Pager4
Pager4 PRO

INSTALLATION AND USER MANUAL

for device version v7.04
Document version: 7.3 14.08.2023

Product models:

- **Pager4 2G.IN4.R2**
- **Pager4 2G.IN6.R1**
- **Pager4 3G.IN4.R2**
- **Pager4 3G.IN6.R1**
- **Pager4 4G.IN4.R2**
- **Pager4 4G.IN6.R1**
- **Pager4 WiFi.IN4.R2**
- **Pager4 WiFi.IN6.R1**
- **Pager4 PRO 2G.IN4.R2**
- **Pager4 PRO 2G.IN6.R1**
- **Pager4 PRO 3G.IN4.R2**
- **Pager4 PRO 3G.IN6.R1**
- **Pager4 PRO 4G.IN4.R2**
- **Pager4 PRO 4G.IN6.R1**
- **Pager4 PRO WiFi.IN4.R2**
- **Pager4 PRO WiFi.IN6.R1**

Table of contents

1 Main functions of the product

The device can be used as an accessory for alarm control panels, as an individual transmitter, or as a 4/6 zone standalone alarm control device with arming/disarming option.

Main 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 that can be uploaded 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 10 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 10 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 2 phone numbers.
- 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 event including partition and zone options.
- Output control can be customized separately for each event using different operation modes.
- Available events: input events, service/error events (new and restore as well).
- Local arming and disarming using dry contacts on inputs (with optional keyswitch, RF remote controller or access control keypad with relay output) .
- Remote arming and disarming, status query and output control by phone call and SMS, as well as through the Internet using the mobile application*.
- IP camera support: forwarding the links of up to 4 IP cameras by e-mail and Push notification along with the alarm messages.

* Available in the **PRO** product model only.
** SMS and call-based functions are not available in the **WiFi** product model.

1.1 Differences between the *Pager4* and the *Pager4 PRO* models

There are differences in function between the **Pager4** and the **Pager4 PRO** product models. The **Pager4 PRO** includes the following extra functions:

- E-mail notification
- Push notification
- **TELL Control Center** multiplatform mobile application (iOS and Android)
- IP camera support

1.2 Differences between the 2G, 3G, 4G and WiFi models

The only difference between the **2G**, **3G** and **4G** models is the type of the modem used. The 3G (UMTS) and the 4G (LTE) communication makes possible higher speed, thereby increasing the speed of reporting. The **2G**, **3G** and the **4G** models can be used in Europe. There is no difference between the mentioned models regarding the available functions or configuration.

For the **2G** model, calls made through the GSM network will delay all other communication, since 2G modems are unable to use multiple communication channels simultaneously.

The **WiFi** model can only be used with a WiFi network. SMS and call-based functions are not available in this model, since it does not have a GSM modem. In turn, this model does not require a SIM card.

1.3 Differences between the IN4.R2 and the IN6.R1 models

The **IN4.R2** model comes with 4 contact inputs (IN1 to IN4) and 2 relay outputs (OUT1, OUT2), while the **IN6.R1** has 6 contact inputs (IN1 to IN6) and 1 relay output (OUT1).

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 Under Voltage Lock Out (UVLO) function

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

2.2 Input wiring

For the inputs, the normally closed or normally open dry contact should be connected between the given input (**IN1**…**IN4/IN6**) and the negative of the power input (**V-**) terminal.

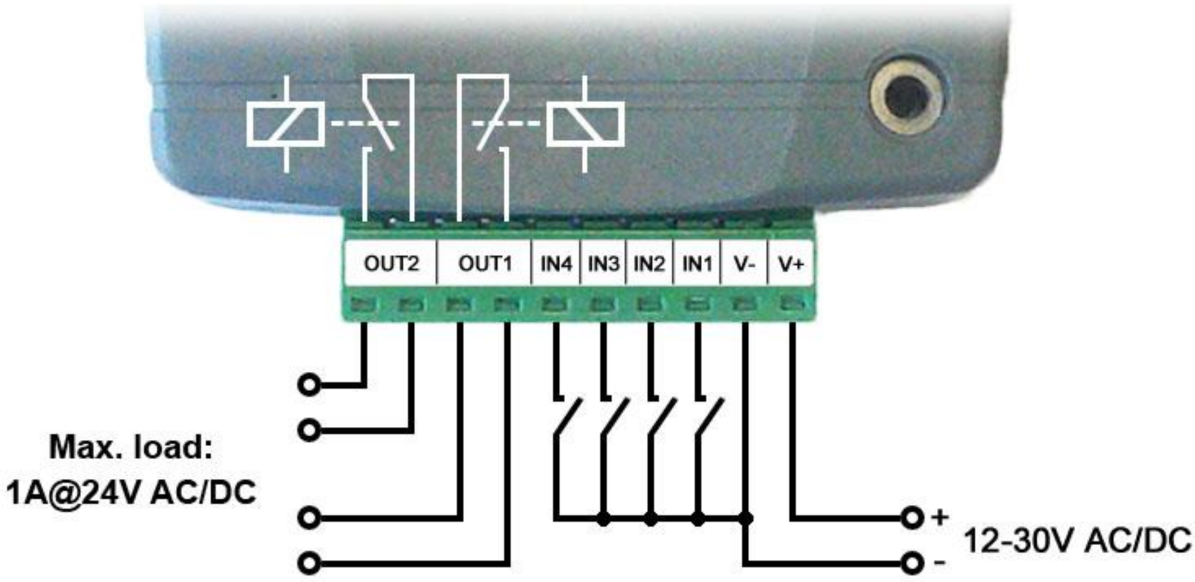
If a normally open dry contact is used to activate the input, choose the **NO** (normally open) option in the given input's settings. In this case, the input will become activated when the open contact between the given input (**IN1**…**IN4/IN6**) and the **V-** terminal becomes closed.

If a normally closed dry contact is used to activate the input, choose the **NC** (normally closed) option in the given input's settings. In this case, the input will become activated when the closed contact between the given input (**IN1**…**IN4/IN6**) and the **V-** terminal becomes open.

2.3 Output wiring

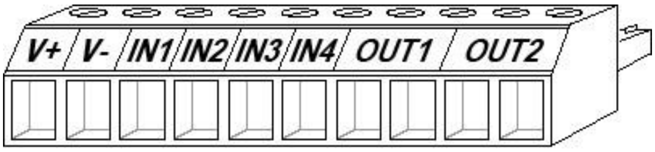
The output provides normally open (N.O.) dry (potential free) relay contact by default and closed contact upon control.

2.4 Connections and wiring (IN4.R2 model)

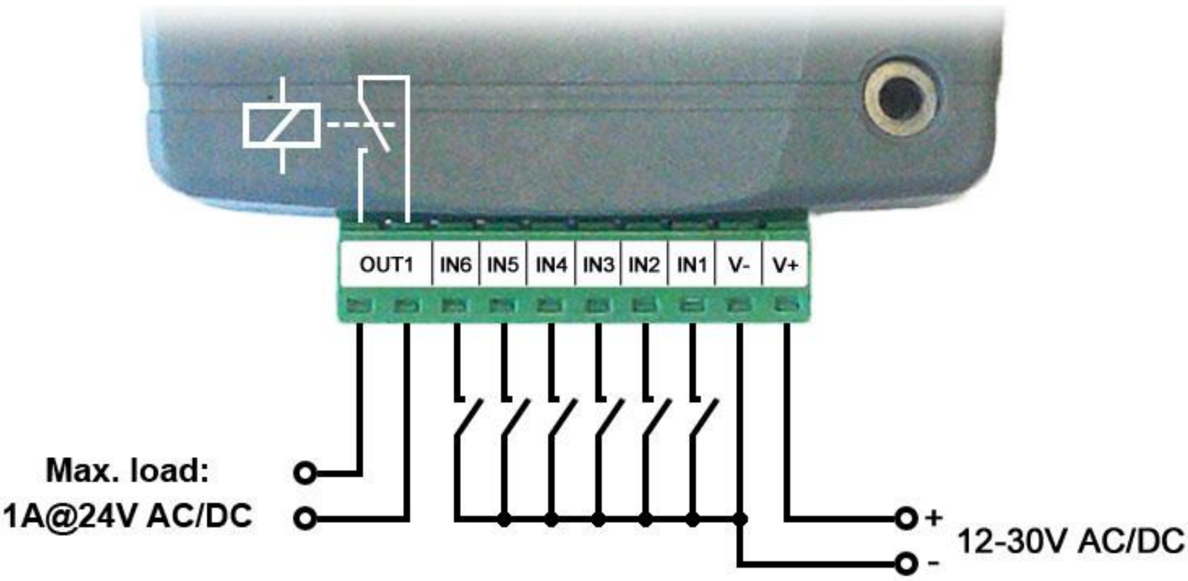


System terminal inputs and outputs:

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

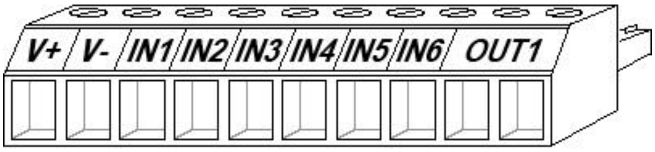


2.5 Connections and wiring (IN6.R1 model)



System terminal inputs and outputs:

V+	Supply voltage ~ / 12…30V AC/DC (min. 500 mA)
V-	Supply voltage ~ / negative (for DC)
IN1	Dry contact input 1
IN2	Dry contact input 2
IN3	Dry contact input 3
IN4	Dry contact input 4
IN5	Dry contact input 5
IN6	Dry contact input 6
OUT1	Relay output (normally open dry contact)



Attention!

We would not advise powering the device directly from the power output of an 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.

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.

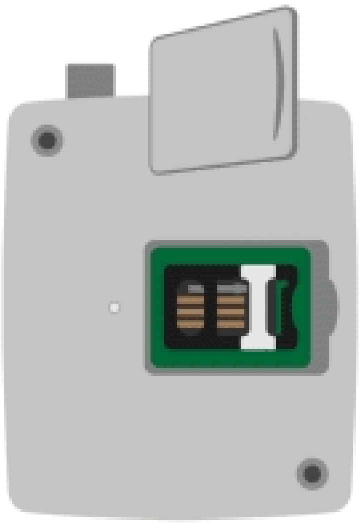
An ideal solution for the above purposes is the power supply designed and manufactured by TELL, which we expressly recommend using for our communicators.

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

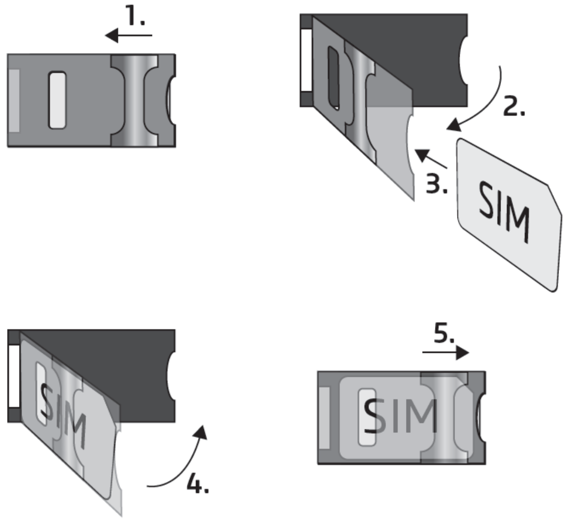
2.6 SIM card holder

The device requires a Mini (2FF) size SIM card.

The SIM card holder can be accessed by removing the cover of the aperture found on the device enclosure.
Note: the **WiFi** device model does not require a SIM card, therefore it has no SIM card holder. The cover can be removed by pressing it with your fingernail towards the LED at the end where the gap is and then pulling it outwards. Insert the SIM card in the holder. The services to be activated on the SIM card installed into the 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 service.



- Installing the SIM card:



- **1.** Pull the metal security lock of the SIM holder towards the LED until you hear a click.
- **2.** Reach under the metallic security lock with your fingernail and pull it outwards to open the holder.
- **3.** Slide the SIM card into the opened part with the contacts facing down, as shown in the figure.
- **4.** Close back the opened part together with the SIM card.
- **5.** Press down the metallic security lock carefully and pull it towards the side of the enclosure until you hear a click.

2.7 Connecting the antenna

Connect the GSM antenna to the FME-M 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.

2.8 Status LED signals

Blinking red	The GSM or WiFi service is unavailable, or system startup/restart is in progress
Permanent red	SIM card error (only for models with built-in modem)
Red blinks fast Green blinks slower	Event reporting is in progress
Green blinks slowly, Red is not lit	Connected to the GSM or WiFi network, device disarmed
Green and red blink alternately	Connected to the GSM or WiFi network, device armed

2.9 Installation

Please check the environment before installing the device.

- 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.

2.10 Putting into operation

- ***Disable the voicemail service and SMS notification about missed calls on the SIM card installed in the device.***
- ***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 both caller identification and caller ID presentation (CLIP) service on the SIM card at the GSM 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 GSM service provider and enable the services in the menu, or visit one of the service provider's personal customer services and ask to enable these services on the SIM card.
- Check the SIM card to be installed correctly into the device.
- Check the GSM antenna to be connected correctly to the device.
- Check the wires to be connected as instructed in the wiring diagram.
- You can power up the device (12…30V AC/DC). Make sure that the power source is sufficient for the operation of the device. The nominal current consumption of the device is 120mA, however, it may increase up to 500mA during communication and output control. If the used power source is not sufficient for the operation of the device, this may cause malfunctions.

2.11 Technical specification

Supply voltage range:	12…30V AC/DC
Nominal current consumption:	120mA
Highest current consumption:	500mA @ 12V DC, 250mA @ 24V DC
Operating temperature:	-20ºC to +70ºC
2G model:	850/900/1800/1900 MHz
3G model:	900/2100 MHz @UMTS, 900/1800 MHz @GSM
4G model:	900/1800 MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE
WiFi model:	2.4 GHz, 802.11 b/g/n
Highest load supported on outputs:	1A @ 24VAC/DC
Dimensions:	84 x 72 x 32mm
Net weight:	200g
Gross weight (packed):	300g

3 General information on the notification process

Notifications are performed based on the events available in the device. Each event can be configured to send report to CMS over IP or DTMF-based voice call, as well as to send notifications to users by call, SMS, Push message or e-mail (depending on device model).

There are 3 groups of events available in the device: input events, service events and custom events.

- An input event is generated when an input is activated, but only if the device is armed or the given input is configured as a 24h zone. Non-24h inputs will not generate events when the device is disarmed.
- Service events are generated automatically by the device, and can send notifications also when the device is disarmed. Service events are such as arming, disarming, error events, periodic test report.
- Custom events are generated by sending any configurable command to the device in a text message. Custom events and commands can be freely configured.

When an event is generated, the device starts sending notifications and performing controls configured for the given event. The notification order corresponds to the order in which the events occur.

Reporting to CMS has priority against notification of users. The number of attempts for reporting to CMS have a separate logic, since reporting to CMS is based on notification templates. You can read more about this in the "***Notification templates***" paragraph. Regarding text message sending and calls, the device makes 3 attempts to send a message and 3 attempts to make a call to a user phone number. The device will no longer try to report events for which reporting failed for more than 24 hours.

Attention! For generating events and sending notifications it is essential that the device system time is set! The setting can be done automatically from the mobile network, via the cloud service, from an NTP server, or from a remote monitoring receiver, and can also be set manually in the "*Status monitoring*" menu.

As it may occur that automatic time synchronization fails (for example, if the given mobile service provider does not support this option, and if the mobile Internet service is not enabled on the SIM card at the same time, so the device cannot use the NTP, cloud, or the remote monitoring synchronization option), for proper operation, please check the system time setting in the "*Status monitoring*" menu and adjust if necessary using the "*Time synchronization*" button.

Notification of users via voice call is not necessarily done in the same order as the phone numbers are recorded in the software.

4 Configuring the Pager4

The device can be configured the following ways:

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

The ***Pager4*** 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 **Pager4** programming software can be used to configure all **Pager4** device models.

4.1 The user interface and configuration options of the software

The user interface language can be selected during installation.

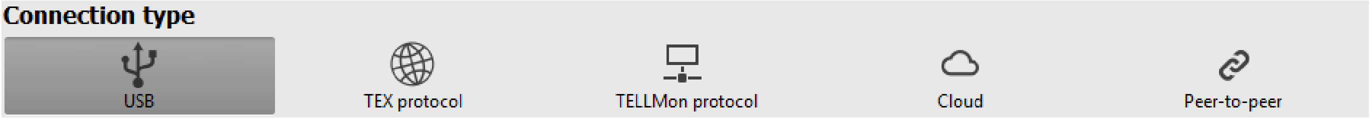
The user interface appearance can be changed using the “***Theme***” dropdown-menu found in the “***Software settings***” / “***Settings***” menu, where you can choose from various appearance themes.

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

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

4.2 Methods 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-B 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 ***Pager4*** device are in the same VPN or a private APN.

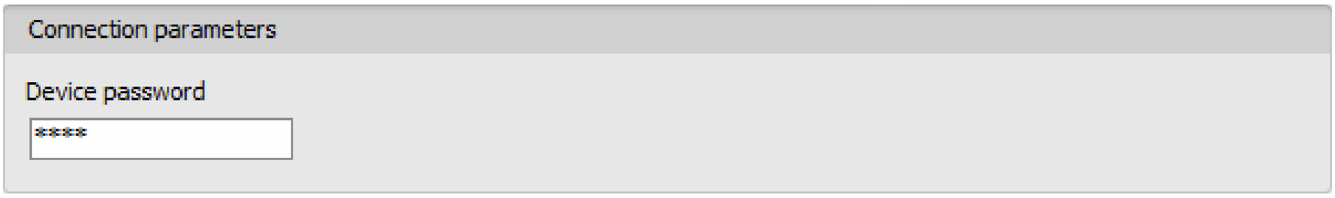
4.2.1 TELL servers and receivers

- **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).

4.2.2 Configuring directly via USB

To start programming the device, follow the instructions below:

- Open the ***Pager4*** 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-B 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, monitor system status, and perform controls.
- To close the connection, click on "***Disconnect***" ✗ button.

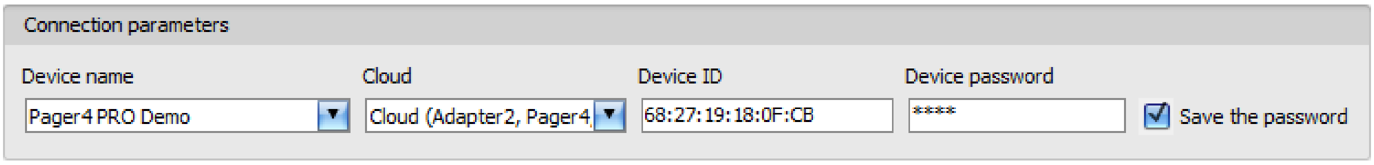
4.2.3 Remote connecting to devices via cloud service

This connection type can be used if the *Pager4* device is connected to the cloud. For this, the APN settings should be configured in the "*General*" settings menu, 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 **Pager4** 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	
Pager4 PRO Demo	Cloud (Adapter2, Pager4	68:27:19:18:0F:CB	****	☑ 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 **Pager4** 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 the configured and authorized user phone numbers. If the connecting request is sent from an unauthorized user phone number, or a number which is not configured in the device, the device password should be added in the message using the "**PWD**" parameter, as specified below. Commands sent from unauthorized phone numbers 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 request command for connecting to the server is: **∗CONNECT,PWD=***device password***#**

Using the "**PWD**" parameter is optional, according to the following:

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, or from ones which are configured, but for which other than the "***Accept - password not required***" option is assigned in the "***Incoming call and SMS handling***" section – such phone numbers are considered unauthorized, therefore in this case the password is required).

Example on the usage of the command mentioned above:

When sending from an authorized phone number: **∗CONNECT#**

When sending from an unauthorized phone number: **∗CONNECT,PWD=1234#**

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)

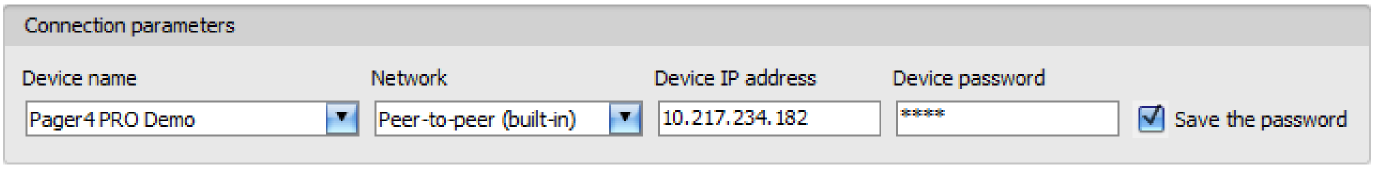
  ☁ connected (gray)
- After connecting using the valid password, you can configure the device, change settings, download event logs, monitor system status and perform controls.
- To disconnect from the device, click on the “***Disconnect***” ☁ button.

4.2.4 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 *Pager4* 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 should be configured in the device you wish to connect to. These settings are available in the "*General*" settings menu.
***For connecting directly to the WiFi product model from outside the local network, configuring port forwarding is required in your router, and the static WAN IP address of the router should be used in the software. The device uses port *6789* and *UDP* protocol. Otherwise, you can only access the device in the local network using its local IP address.**

With this connection type, a direct (peer-to-peer) connection will be established between the device and the **Pager4** 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	
Pager4 PRO Demo	Peer-to-peer (built-in)	10.217.234.182	****	☑ 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 (e.g., you can configure a different network name for the local and the remote connections of your WiFi 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. *For the **WiFi** product model you have to use the WAN IP address of the router to which the device is connected, if you want to connect to the device from outside the local network.

  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)

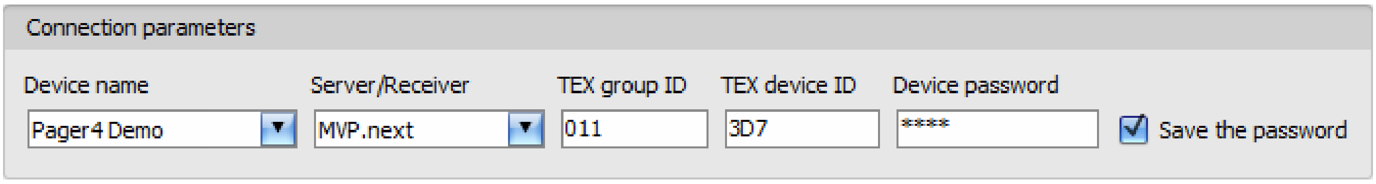
  connected (gray)
- After connecting using the valid password, you can configure the device, change settings, download event logs, monitor system status and perform controls.
- To disconnect from the device, click on the “***Disconnect***” button.

4.2.5 Remote connecting to devices which are using the TEX protocol

This connection type can be used if the *Pager4* 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 *Pager4* 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 ***Pager4*** 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	
Pager4 Demo ▼	MVP.next ▼	011	3D7	*****	☑ 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 **Pager4** 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 **Pager4** 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)

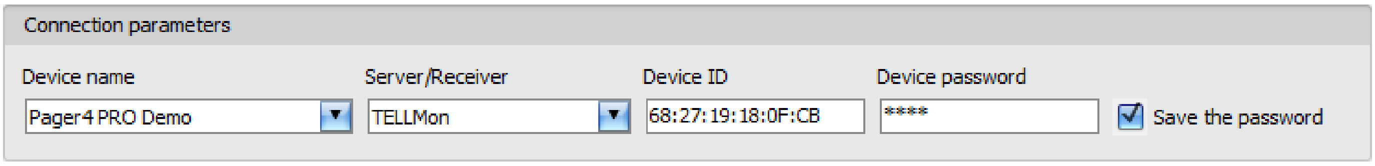
  connected (grey)
- After connecting using the valid password, you can configure the device, change settings, download event logs, monitor system status and perform controls.
- To disconnect from the device, click on the “***Disconnect***” button.

4.2.6 Remote connecting to devices which are using the TELLMon protocol

This connection type can be used if the *Pager4* 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 ***Pager4*** 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	
Pager4 PRO Demo	TELLMon	68:27:19:18:0F:CB	****	☑ 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 **Pager4** 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 *Pager4* 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 to 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:

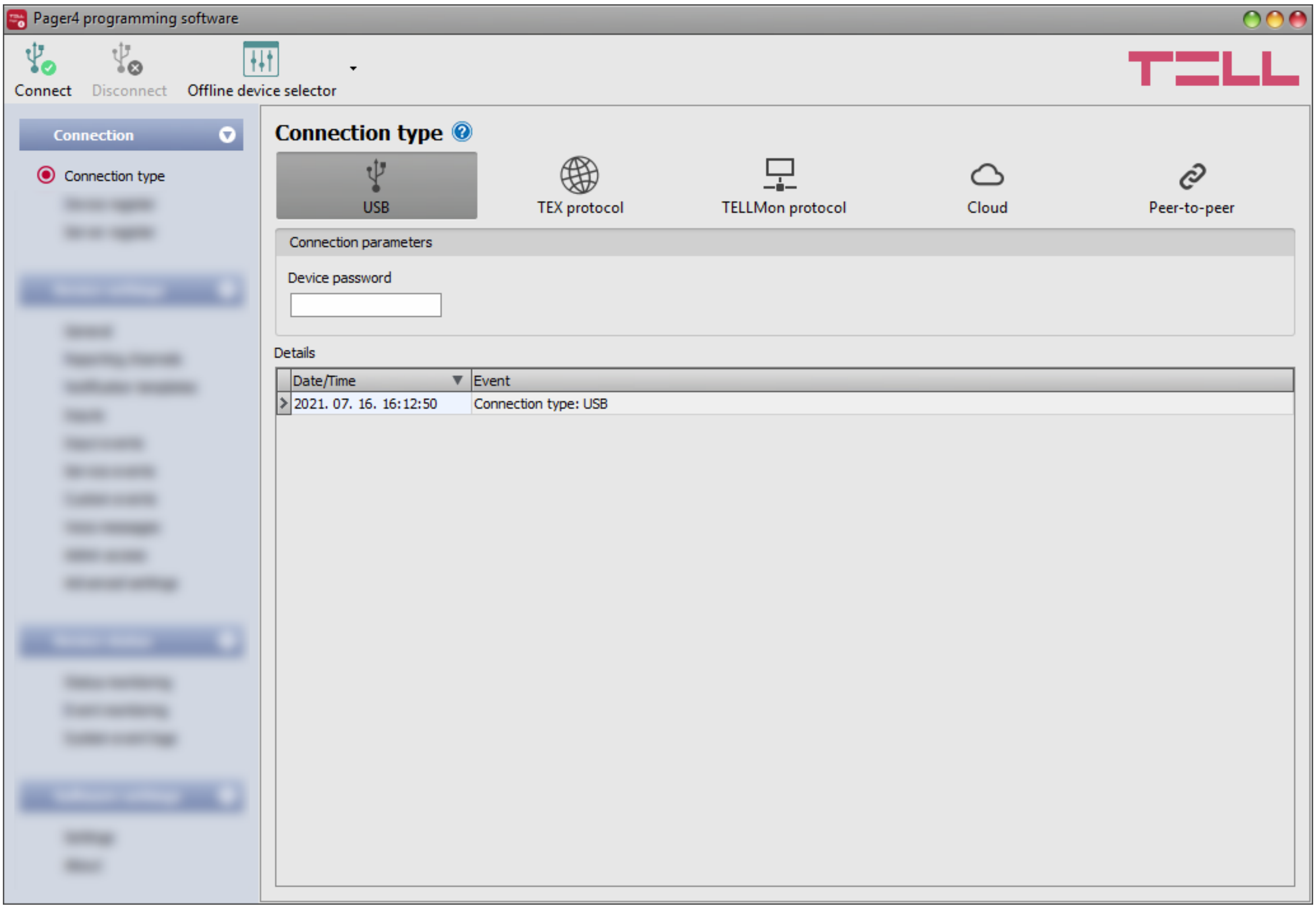
  disconnected (green)

  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.

5 Pager4 programming software usage and feature descriptions

5.1 Connection menu

5.1.1 Viewing the settings options and configuring offline



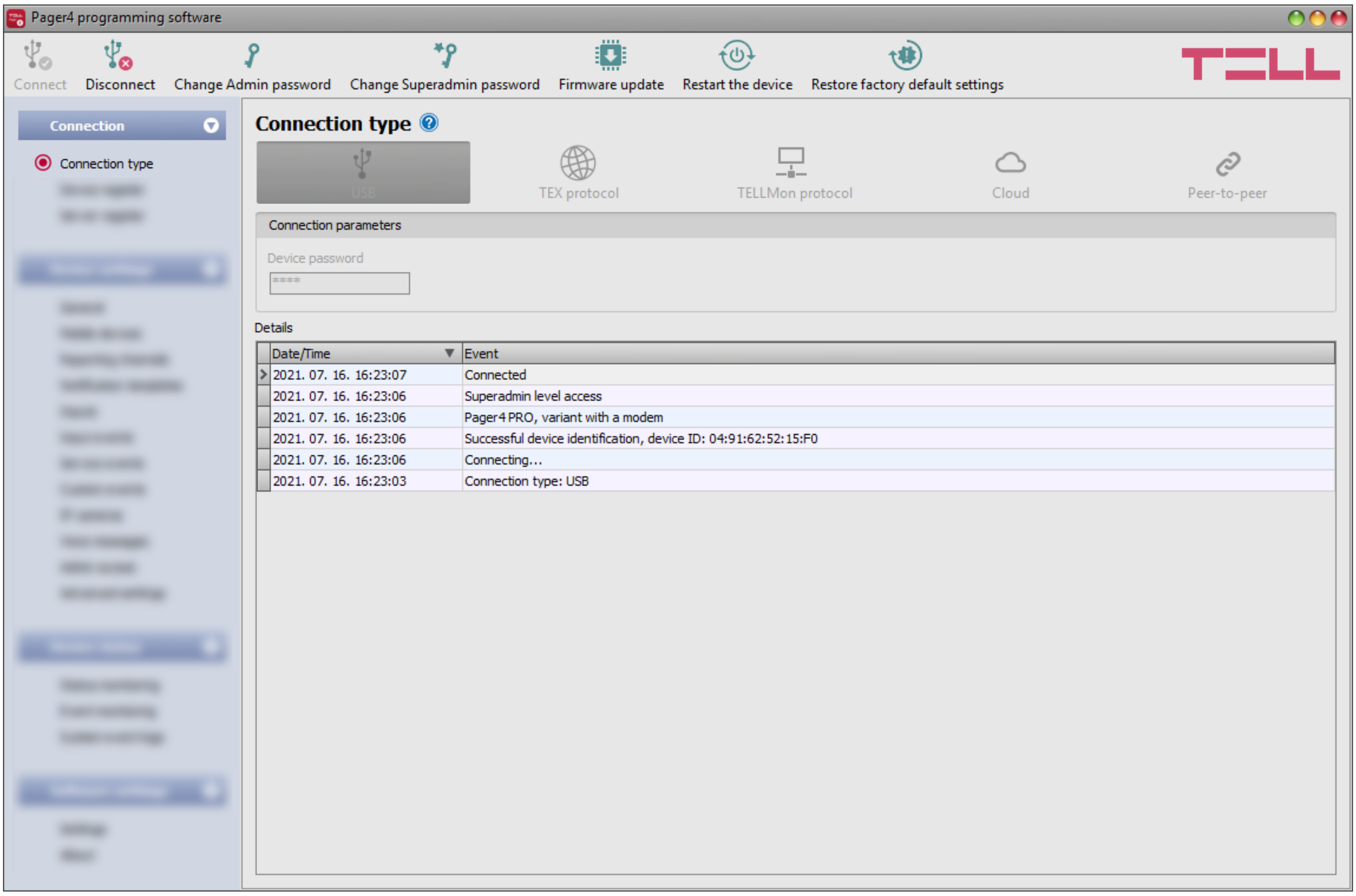
Date/Time	Event
2021. 07. 16. 16:12:50	Connection type: USB

The **Pager4** programming software supports all **Pager4** device models, therefore the software shows the settings and control options available specifically in a given device model, which are different from the common parameters (e.g. differences between the **PRO** and non **PRO**, or device models with a different number of inputs) only when connecting the given device model, i.e. a **Pager4** device has to 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 **Pager4** 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 **Pager4** device model, or to configure and save settings without connecting the device, click on the arrow found next to the "***Offline device selector***" button, select the desired device model from the drop-down menu and then click on the "***Offline device selector***" button to load the settings options of the selected device model.

5.1.2 Connection type



Connection type

Connection parameters

Device password: ****

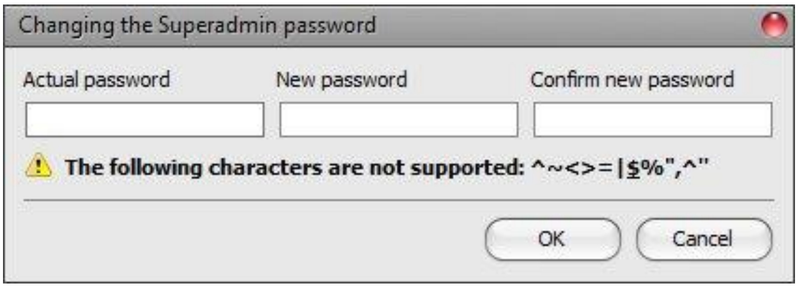
Details

Date/Time	Event
2021. 07. 16. 16:23:07	Connected
2021. 07. 16. 16:23:06	Superadmin level access
2021. 07. 16. 16:23:06	Pager4 PRO, variant with a modem
2021. 07. 16. 16:23:06	Successful device identification, device ID: 04:91:62:52:15:F0
2021. 07. 16. 16:23:06	Connecting...
2021. 07. 16. 16:23:03	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.

  Using this option, you can also update devices with a lower major firmware version (e.g. v6), which are not compatible basically with the latest software, but can be made compatible by updating.

- Restart the device:

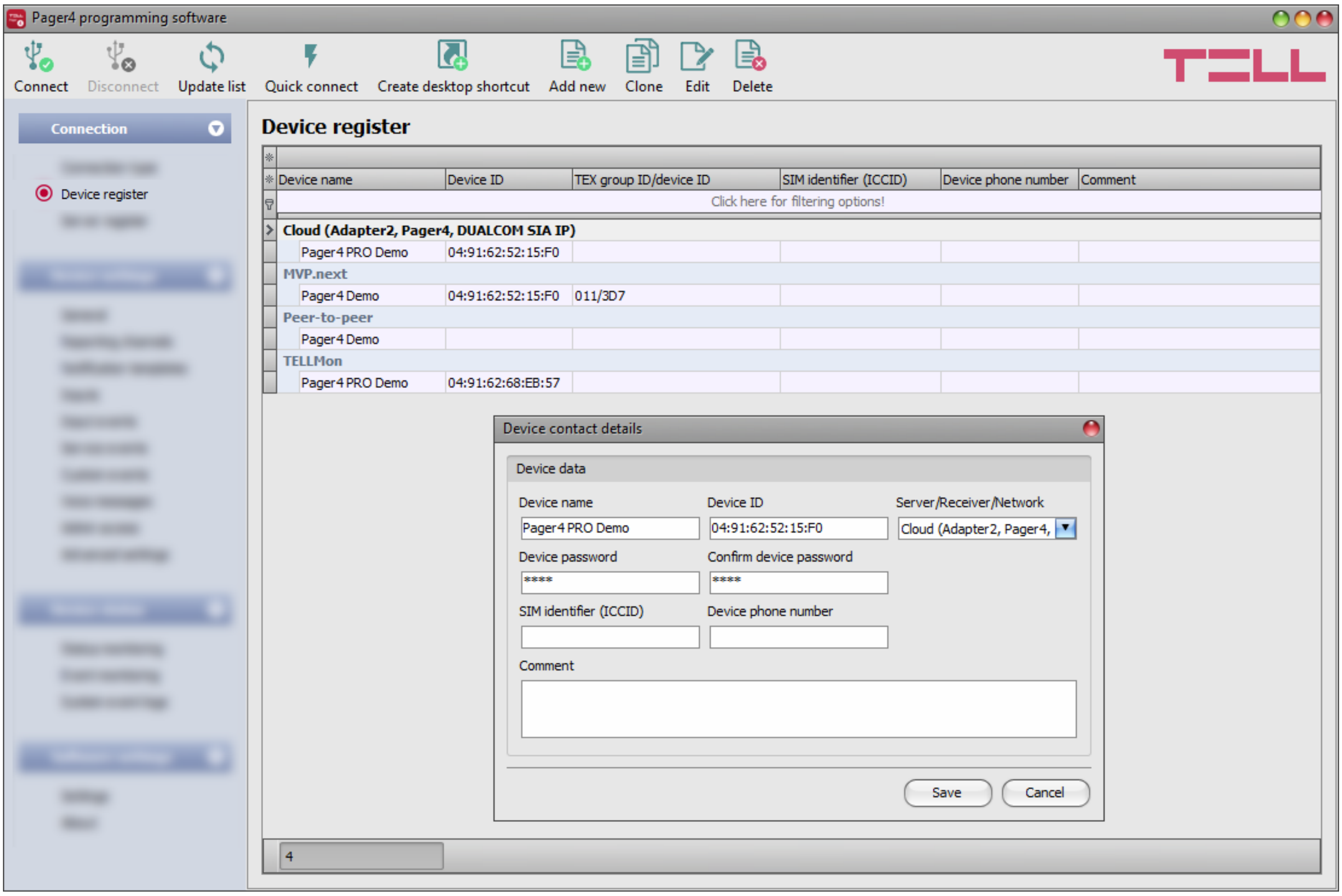
  If needed, you can restart the connected device by clicking on this button.

- 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. A factory reset can also be performed using the microswitch found on the hardware. Further details about this you can find in chapter “***Restoring the factory default settings***”.
  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.

5.1.3 Device register



Device register

Device name	Device ID	TEX group ID/device ID	SIM identifier (ICCID)	Device phone number	Comment
Cloud (Adapter2, Pager4, DUALCOM SIA IP)					
Pager4 PRO Demo	04:91:62:52:15:F0				
MVP.next					
Pager4 Demo	04:91:62:52:15:F0	011/3D7			
Peer-to-peer					
Pager4 Demo					
TELLMon					
Pager4 PRO Demo	04:91:62:68:EB:57				

Device contact details

Device data

Device name: Pager4 PRO Demo
Device ID: 04:91:62:52:15:F0
Server/Receiver/Network: Cloud (Adapter2, Pager4,
Device password: ****
Confirm device password: ****
SIM identifier (ICCID):
Device phone number:
Comment:

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 which is included in the setup of the **Pager4** programming software.

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 insert 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. You can use this option e.g., for separating the records used for remote access and access in the local network for WiFi devices. 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: for devices with a modem, this is 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! For a WiFi device, this is the static WAN IP address of the router to which the device is connected, or the local IP address of the device, in case that you want to access the device in the local network only. If the device is connected via USB, and the SIM card is installed (for devices with a modem), 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 insert the data in this field, when you add a record with new device contact details. Otherwise, you can also enter the IP address manually.

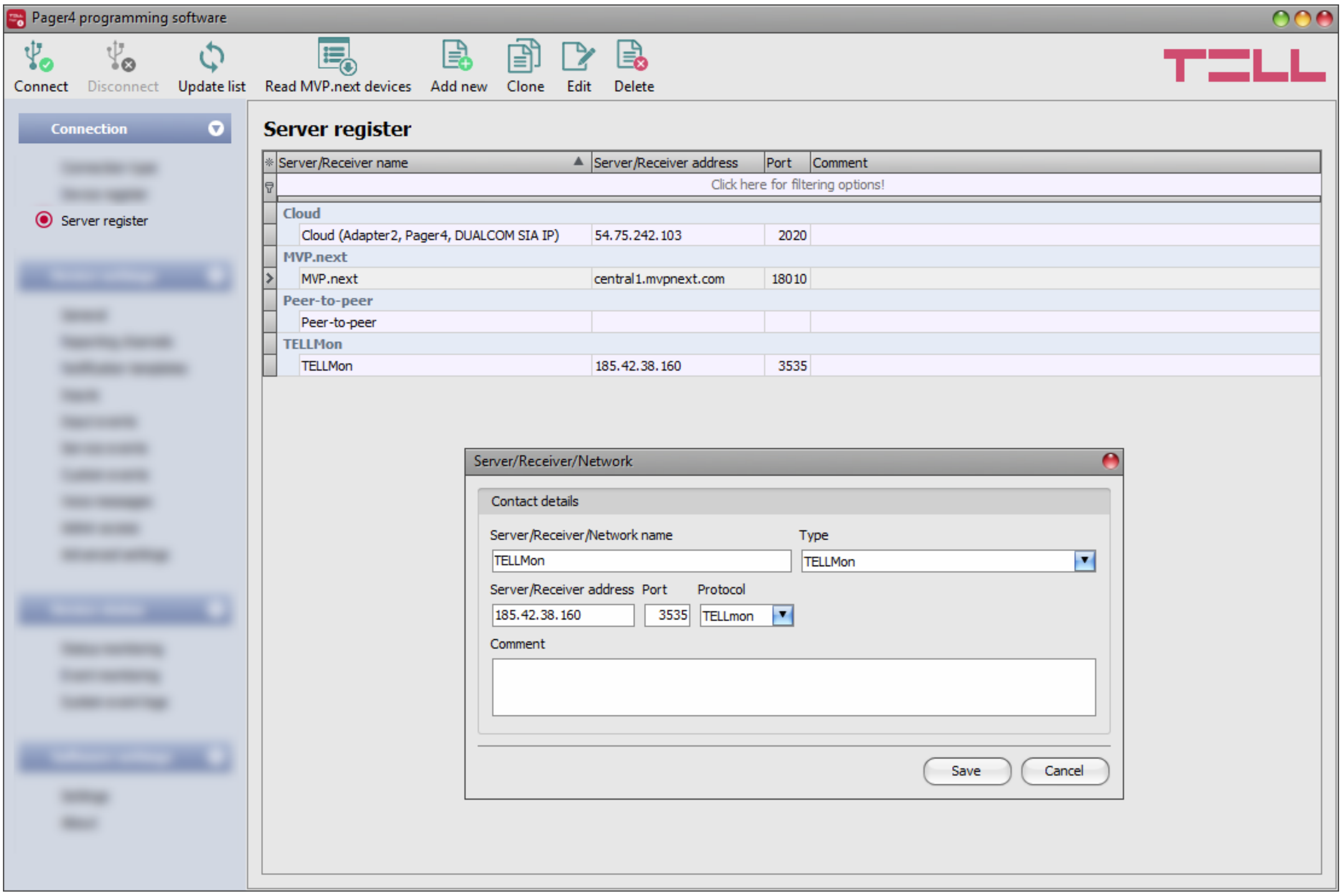
Device password/Confirm device password: the superadmin or admin password configured in the given device, depending on which one you want to use for connecting to the device.

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 insert 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.

5.1.4 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	central1.mvpnext.com	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. You can use this option e.g., for separating the records used for remote access and access in the local network for WiFi devices. 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).

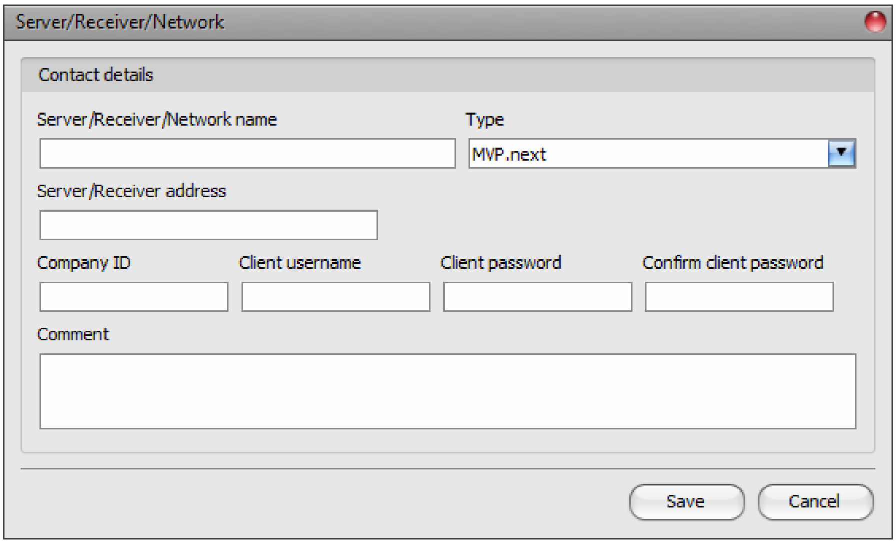
Comment: in this field you can enter custom comments related to the given server, receiver, or network.

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).

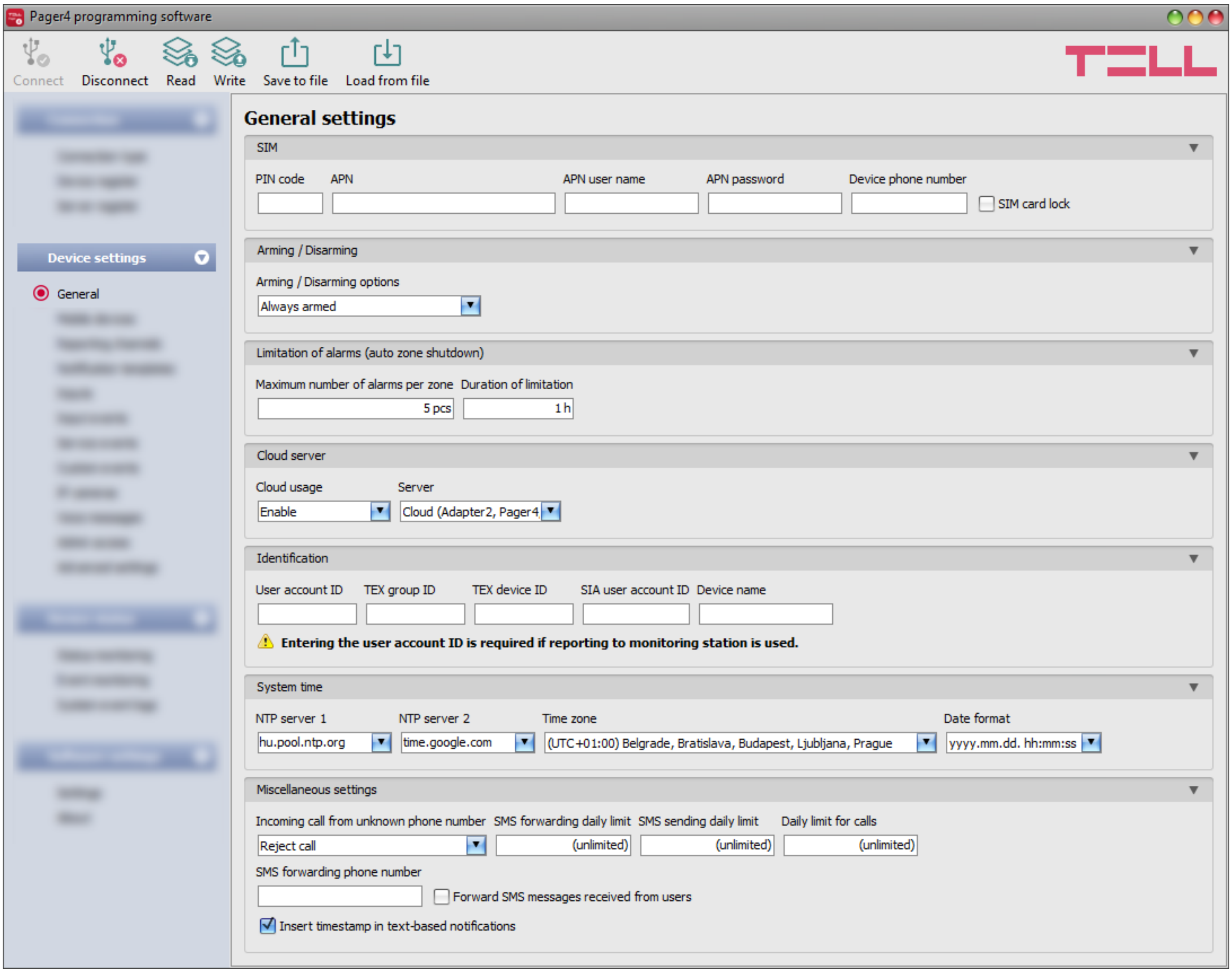
Attention! You can use the registered client username and password in any other programming software that supports the MVP.next, but you can connect to the server with one software only at the same time, using the same username. If you want to use more than one programming software simultaneously, you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

5.2 Device settings menu

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

- **Changing the device settings**: To change the device settings, first you must read the actual settings from the device by clicking on the “***Read***” button in any submenu in the “***Device settings***” menu. Writing the 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.

5.2.1 General



General settings

SIM

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

Arming / Disarming

Arming / Disarming options: Always armed

Limitation of alarms (auto zone shutdown)

Maximum number of alarms per zone: 5 pcs
Duration of limitation: 1 h

Cloud server

Cloud usage: Enable
Server: Cloud (Adapter2, Pager4

Identification

User account ID:
TEX group ID:
TEX device ID:
SIA user account ID:
Device name:

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

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
Date format: yyyy.mm.dd. hh:mm:ss

Miscellaneous settings

Incoming call from unknown phone number: Reject call
SMS forwarding daily limit: (unlimited)
SMS sending daily limit: (unlimited)
Daily limit for calls: (unlimited)
SMS forwarding phone number:
□ Forward SMS messages received from users
☑ Insert timestamp in text-based notifications

In this section 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.

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: the access point name necessary to connect to the Internet. Ask this from the mobile service provider of the SIM card installed in the device. If no APN is configured, the device will not try to connect to the Internet. In this case you can only use the functions which do not require Internet connection, such as voice calls and SMS sending.

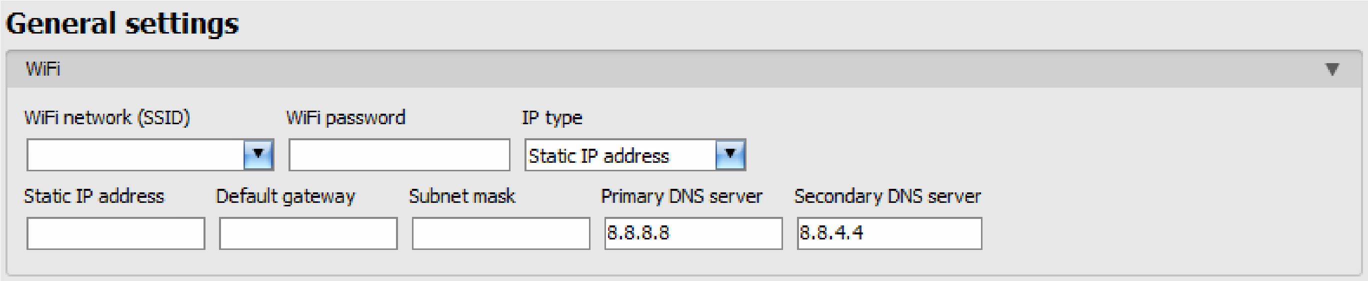
APN user name: a user name is necessary only if the mobile service provider provides this and requires its usage for the given APN.

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.

WiFi (WiFi model only)**:**



General settings

WiFi

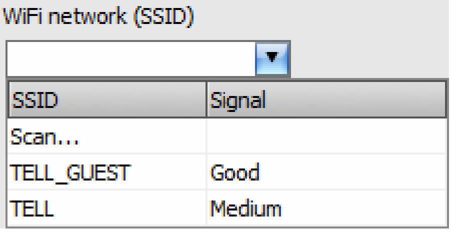
WiFi network (SSID)	WiFi password	IP type
		Static IP address

Static IP address	Default gateway	Subnet mask	Primary DNS server	Secondary DNS server
			8.8.8.8	8.8.4.4

WiFi settings are available in the "***General***" device settings menu when you connect the ***WiFi*** product model.

Configuring the WiFi settings:

- Read the settings from the device by clicking on the "***Read settings***" button.
- Select the "***Scan…***" option in the "***WiFi network (SSID)***" drop-down menu to start scanning available WiFi networks. The network scan assistant will guide you through the scan process.
(If you know the name of the network you want to use, you can either enter the network name and the WiFi password directly in the "***WiFi network (SSID)***" and "***WiFi password***" fields without running a network scan, or run a network scan and select the network and provide the password along the scan process in the assistant.)



WiFi network (SSID)

SSID	Signal
Scan…	
TELL_GUEST	Good
TELL	Medium

- Check the signal of the given network and move the antenna of the device in a better place if necessary.
- If you want to use a static IP instead of DHCP, configure the further network settings too in the "***WiFi***" section.
- Write the changes into the device by clicking on the "***Write settings***" button.

WiFi settings:

WiFi network (SSID): scan available WiFi networks and select the network you want to use.

WiFi password: you can enter the password of the selected WiFi network in this field.

IP type:

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

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

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

Default gateway: the default gateway IP address.

Subnet mask: the applied subnet mask.

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

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

Arming / Disarming:

Arming / Disarming options: the device can also be used as a standalone alarm control device and can be armed/disarmed using dry contacts on inputs or remotely by phone call or SMS, or by using the arming/disarming controls in the programming software. For arming/disarming by dry contacts you can use any accessory which has dry contact outputs, e.g., access control keypad, card reader, RF remote controller, key switch or a simple switch, pushbutton, etc.
To make it possible to use the device according to the demands, different arming/disarming options are available:

- **Always armed**: choose this control mode if you do not wish to arm and disarm the device, but the inputs should always be armed, events should be generated and notifications should be sent when activated. In this case arming and disarming will not be available and all inputs will act as 24h zones.
- **Bistable contact**: choose this control mode if you wish to arm and disarm the device using a toggle switch or relay output (open or closed). This control mode uses input IN4 (for the IN4.R2 model) or input IN6 (for the IN6.R1 model), which in this case can be used for arming/disarming only. When input IN4/IN6 is active, the device will be armed, and when inactive, the device will be disarmed. Assigning the open/closed state of the dry contact to the active/inactive state of the input can be done by configuring the input type (normally open or normally closed) for the given input (IN4/IN6).
For normally open (NO): open=inactive=device disarmed, closed=active=device armed.
For normally closed (NC): open=active=device armed, closed=inactive=device disarmed.
Since the state of the dry contact defines the armed/disarmed status, therefore remote arming and disarming is not available for this control mode.
- **Impulse on one input**: choose this control mode if you wish to arm and disarm the device by dry contact impulses (e.g., pushbutton, or monostable relay output) using up one input. This control mode uses input IN4 (for the IN4.R2 model) or input IN6 (for the IN6.R1 model), which in this case can be used for arming/disarming only. The device will become armed when input IN4/IN6 is activated shortly (impulse), then it will become disarmed upon next short activation of the same input. Assigning the open/closed state of the dry contact to the active/inactive state of the input can be done by configuring the input type (normally open or normally closed) for the given input (IN4/IN6).
For normally open (NO): open=inactive, closed=active.
For normally closed (NC): open=active, closed=inactive.
Remote arming and disarming are also available for this control mode.
- **Impulse on two inputs**: choose this control mode if you wish to arm and disarm the device by dry contact impulses (e.g., pushbuttons, or monostable relay outputs) using up two inputs. This control mode uses inputs IN3 and IN4 (for the IN4.R2 model) or inputs IN5 and IN6 (for the IN6.R1 model), which in this case can be used for arming/disarming only. The device will become armed when input IN3/IN5 is activated shortly (impulse), then it will become disarmed when input IN4/IN6 is activated shortly. Assigning the open/closed state of the dry contact to the active/inactive state of the inputs can be done by configuring the input type (normally open or normally closed) for the given inputs (IN3/IN5 and IN4/IN6).
For normally open (NO): open=inactive, closed=active.
For normally closed (NC): open=active, closed=inactive.
Remote arming and disarming are also available for this control mode.
- **Remote arming/disarming only**: choose this control mode if you wish to use all inputs for custom notifications. In this case, the device cannot be armed and disarmed locally through the inputs. Arming and disarming can only be done remotely by phone call, SMS, or by using the arming/disarming controls in the programming software.

Limitation of alarms (auto zone shutdown):

Maximum number of alarms per zone (1 to 100pcs): in this section you can configure the maximum number of alarms (activation events) to be accepted from one input. This makes it possible to avoid a faulty detector connected to an input to generate alarms and notifications continuously. If the number of alarm events generated by an input reaches the value configured here, the given input will become restricted, and the device will ignore further activation events of the given input.
If the arming/disarming settings are not configured to “***Always armed***”, disarming and rearming the device will re-enable the restricted input, then alarm events will be accepted again from the given input, but again only the number of alarm events configured. If the arming/disarming settings are configured to “***Always armed***”, or the “***24h zone***” option is enabled for the given input, the restricted input will be re-enabled automatically when the time configured at the “***Duration of limitation***” option expires. The restriction only applies to inputs for which the “***Auto shutdown***” option is enabled.

Duration of limitation (1 to 24h): in this section you can configure how long the device should ignore an input which has reached the limitation value entered at "***Maximum number of alarms per zone***" option. When this period expires, the alarm counter will be reset automatically, and the input will be enabled again. This setting only applies to inputs for which both the “***Auto shutdown***” and “***24h zone***” option is enabled, or to any input for which the “***Auto shutdown***” option is enabled, if the arming/disarming settings are configured to „***Always armed***”.

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, control and 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.
The cloud usage cannot be disabled in the ***WiFi*** product model.

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.

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 **Pager4** device. For the **PRO** model, 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.

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.

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

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

Miscellaneous settings:

Incoming call from unknown phone number: in this section you can configure what the device should do upon a phone call received from a phone number which is not configured in the device as a user phone number, or a call received with hidden caller ID. You can configure the device to accept or reject these calls. In case of receiving the call, remote control and status query can be performed after providing the device password. Independently of the selected option, receiving a call from an unknown phone number also generates a service event, which you can configure separately to control the output(s) or send notifications.

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.

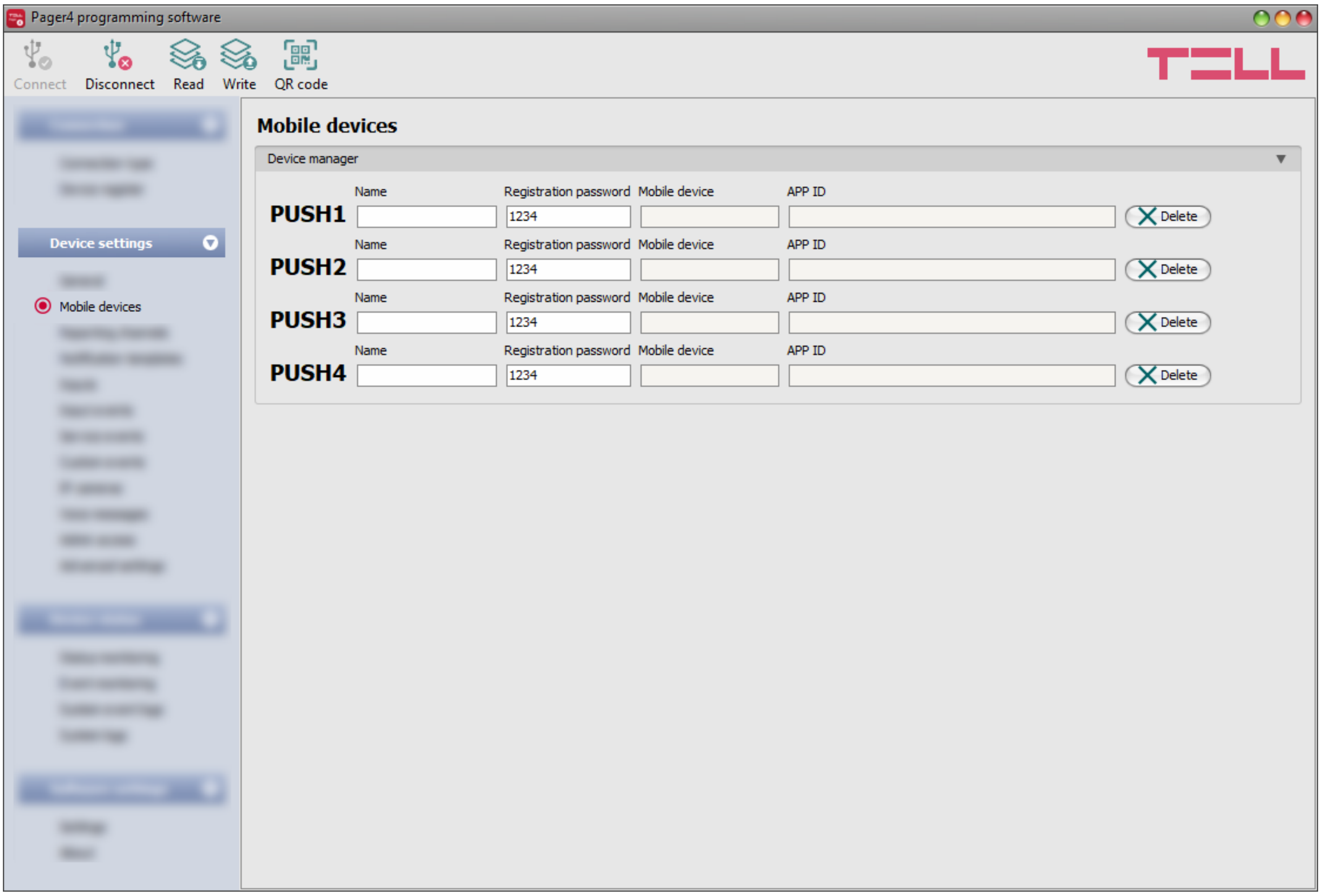
Daily limit for calls: with this setting you can limit the number of voice calls generated by events. When the configured limit is reached, the device will not make further event-generated calls for 24 hours. After 24 hours the call counter resets automatically, and voice calls will be enabled again 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 timestamp in text-based notifications: if this option is enabled, the device will insert the timestamp in each text message at the beginning, which indicates the time of occurrence of the given event. You can select the date format for the time stamp in the "***System time / Date format***" section.

5.2.2 Mobile devices (Pager4 PRO only)



Mobile devices

Device manager

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

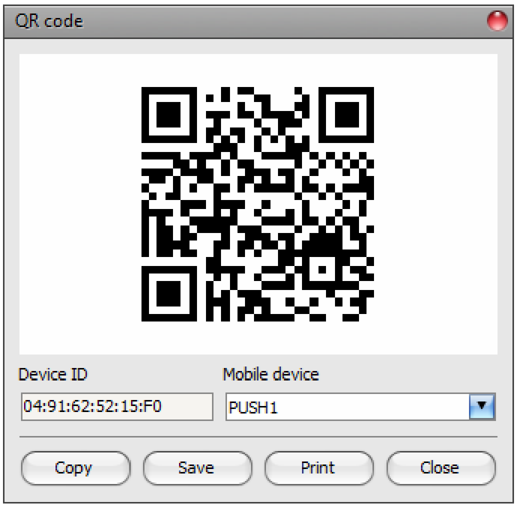
In this menu you can manage the access of mobile applications. The device supports access of up to 4 mobile devices, for which you can configure here the registration password requested upon assigning the mobile application to the device, and it is also possible to delete a mobile device if needed, i.e., to cancel its assignment/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).



Device ID: 04:91:62:52:15:F0

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 ***Pager4*** device, receiving alerts from the device will become available through Push notification too. For this, when configuring events, you can select which of the maximum 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 upon selecting the notification channels when configuring events. The name should not be longer than 50 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

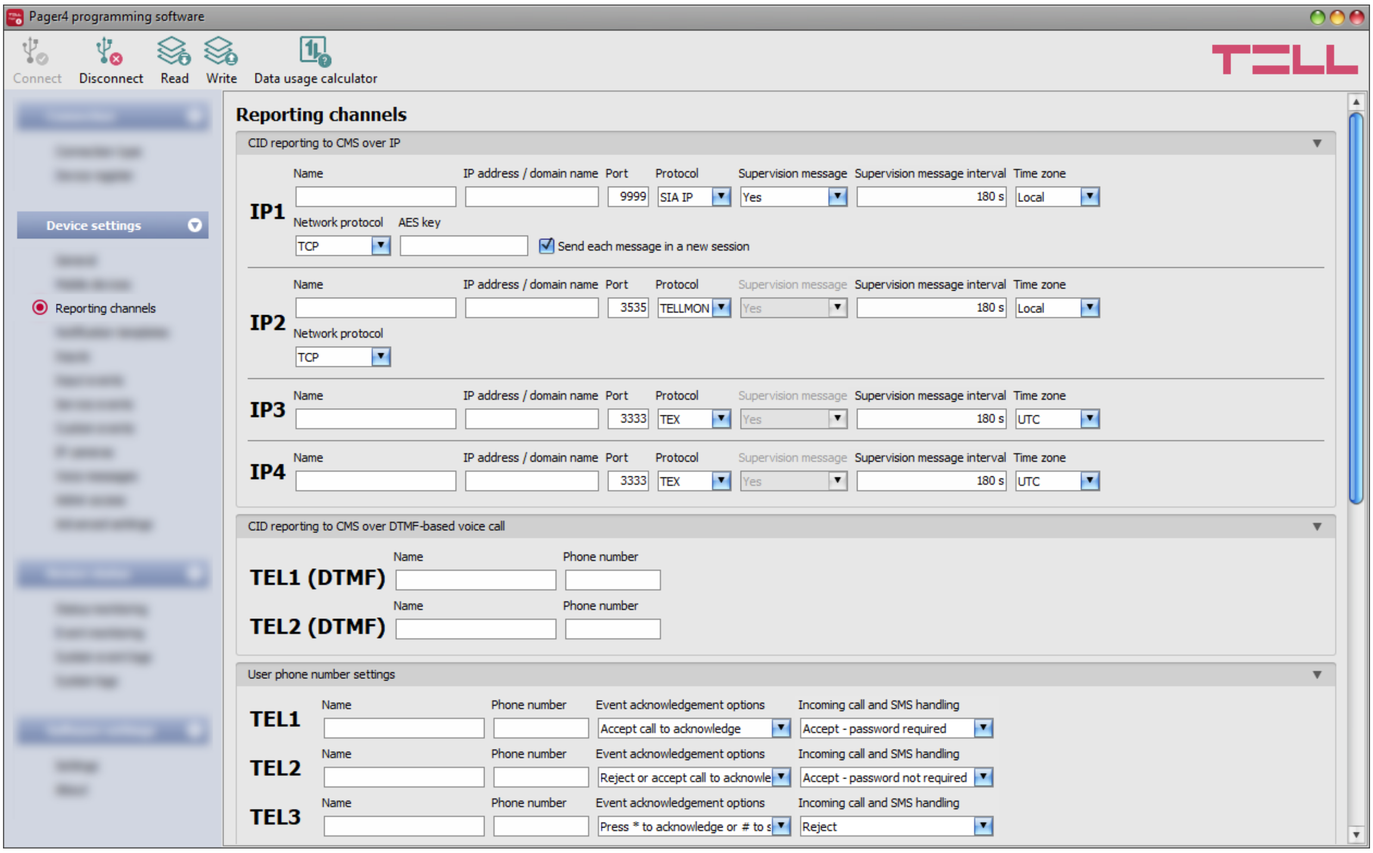
Registration password: the registration password must be provided in the mobile application when you wish to assign it to the device. This password can be configured in this section separately for each mobile device to be assigned. The registration password length is 4 to 8 characters and only letters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

Mobile device: this field shows the name of the given device already assigned, which is read by the mobile application from the mobile device, therefore this name cannot be changed in the programming software.

APP ID: this field shows the identifier of the given assigned mobile device. 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 assignment/registration. In case of deleting a mobile device, the application used on the given device will no longer have access to the ***Pager4*** device.

5.2.3 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			9999	SIA IP	Yes	180 s	Local
IP2			3535	TELLMON	Yes	180 s	Local
IP3			3333	TEX	Yes	180 s	UTC
IP4			3333	TEX	Yes	180 s	UTC

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

IP2: Network protocol: TCP

CID reporting to CMS over DTMF-based voice call

	Name	Phone number
TEL1 (DTMF)		
TEL2 (DTMF)		

User phone number settings

	Name	Phone number	Event acknowledgement options	Incoming call and SMS handling
TEL1			Accept call to acknowledge	Accept - password required
TEL2			Reject or accept call to acknowle	Accept - password not required
TEL3			Press * to acknowledge or # to s	Reject

In this section you can configure all availabilities where reports and notifications should be sent, such as CMS servers and receivers, user phone numbers for calls and SMS sending, and e-mail addresses for notification by e-mail in case of using the ***Pager4 PRO*** model.

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 as follows.

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. The name should not be longer than 35 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

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.

CID reporting to CMS over DTMF-based voice call:

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.

You can configure up to 2 DTMF receiver phone numbers (**TEL1 DTMF** and **TEL2 DTMF**) as follows.

Name: CMS DTMF receiver name. The name entered in this section is used for identification of the receiver within the program, and the program will also use this name when configuring notification templates. The name should not be longer than 50 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Phone number: the phone number of the DTMF receiver.

User phone number settings:

You can configure up to 10 user phone numbers (**TEL1** to **TEL10**) for voice calls, SMS sending and remote control by SMS and calls. **Notification of users via voice call is not necessarily done in the same order as the phone numbers are recorded in the software.**

Name: user name. The name entered in this section will be used upon selecting the notification channels when configuring events. The name should not be longer than 50 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Phone number: user phone number.

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 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. In order 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 and SMS handling: in this section you can configure for each user separately how the device should handle calls and SMS commands received from the given user. Independently of the chosen option, receiving a call from a user phone number will also generate a service event, which you can configure separately to control the output(s) or send notifications.

Available options:

- **Accept - password required**: the device accepts the call which it confirms by a short signal tone, and then the password should be entered to accept commands. The superadmin and admin passwords are both accepted. The user needs to enter the valid password using the phone's keys as follows: **∗9*device password*#** (e.g., **∗91234#**). If the valid password has been entered, the device confirms this by three short signal tones, otherwise a long signal tone will be emitted. If the command is wrong (missing **∗** or #), no signal tone will be emitted. After the password has been accepted, the caller can use commands as specified in the list of DTMF commands. The device will also identify the user's phone number by CLIP service, which makes it possible to perform further actions automatically upon receiving the call. For this, an "***incoming call from user***" event should be configured for the given phone number at the service events.
  SMS commands will only be accepted if the valid device password is included in the message.
- **Accept - password not required**: the device accepts the call which it confirms by a short signal tone, and then commands can be used as specified in the list of DTMF commands, without the need of entering the password. The device will also identify the user's phone number by CLIP service, which makes it possible to perform further actions automatically upon receiving the call. For this, an "***incoming call from user***" event should be configured for the given phone number at the service events.
  SMS commands will also be accepted without including the valid device password in the message.
- **Reject**: the device will reject calls received from the given user phone number but will identify the phone number by CLIP service for further actions, which are available by configuring an "***incoming call from user***" event for the given phone number at the service events. By rejecting the calls, the configured actions can be performed free of charge (except if the given GSM service provider applies a charge for rejected calls as well).
  SMS commands will only be accepted if the valid device password is included in the message.

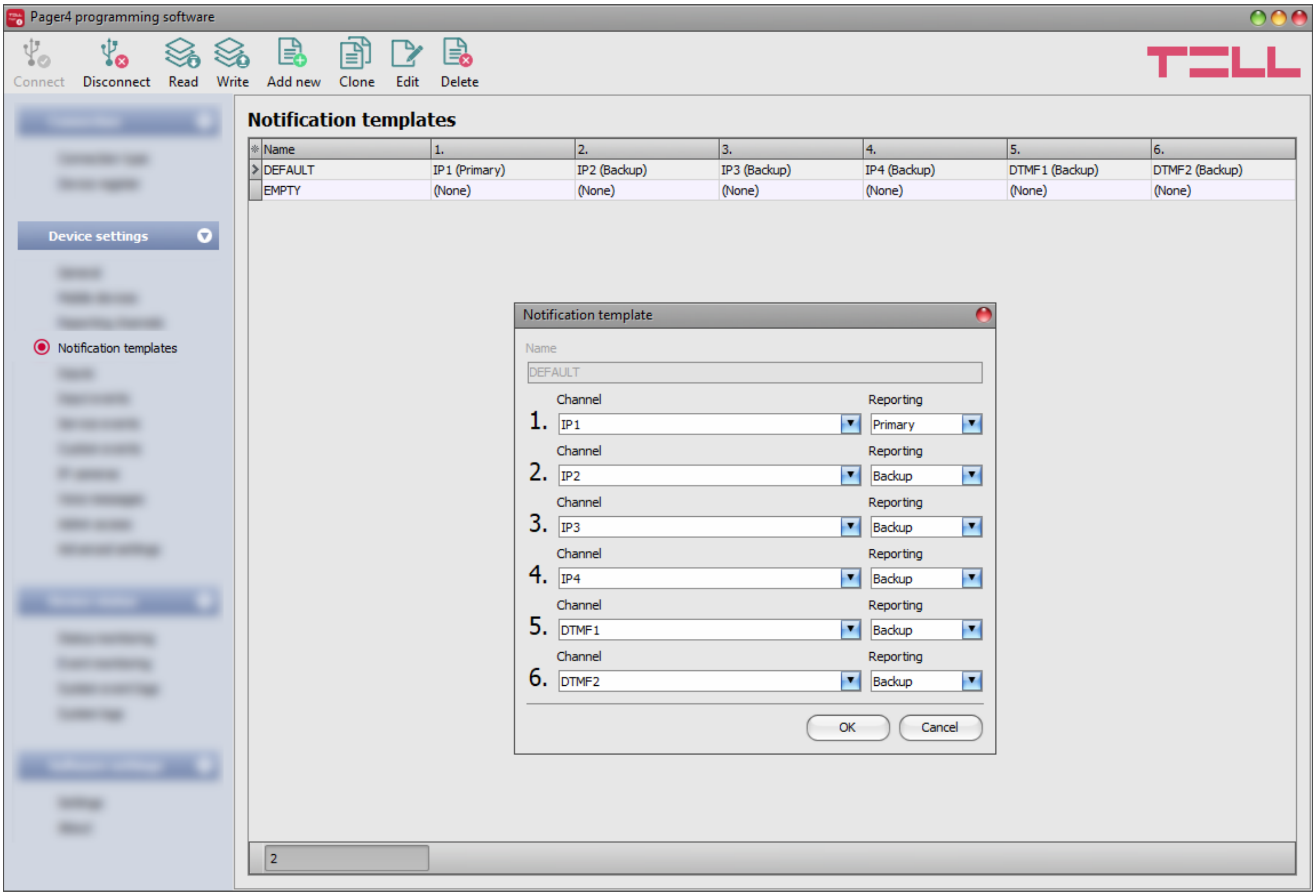
E-mail notification recipients (Pager4 PRO only**):**

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. The name should not be longer than 50 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

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

5.2.4 Notification templates



Notification templates

Name	1.	2.	3.	4.	5.	6.
DEFAULT	IP1 (Primary)	IP2 (Backup)	IP3 (Backup)	IP4 (Backup)	DTMF1 (Backup)	DTMF2 (Backup)
EMPTY	(None)	(None)	(None)	(None)	(None)	(None)

2

Notification template

Name: DEFAULT

	Channel	Reporting
1.	IP1	Primary
2.	IP2	Backup
3.	IP3	Backup
4.	IP4	Backup
5.	DTMF1	Backup
6.	DTMF2	Backup

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 "***EMPTY***" and "***DEFAULT***", which cannot be deleted, but their configuration can be changed if needed. If you wish to add new notification templates, this should be done 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 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.

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:

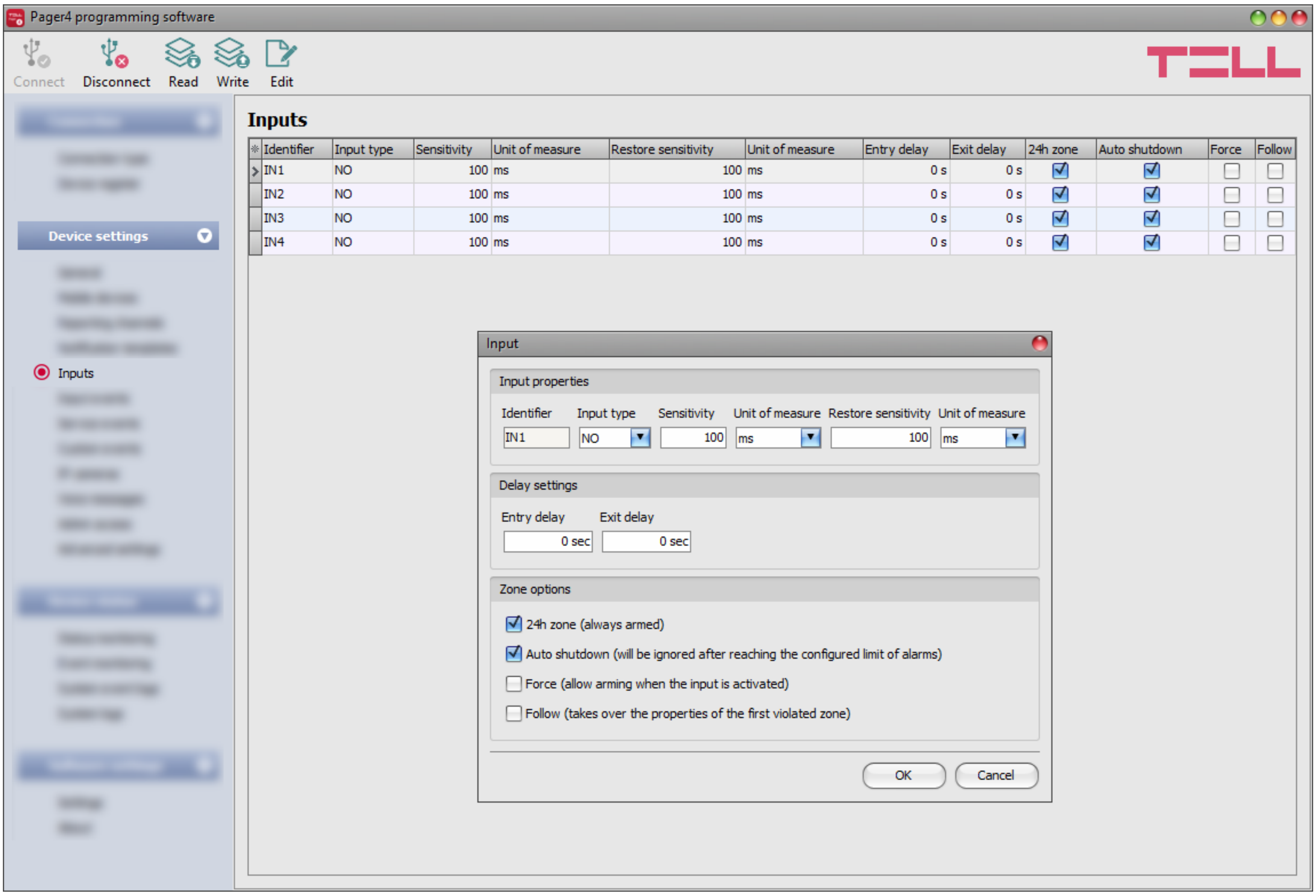
- Reading the settings from the device:
  To read the settings from the device, click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new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

5.2.5 Inputs



Inputs

Identifier	Input type	Sensitivity	Unit of measure	Restore sensitivity	Unit of measure	Entry delay	Exit delay	24h zone	Auto shutdown	Force	Follow
IN1	NO	100	ms	100	ms	0 s	0 s	☑	☑	□	□
IN2	NO	100	ms	100	ms	0 s	0 s	☑	☑	□	□
IN3	NO	100	ms	100	ms	0 s	0 s	☑	☑	□	□
IN4	NO	100	ms	100	ms	0 s	0 s	☑	☑	□	□

Input

Input properties

Identifier	Input type	Sensitivity	Unit of measure	Restore sensitivity	Unit of measure
IN1	NO	100	ms	100	ms

Delay settings

Entry delay	Exit delay
0 sec	0 sec

Zone options

☑ 24h zone (always armed)

☑ Auto shutdown (will be ignored after reaching the configured limit of alarms)

□ Force (allow arming when the input is activated)

□ Follow (takes over the properties of the first violated zone)

OK Cancel

In this menu you can configure the properties and options of the dry contact inputs.

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 input settings:
  To edit the settings of the selected input, click on the "***Edit***" button.

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

Input properties:

Identifier: the identifiers of the inputs cannot be changed. They are used for identification of the inputs in the program.

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/IN6**) and the **V-** terminal (DC power negative) becomes closed.
When set to **NC**, an input event will be generated when the closed contact between the given input (**IN1**…**IN4/IN6**) and the **V-** terminal (DC power negative) becomes open.

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).

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).

Delay settings:

Entry delay: in this section you can configure the time available to disarm the device after violating the given zone. The device ignores state changes of the given input for the time of the entry delay, so input event will not be generated until the time expires. If the time expires and the system is still armed, an input event will be generated. The entry delay can be configured in seconds.

Exit delay: in this section you can configure the time for which state changes of the given input will be ignored after arming the device. If the given zone is violated during the exit delay, input event will not be generated. The exit delay can be configured in seconds.

Zone options:

24h zone: if this option is enabled, the given input becomes armed continuously and does not disarm when the device is disarmed. State changes of the given input will generate input events even if the device is disarmed.

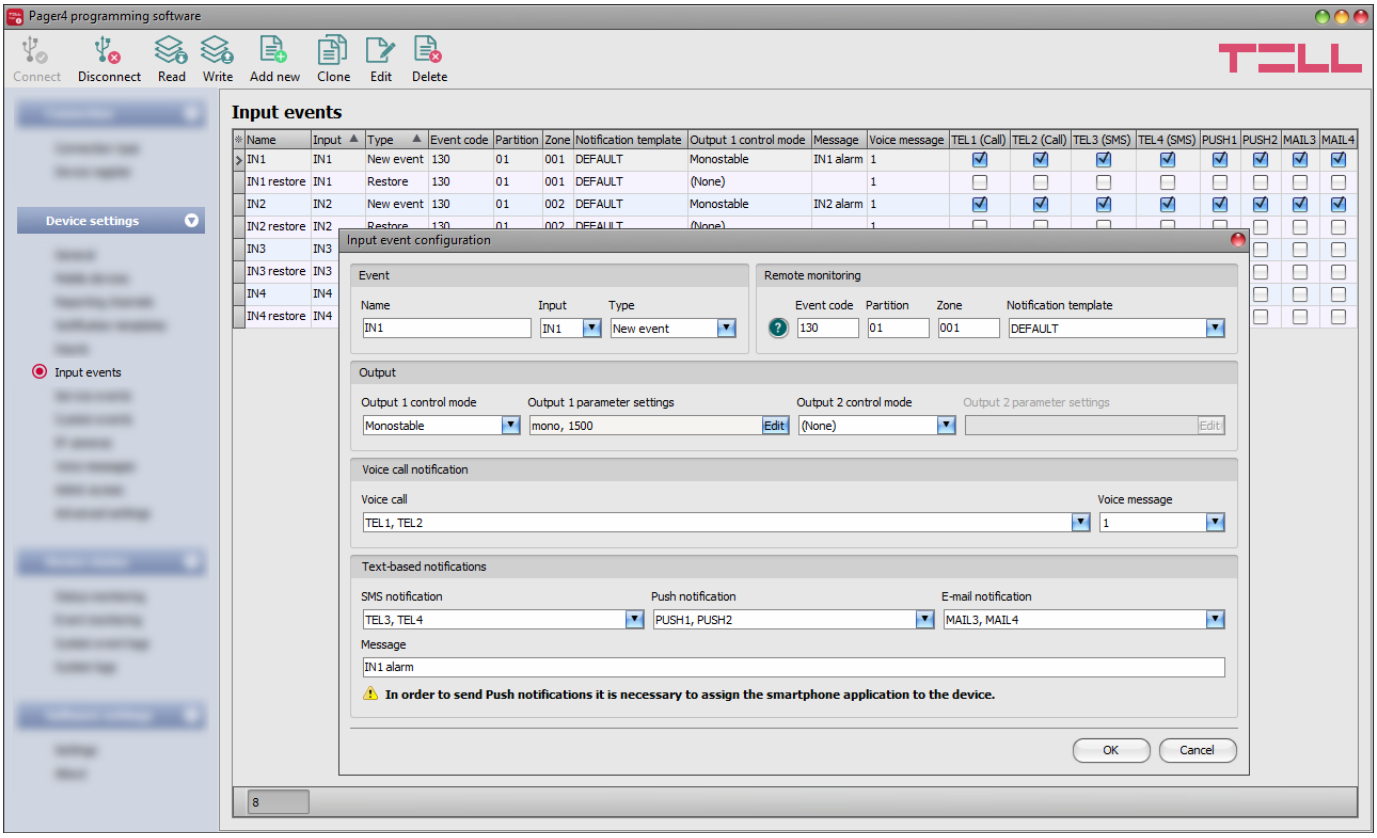
Auto shutdown: if this option is enabled, generating events by the given input will be limited according to the "***Limitation of alarms***" settings in the "***General***" settings menu. The device will ignore state changes of the given input after the number of events generated by it reaches the configured limit. For further details please read the specification of the mentioned settings. If disabled, the given input can generate unlimited number of events.

Force: if this option is enabled the device will ignore the state of the given input upon arming. If the given input is activated upon arming the device, it will become armed after it restores. If this option is disabled, arming will be forbidden if the given input is activated.

Follow: if this option is enabled, the given input will take over the properties (entry delay, instant) of the first violated zone (input) after arming. If entry delay is configured for the first violated zone, the follow zone will use the same entry delay, or if the first violated zone is instant (no entry delay is configured for the given zone), the follow zone will be instant too.

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

5.2.6 Input events



Input events

Name	Input	Type	Event code	Partition	Zone	Notification template	Output 1 control mode	Message	Voice message	TEL1 (Call)	TEL2 (Call)	TEL3 (SMS)	TEL4 (SMS)	PUSH1	PUSH2	MAIL3	MAIL4
IN1	IN1	New event	130	01	001	DEFAULT	Monostable	IN1 alarm	1	☑	☑	☑	☑	☑	☑	☑	☑
IN1 restore	IN1	Restore	130	01	001	DEFAULT	(None)		1	□	□	□	□	□	□	□	□
IN2	IN2	New event	130	01	002	DEFAULT	Monostable	IN2 alarm	1	☑	☑	☑	☑	☑	☑	☑	☑
IN2 restore	IN2	Restore	130	01	002	DEFAULT	(None)		1	□	□	□	□	□	□	□	□
IN3	IN3														□	□	□
IN3 restore	IN3														□	□	□
IN4	IN4														□	□	□
IN4 restore	IN4														□	□	□

Input event configuration

Event

Name: IN1
Input: IN1
Type: New event

Remote monitoring

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

Output

Output 1 control mode: Monostable
Output 1 parameter settings: mono, 1500 [Edit]
Output 2 control mode: (None)
Output 2 parameter settings: [Edit]

Voice call notification

Voice call: TEL1, TEL2
Voice message: 1

Text-based notifications

SMS notification: TEL3, TEL4
Push notification: PUSH1, PUSH2
E-mail notification: MAIL3, MAIL4
Message: IN1 alarm

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

OK Cancel

8

In this menu you can configure the input events generated by the contact inputs. 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 any events or 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 31 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

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

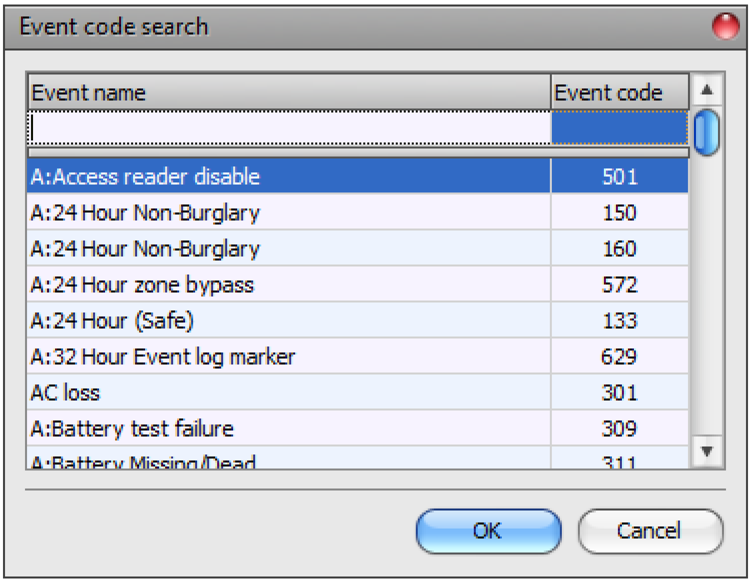
Type: the type of the event, which can be new or restore. New event will be generated when an input is activated, and restore event will be generated when it reverts to its normal state. In the Contact ID protocol, new events are indicated with 1 (or E), and event restorals are indicated with 3 (or R).

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. The event code consists of hexadecimal characters (0...9,A,B,C,D,E,F). The default configuration for input event codes is 130, which means burglar alarm.

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 code search

Event name	Event code
A:Access reader disable	501
A:24 Hour Non-Burglary	150
A:24 Hour Non-Burglary	160
A:24 Hour zone bypass	572
A:24 Hour (Safe)	133
A:32 Hour Event log marker	629
AC loss	301
A:Battery test failure	309
A:Battery Missing/Dead	311

Using 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 you wish to assign to the given event. The default configuration for partition is 01.

Zone: in this section you can configure the zone number you wish to assign to the given event. The default configuration for zones is in accordance with the number of the inputs (001 to 006).

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(s) to be controlled upon occurrence of a given input event.

Output control mode: in this section you can configure the control mode of the output (or the selected output 1 or 2 in case of the IN4.R2 model). 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 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes 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 (Pager4 PRO only)**:** 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 (Pager4 PRO only)**:** in this section you can select the addressees 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 input 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:
$name: the event name configured in the device for the given event.
$in1…**in4/in6**: the actual state of the given contact input (0=idle, 1=activated).
$rel1…**rel2**: the actual state of the given relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

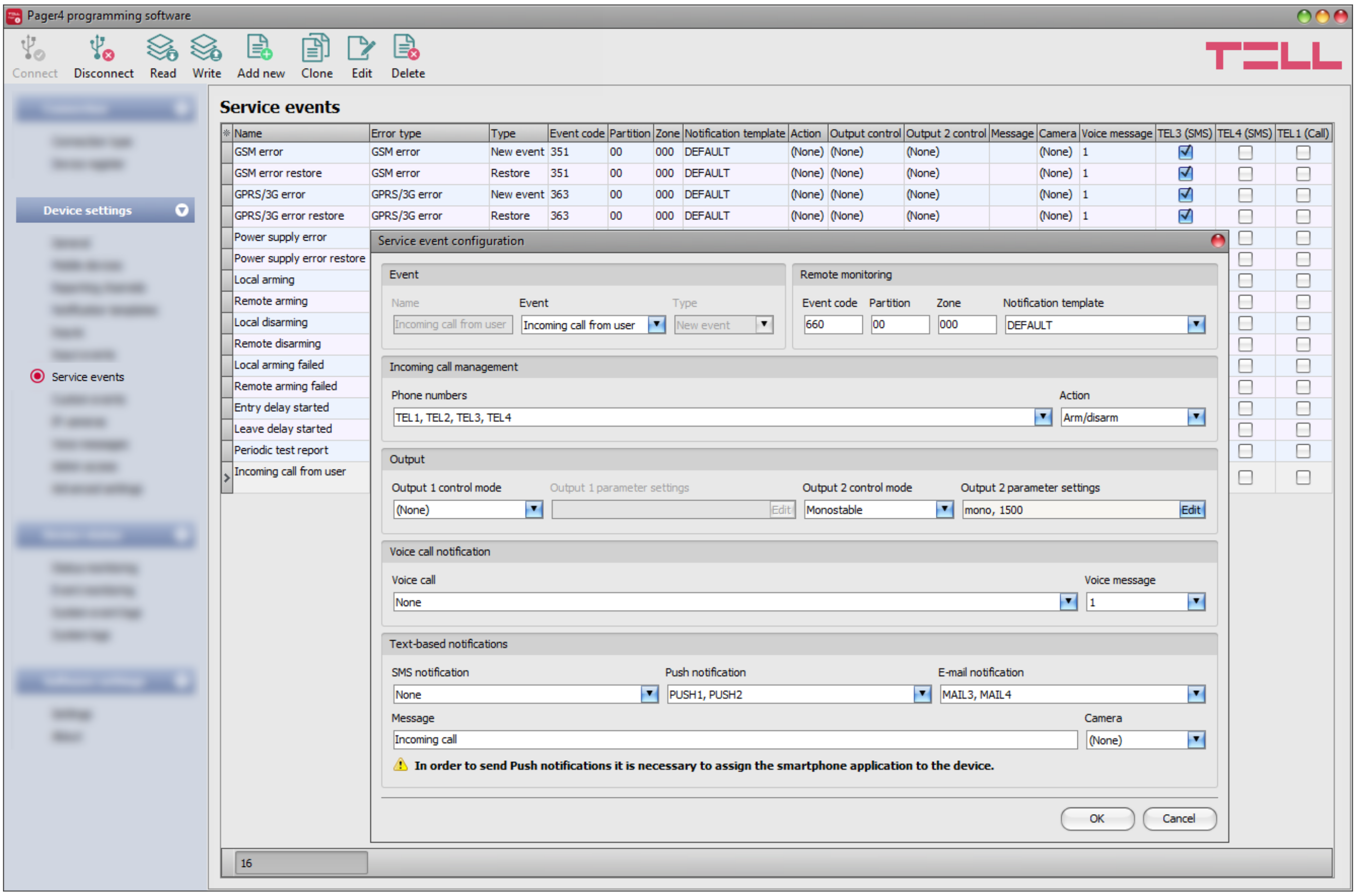
Camera (Pager4 PRO only): in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the "***IP cameras***" menu. If you have configured a Push notification for the given event, the mobile application will automatically offer 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.

5.2.7 Service events



Service events

Name	Error type	Type	Event code	Partition	Zone	Notification template	Action	Output control	Output 2 control	Message	Camera	Voice message	TEL3 (SMS)	TEL4 (SMS)	TEL1 (Call)
GSM error	GSM error	New event	351	00	000	DEFAULT	(None)	(None)	(None)		(None)	1	☑	□	□
GSM error restore	GSM error	Restore	351	00	000	DEFAULT	(None)	(None)	(None)		(None)	1	☑	□	□
GPRS/3G error	GPRS/3G error	New event	363	00	000	DEFAULT	(None)	(None)	(None)		(None)	1	☑	□	□
GPRS/3G error restore	GPRS/3G error	Restore	363	00	000	DEFAULT	(None)	(None)	(None)		(None)	1	☑	□	□
Power supply error														□	□
Power supply error restore														□	□
Local arming														□	□
Remote arming														□	□
Local disarming														□	□
Remote disarming														□	□
Local arming failed														□	□
Remote arming failed														□	□
Entry delay started														□	□
Leave delay started														□	□
Periodic test report														□	□
Incoming call from user														□	□

Service event configuration

Event
Name: Incoming call from user
Event: Incoming call from user
Type: New event

Remote monitoring
Event code: 660
Partition: 00
Zone: 000
Notification template: DEFAULT

Incoming call management
Phone numbers: TEL1, TEL2, TEL3, TEL4
Action: Arm/disarm

Output
Output 1 control mode: (None)
Output 1 parameter settings: Edit
Output 2 control mode: Monostable
Output 2 parameter settings: mono, 1500 Edit

Voice call notification
Voice call: None
Voice message: 1

Text-based notifications
SMS notification: None
Push notification: PUSH1, PUSH2
E-mail notification: MAIL3, MAIL4
Message: Incoming call
Camera: (None)

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

OK Cancel

In this menu you can configure the internal service events generated by the device. 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 31 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

Event: select an event form 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. The device can send report and notification on this event only after the error restores.

- **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. The device can send report and notification on this event over the Internet (e-mail, Push) only after the error restores.

- **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.

- **Local arming**: this type of event is generated upon arming the device locally via the contact inputs.

- **Remote arming**: this type of event is generated upon arming the device remotely by phone call, text message, or by the programming software.

- **Local disarming**: this type of event is generated upon disarming the device locally via the contact inputs.

- **Remote disarming**: this type of event is generated upon disarming the device remotely by phone call, text message, or by the programming software.

- **Local arming failed**: this type of event is generated when local arming fails. This basically occurs when attempting to arm the device locally while an input is activated for which the "***Force***" option is not enabled.

- **Remote arming failed**: this type of event is generated when remote arming fails. This basically occurs when attempting to arm the device remotely while an input is activated for which the "***Force***" option is not enabled.

- **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.

- **Incoming call from user**: 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. You can select user phone numbers for incoming call management and assign an action to them in the "***Incoming call handling***" section.

  Phone numbers: in this section you can select the user phone numbers from which incoming calls will generate an "***incoming call from user***" event, and to which you wish to assign an action.

  Action: in this section you can configure the action to be performed upon receiving a call from the selected user phone numbers.

  Available options:

  - **None**: no action will be performed.
  - **Arm only**: the device will change its state to armed.
  - **Disarm only**: the device will change its state to disarmed.
  - **Arm/Disarm**: the device will change its state call by call from armed to disarmed, respectively from disarmed to armed.

  Note! Remote arming and disarming are only available at specific arming/disarming settings! Please check the arming and disarming options in the "*General*" device settings menu.

- **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 with hidden caller ID.

- **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.

- **Entry delay started**: this type of event is generated when a delayed input is activated while the system is armed, and entry delay starts.

- **Exit delay started**: this type of event is generated upon arming the system, when exit delay starts.

- **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. New event will be generated when a service event occurs, and restore event will be generated when it restores. In the Contact ID protocol, new events are indicated with 1 (or E), while event restores 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. The default event codes are configured according to the standard list of Contact ID event codes.

Partition: in this section you can configure the partition number which you want to assign to the given event. The default configuration for partition is 01, except for error events.

Zone: in this section you can configure the zone number which you want 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(s) to be controlled upon occurrence of the given service event.

Output control mode: in this section you can configure the control mode of the output (or the selected output 1 or 2 in case of the IN4.R2 model). 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 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes 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 (Pager4 PRO only)**:** 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 (Pager4 PRO only)**:** in this section you can select the addressees 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 service event occurs. The device will send the same message for each notification channel (SMS, Push, e-mail).

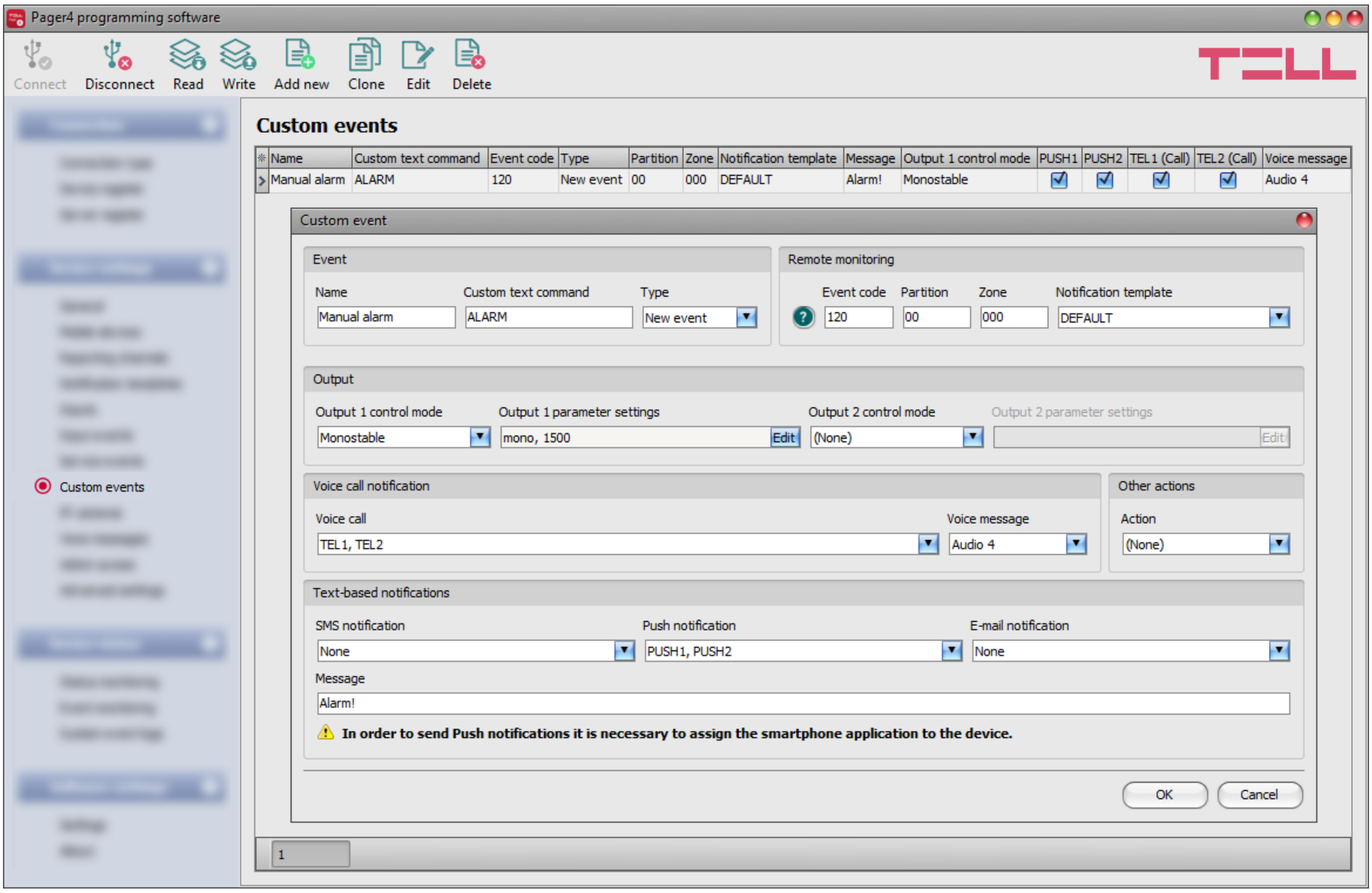
The device is capable to insert various dynamic data in the text of the message using variables. The device will automatically replace the variable written in the message with the data related to the given variable, when it sends the message.

Available variables:
$name: the event name configured in the device for the given event.
$in1…**in4/in6**: the actual state of the given contact input (0=idle, 1=activated).
$rel1…**rel2**: the actual state of the given relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

Camera (Pager4 PRO only): 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.

5.2.8 Custom events



Custom events

Name	Custom text command	Event code	Type	Partition	Zone	Notification template	Message	Output 1 control mode	PUSH1	PUSH2	TEL1 (Call)	TEL2 (Call)	Voice message
Manual alarm	ALARM	120	New event	00	000	DEFAULT	Alarm!	Monostable	☑	☑	☑	☑	Audio 4

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 1 control mode: Monostable
Output 1 parameter settings: mono, 1500 Edit
Output 2 control mode: (None)
Output 2 parameter settings: Edit

Voice call notification
Voice call: TEL1, TEL2
Voice message: Audio 4

Other actions
Action: (None)

Text-based notifications
SMS notification: None
Push notification: PUSH1, PUSH2
E-mail notification: None
Message: Alarm!

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

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, controlling outputs, as well as arming or disarming the device.

With this function you can practically generate any reports to remote monitoring station, notifications to users, and control the device's outputs and arm or disarm the device, 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 chapters *Remote control and status query by SMS* and *Remote connecting to devices via cloud service*), otherwise the device will only perform the default action associated with the command.

The chosen custom commands must not contain a space character! The space character is not supported.

*Arming and disarming will not be executed if the "***Always armed***" or "***Bistable contact***" option is selected at the "***Arming / Disarming options***" in the "***General***" device settings menu. In these cases, the device cannot be armed and disarmed remotely.

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, or from ones which are configured, but for which other than the "***Accept - password not required***" option is assigned in the "***Incoming call and SMS handling***" 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 31 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).

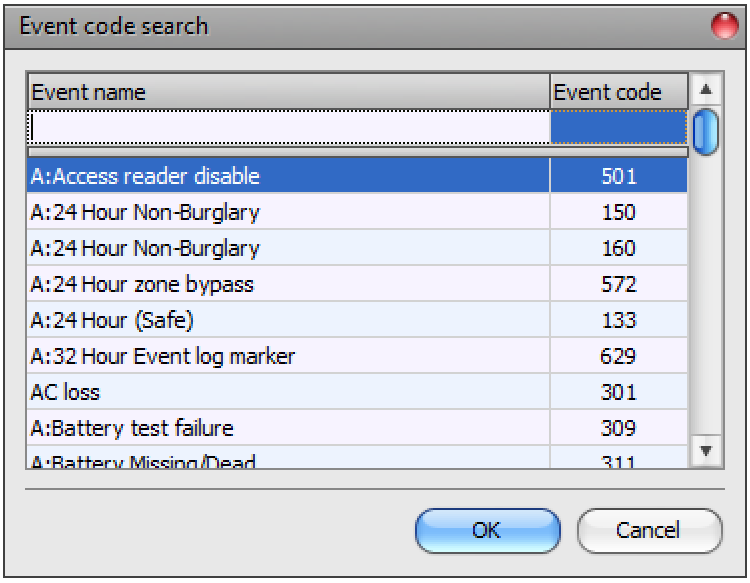
Remote monitoring:

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.

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.

Using 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.



Event name	Event code
A:Access reader disable	501
A:24 Hour Non-Burglary	150
A:24 Hour Non-Burglary	160
A:24 Hour zone bypass	572
A:24 Hour (Safe)	133
A:32 Hour Event log marker	629
AC loss	301
A:Battery test failure	309
A:Battery Missing/Dead	311

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(s) 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 (or the selected output 1 or 2 in case of the IN4.R2 model).

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 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes 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 uploaded, the siren tone will be played continuously throughout the call.

Other actions:

Action: in this section you can choose an arming/disarming action to be executed when the given custom event is generated. Available options:

- **None**: no action will be performed.
- **Arm only**: the device will change its state to armed.
- **Disarm only**: the device will change its state to disarmed.
- **Arm/Disarm**: the device will change its state call by call from armed to disarmed, respectively from disarmed to armed.

Note! Remote arming and disarming is only available at specific arming/disarming settings! Please check the arming and disarming options in the "*General*" device settings menu.

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 (Pager4 PRO only)**:** 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 (Pager4 PRO only)**:** in this section you can select the addressees 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:
$name: the event name configured in the device for the given event.
$in1…**in4/in6**: the actual state of the given contact input (0=idle, 1=activated).
$rel1…**rel2**: the actual state of the given relay output (0=idle, 1=activated).
$ps: the momentarily measured supply voltage value (e.g.: 13563 mV).

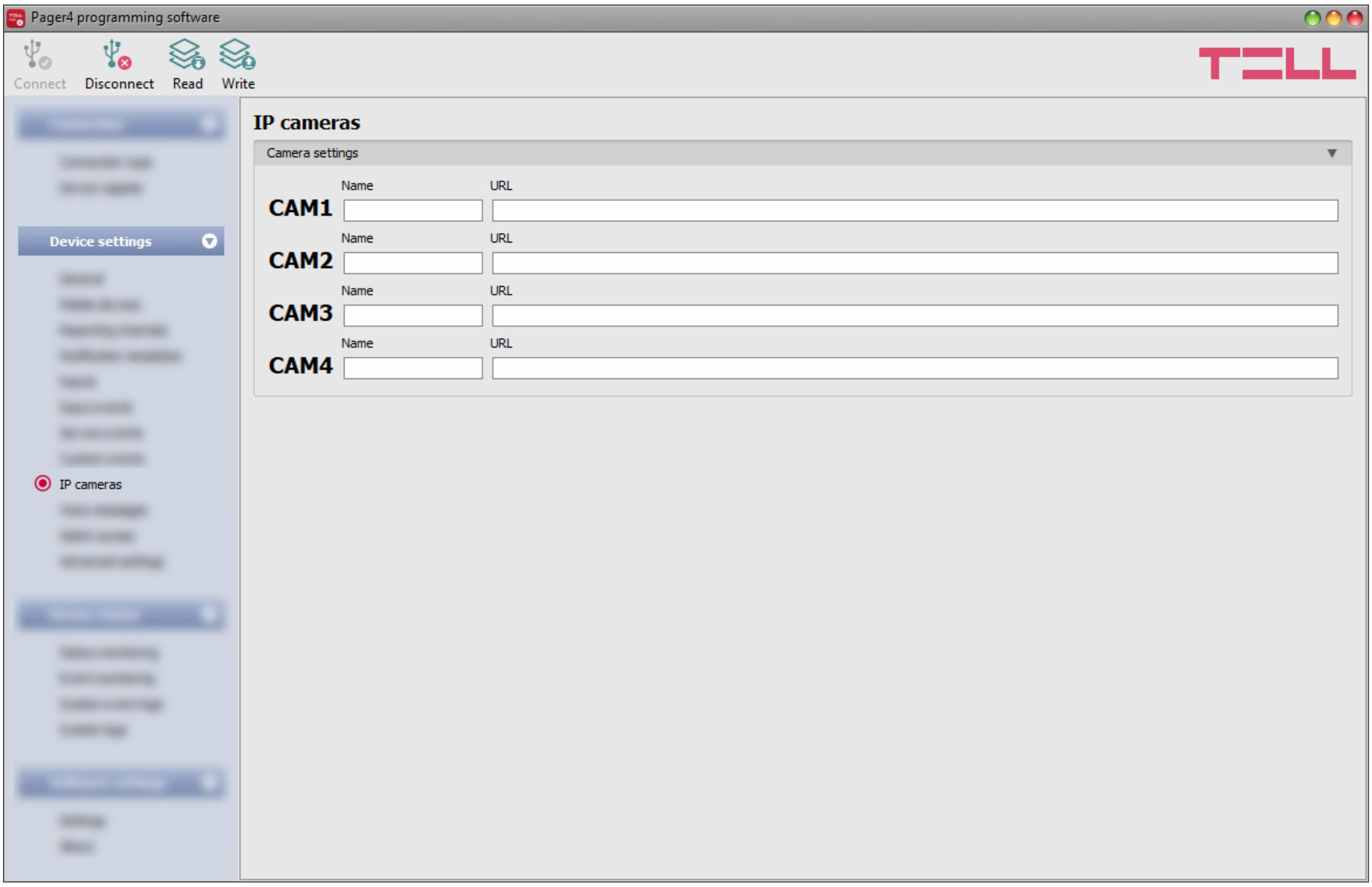
Camera (Pager4 PRO only): in this section you can select the IP camera which you wish to assign to the given event. IP cameras should be configured in advance in the "***IP cameras***" menu. If you have configured a Push notification for the given event, the mobile application will automatically offer 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.

5.2.9 **IP cameras** (Pager4 PRO only)



IP cameras

Camera settings

	Name	URL
CAM1		
CAM2		
CAM3		
CAM4		

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 will be used for identifying the cameras upon assigning them to events when configuring events. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

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: www.tell.hu), 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 *Pager4* 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

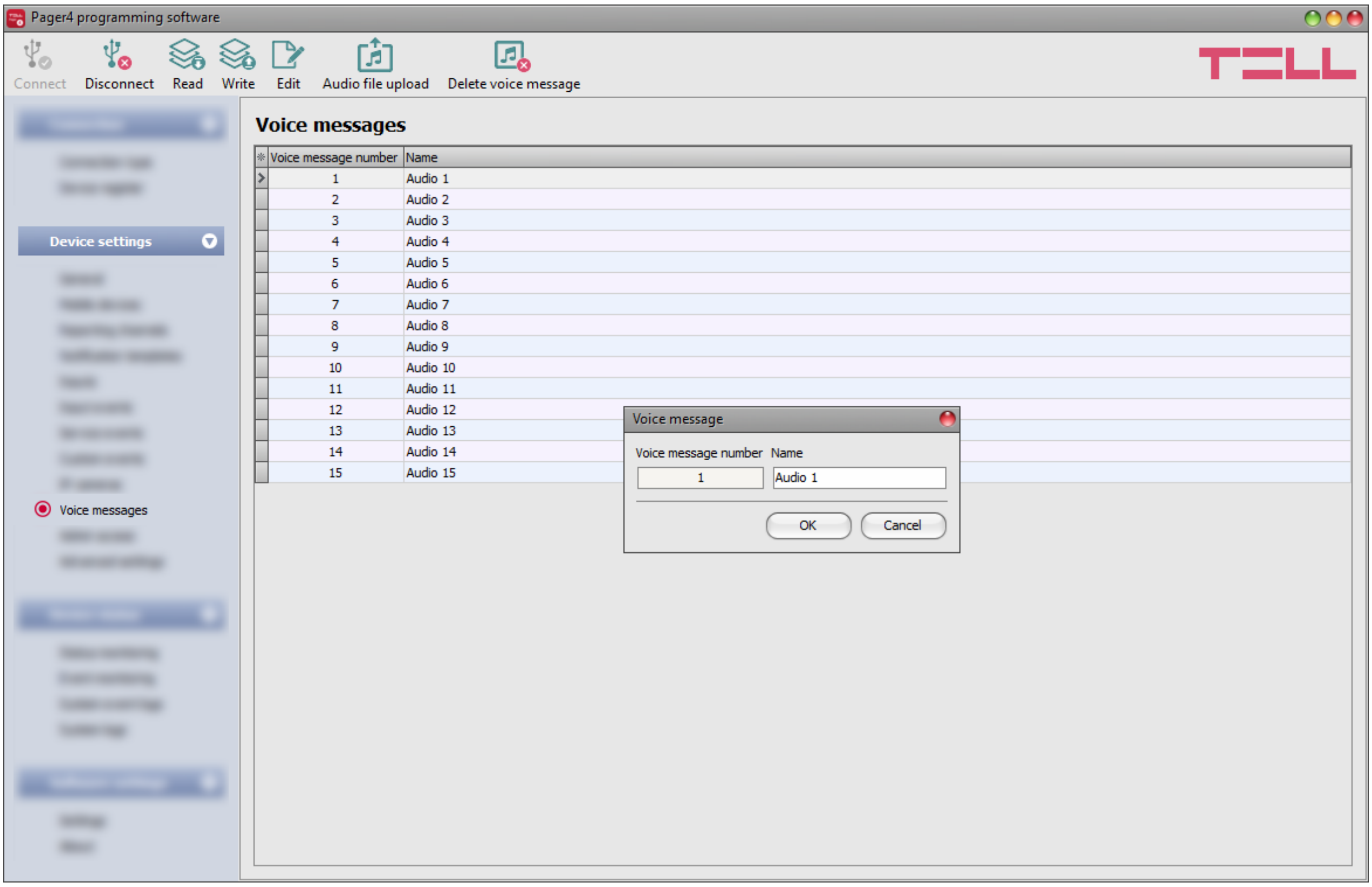
Modified URL in case of using static IP address and username/password:
rtsp://***username:password@WAN IP***:554/cam/realmonitor?channel=1&subtype….

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.

5.2.10 Voice messages



Voice messages

Voice message number	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

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:

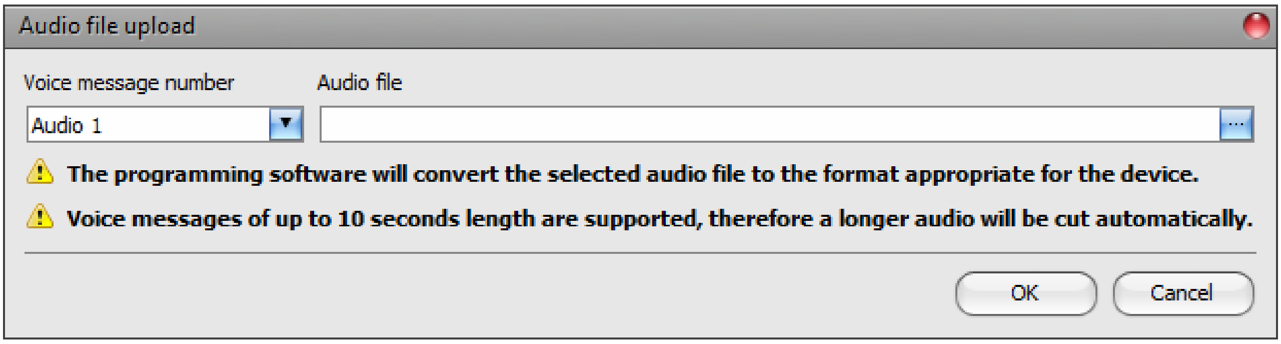
- Reading the settings from the device:
  To read the settings from the device, click on the “***Read***” button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, to take effect, it is necessary to write the new 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. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | $ % " '.

- 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.



⚠ 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.

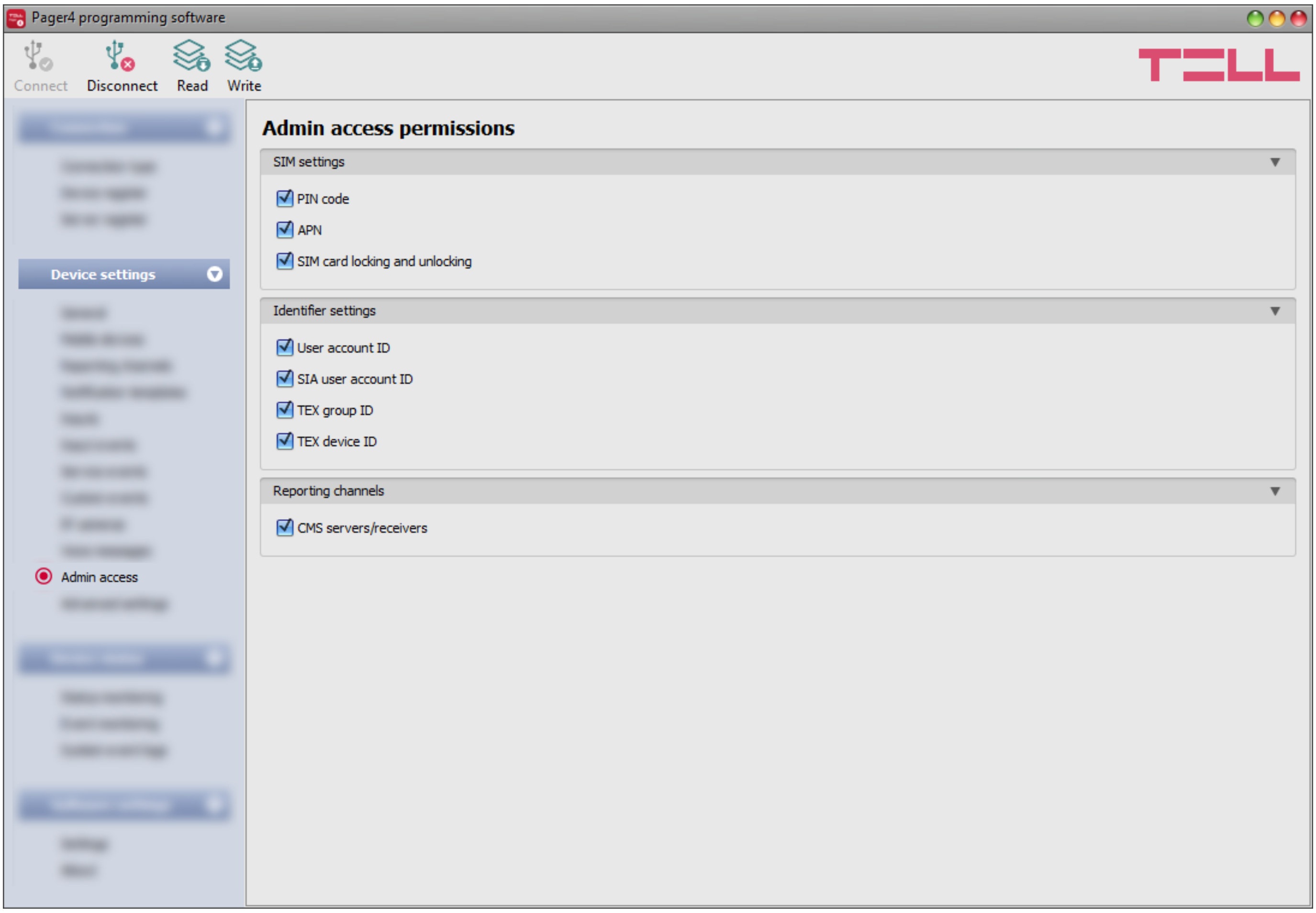
Audio file: click on the browse button found at the end of this field, and then browse the audio file you wish to upload. Click on the "***OK***" button to start uploading the selected file.

- 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.

5.2.11 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.

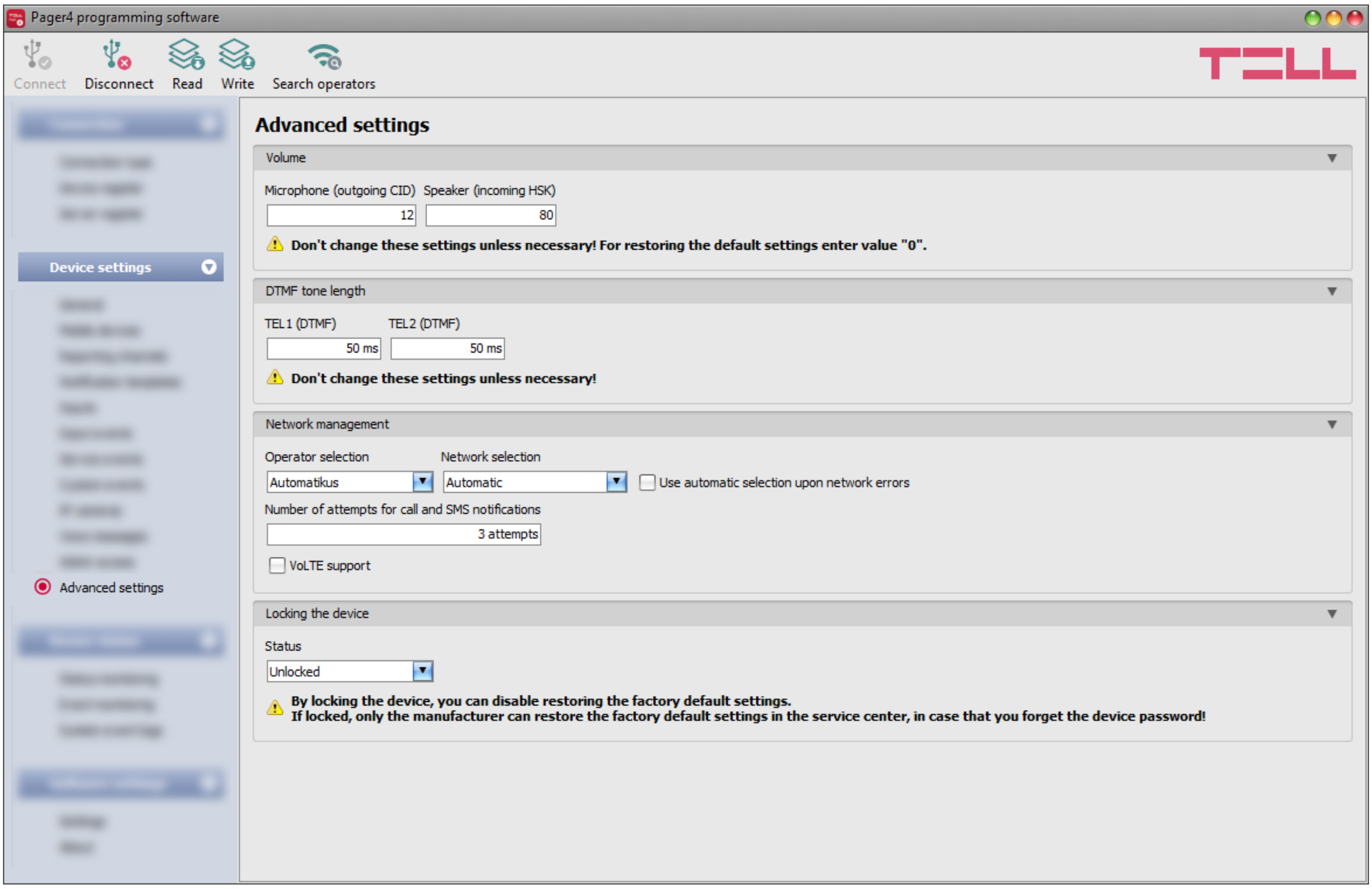
The settings that don’t have a checkmark, i.e. the ones that the Admin user does not have access to, are considered protected. To keep track of the changes made to the protected settings, the device generates a "***Settings changed***" service event if configured in the "***Service events***" menu, whenever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

5.2.12 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".

DTMF tone length

TEL1 (DTMF): 50 ms
TEL2 (DTMF): 50 ms

⚠ Don't change these settings unless necessary!

Network management

Operator selection: Automatikus
Network selection: Automatic
□ Use automatic selection upon network errors

Number of attempts for call and SMS notifications: 3 attempts

□ VoLTE support

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, as well as the in-call volume (siren tone, voice messages, DTMF commands). 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 default settings unless necessary!

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.
- 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, siren tone, voice message) 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, DTMF commands) 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!

DTMF tone length:

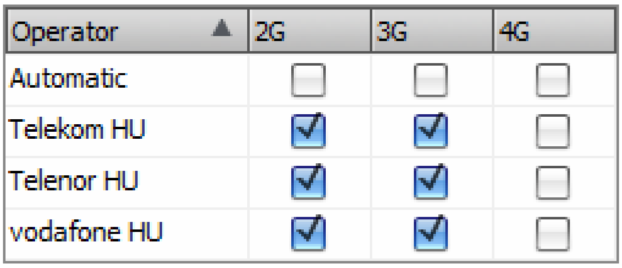
TEL1 (DTMF): adjusts the length of the DTMF tones which affects calls made to the DTMF receiver configured in section “***TEL1***” in the “***Reporting channels***” menu. The setting also affects the spacing between tones accordingly. The value can be set from 50ms to 1000ms.

TEL2 (DTMF): adjusts the length of the DTMF tones which affects calls made to the DTMF receiver configured in section “***TEL2***” in the “***Reporting channels***” menu. The setting also affects the spacing between tones accordingly. The value can be set from 50ms to 1000ms.

Network management:

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

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



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

Network selection: the mobile network management in the device is automatic by default. If you experience problems with the stability of the mobile network in the given location, that is the module 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
- **4G only**: use 4G (LTE) network only

3G network usage is supported by the 3G.IN4.R2 and the 3G.IN6.R1, as well as the 4G.IN4.R2 and the 4G.IN6.R1 models of the Pager4! 4G network usage is supported by the 4G.IN4.R2 and the 4G.IN6.R1 models 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 3G).

Number of attempts for call and SMS notifications: it is possible to configure the maximum number of attempts for sending notifications to users about an event by call or SMS. If the number of attempts reaches the configured value for a given phone number, then the device terminates the notification of the given event to that specific phone number, and it will not perform further attempts. The number of attempts applies to calls end SMS sending separately.

VoLTE support (4G model only): 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 configured APN settings in the device settings. **Do not enable this option if any of the above is not available, otherwise the network connection may fail.**

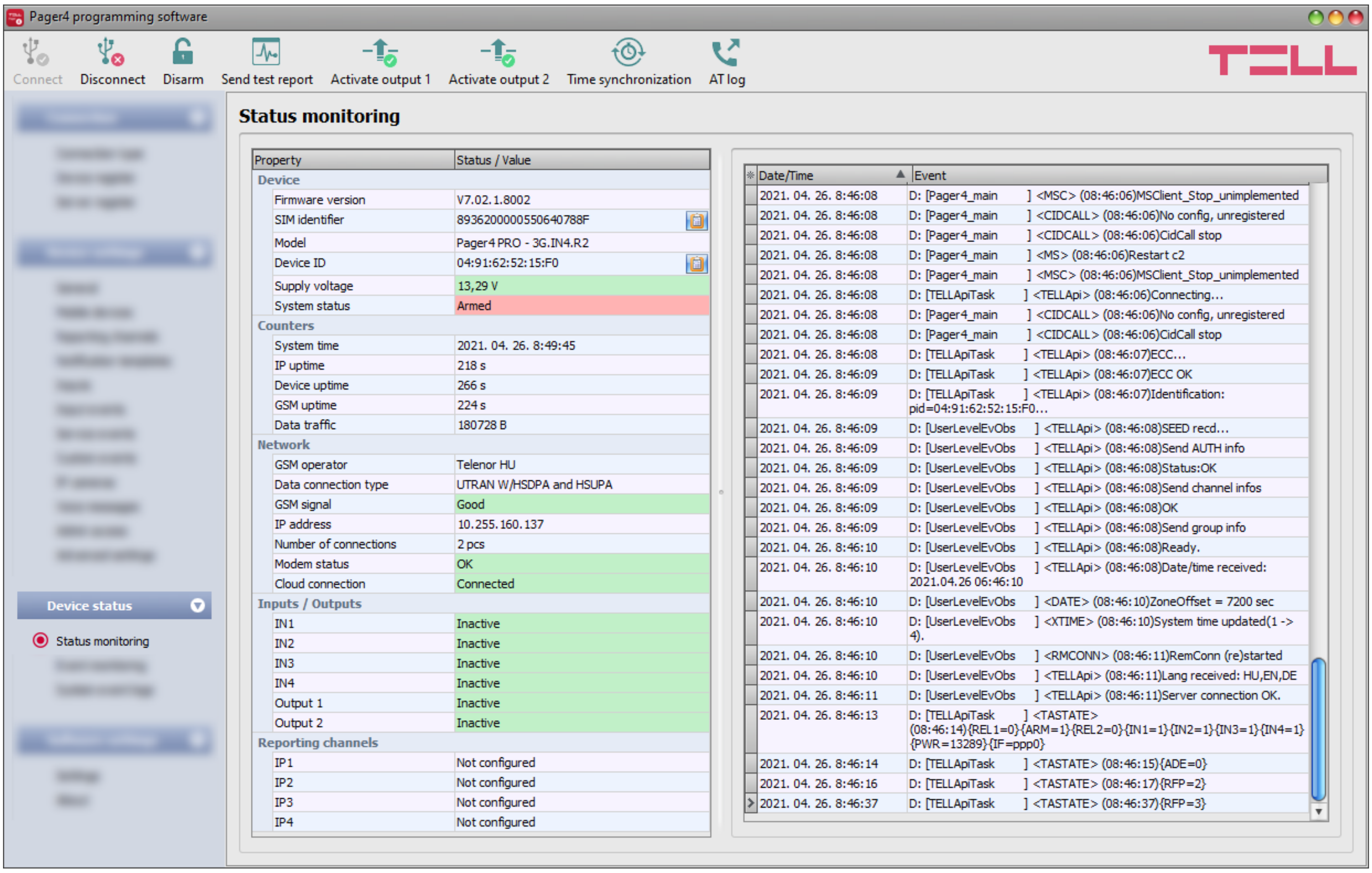
Locking the device:

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

- **Unlocked**: when unlocked, the factory default settings can be restored at any time, 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 the device passwords, only the manufacturer can restore the factory default settings in the service center.

5.3 Device status menu

5.3.1 Status monitoring



Status monitoring

Property	Status / Value
Device	
Firmware version	V7.02.1.8002
SIM identifier	8936200000550640788F
Model	Pager4 PRO - 3G.IN4.R2
Device ID	04:91:62:52:15:F0
Supply voltage	13,29 V
System status	Armed
Counters	
System time	2021. 04. 26. 8:49:45
IP uptime	218 s
Device uptime	266 s
GSM uptime	224 s
Data traffic	180728 B
Network	
GSM operator	Telenor HU
Data connection type	UTRAN W/HSDPA and HSUPA
GSM signal	Good
IP address	10.255.160.137
Number of connections	2 pcs
Modem status	OK
Cloud connection	Connected
Inputs / Outputs	
IN1	Inactive
IN2	Inactive
IN3	Inactive
IN4	Inactive
Output 1	Inactive
Output 2	Inactive
Reporting channels	
IP1	Not configured
IP2	Not configured
IP3	Not configured
IP4	Not configured

Date/Time	Event
2021. 04. 26. 8:46:08	D: [Pager4_main] <MSC> (08:46:06)MSClient_Stop_unimplemented
2021. 04. 26. 8:46:08	D: [Pager4_main] <CIDCALL> (08:46:06)No config, unregistered
2021. 04. 26. 8:46:08	D: [Pager4_main] <CIDCALL> (08:46:06)CidCall stop
2021. 04. 26. 8:46:08	D: [Pager4_main] <MS> (08:46:06)Restart c2
2021. 04. 26. 8:46:08	D: [Pager4_main] <MSC> (08:46:06)MSClient_Stop_unimplemented
2021. 04. 26. 8:46:08	D: [TELLApiTask] <TELLApi> (08:46:06)Connecting...
2021. 04. 26. 8:46:08	D: [Pager4_main] <CIDCALL> (08:46:06)No config, unregistered
2021. 04. 26. 8:46:08	D: [Pager4_main] <CIDCALL> (08:46:06)CidCall stop
2021. 04. 26. 8:46:08	D: [TELLApiTask] <TELLApi> (08:46:07)ECC...
2021. 04. 26. 8:46:09	D: [TELLApiTask] <TELLApi> (08:46:07)ECC OK
2021. 04. 26. 8:46:09	D: [TELLApiTask] <TELLApi> (08:46:07)Identification: pid=04:91:62:52:15:F0...
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)SEED recd...
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)Send AUTH info
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)Status:OK
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)Send channel infos
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)OK
2021. 04. 26. 8:46:09	D: [UserLevelEvObs] <TELLApi> (08:46:08)Send group info
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <TELLApi> (08:46:08)Ready.
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <TELLApi> (08:46:08)Date/time received: 2021.04.26 06:46:10
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <DATE> (08:46:10)ZoneOffset = 7200 sec
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <XTIME> (08:46:10)System time updated(1 -> 4).
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <RMCONN> (08:46:11)RemConn (re)started
2021. 04. 26. 8:46:10	D: [UserLevelEvObs] <TELLApi> (08:46:11)Lang received: HU,EN,DE
2021. 04. 26. 8:46:11	D: [UserLevelEvObs] <TELLApi> (08:46:11)Server connection OK.
2021. 04. 26. 8:46:13	D: [TELLApiTask] <TASTATE> (08:46:14){REL1=0}{ARM=1}{REL2=0}{IN1=1}{IN2=1}{IN3=1}{IN4=1}{PWR=13289}{IF=ppp0}
2021. 04. 26. 8:46:14	D: [TELLApiTask] <TASTATE> (08:46:15){ADE=0}
2021. 04. 26. 8:46:16	D: [TELLApiTask] <TASTATE> (08:46:17){RFP=2}
2021. 04. 26. 8:46:37	D: [TELLApiTask] <TASTATE> (08:46:37){RFP=3}

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 contains information about the internal processes and communication of the device. The system logs help troubleshooting if a malfunction occurs. The program saves the system 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*_module.log”). **The system logs are only available when connected via USB!**

In case of remote connection, status information can be loaded or updated by clicking on the “***Query***” button. The states of the control buttons are also updated based on the status information. The availability of certain status information listed below depends on the product model connected.

Device:

- **Firmware version**: the firmware version of the device.
- **WiFi chip firmware version** (WiFi model only): the firmware version of the WiFi microcontroller unit.
- **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.
- **System status**: armed or disarmed.

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 GSM operator used.
- **Data connection type**: type of actual data connection.
- **GSM signal**: actual GSM signal level (None/Very low, Weak, Medium, Good, Excellent).
- **WiFi network** (WiFi model only): the name (SSID) of the network to which the device is connected
- **Signal** (WiFi model only): the signal level (None/Very low, Weak, Medium, Good, Excellent) of the network to which the device is connected.
- **Searching for WiFi networks** (WiFi model only): network scanning status (Yes=scanning is in progress).
- **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/IN6**: the actual state of the contact inputs.
- **Output1/Output2**: the actual state of the output(s) (OUT1/OUT2)

Reporting channels:

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

When connected to the device locally or remotely, the following options will be available:

- **Query**:
  This button appears in case of remote connection only. By clicking on it, status information will be downloaded from the device. This is not needed for USB connection, since in that case the data is downloaded automatically.
- **Arm**:
  The device can be armed by clicking on this button. This option is not available if the "***Always armed***" or "***Bistable contact***" option is selected at the "***Arming / Disarming options***" in the "***General***" settings menu.
- **Disarm**:
  The device can be disarmed by clicking on this button. This option is not available if the "***Always armed***" or "***Bistable contact***" option is selected at the "***Arming / Disarming options***" in the "***General***" settings menu.
- **Send test report**:
  You can generate a periodic test report event by clicking on this button.

- **Activate output 1** (IN4.R2 model only):

  Output OUT1 can be activated 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.

- **Activate output 2** (IN4.R2 model only):

  Output OUT2 can be activated 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.

- **Activate output** (IN6.R1 model only):

  The output (OUT1) can be activated 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 1** (IN4.R2 model only):

  Output OUT1 can be deactivated by clicking on this button.

- **Deactivate output 2** (IN4.R2 model only):

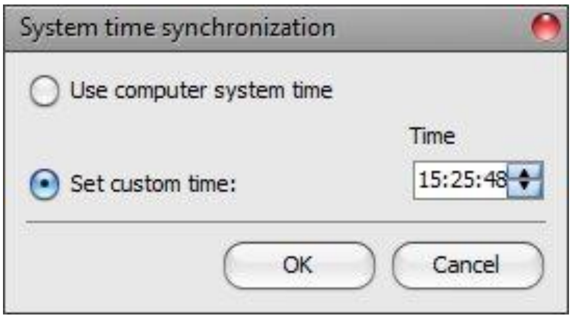
  Output OUT2 can be deactivated by clicking on this button.

- **Deactivate output** (IN6.R1 model only):

  The output (OUT1) can be deactivated by clicking on this button.

- **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

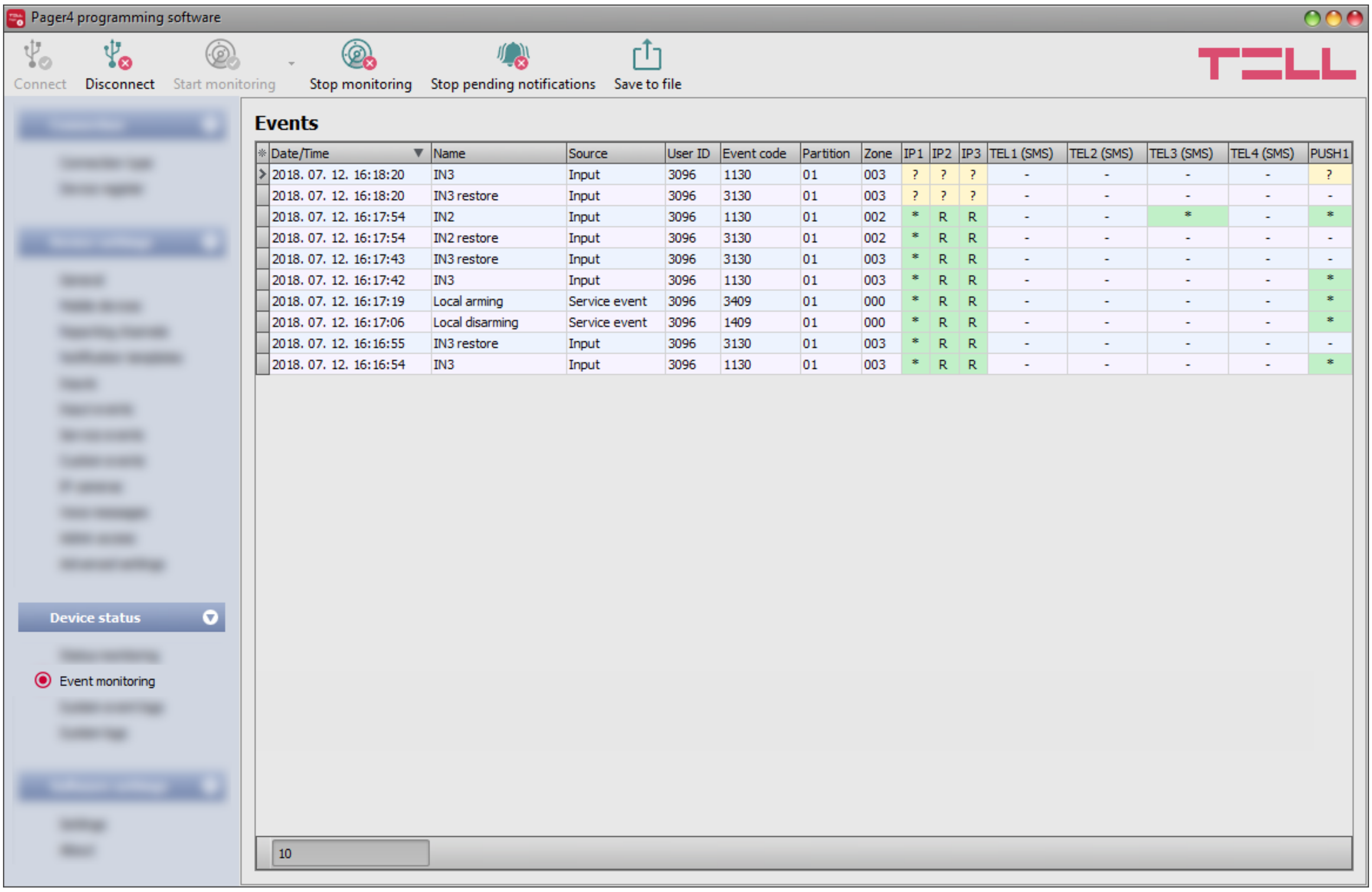
Time

● Set custom time: 15:25:48

- **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.

5.3.2 Event monitoring



Events

Date/Time	Name	Source	User ID	Event code	Partition	Zone	IP1	IP2	IP3	TEL1 (SMS)	TEL2 (SMS)	TEL3 (SMS)	TEL4 (SMS)	PUSH1
2018. 07. 12. 16:18:20	IN3	Input	3096	1130	01	003	?	?	?	-	-	-	-	?
2018. 07. 12. 16:18:20	IN3 restore	Input	3096	3130	01	003	?	?	?	-	-	-	-	-
2018. 07. 12. 16:17:54	IN2	Input	3096	1130	01	002	*	R	R	-	-	*	-	*
2018. 07. 12. 16:17:54	IN2 restore	Input	3096	3130	01	002	*	R	R	-	-	-	-	-
2018. 07. 12. 16:17:43	IN3 restore	Input	3096	3130	01	003	*	R	R	-	-	-	-	-
2018. 07. 12. 16:17:42	IN3	Input	3096	1130	01	003	*	R	R	-	-	-	-	*
2018. 07. 12. 16:17:19	Local arming	Service event	3096	3409	01	000	*	R	R	-	-	-	-	*
2018. 07. 12. 16:17:06	Local disarming	Service event	3096	1409	01	000	*	R	R	-	-	-	-	*
2018. 07. 12. 16:16:55	IN3 restore	Input	3096	3130	01	003	*	R	R	-	-	-	-	-
2018. 07. 12. 16:16:54	IN3	Input	3096	1130	01	003	*	R	R	-	-	-	-	*

In this menu you can view the device's event log and monitor events and the reporting progress online. The device stores the last 1000 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.

- **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.

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

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

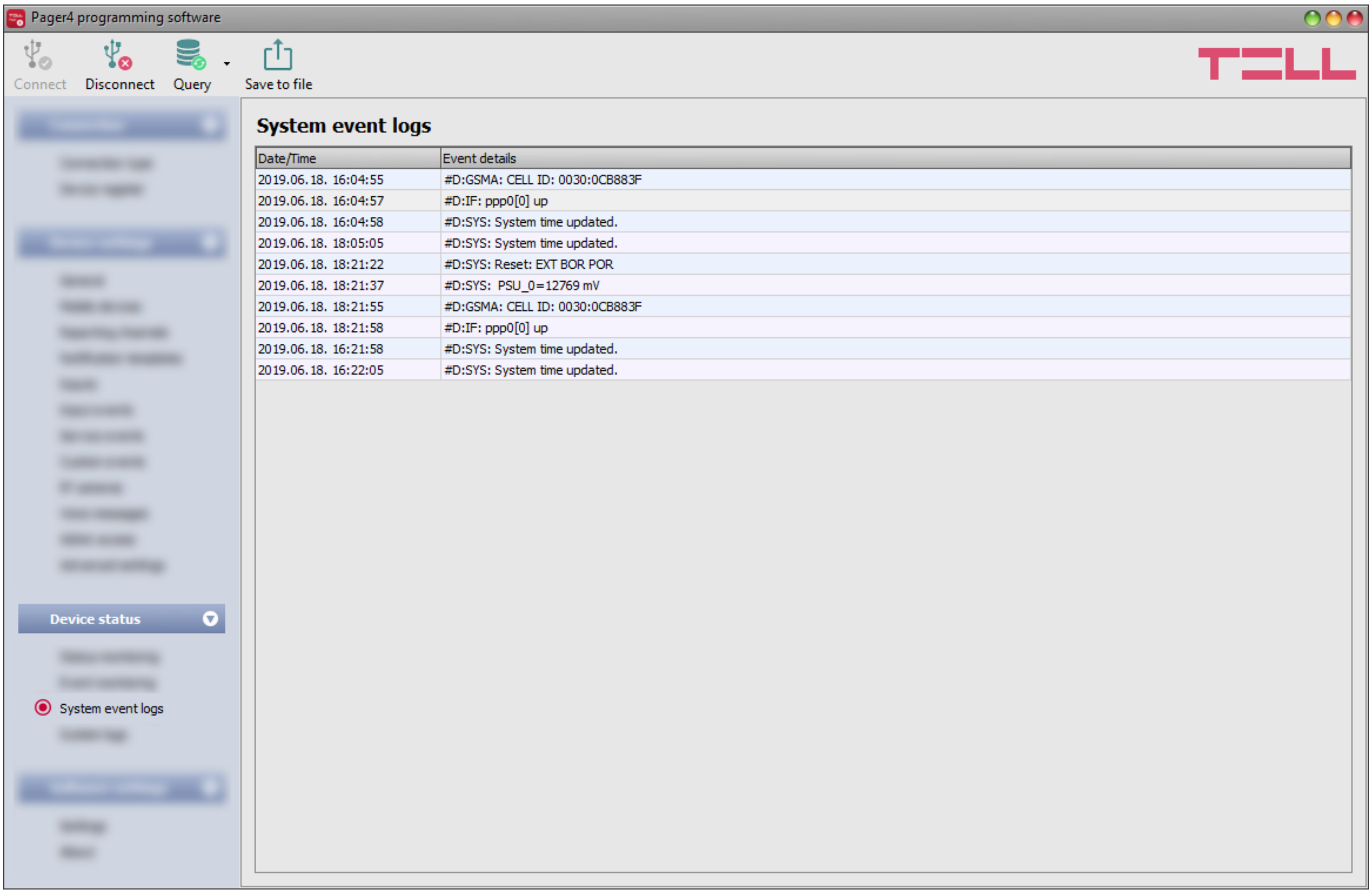
Elements of the event log:

- **Date/time**: event occurrence date and time.
- **Name**: event name, according to the event names configured for input and service events.
- **Source**: source of events (input or service).
- **User ID**: the user ID configured for sending reports to CMS.
- **Event code**: the event's Contact ID event code.
- **Partition**: partition number.
- **Zone**: zone number.
- **IP1**…**IP4**: reporting to IP1…IP4 server/receiver IP addresses.
- **DTMF1**…**DTMF2**: reporting to DTMF receivers by call.
- **TEL1**…**TEL10 (SMS)**: notifications to phone numbers TEL1…TEL10 by SMS.
- **TEL1**…**TEL10 (Call)**: notifications to phone numbers TEL1…TEL10 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 notification status shown in the IP1…IP4, DTMF1…DTMF2, TEL1…TEL10 (SMS). TEL1…TEL10 (Call), PUSH1…PUSH4 and EMAIL1…EMAIL4 columns:

?	New event reporting is in progress.
R	No need to report because reporting to an alternative reporting channel was successful.
*****	Reported successfully.
E	Reporting failed, the configured recipient is not available. In case of reporting to CMS, this status occurs after all attempts for sending the report fail. In case of sending notifications by text message or call, this status occurs after 3 failed attempts per message and per call.
-	No server/receiver IP address or user phone number configured.
T	Timeout, the notification could not be delivered in time.

5.3.3 System event logs



System event logs

Date/Time	Event details
2019.06.18. 16:04:55	#D:GSMA: CELL ID: 0030:0CB883F
2019.06.18. 16:04:57	#D:IF: ppp0[0] up
2019.06.18. 16:04:58	#D:SYS: System time updated.
2019.06.18. 18:05:05	#D:SYS: System time updated.
2019.06.18. 18:21:22	#D:SYS: Reset: EXT BOR POR
2019.06.18. 18:21:37	#D:SYS: PSU_0=12769 mV
2019.06.18. 18:21:55	#D:GSMA: CELL ID: 0030:0CB883F
2019.06.18. 18:21:58	#D:IF: ppp0[0] up
2019.06.18. 16:21:58	#D:SYS: System time updated.
2019.06.18. 16:22:05	#D:SYS: System time updated.

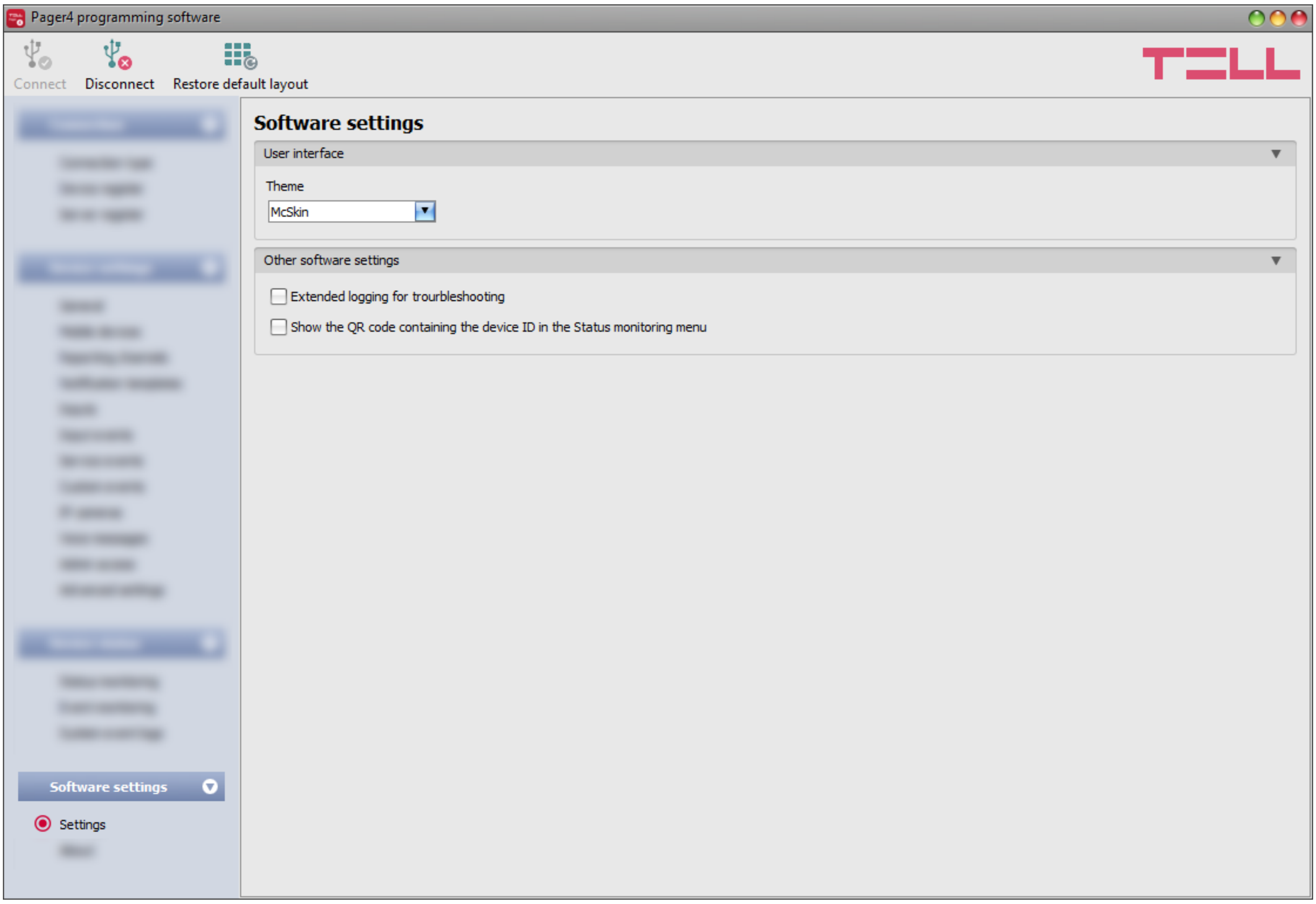
Events related to device operation are shown in the system event logs.

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.

5.4 Software settings menu

5.4.1 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 this menu you can change the user interface skin (appearance), configure certain parameters of the system logs window, and enable extended logging for troubleshooting.

Available options:

- **Restore default layout**:
  To restore the user interface default layout, click on the "***Restore default layout***" button, and then close and restart the program.

User interface:

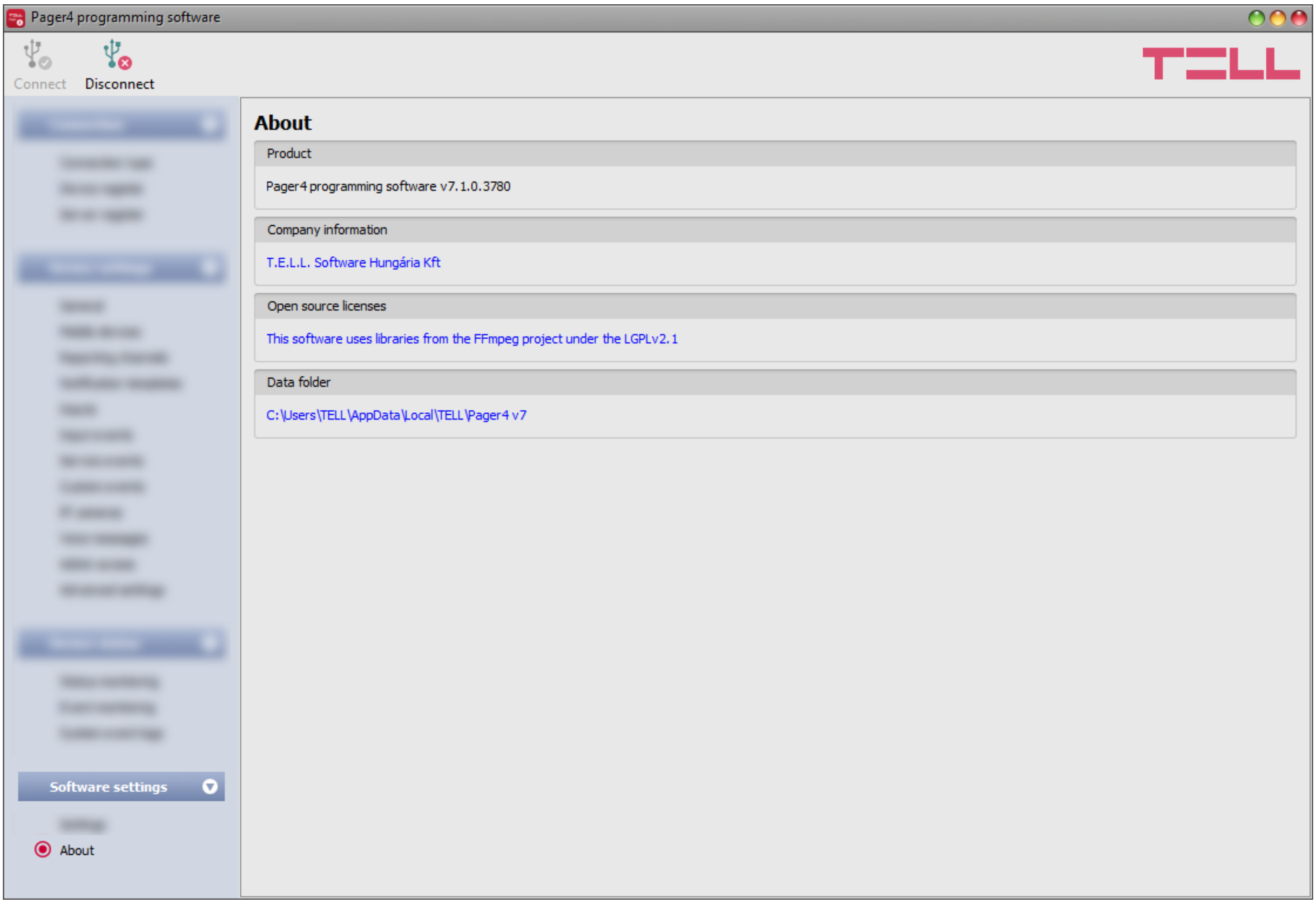
Theme: the user interface appearance can be changed using this dropdown-menu. You can choose from various appearance themes.

Other software settings:

Extended logging for troubleshooting: you can enable this option if you encounter issues with the software. If enabled, the program records 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.

5.4.2 About



About

Product

Pager4 programming software v7.1.0.3780

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\Pager4 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.

6 Controlling the device remotely by DTMF commands and text message

6.1 Remote control and status query by DTMF commands via phone call

The device can be controlled and status query can be performed after calling the number of the SIM card installed into the device. To gain access to controls, the device password will be requested or not, according to the setting configured in the “***Incoming call and SMS handling***” section for the given user phone number, which you can find in the “***Reporting channels***” menu. When calling from a phone number which is not configured in the device, the password will always be requested. The superadmin and admin passwords are both accepted. Thereafter, the following commands can be used by pressing the phone’s keys:

List of DTMF commands		
Command	**Specification**	**Module response**
∗9*password***#**	Entering the device password	Password accepted: 3 beeps Wrong password: 4 low-tone beeps
∗0#	Disarm	3 beeps
∗1#	Arm	6 beeps
∗2#	Armed/disarmed status query	Disarmed: 3 beeps Armed: 6 beeps
∗4#	GSM signal level query	The signal level will be indicated by a number of beeps from 1 to 5
∗3*RS***#**	Control the output(s) *R*: output (relay) number: **1** for the IN6.R1 model, **1** to **2** for the IN4.R2 model *S*: output state: **0** = open, **1** = closed	Becomes open: 3 beeps Becomes closed: 6 beeps
∗3*R***9#**	Output state query *R*: output number: **1** for the IN6.R1 model, **1** to **2** for the IN4.R2 model	Open: 3 beeps Closed: 6 beeps

Example:

1. **Incoming call and SMS handling** setting: case of option “***Accept - password required***” and **superadmin** or **admin password: 1234**:
   a. **Activating output OUT1**:
      - Enter the device password: **∗91234#** (accepted: 3 beeps)
      - Activate output OUT1: **∗311#** (output OUT1 activated/closed: 6 beeps)

   b. **State query on output OUT1**:
      - Enter the device password: **∗91234#** (accepted: 3 beeps)
      - State query on output OUT1: **∗319#** (if output OUT1 is activated/closed: 6 beeps)

2. **Incoming call and SMS handling** setting: case of option “***Accept - password not required***“:
   Deactivating output OUT1: (3 beeps: password accepted) **∗310#** (output OUT1 deactivated/open: 3 beeps)

6.2 Remote control and status query by SMS

Controls and status query can be performed by sending commands in SMS to the phone number of the SIM card installed into the device. The following commands can be used:

SMS Command	Specification
∗**ARM,PWD=**yyyy**,CRQ#**	Arming the device (*please read the note below) If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**DISARM,PWD=**yyyy**,CRQ#**	Disarming the device (*please read the note below) If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R1=ON, PWD=**yyyy**, CRQ#**	Activating output OUT1 (bistable mode) If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R1=OFF, PWD=**yyyy**, CRQ#**	Deactivating output OUT1 If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R1=ON**x**, PWD=**yyyy**, CRQ#**	Activating output OUT1 for "x" (1 to 3600) seconds (monostable mode) Substitute parameter "x" with the desired value. If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R2=ON, PWD=**yyyy**, CRQ#**	Activating output OUT2 (bistable mode) - IN4.R2 model only If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R2=OFF, PWD=**yyyy**, CRQ#**	Deactivating output OUT2 - IN4.R2 model only If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**R2=ON**x**, PWD=**yyyy**, CRQ#**	Activating output OUT2 for "x" (1 to 3600) seconds (monostable mode) - IN4.R2 model only Substitute parameter "x" with the desired value. If needed, use the CRQ and PWD parameter and substitute "yyyy" with the device password (see specifications below).
∗**STATUS, PWD=**yyyy**#**	Requesting status information (the device will send the states of inputs and outputs, armed/disarmed status, and GSM signal level in response SMS). If needed, substitute "yyyy" with the device password (see specification below).

*Arming and disarming will be refused if the "***Always armed***" or "***Bistable contact***" option is selected at the "***Arming / Disarming options***" in the "***General***" device settings menu. In these cases, the device cannot be armed and disarmed remotely.

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, or from ones which are configured, but for which other than the "***Accept - password not required***" option is assigned in the "***Incoming call and SMS handling***" section – such phone numbers are considered unauthorized, therefore in this case the password is required). If the device password is not specified in the control command sent from unauthorized phone numbers, the command will not be executed by the device.

CRQ = request confirmation in response SMS (optional parameter, to be used if confirmation is requested). If this parameter is added to the control command, the device will respond to the sender by SMS with information regarding the execution of the command.

Commands should always begin with star "∗" and end with hash "#" character. It is also possible to send multiple commands in one message, but the message should not exceed 60 characters. If the response message to be received from the device would exceed 60 characters, only the first 60 characters will be sent. In case of making mistakes in the command, the following response will be received: "**SYNTAX ERROR!**" and the command(s) will not be executed.

Responses messages sent by the device (when using the CRQ parameter):

Armed	= the device has been armed
Disarmed	= the device has been disarmed
Arming failed	= the device could not be armed*
Disarming failed	= the device could not be disarmed*
Relay1 activated: 54 sec.	= output OUT1 activated for 54 seconds
Relay1 activated: Permanent.	= output OUT1 activated permanently (bistable mode)
Relay1 deactivated.	= output OUT1 deactivated
Unauthorized User!	= Wrong or missing password

Examples for command usage:

To activate output OUT1 permanently (bistable mode):

- If the command is sent from a phone number for which the " ***Accept - password not required*** " option is selected in the "***Incoming call and SMS handling***" section, and no confirmation is requested, then the command will be: **∗R1=ON#**
- If the command is sent from a phone number for which the " ***Accept - password required*** " or the "***Reject***" option is selected in the "***Incoming call and SMS handling***" section, then device password will also be required, therefore the command will be:

  ∗R1=ON, PWD=1234# (if the superadmin or admin password is 1234)
- If the command is sent from a phone number which is not configured in the device and confirmation is requested, then the command will be: **∗R1=ON, PWD=1111, CRQ#**

Example for module status information sent by the device:

Status information refers to states and values measured in the moment when the device sends the message!

Z1=R **Z2=A** **…** **Z6=R**	shows the state of inputs IN1…IN4/IN6 (**R**=Ready/idle, **A**=Activated)
Armed	shows the armed/disarmed status
R1=ON, 37 sec	shows the state of the output OUT1 (**ON** or **OFF**), the remaining time till deactivation, or "**Permanent**" if it has been activated permanently
RF: 23	shows the GSM signal level from 1 to 31

7 Updating the firmware

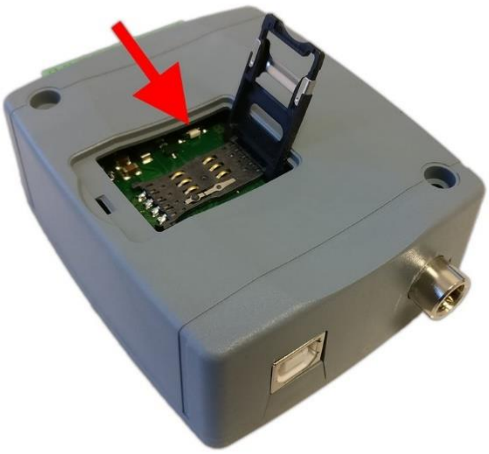
TELL always releases its products with the latest firmware version. However, as our products are being continuously improved, new firmware updates may occasionally be released for the products, which may include new features along with bug fixes. Therefore, it is recommended that you always upgrade your 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 ***Pager4*** 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.
  - Open the update tool and click on the "***FIRMWARE***" button.
  - Keep the reset button pressed while connecting the device to the computer via USB, and then release the button. The reset button is placed on the electronic board, near the corner of the SIM card holder, closed to the status LED (see the picture on the right-hand side). It is easier to access the button if you open the SIM card holder.
  - 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 LED status indicator on the device shows activity. You can then connect to the programming software and check the functioning.



- **Updating via USB using the programming software:**
  - Download the latest firmware file (that has the **.tf3** extension) from the manufacturer's website.
  - Click on the "***Connection type***" menu in the programming software.
  - Click 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.

Using this option, you can also update devices with a lower major firmware version (e.g., v6), which are not compatible basically with the latest software, but can be made compatible by updating.

7.2 Updating remotely over the internet

It is also possible to update the firmware of the ***Pager4*** 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 ***Pager4*** device’s firmware 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

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

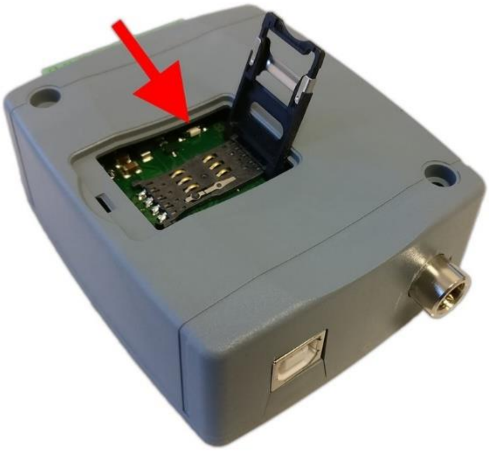
Restoring the factory default settings will be refused by the device if the “***Locked***” option has been selected in the “***Locking the device***” section, in the “***Advanced settings***” menu. In this case, the software will show an error message about that, after the information message shown right after the confirmation, when the factory default settings are restored using the software. 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.

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

8.1 Restoring the factory default settings using the programming software

To restore the factory default settings, click on the “***Restore factory default settings***” button in the “***Connection type***” menu. The reset process may take more than 1 minute, and 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 without entering the device password, but the reset cannot be performed if the device lock option has been enabled in the settings.

8.2 Restoring the factory default settings using the reset button



- Power up the device.
- Long press the reset button for at least 8 seconds, and then release. The reset button is placed on the electronic board, near the corner of the SIM card holder, closed to the status LED (see the picture on the right-hand side). It is easier to access the button if you open the SIM card holder.
- After releasing the button, the status LED will show permanent red light first, and then flashing red light, until the device creates the clean configuration. This process may take up to 1 minute.
- In the meantime, you can install the SIM card and close back the SIM card holder.
- The reset process has completed when the device has connected to the GSM network and the status LED shows a flashing green light.

9 Package content

- ***Pager4*** + terminal connector
- GSM or WiFi antenna (depending on the product model)
- 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