Adapter2 PRO – DIN rail

INSTALLATION AND APPLICATION MANUAL

for device version v8.02
Document version 1.02 16.05.2025

Product models:

- **Adapter2 PRO DIN rail – 4G.IN4.R1**

Table of contents

1 Adapter2 PRO operation

1.1 Key functions of the product

The primary function of the ***Adapter2 PRO*** is forwarding reports of alarm systems to remote monitoring station over the Internet.

► **Product models:**

Adapter2 PRO DIN rail – 4G.IN4.R1

- 4G modem that supports the European frequency bands
- DIN rail mount
- 4 NO/NC inputs
- 1 NO/NC/COM relay output
- 1 telephone line emulator output
- RS232 serial port
- TTL serial port

► **Key functions:**

- Sends SMS, e-mail and Push notification with configurable message for each event.
- Reports events by SMS, e-mail and Push notification, by voice call with voice messages uploadable as audio files, over IP to remote monitoring stations using different communication protocols and by voice call using DTMF-based Contact ID protocol.
- Reporting options:
    - ➢ SMS with configurable message up to 4 phone numbers.
    - ➢ E-mail with configurable message up to 4 addresses.
    - ➢ Push notification with configurable message up to 4 users (mobile applications).
    - ➢ Voice call up to 4 phone numbers with up to 15 uploadable messages of 10 seconds each.
    - ➢ Reporting to CMS (Central monitoring station) over IP up to 4 IP addresses using SIA IP DC-09, TELLMon and TEX protocol.
    - ➢ Reporting to CMS by voice call using DTMF-based (DC-05) Contact ID protocol.
- Up to 10 notification templates can be created and assigned to events to configure the priorities of reporting channels used for reporting to CMS.
- Configurable Contact ID event codes for each input and service event, including partition and zone options.
- Output control can be customized separately for each event using different operation modes, which can also be used to arm or disarm the connected alarm control panel remotely, through the mobile application.
- Available custom events: input events, service, and error events (new and restore as well)
- IP camera support: forwards the links of up to 4 IP cameras by e-mail and Push notification along with the alarm messages.

► Mobile application:

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

GET IT ON Google Play

Available on the App Store

Minimal system requirements:

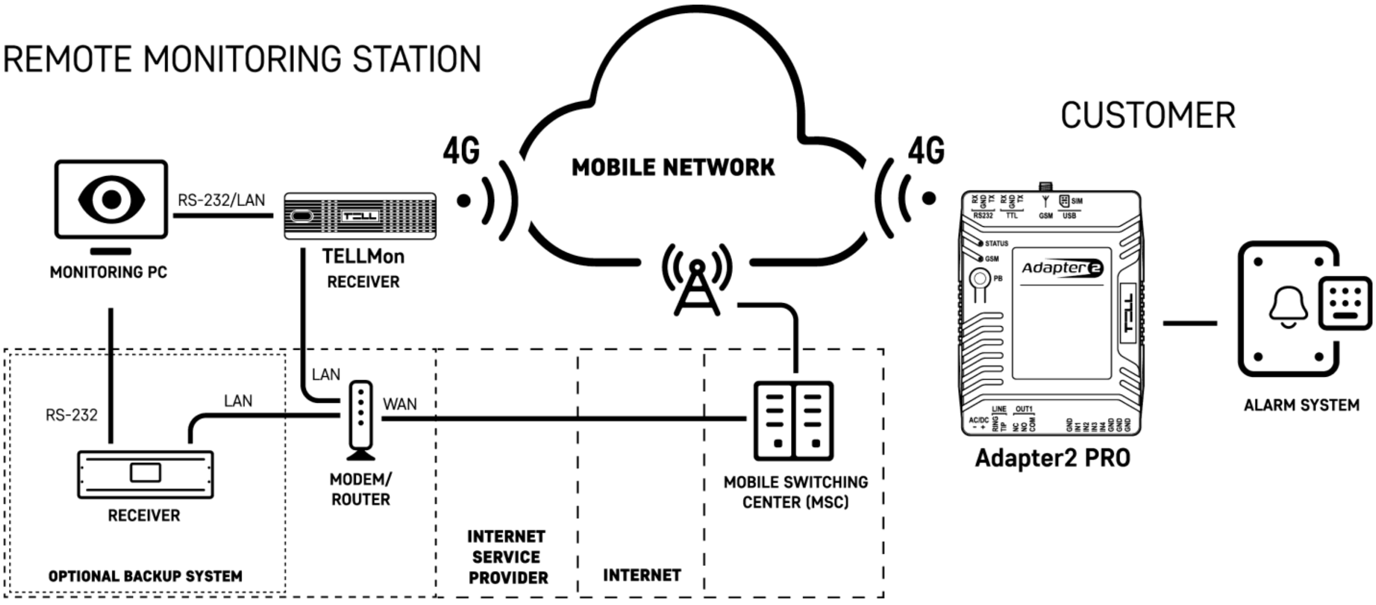
- Android: 8
- iOS: 12

1.2 Under Voltage Lock Out (UVLO) function

UVLO

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

1.3 Remote monitoring application overview



The **Adapter2 PRO** communicates with the TELLMon or SIA DC-09 receivers and MVP.next or TEX-MVP servers through the GSM service provider’s mobile switching center using the GPRS/ /LTE network, and then through the Internet. After processing and conversion, the server forwards the received data packages through serial port towards the monitoring PC that runs the alarm monitoring software. Alternative reporting channels: voice call and SMS.

1.3.1 General information about the notification process

The device sends notifications based on own events available in the device, and based on the configuration of the connected alarm system's events.

There are 4 event categories available in the device: input events, service events, custom events, and alarm system events.

- **Input events**: Input events are generated by triggering the contact inputs on the device.
- **Service events**: Service events are generated automatically by the device, such as error events, own periodic test report, or events on reaching different configured limits.
- **Custom events**: Custom events are generated by freely configurable commands sent to the device in a text message. Custom events and commands can be configured optionally in the device.
- **Alarm system events**: Alarm system events are Contact ID messages received from the connected alarm system via the device's simulated phone line input.

When an event is generated, the device starts the notifications and controls configured for that event. The order of notifications corresponds to the order in which the events occurred.

➢ Reporting to a remote monitoring station

You can assign one from the notification templates configured in advance to each event. In a notification template you can configure, which of the configured monitoring receivers should be notified, and with what priority. Backup reporting by SMS can also be set for the case when reporting fails to all the selected receivers. Reporting a given event will thereby be performed according to the notification template associated with it. Regarding events received from the connected alarm system, it is possible to filter events by event code, partition, and zone number. Thereby, you can add a filter for a group of events or even a specific event, of which reporting can be configured likewise, by assigning a notification template customized as needed. Furthermore, depending on the device settings, as a backup option, the alarm system can also send reports via DTMF based voice call to a landline receiver, by dialing a specific phone number.

➢ Notification sending to users

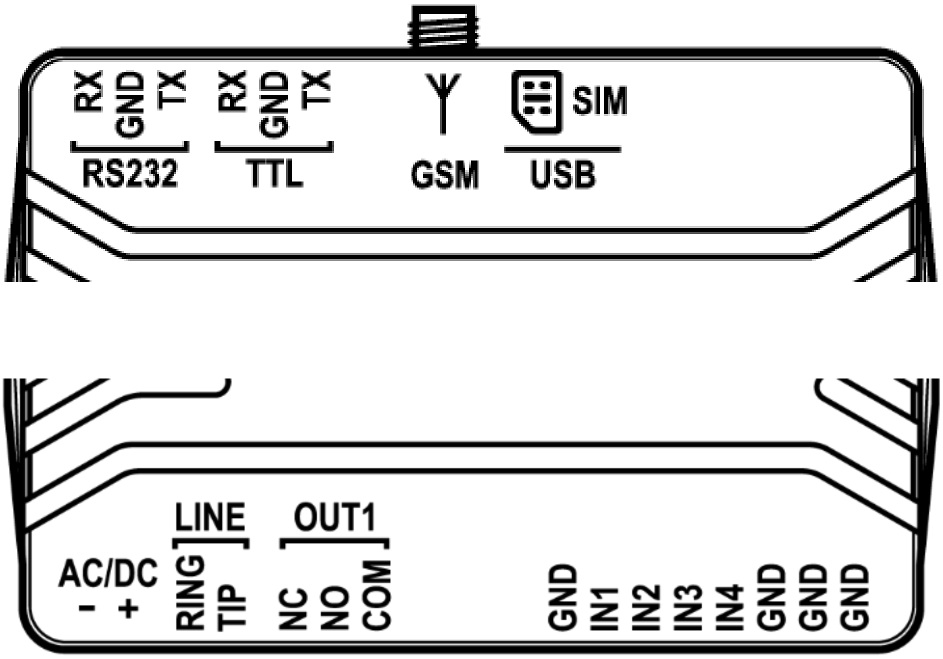
Regardless of reporting to remote monitoring station, you can configure notifications for users by call, SMS, Push message or e-mail.

Reporting to remote monitoring station has priority against notification of users. The device sends the events simultaneously to the configured IP addresses. It sends the ACK signal towards the alarm control panel only when it receives the ACK from at least one of the configured receivers (IP addresses). Regardless to this, event sending continues towards the other receivers. If the device does not receive an ACK signal from any of the configured receivers, it tries to report the event for up to 10 minutes. If reporting to the configured IP addresses fails for the mentioned 10 minutes, the device stops reporting the event and will no longer send notification on the given event, but the event will be shown in the event logs.

2 Connecting the terminals and putting into operation

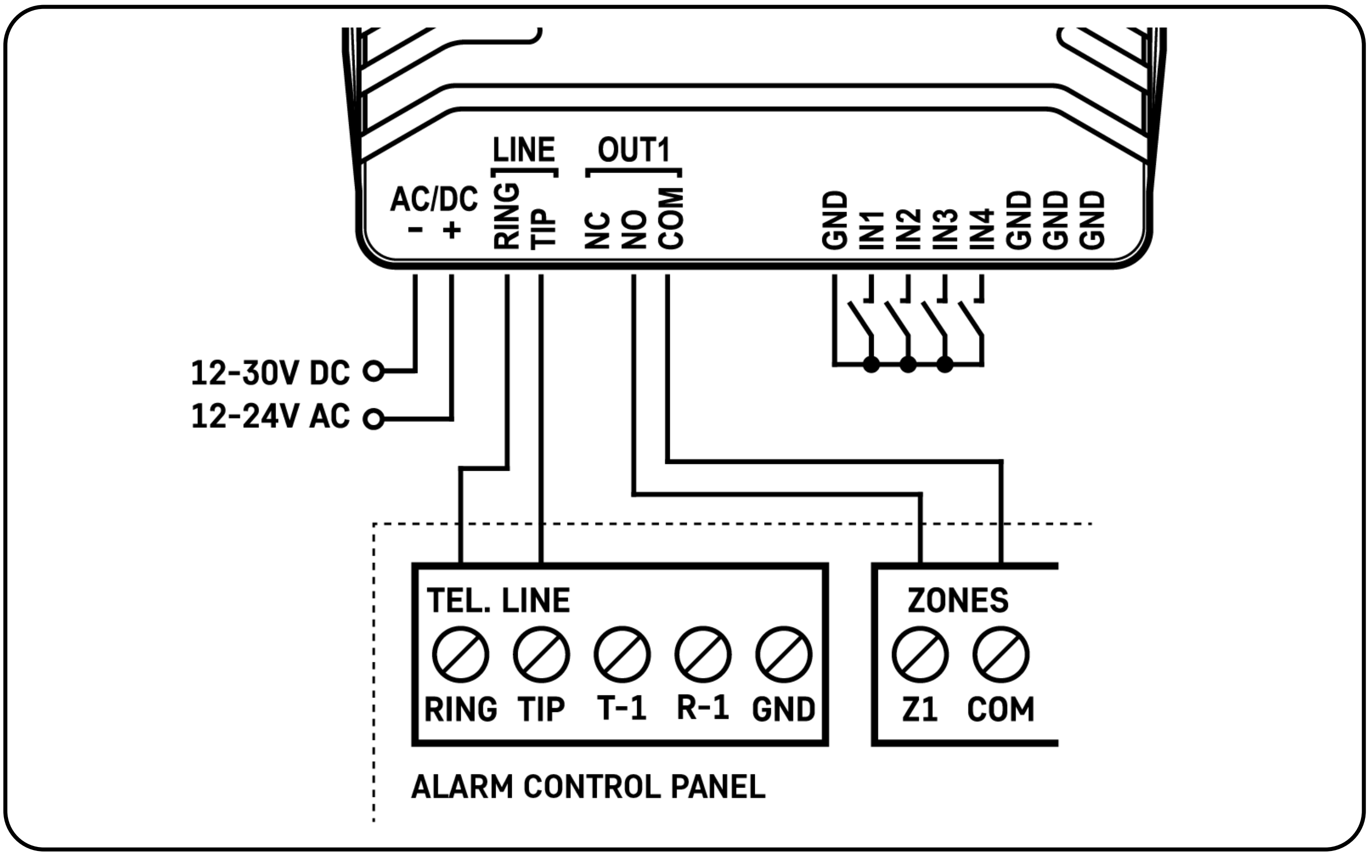
Attention! Do NOT connect the metallic parts of the GSM antenna connector or the terminals of the device directly or indirectly to the protective ground, because this may damage the device!

2.1 System terminals



AC/DC	**-**	Power input (negative for DC)	**12-30VDC or 12-24VAC minimum 500mA**
	+	Power input (positive for DC)	
LINE	**TIP**	Emulated telephone line	**Telephone line output** 48V / 25mA / 600Ω
	RING	Emulated telephone line	
OUT1	**NC**	Normally closed terminal	**Relay output** (dry contacts) max. 1A / 24V DC
	NO	Normally open terminal	
	COM	Common terminal	
IN1		Contact input 1	Use potential free (dry) contacts only
IN2		Contact input 2	
IN3		Contact input 3	
IN4		Contact input 4	
GND		Common terminal of the contact inputs	
RS232	**RX**	RS232 receive (data)	**RS232 serial port** (12V)
	TX	RS232 transmit (data)	
	GND	RS232 common terminal	
TTL	**RX**	TTL receive (data)	**TTL serial port** (5V)
	TX	TTL transmit (data)	
	GND	TTL common terminal	

2.2 Wiring diagram



<u>**Attention!**</u>

<u>Although the *GND* and the power input negative terminals are equivalent, due to the design of internal circuit protections, the *GND* terminal must not be used as negative input for powering the device because this may damage the device! The *GND* terminal should only be used for connecting the contact inputs!</u>

<u>We would not advise powering the device directly from the power output of the alarm control panel (AUX), as we can't guarantee that the given output is able to fully operate the device. Insufficient powering may lead to communication errors and frequent device restarting, making it impossible for the device to operate normally as expected. To avoid this, we suggest that you use a separate power supply for the device.</u>

An uninterruptible power supply with adequate power is essential for the product to operate properly. The power supply must provide a power that can serve the minimum operating voltage and the maximum power consumption of the device. The power feed must be continuous and transient-free even when there is a mains power failure, and the power feed switches to backup battery operation.

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

- Recommended TELL power supply for use with an alarm control panel: **TT40VA-16VAC/24VDC**, which provides power feed (16V AC) also for the alarm control panel at the same time.
- Recommended TELL power supply for other use: **TT25VA-12V5**.

2.3 Input wiring

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

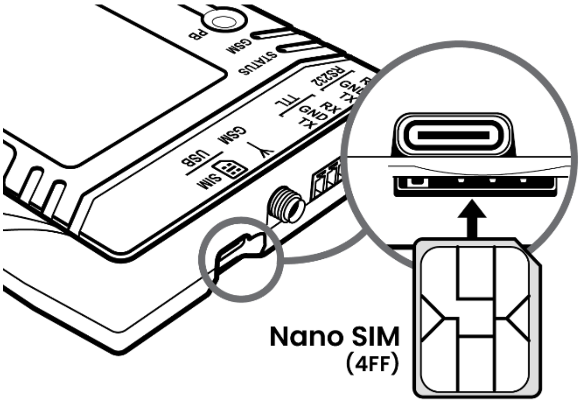
If a normally open dry contact is used to activate the input, choose the **NO** (normally open) option at the given input's settings. In this case, the input becomes activated when the open contact between the given input (**IN1**…**IN4**) and the **GND** terminal is closed.

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

2.4 Output wiring

The **OUT** output has **NO**, **NC**, and **COM** terminals with potential free (dry) contacts. The output provides normally open dry contacts between the **NO** and **COM** terminals as the default state, and closed contacts when controlled. The relay output terminals support a maximum load of **1A** @ 24V DC.

2.5 Preparing and installing the SIM card



- **The device requires a Nano (4FF) size SIM card.**
- The services to be activated on the SIM card installed in the **Adapter2 PRO** device should be chosen according to which services of the device you wish to use. Basically, for communication with receivers and servers it requires a SIM card with mobile Internet access that may use either public or private APN. The functions that use SMS sending need SMS service and the ones that use calls require GSM voice call and VoLTE service.
- **Disable the voicemail service and SMS notification about missed calls on the SIM card installed in the device.**
- **Ask the service provider to activate the VoLTE service on the SIM card.**
This is essential for voice calls to work on the 4G network.
- **The device can handle the SIM card's PIN code. If you want to use the PIN code management, configure the SIM card's PIN code in the programming software in the "*General*" device settings menu. Otherwise, disable PIN code request on the SIM card.**
- **Enable caller identification and caller ID transmission service on the SIM card at the mobile service provider** (these services might not be enabled by default, please check). To enable these services, install the SIM card into a mobile phone, and call the customer service of the card's mobile service provider, and enable the services in the menu, or visit one of the service provider's personal customer services, and ask them to enable these services on the SIM card.
- Install the SIM card as shown in the figure above. Push the card into the socket until you hear a click. If you want to remove the SIM card, press it again, and then pull it out.

2.6 Connecting the antenna

Connect the GSM antenna to the SMA-F socket. The device comes with an antenna that provides good transmission under normal reception circumstances. In case of experiencing signal strength problems or/and wave interference (fading), use a directed antenna, or find a more advantageous mounting place for the antenna. In case of installing the unit into a metal box, the antenna should be mounted outside the box, in a place where the measured GSM signal is the highest available.

2.7 Installation

Please check the environment before installing:

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

2.8 Putting into operation

- Check the firmware version of your device in the "***Status monitoring***" menu, and update the firmware if a newer version is available.
  (Downloads: https://www.tell.hu/en/downloads, instructions: Updating the firmware).
- Make sure that the SIM card is installed correctly in the device.
- Make sure that the antenna is connected correctly to the device.
- Make sure that the wires are connected correctly.
- You can power up the device (12-30V DC or 12-24V AC). Make sure that the power source provides sufficient power for the operation of the **Adapter2 PRO** device. The nominal current consumption of the **Adapter2 PRO** device is 130mA, however, it may rise to 500mA during communication and output control. If the applied power source does not provide sufficient power for the operation of the device, this may cause malfunctions.

2.9 STATUS and GSM LED signals

STATUS LED	Slowly flashing green	Normal operation, connected to the mobile network
	Flashing red	The mobile service is unavailable, or system startup/restart is in progress
	Permanent red	SIM card error
GSM LED	Permanent ON	Searching for network
	200ms ON, 200ms OFF	Data transmission
	800ms ON, 800ms OFF	Registered on the network
	Permanent OFF	Modem powered off

2.10 Technical specification

Supply voltage range:	12-30V DC or 12-24V AC
Nominal current consumption:	130mA
Highest current consumption:	500mA @ 12V DC, 250mA @ 24V DC
Operating temperature:	-20ºC - +70ºC
Transmission frequency (4G modem):	GSM/GPRS/EDGE: 900/1800 MHz LTE/FDD: B1/B3/B5/B7/B8/B20
Highest load supported on output:	1A @ 24V DC
Dimensions:	88.4 x 119 x 23.1mm
Net weight:	144g
Gross weight (packed):	295g

RF emission power:

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

3 Configuring the Adapter2 PRO

The **Adapter2 PRO** can be configured as follows:

- By computer via USB, using the programming software.
- By computer over the Internet, using the programming software.

The **Adapter2** programming software is compatible with the following operating systems:

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

Earlier Windows operating systems are not supported by the software.

Installing the programming software: open the software setup application and follow the instructions of the installation wizard to complete the installation. The latest version of the programming software is available on the manufacturer’s website (http://www.tell.hu).

The **Adapter2** programming software can be used to configure all **Adapter2** device models.

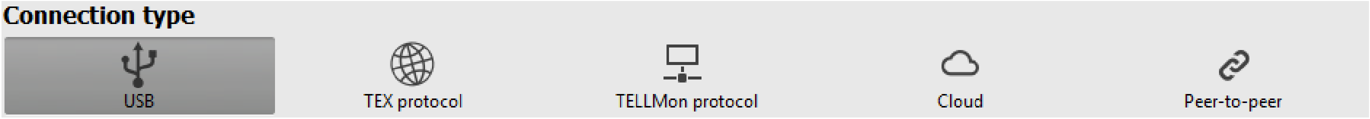
3.1 The user interface and configuration options of the software

The user interface language can be selected during installation.

The user interface appearance can be changed using the “***Theme***” dropdown-menu found in the “***Software settings***” / “***Settings***” menu, where you can choose from various appearance themes. The software saves changes related to appearance upon closing and applies the saved settings when reopened.

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

3.2 Methods for connecting to the device



For connecting to the device using the programming software, the options listed below are available. For the "***TEX protocol***" and the "***TELLMon protocol***" connection options, the communication protocol used by the device depends on how this has been configured in the device by the installer, in accordance with the type of the server/receiver that it is connected to.

USB: connecting directly using a USB-A to USB-C cable.

TEX protocol: connecting remotely over the Internet to a device, which uses the TEX protocol. Choose this option if the device is connected to any of the following servers/receivers via the TEX protocol:

- MVP.next server;
- TELLMon receiver;
- TEX-MVP server;
- TEX BASE or TEX PRO server.

TELLMon protocol: connecting remotely over the Internet to a device, which uses the TELLMon protocol. Choose this option if the device is connected to any of the following servers/receivers via the TELLMon protocol:

- MVP.next server;
- TELLMon receiver.

Cloud: connecting remotely over the Internet, via the cloud server operated by the manufacturer. You can use this option if the device is connected to the cloud.

Peer-to-peer: direct remote IP connection over the Internet. This option can be used if the computer running the programming software, and the SIM card installed in the **Adapter2 PRO** device are in the same VPN or a private APN.

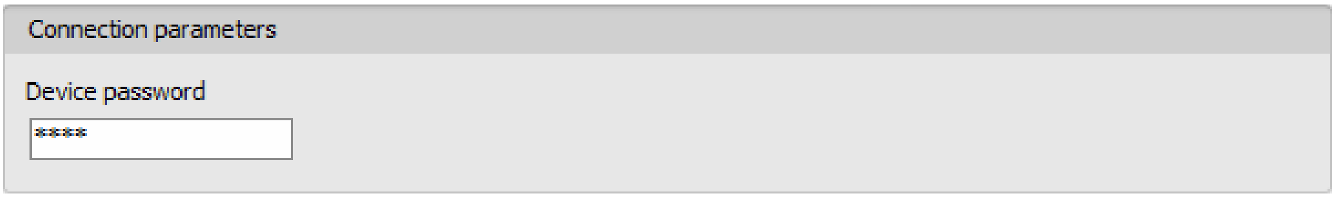
3.2.1 TELL servers and receivers

- **TELLMon**: standalone TELL remote monitoring receiver.
- **MVP.next**: cloud-based TELL remote monitoring server system.
- **Cloud**: cloud-based TELL server used for the mobile applications and remote access of TELL devices.
- **TEX-MVP**: cloud-based TELL remote monitoring server system (discontinued).
- **TEX BASE and TEX PRO**: standalone TELL remote monitoring server (discontinued).

3.2.2 Configuring directly via USB

To start programming the device, follow the instructions below:

- Open the **Adapter2** programming software.
- Select the USB option in the "***Connection type***" menu, power up the device and connect it to the computer using a USB-A to USB-C cable.



Connection parameters

Device password

****

- Enter the device password.
    - Super administrator permission: full access to all settings. (Default password: **1234**).
    - Administrator permission: can only access settings enabled by the superadmin. You can configure the admin password separately (see chapter "***Connection type***").
    - Connecting without a password: only restoring the factory default settings is available, if the device has not been locked.
- Click on the "***Connect***" button.
- If the wrong password is entered, the software connects to the device, but the same functions will be available as when connecting without a password. To try a different password, close the connection using the "***Disconnect***" button, enter the new password, and then connect again using the "***Connect***" button.
- 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. When the device is connected to USB for the very first time, the Windows operating system installs the drivers automatically.
- The connection status is indicated by the USB status icon placed in the upper left corner of the program window:

  USB disconnected (green)

  connected via USB (grey)
- After connecting using the valid password, you can configure the device, change settings, download event logs and monitor system status.
- To close the connection, click on "***Disconnect***" button.

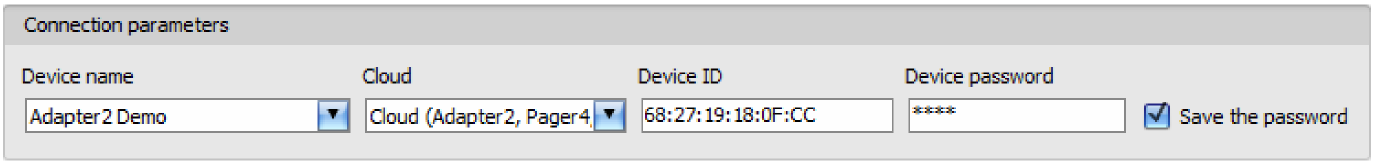
3.2.3 Remote connecting to devices via cloud service

This connection type can be used if the *Adapter2 PRO* device is connected to the cloud. For this, the APN settings must be successfully set, and a SIM card with available mobile Internet service should be installed in the device, which may use either a public or a private APN, but in the latter case, you must arrange with the mobile service provider to open the given private APN for accessing the cloud server IP address at 54.75.242.103, port: 2020.

If the “***Cloud usage***” option is enabled in the “***General***” settings menu, the device will be continuously online, so it can be accessed anytime over the cloud. If you don’t want to enable permanent cloud usage due to the data use that it involves, it is possible to command the device by SMS to connect temporarily to the cloud, about which you can read more in the below.

With this connection type, connection between the device and the **Adapter2** programming software will be established through the cloud server operated by the manufacturer.

The “***System logs***” option of the programming software cannot be used in case of remote connection over the Internet.



Connection parameters

Device name	Cloud	Device ID	Device password	
Adapter2 Demo ▼	Cloud (Adapter2, Pager4, ▼	68:27:19:18:0F:CC	****	☑ Save the password

Device name: from this drop-down menu, you can select the device you want to connect to, if you have already added the contact details of the given device in the “***Device register***” menu.

Cloud: the name of the server where the device is connected. The server named “***Cloud (Adapter2, Pager4, DUALCOM SIA IP)***” is the default. In case of using a proxy, for connecting remotely to the device, it is possible to configure a server IP address and port number different from the default server, by adding a new server in the “***Server register***” menu. If there are further servers recorded, you can choose the appropriate server for the given device in this drop-down menu from the recorded servers.

Device ID: the device identifier of the **Adapter2 PRO** device to which you want to connect to. The device identifier is unique, burned-in during production, and thereby it cannot be changed. The device ID format is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

You can read the device ID of the given device from the “***Device ID***” section in the “***Status monitoring***” menu, via USB connection. The device will also send its device ID in the reply to your request for connecting to the cloud, sent by SMS to the device, about which you can read more below.

Device password: the security password of the device (default superadmin password: **1234**).

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

Connecting to the device through the cloud:

- Select the “***Cloud***” ☁ option in the “***Connection type***” menu.
- If you have already registered the device in the "***Device register***" menu, select the device you want to connect to from the "***Device Name***" drop-down menu. Otherwise, you can either enter the data needed for connecting, in the corresponding fields, which will be recorded automatically in the device register using the entered device ID as the device name, when you start connecting to the device. For this, select the server from the “***Cloud***” drop-down menu, enter the identifier of the device in the “***Device ID***” field, and the device password in the “***Device password***” field.

  Entering the device password.
  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Administrator permission: can only access settings enabled by the superadmin. You can configure the admin password separately (see chapter “***Connection type***”).
  - Connecting remotely without a password is not possible.

- If cloud usage is enabled in the settings of the given device, the device keeps continuous connection with the cloud server. In this case skip the SMS sending process mentioned below. Cloud usage can be enabled in the “***General***” settings menu. If cloud usage is disabled, the device will not keep continuous connection with the cloud, it will only connect upon request. Therefore, if this is the case, before trying to connect remotely to the device, the request for connecting to the server should be sent by SMS to the phone number of the SIM card installed into the device. The device accepts the request for connecting to the cloud server from any phone number if the valid device password is specified in the message. For this, the device password should be added in the message using the “**PWD**” parameter, as specified below. Commands sent with a missing device password or a wrong password, will be ignored by the device and it will not send any reply to these numbers. The **PWD** parameter is not required when the command is sent from a phone number which is configured in the ***Reporting channels*** menu, in the ***User phone number settings*** section (those phone numbers are considered authorized, and can send commands without the password).

The request command for connecting to the server is: **∗CONNECT,PWD=***device password***#**

PWD: the device password can be specified using this parameter. The superadmin and admin passwords are both accepted (default superadmin password: 1234).

Example on the usage of the command mentioned above: **∗CONNECT,PWD=1234#**
When sending from an authorized phone number: **∗CONNECT#**

Send the mentioned request command for connecting to the cloud by SMS to the phone number of the SIM card installed in the device and wait for the device’s reply. As soon as the device successfully connects to the cloud, it will send the following reply:

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

If cloud usage is disabled in the device settings, the device remains connected to the cloud for 10 minutes only and thereafter in case of inactivity it disconnects automatically. Therefore, you have 10 minutes to connect to the device after it sends the reply message.

If you receive no message from the device within 1 or 2 minutes, please make sure that the settings are correct and that the circumstances of sending the request for connecting satisfy the conditions mentioned above.

Possible error messages:

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

If the APN settings are not configured in the device, or if they are wrong, you can configure this using the following SMS commands. It is also possible to configure the cloud settings, but normally the factory default values are configured for this.

SMS command	Specification
∗APN=*APN***,PWD=***device password#*	Configuring the APN
∗APN=*APN***,***username***,***password***,PWD=***device password#*	Configuring the APN along with the username and password belonging to it
∗CONNECT=*server address***:***port nr***,PWD=***device password#*	Configuring the cloud server address and port number, then connecting to the server

Example on the usage of the commands mentioned above:

∗APN=internet,PWD=1234#

∗APN=net,guest,guest,PWD=1234#

∗CONNECT=54.75.242.103:2020,PWD=1234#

Wait for the device's reply. After it has confirmed that it has connected to the cloud, continue with the next step.

- Click on the "***Connect***" ☁ button and wait for the connection to establish. The process of connecting may take a few seconds.
- The connection status is indicated by the status icon in the top left corner of the program window:

  ☁ disconnected (green)

  ☁ connected (gray)

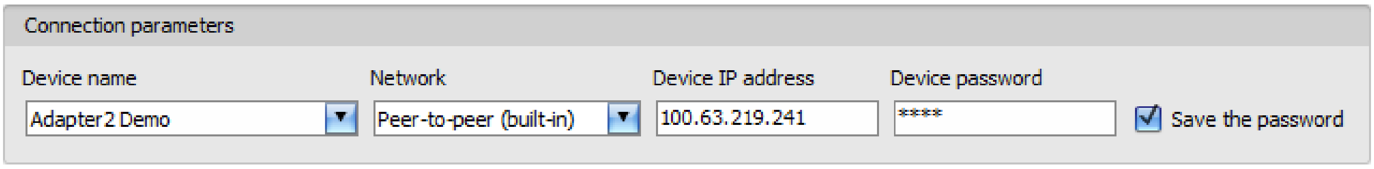
- After connecting using the valid password, you can configure the device, change settings, download event logs, and monitor system status.
- To disconnect from the device, click on the "***Disconnect***" ☁ button.

3.2.4 Remote connecting to devices via peer-to-peer connection

This connection type can only be used in a private APN, or through a virtual private network (VPN) connected to the given private APN. In case of using a private APN, sending and receiving data between the SIM cards in the given APN should be enabled. The SIM card installed in the *Adapter2 PRO* device you wish to connect remotely to, should have a static IP address and should be part of the given private APN, respectively VPN, just like the computer from which you wish to connect to the device. If the computer is not part of the given private APN through VPN, then you can connect to the device trough a mobile Internet stick connected to the computer, in which you must use a SIM card that is part of the given private APN. Also, the APN settings must be successfully set in the device you want to connect to.

With this connection type, a direct (peer-to-peer) connection will be established between the device and the **Adapter2** programming software.

The “***System logs***” option of the programming software cannot be used in case of remote connection over the Internet.



Connection parameters

Device name	Network	Device IP address	Device password	
Adapter2 Demo ▼	Peer-to-peer (built-in) ▼	100.63.219.241	****	☑ Save the password

Device name: from this drop-down menu, you can select the device you want to connect to, if you have already added the contact details of the given device in the “***Device register***” menu.

Network: the name of the network used for connecting to the device. The program contains a built-in network name “***Peer-to-peer***”, which can be used as the default. If needed, you can add further network names in the “***Server register***” menu, which you can use to organize your devices.

Device IP address: the static IP address of the device you want to connect to. You can read the device IP address of the given device from the “***IP address***” section in the “***Status monitoring***” menu, via USB connection.

Device password: the security password of the device (default superadmin password: **1234**).

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

Connecting to the device through peer-to-peer connection:

- Select the “***Peer-to-peer***” option in the “***Connection type***” menu.
- If you have already registered the device in the "***Device register***" menu, select the device you want to connect to from the "***Device Name***" drop-down menu. Otherwise, you can either enter the data needed for connecting, in the corresponding fields, which will be recorded automatically in the device register using the entered device ID as the device name, when you start connecting to the device. For this, select the network from the “***Network***” drop-down menu, enter the IP address of the device in the “***Device IP address***” field, and the device password in the “***Device password***” field.

  Entering the device password.
  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Administrator permission: can only access settings enabled by the superadmin. You can configure the admin password separately (see chapter “***Connection type***”).
  - Connecting remotely without a password is not possible.
- Click on the “***Connect***” button.
- The connection status is indicated by the status icon in the top left corner of the program window:

  disconnected (green)

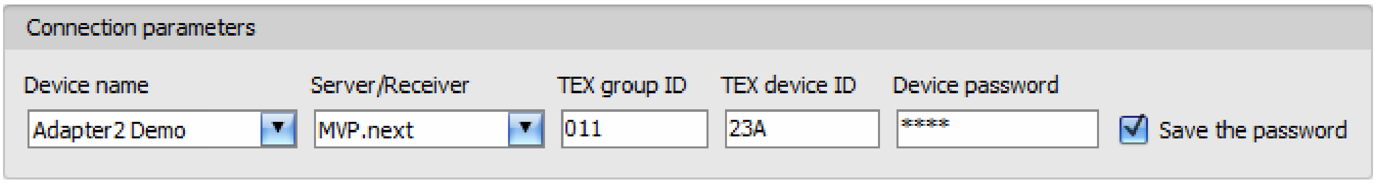
  connected (gray)
- After connecting using the valid password, you can configure the device, change settings, download event logs, and monitor system status.
- To disconnect from the device, click on the “***Disconnect***” button.

3.2.5 Remote connecting to devices which are using the TEX protocol

This connection type can be used if the *Adapter2 PRO* device you want to access remotely has been configured to communicate with the given server using the TEX protocol. This is an early custom TELL protocol which is supported by the *Adapter2 PRO* device to be able to communicate with the older TEX-MVP and TEX BASE/PRO servers. Therefore, this connection type should be used basically to connect to the device via these servers. However, for compatibility with the old TEX communicators, the TELLMon receiver and the MVP.next server also support the TEX protocol. Therefore, still this connection type should be used if the device is connected to a TELLMon receiver or an MVP.next server, and it has been configured to communicate with the given server or receiver using the TEX protocol for some reason.
Further details on the remote access of devices via the MVP.next server you can find in chapter "*Server register / Remote access of devices via the MVP.next server*".

With this connection type, connection between the device and the **Adapter2** programming software can be established through the server/receiver on which the device is online.

The "***System logs***" option of the programming software cannot be used in case of a remote connection over the Internet.



Connection parameters

Device name	Server/Receiver	TEX group ID	TEX device ID	Device password	
Adapter2 Demo ▼	MVP.next ▼	011	23A	****	☑ Save the password

Device name: from this drop-down menu, you can select the device you want to connect to, if you have already added the contact details of the given device in the "***Device register***" menu.

Server/Receiver: the name of the server or receiver where the device is connected. The server or receiver contact details should be recorded in advance in the "***Server register***" menu.

TEX group ID: the CMS identifier of the **Adapter2 PRO** to which you want to connect to. The TEX group ID can be configured in the device settings. Its format is: **FFF** (3 hexadecimal characters).

TEX device ID: the TEX identifier of the **Adapter2 PRO** to which you want to connect to. The TEX identifier can be configured in the device settings. Its format is: **FFF** (3 hexadecimal characters).

Device password: the security password of the device (default superadmin password: **1234**).

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

Connecting to the device through a server/receiver which uses the TEX protocol:

- Select the "***TEX protocol***" 🌐 option in the "***Connection type***" menu.
- If you have already registered the device in the "***Device register***" menu, select the device you want to connect to from the "***Device Name***" drop-down menu. Otherwise, you can either enter the data needed for connecting, in the corresponding fields, which will be recorded automatically in the device register using the entered device ID as the device name, when you start connecting to the device. For this, select the server from the "***Server/Receiver***" drop-down menu, where the device is connected, enter the CMS identifier in the "***TEX group ID***" field, the TEX identifier of the device in the "***TEX device ID***" field, and the device password in the "***Device password***" field. The server or receiver contact details should be recorded in advance in the "***Server register***" menu.

Entering the device password.

  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Administrator permission: can only access settings enabled by the superadmin. You can configure the admin password separately (see chapter "***Connection type***").
  - Connecting remotely without a password is not possible.

- Click the "***Connect***" 🌐 button.
- The connection status is indicated by the status icon in the top left corner of the program window:

  🌐 disconnected (green)

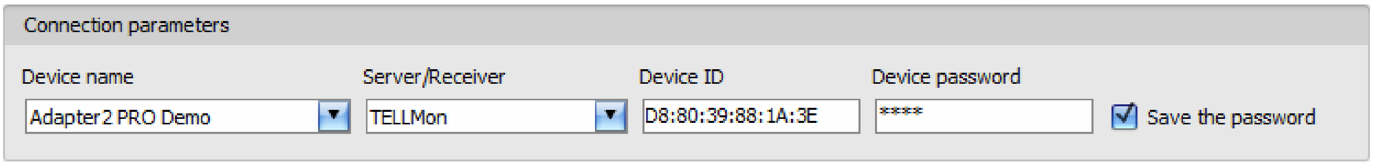
  🌐 connected (grey)
- After connecting using the valid password, you can configure the device, change settings, download event logs and monitor system status.
- To disconnect from the device, click on the "***Disconnect***" 🌐 button.

3.2.6 Remote connecting to devices which are using the TELLMon protocol

This connection type can be used if the *Adapter2 PRO* device you want to access remotely is connected to a TELLMon receiver or an MVP.next server, and it has been configured to communicate with the given server or receiver using the TELLMon protocol.
Further details on the remote access of devices via the MVP.next server you can find in chapter "*Server register / Remote access of devices via the MVP.next server*".

With this connection type, connection between the device and the **Adapter2** programming software can be established through the receiver on which the device is online.

The "***System logs***" option of the programming software cannot be used in case of remote connection over the Internet.



Connection parameters

Device name	Server/Receiver	Device ID	Device password	
Adapter2 PRO Demo	TELLMon	D8:80:39:88:1A:3E	****	☑ Save the password

Device name: from this drop-down menu, you can select the device you want to connect to, if you have already added the contact details of the given device in the "***Device register***" menu.

Server/Receiver: the name of the server or receiver where the device is connected. The server or receiver contact details should be recorded in advance in the "***Server register***" menu.

Device ID: the device identifier of the **Adapter2 PRO** device to which you want to connect to. The device identifier is unique, burned-in during production, and thereby it cannot be changed. The device ID format is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

You can read the device ID of the given device from the "***Device ID***" section in the "***Status monitoring***" menu, via USB connection, or from the user interface of the server or receiver.

Device password: the security password of the device (default superadmin password: **1234**).

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

Connecting to the device through a server/receiver which uses the TELLMon protocol:

- Select the “***TELLMon protocol***” option in the “***Connection type***” menu.
- If you have already registered the device in the "***Device register***" menu, select the device you want to connect to from the "***Device Name***" drop-down menu. Otherwise, you can either enter the data needed for connecting, in the corresponding fields, which will be recorded automatically in the device register using the entered device ID as the device name, when you start connecting to the device. For this, select the server or receiver from the “***Server/Receiver***” drop-down menu, where the device is connected, enter the identifier of the device in the “***Device ID***” field, and the device password in the “***Device password***” field. The server or receiver contact details should be recorded in advance in the “***Server register***” menu

  Entering the device password.
  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Administrator permission: can only access settings enabled by the superadmin. You can configure the admin password separately (see chapter “***Connection type***”).
  - Connecting remotely without a password is not possible.
- Click on the “***Connect***” button.
- **The *Adapter2 PRO* device that communicates using the TELLMon protocol is not online continuously. The device connects to the server or receiver only when it sends a supervision message or reports an event. Therefore, after clicking on the “*Connect*” button, you will have to wait for the device until it next connects to the server or receiver to send a supervision message or report an event. This is the moment when the programming software can connect to the device. Therefore, if the device is configured to rarely send supervision messages to the server or receiver, the programming software can connect to the device after a long time only (depending on the configured supervision message sending interval).**
- The connection status is indicated by the status icon in the top left corner of the program window:

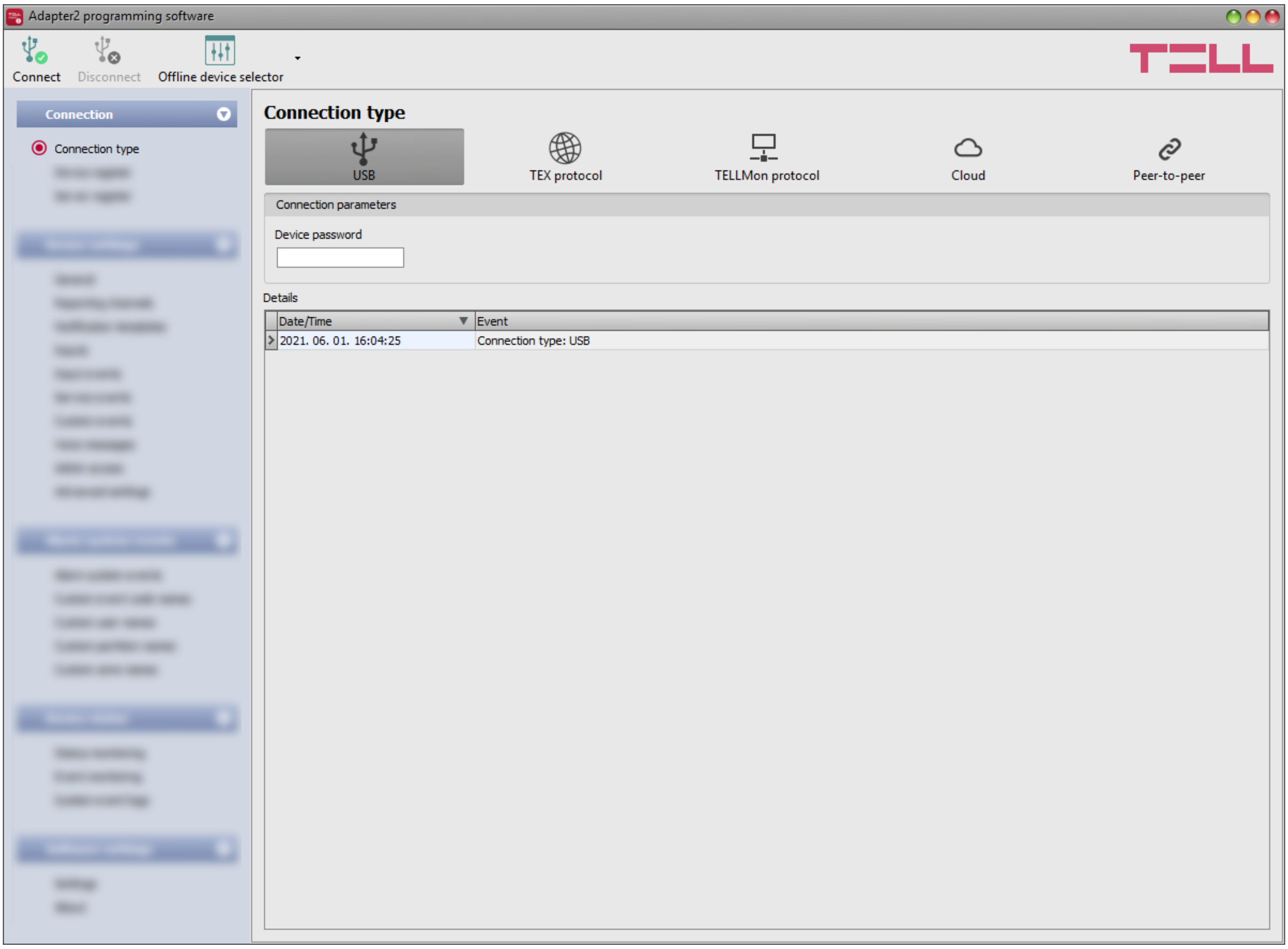
  disconnected (green)

  connected (gray)
- After connecting using the valid password, you can configure the device, change settings, download event logs, monitor system status, and perform controls.
- To disconnect from the device, click on the “***Disconnect***” button.

4 Adapter2 programming software usage and feature descriptions

4.1 Connection menu

4.1.1 Viewing the settings options and configuring offline



Connection type

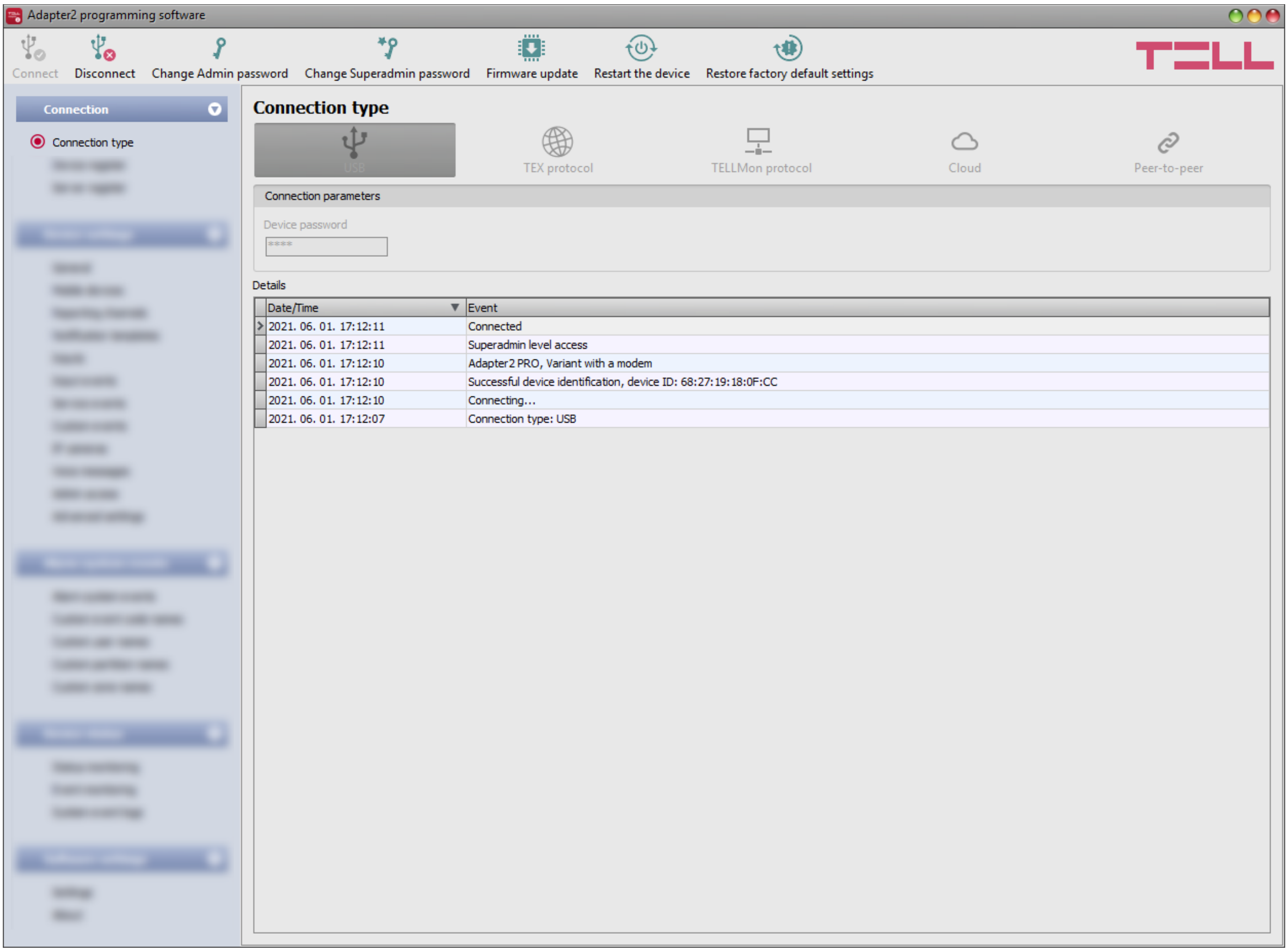
Date/Time	Event
2021. 06. 01. 16:04:25	Connection type: USB

The **Adapter2** programming software supports all **Adapter2** device models. Therefore, the software shows the settings options available specifically in a given device model, which are different from the common parameters, only when connecting the given device model, i.e., an **Adapter2** device must be connected in order to show the specific settings options of that device model.

However, using the “***Offline device selector***” it is possible to view the settings options of any **Adapter2** device model and to configure and save the settings in advance offline, without connecting the device.

If you wish to view the settings options of a **Adapter2** 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.

4.1.2 Connection type



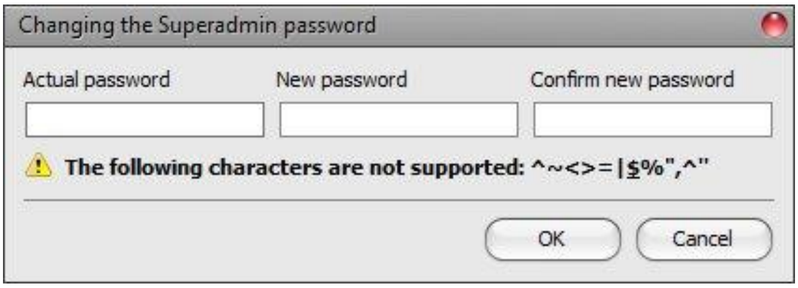
Connection type

Date/Time	Event
2021. 06. 01. 17:12:11	Connected
2021. 06. 01. 17:12:11	Superadmin level access
2021. 06. 01. 17:12:10	Adapter2 PRO, Variant with a modem
2021. 06. 01. 17:12:10	Successful device identification, device ID: 68:27:19:18:0F:CC
2021. 06. 01. 17:12:10	Connecting...
2021. 06. 01. 17:12:07	Connection type: USB

In the “***Connection type***” menu you can select the method for connecting to the device (USB or different options for connecting over the Internet), view information about the connection process, change the admin and superadmin passwords, restart the device, and restore the factory default settings in the device.

The default superadmin password is **1234**. If you want to use the admin level access as well, for this the password should be configured separately by clicking on the “***Change Admin password***” button (for “***Actual password***” enter the superadmin password).

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



The following characters are not supported: ^~<>=|$%",^"

Available options:

- **Change Admin password**:

  You can change the administrator level password after clicking on this button.

- **Change Superadmin password**:

  You can change the superadministrator level password after clicking on this button.

Enter the actual password, then the new password and its confirmation, then click “***OK***”. 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: ^ ~ < > = | $ % " '.

- Updating the firmware:
  By clicking on the “***Firmware update***” button, you can update the firmware of the device. Clicking on this button will open a new window, where you can browse the firmware file with the **tf3** extension. When uploading the firmware is finished, the window that shows the progress will close automatically, and then 5 seconds later, the device will restart with the new firmware.

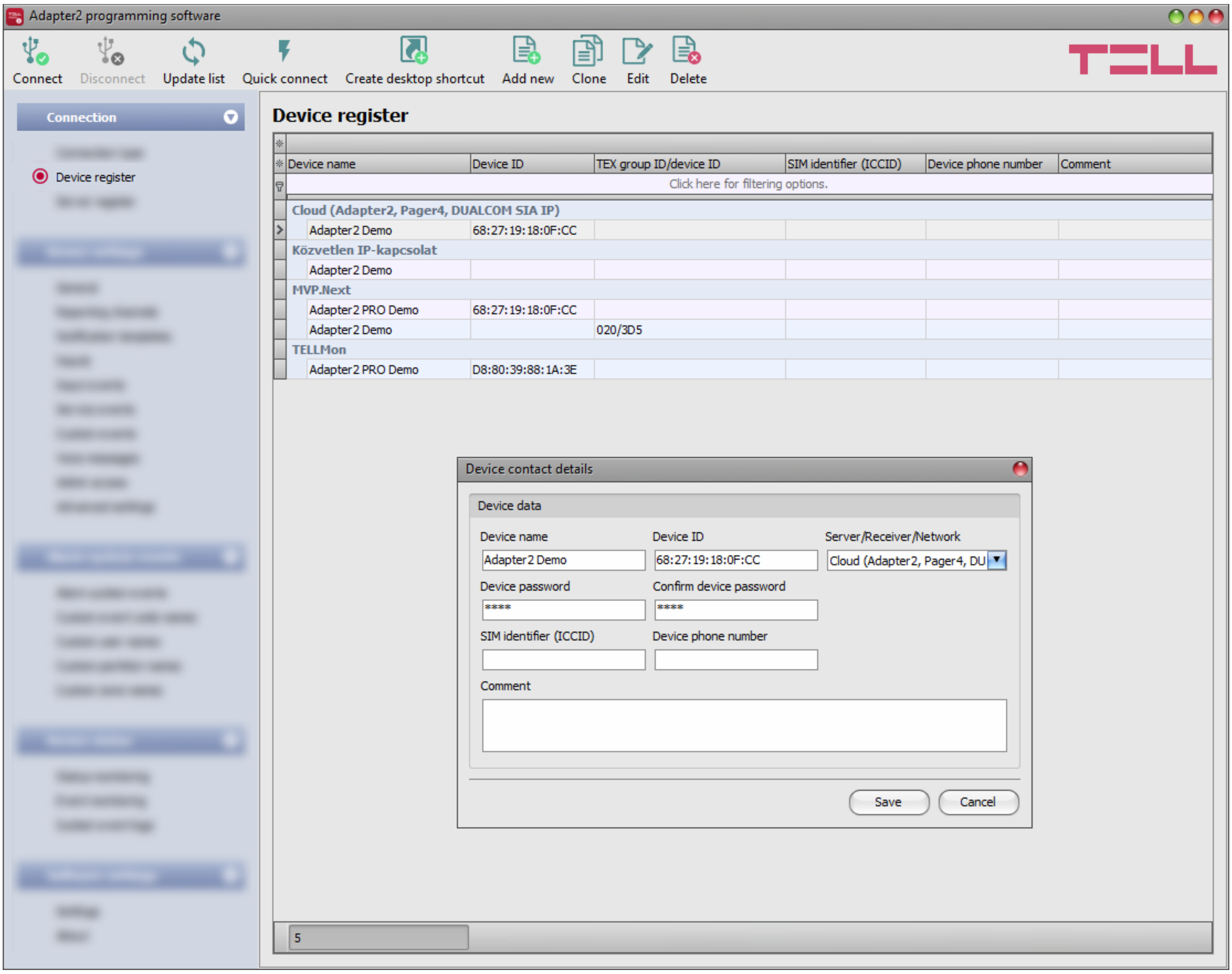
- Restart the device:
  If necessary, you can restart the connected device by clicking on this button.

- Restore factory default settings:

  By clicking on this button, you can restore the factory default settings in the device. Restoring the factory default settings will erase the actual settings, therefore please save your settings if needed. The reset process may take more than 1 minute and involves a device restart. Wait until the device restarts and the **STATUS** LED on the device shows activity again.

  The option of restoring the factory default settings is also available when you connect to the device without entering the device password. Restoring the factory default settings will be refused by the device if the “***Locked***” option has been selected in the “***Locking the device***” section, in the “***Advanced settings***” menu. In this case, the software will show an error message about that, after the information message shown right after the confirmation. If you have forgotten the superadmin password, and the device has been locked with the mentioned option, only the manufacturer can restore the factory default settings in the service center.

4.1.3 Device register



Device register

Click here for filtering options.

Device name	Device ID	TEX group ID/device ID	SIM identifier (ICCID)	Device phone number	Comment
Cloud (Adapter2, Pager4, DUALCOM SIA IP)					
Adapter2 Demo	68:27:19:18:0F:CC				
Közvetlen IP-kapcsolat					
Adapter2 Demo					
MVP.Next					
Adapter2 PRO Demo	68:27:19:18:0F:CC				
Adapter2 Demo		020/3D5			
TELLMon					
Adapter2 PRO Demo	D8:80:39:88:1A:3E				

5

Device contact details

Device data

Device name: Adapter2 Demo
Device ID: 68:27:19:18:0F:CC
Server/Receiver/Network: Cloud (Adapter2, Pager4, DU
Device password: ****
Confirm device password: ****
SIM identifier (ICCID):
Device phone number:
Comment:

Save Cancel

The device register serves for storing and easy handling of device contact details used for remote programming. You can add new device contact details to the database and edit, delete, and clone entries for easy adding of devices with similar contact details.

When connecting remotely, you can easily select by name the device you wish to connect to from the "***Device name***" drop-down menu, from the devices added to the database. You can also connect remotely to a device directly from the device register, by selecting the device, and then clicking on the ***Quick connect*** button.

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

If you enter new device contact details in the "***Connection type***" menu, the program will add this automatically to the device register database using the device ID or the device IP address as device name (depending on the connection type), which you can change later by editing the given record in the device register. The database is stored locally on the computer.

If needed, you can import a database exported from an earlier version of the program using the **MMTool** software that can be installed together with the programming software. The **MMTool** software is included in the programming software setup package and can be selected for installation in the setup wizard.

If your devices are connected to an MVP.next server and you have a registered MVP.next remote monitoring account, it is possible to read and save the data of your devices automatically in the device register. You can find the details on this in chapter “***Server register***”.

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

: update the records from database

: quick remote connect to the selected device

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

: add new device

: clone entry (duplicate)

: edit entry

: delete entry

Data stored in the device register:

Device name: custom device name

Device ID: the unique device identifier, which is burned-in during production, and therefore it cannot be changed. If the device is connected via USB, the software will read the device ID automatically from the device and will paste the data in this field when you add a record with new device contact details. If automated reading fails, you can enter the device ID manually or copy it from the “***Status monitoring***” menu.
The format of the device identifier is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

Server/Receiver/Network: you can configure multiple remote contact details for the same device (Cloud, TELLMon, MVP.next, TEX-MVP, Peer-to-peer), according to what type of server or receiver the device connects to. The contact details of the servers or receivers should be recorded in advance in the “***Server register***” menu, and then, in this drop-down menu you can choose from the servers and receivers recorded there, to associate with the given device. If a device is available on multiple servers or receivers, and you want to record the contact details of the given device for all these, you can do this by adding separate records, and selecting the appropriate server or receiver for each record.

For devices with a “***Peer-to-peer***” connection, you can add custom “networks” in the “***Server register***” menu, which you can use to organize these devices by associating them with the added networks in the “***Device register***” menu. If you do not want to organize the devices that can be accessed via peer-to-peer connection, associate these devices with the default “***Peer to peer***” network.

Protocol (for the MVP.next server only): select the communication protocol used by the device (TELLMon or TEX). The SIA DC-09 protocol is not available because the SIA DC-09 does not support remote programming.

TEX group ID (for the TEX protocol only): the CMS identifier configured in the device settings, necessary for the TEX protocol. The format of the TEX device ID is: **FFF** (3 hexadecimal characters).

TEX device ID (for the TEX protocol only): the TEX identifier configured in the device settings, necessary for the TEX protocol. The format of the TEX device ID is: **FFF** (3 hexadecimal characters).

Device IP address: the IP address of the SIM card installed in the device. The peer-to-peer connection only works with a static IP used in a private APN. If the device is connected via USB and the SIM card is installed, and the device has successfully received an IP address from the network, the software will read the IP address automatically from the device and will paste the data in this field when you add a record with new device contact details. Otherwise, you can also enter the IP address manually.

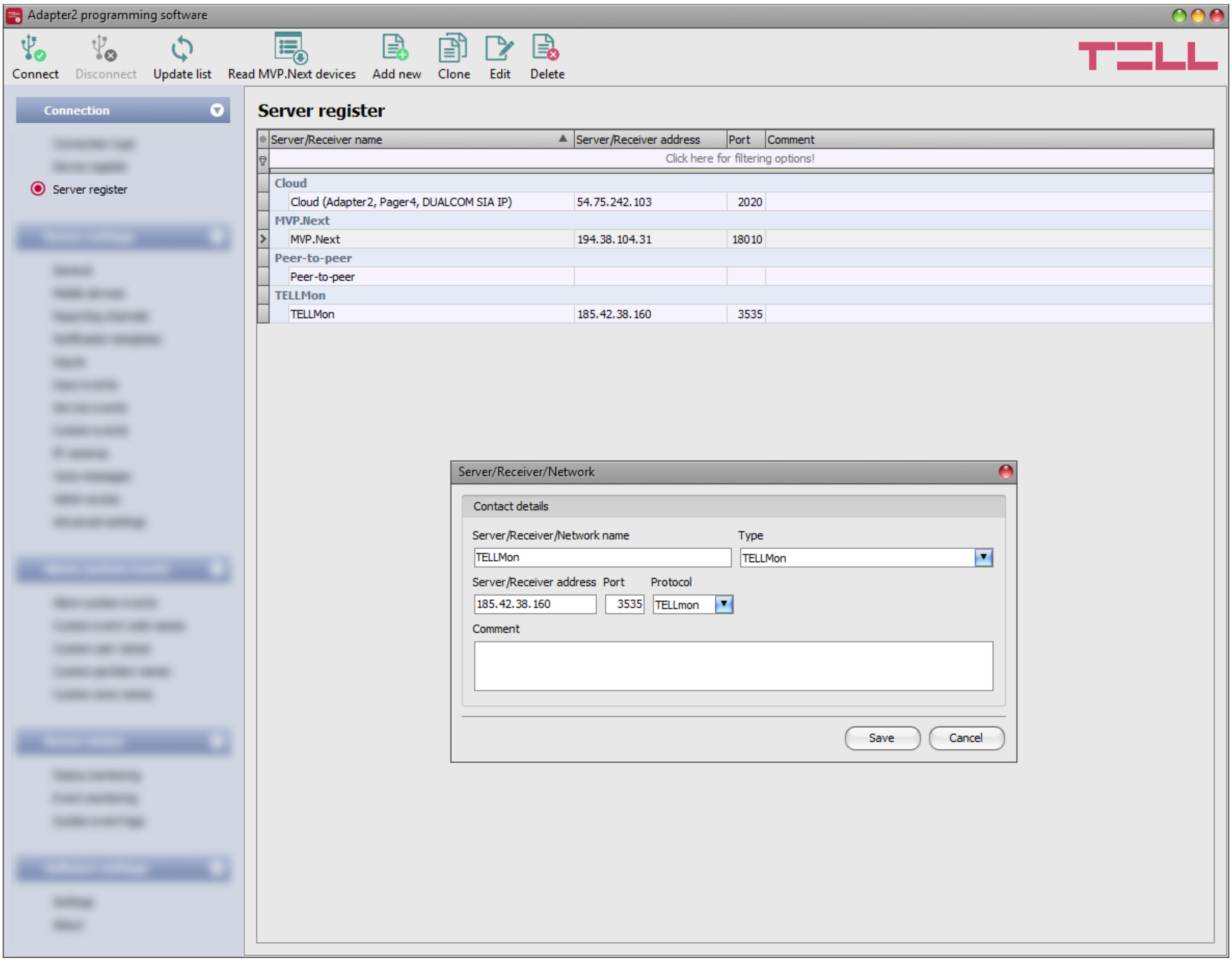
Device password/Confirm device password: the superadmin or admin password configured in the given device, depending on which one you want to use for connecting to the device.

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 software will read the ICCID automatically from the device and will paste the data in this field when you add a record with new device contact details. If automated reading fails, you can enter the ID manually, or copy from the "***Status monitoring***" menu. The ICCID has no specific function, its purpose is informational.

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

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

4.1.4 Server register



Server register

Server/Receiver name	Server/Receiver address	Port	Comment
Click here for filtering options!			
Cloud			
Cloud (Adapter2, Pager4, DUALCOM SIA IP)	54.75.242.103	2020	
MVP.Next			
MVP.Next	194.38.104.31	18010	
Peer-to-peer			
Peer-to-peer			
TELLMon			
TELLMon	185.42.38.160	3535	

Server/Receiver/Network

Contact details

Server/Receiver/Network name: TELLMon
Type: TELLMon
Server/Receiver address: 185.42.38.160
Port: 3535
Protocol: TELLmon
Comment:

The server register is used for storing the contact details of the monitoring servers and receivers and to facilitate quick remote connecting to the devices. In the “***Server register***” menu you can record your monitoring servers and receivers, and then you can associate them with your devices in the “***Device register***” menu, when recording the contact details of your devices. You can add new server or receiver contact details to the database, and edit, delete, and clone entries for easy adding of servers or receivers with similar contact details.

If needed, for devices with a “***Peer-to-peer***” connection, you can add custom “networks”, which you can use to organize these devices by associating them with the added networks in the “***Device register***” menu. The program contains a built-in “network” named “***Peer-to-peer***”, which can be used as the default.

If you are using the device in in a private network, where there is no option to enable access to the cloud server, the program offers an option to add custom cloud contact details here in the “***Server register***” menu. This can be an IP address and port number available in the given private network, which you can then select as the default cloud server in the device settings, in the “***General***” menu. Thus, it is not necessary to enable access to the cloud server in the private network, just configure port forwarding from the chosen IP address and port number to the cloud IP address and port number (**54.75.242.103:2020**)

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

: update the records from database

: read devices from MVP.next server

: add new server, receiver or network

: clone entry (duplicate)

: edit entry

: delete entry

Data stored in the server register:

Server/Receiver/Network name: custom server, receiver, or network name.

Type: the server, receiver. or network type (Cloud, TELLMon, Peer-to-peer, MVP.next).

Server/Receiver address: the IP address or domain name of the server or receiver.

Port: the communication port number of the server or receiver.

Protocol (for the TELLMon receiver only): the communication protocol used by the receiver (TELLMon or TEX). If there are devices connected to the receiver mixed, through both protocols, it is necessary to add the receiver with both protocols separately in the register, to access all devices.

Company ID (for the MVP.next server only): the registered company ID is required only for the MVP.next server.

Client username (for the MVP.next server only): the username configured for the “***Programming software***”-type client application on the MVP.next server’s user interface (see details below).

Client password/Confirm client password (for the MVP.next server only): the password configured for the given client username on the MVP.next server’s user interface (see details below).

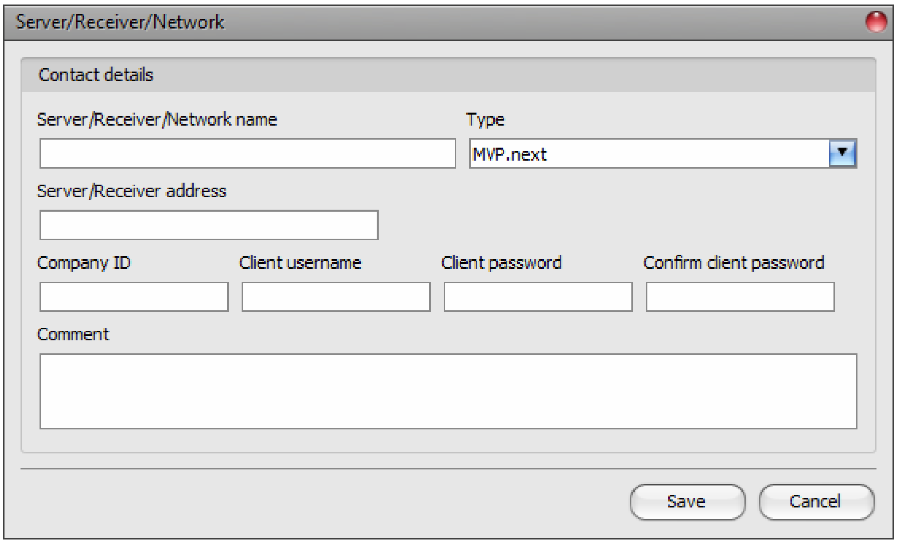
Comment: in this field you can enter custom comments related to the given server, receiver, or network.

Remote access of devices via the MVP.next server:

If your devices are connected to an MVP.next server and you have a registered MVP.next remote monitoring account, it is possible to download and save the data of your devices automatically in the device register.

Through the MVP.next server it is only possible to download the data of your devices, and access your devices remotely with a registered programming software (client application). Therefore, it is necessary to register your programming software as follows:

- Sign in into your MVP.next account on the server's user interface.
- Add a "***Programming software***"-type client application with a unique username and password in the **Settings→Client applications** menu.
- Associate the client application with the desired device group or groups that contain the devices you want to access remotely.
- Add an "***MVP.next***"-type server in the server register, in the programming software, and enter the company ID of your MVP.next account and the username and password configured for the registered "Programming software"-type client application.



Type: MVP.next

- To download the data of your devices from the server, select the added server in the list by clicking on it, and then click on the "***Read MVP.next devices***" button. If the provided credentials are correct, the program will download the device list along with the data of your devices and will save them in the device register. After a successful device list download it is possible to connect remotely to your devices in the "***Connection type***" menu, after selecting the appropriate protocol button (TELLMon or TEX).

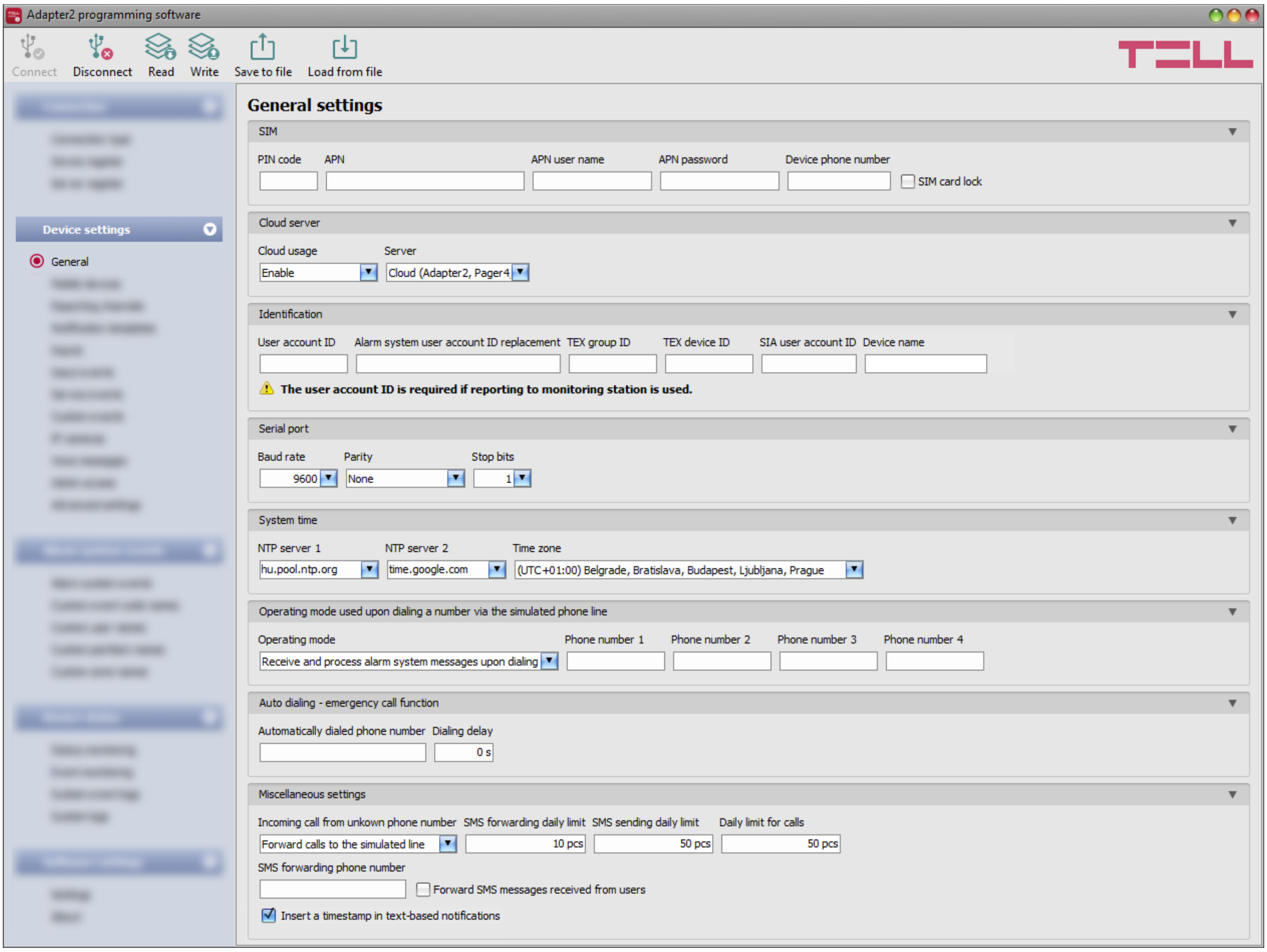
Attention! You can use the registered client username and password in any other programming software that supports the MVP.next, but you can connect to the server with one software only at the same time, using the same username. If you want to use more than one programming software simultaneously, you need to register each software separately as client-type programming software on the server, with different usernames.

4.2 Device settings menu

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

- **Changing the device settings**: To change the device settings, first you must read the actual settings from the device by clicking the "***Read***" button in a submenu in either "***Device settings***" or "***Alarm system events***" menu. Writing the new settings into the device using the "***Write***" 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***" button.
- **Overwriting the device settings**: If you want to completely overwrite the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the desired settings in the submenus, and then click on the "***Save to file***" button in the "***General***" device settings menu. You can import the saved backup into the program using the "***Load from file***" button, and then write imported settings into the device by clicking on the "***Write***" button. This is useful when you want to configure many devices with the same settings.

4.2.1 General device settings



General settings

SIM

PIN code:
APN:
APN user name:
APN password:
Device phone number:
□ SIM card lock

Cloud server

Cloud usage: Enable
Server: Cloud (Adapter2, Pager4

Identification

User account ID:
Alarm system user account ID replacement:
TEX group ID:
TEX device ID:
SIA user account ID:
Device name:

⚠ **The user account ID is required if reporting to monitoring station is used.**

Serial port

Baud rate: 9600
Parity: None
Stop bits: 1

System time

NTP server 1: hu.pool.ntp.org
NTP server 2: time.google.com
Time zone: (UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Operating mode used upon dialing a number via the simulated phone line

Operating mode: Receive and process alarm system messages upon dialing
Phone number 1:
Phone number 2:
Phone number 3:
Phone number 4:

Auto dialing - emergency call function

Automatically dialed phone number:
Dialing delay: 0 s

Miscellaneous settings

Incoming call from unkown phone number: Forward calls to the simulated line
SMS forwarding daily limit: 10 pcs
SMS sending daily limit: 50 pcs
Daily limit for calls: 50 pcs
SMS forwarding phone number:
□ Forward SMS messages received from users
☑ Insert a timestamp in text-based notifications

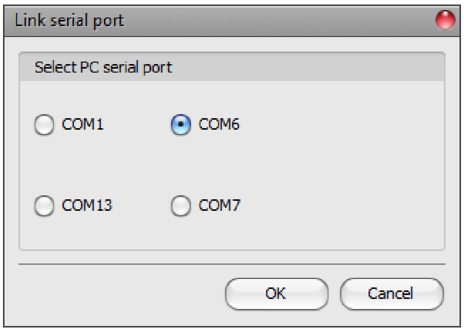
In this menu you can configure the general settings of the device.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Saving settings to file:
  To save all device settings to file, click on the "***Save to file***" button.
- Loading settings from file:
  To load saved settings from file, click on the "***Load from file***" button.

- Link remote serial port:

  This button is only available when connected remotely. Clicking on this button, you can create a serial data connection between the device's RS232 or TTL port and the selected PC communication port (e.g., for remote programming of an alarm control panel connected to the serial port of the device). Clicking on this button again, you can close the serial data connection. For using this function to remotely program an alarm control panel, a third-party software is required (e.g., com0com) that can create a linked pair of virtual serial ports. Data flow (functional check) is indicated by the two blue (RX / TX) status indicators showing up next to the serial port settings.

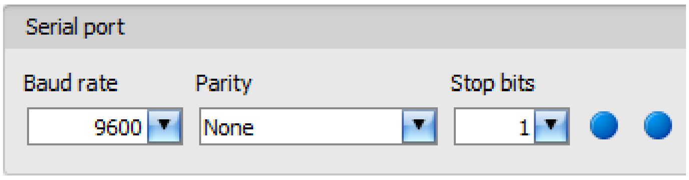


Link serial port

Select PC serial port

○ COM1 ● COM6

○ COM13 ○ COM7



Serial port

Baud rate: 9600

Parity: None

Stop bits: 1 ● ●

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

SIM:

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

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

> **Note: If automatic APN setting fails (the device does not get an IP address), configure the APN even if you don't want to use the device with an Internet connection, because with certain service providers it happens that without that the modem cannot connect to the mobile network at all, or it does not receive a time setting from the network.**

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

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

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

SIM card lock: if you enable this option, the device will remember the ID of the SIM card installed, and will refuse to operate with any other SIM card until the option is disabled.

Cloud server:

Cloud usage: if this option is enabled, the device will connect to the cloud server operated by the manufacturer and will stay connected permanently. To ensure a continuous connection and availability, the device sends supervision messages that use about **12 MB data per month** on its own. Using the cloud server, special services become available, such as remote programming and remote monitoring of your device over the cloud. If this option is enabled, the device will always be online and thereby accessible anytime. If this option is disabled, you can still initiate a temporary cloud connection manually, by sending a command via SMS to the phone number of the device. You can read more about this in the "***Remote connecting to devices via cloud service***" paragraph. In case of using a SIM card that uses a private APN, the given private APN should be opened at the mobile service provider to access the cloud server IP address at 54.75.242.103, port: 2020.

Server: you can select the default cloud server in this drop-down menu. If you are using the device in in a private network, where there is no option to enable access to the cloud server, the program offers an option to add custom cloud contact details in the "***Server register***" menu. This can be an IP address and port number available in the given private network, which you can then select as the default cloud server in this drop-down menu. Thus, it is not necessary to enable access to the cloud server in the private network, just configure port forwarding from the chosen IP address and port number to the cloud IP address and port number (**54.75.242.103:2020**).

Identification:

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

Alarm system user account ID replacement: if you enter a user account identifier in this field, the device will replace the user account ID in the Contact ID messages received from the connected alarm system, configured in the alarm control panel, with the identifier number entered here, and will send the messages to the remote monitoring station with this user account ID. This option comes handy when you want to change the user account ID in the alarm control panel, but you have no access to its settings.

TEX group ID: the CMS identifier in hexadecimal format. This is only required if the TEX protocol is used for reporting to CMS. If you do not possess this identifier, please contact your reseller.

TEX device ID: the device identifier in hexadecimal format. This is only required if the TEX protocol is used for reporting to CMS. The length is 3 characters, and the following characters can be used: 0…9, A, B, C, D, E, F.

SIA user account ID: in case of using the SIA IP protocol, the supervision messages are sent to CMS using the user account ID configured in this section. The length of the SIA user account ID is 1 to 6 hexadecimal characters, and the following characters can be used: 0..9, A, B, C, D, E, F. Do not fill in the account ID section with zeros!

Device name: in this field you can enter a custom name for your **Adapter2 PRO** device. The system will use this name in the subject of e-mail notifications.
Attention! The following characters should not be used: ^ ~ < > = ' " , | ? $ & %

Note! The user account ID, group ID, device ID and SIA user account ID are only needed if reporting to CMS is used.

Serial port:

In this section you can configure the transparent RS232/TTL serial port settings. The serial port on the device enables transparent data communication between the device and the ***Remote Serial Client*** software developed for this purpose, or the ***Adapter2*** programming software. The purpose of the serial port is to enable remote programming of the alarm control panel connected to the device, over the Internet. Configure the settings according to the requirements of the device (alarm control panel or other device) connected to the serial port of the ***Adapter2 PRO***.
Available options: baud rate, parity and stop bits.
You can find further help on how to configure the serial port for use with the most popular alarm systems, in paragraph "***Remote programming of alarm control panels***".

System time:

NTP server 1,2: in this section you can select one of the default NTP servers or you can also configure custom NTP servers which you wish to use for system time synchronization. The device synchronizes the system time from the GSM network and if this fails, it will use the NTP servers. If synchronization from the NTP servers also fails, it will synchronize the date and time using the timestamp received from a CMS server/receiver, if CMS is used.

Time zone: select the time zone according to the location of installation. The device adjusts the system time according to the time zone setting. If the setting is wrong, there will be difference between the system time and the local time and therefore the timestamps of the events will also be wrong, and the periodic test report will also be sent at the wrong time of day.

Operating mode used upon dialing a number via the simulated phone line:

Operating mode:

- **Start a GSM voice call upon any dialed phone number:** the device will not send the handshake signal but will initiate a GSM voice call to the dialed phone number and will make possible DTMF communication or speech through the simulated phone line. The device will also send the report via IP in parallel with the DTMF-based reporting.
- **Receive and process alarm system messages upon dialing the specified numbers; for other phone numbers start a GSM voice call:** you can configure up to 4 phone numbers and if the alarm control panel dials one of these through the simulated phone line, the device will send the handshake signal and will receive the reports of the alarm control panel, respectively will send these over IP according to the settings. If the alarm control panel dials a different phone number which is not configured in this section, the device will initiate a GSM voice call to the dialed phone number and will make possible DTMF communication or speech through the simulated phone line. This function offers the possibility for backup reporting to DTMF receivers. For this, the alarm control panel should be configured such way, that if reporting to the phone numbers (max. 4) specified in this section fails, the alarm control panel should call a different phone number (the DTMF receiver's number) to which the device will already initiate a GSM voice call. The device will also send the report via IP in parallel with the DTMF-based reporting.
- **Receive and process alarm system messages upon any number dialed:** no matter what number the alarm control panel dials through the simulated phone line, the device will automatically send the handshake signal and will receive the reports of the alarm control panel, respectively will send these over IP according to the settings. This option can be used for easy alignment if you wish to send reports only over IP, but you do not know what number the alarm control panel dials or cannot change that.

If you connect an alarm control panel to the simulated line, no matter which operating mode you choose, the device will process alarm system messages received or passed through by call. Thereby, it is possible to send further notifications (voice call, SMS, Push, e-mail) about these messages, according to the alarm system event settings. The difference between the operating modes is just that the device will or will not pass through the call to the GSM network, depending on the number dialed by the alarm control panel.

Configure the connected alarm control panel to wait for the dial tone before dialing!

Attention! Please note that in certain cases you may experience issues with reporting to CMS over DTMF-based voice call. Success of communication highly depends on the properties of the given GSM network, such as line quality, line noise and DTMF handling. Due to network digitalization, DTMF signal tones might get distorted while being processed by the network in such extent that the receiver will not be able to interpret the transmitted Contact ID event codes. The risk of this is even higher if the signal is transmitted through multiple GSM operators (e.g., if using SIM cards from different operators on the transmission and reception site). The device offers an option to adjust the signals to correct such problems, therefore, if necessary, special DTMF communication parameters can be configured in the "***Advanced settings***" menu.

Auto dialing – emergency call function:

Automatically dialed phone number: this function can be used for some special applications (e.g., automatic emergency call). If configured so, the device will dial the given number automatically through the GSM network after the delay configure in the "***Dialing delay***" section, upon picking up the receiver of the landline phone device connected to the ***Adapter2 PRO***. When the automatic dialing function is used, the device can also be used with an alarm control panel, if an appropriate dialing delay is configured.

Due to security reasons, the auto dialing feature is not available if "***Receive and process alarm system messages upon any number dialed***" option is selected under "***Operating mode***".

Dialing delay: the device will dial the phone number configured in the "***Automatically dialed phone number***" section after the delay configured here, when it detects off-hook on the simulated line output. If you wish to use the auto dialing function when the device is being used with an alarm control panel, configure the dialing delay so that the alarm control panel should have enough time to start dialing the number it has to call, still before the device starts dialing the number to be called automatically. The device will not make a call to the number to be dialed automatically if it detects dialing on the simulated line during the configured dialing delay. In this case it will manage the communication received through the simulated line.

Miscellaneous settings:

Incoming call from unknown phone number: in this section you can configure what the device should do when it receives a call from a phone number which is not configured in the device as a user phone number, or a call from private number (with hidden caller ID).

Available options:

- **Forward calls to the simulated line**: the device will forward these calls to the simulated phone line output (**LINE**). If a landline phone device is connected to the line output, the phone will ring, and speech communication is possible after accepting the call. Regardless of this setting, when a call is received from an unknown phone number, a related service event is generated for which you can configure output control or notification sending.
- **Reject calls**: the device will reject calls received from the given phone number.

SMS forwarding daily limit: with this setting you can limit the number of SMS messages to be forwarded per day. When the configured limit is reached, the device will not forward new incoming SMS messages for 24 hours. After 24 hours the message counter resets automatically, and incoming messages will be forwarded again up to the configured limit. When the limit is reached, a service event will be generated, which you can configure separately to control the output(s) or send notifications. The SMS forwarding daily limit can be disabled and set to unlimited by deleting the entered value.

> **Attention!** After reaching the configured limit, but before the message counter resets, the device deletes all incoming messages without forwarding!

SMS sending daily limit: with this setting you can limit sending of SMS messages generated by events. When the configured limit is reached, the device will not send further event-generated SMS messages for 24 hours. After 24 hours the message counter resets automatically, and SMS message sending will be enabled again up to the configured limit. When the limit is reached, a service event will be generated, which you can configure separately to control the output(s) or send notifications. The SMS sending daily limit can be disabled and set to unlimited by deleting the entered value.

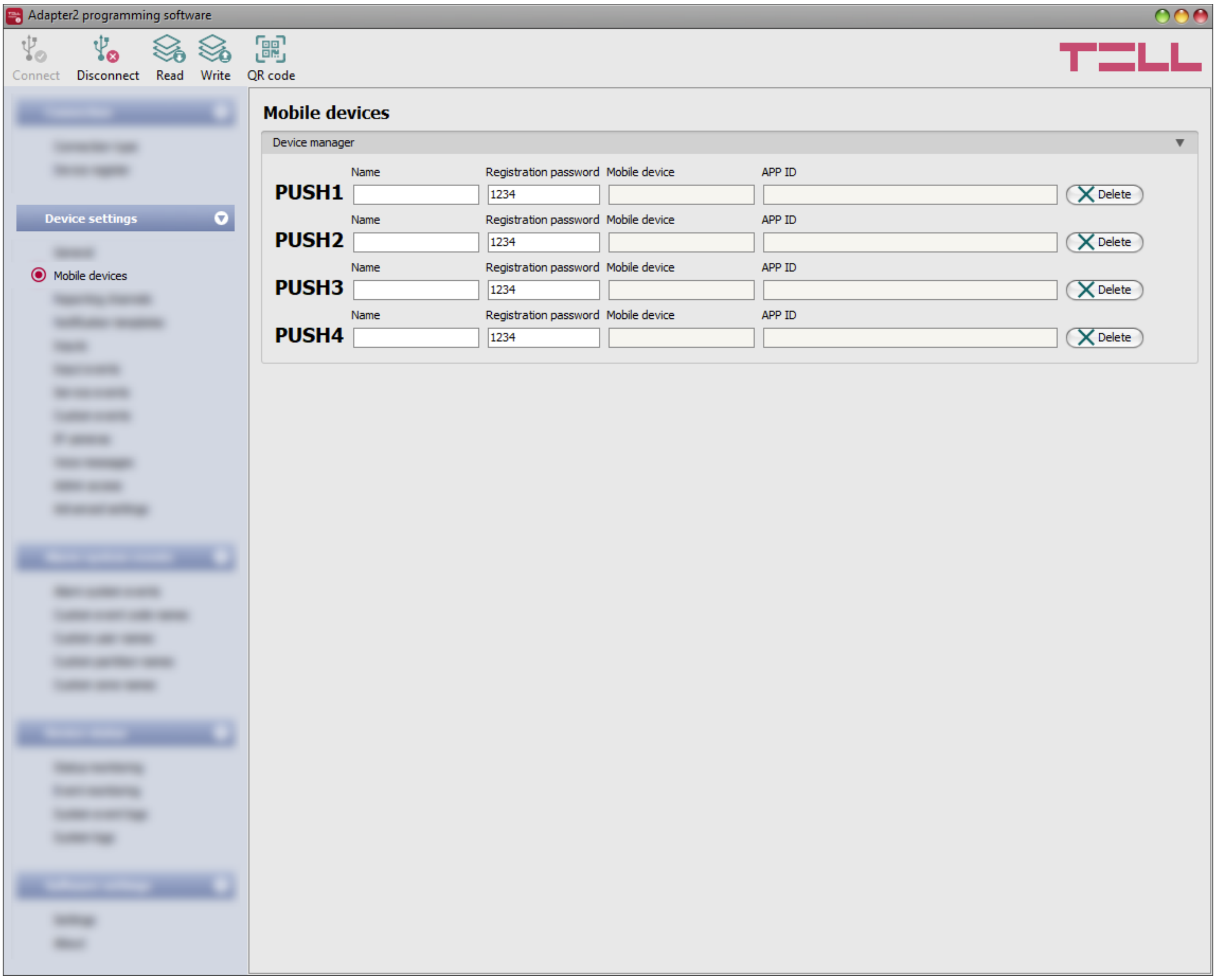
Daily limit for calls: with this setting you can limit the number of voice calls generated by events. When the configured limit is reached, the device will not make further event-generated calls for 24 hours. After 24 hours the call counter resets automatically, and voice calls will be enabled again up to the configured limit. When the limit is reached, a service event will be generated, which you can configure separately to control the output(s) or send notifications. The daily limit for calls can be disabled and set to unlimited by deleting the entered value.

SMS forwarding phone number: the device forwards the messages received by its SIM card to the phone number configured in this section (e.g., balance information received from the GSM service provider in case of pre-pay card). The received messages are deleted automatically after forwarding. If no phone number is configured, the device deletes all incoming messages without forwarding.

Forward SMS messages received from users: if this option is enabled, the device will also forward SMS messages received from user phone numbers configured in the “***Reporting channels***” menu (e.g., commands sent to the device via SMS), to the phone number entered in the “***SMS forwarding phone number***” field. If this option is disabled, the device will only forward messages received from other phone numbers, but not messages received from users.

Insert a timestamp in text-based notifications: if this option is enabled, the device will insert a timestamp in each text message at the beginning, which indicates the time of occurrence of the given event.

4.2.2 Mobile devices



Mobile devices

Device manager

	Name	Registration password	Mobile device	APP ID	
PUSH1		1234			✕ Delete
PUSH2		1234			✕ Delete
PUSH3		1234			✕ Delete
PUSH4		1234			✕ Delete

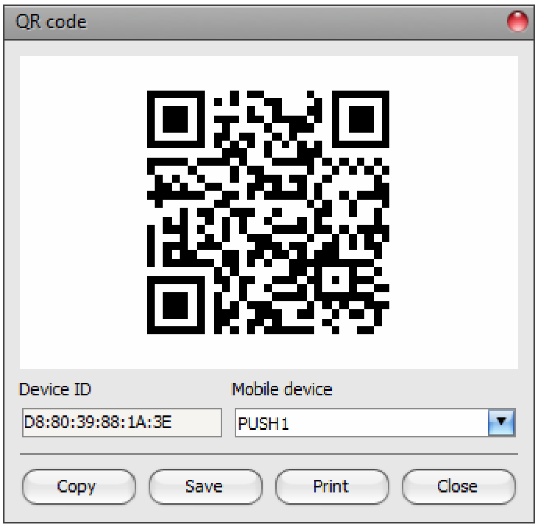
In this menu you can manage the access of mobile applications. The device supports access of up to 4 mobile devices, for which you can configure here the registration password requested upon assigning the mobile application to the device, and it is also possible to delete a mobile device if needed, i.e., to cancel its registration. The mobile application can be assigned to the device with the help of a QR code, which you can generate by clicking on the "***QR code***" button.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.

- QR code:

  The “***QR code***” button can be used to generate the QR code necessary for assigning the mobile application to the device. The QR code includes connection data: device ID, server IP address and port number, and the sequence number of the mobile device / user (1 to 4).



QR code

Device ID: D8:80:39:88:1A:3E

Mobile device: PUSH1

A different QR code belongs to each mobile device (1 to 4). You can select the desired mobile device using the “***Mobile device***” drop-down menu. The QR code selected this way can be copied to clipboard, saved to file, or printed by clicking on the appropriate buttons.

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

Device manager:

In case of assigning a mobile application to the ***Adapter2 PRO*** device, receiving alerts from the device will become available through Push notification too. For this, when configuring events, you can select which of the up to 4 (**PUSH1…PUSH4**) assigned mobile devices you wish to receive a Push notification on when the given event occurs.

Name: the name of mobile device’s user. The name entered in this section will be used to identify the mobile devices when selecting the notification channels upon configuring events.

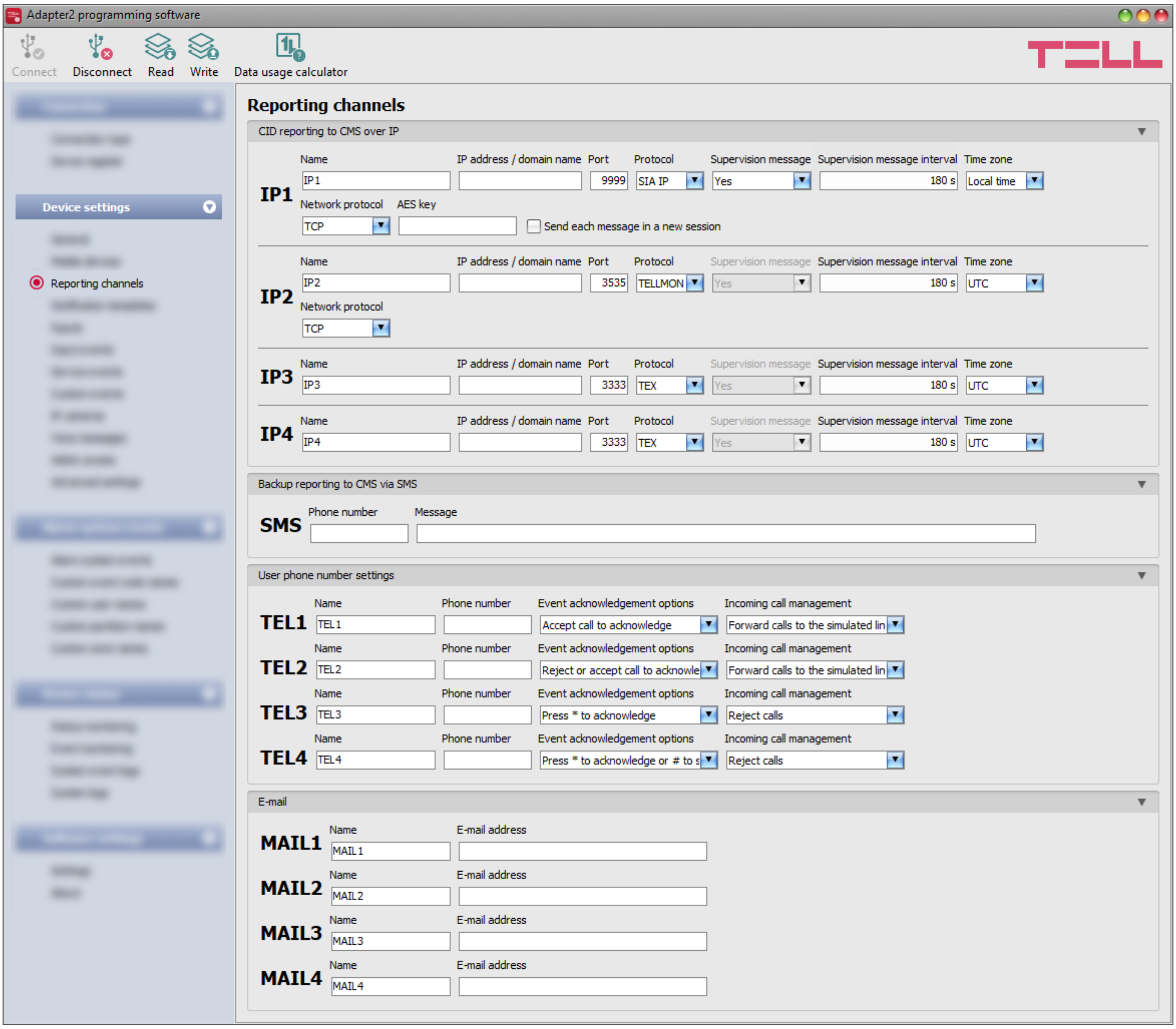
Registration password: the registration password must be provided in the mobile application when you wish to assign it to the device. This password can be configured in this section separately for each mobile device you wish to register. The registration password length is 4 to 8 characters and only letters and numbers are accepted. Accented letters are not accepted.

Mobile device: in this field the name of an already registered mobile device is shown, which is read by the mobile application from the mobile device itself, therefore this name cannot be changed in the programming software.

APP ID: in this field the identifier of an already registered mobile device is shown. This identifier is used to identify the mobile device and it is unique for each device.

Delete: the “***Delete***” button is used to delete the given mobile device, i.e., to cancel its registration. In case of deleting a mobile device, the application used on the given device will no longer have access to the ***Adapter2 PRO*** device.

4.2.3 Reporting channels



Reporting channels

CID reporting to CMS over IP

	Name	IP address / domain name	Port	Protocol	Supervision message	Supervision message interval	Time zone
IP1	IP1		9999	SIA IP	Yes	180 s	Local time
IP2	IP2		3535	TELLMON	Yes	180 s	UTC
IP3	IP3		3333	TEX	Yes	180 s	UTC
IP4	IP4		3333	TEX	Yes	180 s	UTC

IP1 – Network protocol: TCP; AES key: ; □ Send each message in a new session

IP2 – Network protocol: TCP

Backup reporting to CMS via SMS

	Phone number	Message
SMS		

User phone number settings

	Name	Phone number	Event acknowledgement options	Incoming call management
TEL1	TEL1		Accept call to acknowledge	Forward calls to the simulated lin
TEL2	TEL2		Reject or accept call to acknowle	Forward calls to the simulated lin
TEL3	TEL3		Press * to acknowledge	Reject calls
TEL4	TEL4		Press * to acknowledge or # to s	Reject calls

E-mail

	Name	E-mail address
MAIL1	MAIL1	
MAIL2	MAIL2	
MAIL3	MAIL3	
MAIL4	MAIL4	

In the "***Reporting channels***" menu you can configure the availabilities where notifications should be sent, such as monitoring servers or receivers, user phone numbers for calls and SMS sending, and e-mail addresses for notification by e-mail.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Data usage calculator:
  The data usage calculator shows an estimated monthly data usage based on the configured settings and the expected number of reports and messages. For this, you need to provide the expected number of reports and messages only.

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

CID reporting to CMS over IP:

You can configure up to 4 CMS servers or receivers with the following parameters:

Name: CMS server or receiver name. The name entered in this section is used for identification of the server/receiver within the program, and the program will also use this name when configuring notification templates.

IP address/domain name: CMS server or receiver IP address or domain name. When a SIM card with a private APN is used, and the given server or receiver is not in the same APN, it is necessary to enable access of the server/receiver IP address in the given APN.

Port: CMS server or receiver communication port number.

Default port numbers:

TELLMon protocol (TCP):	**3535**
TELLMon protocol (UDP):	**3545**
TEX protocol:	**3333**
SIA IP (DC-09) protocol:	**9999**

Protocol: select the appropriate communication protocol for the given server or receiver from the drop-down menu.

Available protocols:

- **TELLMon** (custom TELL protocol for the **TELLMon** receiver and the **MVP.next** server);
- **TEX** (custom TELL protocol for the **TEX-MVP** and the **TEX BASE/PRO** servers);
- **SIA IP** (SIA DC-09 protocol for other receivers that support this protocol. Not recommended for servers and receivers developed by TELL!).

Supervision message: enable/disable supervision message sending. Supervision message sending cannot be disabled in case of using the TEX or the TELLMon communication protocol.

Supervision message interval: if supervision message sending is enabled, you can configure the interval of message sending from 30 to 86400 seconds for the SIA IP protocol, 30 to 600 seconds for the TELLMon protocol, and 60 to 600 seconds for the TEX protocol.

Time zone: in this section you can select whether the given server or receiver sends the timestamp used for synchronizing the system time in **UTC** or **local time**. It is important to select the appropriate option for each server and receiver, since if the system time is set incorrectly, events will be stored with the wrong timestamp.

Network protocol: according to the chosen communication protocol you can use **TCP** or **UDP** network protocol. The **UDP** protocol allows for less data traffic. For the **TEX** communication protocol only the **TCP** network protocol option is available.

AES key: the custom AES encryption key can be used for SIA IP protocol only. If an encryption key is configured, the SIA IP packages will be encrypted with the given key, and they must be decrypted on the receiver side using the same key. The maximum length of the AES key is up to 16 characters, or up to 32 characters in case of using hexadecimal format.

Send each message in a new session: if required for the given receiver, for the **SIA IP** protocol it can be enabled to send each message in a new TCP session. In case of using UDP, the device will open a new port for each message, if this option is enabled.

Backup reporting to CMS via SMS:

In case that the device fails to report the connected alarm system’s messages to the CMS servers or receivers, as a backup solution, it is possible to forward the reports via SMS to a configurable phone number. For this, it is necessary to enable the “***Backup reporting via SMS***” option in the notification template assigned to the affected events.

Phone number: the CMS phone number where you want to forward the reports via SMS. It is recommended to enter the phone number in international format (e.g.: +3630…).

Message: the text of the message for backup reporting. This can be a specific custom message, or you can use the variables supported by the device, which the device will replace automatically with the data of the report received from the alarm system, as follows:

$cn: event name, **$cp**: partition name, **$cz**: zone name,
$cid: the complete Contact ID message (e.g. 123418113001001).
Further information about variables are available in paragraph "***Alarm system events***".

User phone number settings:

You can configure up to 4 user phone numbers (**TEL1** to **TEL4**) to which the device sends notifications by voice call or SMS. Depending on the settings, the device can forward calls received from these numbers to the simulated phone line output.

Name: user name. The name entered in this section will be used when selecting the notification channels upon configuring events.

Phone number: user phone number. It is recommended to enter the phone number in international format (e.g.: +3630…).

Event acknowledgement options: when the device sends a notification by call, it requires a confirmation that the notification has been received, otherwise it will retry to deliver the notification. In this section you can configure the actions required from each user for acknowledging upon receiving a notification by voice call. Available options:

- **Accept call to acknowledge**: notifications will be acknowledged automatically upon accepting the calls. After accepting the call, wait at least 3 seconds before ending the call.
- **Reject or accept call to acknowledge**: notifications will be acknowledged automatically if the calls are rejected by user, and also if the calls are accepted.
- **Press ∗ to acknowledge**: notifications need to be acknowledged by pressing the star (∗) key on the phone after accepting the call. The device will confirm that it has received the command by a short signal tone. It is also possible to acknowledge notifications via SMS. The SMS-based acknowledgement will acknowledge notifications initiated to the phone number of the SMS sender. To acknowledge a notification via SMS, send the **STOP** message to the phone number of the SIM card installed in the device.
- **Press ∗ to acknowledge or # to stop notification**: notifications need to be acknowledged by pressing the star (∗) key on the phone after accepting the call. The device will confirm that it has received the command by a short signal tone. Notification of further users on the given event can be stopped by pressing the hash (#) key on the phone. The device will confirm that it has received this command by three short signal tones. By pressing the hash (#) key, this also confirms reception of the notification at the same time, so it is not necessary to press the star (∗) key too.
  By this option it is also possible to cancel all pending notifications for all events by entering the **∗*device password*#** command (e.g., **∗1234#**) using the phone's keys. The superadmin and admin passwords are both accepted.
  It is also possible to acknowledge notifications via SMS. The SMS-based acknowledgement will acknowledge notifications initiated to the phone number of the SMS sender. To acknowledge a notification via SMS, send the **STOP** message to the phone number of the SIM card installed in the device. To stop all pending notifications, send the **STOP ALL** message to the phone number of the SIM card installed in the device.

Incoming call management: in this section you can configure for each user what should the device do when it receives a call from the given user. Available options:

- **Forward calls to the simulated line**: calls received from the given phone number will be forwarded to the simulated phone line output. If a landline phone device is connected to the line output, the phone will ring, and speech communication is possible after accepting the call.
- **Reject calls**: the device will reject calls received from the given phone number.

Regardless of this setting, when a call is received from a user phone number, a related service event is generated for which you can configure output control or notification sending.

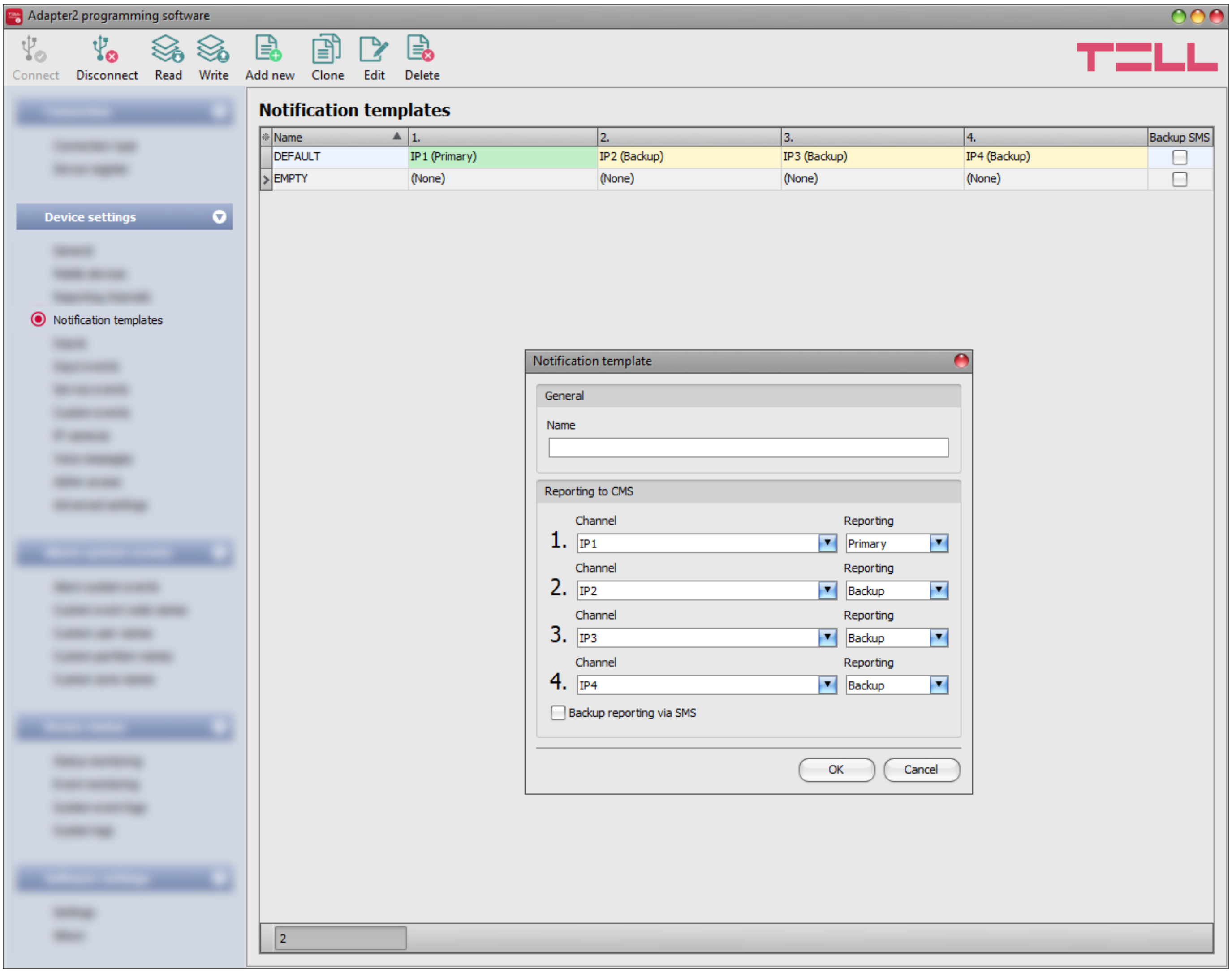
E-mail notification recipients:

You can configure up to 4 e-mail addresses (**MAIL1** to **MAIL4**) to which the device will send notification upon event occurrence, according to the event settings.

Name: user/recipient name. The name entered in this section will be used upon selecting the notification channels when configuring events.

E-mail address: user/recipient e-mail address. You can configure 1 e-mail address per user.

4.2.4 Notification templates



Notification templates

Name	1.	2.	3.	4.	Backup SMS
DEFAULT	IP1 (Primary)	IP2 (Backup)	IP3 (Backup)	IP4 (Backup)	□
EMPTY	(None)	(None)	(None)	(None)	□

Notification template

General

Name

Reporting to CMS

	Channel	Reporting
1.	IP1	Primary
2.	IP2	Backup
3.	IP3	Backup
4.	IP4	Backup

□ Backup reporting via SMS

OK Cancel

Notification templates should only be configured if reporting to CMS is needed. In this menu you can configure different templates according to which the device will send reports to CMS servers and receivers. For quick and easy setup, the device contains 2 built-in templates, named as "***DEFAULT***" and "***EMPTY***". The "***DEFAULT***" template cannot be deleted, but its configuration can be changed if needed. If you wish to add new notification templates, it is appropriate to do this prior to configuring events. Any template can be assigned to any event; thus, reports can be directed to the desired servers and receivers, with the desired priorities. Servers/receivers are classified into two groups, primary and backup. When an event occurs, the given report will be sent to all servers and receivers configured as primary in the notification template associated with the given event. In case that none of the primary servers/receivers are available, the device will try to report to the servers/receivers configured as backup. The device will send the acknowledgement signal to the connected alarm control panel when the event is received and acknowledged by at least one of the servers or receivers.

The order of reporting to servers and receivers configured as backup in a template corresponds to the numbering (1 to 6) of the channels in the template. The priority depends on the classification of the configured servers/receivers (primary or backup). Primary servers/receivers will be notified first. Reports will be sent to all primary servers/receivers, while backup servers/receivers will only be notified if reporting to all primary ones fail. In this case, the device will try to report to the first highest priority backup server/receiver, and then, if this fails, to the second one, and so on.

Additionally, if a reporting channel fails, the devices will keep sending supervision messages to the given server/receiver by the configured supervision sending interval to check its availability, and will send the report as soon as it becomes available. The device will no longer try to report events for which reporting failed for more than 1 hour.

In case that the device fails to report the connected alarm system's messages to all configured CMS servers or receivers, as a backup solution, it is possible to forward the reports via SMS to a configurable phone number. For this, enable the "***Backup reporting via SMS***" option and configure the phone number and the message in the "***Reporting channels***" menu. Further information about this option you can find in paragraph "***Reporting channels***".

Notification templates cannot be deleted while they are associated with an event. The system supports adding up to **10 notification templates**, including the built-in ones.

Available options:

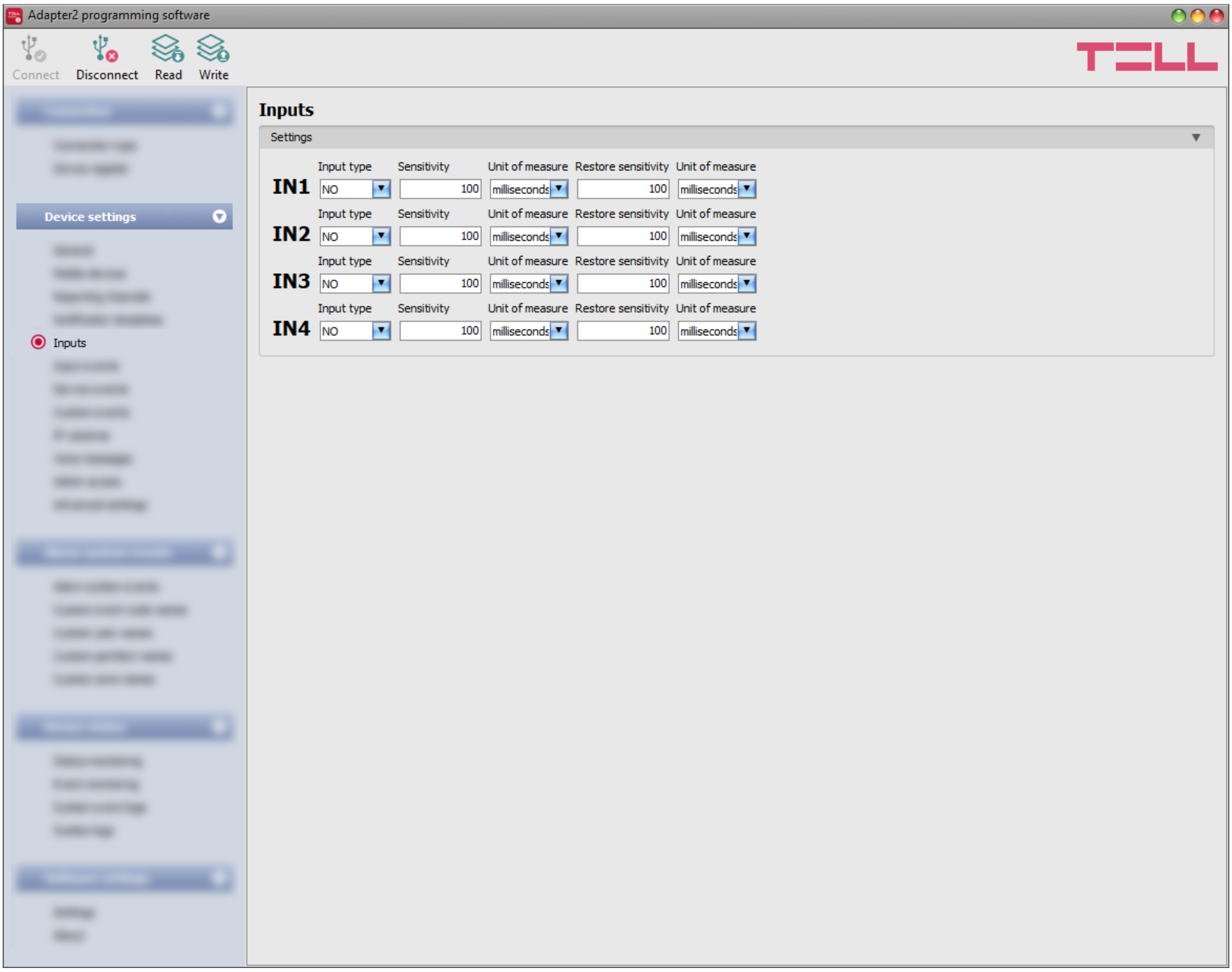
- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new notification template:
  To add a new notification template, click on the "***New***" button.
- Creating a copy of an existing template:
  To create a copy of the selected template, click on the "***Clone***" button. Please note that the new copy should have a different unique name.
- Editing an existing template:
  To edit the selected template, click on the "***Edit***" button.
- Deleting a template:
  To delete the selected template, click on the "***Delete***" button.

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

Creating a new notification template:

- Click on the "***New***" button.
- Enter a name for the new template. The name should not be longer than 20 characters, and the following characters should not be used: ^ ~ < > = | $ % " '.
- Configure the channels and the reporting priority.
- Click on the "***OK***" button.
- Click on the "***Write***" button.

4.2.5 Inputs



	Input type	Sensitivity	Unit of measure	Restore sensitivity	Unit of measure
IN1	NO	100	milliseconds	100	milliseconds
IN2	NO	100	milliseconds	100	milliseconds
IN3	NO	100	milliseconds	100	milliseconds
IN4	NO	100	milliseconds	100	milliseconds

In the “***Inputs***” menu you can configure the default state of the 4 contact inputs, activation sensitivity, and input restore sensitivity can also be configured.

Available options:

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

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

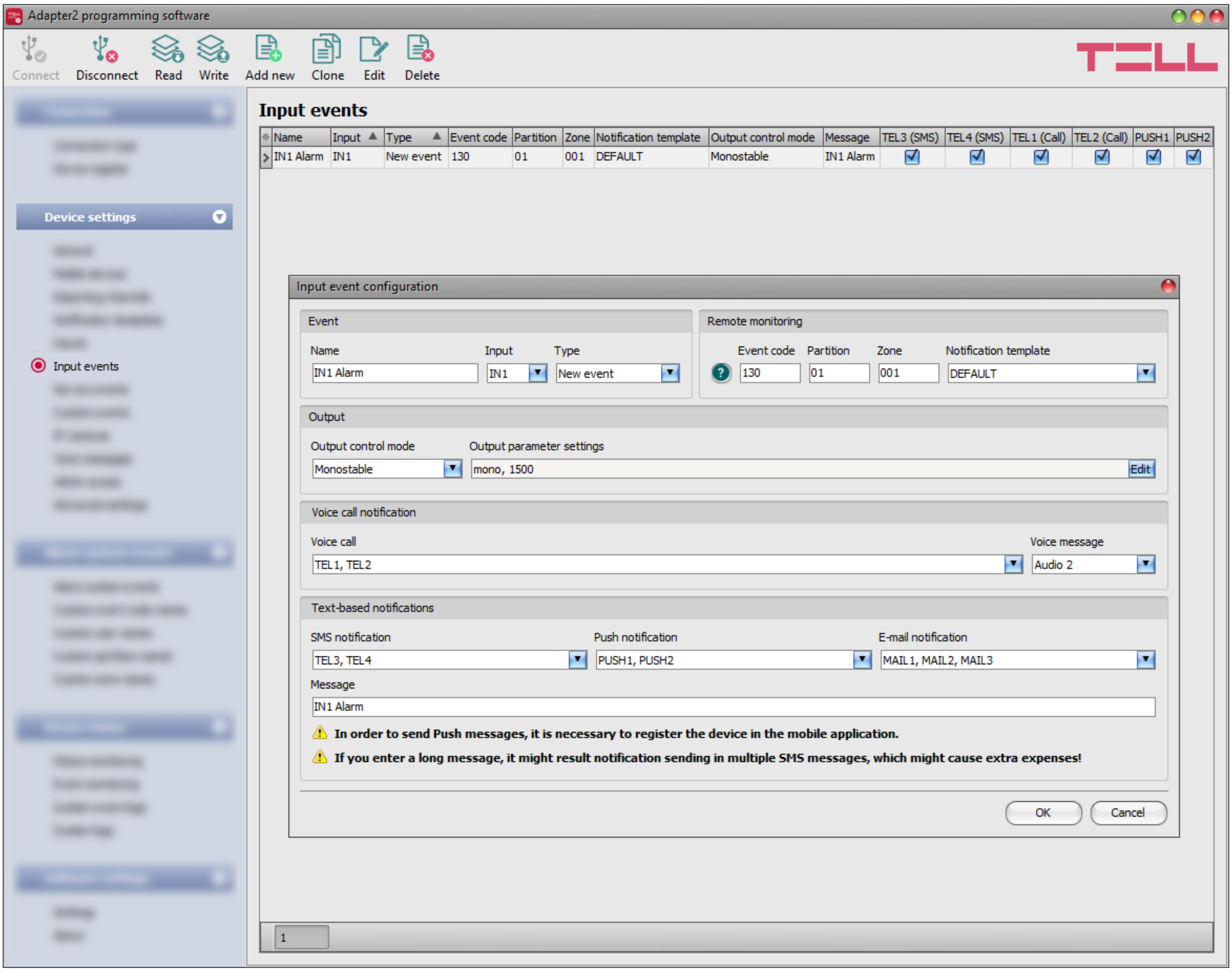
Settings:

Input type: the input can be normally open (**NO**), or normally closed (**NC**).
When set to **NO**, an input event will be generated when the open contact between the given input (**IN1**…**IN4**) and the **GND** terminal is closed.
When set to **NC**, an input event will be generated when the closed contact between the given input (**IN1**…**IN4**) and the **GND** terminal is opened.

Sensitivity / Unit of measure: state changes of the input shorter than the value entered in this section regarding activation of the input are ignored by the device. The unit of measure can also be selected (milliseconds, seconds, or minutes). The sensitivity can be configured from 5 milliseconds to 1 hour.

Restore sensitivity / Unit of measure: state changes of the input shorter than the value entered in this section regarding restoration of the input are ignored by the device. The unit of measure can also be selected (milliseconds, seconds, or minutes). The sensitivity can be configured from 5 milliseconds to 1 hour.

4.2.6 Input events



Input events

Name	Input	Type	Event code	Partition	Zone	Notification template	Output control mode	Message	TEL3 (SMS)	TEL4 (SMS)	TEL1 (Call)	TEL2 (Call)	PUSH1	PUSH2
IN1 Alarm	IN1	New event	130	01	001	DEFAULT	Monostable	IN1 Alarm	☑	☑	☑	☑	☑	☑

Input event configuration

Event
Name: IN1 Alarm
Input: IN1
Type: New event

Remote monitoring
Event code: 130
Partition: 01
Zone: 001
Notification template: DEFAULT

Output
Output control mode: Monostable
Output parameter settings: mono, 1500

Voice call notification
Voice call: TEL1, TEL2
Voice message: Audio 2

Text-based notifications
SMS notification: TEL3, TEL4
Push notification: PUSH1, PUSH2
E-mail notification: MAIL1, MAIL2, MAIL3
Message: IN1 Alarm

⚠ **In order to send Push messages, it is necessary to register the device in the mobile application.**

⚠ **If you enter a long message, it might result notification sending in multiple SMS messages, which might cause extra expenses!**

In this menu you can configure the events generated by the 4 contact inputs and notifications to be sent when an input event occurs. Input events should be added and configured for the inputs you wish to use. If no input event is configured for an input, the given input will not generate events, nor send notifications. You can add one new and one restore event for each input.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new input event:
  To add a new input event, click on the "***New***" button.
- Creating a copy of an existing input event:
  To create a copy of the selected input event, click on the "***Clone***" button. Please note that the new copy should have a different unique name.
- Editing input event settings:
  To edit the settings of the selected input event, click on the "***Edit***" button.
- Deleting an input event:
  To delete the selected input event, click on the "***Delete***" button.

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

Event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Input: the contact input, which will generate the given event.

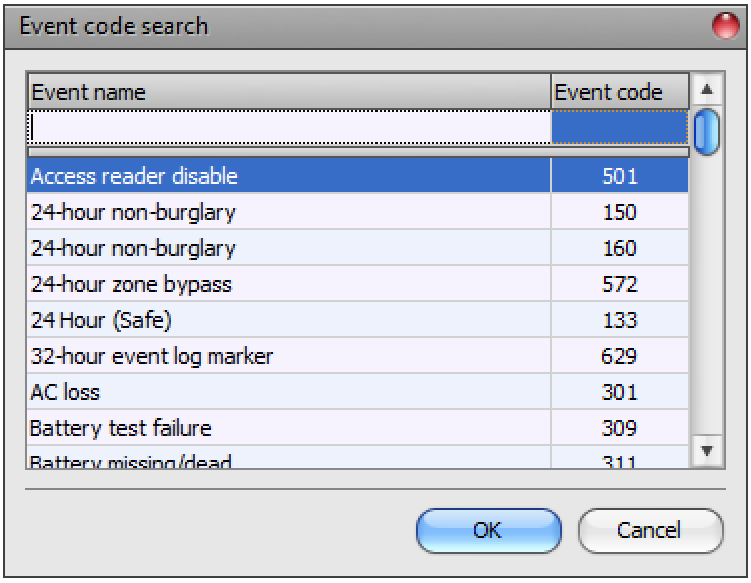
Type: the type of the event, which can be new or restore. New event will be generated when an input is activated, and restore event will be generated when it reverts to its normal state. In the Contact ID protocol, new events are indicated with 1 (or E), and event restorals are indicated with 3 (or R).

Remote monitoring:

In this section you can configure the Contact ID event code for reporting to CMS and can select one of the preconfigured notification templates for the given event. The Contact ID event code should only be configured if reporting to CMS is used, otherwise select the notification template named “***EMPTY***”.

Event code: in this section you can configure the 3-digit Contact ID event code, which you want to assign to the given event (e.g., 130 = burglar alarm). The event code consists of hexadecimal characters (0...9,A,B,C,D,E,F).

The software includes a built-in event code search tool which contains the list of standard Contact ID codes. The search tool opens by clicking on the ? icon with the question mark symbol placed in front of the event code input field.



Event name	Event code
Access reader disable	501
24-hour non-burglary	150
24-hour non-burglary	160
24-hour zone bypass	572
24 Hour (Safe)	133
32-hour event log marker	629
AC loss	301
Battery test failure	309
Battery missing/dead	311

In the event code search tool, you can search for events by name or by event code. For searching by name, start typing the name of the searched event code in the field under the “***Event name***” column header. For searching by event code, start typing the searched event code number in the field under the “***Event code***” column header. The search tool will filter the list automatically according to the hits. You can select an event code by clicking on it in the list, then the program will paste this automatically into the event code input field after clicking on the “***OK***” button.

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

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

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events. If you do not want to send a report to CMS on the given event, select the template named “***EMPTY***”.

Output:

In this section you can configure the output to be controlled when the given input event occurs.

Output control mode: in this section you can configure the control mode of the output.

Available options:

- **None**: the output will not be used.
- **Monostable**: the output will be activated for the time configured in the **"*Duration*"** section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 1 hour.
- **Bistable ON**: the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF**: the output will become deactivated.
- **State change**: the output will change state (if deactivated, it will become activated and if activated, it will become deactivated).
- **Pulse series**: the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 1 hour, the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 1 hour too.

Output parameter settings: this option becomes available if an output control mode is selected which has further settings. In this section you can configure the additional settings of specific output control modes, such as timings for monostable control and pulse series. Click on the "***Edit***" button to open the parameter configuration window.

Voice call notification:

In this section you can configure phone calls to be made when the given input event occurs. The device will call the selected phone numbers and play the selected voice messages. You can upload voice messages as audio files in the "***Voice messages***" menu.

Voice call: in this section you can select the user phone numbers to which calls should be made. The phone numbers should be configured in advance in the "***Reporting channels***" menu. Calls will be made to the numbers enabled with the help of the checkboxes in the drop-down list.

Voice message: in this section you can select the voice message which should be played in the calls when the given event occurs. When receiving a call from the device, a built-in siren tone will be played before each voice message. If a voice message has been configured for which no message has been uploaded, the siren tone will be played continuously throughout the call.

Text-based notifications:

In this section you can configure text-based messages to be sent when the given input event occurs.

SMS notification: in this section you can select the user phone numbers to which SMS message should be sent when the given event occurs. The phone numbers should be configured in advance 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 list.

Push notification: in this section you can select the mobile devices to which Push notification should be sent when the given event occurs. The mobile devices should be configured in advance in the "***Mobile devices***" menu. Push notification will be sent to the mobile devices enabled with the help of the checkboxes in the drop-down list.

E-mail notification: in this section you can select the recipients to whom e-mail should be sent when the given event occurs. The e-mail addresses should be configured in advance in the "***Reporting channels***" menu. E-mail will be sent to the addressees enabled with the help of the checkboxes in the drop-down list.

Message: in this field you can enter a custom message of maximum 45 characters, which you wish to be sent to the selected phone numbers, mobile devices, or e-mail addresses when the given event occurs. The device will send the same message for each notification channel (SMS, Push, e-mail).

The device is capable to insert various dynamic data in the text of the message using variables. The device will automatically replace the variable written in the message with the data related to the given variable when it sends the message.

Available variables:
$cid: the full Contact ID message configured for the given event (e.g.: 123418113001001).
$cc: the Contact ID event code configured for the given event (e.g.: 130).
$cp: the partition number configured for the given event (e.g.: 01).
$cz: the zone number configured for the given event (e.g.: 001).
$name: the event name configured in the device for the given event.
$in1…**in4**: the actual state of the given contact input (0=idle, 1=activated).
$rel1: the actual state of the relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

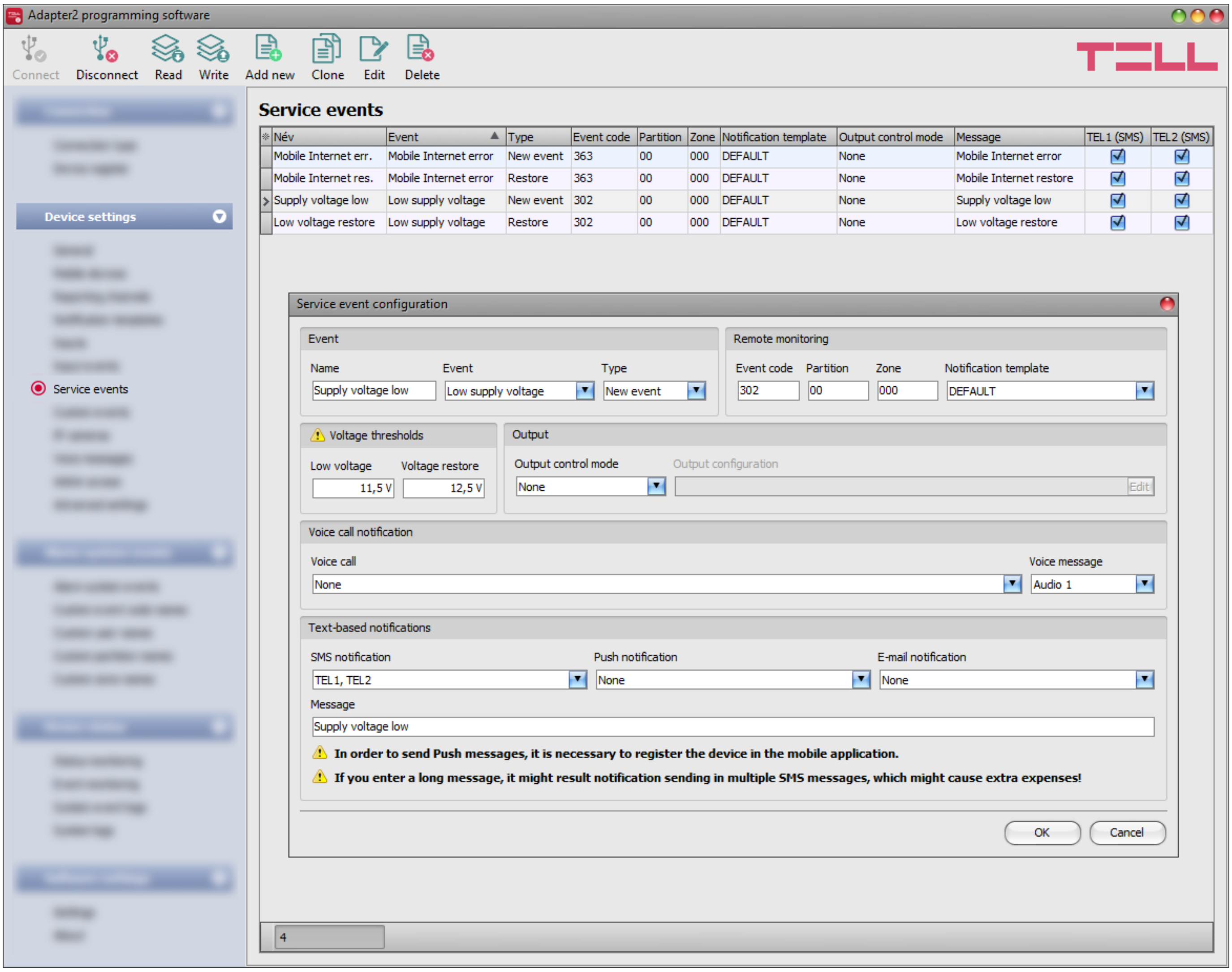
Camera: in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the "***IP cameras***" menu. If you have configured a Push notification for the given event, the mobile application will automatically offer to view the picture of the IP camera associated with the given event, when the message is received. If you have configured an e-mail notification for the given event, the URL of the IP camera assigned to the event will be sent along with the message in the given e-mail.

Click "***OK***" to accept the changes or "***Cancel***" to quit without saving.

Adding a new input event:

- Click on the "***New***" button.
- Configure the input event based on the above.
- Click on the "***Write***" button to write the changes into the device.

4.2.7 Service events



Service events

Név	Event	Type	Event code	Partition	Zone	Notification template	Output control mode	Message	TEL1 (SMS)	TEL2 (SMS)
Mobile Internet err.	Mobile Internet error	New event	363	00	000	DEFAULT	None	Mobile Internet error	☑	☑
Mobile Internet res.	Mobile Internet error	Restore	363	00	000	DEFAULT	None	Mobile Internet restore	☑	☑
Supply voltage low	Low supply voltage	New event	302	00	000	DEFAULT	None	Supply voltage low	☑	☑
Low voltage restore	Low supply voltage	Restore	302	00	000	DEFAULT	None	Low voltage restore	☑	☑

Service event configuration

Event

Name: Supply voltage low
Event: Low supply voltage
Type: New event

Remote monitoring

Event code: 302
Partition: 00
Zone: 000
Notification template: DEFAULT

Voltage thresholds

Low voltage: 11,5 V
Voltage restore: 12,5 V

Output

Output control mode: None
Output configuration: Edit

Voice call notification

Voice call: None
Voice message: Audio 1

Text-based notifications

SMS notification: TEL1, TEL2
Push notification: None
E-mail notification: None

Message: Supply voltage low

⚠ **In order to send Push messages, it is necessary to register the device in the mobile application.**

⚠ **If you enter a long message, it might result notification sending in multiple SMS messages, which might cause extra expenses!**

OK Cancel

In the “***Service events***” menu you can configure the custom service events of the device and notifications to be sent when a service event occurs. Service events you wish to use should be added and configured. If a service event is not added, the given event will not be generated, and the device will not send notifications related to that event. For each service event you can add one new and one restore event, except for events for which only the new event is interpretable. These events have a fixed event type, which you cannot change.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new service event:
  To add a new service event, click on the "***New***" button.
- Creating a copy of an existing service event:
  To create a copy of the selected service event, click on the "***Clone***" button. Please note that the new copy should have a different unique name.
- Editing service event settings:
  To edit the settings of the selected service event, click on the "***Edit***" button.
- Deleting a service event:
  To delete the selected service event, click on the "***Delete***" button.

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

Event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Event: select an event from the available service events in the drop-down menu.

Available service events:

- **GSM error**: this type of event is generated if the device loses the connection with the GSM network, or it is unable to register on the GSM network for at least 60 seconds. A restore event is generated upon successful registration on the GSM network. Most common reasons for this type of error are the following: there is no SIM card installed in the device, or the card is not installed properly, the card is damaged, or the service is not available on the SIM card, low GSM signal, the GSM antenna is not connected, insufficient supply voltage/current.
- **Mobile Internet error**: this type of event is generated if the device is unable to establish the Internet connection for at least 60 seconds. A restore event is generated when the Internet connection restores. Most common reasons for this type of error are the following: wrong APN configured, or the mobile Internet service is not enabled on the SIM card.

- **Low supply voltage**: the device has built-in supply voltage monitoring function. Low supply voltage event is generated when the supply voltage level is continuously on, or drops below the configured low supply voltage threshold value, for at least 30 seconds. Low supply voltage restore event is generated when the supply voltage level is continuously on, or returns above the configured low supply voltage restore threshold value, for at least 30 seconds, after a "***Low supply voltage***" event. You can configure the threshold values in the event dialog window.

  Low voltage threshold: In this section you can configure the threshold from 9.5V to 30V, at which the device will generate the "***Low supply voltage***" event.

  Voltage restore threshold: In this section you can configure the threshold from 10 to 30V, at which the device will generate the "***Low supply voltage***" restore event.

- **Output control by mobile device (1…4)**: this type of event is generated when the output of the device is controlled from one of the mobile devices (1 to 4) through the mobile application. Activating the output will generate a new event, while deactivating will generate a restore.
- **Incoming call from user (1…4)**: this type of event is generated when the device receives a call from a user phone number configured in the device. The caller ID (phone number) should be presented in the call to be identified by the device via CLIP service.
- **Incoming call from unknown number**: this type of event is generated when the device receives a call from a phone number which is not configured in the device as a user phone number, or a call received from a private number (with hidden caller ID).
- **Periodic test report**: this type of event is used for supervising the operation of the device and it is generated automatically based on the settings below.

  Interval of sending (1…168h): the interval of periodic test report sending. If you change this setting, make sure to click on the "***Periodic test report***" button found in the "***Status monitoring***" menu, to generate a test report and validate the new settings. Otherwise, the next test report will still be sent based on the previous setting.

  Time of day (hh:mm): the time of day for periodic test report sending.

- **First data usage limit reached**: this type of event is generated when the device data usage reaches the limit configured in Megabytes in the "***First data usage limit warning***" field.

  Billing cycle date: This field can be used to mark the day of the month on which the mobile service provider resets and bills the amount of data used for the current month.

  Data rounding unit: This field can be used to configure the data rounding unit used by your mobile service provider. This value will strongly influence the device's monthly data usage. You can check the data rounding unit for your data plan in the general terms and conditions of your mobile service provider.

  The "***Billing cycle date***" and "***Data rounding unit***" settings are common for the "***Second data usage limit warning***" and "***Second data usage limit warning***" service events, i.e., they use the same configured values. If you change these settings for one of the two events, they will change automatically for the other event as well.

- **Second data usage limit reached**: this type of event is generated when the device data usage reaches the limit configured in Megabytes in the "***Second data usage limit warning***" field.

- **Settings changed:** this type of event is generated when the Superadmin user changes a protected setting, that the Admin user has no access to (which is disabled in the "***Admin access***" menu.)
- **SMS sending daily limit reached**: this type of event is generated when the number of event SMS messages sent by the device on the given day reaches the value configured at the "***SMS sending daily limit***" option in the "***General***" device settings menu.
- **SMS forwarding daily limit reached**: this type of event is generated when the number of incoming SMS messages forwarded by the device on the given day reaches the value configured at the "***SMS forwarding daily limit***" option in the "***General***" device settings menu.
- **Daily call limit reached**: this type of event is generated when the number of calls initiated by the device on the given day reaches the value configured at the "***Daily limit for calls***" option in the "***General***" device settings menu.

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

Remote monitoring:

In this section you can configure the Contact ID event code for reporting to CMS and can select the preconfigured notification template for the given event. The Contact ID event code should only be configured if reporting to CMS is used, otherwise select the notification template named "***EMPTY***".

Event code: in this section you can configure the 3-digit Contact ID event code, consisting of characters 0...9,A,B,C,D,E,F, which you wish to assign to the given event (e.g. 302 = battery fault).

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

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

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events. If you do not want to send a report to CMS on the given event, select the template named "***EMPTY***".

Output:

In this section you can configure the output to be controlled when the given service event occurs.

Output control mode: in this section you can configure the control mode of the output.

Available options:

- **None**: the output will not be used.
- **Monostable**: the output will be activated for the time configured in the **“*Duration*”** section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 1 hour.
- **Bistable ON**: the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF**: the output will become deactivated.
- **State change**: the output will change state (if deactivated, it will become activated and if activated, it will become deactivated).
- **Pulse series**: the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 1 hour, the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 1 hour too.

Output parameter settings: this option becomes available if an output control mode is selected which has further settings. In this section you can configure the additional settings of specific output control modes, such as timings for monostable control and pulse series. Click on the “***Edit***” button to open the parameter configuration window.

Voice call notification:

In this section you can configure phone calls to be made when the given service event occurs. The device will call the selected phone numbers and play the selected voice messages. You can upload voice messages as audio files in the “***Voice messages***” menu.

Voice call: in this section you can select the user phone numbers to which calls should be made. The phone numbers should be configured in advance in the “***Reporting channels***” menu. Calls will be made to the numbers enabled with the help of the checkboxes in the drop-down list.

Voice message: in this section you can select the voice message which should be played in the calls when the given event occurs. When receiving a call from the device, a built-in siren tone will be played before each voice message. If a voice message has been configured for which no message has been uploaded, the siren tone will be played continuously throughout the call.

Text-based notifications:

In this section you can configure text-based messages to be sent when the given service event occurs.

SMS notification: in this section you can select the user phone numbers to which SMS message should be sent when the given event occurs. The phone numbers should be configured in advance 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 list.

Push notification: in this section you can select the mobile devices to which Push notification should be sent when the given event occurs. The mobile devices should be configured in advance in the “***Mobile devices***” menu. Push notification will be sent to the mobile devices enabled with the help of the checkboxes in the drop-down list.

E-mail notification: in this section you can select the recipients to whom e-mail should be sent when the given event occurs. The e-mail addresses should be configured in advance in the “***Reporting channels***” menu. E-mail will be sent to the addressees enabled with the help of the checkboxes in the drop-down list.

Message: in this field you can enter a custom message of maximum 45 characters, which you wish to be sent to the selected phone numbers, mobile devices, or e-mail addresses when the given event occurs. The device will send the same message for each notification channel (SMS, Push, e-mail).

The device is capable to insert various dynamic data in the text of the message using variables. The device will automatically replace the variable written in the message with the data related to the given variable when it sends the message.

Available variables:
$cid: the full Contact ID message configured for the given event (e.g.: 123418113001001).
$cc: the Contact ID event code configured for the given event (e.g.:130).
$cp: the partition number configured for the given event (e.g.: 01).
$cz: the zone number configured for the given event (e.g.: 001).
$name: the event name configured in the device for the given event.
$in1…**in4**: the actual state of the given contact input (0=idle, 1=activated).
$rel1: the actual state of the relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

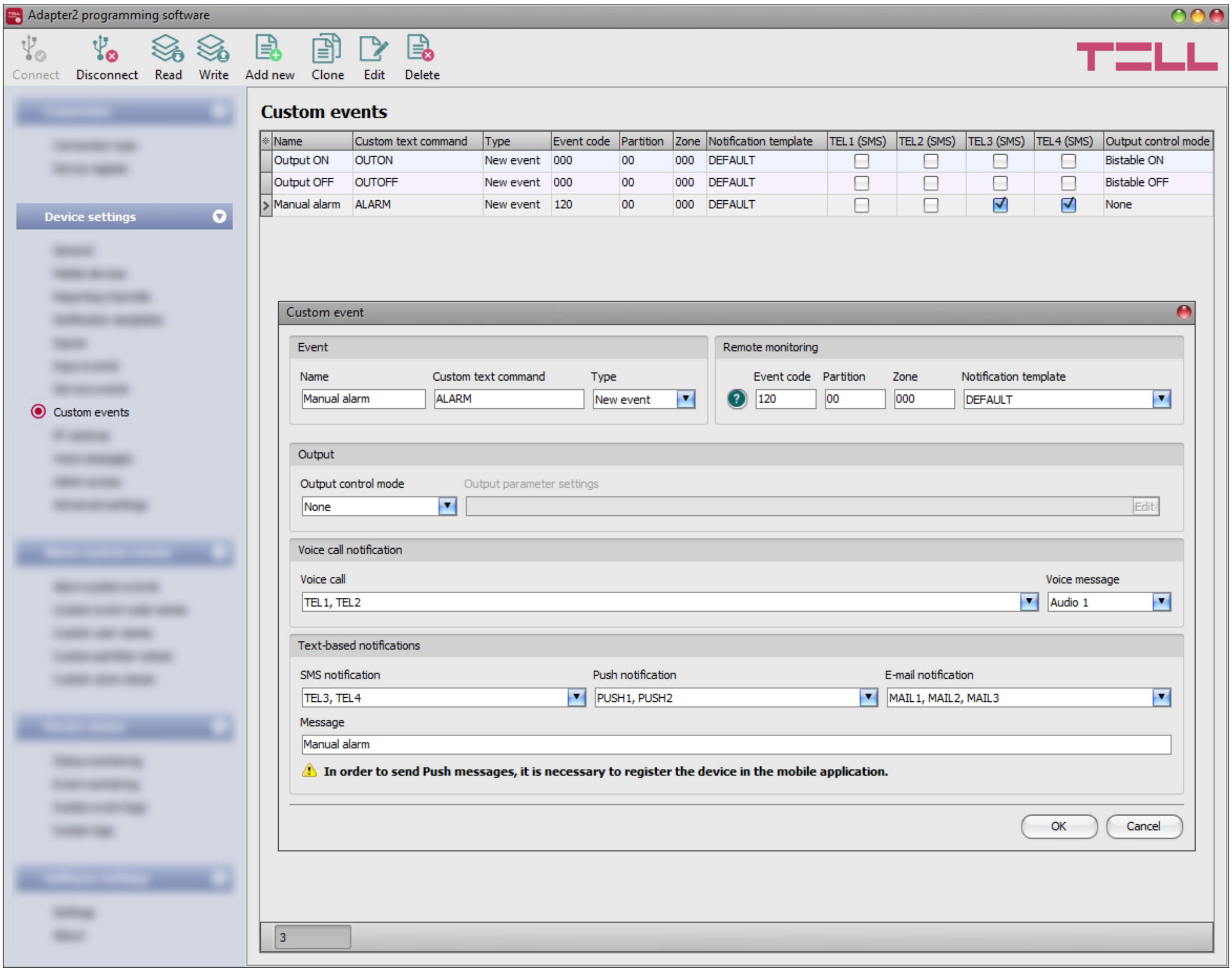
Camera: in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the “***IP cameras***” menu. If you have configured a Push notification for the given event, the mobile application will automatically offer to view the picture of the IP camera associated with the given event, when the message is received. If you have configured an e-mail notification for the given event, the URL of the IP camera assigned to the event will be sent along with the message in the given e-mail.

Click “***OK***” to accept the changes or “***Cancel***” to quit without saving.

Adding a new service event:

- Click on the “***New***” button.
- Configure the service event based on the above.
- Click on the “***Write***” button to write the changes into the device.

4.2.8 Custom events



Custom events

Name	Custom text command	Type	Event code	Partition	Zone	Notification template	TEL1 (SMS)	TEL2 (SMS)	TEL3 (SMS)	TEL4 (SMS)	Output control mode
Output ON	OUTON	New event	000	00	000	DEFAULT	□	□	□	□	Bistable ON
Output OFF	OUTOFF	New event	000	00	000	DEFAULT	□	□	□	□	Bistable OFF
Manual alarm	ALARM	New event	120	00	000	DEFAULT	□	□	☑	☑	None

Custom event

Event
Name: Manual alarm
Custom text command: ALARM
Type: New event

Remote monitoring
Event code: 120
Partition: 00
Zone: 000
Notification template: DEFAULT

Output
Output control mode: None
Output parameter settings

Voice call notification
Voice call: TEL1, TEL2
Voice message: Audio 1

Text-based notifications
SMS notification: TEL3, TEL4
Push notification: PUSH1, PUSH2
E-mail notification: MAIL1, MAIL2, MAIL3
Message: Manual alarm

⚠ **In order to send Push messages, it is necessary to register the device in the mobile application.**

3

In this menu you can configure custom events, which the device generates upon receiving a custom command by text message (SMS). You can freely configure the custom command for each event. Just like input and service events, custom events enable sending reports to remote monitoring station, notifications to users, as well as controlling the output.

With this function you can practically generate any reports to remote monitoring station, notifications to users, and control the device's output, by sending custom commands of your choice in a text message (SMS) to the device's phone number.

Attention! Custom commands must be different than the available default SMS commands (see paragraph *Remote connecting to devices via cloud service*), otherwise the device will only perform the default action associated with the command.

It is possible to send more than one command in one message, but the message should not exceed 60 characters. The device will not execute commands which are entered in the message beyond the 60 characters limit. The device will not react in case of receiving an incorrect or non-existing command.

PWD: the device password can be specified using this parameter. The superadmin and admin passwords are both accepted (default superadmin password: 1234). The **PWD** is an optional parameter which should be used only when sending commands from phone numbers which are not configured in the device in the ***Reporting channels*** menu, in the ***User phone number settings*** section – such phone numbers are considered unauthorized, therefore in this case the password is required. If the device password is not specified along with the control command sent from unauthorized phone numbers, the command will not be executed by the device.

Commands sent from unauthorized phone numbers should always begin with a star "∗" and end with a hash "#" character.

Example on using custom commands:

The following custom commands will be used in the example: Alert, Open

- **When sending from authorized phone numbers:**
  - Sending one command: **Alert** or **∗Alert#**
  - Sending multiple commands: **Alert,Open** or **Alert Open** or **∗Alert,Open#**

- **When sending from unauthorized phone numbers:**
  - Sending one command: **∗Alert,PWD=*1234*#** or **∗Alert#∗PWD=*1234*#**
  - Sending multiple commands: **∗Alert,Open,PWD=*1234*#** or
    ∗Alert#∗Open#∗PWD=*1234*#

Available options in the software:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new custom event:
  To add a new custom event, click on the "***New***" button.
- Creating a copy of an existing custom event:
  To create a copy of the selected custom event, click on the "***Clone***" button. Please note that the new copy should have a different unique name.
- Editing custom event settings:
  To edit the settings of the selected custom event, click on the "***Edit***" button.
- Deleting a custom event:
  To delete the selected custom event, click on the "***Delete***" button.

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

Event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Custom text command: enter any text command which you want to send in a text message (SMS) to the device’s phone number to generate the given custom event, and send report, notifications and execute controls configured for the given event.

Type: the type of the custom event, which can be new or restore. In the Contact ID protocol, new events are indicated with 1 (or E), while event restorals are indicated with 3 (or R).

Remote monitoring:

In this section you can configure the Contact ID event code for reporting to CMS and can select the preconfigured notification template for the given event. The Contact ID event code should only be configured if reporting to CMS is used, otherwise select the notification template named “***EMPTY***”.

Event code: in this section you can configure the 3-digit Contact ID event code, consisting of characters 0...9,A,B,C,D,E,F, which you wish to assign to the given event.

Partition: in this section you can configure the partition number you wish to assign to the given event.

Zone: in this section you can configure the zone number you wish to assign to the given event.

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events. If you do not want to send a report to CMS on the given event, select the template named “***EMPTY***”.

Output:

In this section you can configure the output to be controlled upon occurrence of the given custom event.

Output control mode: in this section you can configure the control mode of the output.

Available options:

- **None**: the output will not be used.
- **Monostable**: the output will be activated for the time configured in the **"*Duration*"** section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 60 minutes.
- **Bistable ON**: the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF**: the output will become deactivated.
- **State change**: the output will change state (if deactivated, it will become activated and if activated, it will become deactivated).
- **Pulse series**: the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 1 hour, the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 1 hour too.

Output parameter settings: this option becomes available if an output control mode is selected which has further settings. In this section you can configure the additional settings of specific output control modes, such as timings for monostable control and pulse series. Click on the "***Edit***" button to open the parameter configuration window.

Voice call notification:

In this section you can configure phone calls to be made when the given custom event occurs. The device will call the selected phone numbers and play the selected voice messages. You can upload voice messages as audio files in the "***Voice messages***" menu.

Voice call: in this section you can select the user phone numbers to which calls should be made. The phone numbers should be configured in advance in the "***Reporting channels***" menu. Calls will be made to the numbers enabled with the help of the checkboxes in the drop-down list.

Voice message: in this section you can select the voice message which should be played in the calls when the given event occurs. When receiving a call from the device, a built-in siren tone will be played before each voice message. If a voice message has been configured for which no message has been recorded, the siren tone will be played continuously throughout the call.

Text-based notifications:

In this section you can configure text-based messages to be sent when the given custom event occurs.

SMS notification: in this section you can select the user phone numbers to which SMS message should be sent when the given event occurs. The phone numbers should be configured in advance 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 list.

Push notification: in this section you can select the mobile devices to which Push notification should be sent when the given event occurs. The mobile devices should be configured in advance in the “***Mobile devices***” menu. Push notification will be sent to the mobile devices enabled with the help of the checkboxes in the drop-down list.

E-mail notification: in this section you can select the recipients to whom e-mail should be sent when the given event occurs. The e-mail addresses should be configured in advance in the “***Reporting channels***” menu. E-mail will be sent to the addressees enabled with the help of the checkboxes in the drop-down list.

Message: in this field you can enter a custom message of maximum 45 characters, which you wish to send to the selected phone numbers, mobile devices, or e-mail addresses when the given event occurs. The device will send the same message for each notification channel (SMS, Push, e-mail).

The device is capable to insert various dynamic data in the text of the message using variables. The device will automatically replace the variable written in the message with the data related to the given variable when it sends the message.

Available variables:
$cid: the full Contact ID message configured for the given event (e.g.: 123418113001001).
$cc: the Contact ID event code configured for the given event (e.g.:130).
$cp: the partition number configured for the given event (e.g.: 01).
$cz: the zone number configured for the given event (e.g.: 001).
$name: the event name configured in the device for the given event.
$in1…**in4**: the actual state of the given contact input (0=idle, 1=activated).
$rel1: the actual state of the relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

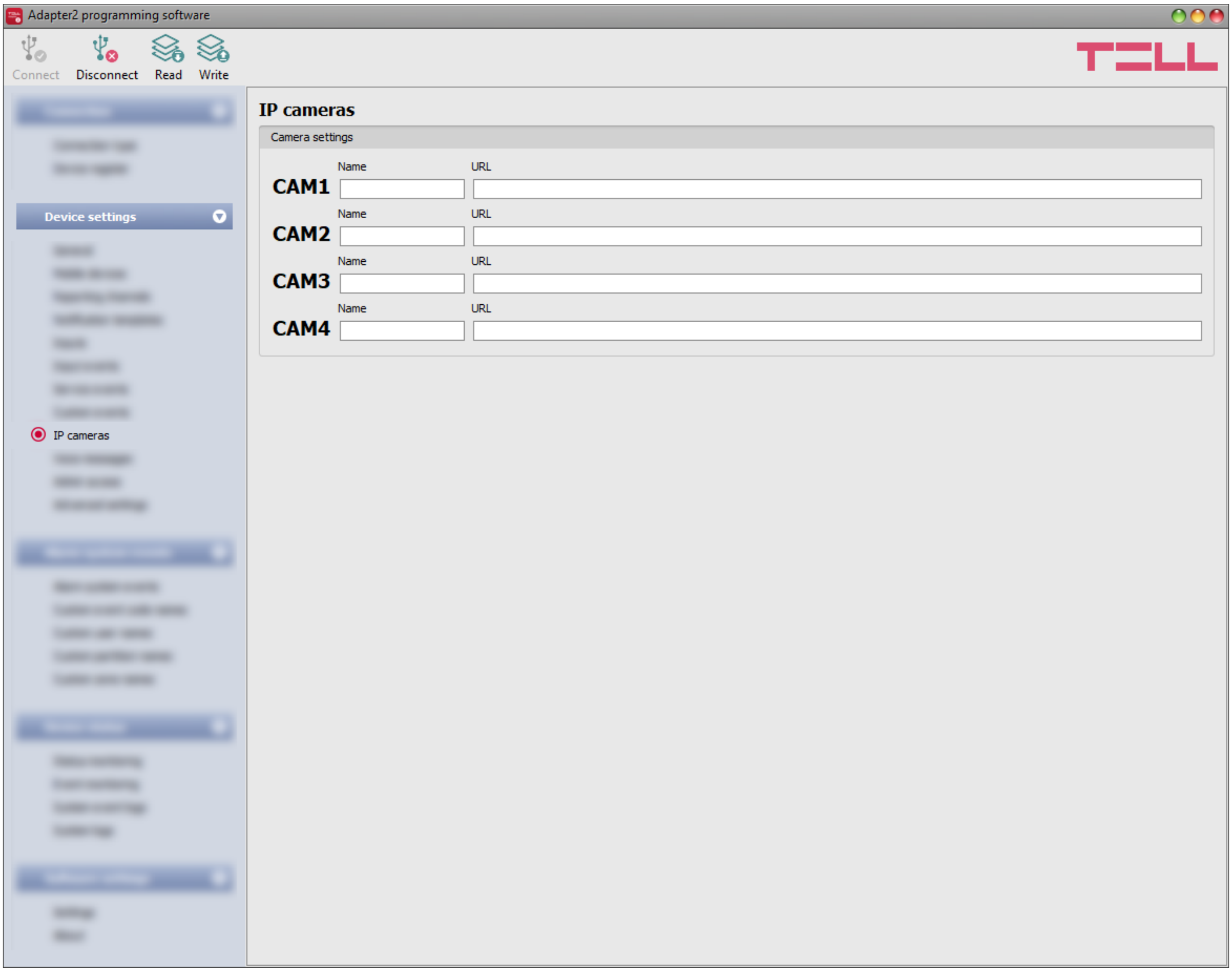
Camera: in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the “***IP cameras***” menu. If you have configured a Push notification for the given event, the mobile application will automatically offer to view the picture of the IP camera associated with the given event, when the message is received. If you have configured an e-mail notification for the given event, the URL of the IP camera assigned to the event will be sent along with the message in the given e-mail.

Click “***OK***” to accept the changes or “***Cancel***” to quit without saving.

Creating a custom event:

- click on the “***New***” button.
- Configure the new custom event based on the specification above.
- Click on the “***Write***” button to write the changes into the device.

4.2.9 IP cameras



In this menu you can configure the availabilities of up to 4 IP cameras with ONVIF support, which then can be assigned to events in the event settings. If e-mail notifications are configured for events, the URL of the IP camera assigned to the given events will be sent along with the messages in the given e-mails when the events occur. If Push notification is configured for an event, the picture of the IP camera assigned to the given event can be viewed in the mobile application upon receiving the Push notification.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.

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

Camera settings:

Name: in this section you can enter a custom name for your camera. The name entered in this section can be used to identify the cameras upon assigning them to events when configuring events.

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.

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

To access the camera pictures from outside your local network, it is necessary to replace the local IP address and port in the URL obtained using 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 *Adapter2* programming software.

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

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

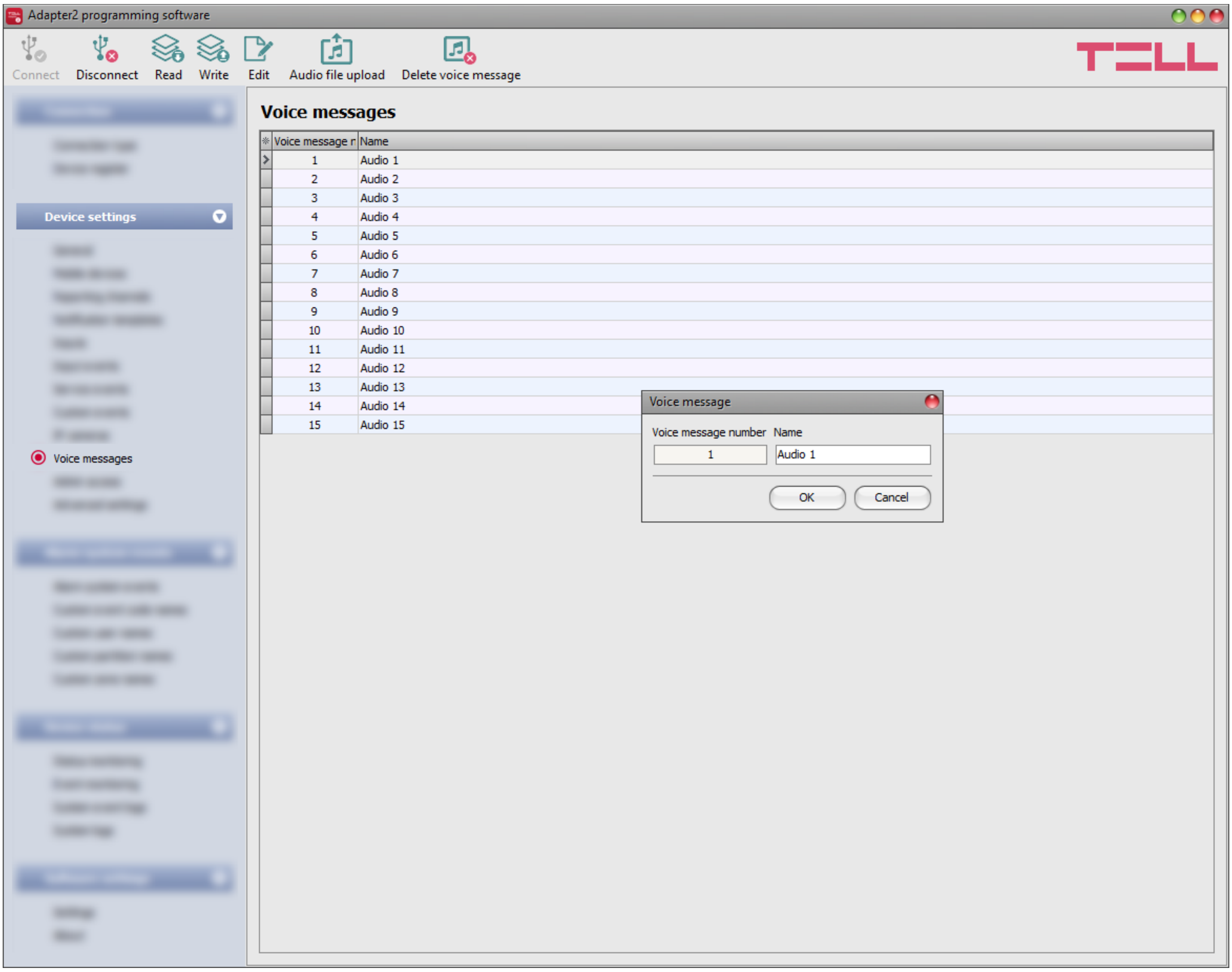
Modified URL in case of using static IP address and username/password:
rtsp://***username:password@WAN IP***:554/cam/realmonitor?channel=1&subtype….

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

Modified URL in case of using 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 you can find in the "***Reference guide to the ONVIF camera support function***" document.

4.2.10 Voice messages



Voice messages

Voice message r	Name
1	Audio 1
2	Audio 2
3	Audio 3
4	Audio 4
5	Audio 5
6	Audio 6
7	Audio 7
8	Audio 8
9	Audio 9
10	Audio 10
11	Audio 11
12	Audio 12
13	Audio 13
14	Audio 14
15	Audio 15

Voice message

Voice message number: 1
Name: Audio 1

OK Cancel

In this menu you can upload audio files used for notifications via voice calls, and you can also configure a custom name for each voice message. The audio files can be uploaded in **mp3** or **wav** format. Uploaded audio files are automatically converted by the software into the format appropriate for the device. Voice messages of up to 10 seconds length are supported, therefore a longer audio file will be cut automatically.

Available options:

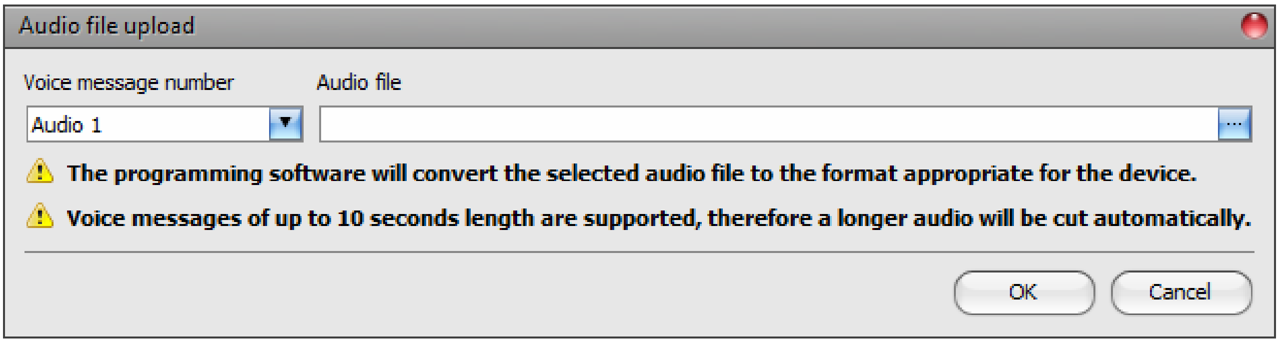
- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.

- Editing the name of an audio file:

  To edit the name of the selected audio file, click on the "***Edit***" button.

- Uploading an audio file:

  To upload an audio file to the selected voice message, click on the "***Audio file upload***" button. This will open a dialog box where you can browse the audio file.



Audio file upload

Voice message number: Audio 1

Audio file:

⚠ The programming software will convert the selected audio file to the format appropriate for the device.

⚠ Voice messages of up to 10 seconds length are supported, therefore a longer audio will be cut automatically.

  Voice message number: after clicking on the "***Audio file upload***" button, the voice message number selected in the table will be selected automatically in the dialog box as well, but you can also select a different voice message number using the drop-down menu. The audio file will be uploaded into the voice message slot selected in the drop-down menu.

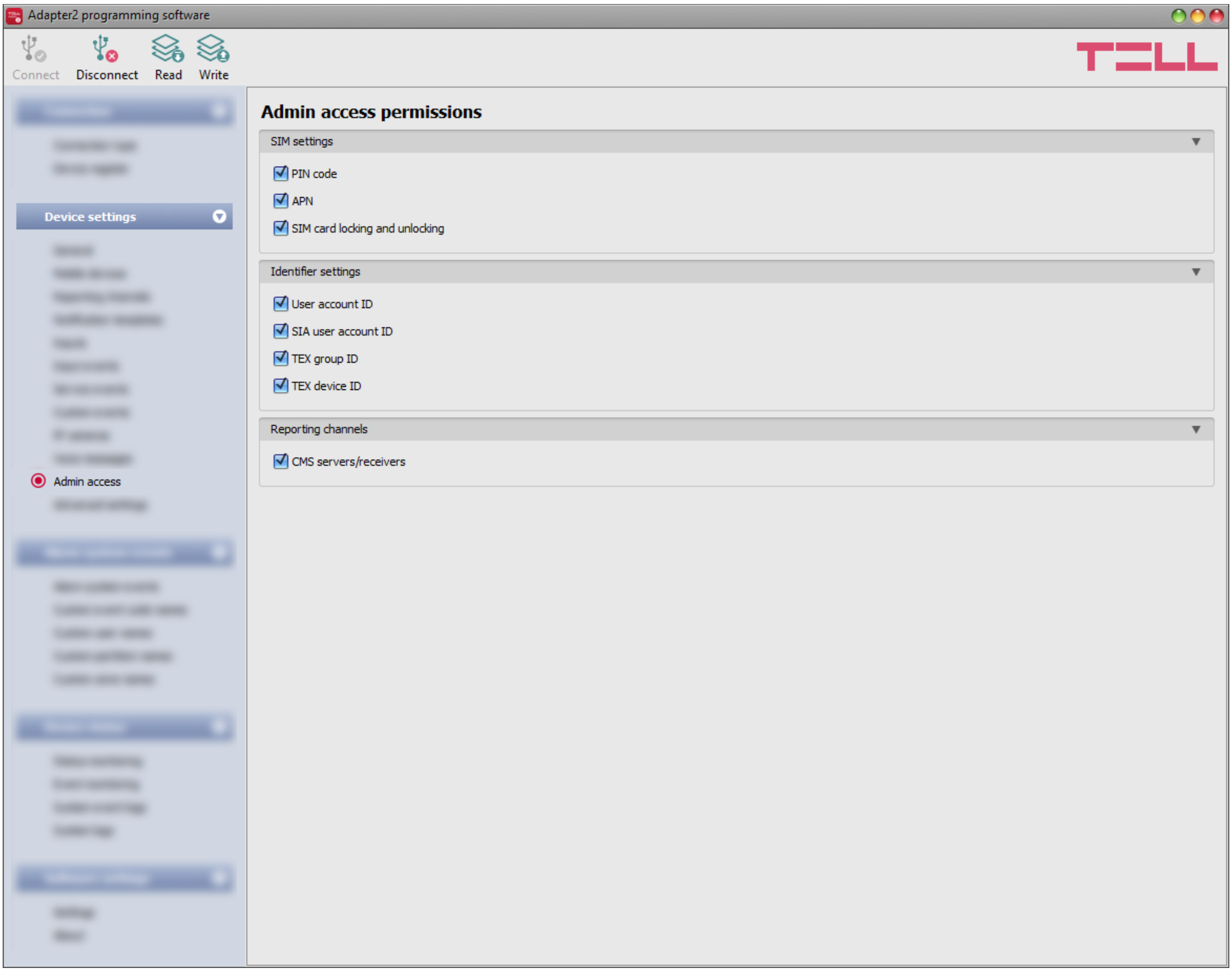
  Audio file: click on the browse button found at the end of this field, and then browse the audio file you wish to upload. Click on the "***OK***" button to start uploading the selected file.

- Delete audio file:

  To delete an audio file, select the message you want to delete by clicking on it, and then click on the "***Delete audio file***" button.

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

4.2.11 Admin access



Admin access permissions

SIM settings

☑ PIN code

☑ APN

☑ SIM card locking and unlocking

Identifier settings

☑ User account ID

☑ SIA user account ID

☑ TEX group ID

☑ TEX device ID

Reporting channels

☑ CMS servers/receivers

In this menu you can configure permissions for the Admin user to access protected settings. The Admin user can only modify the settings enabled in the list. The Admin access options can only be configured by the Superadmin.

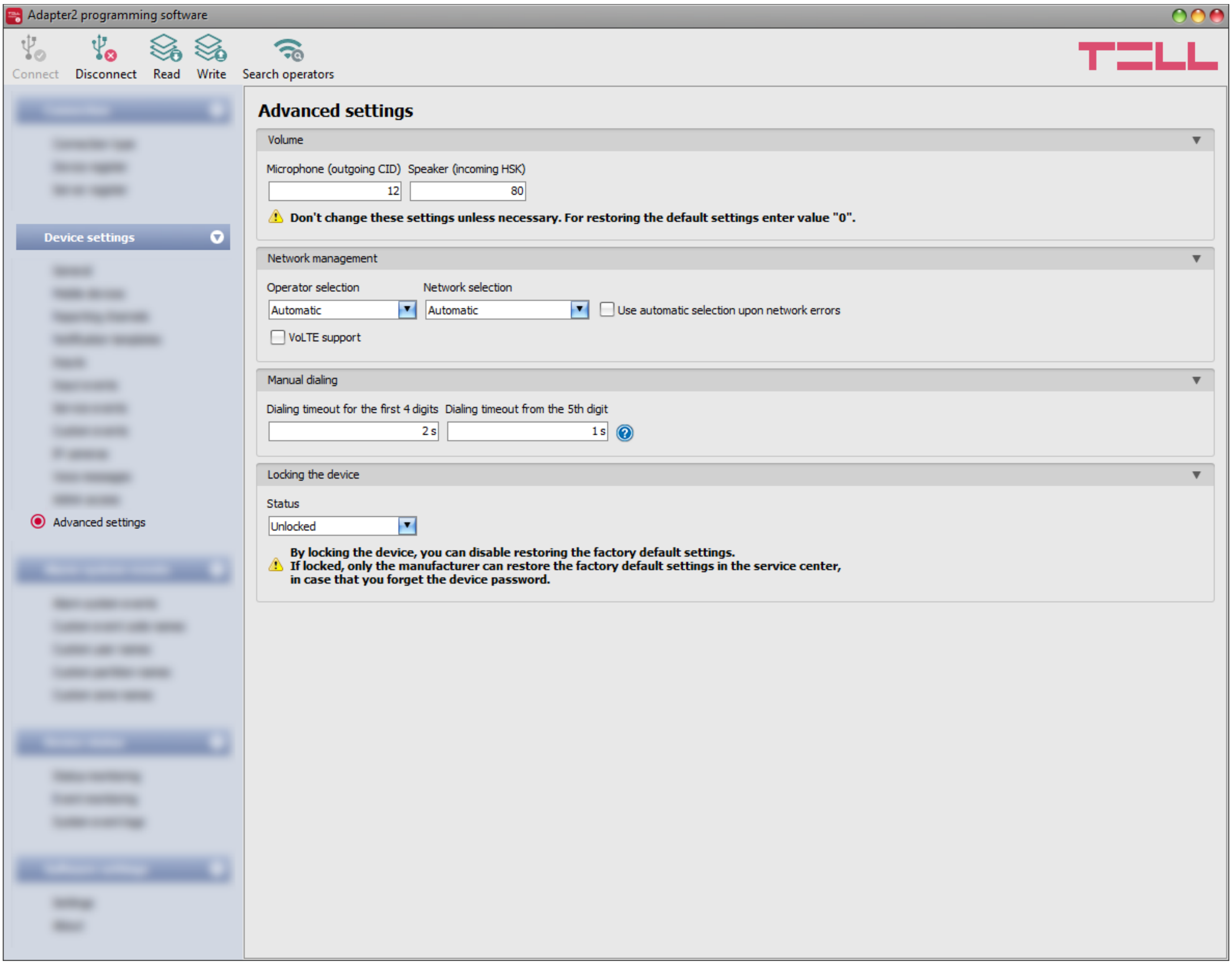
The settings that don’t have a checkmark, i.e. the ones that the Admin user does not have access to, are considered protected. To keep track of the changes made to the protected settings, the device generates a "***Settings changed***" service event if configured in the *"**Service events**"* menu, whenever the Superadmin makes any changes to any of these protected settings.

Available options:

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

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

4.2.11 Advanced settings



Advanced settings

Volume

Microphone (outgoing CID): 12

Speaker (incoming HSK): 80

⚠ Don't change these settings unless necessary. For restoring the default settings enter value "0".

Network management

Operator selection: Automatic

Network selection: Automatic

□ Use automatic selection upon network errors

□ VoLTE support

Manual dialing

Dialing timeout for the first 4 digits: 2 s

Dialing timeout from the 5th digit: 1 s

Locking the device

Status: Unlocked

⚠ By locking the device, you can disable restoring the factory default settings. If locked, only the manufacturer can restore the factory default settings in the service center, in case that you forget the device password.

In this menu you can configure advanced settings which affect communication to CMS over DTMF-based voice call and the in-call volume for calls to users (siren tone, voice messages). Special DTMF communication parameters can be configured to adjust signals in case of experiencing problems with reporting to CMS over DTMF-based voice call. The default mobile operator and network to be used by the modem and device lock settings can also be configured here.

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

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.

- Searching mobile operators:

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

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

Volume:

Microphone (outgoing CID): adjusts the microphone volume, which makes outgoing tones (Contact ID) louder or softer in voice calls. The value can be set from 1 to 15.

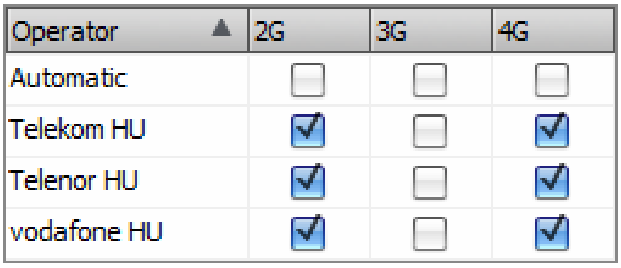
Speaker (incoming HSK): adjusts the speaker volume, which makes incoming tones (HSK and ACK) louder or softer in voice calls. The value can be set from 1 to 100.

Note! Even minor changes of the values result significant tone volume changes!

Network management:

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

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



Operator ▲	2G	3G	4G
Automatic	☐	☐	☐
Telekom HU	☑	☐	☑
Telenor HU	☑	☐	☑
vodafone HU	☑	☐	☑

Network selection: 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 the network you wish to use manually.

Available options:

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

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

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

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

Manual dialing:

If you are using the device with a telephone handset, for manual dialing of telephone numbers you can configure the time the device should wait after each entered digit, before it starts dialing the number. You can set the time separately for the first 4 digits, and from the 5th digit up to the end of the number.

Dialing timeout for the first 4 digits: in this section you can set the time the device waits after each digit before it starts dialing the entered number, when you enter the first 4 digits of the number.

Dialing timeout from the 5th digit: in this section you can set the time the device waits after each digit before it starts dialing the entered number, when you enter the 5th and next digits of the number.

Locking the device:

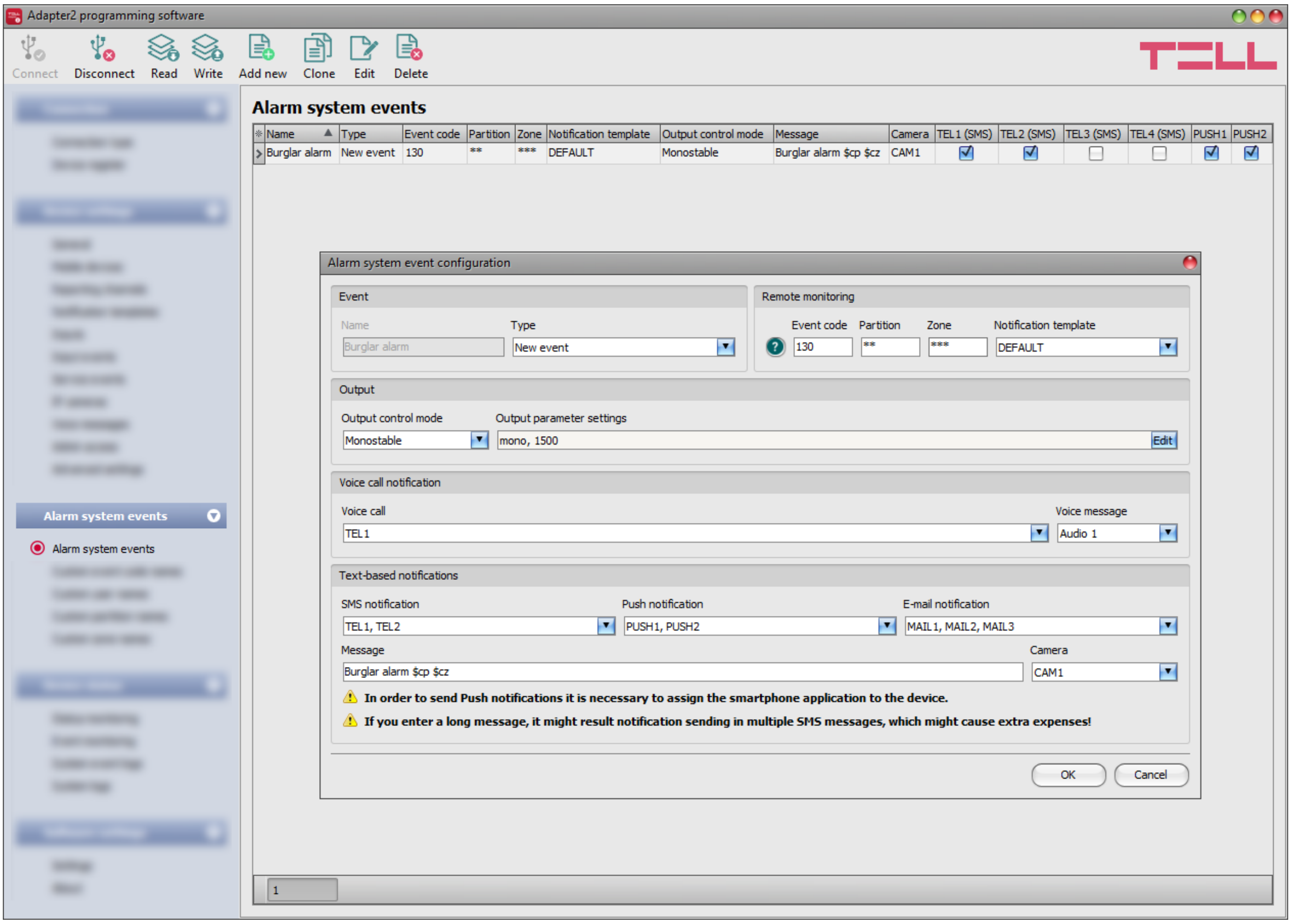
Status: you can lock your device with this setting, so that the factory default settings cannot be restored without knowing the device password.

- **Unlocked**: when unlocked, the factory default settings can be restored anytime, also without knowing the device password.
- **Locked**: when locked, restoring the factory default settings is disabled. You can restore the factory default settings only after logging in with the Superadmin or Admin password and changing the setting to unlocked. If you forget these passwords, only the manufacturer can restore the factory default settings in the service center.

4.3 Alarm system events menu

In this menu group you can configure settings of events sent by the alarm system.

4.3.1 Alarm system events



Alarm system events

Name	Type	Event code	Partition	Zone	Notification template	Output control mode	Message	Camera	TEL1 (SMS)	TEL2 (SMS)	TEL3 (SMS)	TEL4 (SMS)	PUSH1	PUSH2
Burglar alarm	New event	130	**	***	DEFAULT	Monostable	Burglar alarm $cp $cz	CAM1	☑	☑	□	□	☑	☑

Alarm system event configuration

Event
Name: Burglar alarm
Type: New event

Remote monitoring
Event code: 130
Partition: **
Zone: ***
Notification template: DEFAULT

Output
Output control mode: Monostable
Output parameter settings: mono, 1500

Voice call notification
Voice call: TEL1
Voice message: Audio 1

Text-based notifications
SMS notification: TEL1, TEL2
Push notification: PUSH1, PUSH2
E-mail notification: MAIL1, MAIL2, MAIL3
Message: Burglar alarm $cp $cz
Camera: CAM1

⚠ In order to send Push notifications it is necessary to assign the smartphone application to the device.

⚠ If you enter a long message, it might result notification sending in multiple SMS messages, which might cause extra expenses!

The “***Alarm system events***” menu can be used to filter Contact-ID event codes received from the alarm control panel connected to the device. For each event filter added you can configure separately which notification template to use for reporting to monitoring station, which user to notify by call, SMS, Push notification or email and what message to send, and to control or not the output when the given event code is received from the alarm control panel, or an event code is received which matches the conditions configured in the given event filter.

When entering the event code, partition, and zone, you can use the "∗" character to define a group of events. This means that when any hexadecimal number is received from the alarm control panel in the place of the "∗" character written in the code, but the rest of the event code matches the event received from the alarm control panel, the given event will be processed. When receiving an event code from the alarm control panel, the device compares the received event with the event filters added to the table and if it finds a matching one, it performs the reporting and output control according to the settings of the given alarm system event filter. The device compares the events starting with the event type, then the event code, and finally with the partition and zone, in this order.

The device chooses in each case the added alarm system event filter which matches best the event code received from the alarm control panel. For example if it finds two added alarm system event filters at which the event type, the event code and the partition matches the event received from the alarm control panel, but at one of them the zone section matches too, while at the other one the zone section is filled in with "*" characters, so the received event matches both alarm system event filters, the device will choose the one at which the zone section matches too.

If an event code is received from the alarm control panel which does not match any of the event filters configured, i.e., the device cannot find a reporting configuration for the given event code, then it will report the given event to CMS automatically using the notification template named "***DEFAULT***" to ensure that all events are reported.

If you wish to report only specific events to CMS, add a filter that applies to all events, where choose the "***New event, Restore, Repeat***" option for event type and fill the event code, partition, and zone number fields with "*" characters, and select for this the notification template named "***EMPTY***". With this, reporting to CMS of any event received from the alarm control panel will be disabled. Thereafter, configure and add the events you wish to be reported. In this case only the specified events will be reported, and the device will send the kiss-off (ACK) signal to the alarm control panel for all other events but will not report them to CMS.

The system supports adding up to **500** alarm system event filters.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding new alarm system event:
  To add a new alarm system event, click on the "***New***" button.
- Creating a copy of an existing alarm system event:
  To create a copy of the selected alarm system event, click on the "***Clone***" button. Please note that the new copy should have a different unique name.
- Editing alarm system event settings:
  To edit the settings of the selected alarm system event, click on the "***Edit***" button.
- Deleting an alarm system event:
  To delete the selected alarm system event, click on the "***Delete***" button.

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

Event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

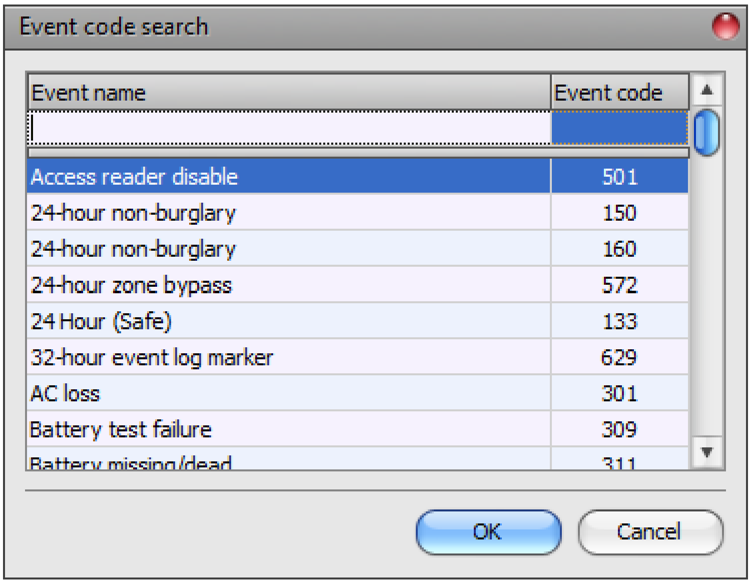
Type: the type of the event. You can choose from the following options: new event, restore, repeat, new event + restore, new event + repeat, restore + repeat, new event + restore + repeat.

Remote monitoring:

In this section you can configure the Contact ID event code expected from the alarm control panel and can assign one of the preconfigured notification templates to the given event.

Event code: in this section you can configure the 3-digit Contact ID event code, consisting of characters 0..9,A,B,C,D,E,F, or "∗", which you wish to filter, from the messages coming from the alarm control panel.

The software includes a built-in event code search tool which contains the list of standard Contact ID codes. The search tool opens by clicking on the ? icon with the question mark symbol placed in front of the event code input field.



Event name	Event code
Access reader disable	501
24-hour non-burglary	150
24-hour non-burglary	160
24-hour zone bypass	572
24 Hour (Safe)	133
32-hour event log marker	629
AC loss	301
Battery test failure	309
Battery missing/dead	311

In the event code search tool, you can search for events by name or by event code. For searching by name, start typing the name of the searched event code in the field under the "***Event name***" column header. For searching by event code, start typing the searched event code number in the field under the "***Event code***" column header. The search tool will filter the list automatically according to the hits. You can select an event code by clicking on it in the list, then the program will paste this automatically into the event code input field after clicking on the "***OK***" button.

Partition: in this section you can configure the partition number consisting of characters 00…99, or "∗", which you wish to filter from the messages coming from the alarm control panel.

Zone: in this section you can configure the zone number consisting of characters 000…999, or "∗", which you wish to filter from the messages coming from the alarm control panel.

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events. If you do not want to send a report to CMS on the given event, select the template named "***EMPTY***".

Output:

In this section you can configure the output to be controlled upon receiving the configured alarm system event.

Output control mode: in this section you can configure the control mode of the output.

Available options:

- **None**: the output will not be used.
- **Monostable**: the output will be activated for the time configured in the ***"Duration"*** section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 1 hour.
- **Bistable ON**: the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF**: the output will become deactivated.
- **Pulse series**: the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 1 hour, the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 1 hour too.

Output parameter settings: this option becomes available if an output control mode is selected which has further settings. In this section you can configure the additional settings of specific output control modes, such as timings for monostable control and pulse series. Click on the "***Edit***" button to open the parameter configuration window.

Voice call notification:

In this section you can configure phone calls to be made when the given alarm system event occurs. The device will call the selected phone numbers and play the selected voice messages. You can upload voice messages as audio files in the "***Voice messages***" menu.

Voice call: in this section you can select the user phone numbers to which calls should be made. The phone numbers should be configured in advance in the "***Reporting channels***" menu. Calls will be made to the numbers enabled with the help of the checkboxes in the drop-down list.

Voice message: in this section you can select the voice message which should be played in the calls when the given event occurs. When receiving a call from the device, a built-in siren tone will be played before each voice message. If a voice message has been configured for which no message has been uploaded, the siren tone will be played continuously throughout the call.

Text-based notifications:

In this section you can configure text-based messages to be sent when the given alarm system event occurs.

SMS notification: in this section you can select the user phone numbers to which SMS message should be sent when the given event occurs. The phone numbers should be configured in advance 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 list.

Push notification: in this section you can select the mobile devices to which Push notification should be sent when the given event occurs. The mobile devices should be configured in advance in the "***Mobile devices***" menu. Push notification will be sent to the mobile devices enabled with the help of the checkboxes in the drop-down list.

E-mail notification: in this section you can select the recipients to whom e-mail should be sent when the given event occurs. The e-mail addresses should be configured in advance in the "***Reporting channels***" menu. E-mail will be sent to the addressees enabled with the help of the checkboxes in the drop-down list.

Message: in this field you can enter a custom message of maximum 45 characters, which you wish to be sent to the selected phone numbers, mobile devices, or e-mail addresses when the given event occurs. The device will send the same message for each notification channel (SMS, Push, e-mail).

The device is capable to insert various dynamic data in the text of the message using variables. The device will automatically replace the variable written in the message with the data related to the given variable when it sends the message.

Available variables:

$cn: the event name configurable in the "***Custom event code names***" menu, associated with the event code received from the alarm control panel. If you have not modified the new/restore event name, the device will replace the variable with the default event name in the message.

$cp: the partition name configurable in the "***Custom partition names***" menu, associated with the partition number received from the alarm control panel. If a custom partition name has not been configured for the given partition number, the device will replace the variable with the partition number in the message. (e.g.: 01).

$cz: the zone or user name configurable in the "***Custom zone names***" and "***Custom user names***" menu, associated with the zone/user number received from the alarm control panel. If a custom zone or user name has not been configured for the given zone/user number, the device will replace the variable with the zone/user number in the message. (e.g.: 001).

$cid: the complete Contact ID message received from the alarm control panel (eg.: 123418113001001).

$cc: the Contact ID event code received from the alarm control panel (e.g.:130).

$name: the name configured for the given event in the "***Alarm system events***" menu.

$in1…**in4**: the actual state of the given contact input (0=idle, 1=activated)

$rel1: the actual state of the relay output (0=idle, 1=activated)

$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

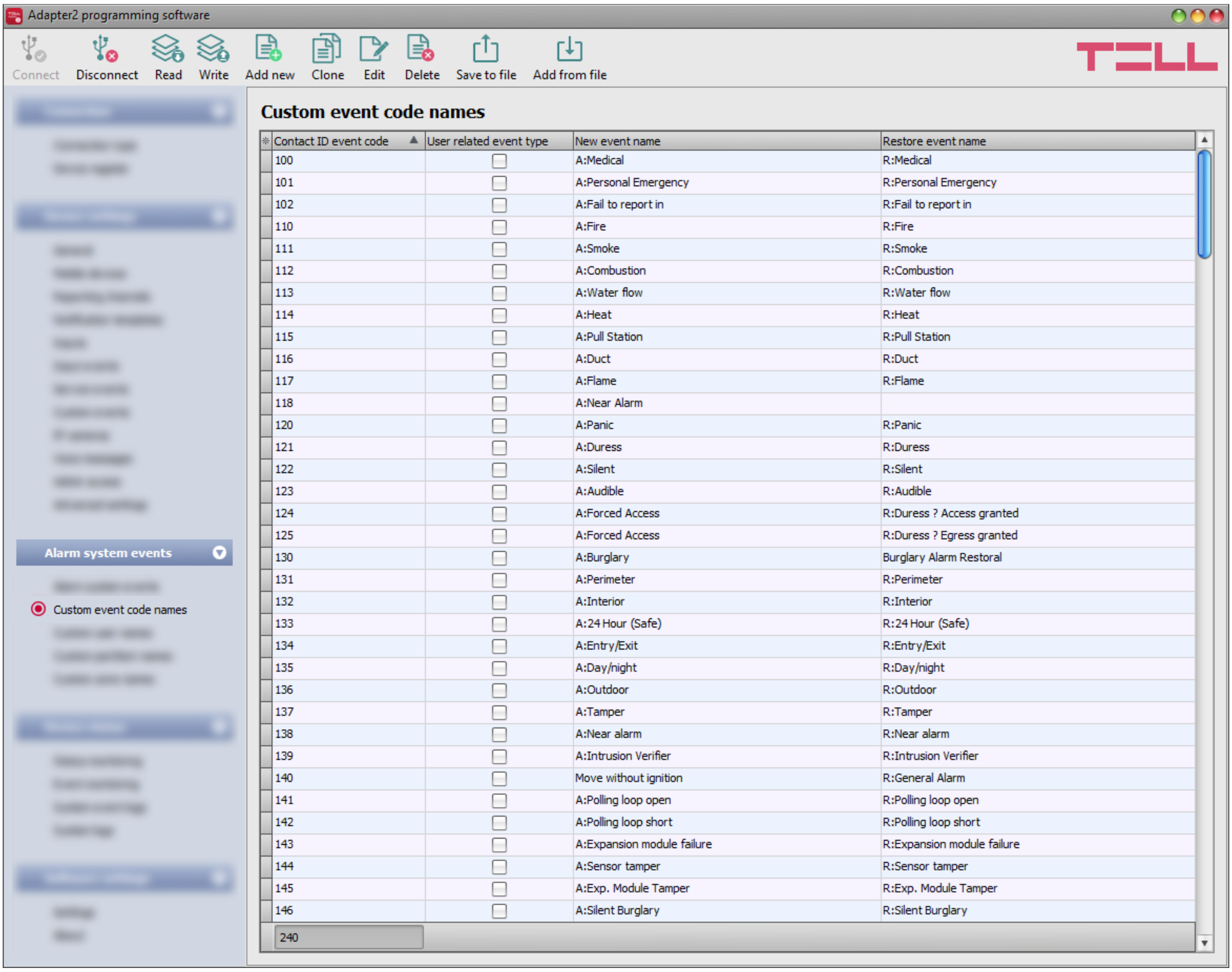
Camera: in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the "***IP cameras***" menu. If you have configured a Push notification for the given event, the mobile application will automatically offer to view the picture of the IP camera associated with the given event, when the message is received. If you have configured an e-mail notification for the given event, the URL of the IP camera assigned to the event will be sent along with the message in the given e-mail.

Click "***OK***" to accept the changes or "***Cancel***" to quit without saving.

Adding a new alarm system event filter:

- Click on the "***New***" button.
- Configure the event you wish to filter based on the above.
- Click on the "***Write***" button to write the changes into the device.

4.3.2 Custom event code names



Custom event code names

Contact ID event code	User related event type	New event name	Restore event name
100	☐	A:Medical	R:Medical
101	☐	A:Personal Emergency	R:Personal Emergency
102	☐	A:Fail to report in	R:Fail to report in
110	☐	A:Fire	R:Fire
111	☐	A:Smoke	R:Smoke
112	☐	A:Combustion	R:Combustion
113	☐	A:Water flow	R:Water flow
114	☐	A:Heat	R:Heat
115	☐	A:Pull Station	R:Pull Station
116	☐	A:Duct	R:Duct
117	☐	A:Flame	R:Flame
118	☐	A:Near Alarm	
120	☐	A:Panic	R:Panic
121	☐	A:Duress	R:Duress
122	☐	A:Silent	R:Silent
123	☐	A:Audible	R:Audible
124	☐	A:Forced Access	R:Duress ? Access granted
125	☐	A:Forced Access	R:Duress ? Egress granted
130	☐	A:Burglary	Burglary Alarm Restoral
131	☐	A:Perimeter	R:Perimeter
132	☐	A:Interior	R:Interior
133	☐	A:24 Hour (Safe)	R:24 Hour (Safe)
134	☐	A:Entry/Exit	R:Entry/Exit
135	☐	A:Day/night	R:Day/night
136	☐	A:Outdoor	R:Outdoor
137	☐	A:Tamper	R:Tamper
138	☐	A:Near alarm	R:Near alarm
139	☐	A:Intrusion Verifier	R:Intrusion Verifier
140	☐	Move without ignition	R:General Alarm
141	☐	A:Polling loop open	R:Polling loop open
142	☐	A:Polling loop short	R:Polling loop short
143	☐	A:Expansion module failure	R:Expansion module failure
144	☐	A:Sensor tamper	R:Sensor tamper
145	☐	A:Exp. Module Tamper	R:Exp. Module Tamper
146	☐	A:Silent Burglary	R:Silent Burglary

240

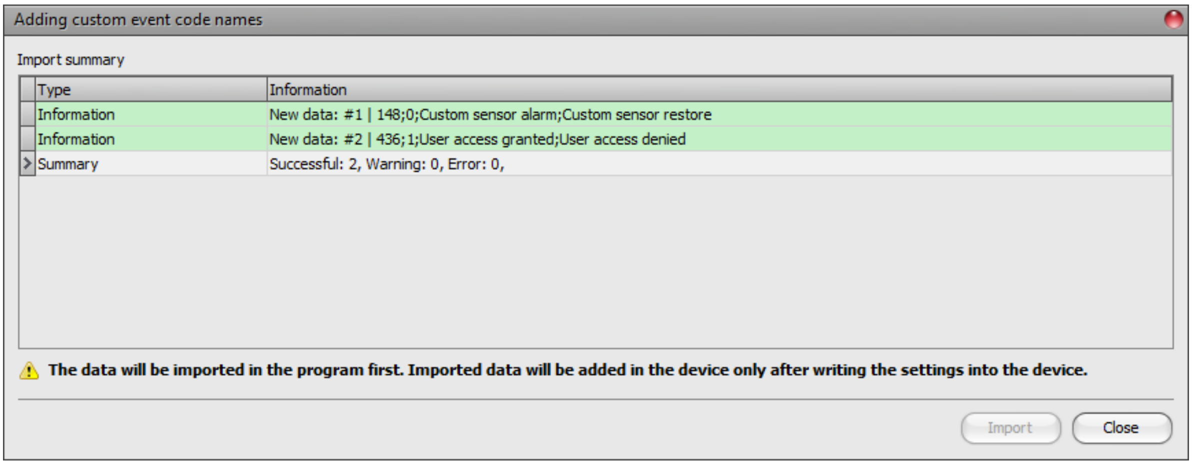
The table found in the “***Custom event code names***” menu contains the default Contact ID event codes and event names. If needed, you can rename the events generated by the connected alarm control panel, or add new custom events if your alarm control panel would use an evet code that is missing from the event code table of the device. The device can use the event code names displayed here in text-notifications (SMS, Push, e-mail). The ***$cn*** variable written in the text of the message will be replaced by the device automatically with the event name associated in the table with the event code received from the alarm control panel, when sending the message. This will result in the message being received with the specific name of the event instead of the raw event code.

You can record altogether up to **370** custom event codes and default event code name changes in the system.

User related event type: this setting is used to qualify an event as user related or zone related. If the checkbox is enabled, the device will consider the given event as user related, and if it is disabled, the event will be considered as zone related. This option is relevant when you use the **$cz** variable in messages, which the device will replace with a configured custom user name or zone name. The device can decide from this setting, whether it has to replace the variable in the message with a user name or a zone name, when it reports the given event via text message.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new custom event code:
  To add a new custom event code, click on the "***New***" button.
- Creating a copy of an existing event code:
  To create a copy of the selected event code, click on the "***Clone***" button. Please note that the new copy should have a different unique event code.
- Editing event code name:
  To edit the name of the selected event code, click on the "***Edit***" button.
- Deleting a custom event code:
  To delete the selected custom event code, click on the "***Delete***" button.
- Saving the custom event code names database to file:
  To save the custom event code names to file in csv format, click on the "***Save to file***" button.
- Adding custom event code names from file:
  It is possible to add custom event code names from a csv file prepared in advance. To add custom event code names from file, click on the "***Add from file***" button, browse the file, and then click on the "***Import***" button. By this, the program will read the entries from the selected file and will prepare an import summary. The event code names stored in the device will not be deleted by adding entries from file, but the imported entries will be added to the existing ones.



Adding custom event code names

Import summary

Type	Information
Information	New data: #1 | 148;0;Custom sensor alarm;Custom sensor restore
Information	New data: #2 | 436;1;User access granted;User access denied
Summary	Successful: 2, Warning: 0, Error: 0,

⚠ The data will be imported in the program first. Imported data will be added in the device only after writing the settings into the device.

The structure requirements of the CSV file to be imported:

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 entries starting from the second line. The line should start with the 3-digit event code, followed by the event type indicator (**0**=zone related event, **1**=user related event), the custom new event name, and then the custom restore event name, each separated by a semicolon. Example:

```
148;0;Custom sensor alarm;Custom sensor restore
436;1;User access granted;User access denied
```

The easiest way to prepare the file is exporting the custom event code names database from the program using the "***Save to file***" button, and then edit the exported file and enter the desired custom data in the file by the analogy of the file content, and finally delete the original entries from the file.

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

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

Information (green background color): entries imported successfully.

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

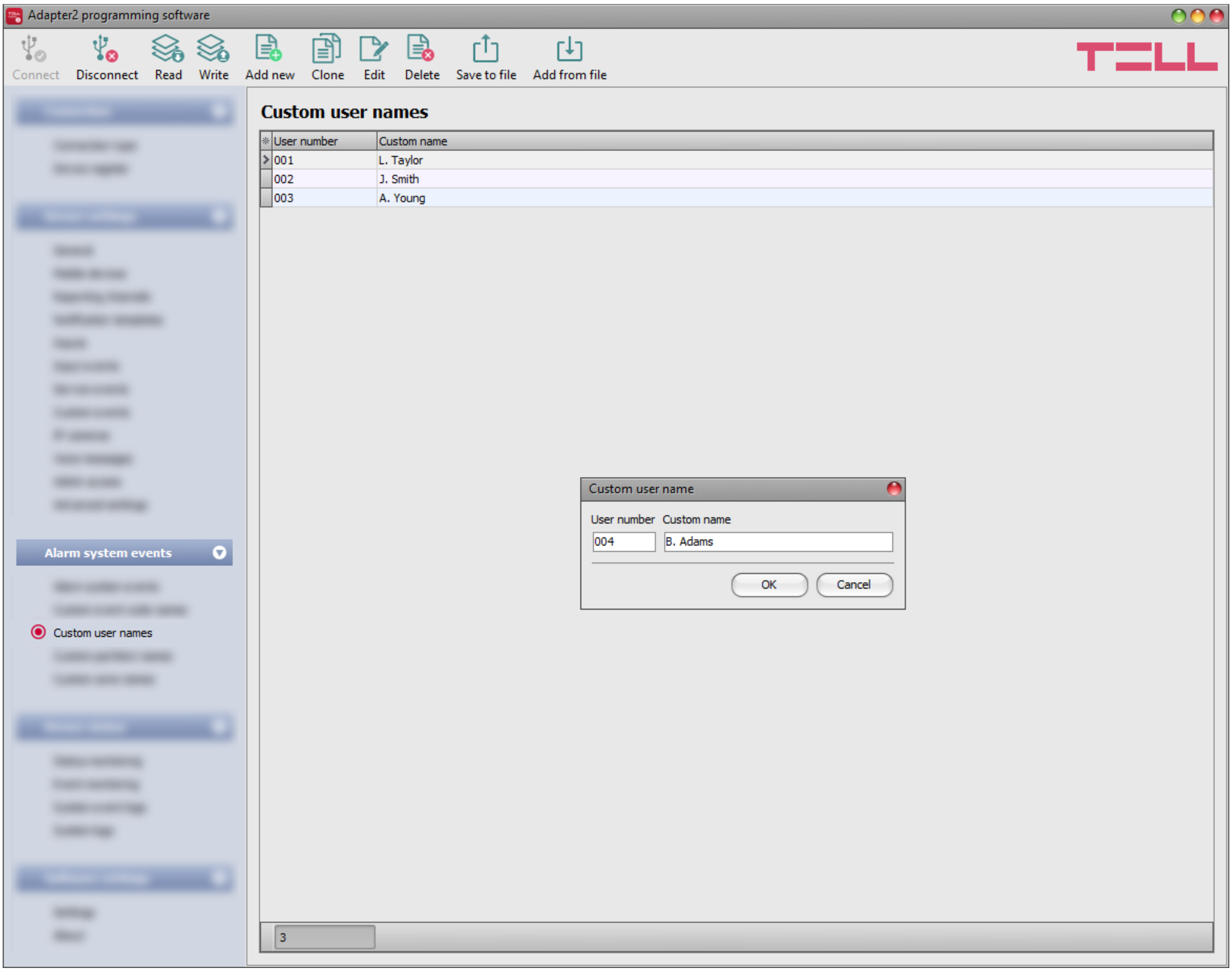
Error (red background color): entries with errors, which the program cannot process.

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

You can find a summary line at the bottom of the list, showing 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 list of custom event code names. After that, you can edit and continue to configure the entries imported into the program as needed, and when finished, write the settings into the device by clicking on the "***Write***" button.

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

4.3.3 Custom user names



Custom user names

User number	Custom name
001	L. Taylor
002	J. Smith
003	A. Young

3

Custom user name

User number	Custom name
004	B. Adams

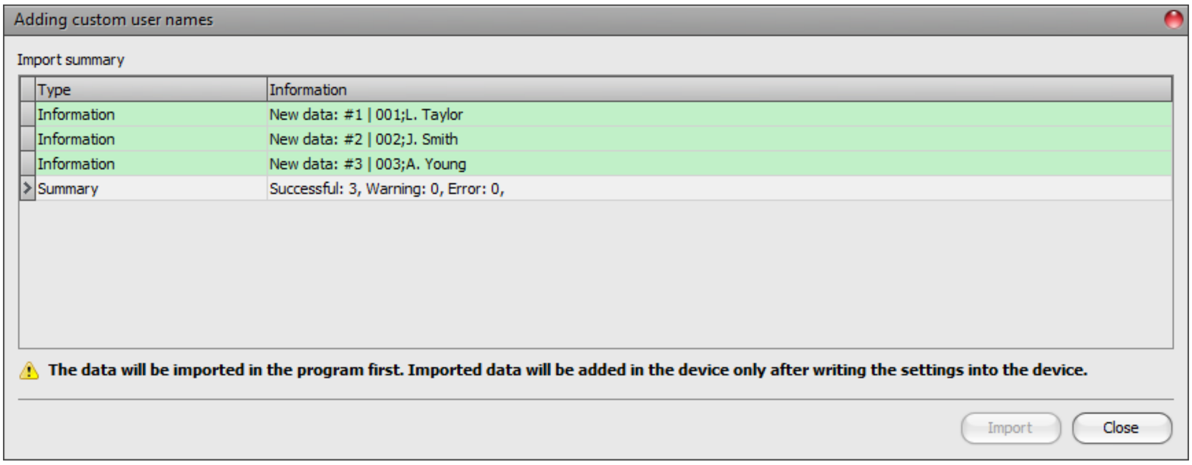
In the “***Custom user names***” menu you can associate names with users configured in the alarm control panel, by the user number. The device can use the custom user names configured here in text-notifications (SMS, Push, e-mail). The ***$cz*** variable written in the text of the message will be replaced by the device automatically with the user name associated with the user number received from the alarm control panel, when the device reports a user related event. This will result in the message being received with the specific name of the user instead of the raw user number. The user related events can be configured in the “***Custom event code names***” menu.

If a custom user name has not been configured for the given user number, the device will replace the variable with the user number in the message. (e.g.: 001).

The system can store up to **20** custom user names.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new custom username:
  To add a new custom user name, click on the "***New***" button.
- Creating a copy of an existing custom user name:
  To create a copy of the selected custom user name, click on the "***Clone***" button. Please note that the new copy should have a different unique user number.
- Editing a custom user name:
  To edit the selected custom user name, click on the "***Edit***" button.
- Deleting a custom user name:
  To delete the selected custom user name, click on the "***Delete***" button.
- Saving the custom user names database to file:
  To save the custom user names to file in csv format, click on the "***Save to file***" button.
- Adding custom user names from file:
  It is possible to add custom user names from a csv file prepared in advance. To add custom user names from file, click on the "***Add from file***" button, browse the file, and then click on the "***Import***" button. By this, the program will read the entries from the selected file and will prepare an import summary. If there are already custom user names stored in the device, those will not be deleted by adding entries from file, but the imported user names will be added to the existing ones.



Adding custom user names

Import summary

Type	Information
Information	New data: #1 | 001;L. Taylor
Information	New data: #2 | 002;J. Smith
Information	New data: #3 | 003;A. Young
Summary	Successful: 3, Warning: 0, Error: 0,

⚠ **The data will be imported in the program first. Imported data will be added in the device only after writing the settings into the device.**

The structure requirements of the CSV file to be imported:

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 entries starting from the second line. The line should start with the 3-digit user number, followed by a semicolon, and then the user name. Example:

```
001;L. Taylor
002;J. Smith
```

The easiest way to prepare the file is adding at least one custom user name in the program, and then export it to csv file using the “***Save to file***” button, and then edit the exported file and enter the further custom user names in the file by the analogy of the file content.

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

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

Information (green background color): entries imported successfully.

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

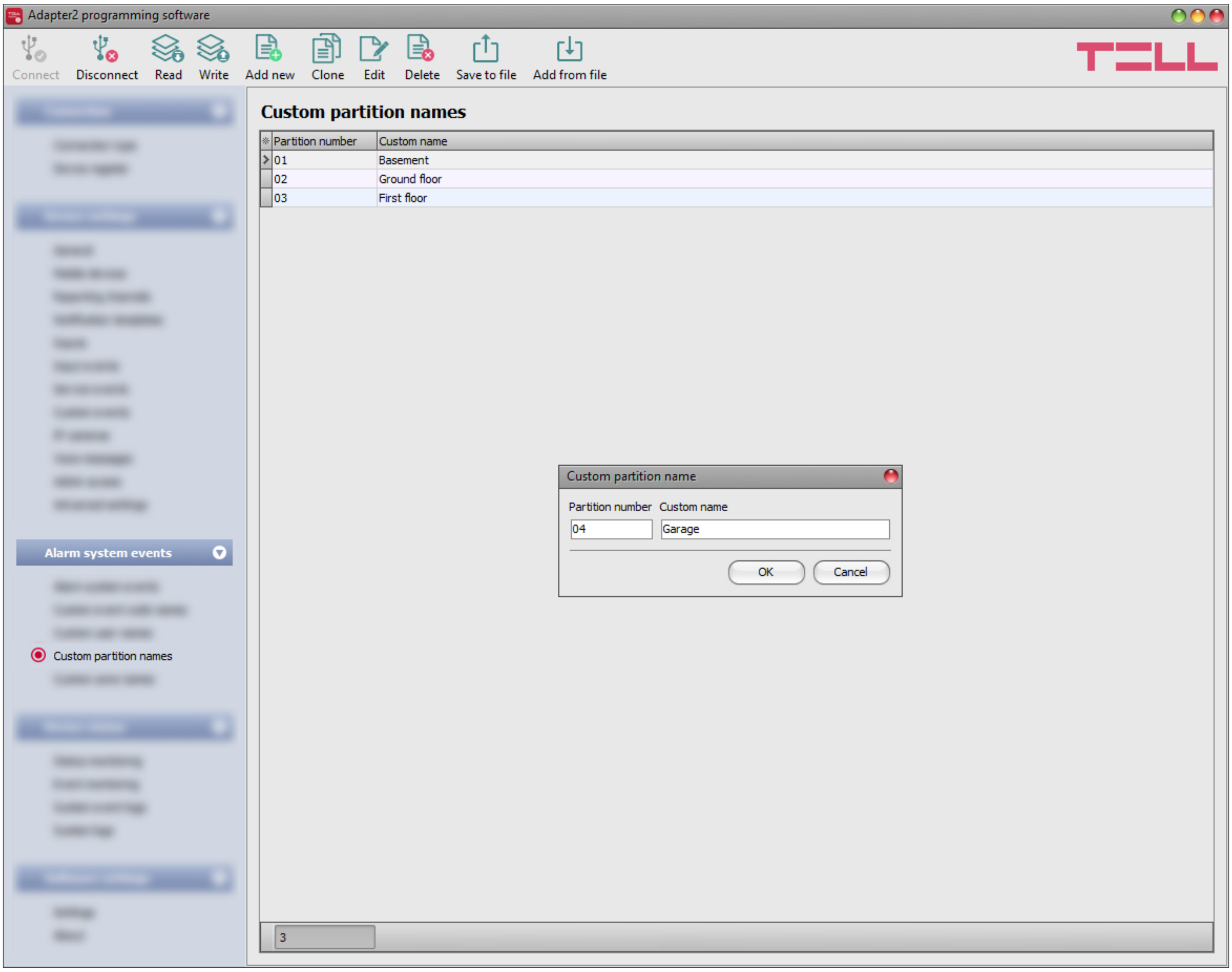
Error (red background color): entries with errors, which the program cannot process.

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

You can find a summary line at the bottom of the list, showing 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 list of custom user names. After that, you can edit and continue to configure the entries imported into the program as needed, and when finished, write the settings into the device by clicking on the “***Write***” button.

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

4.3.4 Custom partition names



Custom partition names

Partition number	Custom name
01	Basement
02	Ground floor
03	First floor

Custom partition name

Partition number: 04

Custom name: Garage

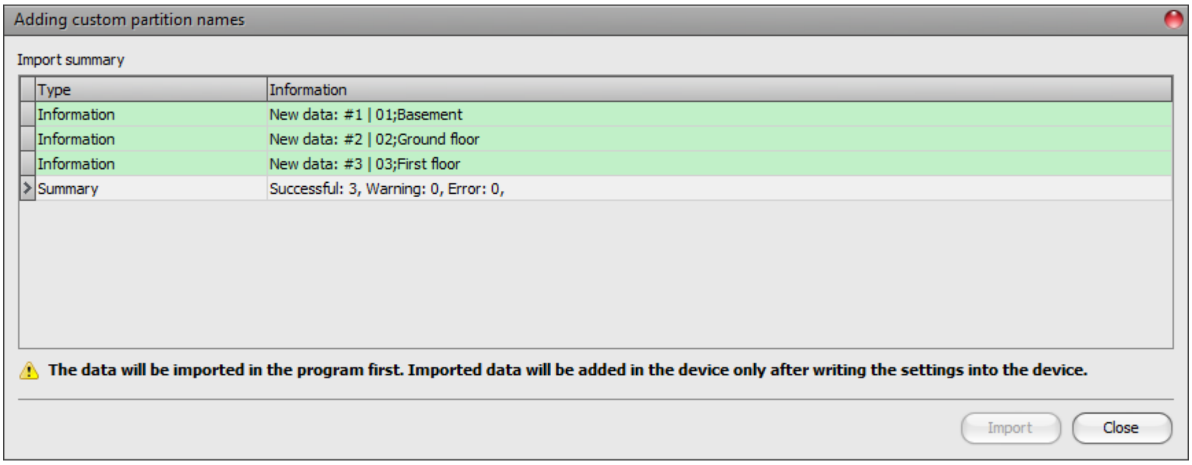
In the “***Custom partition names***” menu you can associate names with partitions configured in the alarm control panel, by the partition number. The device can use the custom partition names configured here in text-notifications (SMS, Push, e-mail). The ***$cp*** variable written in the text of the message will be replaced by the device automatically with the partition name associated with the partition number received from the alarm control panel, when sending the message. This will result in the message being received with the specific name of the partition instead of the raw partition number.

If a custom partition name has not been configured for the given partition number, the device will replace the variable with the partition number in the message. (e.g.: 01).

The system can store up to **20** custom partition names.

Available options:

- Read the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Write the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new custom partition name:
  To add a new custom partition name, click on the "***New***" button.
- Creating a copy of an existing custom partition name:
  To create a copy of the selected custom partition name, click on the "***Clone***" button. Please note that the new copy should have a different unique partition number.
- Editing a custom partition name:
  To edit the selected custom partition name, click on the "***Edit***" button.
- Deleting a custom partition name:
  To delete the selected custom partition name, click on the "***Delete***" button.
- Saving the custom partition names database to file:
  To save the custom partition names to file in csv format, click on the "***Save to file***" button.
- Adding custom partition names from file:
  It is possible to add custom partition names from a csv file prepared in advance. To add custom partition names from file, click on the "***Add from file***" button, browse the file, and then click on the "***Import***" button. By this, the program will read the entries from the selected file and will prepare an import summary. If there are already custom partition names stored in the device, those will not be deleted by adding entries from file, but the imported partition names will be added to the existing ones.



Type	Information
Information	New data: #1 | 01;Basement
Information	New data: #2 | 02;Ground floor
Information	New data: #3 | 03;First floor
Summary	Successful: 3, Warning: 0, Error: 0,

⚠ The data will be imported in the program first. Imported data will be added in the device only after writing the settings into the device.

The structure requirements of the CSV file to be imported:

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 entries starting from the second line. The line should start with the 2-digit partition number, followed by a semicolon, and then the partition name. Example:

01;Basement
02;Ground floor

The easiest way to prepare the file is adding at least one custom partition name in the program, and then export it to csv file using the "***Save to file***" button, and then edit the exported file and enter the further custom partition names in the file by the analogy of the file content.

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

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

Information (green background color): entries imported successfully.

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

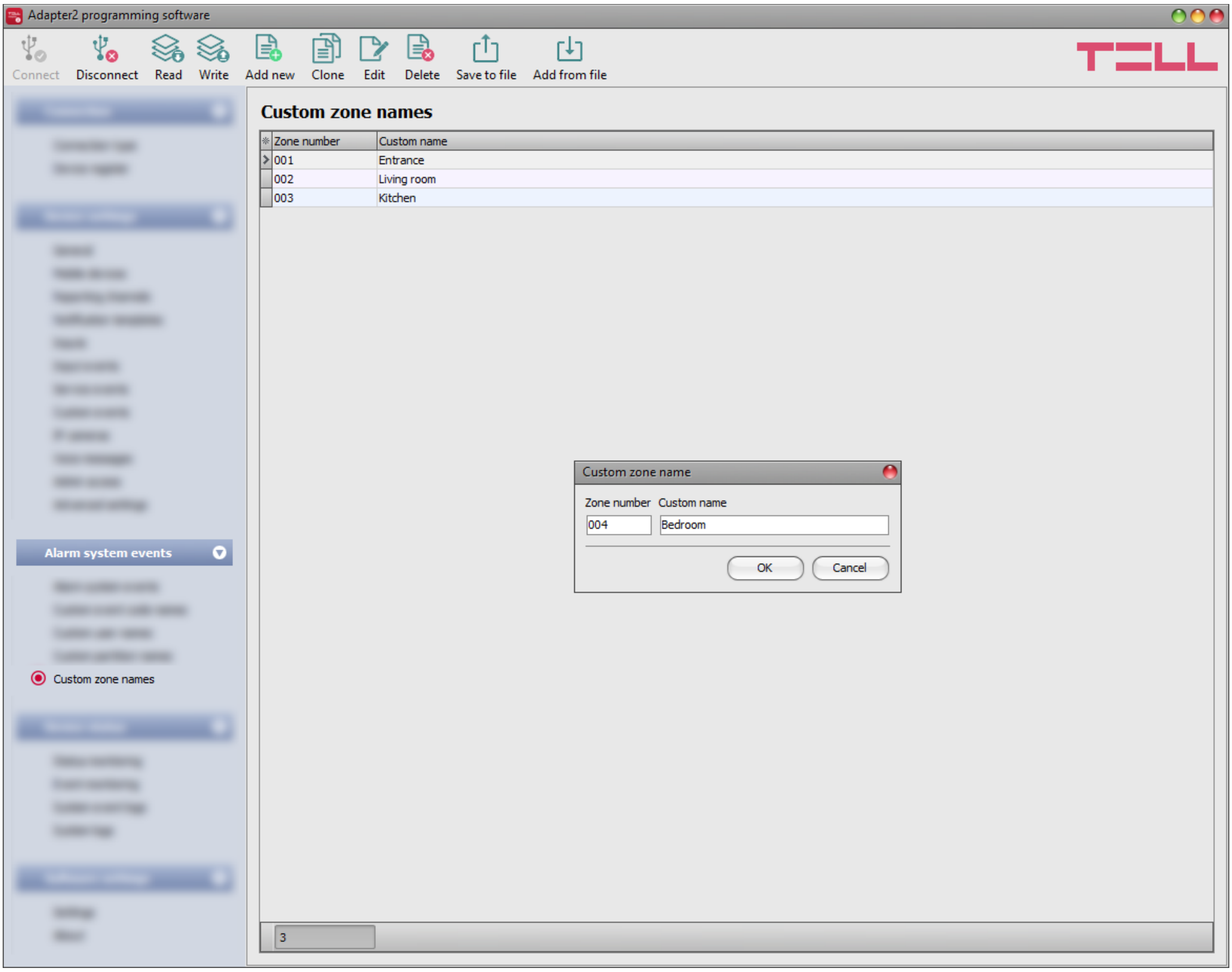
Error (red background color): entries with errors, which the program cannot process.

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

You can find a summary line at the bottom of the list, showing 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 list of custom partition names. After that, you can edit and continue to configure the entries imported into the program as needed, and when finished, write the settings into the device by clicking on the "***Write***" button.

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

4.3.5 Custom zone names



Custom zone names

Zone number	Custom name
001	Entrance
002	Living room
003	Kitchen

3

Custom zone name

Zone number: 004
Custom name: Bedroom

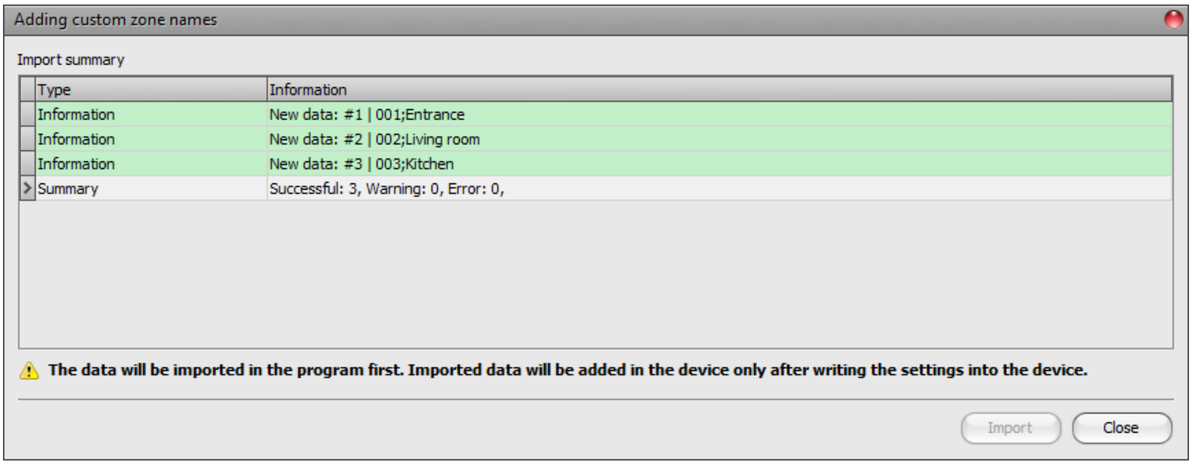
In the “***Custom zone names***” menu you can associate names with zones configured in the alarm control panel, by the zone number. The device can use the custom zone names configured here in text-notifications (SMS, Push, e-mail). The ***$cz*** variable written in the text of the message will be replaced by the device automatically with the zone name associated with the zone number received from the alarm control panel, when the device reports a zone related event. This will result in the message being received with the specific name of the zone instead of the raw zone number.

If a custom zone name has not been configured for the given zone number, the device will replace the variable with the zone number in the message. (e.g.: 001).

The system can store up to **100** custom zone names.

Available options:

- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the "***Write***" button. This will write the changes only, but all changes made in any menu.
- Adding a new custom zone name:
  To add a new custom zone name, click on the "***New***" button.
- Creating a copy of an existing custom zone name:
  To create a copy of the selected custom zone name, click on the "***Clone***" button. Please note that the new copy should have a different unique zone number.
- Editing a custom zone name:
  To edit the selected custom zone name, click on the "***Edit***" button.
- Deleting a custom zone name:
  To delete the selected custom zone name, click on the "***Delete***" button.
- Saving the custom zone names database to file:
  To save the custom zone names to file in csv format, click on the "***Save to file***" button.
- Adding custom zone names from file:
  It is possible to add custom zone names from a csv file prepared in advance. To add custom zone names from file, click on the "***Add from file***" button, browse the file, and then click on the "***Import***" button. By this, the program will read the entries from the selected file and will prepare an import summary. If there are already custom zone names stored in the device, those will not be deleted by adding entries from file, but the imported zone names will be added to the existing ones.



Import summary

Type	Information
Information	New data: #1 | 001;Entrance
Information	New data: #2 | 002;Living room
Information	New data: #3 | 003;Kitchen
Summary	Successful: 3, Warning: 0, Error: 0,

⚠ **The data will be imported in the program first. Imported data will be added in the device only after writing the settings into the device.**

The structure requirements of the CSV file to be imported:

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 entries starting from the second line. The line should start with the 3-digit zone number, followed by a semicolon, and then the zone name. Example:

```
001;Entrance
002;Living room
```

The easiest way to prepare the file is adding at least one custom zone name in the program, and then export it to csv file using the "***Save to file***" button, and then edit the exported file and enter the further custom zone names in the file by the analogy of the file content.

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

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

Information (green background color): entries imported successfully.

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

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

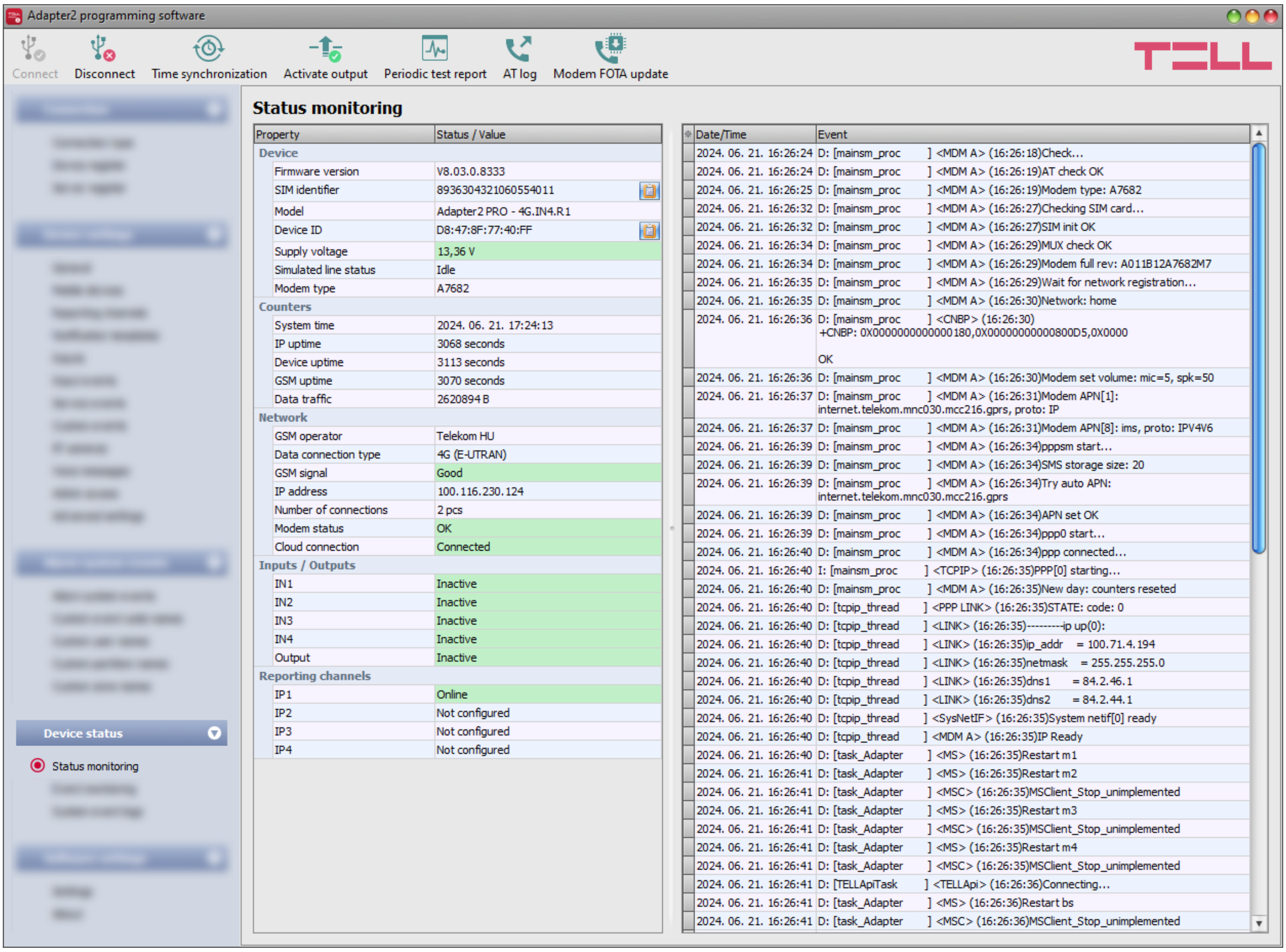
The program will not import entries marked as "*Warning*" or "*Error*" into the system!

You can find a summary line at the bottom of the list, showing 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 list of custom zone names. After that, you can edit and continue to configure the entries imported into the program as needed, and when finished, write the settings into the device by clicking on the "***Write***" button.

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

4.4 Device status menu

4.4.1 Status monitoring



Status monitoring

Property	Status / Value
Device	
Firmware version	V8.03.0.8333
SIM identifier	8936304321060554011
Model	Adapter2 PRO - 4G.IN4.R1
Device ID	D8:47:8F:77:40:FF
Supply voltage	13,36 V
Simulated line status	Idle
Modem type	A7682
Counters	
System time	2024. 06. 21. 17:24:13
IP uptime	3068 seconds
Device uptime	3113 seconds
GSM uptime	3070 seconds
Data traffic	2620894 B
Network	
GSM operator	Telekom HU
Data connection type	4G (E-UTRAN)
GSM signal	Good
IP address	100.116.230.124
Number of connections	2 pcs
Modem status	OK
Cloud connection	Connected
Inputs / Outputs	
IN1	Inactive
IN2	Inactive
IN3	Inactive
IN4	Inactive
Output	Inactive
Reporting channels	
IP1	Online
IP2	Not configured
IP3	Not configured
IP4	Not configured

```
Date/Time               Event
2024. 06. 21. 16:26:24  D: [mainsm_proc    ] <MDM A> (16:26:18)Check...
2024. 06. 21. 16:26:24  D: [mainsm_proc    ] <MDM A> (16:26:19)AT check OK
2024. 06. 21. 16:26:25  D: [mainsm_proc    ] <MDM A> (16:26:19)Modem type: A7682
2024. 06. 21. 16:26:32  D: [mainsm_proc    ] <MDM A> (16:26:27)Checking SIM card...
2024. 06. 21. 16:26:32  D: [mainsm_proc    ] <MDM A> (16:26:27)SIM init OK
2024. 06. 21. 16:26:34  D: [mainsm_proc    ] <MDM A> (16:26:29)MUX check OK
2024. 06. 21. 16:26:34  D: [mainsm_proc    ] <MDM A> (16:26:29)Modem full rev: A011B12A7682M7
2024. 06. 21. 16:26:35  D: [mainsm_proc    ] <MDM A> (16:26:29)Wait for network registration...
2024. 06. 21. 16:26:35  D: [mainsm_proc    ] <MDM A> (16:26:30)Network: home
2024. 06. 21. 16:26:36  D: [mainsm_proc    ] <CNBP> (16:26:30)
                        +CNBP: 0X0000000000000180,0X00000000000800D5,0X0000

                        OK
2024. 06. 21. 16:26:36  D: [mainsm_proc    ] <MDM A> (16:26:30)Modem set volume: mic=5, spk=50
2024. 06. 21. 16:26:37  D: [mainsm_proc    ] <MDM A> (16:26:31)Modem APN[1]:
                        internet.telekom.mnc030.mcc216.gprs, proto: IP
2024. 06. 21. 16:26:37  D: [mainsm_proc    ] <MDM A> (16:26:31)Modem APN[8]: ims, proto: IPV4V6
2024. 06. 21. 16:26:39  D: [mainsm_proc    ] <MDM A> (16:26:34)pppsm start...
2024. 06. 21. 16:26:39  D: [mainsm_proc    ] <MDM A> (16:26:34)SMS storage size: 20
2024. 06. 21. 16:26:39  D: [mainsm_proc    ] <MDM A> (16:26:34)Try auto APN:
                        internet.telekom.mnc030.mcc216.gprs
2024. 06. 21. 16:26:39  D: [mainsm_proc    ] <MDM A> (16:26:34)APN set OK
2024. 06. 21. 16:26:39  D: [mainsm_proc    ] <MDM A> (16:26:34)ppp0 start...
2024. 06. 21. 16:26:40  D: [mainsm_proc    ] <MDM A> (16:26:34)ppp connected...
2024. 06. 21. 16:26:40  I: [mainsm_proc    ] <TCPIP> (16:26:35)PPP[0] starting...
2024. 06. 21. 16:26:40  D: [mainsm_proc    ] <MDM A> (16:26:35)New day: counters reseted
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <PPP LINK> (16:26:35)STATE: code: 0
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <LINK> (16:26:35)---------ip up(0):
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <LINK> (16:26:35)ip_addr    = 100.71.4.194
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <LINK> (16:26:35)netmask    = 255.255.255.0
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <LINK> (16:26:35)dns1       = 84.2.46.1
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <LINK> (16:26:35)dns2       = 84.2.44.1
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <SysNetIF> (16:26:35)System netif[0] ready
2024. 06. 21. 16:26:40  D: [tcpip_thread   ] <MDM A> (16:26:35)IP Ready
2024. 06. 21. 16:26:40  D: [task_Adapter   ] <MS> (16:26:35)Restart m1
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MS> (16:26:35)Restart m2
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MSC> (16:26:35)MSClient_Stop_unimplemented
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MS> (16:26:35)Restart m3
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MSC> (16:26:35)MSClient_Stop_unimplemented
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MS> (16:26:35)Restart m4
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MSC> (16:26:35)MSClient_Stop_unimplemented
2024. 06. 21. 16:26:41  D: [TELLApiTask    ] <TELLApi> (16:26:36)Connecting...
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MS> (16:26:36)Restart bs
2024. 06. 21. 16:26:41  D: [task_Adapter   ] <MSC> (16:26:36)MSClient_Stop_unimplemented
```

The "***Status monitoring***" menu provides information on actual system status. Please note that for faster communication, in case of remote connection some of the options are not available. Status information loads and refreshes automatically only when connected through USB. The system logs are shown in the window on the right hand side, which provides information about the internal processes of the device and communication. The system logs help troubleshooting if malfunction occurs. The program saves the system logs to file automatically in the "***Logs***" folder, which you can access easily by clicking on the path link shown in the "***About***" menu in the "***Data folder***" section (the file name looks as follows: "*the actual date*_module.log"). **The system logs are only available when connected via USB!**

Available status information:

Device:

- **Firmware version**: the firmware version of the device.
- **SIM identifier**: the identifier (ICCID) of the SIM card installed in the device. You can copy the ID to clipboard by clicking the notepad icon on the right-hand side.
- **Model:** the device type/model.
- **Device ID:** the unique identifier of the device (6x2 hexadecimal characters). This identifier is burned-in during production and thereby it is unchangeable. You can copy the ID to clipboard by clicking the notepad icon on the right-hand side.

- **Supply voltage**: value of measured supply voltage. The value is considered to be no more than indicative, and cannot be compared with a value shown by a precise measuring instrument.
- **Simulated line status**: the status of the simulated phone line.
- **Modem type**: the type of the modem built in the device.

Counters:

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

Network:

- **GSM operator**: the name of the mobile operator currently used.
- **Data connection type**: the current data connection type:
  4G (E-UTRAN), 2G (GPRS/EGDE).
- **GSM signal**: actual GSM signal level (None/Very low, Weak, Medium, Good, Excellent).
- **IP address**: the actual IP address of the device.
- **Number of connections**: the number of active connections with servers/receivers.
- **Modem status**: the actual status of the GSM modem.
- **Cloud connection**: the cloud connection status.

Inputs / Outputs:

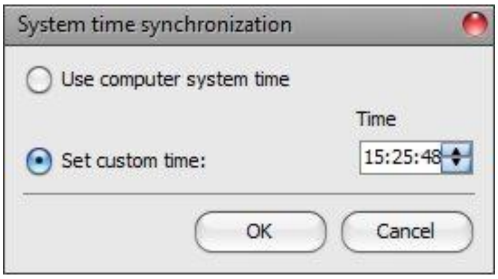
- **IN1…IN4**: the actual state of the contact inputs.
- **Output**: the actual state of the output (OUT)

Reporting channels:

- **IP1…IP4**: connection status of the configured servers and IP receivers

After connecting to the device locally or remotely, the following options become available:

- **Query**:
  This button is only available when connected to the device remotely. Status information can be loaded or updated by clicking on this button. This is not needed when connected via USB, because in this case status information loads and refreshes automatically.
- **Time synchronization**:
  This button is used to synchronize the device system time with the PC system time, or set custom time, according to your choice.



System time synchronization

○ Use computer system time

● Set custom time: Time 15:25:48

- **Activate output**:

  You can activate the output (OUT) by clicking on this button. The output remains activated until deactivated manually or by an event, which has been configured to control the given output in a way that deactivates it, or a power loss occurs.

- **Deactivate output**:

  You can deactivate the output (OUT) by clicking on this button.

- **Periodic test report:**

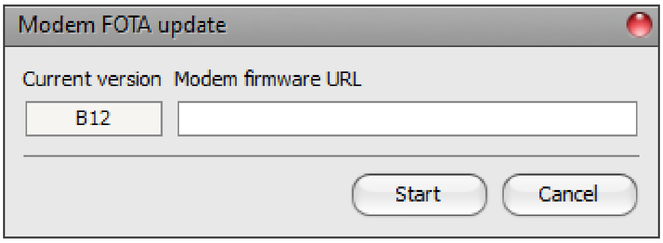
  You can generate a periodic test report event by clicking on this button.

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

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

- **Modem FOTA update:**

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



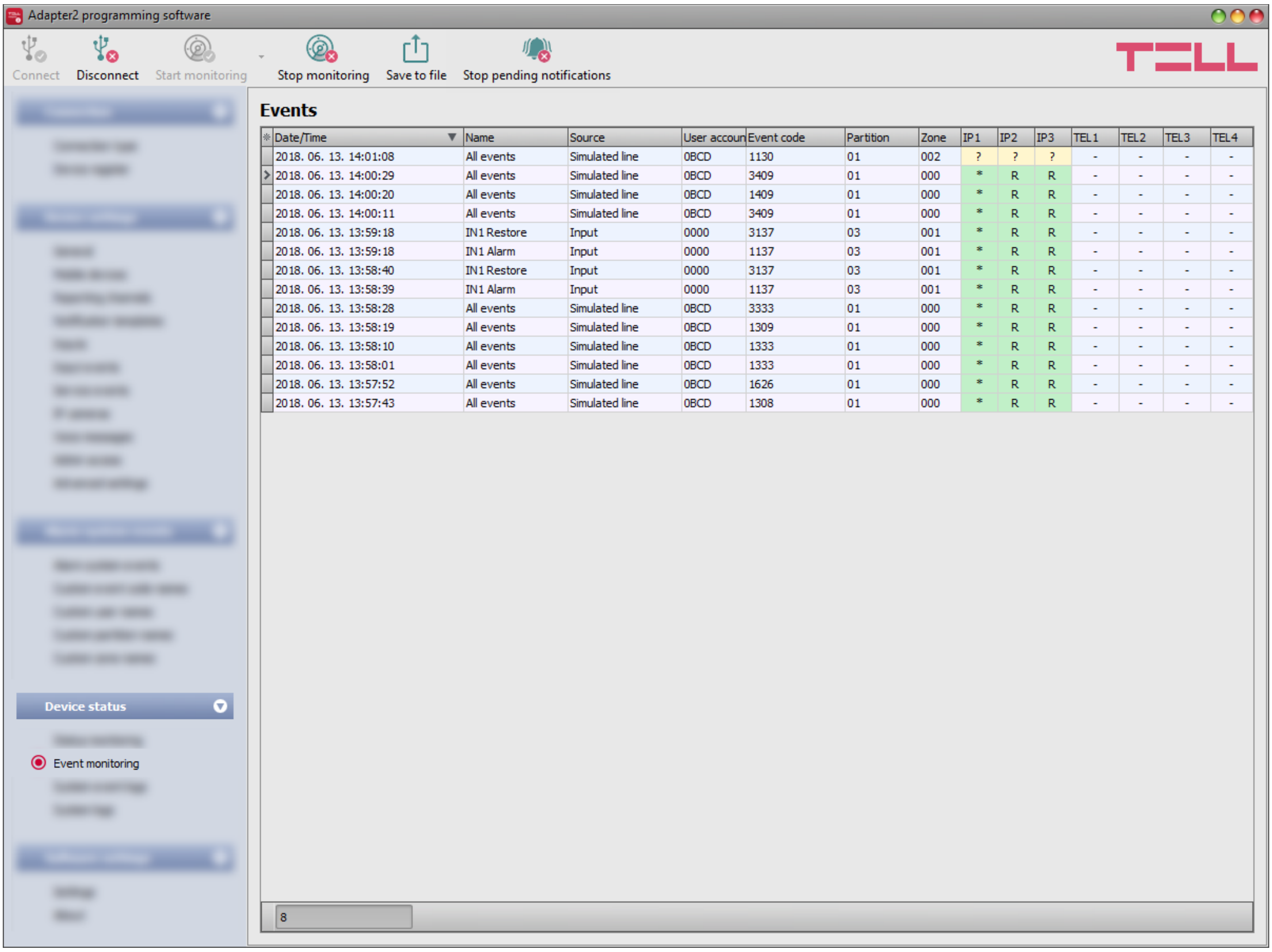
Modem FOTA update

Current version: B12

Modem firmware URL:

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

4.4.2 Event monitoring



Events

Date/Time	Name	Source	User accoun	Event code	Partition	Zone	IP1	IP2	IP3	TEL1	TEL2	TEL3	TEL4
2018. 06. 13. 14:01:08	All events	Simulated line	0BCD	1130	01	002	?	?	?	-	-	-	-
2018. 06. 13. 14:00:29	All events	Simulated line	0BCD	3409	01	000	*	R	R	-	-	-	-
2018. 06. 13. 14:00:20	All events	Simulated line	0BCD	1409	01	000	*	R	R	-	-	-	-
2018. 06. 13. 14:00:11	All events	Simulated line	0BCD	3409	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:59:18	IN1 Restore	Input	0000	3137	03	001	*	R	R	-	-	-	-
2018. 06. 13. 13:59:18	IN1 Alarm	Input	0000	1137	03	001	*	R	R	-	-	-	-
2018. 06. 13. 13:58:40	IN1 Restore	Input	0000	3137	03	001	*	R	R	-	-	-	-
2018. 06. 13. 13:58:39	IN1 Alarm	Input	0000	1137	03	001	*	R	R	-	-	-	-
2018. 06. 13. 13:58:28	All events	Simulated line	0BCD	3333	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:58:19	All events	Simulated line	0BCD	1309	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:58:10	All events	Simulated line	0BCD	1333	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:58:01	All events	Simulated line	0BCD	1333	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:57:52	All events	Simulated line	0BCD	1626	01	000	*	R	R	-	-	-	-
2018. 06. 13. 13:57:43	All events	Simulated line	0BCD	1308	01	000	*	R	R	-	-	-	-

In this menu you can view the device's event log and monitor events and the reporting progress online. The device stores last 100 events in its event log.

Available options:

- **Start monitoring**:
  By clicking on this button, the program will download the stored and will display new events as well. By clicking on the arrow next to this button, you can choose from the drop-down menu, how many events you want to see in the list: last 10, 20 or all.

- **Stop monitoring**:
  Suspends listing of new events. New events will not be listed until event monitoring is restarted.

- **Save to file**:
  By clicking on this button, the listed event log can be saved to file in semicolon-separated CSV format.

- **Stop pending notifications**:
  By clicking on this button, a command will be sent to the device to cancel pending notifications, which have not been delivered yet. Notifications already in progress will not be terminated.

When connected to the device remotely, the event log can be downloaded only, online monitoring is not available.

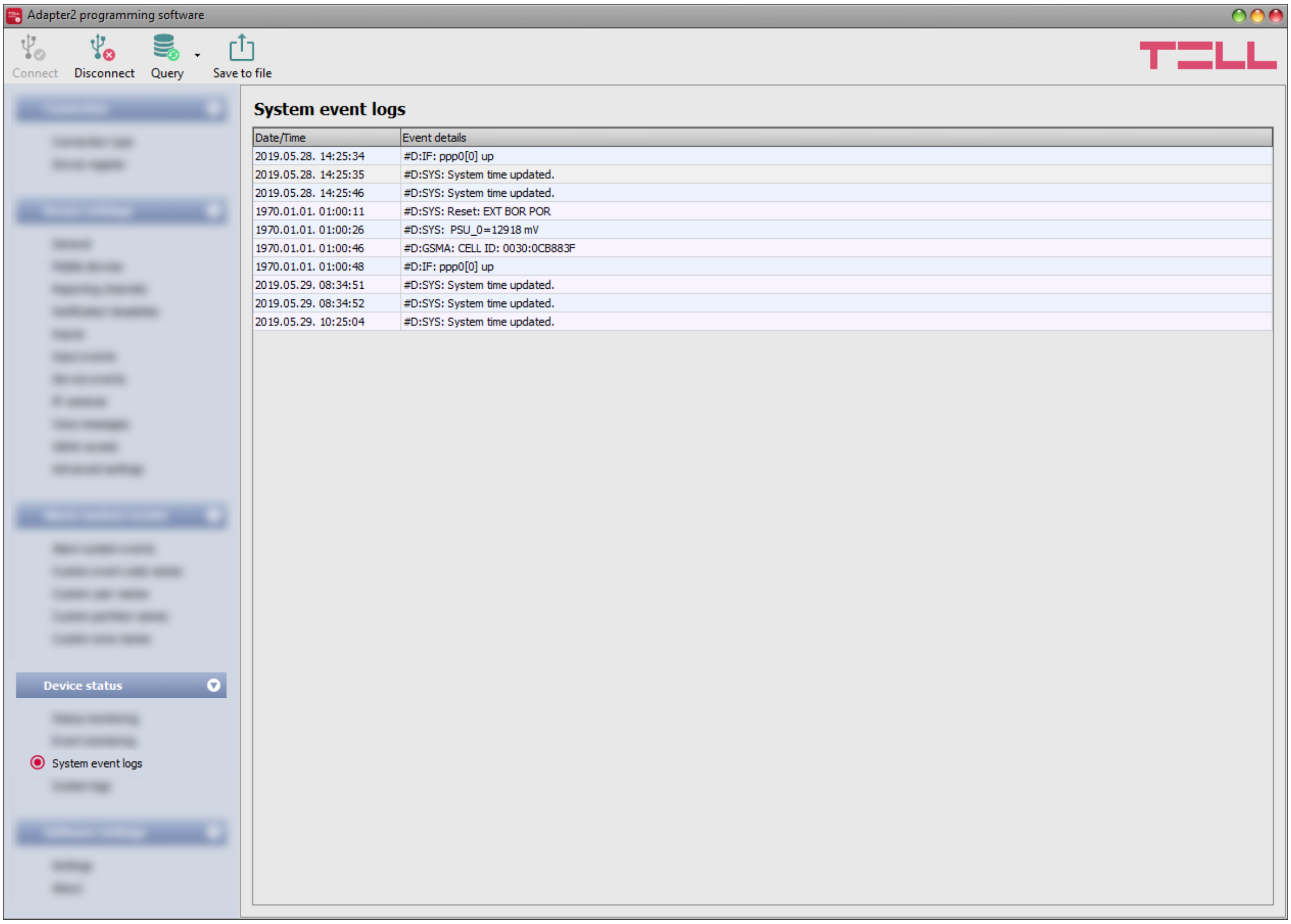
Elements of the event log:

- **Date/time**: event date/time.
- **Name**: event name, according to the event names configured at alarm system events, input events and service events.
- **Source**: event source.
- **User account ID**: the user account ID according to the source.
- **Event code**: Contact ID event code.
- **Partition**: partition number.
- **Zone**: zone number.
- **IP1**…**IP4**: reporting to IP1…IP4 server/receiver IP addresses.
- **Backup SMS**: backup reporting to CMS via SMS.
- **TEL1**…**TEL4 (SMS)**: notifications to phone numbers TEL1…TEL4 by SMS.
- **TEL1**…**TEL4 (Call)**: notifications to phone numbers TEL1…TEL4 by voice call
- **PUSH1**…**PUSH4**: notifications to mobile devices 1…4 by Push notification.
- **EMAIL1**…**EMAIL4**: notifications to addressees 1…4 by e-mail.

Legend of marks shown in IP1…IP4, Backup SMS, TEL1…TEL4 (SMS). TEL1…TEL4 (Call), PUSH1…PUSH4 and EMAIL1…EMAIL4 columns:

? – new event reporting in progress.
R – no need to report.
***** – reported successfully.
E – reporting failed.
- – no server/receiver IP address or phone number configured.

4.4.3 System event logs



System event logs

Date/Time	Event details
2019.05.28. 14:25:34	#D:IF: ppp0[0] up
2019.05.28. 14:25:35	#D:SYS: System time updated.
2019.05.28. 14:25:46	#D:SYS: System time updated.
1970.01.01. 01:00:11	#D:SYS: Reset: EXT BOR POR
1970.01.01. 01:00:26	#D:SYS: PSU_0=12918 mV
1970.01.01. 01:00:46	#D:GSMA: CELL ID: 0030:0CB883F
1970.01.01. 01:00:48	#D:IF: ppp0[0] up
2019.05.29. 08:34:51	#D:SYS: System time updated.
2019.05.29. 08:34:52	#D:SYS: System time updated.
2019.05.29. 10:25:04	#D:SYS: System time updated.

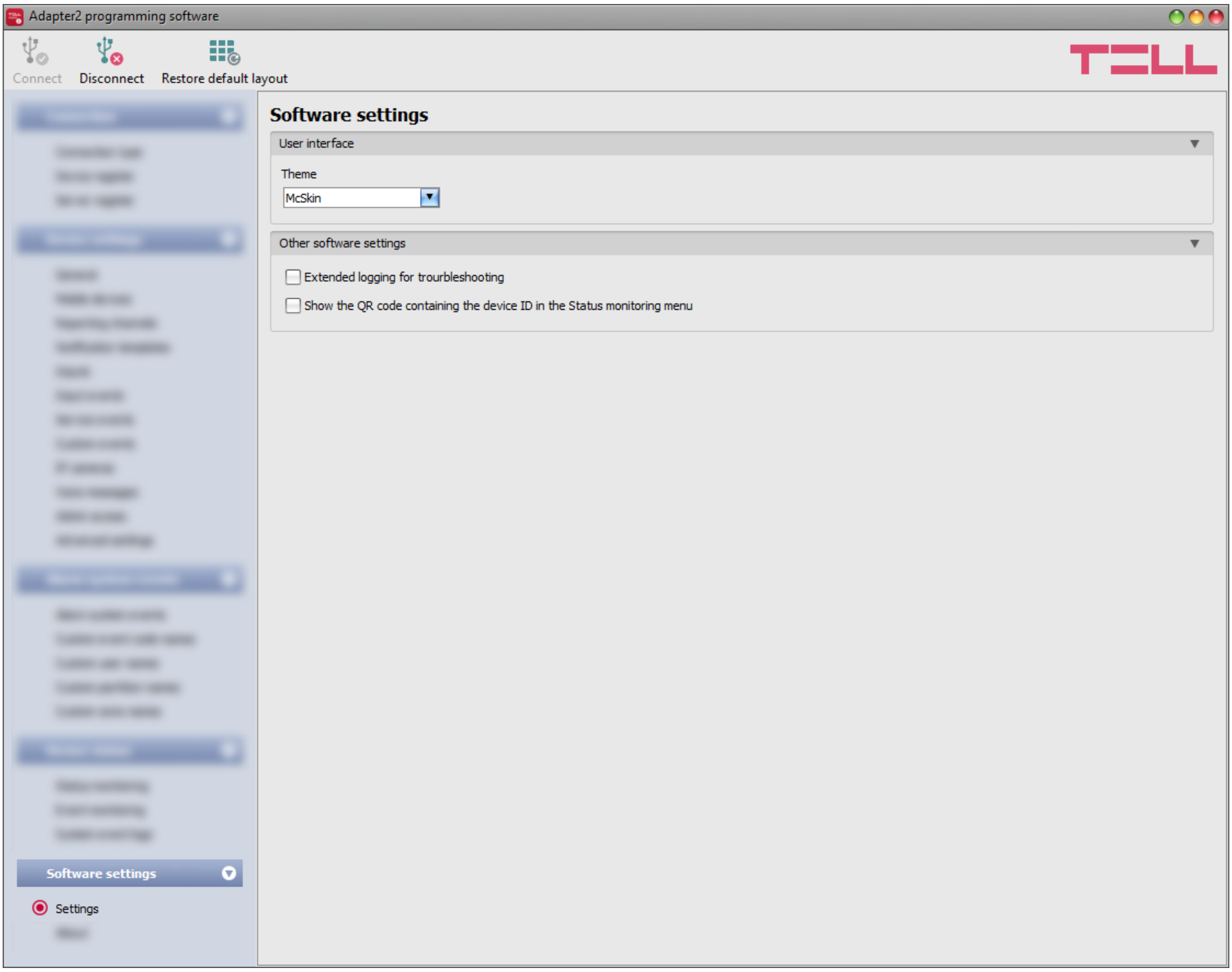
Events related to device operation are shown in the system event logs.

To download the system event logs from the device, open the “**Read**” drop-down menu, select how many events you want to download from the latest ones (10, 20 or all), and then click on the “**Read**” button.

You can save the downloaded system event logs to file in CSV format. To save the logs to file, click on the “***Save to file***” button.

4.5 Software settings menu

4.5.1 Settings



Software settings

User interface

Theme: McSkin

Other software settings

☐ Extended logging for tourbleshooting

☐ Show the QR code containing the device ID in the Status monitoring menu

In the “***Settings***” menu you can change the user interface skin and language.

Available options:

- **Restore default layout**:
  To restore the user interface default layout, click on the “***Restore default layout***” button.

User interface:

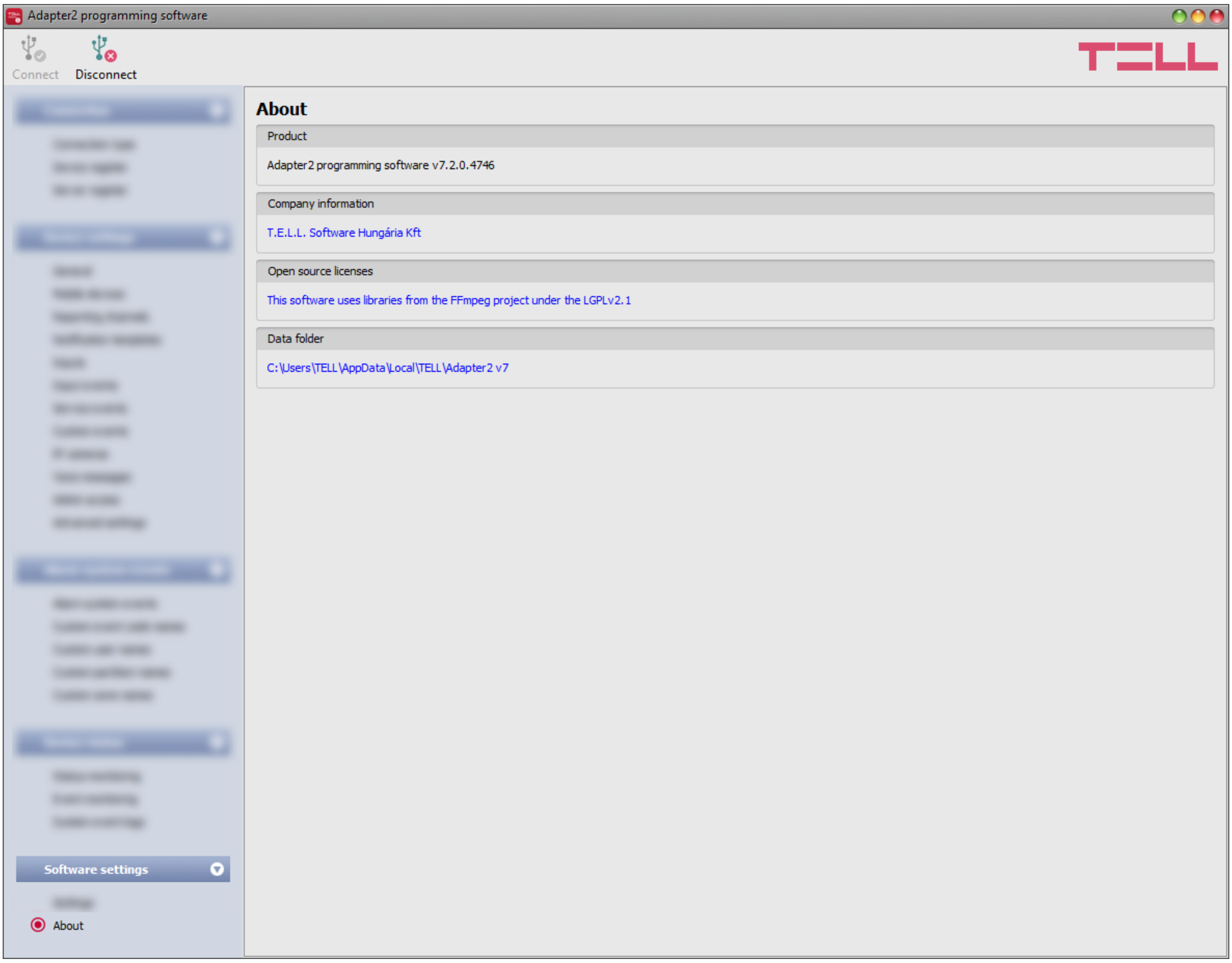
Theme: the user interface appearance can be changed using this dropdown-menu. You can choose from various appearance themes.

Other software settings:

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

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

4.5.2 About



About

Product

Adapter2 programming software v7.2.0.4746

Company information

T.E.L.L. Software Hungária Kft

Open source licenses

This software uses libraries from the FFmpeg project under the LGPLv2.1

Data folder

C:\Users\TELL\AppData\Local\TELL\Adapter2 v7

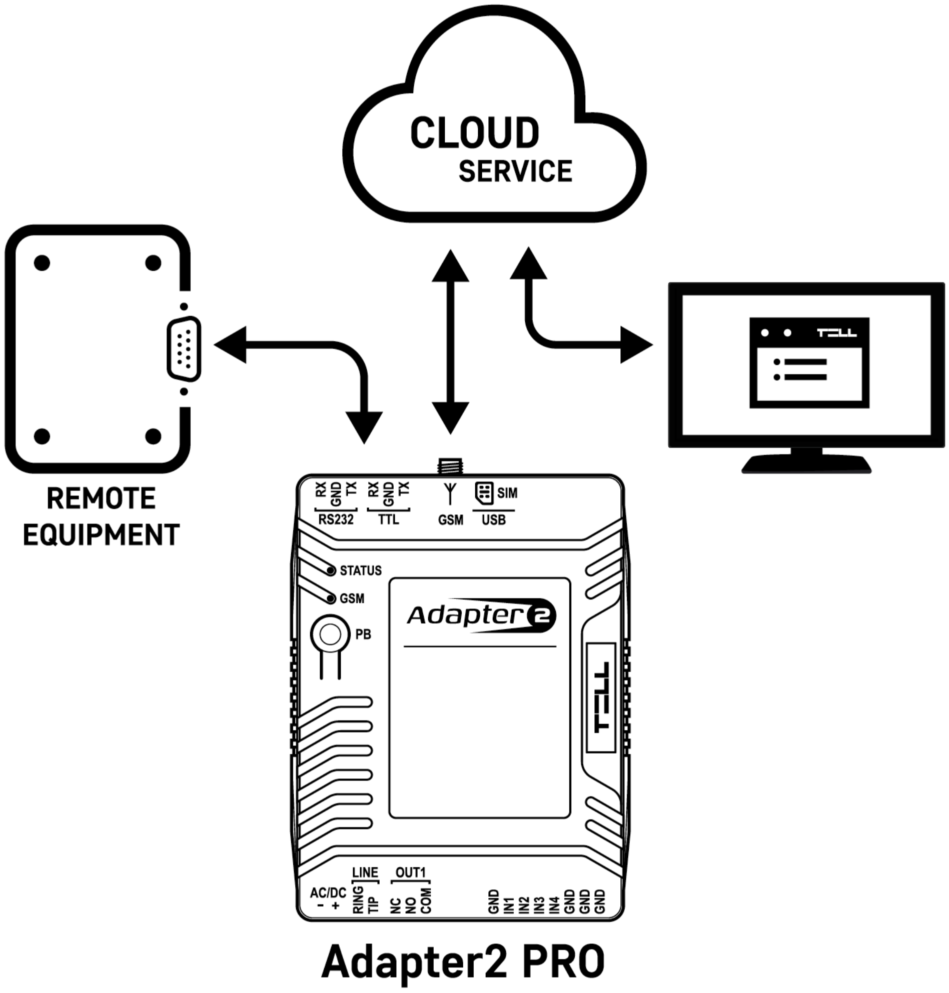
The "***About***" menu shows the availabilities of the manufacturer, the version of the programming software and the path of the data folder where the software stores the logs. By clicking on the path, the program will open the data folder in the file manager.

5 Transparent serial port

The serial port of the product has an **RS232** and a **TTL** output connected in parallel. As the two port types are connected to a common serial port inside the device, only one of them can be used at a time. Choose the port type that is compatible with the equipment to be connected.
The serial port of the device is suitable for bidirectional transparent data transfer over the Internet. It can be used for e.g., remote programming of the connected alarm control panel or can provide a solution for remote communication of other devices or equipment which are using an RS232 or a TTL serial port. The Internet connection between the remote device or equipment and the computer is ensured by the ***Adapter2 PRO*** and the ***Remote Serial Client*** software, or the ***Adapter2*** programming software. For this, the chosen serial port of the ***Adapter2 PRO*** should be connected to the serial port of the given device or equipment, and then data can be sent to and received from the device or equipment on the PC through the virtual serial port created by the ***Remote Serial Client*** software.

In case of using the ***Adapter2*** programming software, the remote data connection can be established using the ***Link remote serial port*** button placed in the ***General*** settings menu. This option also requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com), which provides the serial link between the programming software and the application you want to use.

The ***Remote Serial Client*** and the ***Adapter2*** programming software can both be used to connect to the serial port of the device, with the difference that the ***Remote Serial Client*** program can create a virtual port for communication, while the programming software requires third-party software that can create a linked pair of virtual serial ports.



5.1 Remote programming of alarm control panels

For remote programming, the device establishes transparent serial data communication through IP connection. To establish the remote connection between the programming software of the alarm system and the alarm control panel, you can use the ***Remote Serial Client*** or the ***Adapter2*** programming software. The chosen serial port of the ***Adapter2 PRO*** must be connected to the serial port of the alarm control panel, and the programming software of the alarm system connects to the virtual serial port created by the ***Remote Serial Client*** software.
In case of using the ***Adapter2*** programming software, the remote data connection can be established using the ***Link remote serial port*** button placed in the ***General*** settings menu. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com), which provides the serial link between the ***Adapter2*** programming software and the programming software of the alarm control panel.

Attention! The transparent serial data transfer works through the cloud service only. Therefore, to use this function, it is necessary for the device to be connected to the cloud server.

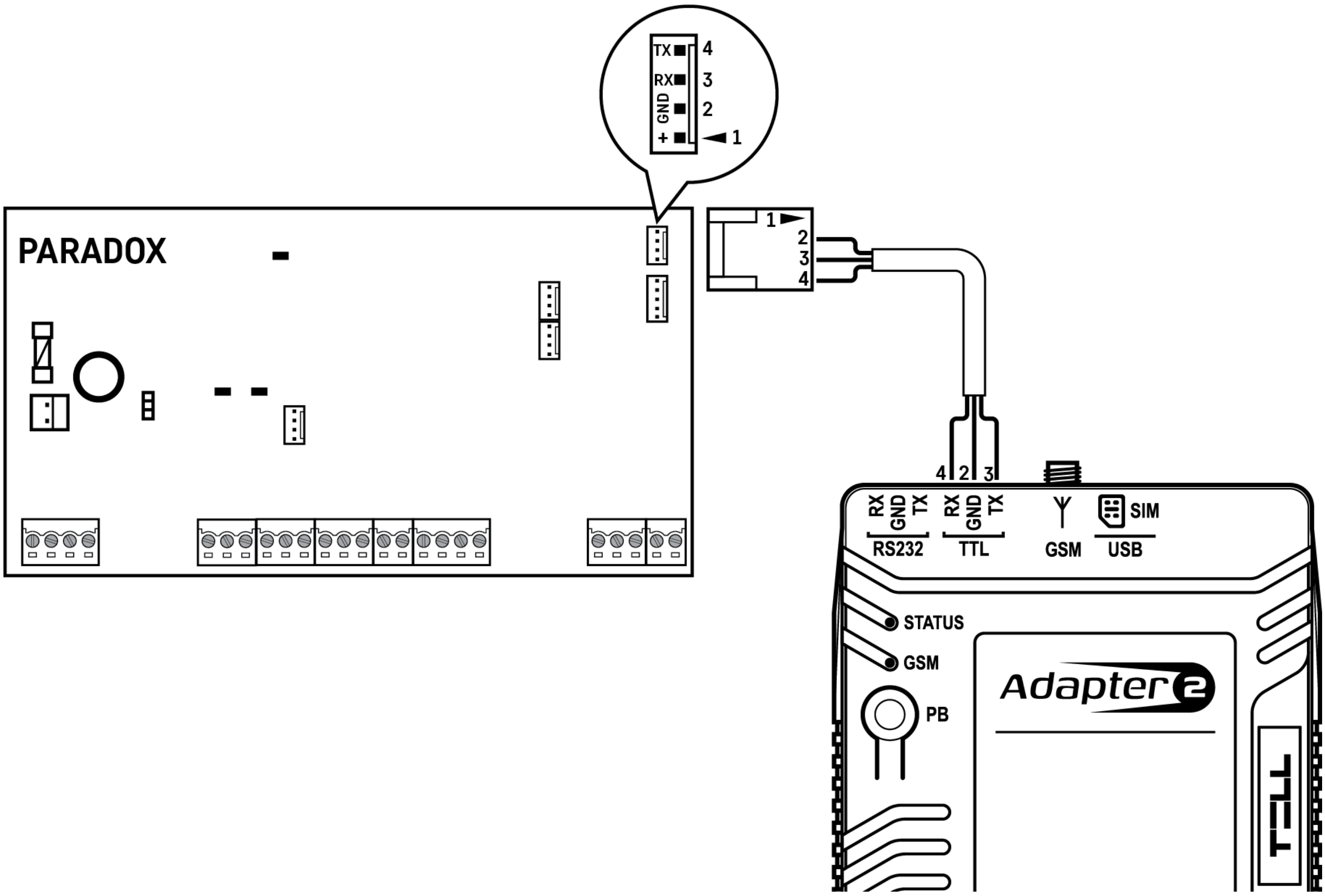
Attention! Please note that data transfer through the serial port of the *Adapter2* may generate high data traffic, which may result in an increased data usage on the SIM card installed in the device.

Remote programming was tested with the following alarm control panels:

• Paradox	EVO192, SP5500, SP4000
• DSC	NEO HS2016, PC1616
• Texecom	Premier, Premier Elite
• Bentel	KYO 8
• Inim	Ability, Smart Living
• Satel	CA-10

5.1.1 Paradox alarm systems

- **Installation:**



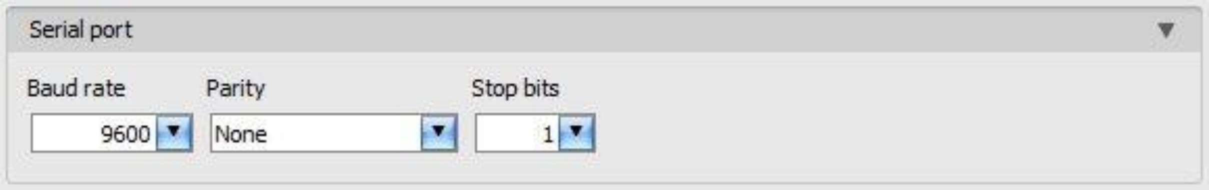
Wiring diagram for Paradox alarm systems

For connecting Paradox alarm control panels, a cable with a special plug is needed, which is available under the name **E-Shift-PAR cable** in TELL's product range. Connect the bare wire end of the cable to the **TTL** port of the **Adapter2 PRO** as shown in the figure above, then connect the other end with the plug onto the alarm control panel.

- **Software settings:**

Configure the serial port settings in the “***Serial port***” section of the “***General***” menu, in the ***Adapter2*** programming software, as shown in the figure below.

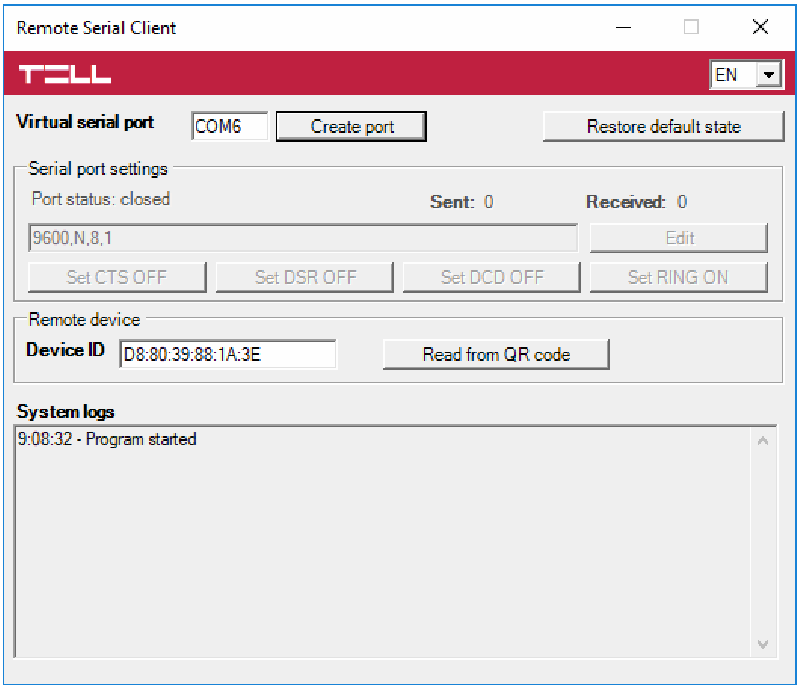
For Spectra alarm control panels:	Baud rate=9600, Parity=None, Stopbits=1
For EVO alarm control panels:	Baud rate=57600, Parity=None, Stopbits=1



Serial port

Baud rate: 9600
Parity: None
Stop bits: 1

To establish the connection between the alarm control panel and its programming software, it is necessary to install the ***Remote Serial Client*** software. This client software ensures the connection between the PC and the ***Adapter2 PRO*** device, as well as it creates a virtual serial port for the programming software of the alarm system.
As an alternative, the remote data connection can also be established using the ***Link remote serial port*** button placed in the ***General*** settings menu in the ***Adapter2*** programming software. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com).



Remote Serial Client

Virtual serial port: COM6

Serial port settings
Port status: closed
Sent: 0
Received: 0
9600,N,8,1

Remote device
Device ID: D8:80:39:88:1A:3E

System logs
9:08:32 - Program started

Open the ***Remote Serial Client*** software and configure the settings in the order below:

Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***Adapter2 PRO*** device connected to the alarm control panel.
Using the “***Read from QR code***” button, you can also read the device ID from the image file saved from the programming software, that contains the QR code with the device ID.

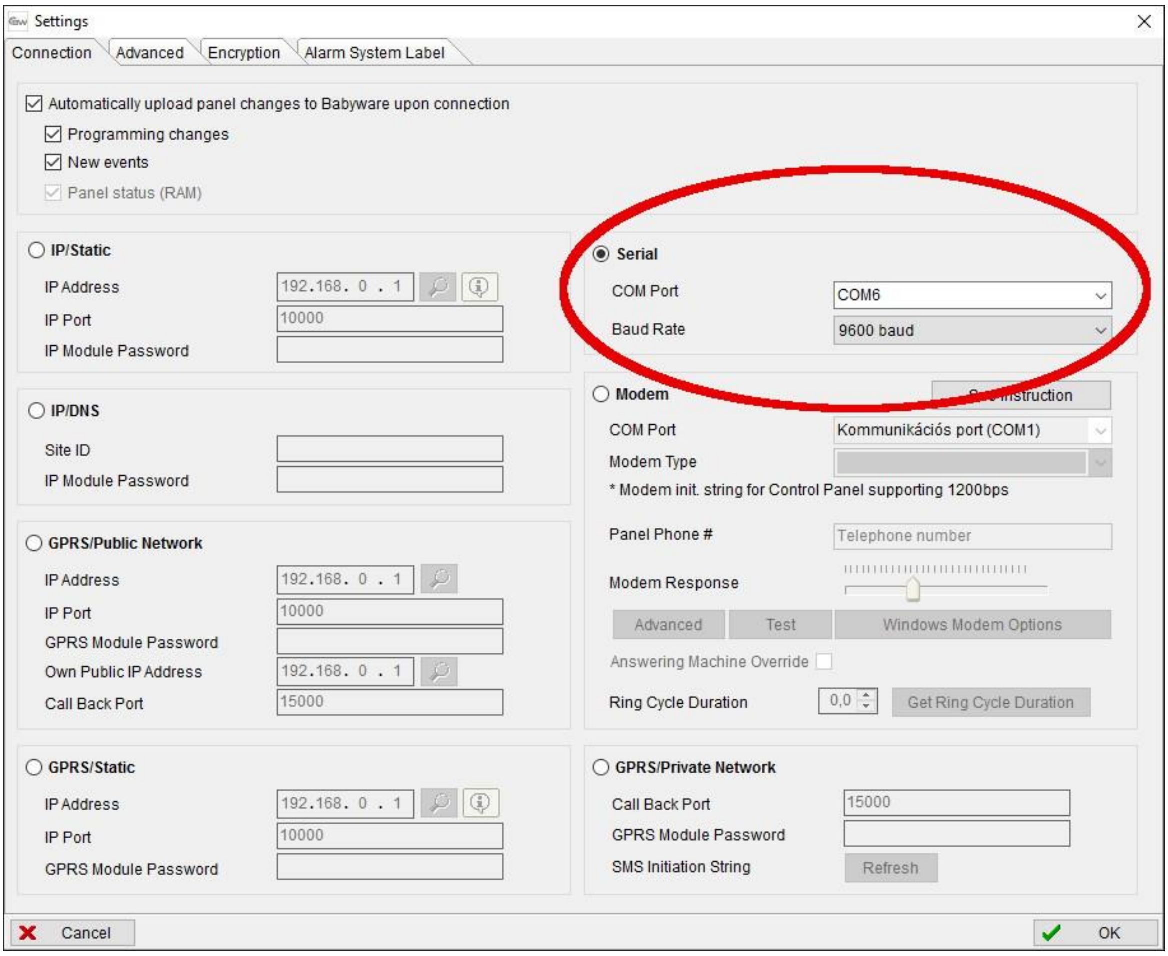
Virtual serial port: enter the number of the virtual port you wish to create (e.g.: COM6).

System logs: shows information about program operation and displays data received through the serial port.

Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***Adapter2 PRO*** device should be online to create the virtual serial port.

Example for selecting the serial communication port in the ***Babyware*** programming software:

For Spectra alarm control panels: Baud rate=9600 baud
For EVO alarm control panels: Baud rate=57600 baud



Settings

Connection | Advanced | Encryption | Alarm System Label

☑ Automatically upload panel changes to Babyware upon connection
☑ Programming changes
☑ New events
☑ Panel status (RAM)

○ IP/Static
IP Address: 192.168. 0 . 1
IP Port: 10000
IP Module Password:

● Serial
COM Port: COM6
Baud Rate: 9600 baud

○ Modem
COM Port: Kommunikációs port (COM1)
Modem Type:
* Modem init. string for Control Panel supporting 1200bps
Panel Phone #: Telephone number
Modem Response
Answering Machine Override □
Ring Cycle Duration: 0,0

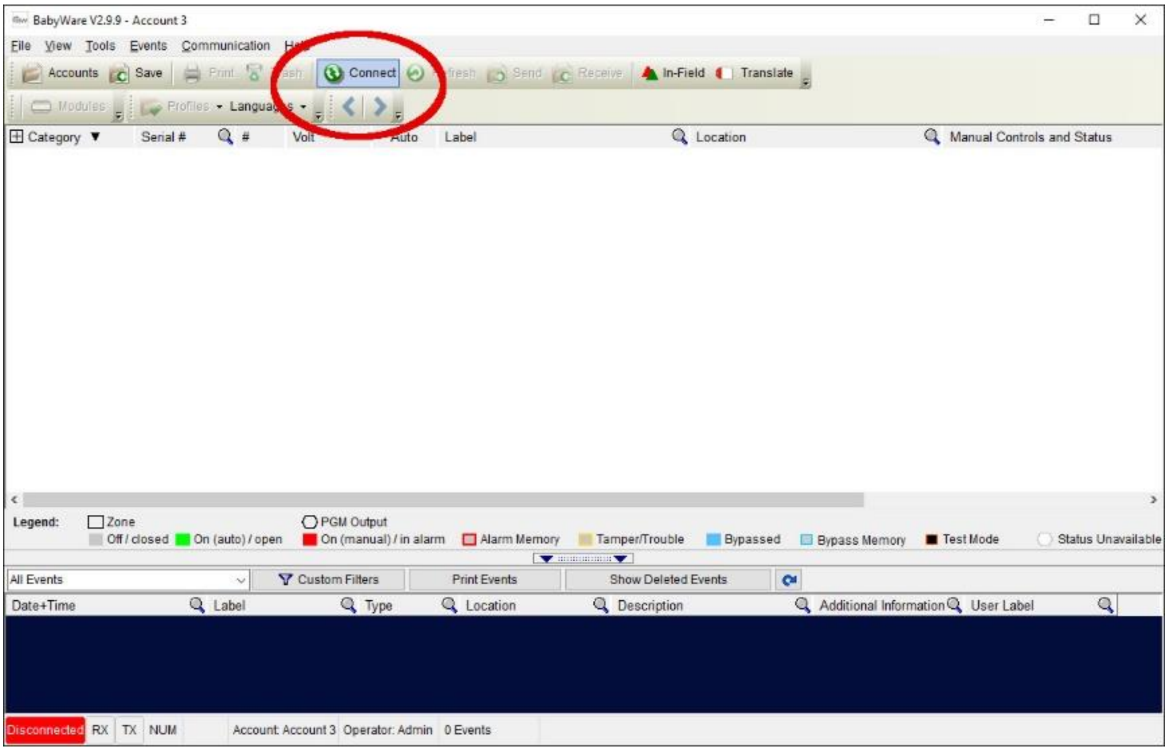
○ IP/DNS
Site ID:
IP Module Password:

○ GPRS/Public Network
IP Address: 192.168. 0 . 1
IP Port: 10000
GPRS Module Password:
Own Public IP Address: 192.168. 0 . 1
Call Back Port: 15000

○ GPRS/Static
IP Address: 192.168. 0 . 1
IP Port: 10000
GPRS Module Password:

○ GPRS/Private Network
Call Back Port: 15000
GPRS Module Password:
SMS Initiation String

Start connecting:



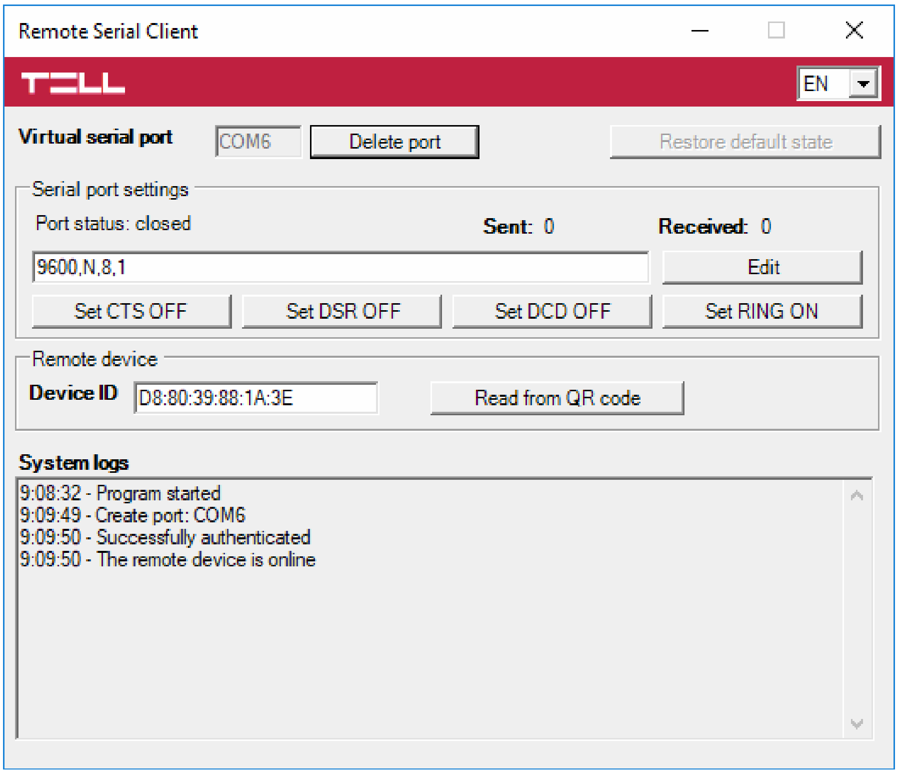
BabyWare V2.9.9 - Account 3

Legend: □ Zone, ○ PGM Output, ▨ Off / closed, 🟩 On (auto) / open, 🟥 On (manual) / in alarm, □ Alarm Memory, ▨ Tamper/Trouble, ▨ Bypassed, ▨ Bypass Memory, ■ Test Mode, ○ Status Unavailable

Disconnected | RX | TX | NUM | Account: Account 3 | Operator: Admin | 0 Events

Then the programming software will open the serial port and will establish the connection with the alarm control panel.

After you have finished remote programming the alarm control panel, you can delete the created virtual serial port by clicking on the “***Delete port***” button.

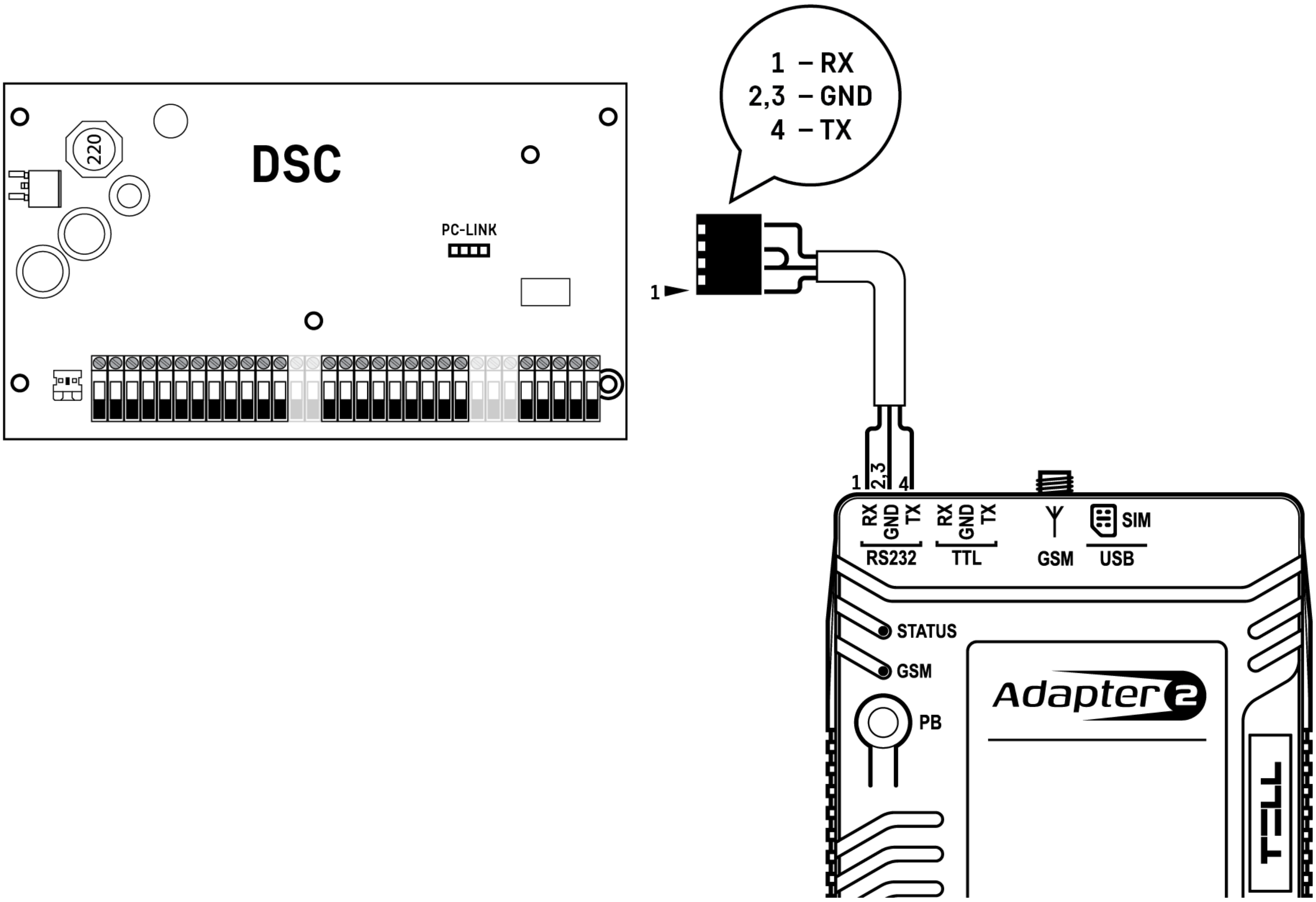


```
9:08:32 - Program started
9:09:49 - Create port: COM6
9:09:50 - Successfully authenticated
9:09:50 - The remote device is online
```

In case of using the ***Adapter2*** programming software, you can close the serial data connection using the ***Unlink remote serial port*** ⇅ button placed in the ***General*** settings menu.

5.1.2 DSC alarm systems

- **Installation:**

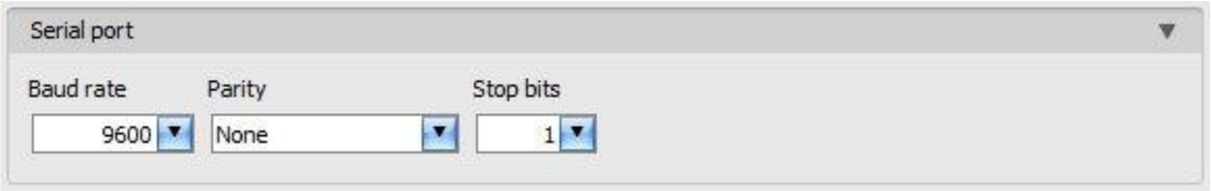


Wiring diagram for DSC alarm systems

For connecting DSC alarm control panels, a cable with a special plug is needed, which is available under the name **E-Shift-D cable** in TELL's product range. Connect the bare wire end of the cable to the **RS232** port of the **Adapter2 PRO** as shown in the figure above, then connect the other end with the plug onto the alarm control panel.

- **Software settings:**

Configure the serial port settings in the "***Serial port***" section of the "***General***" menu, in the ***Adapter2*** programming software, as shown in the figure below (Baud rate=9600, Parity=None, Stopbits=1):



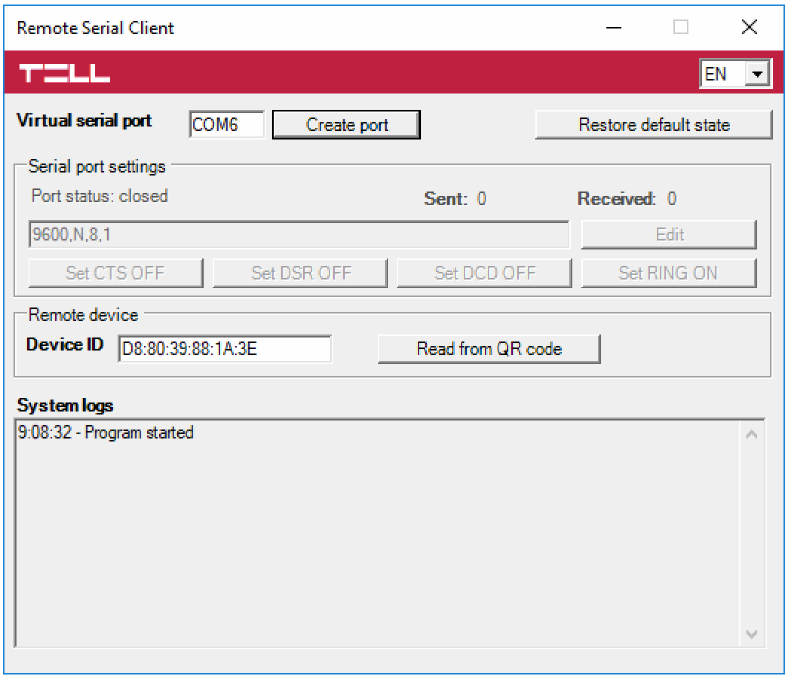
Serial port

Baud rate: 9600

Parity: None

Stop bits: 1

To establish the connection between the alarm control panel and its programming software, it is necessary to install the ***Remote Serial Client*** software. This client software ensures the connection between the PC and the ***Adapter2 PRO*** device, as well as it creates a virtual serial port for the programming software of the alarm system.
As an alternative, the remote data connection can also be established using the ***Link remote serial port*** button placed in the ***General*** settings menu in the ***Adapter2*** programming software. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com).



Remote Serial Client

Virtual serial port: COM6

Serial port settings

Port status: closed

Sent: 0

Received: 0

9600,N,8,1

Remote device

Device ID: D8:80:39:88:1A:3E

System logs

```
9:08:32 - Program started
```

Open the ***Remote Serial Client*** software and configure the settings in the order below:

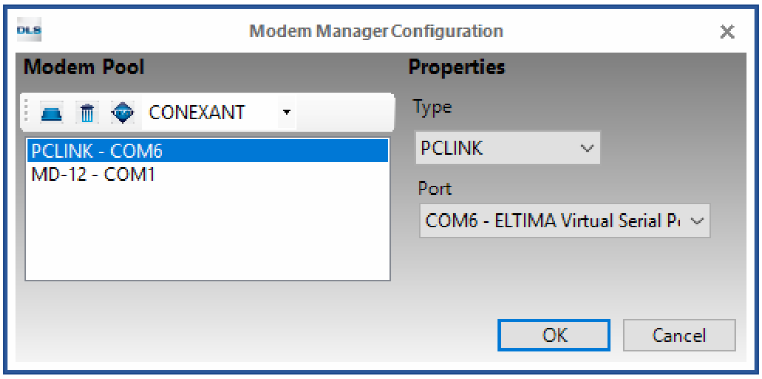
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***Adapter2 PRO*** device connected to the alarm control panel.
Using the “***Read from QR code***” button, you can also read the device ID from the image file saved from the programming software, that contains the QR code with the device ID.

Virtual serial port: enter the number of the virtual port you wish to create (e.g.: COM6).

System logs: shows information about program operation and displays data received through the serial port.

Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***Adapter2 PRO*** device should be online to create the virtual serial port.

Example for selecting the serial communication port in the ***DLS 5*** programming software:



Modem Manager Configuration

Modem Pool

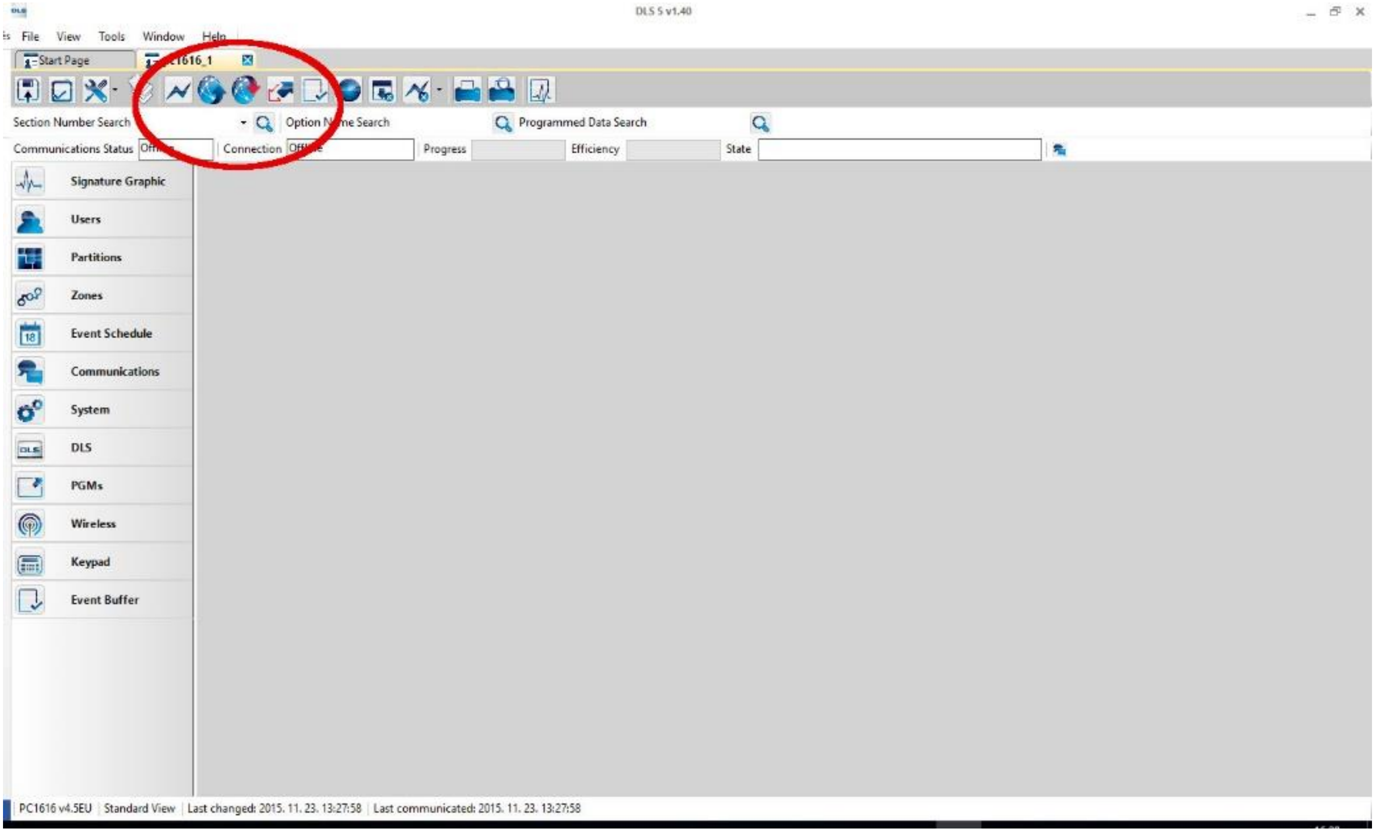
PCLINK - COM6
MD-12 - COM1

Properties

Type: PCLINK

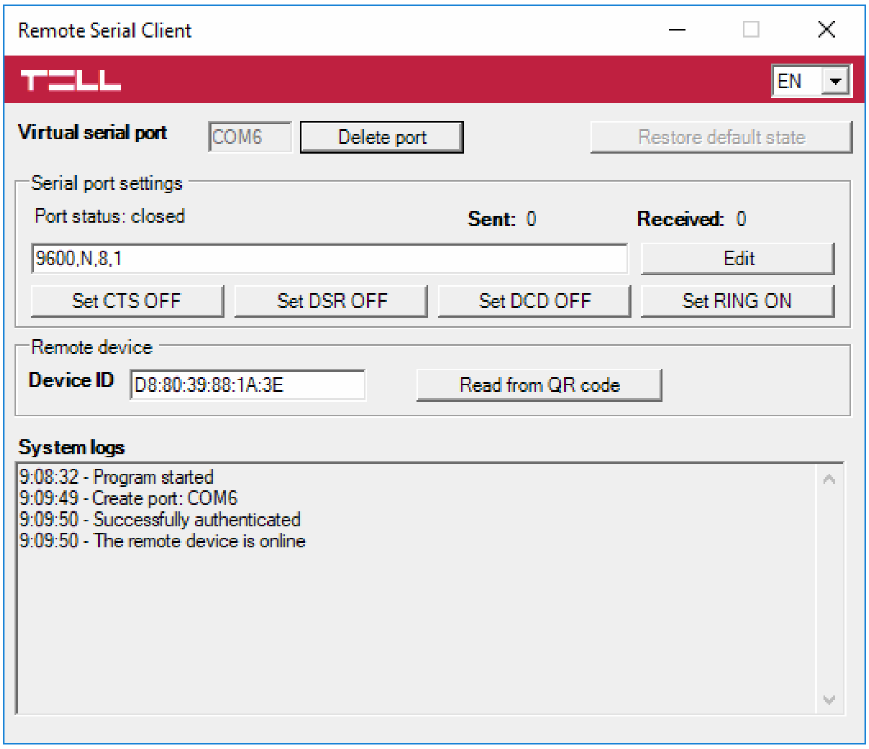
Port: COM6 - ELTIMA Virtual Serial P

Start connecting:



Then the programming software will open the serial port and will establish the connection with the alarm control panel.

After you finished remote programming the alarm control panel, you can delete the created virtual serial port by clicking on the "***Delete port***" button.



Virtual serial port COM6

Serial port settings

Port status: closed **Sent:** 0 **Received:** 0

9600,N,8,1

Remote device

Device ID D8:80:39:88:1A:3E

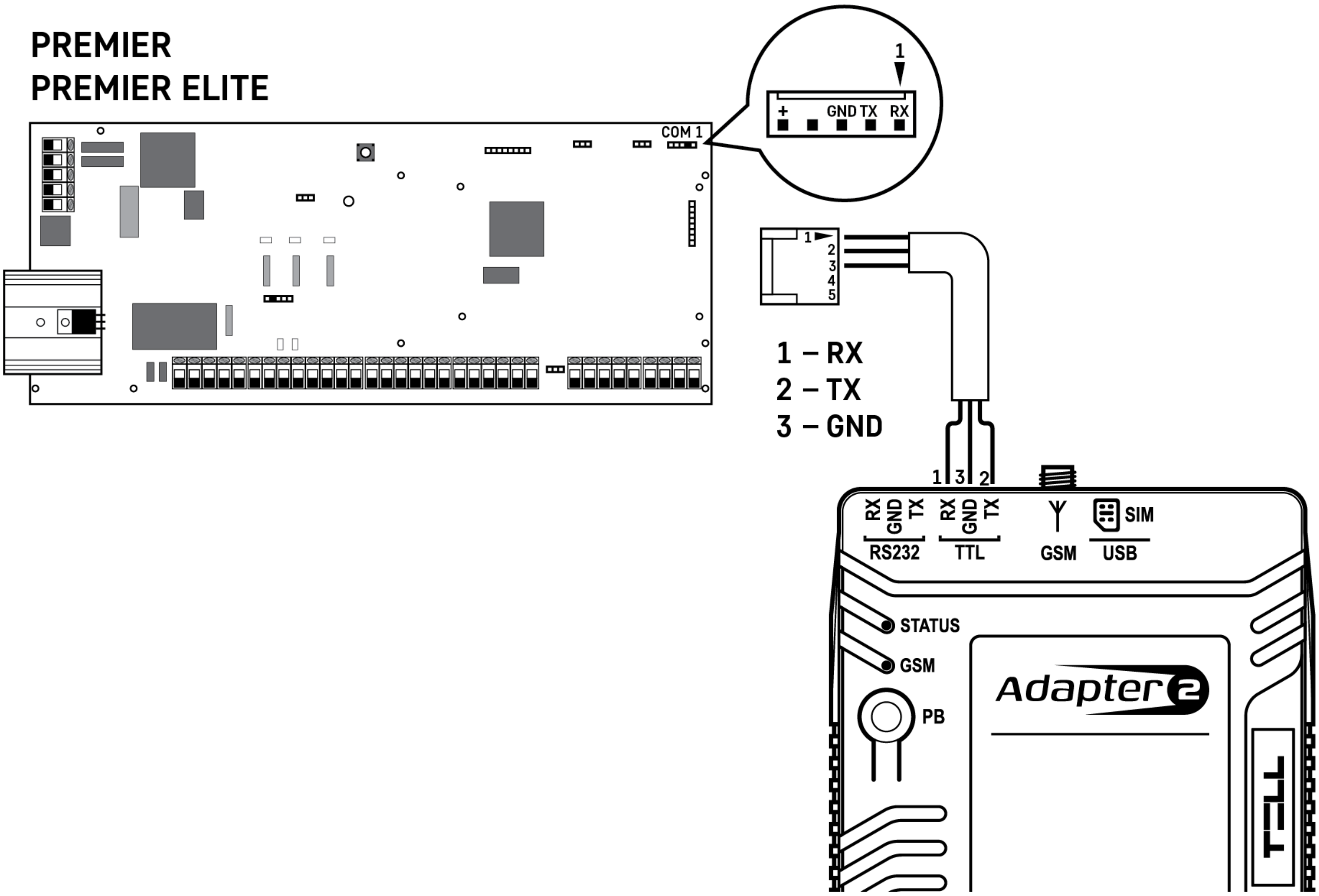
System logs

```
9:08:32 - Program started
9:09:49 - Create port: COM6
9:09:50 - Successfully authenticated
9:09:50 - The remote device is online
```

In case of using the ***Adapter2*** programming software, you can close the serial data connection using the ***Unlink remote serial port*** button placed in the ***General*** settings menu.

5.1.3 Premier and Premier Elite alarm systems

- **Installation:**

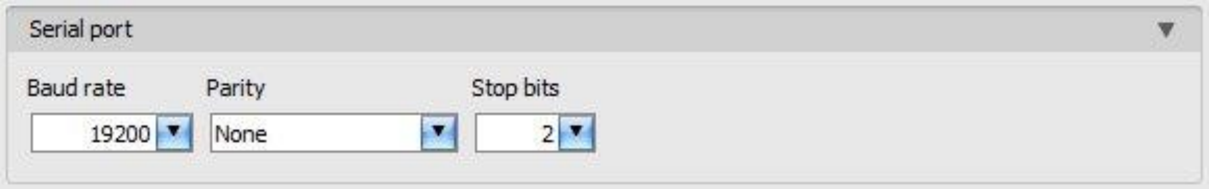


Wiring diagram for Premier alarm systems

For connecting Premier alarm control panels, a cable with a special plug is needed, which is available under the name **E-Shift-PRE cable** in TELL's product range. Connect the bare wire end of the cable to the **TTL** port of the **Adapter2 PRO** as shown in the figure above, then connect the other end with the plug onto the alarm control panel.

- **Software settings:**

Configure the serial port settings in the "***Serial port***" section of the "***General***" menu, in the ***Adapter2*** programming software, as shown in the figure below (Baud rate=19200, Parity=None, Stopbits=2):

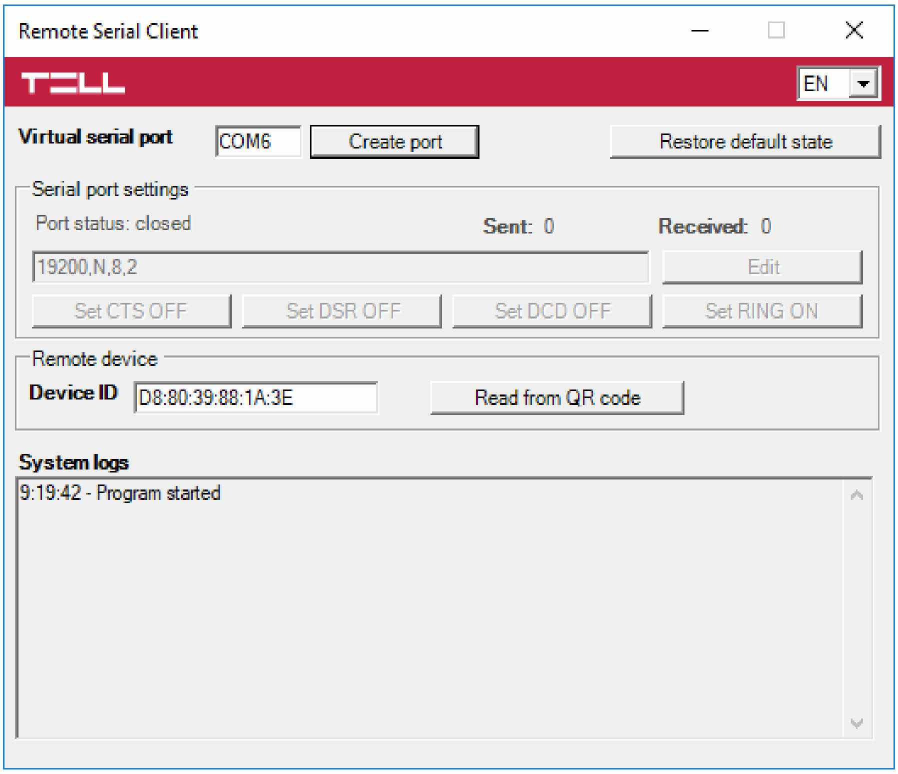


Serial port

Baud rate: 19200
Parity: None
Stop bits: 2

To establish the connection between the alarm control panel and its programming software, it is necessary to install the ***Remote Serial Client*** software. This client software ensures the connection between the PC and the ***Adapter2 PRO*** device, as well as it creates a virtual serial port for the programming software of the alarm system.

As an alternative, the remote data connection can also be established using the ***Link remote serial port*** button placed in the ***General*** settings menu in the ***Adapter2*** programming software. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com).



Virtual serial port COM6

Port status: closed **Sent:** 0 **Received:** 0

19200,N,8,2

Device ID D8:80:39:88:1A:3E

System logs

```
9:19:42 - Program started
```

Open the ***Remote Serial Client*** software and configure the settings in the order below:

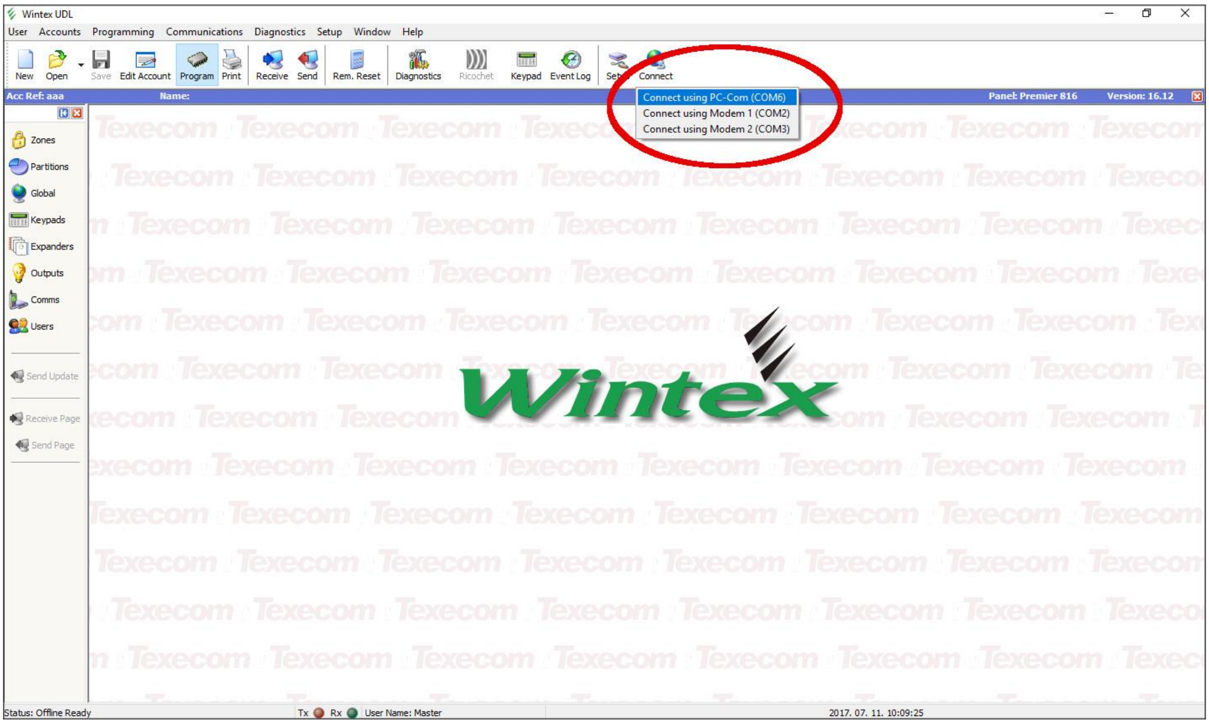
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***Adapter2 PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains the QR code with the device ID.

Virtual serial port: enter the number of the virtual port you wish to create (e.g.: COM6).

System logs: shows information about program operation and displays data received through the serial port.

Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***Adapter2 PRO*** device should be online to create the virtual serial port.

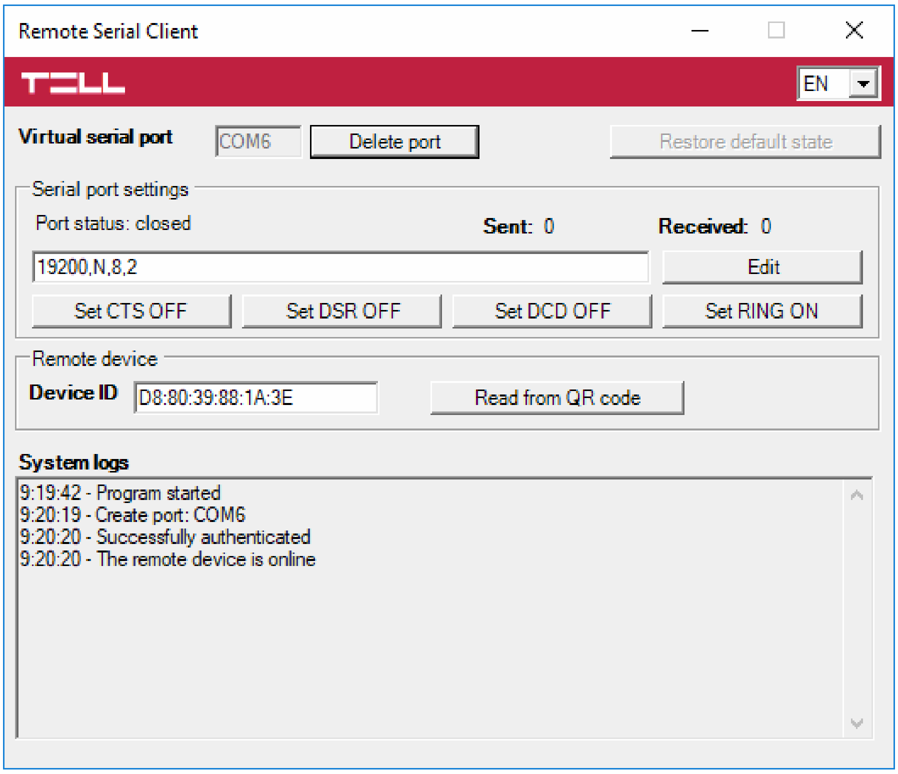
Example for selecting the serial communication port in the ***Wintex*** programming software:



Acc Ref: aaa
Name:
Panel: Premier 816
Version: 16.12
Status: Offline Ready
User Name: Master
2017. 07. 11. 10:09:25

Then the programming software will open the serial port and will establish the connection with the alarm control panel.

After you have finished remote programming the alarm control panel, you can delete the created virtual serial port by clicking on the “***Delete port***” button.



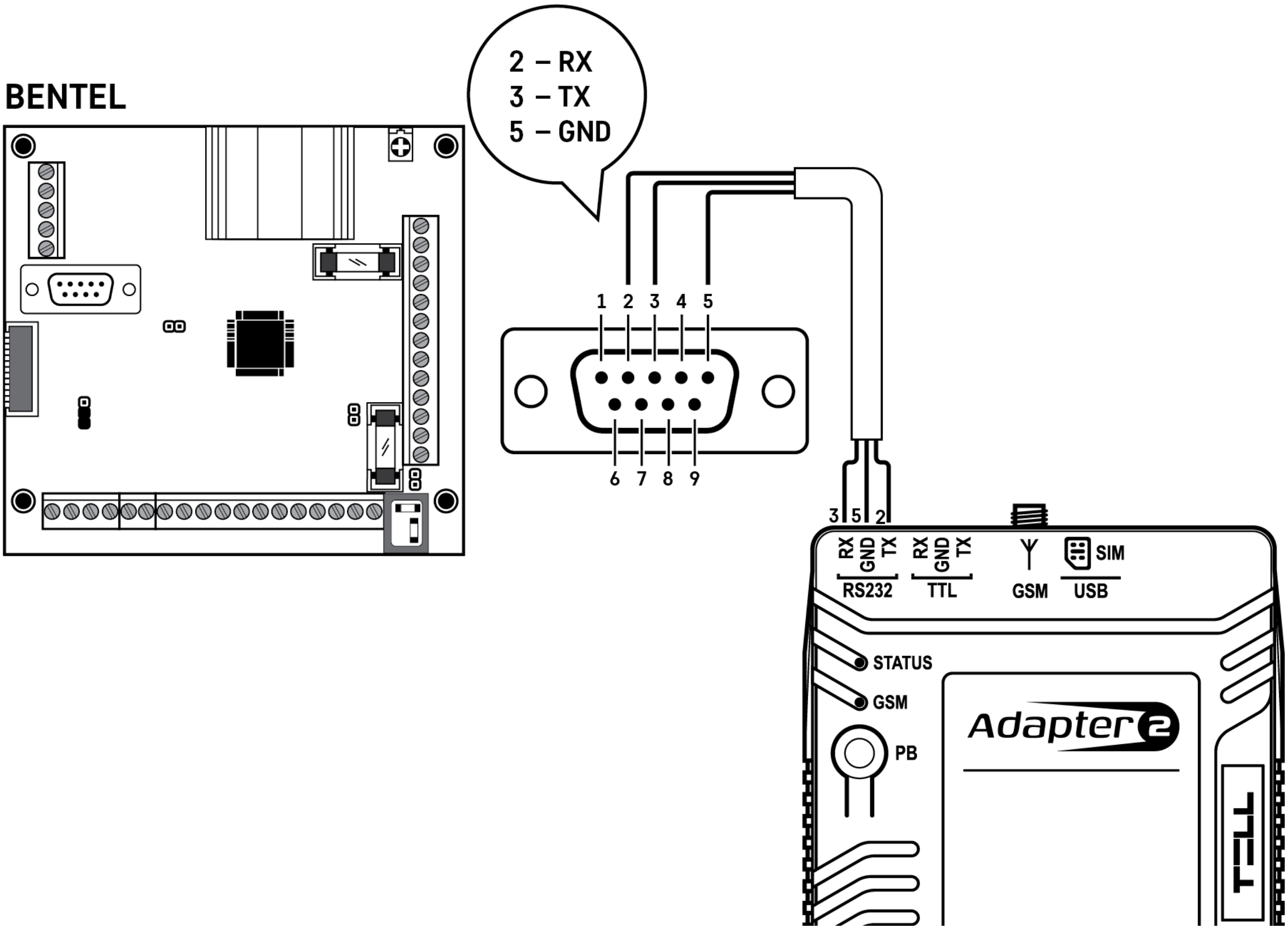
Virtual serial port: COM6
Port status: closed
Sent: 0
Received: 0
19200,N,8,2
Device ID: D8:80:39:88:1A:3E

```
9:19:42 - Program started
9:20:19 - Create port: COM6
9:20:20 - Successfully authenticated
9:20:20 - The remote device is online
```

In case of using the ***Adapter2*** programming software, you can close the serial data connection using the ***Unlink remote serial port*** button placed in the ***General*** settings menu.

5.1.4 Bentel alarm systems

- **Installation:**

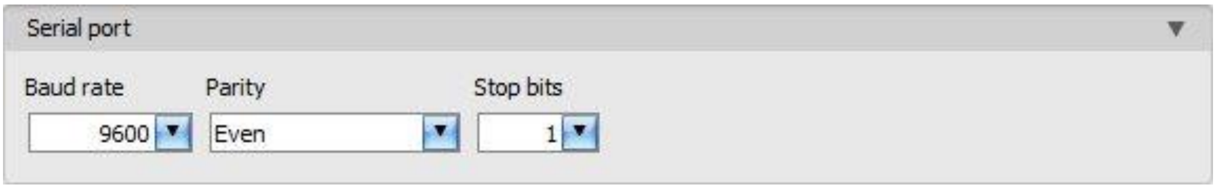


Wiring diagram for Bentel alarm systems

Connect the bare wire end of the serial programming cable to the **RS232** serial port of the **Adapter2 PRO** device as shown in the figure above, then connect the other end with the D-SUB plug onto the alarm control panel.

- **Software settings:**

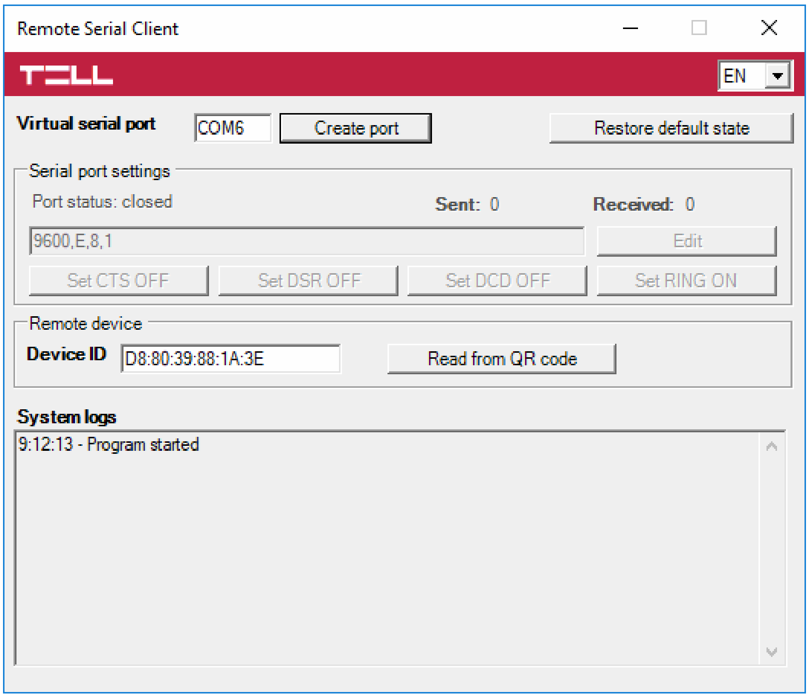
Configure the serial port settings in the “***Serial port***” section of the “***General***” menu, in the ***Adapter2*** programming software, as shown in the figure below (Baud rate=9600, Parity=Even, Stopbits=1):


Serial port

Baud rate: 9600
Parity: Even
Stop bits: 1

To establish the connection between the alarm control panel and its programming software, it is necessary to install the ***Remote Serial Client*** software. This client software ensures the connection between the PC and the ***Adapter2 PRO*** device, as well as it creates a virtual serial port for the programming software of the alarm system.

As an alternative, the remote data connection can also be established using the ***Link remote serial port*** button placed in the ***General*** settings menu in the ***Adapter2*** programming software. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com).



Remote Serial Client

TELL EN

Virtual serial port: COM6 | Create port | Restore default state

Serial port settings

Port status: closed — Sent: 0 — Received: 0

9600,E,8,1 | Edit

Set CTS OFF | Set DSR OFF | Set DCD OFF | Set RING ON

Remote device

Device ID: D8:80:39:88:1A:3E | Read from QR code

System logs

```
9:12:13 - Program started
```

Open the ***Remote Serial Client*** software and configure the settings in the order below:

Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***Adapter2 PRO*** device connected to the alarm control panel.

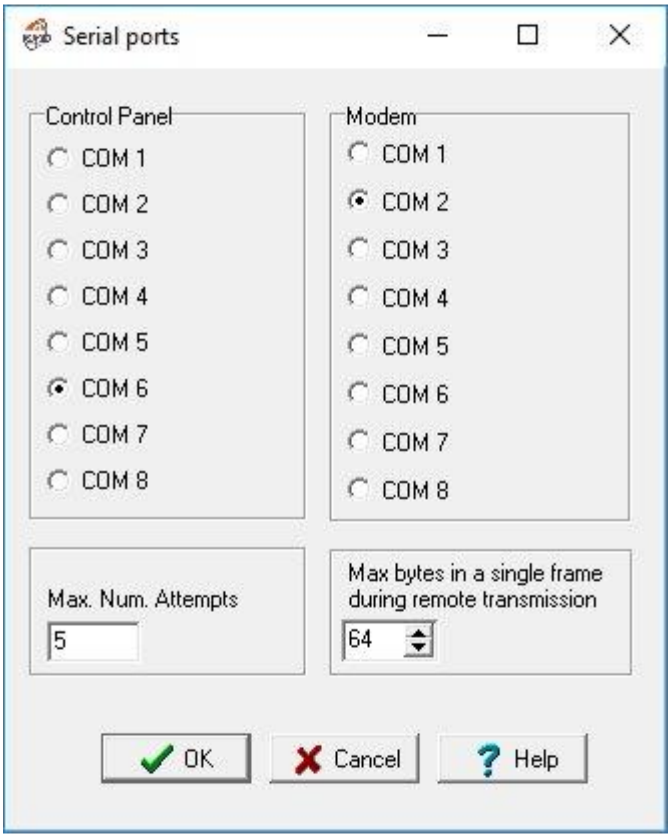
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains the QR code with the device ID.

Virtual serial port: enter the number of the virtual port you wish to create (e.g.: COM6).

System logs: shows information about program operation and displays data received through the serial port.

Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***Adapter2 PRO*** device should be online to create the virtual serial port.

Example for selecting the serial communication port in the ***Bentel Security Suite*** programming software (see the figure on the right-hand side).



Serial ports

Control Panel: ○ COM 1, ○ COM 2, ○ COM 3, ○ COM 4, ○ COM 5, ● COM 6, ○ COM 7, ○ COM 8

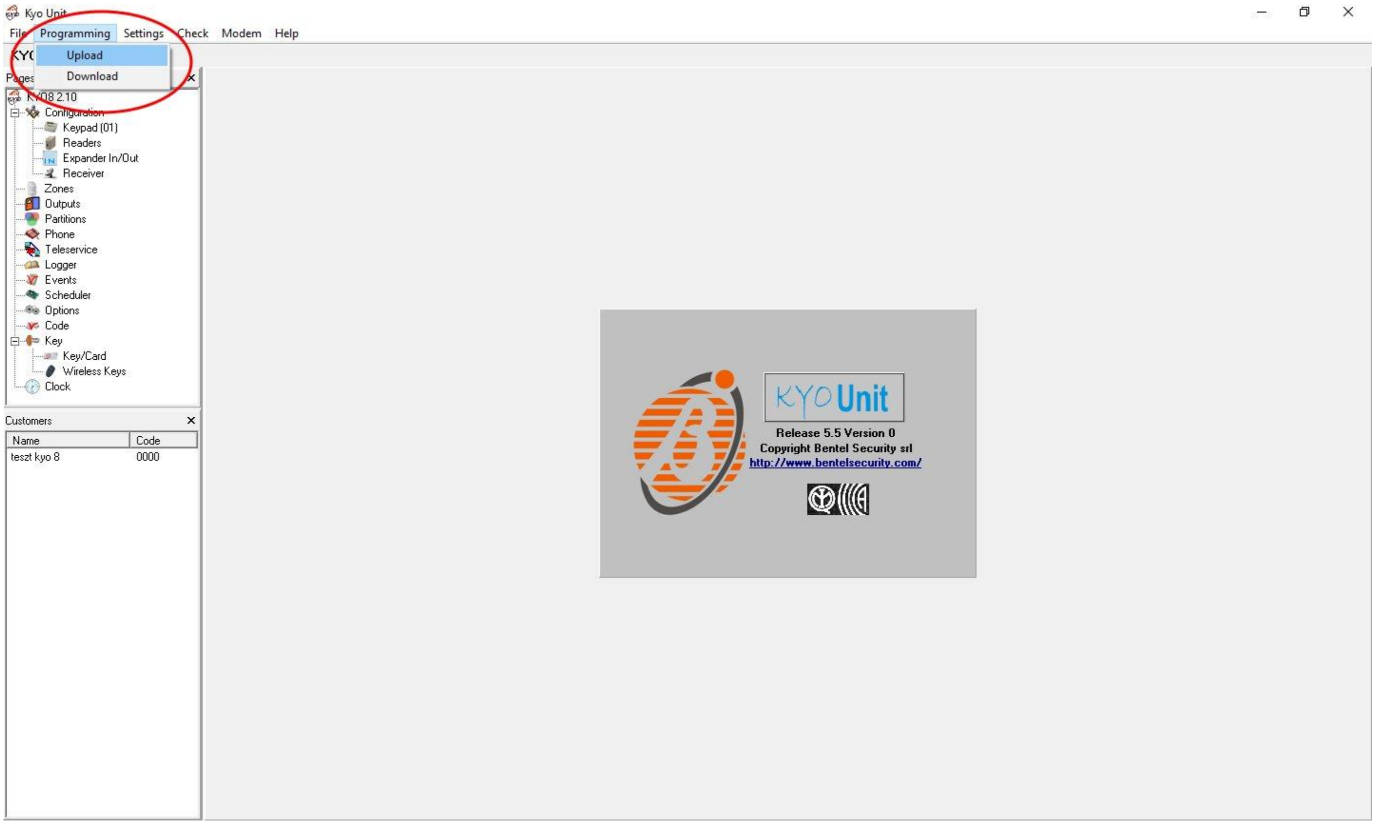
Modem: ○ COM 1, ● COM 2, ○ COM 3, ○ COM 4, ○ COM 5, ○ COM 6, ○ COM 7, ○ COM 8

Max. Num. Attempts: 5

Max bytes in a single frame during remote transmission: 64

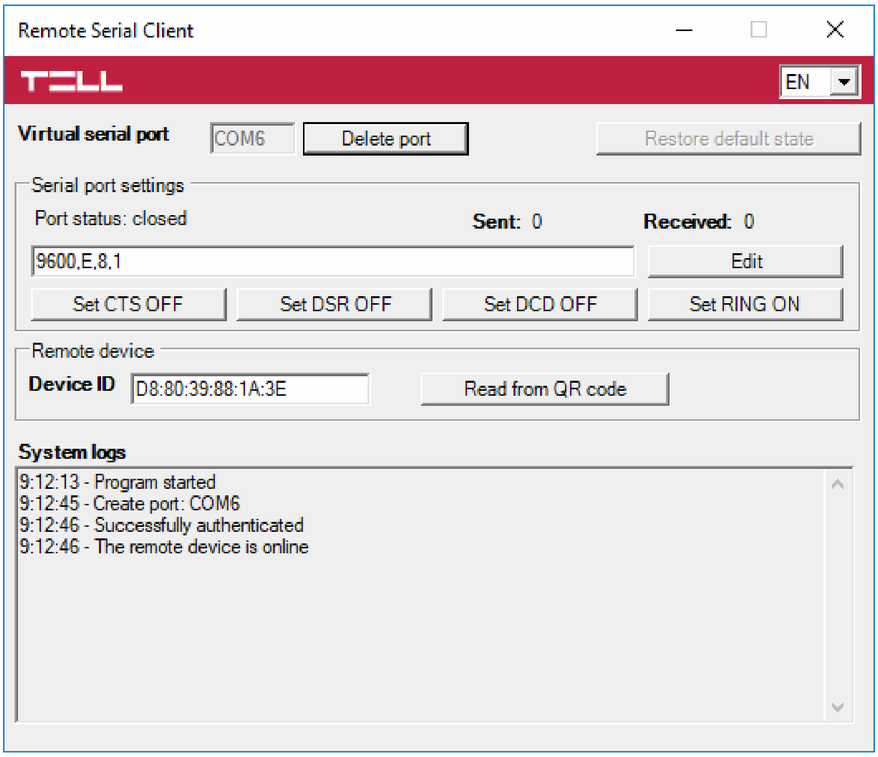
✓ OK | ✗ Cancel | ? Help

Start connecting:



Then the programming software will open the serial port and will establish the connection with the alarm control panel.

After you finished remote programming the alarm control panel, you can delete the created virtual serial port by clicking on the "***Delete port***" button.



Virtual serial port: COM6

Port status: closed

Sent: 0

Received: 0

9600,E,8,1

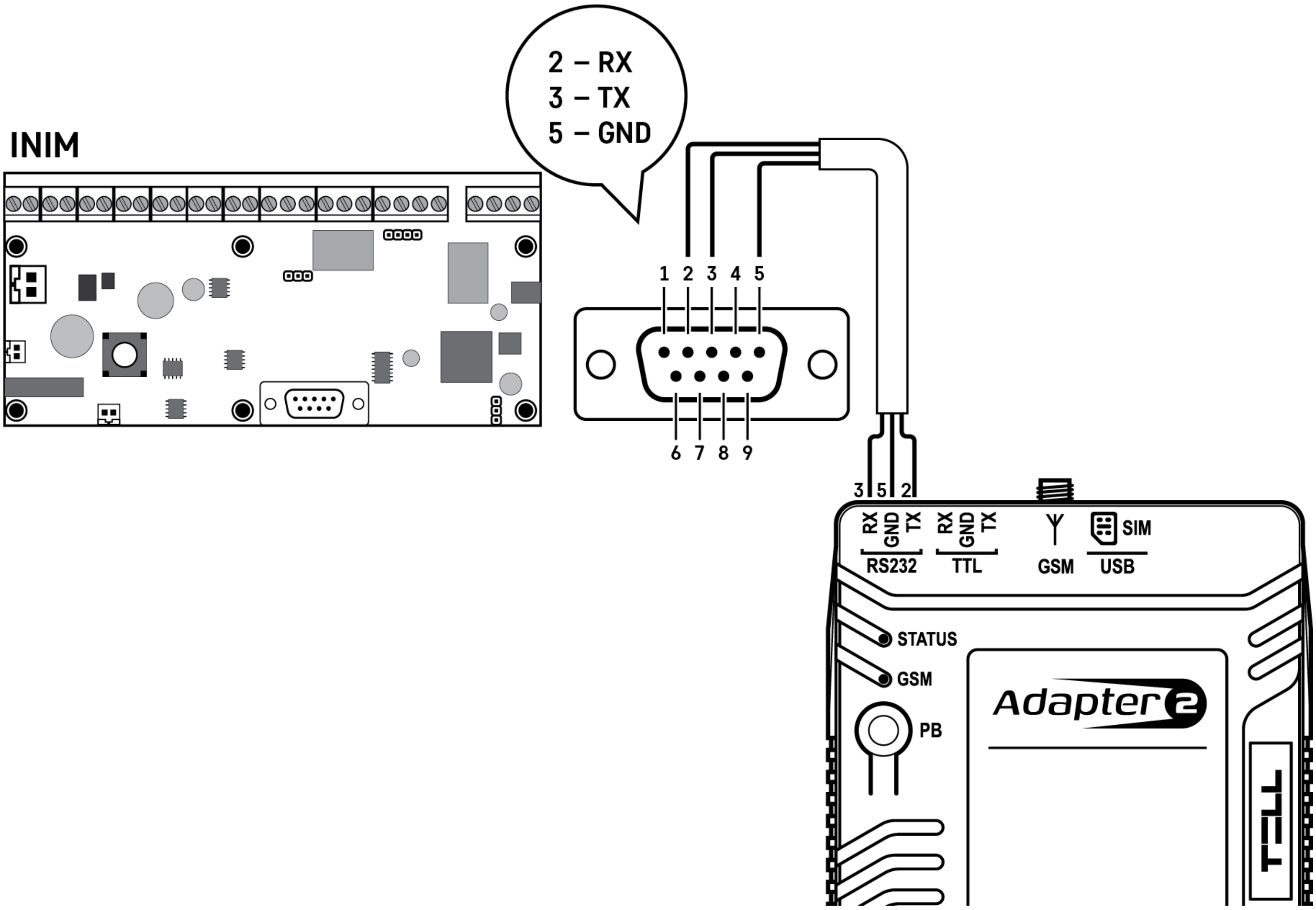
Device ID: D8:80:39:88:1A:3E

```
9:12:13 - Program started
9:12:45 - Create port: COM6
9:12:46 - Successfully authenticated
9:12:46 - The remote device is online
```

In case of using the ***Adapter2*** programming software, you can close the serial data connection using the ***Unlink remote serial port*** button placed in the ***General*** settings menu.

5.1.5 Inim alarm systems

- **Installation:**

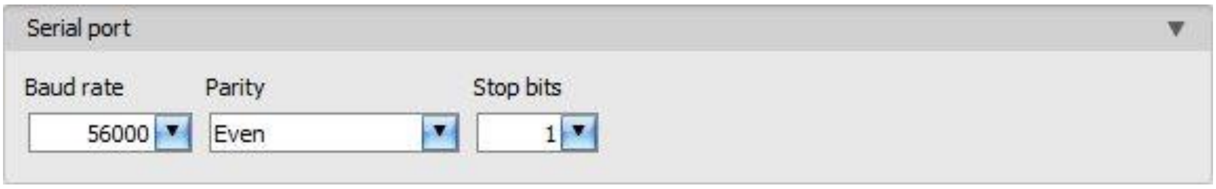


Wiring diagram for Inim alarm systems

Connect the bare wire end of the serial programming cable to the **RS232** serial port of the **Adapter2 PRO** device as shown in the figure above, then connect the other end with the D-SUB plug onto the alarm control panel.

- **Software settings:**

Configure the serial port settings in the "***Serial port***" section of the "***General***" menu, in the ***Adapter2*** programming software, as shown in the figure below (Baud rate=56000, Parity=Even, Stopbits=1):



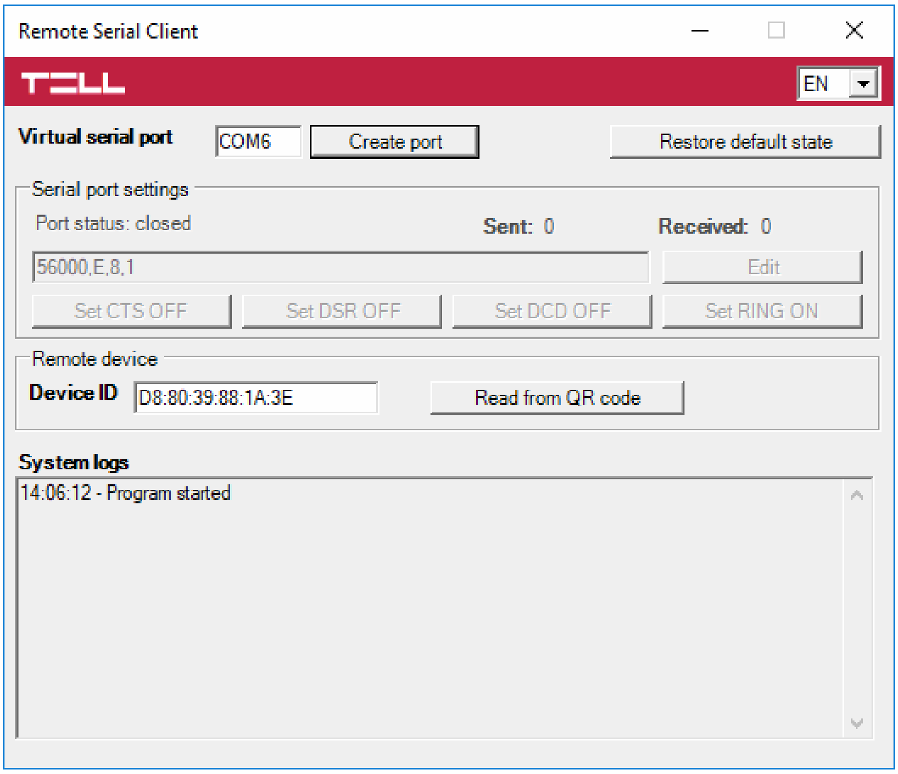
Serial port

Baud rate: 56000

Parity: Even

Stop bits: 1

To establish the connection between the alarm control panel and its programming software, it is necessary to install the ***Remote Serial Client*** software. This client software ensures the connection between the PC and the ***Adapter2 PRO*** device, as well as it creates a virtual serial port for the programming software of the alarm system.
As an alternative, the remote data connection can also be established using the ***Link remote serial port*** button placed in the ***General*** settings menu in the ***Adapter2*** programming software. This option requires a third-party software that can create a linked pair of virtual serial ports (e.g., com0com).



Remote Serial Client

Virtual serial port: COM6

Serial port settings

Port status: closed

Sent: 0

Received: 0

56000,E,8,1

Remote device

Device ID: D8:80:39:88:1A:3E

System logs

```
14:06:12 - Program started
```

Open the ***Remote Serial Client*** software and configure the settings in the order below:

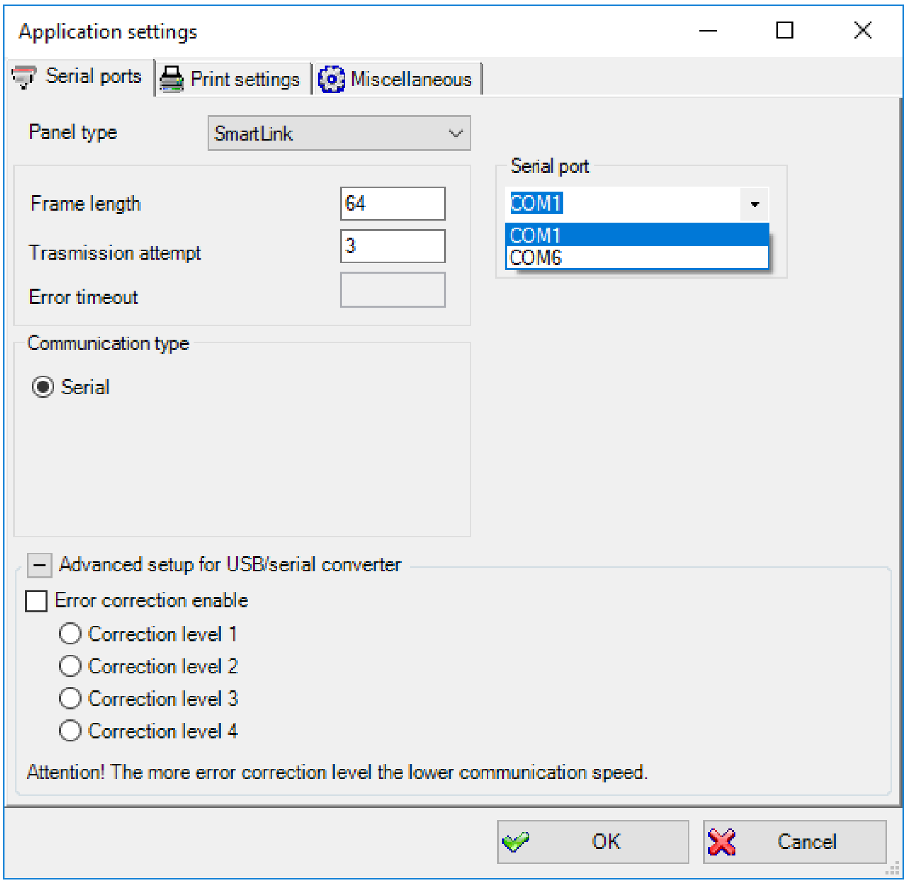
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***Adapter2 PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains the QR code with the device ID.

Virtual serial port: enter the number of the virtual port you wish to create (e.g.: COM6).

System logs: shows information about program operation and displays data received through the serial port.

Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***Adapter2 PRO*** device should be online to create the virtual serial port.

Example for selecting the serial communication port in the ***Ability Suite*** programming software, in the “***Settings / Application settings***” menu:



Application settings

Serial ports | Print settings | Miscellaneous

Panel type: SmartLink

Frame length: 64

Trasmission attempt: 3

Error timeout:

Serial port: COM1

COM1
COM6

Communication type

● Serial

⊟ Advanced setup for USB/serial converter

□ Error correction enable

○ Correction level 1

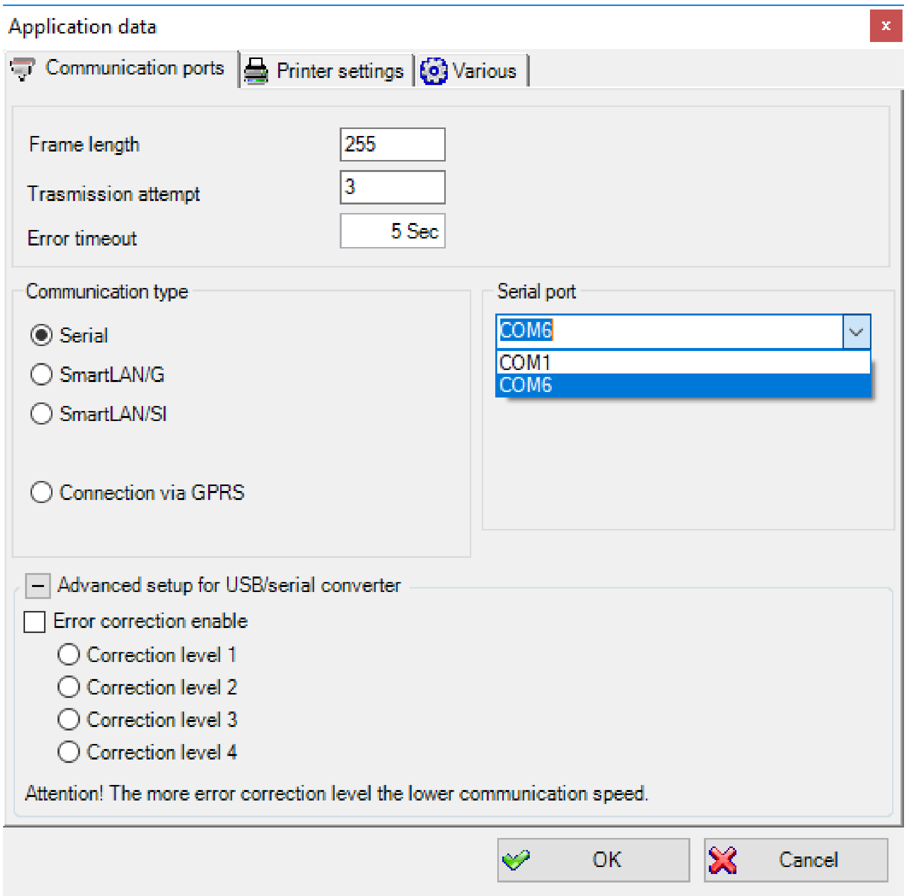
○ Correction level 2

○ Correction level 3

○ Correction level 4

Attention! The more error correction level the lower communication speed.

Example for selecting the serial communication port in the ***Smart League*** programming software, in the “***Settings / Application settings***” menu:



Application data

Communication ports | Printer settings | Various

Frame length: 255

Trasmission attempt: 3

Error timeout: 5 Sec

Communication type

● Serial

○ SmartLAN/G

○ SmartLAN/SI

○ Connection via GPRS

Serial port: COM6

COM1
COM6

⊟ Advanced setup for USB/serial converter

□ Error correction enable

○ Correction level 1

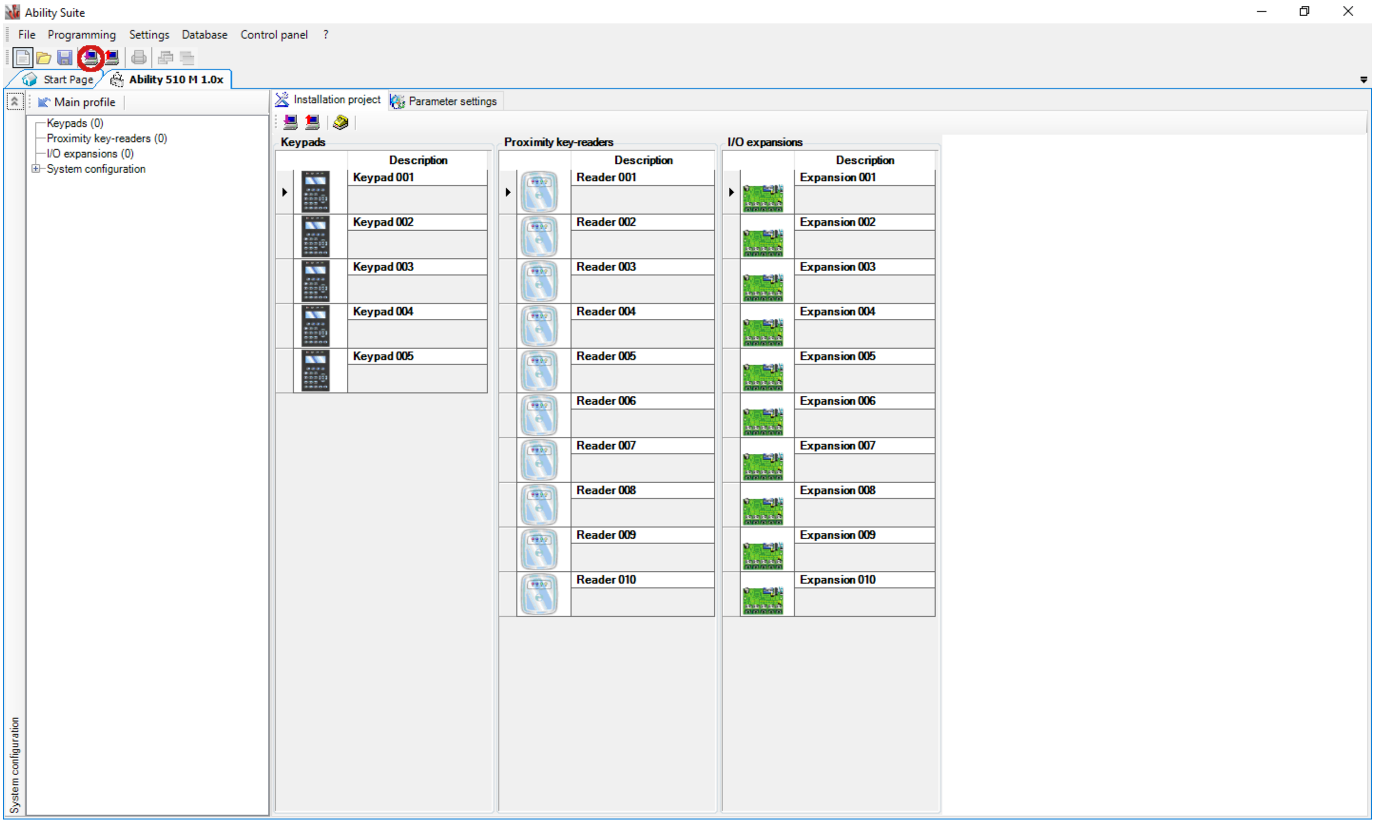
○ Correction level 2

○ Correction level 3

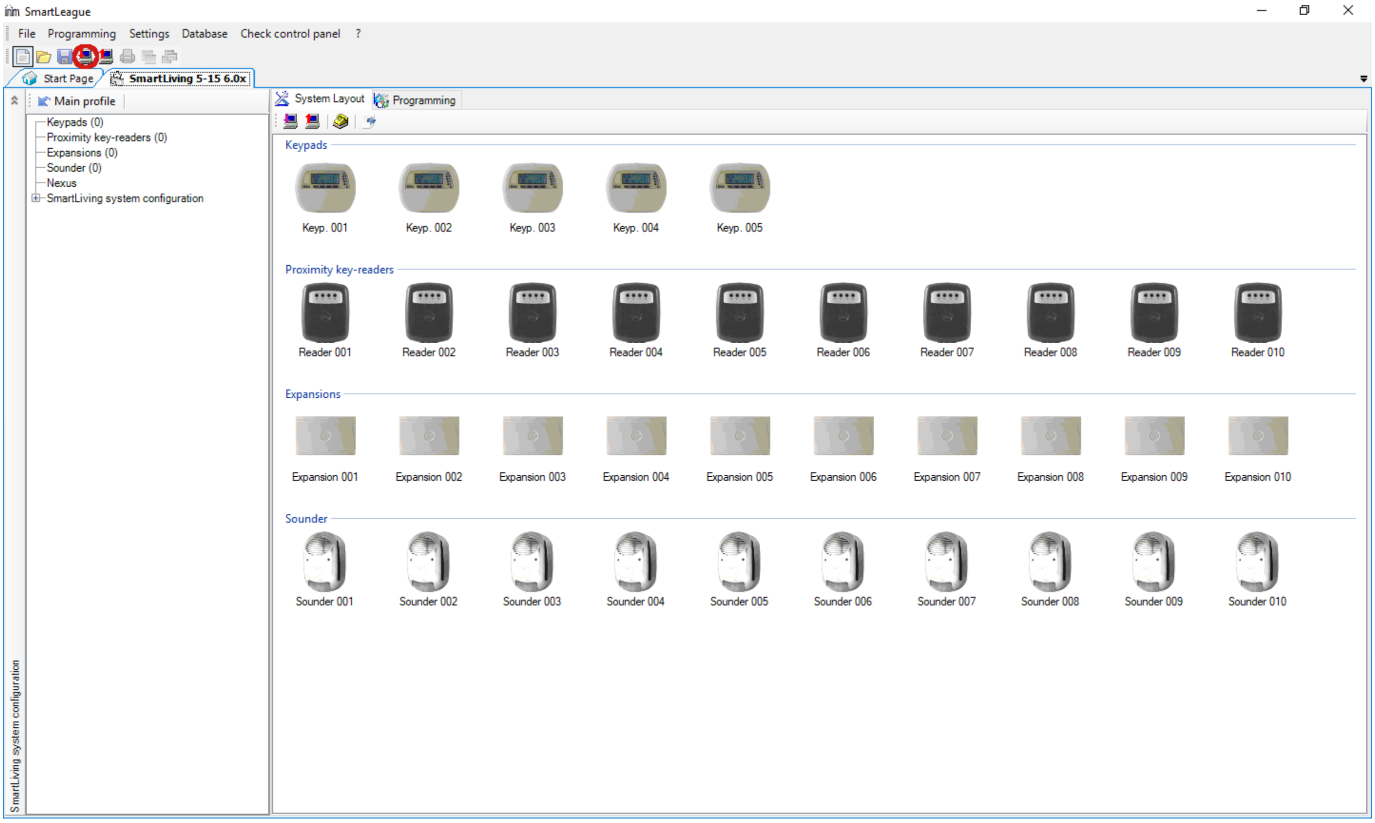
○ Correction level 4

Attention! The more error correction level the lower communication speed.

Start connecting with the ***Ability Suite*** programming software:

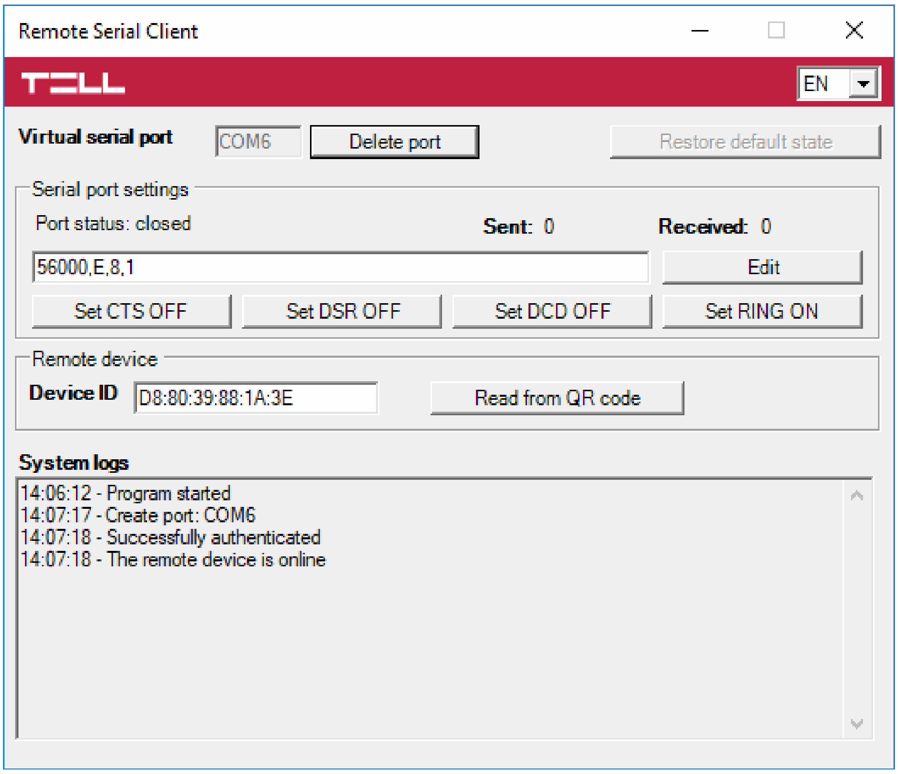


Start connecting with the ***Smart League*** programming software:



Then the programming software will open the serial port and will establish the connection with the alarm control panel.

After you finished remote programming the alarm control panel, you can delete the created virtual serial port by clicking on the “***Delete port***” button.



Virtual serial port: COM6

Serial port settings

Port status: closed Sent: 0 Received: 0

56000,E,8,1

Remote device

Device ID: D8:80:39:88:1A:3E

System logs

```
14:06:12 - Program started
14:07:17 - Create port: COM6
14:07:18 - Successfully authenticated
14:07:18 - The remote device is online
```

In case of using the ***Adapter2*** programming software, you can close the serial data connection using the ***Unlink remote serial port*** button placed in the ***General*** settings menu.

6 Arming and disarming the alarm control panel through the mobile application

It is possible to arm and disarm the connected alarm control panel via the mobile application if the given alarm control panel can be armed and disarmed by potential free (dry) relay contact pulses through one of its inputs. To use this feature, follow the instructions below:

- Connect the relay output (**NO** and **COM**) of the **Adapter2 PRO** to the alarm control panel’s arming and disarming input.
- Set the given input in the alarm control panel to arm and disarm the entire system with normally open (**NO**) pulse control.
- Open the settings of the registered **Adapter2 PRO** in the “***Device settings***” menu in the mobile application and tap on the output edit icon in the “***Outputs***” section. Enable the “***Pulse control***” option, and then apply the changes. You can leave the duration of control at the default value (***1 second***).

To arm and disarm the alarm control panel, activate the output of the **Adapter2 PRO** in the mobile application. Each output activation creates a closed contact between the **NO** and **COM** terminals of output **OUT** for the period of time configured (1 second), and then it reverts to default open state automatically. At the same time, the mobile application also resets the output control button to its default state.

7 Updating the firmware

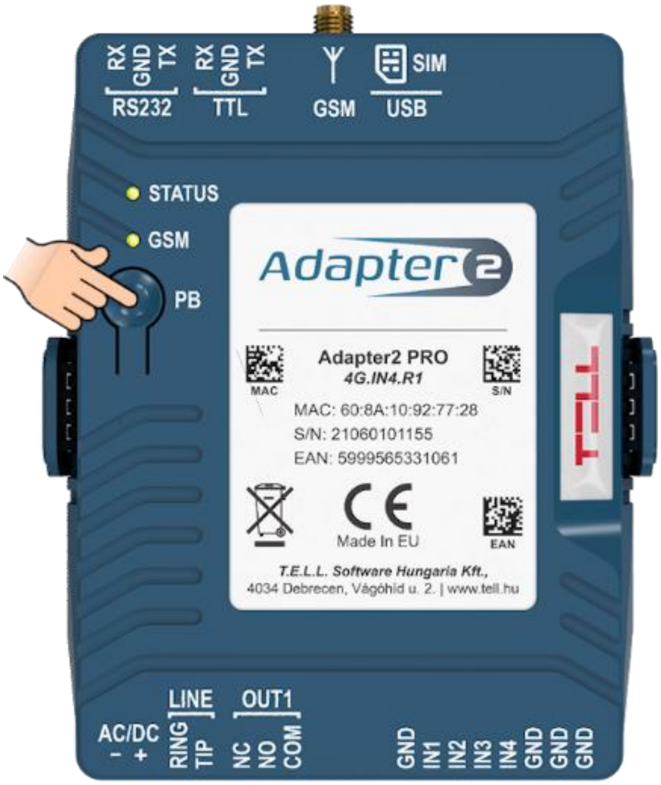
TELL always releases its products with the latest firmware version. However, as our products are being continuously improved, new firmware updates may occasionally be released for the products, which may include new features along with bug fixes. Therefore, it is recommended that you always upgrade your product to the latest firmware version available. All released firmware versions are available on the TELL website, including older versions.
ATTENTION! Downgrading to an earlier version is not supported! Always upgrade your product to the latest version. Otherwise, your settings could get wiped due to differences in functionality between versions, or the product may become unusable due to unsupported components. (A newer hardware may contain new components, e.g., a new flash memory, modem, etc., which are not supported by an earlier firmware.)

You can update the firmware of your ***Adapter2 PRO*** device locally via USB, or remotely via the Internet. You can find the firmware file or the desktop update application needed for the update on the manufacturer's website (https://tell.hu/en) in the product downloads section.

7.1 Updating via USB

You can update the firmware via USB using the desktop update tool (application) or the programming software.

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



  - Wait until the **STATUS** LED on the device shows activity. You can then connect to the programming software and check the functioning.

- **Updating via USB using the programming software:**
  - Download the latest firmware file (that has the **.tf3** extension) necessary for updating, from the manufacturer’s website.
  - Click on the “***Connection type***” menu in the programming software.
  - Click the „***Firmware update***” ⬇ button, and then browse the **.tf3** firmware file.
  - The update process will start automatically as soon as you click on the “***Open***” button. Once the firmware is loaded, the progress window will close automatically and the device will restart in a few seconds, running on the new firmware.

7.2 Updating remotely over the internet

It is also possible to update the firmware of the ***Adapter2 PRO*** 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, as specified above.

The following methods are available for updating the firmware of the ***Adapter2 PRO*** device remotely:

- Updating in case that you use a **TELLMon** receiver:
  - Directly from the **TELLMon** receiver, by loading the firmware file in the receiver.
  - Using the programming software, via the TELLMon protocol.
  - Using the programming software, via the TEX protocol.
  - Using the programming software, over the cloud.
- Updating in case that you use an **MVP.next** server:
  - Using the programming software, via the TELLMon protocol.
  - Using the programming software, via the TEX protocol.
  - Using the programming software, over the cloud.
- Updating in case that you use a **TEX-MVP** or a **TEX BASE/PRO** server:
  - Using the programming software, via the TEX protocol.
  - Using the programming software, over the cloud.
- Updating in case that you use a **SIA DC-09** compatible IP receiver:
  - Using the programming software, over the cloud.

8 Restoring the factory default settings

You can restore the factory default settings using the programming software.

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

To restore the factory default settings, click on the “***Restore factory default settings***” button in the “***Connection type***” menu. The reset process may take more than 1 minute, and it will restart the device. Wait until the device restarts and the **STATUS** LED on the device shows activity again. The option of restoring the factory default settings is also available when you connect to the device without entering the device password.

Restoring the factory default settings will be refused by the device if the “***Locked***” option has been selected in the “***Locking the device***” section, in the “***Advanced settings***” menu. In this case, the software will show an error message about that, after the information message shown right after the confirmation. If you have forgotten the superadmin password, and the device has been locked with the mentioned option, only the manufacturer can restore the factory default settings in the service center.

9 Contents of the package

- **Adapter2 PRO** + terminal connector
- GSM antenna
- Quick start guide
- Warranty card

10 About the manufacturer

Company: T.E.L.L. Software Hungária Kft
Address: 4034 Debrecen, Vágóhíd u. 2., Hungary
Website: www.tell.hu