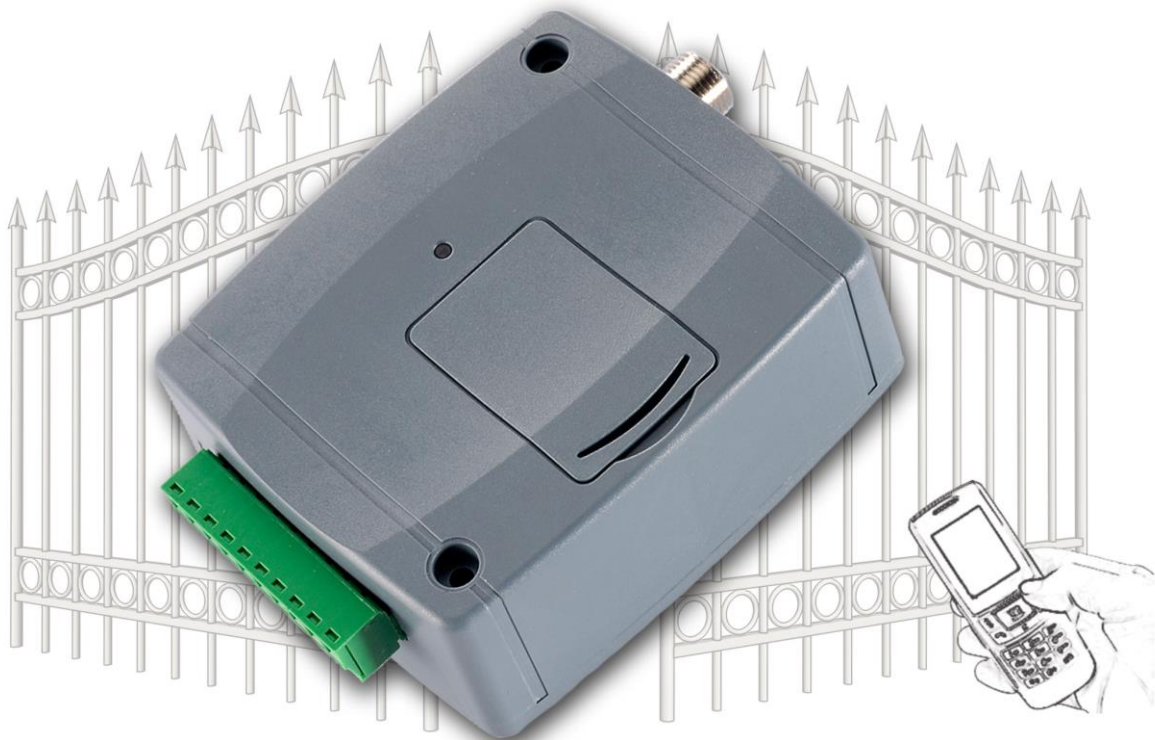**TELL**

Gate Control PRO 20
Gate Control PRO 1000

INSTALLATION AND APPLICATION MANUAL

for device version v7.00 and newer
Document version: 4.0 25.03.2019

► **Features:**

- Control of outputs over the internet using mobile application
- Control of outputs by free phone calls using caller identification
- 5 different control modes
- 4 NO/NC inputs, 2 NO relay outputs
- 50 configurable access templates
- Configurable holidays
- Automatic timed controls
- 20 and 1000 user variant
- Reports the status of the 4 contact inputs by e-mail, SMS or GSM call

- Stores the latest 1000 events in the event log memory
- Programmable via USB, internet and mobile application

► **Application area:**

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

Table of contents

Dear Customer,

Thank you for choosing our product. This manual includes important information and instructions regarding the product. Please read this manual before using the product.
The latest version of the product's programming software and manuals are available on the manufacturer's website at: https://tell.hu/en/products/gsm-automation/gate-control-pro

1   General operation of the *Gate Control PRO*

The *Gate Control PRO* device was basically designed for control of electric gates and barriers, however it can be used to control other devices as well. Controlling can be performed according to the configured control mode by making a phone call to the SIM card installed into the device and/or over the internet, using the mobile application. During the installation you can choose out of 5 control modes the one which is appropriate for your application. In case of controlling by call, the system uses caller identification to identify the caller/user. Since to identify the caller and perform the control is enough to identify the caller ID, the system rejects the call, thereby the call will be free of charge. However, it is possible that the GSM service provider applies call set-up fee for rejected calls (this is operator-dependent, please ask your GSM 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 log. When controlling by mobile application, the system identifies the user by the identifier of the smart device, which can be read from the Gate Control mobile application.

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

The services to be activated on the SIM card installed into the *Gate Control PRO* device should be chosen according to which services of the device you wish to use. For usage with the mobile application and for the functions that use e-mail sending mobile internet service is necessary. The functions that use SMS sending need SMS service and the ones that use calls require GSM voice call service. For accessing the Internet the SIM card should use a public APN.

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

1.1   Data traffic

The expected data traffic of the SIM card installed into the *Gate Control PRO* device at minimal usage may reach even up to ~20 MB per month. The data traffic rate depends on the frequency of use, the stability of the mobile network and the used services. The services using data traffic, such as control by mobile application, remote programming, remote download of event logs, remote firmware update, sending of emails and reports, all contribute to the increase of the SIM card's data traffic. The extent of the data traffic increase depends on how frequent and for how long the mentioned services are used. Depending on the usage, the data traffic may reach the multiple of the amount mentioned for minimal usage.

1.2 Operation of the contact inputs

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

1.2.1 Dedicated input functions

Input IN1: in addition to the notification functions mentioned above, input IN1 is dedicated by factory default to the doorbell function. This means that if the system is used with the mobile application, the system will send a "***Doorbell***" Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering input IN1. If you connect your doorbell to input IN1, this way, enabled mobile devices will be notified via Push message about doorbell ringing.

Input IN2: in addition to the notification functions mentioned above, input IN2 is dedicated by factory default to the failure notification function. This means that if the system is used with the mobile application, the system will send a "***Technical or device failure***" Push message to all mobile devices for which this notification option is enabled in the settings, upon triggering input IN2.

The properties of the functions dedicated to the inputs mentioned above (e.g. message, associating with another input) cannot be changed. You can enable Push messages for each mobile device separately in the "***Mobile devices***" menu in the programming software. Push message sending works via the Internet using free of charge Push notification service.

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

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

2 Processing of personal data

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

Users' consent to processing their personal data shall be deemed to be given on the basis of 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 wish to use the system.

The system stores the personal data in the device's memory. The personal data are not accessible for third party, only 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 turns off automatically if the supply voltage drops under a critical 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 negative of the power input (**V-**).

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 notification sending by SMS, e-mail or call is initiated when the given input (**IN1**…**IN4**) and the **V-** terminal is shorted.

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 notification sending by SMS, e-mail or call is initiated when shorting between the given input (**IN1**…**IN4**) and the **V-** terminal is removed.

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

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

3.3 Output wiring

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

For control modes 1, 2, 4, 5:

OUT1: normally open dry relay contact (N.O.)
OUT2: normally open dry relay contact (N.O.)

For control mode 3:

OUT1: normally open dry relay contact (N.O.)
OUT2: normally closed dry relay contact (N.C.)

The normally open (N.O.) output provides open contact by default and closed contact upon control. The normally closed (N.C.) output provides closed contact by default and open contact upon control. The outputs provide dry (potential free) relay contacts. The relay contacts can take a maximum load of **1A**@24V AC/DC.

You can find a detailed description about control modes in the "***Outputs***" chapter.


3.4 Connections

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

3.4.1 Wiring diagrams

System terminal inputs and outputs:

V+	Supply voltage 12…30V AC/DC (min. 500mA)
V-	Supply voltage negative (if DC)
IN1	Dry contact input 1
IN2	Dry contact input 2
IN3	Dry contact input 3
IN4	Dry contact input 4
OUT1	Relay output 1 (normally open dry contact, max. 1A@24V AC/DC)
OUT2	Relay output 2 (normally open dry contact, max. 1A@24V AC/DC)
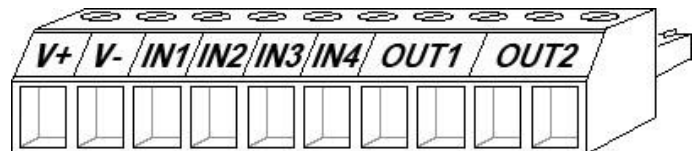
Control mode 1:

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


Wiring for two gates with position limit switch (control mode 1 and 2)
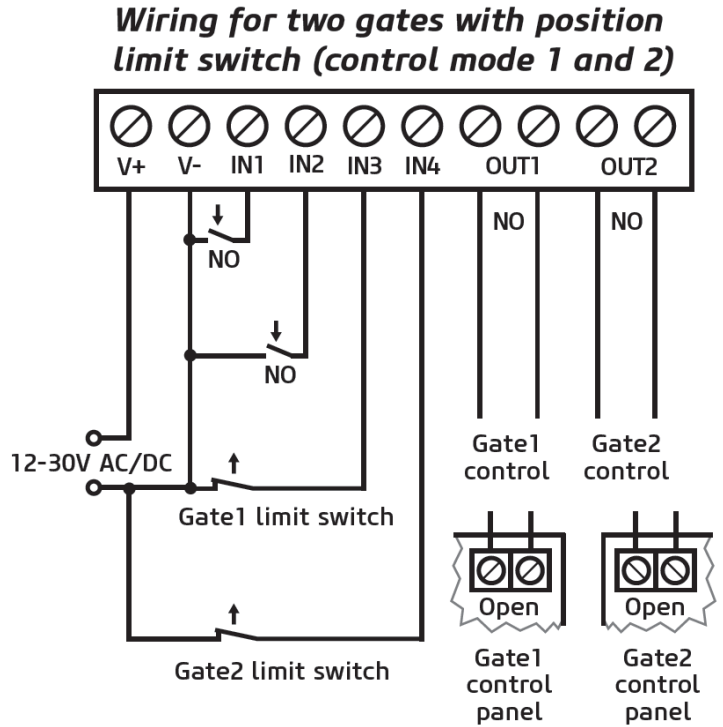
Control mode 2:

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

Control mode 3:

- For single-gate automations that require triggers for opening and closing on the same input.
- Opening and then closing by a single call/control command.
- Output OUT1 is normally open (NO), while OUT2 is normally closed (NC).
- Output OUT1 is used to control the gate, while OUT2 is used to interrupt the photocell sensor circuit, thereby providing an option to keep the gate open for the configured period of time.
- Keeping the gate open permanently on a second call/control command.
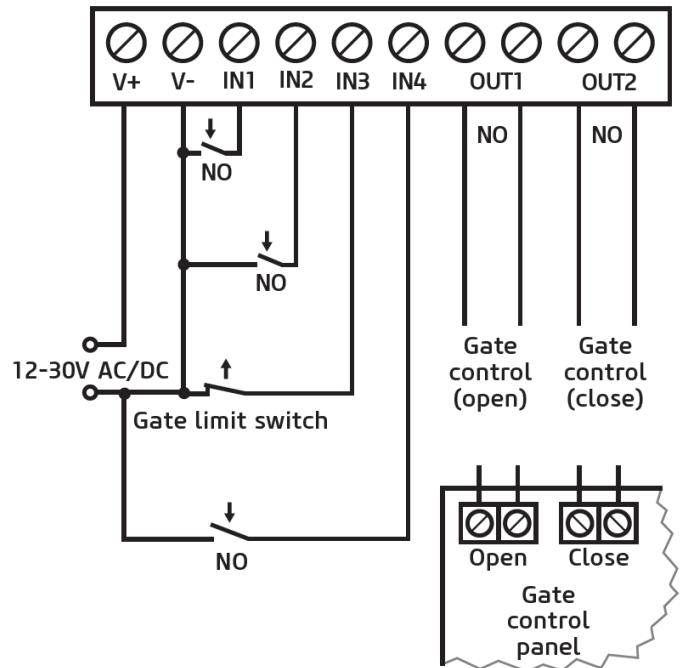- The gate position limit switch can be connected to input IN3.

**Wiring for one gate with photocell and position limit switch (control mode 3)**

8
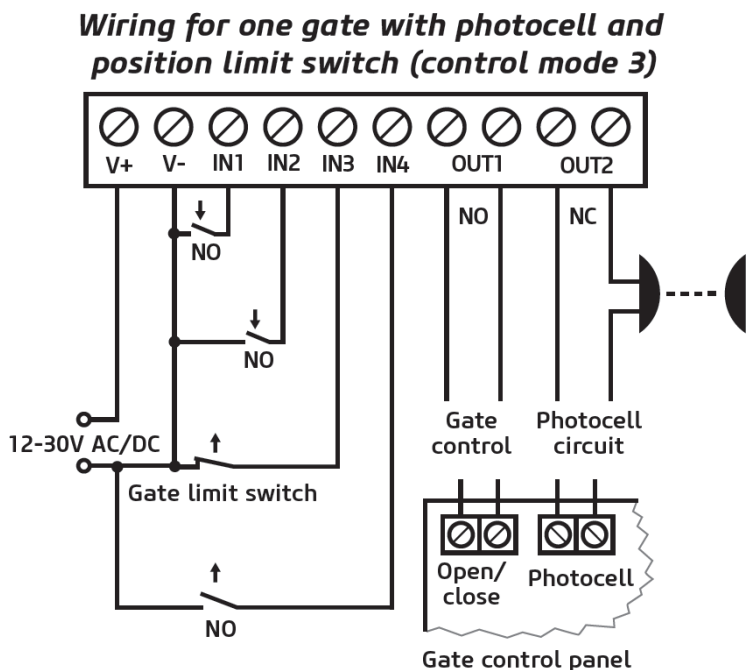
Control mode 4:

- For single-gate automations that require triggers for opening and closing on different inputs.
- Opening and then closing by a single call/control command.
- Both outputs are normally open (NO).
- The opening trigger is provided by output OUT1 and the closing trigger is provided by output OUT2.
- Keeping the gate open permanently on a second call/control command.
- The gate position limit switch can be connected to input IN3.

Control mode 5:

- For single-gate automations that require triggers for opening and closing on different inputs.
- Opening and then closing by separate calls/control commands.
- Both outputs are normally open (NO).
- The opening trigger is provided by output OUT1 and the closing trigger is provided by output OUT2.
- The gate position limit switch can be connected to input IN3.

Wiring for one gate with position limit switch (control modes 4 and 5)

9

3.5 SIM card holder

The SIM card holder can be accessed by removing the cover of the aperture found on the device enclosure. The cover can be removed by pressing it with your fingernail towards the status LED at the edge where the gap is, and then pulling it outwards. Insert the SIM card into the holder. The services to be activated on the SIM card installed into the *Gate Control PRO* device should be chosen according to which services of the device you wish to use. For usage with the mobile application and for the functions that use e-mail sending, mobile Internet service is necessary. The functions that use SMS sending need SMS service and the ones that use calls require GSM 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 GSM service provider.

- Installing the SIM card:
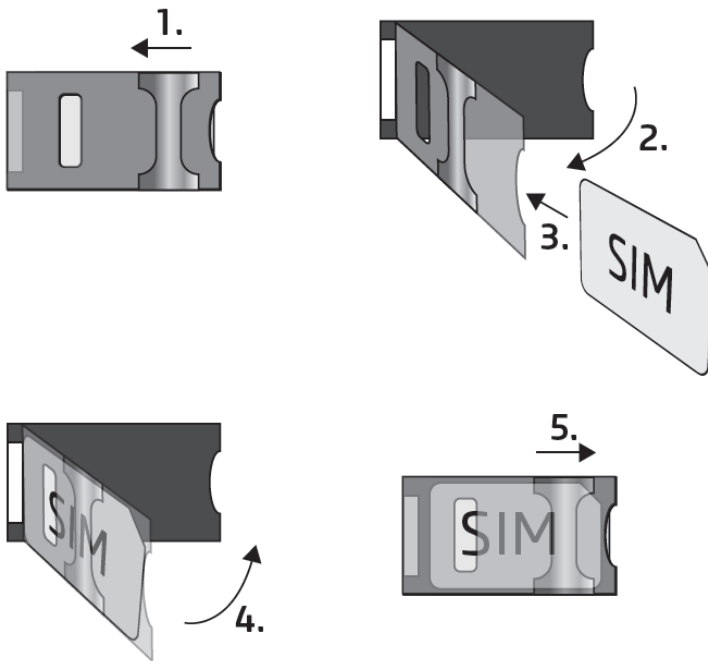
1. Pull the metal security lock of the SIM holder towards the LED until you hear a click.

2. Reach under the metallic security lock with your fingernail and pull it outwards to open the holder.

3. Slide the SIM card into the opened part with the contacts facing down, as shown in the figure.

4. Close back the opened part together with the SIM card.

5. Press down the metallic security lock carefully and pull it towards the side of the enclosure until you hear a click.

3.6 Connecting the antenna

Connect the GSM antenna to the FME-M 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 strength 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 high degree of humidity.

3.8 Putting into operation

- *Disable voicemail and notification in SMS about missed calls on the SIM card installed in the device.*
- *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 GSM 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 GSM service provider and enable the service in the menu, or visit one of the service provider's personal customer services and ask to enable this service on the SIM card.
- Make sure that the SIM card is installed correctly into the device.
- Make sure that the GSM antenna is connected correctly to the device.
- Make sure that the wires are connected correctly.
- You can now power up the device (12-30V AC/DC). Make sure that the power source provides sufficient power for the operation of the *Gate Control PRO* device. The nominal current consumption of the *Gate Control PRO* device is 120mA, however it may rise up 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. For such cases you can order an auxiliary power adapter separately from the manufacturer.
Attention! USB power is not sufficient to operate the device! The device will not turn on the modem, i.e. it will not connect to the GSM network if powered from USB only!

3.9 Status LED signals

Slowly flashing green	Normal operation, connected to the GSM network
Flashing red	GSM service unavailable or system startup/restart is in progress
Permanent red	SIM card error

3.10 Technical specification

Supply voltage range:	12…30V AC/DC
Nominal current consumption:	120mA
Highest current consumption:	500mA@12V DC, 250mA@24V DC
Operating temperature:	-20ºC - +70ºC
Transmission frequency:	
2G model:	850/900/1800/1900 MHz
3G model:	900/2100 MHz @UMTS, 900/1800 MHz @GSM
3GA model:	800/850/900/1900/2100 MHz @UMTS 850/900/1800/1900 MHz @GSM
Highest load supported on outputs:	1A@24V AC/DC
Dimensions:	84 x 72 x 32mm
Weight:	200g (packed: 300g)

4 Configuring the *Gate Control PRO* device

The *Gate Control PRO* device can be configured as follows:
- by computer via USB, using the programming software
- by computer over the Internet, using the programming software*
- by the mobile application over the Internet (only settings related to user management are available)*
  You can read more about configuring by the mobile application in the app's user's manual.

*The functions marked with * character are only available when a SIM card with mobile Internet access is installed in the *Gate Control PRO* device and the server access is configured correctly, i.e. if the device is online, connected to the cloud. If you wish 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*" and "*Cloud*" paragraphs found in the "*General*" device settings chapter.

The *Gate Control* programming software is compatible with the following operating systems:
- **Windows 10 (32/64 bit)**
- **Windows 8.x (32/64 bit)**
- **Windows 7 (32/64 bit)**

Installing the programming software: open the software setup application and follow the instructions of the installation wizard to complete the installation.
You can download the latest version of the programming software from the manufacturer's website (https://tell.hu/en/products/gsm-automation/gate-control-pro).

4.1 The user interface and configuration options of the software:

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

You can change the appearance (skin) of the user interface using the "*Skin*" 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.

4.2   Methods of connecting to the device

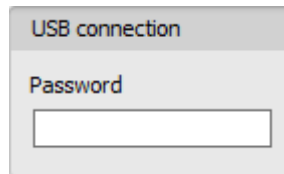For connecting to the device using the programming software, the following options are available:

USB: direct connection using a USB A-B 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-B 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 in order 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, download event logs, and view device status information.

- To close the connection, click on "**Disconnect**" 🔌 button.

4.2.2 Connecting to the device over the Internet

For connecting via the Internet, it is necessary that the *Gate Control PRO* device you wish to connect to uses the cloud service. For this, the APN settings should be configured and the "*Cloud usage*" option should be enabled in the "*General*" device settings menu, and it is also necessary to have installed 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 GSM service provider.

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 by super admin or admin users for whom remote access has been configured. For connecting remotely to the device, the user name 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 configured, you need to configure the remote access for the super admin or admin user for whom you wish 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. For adding a new user, follow the steps specified in the "***Users***" chapter. For configuring a new remote access, follow the steps specified in the "***Remote access***" chapter.

➢ **Remote access levels:**

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

With **Admin** role: can access everything except the settings in the following menus:
General, Customization, Inputs, Reporting channels, Input events, Outputs, Reports, IP cameras, Advanced settings.

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.

In order to make it easier to connect to a device remotely, the program includes a device register which enables you to add device availabilities 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**

Remote access					▼
Device name	Server address	Port	SIM identifier (ICCID)	User name	Password
▼	54.75.242.103	2016	8936303410171333468F		

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

Server address: the IP address of the cloud server (default: **54.75.242.103**).

Port: the port number of the cloud server (default: **2016**)

SIM-identifier (ICCID): the identifier of the SIM card installed in the *Gate Control PRO* device you want to connect to. You can first read and copy the SIM identifier of the given device in the "*SIM identifier*" field found in the "*Status monitoring*" menu, when connected via USB.

- Click on the "*Connection type*" menu and select the "*Cloud*" ☁ option.

- If you have already added the device availabilities in the device register, select the device you want to connect to from the "*Device name*" drop-down menu. Otherwise, enter the "*Server address*" and „*Port*" number of the cloud server, and the "*SIM identifier (ICCID)*" of the device.

- Enter the super admin (or admin) "*User name*" and the remote access "*Password*" configured for this.

- 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, download event logs, and view device status information.

- To close the connection, click on "*Disconnect*" ☁ button.

5 How to use the *Gate Control* programming software

5.1 Connection menu group

5.1.1 Viewing the settings options and configuring offline
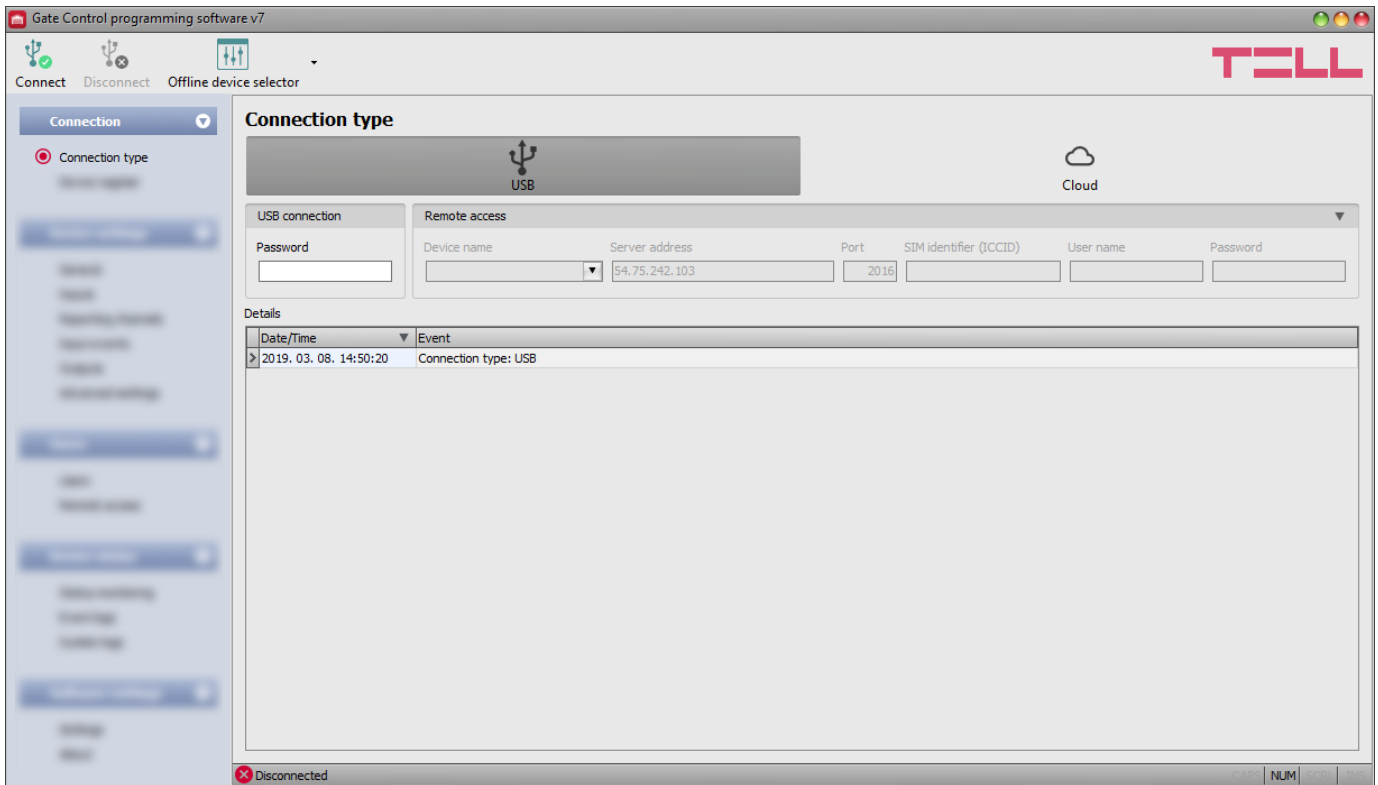
The **Gate Control** programming software supports all **Gate Control PRO** and **BASE** device models, therefore the software shows the settings options available specifically in a given device model, which are different from the common parameters (e.g. differences between the **PRO** and the **BASE**, or device models with a different user capacity) only when the given device model is connected, i.e. a **Gate Control PRO** 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 PRO** device and to configure and save the settings in advance offline, without connecting the device.

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

"**Offline device selector**" button, select the desired device model from the drop-down

menu and then click on the "**Offline device selector**" button to load the settings options of the selected device model.

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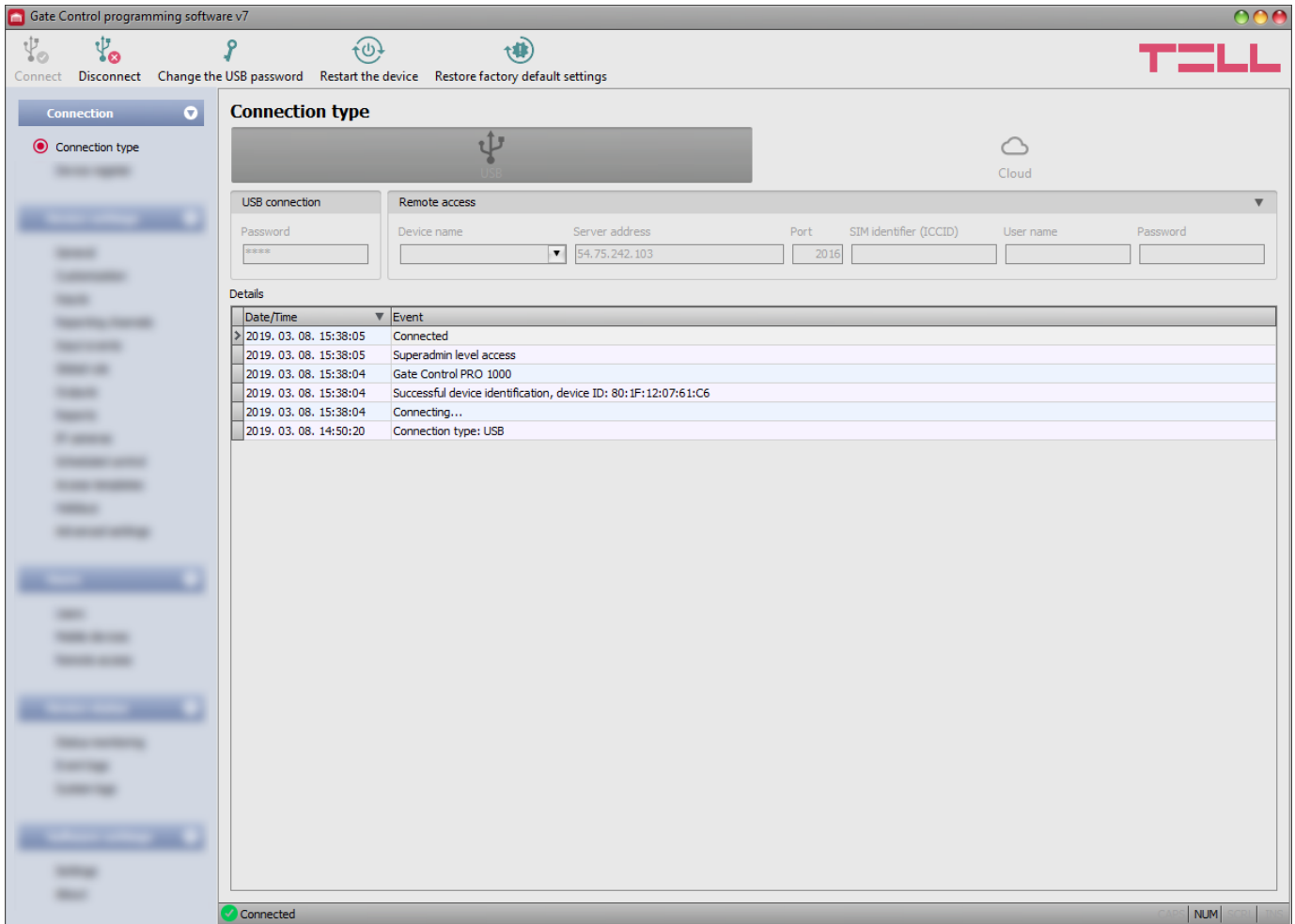
In the "**Connection type**" menu you can select the method of connecting to the device (USB or cloud), view information about the connection process, change the device's USB password, restart the device, and restore the factory default settings in the device.
The default USB password is **1234**.

Available options:

- Changing the USB password:

  🔑 You can change the USB password of the device after clicking on this button.

Enter the actual USB password, then the new password, confirm the new password, and then click on the "**OK**" button. The password should consist of at least 4, but not more than 8 characters. Accepted characters are: numbers (0...9), lower case letters (a...z), and capital letters (A...Z).
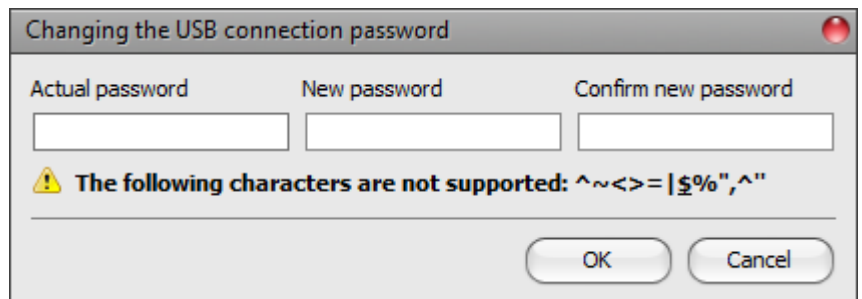
Attention! The following characters should not be used: ^ ~ < > = ' " , | $ & %

- Restart the device:

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

- Restore 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 starts working again. The option of restoring the factory default settings is also available without entering the USB password of the device. Factory reset can also be performed using the microswitch found on the hardware. Further details you can find in chapter "***Restoring the factory default settings***".

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.

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

5.1.3 Device register
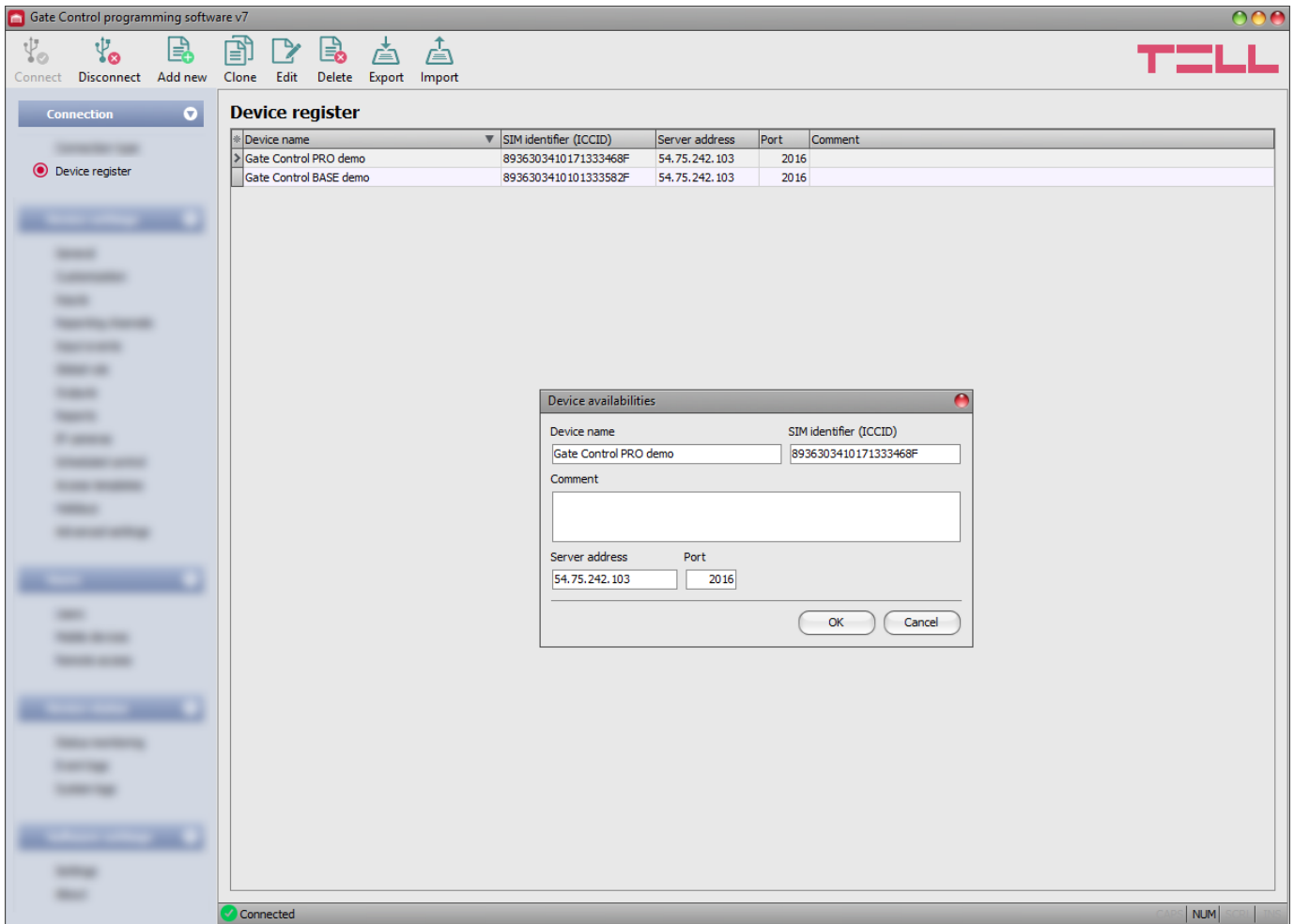
The device register serves for storing and easy management of **Gate Control PRO** and **BASE** device availabilities used for remote access. You can add new device availabilities to the database and also edit, delete and clone entries for easy adding devices with similar availabilities.

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.

If you enter a new device availability in the connection type section, the program will add it automatically to the device register database using the SIM identifier as device name, which you can then change by editing the given entry. The program stores the device register database locally on the computer.

Available options:

- Add new device availability:

    Click on the "***New***" button to add a new device availability.

- Copy an existing device availability:

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

- Edit an existing device availability:

    To edit the selected device availability, click on the "***Edit***" button.

- Delete a device availability:

    To delete the selected device availability, click on the "***Delete***" button.

- Export the database:

    To save the device register database to file, click on the "***Export***" button.

- Import a database:

    To import a saved device register database from file, click on the "***Import***" button.

Data stored by the device register:

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

Server address: the IP address of the cloud server.

Port: the communication port number of the cloud server.

SIM identifier (ICCID): the identifier of the SIM card installed in the device. If the device is connected via USB and the SIM card is installed, the program will read the identifier from the device and will paste it in this box when you add a new device availability.

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

5.2   Device settings menu group

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

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

- **Changing the device settings**: In order to change the device settings, first please read the actual settings from the device by clicking on the "***Read settings***" button in any submenu. Writing the settings into the device using the "***Write settings***" button is not possible until the settings are read. After making changes in the settings, write the settings into the device by clicking on the "***Write settings***" button.

- **Overwriting the full device configuration (device settings, users, mobile devices, and remote access entries)**: If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users and the settings in the submenus, and then click on the "***Create system backup***" button in the "***General***" device settings menu. You can import the saved backup into the program using the "***Restore from backup***" button, and then write imported settings into the device by category, using the "***Write settings***" and the "***Write users***" buttons.

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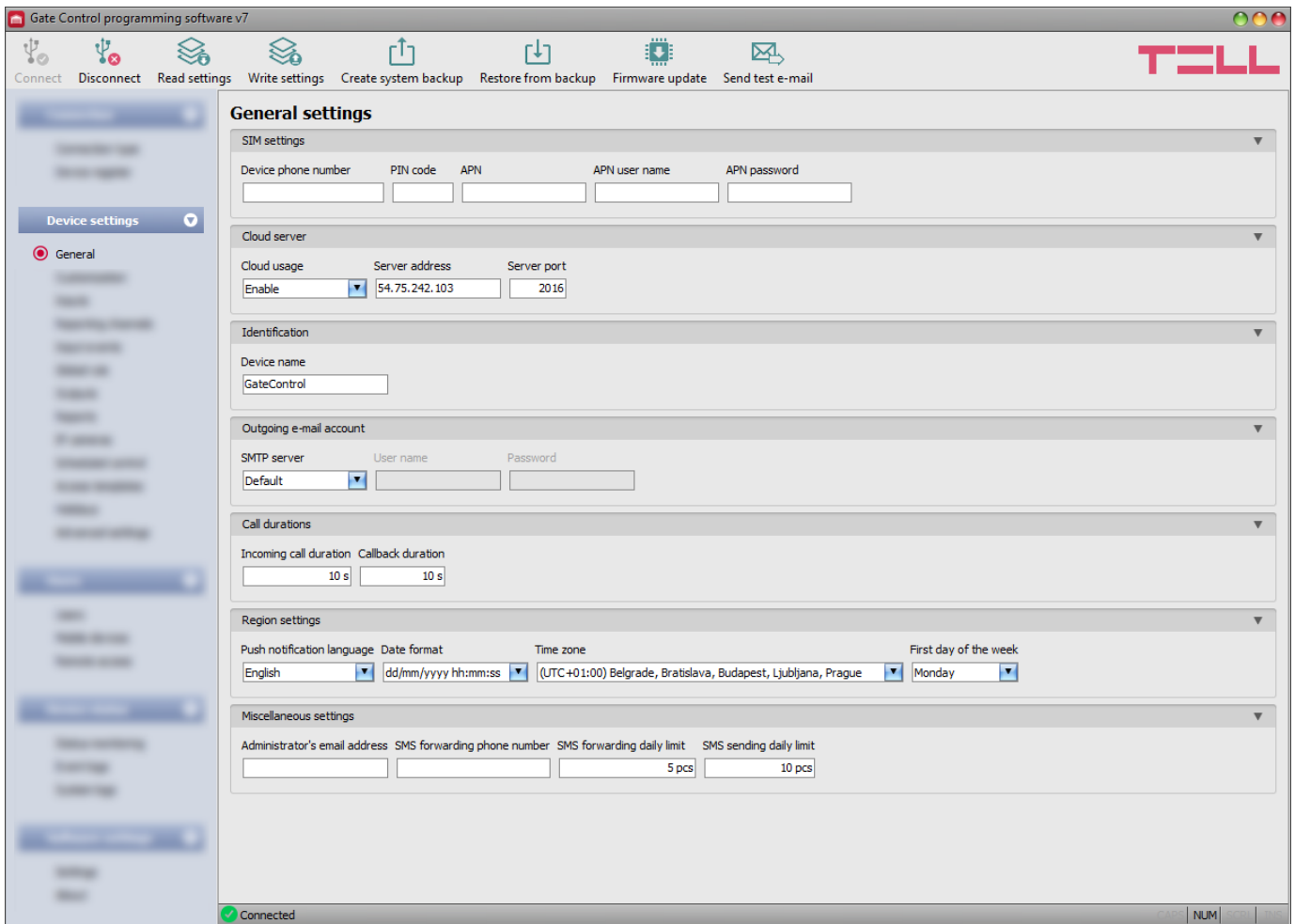
In this menu you can configure the parameters related to the general operation of the device.

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, in order 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.

- 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 with the new firmware.

- Sending a test e-mail:

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

Please note that you have to write the settings into the device in order to be applied after a change is made. 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 PRO* device. The system will use this in the mobile application to control the gate by a backup GSM call if a problem occurs with the mobile Internet connection when you wish to control a gate.

PIN code: if you want to lock the SIM card with a PIN code, enter in this section the PIN code of the SIM card installed in the device and enable PIN code request on the SIM card using a cellphone. Otherwise disable PIN code request on the SIM card. If the wrong PIN code has been entered, the device will try the code only once each time the code is changed in the settings, and "PIN code error" message will be shown in the system logs. 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: the APN (access point name) necessary for connecting to the Internet. Ask this from the GSM service provider of the SIM card installed in the device. If no APN is configured, the device will not try to connect to the Internet. If you want to use the Internet based functions of the device, it is necessary to configure the APN and use a SIM card with available mobile Internet service in the *Gate Control PRO* device.

APN user name: necessary only if the GSM service provider provides this and requires its usage for the given APN.

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

Cloud:

Cloud usage: the system can be configured to connect to the Internet and stay online continuously, or to connect only occasionally, when needed. If this option is enabled, the device will connect to the cloud server operated by the manufacturer and will stay connected continuously. For using the Internet based online services of the system, continuous mobile Internet connection is needed, which results in larger data traffic.
If you enable cloud usage, the following services will be available:
- **mobile application usage**
- **remote access, remote programming**
- **remote firmware update,**

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

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

Attention! If you are using the device model equipped with a 2G modem, or the device is connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, the services mentioned above that require Internet connection, will be suspended for the duration of the call. Functions that make outgoing calls:

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

Server address: the IP address of the cloud server (default IP: **54.75.242.103**)

Server port: the port number of the cloud server (default port: **2016**)

Identification:

Device name: here you can enter a custom name for your **Gate Control PRO** device. This name will also be used in reports.
Attention! The following characters should not be used: ^ ~ < > = ' " , | $ & %

Outgoing e-mail account:

The system uses by default the SMTP server provided by the cloud service for sending e-mails, but it offers an option to configure your own Gmail account.

SMTP server:

- **Default**: the system will use the SMTP server provided by the cloud service for sending e-mails. In this case, notification and report e-mails will be sent from the following e-mail address: noreply.gatecontrol@devicemail.net

- **Gmail account**: with this option you can configure a Gmail account to be used by the system for sending e-mails. In this case, the system will send notification and report e-mails from the e-mail address of the configured Gmail account.

User name: the Gmail account's user name.

Password: the Gmail account's password.

When you have finished configuring this option, use the "**Send test e-mail**" button to send a test e-mail and make sure that the e-mail sending function is operational. Using the e-mail sending functions requires mobile Internet service.

Call durations:

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

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

Region settings:

Push notification language: using the drop-down menu you can select the language for Push notification messages sent by the system to the registered mobile devices. If you change this setting, in order to take effect you need to restart the device.

Date format: using the drop-down menu you can select the date format used by the system in the event logs, in the system logs, and for the timestamp in notifications:
- yyyy.mm.dd. hh:mm:ss
- dd/mm/yyyy hh:mm:ss

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

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

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

Miscellaneous settings:

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

SMS forwarding phone number: the system can forward messages received on the SIM card installed in the device to the phone number specified here (e.g. balance information received from the GSM 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. In case of entering value "0", SMS forwarding will be disabled, i.e. incoming SMS messages will not be forwarded, but deleted automatically. 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 generate by inputs for 24 hours. After 24 hours, the counter resets automatically and message sending will be enabled again up to the configured limit. In case of entering value "0", input-generated SMS sending will be disabled. The SMS sending daily limit can be disabled and set to unlimited by deleting the entered value.
Attention! Messages generated after reaching the configured limit, but still before the message counter is reset will neither be sent subsequently, but the system records the events in the event logs.

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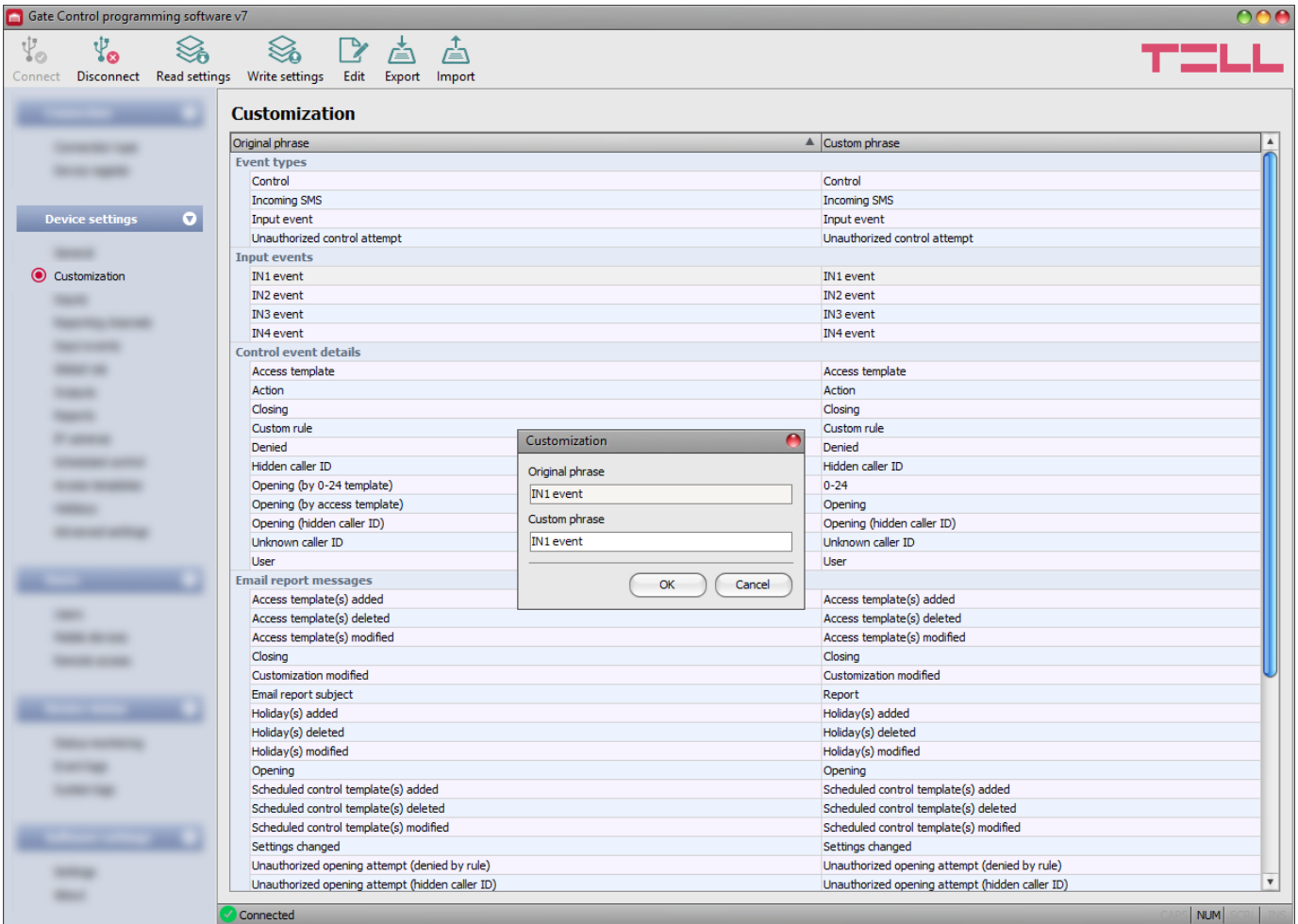
In this menu you can change default text elements and phrases used in the event logs, e-mail messages, and certain Push and SMS messages. The phrases which you can change are listed in the "**Custom phrase**" column.

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

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

Available options:

- Reading the settings from the device:

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

- Writing the settings into the device:

  After changing the settings or entering new settings, in order 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 entry:

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

- Export entries:

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

- Import entries:

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

Please note that you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

The manufacturer provides the default English, German, Czech and Hungarian set of words for the customization function, which you can find in the "**Localization**" folder of the program installation directory under the following file names: "**GC_Customization_V7_EN.csv**", "**GC_Personalisierung_V7_DE.csv**", "**GC_Prizpusobeni_V7_CZ.csv**" and "**GC_szemelyre_szabas_V7_HU.csv**". If you want to replace the actual set of words used by the device, read the settings from the device using the "**Read settings**" button, click on the "**Import**" button, browse and select one of the mentioned language files, and then write the changes into the device using the "**Write settings**" button.

5.2.3 Inputs
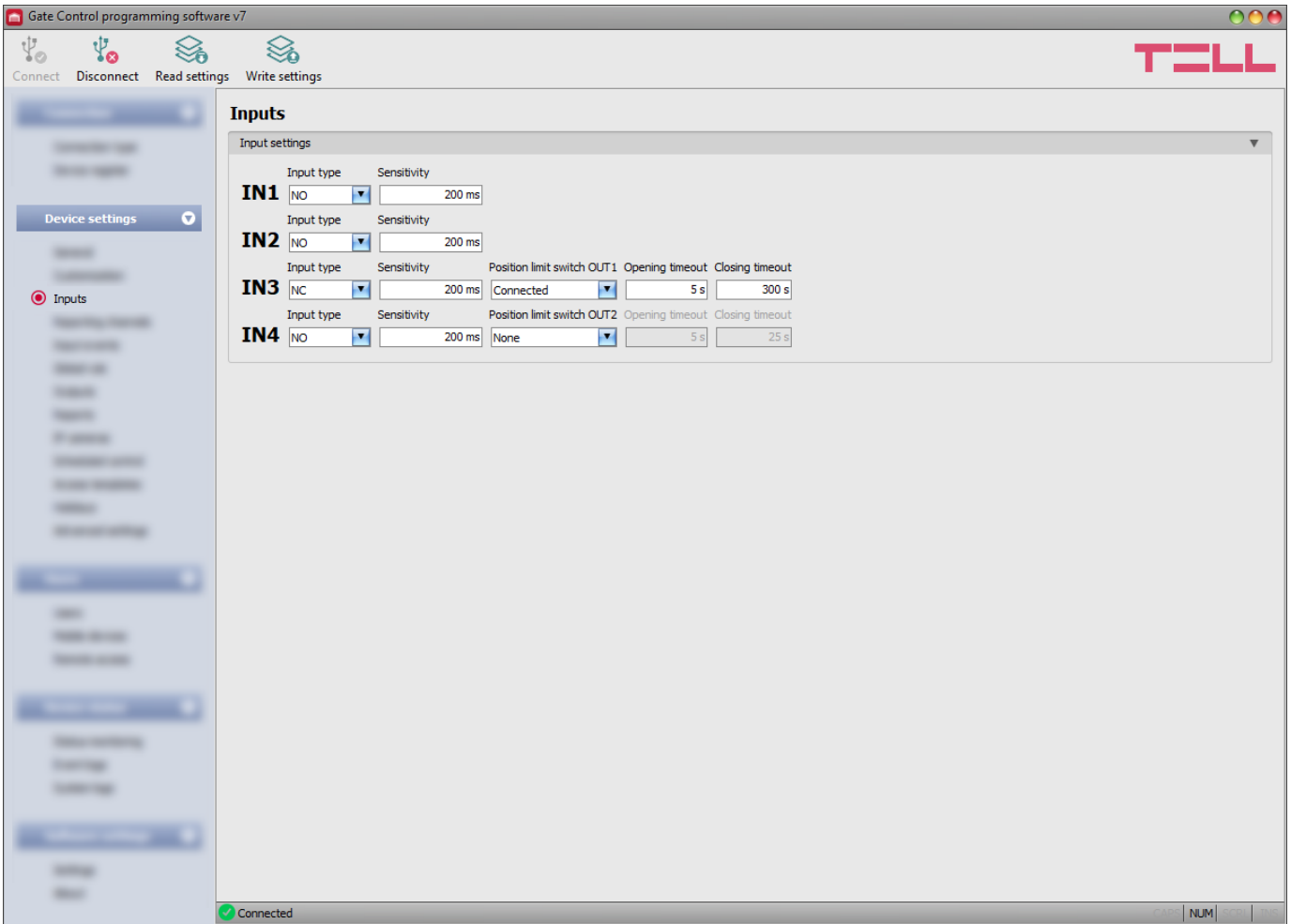
In this menu you can configure the properties and options of the IN1…IN4 contact inputs. When the contact inputs are triggered, the system generates input events. You can configure notifications for each input event in the "**Input events**" menu, which will be sent to the phone numbers and/or e-mail addresses configured in the "**Reporting channels**" menu.

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, in order 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 you have to write the settings into the device in order to be applied after a change is made. 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 „V-" terminal (DC power negative).

27

Special input functions available when using the system with the mobile application:

IN1: doorbell notification function (via Push message)

IN2: technical error notification function (via Push message)

IN3: gate position limit error notification (via Push message) on gate controlled by output OUT1

IN4: gate position limit error notification (via Push message) on gate controlled by output OUT2

You can learn more about these functions in the „*__Operation of the contact inputs__*" paragraph.

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

Position limit switch OUT1: enabling the gate position limit switch connected to input IN3, installed on the gate controlled by output OUT1. If the gate position limit switch is connected, the device monitors if the gate opens within the time interval configured in the "*__Opening timeout__*" section, and if it closes within the time interval configured in the "*__Closing timeout__*" section. If the gate fails to open or close within the configured intervals, the device sends notifications via Push message and/or SMS, according to the settings. You can change the text of these notifications in the "*__Customization__*" menu, if needed. The system considers the idle state of the position limit switch as the closed state of the gate. In case of NO (normally open) wiring, the open state, while for NC (normally closed) wiring the closed state of the position limit switch is considered as the idle state.
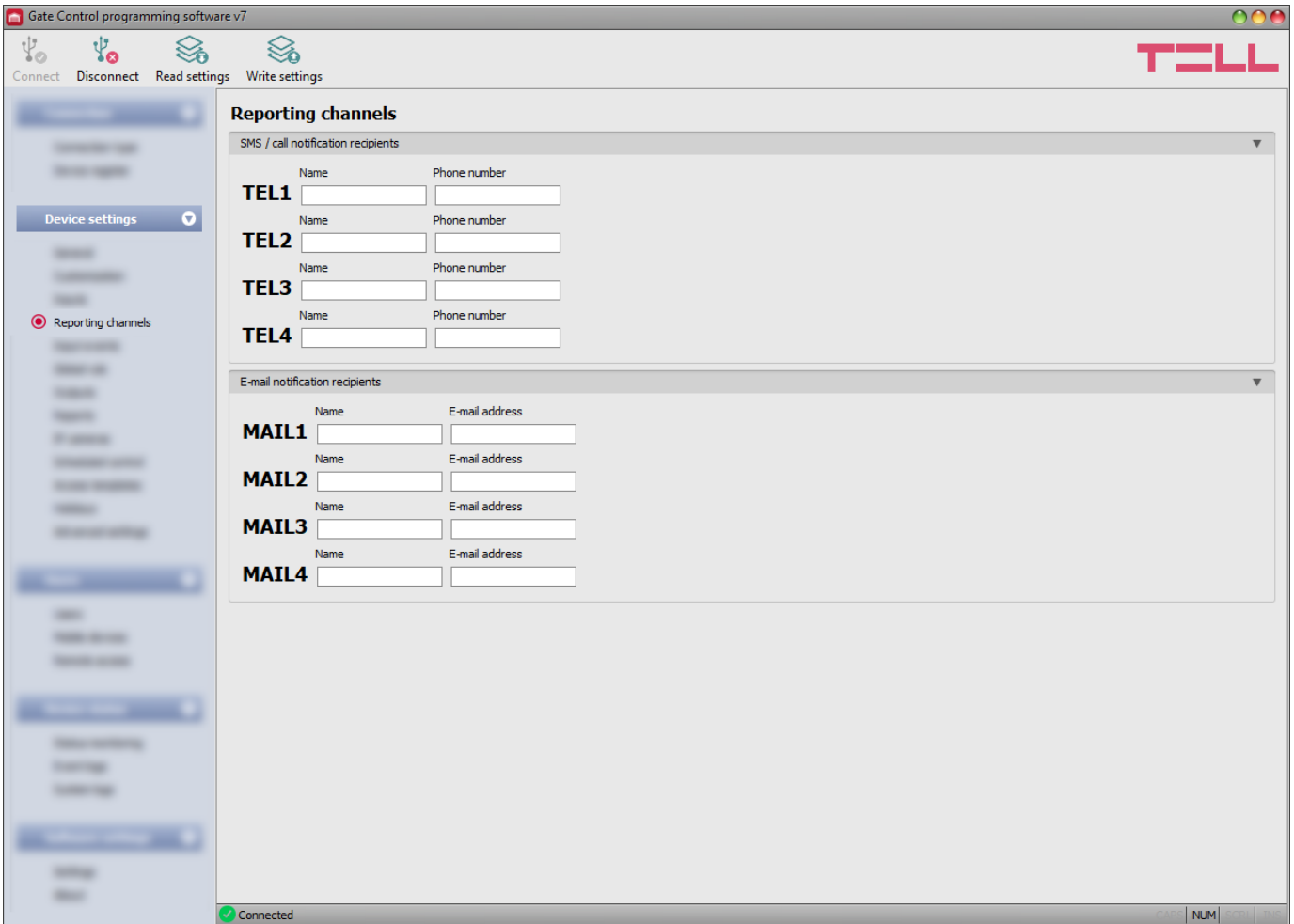
Available options:
-   **None**: there is no position limit switch connected to input IN3
-   **Connected**: the position limit switch is connected to input IN3

Position limit switch OUT2: enabling the gate position limit switch connected to input IN4, installed on the gate controlled by output OUT2. This option is only available for control modes 1 and 2, for connecting the position limit switch of the second gate. If the gate position limit switch is connected, the device monitors if the gate opens within the time interval configured in the "*__Opening timeout__*" section, and if it closes within the time interval configured in the "*__Closing timeout__*" section. If the gate fails to open or close within the configured intervals, the device sends notifications via Push message and/or SMS, according to the settings. You can change the text of these notifications in the "*__Customization__*" menu, if needed. In case of NO (normally open) wiring, the open state, while for NC (normally closed) wiring the closed state of the position limit switch is considered as the idle state.

Available options:
-   **None**: there is no position limit switch connected to input IN4
-   **Connected**: the position limit switch is connected to input IN4

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

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

5.2.4 Reporting channels

In this menu you can configure the telephone and e-mail availabilities, 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, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

29

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 you are using the device model equipped with a 2G modem, or the device is connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call.

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.

E-mail notification recipients:

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

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

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

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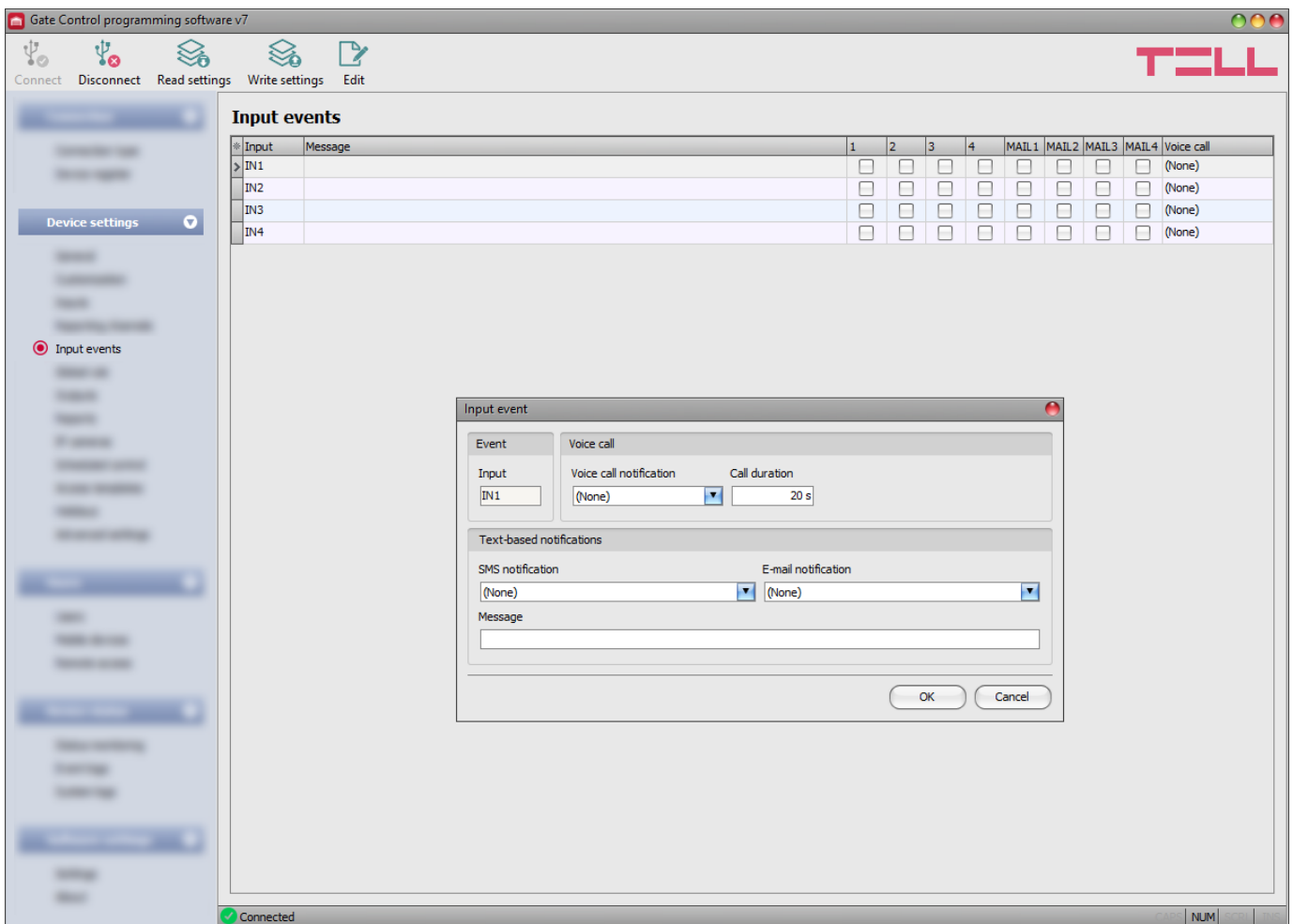
In this menu you can configure SMS, e-mail and voice call notifications to be sent upon activating the contact inputs **IN1**…**IN4**..

Available options:

- Reading the settings from the device:

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

- Writing the settings into the device:

  After changing the settings or entering new settings, in order 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 you have to write the settings into the device in order to be applied after a change is made. 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. <u>This function only serves to ring a phone number upon activating an input, thus the notification will be of charge if the called person does not accept or rejects the call.</u> 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 you are using the device model equipped with a 2G modem, or the device is connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call.

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

Text-based notifications:

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

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

Message: in this field you can enter a custom message of maximum 45 characters, which you want to be sent to the selected phone numbers and e-mail recipients, when the given event occurs. The device will send the same message for both types of notification (SMS and e-mail).

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

5.2.6 Global rule
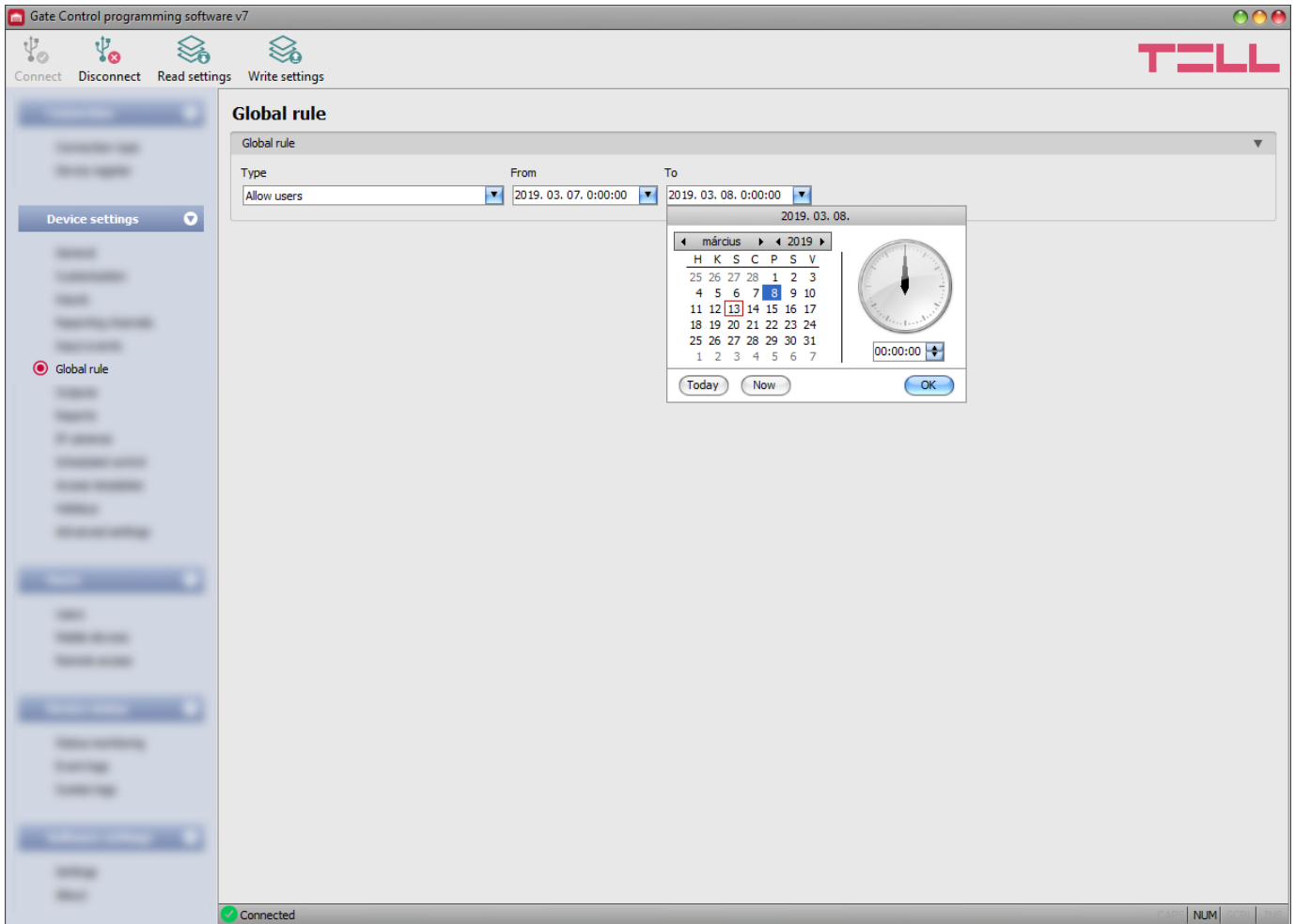
The global rule assures an option for easy overriding of control permissions and entry periods defined by configured access templates. The global rule has no effect on custom rules configured for users. Custom rules remain in effect independently from the global rule settings.

Available options:

- Reading the settings from the device:
  To read the settings from the device click on the "***Read settings***" button. This will read all settings in all menus in the "***Device settings***" menu group.

- Writing the settings into the device:
  After changing the settings or entering new settings, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

Global rule:

Type:

None: when this option is selected, control permissions are considered according to the configured access templates, holidays and user custom rules.

Allow users: when this option is selected, the system allows solely registered users to control the system, and ignores any configured access templates and holidays. Users may control the system using the mobile application or by call, if they send their caller ID (or either hide the caller ID in case of using control mode 1).

Allow everyone with caller identification: when this option is selected, the system allows anyone (unregistered users as well) to control the system with caller identification, and ignores any configured access templates and holidays. Anyone who sends the caller ID may control the system by call. When a call with a hidden caller ID is received, the control attempt will be rejected, except when controlling output OUT2 in control mode 1. Users may still control the system using the mobile application.

Allow everyone: when this option is selected, the system allows anyone (unregistered users as well) to control the system, and ignores any configured access templates and holidays. Anyone may control the system whether it sends the caller ID or calls with hidden caller ID, for any of the control modes. Users may still control the system using the mobile application.

Deny: when this option is selected, the system rejects all control attempts, except for users with a configured custom rule that grants them permission for control.

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

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

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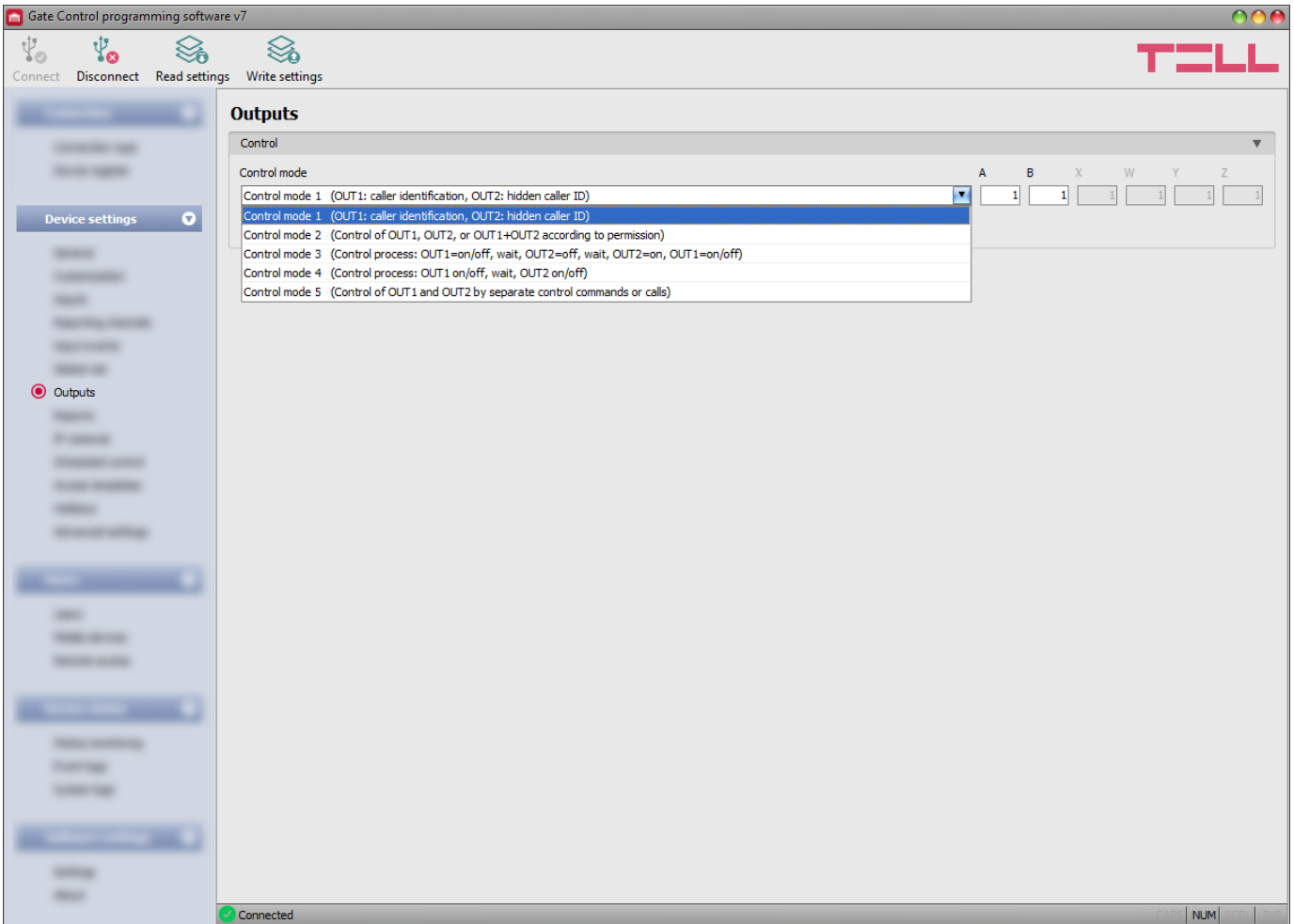
In this menu you can configure how outputs OUT1 and OUT2 should operate when controlled. The operation mode of the outputs can be configured by selecting a control mode. You can choose out of five control modes for compatibility with various control boards of different gates. Choose the control mode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

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, in order 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.

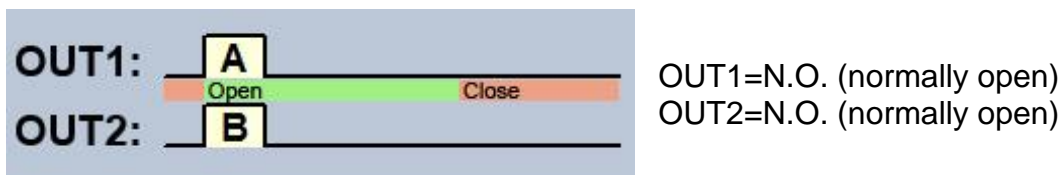**Please note that you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.**

Control:

Control mode:

Control mode 1

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

OUT1: A Open Close
OUT2: B

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

A = OUT1 impulse length (seconds) => for opening gate A
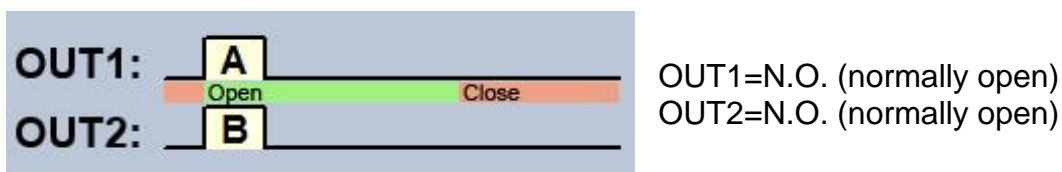**B** = OUT2 impulse length (seconds) => for opening gate B

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

Selective control of outputs OUT1 and OUT2 by using caller identification and hidden caller ID. If the caller sends the caller ID, output OUT1 will be activated. If the caller hides the caller ID, output OUT2 will be activated, which also allows for controlling two different gates by call, by using this control mode. 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#+3630….). 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. +3630…. and #31#+3630…). The outputs provide an open contact by default and they become closed upon control. The trigger impulse length of output OUT1 can be configured by parameter "**A**", while the trigger impulse 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! <u>Anyone</u> 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 two gates or one gate with two opening options (partial/total opening).

OUT1: A Open Close
OUT2: B

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

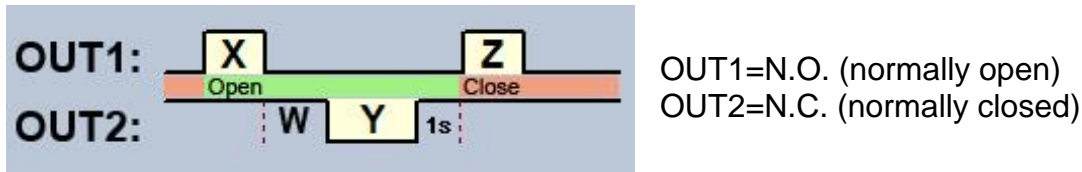**A** = OUT1 impulse length (seconds) => for opening gate A
B = OUT2 impulse length (seconds) => for opening gate B

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

Selective or simultaneous control of outputs OUT1 and OUT2 using caller identification, based on configured user permissions. Permissions can be configured for each user separately, to activate output OUT1 only, output OUT2 only, or both outputs at the same time upon control. Thereby, this control mode enables you to control two different gates. The outputs provide an open contact by default and they become closed upon control. The trigger impulse length of output OUT1 can be configured by parameter "**A**", while the trigger impulse 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=N.O. (normally open)
OUT2=N.C. (normally closed)

X = OUT1 impulse length (seconds) => for gate opening
W = delay before interrupting the infrared photocell loop (seconds)
Y = OUT2 impulse length (seconds) => for keeping the gate locked in open state
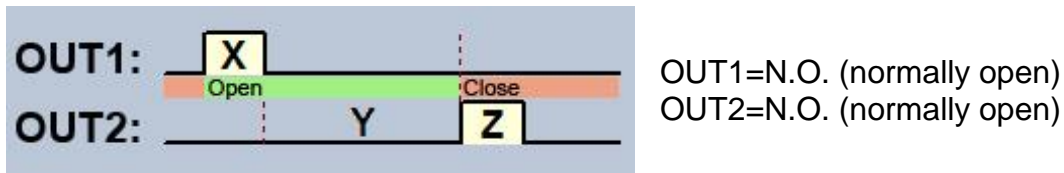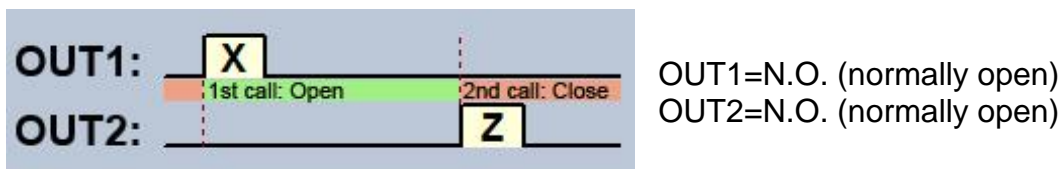**Z** = OUT1 impulse length (seconds) => for gate closing

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. Upon controlling the device, output OUT1 gives a closed contact for **X** seconds, then after **W** seconds output OUT2 gives an open contact for **Y** seconds, then after 1 second output OUT1 gives again a closed contact 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 impulse opens the gate, the second one closes it). The opening and closing trigger impulses are provided by OUT1, while inserting the OUT2 contact in the loop of the infrared photocell, it keeps 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 impulse. In this case you should set parameter **Z** to 0 seconds, thus there will not be a gate closing trigger impulse. 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**).

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

Control mode 4

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

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

X = OUT1 impulse length (seconds) => for gate opening
Y = keeping the gate open (seconds) => for keeping the gate locked in open state
Z = OUT2 impulse length (seconds) => for gate closing

Starting a process of opening and closing by a single call/control command, using caller identification. In idle state, outputs OUT1 and OUT2 provide an open contact. Upon controlling the device, output OUT1 gives a closed contact for **X** seconds, then after **Y** seconds output OUT2 gives a closed contact 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 impulse on an input opens the gate, another trigger impulse on a different input closes the gate).

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

Control mode 5

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

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

X = OUT1 impulse length (seconds) => for gate opening
Z = OUT2 impulse length (seconds) => for gate closing

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

Opening and closing by separate calls/control commands. In idle state, outputs OUT1 and OUT2 provide an open contact. Output OUT1 gives a closed contact for **X** seconds upon the first control command/call, then upon the second control command/call from the same user output OUT2 gives a closed contact for **Z** seconds. You can use this control mode if the gate automation control board requires triggers for opening and closing on the same input or on two different inputs. If opening and closing control is done on the same input, outputs OUT1 and OUT2 should be connected in parallel to the input to be controlled. This control mode cannot be used with hidden caller ID.

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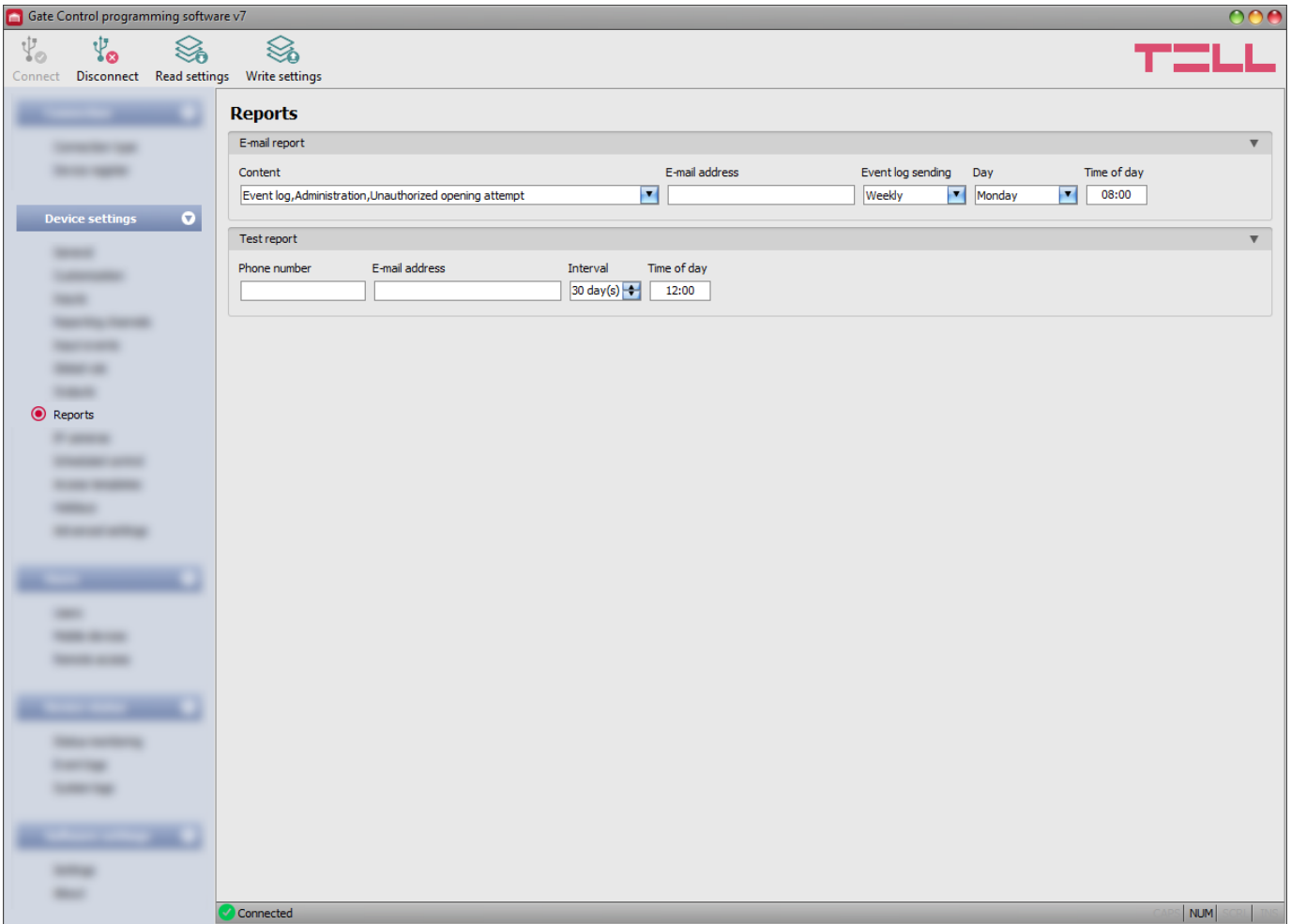
In this menu you can configure available reports which the system can send by e-mail or SMS.

Available options:

- Reading the settings from the device:
  To read the settings from the device click on the "**Read settings**" button. This will read all settings in all menus in the "**Device settings**" menu group.

- Writing the settings into the device:
  After changing the settings or entering new settings, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

E-mail reports:

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

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

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

E-mail address: enter the e-mail address where the selected reports should be sent. You can enter multiple addresses separated by comma.

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

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

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

Test report:

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

Phone number: enter the phone number to which test reports should be sent by SMS.

E-mail address: enter the e-mail address to which test reports should be sent by e-mail. You can enter multiple e-mail addresses separated by comma. The e-mail sending function requires mobile Internet service.

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

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

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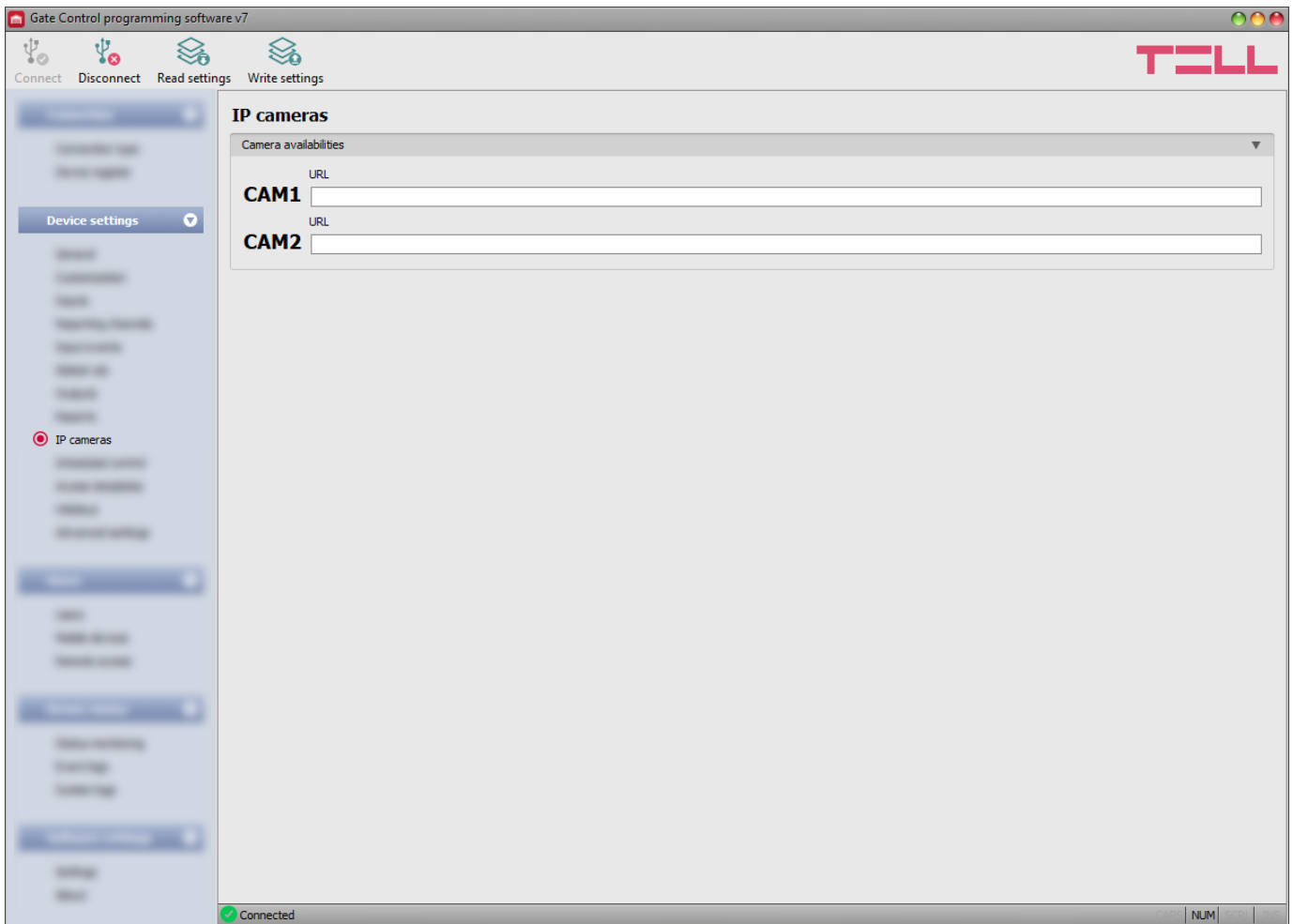
You can configure in the **Gate Control PRO** system the availabilities of up to 2 IP cameras which support the ONVIF standard. The system makes available the pictures of the configured IP cameras in the mobile application. Permission for viewing the camera pictures can be configured for each user and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

Available options:

- Reading the settings from the device:

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

- Writing the settings into the device:

  After changing the settings or entering new settings, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "Write settings" button.

Camera availabilities:

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

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

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

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

Example for modification of the stream URL, if only one camera is used:
Original URL:
rtsp://192.168.1.240:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a static IP address:
rtsp://*WAN IP*:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a static IP address and username/password:
rtsp://*username:password@WAN IP*:554/cam/realmonitor?channel=1&subtype….

Modified URL in case of using a domain name:
rtsp://*domain name*:554/cam/realmonitor?channel=1&subtype=0&unicast=true&proto=Onvif

Modified URL in case of using a domain name and username/password:
rtsp://*username:password@domain name*:554/cam/realmonitor?channel=1&subtype….

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

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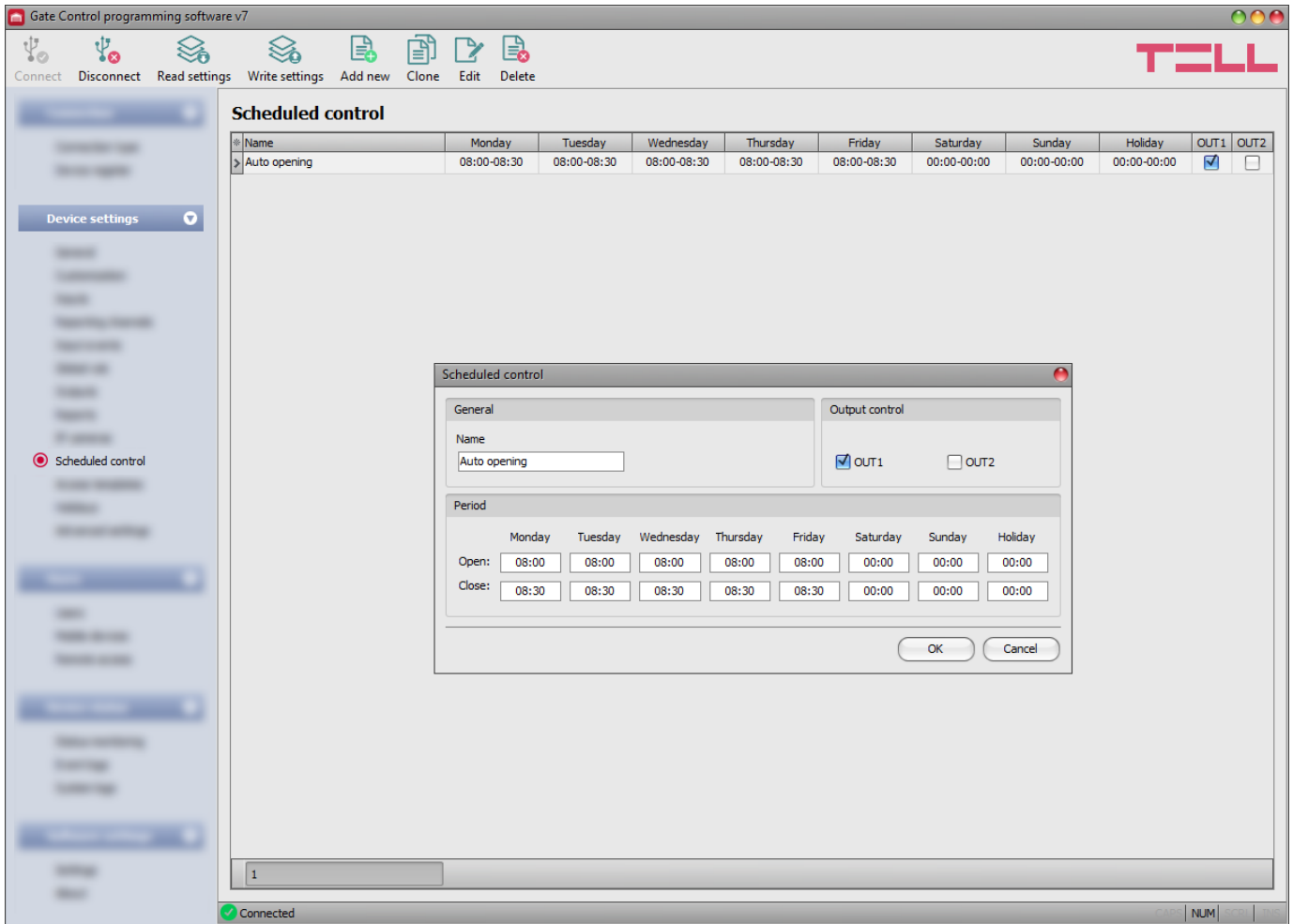
The scheduled control function is used to control the outputs automatically at the configured time of day. The time of control can be configured in control templates. This function is useful when it is needed to open the gate automatically at certain times of day and keep it locked in open state for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

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

- in case of using control mode 1 or 2, output OUT1 and output OUT2 give a permanent closed contact during the interval between the time configured at "*Open*" and "*Close*" options. The scheduled control function can be used with these control modes for example with gate automations which keep the gate locked in open state while the controlling signal (closed contact) is present on their control input. In the "*Output control*" section, you can configure which output to be controlled by the scheduled control function (output OUT1, OUT2 or both at the same time).

- in case of using control mode 3, output OUT1 gives a closed contact for **X** seconds at the time configured at the "*Open*" option, then after **W** seconds (gate opening interval) output OUT2 gives a permanent open contact, that interrupts the photocell loop and keeps the gate locked in open state till the time configured at the "*Close*" option, when output OUT1 gives a closed contact again for **Z** seconds.

- for control modes 4 and 5, output OUT1 gives a closed contact for **X** seconds at the time configured at "*Open*" option, then output OUT2 gives a closed contact for **Z** seconds at the time configured at "*Close*" option.

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

If the gate's position limit switch is connected to the device, the device will monitor if the gate opens and closes at the configured times of day. If opening or closing fails, the device sends notification about the gate position limit error by Push notification and/or SMS, according to the settings, and for control modes 3, 4 and 5 it repeats the opening or closing trigger impulse by 1 minute, i.e. it keeps trying to open or close the gate. The opening trigger impulse is repeated by 1 minute until the gate opens, i.e. opening is confirmed by the position limit switch, but up to the closing time configured in the given control template. The closing trigger impulse is repeated by 1 minute until the gate closes, i.e. closing is confirmed by the position limit switch, but up to the next daily device restart or power loss. The device sends the gate position limit error notification by SMS only once, while if the error still persists, by Push notification it is resent upon each opening or closing attempt, i.e. by 1 minute, but up to 3 messages only.

Available options:

- Reading the settings from the device:
  To read the settings from the device click on the "*Read settings*" button. This will read all settings in all menus in the "*Device settings*" menu group.

- Writing the settings into the device:
  After changing the settings or entering new settings, in order 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.

- Add a new scheduled control template:
  Click on the "*New*" button to add a new scheduled control template.

- Copy an existing scheduled control template:
  To create a copy of the selected scheduled control template, click on the "*Clone*" button. Please note that the new copy should have a different unique name.

- Edit an existing scheduled control template:
  To edit the selected scheduled control template, click on the "*Edit*" button.

- Delete a scheduled control template:
  To delete the selected scheduled control template, click on the "*Delete*" button.

Please note that you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

General:

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

Output control:

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

Period:

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

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

➢ **Creating a new scheduled control template:**

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

The system allows for adding up to 20 scheduled control templates.
If you wish to disable scheduled control of the outputs for a certain day, then enter value **00:00** into both time fields ("***Open***" and "***Close***") for the given day. In the "***Holiday***" section you can configure the scheduled control period for holidays. The holidays can be configured in the "***Holidays***" menu for several years in advance.

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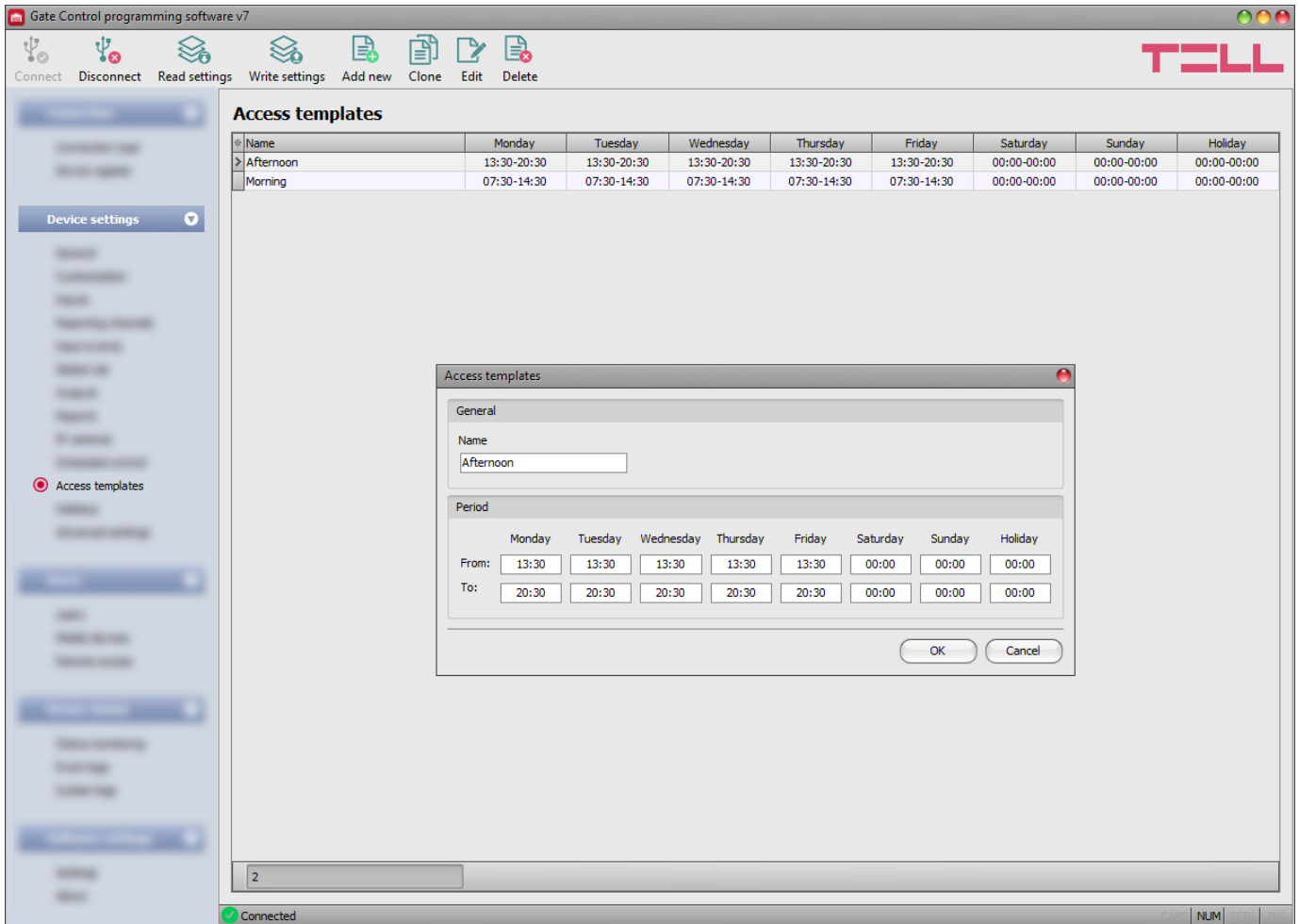
The access templates are used to configure the allowed entry period for users. You can associate any of the created access templates, even more of them, with any user in the "*Users*" menu, thus the periods (even more intervals a day) can be defined for each user when they are allowed to control the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

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, in order 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.

45

- Add a new access template:

  Click on the "**New**" button to add a new access template.

- Copy an existing access template:

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

- Edit an existing access template:

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

- Delete an access template:

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

Please note that you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

General:

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

Period:

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

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

➢ **Creating an access template:**

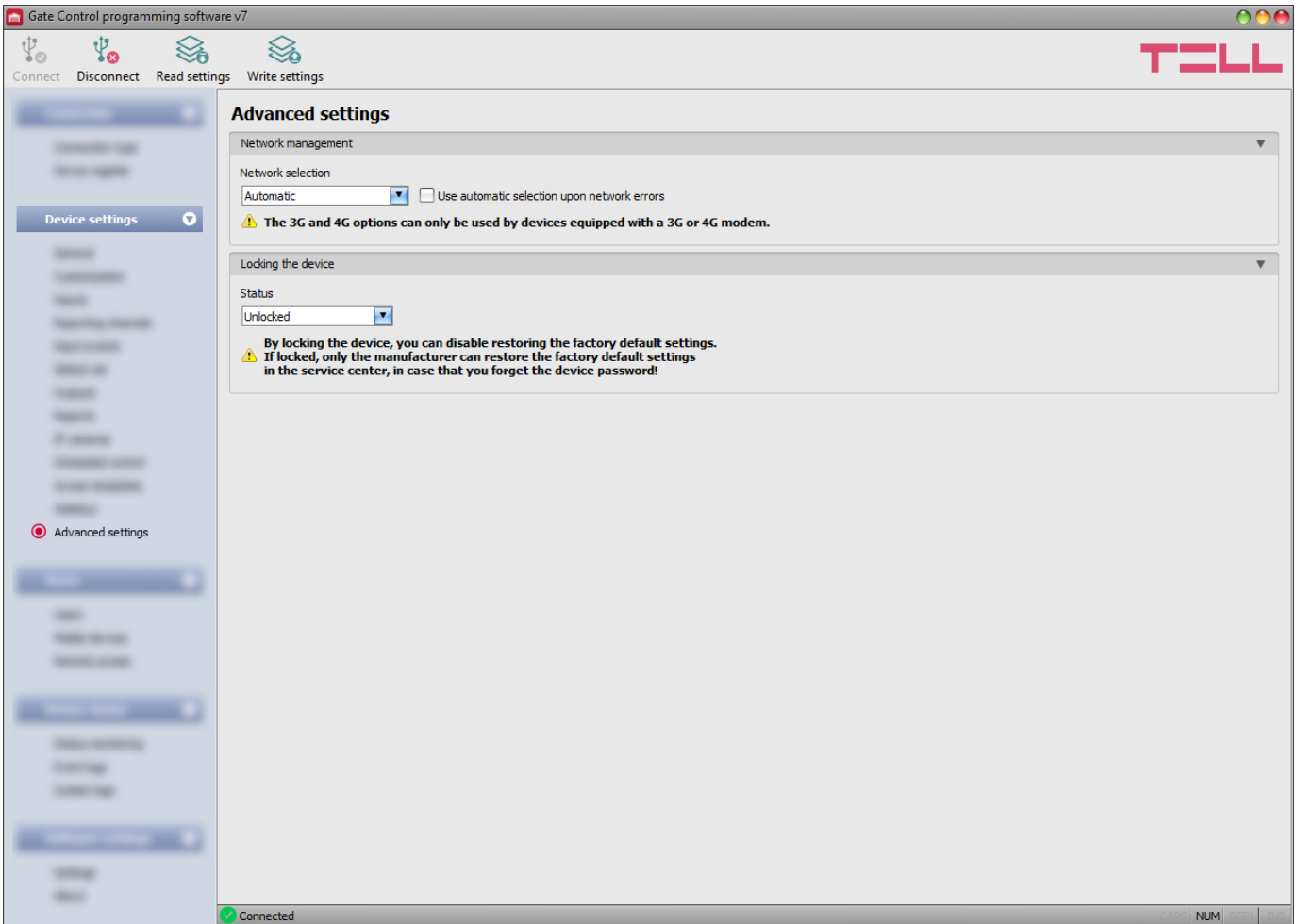- If you haven't read the settings yet, click on the "**Read settings**" button to read the settings from the device.

- Click on the "**New**" button.
- Configure the template name.
- Configure the allowed entry periods for each day of the week and holiday.
- Click on the "**OK**" button.

- Click on the "**Write settings**" button.

The system allows for adding up to 50 access templates.
Controlling the gate is allowed from the time of day configured in the "**From**" fields of the access template, until the end of the minute value of the time of day configured in the "**To**" fields, i.e. if you configure e.g. 17:30 in the "**To**" section, the user will be allowed to control the gate until 17:30:59, but no longer at 17:31. If you wish to forbid entry for a certain day, enter value **00:00** into both time fields of the given day. In the "**Holiday**" section you can configure the allowed entry period for holidays. The holidays can be configured in the "**Holidays**" menu for several years in advance.

5.2.12 Holidays

You can select the holidays for several years in advance by double clicking on the dates in the calendar. The selected dates will be highlighted with red background color. To unselect a date, double click again on it. Entry will be allowed on the selected holidays within the time period configured in the "**Holiday**" section of the access templates, and will be forbidden outside the time period. You can override the entry periods defined in access templates using custom or global rules.

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

Available options:

- Reading the settings from the device:
  To read the settings from the device click on the "**Read settings**" button. This will read all settings in all menus in the "**Device settings**" menu group.

- Writing the settings into the device:
  After changing the settings or entering new settings, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" button.

47

5.2.13 Advanced settings

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

Recommended for experts only! Do not change the 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, in order 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 you have to write the settings into the device in order to be applied after a change is made. For this, click on the "*Write settings*" **button.**

Network management:

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
- **4G only**: use 4G (LTE) network only

3G network usage is supported by Gate Control PRO 20/1000 - 3G and - 4G models only!
4G network usage is supported by the Gate Control PRO 20/1000 - 4G model only!

Use automatic selection upon network errors: if this option is enabled, the device will switch to another available network when service error occurs, even if the use of a specific network (2G, 3G or 4G) is selected in the settings.

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 anytime, 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.

5.3 Users menu group

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

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

- **Changing the user, mobile device, or remote access settings**: In order to change the settings of user entries, mobile device entries, or remote access entries, the device settings and user related entries stored in the device are needed. Therefore, first please read the actual settings from the device by clicking on the "*Read settings*" button in any submenu in the "*Device settings*" menu group, and then read the user entries by clicking on the "*Read users*" button in any submenu in the "*Users*" 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 user related settings, write the entries into the device by clicking on the "*Write users*" button.

- **Overwriting the full device configuration (device settings, users, mobile devices, and remote access entries)**: If you want to completely overwrite the users and the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the users and the settings in the submenus, and then click on the "*Create system backup*" button in the "*General*" device settings menu. You can import the saved backup into the program using the "*Restore from backup*" button, and then write imported settings into the device by category, using the "*Write settings*" and the "*Write users*" buttons.

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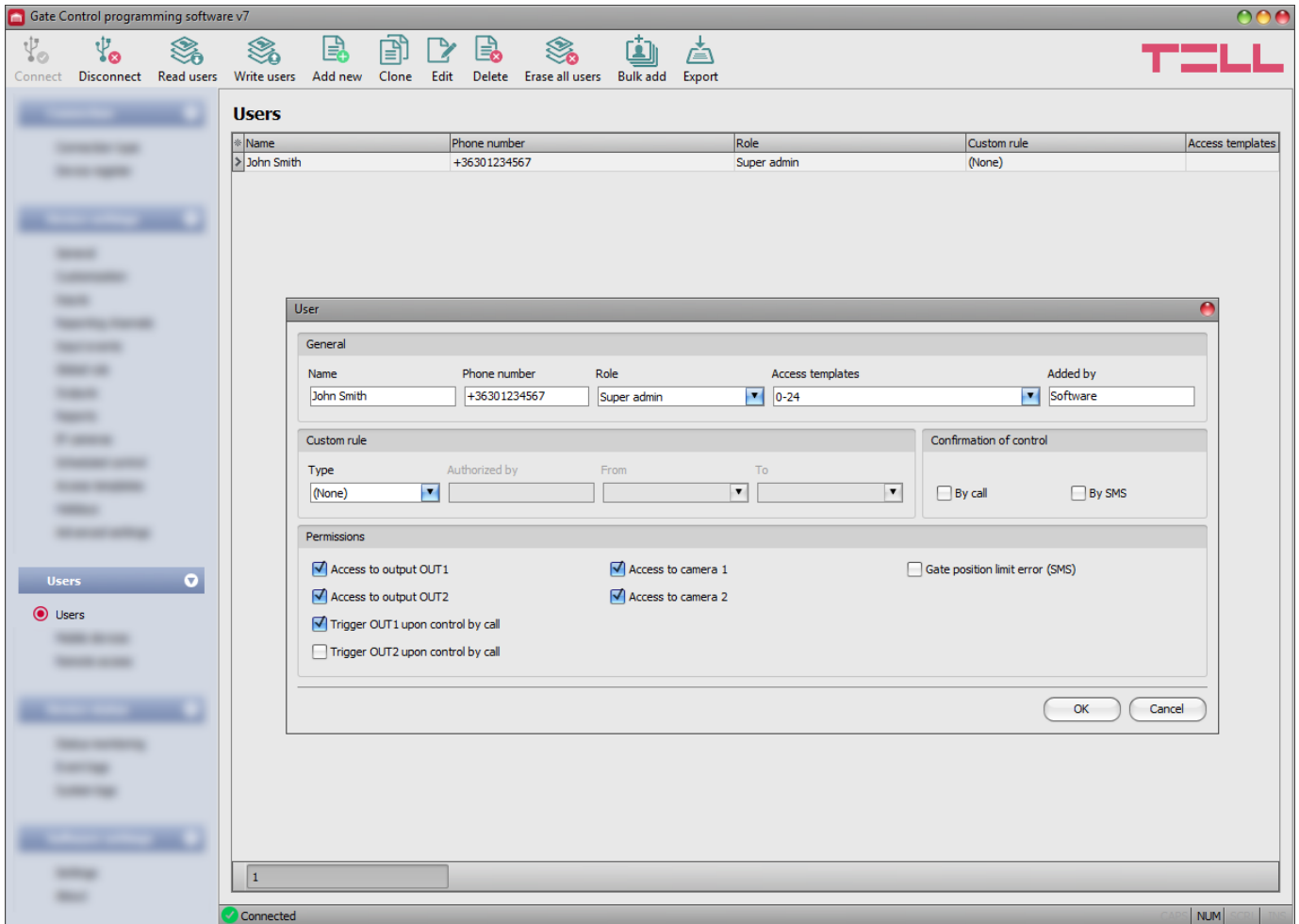
In this menu you can add users and configure user permissions, as well as configure custom entry rules separately for each user, if needed.

The system can be controlled from registered user phone numbers and mobile applications, unless the global rule is configured otherwise. Depending on the device model you own, you can register up to 20 or 1000 users with different roles and permissions.

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.

- Writing the users into the device:

  After changing the settings or adding new entries, in order 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.

- Add new user:

  Click on the "**New**" button to add a new user.

- Copy 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.

- Edit an existing user:

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

- Delete a user:

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

- Erase all users:

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

- Bulk add users:

  To add users from CSV file of 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.

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

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

The file should contain the users starting from the second line. The line should start with the user name, followed by a semicolon, and then the phone number (e.g.: John Smith;+36301234567).

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

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

Information (green background color): user entries imported successfully.

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

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

The program will not import entries marked as "*Warning*" or "*Error*" into the system!

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 user names and the associated phone numbers.

Please note that after you make changes, you have to write the users into the device in order to apply the changes. For this, click on the "*Write users*" button.

➢ **Adding a new user:**

- If you haven't read the settings and the users from the device yet, click on the "*Read settings*" button in any submenu in the "*Device settings*" menu group, and then click on the "*Read users*" button in the "*Users*" menu.

- Click on the "*New*" button.
- Enter the user's name and phone number.
- Select the user's role.
- Select access templates if needed.
- Configure the user's permissions.
- Click on the "*OK*" button.

- Click on the "*Write users*" button.

➢ **Adding the first super admin or admin user and registering the mobile application**

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

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

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

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

➢ **User settings:**

General:

Name: the user name should not exceed 40 characters, and the following characters should not be used: ^ ~ < > = ' " , | $ & %
The user name is case sensitive

Phone number: enter the phone number in international format (e.g. +3630….). The system accepts maximum 20 digits. Accepted characters are "**+**", "**0…9**" only.

Role: you can choose out of 3 role levels:

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

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

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

Custom rule:

You can override the access templates associated with a user using the custom rule. This function is useful when entry permission of a given user has to be different in some manner from the access templates (e.g. any user may control the system on a certain day except this user, because he is on vacation, etc., or even on a weekend day, entry is forbidden for all users, except this user who needs to work). The global rule will not override configured custom rules.

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

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

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

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

Confirmation of control:

By call: the system can confirm a successful control of the gate by making a call to the phone number of the user who controlled the gate. You can enable this option for each user separately.
    Attention! If you are using the device model equipped with a 2G modem, or the device is connected to the 2G network, when using functions that make an outgoing call, the Internet connection will be interrupted for the duration of the call, because the 2G network does not support voice calls and mobile Internet usage at the same time. In such a case, services that require Internet connection (mobile app usage, remote access, remote firmware update, e-mail sending) will be suspended for the duration of the call.

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

Permissions:

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

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

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

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

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

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

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

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

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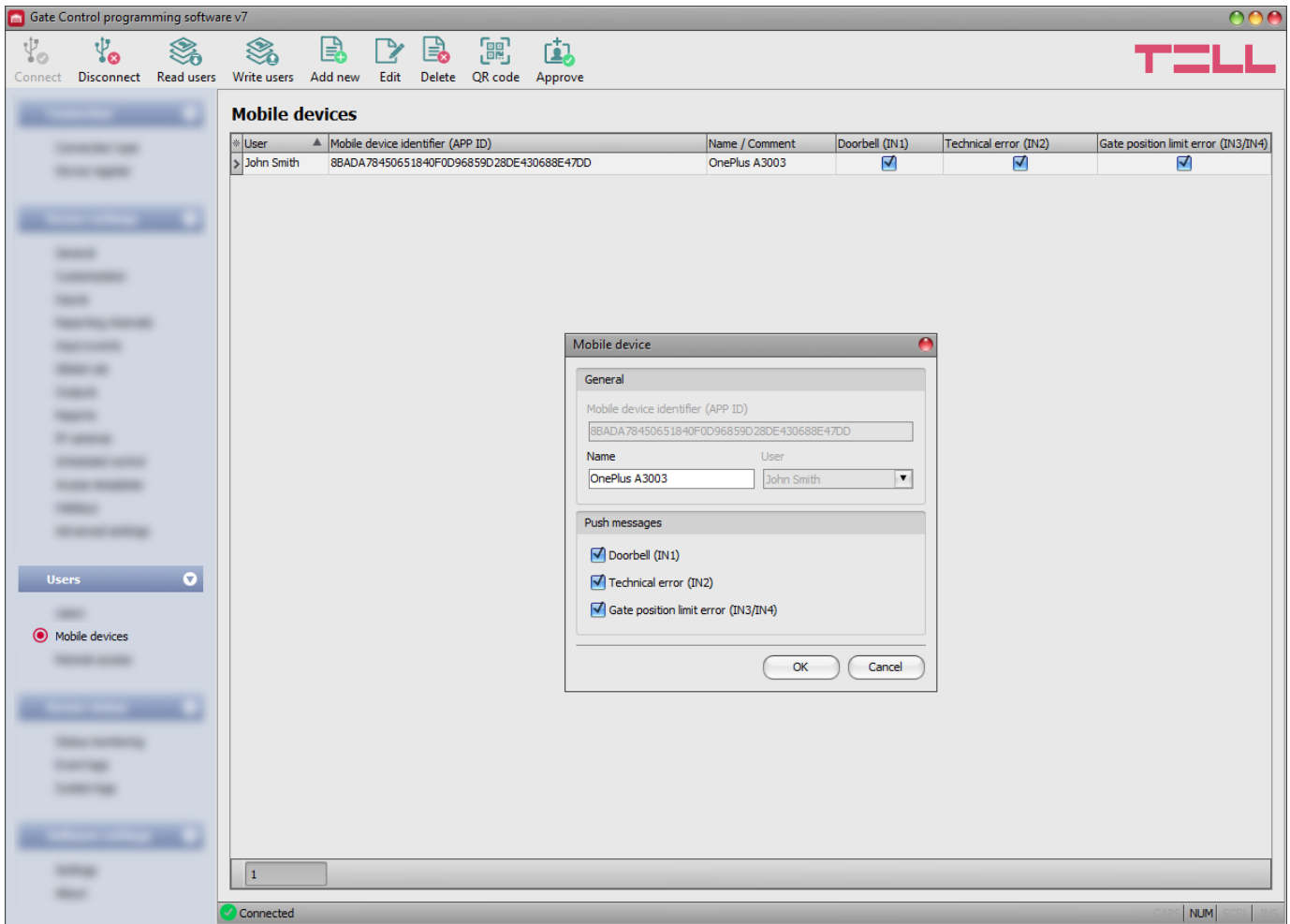
Mobile devices with registered mobile applications and ones waiting for approval are listed in this menu. This is where you can configure which mobile devices shall receive Push notifications. You can register altogether up to 2000 mobile devices and remote access passwords in the system, which are distributed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

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

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.

- Writing the users into the device:
  After changing the settings or adding new entries, in order 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.

57

- Add new mobile device manually:

   Click on the "**New**" button to add a new mobile device manually. Adding a mobile device manually might be needed if you have deleted a user or a mobile device, and want to add the device again without having to ask the given user to register the mobile application again. Otherwise, mobile devices are added automatically upon registration, i.e. you do not have to add them manually.

- Edit the settings of an existing mobile device:

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

- Delete a mobile device:

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

- QR code:

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

The programming software generates two QR codes:

> **QR code for direct app registration**

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

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

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

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

• Approve:

The "*Approve*" button is used to approve mobile app registrations waiting for approval. After clicking on this button, you have to write the users into the device in order to validate the approval in the system. A user with a mobile application waiting for approval cannot control the system until approved by an administrator through their mobile application, or using this button in the software. Registrations waiting for approval are highlighted with yellow background color in the list. This button is not available when an already approved mobile device is selected.

Please note that after you make changes, you have to write the users into the device in order to apply the changes. For this, click on the "*Write users*" button.

Mobile device settings:

General:

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

Name: you can enter a custom name for the mobile device in this section. The name entered here is used to identify the mobile device in the program and in the event logs. The device name should not exceed 40 characters, and the following characters should not be used:
^ ~ < > = ' " , | $ & %

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

Push messages:

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

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

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

➢ **Explanation of background colors of entries**

Mobile devices shown in the "***Mobile devices***" menu are displayed with different background colors. The background colors represent the following statuses:

- two skin dependent light colors: alternation of the two light colors serves for distinguishing the lines more easily.

- yellow: mobile device registration waiting for approval.

➢ **Adding a new mobile device manually:**

Adding a mobile device manually might be needed if you have deleted a user or a mobile device, and want to add the device again without having to ask the given user to register the mobile application again. Otherwise, mobile devices are added automatically upon registration, i.e. you do not have to add them manually.

- If you haven't read the settings and the users from the device yet, click on the

  "***Read settings***" button in any submenu in the "***Device settings***" menu group, and

  then click on the "***Read users***" button in the "***Users***" menu.

- Click on the "***New***" button.
- Paste the "***APP ID***" identifier found in the mobile application in the ***Settings->About*** menu, into the "***Mobile device identifier (APP ID)***" field. You can copy the identifier from the mobile application and send it by e-mail or Skype or other application to your PC, where you can copy it again an paste into the "***Mobile device identifier (APP ID)***" field, thus you don't have to type in the long code.
- Enter a custom name for the mobile device in the "***Name***" field.
- Select the user who you want to associate the mobile device with in the "***User***" drop-down menu.
- Enable the Push messages required for the given mobile device.
- Click on the "***OK***" button.

- Click on the "***Write users***" button.

5.3.3 Remote access
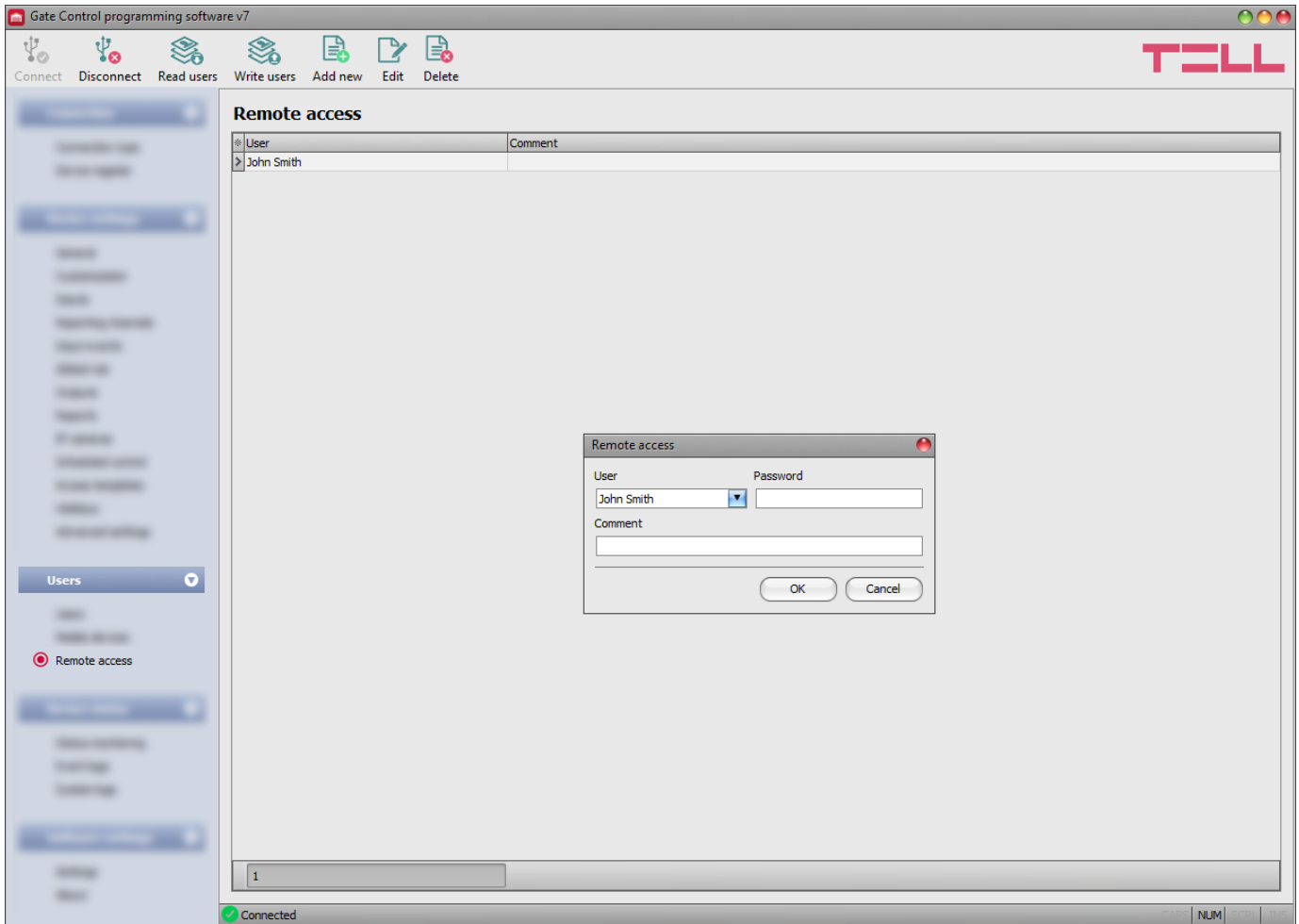
In this menu you can configure passwords for remote access, for super admins and admins. In the possession of the user name and password, the super admin or admin will be authorized to connect to the system remotely over the Internet, using the programming software. You can register altogether up to 2000 mobile devices and remote access passwords in the system, which are distributed dynamically among registered users.

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.

- Writing the users into the device:

    After changing the settings or adding new entries, in order 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.

- Add new remote access:

    Click on the "***New***" button to add a new remote access.

- Edit the settings of an existing remote access:

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

- Delete a remote access:

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

Please note that after you make changes, you have to write the users into the device in order 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: in this section you can configure the remote access password. The password configured here, and the given user's user name will be required in the "*Connection type*" menu, in the "*Remote access*" section, for connecting remotely to the device.

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

➢ **Remote access levels:**

With **Super admin** role:	full access, can access all settings.
With **Admin** role:	can access everything except the settings in the following menus: ***General, Customization, Inputs, Reporting channels, Input events, Outputs, Reports, IP cameras, Advanced settings.***
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 settings*" button in any submenu in the "*Device settings*" menu group, and then click on the "*Read users*" button in the "*Users*" menu.
- Click on the "*New*" button.
- Select the user from the "*User*" drop-down menu, whom you want to grant remote access.
- Configure the remote access password in the "*Password*" field.
- You can write a comment in the "*Comment*" field, if needed.
- Click on the "*OK*" button.

- Click on the "*Write users*" button.

5.4 Device status menu group

5.4.1 Status monitoring

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.

Available options:

- **Read**:

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

- **Time synchronization**:

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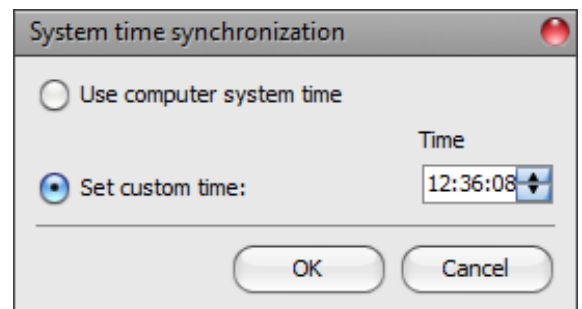
Device:

- **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.
- **Supply voltage**: value of the supply voltage measured.
- **Device ID**: the unique identifier of the device (6x2 hexadecimal characters). This identifier is burned-in during production and thereby it is unchangeable.

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 GSM network.

Network:

- **GSM operator**: the name of the currently used GSM operator.
- **GSM signal**: actual GSM signal level (None/Very low, Weak, Medium, Good, Excellent). For models with a 3G modem, the displayed signal level is an informative, calculated value. Therefore, a low signal level does not necessarily mean that the device will not work properly.
- **Data connection type**: the type of the currently used data connection.
- **IP address**: the actual IP address of the device.

Inputs / Outputs:

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

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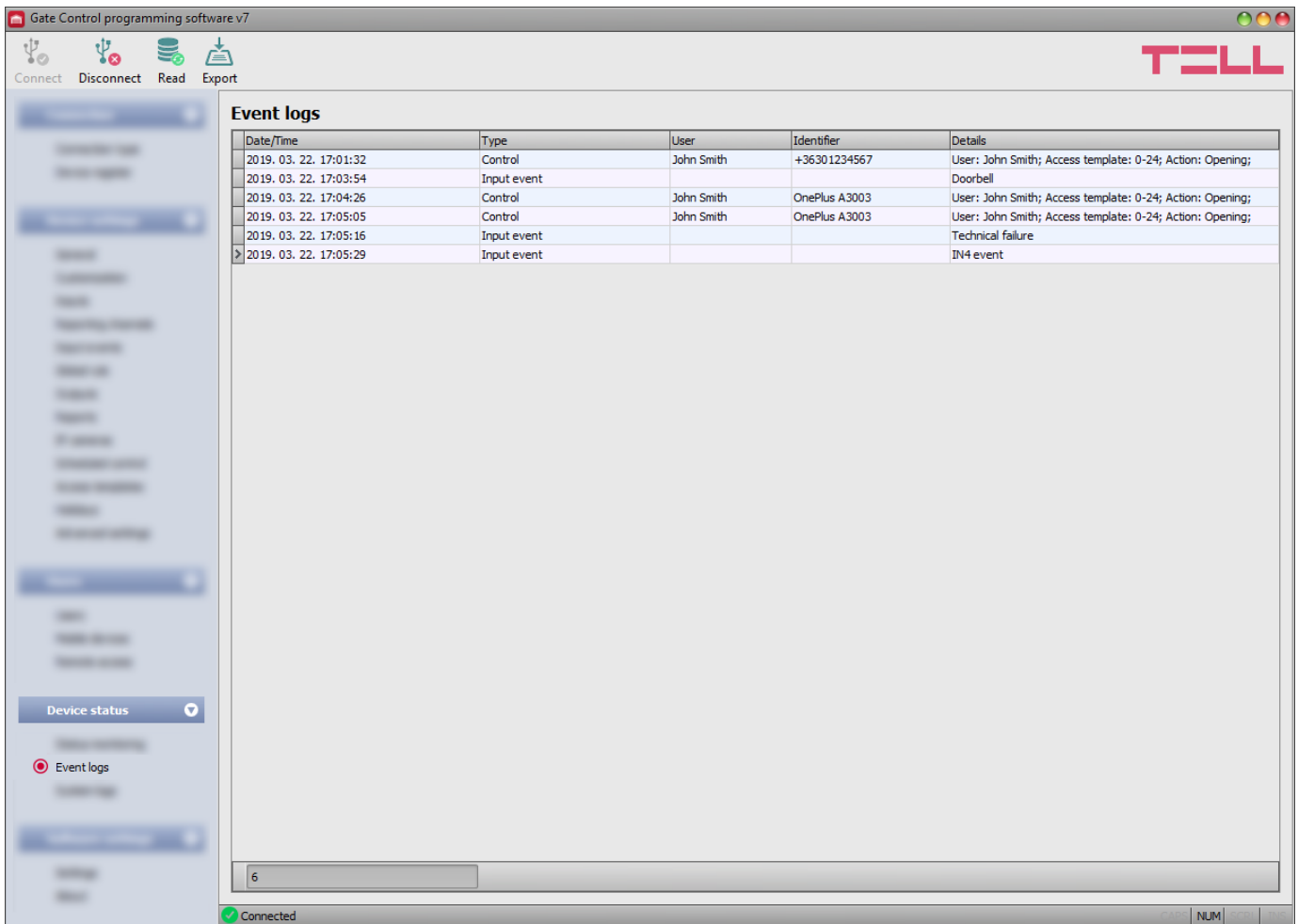
In this menu you can view and export the event logs to file, which includes control and input events recorded by the system. The system stores the latest 1000 events in the event log memory.

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.
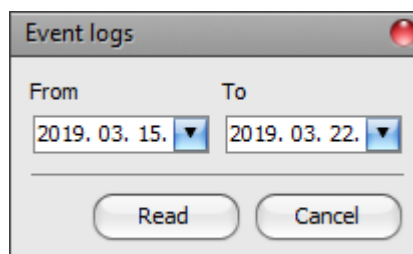
- **Export**:

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

5.4.3 System logs

In this section you can view information about the internal processes of the device and communication. These details help troubleshooting, if malfunction occurs. **This option is only available when connected thtough USB!**

5.5 Software settings menu group

5.5.1 Settings
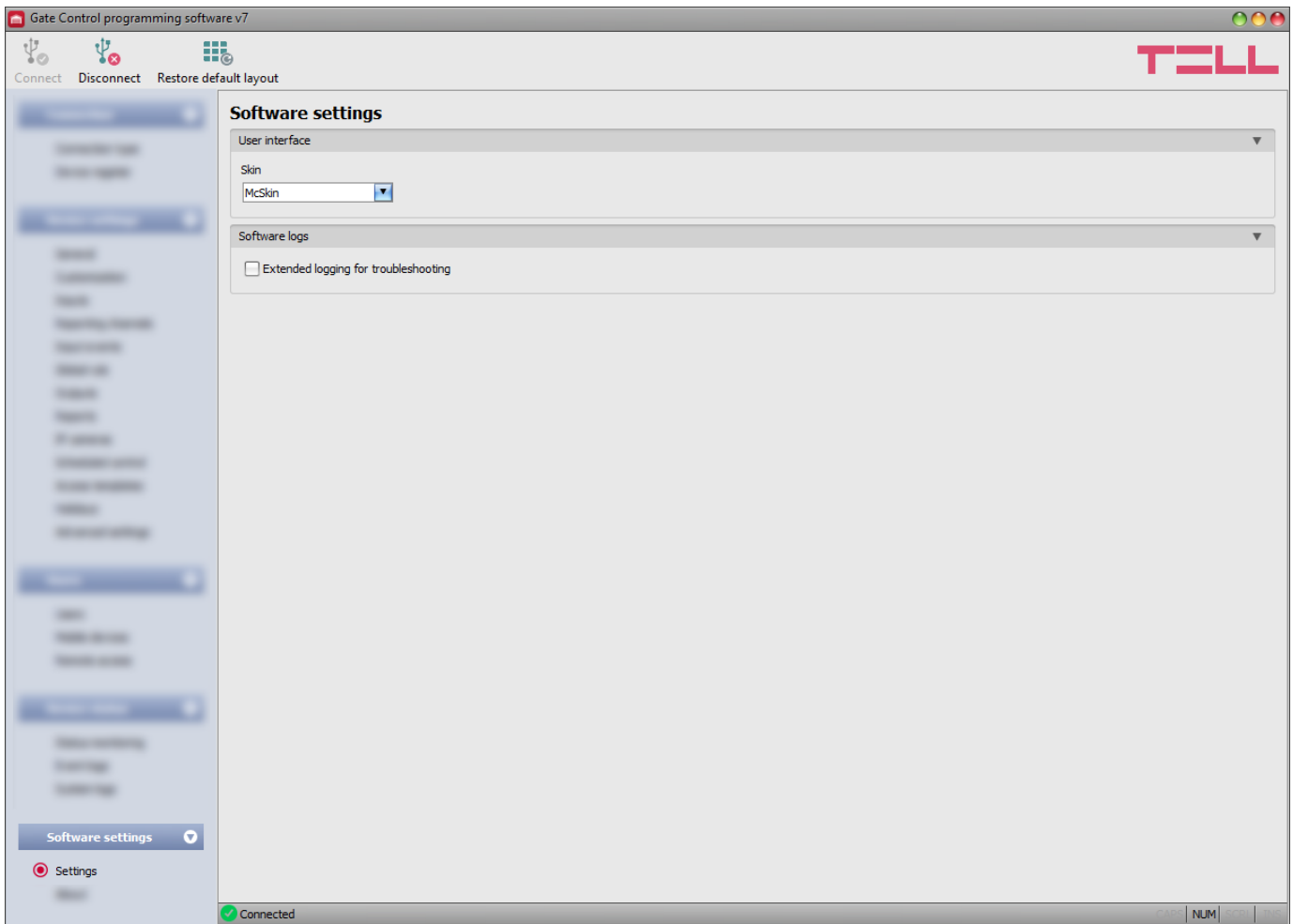
In this menu you can change the user interface skin (appearance), and can also enable extended logging for troubleshooting.

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:

Skin: you can change the user interface skin using the dropdown-menu. You can choose out of several appearance themes.

Software logs:

Extended logging for troubleshooting: you can enable this option if you encounter issues when using the system. If you enable this option, the program will record detailed logs while the system operates, and will save these logs in the "**Logs**" folder, which you can open by clicking on the link found in the "**About**" menu, in the "**Data folder**" section. The detailed logs help the manufacturer in troubleshooting.

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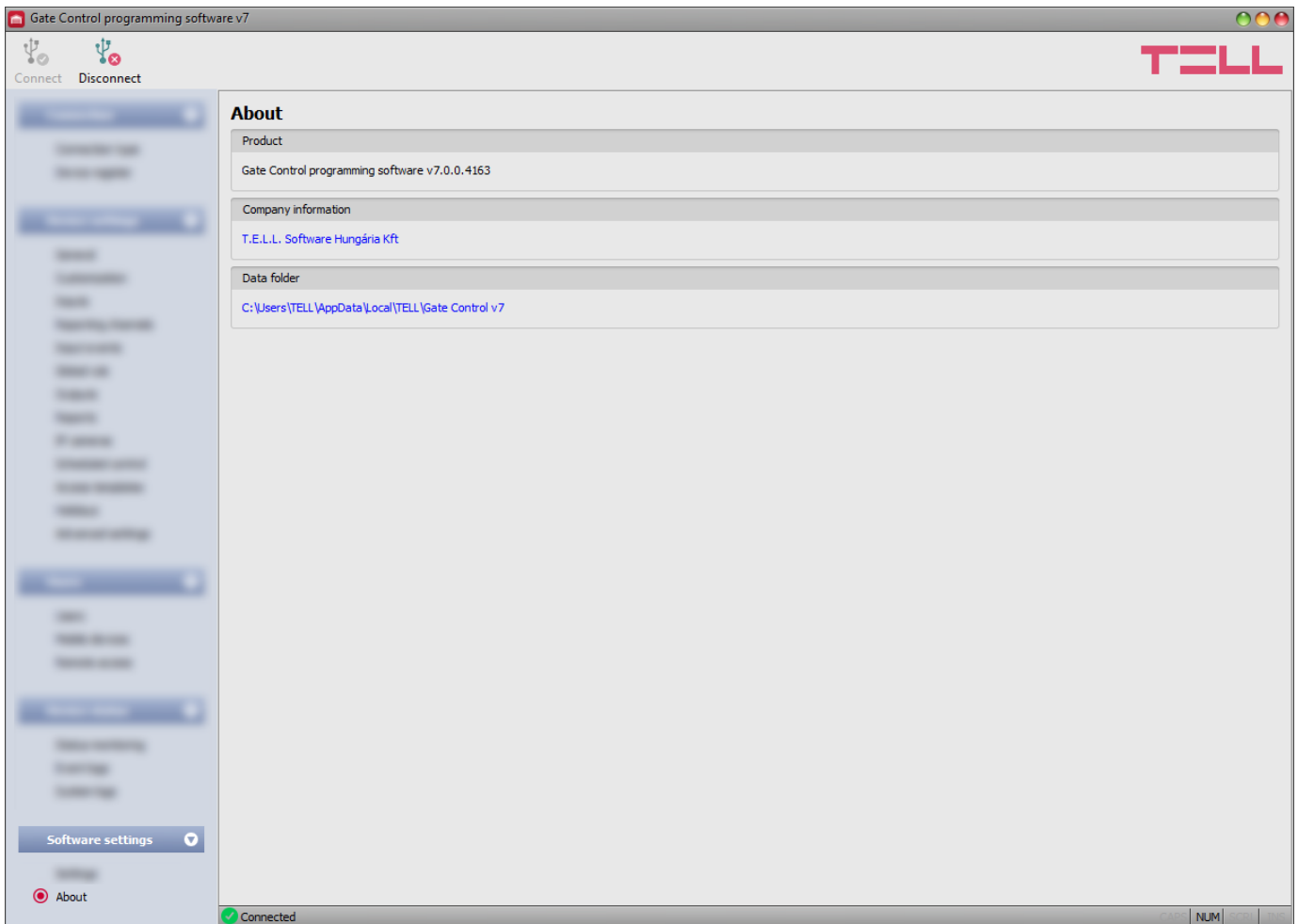
In this menu you can view the availabilities of the manufacturer, the version of the programming software, and the path of the data folder where the software stores system logs. By clicking on the path, the program will open the data folder in the file manager.

6 Replacing the SIM card

If "**Cloud usage**" is enabled in the settings, the **Gate Control PRO** device is identified in the system using the identification number of the SIM installed in the device, therefore replacing the SIM card affects the operation of the system. If it is necessary to replace the SIM card for any reason, please follow the instructions below:

- Power down the device, replace the SIM card, and then power up the device.

- If the phone number of the device has also changed by replacing the SIM card, update the phone number in the "**General**" device settings.

- After replacing the SIM card, it is necessary to delete the **Gate Control PRO** device in the mobile application on all registered mobile devices, and register the device again.

If "**Cloud usage**" is disabled and the device is not used with the mobile application, to replace the SIM card, just power down the device, replace the SIM card, and then power up the device again.

7 Updating the firmware

You can update the firmware on the *Gate Control PRO* device locally, through USB, or remotely, over the Internet. The firmware file, or the desktop update application necessary for updating the device, are available on the manufacturer's website (https://tell.hu/en), in the product downloads.

7.1 Updating through USB

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

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

  - Download the desktop update application that has the **.exe** extension, necessary for updating, from the manufacturer's website. The update application includes the firmware as well, therefore the file name is identical with the firmware version number.
  - Open the update application and click on the "*FIRMWARE*" button.
  - Connect the device to the computer via USB.
  - Click on the "*Start*" button, and then power up the device. 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 LED status indicator on the device shows activity. After that, you can connect with the programming software and check the operation.

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

  - Download the latest firmware file that has the **.tf3** extension, necessary for updating, from the manufacturer's website.
  - Click on the "*General*" device settings menu in the programming software.
  - Click on the "*Firmware update*" button, and then browse the firmware file that has the **.tf3** extension.
  - The update process will start automatically as soon as you click on the "*Open*" button. When firmware uploading has completed, the progress window closes automatically and a few seconds later the device restarts with the new firmware.

7.2 Updating remotely over the Internet

There is also an option to update the firmware of the *Gate Control PRO* device remotely 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, specified above.

8 Restoring the factory default settings

Restoring the factory default settings 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 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.
You can restore the factory default settings using the programming software, or the reset 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 involves a device restart. Wait until the device restarts and the status LED on the device starts working again. The option of restoring the factory default settings is also available without entering the USB password of the device.

8.2 Restoring the factory default settings using the reset button:

- Power up the device.

- Long press the reset button for at least 8 seconds, and then release. The reset microswitch is placed in horizontal position on the PCB, near the corner of the SIM card holder, closed to the status LED (see the picture on the right hand side). It is easier to access the button if you open the SIM card holder.

- After releasing the reset button, the status LED will turn permanent red first, and then it will start blinking in red.

- Install the SIM card and close back the SIM holder.

- During the factory reset process, the device has to create the full a clean configuration stock, which may take 2.5 to 3 minutes. Meanwhile, the status LED keeps flashing in red.

- The factory reset has completed when the device connects to the GSM network and the status LED flashes in green.

9 Contents of the package

- *Gate Control PRO* + system terminal
- GSM 900/1800 MHz antenna
- Quick start guide
- Warranty card