

Gate Control BASE 1000 – DIN rail

INSTALLATION AND APPLICATION MANUAL

for device version v10.01

Document version: 1.0 25.04.2025



Product models:

- Gate Control BASE 1000 DIN rail - 4G.IN4.R2

Table of contents

1	General operation of the <i>Gate Control BASE</i>	5
1.1	Setting the system time	6
1.2	Data traffic	6
1.3	Operation of the contact inputs	6
2	Processing of personal data	6
2.1	Responsibility of the Manufacturer	7
3	Connecting the terminals and putting into operation	7
3.1	Under Voltage Lock Out (UVLO) function	7
3.2	Input wiring	7
3.3	Output wiring	7
3.4	Connections	8
3.4.1	Wiring diagrams according to output control modes	8
3.5	Preparing and installing the SIM card	12
3.6	Connecting the antenna	12
3.7	Installation	12
3.8	Putting into operation	13
3.9	STATUS and GSM LED signals	13
3.10	Technical specification	14
4	Configuring the <i>Gate Control BASE</i> device	15
4.1	The user interface and configuration options of the software:	15
4.2	Methods of connecting to the device	16
4.2.1	Connecting to the device via USB	16
4.2.2	Connecting to the device over the Internet	17
5	<i>Gate Control</i> programming software usage and feature descriptions	21
5.1	Connection menu group	21
5.1.1	Viewing the settings options and configuring offline	21
5.1.2	Connection type	22
5.1.3	Device register	24
5.1.4	Server register	26
5.2	Device settings menu group	28
5.2.1	General	29
5.2.2	Inputs	32
5.2.3	Reporting channels	33
5.2.4	Input events	34
5.2.5	Outputs	36
5.2.6	Advanced settings	40
5.3	Users menu group	43
5.3.1	Users	44
5.3.2	Remote access	49
5.4	Device status menu group	52
5.4.1	Status monitoring	52
5.4.2	Event logs	56
5.5	Software settings menu group	57
5.5.1	Settings	57
5.5.2	About	58

6	Configuring the <i>Gate Control BASE</i> by SMS, using a mobile phone	58
6.1	Detailed specification of SMS commands	60
7	Updating the firmware	65
7.1	Updating via USB	65
7.2	Updating remotely over the Internet	66
8	Restoring the factory default settings	66
8.1	Restoring the factory default settings using the programming software	66
8.2	Restoring the factory default settings using the PB button	67
9	Package content	67

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-base>

► **Product models:**

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

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

► **Product features:**

- 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, 2 NO/NC/COM relay outputs
- Up to 1000 users
- Reports the status of the 4 contact inputs by SMS or by call
- Stores the latest 1200 events in the event log memory
- Programmable via USB, the Internet, and SMS

► **Application area:**

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

1 General operation of the *Gate Control BASE*

The ***Gate Control BASE*** 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 number of the SIM card installed into the device. 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. When controlling the system by call, it 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.

Controlling (opening/closing) is possible only from authorized phone numbers registered in the device, or from any phone number, according to the configuration: **if there are users registered with phone numbers in the user list, only calls from these phone numbers can control the device. If there are no users registered, calls from any phone number will control the device (in this case the device can only be configured through USB). If you use output control mode No. 1, calls from a private (hidden) number will control output OUT2 in any case.**

The system supports up to 1000 users, for which different options and permissions can be configured, such as role, 0-24 entry period, and access to outputs (gates), depending on the output control mode chosen.

Users who are granted the “***0-24 entry period***” permission can control the system anytime, while users who are not granted this permission can control the system over the day only within the time interval configured in the “***Permitted entry period***” section in the “***General***” device settings menu, i.e., control requests received from these users will be executed by the device within the configured time period, and will be rejected outside the given period. If there are no users registered in the device, the system can be controlled by anyone from any phone number only within the configured permitted entry period.

The services to be activated on the SIM card installed into the ***Gate Control BASE*** device should be chosen according to which services of the device you want to use. For accessing the device remotely (remote programming) over the Internet, 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.

1.1 Setting the system time

For proper operation of functions that require the exact time (event logs, permitted entry period), setting the system time is necessary. The module sets the system date and time automatically on each power up and by 24 hours on each scheduled daily restart, by reading the local time from the mobile network. Thereby, when switching between summer and winter time, the device will adjust the date and time automatically within 24 hours or upon restore from a power loss. However, it may happen that the given mobile operator does not provide the date and time, or this function does not work properly. In this case it is necessary to set the system time manually, which you can do in the programming software or via SMS. The device will also synchronize the system time automatically from the cloud when it connects to the server.

For setting the system time using the programming software, click on the “**Time synchronization**”  button in the “**Status monitoring**” menu (further details in chapter “[Status monitoring](#)”).

1.2 Data traffic

In case of using remote access over the Internet, use a SIM card with at least 20MB/month data plan in the **Gate Control BASE** device. 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 remote programming, remote download of event logs, remote firmware update, 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 minimal data usage (<20MB).

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, according to the settings. This function can be used for e.g., sending notification by SMS about the state of tamper or other switches, control board error or other outputs. You can configure the recipient phone numbers 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.

2 Processing of personal data

The users can control the system with the help of their phone numbers associated with usernames, therefore, to operate the system, it is necessary that the users who want to use the system, provide their 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’ 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.

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!

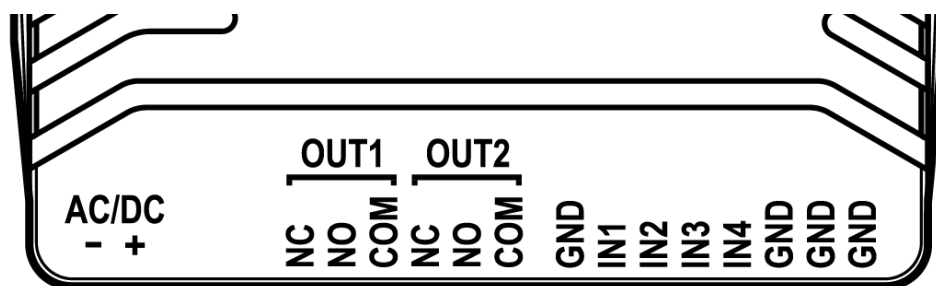
A power supply with adequate power is essential for the product to operate properly. The power supply must provide a power that can serve the minimum operating voltage and the maximum power consumption of the device. The power feed must be continuous and transient-free.

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

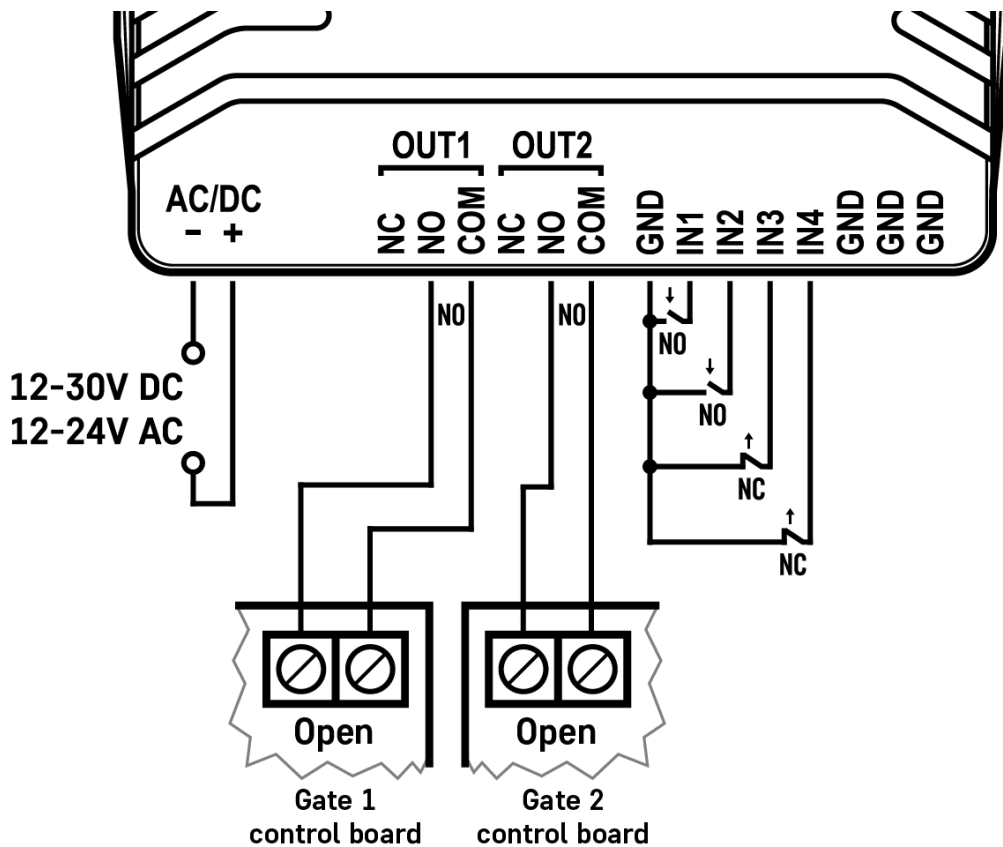
System terminal inputs and outputs:



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.
- A control call only opens the gate. Closing must be done automatically by the gate automation control board.



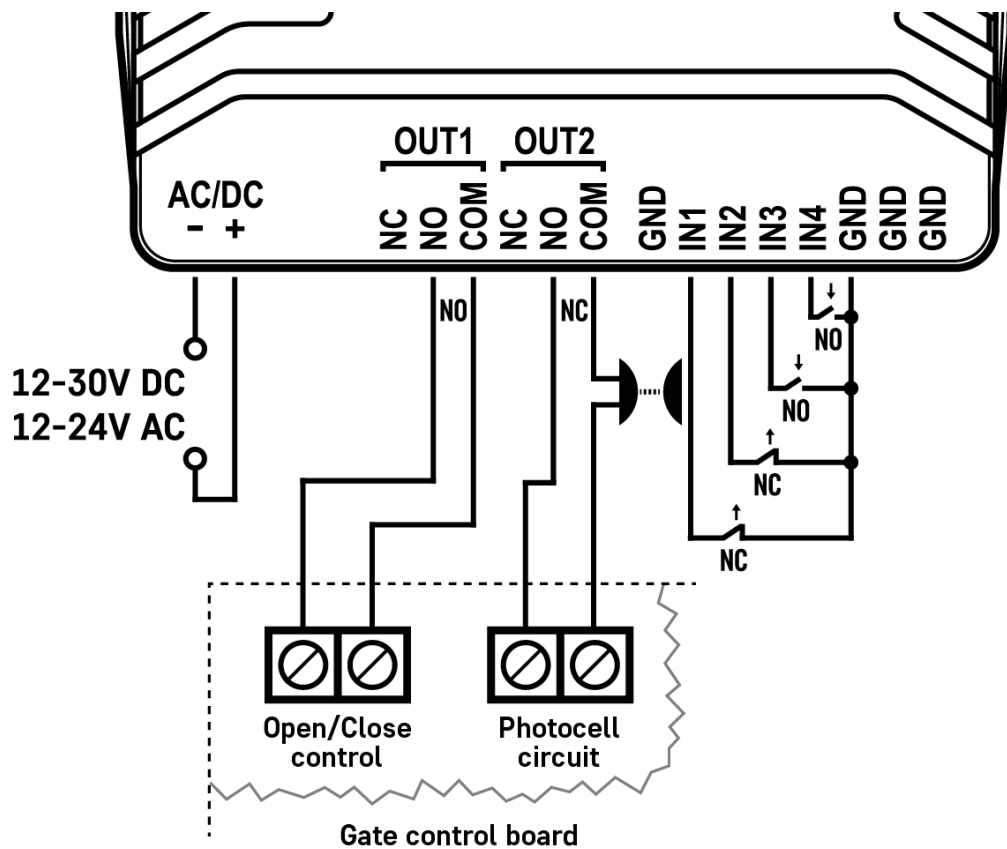
Control modes 1 and 2: Wiring for one or two gates

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).
- Output control permission can be configured separately for each user and each output.
- A control call only opens the gate. Closing must be done automatically by the gate automation control board.

Control mode 3:

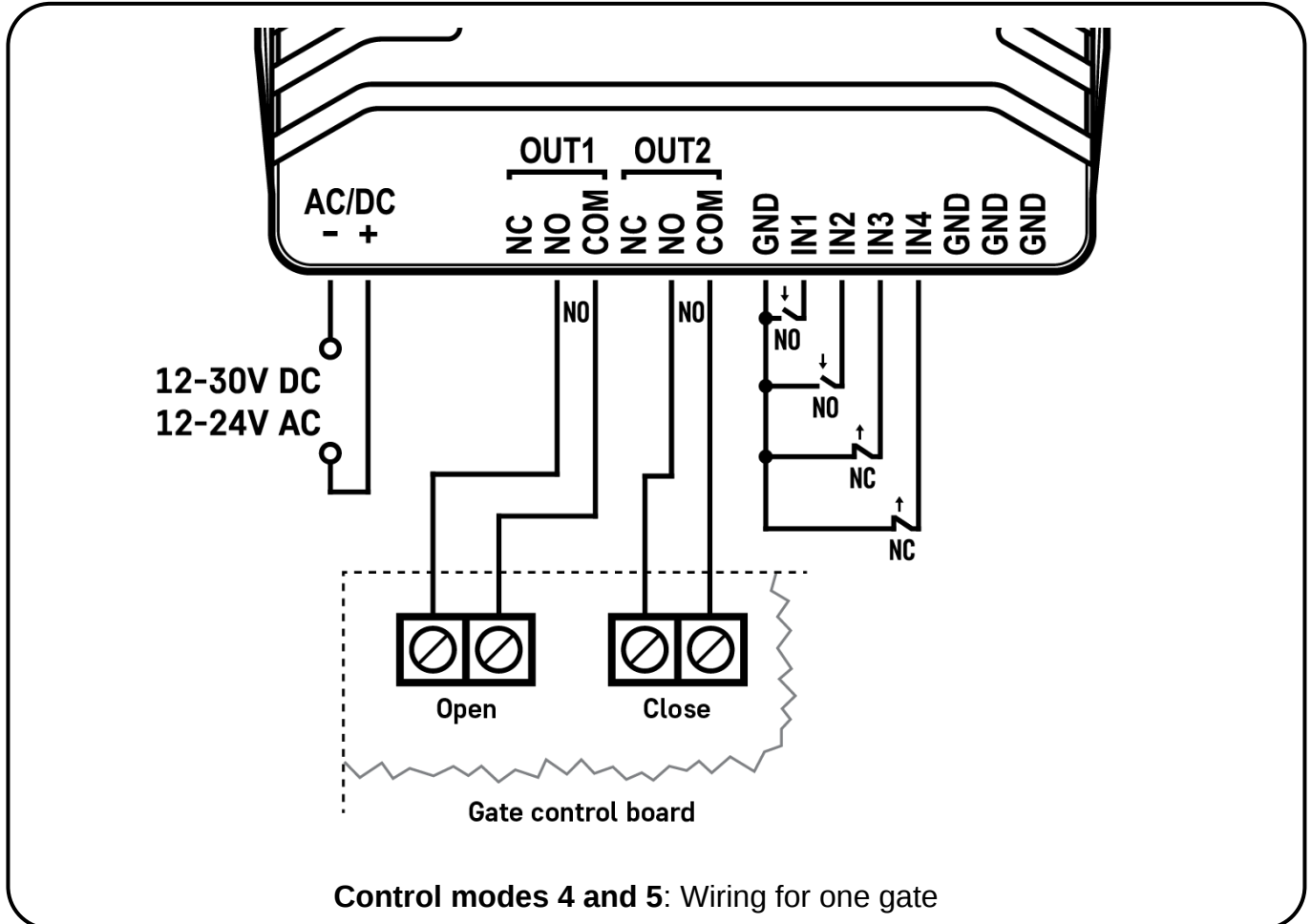
- For single-gate automations that require triggers for opening and closing on the same input.
- Opening and then closing by a single call.
- Output OUT1 is in an idle state, while OUT2 is activated by default.
- Output OUT1 is used to control the gate, while OUT2 is used to interrupt the photocell sensor 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 mode 3: Wiring for one gate with photocell control

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.
- Both outputs are in an idle state by default and are activated when controlled.
- The opening trigger signal is provided by output OUT1, and the closing trigger signal is provided by output OUT2.
- Holding the gate locked in an open state permanently on a second call.

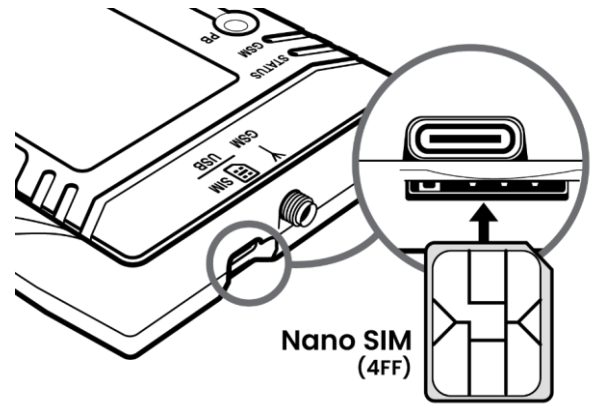


Control mode 5:

- For single-gate automations that require triggers for opening and closing on different inputs.
- Opening and then closing by separate calls.
- Both outputs are in an idle state by default and are activated when controlled.
- The opening trigger signal is provided by output OUT1, and the closing trigger signal is provided by output OUT2.

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 BASE** device should be chosen according to which services of the device you want to use. For accessing the device remotely (remote programming) over the Internet, mobile Internet service is necessary. 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 programming software in the "General" device settings menu. Otherwise disable PIN code request on the SIM card.**
- **Enable caller identification service on the SIM card at the mobile service provider** (this service might not be enabled by default, please check). To enable this service, install the SIM card into a mobile phone and call the customer service of the card's mobile service provider and enable the service in the menu, or visit one of the service provider's personal customer services and ask them to enable this service 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 BASE** device. The nominal current consumption of the **Gate Control BASE** 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. If the system time is wrong, try the following options:
 - Set the APN manually in the “**General**” settings menu, and then restart the device.
 - You can also synchronize the date and time manually in the “**Status monitoring**” menu, or by sending the #DT message to the phone number of the SIM card installed in the device, but with these options 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

STATUS LED	Slowly flashing green	Normal operation, connected to the mobile network
	Flashing red	The mobile service is unavailable, or system startup/restart is in progress, or SIM card error, or applying an uploaded firmware is in progress.
	Permanent red	Registering on the mobile network, or PIN code request, or firmware upload via USB is in progress.
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 AC/DC
Dimensions:	88.4 x 119 x 23.1mm
Weight:	135g (packed: 291g)

RF emission power:

Frequency	Power	Minimum power
EGSM900 (GMSK)	33dBm $\pm$ 2dB	5dBm $\pm$ 5dB
DCS1800 (GMSK)	30dBm $\pm$ 2dB	0dBm $\pm$ 5dB
EGSM900 (8-PSK)	27dBm $\pm$ 3dB	5dBm $\pm$ 5dB
DCS1800 (8-PSK)	26dBm +3/-4dB	0dBm $\pm$ 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 BASE* device

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

- by computer via USB, using the programming software
- by computer over the Internet, using the programming software
- by SMS, using a mobile phone

Remote programming over the Internet is only available when a SIM card with mobile Internet access is installed in the **Gate Control BASE** device and the device has successfully 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 "[SIM settings](#)" paragraph 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.

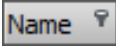
You can download the latest version of the programming software from the manufacturer's website: <https://tell.hu/en/products/gsm-automation/gate-control-base>

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:

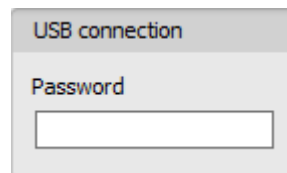
USB: direct connection using a USB A to USB-C cable.

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 BASE** device you want to connect to uses the cloud service. For this, 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 of the super admin or admin user are required. Therefore, if there is no user configured in the system yet, first it is necessary to add a super admin or admin user and configure the remote access for that user via USB connection. If there are already users registered, you need to configure the remote access for the super admin or admin user for whom you want to grant remote access. Thereby, practically you can grant remote access for any user according to its role. 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:

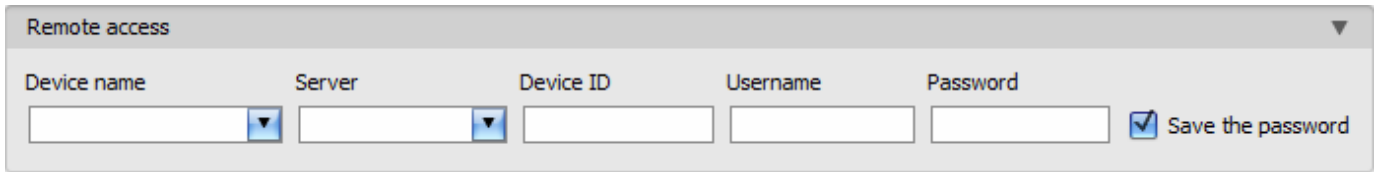
With Super admin role:	Full access, can access all settings.
With Admin role:	Has permission to manage users only, therefore, has no access to menus included in the “ Device settings ” menu group.
With User role:	Has no remote access permission, cannot access anything, therefore it makes no sense to 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

To connect 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 online. 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 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.

Device ID: the identifier of the **Gate Control BASE** 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.

- The **Gate Control BASE** device does not keep continuous connection with the cloud, it only connects to the server upon request. Therefore, before trying to connect remotely to the device, the request for connecting to the cloud should be sent by 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#**) by SMS to the phone number of the SIM card installed in the **Gate Control BASE** 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 will stay 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 missing Internet service.

If the APN is not configured, or the configured value is wrong, the Super administrator user can configure this 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.

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, an outgoing call will block the Internet connection, i.e., a possible remote connection in progress will be suspended for the duration of the call.

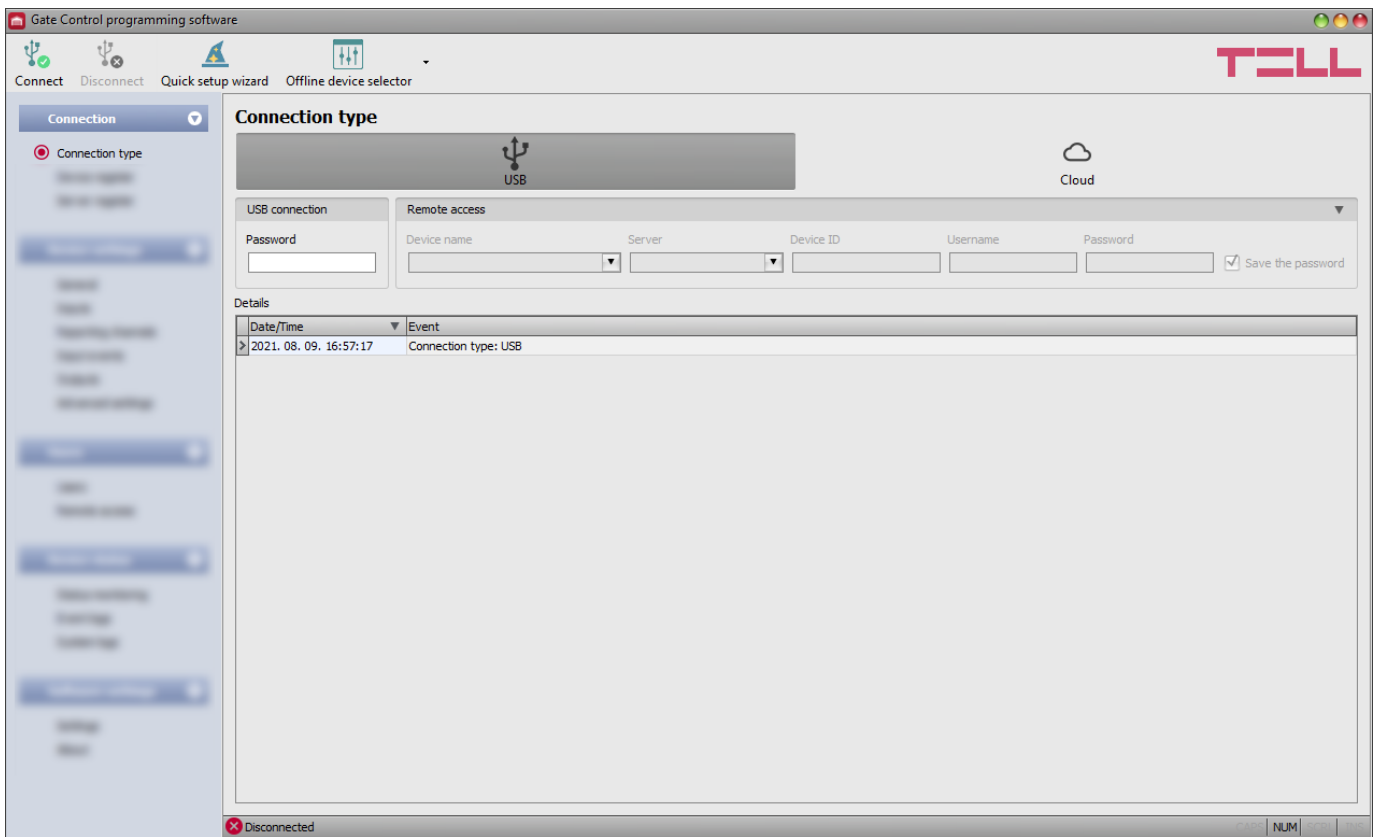
Functions that make outgoing calls:

- **notification by call upon activating a contact input**

5 Gate Control programming software usage and feature descriptions

5.1 Connection menu group

5.1.1 Viewing the settings options and configuring offline



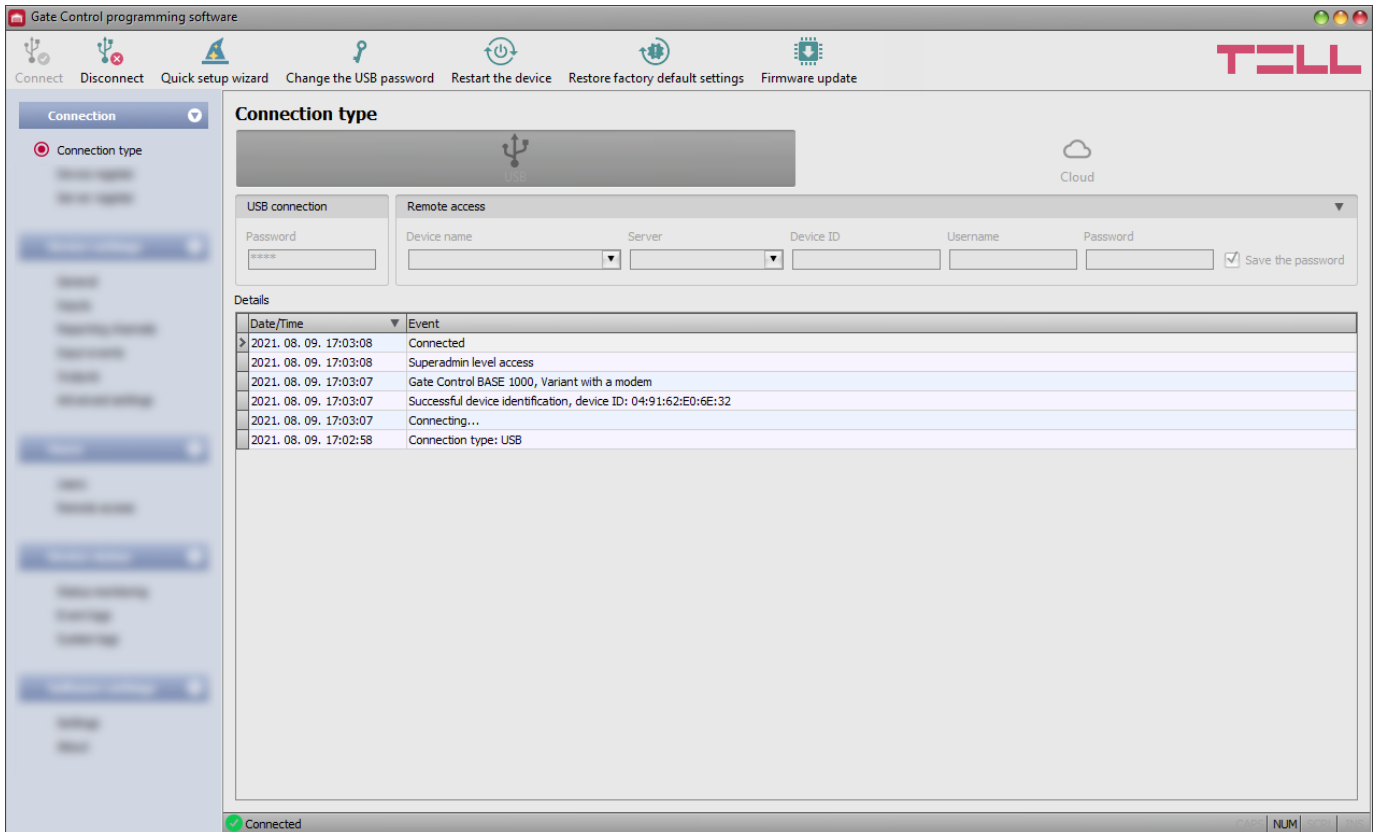
The **Gate Control** programming software supports all **Gate Control BASE** and **PRO** device models, therefore the software shows the settings options available specifically in a given device model, which are different from the common parameters (e.g., differences between the **BASE** and the **PRO**,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

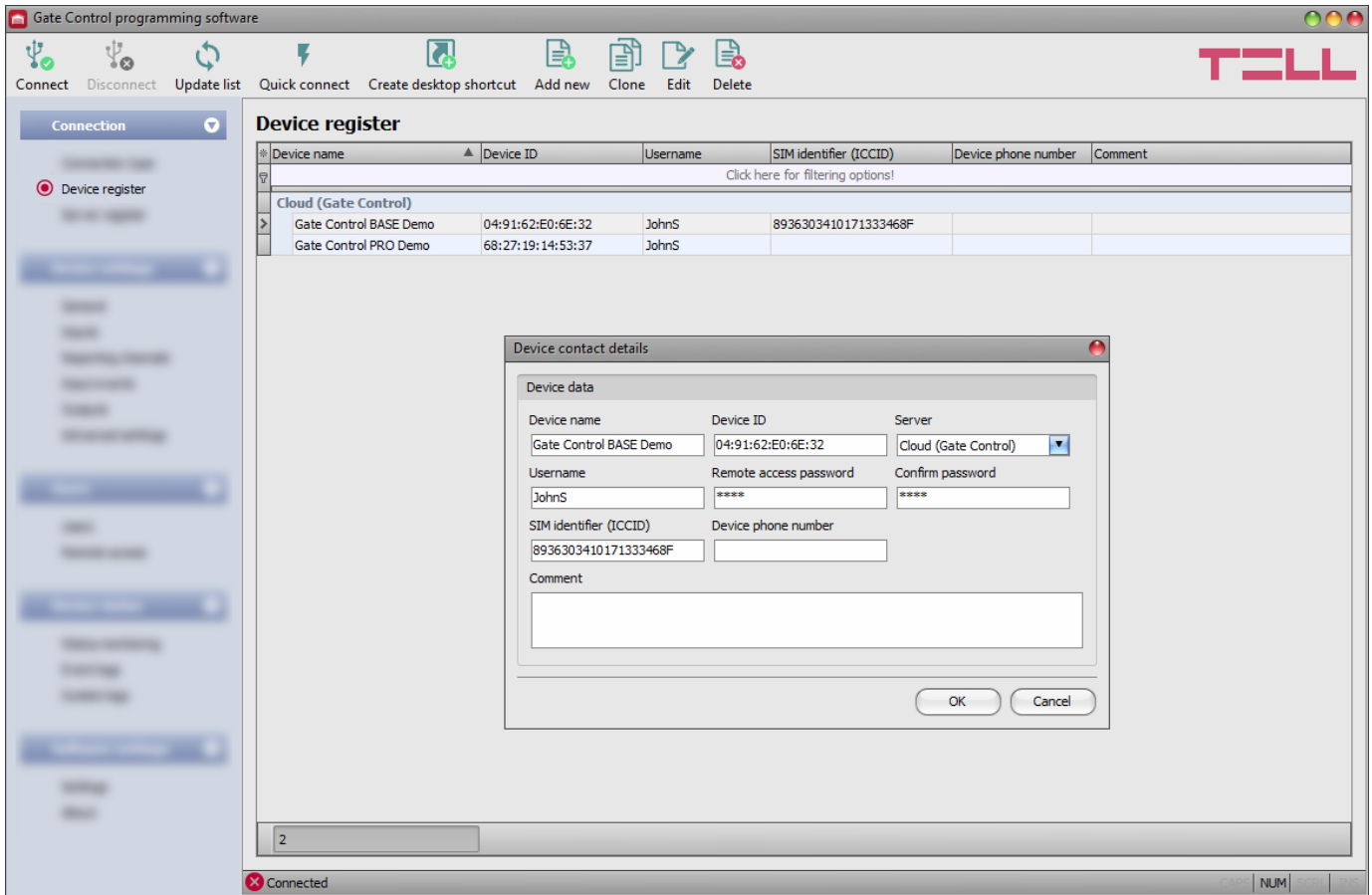
The factory default settings cannot be restored if the device has been locked in the settings. If you have forgotten the USB password of the device and the device is locked, only the manufacturer can restore the factory default settings in the service center.

- **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 BASE** and **PRO** 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	JohnS
Gate Control PRO Demo	68:27:19:14:53:37	JohnS

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.

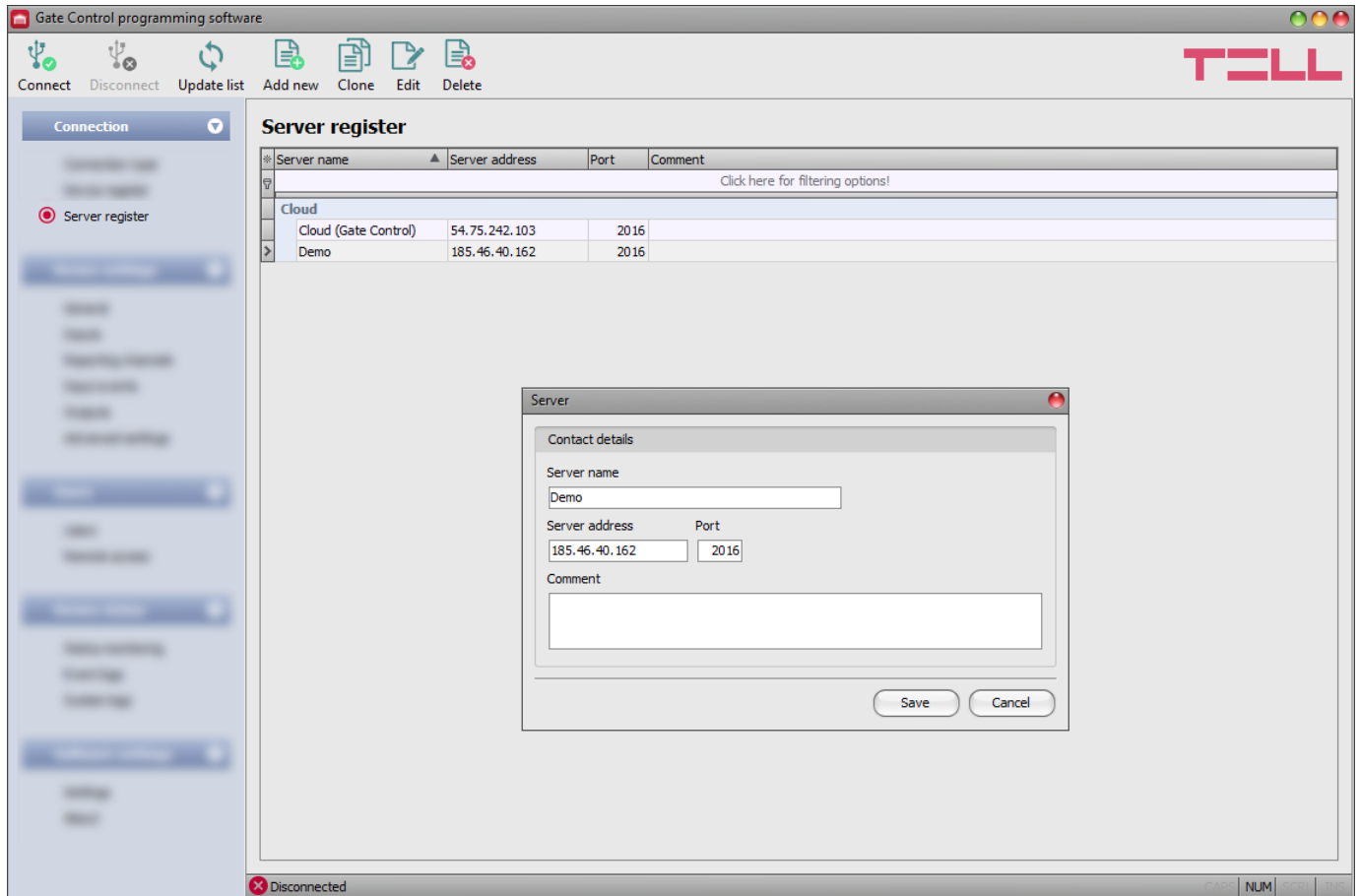
Remote access password / Confirm password: the password configured for the given user in the “**Remote access**” menu in the settings of the given device, used to connect remotely to the device.

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 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, 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.

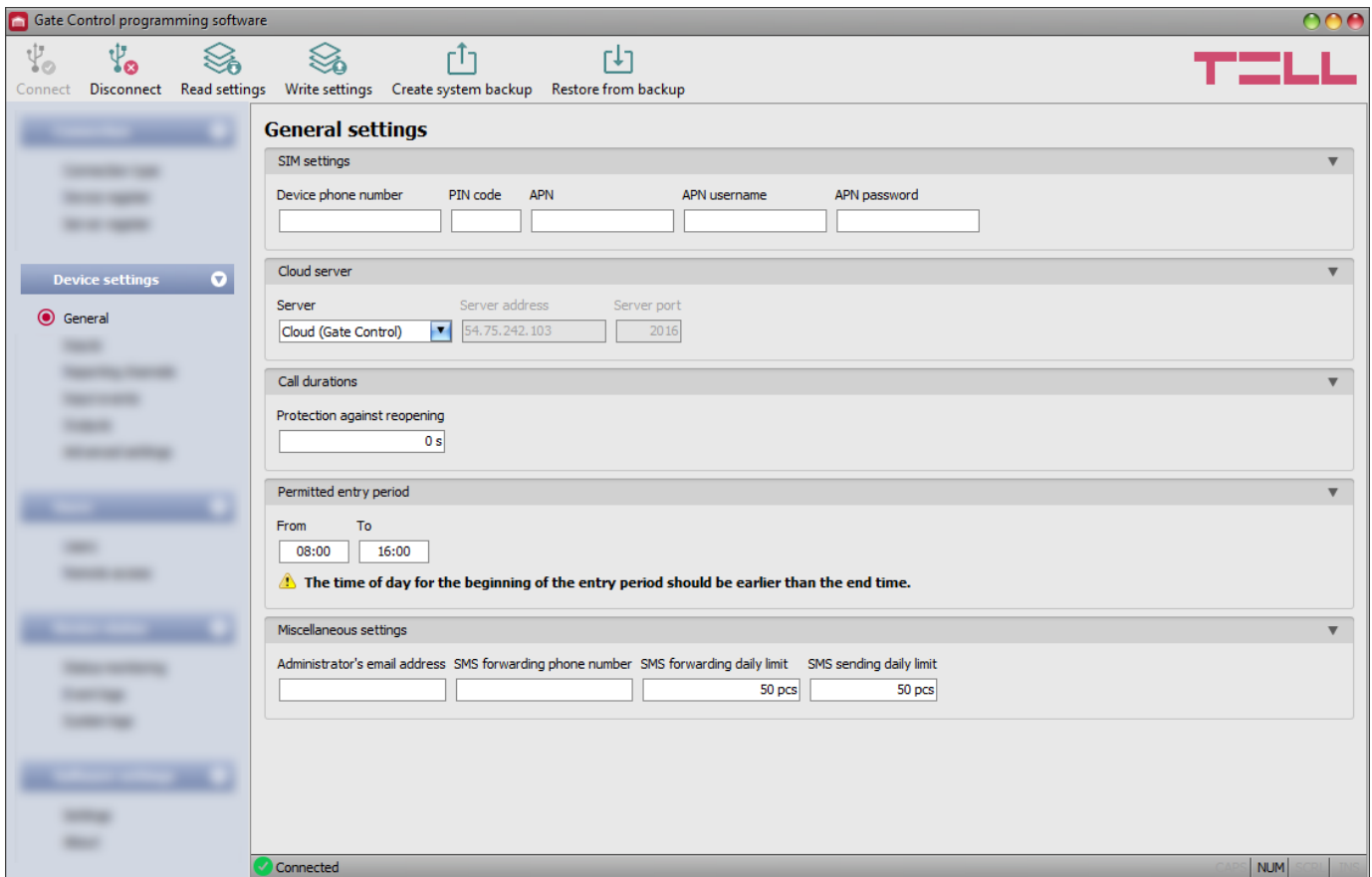
- **Overwriting the full device configuration (device settings, users, and remote access entries):** If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users and the settings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



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 settings into the device by clicking on the “**Write settings**”  and “**Write users**”  buttons. This option is only available when connected via USB.

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.

SIM settings:

Device phone number: enter the phone number of the SIM card installed in the **Gate Control BASE** device. The device will not use this; it is for informational purpose.

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 when connecting to the cloud – 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.

Note: If automatic APN setting fails (the device does not get an IP address when connecting to the cloud), 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.

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:

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).

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.

Permitted entry period:

Users who are granted the “**0-24 entry period**” permission configurable in the user settings, can control the system anytime, while users who are not granted this permission can control the system over the day only within the time interval configured in the “**Permitted entry period**” section in the “**General**” device settings menu, i.e., control requests received from these users will be executed by the device within the configured time period, and will be rejected outside the given period. If there are no users registered in the device, the system can be controlled by anyone from any phone number only within the configured permitted entry period.

From: permitted daily entry period start (hh:mm)

To: permitted daily entry period end (hh:mm)

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.

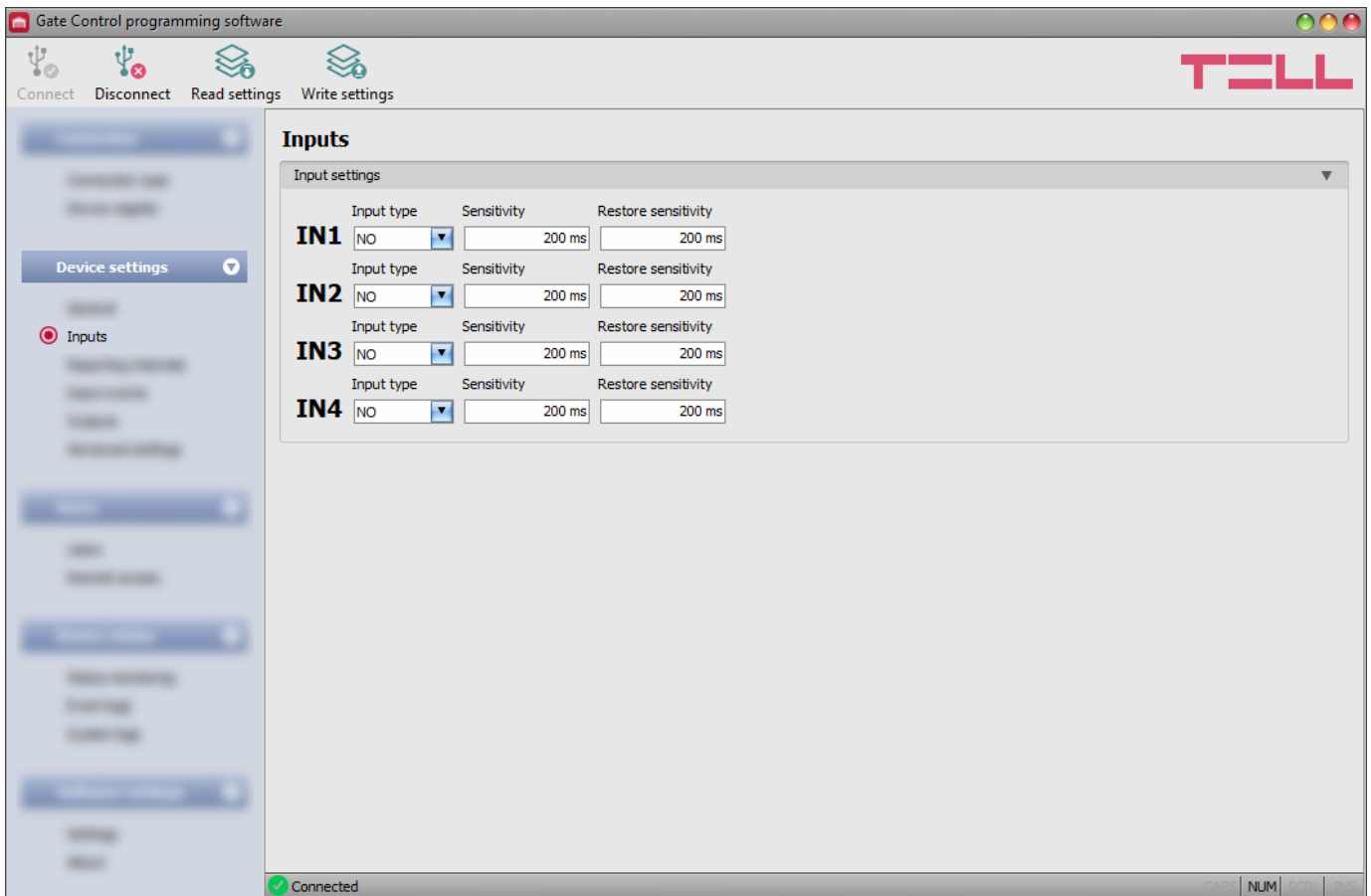
SMS forwarding daily limit: with this option you can limit the number of SMS messages to be forwarded per day. When the configured limit is reached, the system will not forward new incoming SMS messages for 24 hours. After 24 hours, the counter resets automatically and message forwarding will be enabled 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 Inputs



In this menu you can configure the properties and options of the contact inputs IN1...IN4. The system generates input events when the contact inputs are triggered. You can configure notifications for each input event in the “**Input events**” menu, which will be sent to the phone numbers configured in the “**Reporting channels**” menu.

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.

5.2.3 Reporting channels

The screenshot shows the 'Gate Control programming software' window. The top toolbar includes 'Connect', 'Disconnect', 'Read settings', and 'Write settings' buttons, along with the 'TZLL' logo. The left sidebar has a 'Device settings' dropdown menu with 'Reporting channels' selected. The main area is titled 'Reporting channels' and contains a section for 'SMS / call notification recipients'. This section has four rows, each with a label (TEL1, TEL2, TEL3, TEL4) and two input fields for 'Name' and 'Phone number'. At the bottom left, a green status indicator shows 'Connected'. At the bottom right, there are fields for 'NUM' and 'SMS'.

In this menu you can configure the telephone 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.

SMS / call notification recipients:

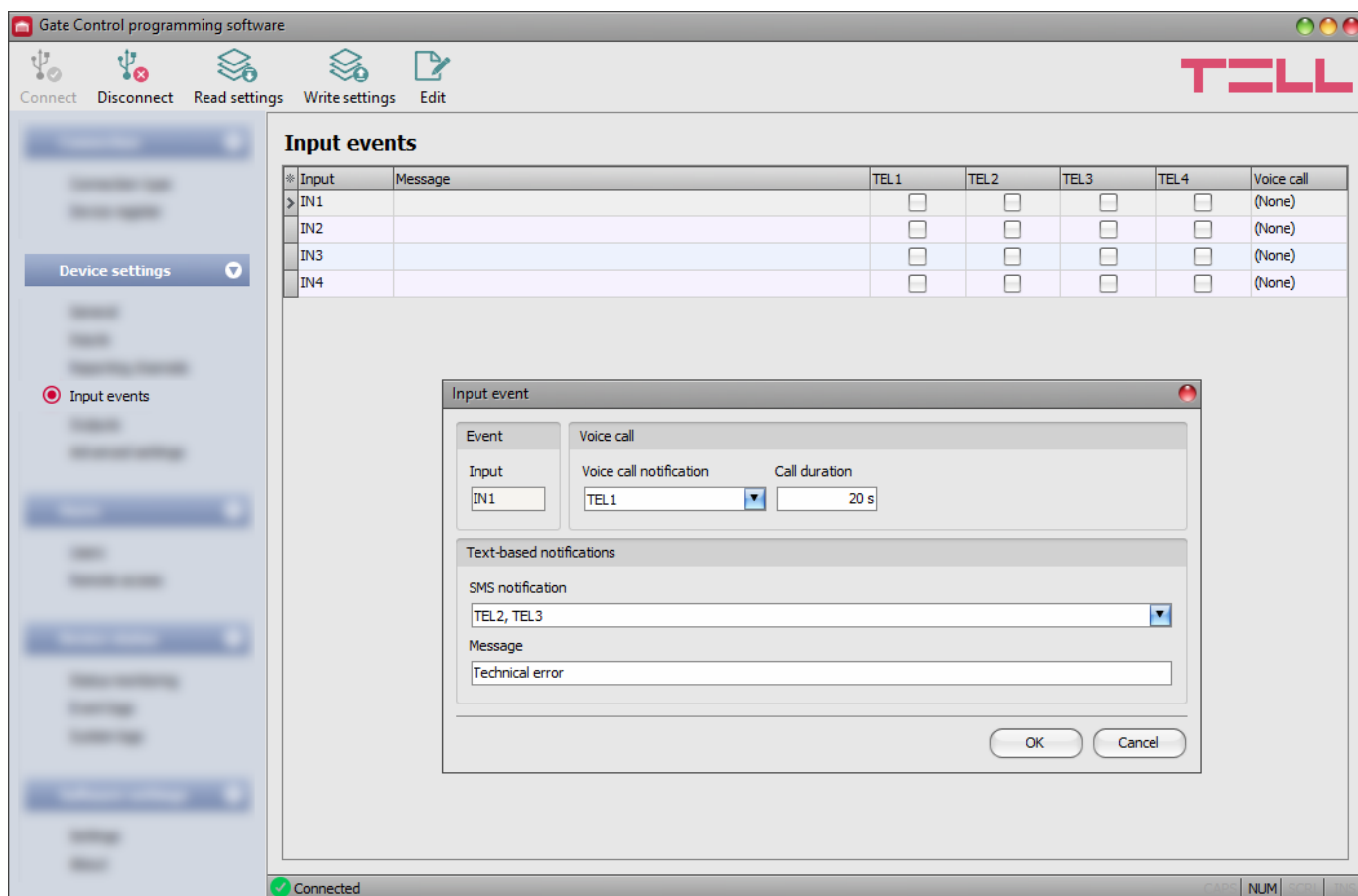
You can configure up to 4 phone numbers (**TEL1...TEL4**) which the system can notify by SMS or call, when contact inputs are activated.

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, an outgoing call will block the Internet connection, i.e., a possible remote connection in progress will be suspended for the duration of the call.

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.

5.2.4 Input events



The screenshot shows the 'Gate Control programming software' window. The 'Input events' tab is selected in the left sidebar. The main area displays a table for configuring input events. Below the table, an 'Input event' dialog box is open, showing configuration for 'IN1'.

* Input	Message	TEL1	TEL2	TEL3	TEL4	Voice call
IN1		☐	☐	☐	☐	(None)
IN2		☐	☐	☐	☐	(None)
IN3		☐	☐	☐	☐	(None)
IN4		☐	☐	☐	☐	(None)

Input event dialog box:

- Event:** IN1
- Voice call:**
 - Voice call notification: TEL1
 - Call duration: 20 s
- Text-based notifications:**
 - SMS notification: TEL2, TEL3
 - Message: Technical error

Buttons: OK, Cancel

In this menu you can configure SMS 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, an outgoing call will block the Internet connection, i.e., a possible remote connection in progress will be suspended for the duration of the call.

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).

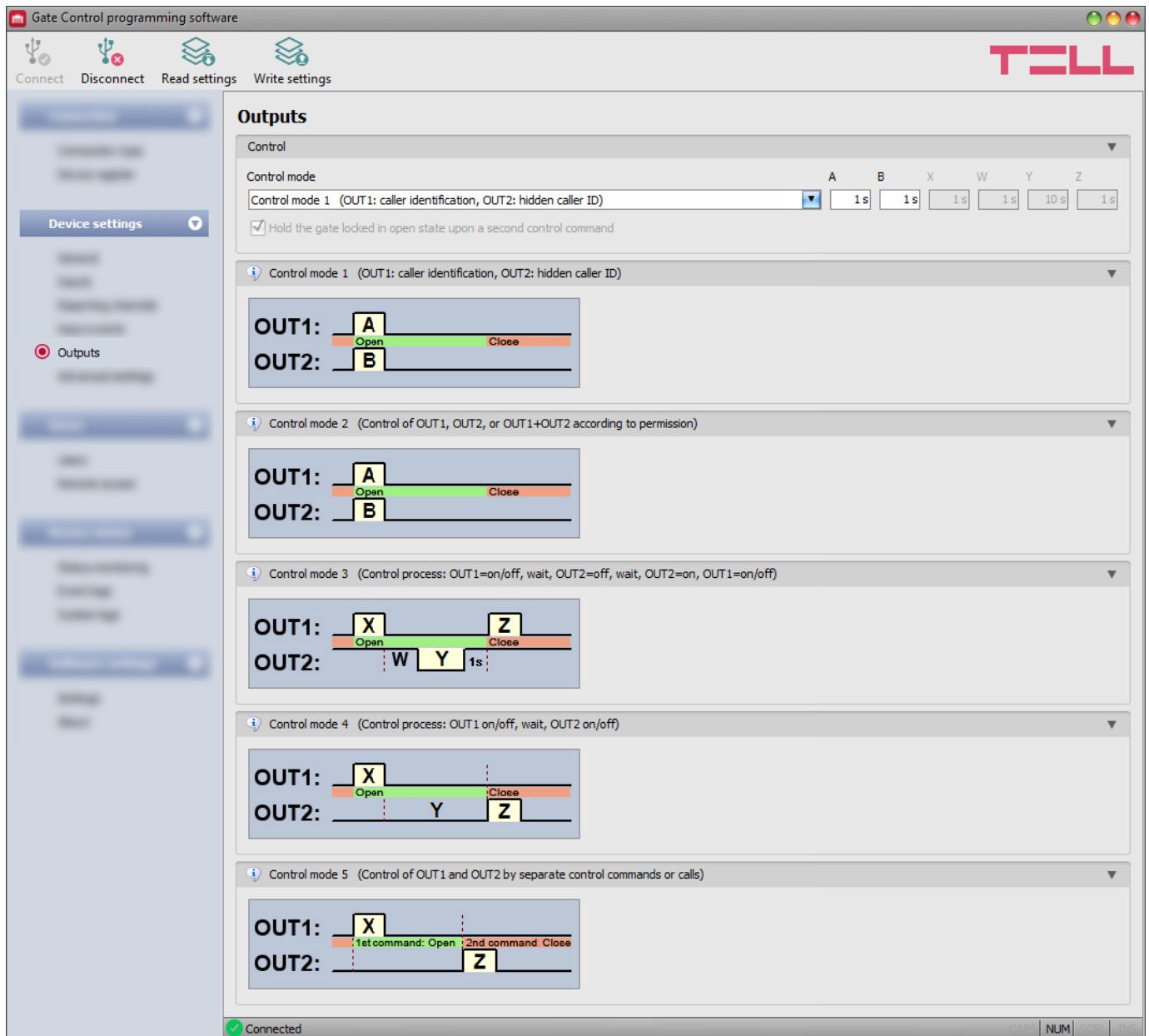
Text-based notifications:

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.

Message: in this field you can enter a custom message of maximum 36 characters, which you want to be sent to the selected phone numbers when the given event occurs.

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

5.2.5 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.

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.

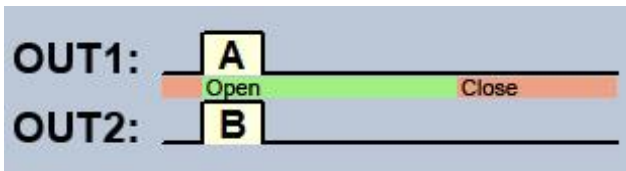
Please note that after you make changes, you must write the settings into the device to be applied. For this, click on the “**Write settings**”  button.

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

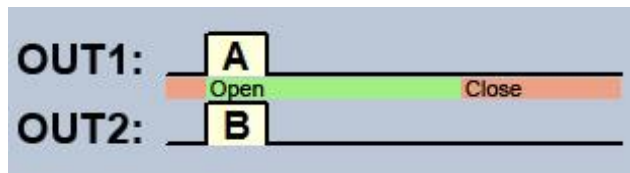
Selective control of outputs OUT1 and OUT2 by using caller identification and hidden caller ID (private number). If the caller sends the caller ID, output OUT1 will be activated. If the caller hides the caller ID (i.e., calls from a private number), output OUT2 will be activated. Thereby, using this 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

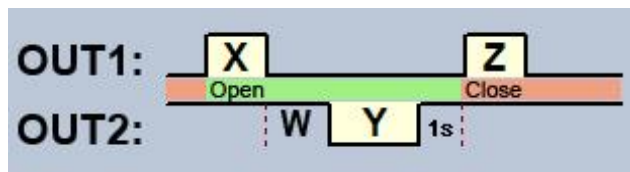
B = OUT2 pulse length (seconds) => for opening gate B

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

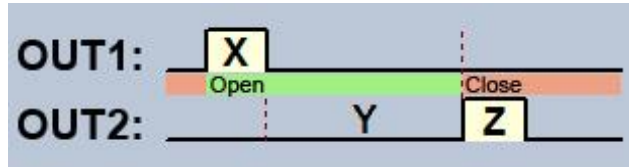
Starting a process of opening and closing by a single call/control command, using caller identification. In idle state, output OUT1 provides an open contact, while output OUT2 provides a closed contact between the **NO** and **COM** terminals. Upon controlling the device, output OUT1 becomes activated (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 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 call is received from the same user, or a new 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) $\Rightarrow$ for gate opening

Y = holding the gate open (seconds) $\Rightarrow$ for holding the gate locked in open state

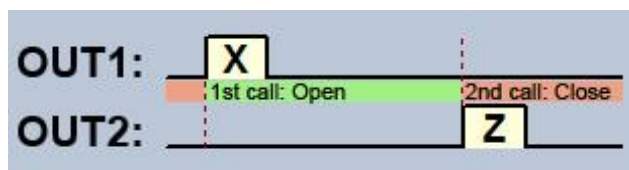
Z = OUT2 pulse length (seconds) $\Rightarrow$ for gate closing

Starting a process of opening and closing by a single call, 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 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 call is received from the same user, or a new 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.



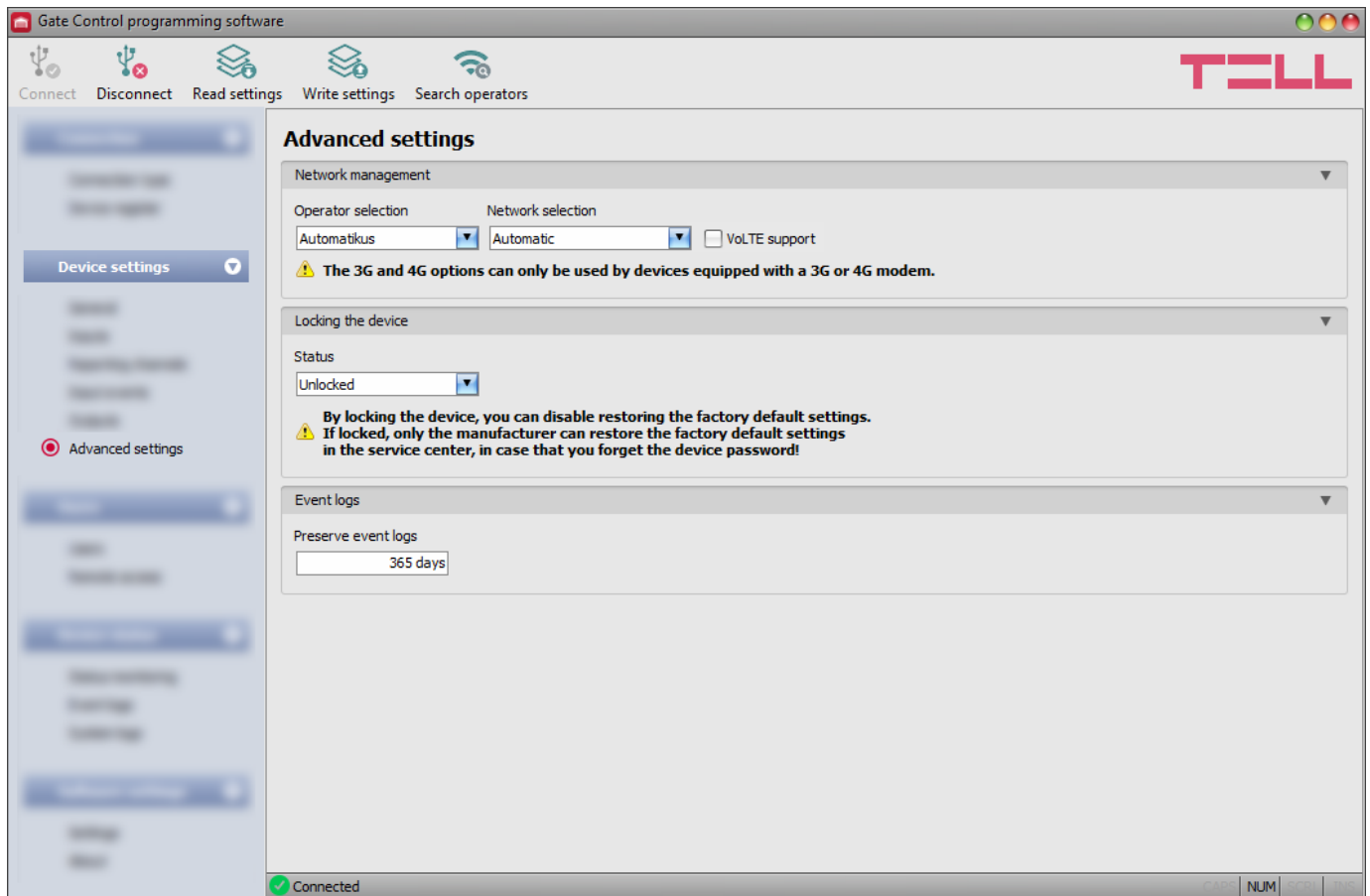
OUT1=N.O. (normally open)
OUT2=N.O. (normally open)

X = OUT1 pulse length (seconds) $\Rightarrow$ for gate opening

Z = OUT2 pulse length (seconds) $\Rightarrow$ for gate closing

Opening and closing by separate calls. 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 call, and then, upon the second call from the same user, 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.

5.2.6 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	☐	☐	☐
Telekom HU	☒	☒	☐
Telenor HU	☒	☒	☐
vodafone HU	☒	☒	☐

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 1200 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 and remote access settings in the submenus available in the “**Users**” menu.

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

- **Changing the user or remote access settings:**

To change the settings of user 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, and remote access entries):**

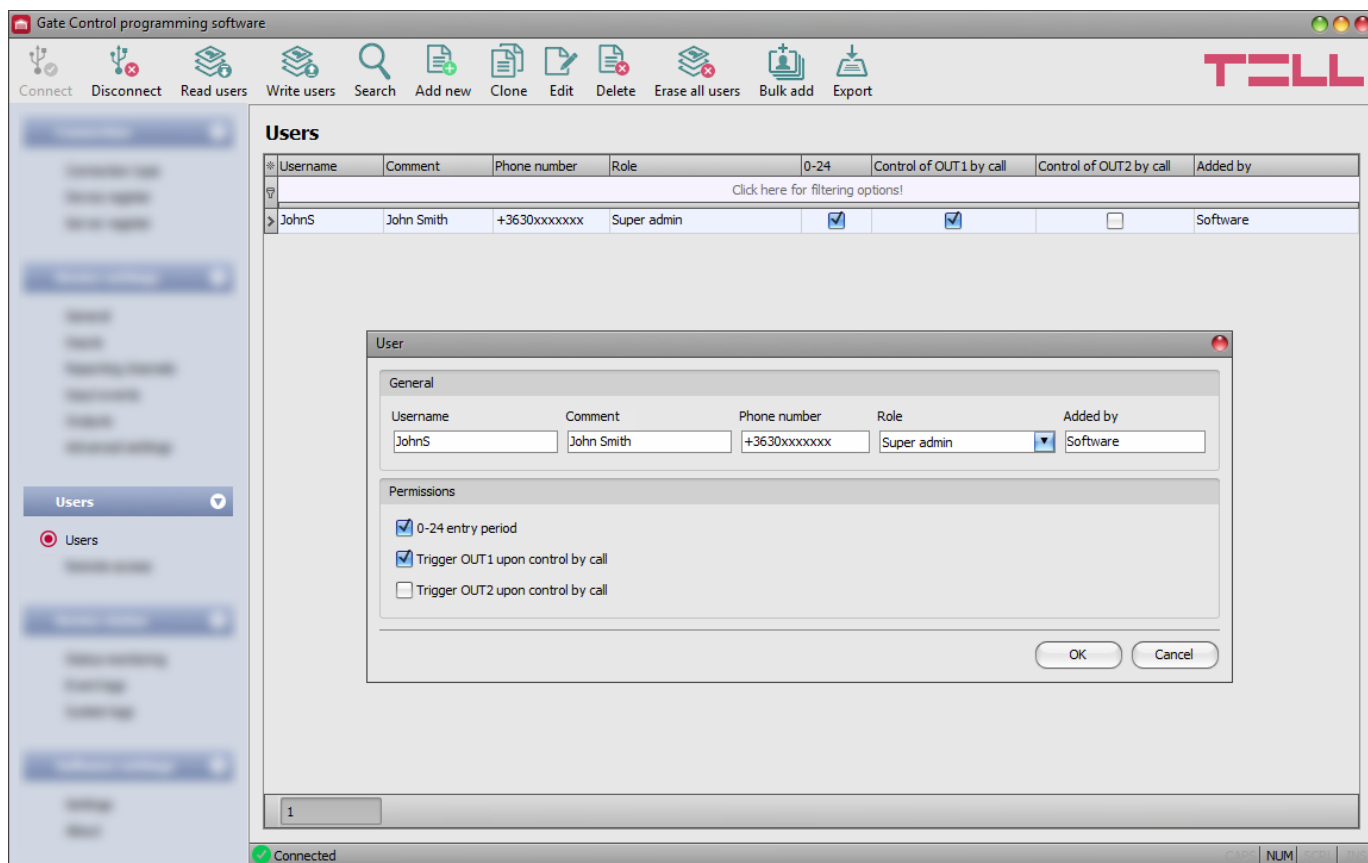
If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users

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.

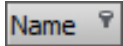
5.3.1 Users



In this menu you can add users and configure user permissions.

The system can be controlled from registered user phone numbers, or from any phone number, if there are no users registered in the system. You can register up to 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 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

User settings

☐ Use the settings found in the CSV file ☒ Configure on this interface

General

Role: User Added by: Software

Permissions

☐ 0-24 entry period
☒ 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
Warning	Invalid user role/permission!: #4 JS05
Warning	Name missing!: #5 +3630xxxxxxx
Error	Error in line: #6
Information	New user: Jen118
> Summary	Successful: 4, Warning: 2, 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 enables you to import a simple user list, or an extended file that also contains user settings. The program detects the type of the list you want to import automatically, based on the file content.

The program considers the first line of the CSV file as the header!

- **Simple user list:**

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

- **Extended user list with user settings:**

The file must contain the header shown in the example below in the first line. Do not change the header! Starting from the second line, the file must contain the users and their settings. The line should start with the username, followed by the comment, the phone number, the role, the 0-24, OUT1 and OUT2 permissions, and finally the registerer's username, each separated by semicolons.

Example:

User name;Full name;Phone number;Role;24h;OUT1;OUT2;Added by

JSmith;John Smith;+3630xxxxxxx;S;1;1;0;Software

Possible values for user roles that you can configure in the file:

- U:** user
- A:** administrator
- S:** super administrator

Possible values for the 0-24, OUT1, and OUT2 permission parameters:

- 0:** disabled
- 1:** enabled

If the file you want to import contains user settings too (role, permissions), you can choose in the “**User settings**” section of the bulk add window to preserve and apply the user settings found in the CSV file or configure the settings in that window and apply generally to all imported users.

The program will indicate, if there are issues in the file to be imported, e.g., duplicate usernames, phone numbers, or usernames 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 username and/or the phone number appears more than once in the file, or already exists among the users registered in the device, or the username or the phone number is missing.

Error (red background color): entries with errors that 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 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.

➤ User settings:

General:

Username: the user’s short username must not exceed 40 characters, and the following characters must 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 must not exceed 40 characters, and the following characters must 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 and settings.

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.

Permissions:

0-24 entry period: if this option is enabled, the given user can control the system anytime over the day. If this option is disabled, the given user can control the system over the day only within the time interval configured in the “**Permitted entry period**” section in the “**General**” device settings menu, i.e., control requests received from this user will be executed by the device within the configured time period, and will be rejected outside the given period.

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.

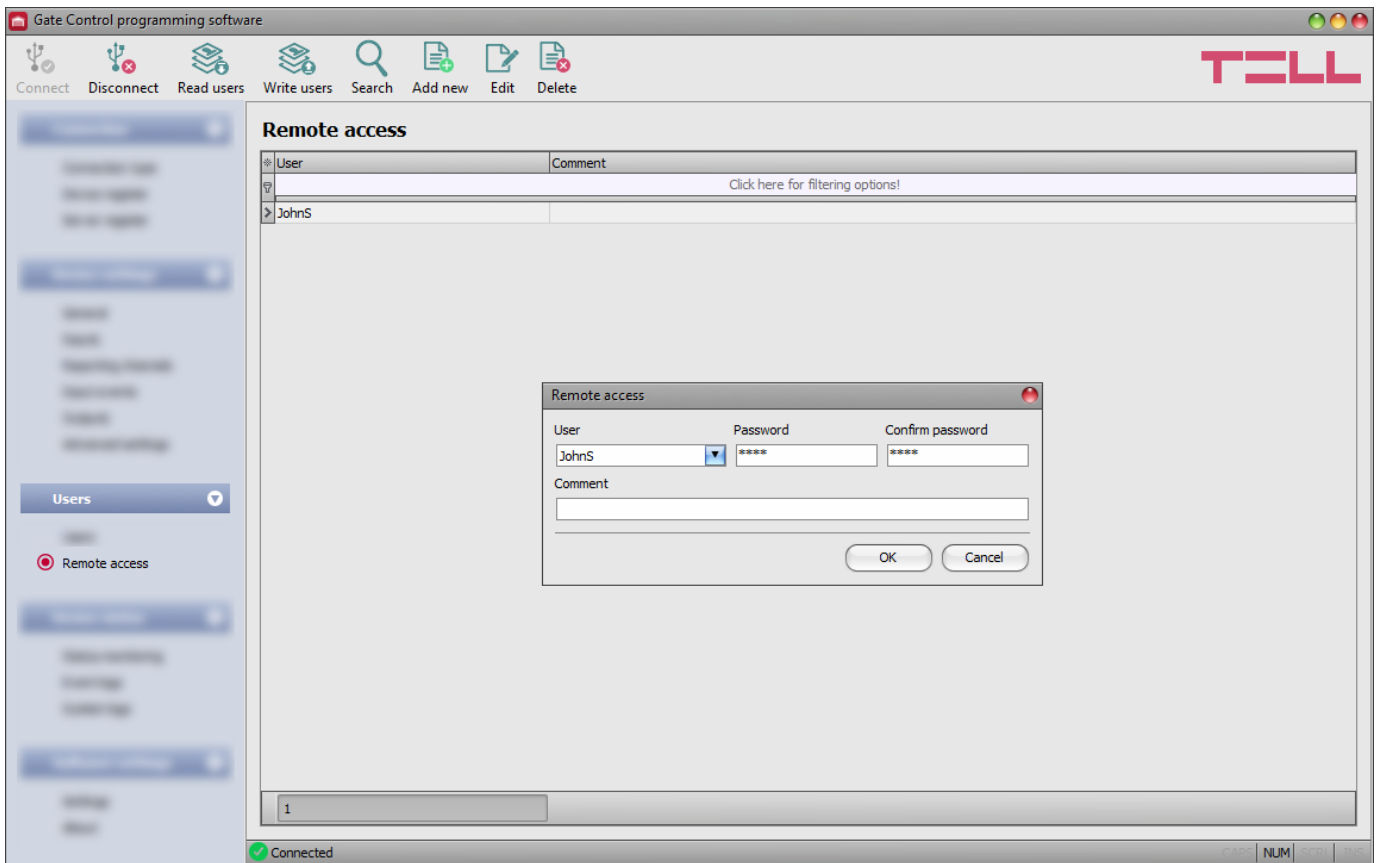
Trigger OUT2 upon control by call: if this option is enabled, the device will control output OUT2 when the given user controls the system by call, or the user’s mobile application controls the system by call, if controlling over the Internet fails due to a connection error.

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 at the same time. 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.

➤ Adding a new user:

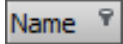
- Click on the “**Add new**”  button.
- Enter the user’s username and phone number.
- Select the user’s role.
- Configure the user’s permissions.
- Click on the “**OK**” button.
- Click on the “**Write users**”  button.

5.3.2 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. You can register up to 2000 remote access passwords in the system.

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:	Has permission to manage users only, therefore, has no access to menus included in the " Device settings " menu group.
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**" and the "**Confirm password**" fields.
- 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 displays the 'Gate Control programming software' window. The top toolbar includes buttons for 'Connect', 'Disconnect', 'Time synchronization', 'Toggle output 1', 'Toggle output 2', 'AT log', and 'Modem FOTA update'. The 'Status monitoring' menu is selected on the left sidebar. The main area is divided into three sections: 'Property', 'Counters', and 'Network'. The 'Property' section shows device details like firmware version (V10.01.3.8331), model (Gate Control BASE 1000), and SIM identifier (8936304321060554011). The 'Counters' section shows system time (2024.08.07.11:17:29) and uptime for IP, device, and GSM. The 'Network' section shows GSM operator (Telekom HU), signal (Excellent), and connection type (4G E-UTRAN). The 'Inputs / Outputs' section shows IN1-OUT2 status (all Idle). The 'Logs' section on the right shows a list of system events, including power on, AT check, SIM init, and network registration.

Property	Status / Value
Device	
Firmware version	V10.01.3.8331
Model	Gate Control BASE 1000
SIM identifier (ICCID)	8936304321060554011
Supply voltage	13,54 V
Device ID	60:8A:10:A1:37:63
MAC address	60:8A:10:A1:37:63
Modem type	A7682 (2G, 4G)
Counters	
System time	2024.08.07.11:17:29
IP uptime	0 s
Device uptime	175 s
GSM uptime	132 s
Network	
GSM operator	Telekom HU
GSM signal	Excellent
Data connection type	4G (E-UTRAN)
Modem IP address	
Cloud connection	Disconnected
Inputs / Outputs	
IN1	Idle
IN2	Idle
IN3	Idle
IN4	Idle
OUT1	Idle
OUT2	Idle

Logs
(11:14:55)Power on
(11:15:10)Check...
(11:15:10)AT check OK
(11:15:11)Modem type: A7682
(11:15:19)Checking SIM card...
(11:15:19)SIM init OK
(11:15:19)Checking SIM PIN...
(11:15:19)SIM init OK
(11:15:21)MUX check OK
(11:15:21)Modem full rev: A011B12A7682M7
(11:15:21)Wait for network registration...
(11:15:22)Network: home
(11:15:22)Modem set volume: mic=8, spk=56
(11:15:23)Modem APN[1]: internet.telekom.mnc030.mcc216.gprs, proto: IP
(11:15:23)Modem APN[8]: ims, proto: IPV4V6
(11:15:25)pppsm start...
(11:15:25)SMS storage size: 20
(11:15:26)New day: counters reseted

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 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 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.

Inputs / Outputs:

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

Available options:

- **Read:**

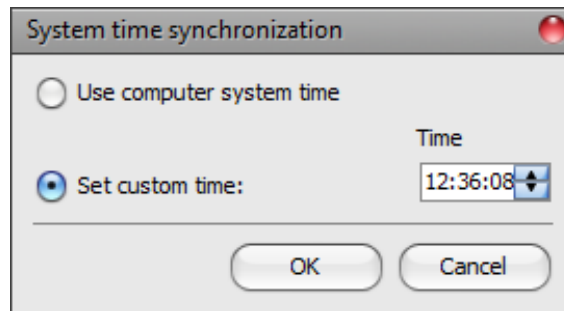


This button is available only when connected remotely to the device. By clicking on this button, the program will read the status information from the device. This is not needed when connected via USB, since in that case the data are read and refreshed automatically.

- **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 the automatic synchronization from the mobile network fails. The device will also synchronize the system time automatically from the cloud when it connects to the 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 any 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:**



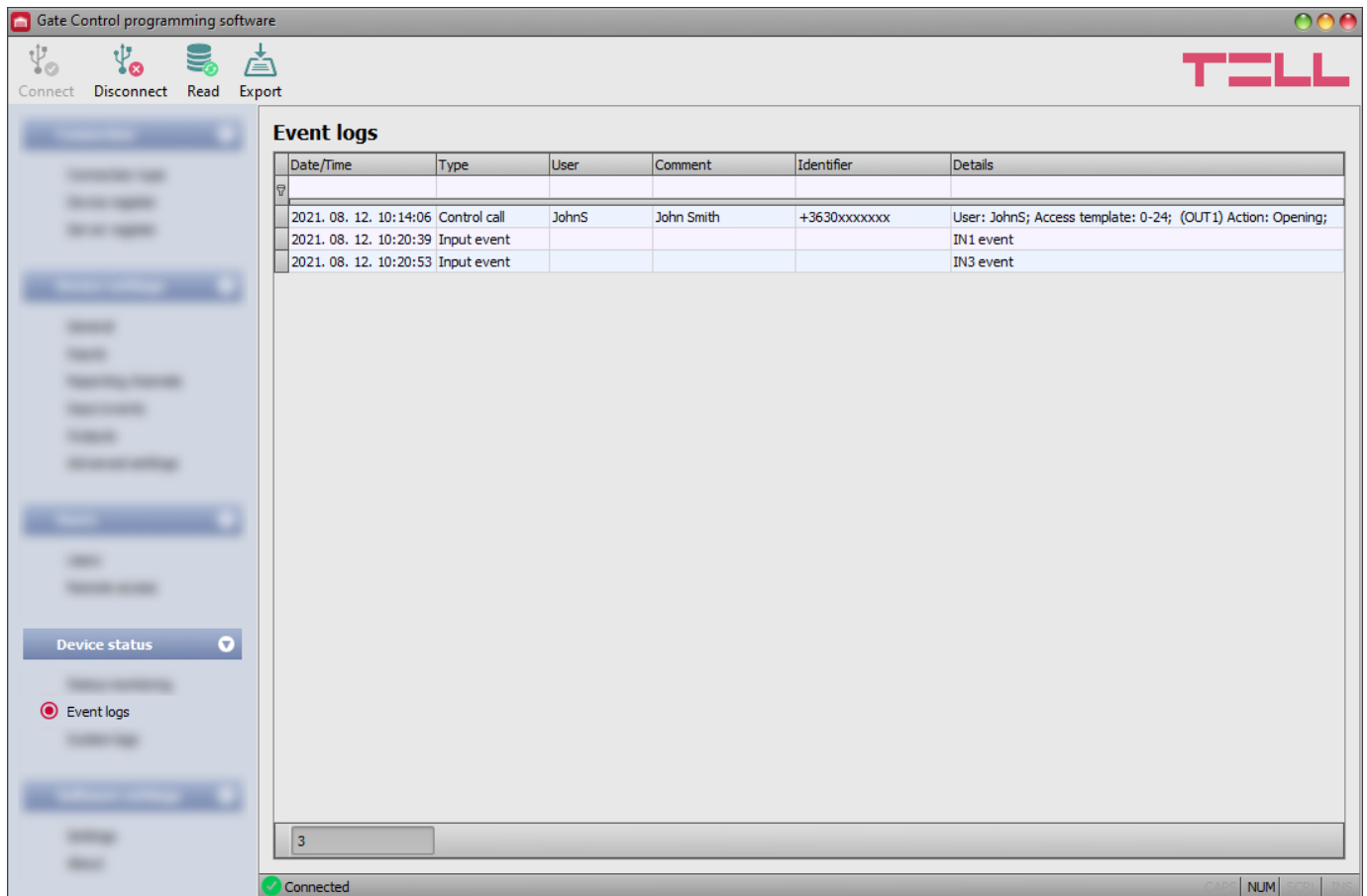
Using this button, you can update the firmware of the modem installed in the device. The manufacturer of the modem also continuously improves their products, therefore, new firmware updates may occasionally be released for the modem, which along with bug fixes, may include improvements following the 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 1200 events in the event log memory.

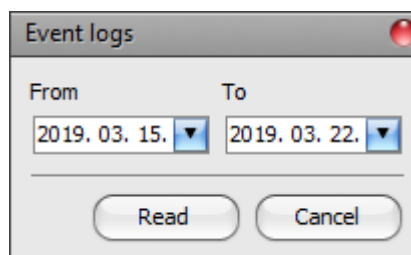
The values configured in the “**Comment**” field in the user settings are not stored in the event logs. The data in the “**Comment**” column is filled in by the software from the user list. Therefore, data will only be shown in this column if you read the users from the device before reading the event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



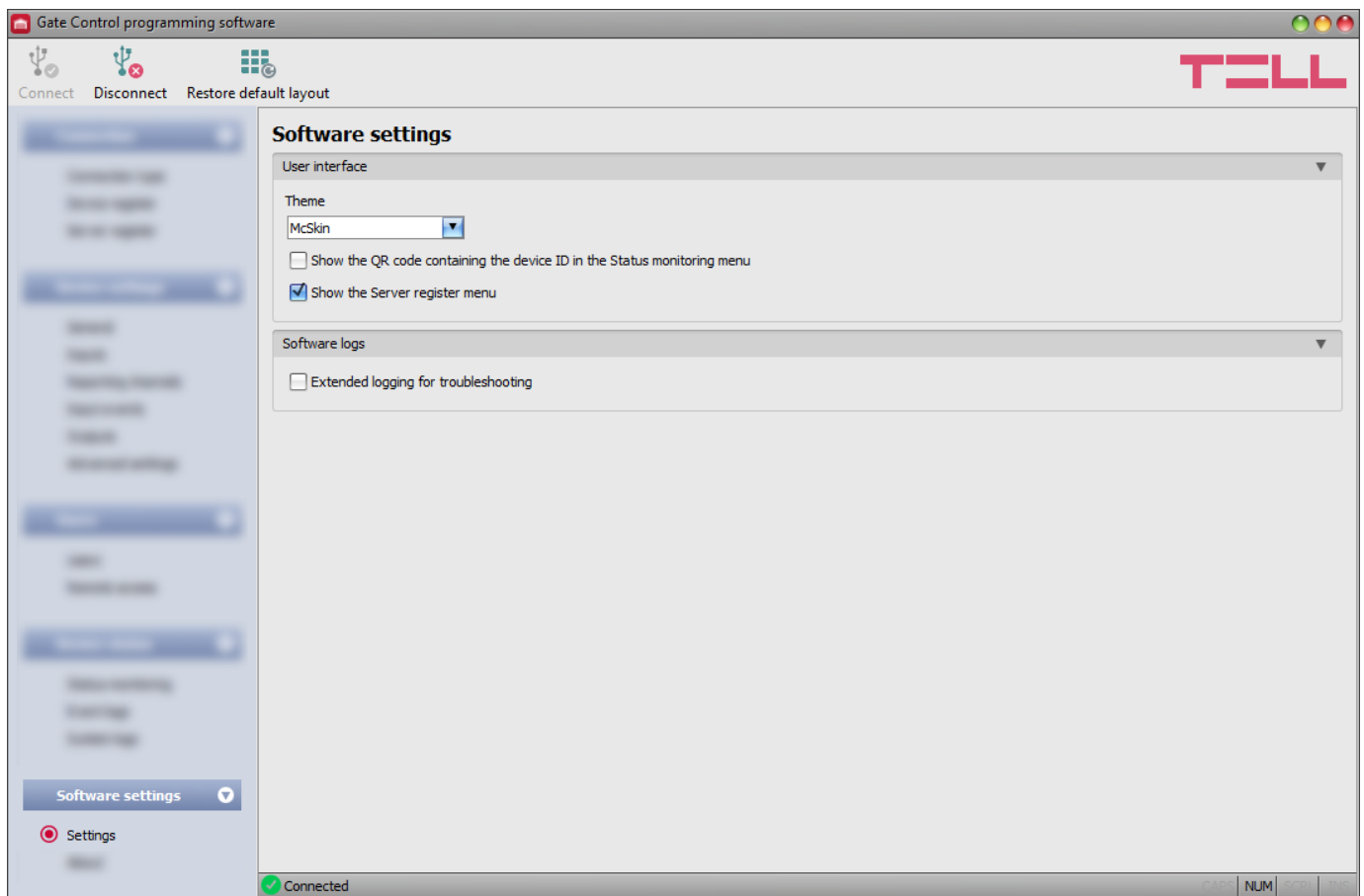
- **Export:**



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.

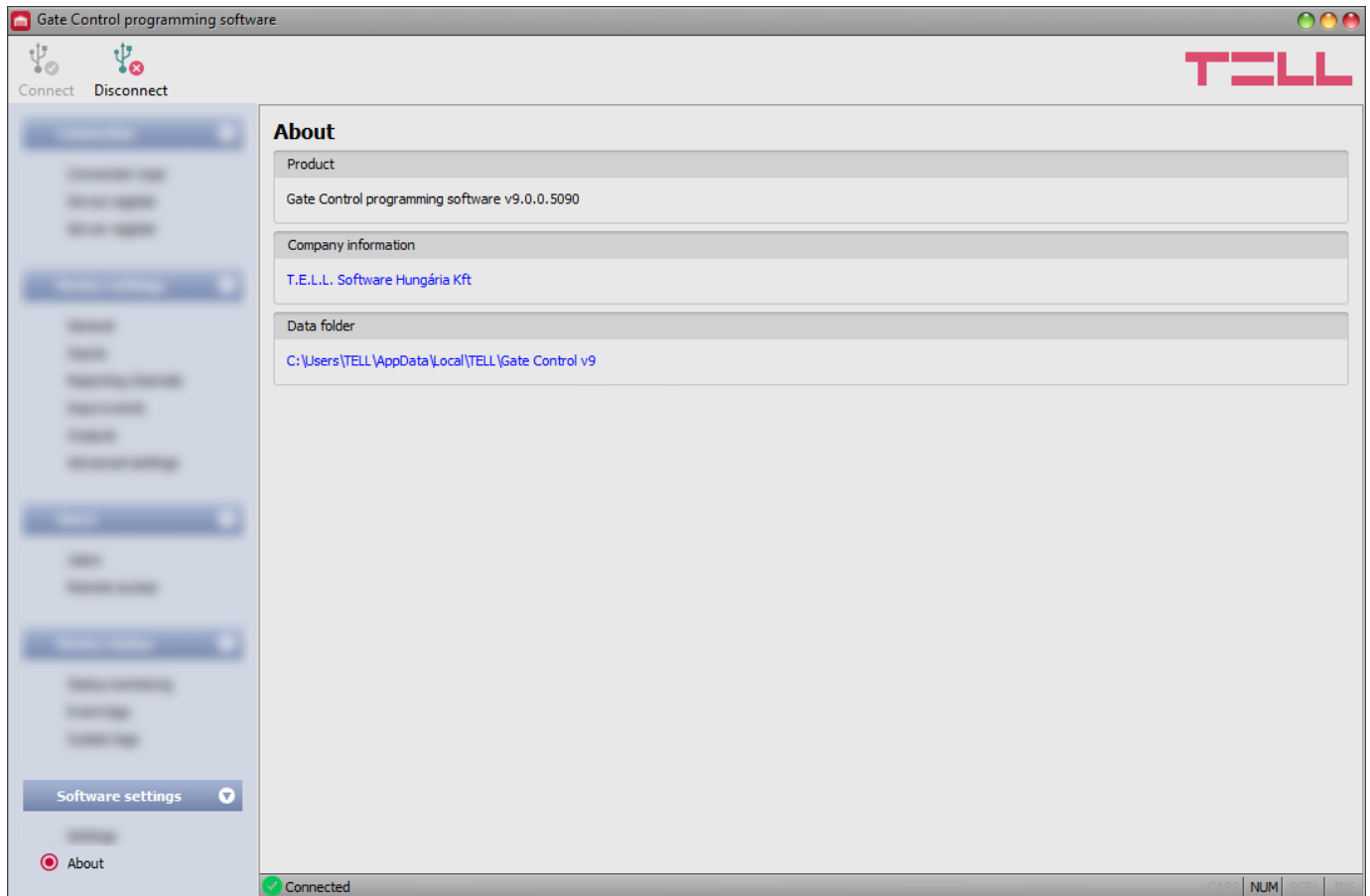
Show the QR code containing the device ID in the Status monitoring menu: if this option is enabled, the QR code that contains the device ID will be shown in the “**Status monitoring**” menu. This is used by the manufacturer to record devices produced.

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 Configuring the *Gate Control BASE* by SMS, using a mobile phone

It is possible to change the device’s most important settings, and to add or delete users using commands sent by SMS to the phone number of the SIM card installed in the device. Commands are accepted from super admins or admins registered in the device, according to their access level:

Each command must begin with the star * character and must end with the hash # character. You can send multiple commands in one message, but the message must not be longer than 60 characters. The device will process commands to the last hash # character that is still within the 60 characters limit in the message, and commands found beyond this will be ignored. The device will send a confirmation about processed commands only.

The available SMS commands are summarized in the table below. You can find the detailed specification of the commands below the table. The Super admin can use all available commands, while the Admin is authorized to use only commands related to user management (these are marked separately in the table).

Action	SMS command
Quick registration of the Super admin user	*SUPERADMIN# *SUPERADMIN=USERNAME,COMMENT,REMOTE ACCESS PASSWORD#
New user registration with detailed configuration (also available with Admin role)	*n=PHONE NUMBER,USERNAME,COMMENT,ROLE,ENTRY PERIOD,OUTPUT#
Deleting a user (also available with Admin role)	*d=USERNAME# *d=PHONE NUMBER#
Deleting all users (also available with Admin role)	*ERASEALLUSERS#
Configuring the permitted entry period	*EP=FROM,TO#
Configuring the output control mode	*M=1,A=1,B=1# *M=2,A=1,B=1# *M=3,X=1,Y=1,W=15,Z=1,O=1# *M=4,X=1,Y=1,Z=1,O=1# *M=5,X=1,Z=1#
Configuring the contact inputs	*I1=INPUT TYPE,SENSITIVITY# *I2=INPUT TYPE,SENSITIVITY# *I3=INPUT TYPE,SENSITIVITY# *I4=INPUT TYPE,SENSITIVITY#
Configuring phone numbers for SMS / call-based notification	*T1=PHONE NUMBER# *T2=PHONE NUMBER# *T3=PHONE NUMBER# *T4=PHONE NUMBER#
Associating SMS message text with inputs	*S1=MESSAGE TEXT# *S2=MESSAGE TEXT# *S3=MESSAGE TEXT# *S4=MESSAGE TEXT#
Configuring the SMS forwarding phone number	*SF=PHONE NUMBER#
Configuring the device phone number	*MT=PHONE NUMBER#
Restoring the USB password to factory default	*PWRESET#
Initiating a cloud connection (also available with Admin role)	*CONNECT#
Configuring the APN	*APN=APN#
Configuring the APN with related username and password	*APN=APN,username,password#
Setting the system time (Can be sent from any phone number)	#DT

6.1 Detailed specification of SMS commands

- Quick registration of the Super admin user:

You can register only one Super admin user by SMS, and only if there are no Super admins registered in the system yet. The first Super admin can be registered simply with the username "SUPERADMIN" and remote access password "1234", or the chosen username, comment, and remote access password can be specified in the message. For this, two different commands are available.

SMS command	Reply from device	Meaning of reply message
*SUPERADMIN# or *SUPERADMIN=USERNAME, COMMENT,REMOTE ACCESS PASSWORD# *You can skip the <i>REMOTE ACCESS PASSWORD</i> parameter.	YOU ARE REGISTERED AS SUPERADMIN!	Super admin registered successfully
	ERROR: SUPERADMIN USER ALREADY REGISTERED!	Error: at least one Super admin is already registered
	ERROR: USERNAME ALREADY REGISTERED!	Error: the given username already exists in the system
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)

- Registering a new user (also available with Admin role):

SMS command	Reply from device	Meaning of reply message
*n=PHONE NUMBER,USERNAME, COMMENT,ROLE,ENTRY PERIOD,OUTPUT# Examples: *n=+3630xxxxxxx,JSmith,John Smith,A,N,B# *n=+3620xxxxxxx,Pete,Peter Adams,1# *n=+3670xxxxxxx,Jimmy,Jim Taylor,2#	NEW USER REGISTERED.	New user registered successfully
	NUMBER ERROR!	The phone number is too short or too long
	USERNAME ERROR!	The username is missing, or it is too long
	USER ALREADY EXISTS!	The given phone number already exists in the system
	MISSING PARAMETER	The OUTPUT parameter is missing for control mode 1 or 2
	ERROR: INVALID CHARACTER: "X"!	Wrong parameter (X) in the command
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

Command parameter values:

ROLE:
S = Super admin
A = Admin
U = User (default)

ENTRY PERIOD:
N = 0-24
L = in the permitted entry period (default)

OUTPUT:
1 = OUT1
2 = OUT2
B = OUT1 and OUT2

*You can skip the *ROLE* and *ENTRY PERIOD* parameters. In this case the device will set the default values automatically. If the *COMMENT* parameter is not specified, the device will write the specified *ROLE* parameter (S/A/U) in the *Comment* field.

- **Deleting a user (also available with Admin role):**

SMS command	Reply from device	Meaning of reply message
*d=USERNAME# or *d=PHONE NUMBER#	DELETE SUCCESFULL	User deleted successfully
	DELETE FAILED, USER NOT FOUND!	The given username or phone number does not exist in the system
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- **Deleting all users (also available with Admin role):**

SMS command	Reply from device	Meaning of reply message
*ERASEALLUSERS#	USERS ERASED!	All users deleted successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- **Configuring the permitted entry period:**

SMS command	Reply from device	Meaning of reply message
*EP=FROM,TO# Example: *EP=08:00,16:30#	ENTRY PERIOD CHANGED	Permitted entry period changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

Command parameter values:

FROM: permitted daily entry period start (hh:mm)

TO: permitted daily entry period end (hh:mm).

- Configuring the output control mode:

SMS command	Reply from device	Meaning of reply message
*M=1,A=1,B=1# *M=2,A=1,B=1# *M=3,X=1,Y=1,W=15,Z=1,O=1# *M=4,X=1,Y=1,Z=1,O=1# *M=5,X=1,Z=1#	MODE 1 ACTIVATED	Control mode 1. set successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

Command parameter values:

M=1...5 Output control mode number (1...5).
A=0...255 OUT1 pulse length (seconds) => for opening gate "A".
B=0...255 OUT2 pulse length (seconds) => for opening gate "B".
X=0...255 OUT1 pulse length (seconds) => for gate opening.
W=0...255 Delay before interrupting the photocell loop (seconds).
Y=0...255 For M=3: OUT2 pulse length (seconds) => for holding the gate open.
For M=4: gate held open duration (seconds) => for holding the gate open.
Z=0...255 OUT1 pulse length (seconds) => for gate closing.
O=0...1 Holding the gate locked in open state upon a second call:
O=1 function enabled
O=0 function disabled

- Configuring contact inputs:

SMS command	Reply from device	Meaning of reply message
*I1=INPUT TYPE,SENSITIVITY# *I2=INPUT TYPE,SENSITIVITY# *I3=INPUT TYPE,SENSITIVITY# *I4=INPUT TYPE,SENSITIVITY# Examples: *I1=NO,200# *I3=NC,200#	IN1 INPUT TYPE CHANGED	Input IN1 settings changed successfully
	INVALID INPUT TYPE: "X"	Wrong input type (X)
	INVALID INPUT SENSE: "X"	Wrong input sensitivity (X)
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

Command parameter values:

I1...I4: input number (Input 1...4)
INPUT TYPE: **NO** = normally open
NC = normally closed
SENSITIVITY: **100...600000** (ms)

- **Configuring phone numbers for SMS / call based notification:**

SMS command	Reply from device	Meaning of reply message
*T1=PHONE NUMBER# *T2=PHONE NUMBER# *T3=PHONE NUMBER# *T4=PHONE NUMBER#	SMS1 NUMBER CHANGED	Notification phone number 1 changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- **Associating SMS message text with inputs:**

SMS command	Reply from device	Meaning of reply message
*S1=MESSAGE TEXT# *S2=MESSAGE TEXT# *S3=MESSAGE TEXT# *S4=MESSAGE TEXT#	SMS1 TEXT CHANGED	Message text associated with input 1 changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

*The message text must not exceed 36 characters.

- **Configuring the SMS forwarding phone number:**

SMS command	Reply from device	Meaning of reply message
*SF=PHONE NUMBER#	SMS FWD NUMBER CHANGED	SMS forwarding phone number changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- **Configuring the device phone number:**

SMS command	Reply from device	Meaning of reply message
*MT=PHONE NUMBER#	MODULE PHONE NR CHANGED	Device phone number changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- **Restoring the USB password to factory default:**

SMS command	Reply from device	Meaning of reply message
*PWRESET#	PW reset OK, new PW:1234	USB password restored to 1234
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- Initiating a cloud connection (also available with Admin role):

SMS command	Reply from device	Meaning of reply message
*CONNECT#	Connected to 54.75.242.103:2016 ID=device identifier	Connected to the cloud, device identifier=....
	Server not found (address=IP:port)	Connecting failed: wrong APN setting, or mobile Internet service problem, or wrong server address or port number
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- Configuring the APN:

SMS command	Reply from device	Meaning of reply message
*APN=APN#	APN CHANGED.	APN changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- Configuring the APN with username and password:

SMS command	Reply from device	Meaning of reply message
*APN=APN,username,password#	APN CHANGED.	APN changed successfully
	SYNTAX ERROR!	Wrong command (* or # is missing, or other typing error)
	ACCESS DENIED!	No permission for this operation

- Setting the system time:

SMS command	Reply from device	Meaning of reply message
#DT	Date/Time set: 27-06-2021 13:45	System time set successfully to the date and time sent by the device

The device synchronizes the date and time from the time stamp of the message received.

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 BASE** 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-base>) 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 that asks 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 shows activity. 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 BASE** 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 default 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 mobile network and the **STATUS** LED shows a flashing green light.



9 Package content

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