.....	19
4.2.1	Connecting to the device via USB	19
4.2.2	Connecting to the device over the Internet	20
5	<i>Gate Control</i> programming software usage and feature descriptions.....	24
5.1	Connection menu group.....	24
5.1.1	Viewing the settings options and configuring offline	24
5.1.2	Connection type	25
5.1.3	Device register	27
5.1.4	Server register	29
5.2	Device settings menu group	31
5.2.1	General.....	32
5.2.2	Customization.....	37
5.2.3	Inputs.....	39
5.2.4	Reporting channels	43
5.2.5	Input events.....	45
5.2.6	Group rules.....	47
5.2.7	Outputs.....	50
5.2.8	Reports.....	54
5.2.9	IP cameras	56
5.2.10	Scheduled control.....	58
5.2.11	Access templates	61
5.2.12	Remote monitoring events.....	63
5.2.13	Holidays.....	66
5.2.14	Advanced settings	67
5.3	Users menu group	70
5.3.1	Users	71
5.3.2	Mobile devices.....	78
5.3.3	Remote access.....	82

5.4	Device status menu group	85
5.4.1	Status monitoring	85
5.4.2	Event logs.....	89
5.5	Software settings menu group	90
5.5.1	Settings	90
5.5.2	About.....	91
6	Replacing the SIM card	92
7	Updating the firmware	92
7.1	Updating via USB.....	93
7.2	Updating remotely over the Internet.....	93
8	Restoring the factory default settings	94
8.1	Restoring the factory default settings using the programming software.....	94
8.2	Restoring the factory default settings using the PB button.....	94
9	Package content.....	94

Dear Customer,

Thank you for choosing our product. This manual includes important information and instructions regarding the product. Please read this manual before using the product.

The latest version of the product's programming software and manuals are available on the manufacturer's website at: <https://tell.hu/en/products/gsm-automation/gate-control-pro>

► Product models:

Gate Control PRO 20 DIN rail – 4G.IN4.R2

- Capacity of 20 users
- 4G modem that supports the European frequency bands
- DIN rail mount

Gate Control PRO 1000 DIN rail – 4G.IN4.R2

- Capacity of 1000 users
- 4G modem that supports the European frequency bands
- DIN rail mount

Gate Control PRO 1000 Monitoring DIN rail – ETH.4G.IN4.R2

- Capacity of 1000 users
- Ethernet interface
- 4G modem that supports the European frequency bands
- DIN rail mount
- Remote alarm monitoring feature

► Product features:

- Control of outputs over the internet using the mobile application
- Control of outputs by free phone calls using caller identification
- 5 different control modes for compatibility with most gate automation control boards
- 4 NO/NC inputs and 2 NO/NC/COM relay outputs
- 50 configurable access templates
- Configurable holidays
- Scheduled controls
- 20 and 1000 user variants
- Reports the status of the 4 contact inputs by e-mail, SMS or phone call
- Reports events to remote monitoring station over IP, to a primary and a backup receiver
- Supported reporting protocol: TELLMon (TELL custom protocol)

Additional features in the *Monitoring* product variant:

- Compatible TELL monitoring servers and receivers: TELLMon, MVP.next
- Stores the latest 1000 events in the event log memory
- Programmable via USB, the Internet, and mobile application

► Application area:

- Control of garage doors, gates, barriers, electric devices
- Reporting the state of error outputs or switches

► Mobile application:

The device can be used with the **Gate Control PRO** mobile app, available on the following platforms:

Minimal system requirements:

- Android: 6
- iOS: 10



1 General operation of the **Gate Control PRO**

The **Gate Control PRO** device was basically designed for control of electric gates and barriers. However, it can be used to control other devices as well. Controlling can be performed according to the configured control mode by making a phone call to the SIM card installed into the device and/or over the internet, using the mobile application. For compatibility with most gate automation control boards, upon setup you can choose out of 5 different control modes, the one which is appropriate for your gate automation. In case of controlling by call, the system uses caller identification to identify the caller/user. Since to identify the caller and perform the control it is sufficient to identify the caller ID, the system rejects the call, thereby the call will be free of charge. However, it is possible that the mobile service provider applies a call set-up fee on rejected calls (this is operator-dependent, please ask your mobile service provider). When calling from an authorized phone number, the device rejects the call and activates the appropriate output(s) and stores the event in the event logs. When controlling by mobile application, the system identifies the user by the identifier of the smart device, which can be read from the Gate Control mobile application.

Depending on the product variant, the system supports up to 20 or 1000 users to which different permissions and access periods, as well as custom access rules can be assigned. The access periods can be configured by access templates which can be assigned to users. The system will accept control commands from the given user within the access period and will reject them when out of the period.

The services to be activated on the SIM card installed into the **Gate Control PRO** device should be chosen according to which services of the device you want to use. For usage with the mobile application and for the functions that use e-mail sending mobile internet service is necessary. The functions that use SMS sending need SMS service and the ones that use calls require voice call service. For accessing the Internet, the SIM card may use either a public or a private APN, but in case of using a SIM card that works in a private APN, accessing the cloud server IP address in the given APN must be specifically enabled at the mobile service provider.

Attention! If you do not connect the gate's position limit switch to the **Gate Control PRO** device, the system will not have information about the open/closed state of the gate. In this case the alternative control options (remote controller, pushbutton, etc.) used parallel with the device may cause malfunctions, since the device will not be notified about opening and closing the gate with e.g., a remote controller.

1.1 Emergency control by SMS

In case of emergency, it is possible to hold the gate locked in open state, respectively close the gate by sending commands in text (SMS) messages to the phone number of the SIM card installed in the device. In case of emergency opening, the device will open the gate and will close it back only when it receives the emergency closing command. The device accepts the emergency opening and closing commands from different users as well. You can find the settings for this function in the “**General**” device settings menu.

Only **Admin** or **Super admin** users registered in the device are authorized to use emergency control. For this, it is necessary to register the username in the “**Users**” menu, and a remote access password in the “**Remote access**” menu, which the user must write in the SMS message to validate his permission. Otherwise, the device will reject the emergency control request. Providing the user’s phone number is not necessarily required for using this function. For example, if it is needed to grant access to a remote monitoring company or the firefighters, the phone number which they will use to control the gate might not be necessarily known in advance. Therefore, for this function the device will not verify the user phone number for identification, but the username and the remote access password. Further on, it will also disregard the output control permissions configured for the given user, i.e., in case of emergency control it enables control of any output, regardless to the output control permission settings.

Attention! The username used with this function must not contain accented characters!

If the emergency control function is enabled in the settings, you can control the device using the following SMS commands, depending on the configured control mode (see chapter “[Outputs](#)”):

For control modes 1 and 2:

SMS message to be sent	Action
OPEN1,username,password	Control output OUT1 (open)
OPEN2,username,password	Control output OUT2 (open)
OPEN,username,password	Control outputs OUT1 and OUT2 at the same time (open)
CLOSE,username,password	Control outputs OUT1 and OUT2 at the same time (close)

For control modes 3, 4 and 5:

SMS message to be sent	Action
OPEN,username,password	Open
CLOSE,username,password	Close

1.2 Data traffic

The expected data traffic on the SIM card installed in the **Gate Control PRO** device may reach even up to ~20 MB per month at a minimal use. (For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.) The extent of data usage depends on the frequency of use, stability of the mobile network, and the services used. The services that use data traffic, such as control by mobile application, remote programming, remote download of event logs, remote firmware update, sending of emails and reports, all contribute to the increase of the SIM card’s data usage. The extent of the data usage increase depends on how frequently and for how long the mentioned services are used. Therefore, depending on the usage of the device, the data usage may reach even the multiple of the amount mentioned for minimal data usage.

For the product variant with an Ethernet port: If the wired Internet is connected, the device will use mobile data as a backup only in the event of a wired Internet outage. In this case, to avoid interruption of online processes, the device reverts to the wired Internet use only after the scheduled daily restart or a manual restart.

1.3 Operation of the contact inputs

The device has 4 configurable NO/NC contact inputs. By activating the inputs, notifications can be sent by SMS or call up to 4 phone numbers, or by e-mail, according to the settings. This function can be used for e.g., sending notification by SMS or e-mail about the state of tamper or other switches, control board error or other outputs. You can configure the recipient phone numbers and e-mail addresses in the programming software, in the “**Reporting channels**” menu. Associating the contact details with input events can be done in the “**Input events**” menu. You can configure the properties of the inputs in the “**Inputs**” menu.

1.3.1 Dedicated input functions

In addition to the notification functions mentioned above, depending on the input settings, **inputs IN1** and **IN2** can be used for doorbell or technical error notification via Push message, or for output control, i.e., for opening the gate by an external dry contact. In case of using output control mode 1 or 2, you can also select the output (OUT1 or OUT2) to be controlled by the given input.

- **Doorbell function:** if the system is used with the mobile application, the system will send a “**Doorbell**” Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering the given input. If you connect your doorbell to the given input, this way, enabled mobile devices will be notified via Push message about doorbell ringing.
- **Technical error notification function:** if the system is used with the mobile application, the system will send a “**Technical or device failure**” Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering the given input.

The Push message text sent by the dedicated input functions cannot be changed. You can enable Push messages for each mobile device separately in the “**Mobile devices**” menu in the programming software. Push message sending works via the Internet using Push notification service, which is free of charge.

Inputs IN3 and IN4: in addition to the notification functions mentioned above, inputs IN3 and IN4 are dedicated by factory default to gate position limit switches (for detecting the position limit of gates). In case of using control mode 1 or 2, the position limit switch of gate “A” should be connected to input IN3, while the position limit switch of gate “B” should be connected to input IN4. In case of using control modes 3, 4 or 5 the gate’s position limit switch should be connected to input IN3. If the position limit switch is connected, the system can send notifications via Push and/or SMS when the gate fails to open or close.

You can configure the gate position limit switches in the “**Inputs**” menu in the programming software. You can enable SMS-based error notifications for each user separately in the “**Users**” menu, and Push-based error notifications for each mobile device separately in the “**Mobile devices**” menu. You can change the message text in the “**Customization**” menu, if needed.

2 Processing of personal data

The users can control the system with the help of their usernames, phone numbers and/or mobile application identifiers, therefore, to operate the system, it is necessary that users who want to use the system, provide their names (usernames) and phone numbers (hereinafter referred to as personal data) to the system administrators configured in the device, who will write these personal data into the system. Users can provide the personal data directly, or indirectly with the help of a registration request sent using the mobile application used to control the system. When sending a registration request, the mobile application identifier will also be forwarded automatically.

Users' consent to processing their personal data shall be deemed to be given based on their clear and explicit consent by providing voluntarily the personal data in a direct or indirect way. The purpose of personal data processing is to ensure access to the system and thus to provide permission of use for users who want to use the system.

The system stores the personal data in the device's memory. The personal data are not accessible for third party, except for the system operator/installer and the assigned system administrators. The assigned system administrators are obliged to treat the personal data confidentially, in line with the legislative provisions, and shall not disclose the data to third party.

2.1 Responsibility of the Manufacturer

The Manufacturer takes any kind of responsibility for and in connection with the functionality and use of the system – including proper use of hardware and software – according to the relevant provisions of law. The Manufacturer takes no responsibility for damage resulting from:

- the user having lost the device for controlling the system, or this device or his personal data mentioned above having been stolen, thus enabling an unauthorized person to have access to the system;
- the user having intentionally, in good faith, directly or indirectly given his personal data or the device suitable for controlling the system to a third person.

3 Connecting the terminals and putting into operation

3.1 Under Voltage Lock Out (UVLO) function



The product is provided with built-in automatic power disconnection (Under Voltage Lock Out) function. The device will turn off automatically when the supply voltage drops under a critical level, and turns back on when the voltage restores to operational level.

3.2 Input wiring

For the inputs, the normally closed or normally open dry contact should be connected between the given input (**IN1...IN4**) and the **GND** terminal.

If a normally open dry contact trigger is used, choose the **NO** (normally open) option at the given input's settings. In this case, the input becomes activated, and the configured notifications will be sent when the open contact between the given input (**IN1...IN4**) and the **GND** terminal is closed.

If a normally closed dry contact trigger is used, choose the **NC** (normally closed) option at the given input's settings. In this case, the input becomes activated, and the configured notifications will be sent when the closed contact between the given input (**IN1...IN4**) and the **GND** terminal is opened.

- **Connecting the gate position limit switch:**

When using control mode 1 or 2 with a single gate, the position limit switch of the gate controlled by output OUT1 should be connected to input IN3. If two gates are controlled, the position limit switch of the gate controlled by output OUT2 should be connected to input IN4. For control modes 3, 4 and 5 the position limit switch of the gate should be connected to input IN3.

3.3 Output wiring

Connecting the outputs should be done according to the output control mode chosen. The default state of the outputs for given control modes is the following:

For control modes 1, 2, 4, 5:

OUT1: in an idle state by default (open relay contact between **NO** and **COM**)

OUT2: in an idle state by default (open relay contact between **NO** and **COM**)

For control mode 3:

OUT1: in an idle state by default (open relay contact between **NO** and **COM**)

OUT2: in an activated state by default (closed relay contact between **NO** and **COM**)

The output which is by default in an idle state provides an open contact between the **NO** and **COM** terminals, and a closed contact when controlled.

The output which is by default in an activated state provides a closed contact between the **NO** and **COM** terminals, and an open contact when controlled.

The outputs provide dry (potential free) relay contacts. The relay contacts can take a maximum load of **1A@24V DC**.

You can find a detailed description about control modes in the "[Outputs](#)" chapter.

3.4 Connections

Attention! Do NOT connect the metallic parts of the antenna connector or the device's terminals directly or indirectly to the protective ground, because this may damage the device!

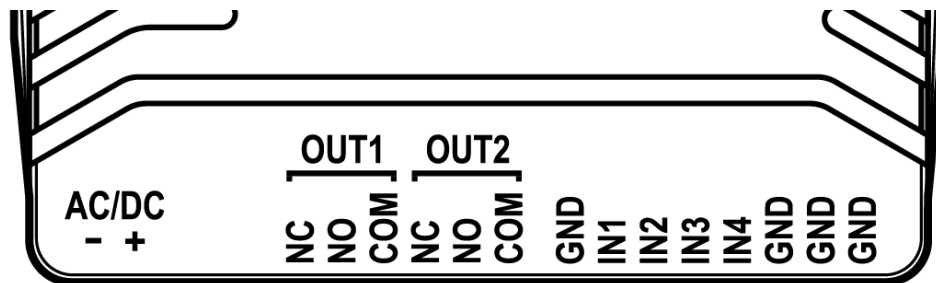
A power supply with adequate power is essential for the product to operate properly. The power supply must provide a power that can serve the minimum operating voltage and the maximum power consumption of the device. The power feed must be continuous and transient-free.

An ideal solution for the above purposes is the power supply designed and manufactured by TELL, which we expressly recommend using for our devices.

- Recommended TELL power supply: **TT25VA-12V5**.

3.4.1 Wiring diagrams according to output control modes

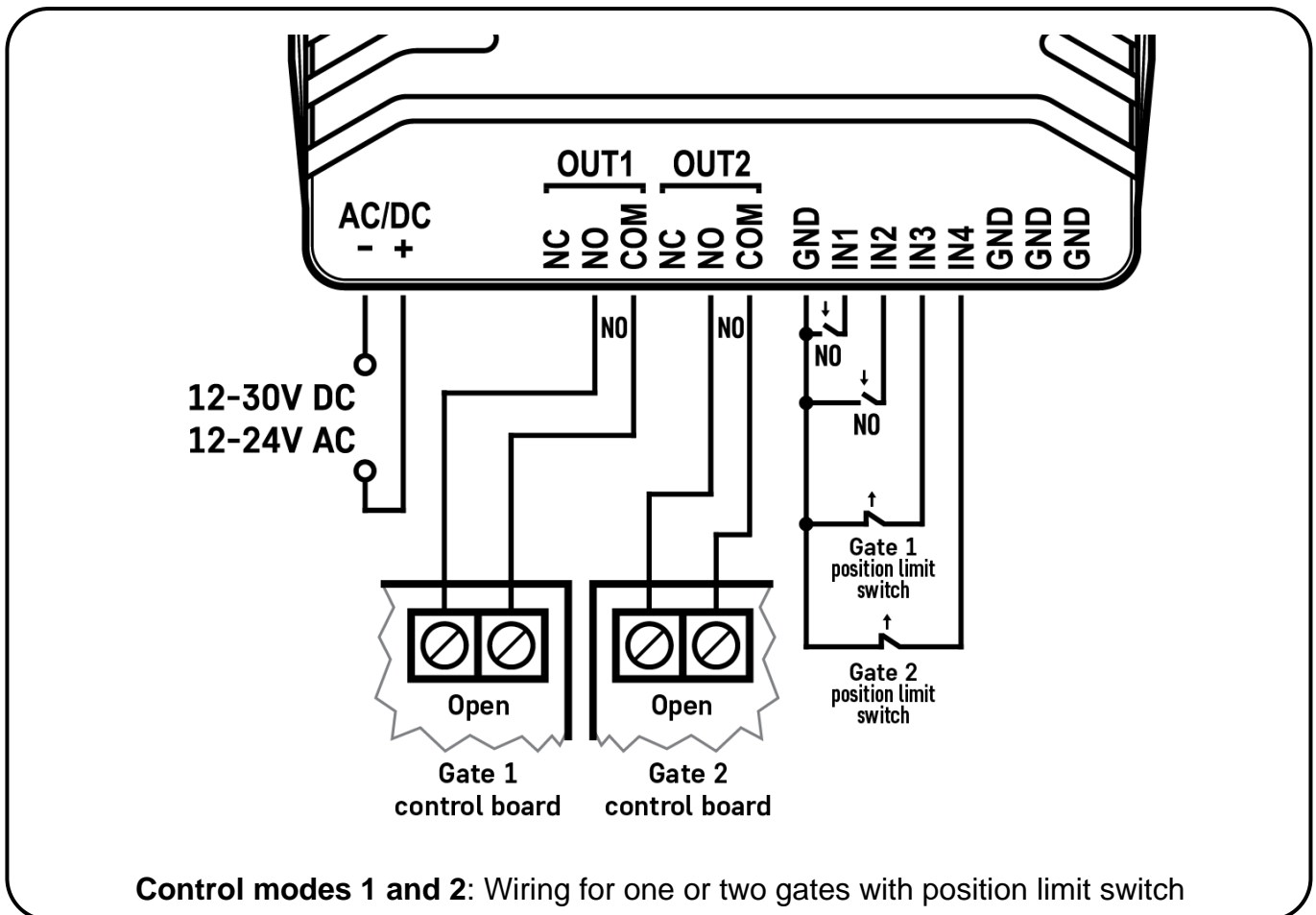
System terminal inputs and outputs:



AC/DC	-	Power input (negative for DC)	12-30VDC or 12-24VAC minimum 500mA
	+	Power input (positive for DC)	
OUT1	NC	Normally closed terminal	Relay output 1 (dry contacts) max. 1A / 24V DC
	NO	Normally open terminal	
	COM	Common terminal	
OUT2	NC	Normally closed terminal	Relay output 2 (dry contacts) max. 1A / 24V DC
	NO	Normally open terminal	
	COM	Common terminal	
IN1		Contact input 1	Use potential free (dry) contacts only
IN2		Contact input 2	
IN3		Contact input 3	
IN4		Contact input 4	
GND		Common terminal of the contact inputs	

Control mode 1:

- For one or two gates, or one gate with two opening options (partial/total opening).
- Both outputs are in an idle state by default and are activated when controlled.
- OUT1 is controlled by calls with caller identification.
- OUT2 is controlled by calls from private (hidden) numbers.
- You can control both outputs separately with the mobile app.
- Gate position limit switches can be connected to inputs IN3 (for gate No. 1) and IN4 (for gate No. 2).
- A control call/command only opens the gate. Closing must be done automatically by the gate automation control board.

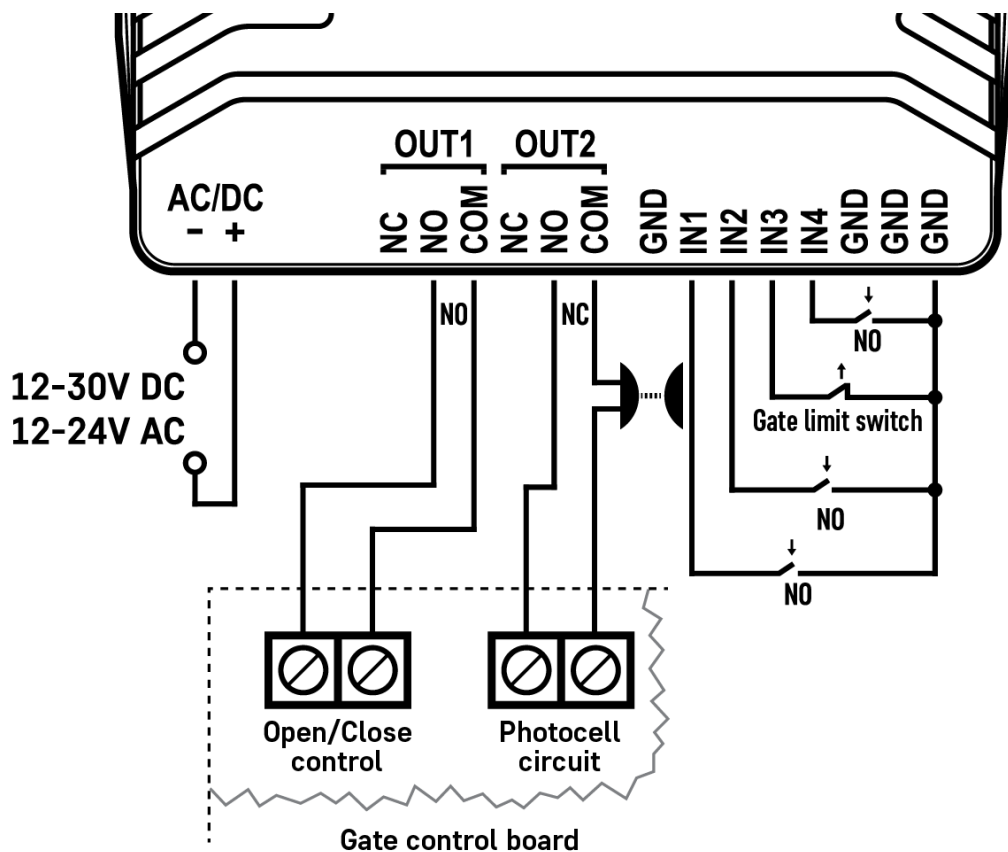


Control mode 2:

- For one or two gates, or one gate with two opening options (partial/total opening).
- Both outputs are in an idle state by default and are activated when controlled.
- Both outputs are controlled by calls with caller identification as configured (OUT1 only, OUT2 only, or both at the same time).
- You can control both outputs separately with the mobile app.
- Output control permission can be configured separately for each user and each output.
- Gate position limit switches can be connected to inputs IN3 (for gate No. 1) and IN4 (for gate No. 2).
- A control call/command only opens the gate. Closing must be done automatically by the gate automation control board.

Control mode 3:

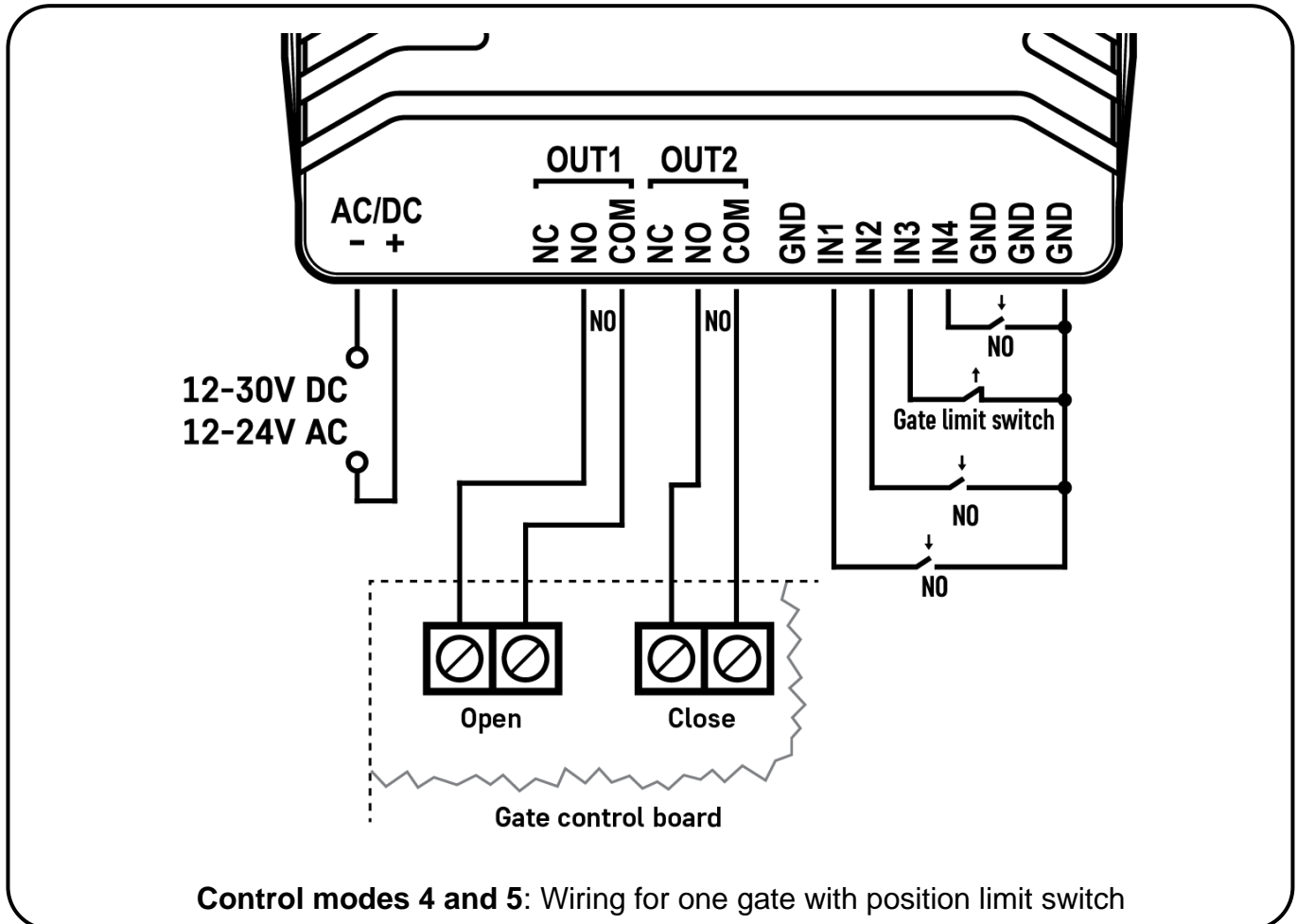
- For single-gate automations that require triggers for opening and closing on the same input.
- Opening and then closing by a single call/control command.
- Output OUT1 is in an idle state, while OUT2 is activated by default.
- Output OUT1 is used to control the gate, while OUT2 is used to interrupt the photocell sensor circuit, thereby providing an option to hold the gate locked in open state for the configured period.
- Holding the gate locked in an open state permanently on a second call/control command.
- The gate position limit switch can be connected to input IN3.



Control mode 3: Wiring for one gate with photocell control and position limit switch

Control mode 4:

- For single-gate automations that require triggers for opening and closing on different inputs.
- Opening and then closing by a single call/control command.
- Both outputs are in an idle state by default and are activated when controlled.
- The opening trigger is provided by output OUT1, and the closing trigger is provided by output OUT2.
- Holding the gate locked in an open state permanently on a second call/control command.
- The gate position limit switch can be connected to input IN3.

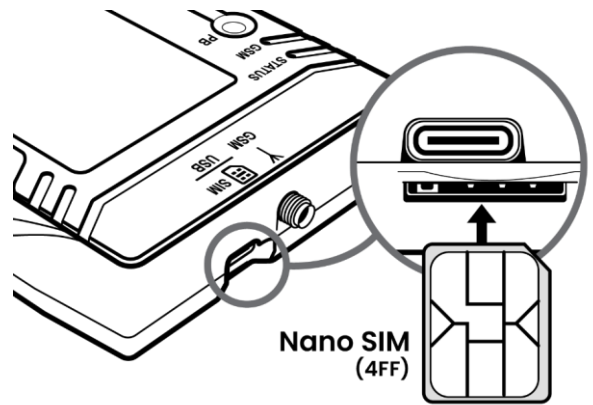


Control mode 5:

- For single-gate automations that require triggers for opening and closing on different inputs.
- Opening and then closing by separate calls/control commands.
- Both outputs are in an idle state by default and are activated when controlled.
- The opening trigger is provided by output OUT1, and the closing trigger is provided by output OUT2.
- The gate position limit switch can be connected to input IN3.

3.5 Preparing and installing the SIM card

- The device requires a Nano (4FF) size SIM card.
- The services to be activated on the SIM card installed in the **Gate Control PRO** device should be chosen according to which services of the device you want to use. Mobile Internet service is necessary for use with the mobile application, and for the functions that use e-mail sending. The functions that use SMS sending need SMS service, and the ones that use calls require voice call and VoLTE service. For accessing the Internet, the SIM card may use either a public or a private APN, but in case of using a SIM card that works in a private APN, accessing the cloud server IP address in the given APN must be specifically enabled at the mobile service provider.
- Disable voicemail and notification in SMS about missed calls on the SIM card installed in the device.
- Ask the service provider to activate the VoLTE service on the SIM card. This is essential for voice calls to work on the 4G network.
- The device can manage the SIM card's PIN code. If you enable PIN code request on the SIM card, configure the SIM card's PIN code in the "General" device settings menu in the programming software. Otherwise, disable PIN code request on the SIM card.
- Enable caller identification and caller ID transmission service on the SIM card at the mobile service provider (these services might not be enabled by default, please check). To enable these services, install the SIM card into a mobile phone, and call the customer service of the card's mobile service provider, and enable the services in the menu, or visit one of the service provider's personal customer services, and ask them to enable these services on the SIM card.
- Install the SIM card as shown in the figure above. Push the card into the socket until you hear a click. If you want to remove the SIM card, press it again, and then pull it out.



3.6 Connecting the antenna

Connect the antenna to the SMA-F socket. The device comes with an antenna which provides good transmission under normal reception circumstances. In case of experiencing signal strength problems or/and wave interference (fading), use another (directed) type of antenna or find a more suitable mounting place for the antenna.

3.7 Installation

Please check the environment before installing:

- Verify the GSM signal level with your mobile phone. It may happen that the signal strength is not sufficient in the desired mounting place. In this case the planned installation place can be changed before mounting the device.
- Do not mount the unit in places where it could be affected by strong electromagnetic disturbances (e.g., in the vicinity of electric motors, high voltage, etc.).
- Do not mount the unit in wet places or places with a high degree of humidity.

3.8 Putting into operation

- Check the firmware version of your device in the “**Status monitoring**” menu, and update the firmware if a newer version is available.
(Downloads: <https://www.tell.hu/en/downloads>, instructions: [Updating the firmware](#)).
- Make sure that the SIM card is installed correctly in the device.
- Make sure that the antenna is connected correctly to the device.
- Make sure that the wires are connected correctly.
- You can now power up the device (12-30V DC or 12-24V AC). Make sure that the power source provides sufficient power for the operation of the **Gate Control PRO** device. The nominal current consumption of the **Gate Control PRO** device is 130mA, however, it may rise to 500mA during communication and relay control. If the applied power source does not provide sufficient power for the operation of the device, this may cause malfunctions. In this case, you can order an auxiliary power adapter separately from the manufacturer.
Attention! USB power is not sufficient to operate the device! Proper operation of the device is not guaranteed if it is powered from USB only!
- Check the system time in the “**Status monitoring**” menu in the programming software. The correct system time is necessary for a proper operation of the device. The device can synchronize the date and time automatically from the mobile network or via cloud connection. However, not all mobile operators provide the date and time, or the wrong date and time is received. In such case the device can only synchronize the date and time from the cloud. If the system time is wrong, try the following options:
 - Make sure that the “**Cloud usage**” option is enabled in the “**General**” settings menu. The cloud connection requires Internet connection (via the Ethernet or mobile Internet on the SIM card installed in the device).
 - If you are using the device with mobile Internet only, set the APN manually in the “**General**” settings menu.
 - You can also synchronize the date and time manually in the “**Status monitoring**” menu but with this option it is not guaranteed that the device can keep the time setting accurate on a long term due to power outages or device restarts caused by connection issues.

3.9 STATUS and GSM LED signals

Gate Control PRO 20/1000 DIN rail – 4G.IN4.R2		
STATUS LED	Flashing green	• Connected to the mobile network
	Flashing red	• System startup/restart
	Permanent red	• Connecting to the mobile network • PIN code request • SIM card error
	Permanent green	• Bootloader mode • Firmware upload via USB
GSM LED	Permanent ON	• Searching for network
	200ms ON, 200ms OFF	• Data transmission
	800ms ON, 800ms OFF	• Registered on the network
	Permanent OFF	• Modem powered off

Gate Control PRO 1000 Monitoring DIN rail – ETH.4G.IN4.R2			
		LAN mode, modem disabled	LAN + modem mode
STATUS LED	Flashing green	• Connected to cloud	• Connected to cloud
	Flashing red	• Connecting to LAN • System startup/restart	• LAN and mobile connection lost • System startup/restart
	Permanent red	-	• Connecting to LAN • Connecting to the mobile network • PIN code request • SIM card error
	Permanent green	• Bootloader mode • Firmware upload via USB	• Bootloader mode • Firmware upload via USB
GSM LED	Permanent ON	• Searching for network	
	200ms ON, 200ms OFF	• Data transmission	
	800ms ON, 800ms OFF	• Registered on the network	
	Permanent OFF	• Modem powered off	

3.10 Technical specification

Supply voltage range:	12-30V DC or 12-24V AC	
Nominal current consumption:	130mA	
Highest current consumption:	500mA@12V DC	
Operating temperature:	-20°C - +70°C	
Transmission frequency (4G modem):	GSM/GPRS/EDGE: 900/1800 MHz LTE/FDD: B1/B3/B5/B7/B8/B20	
Highest load supported on outputs:	1A@24V DC	
Dimensions:	88.4 x 119 x 23.1mm	
Weight (net):	Gate Control PRO 20	135g
	Gate Control PRO 1000	135g
	Gate Control PRO 1000 Monitoring	140g
Weight (packed):	Gate Control PRO 20	296g
	Gate Control PRO 1000	296g
	Gate Control PRO 1000 Monitoring	301g

RF emission power:

Frequency	Power	Minimum power
EGSM900 (GMSK)	33dBm ± 2dB	5dBm ± 5dB
DCS1800 (GMSK)	30dBm ± 2dB	0dBm ± 5dB
EGSM900 (8-PSK)	27dBm ± 3dB	5dBm ± 5dB
DCS1800 (8-PSK)	26dBm +3/-4dB	0dBm ± 5dB
LTE-FDD B1	23dBm +/-2.7dB	<-40dBm
LTE-FDD B3	23dBm +/-2.7dB	<-40dBm
LTE-FDD B5	23dBm +/-2.7dB	<-40dBm
LTE-FDD B7	23dBm +/-2.7dB	<-40dBm
LTE-FDD B8	23dBm +/-2.7dB	<-40dBm
LTE-FDD B20	23dBm +/-2.7dB	<-40dBm

4 Configuring the *Gate Control PRO* device

The **Gate Control PRO** device can be configured as follows:

- by computer via USB, using the programming software
- by computer over the Internet, using the programming software*
- by the mobile application over the Internet (only settings related to user management are available)*

You can read more about configuring by the mobile application in the app's user's manual.

*The functions marked with the * character are only available when the device is connected to the Internet via the Ethernet port (product variant with an Ethernet port), or a SIM card with mobile Internet access is installed in the **Gate Control PRO** device, and the cloud access is configured correctly, i.e., if the device is online, connected to the cloud. If you want to use the system's Internet-based services, it is necessary to configure in advance the settings needed for accessing the Internet. You can learn more about these settings in the "[Ethernet](#)", "[SIM settings](#)" and "[Cloud](#)" paragraphs found in the "[General](#)" device settings chapter.

The **Gate Control** programming software is compatible with the following operating systems:

- **Windows 10 (32/64 bit)**

Earlier Windows operating systems are not supported by the software.

Installing the programming software: open the software setup application and follow the instructions of the installation wizard to complete the installation.

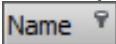

You can download the latest version of the programming software from the manufacturer's website: <https://tell.hu/en/products/gsm-automation/gate-control-pro>

4.1 The user interface and configuration options of the software:

You can select the language of the user interface when you install the software.

You can change the appearance (skin) of the user interface using the "**Theme**" dropdown-menu found in the "**Settings**" menu under the "**Software settings**" menu group, where you can choose out of several appearance themes.

The software saves the changes related to appearance upon closing and applies the saved settings when reopened.

In the menus that contain a spreadsheet, an advanced filter is available in each column by clicking on the filter icon , which appears on the right-hand edge of each column header by moving the mouse pointer on the given header. You can use the filters to filter data in any column. You can toggle between ascending and descending data sorting by clicking on a column's header. You can toggle between show/hide columns or change the order of the columns in the spreadsheet by drag-and-drop, after clicking on the button marked with a star  in the top left corner of the spreadsheet. You can also change the order of the columns by moving the header of the columns.

4.2 Methods of connecting to the device

Connection type




For connecting to the device using the programming software, the following options are available:

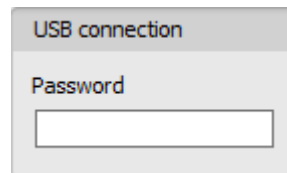
USB: direct connection using a USB-A to USB-C cable.





Cloud: remote connection through the Internet via the cloud server operated by the manufacturer.

4.2.1 Connecting to the device via USB

To start programming the device, follow the instructions below:

- Open the **Gate Control** programming software.
- Select the “**USB**”  option found in the “**Connection type**” menu under the “**Connection**” menu group, power up the device and connect it to the computer using a USB A to USB-C cable. The software connects to the device using standard HID driver, which is integrated in Windows operating systems, thus there is no need to install special USB drivers. The operating system will install the drivers automatically when you first connect the device to USB.
- The program requires the USB password to allow connecting to the device. Enter the device’s USB password in the “**Password**” field found in the “**USB connection**” section. The default password is **1234**.



- Click on the “**Connect**”  button.
- The connection status is shown in the status bar found at the bottom of the program window:
 -  : Connected (green)
 -  : Disconnected (red)
- After the connection has been successfully established, you can read and change settings, manage users, download event logs, and view device status information. The program will read the settings from the device automatically after connecting to the device. If you want to view or manage users or their settings, you need to read the users separately from the device.
- To close the connection, click on “**Disconnect**”  button.

4.2.2 Connecting to the device over the Internet

For connecting via the Internet, it is necessary that the *Gate Control PRO* device you want to connect to uses the cloud service. For this, the “*Cloud usage*” option must be enabled in the “*General*” device settings menu. For connecting via the mobile Internet, the APN settings must be successfully set, and it is also necessary to use a SIM card with available mobile Internet service in the device, which may use either a public or a private APN, but in case of using a SIM card that works in a private APN, accessing the cloud server IP address in the given APN must be specifically enabled at the mobile service provider. The cloud contact details are the following:

Server address:	54.75.242.103
Port number:	2016

With this connection type, connection between the device and the *Gate Control* programming software will be established through the cloud server operated by the manufacturer.

The “*System logs*” option in the programming software is not available when connected remotely over the Internet.

The device can be accessed remotely only by users registered with super admin or admin role, for whom remote access has also been configured. To connect remotely to the device, the username and remote access password configured for the super admin or admin user are required. The default settings include a hidden default superadmin user which can be used to connect to the device remotely over the cloud until a new user is registered with *Super admin* or *Admin* role, and with a remote access password. If there is at least one remote access password added, the default superadmin access will be disabled automatically, and will no longer work. The default superadmin provides full access to remote programming.

Security warning! If you delete all remote access password records, the default superadmin user will be reenabled automatically, and can again be used to connect to the device remotely! The purpose of this is preventing you from locking yourself out from remote access.

The default superadmin credentials are:

Username:	superadmin
Password:	password

The user signing in remotely via the programming software can only access specific settings and options according to its permission level (role). To add a new user, follow the steps specified in the “[Users](#)” chapter. To configure a new remote access, follow the steps specified in the “[Remote access](#)” chapter.


➤ Remote access levels:

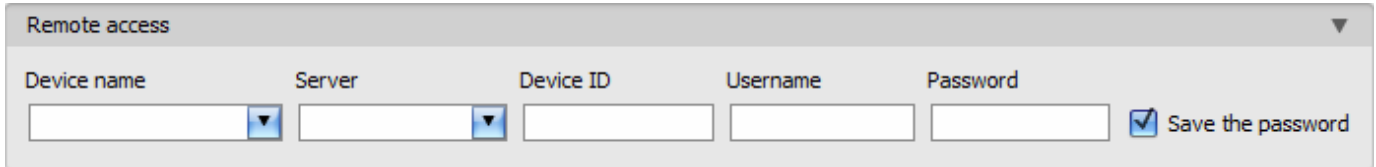
With Super admin role:	Full access, can access all settings.
With Admin role:	Can access the following menus only: Group rules, Scheduled control, Access templates, Remote monitoring events (the “Monitoring” product variant only), Holidays, Users, Mobile devices, Remote access, Status monitoring, Event logs, System logs.
With User role:	Has no remote access permission, cannot access anything, therefore it makes no sense to configure remote access for a normal user.

You can configure the user roles in the user settings, using the “*Role*” drop-down menu.

To make it easier to connect to a device remotely, the program includes a device register which enables you to add device contact details in advance in the program's device register database. You can learn more about this in the "[Device register](#)" chapter.

➤ Connecting to the device over the Internet

For connecting to the device remotely over the Internet, choose the "**Cloud**"  option in the "**Connection type**" menu.



Device name: if you have already added the device contact details in the program's device register, you can select the device you want to connect to from the drop-down menu.


Server: the name of the server where the device is connected. The server named "**Cloud (Gate Control)**" is the default. In case of using a proxy, for connecting remotely to the device, it is possible to configure a server IP address and port number different from the default server, by adding a new server in the "**Server register**" menu. If there are further servers recorded, you can choose the appropriate server for the given device in this drop-down menu, from the recorded servers. The "**Server register**" menu is hidden by default, since it is not necessary in most cases. You can find the option used to enable showing this menu in the "**Software settings / Settings**" menu.





Device ID: the identifier of the **Gate Control PRO** device you want to connect to. You can first read and copy the identifier of the given device in the "**Device ID**" field found in the "**Status monitoring**" menu, when connected via USB.

Username: your superadmin or admin username registered in the "**Users**" menu, which you want to use to connect to the device.

Password: the password registered for the given username in the "**Remote access**" menu.

Save the password: in case that you have provided the data necessary for connecting to the device here in the "**Connection parameters**" section, and you enable this option, the program will also save the entered password in the device register, when you initiate a connection to the device.

- Click on the "**Connection type**" menu and select the "**Cloud**"  option.
- If you have already registered the device in the "**Device register**" menu, select the device you want to connect to from the "**Device name**" drop-down menu. Otherwise, you can either enter the data needed for connecting in the corresponding fields, which will be recorded automatically in the device register using the entered device ID as the device name, when you start connecting to the device. For this, select the server from the "**Server**" drop-down menu, enter the identifier of the device in the "**Device ID**" field, the super admin (or admin) username in the "**Username**" field, and the remote access password configured for that, in the "**Password**" field.

- Click on the “**Connect**”  button and wait for the connection to establish. The connection process may take a few seconds.
- The connection status is shown in the status bar found at the bottom of the program window:
 -  : Connected (green)
 -  : Disconnected (red)
- After the connection has been successfully established, you can read and change settings, manage users, download event logs, and view device status information, depending on your access level.
- To close the connection, click on “**Disconnect**”  button.

Attention! If the modem is currently connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such cases, outgoing calls will block the Internet connection, i.e., a possible remote connection in progress will be suspended for the duration of the call. For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.

Functions that make outgoing calls:

- **notification by call upon activating a contact input**
- **confirmation of controls by call**

➤ **Connecting to the device over the Internet if cloud usage is disabled**

If you are not using the device with the mobile app, and the “**Cloud usage**” option is disabled therefore in the “**General**” device settings menu, the device will only connect to the server upon request. Therefore, before trying to connect remotely to the device, the request for connecting to the cloud must be sent via SMS to the phone number of the SIM card installed in the device:

CONNECT#

The device accepts the command for connecting to the cloud from **Admin** and **Super admin** users only. If the command is sent from any other phone number, the device will ignore the request and will not send a reply.

Send the request command for connecting to the cloud (**CONNECT#**) via SMS to the phone number of the SIM card installed in the **Gate Control PRO**, and wait for the device’s reply. As soon as the device connects to the cloud, it will send the following reply:

Connected to (*IP address:port number*)
ID=(*device identifier*)

The device stays connected to the cloud for 10 minutes, and thereafter, in case of inactivity, it disconnects automatically. Therefore, you have **10 minutes** to connect to the device remotely, after it sends the reply message.

If no reply is received from the device within 1 or 2 minutes, please make sure that the settings are correct and the circumstances of sending the command for connecting satisfy the conditions mentioned above.

Possible error messages:

Missing APN	The APN is not configured.
Network connection error	The device is unable to connect to the Internet due to an error, wrong settings, or unavailable Internet service.





If the APN is not configured, or the configured value is wrong, the Super administrator user can configure that using the following SMS commands (the Admin user has no permission to configure device settings):

SMS command	Specification
*APN=APN#	Configuring the APN
*APN=APN,username,password#	Configuring the APN along with the username and password belonging to it

Example on the use of the commands mentioned above:

***APN=internet#**

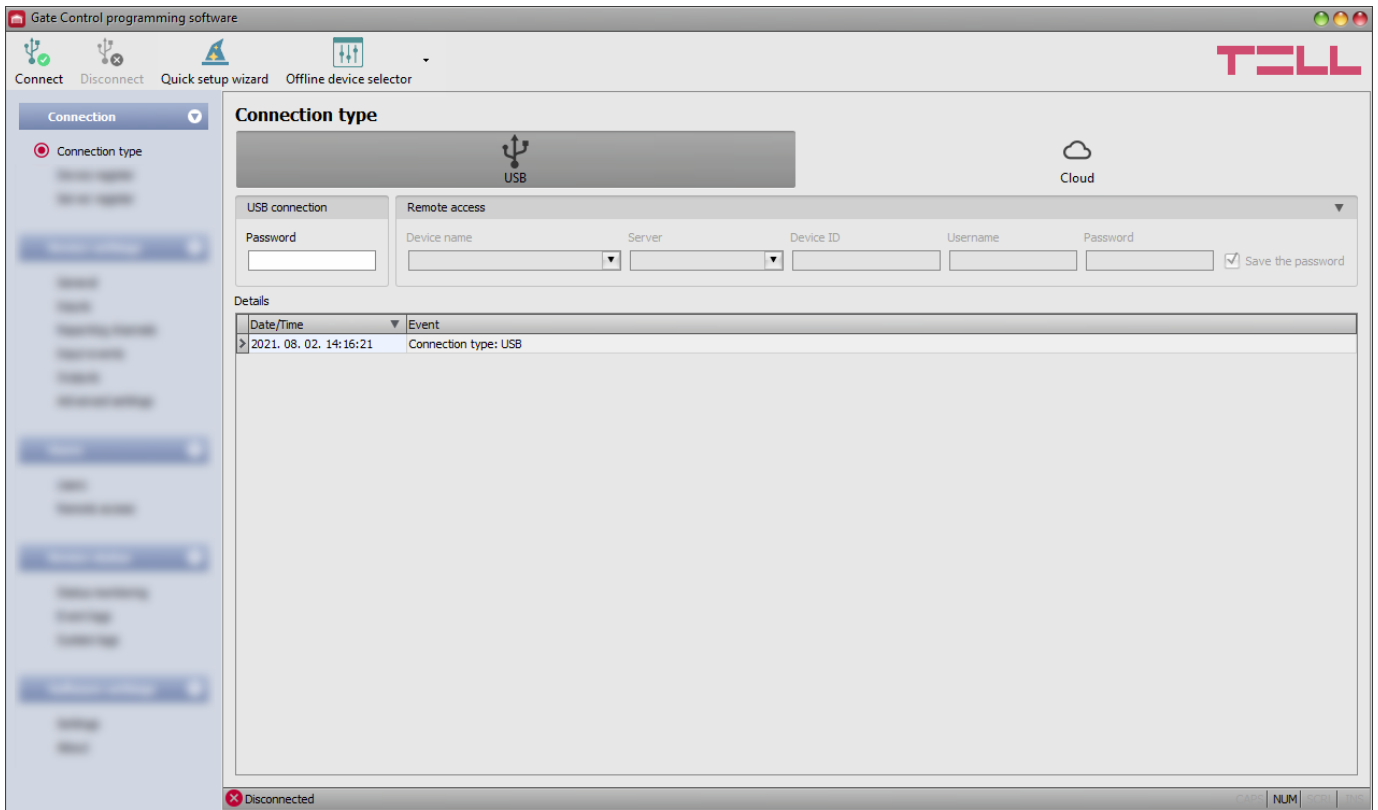
***APN=net,guest,guest#**

- After receiving the reply from the device, click on the “**Connect**”  button and wait for the connection to establish. The connection process may take a few seconds.
- The connection status is shown in the status bar found at the bottom of the program window:
 -  : Connected (green)
 -  : Disconnected (red)
- After the connection has been successfully established, you can read and change settings, manage users, download event logs, and view device status information, depending on your access level.
- To close the connection, click on “**Disconnect**”  button.

5 Gate Control programming software usage and feature descriptions

5.1 Connection menu group



5.1.1 Viewing the settings options and configuring offline



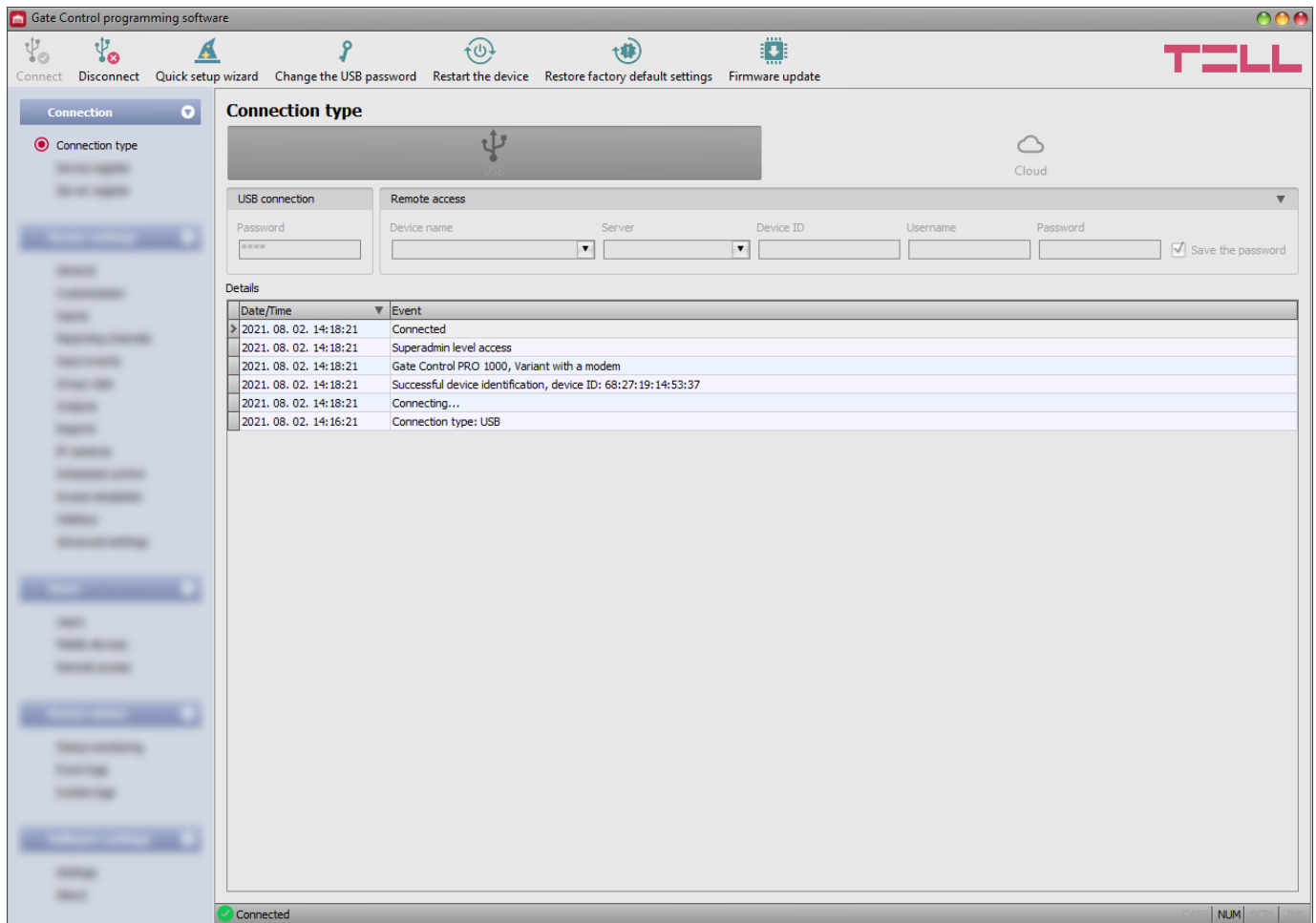
The **Gate Control** programming software supports all **Gate Control PRO** and **BASE** device models, therefore the software shows the settings options available specifically in a given device model, which are different from the common parameters (e.g., differences between the **PRO** and the **BASE**, or device models with a different user capacity) only when the given device model is connected, i.e., a **Gate Control PRO** or **BASE** device must be connected in order to show the specific settings options for that device model.

However, using the “**Offline device selector**” it is possible to view the settings options of the **Gate Control PRO** device and to configure and save the settings in advance offline, without connecting the device.

If you want to view the settings options of a **Gate Control PRO** or **BASE** device model, or to configure and save settings without connecting the device, click on the arrow found next to the

“**Offline device selector**”  button, select the desired device model from the drop-down menu and then click on the “**Offline device selector**”  button to load the settings options of the selected device model.

5.1.2 Connection type



In the “**Connection type**” menu you can select the method of connecting to the device (USB or cloud), view information about the connection process, change the device’s USB password, restart the device, and restore the factory default settings in the device. The default USB password is **1234**.

Details: you can follow the connection progress in this window.


Available options:


- **Quick setup wizard:**



This button is used to start the quick setup wizard, which will guide you through the essential settings and helps you to get the device up and running quickly. The wizard starts automatically if you connect a device with blank settings (e.g., a new device that has not been configured yet, or after performing a factory reset).

- **Changing the USB password:**

 You can change the USB password of the device after clicking on this button. Enter the current USB password, then the new password, confirm the new password, and then click on the “OK” button. The password should consist of at least 4, but not more than 8 characters. Accepted characters are: numbers (0...9), lower case letters (a...z), and capital letters (A...Z).




Attention! The following characters should not be used: ^ ~ < > = ' \" , | ? \$ & %

- **Restarting the device:**


 You can restart the connected device if needed by clicking on this button.

- **Restoring the factory default settings:**

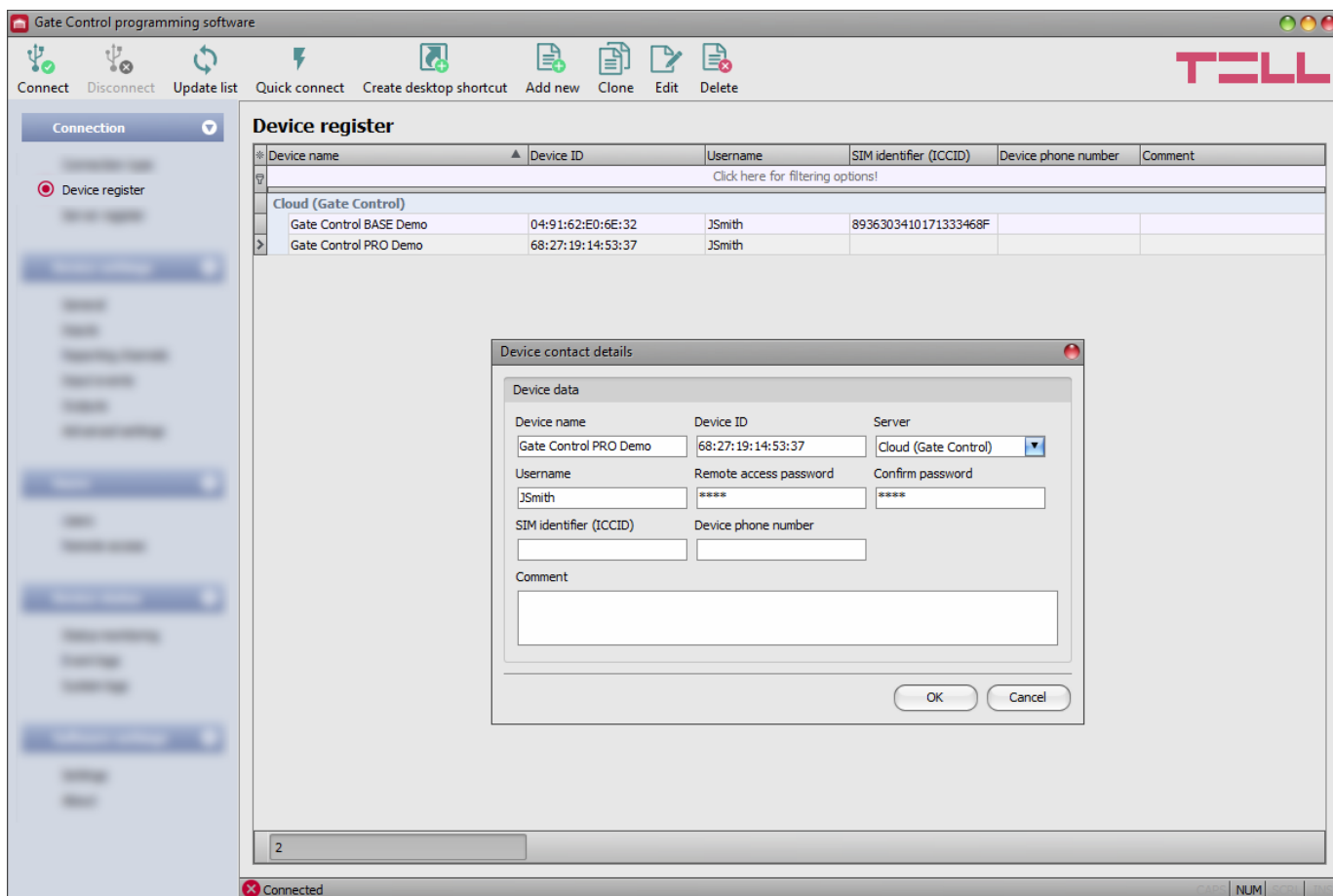
 You can restore the factory default settings in the device by clicking on this button. This option is available only when connected via USB. Restoring the factory default settings will erase the actual settings, therefore please save your settings if needed. The reset process may take more than 1 minute and involves a device restart. Wait until the device restarts and the **STATUS** LED on the device shows activity again. The factory reset can also be performed using the **PB** button found on the device. Further details you can find in chapter “[Restoring the factory default settings](#)”. If you have forgotten the USB connection password, restoring the factory default settings can only be done using the **PB** button found on the device.

The factory default settings cannot be restored if the device has been locked in the settings. If you have forgotten the USB password of the device and the device is locked, only the manufacturer can restore the factory default settings in the service center.

- **Updating the device firmware:**

 By clicking on the “**Firmware update**” button, you can update the firmware of the device. After clicking on the button, a pop-up window opens, where you can browse the firmware file with **tf3** extension. When firmware uploading has completed, the progress window closes automatically and a few seconds later the device restarts running on the new firmware.

5.1.3 Device register



The device register serves for storing and easy management of **Gate Control PRO** and **BASE** device contact details used for remote access. You can add new device contact details to the database and edit, delete, and clone entries for easy adding devices with similar contact details. When connecting remotely, you can easily select by name the device you want to connect to from the “**Device name**” drop-down menu, out of the devices you have added to the database.

Device name	Device ID/ICCID	Username
Gate Control BASE Demo	8936303410171333468F	JSmith
Gate Control PRO Demo	68:27:19:14:53:37	JSmith

You can also connect remotely to a device directly from the device register, by selecting the device, and then clicking on the **Quick connect** button.

You can use the “**Create desktop shortcut**” button to create a shortcut on your desktop for the device selected in the device register. The shortcut will open the software and will initiate a remote connection to the given device automatically.

If you enter new device contact details in the connection type section, the program will add this automatically to the device register database using the device ID as device name, which you can change by editing the given record in the device register. The database is stored locally on the computer. If needed, you can import a database exported from an earlier version of the program using the **MMTool** software that can be installed together with the programming software. The **MMTool** software is included in the programming software setup package and can be selected for installation in the setup wizard.

Available options:

- Update the records from database:



To update the listed records from database, click on the “**Update list**” button.

- Quick remote connect to the selected device:



To connect to the selected device, click on the “**Quick connect**” button. The program will switch to the “**Connection type**” menu and start connecting automatically.

- Creating a shortcut on the desktop, used to connect immediately to the selected device:



To create a shortcut on the desktop, click on the “**Create desktop shortcut**” button.

- Adding new device contact details:



Click on the “**Add new**” button to add new device contact details.

- Creating a copy of existing contact details of a device:



To create a copy of the contact details of the selected device, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing existing device contact details:



To edit the contact details of the selected device, click on the “**Edit**” button.

- Deleting the contact details of a device:



To delete the contact details of the selected device, click on the “**Delete**” button.

Data stored by the device register:

Device name: you can enter a custom name for the device in this section.

Device ID: the unique identifier of the device. If the device is connected via USB, the program will read the identifier from the device and will paste it in this box when you add new device contact details.

Server: in case of using a proxy, for connecting remotely to the device, it is possible to configure a server IP address and port number different from the default server, by adding a new server in the “**Server register**” menu. If there are further servers recorded, you can choose in this drop-down menu a connection option for the given device from the recorded servers. The “**Server register**” menu is hidden by default, since in most cases using it is not necessary. You can find the option used to enable showing this menu in the “**Software settings / Settings**” menu.

Username: the username of the user recorded in the “**Remote access**” menu in the settings of the given device, authorized to connect remotely to the device.

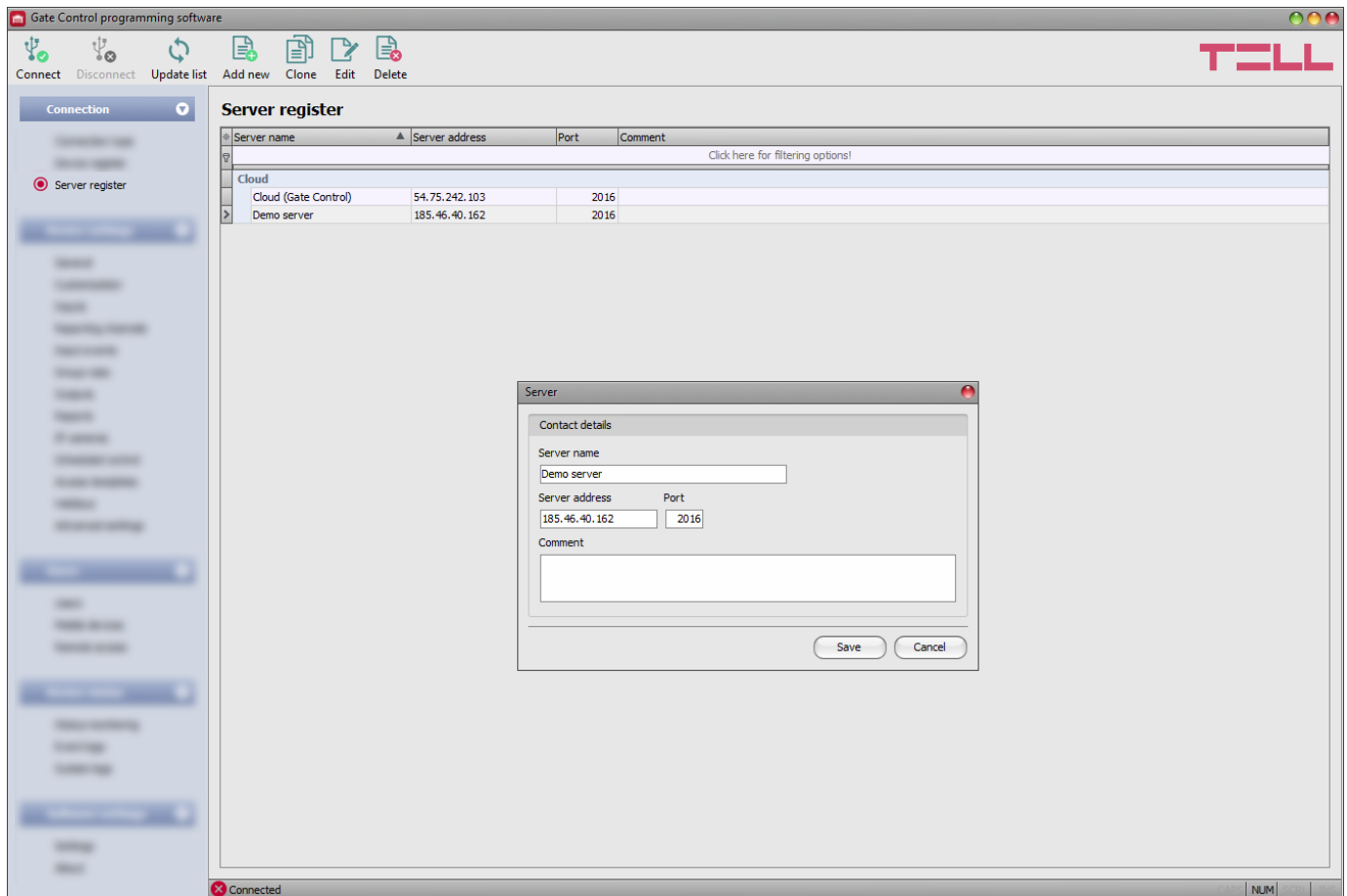
Remote access password / Confirm password: the password configured for the given user in the “**Remote access**” menu in the settings of the given device, used to connect remotely to the device.

SIM identifier (ICCID): the identifier of the SIM card installed in the device (if the SIM card is installed, the software reads the ICCID automatically from the device and inserts the data in this field when you add new contact details for a device). If automated reading fails, you can enter the ID manually or copy it from the “**Status monitoring**” menu. The ICCID has no specific function, its purpose is informational.

Device phone number: in this field you can enter the phone number of the SIM card installed in the device. It has no specific function, its purpose is informational.

Comment: in this section you can write a custom comment for the given device.

5.1.4 Server register



The server register is used for storing the contact details of servers. The “**Server register**” menu is hidden by default, since it in most cases using it is not necessary. It is needed only if you are using a proxy for Internet traffic management, or if you are using the device in a private network, where there is no option to enable access to the cloud server. In this case, for connecting remotely to the device, in this menu it is possible to configure a custom server IP address and port number different from the default server, and then assign the server registered here to your devices in the “**Device register**” menu.

Thereby, connecting remotely to your recorded devices will be done through the server you have associated with them. You can find the option used to enable showing the “**Server register**” menu in the “**Software settings / Settings**” menu. You can add new server contact details to the database and edit, delete, and clone entries for easy adding of servers with similar contact details.

If you are using the device in a private network, where there is no option to enable access to the cloud server, in the “**Server register**” menu you can add an IP address and port number available in the given private network, which you can then select as the default cloud server in the device settings, in the “**General**” menu. Thus, it is not necessary to enable access to the cloud server in the private network, just configure port forwarding from the chosen IP address and port number to the cloud IP address and port number (**54.75.242.103:2016**)

Function buttons available in the “**Server register**” menu:

- Update the records from database:



To update the listed records from database, click on the “**Update list**” button.

- Adding new server contact details:



Click on the “**Add new**” button to add new server contact details.

- Creating a copy of existing contact details of a server:



To create a copy of the contact details of the selected server, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing existing server contact details:



To edit the contact details of the selected server, click on the “**Edit**” button.

- Deleting the contact details of a server:



To delete the contact details of the selected server, click on the “**Delete**” button.

Data stored by the server register:

Server name: custom server name.

Server address: the IP address or domain name of the server.

Port: the communication port number of the server.


Comment: in this field you can enter custom comments related to the given server.


5.2 Device settings menu group

You can configure the device settings in the submenus available in the “**Device settings**” menu.

Attention! The device handles the device settings and user settings (users, mobile devices, remote access) as two different data categories, therefore you must read and write them separately in the device. The program reads the device settings from the device automatically when it connects to the device, while users are not read automatically. You can find details on user management in chapter “[Users menu group](#)”.



- **Changing the device settings:** To change the device settings, reading the settings stored in the device is needed, which is done automatically after connecting to the device. However, you can also read the settings manually anytime by clicking on the



“**Read settings**”  button in any submenu under the “**Device settings**” menu group.

Writing the settings into the device using the “**Write settings**”  button is not possible until the settings are read. After making changes in the settings, write the settings into the

device by clicking on the “**Write settings**”  button.

- **Overwriting the full device configuration (device settings, users, mobile devices, and remote access entries):** If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users and the settings in the submenus, and then click on the

“**Create system backup**”  button in the “**General**” device settings menu. You can import the saved backup into the program using the “**Restore from backup**”  button, and then






write imported settings into the device by category, using the “**Write settings**”  and the “**Write users**”  buttons.

5.2.1 General

The screenshot displays the 'Gate Control programming software' window. The top toolbar includes buttons for 'Connect', 'Disconnect', 'Read settings', 'Write settings', 'Create system backup', 'Restore from backup', and 'Send test e-mail'. The left sidebar shows a tree view with 'Device settings' expanded and 'General' selected. The main panel is titled 'General settings' and contains several sections: 'Ethernet' (IP type, Static IP address, Default gateway, Subnet mask, Primary DNS server, Secondary DNS server), 'SIM settings' (Modem, Device phone number, PIN code, APN, APN username, APN password), 'Cloud server' (Cloud usage, Server, Server address, Server port), 'Identification' (Device name), 'Call durations' (Protection against reopening, Incoming call duration, Callback duration), 'Emergency control by SMS' (Enable emergency control function, Send notification on emergency control to the SMS forwarding phone number), 'Region settings' (Date format, Time zone, First day of the week), and 'Miscellaneous settings' (Administrator's email address, SMS forwarding phone number, SMS forwarding daily limit, SMS sending daily limit). The bottom status bar shows 'Connected' and 'NUM'.

In this menu you can configure the parameters related to the general operation of the device.


Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.
- Creating a system backup:
 To create a full system backup, i.e., to save the device settings and users to file, click on the “**Create system backup**” button, select the target folder, enter a name for the file, and then click on the “**Save**” button.
- Restoring the system from a system backup:
 To restore the settings and users from a system backup, click on the “**Restore from backup**” button, browse the backup file, click on the “**Open**” button, and then write the imported data into the device by clicking on the “**Write settings**”  button. This action will write the settings and the users as well in the device. This option is only available when connected via USB.

- Sending a test e-mail:



The “**Send test e-mail**” button can be used to check if the e-mail sending function is operational. To send a test e-mail, click on the button, enter the e-mail address, and then click on the “**Send**” button. If the test message does not arrive to the given e-mail address, check the “**Ethernet**” and the “**APN**” settings.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

Ethernet (only the product variant with an Ethernet port):

In this section you can configure the Ethernet network interface settings.

IP type:

- **DHCP:** requesting and applying network settings automatically.
- **Static IP-address:** using a fix IP address and configuring the network settings manually.

If you have selected the “**Static IP address**” option in the “**IP type**” section, the following network settings become available:

Static IP address: you can configure a static IP address for the device in this section.

Default gateway: the default gateway IP address.

Subnet mask: the applied subnet mask.

Primary DNS server: the IP address of the primary DNS server.

Secondary DNS server: the IP address of the secondary DNS server.

SIM settings:

Device phone number: enter the phone number of the SIM card installed in the **Gate Control PRO** device. The system will use this in the mobile application to control the gate by a backup phone call if a problem occurs with the mobile Internet connection when you want to control a gate.

PIN code: if you want to lock the SIM card with a PIN code, enter in this section the PIN code of the SIM card installed in the device and enable PIN code request on the SIM card using a cellphone. Otherwise disable PIN code request on the SIM card. If the wrong PIN code has been entered, the device will try the code only once each time the code is changed in the settings, and “PIN code error” message will be shown in the system logs. After an unsuccessful attempt, the device will delete the wrong PIN code in the settings, after that it may restart depending on the type of the modem, and then the “PIN code need!” message will be shown in the system logs. If you experience this, enter the correct PIN code. If the wrong code is configured 3 times consecutively, the SIM card will reach the PUK code request stage. In this case, install the SIM card into a cellphone, unlock the card by entering the PUK code when requested, and configure the valid PIN code in the device settings.

APN: access point name. The device attempts to set the APN automatically from the mobile operator. If automatic setting fails (the device does not get an IP address – you can check this in the “**Status monitoring**” menu), you can also configure the APN manually in this field. When left blank, the device will use automatic APN setting (restarting the device is necessary after changing the APN settings). The APN is available on the website of the mobile service provider.

For the product variant without an Ethernet port, or if you want to use the product variant with an Ethernet port without wired Internet, a SIM card with data is required in the **Gate Control PRO** device to use the system’s Internet-based services.

Note: If automatic APN setting fails (the device does not get an IP address), configure the APN even if you don't want to use the device with an Internet connection, because with certain service providers it happens that without that the modem cannot connect to the mobile network at all, or it does not receive a time setting from the network. If you do not want to use the device with an Internet connection and/or there is no mobile Internet on the SIM card, disable the “**Cloud usage**” option.

APN username: necessary only if the mobile service provider provides this and requires its usage for the given APN.

APN password: necessary only if the mobile service provider provides this and requires its usage for the given APN.

Cloud server:

Cloud usage: the system can be configured to connect to the Internet and stay online continuously, or to connect only occasionally, when needed. If this option is enabled, the device will connect to the cloud server operated by the manufacturer and will stay connected continuously. For using the Internet based online services of the system, a continuous Internet connection is needed, which increases the data traffic.

If you enable cloud usage, the following services will be available:

- **mobile application usage**
- **remote access, remote programming**
- **remote firmware update,**

If you disable cloud usage, the device can be controlled only by call, but the following e-mail functions will still be available, because they do not require continuous Internet connection:

- **e-mail sending upon activating a contact input**
- **e-mail reports**
- **test report by e-mail**

Attention! If the modem is currently connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, the services mentioned above that require Internet connection will be suspended for the duration of the call. For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.

Functions that make outgoing calls:

- **notification by call upon activating a contact input**
- **confirmation of control by call**

Server: you can select the default cloud server in this drop-down menu. If you are using the device in a private network, where there is no option to enable access to the cloud server, the program offers an option to add custom cloud contact details in the “**Server register**” menu. This can be an IP address and port number available in the given private network, which you can then select as the default cloud server in this drop-down menu. Thus, it is not necessary to enable access to the cloud server in the private network, just configure port forwarding from the chosen IP address and port number to the cloud IP address and port number (54.75.242.103:2016).

Identification:

Device name: here you can enter a custom name for your **Gate Control PRO** device. This name will also be used in reports.

Attention! The following characters should not be used: ^ ~ < > = ' " , | ? \$ & %

Call durations:

Protection against reopening: a call made with certain cellphones on certain networks may generate another call to the device due to rejection, that results in another unwanted control action (e.g., the gate stops while opening). With this option, you can set the device to ignore further calls from the same phone number within the specified time. If this phenomenon is detected, the recommended setting is 10 s.

Incoming call duration: the time after which the system rejects incoming calls can be configured here in seconds. In case of entering value “0”, the system will reject incoming calls immediately after obtaining the caller ID.

Callback duration: the system can confirm a control by calling back the user’s number. Confirmation of control by call can be enabled separately for each user. With this setting you can configure how long the system should ring the user’s phone during the call. When this time expires, the system will end the call automatically.

Emergency control by SMS:

In case of emergency, it is possible to open and hold the gate locked in open state, respectively close the gate by text message (SMS). You can read more about this in chapter “[Emergency control by SMS](#)”.

Enable emergency control function: with this option you can enable or disable the emergency control by SMS function.

Send notification on emergency control to the SMS forwarding phone number: if this option is enabled, the device will send notification by SMS to the phone number configured in the “**SMS forwarding phone number**” section, when a user performs emergency control by SMS.

Region settings:

Date format: using the drop-down menu you can select the date format used by the system for the timestamp in notifications:

- yyyy.MM.dd. hh:mm:ss
- dd/MM/yyyy hh:mm:ss

Time zone: using the drop-down menu you can select the time zone according to the installation location. The system adjusts the system time according to the selected time zone. If the setting is incorrect, there will be difference between the system time and the local time, which affects the timestamps of events and the operation as well, since access templates, rules and scheduled controls are all based on the system time.

Automatic daylight saving: the system manages daylight saving automatically in accordance with the configured time zone.

First day of the week: using the drop-down menu you can select the day the week starts with. This is used to support international usage.

Miscellaneous settings:

Administrator's e-mail address: the system sends notifications about version updates to the e-mail address specified here.

SMS forwarding phone number: the system can forward messages received on the SIM card installed in the device to the phone number specified here (e.g., balance information received from the mobile service provider in case of using a pre-pay card). Received messages are deleted automatically after forwarding. If no phone number is configured, the system deletes all incoming messages without forwarding.

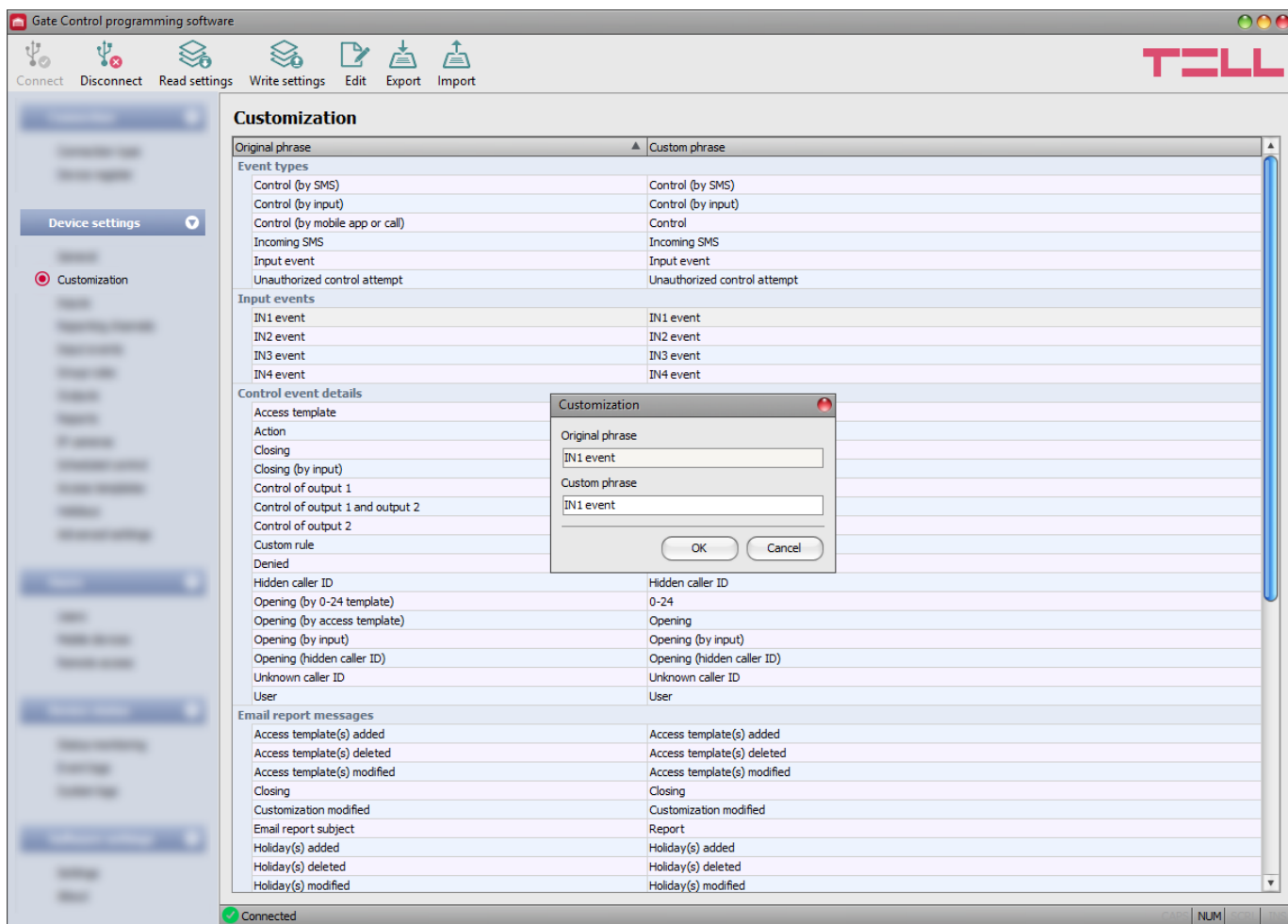
SMS forwarding daily limit: with this option you can limit the number of SMS messages to be forwarded per day. When the configured limit is reached, the system will not forward new incoming SMS messages for 24 hours. After 24 hours, the counter resets automatically and message forwarding will be enabled again up to the configured limit. The SMS forwarding daily limit can be disabled and set to unlimited by deleting the entered value.

Attention! After reaching the configured limit, but still before the message counter is reset, the system deletes all incoming messages without forwarding!




SMS sending daily limit: with this option you can limit the number of SMS messages generated by activating the inputs. When the configured limit is reached, the system will not send further SMS messages generated by inputs for 24 hours. After 24 hours, the counter resets automatically and message sending will be enabled again up to the configured limit. The SMS sending daily limit can be disabled and set to unlimited by deleting the entered value.

Attention! Messages generated after reaching the configured limit, but still before the message counter is reset will neither be sent subsequently, but the system records the events in the event logs.

5.2.2 Customization



In this menu you can change default text elements and phrases used in the event logs, e-mail messages, and certain Push and SMS messages. The phrases which you can change are listed in the “**Custom phrase**” column.

To change phrases, first read the settings from the device using the “**Read settings**”  button, then double click on the entry you want to change, or select it by a single click and then click on the “**Edit**”  button. Enter the custom phrase in the dialog window, click on the “**OK**” button, and then write the changes into the device using the “**Write settings**”  button.

Attention! The following characters should not be used: ^ ~ < > = ' " , | ? \$ & %

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

- Editing an entry:



To edit the selected entry, click on the “**Edit**” button.

- Exporting entries:




To export the custom phrases to file in CSV format, click on the “**Export**” button.




- Importing entries:



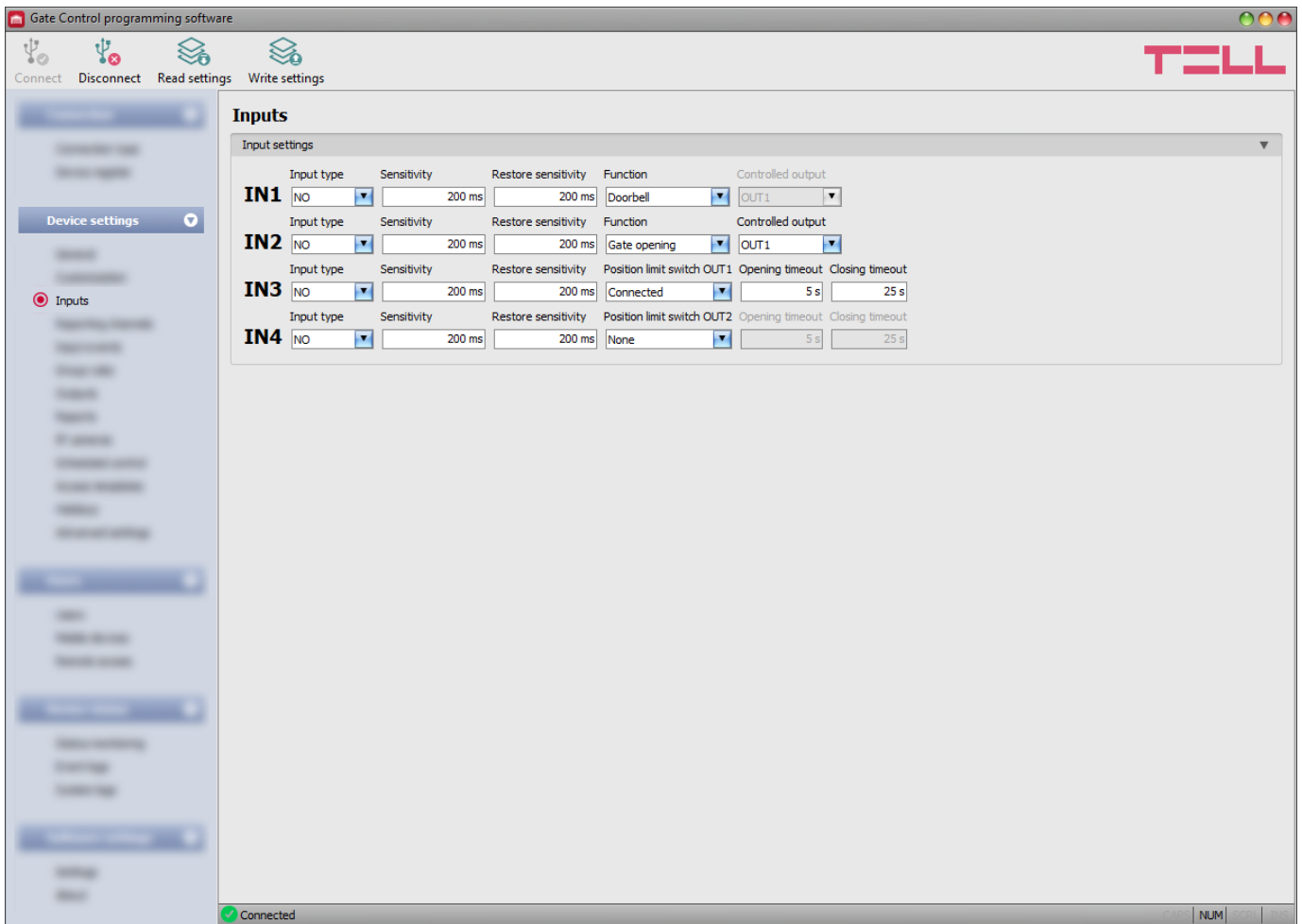
To import the custom phrases from a CSV file, click on the “**Import**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “Write settings**”  button.**

The manufacturer provides the default English, German, Czech and Hungarian set of words for the customization function, which you can find in the “**Localization**” folder of the program installation directory under the following file names: “**GC_Customization_V10_EN.csv**”, “**GC_Personalisierung_V10_DE.csv**”, “**GC_Prizpusobeni_V10_CZ.csv**” and “**GC_szemelyre_szabas_V10_HU.csv**”. If you want to replace the actual set of words used by

the device, read the settings from the device using the “**Read settings**”  button, click on the “**Import**”  button, browse and select one of the mentioned language files, and then write the changes into the device using the “**Write settings**”  button.

5.2.3 Inputs



In this menu you can configure the properties and options of the contact inputs IN1...IN4. When the contact inputs are triggered, the system generates input events. You can configure notifications for each input event in the “***Input events***” menu, which will be sent to the phone numbers and/or e-mail addresses configured in the “***Reporting channels***” menu. In addition, the inputs have further configurable functions, as follows:

Inputs IN1 and IN2 can also be used to open the gate, or report doorbell activity or a technical error via Push message, when triggered by an external dry contact.

Input IN3: gate position limit error notification (Push message) on the gate controlled by OUT1.

Input IN4: gate position limit error notification (Push message) on the gate controlled by OUT2.

You can read more about input functions under the “[Operation of the contact inputs](#)” paragraph.

Available options:

- Reading the settings from the device:




To read the settings from the device click on the “***Read settings***” button. This will read all settings in all menus in the “***Device settings***” menu group.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “***Write settings***” button. This will write into the device the values changed in the menus in the “***Device settings***” menu group.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “***Write settings***”  button.

Input settings:

Input type: you can configure an input as normally open (**NO**) or normally closed (**NC**). When set to **NO**, an event is generated when the input circuit is closed, while when set to **NC**, opening the input circuit generates an event. The input is closed when the given input **IN1...IN4** is shorted to the **GND** terminal.

Sensitivity: input sensitivity specified in milliseconds. State changes of the input shorter than the configured value, that trigger an input activation, are ignored by the system.

Restore sensitivity: input restore sensitivity specified in milliseconds. State changes of the input shorter than the configured value, that trigger an input restore, are ignored by the system.

Function: for inputs IN1 and IN2 you can select a function. These two inputs can also be used to open the gate, or report doorbell activity or a technical error via Push message.

Available options:

- **Doorbell:** if this option is selected, the system will send the “**Doorbell**” notification via Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering the given input.
- **Technical error:** if this option is selected, the system will send the “**Technical or device failure**” notification via Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering the given input.
- **Gate opening:** if this option is selected, the given input can be used to control the outputs, i.e., to open the gate by triggering a toggle switch, a pushbutton, or a relay contact connected to the given input. In case of using output control mode 1 or 2, you can also select the output (OUT1 or OUT2) to be controlled by the input.
- **Supervised gate opening:** if this option is selected, the given input can be used to control the outputs, i.e., to open the gate by triggering a toggle switch, a pushbutton, or a relay contact connected to the given input. In case of using output control mode 1 or 2, you can also select the output (OUT1 or OUT2) to be controlled by the input. Compared to the simple “**Gate opening**” option, this option requires connecting the position limit switches of the gates and configuring for supervised control – see below: “**Connected (supervised control)**” option. The device will perform supervised gate opening by taking into account the status of the position limit switch, i.e., it will not initiate an opening control if the gate is open.

Position limit switch OUT1: enabling the gate position limit switch connected to input IN3, installed on the gate controlled by output OUT1.

Available options:

- **None:** choose this option if you do not connect a gate position limit switch to input IN3.
- **Connected (supervised control):** choose this option if you have connected the position limit switch installed on the gate controlled by output OUT1 to input IN3, and you want to use the following functions:
 - **Notification about opening and closing failure:** the device monitors if the gate opens within the time interval configured in the “**Opening timeout**” section, and if it closes within the time interval configured in the “**Closing timeout**” section. If the gate fails to open or close within the configured intervals, the device sends notifications via Push message and/or SMS, according to the settings. You can change the text of these notifications in the “**Customization**” menu, if needed. The system considers the idle state of the position limit switch as the closed state of the gate. In case of NO (normally open) wiring, the open state, while for NC (normally closed) wiring the closed state of the position limit switch is considered as the idle state.
 - **Ignoring opening control, if the gate is open:** if the gate position limit switch indicates that the gate is open, the system will ignore opening commands sent by users.
 - **Ignoring closing control, if the gate is closed:** if the gate position limit switch indicates that the gate is closed, the system will ignore closing commands sent by users.
 - **Ignoring opening and closing control, if the gate is held open by a scheduled control in progress:** if the gate is held locked in open state by a configured scheduled control plan, the system will ignore opening and closing commands sent by users.
- **Connected (status indication only):** choose this option if you have connected the position limit switch installed on the gate controlled by output OUT1 to input IN3, but you do not want to use the functions mentioned above. With this option, the system will use the gate position limit switch only to indicate the open and closed state of the gate, and will not make any function depend on the state of the position limit switch.

Position limit switch OUT2: enabling the gate position limit switch connected to input IN4, installed on the gate controlled by output OUT2. This option is only available for control modes 1 and 2, for connecting the position limit switch of the second gate.

Available options:

- **None:** choose this option if you do not connect a gate position limit switch to input IN4.
- **Connected (supervised control):** choose this option if you have connected the position limit switch installed on the gate controlled by output OUT2 to input IN4, and you want to use the following functions:
 - **Notification about opening and closing failure:** the device monitors if the gate opens within the time interval configured in the “**Opening timeout**” section, and if it closes within the time interval configured in the “**Closing timeout**” section. If the gate fails to open or close within the configured intervals, the device sends notifications via Push message and/or SMS, according to the settings. You can change the text of these notifications in the “**Customization**” menu, if needed. The system considers the idle state of the position limit switch as the closed state of the gate. In case of NO (normally open) wiring, the open state, while for NC (normally closed) wiring the closed state of the position limit switch is considered as the idle state.
 - **Ignoring opening control, if the gate is open:** if the gate position limit switch indicates that the gate is open, the system will ignore opening commands sent by users.
 - **Ignoring closing control, if the gate is closed:** if the gate position limit switch indicates that the gate is closed, the system will ignore closing commands sent by users.
 - **Ignoring opening and closing control, if the gate is held open by a scheduled control in progress:** if the gate is held locked in open state by a configured scheduled control plan, the system will ignore opening and closing commands sent by users.
- **Connected (status indication only):** choose this option if you have connected the position limit switch installed on the gate controlled by output OUT2 to input IN4, but you do not want to use the functions mentioned above. With this option, the system will use the gate position limit switch only to indicate the open and closed state of the gate, and will not make any function depend on the state of the position limit switch.

Opening timeout: enter the time interval in seconds, within which the gate should open starting from receiving an opening control command. If the gate fails to open within the configured interval (i.e., the position limit switch does not change state), the device sends an opening error notification via Push message and/or SMS, according to the settings. The opening timeout is counted for all control modes from receiving an opening control command (pulses A, B, X).

Closing timeout: enter the time interval in seconds, within which the gate should close, starting from receiving an opening control command (or from receiving a closing control command in case of control mode 5). If the gate fails to close within the configured interval (i.e., the position limit switch does not change state), the device sends a closing error notification via Push message and/or SMS, according to the settings. For control modes 1, 2, 3 and 4, the closing timeout is counted from receiving an opening control command (pulses A, B, X), while for control mode 5 this is counted from receiving a closing control command (pulse Z).

5.2.4 Reporting channels

Gate Control programming software

Connect Disconnect Read settings Write settings

TELL

Reporting channels

TELL remote monitoring receivers

	Primary IP address / Domain name	Port	Supervision message interval	User account ID
IP1	<input type="text"/>	<input type="text" value="3535"/>	<input type="text" value="180 s"/>	<input type="text"/>
IP2	<input type="text"/>	<input type="text" value="3535"/>	<input type="text" value="180 s"/>	<input type="text"/>

SMS / call notification recipients

	Name	Phone number
TEL1	<input type="text"/>	<input type="text"/>
TEL2	<input type="text"/>	<input type="text"/>
TEL3	<input type="text"/>	<input type="text"/>
TEL4	<input type="text"/>	<input type="text"/>



E-mail notification recipients


	Name	E-mail address
MAIL1	<input type="text"/>	<input type="text"/>
MAIL2	<input type="text"/>	<input type="text"/>
MAIL3	<input type="text"/>	<input type="text"/>
MAIL4	<input type="text"/>	<input type="text"/>

Connected NUM

In this menu you can configure the telephone and e-mail contact details, to which you want to send notifications about events generated by triggering the **IN1...IN4** contact inputs.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

TELL remote monitoring receivers (the *Monitoring* product variant only):

The device can report to a remote monitoring station (CMS) over IP, to a primary and a backup receiver, using the TELLMon protocol. The device is solely compatible with the TELLMon receiver and MVP.next server produced by TELL. The supported remote monitoring events can be configured in the “**Remote monitoring events**” menu.

Primary IP address / Domain name: the primary CMS server or receiver IP address or domain name. The device sends reports to this address first. For use with the mobile Internet, when a SIM card with a private APN is used and the given server or receiver is not in the same APN, it is necessary to enable access for the server/receiver IP address in the given APN.

Backup IP address / Domain name: the backup CMS server or receiver IP address or domain name. The device sends reports to this address if reporting to the primary address fails.

Port: CMS server or receiver communication port number.

Default port number:

- TELLMon protocol (TCP): **3535**

Supervision message interval: this option enables you to configure the interval of supervision message sending to the CMS server/receiver. The Supervision message interval can be configured from 60 to 600 seconds.

User account ID: the user account ID necessary for Contact ID based reporting to CMS. The events and the supervision messages are sent to the configured servers or receivers using the user account ID configured in this section. The user account ID length is 4 hexadecimal characters, and the following characters can be used: 0..9, A, B, C, D, E, F.

SMS / call notification recipients:

You can configure up to 4 phone numbers (**TEL1...TEL4**) which the system can notify by SMS or call, when contact inputs are activated.

Attention! If the modem is currently connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call. For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.

Name: the name of the phone number's owner. The program will use the name entered in this section for listing the available notification channels when configuring events.

Phone number: the phone number to be notified. Use international format with the country code (e.g., +36...), otherwise, SMS sending may fail.

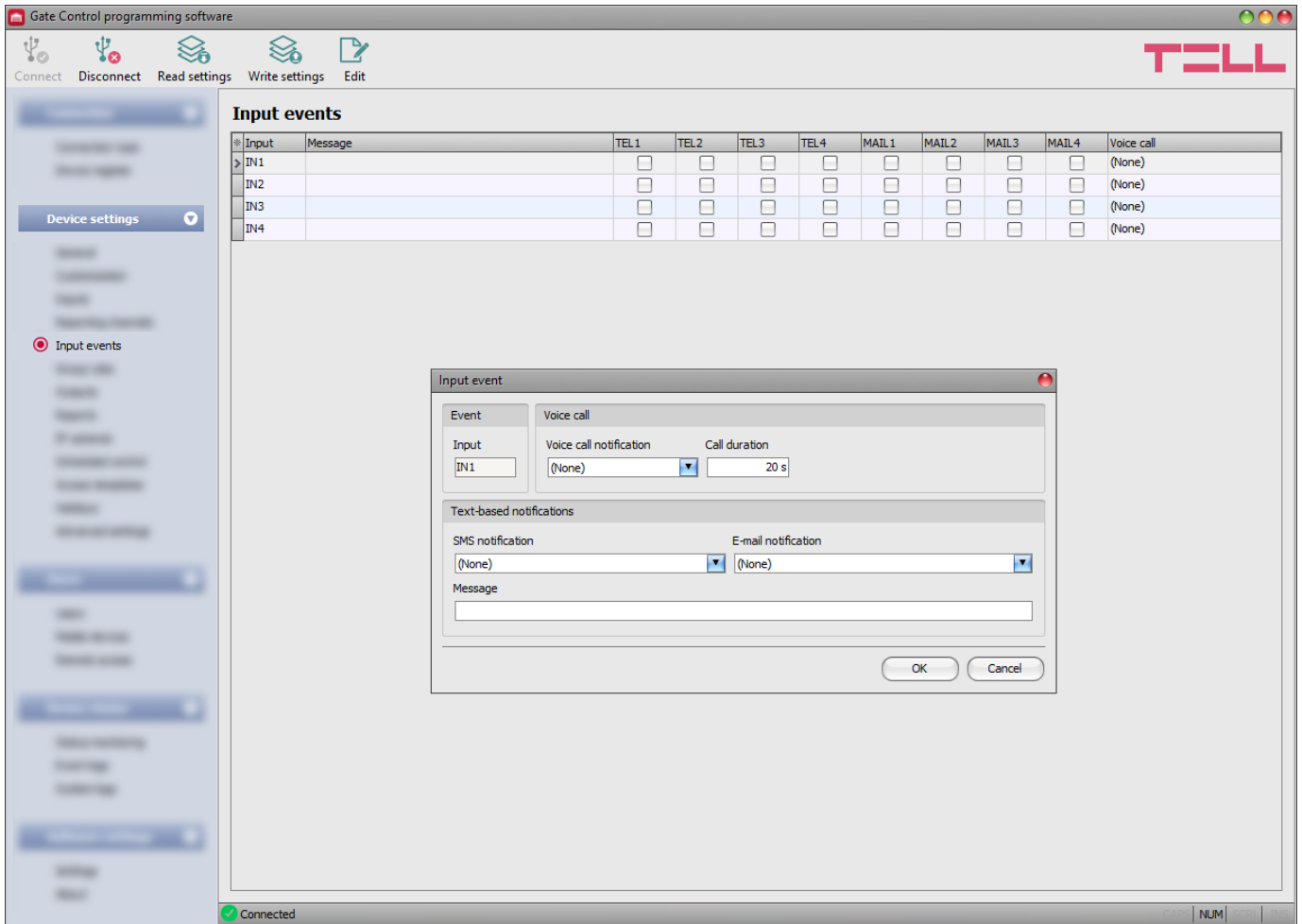
E-mail notification recipients:

You can configure up to 4 e-mail addresses (**MAIL1...MAIL4**) which the system can notify in e-mail when contact inputs are activated. E-mail sending requires Internet service.

Name: the recipient's name. The program will use the name entered in this section for listing the available notification channels when configuring events.




E-mail address: the e-mail address to be notified. You can enter one e-mail address per user.


5.2.5 Input events



In this menu you can configure SMS, e-mail, and voice call notifications to be sent upon activating the contact inputs **IN1...IN4**.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.
- Edit an event:
 To edit the settings of the selected event, click on the “**Edit**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

Event:

Input: the index number of the input that generates the given event. This data cannot be changed.

Voice call:

Voice call notification: you can select from the drop-down menu, which phone number to be notified by voice call when the given event occurs. The system will not play any sound or voice message in the call. This function only serves to ring a phone number upon activating an input, thus the notification will be charged if the person called does not accept or rejects the call. For this type of notification you can select one phone number per event. The phone numbers to be notified can be configured in the “**Reporting channels**” menu.

Attention! If the modem is currently connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call. For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.

Call duration: in this section you can configure the duration of a call in seconds, that is how long the phone device called should ring. When the configured period expires, the system ends the call automatically, or the person called may also reject the call earlier. The notification is free of charge if the person called does not accept or rejects the call (please also check this with your mobile operator, as some operators may charge a connection fee for rejected calls as well).

Text-based notifications:

SMS notification: in this section you can select the phone numbers which you want to be notified by SMS when the given event occurs. The phone numbers to be notified can be configured in the “**Reporting channels**” menu. The text message will be sent to the numbers enabled with the help of the checkboxes in the drop-down menu.

E-mail notification: in this section you can select the recipients which you want to be notified by e-mail when the given event occurs. The e-mail addresses to be notified can be configured in the “**Reporting channels**” menu. The text message will be sent to the recipients enabled with the help of the checkboxes in the drop-down menu. The e-mail sending function requires Internet service.

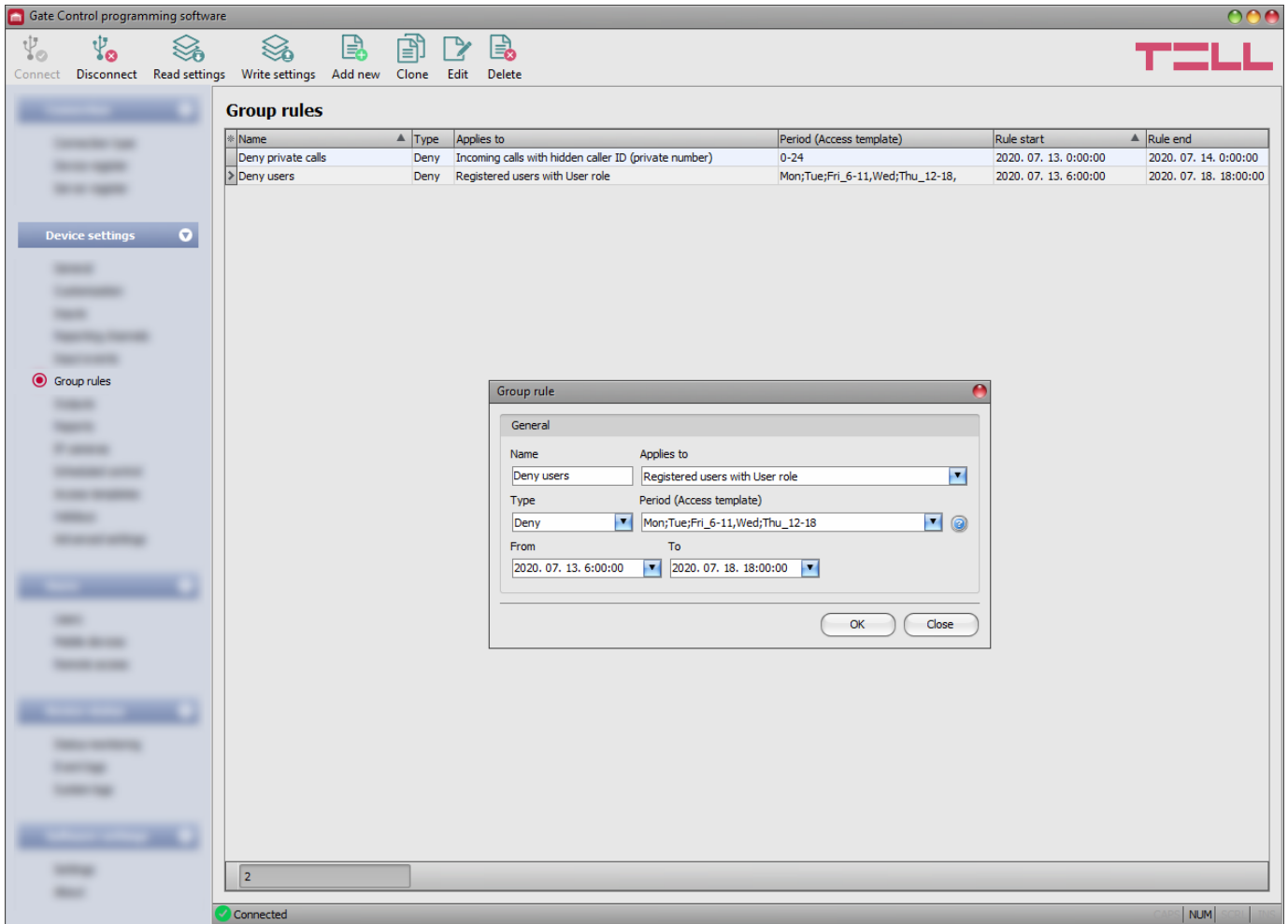
Message: in this field you can enter a custom message of maximum 45 characters, which you want to be sent to the selected phone numbers and e-mail recipients, when the given event occurs. The device will send the same message for both types of notification (SMS and e-mail). You can use the **\$dt** variable in the message, which will be replaced with the current date and time in brackets, for example:

Configured message: *Technical error \$dt*

Received message: *Technical error (2024.07.26 15:34:08)*



Attention! The following characters should not be used: ^ ~ < > = ' " , | ? & %

5.2.6 Group rules



The group rules assure an option for easy overriding control permissions and entry periods defined by configured access templates, regarding groups of users. The group rules have no effect on custom rules configured for users, since custom rule have a higher priority. Custom rules remain in effect independently from the group rules settings. The denying rules have priority against the allowing ones in the rule system. Therefore, if you accidentally configure group rules with opposite effect (for same user group, with overlapping validity periods), the denying rules will take effect while the allowing ones will be ignored.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

- Adding a new group rule:



To add a new group rule, click on the “**Add new**” button.

- Creating a copy of an existing group rule:



To create a copy of an existing group rule, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing an existing group rule:




To edit an existing group rule, click on the “**Edit**” button.

- Deleting a group rule:



To delete a group rule, click on the “**Delete**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

Group rule settings:

General:

Name: the custom name of the group rule. The name should not be longer than 30 characters, and the following characters cannot be used: ^ ~ < > = ' " , | ? \$ & %

Applies to:

Registered users with User role: using this option, you can grant or deny permission to control the gate for users registered with “**User**” role.

Registered users with Admin role: using this option, you can grant or deny permission to control the gate for users registered with “**Admin**” role.

Registered users with Super admin role: using this option, you can grant or deny permission to control the gate for users registered with “**Super admin**” role.

All registered users: using this option, you can grant or deny permission to control the gate for all registered users, regardless of their role.

All (registered and unknown): using this option, you can grant or deny permission to control the gate for everyone (registered users regardless of their role, and incoming calls from unknown phone numbers with presented or hidden caller ID / private number).

Incoming calls with hidden caller ID (private number): using this option, you can grant or deny permission to control the gate for calls received with hidden caller ID. In case of using output control mode 1, calls received with hidden caller ID enabled by the rule will control output OUT2. In case of using output control mode 2, calls received with hidden caller ID enabled by the rule will control outputs OUT1 and OUT2 at the same time. This rule option is not available in case of using output control mode 5.

Incoming calls from unregistered users, with presented caller ID: using this option, you can grant or deny permission to control the gate for calls received with presented caller ID from unregistered phone numbers. In case of using output control mode 1, calls received from unregistered phone numbers enabled by the rule will control output OUT1. In case of using output control mode 2, calls received from unregistered phone numbers enabled by the rule will control outputs OUT1 and OUT2 at the same time.

Type: you can select the rule type (allow or deny) using this drop-down menu.




Period (Access template): if you want to configure the rule to take effect only on certain days of the week and/or only in certain daily time intervals during the validity period, you can do this by assigning one or more (maximum 4) access templates to the rule. In this case, the rule will only take effect within the time intervals configured in the access template(s) assigned to it. You can add and configure access templates in the “**Access templates**” menu.

If you do not want to specify a daily time interval, choose the “**0-24**” option. This way the rule will be in effect all day and each day in the set period.

From: in this section you can configure the start date and time of the group rule’s validity period. You can select the date and enter the time in the calendar after opening the drop-down menu.

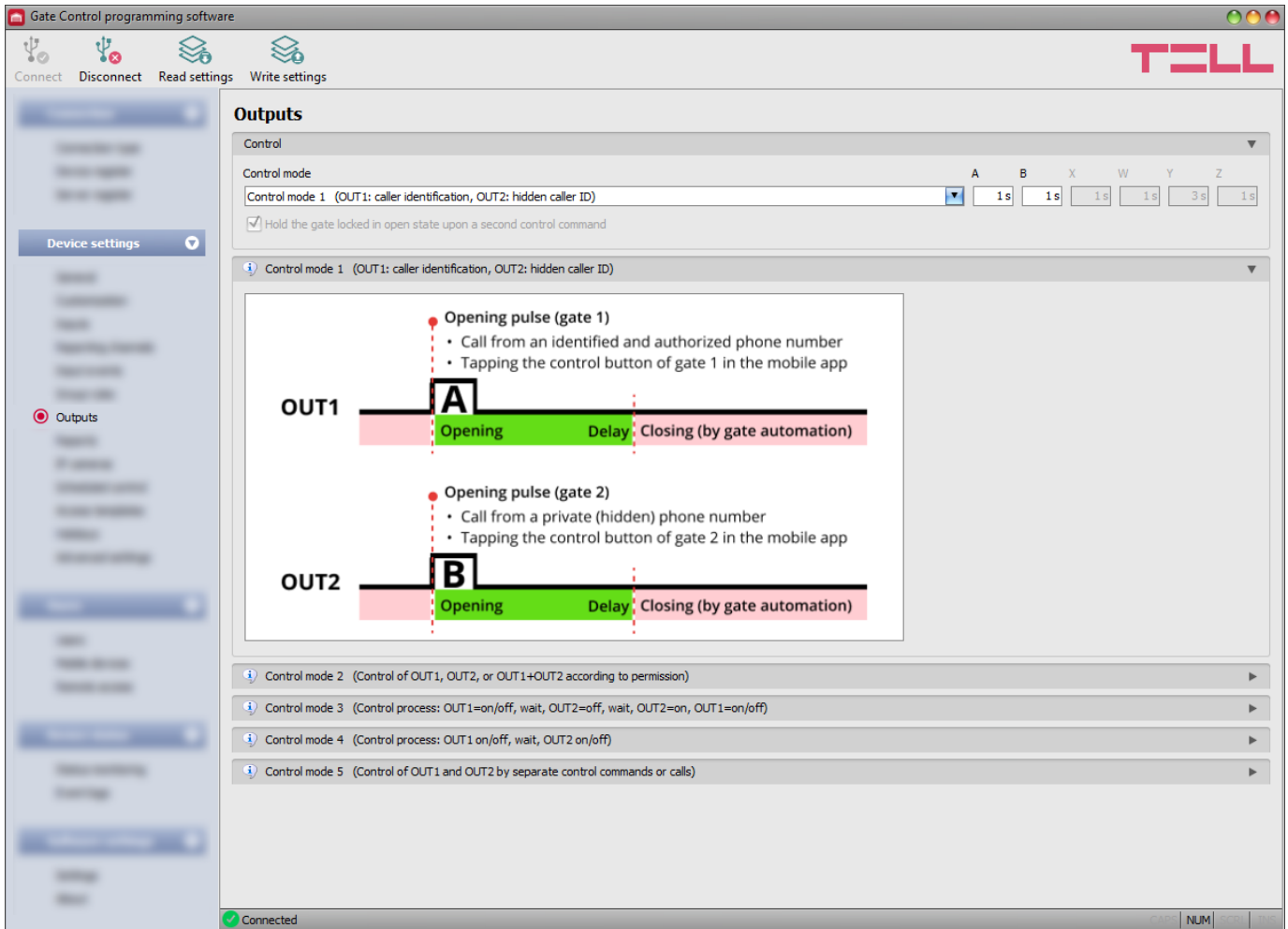
To: in this section you can configure the end date and time of the group rule’s validity period. You can select the date and enter the time in the calendar after opening the drop-down menu.

➤ **Creating a new group rule:**

- If you haven’t read the settings yet, click on the “**Read settings**”  button to read the settings from the device.
- Click on the “**Add new**”  button.
- Configure the group rule name.
- Select the user group which the rule will apply to.
- Select the rule type.
- If you want the rule to take effect only on certain days of the week and/or only in certain daily time intervals, add and configure access templates accordingly in the “**Access templates**” menu, and then select the appropriate template or templates for the rule.
- Configure the rule validity start and end time.
- Click on the “**OK**” button.
- Click on the “**Write settings**”  button.

You can add up to 50 group rules in the system.

5.2.7 Outputs



In this menu you can configure how outputs OUT1 and OUT2 should operate when controlled. The operating mode of the outputs can be configured by selecting a control mode. You can choose out of five control modes for compatibility with various control boards of different gates. Choose the control mode which is appropriate for the control signal requirements of the given gate's control board.

Note: The device restarts automatically after changing the control mode, since this affects its whole functionality. If a scheduled control is in progress when changing the control mode, the device waits maximum 10 minutes for the scheduled control to end before it restarts. If this is the case and you want the change to take effect immediately, restart the device by powering off and on.

You can find the wiring instructions for each control mode in the “[Wiring diagrams](#)” chapter.

Available options:

- Reading the settings from the device:




To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

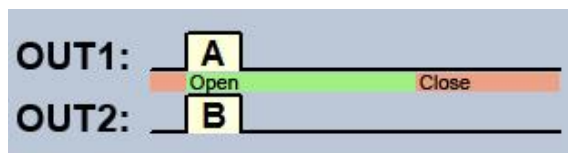
Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “Write settings”  **button.**

Control:

Control mode:

Control mode 1

For one or two gates or one gate with two opening options (partial/total opening).



OUT1: in an idle state by default
OUT2: in an idle state by default

A = OUT1 pulse length (seconds) => for opening gate A

B = OUT2 pulse length (seconds) => for opening gate B

With this control mode, the two outputs can be controlled separately over the Internet using the mobile application.

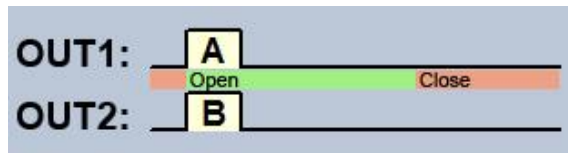
Selective control of outputs OUT1 and OUT2 by using caller identification and hidden caller ID (private number). If the caller sends the caller ID, output OUT1 will be activated. If the caller hides the caller ID (i.e., calls from a private number), output OUT2 will be activated. Thereby, using this control mode you can control up to two different gates by call. Controlling with hidden caller ID can be used by unlimited number of users (registered users too), since this does not require user registration. You can hide the caller ID by dialing the **#31#** code in front of the device's phone number (e.g., **#31#+3630xxxxxxx**). If you want to control both outputs, for easier handling you can add the device's phone number to your cellphone's phonebook in both formats (e.g., **+3630xxxxxxx** and **#31#+3630xxxxxxx**).

The outputs provide an open contact between the **NO** and **COM** terminals in idle state, and a closed contact upon control. The trigger pulse length of output OUT1 can be configured by parameter “**A**”, while the trigger pulse length of output OUT2 can be configured by parameter “**B**”. The values are considered in seconds. The gate's control board must close the gate automatically.

Attention! Anyone can control output OUT2 with hidden caller ID, not only registered users! This option should be used for low-security applications only, since an incoming call (with hidden caller ID) made to the wrong number may also activate the output! For better security, do not publish the device's phone number.

Control mode 2

For one or two gates or one gate with two opening options (partial/total opening).



OUT1: in an idle state by default
OUT2: in an idle state by default

A = OUT1 pulse length (seconds) => for opening gate A

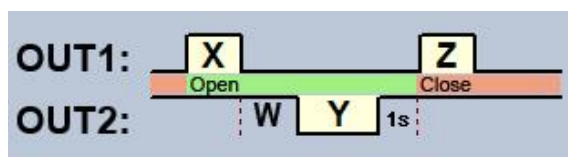
B = OUT2 pulse length (seconds) => for opening gate B

With this control mode, the two outputs can be controlled separately over the Internet using the mobile application.

Selective or simultaneous control of outputs OUT1 and OUT2 using caller identification, based on configured user permissions. Permissions can be configured for each user separately, to activate output OUT1 only, output OUT2 only, or both outputs at the same time upon control. Thereby, this control mode enables you to control two different gates. The outputs provide an open contact between the **NO** and **COM** terminals in idle state, and a closed contact upon control. The trigger pulse length of output OUT1 can be configured by parameter "**A**", while the trigger pulse length of output OUT2 can be configured by parameter "**B**". The values are considered in seconds. The gate's control board must close the gate automatically.

Control mode 3

For single-gate automations that require triggers for opening and closing on the same input.



OUT1: in an idle state by default
OUT2: in an activated state by default

X = OUT1 pulse length (seconds) => for gate opening

W = delay before interrupting the infrared photocell loop (seconds)

Y = OUT2 pulse length (seconds) => for holding the gate locked in open state

Z = OUT1 pulse length (seconds) => for gate closing

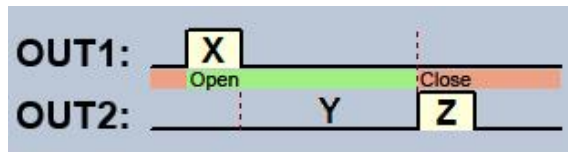
Starting a process of opening and closing by a single call/control command, using caller identification. In idle state, output OUT1 provides an open contact, while output OUT2 provides a closed contact between the **NO** and **COM** terminals. Upon controlling the device, output OUT1 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for **X** seconds, then after **W** seconds output OUT2 switches to idle state (gives an open contact between the **NO** and **COM** terminals) for **Y** seconds, then after 1 second output OUT1 becomes activated again (gives a closed contact between the **NO** and **COM** terminals) for **Z** seconds. You can use this control mode if the gate automation control board requires the triggers for opening and closing on the same input (the first trigger pulse opens the gate, the second one closes it). The opening and closing trigger pulses are provided by OUT1, while inserting the OUT2 contact in the loop of the infrared photocell, it holds the gate locked in open state for **Y** seconds (interrupts the photocell loop, just like when an obstacle shows up in the photocell's ray, thus the gate will not close).

If the gate's control board closes the gate automatically, there is no need for the **Z** trigger pulse. In this case, you should set parameter **Z** to 0 seconds, thus there will not be a gate closing trigger pulse. For certain gate automations, the gate stops immediately if the photocell loop is interrupted during gate opening. To avoid this, a delay can be configured by parameter **W**, which can be used to delay the interruption of the photocell loop. In such case, configure for parameter **W** the maximum duration of a gate opening plus 3 to 5 seconds (e.g., if it takes 12 seconds for the gate to open, configure 15 to 17 seconds for parameter **W**).

Hold the gate locked in open state upon a second control command: if this option is enabled, the gate remains open permanently ($Y=\text{infinite}$) after receiving a second control command/call from the same user while the gate is opening or in open state (during the $X+W+Y$ period). The gate will close when a third control command/call is received from the same user, or a new control command/call is received from a **different user**. This function cannot be used with hidden caller ID.

Control mode 4

For single-gate automations that require triggers for opening and closing on different inputs.



OUT1: in an idle state by default
OUT2: in an idle state by default

X = OUT1 pulse length (seconds) => for gate opening

Y = holding the gate open (seconds) => for holding the gate locked in open state

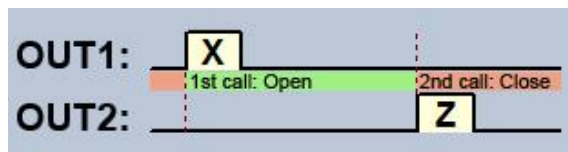
Z = OUT2 pulse length (seconds) => for gate closing

Starting a process of opening and closing by a single call/control command, using caller identification. In idle state, outputs OUT1 and OUT2 provide an open contact between the **NO** and **COM** terminals. Upon controlling the device, output OUT1 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for X seconds, then after Y seconds output OUT2 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for Z seconds. You can use this control mode if the gate automation control board requires triggers for opening and closing on two different inputs (a trigger pulse on an input opens the gate, another trigger pulse on a different input closes the gate).

Hold the gate locked in open state upon a second control command: if this option is enabled, the gate remains open permanently ($Y=\text{infinite}$) after receiving a second control command/call from the same user while the gate is opening or in open state (during the $X+Y$ period). The gate will close when a third control command/call is received from the same user, or a new control command/call is received from a **different user**. This function cannot be used with hidden caller ID.

Control mode 5

For single-gate automations that require triggers for opening and closing on different inputs.



OUT1: in an idle state by default
OUT2: in an idle state by default

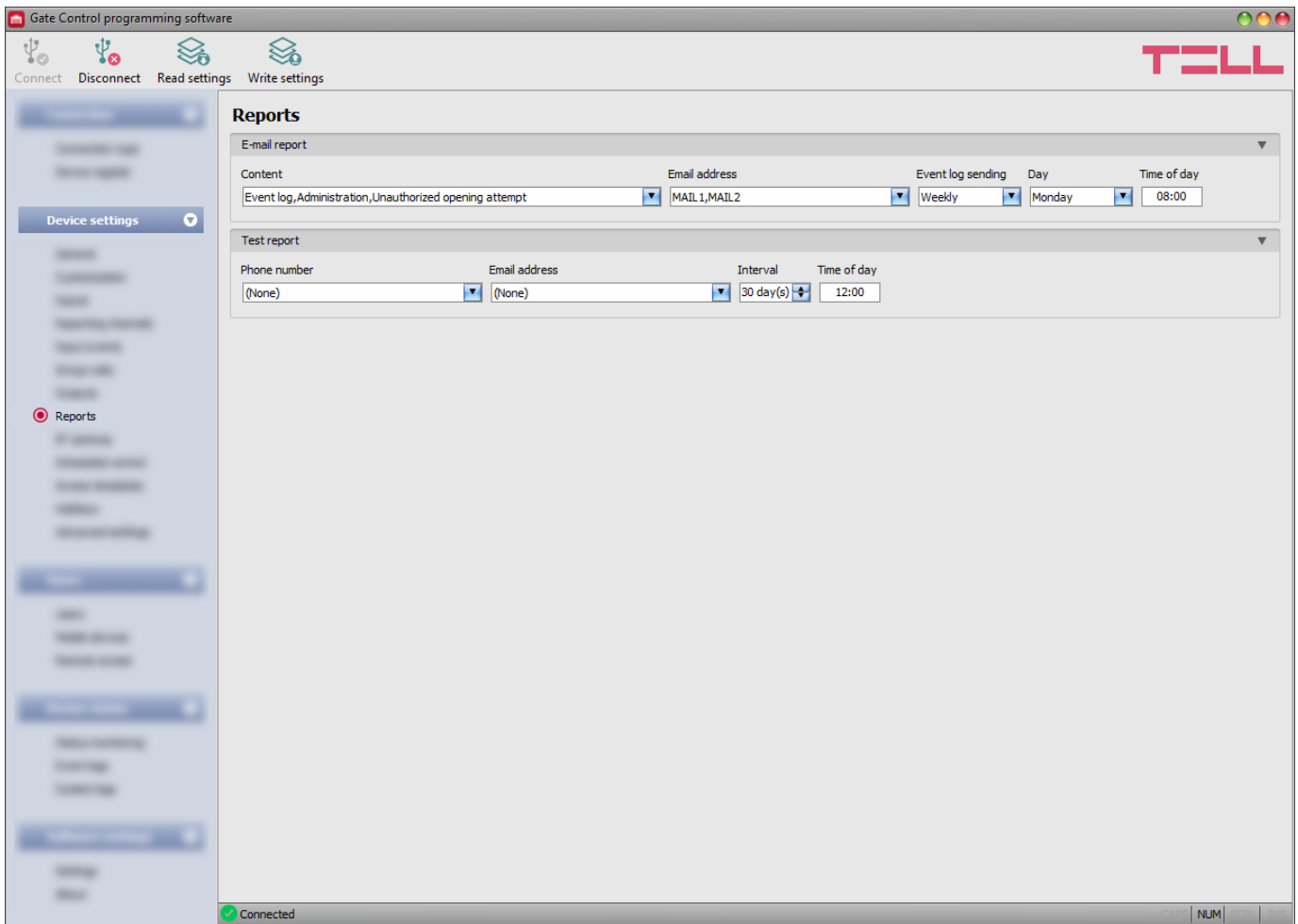
X = OUT1 pulse length (seconds) => for gate opening

Z = OUT2 pulse length (seconds) => for gate closing

With this control mode, the two outputs, that is opening and closing, can be controlled with separate buttons in the mobile application.



Opening and closing by separate calls/control commands. In idle state, outputs OUT1 and OUT2 provide an open contact between the **NO** and **COM** terminals. Output OUT1 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for X seconds upon the first control command/call, and then, upon the second control command/call, output OUT2 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for Z seconds. You can use this control mode if the gate automation control board requires triggers for opening and closing on the same input or on two different inputs. If opening and closing control is done on the same input, outputs OUT1 and OUT2 should be connected in parallel to the input to be controlled. This control mode cannot be used with hidden caller ID.


5.2.8 Reports



In this menu you can configure available reports which the system can send by e-mail or SMS.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

E-mail reports:

The system can send the event logs and monitored events by e-mail as reports. The report sending function requires Internet service.

Content: open the drop-down menu and select the report types which you want to receive by e-mail.

- **Event log:** a full event log can be sent daily or weekly.
- **Administration:** instant e-mail sending upon changing settings.
- **Unauthorized opening attempt:** instant e-mail sending when a user attempts unauthorized control (out of permitted entry period, in a restricted period, with hidden caller ID for control modes 2...5, or if the user is unknown)
- **Open-Close:** instant e-mail sending upon user-initiated open/close control.

E-mail address: select the e-mail address where the selected reports should be sent. You can configure the e-mail addresses in the "[Reporting channels](#)" menu.

Event log sending: select the event log sending interval. The system will send the event entries not sent yet but accumulated in the meantime, by the configured interval. There is a special case when the system will not send the event logs by the configured interval. This happens when the event storage is full. In this case, the logs will be sent as soon as the storage becomes full. Thereafter, it reverts to the normal sending interval.

Day: if you have selected weekly sending, select which day the event logs should be sent.

Time of day: enter the time of day for event log sending.

Test report:

The system can send periodic test reports via SMS and e-mail, by the configured interval.

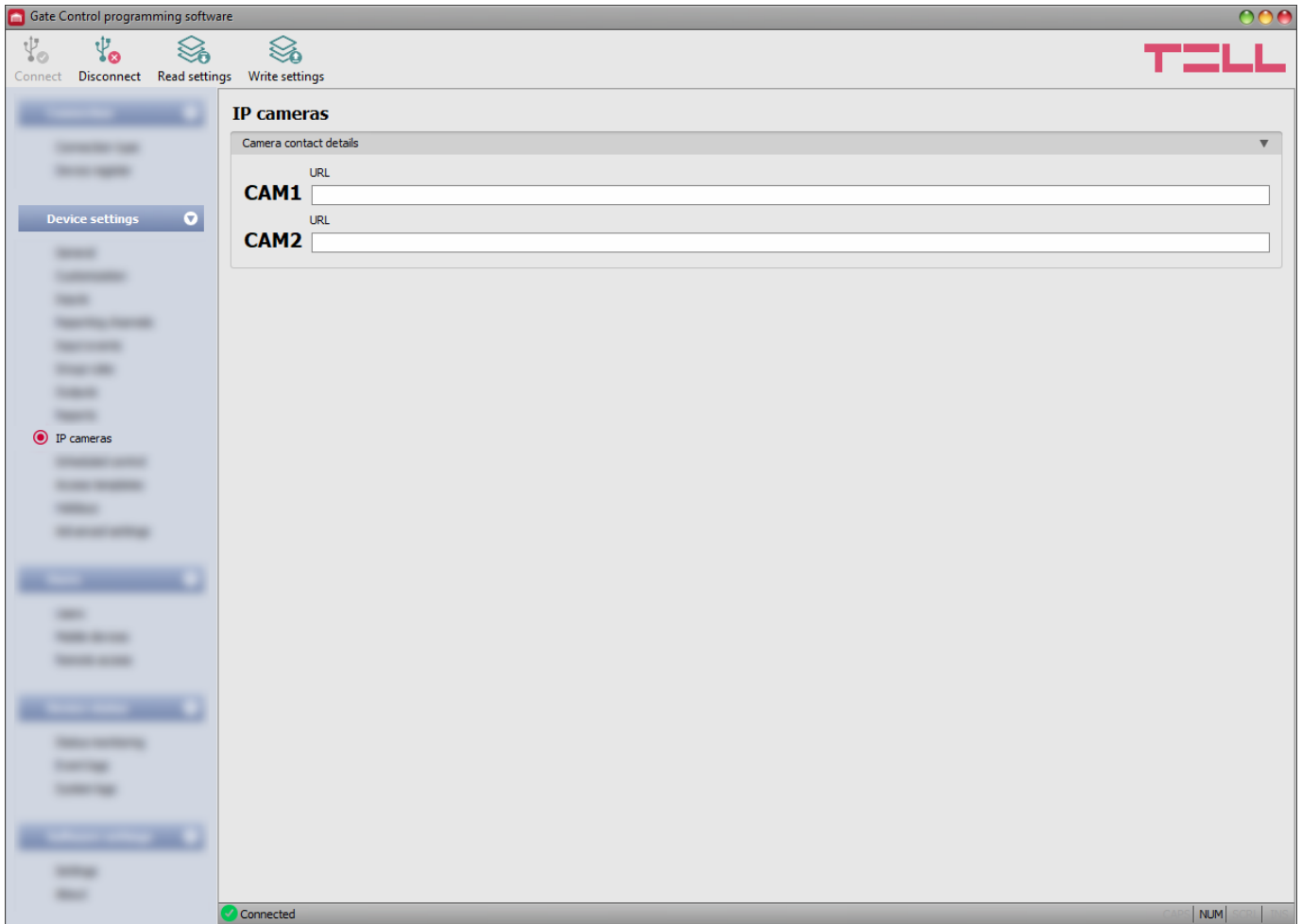
Phone number: select the phone numbers to which test reports should be sent by SMS. You can configure the phone numbers in the "[Reporting channels](#)" menu.

E-mail address: select the e-mail address to which test reports should be sent by e-mail. You can the e-mail addresses in the "[Reporting channels](#)" menu. The e-mail sending function requires Internet service.

Interval: the interval of test report sending specified in days.



Time of day: the time of day for test report sending.


5.2.9 IP cameras



You can configure in the **Gate Control PRO** system the contact details of up to 2 IP cameras which support the ONVIF standard. The system makes available the pictures of the configured IP cameras in the mobile application. Permission for viewing the camera pictures can be configured for each user and each camera separately in the user settings.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

Camera contact details:

URL: the picture path (link) of the IP cameras (**CAM1** and **CAM2**). You can enter the stream (live picture) or snapshot URL. The mobile application will show the live picture or the snapshot accordingly. Viewing a live picture generates higher data traffic on the mobile device.

This function works only with cameras that support the ONVIF standard! The manufacturer does not guarantee that the *Gate Control PRO* can be used with any IP camera, therefore, still before purchasing the *Gate Control PRO* device, the *Gate Control* mobile application assures an option to test the camera in advance and make sure that your camera works properly with the *Gate Control* mobile application (further details are available in the user's guide of the mobile application).

There are multiple methods to obtain the camera URLs. You can use the "***IP Camera Detector***" software made by the manufacturer (available on the manufacturer's website: <https://tell.hu/en/products/remote-management-software/ip-camera-detector>), the "***ONVIF Device Manager***" software (<http://sourceforge.net/projects/onvifdm>), or the camera's own software or technical manual.

To access the camera pictures from outside your local network, it is necessary to replace the local IP address and port in the URL obtained with the ONVIF camera detector program, with the external (WAN) IP address of your router and the external port, and after this enter the modified URL in the *Gate Control* programming software.

Example for modification of the stream URL, if only one camera is used:

Original URL:

rtsp://192.168.1.240:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a static IP address:

rtsp://***WAN IP***:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a static IP address and username/password:

rtsp://***username:password@WAN IP***:554/cam/realmonitor?channel=1&subtype....

Modified URL in case of using a domain name:

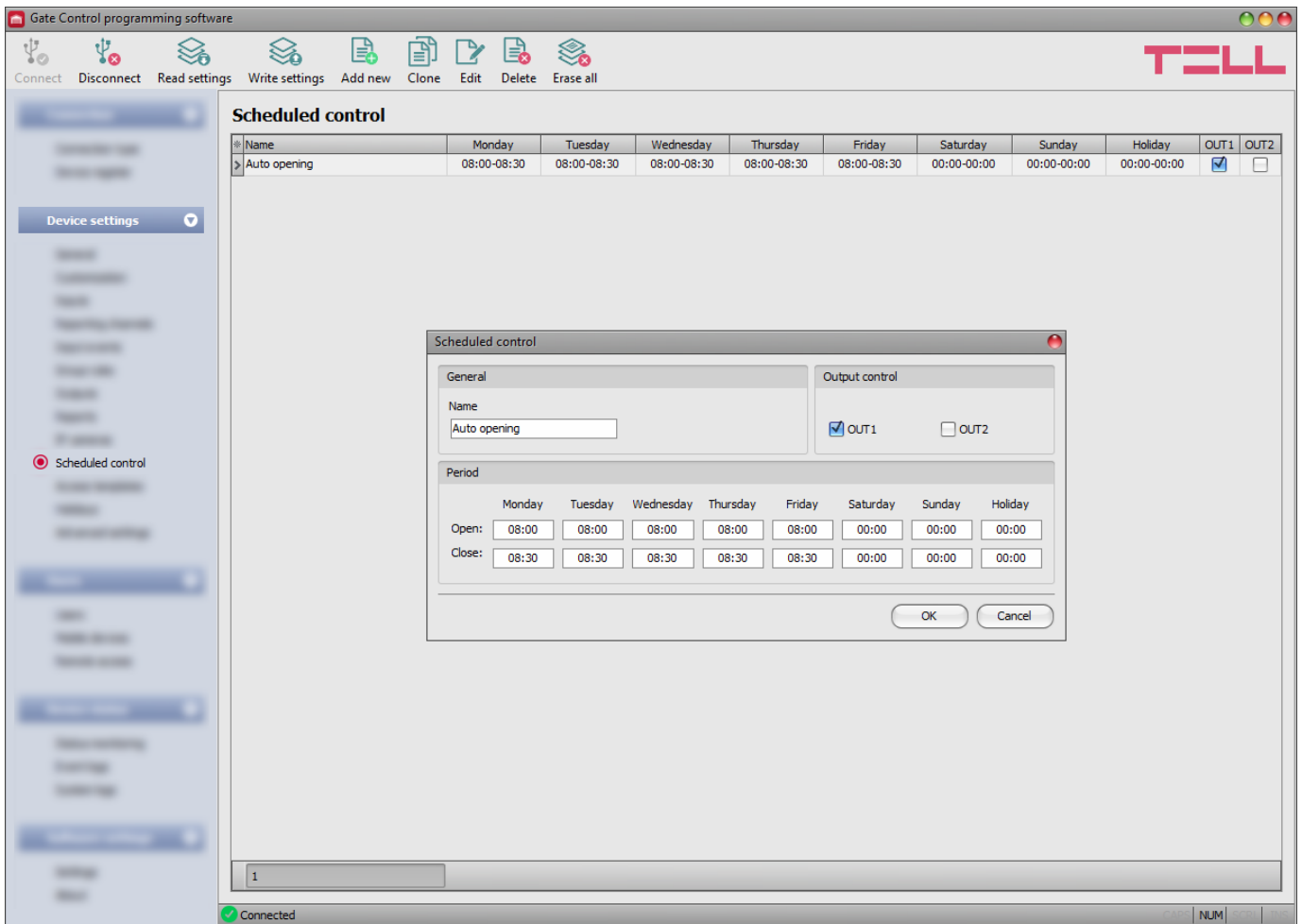
rtsp://***domain name***:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a domain name and username/password:

rtsp://***username:password@domain name***:554/cam/realmonitor?channel=1&subtype....

Further details and information on router configuration, port forwarding and dyndns configuration, are available in the "***Reference guide to the ONVIF camera support function***" document.

5.2.10 Scheduled control



The scheduled control function is used to control the outputs automatically at the configured time of day. The time of control can be configured in control plans. This function is useful when it is needed to open the gate automatically at certain times of day and hold it locked in open state for a given period of time, due to e.g., higher traffic, sparing thereby the mechanical parts and avoiding the users to have to open the gate every few seconds (e.g., in the morning, when a large number of people arrive at their workplace practically at the same time). It is also possible to configure multiple automatic opening periods for the same day by adding multiple plans.

Regarding the duration of opening and closing pulses, the scheduled control function always takes into consideration the time intervals configured for the given control mode, but the operation is different in certain control modes:








- in case of using control mode 1 or 2, output OUT1 and output OUT2 become activated permanently (they give a closed contact between the **NO** and **COM** terminals) during the interval between the time configured at “**Open**” and “**Close**” options. The scheduled control function can be used with these control modes for example with gate automations which hold the gate locked in open state while the controlling signal (closed contact) is present on their control input. In the “**Output control**” section, you can configure which output to be controlled by the scheduled control function (output OUT1, OUT2 or both at the same time).
- in case of using control mode 3, output OUT1 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for **X** seconds at the time configured at the “**Open**” option, then, after **W** seconds (gate opening interval) output OUT2 switches to a permanent idle state (gives a permanent open contact between the **NO** and **COM** terminals that interrupts the photocell loop and holds the gate locked in open state till the time configured at the “**Close**” option, when output OUT1 becomes activated again (gives a closed contact between the **NO** and **COM** terminals) for **Z** seconds.


- for control modes 4 and 5, output OUT1 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for **X** seconds at the time configured at “**Open**” option, and then, output OUT2 becomes activated (gives a closed contact between the **NO** and **COM** terminals) for **Z** seconds at the time configured at “**Close**” option.

Holding the gate open over midnight: if closing is scheduled to 23:59 and opening is configured for the next day from 0:00, closing will not be executed at 23:59, i.e., the device will not close the gate for 1 minute, but will continue holding the gate locked in open state according to the control plan configured for the next day. This rule applies explicitly to this specific case and will not apply to any other times of day.

If the gate’s position limit switch is connected to the device, the device will monitor if the gate opens and closes at the configured times of day. If opening or closing fails, the device sends notification about the gate position limit error by Push notification and/or SMS, according to the settings, and for control modes 3, 4 and 5 it repeats the opening or closing trigger pulse, i.e., it keeps trying to open or close the gate. The opening trigger pulse is repeated until the gate opens, i.e., opening is confirmed by the position limit switch, but up to the closing time configured in the given control plan. The closing trigger pulse is repeated until the gate closes, i.e., closing is confirmed by the position limit switch, but up to the next daily device restart or power loss. The trigger pulses are repeated by 1 minute if the configured gate opening/closing timeout value is lower than 60 seconds. If the configured opening/closing timeout value is higher than 60 seconds, the trigger pulse is repeated with a frequency according to the set value. The timeout values can be configured in the “**Inputs**” menu. The device sends the gate position limit error notification by SMS only once, while if the error still persists, by Push notification it is resent upon each opening or closing attempt, but up to 3 messages only.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.
- Adding a new scheduled control plan:
 Click on the “**Add new**” button to add a new scheduled control plan.
- Creating a copy of an existing scheduled control plan:
 To create a copy of the selected scheduled control plan, click on the “**Clone**” button. Please note that the new copy should have a different unique name.
- Editing an existing scheduled control plan:
 To edit the selected scheduled control plan, click on the “**Edit**” button.
- Deleting a scheduled control plan:
 To delete the selected scheduled control plan, click on the “**Delete**” button.
- Erasing all scheduled control plans:
 To erase all scheduled control plans, click on the “**Erase all**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

General:

Name: you can enter a custom name for the scheduled control plan in this section. The plan name should not exceed 16 characters, and the following characters should not be used: ^ ~ < > = ' " , | ? \$ & %

Output control:




OUT1, OUT2: if control mode 1 or 2 is used, you can select the output to be controlled by the scheduled control (OUT1 only, OUT2 only, or both at the same time).

Period:

Open: in this section you can configure the time of day for scheduled gate opening, for each day of the week and holidays.

Close: in this section you can configure the time of day for scheduled gate closing, for each day of the week and holidays.

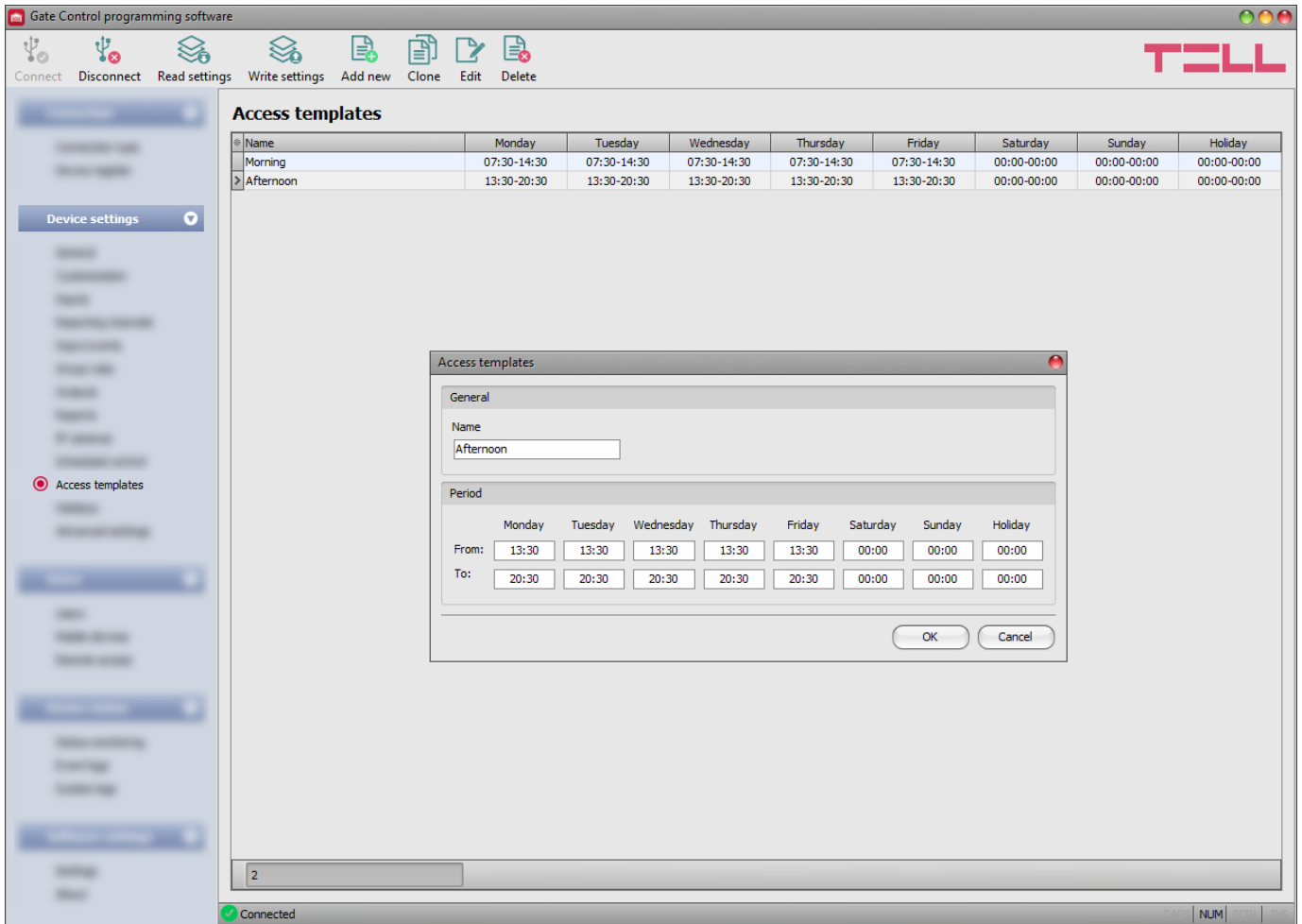
➤ Creating a new scheduled control plan:

- If you haven't read the settings yet, click on the “**Read settings**”  button to read the settings from the device.
- Click on the “**Add new**”  button.
- Configure the plan name.
- In case of using control mode 1 or 2, select which output to be controlled by the scheduled control (output OUT1, OUT2 or both at the same time).
- Configure the control periods for each day of the week and holiday.
- Click on the “**OK**” button.
- Click on the “**Write settings**”  button.

The system allows for adding up to 20 scheduled control plans.

If you want to disable scheduled control of the outputs for a certain day, then enter value **00:00** into both time fields (“**Open**” and “**Close**”) for the given day. In the “**Holiday**” section you can configure the scheduled control period for holidays. The holidays can be configured in the “**Holidays**” menu for several years in advance.

5.2.11 Access templates



The access templates are used to configure the allowed entry period for users. You can associate any of the created access templates, even more of them, with any user in the “**Users**” menu, thus the periods (even more intervals a day) can be defined for each user when they are allowed to control the system. When a user associated with an access template tries to control the system beyond an entry period configured in the given access template, the system will reject the control command of the given user, except if a configured group or custom rule overrides the access template.

The access templates are also used to configure the periods allowed or denied by group rules.

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

- Adding a new access template:



Click on the “**Add new**” button to add a new access template.

- Creating a copy of an existing access template:



To create a copy of the selected access template, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing an existing access template:




To edit the selected access template, click on the “**Edit**” button.

- Deleting an access template:



To delete the selected access template, click on the “**Delete**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “Write settings**”  button.**

General:

Name: you can enter a custom name for the access template in this section. The template name should not exceed 16 characters, and the following characters should not be used:




^ ~ < > = ' " , | ? \$ & %

Period:

From: in this section you can configure the time of day for each day of the week and holidays, from which, gate controlling will be allowed in the given template.

To: in this section you can configure the time of day for each day of the week and holidays, until which, gate controlling will be allowed in the given template.

➤ Creating an access template:

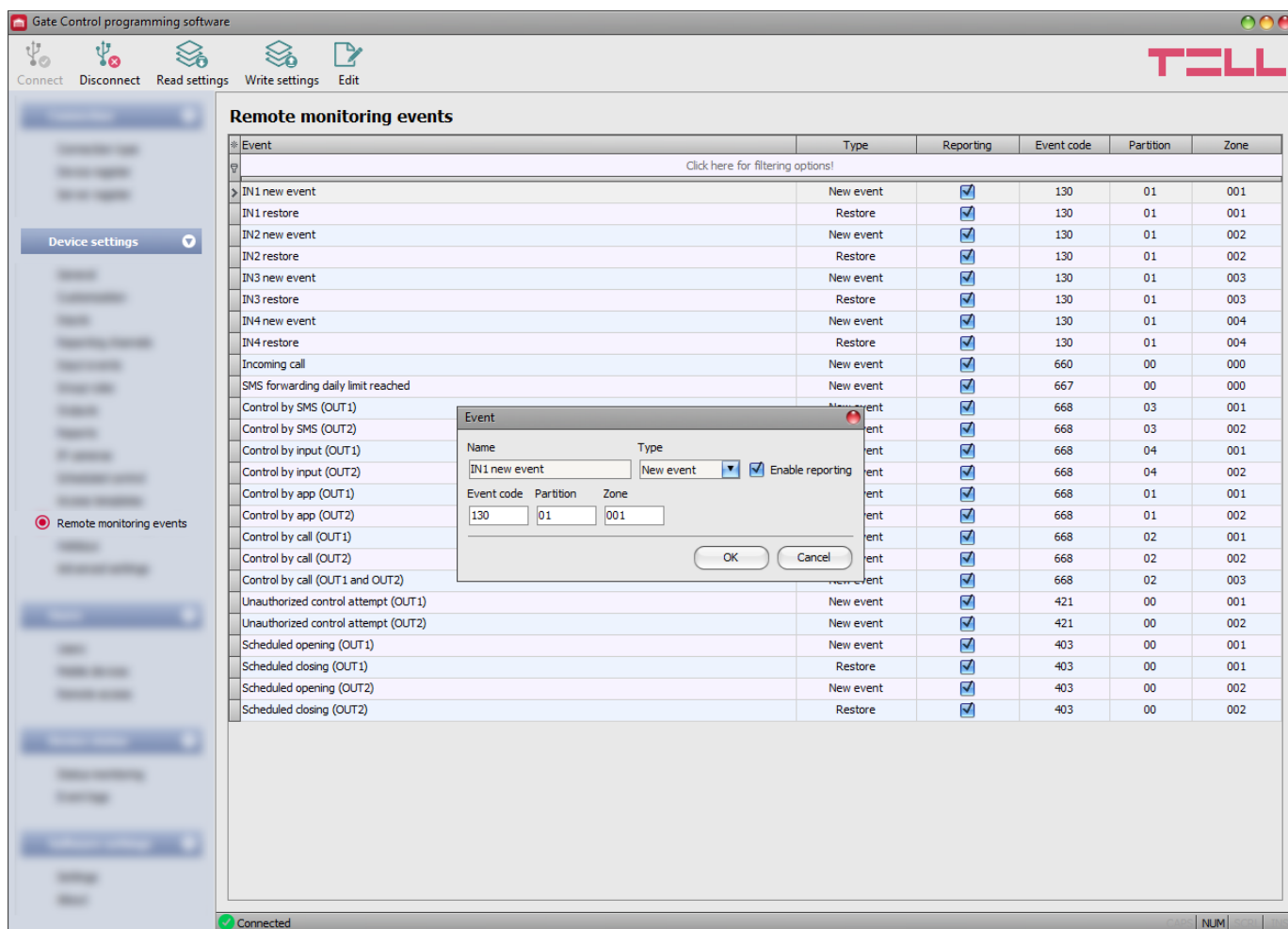
- If you haven’t read the settings yet, click on the “**Read settings**”  button to read the settings from the device.
- Click on the “**Add new**”  button.
- Configure the template name.
- Configure the allowed entry periods for each day of the week and holiday.
- Click on the “**OK**” button.
- Click on the “**Write settings**”  button.

The system allows for adding up to 50 access templates.

Controlling the gate is allowed from the time of day configured in the “**From**” fields of the access template, until the end of the minute value of the time of day configured in the “**To**” fields, i.e., if you configure e.g., 17:30 in the “**To**” section, the user will be allowed to control the gate until 17:30:59, but no longer at 17:31. If you want to forbid entry for a certain day, enter value **00:00** into both time fields of the given day. In the “**Holiday**” section you can configure the allowed entry period for holidays. The holidays can be configured in the “**Holidays**” menu for several years in advance.




5.2.12 Remote monitoring events


(available in the *Monitoring* product variant only)



The events available for reporting to remote monitoring station can be configured in this menu. Each event has a default Contact ID event code, partition, and zone number, which you can change as needed, and you can also enable or disable reporting separately for each event.

Available options:

- Reading the settings from the device:
 To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.
- Editing a remote monitoring event:
 To edit the selected remote monitoring event, click on the “**Edit**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

Remote monitoring events:

IN1...IN4 new event: this event is generated when input IN1...IN4 is triggered.

IN1...IN4 restore: this event is generated when input IN1...IN4 restores.

Incoming call: this event is generated when there is an incoming call.

SMS forwarding daily limit reached: this event is generated when the number of forwarded SMS messages reaches the daily limit configured in the “**General**” device settings menu.

SMS sending daily limit reached: this event is generated when the number of SMS messages generated and sent by the device reaches the daily limit configured in the “**General**” device settings menu.

Control by SMS (OUT1): this event is generated when output OUT1 is controlled by an emergency control SMS command.

Control by SMS (OUT2): this event is generated when output OUT2 is controlled by an emergency control SMS command.

Control by input (OUT1): this event is generated when output OUT1 is controlled by input IN1 or IN2, according to the settings in the “**Inputs**” menu.

Control by input (OUT2): this event is generated when output OUT2 is controlled by input IN1 or IN2, according to the settings in the “**Inputs**” menu.

Control by app (OUT1): this event is generated when a user controls output OUT1 via the mobile app.

Control by app (OUT2): this event is generated when a user controls output OUT2 via the mobile app.

Control by call (OUT1): this event is generated when a user controls output OUT1 via call.

Control by call (OUT2): this event is generated when a user controls output OUT2 via call.

Control by call (OUT1 and OUT2): this event is generated when a user controls outputs OUT1 and OUT2 at the same time via call.

Unauthorized control attempt (OUT1): this event is generated when someone attempts to control output OUT1 without authorization (e.g., from an unregistered phone number, or a user attempting control during a period not permitted by a configured rule).

Unauthorized control attempt (OUT2): this event is generated when someone attempts to control output OUT2 without authorization (e.g., from an unregistered phone number, or a user attempting control during a period not permitted by a configured rule).

Scheduled opening (OUT1): this event is generated when output OUT1 opens the gate based on a configured scheduled control.

Scheduled closing (OUT1): this event is generated when output OUT1 closes the gate based on a configured scheduled control.

Scheduled opening (OUT2): this event is generated when output OUT2 opens the gate based on a configured scheduled control.

Scheduled closing (OUT2): this event is generated when output OUT2 closes the gate based on a configured scheduled control.

Supply voltage low (< 11 V): this event is generated when the supply voltage value drops below the 11 V safety lower limit.

Supply voltage low restore (> 11.5 V): this event is generated when the supply voltage value returns above 11.5 V after a “**Supply voltage low**” event.

Supply voltage high (≥ 31 V): this event is generated when the supply voltage value matches or rises above the 31 V safety upper limit.

Supply voltage high restore (< 31 V): this event is generated when the supply voltage value returns below 31 V after a “**Supply voltage high**” event.

Periodic test report: this event is generated based on the interval and time of day settings configured in the “**Test report**” section, in the “**Reports**” menu.

Opening: this event is generated as an aggregated opening control when gate opening control occurs in any way, on any output.

Closing: this event is generated as an aggregated closing control when gate closing control occurs in any way, on any output (available with control mode No. 5 only).

Event:

Name: the name of the event. The event name is used for identification of the given event within the program.

Type: the type of the event, which can be new or restore. A new event is generated when the event occurs, and a restore event is generated when it restores. In the Contact ID protocol, new events are indicated with prefix 1 (or E), while restores are indicated with 3 (or R).

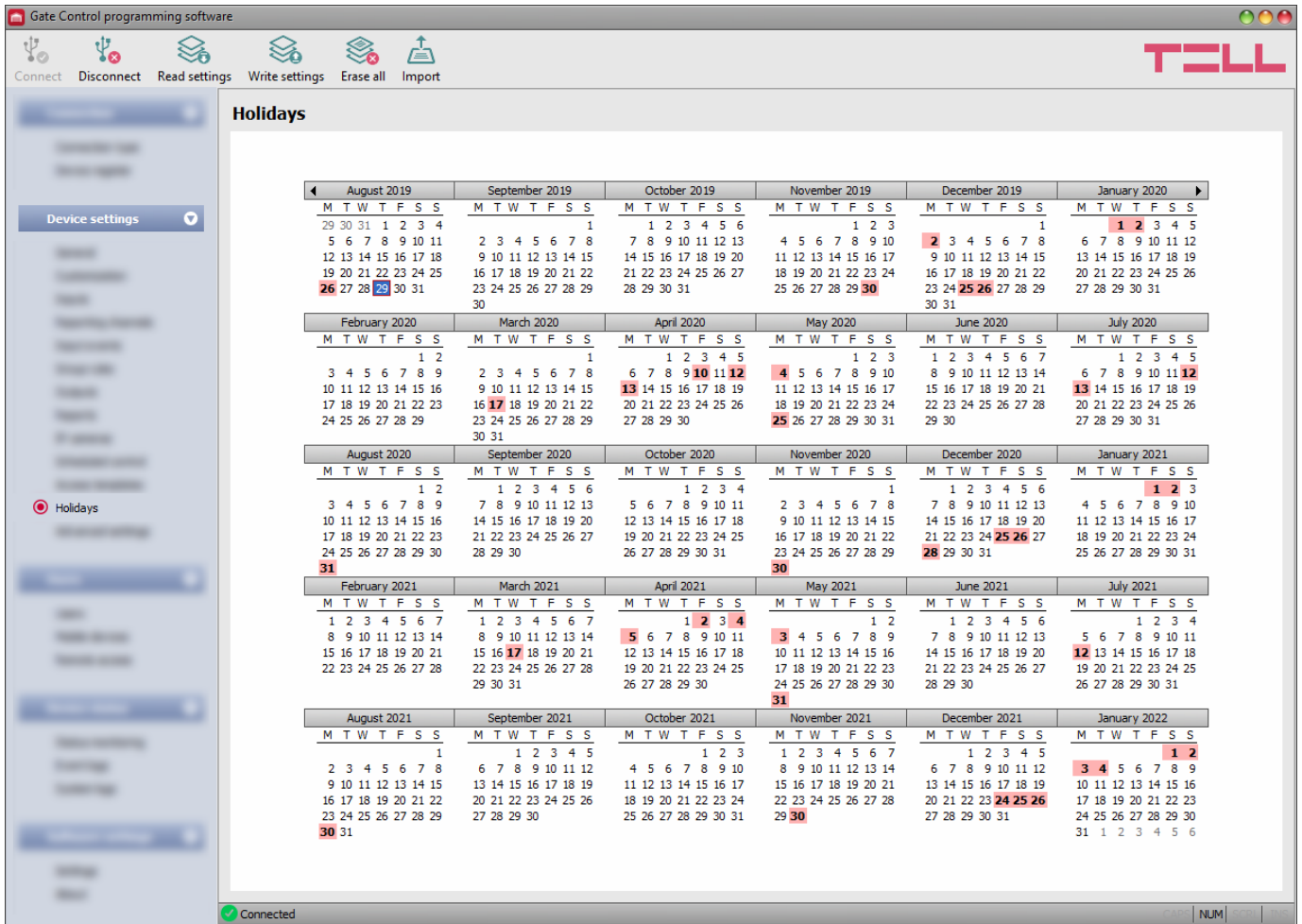
Enable reporting: you can enable or disable reporting of the given event to the remote monitoring station using this checkbox.

Event code: in this section you can configure the 3-digit Contact ID event code which you want to assign to the given event (e.g., 300 = system trouble). The event code consists of hexadecimal characters (0..9,A,B,C,D,E,F).

Partition: in this section you can configure the 2-digit partition number from 00 to 99, which you want to assign to the given event.

Zone: in this section you can configure the 3-digit zone number from 000 to 999, which you want to assign to the given event.

5.2.13 Holidays



You can select the holidays for several years in advance by double clicking on the dates in the calendar. The selected dates will be highlighted with red background color. To unselect a date, double click again on it. The system enables you to import holidays from a TXT file. Each date must be written in a new line in the file, and using strictly the following format:

dd/MM/yyyy or **yyyy.MM.dd** (e.g.: **25/12/2022** or **2022.12.25**)

Entry will be allowed on the selected holidays within the time interval configured in the “**Holiday**” section in the access templates and will be forbidden outside the time interval. You can override the entry periods defined in access templates using custom or group rules.

For scheduled control templates, the “**Holiday**” section of the template enables you to configure the time interval when the system will control the gate automatically on the configured holidays.

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

- Erasing all holidays:




To erase all holidays, click on the “**Erase all**” button.

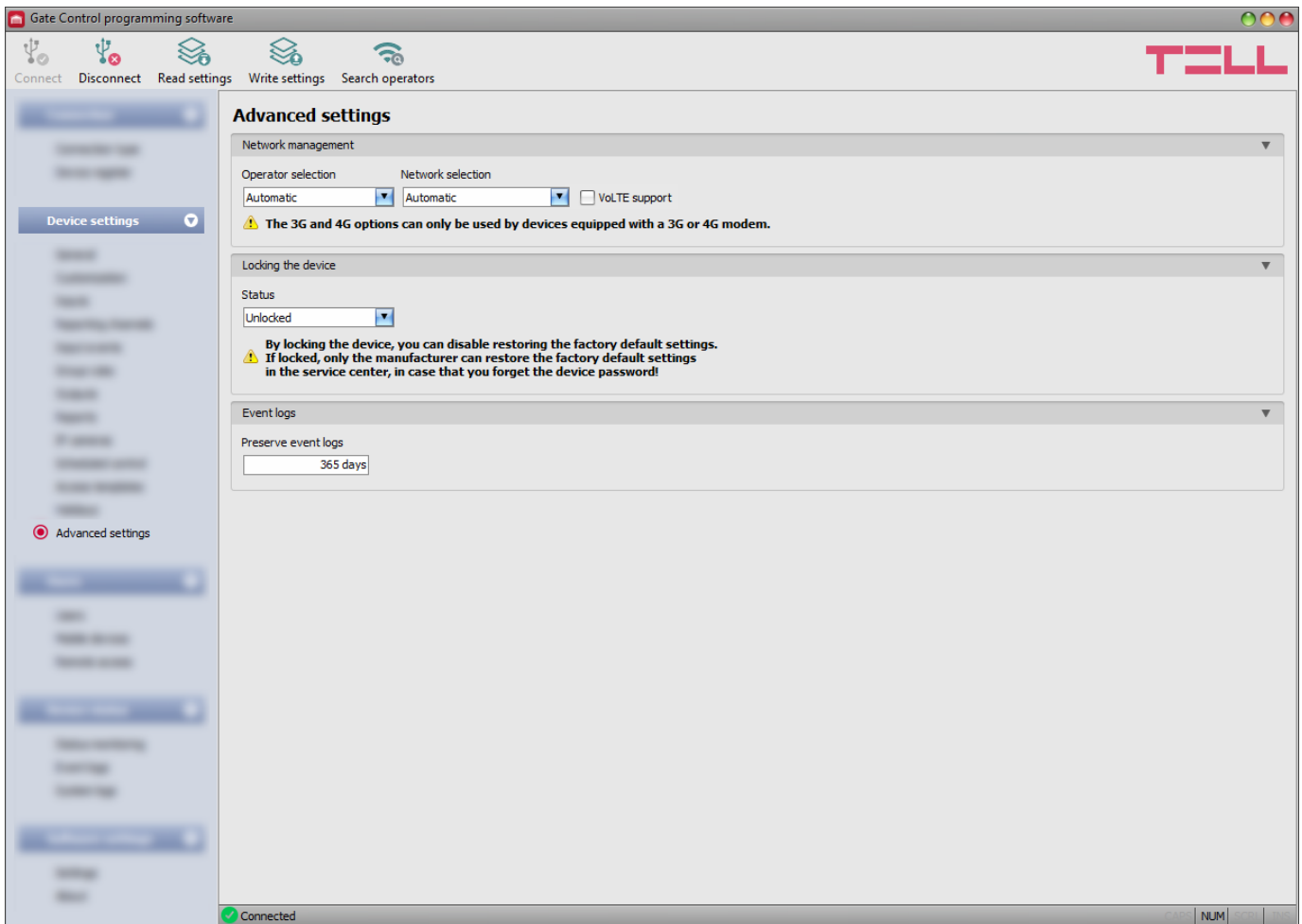
- Importing holidays:



To import a holiday database from CSV or TXT file, click on the “**Import**” button.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

5.2.14 Advanced settings



In this menu you can configure the device lock settings and select the default mobile operator and network to be used by the modem.

Recommended for experts only! Do not change the factory default settings unless necessary!

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read settings**” button. This will read all settings in all menus in the “**Device settings**” menu group.

- Writing the settings into the device:




After changing the settings or entering new settings, to take effect in the system, it is necessary to write the settings into the device by clicking on the “**Write settings**” button. This will write into the device the values changed in the menus in the “**Device settings**” menu group.

- Searching mobile operators:



To search mobile operators, click on the “**Search operators**” button. This is needed when you want to select a certain operator in the “**Operator selection**” drop-down menu to force the modem to use the given operator. After clicking on this button, the device will restart the modem and will reconnect to the mobile network to start operator searching. The search process may take up to 3 minutes. The end of the process will be indicated by a pop-up message, after which the list of available operators in the “**Operator selection**” drop-down menu will be updated automatically according to the search results.

Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “Write settings**”  button.**

Available options:

Network management:

Operator selection: using this drop-down menu you can select a mobile operator available with the given SIM card. To get the list of available operators, you must click on the “**Search operators**” button. If you select and set an operator, the device will use only the selected operator’s network. Please note that the search results may also contain operators which are not supported by your SIM card. If you accidentally select an unsupported operator, the device will use the default operator chosen automatically.

In the list of available operators, the program will indicate which networks (2G/3G/4G) of the given operators are available with the given SIM card, in the given location and with the given product model (it depends on the type of the modem). The default setting is the “**Automatic**”, i.e., the device will automatically choose the operator preferred by the given SIM card.

Operator ▲	2G	3G	4G
Automatic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telekom HU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Telenor HU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
vodafone HU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Network selection: the mobile network management in the device is automatic by default. If you experience problems with the stability of the mobile network in the given location, that is the device switches frequently between networks, you can select manually the network you want to use.

Available options:

- **Automatic:** the device will select the network automatically.
- **2G only:** use 2G (GPRS) network only.
- **3G only:** use 3G (UMTS) network only
Do not select this option for the **A7682** modem, as it does not support 3G technology! You can check the modem type in the “**Status monitoring**” menu.
- **4G only:** use 4G (LTE) network only

VoLTE support: this option must only be used for the **EG91** and **EG95** modems! You can check the modem type in the “**Status monitoring**” menu.

For the **EG91** and **EG95** modems: if you enable this option, the device will try to connect to the VoLTE service through which it can make and receive LTE-based calls. This requires mobile Internet and VoLTE service enabled on the SIM card installed in the device, and successfully configured APN settings. **Do not enable this option if any of the above is not available, otherwise the network connection may fail.**

Locking the device:

Status: you can lock your device with this setting, that is the factory default settings cannot be restored without knowing the device’s USB password.

- **Unlocked:** when unlocked, the factory default settings can be restored at any time, also without knowing the device’s USB password.
- **Locked:** when locked, restoring the factory default settings is disabled. You can restore the factory default settings only after logging in with the valid USB password of the device and changing the setting to unlocked. If you forget the USB password of the device, only the manufacturer can restore the factory default settings at the service center.

Event logs:

Preserve event logs: to fulfill GDPR requirements, the device records and stores event logs for the time interval configured in this section, but up to 1000 entries, which is the physical limit of the event logs. The device will delete entries older than the configured interval automatically when new entries are recorded. Thereby, the event logs will always keep available the latest events.


5.3 Users menu group


You can configure the user settings, mobile device settings, and remote access settings in the submenus available in the “**Users**” menu.


Attention! The device handles the device settings and user settings (users, mobile devices, remote access) as two different data categories, therefore you must read and write them separately in the device.

- **Changing the user, mobile device, or remote access settings:**

To change the settings of user records, mobile device records, or remote access records, you must read the user you want to edit from the device. For this, you can read all users by


clicking on the “**Read users**”  button in any submenu in the “**Users**” menu group, or you

can use the search tool by clicking on the “**Search**”  button to read a specific user or users only. If you haven’t read the device settings yet, the program will read these too automatically before reading the users. After making changes in the user

related settings, write the entries into the device by clicking on the “**Write users**”  button. If you have also changed the device settings and you haven’t written the changes into the device yet, the program will write these changes too before writing the users.

- **Overwriting the full device configuration (device settings, users, mobile devices, and remote access entries):**

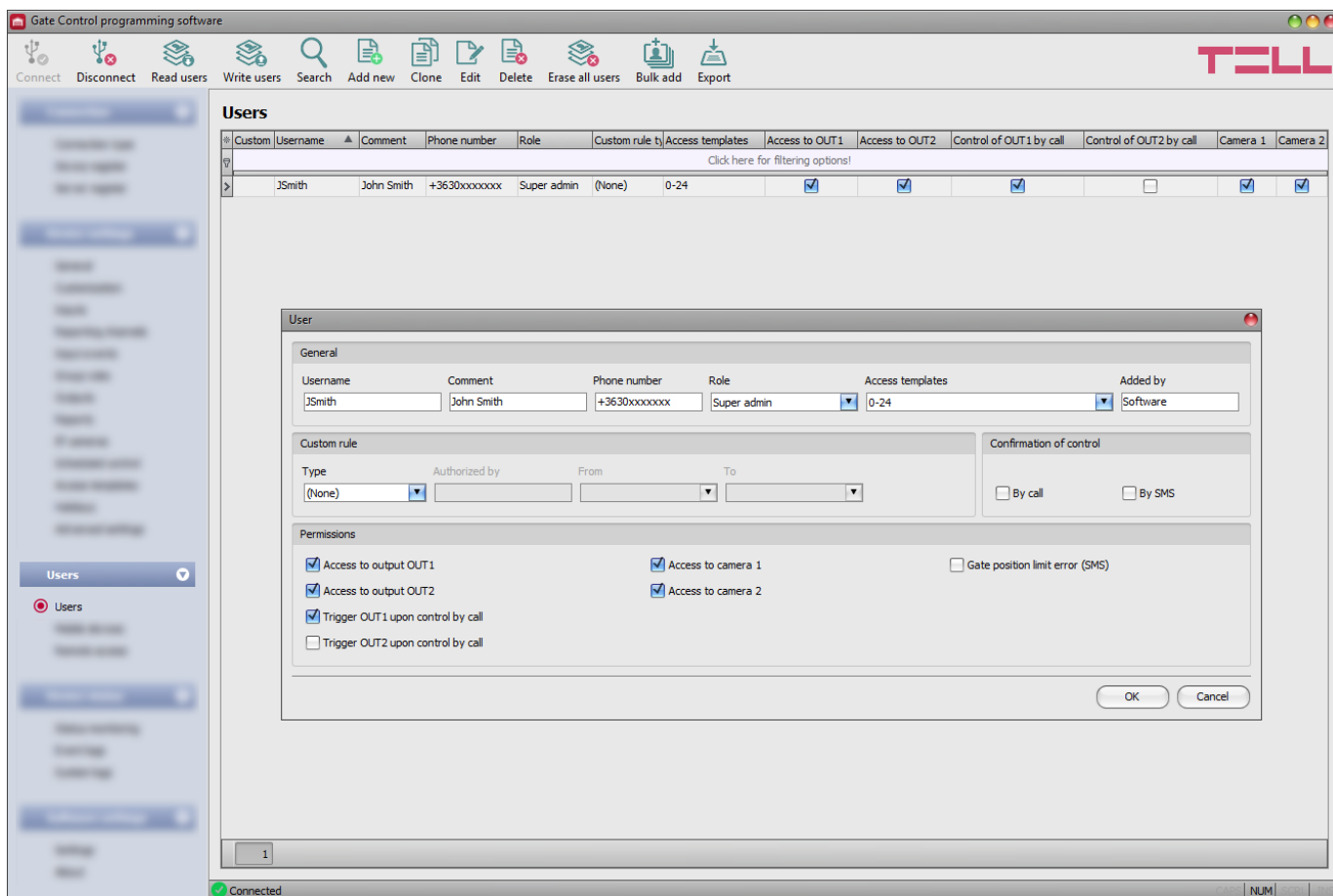
If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users

and the settings in the submenus, and then click on the “**Create system backup**”  button in the “**General**” device settings menu. You can import the saved backup into the

program using the “**Restore from backup**”  button, and then write imported settings into

the device by category, using the “**Write settings**”  and the “**Write users**”  buttons.

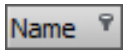

5.3.1 Users



In this menu you can add users and configure user permissions, as well as configure custom entry rules separately for each user if needed.

The system can be controlled from registered user phone numbers and mobile applications, unless a group rule is configured which affects this. Depending on the product variant, you can register up to 20 or 1000 users with different roles and permissions.

You can filter data in any column using the filter placed under the header of the spreadsheet. Filtering can be cancelled by deleting the entered or selected filter condition.

An advanced filter is also available for each column by clicking on the filter icon  which appears on the right-hand edge of each column header by moving the mouse pointer on the given header. You can toggle between ascending and descending data sorting by clicking on a column's header. You can toggle between show/hide columns or change the order of the columns in the spreadsheet by drag-and-drop, after clicking on the button marked with a star  in the top left corner of the spreadsheet. You can also change the order of the columns by moving the header of the columns.

Available options:

- Reading the users from the device:



To read the users stored in the device, click on the “**Read users**” button. This will read all entries in all menus in the “**Users**” menu group. Additionally, if you haven’t read the device settings yet separately, it will also read all entries in the “**Device settings**” menu group. If you want to read a specific user or users only, use the “**Search**” option.

- Writing the users into the device:



After changing the settings or adding new entries, to take effect in the system, it is necessary to write the users into the device by clicking on the “**Write users**” button. This will write into the device all entries in all menus in the “**Users**” menu group. Additionally, if you have changed the device settings but haven’t written the them yet separately into the device the, it will also write all entries in the “**Device settings**” menu group.

- Search users:



To search users, click on the “**Search**” button, and enter the searched name or phone number. The search engine can search for a piece of text in usernames, comments, and phone numbers. The program will list the results in the table.

- Adding a new user:



Click on the “**Add new**” button to add a new user.

- Creating a copy of an existing user:



To create a copy of the selected user, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing an existing user:



To edit the selected user, click on the “**Edit**” button.

- Deleting a user:



To delete the selected user, click on the “**Delete**” button.

- Erasing all users:



To erase all users, click on the “**Erase all users**” button.

- Bulk adding users:



To add users from CSV file or from database exported from an earlier device model, click on the “**Bulk add users**” button, select the file extension of the file that containing the users, and then browse the file. After this, the program will open a new window, where you can configure the settings and permissions of users to be added. All users will be added with the same settings and permissions configured here. Users already stored in the device will not be erased by bulk adding new users. Imported users will be added to the ones stored in the device. After configuring the user settings, click on the “**Import**” button. By this, the program will read the user entries from the selected file and will prepare an import summary.

Bulk add users

General

Role: User Access templates: 0-24 Added by: Software

Custom rule

Type: (None) Authorized by: From: To:

Confirmation of control

☐ By call ☐ By SMS

Permissions

☒ Access to output OUT1 ☐ Access to camera 1 ☐ Gate position limit error (SMS)

☐ Access to output OUT2 ☐ Access to camera 2

☒ Trigger OUT1 upon control by call

☐ Trigger OUT2 upon control by call

Import summary

Type	Information
Information	New user: LisaT
Information	New user: Pete
Information	New user: Nicky
Information	New user: JS05
Warning	Name missing!: #5 +3630xxxxxxx
Error	Error in line: #6
Information	New user: Jen118
Summary	Successful: 5, Warning: 1, Error: 1,

Users will be imported in the program first. Imported users will be added in the device only after writing the users into the device.

Import Close

The structure requirements of the CSV file, in case of importing from CSV:

The program considers the first line of the CSV file as the header. Therefore, it will not process the first line!

The file should contain the users starting from the second line. The line should start with the username, followed by a semicolon, and then the comment, and then again, a semicolon followed by the phone number.

Example:

Username;Comment;Phone number

JSmith;John Smith;+3630xxxxxxx

The program will indicate, if there are issues in the file to be imported, e.g., duplicate usernames, phone numbers, or names or phone numbers which already exist in the device in that particular case, or other entries that the program cannot process.

The program classifies the entries into 3 categories, which you can find in the **"Type"** column, and marks each with a different background color for better transparency:


Information (green background color): user entries imported successfully. If the imported file contains multiple records with the same username, the program will overwrite in order each such record with the next one, thus it will keep the values of the last such record (of **"Warning"** category, with **"Updated user"** comment).

Warning (yellow background color): entries processed successfully, but the name and/or the phone number appears more than once in the file, or already exists among the users registered in the device, or the name or the phone number is missing.

Error (red background color): entries with errors, which the program cannot process.

The program will not import entries marked as **"Warning" or **"Error"** into the system! An exception to this is the case mentioned above, when the file contains duplicate usernames.**


At the bottom of the list, you can find a summary line with the number of entries imported successfully, the ones marked as warnings, and the ones with errors. You can close the window by clicking on the “**Close**” button, after which the entries imported successfully will show up in the user list. After that, you can edit and continue to configure the users imported into the program as needed, and when

finished, write the users into the device by clicking on the “**Write users**”  button.



- Save users to file:



Click on the “**Export**” button to save the users to file in CSV format. The program will export the usernames, the comments, and the associated phone numbers.

Please note that after you make changes, you must write the users into the device to apply the changes. For this, click on the “Write users**”  button.**

➤ Adding a new user:

- Click on the “**Add new**”  button.
- Enter the user’s username and phone number.
- Select the user’s role.
- Select access templates if needed.
- Configure the user’s permissions.
- Click on the “**OK**” button.
- Click on the “**Write users**”  button.



➤ Adding the first super admin or admin user and registering the mobile application

It is practical to add the first super admin or admin user using the programming software and configure the user’s role (super admin or admin) and permissions (control permissions, camera access, notifications) by following the steps specified above. After that, there are several options for registering the mobile application. These options are offered by the Admin mobile application:

- Registering over the Internet:
 - by reading the QR code for app registration requiring approval
 - by reading the QR code for direct app registration
 - by filling in the data fields manually
- Registering by SMS

The easiest and fastest way from the options mentioned above is registering over the Internet using the QR code for app registration requiring approval. For this, follow the steps below:

- In the mobile application, choose the option for registration over the Internet, and then enter the username configured with the programming software.
- Connect the **Gate Control PRO** device to the PC, and then read the settings from the device in the programming software.

- Click on the “**QR code**”  button in the “**Mobile devices**” menu in the programming software, and then click on the “**QR code for app registration requiring approval**” tab.
- Tap on the “**Read QR code**” button in the mobile application and read the QR code for app registration requiring approval from the programming software.
- Send the registration request by tapping on the “**Send**” button in the mobile application.
- You will receive the registration request on the same mobile device in a few seconds by a Push message. Open your phone’s notification manager and tap on the received message. By this, the mobile application will open the registration form. Tap on the “**Approve**” button at the bottom of the form to approve the registration. As an alternative, you can approve the registration in the programming software too, in the “**Mobile devices**” menu. For this, select your device in the list by clicking on it, and then click on the “**Approve**”  button.
- After that, the mobile application will connect to the **Gate Control PRO** device, it will validate the registration, and then it will add the device icon on the main screen.

➤ User settings:

General:

Username: the user’s short username should not exceed 40 characters, and the following characters should not be used: ^ ~ < > = ' " , | ? \$ & %. The username is used to identify the user in the system. The username is case sensitive!

Comment: you can add a custom comment to the given user that should not exceed 40 characters, and the following characters should not be used: ^ ~ < > = ' " , | ? \$ & %. The comment is an additional data, which is also covered by the search function. This makes easier searching and filtering users in the system. The comment is case sensitive!

Phone number: enter the phone number in international format (e.g., +3630xxxxxxx). The system accepts maximum 19 digits. Accepted characters are “+”, “0...9” only.

Role: you can choose out of 3 role levels:

- **User:** can only control the system.
- **Admin:** can control the system and manage users (add/modify/delete).
- **Super admin:** full permission, can control the system and manage users, settings, templates, and holidays.

Access templates: you can associate any of the configured access templates, even multiple templates with a user. If there is no access template associated with the given user, then a 0-24-hour template will be associated automatically, which means that the given user can control the system at any time, 24 hours a day. You can associate access templates with a user by enabling the given templates in the drop-down menu using the checkboxes.

Added by: in this section, the system shows the identifier of the admin or super admin, who has registered the new user. This is filled in automatically by the system. If the new user has been added using the programming software, the system will show “**Software**” in this section.

Custom rule:

Using the custom rule, you can override configured group rules and access templates associated with a user. This function is useful when entry permission of a given user must be different in some manner from the access templates (e.g., any user may control the system on a certain day except this user, because he is on vacation, etc., or even on a weekend day, entry is forbidden for all users, except this user who needs to work). Group rules will not override configured custom rules. If a custom rule is configured for a user, the program will indicate that in the “**Custom rule**” column in the user list.

Type:

- **None:** there is no custom rule configured.
- **Allow:** control of the system will be allowed in the specified period, against any associated access templates or a group rule, which may normally forbid access.
- **Deny:** control of the system will be denied in the specified period, against any associated access templates or a group rule, which may allow access.

Authorized by: in this section, the system shows the identifier of the admin or super admin, who has configured the custom rule for the given user. This is filled in automatically by the system. If the custom rule has been configured using the programming software, the system will show “**Software**” in this section.

From: enter the date and time for the beginning of the custom rule’s period of validity. You can select the date and enter the time in the calendar after opening the drop-down menu.

To: enter the date and time for the end of the custom rule’s period of validity. You can select the date and enter the time in the calendar after opening the drop-down menu.

Confirmation of control:

By call: the system can confirm a successful control of the gate by making a call to the phone number of the user who controlled the gate. You can enable this option for each user separately.

Attention! If the modem is currently connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call. For the product variant with an Ethernet port, this should be considered if the device is used with mobile data only.

By SMS: the system can confirm a successful control of the gate by sending an SMS message to the phone number of the user who controlled the gate. You can enable this option for each user separately.

Permissions:

If you are using one of the control modes for 2 gates (control mode 1 or 2), you can enable permissions for each user separately, to control output OUT1 only, output OUT2 only, or both outputs separately over the Internet, using the mobile application. If the option to control output OUT1 and/or OUT2 is enabled for a user, you can also select which output should the device control (output OUT1 only, output OUT2 only, or both outputs at the same time), when the given user controls the system by call, or the user’s mobile application controls the system by call, if controlling over the Internet fails due to a connection error. Unfortunately, it cannot be determined from a call, which output the user would like to control, therefore it needs to be configured in advance with this option, which output (or both at the same time) the system should control in such a case.

Access to output OUT1: if this option is enabled, the user can control output OUT1. Accordingly, the “**Gate1**” control button will be available in the given user’s mobile application. This option is only available when control mode 1 or 2 is used.

Access to output OUT2: if this option is enabled, the user can control output OUT2. Accordingly, the “**Gate2**” control button will be available in the given user’s mobile application. This option is only available when control mode 1 or 2 is used.

Trigger OUT1 upon control by call: if this option is enabled, the device will control output OUT1 when the given user controls the system by call, or the user’s mobile application controls the system by call, if controlling over the Internet fails due to a connection error.

Trigger OUT2 upon control by call: if this option is enabled, the device will control output OUT2 when the given user controls the system by call, or the user’s mobile application controls the system by call, if controlling over the Internet fails due to a connection error.

Access to camera 1: if this option is enabled and the URL for IP camera 1 is configured, the “**Camera 1**” button will be available in the given user’s mobile application, which can be used to view the picture of the given camera.

Access to camera 2: if this option is enabled and the URL for IP camera 2 is configured, the “**Camera 2**” button will be available in the given user’s mobile application, which can be used to view the picture of the given camera.

Gate position limit error (SMS): if this option is enabled, the device sends notification by SMS to the user’s phone number, if the gate fails to open or close within the configured time intervals. If a gate position limit error occurs, the device will send the error notification by SMS to all users for which this option is enabled. This function works only if the position limit switch of the gate is connected to input IN3 (and IN4, in case of 2 gates), and is enabled in the “**Inputs**” menu.

➤ **Status indicator columns:**


Custom rule: the program uses icons in this column to mark users for whom a custom rule is configured.



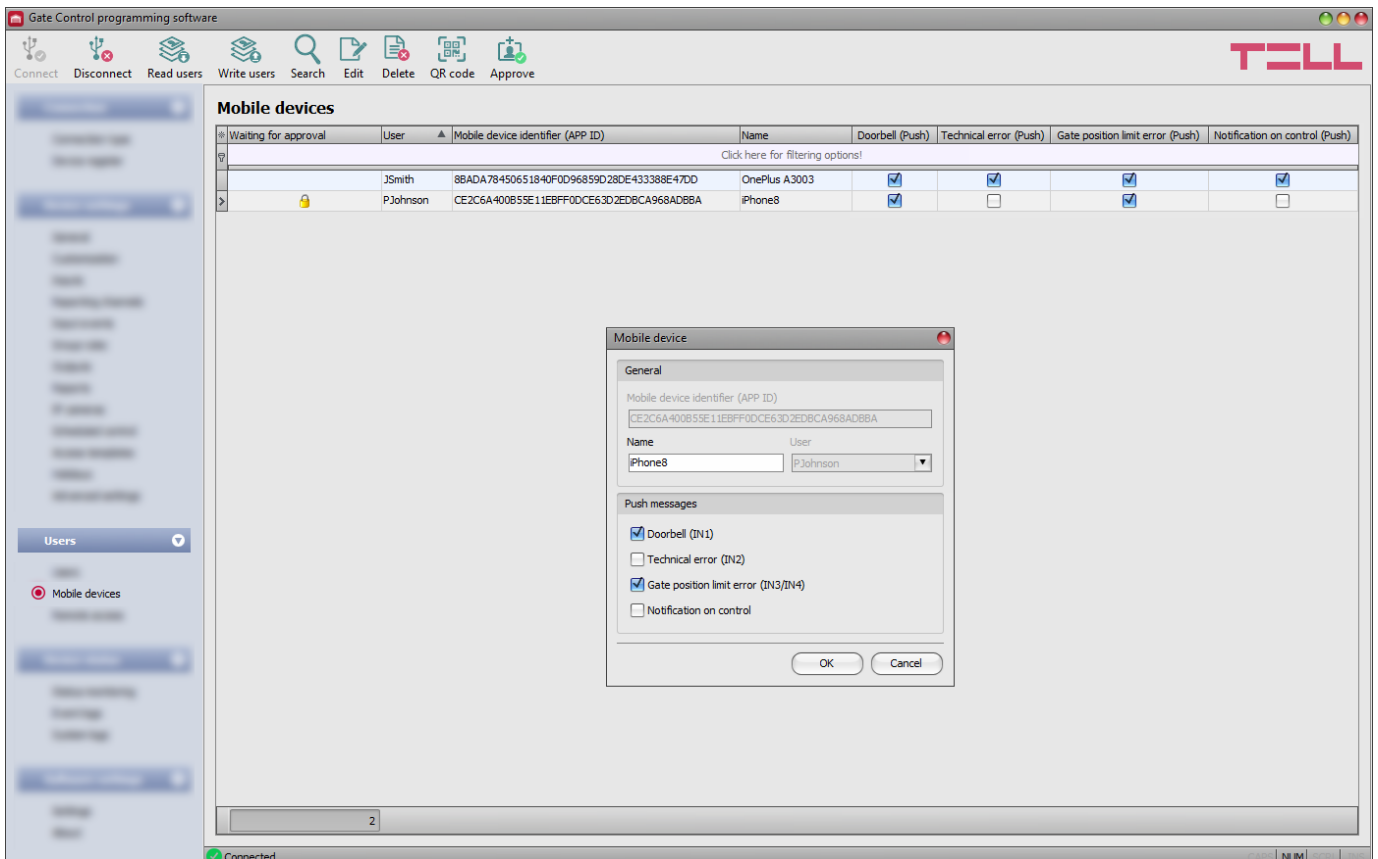
(green icon): a permitting custom rule.



(red icon): a restricting custom rule.

Waiting for approval or rejected: the program uses a yellow icon  in this column to mark users whose mobile app registration that required approval has not been approved yet or has been rejected by an admin or super admin.

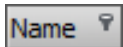

5.3.2 Mobile devices



Mobile devices with registered mobile applications and ones waiting for approval are listed in this menu. This is where you can configure which mobile devices shall receive Push notifications. For the 1000-user product variant you can register altogether up to 2000, while the 20-user product variant allows you to register up to 40 mobile devices and remote access passwords in the system, which are distributed dynamically among registered users. The QR codes used for registering the mobile application are also available in this menu.

You can register the mobile application with direct app registration, by reading the QR code for direct app registration, also directly by SMS, or by submitting a registration request by reading the QR code for app registration requiring approval. When registering with direct app registration, the mobile device is validated and added automatically in the system, while for registration that requires approval, a registration request is sent by Push message to the administrators configured in the system, who may approve or refuse the registration. After approving the registration, the approved mobile device will be validated and added in the system. As an alternative, you can approve registrations in the programming software too, in this menu.

You can filter data in any column using the filter placed under the header of the data table. Filtering can be cancelled by deleting the entered or selected filter condition.

An advanced filter is also available for each column by clicking on the filter icon  which appears on the right-hand edge of each column header by moving the mouse pointer on the given header. You can toggle between ascending and descending data sorting by clicking on a column's header. You can toggle between show/hide columns or change the order of the columns in the spreadsheet by drag-and-drop, after clicking on the button marked with a star  in the top left corner of the spreadsheet. You can also change the order of the columns by moving the header of the columns.

Available options:

- Reading the users from the device:



To read the users stored in the device, click on the “**Read users**” button. This will read all entries in all menus in the “**Users**” menu group. Additionally, if you haven’t read the device settings yet separately, it will also read all entries in the “**Device settings**” menu group. If you want to read a specific user or users only, use the “**Search**” option.

- Writing the users into the device:



After changing the settings or adding new entries, to take effect in the system, it is necessary to write the users into the device by clicking on the “**Write users**” button. This will write into the device all entries in all menus in the “**Users**” menu group. Additionally, if you have changed the device settings but haven’t written them yet separately into the device, it will also write all entries in the “**Device settings**” menu group.

- Search users:



To search users, click on the “**Search**” button, and enter the searched name or phone number. The search engine can search for a piece of text in usernames, comments, and phone numbers. The program will list the results in the table.

- Editing the settings of an existing mobile device:



To edit the settings of the selected mobile device, click on the “**Edit**” button.

- Deleting a mobile device:



To delete the selected mobile device, click on the “**Delete**” button. If you delete a mobile device, the system can no longer be controlled via the Internet from the mobile application on the given mobile device. However, control by call may still work if you have not deleted the user, and control permission is enabled for the given user.

- QR code:



By clicking on the “**QR code**” button, you can access the QR codes used for registering the mobile application. The QR codes include the connection data: device identifier, server IP address and port number. To generate the QR codes, it is necessary that the program reads the device identifier from the device, therefore this button is only available when the device is connected to the software.



The programming software generates two QR codes:

➤ **QR code for direct app registration**

By reading this QR code in the **Gate Control** mobile application, you can register the mobile application directly in the **Gate Control PRO** device. To use this registration option, it is necessary to configure the “**App registration password**”. This password must be entered in the mobile application when registering. By owning the QR code for direct app registration and the app registration password, anyone can register the mobile application installed on their mobile device in the given **Gate Control PRO** device.

➤ **QR code for app registration requiring approval**


By reading this QR code in the **Gate Control** mobile application, you can register the mobile application in the **Gate Control PRO** device by a registration request sent to the administrators configured in the given **Gate Control PRO** device. The app registration will be fulfilled when an administrator approves the request.


Note! If a registration request that requires approval is not approved nor refused, and then, the given user tries to register using direct app registration, the registration will fail and the app will give an error message, since the registration already exists. In this case, the administrator must approve, refuse, or delete the given registration in the programming software.

You can read the QR code you want to use with your mobile device directly from the PC screen, or from a printed sheet, if printed. For direct printing, click on the “**Print**” button found below the QR code, or copy the QR code to clipboard using the “**Copy to clipboard**” button, and then paste into a new document (e.g., Word) where you can also add instructions of use, and print from there. You can also save the QR code to file in BMP format, using the “**Save to file**” button.

- Approve:



The “**Approve**” button is used to approve mobile app registrations waiting for approval. To approve a registration, select the mobile device which you want to approve, and then click on the “**Approve**” button. After clicking on this button, you must write the users into the device to validate the approval in the system. A user with a mobile application waiting for approval cannot control the system until approved by an administrator through their mobile application or using this button in the software. Registrations waiting for approval are marked with a yellow padlock  icon in the table’s “**Waiting for approval**” column. This button is not available when an already approved mobile device is selected.

Please note that after you make changes, you must write the users into the device to apply the changes. For this, click on the “Write users**”  button.**

Mobile device settings:

General:

Mobile device identifier (APP ID): the mobile device’s unique identifier, used by the system to identify the device.

Name: you can enter a custom name for the mobile device in this section. The name entered here is used to identify the mobile device in the program and in the event logs. The device name should not exceed 40 characters, and the following characters should not be used:

^ ~ < > = ' " , | ? \$ & %

User: when adding a new mobile device manually, you can select the user, who you want to associate the new mobile device with. For registrations performed by users, the user cannot be changed.

Push messages:

Attention! Push messages are sent to maximum 40 mobile devices!

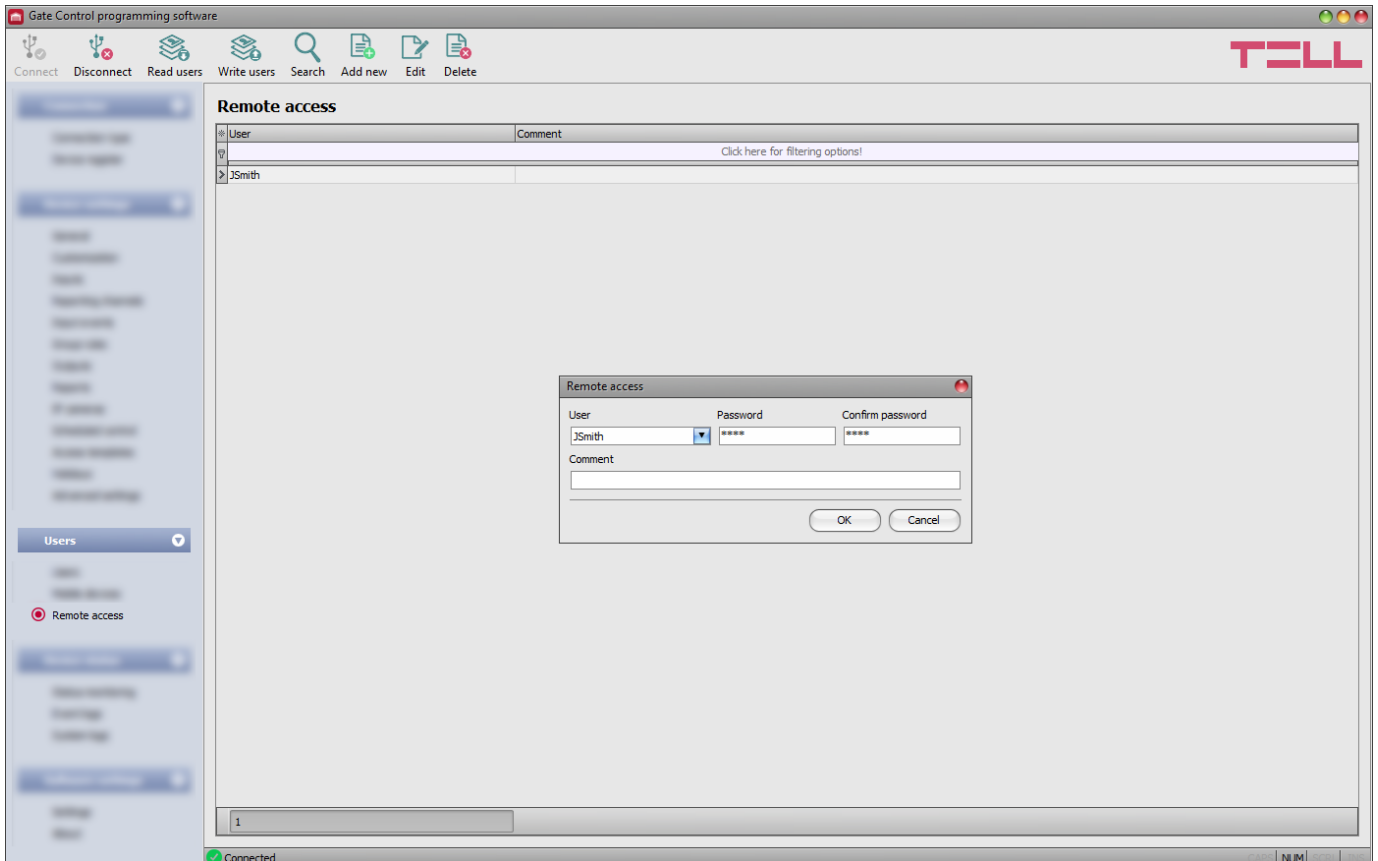
Doorbell (IN1): if this option is enabled, the system will send a “**Doorbell**” Push message to the given mobile device upon triggering input IN1.

Technical error (IN2): if this option is enabled, the system will send a “**Technical or device failure**” Push message to the given mobile device upon triggering input IN2.

Gate position limit error (IN3/IN4): if this option is enabled, the system will send a Push message to the given mobile device if the gate fails to open or close within the configured time intervals. You can change the message text in the “**Customization**” menu, if needed.

Notification on control: if this option is enabled, the device will send notification via Push message to the given mobile device upon each user-initiated output control, including the username of the user in the message.

5.3.3 Remote access



In this menu you can configure passwords for remote access, for super admins and admins. In the possession of the username and password, the super admin or admin will be authorized to connect to the system remotely over the Internet, using the programming software. For the 1000-user product variant you can register altogether up to 2000, while the 20-user product variant allows you to register up to 40 mobile devices and remote access passwords in the system, which are distributed dynamically among registered users.

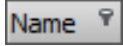

The default settings include a hidden default superadmin user which can be used to connect to the device remotely over the cloud until a new user is registered with **Super admin** or **Admin** role, and with a remote access password. If there is at least one remote access password added, the default superadmin access will be disabled automatically, and will no longer work. The default superadmin provides full access to remote programming.

Security warning! If you delete all remote access password records, the default superadmin user will be reenabled automatically, and can again be used to connect to the device remotely! The purpose of this is preventing you from locking yourself out from remote access.

The default superadmin credentials are:

Username: **superadmin**
Password: **password**

You can filter data in any column using the filter placed under the header of the data table. Filtering can be cancelled by deleting the entered or selected filter condition.

An advanced filter is also available for each column by clicking on the filter icon  which appears on the right-hand edge of each column header by moving the mouse pointer on the given header. You can toggle between ascending and descending data sorting by clicking on a column's header. You can toggle between show/hide columns or change the order of the columns in the spreadsheet by drag-and-drop, after clicking on the button marked with a star  in the top left corner of the spreadsheet. You can also change the order of the columns by moving the header of the columns.

Available options:

- Reading the users from the device:



To read the users stored in the device, click on the “**Read users**” button. This will read all entries in all menus in the “**Users**” menu group. Additionally, if you haven't read the device settings yet separately, it will also read all entries in the “**Device settings**” menu group. If you want to read a specific user or users only, use the “**Search**” option.

- Writing the users into the device:

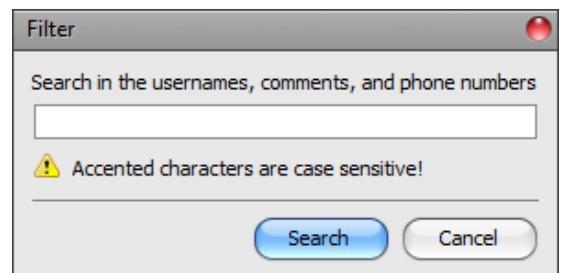


After changing the settings or adding new entries, to take effect in the system, it is necessary to write the users into the device by clicking on the “**Write users**” button. This will write into the device all entries in all menus in the “**Users**” menu group. Additionally, if you have changed the device settings but haven't written them yet separately into the device, it will also write all entries in the “**Device settings**” menu group.

- Search users:



To search users, click on the “**Search**” button, and enter the searched name or phone number. The search engine can search for a piece of text in usernames, comments, and phone numbers. The program will list the results in the table.



- Adding a new remote access:



Click on the “**Add new**” button to add a new remote access.

- Editing the settings of an existing remote access:




To edit the settings of the selected remote access, click on the “**Edit**” button.

- Deleting a remote access:



To delete the selected remote access, click on the “**Delete**” button.

Please note that after you make changes, you must write the users into the device to apply the changes. For this, click on the “**Write users**”  button.

Remote access settings:

User: using the drop-down menu, you can select the super admin or admin user, for whom you want to configure the remote access password.

Password / Confirm password: in this section you can configure and confirm the remote access password. The password configured here, and the given user's username will be required in the "**Connection type**" menu, in the "**Remote access**" section, for connecting remotely to the device.

Comment: in this section you can write a custom comment for the given remote access.

➤ Remote access levels:




With **Super admin** role: full access, can access all settings.

With **Admin** role: can access the following menus only:
Group rules, Scheduled control, Access templates, Remote monitoring events (the "Monitoring" product variant only), **Holidays, Users, Mobile devices, Remote access, Status monitoring, Event logs, System logs.**

With **User** role: has no remote access permission, cannot access anything, therefore it makes no sense to configure remote access for normal users.

You can configure the user roles in the user settings, using the "**Role**" drop-down menu.

➤ Configuring a new remote access:

- If you haven't read the settings and the users from the device yet, click on the "**Read users**"  button in the "**Users**" menu.
- Click on the "**Add new**"  button.
- Select the user from the "**User**" drop-down menu, whom you want to grant remote access.
- Configure the remote access password in the "**Password**" field.
- You can write a comment in the "**Comment**" field, if needed.
- Click on the "**OK**" button.
- Click on the "**Write users**"  button.

5.4 Device status menu group

5.4.1 Status monitoring

The screenshot shows the 'Gate Control programming software' interface. The 'Status monitoring' window is active, displaying the following data:

Property	Status / Value
Device	
Firmware version	V10.01.4.8335
Model	Gate Control PRO 1000 - ETH
SIM identifier (ICCID)	8936304321060554011F
Supply voltage	14,39 V
Device ID	FC:0F:E7:62:D7:32
MAC address	FC:0F:E7:62:D7:32
Modem type	A7682 (2G, 4G)
Counters	
System time	2024. 07. 27. 14:49:05
IP uptime	140 s
Device uptime	173 s
GSM uptime	127 s
Network	
GSM operator	Telekom HU
GSM signal	Good
Data connection type	4G (E-UTRAN)
Modem IP address	10.194.127.161
Cloud connection	Connected
LAN IP address	192.168.0.118
Ethernet connection	Internet connection OK
Inputs / Outputs	
IN1	Idle
IN2	Idle
IN3	Activated
IN4	Activated
OUT1	Idle
OUT2	Idle
Remote monitoring	
IP1	Connected
IP2	Connected

The 'Logs' window on the right displays a list of system events, including:

- (18:09:03)Online mode switched on
- (18:09:07)Power on
- (18:09:22)Check...
- (18:09:25)AT check OK
- (18:09:26)Modem type: A7682
- (18:09:26)Eth0 DHCP start
- (18:09:28)DHCP Ready
- (18:09:28)System netif[0] ready, ip: 192.168.0.118
- (18:09:28)Netif up...
- (18:09:28)Netif up...
- (18:09:29)Connecting...
- (18:09:29)Ufesign send start
- (18:09:29)Ufesign send start
- (18:09:29)Connect...
- (18:09:29)Connected
- (18:09:29)Connect...
- (18:09:30)Connected
- (18:09:30)Connect OK, new sessionId = 51159472
- (18:09:30)Ack OK
- (18:09:30)Connect OK, new sessionId = 4589096
- (18:09:30)Ack OK
- (18:09:33)ECC...
- (14:01:00)Checking SIM card...
- (18:09:33)ECC OK
- (18:09:33)Identification: pid=FC:0F:E7:62:D7:32...
- (18:09:34)SEED recd...
- (18:09:34)Send AUTH info
- (18:09:34)Status:OK
- (18:09:34)Send channel infos
- (18:09:34)OK
- (18:09:34)Send group info
- (18:09:34)Ready.
- (18:09:34)Date/time received: 2024.07.27 12:01:00
- (14:01:00)TEST period time elapsed
- (14:01:00)SIM init OK
- (14:01:00)ZoneOffset = 7200 sec
- (14:01:00)System time updated(0 -> 4).
- (14:01:00)Time set...
- (14:01:01)Lang received: HU,EN,DE
- (14:01:01)MUX check OK
- (14:01:01)Connection OK

In this menu you can read information about the actual system status. Status information is read from the device and refreshed automatically only when connected through USB. When connected remotely, you can read and refresh the status information by clicking on the “**Read**” button. The availability of certain status information listed below depends on the connected device model.

The system logs are shown in the window on the right hand side, which provides information about the internal processes of the device and communication. The system logs help troubleshooting if malfunction occurs. The program saves the system logs to file automatically in the “**Logs**” folder, which you can access easily by clicking on the path link shown in the “**About**” menu in the “**Data folder**” section (the file name looks as follows: “*the actual date_module.log*”). **The system logs are only available when connected via USB!**

Available status information:

Device:

- **Firmware version:** the firmware version of the device.
- **Model:** the device model.
- **SIM identifier (ICCID):** the identifier (ICCID) of the SIM card installed in the device. You can copy the identifier to clipboard by clicking the notepad icon on the right-hand side.
- **Supply voltage:** value of the supply voltage measured. The value is considered to be no more than indicative, and cannot be compared with a value shown by a precise measuring instrument.
- **Device ID:** the identifier used by the device to identify itself on the cloud. The mobile app and the programming software can connect to the device using the identifier shown here. The device ID is basically the same as the MAC address. You can copy the identifier to clipboard by clicking the notepad icon on the right-hand side.
- **MAC address:** the unique identifier of the device (6x2 hexadecimal characters). This identifier is burned-in during production, and therefore it cannot be changed.
- **Modem type:** the type of the modem built in the device.

Counters:

- **System time:** the system date and time.
- **IP uptime:** elapsed time since the device has last connected to the Internet.
- **Device uptime:** elapsed time since the device has been powered up.
- **GSM uptime:** elapsed time since the device has last connected to the mobile network.

Network:

- **GSM operator:** the name of the currently used mobile operator.
- **GSM signal:** actual GSM signal level (None/Very low, Weak, Medium, Good, Excellent).
- **Data connection type:** the type of data connection currently being used: 4G (E-UTRAN), 2G (GPRS/EGDE).
- **Modem IP address:** the actual IP address of the modem.
- **Cloud connection:** the cloud server connection status.
- **LAN IP address:** the actual local IP address of the device (only the product variant with an Ethernet port).
- **Ethernet connection:** the Ethernet connection status (only the product variant with an Ethernet port).

Inputs / Outputs:

- **IN1...IN4:** the actual state of the contact inputs.
- **OUT1/OUT2:** the actual state of the outputs.

Remote monitoring (the *Monitoring* product variant only):

- **IP1:** the primary remote monitoring server/receiver connection status.
- **IP2:** the backup remote monitoring server/receiver connection status.

Available options:

- **Read:**

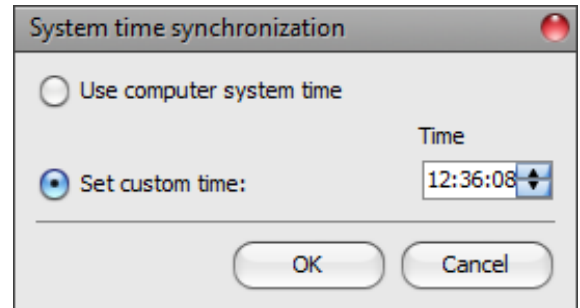


This button is available only when connected remotely to the device. By clicking on this button, the program will read the status information from the device. This is not needed when connected via USB, since in that case the data are read and refreshed automatically.

- **Time synchronization:**



This button is used to synchronize the device system time with the PC system time, or set a custom time, up to your choice. The system time needs to be synchronized only if cloud usage is disabled. Otherwise, the time will be synchronized automatically from the cloud server. Before synchronizing the time with the PC system time, please check if the PC system time is correct.



- **Toggle output 1:**



You can control output OUT1 by clicking on this button. The output will change state upon each click.

- **Toggle output 2:**



You can control output OUT2 by clicking on this button. The output will change state upon each click.

Attention! The output control buttons are designed to give you an option to override operation when necessary and justified, i.e., to control the outputs differently from the normal control process. When using these control buttons, the system will control the outputs according to your request, ignoring the state of gate position limit switches and other controls in progress, regardless of the actual control status. Please note that the use of these buttons may prevent proper operation!

- **Enable and disable AT command logging:**



The “**AT log**” button is used to enable and disable logging of AT commands. This serves for troubleshooting, for viewing detailed information on the operation of the modem.

- **Modem FOTA update:**



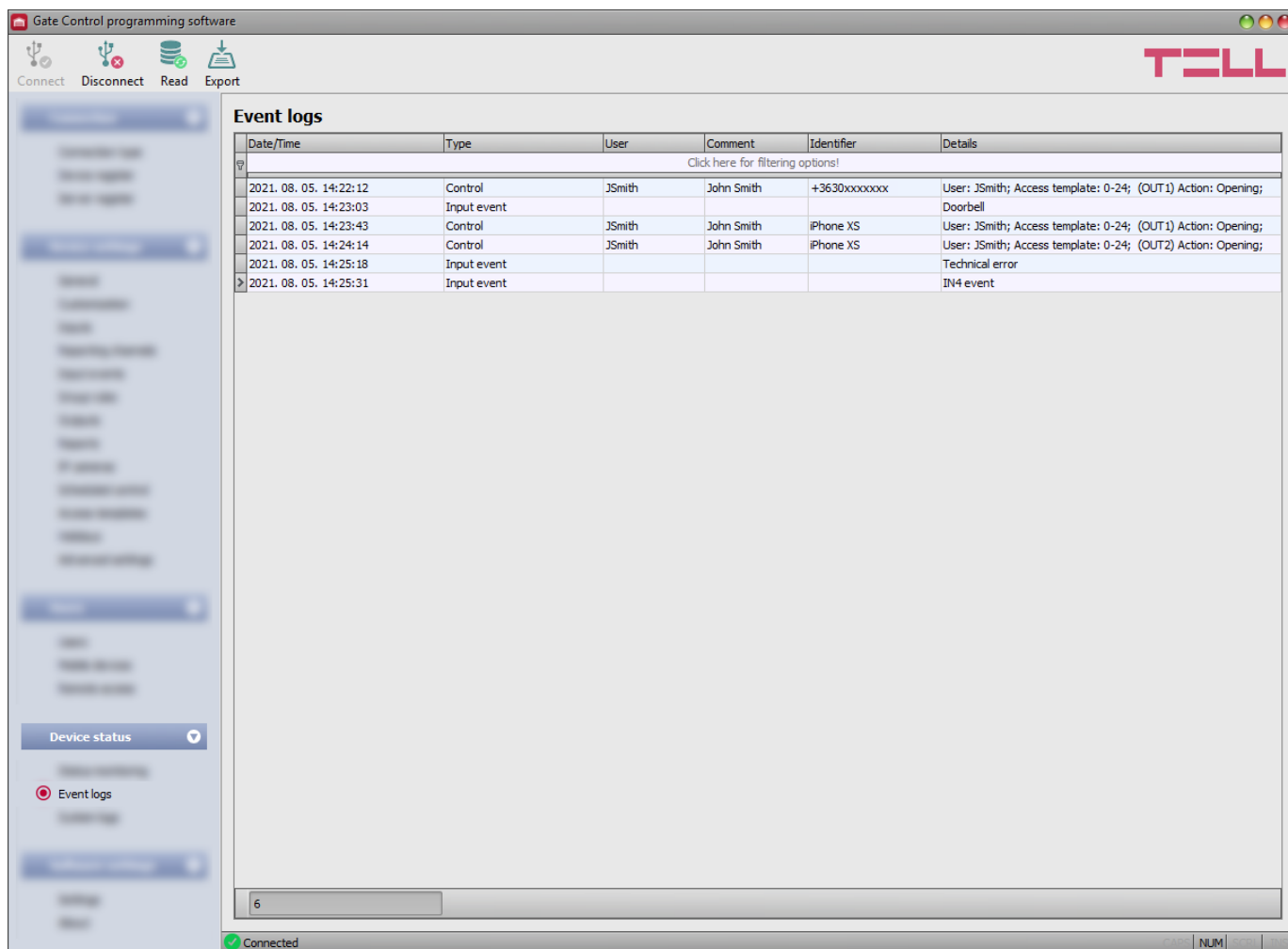
Using this button, you can update the firmware of the modem installed in the device. The manufacturer of the modem also continuously improves their products, therefore, new firmware updates may occasionally be released for the modem, which along with bug fixes, may include improvements following the evolution of mobile networks. Therefore, it is recommended that you always upgrade the modem as well to the latest firmware version available, especially if you experience a malfunction related to mobile network functioning (e.g., VoLTE calls are not working despite the service is enabled on the SIM card). The update is done over the mobile Internet, therefore, it requires a SIM card with data service, and the device must run with the latest firmware version. After clicking on the button, a new window pops up which shows the current firmware version of the modem. You can start the update after inserting the firmware URL (link) which you can request from TELL technical support.

Current version	Modem firmware URL
B12	

Start Cancel

The device will restart after starting the update, and then it will download the necessary file and will update the modem. The process may take up to 15-20 minutes. Wait until the device reconnects to the network and the **STATUS** LED starts blinking in green. Do not turn off the power feed before that because doing so may damage the modem. After that, by clicking again on the button you can check in the “**Current version**” field if updating was successful.

5.4.2 Event logs



In this menu you can view and export the event logs to file, which includes control and input events recorded by the system. The system stores the latest 1000 events in the event log memory.

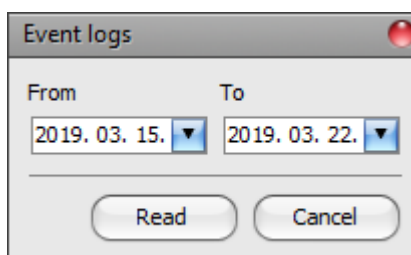
The values configured in the “**Comment**” field in the user settings are not stored in the event logs. The data in the “**Comment**” column is filled in by the software from the user list. Therefore, data will only be shown in this column if you read the users from the device before reading the event logs.

Available options:

- **Read:**



After clicking on this button, the program opens a dialog window, where you can specify the period, for which you want to read the event logs from the device. Select the start and end date using the drop-down menus, and then click on the “**Read**” button.



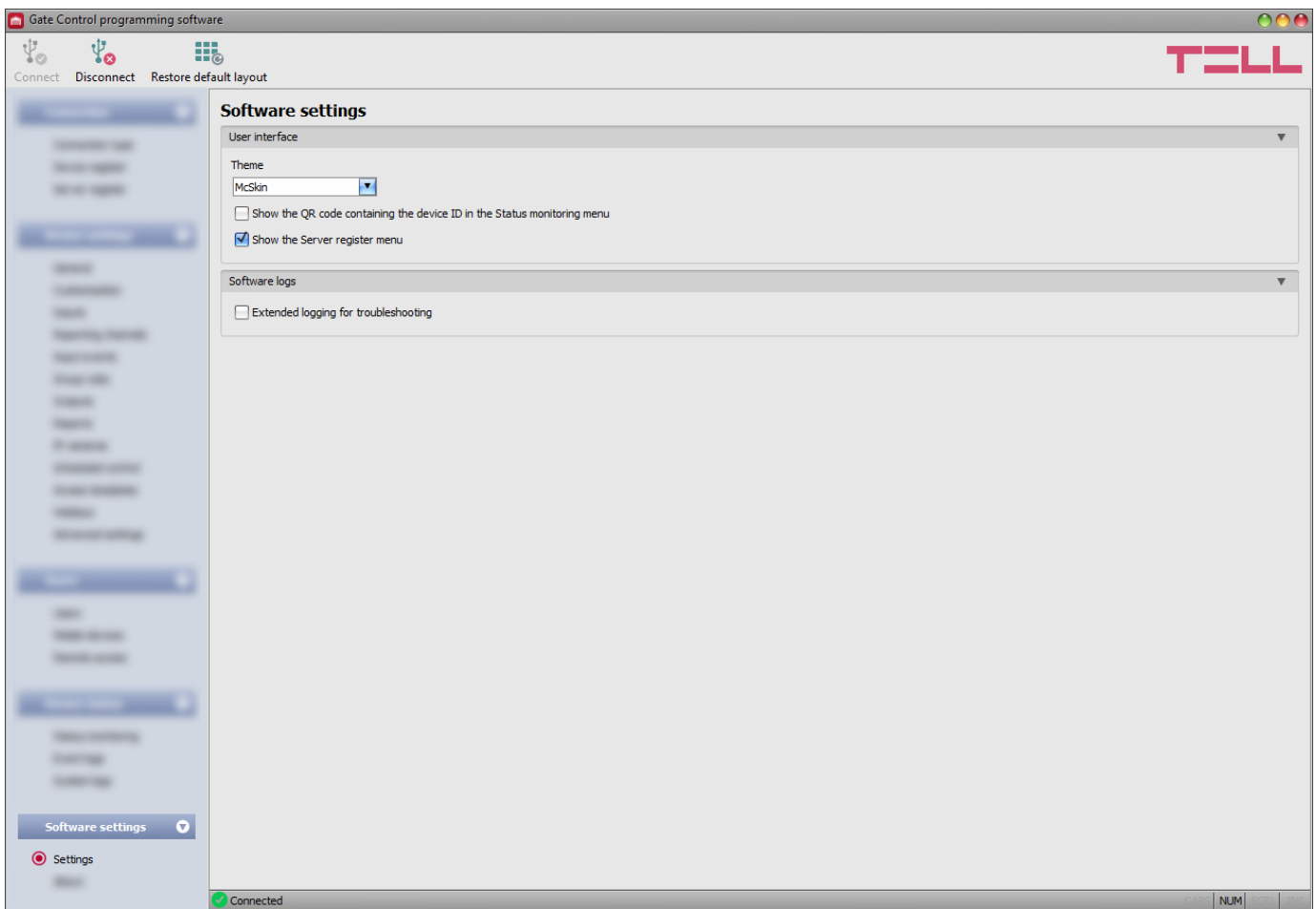
- **Export:**



You can use this button to save the event logs shown in the window to file in CSV format.

5.5 Software settings menu group

5.5.1 Settings



In this menu you can change the user interface appearance and can also enable the “**Server register**” menu, and extended logging for troubleshooting.

Available options:

- **Restore default layout:**



To restore the user interface default layout, click on the “**Restore default layout**” button, and then close and open the program again.

User interface:

Theme: the user interface appearance can be changed using this dropdown-menu. You can choose from various appearance themes.

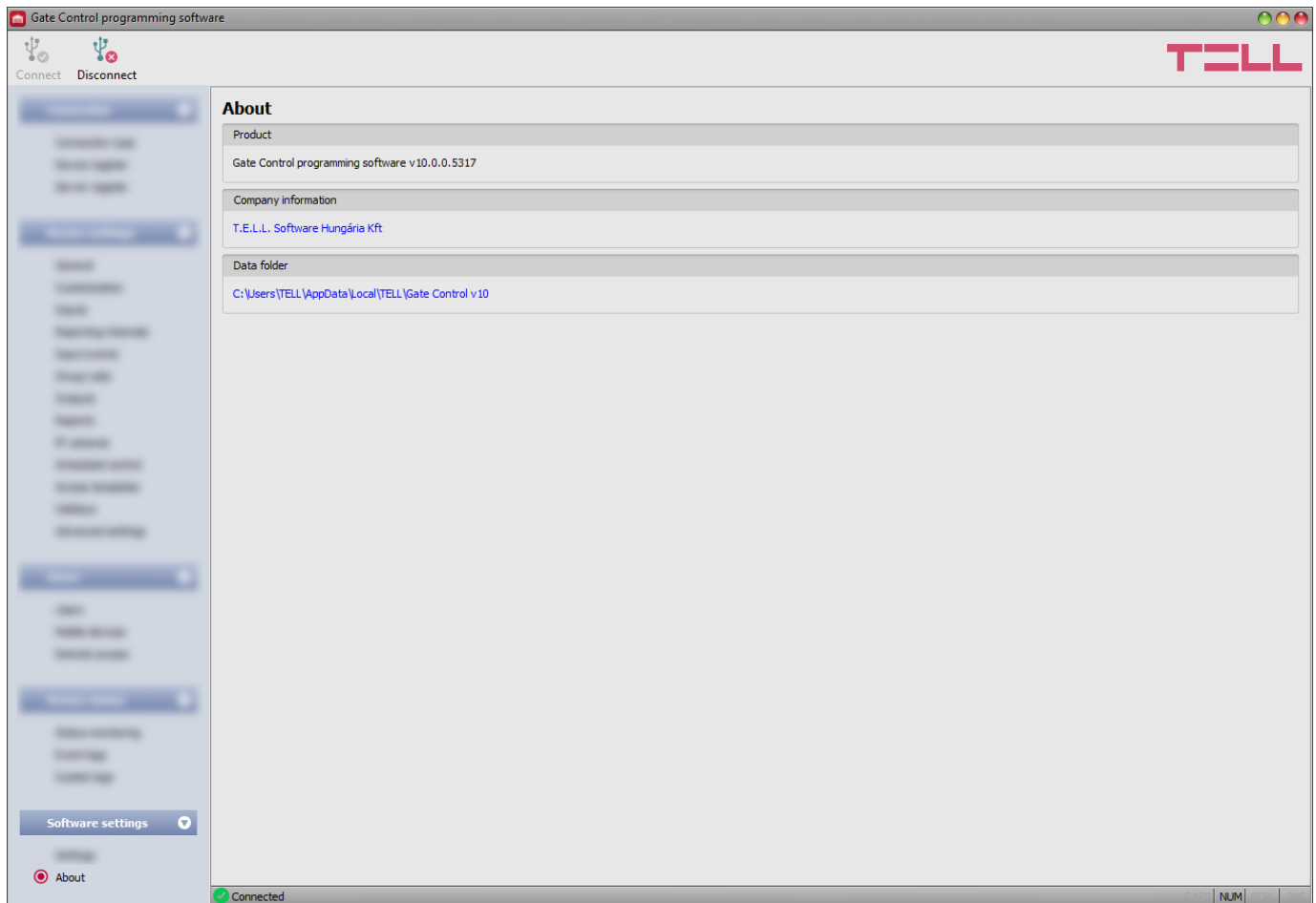
Show the QR code containing the device ID in the Status monitoring menu: if this option is enabled, the QR code that contains the device ID will be shown in the “**Status monitoring**” menu. This is used by the manufacturer to record devices produced.

Show the Server register menu: if this option is enabled, the “**Server register**” menu will be available in the “**Connection**” menu group. The “**Server register**” menu is hidden by default, since it in most cases using it is not necessary. It is needed only if you are using a proxy for Internet traffic management.

Software logs:

Extended logging for troubleshooting: you can enable this option if you encounter issues with the software. If you enable this option, the program will record detailed logs while the system operates. The program saves the software logs to file automatically in the “**Logs**” folder, which you can access easily by clicking on the link found in the “**About**” menu, in the “**Data folder**” section (the file name looks as follows: “*the actual date_remoter.log*”). The detailed logs help the manufacturer in troubleshooting.

5.5.2 About



In this menu you can view the contact details of the manufacturer, the version of the programming software, and the path of the data folder where the software stores system logs. By clicking on the path, the program will open the data folder in the file manager.

6 Replacing the SIM card

If it is necessary to replace the SIM card for any reason, please follow the instructions below:

- ***Disable voicemail and notification in SMS about missed calls on the new SIM card.***
- ***If you enable PIN code request on the SIM card, configure the SIM card's PIN code in the programming software in the "General" device settings menu. Otherwise disable PIN code request on the SIM card.***
- ***Enable caller identification and caller ID transmission service on the SIM card at the mobile service provider*** (these services might not be enabled by default, please check). To enable these services, install the SIM card into a mobile phone and call the customer service of the card's mobile service provider, and enable the services in the menu, or visit one of the service provider's personal customer services and ask to enable these services on the SIM card.
- Power down the device, replace the SIM card, and then power up the device.
- If the phone number of the device has also changed by replacing the SIM card, update the phone number in the "**General**" device settings.

7 Updating the firmware

TELL always releases its products with the latest firmware version. However, as our products are being continuously improved, new firmware updates may occasionally be released for the products, which may include new features along with bug fixes. Therefore, it is recommended that you always upgrade your product to the latest firmware version available. All released firmware versions are available on the TELL website, including older versions.

ATTENTION! Downgrading to an earlier version is not supported! Always upgrade your product to the latest version. Otherwise, your settings could get wiped due to differences in functionality between versions, or the product may become unusable due to unsupported components. (A newer hardware may contain new components, e.g., a new flash memory, modem, etc., which are not supported by an earlier firmware.)

You can update the firmware on the **Gate Control PRO** device locally via USB or remotely via the Internet. You can find the firmware file or the desktop update application needed for the update on the manufacturer's website (<https://tell.hu/en/products/gsm-automation/gate-control-pro>) in the product downloads section.

7.1 Updating via USB


You can update the firmware through USB using the desktop update application, or the programming software.

- **Updating via USB using the desktop update application**

- Download the latest desktop update application (that has the **.exe** extension) from the manufacturer's website. The update application includes the firmware as well, therefore the file name is the same as the firmware version number.
- The device must be powered down.
- Open the update application and click on the **"FIRMWARE"** button.
- Press and hold the **PB** button while connecting the device to the computer via USB, and then release the button.
- Power up the device and then click on the **"Start"** button. Do not power down the device later on!
- Wait until the progress bar shows that the process has completed.
- Use the **"Cancel"** button to close the pop-up window that shows up while loading the firmware, with a question asking if you want to format the drive.
- You can close the update application when the progress bar shows that the process has completed.
- Wait until the **STATUS** LED on the device starts blinking slowly. You can then connect to the programming software and check the functioning.



- **Updating via USB using the programming software**

- Download the latest firmware file (that has the **.tf3** extension) from the manufacturer's website.
- Click on the **"Connection type"** menu in the programming software.
- Click on the **"Firmware update"**  button, and then browse the **.tf3** firmware file.
- The update process will start automatically as soon as you click on the **"Open"** button. Once the firmware is loaded, the progress window will close automatically, and the device will restart a few seconds later running on the new firmware.

7.2 Updating remotely over the Internet

It is also possible to remotely update the firmware of the **Gate Control PRO** device over the Internet, using the programming software. After establishing the remote connection, the steps for remote update are the same as the steps for updating through USB, as specified above.

8 Restoring the factory default settings

The factory reset process will delete all settings, users, and the event logs in the device, and will restore the factory default values, including the USB password! Create a system backup if needed, before performing the factory reset.

The factory default settings cannot be restored if the device has been locked in the “**Advanced settings**” menu. If you have forgotten the USB password of the device and the device is locked, only the manufacturer can restore the factory default settings in the service center.

You can perform a factory reset using the programming software, or the **PB** button found on the device.

8.1 Restoring the factory default settings using the programming software

To restore the factory default settings, click on the “**Restore factory default settings**” button in the “**Connection type**” menu. The reset process may take more than 1 minute, and it will restart the device. Wait until the device restarts and the **STATUS** LED on the device shows activity again. The settings cannot be restored if the device lock option has been enabled in the settings.

If you have forgotten the USB connection password, restoring the factory default settings can only be done using the **PB** button found on the device.

8.2 Restoring the factory default settings using the PB button

- Power up the device.
- Long press the **PB** button for at least 8 seconds, and then release. The **PB** button is placed on the casing under the status LEDs.
- After releasing the button, the **STATUS** LED will show permanent red light first, and then flashing red light, until the device creates the clean configuration. This process may take up to 3 minutes.
- The reset process has completed when the device has connected to the network and the **STATUS** LED shows a flashing green light.



9 Package content

- **Gate Control PRO** + terminal connector
- GSM antenna
- Quick start guide
- Warranty card