ecoLINE PRO

INSTALLATION AND APPLICATION MANUAL

for device version v2.00
Document version 2.0 16.09.2020

Product models:

- **ecoLINE PRO 2G.IN4.R1**
- **ecoLINE PRO 3G.IN4.R1**
- **ecoLINE PRO 3GA.IN4.R1**
- **ecoLINE PRO 4G.IN4.R1**
- **ecoLINE PRO 4GA.IN4.R1**

Table of contents

1 ecoLINE PRO operation 4
1.1 Key functions of the product 4
1.2 Differences between the 2G, 3G, 3GA, 4G and 4GA models 4
1.3 Under Voltage Lock Out (UVLO) function 4
1.4 Remote monitoring application overview 5
1.4.1 Event sending and acknowledging 5
2 Terminal wiring and putting into operation 6
2.1 Input wiring 6
2.2 Connections and wiring 6
2.3 SIM card holder 7
2.4 Connecting the antenna 7
2.5 Installation 7
2.6 Putting into operation 8
2.7 LED indicator signals 8
2.8 Technical specification 8
3 Configuring the ecoLINE PRO 9
3.1 The user interface and configuration options of the software 9
3.2 Methods for connecting to the device 9
3.2.1 Configuring directly via USB 10
3.2.2 Remote connecting to devices via cloud service 11
3.2.3 Remote connecting to devices which are using the TEX-MVP protocol 14
3.2.4 Remote connecting to devices which are using the TELLMon protocol 15
4 ecoLINE PRO programming software usage and feature descriptions 16
4.1 Connection menu 16
4.1.1 Viewing the settings options and configuring offline 16
4.1.2 Connection type 17
4.1.3 Device register 18
4.1.4 Server register 20
4.2 Device settings menu 21
4.2.1 General 22
4.2.2 Inputs 26
4.2.3 Output 28
4.2.4 Mobile devices 30
4.2.5 Functions and permissions 32
4.3 Device status menu 34
4.3.1 Status monitoring 34
4.3.2 Event monitoring 36
4.4 Software settings menu 38
4.4.1 Settings 38
4.4.2 About 39

5 Transparent serial port 40
5.1 Remote programming of alarm control panels 40
5.1.1 Paradox alarm systems 41
5.1.2 DSC alarm systems 45
5.1.3 Premier and Premier Elite alarm systems 48
5.1.4 Bentel alarm systems 51
5.1.5 Inim alarm systems 54
6 Arming and disarming the alarm control panel through the mobile application 58
7 Updating the firmware 59
7.1 Updating via USB 59
7.2 Updating remotely over the internet 59
8 Restoring the factory default settings 60
9 Contents of the package 60
10 About the manufacturer 60

1 ecoLINE PRO operation

1.1 Key functions of the product

The basic function of the ***ecoLINE PRO*** is forwarding reports of alarm control panels to remote monitoring station over the mobile Internet, using multiple protocols, as well as sending Push messages to users about these reports.

Features:

- 4 configurable NO/NC contact inputs for sending custom reports.
- 1 NO relay output controllable in the mobile application.
- Forwards reports of the connected alarm system and events generated by own inputs to remote monitoring station over the Internet, up to 2 IP addresses, using SIA IP DC-09, TELLMon or TEX protocol.
- **ecoLINE PRO** multiplatform mobile application (iOS, Android).
- Sends Push messages about alarm system events and own input events to up to 20 registered mobile devices.
- Configurable Contact ID event codes for each contact input, including partition and zone options.
- Output control through the mobile application, which can also be used to arm or disarm the connected alarm system remotely.

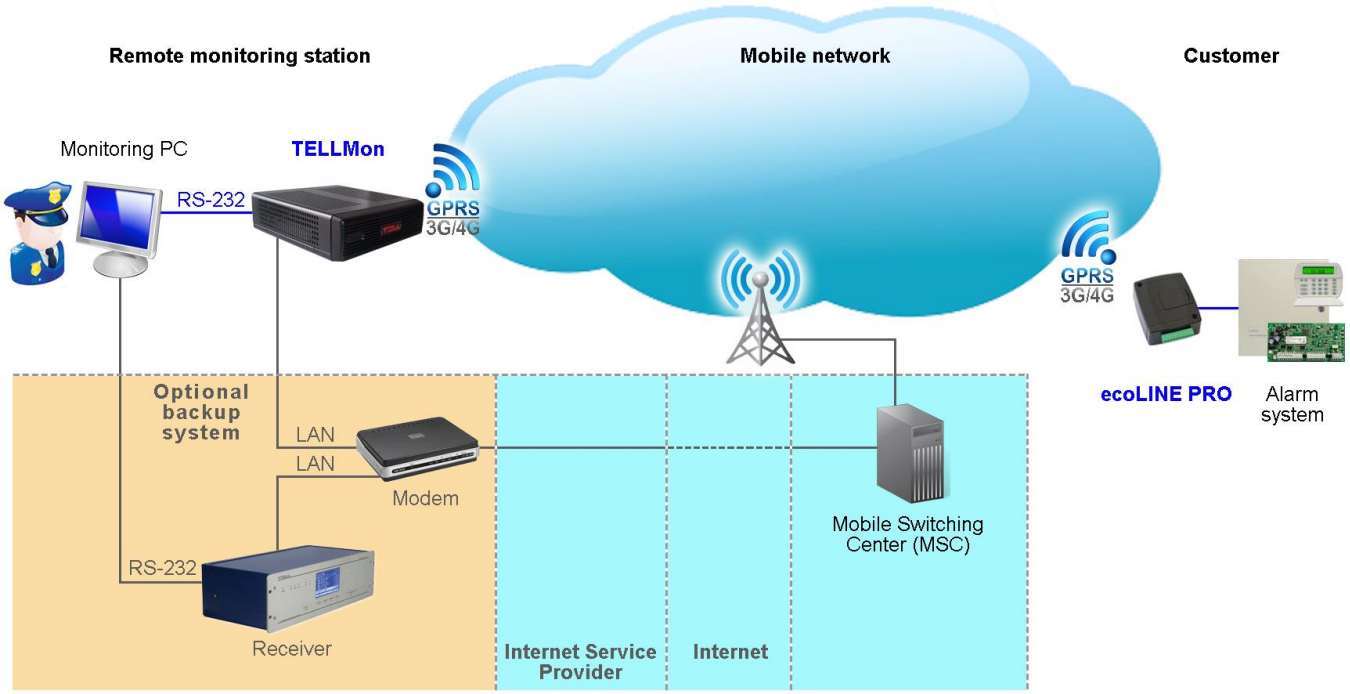
1.2 Differences between the 2G, 3G, 3GA, 4G and 4GA models

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, while the **3GA** model is equipped with a pentaband UMTS/HSPA modem that can be used worldwide. The **4GA** model is equipped with a multiband LTE modem which can be used in North America. There is no difference between the mentioned models with regard to the available functions or configuration.

1.3 Under Voltage Lock Out (UVLO) function

The **ecoLINE PRO** 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 the operational level.

1.4 Remote monitoring application overview



The **ecoLINE PRO** communicates with SIA DC-09 receivers, TELLMon receivers and TEX-MVP servers through the GSM service provider's mobile switching center using the GPRS/UMTS/LTE network, and then through the Internet. After processing and conversion, the receiver forwards the received data packages through a serial port towards the monitoring PC that runs the alarm monitoring software.

1.4.1 Event sending and acknowledging

The device attempts to sends the reports first to the configured primary IP address. If this fails, it will attempt to send the reports to the backup IP address. The device will send the ACK signal towards the alarm control panel only when it receives the ACK signal from at least one of the configured receivers (IP addresses). If the device does not receive an ACK signal from any of the configured receivers, it will attempt to resend the report up to 10 times per IP address. An exception to this is when the device is banned in the given receiver, since in this case it will not even attempt to send a report to that receiver. If the device still fails to send a report for the 10th attempt to a configured IP address, it will stop reporting the event and will no longer send notification on the given event, but the event will be shown in the event logs.

If there are no remote monitoring receiver IP addresses configured at all, the device will send ACK signals to the alarm control panel automatically.

Whether a remote monitoring receiver is configured or not, the device will send Push notifications to the registered mobile devices on the event categories enabled in the settings and by users in the mobile application.

2 Terminal wiring and putting into operation

2.1 Input wiring

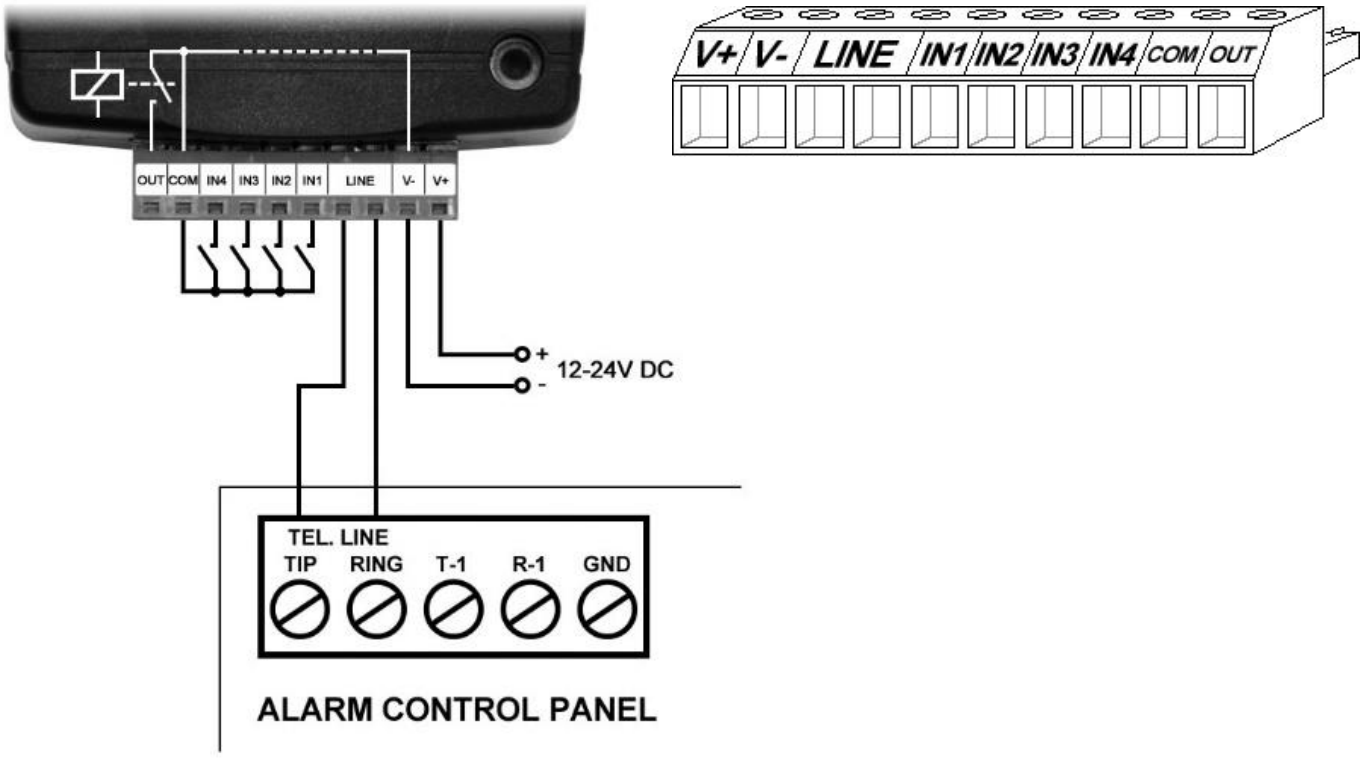
For the inputs, the normally closed or normally open dry contact should be connected between the given input (**IN1**…**IN4**) and the negative of the power input (**V-**) or the **COM** terminal.

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**) and the **V-** terminal (or the **COM** 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**) and the **V-** terminal (or the **COM** terminal) becomes open.

2.2 Connections and wiring

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!



System terminal inputs and outputs:

V+ Supply voltage 12…24V DC (min. 500mA)
V- Supply voltage negative
LINE Simulated phone line output (connect to alarm system phone line input terminals)
IN1 Dry contact input 1
IN2 Dry contact input 2
IN3 Dry contact input 3
IN4 Dry contact input 4
COM Common negative for the contact inputs and the output (potential equivalent with **V-**)
OUT Relay output (switches the negative, max. 1A)

Attention!

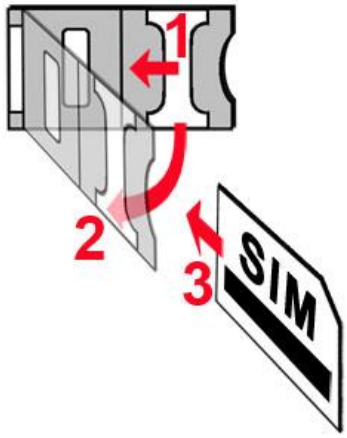
Although the *COM* and *V-* terminals are equivalent, due to the design of internal circuit protections, the *COM* terminal shall not be used as negative input for powering the device, because this may damage the device! The *COM* terminal should only be used for connecting the contact inputs and the relay output!

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

2.3 SIM card holder

The SIM card holder can be accessed by removing the cover of the aperture found on the device enclosure. The cover can be removed by pressing it with your fingernail towards the 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 **ecoLINE PRO** device should be chosen according to the services of the device. For communication with receivers and servers and use with the mobile application, it requires a SIM card with available mobile Internet, that may use either public or private APN.

- 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 to open the holder.
- **3.** Slide the SIM card into the opened part with the contacts facing down, as shown in the figure.
- Fold back the opened part together with the SIM card.
- Secure the SIM card by pressing down carefully the metallic security lock and pulling it towards the side of the enclosure until you hear a click.

2.4 Connecting the antenna

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

2.5 Installation

Please check the environment before installing:

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

2.6 Putting into operation

- ***Disable voicemail and notification in SMS about missed calls on the SIM card installed into the device.***
- ***The device can handle the SIM card's PIN code. If you wish to use the PIN code management, configure the SIM card's PIN code in the programming software in the "Device settings / General" section. Otherwise disable PIN code request 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 (12-24V DC). Make sure that the power source is sufficient for the operation of the **ecoLINE PRO** device. The nominal current consumption of the **ecoLINE PRO** 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.

2.7 LED indicator signals

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

2.8 Technical specification

Supply voltage range:	12…24V DC
Nominal current consumption:	120mA
Highest current consumption:	500mA @ 12V DC, 250mA @ 24V DC
Operating temperature:	-20ºC - +70ºC
Transmission frequency:	
2G model:	850/900/1800/1900 MHz
3G model:	900/2100 MHz @UMTS, 900/1800 MHz @GSM
3GA model:	800/850/900/1900/2100 MHz @UMTS 850/900/1800/1900 MHz @GSM
4G model:	900/1800 MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE
4GA model:	B2/B4/B5@WCDMA, B2/B4/B5/B12/B13@LTE
Highest load supported on output:	1A @ 24VDC
Modem type:	
2G model:	Quectel M95
3G model:	Quectel UG95
3GA model:	Quectel UG96
4G model:	Quectel EG91-E
4GA model:	Quectel EG91-NA
Dimensions:	84 x 72 x 32mm
Net weight:	200g
Gross weight (packed):	300g

3 Configuring the ecoLINE PRO

The **ecoLINE PRO** can be configured the following ways:

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

The **ecoLINE PRO** 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 can be downloaded from the manufacturer's website (http://www.tell.hu).

3.1 The user interface and configuration options of the software

The user interface language can be selected during installation.

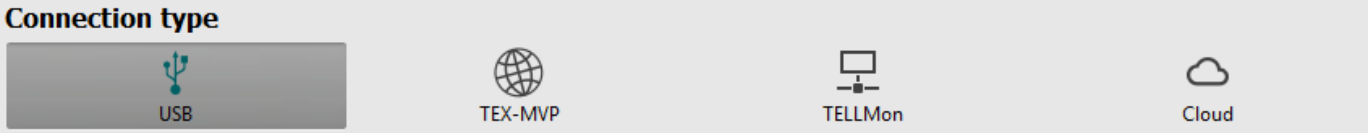
The user interface appearance can be changed using the "***Skin***" dropdown-menu found in the "***Software settings***" / "***Settings***" menu, where you can choose out of multiple appearance themes.

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

Built-in help:

Some settings options in the software have an additional icon: or . By holding the mouse pointer on the icon, a tooltip will be shown with information about the given option. Options with the icon require expertise and special attention!

3.2 Methods for connecting to the device



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

USB: direct connection using a USB A-B cable.

TEX-MVP: remote connection through the Internet via the TEX-MVP server. This option can be used by central monitoring stations that own a TEX-MVP server.

TELLMon: remote connection through the Internet via the TELLMon receiver. This option can be used by central monitoring stations that own a TELLMon receiver.

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

3.2.1 Configuring directly via USB

To start programming the device, follow the instructions below:

- Open the **ecoLINE PRO** 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-B cable.
- Enter the connection password.
  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Installer permission: can only access settings enabled by the super administrator.
  - Connecting without password: only restoring the factory default settings is available, if the device has not been locked.
- Click on the "***Connect***"  button.
- If the wrong password is entered, the software connects to the device, but the same functions will be available as when connecting without a password. To try a different password, close the connection using the "***Disconnect***"  button, enter the new password and then connect again using the "***Connect***"  button.
- The software connects to the device using standard HID driver which is integrated in Windows operating systems, thus there is no need to install special USB drivers. When the device is connected to USB for the very first time, the Windows operating system installs the drivers automatically.
- The connection status is indicated by the USB status icon placed in the upper left corner of the program window:

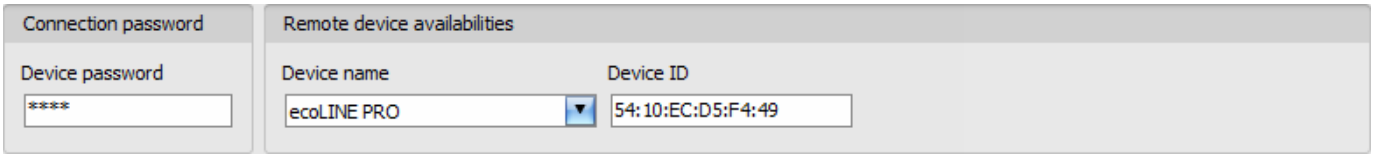
   USB disconnected (green)

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

3.2.2 Remote connecting to devices via cloud service

This connection type can be used if the *ecoLINE PRO* device is connected to the cloud. A prerequisite for this is that the APN should be configured, 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 have to arrange with the mobile service provider to open the given private APN for accessing the cloud server IP address at 52.30.109.179, port: 2020. In order to connect to the cloud, cloud usage should be enabled in the settings, in the "*Functions and permissions*" menu. 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 **ecoLINE PRO** programming software will be established through the cloud server operated by the manufacturer.



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

Device ID: the device identifier of the **ecoLINE PRO** device to which you wish to connect. The format of this unique, burned-in during production and thereby unchangeable device identifier used for cloud connection is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

You can read the device ID of the given device in the "***Device ID***" section of the "***Status monitoring***" menu, when connected to the device. The device will also send its device ID as a reply to your request for connecting to the cloud server, sent by SMS to the device, about which you can read more below.

Connecting to the device through the cloud server:

- Select the "***Cloud***" option in the "***Connection type***" section.
- If you have registered the device in the "***Device register***" menu, select the device you want to access from the "***Device Name***" drop-down menu, or enter the device ID of the device in the "***Device ID***" field, and the connection password in the "***Device password***" field.

  Connection password:

  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Installer permission: can only access settings enabled by the super administrator. The installer password should be configured 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 based server. In this case, skip the SMS sending process mentioned below. You can enable cloud usage in the "***Functions and 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 in the device.

  The device accepts the request for connecting to the cloud from any phone number, if the valid device password is added in the message. The device password should be written in the message at the beginning, as specified below. Commands sent with a missing device password or a wrong password, will be ignored by the device and it will not send any reply to these numbers.

  The request command for connecting to the server is:

  ***device password*,connect#**

  device password: type the device password at the beginning of the message. The superadmin and installer passwords are both accepted (default superadmin password: 1234).

  Example on the usage of the command mentioned above: **1234,connect#**

  Send the mentioned request command for connecting to the server by SMS to the phone number of the SIM card installed into the device and wait for the device's reply. The device will immediately send the reply below, and will start connecting to the cloud:

  Connecting…

  The device will send a new message as soon as it connects to the cloud successfully:

  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 no reply is received 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. If you receive no message about a successful connection, it means that the device failed to connect to the cloud.

  Possible error messages:

Wrong password	Wrong superadmin or installer password
Missing APN	the APN is not configured

If the APN settings are not configured in the device, or if they are wrong, you can configure these using the following SMS commands:

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

Example on the usage of the commands mentioned above:

✶1234,apn=internet#

✶1234,apn=net,guest,guest#

Possible error messages:

Wrong password	Wrong superadmin or installer password
Denied (no permission)	No permission to change the APN with the installer password
Changing the APN settings failed	Changing the APN settings failed (typing error in the message, or other error)

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

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

   disconnected (green)

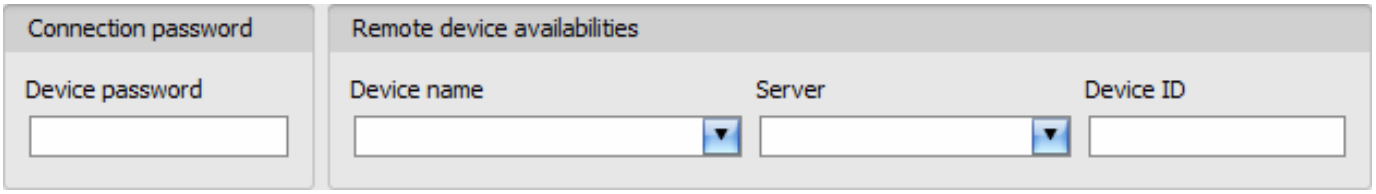
   connected (gray)

- After connecting using the valid password, you can configure the device, change settings, download event logs and monitor system status. The program will read the settings from the device automatically after connecting to the device.
- To disconnect from the device click on the "***Disconnect***"  button.

3.2.3 Remote connecting to devices which are using the TEX-MVP protocol

This connection type can be used if the *ecoLINE PRO* device you wish to connect remotely to, is connected to a TEX-MVP server. Also use this connection type if the *ecoLINE PRO* device is connected to a TELLMon receiver and the device is configured to communicate with the TELLMon receiver using the TEX-MVP protocol.

With this connection type, connection between the device and the **ecoLINE PRO** programming software can be established through the server/receiver where the device is online.



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

Server: the name of the server or receiver where the device is online. The server availabilities should be recorded in advance in the "***Server register***" menu.

Device ID: the "TEX" identifier of the **ecoLINE PRO** to which you wish to connect to. The format of the "TEX" device identifier is: **FFF** (3 hexadecimal characters).

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

- Select the "***TEX-MVP***" option in the "***Connection type***" section.
- If you have registered the device in the "***Device register***" menu, select the device you want to access from the "***Device Name***" drop-down menu, or select the server/receiver where the device is online, from the "***Server***" drop-down menu, and enter the device identifier in the "***Device ID***" field, and the connection password in the "***Device password***" field. The server availabilities should be recorded in advance in the "***Server register***" menu.

  Connection password:

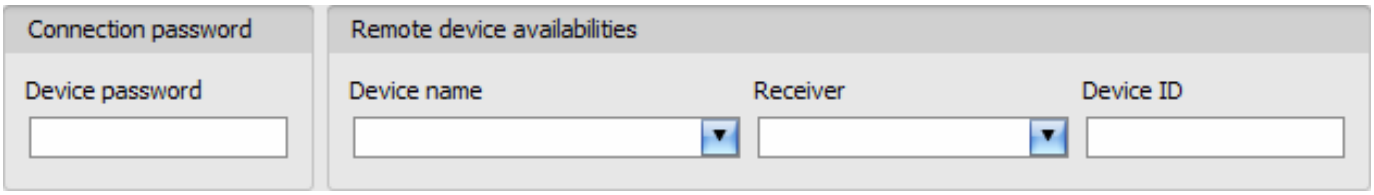
  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Installer permission: can only access settings enabled by the super administrator. The installer password should be configured separately (see chapter "***Connection type***").
  - Connecting remotely without a password is not possible.

- Click the "***Connect***" button.
- The connection status is indicated by the status icon in the top left corner of the program window:
  disconnected (green)
  connected (grey)
- After connecting using the valid password, you can configure the device, change settings, download event logs and monitor system status. The program will read the settings from the device automatically after connecting to the device.
- To disconnect from the device click on the "***Disconnect***" button.

3.2.4 Remote connecting to devices which are using the TELLMon protocol

This connection type can be used if the *ecoLINE PRO* device you wish to connect remotely to, is connected to a TELLMon receiver and the device is configured to communicate with the TELLMon receiver using the TELLMon protocol.

With this connection type, connection between the device and the **ecoLINE PRO** programming software can be established through the receiver where the device is online.



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

Receiver: the name of the receiver where the device is online. The receiver availabilities should be recorded in advance in the "***Server register***" menu.

Device ID: the device identifier of the **ecoLINE PRO** device to which you wish to connect to. The format of this unique, burned-in during production and thereby unchangeable device identifier used for the TELLMon protocol is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

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

- Select the "***TELLMon***" option in the "***Connection type***" section.
- If you have registered the device in the "***Device register***" menu, select the device you want to access from the "***Device Name***" drop-down menu, or select the receiver where the device is online, from the "***Server***" drop-down menu, and enter the device identifier in the "***Device ID***" field, and the connection password in the "***Device password***" field. The receiver availabilities should be recorded in advance in the "***Server register***" menu.

  Connection password:

  - Super administrator permission: full access to all settings. (Default password: **1234**).
  - Installer permission: can only access settings enabled by the super administrator. The installer password should be configured separately (see chapter "***Connection type***").
  - Connecting remotely without a password is not possible.
- Click on the "***Connect***" button.
- **The *ecoLINE PRO* device that communicates using the TELLMon protocol is not online continuously. The device connects to the receiver only when it sends a supervision or event message, therefore after clicking the "*Connect*" button, you have to wait until the device next connects to the receiver for sending a supervision or event message. This is when the programming software will have possibility to connect to the device. Therefore, if the device is configured to rarely send supervision messages towards the TELLMon receiver, in this case the programming software will be able to connect to the device after a long time only (depending on the interval of supervision message sending).**
- The connection status is indicated by the status icon in the top left corner of the program window:

  disconnected (green)

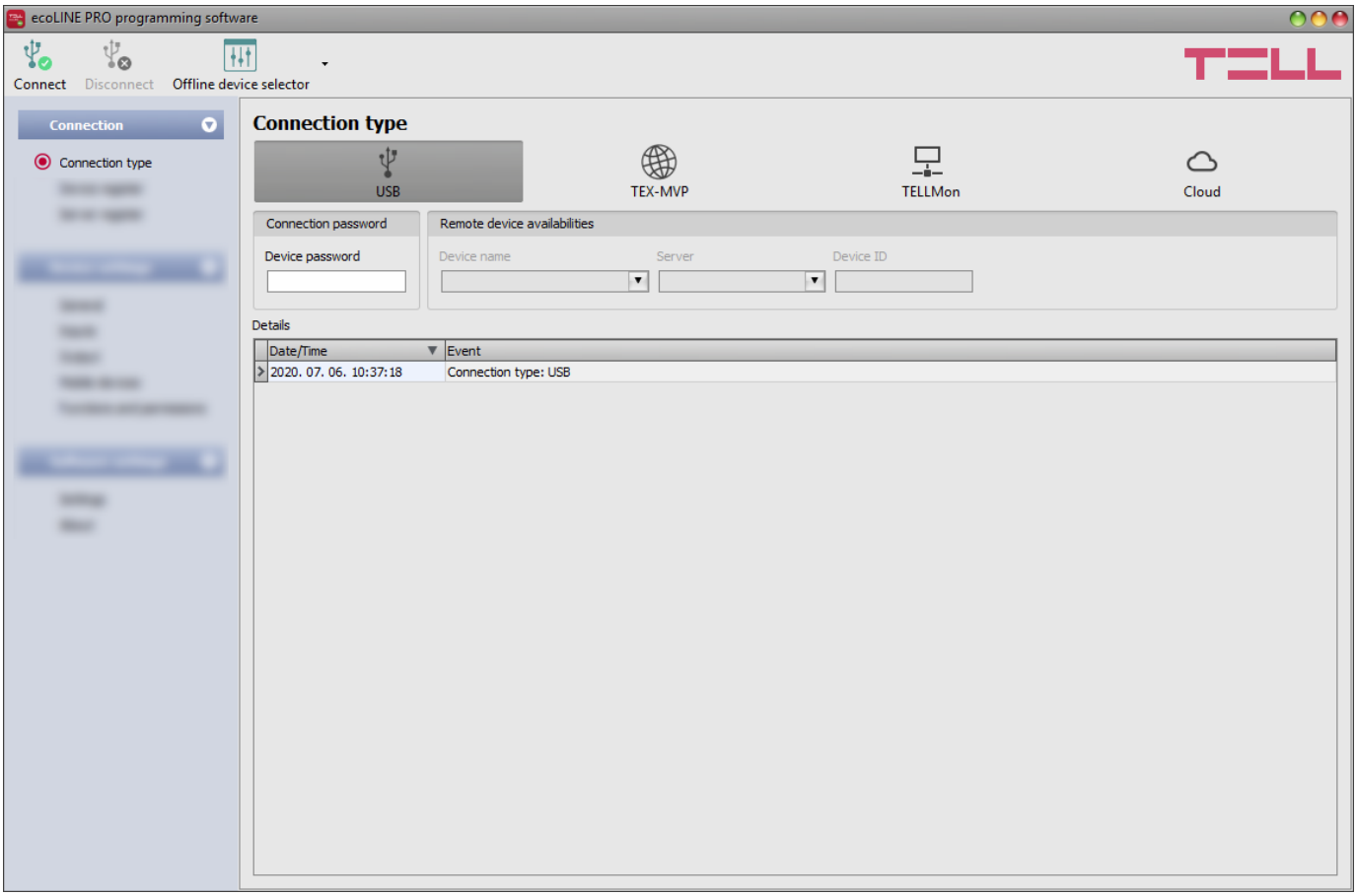
  connected (gray)

- After connecting using the valid password, you can configure the device, change settings, download event logs, monitor system status and perform controls. The program will read the settings from the device automatically after connecting to the device.
- To disconnect from the device click on the "***Disconnect***" button.

4 ecoLINE PRO programming software usage and feature descriptions

4.1 Connection menu

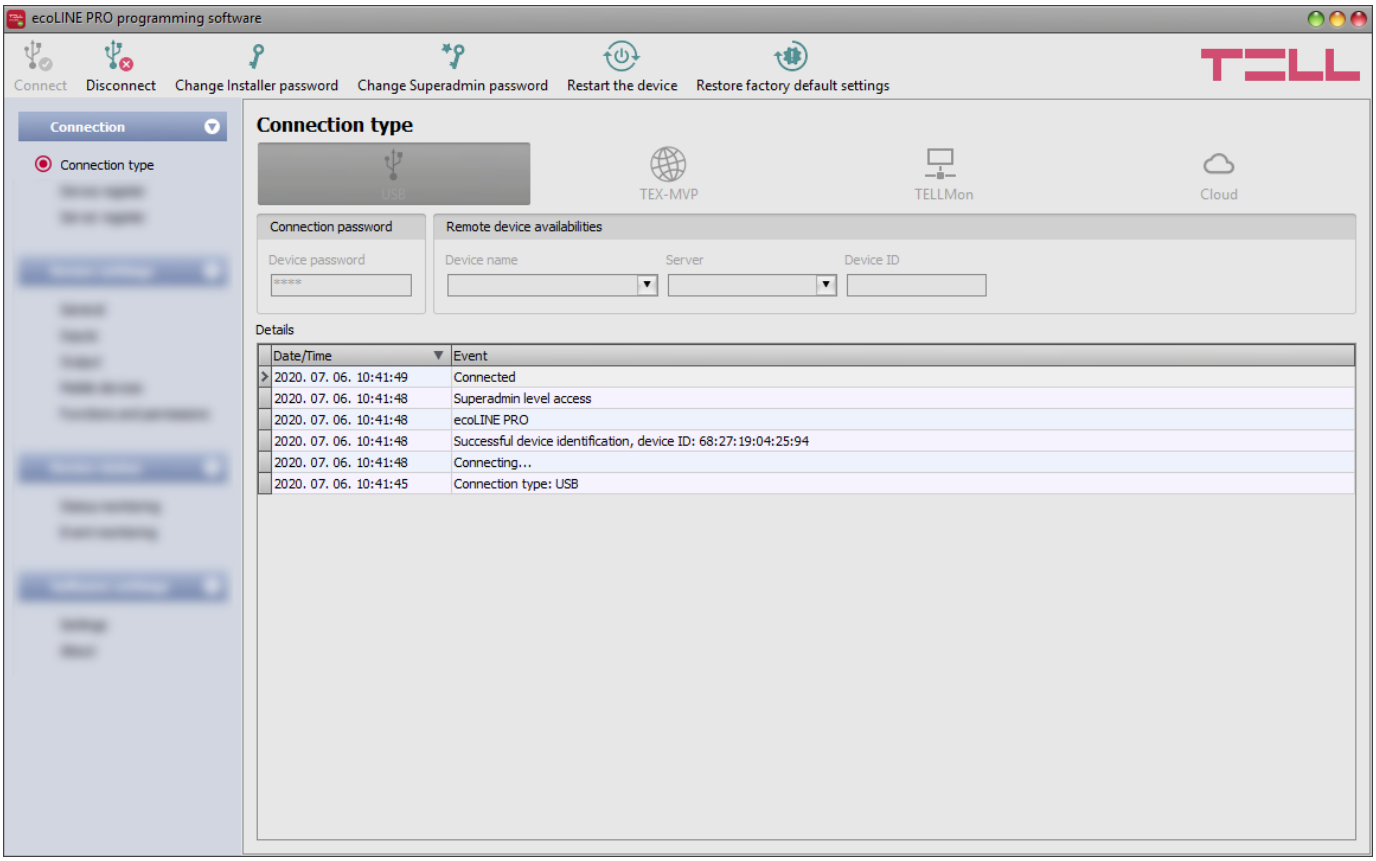
4.1.1 Viewing the settings options and configuring offline



Using the "***Offline device selector***" it is possible to view the settings options of the **ecoLINE PRO** device and to configure and save the settings in advance offline, without connecting the device.

If you wish to view the settings options of the **ecoLINE PRO** device, 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 user level from the drop-down menu, and then click on the "***Offline device selector***" button to load the settings options of the selected permission level.

4.1.2 Connection type



In the "***Connection type***" menu the type of connection can be selected (USB or different options for connecting over the Internet), information can be seen about the connection process, and the installer and superadmin password can be changed. The default superadmin password is **1234**. If you wish to use the installer level access as well, for this the password should be configured separately by clicking on the "***Change Installer password***" button (for "***Actual password***" enter the superadmin password).

Available options:

- Change Installer password:

  The installer level password can be changed after clicking on this button.

- Change Superadmin password:

  The superadministrator level password can be changed 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: ^ ~ < > = | $ % " '.

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

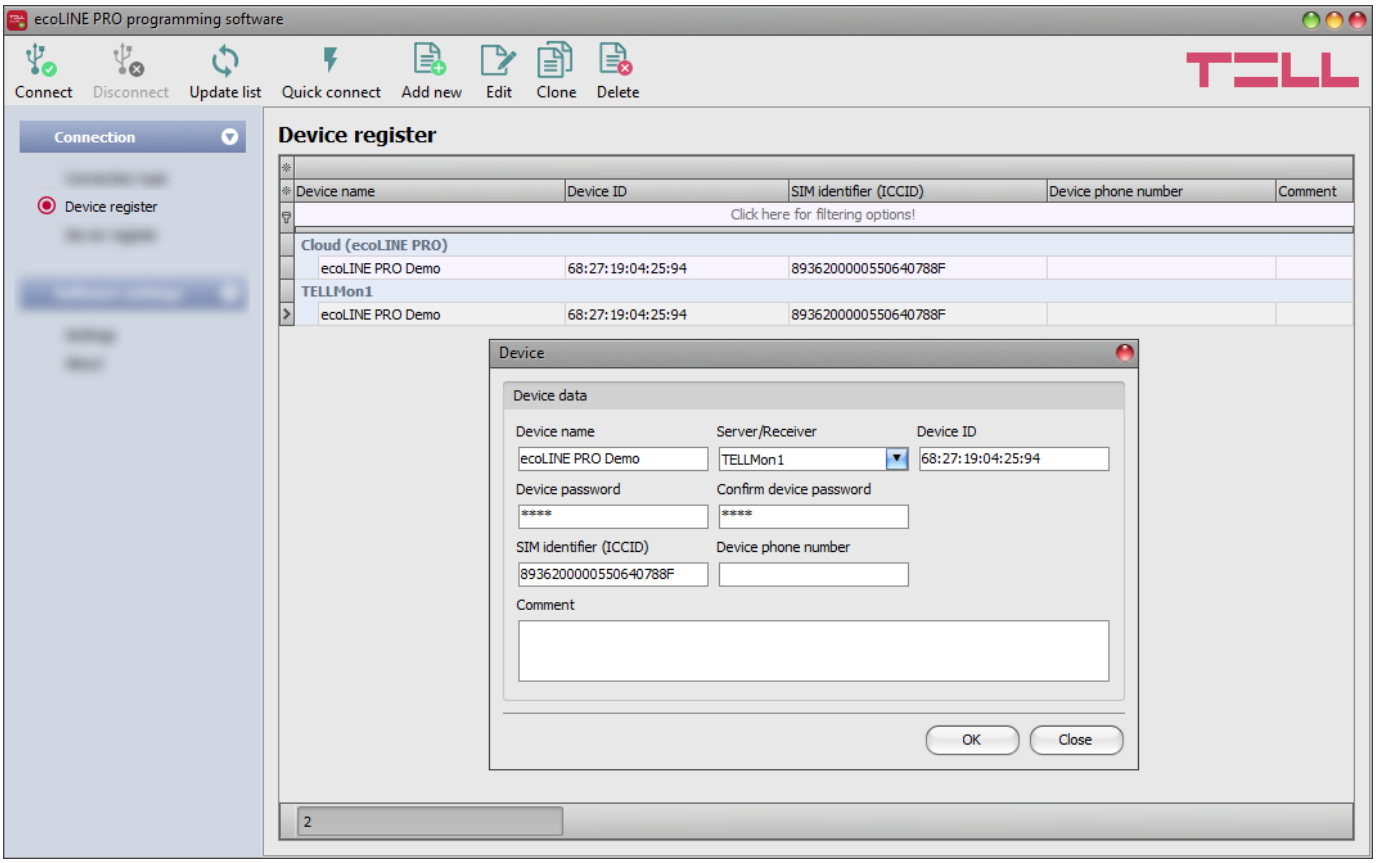
- Restart the device:

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

- Restore factory default settings:

  By clicking on this button, you can restore the factory default settings in the device. Restoring the factory default settings will erase the actual settings, therefore please save your settings if needed. The reset process may take more than 1 minute and involves a device restart. Wait until the device restarts and the LED indicator starts working again. The option of restoring the factory default settings is also available without entering the device password. The factory default settings cannot be restored if the device has been locked in the settings. If you have forgotten the device passwords and the device is locked, only the manufacturer can restore the factory default settings in the service center.

4.1.3 Device register



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 also 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, using 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.

If you add a new device availability in the connection type section, the program will add it automatically to the device register database by using the device ID as device name, which you can then change by editing the given entry. 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 available on the product's page on the manufacturer's website.

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

 : update the records from database

 : quick remote connect to the selected device

 : add new device

 : clone entry (duplicate)

 : edit entry

 : delete entry

Data stored by the device register:

Device name: custom device name

Server/Receiver: you can configure multiple remote availabilities for the same device (Cloud, TELLMon, TEX-MVP), according to what type of server or receiver the device connects to. The availabilities 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. If a device is available on multiple servers or receivers, and you want to record the availabilities 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.

To make the device registration easier, for the Cloud and the TELLMon server type the program will automatically read the device identifier from the device connected via USB, and will insert this in the appropriate field.

Device ID: the device identifier. The format of the device identifier is:

- for cloud usage and the TELLMon protocol: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters, unique, burned-in during production and thereby unchangeable device identifier). The device ID (used for cloud connection and the TELLMon protocol) of the connected device is shown in the “***Status monitoring***” menu / “***Device ID***” field.
- for the TEX-MVP protocol: **FFF** (3 hexadecimal characters).

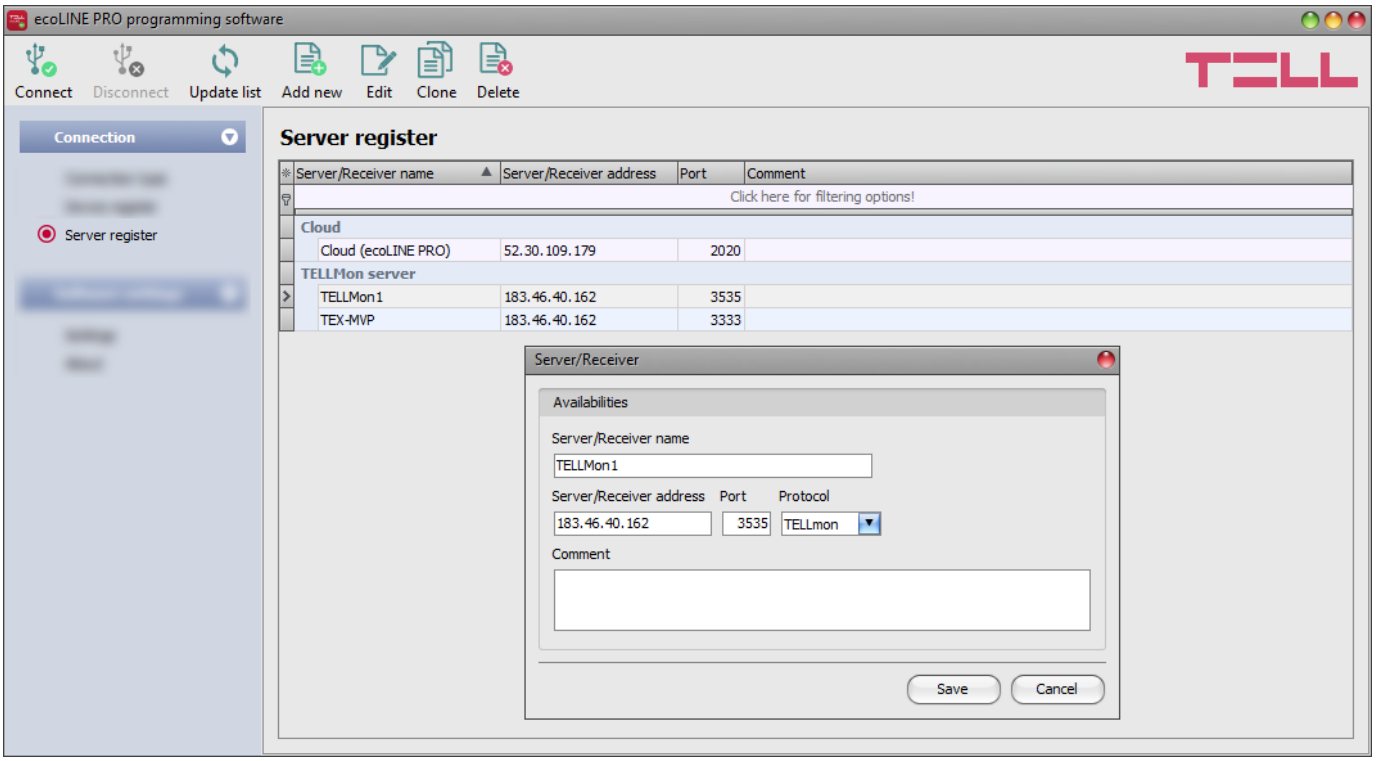
Device password/Confirm device password: the superadmin or installer password configured in the given device, depending on which one you want to use for connecting to the device.

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

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

4.1.4 Server register



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 these with the 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 also edit, delete and clone entries for easy adding of servers or receivers with similar contact details.

Function buttons available in the "***Server register***" menu:

: update the records from database

: add new server or receiver

: clone entry (duplicate)

: edit entry

: delete entry

Data stored by the server register:

Server/receiver name: custom server/receiver name.

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

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

Protocol: the communication protocol used by the server/receiver.

Server password: for the TEX protocol the 20 hexadecimal-character server password (5x4 characters separated by hyphen) is required.

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

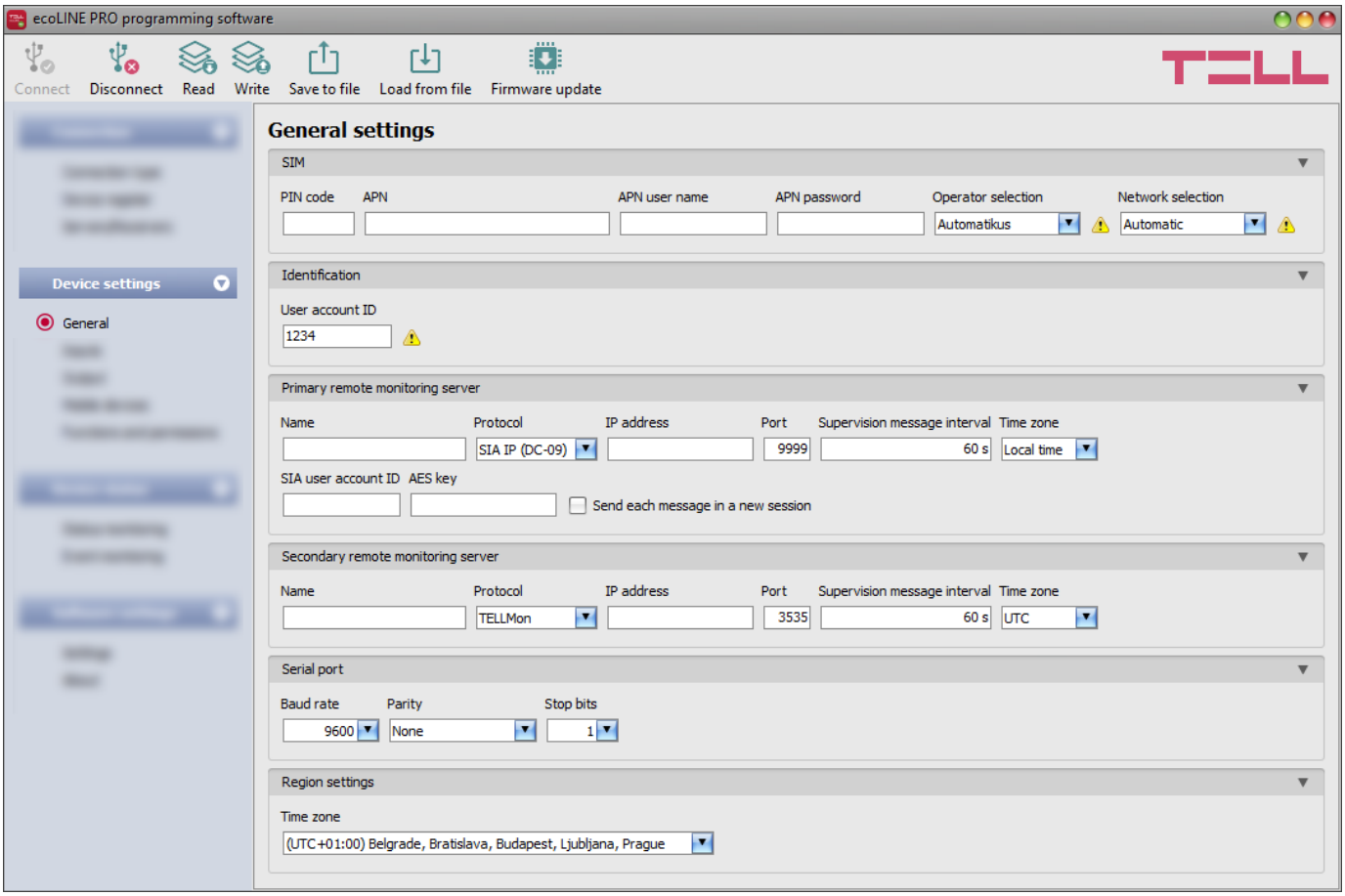
4.2 Device settings menu

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

- **Changing the device settings**: In order to change the device settings, reading the settings stored in the device is needed, which is done automatically after connecting to the device. However, you can also read the settings manually anytime by clicking on the "***Read***"  button in any submenu under the "***Device settings***" menu group. Writing the new settings into the device using the "***Write***"  button is not possible until the settings are read. After making changes in the settings, write the settings into the device by clicking on the "***Write***"  button. The program will warn you to write the settings when leaving a page where changes have been made.

- **Overwriting the device settings**: If you want to completely overwrite the settings, you can import and write data from a from a previously made system backup. To create a system backup file, configure the desired settings in the submenus, and then click on the "***Save to file***"  button in the "***General***" device settings menu. You can import the saved backup into the program using the "***Load from file***"  button, and then write imported settings into the device by clicking on the "***Write***"  button. This is useful when you want to configure many devices with the same settings.

4.2.1 General



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

Available options:

- Reading the settings from the device:
  To read the settings from the device click on the "***Read***" button. This will read all settings in all menus.
- Writing the settings into the device:
  After changing the settings or entering new settings, in order 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.
- Updating the firmware:
  By clicking on the "***Firmware update***" button, the firmware of the device can be updated. Clicking on the button, opens a pop-up window, where you can browse the firmware file with **tf3** extension. When firmware upload is finished, the progress window closes automatically and 5 seconds later the device restarts with the new firmware.

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

SIM:

PIN code: if you wish to use PIN code management, enter in this section the PIN code of the SIM card installed into 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. If the wrong code is configured 3 times consecutively, the SIM card will reach the PUK code request stage. In this case install the SIM card into a cellphone, unlock the card by entering the PUK code when requested, and configure the valid PIN code in the device settings.

APN: the APN name necessary to connect to the Internet. (ask this from the GSM service provider of the SIM card installed into the device). If no APN is configured, the device will not be able to connect to the Internet and thereby it cannot operate.

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

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

Network selection: mobile network management is automatic by default in the device. If you experience problems with the stability of the mobile network in the given location, i.e. the device switches frequently from one network to another, you can select manually the network you wish to use.

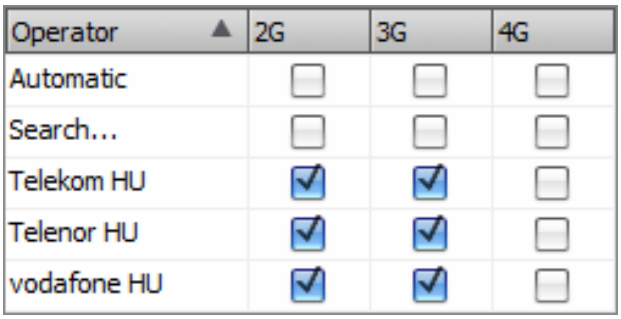
Available options:

- **Automatic**: the device will select the network automatically.
- **2G only**: use 2G (GPRS) network only.
- **3G only**: use 3G (UMTS) network only
- **4G only**: use 4G (LTE) network only

3G network usage is supported by the 3G(A).IN4.R1 and the 4G(A).IN4.R1 model of the *ecoLINE PRO* only! 4G network usage is supported by the 4G(A).IN4.R1 model only!

Operator selection: using this drop-down menu, you can select a mobile operator available with the given SIM card. For getting the list of available operators, choose the "***Search…***" option in the drop-down menu, which will start the operator search. In order to perform the operator search, the device will restart the modem and will reconnect to the mobile network. 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 will be updated automatically in the "***Operator selection***" drop-down menu according to the search results.

If you select and set an operator, the device will use solely the selected operator's network. Please note that the search may also result 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).
Attention! 2G modems are not capable to identify these networks, therefore this information is not available in the product model equipped with a 2G modem. The default setting is the "***Automatic***", i.e. the device will automatically choose the operator preferred by the given SIM card.

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 are also sent using the user account ID configured in this section. **The device replaces the user account ID in the messages received from the connected alarm control panel automatically with the identifier configured here.** The user account ID length is 4 hexadecimal characters and the following characters can be used: 0..9, A, B, C, D, E, F.

Note! The user account ID and server settings are only needed if reporting to CMS is used.

Primary remote monitoring server:

In this section you can configure the primary monitoring server or receiver availabilities.

Name: CMS server or receiver name. The name entered in this section is used for identification of the server/receiver within the program.

Protocol: select the appropriate communication protocol for the given server or receiver from the drop-down menu. Each protocol uses the TCP network protocol.
Available protocols: **SIA IP** (ANSI/SIA DC-09-2007), **TELLMon**, **TEX**.

IP address: CMS server or receiver IP address. 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 open the private APN to access the given server/receiver IP address.

Port: CMS server or receiver communication port number.

Supervision message interval: in this section you can configure the supervision message sending interval, which can be configured from 30 to 86400 seconds, depending on the selected communication 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.

SIA user account ID: in case of using the ***SIA DC-09*** protocol, 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!

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 have to 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, in case of the ***SIA DC-09*** protocol it can be enabled to send each message in a new TCP session.

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.

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.

Secondary remote monitoring server:

In this section you can configure the secondary or backup monitoring server or receiver availabilities. The configuration options are the same as those for the primary server.

Serial port:

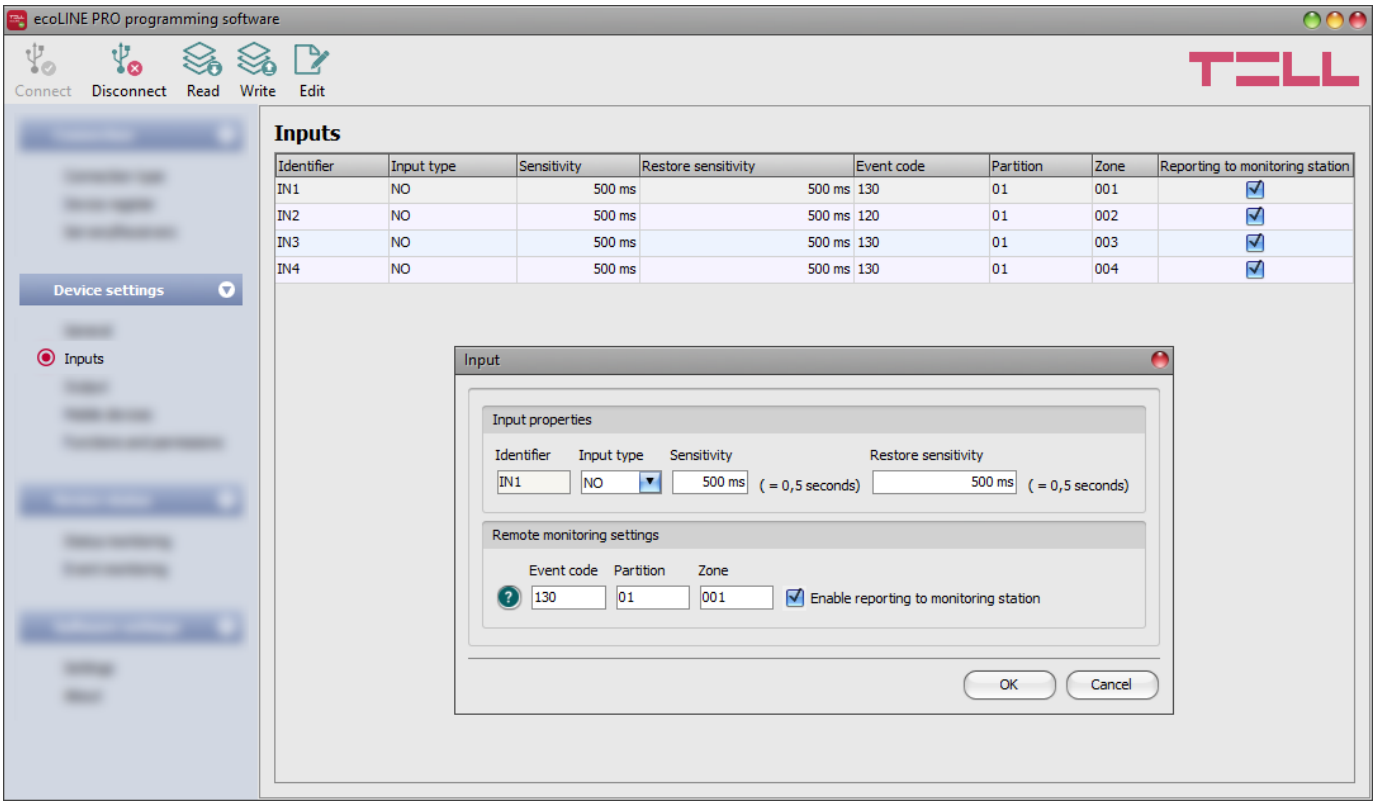
In this section you can configure the transparent serial port settings. The serial port on the device enables transparent data communication between the device and the ***Remote Serial Client*** software developed for this purpose. The purpose of the serial port is to enable remote programming of the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

Region settings:

Time zone: using the drop-down menu you can select the time zone according to the location of installation. The device sets the system time according to the selected time zone. If the setting is wrong, there will be a difference between the system time and the local time, which affects the timestamps of the events.

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

4.2.2 Inputs



In the "***Inputs***" menu you can configure the default state of the 4 contact inputs, input activation and restore sensitivity, the event code, partition and zone number used for reporting to a remote monitoring station, and you can also enable or disable reporting of input events to a monitoring station.

You can enable Push message sending about input events in the "***Mobile devices***" menu. The text of Push messages can be configured for each input separately in the mobile application.

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, in order 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 the settings have to be written in the device in order to be applied after a change is made. For this, click on the "*Write*" button.

Input properties:

Identifier: the identifiers of the inputs cannot be changed. They are used to identify the inputs in the program.

Input type: the input can be normally open (**NO**), or normally closed (**NC**). When set to **NO**, event is generated when the input circuit is closed, while when set to **NC**, opening the input circuit generates an event. The input is closed when the given input **IN1…IN4** is shorted to „**V-**" terminal (DC power negative) or to the **COM** terminal.

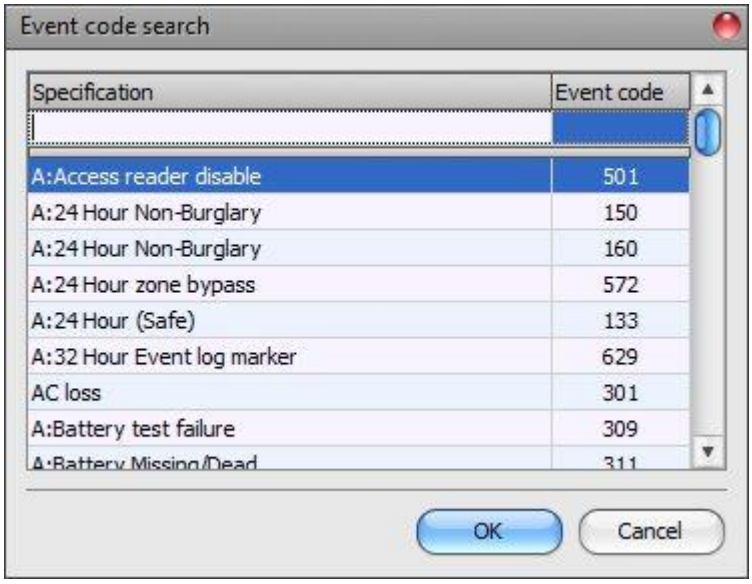
Sensitivity: state changes of the input shorter than the value entered in this section with regard to activation of the input are ignored by the device. The value can be configured from 200 milliseconds (0.2 seconds) to 60000 milliseconds (60 seconds).

Restore sensitivity / Unit of measure: state changes of the input shorter than the value entered in this section with regard to restoration of the input are ignored by the device. device. The value can be configured from 200 milliseconds (0.2 seconds) to 60000 milliseconds (60 seconds).

Remote monitoring settings:

Event code: in this section you can configure the 3-digit Contact ID event code, which you want to assign to the given input (e.g. 130 = burglar alarm). The event code consists of hexadecimal characters (0..9,A,B,C,D,E,F). The device associates the event type (new event / restore) to the event automatically, based on the configured input type (NO/NC) and the input state.

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



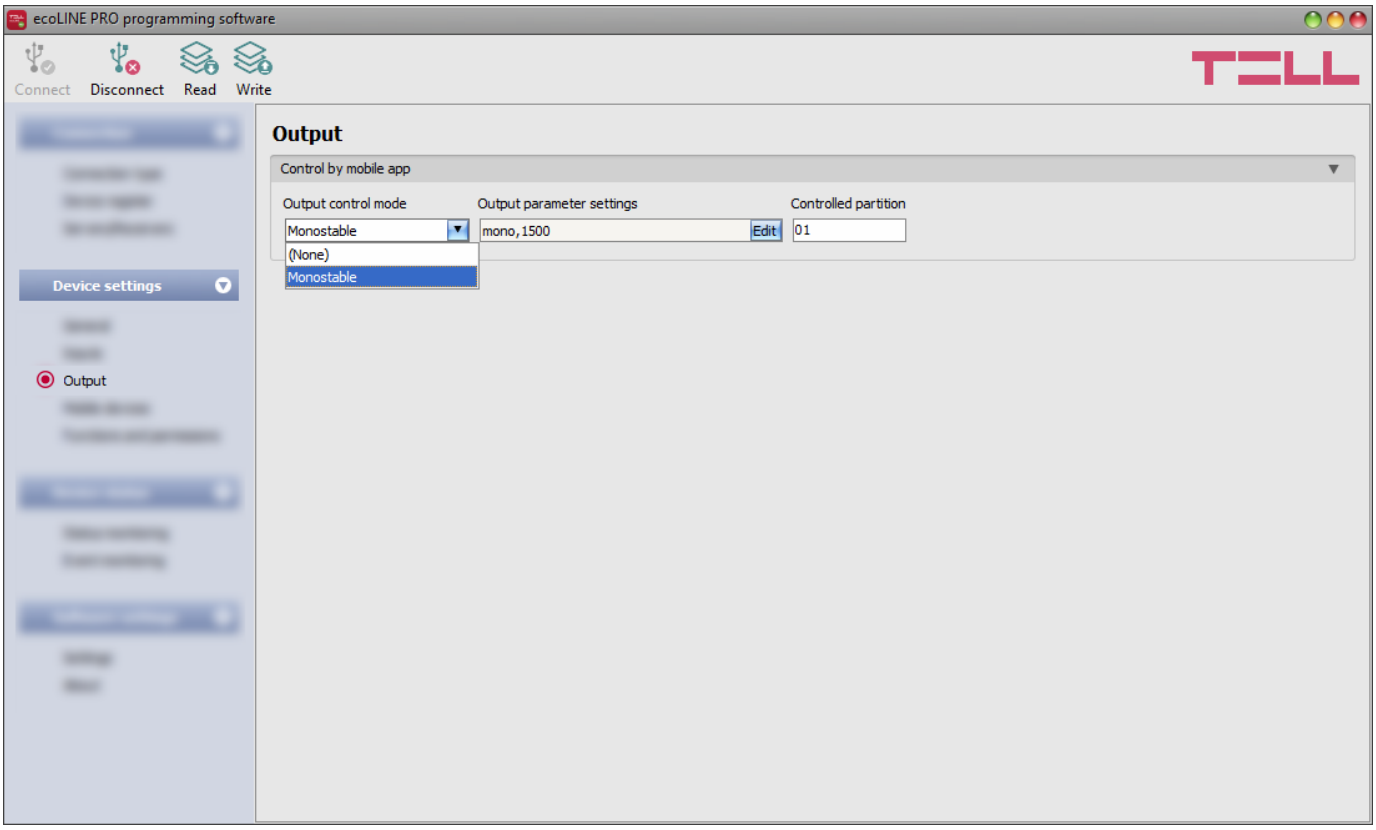
In the event code search tool you can search for events by name or by event code. For searching by name, start typing the name of the searched event code in the field under the "***Specification***" column header. For searching by event code, start typing the searched event code number in the field under 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, and then the program will paste this automatically into the event code input field, after clicking on the "***OK***" button.

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

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

Enable reporting to monitoring station: using this checkbox, you can enable or disable reporting of events generated by the given input to the remote monitoring station.

4.2.3 Output



In this menu you can configure the control mode of the device's relay output. The output can be solely controlled using the mobile application. When controlled by a user, the output will operate according to the configured control mode.
The output can be used to arm and disarm the connected alarm system using the mobile application, if the given alarm system supports arming and disarming by an external dry contact. Apart from this, the output can be used for other control purpose too, considering the load rating.

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, in order 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 the settings have to be written in the device in order to be applied after a change is made. For this, click on the "*Write*" button.

Control by mobile app:

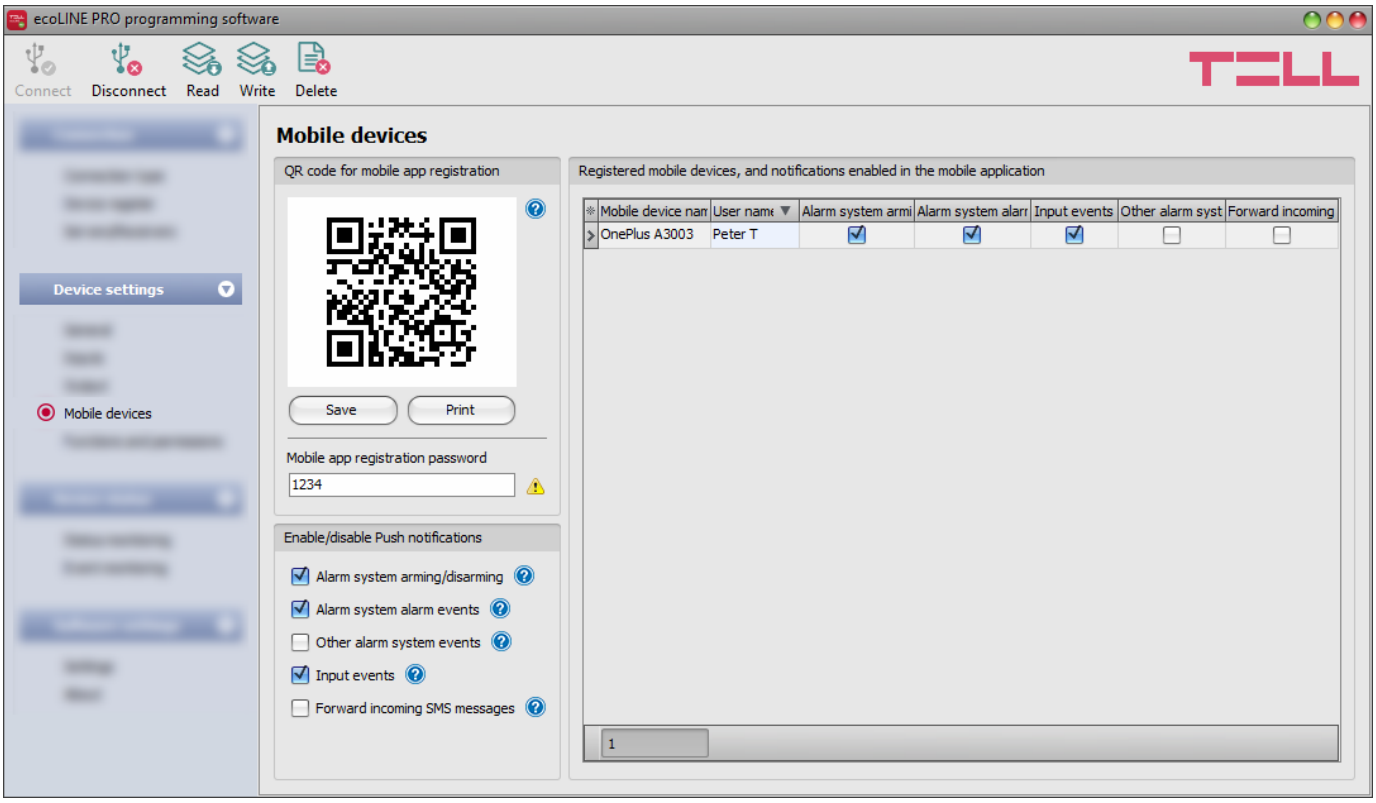
Output control mode: in this section you can configure the control mode of the output (or the selected output 1 or 2 in case of the IN4.R2 model). Available options:

- **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 100 milliseconds to 10 minutes.

Output parameter settings: in this section you can configure the duration of the control impulse. Click on the "***Edit***" button to open the parameter configuration window.

Controlled partition: the contact output can be used to arm or disarm one partition of the alarm system. In this field you can configure the number of the partition you want to control. The device will monitor the configured partition only, and a status change will occur in the partition status indicator found in the device and in the mobile application, only if arming or disarming occurs specifically in the configured partition.
In case of a non-partitioned alarm system, the partition number may be 00 or 01, depending on what partition number the alarm system sends in the Contact ID reports (you can check this in the system logs found in the ***Status monitoring*** menu, when the alarm system reports an arming or disarming event, e.g. CID: 1234183401**01**0010).

4.2.4 Mobile devices



In this menu you can find the QR code used for registering the mobile application, you can configure the registration password requested during the mobile app registration, and you can also enable or disable the event categories for Push message sending to registered mobile devices. Users can also enable or disable notifications in the mobile application, for the event categories enabled in this menu. Thereby, they can customize notifications they want to receive on their mobile device. The device supports registration of up to 20 mobile devices. It is also possible to delete a mobile device if needed, i.e. to cancel its registration. The mobile application can be associated with the device using the QR code.
In order to use the mobile application, it is necessary to enable cloud usage in the "***Functions and permissions***" menu.
The device works with the ***ecoLINE PRO*** mobile app available for iOS devices in the AppStore and for Android on Google Play.

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, in order 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.
- Deleting a mobile device:
  To delete the selected mobile device, click on the "***Delete***" button.

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

QR code for mobile app registration:

After installing the mobile application, you can associate the mobile app with the **ecoLINE PRO** device by reading this QR code in the mobile application and entering the registration password configured here. You can associate up to 20 mobile devices with the **ecoLINE PRO**.

If a mobile application is registered, the device can send Push messages to the given mobile device about events generated by its own inputs, and about reports received from the connected alarm system, and the device's output can also be controlled in the mobile app.

Mobile app registration password: the registration password configured here has to be provided in the mobile application when you wish to associate it with the device. The registration password length is 4 to 8 characters and only letters and numbers are accepted. Accented letters are not accepted.

Enable/disable Push notifications:

Push notification settings apply to all registered mobile devices at the same time. Notifications enabled here can be further enabled or disabled by users on each mobile device on demand. The device will not send notifications to mobile devices on event categories which are disabled.

Alarm system arming/disarming: enable Push message sending to the registered mobile devices about arming/disarming events of the alarm system connected to the device.

Alarm system alarm events: enable Push message sending to the registered mobile devices about alarm events of the alarm system connected to the device.

Other alarm system events: enable Push message sending to the registered mobile devices about other events (e.g. failures) of the alarm system connected to the device.

Input events: enable Push message sending to the registered mobile devices about events generated by the contact inputs of the device. The message text for each input can be configured in the mobile application.

Forward incoming SMS messages: if this option is enabled, the device will forward SMS messages received by its SIM card (e.g. balance information received from the GSM service provider, in case of pre-pay card) to the registered mobile devices in Push messages. The received SMS messages are deleted automatically after forwarding. If this option is disabled, the device will delete all SMS messages received by its SIM card without forwarding.

Registered mobile devices, and notifications enabled in the mobile application:

Mobile devices associated with the **ecoLINE PRO** device are listed in this table.

Mobile device: in this field the name of an already registered mobile device is shown, which is read by the mobile application directly from the mobile device.

User name: the name provided by the user upon registering the mobile application.

Alarm system arming/disarming: the checkbox in this column shows whether the user has enabled on the given mobile device reception of notifications about the connected alarm system's arming/disarming events.

Alarm system alarm events: the checkbox in this column shows whether the user has enabled on the given mobile device reception of notifications about the connected alarm system's alarm events.

Other alarm system events: the checkbox in this column shows whether the user has enabled on the given mobile device reception of notifications about the connected alarm system's other events (e.g. failures).

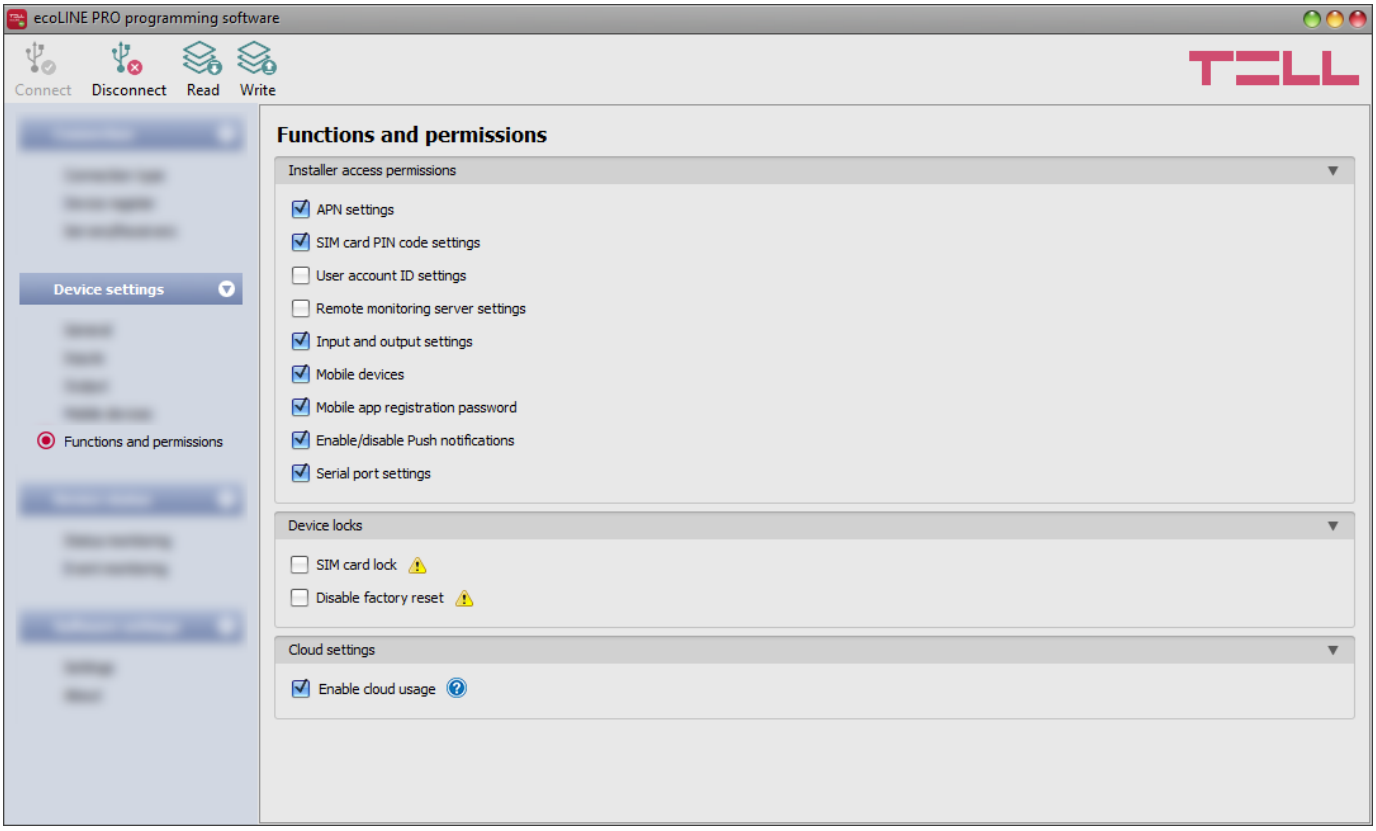
Input events: the checkbox in this column shows whether the user has enabled on the given mobile device reception of notifications about events generated by the device's contact inputs.

Forward incoming SMS messages: the checkbox in this column shows whether the user has enabled on the given mobile device reception of notifications about SMS messages received on the SIM card installed in the device.

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

Deleting a mobile device: you can delete a registered mobile device (i.e. cancel its registration) by selecting the mobile device and then clicking on the "***Delete***" button. If you delete a mobile device, the application used on the given device will no longer access the **ecoLINE PRO** device.

4.2.5 Functions and permissions



In this menu you can configure the installer access permissions, device lock and function settings. Only the super administrator can configure the settings in this menu.

The settings that don't have a checkmark, i.e. the ones that the Installer does not have access to, are considered protected.

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, in order 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.

Installer access permissions:

In this section you can enable or disable the installer's access to protected settings (for the user who sings in with the installer password). The installer can change only settings options which are enabled in the list.

Device locks:

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

Disable factory reset: you can lock your device with this setting, so that the factory default settings cannot be restored without signing in with the Superadmin password. If you enable this option, restoring the factory default settings will be disabled. In this case you can restore the factory default settings only after signing in with the Superadmin password and disabling this option. If you forget the Superadmin password, only the manufacturer can restore the factory default settings in the service center. If this option is disabled, the device will be unlocked and factory default settings can be restored anytime, even without signing in with a password.

Cloud settings:

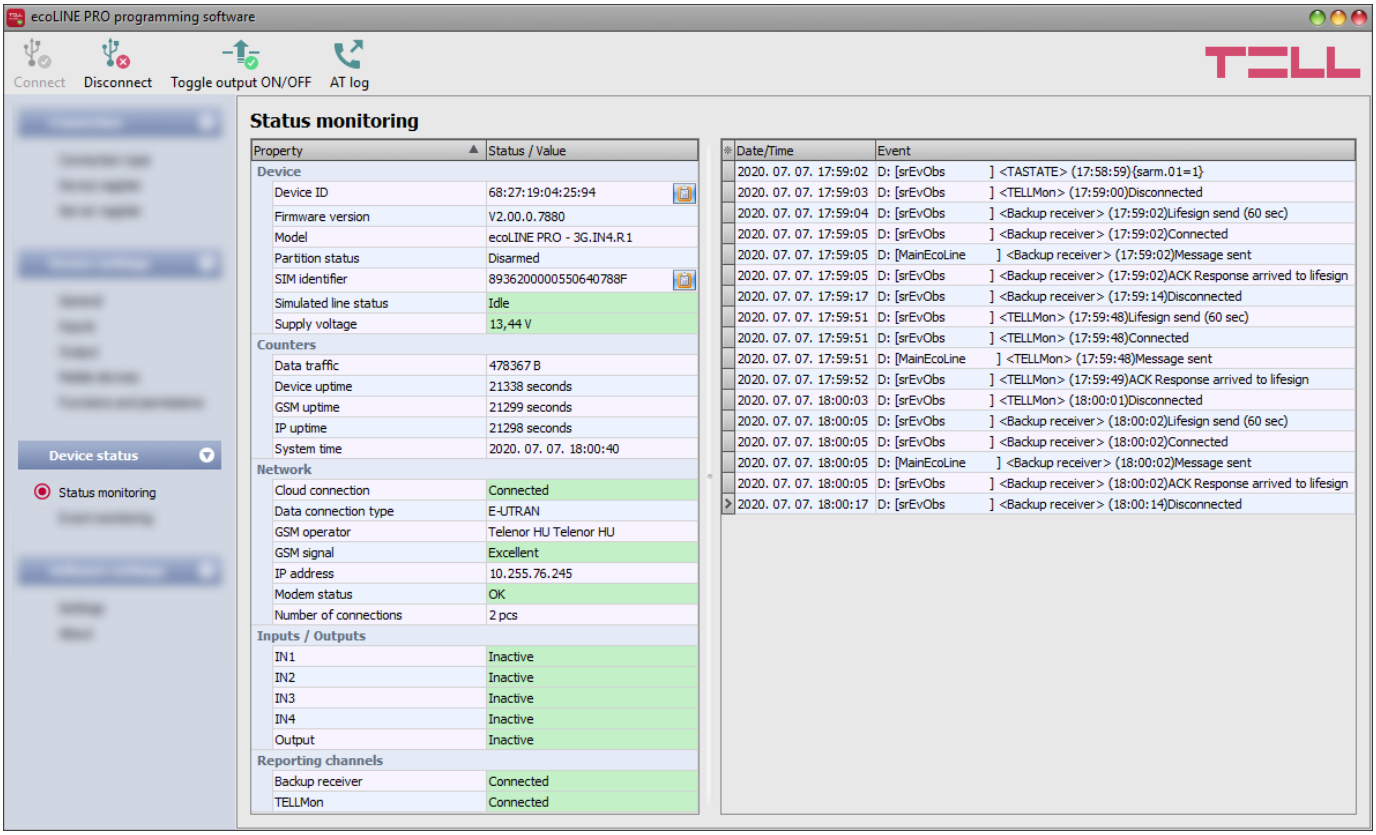
Enable cloud usage: enable this option if you want to use the device with the mobile application, or if you want to access it remotely with the programming software over cloud connection. If this option is enabled, the device will connect to the server operated in the cloud by the manufacturer, and will stay connected permanently, thereby it will be available through the Internet anytime. If this option is disabled, the device will only connect temporary to the cloud when there are Push messages to send, therefore it will be essentially unavailable with the mobile application. You can also initiate a temporary cloud connection manually, by sending a request by SMS to the phone number of the device. You can read more about this in the "***Remote connecting to devices via cloud service***" paragraph. Maintaining the cloud connection and cloud usage involve use of mobile data. In order to ensure a continuous connection and availability, the device sends supervision messages that use about **12 MB data per month** on its own.

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 52.30.109.179, port: 2020.

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

4.3 Device status menu

4.3.1 Status monitoring



The "***Status monitoring***" menu provides information on actual system status. Please note that for faster communication, some of the options are not available when connected remotely. Status information loads and refreshes automatically only when connected through USB.

In the window on the right side the system logs are shown, which provides information about the internal processes of the device and communication. These details help troubleshooting if malfunction occurs. The program saves the system logs to file automatically in the "***Logs***" folder, which you can access the easiest by clicking on the path link shown in the "***Data folder***" section in the "***About***" menu. **System logs are only available when connected via USB!**

Available status information:

Device:

- **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.
- **Firmware version**: the firmware version of the device.
- **Model:** the device type/model.
- **Partition status**: the status of the controlled partition in the alarm system (Armed / Disarmed). The device reads the status from arming and disarming reports sent by the alarm system. Therefore, after installation or a power loss, the device will set the correct status when the alarm system reports an arming or disarming event.
- **SIM identifier**: the identifier (ICCID) of the SIM card installed into the device. You can copy the ID to clipboard by clicking the notepad icon on the right hand side.
- **Simulated line status**: the status of the simulated phone line.
- **Supply voltage**: value of measured supply voltage.

Counters:

- **Data traffic**: data traffic 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.
- **IP uptime**: elapsed time since the device has last connected to the Internet.
- **System time**: the system date and time.

Network:

- **Cloud connection**: the cloud server connection status.
- **Data connection type**: type of actual data connection.
- **GSM operator**: the name of the GSM operator used actually.
- **GSM signal**: actual GSM signal level (None/Very low, Weak, Medium, Good, Excellent).
- **IP address**: the actual IP address of the device.
- **Modem status**: the actual status of the GSM modem. If it shows the "***SIM card locked***!" message, the device has been locked with a SIM card used earlier (see paragraph "***SIM card lock***". You can disable the lock in the settings.
- **Number of connections**: the number of active connections with servers/receivers.

Inputs / Outputs:

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

Reporting channels:

- **IP1…IP2**: connection status of the configured servers and IP receivers

After connecting to the device remotely, the following option becomes available:

- **Toggle output ON/OFF**:

You can toggle the output (OUT) on and off by clicking on this button. If switched on, the output remains activated until deactivated in the software or in the mobile app, or a power loss occurs.

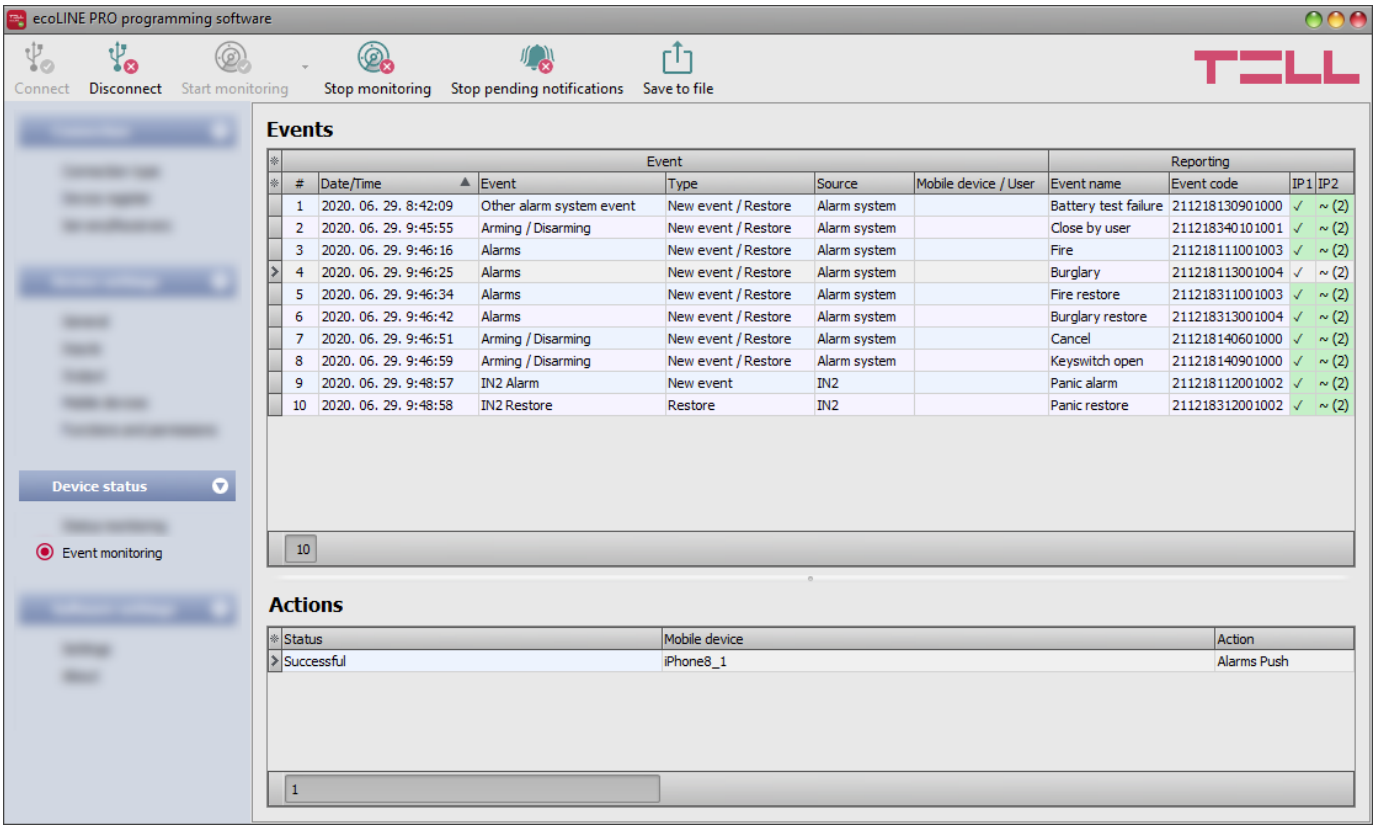
- **Query**:

This button is only available when connected to the device remotely. Status information can be loaded or updated by clicking on this button. This is not needed when connected via USB, because in this case status information will load and refresh automatically.

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

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

4.3.2 Event monitoring



In this menu the device's event log can be viewed and also enables you to monitor events and reporting progress online. The device stores last 100 events in its event log memory.

You can see the events and the reporting status in the "***Events***" window, while other actions configured and performed by events are available in the "***Actions***" window. To view the actions performed by an event, select the event in the "***Events***" window by clicking on it.

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 to be displayed 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:

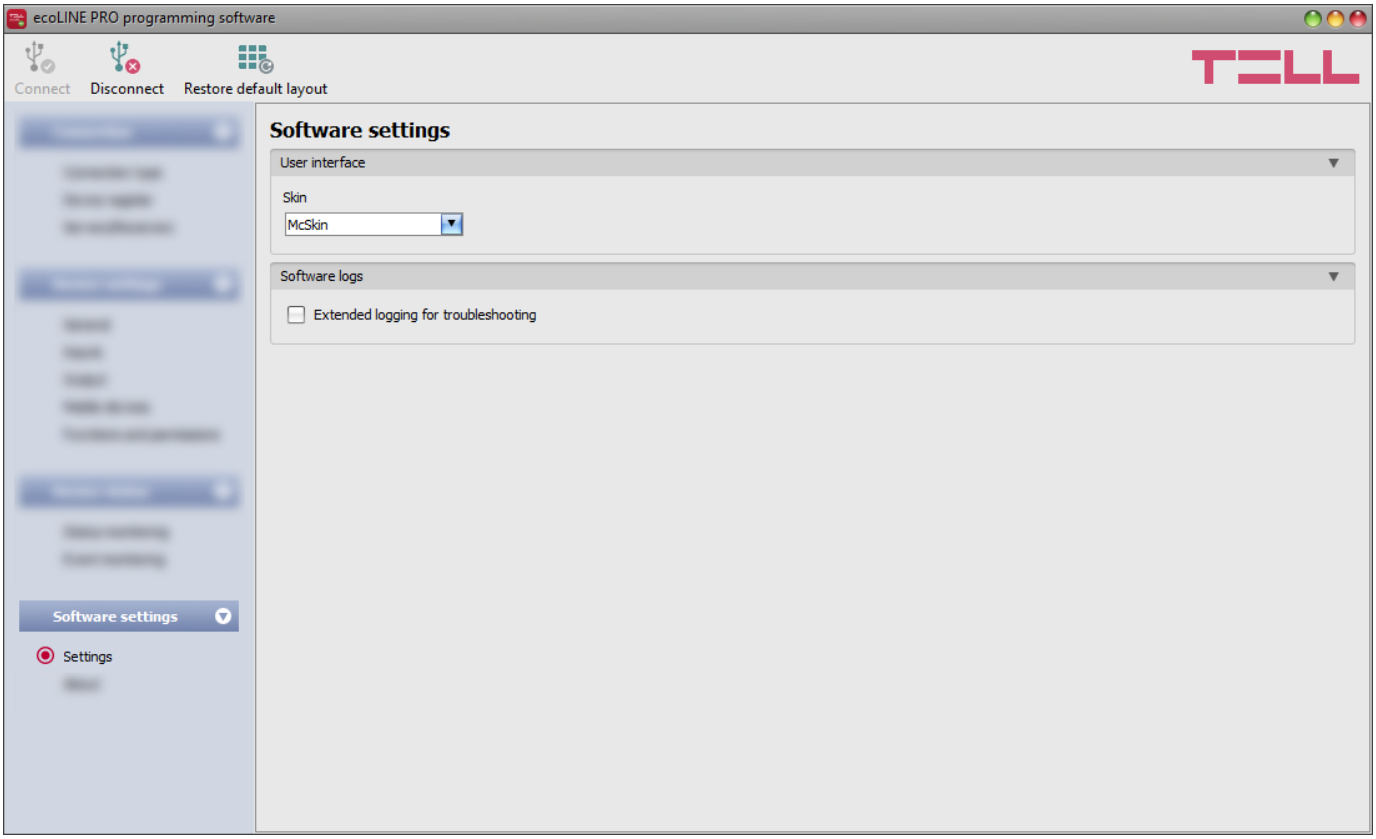
- #: the ordinal number of events.
- **Date/time**: event occurrence date and time.
- **Event**: the name of the event.
- **Type**: event type (New event / Restore).
- **Source**: event source (Input or Alarm system).
- **Mobile device / User**: the name of the mobile device and user who generated the given event (information is shown for output control events only).
- **Event name**: the event name based on the default Contact ID code table.
- **Event code**: Contact ID event code.
- **IP1**…**IP2**: reporting to IP1…IP2 server/receiver IP addresses.

Legend of marks shown in the IP1…IP2 columns:

?	Event reporting is in progress.
~ (2)	Secondary channel: No need to report because reporting through the primary channel was successful.
✓	Successful reporting.
! (1)	Reporting failed (reporting failed through the primary channel, but through the secondary channel it was successful).
! (N)	Reporting failed (a negative acknowledgement signal has been received /NAK/).
! (A)	Reporting failed (authentication error).
! (I)	Reporting failed (an invalid response has been received).
! (?)	Reporting failed (no response received).
! (S)	Reporting failed (TCP packet sending failed).
! (B)	Reporting failed (the device has been blocked on the server/receiver side).
! (R)	Reporting failed (server/receiver error).

4.4 Software settings menu

4.4.1 Settings



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

Available options:

- **Restore default layout**:
  To restore the user interface default layout click on the "***Restore default layout***" button.

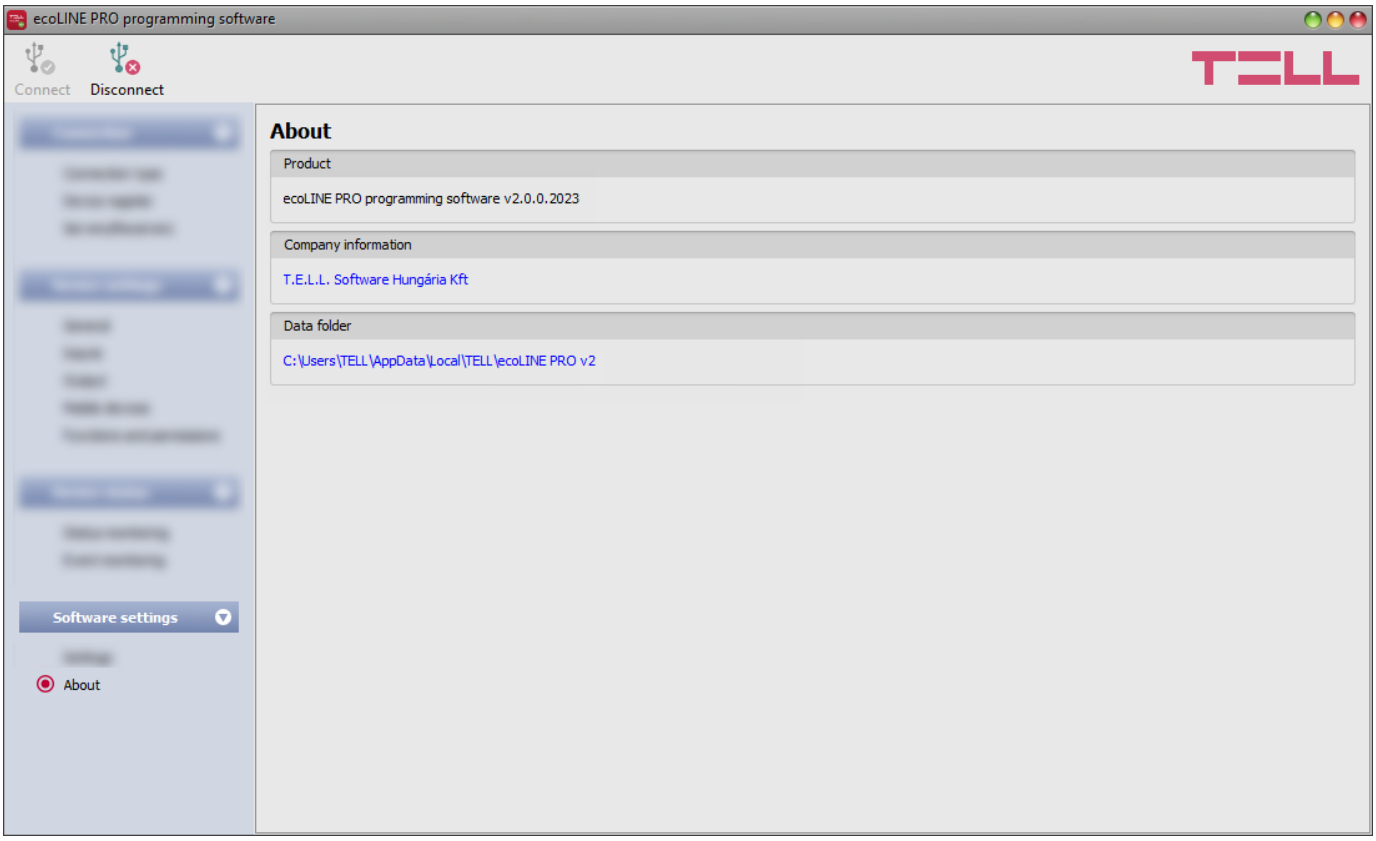
User interface:

Skin: the user interface skin can be changed using the dropdown-menu. You can choose between multiple appearance themes.

Software logs:

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

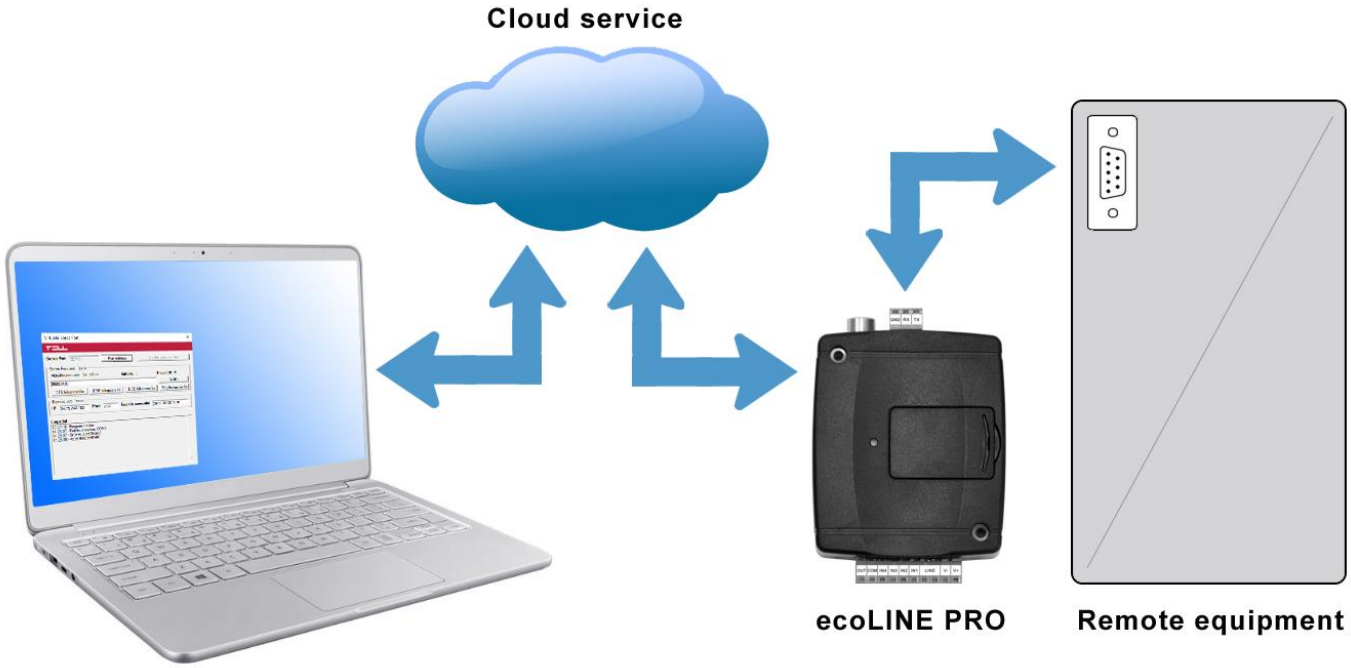
4.4.2 About



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 link, the data folder will be opened in the file manager.

5 Transparent serial port

The serial port of the device is suitable for bidirectional transparent data transfer over the Internet. It can be used for e.g. remote programming of the connected alarm control panel or can provide a solution for remote communication of other devices or equipment which are using an RS232 serial port. The Internet connection between the remote device or equipment and the computer is ensured by the ***ecoLINE PRO*** and the ***Remote Serial Client*** software. For this, the serial port of the ***ecoLINE PRO*** should be connected to the serial port of the given device or equipment, and then data can be sent to and received from the device or equipment on the PC through the virtual serial port created by the ***Remote Serial Client*** software.



5.1 Remote programming of alarm control panels

For remote programming, the device establishes transparent serial data communication through IP connection. The remote connection between the programming software of the alarm system and the alarm control panel is ensured by the ***ecoLINE PRO*** device and the ***Remote Serial Client*** software. For this, the serial port of the ***ecoLINE PRO*** should be connected to the serial port of the alarm control panel, and the programming software of the alarm system connects to the virtual serial port created by the ***Remote Serial Client*** software.

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

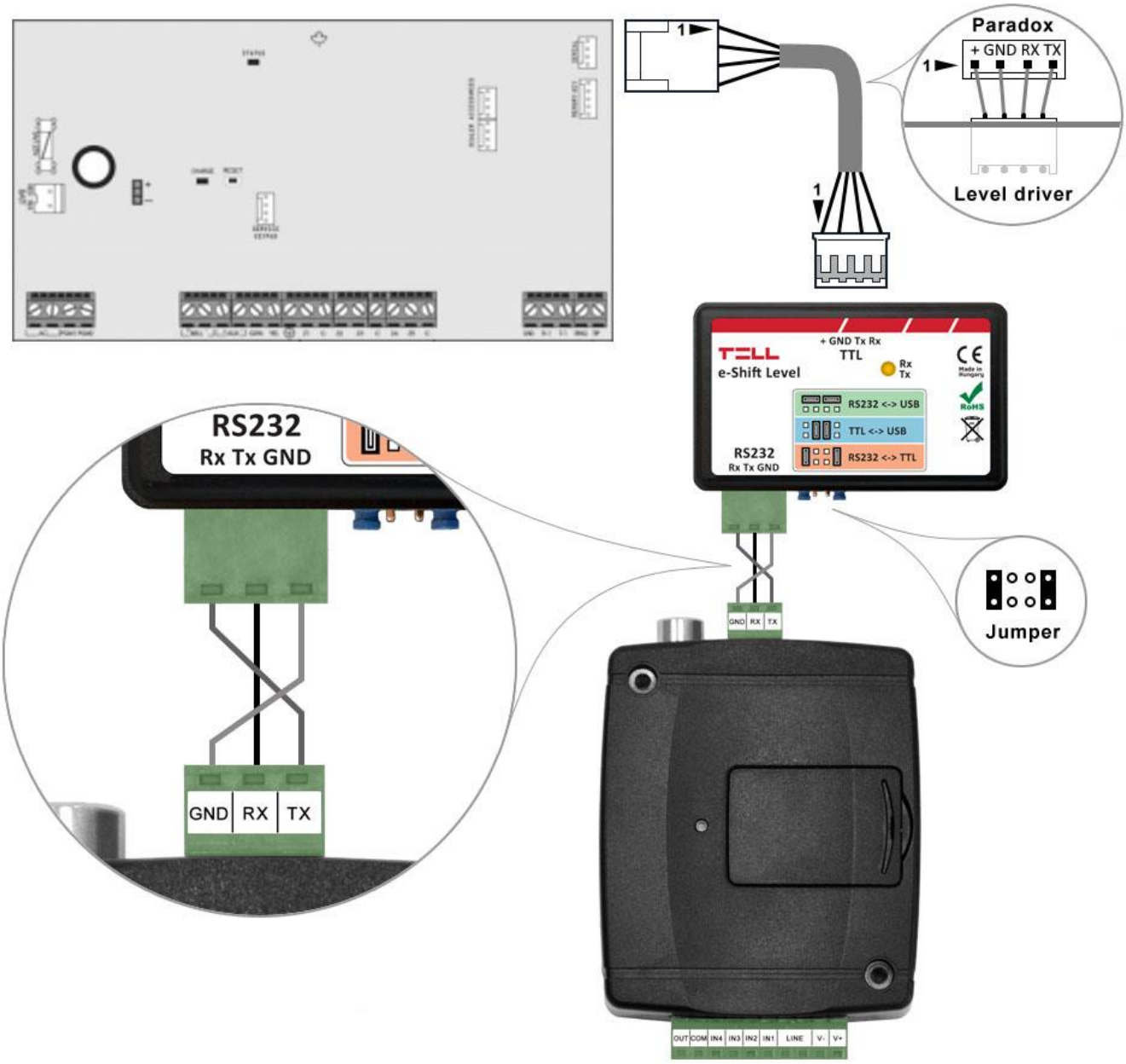
Attention! Please note that data transfer through the serial port of the *ecoLINE PRO* may generate high data traffic, which may result in an increased data usage on the SIM card installed in the device.

Remote programming was tested with the following alarm control panels:

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

5.1.1 Paradox alarm systems

- **Installation:**



Wiring diagram for Paradox alarm systems

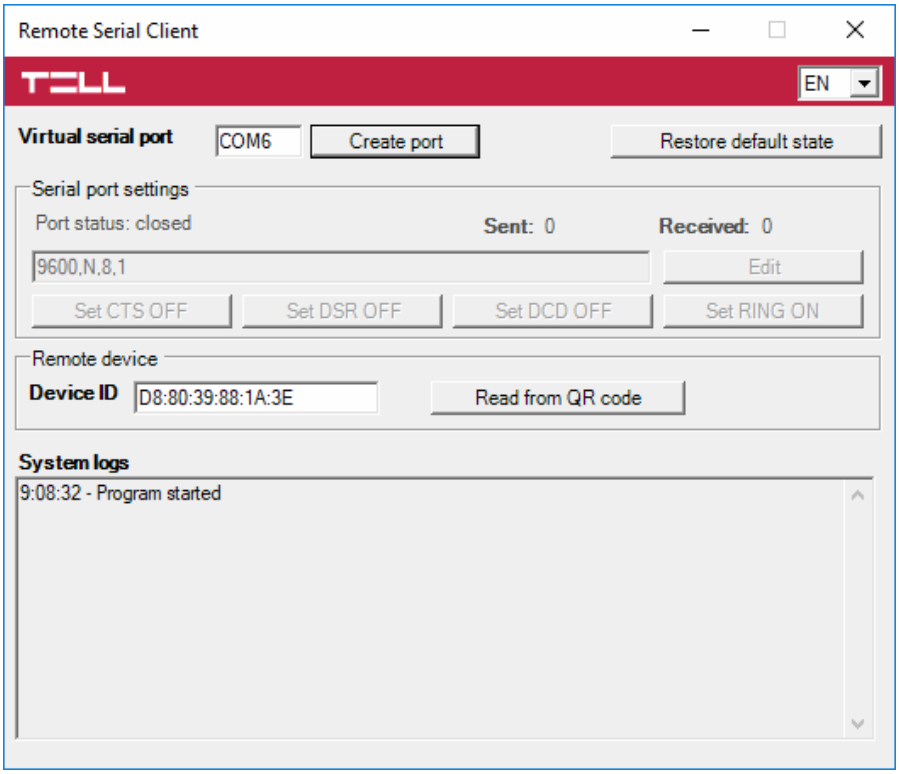
For Paradox alarm control panels a level driver interface is needed to establish the serial link. TELL offers its own level driver interface produced for this purpose. Connect the serial port output of the level driver interface to the serial port of the ***ecoLINE PRO***, then link the level driver interface with the alarm control panel using the supplied special cable, as shown in the figure above. Configure the jumpers of the driver level interface as well as shown in the figure above.

- **Software settings:**

Configure the serial port settings in the "***Serial port***" section of the "***General***" menu, in the ***ecoLINE PRO*** programming software, as shown in the figure below.

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

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



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

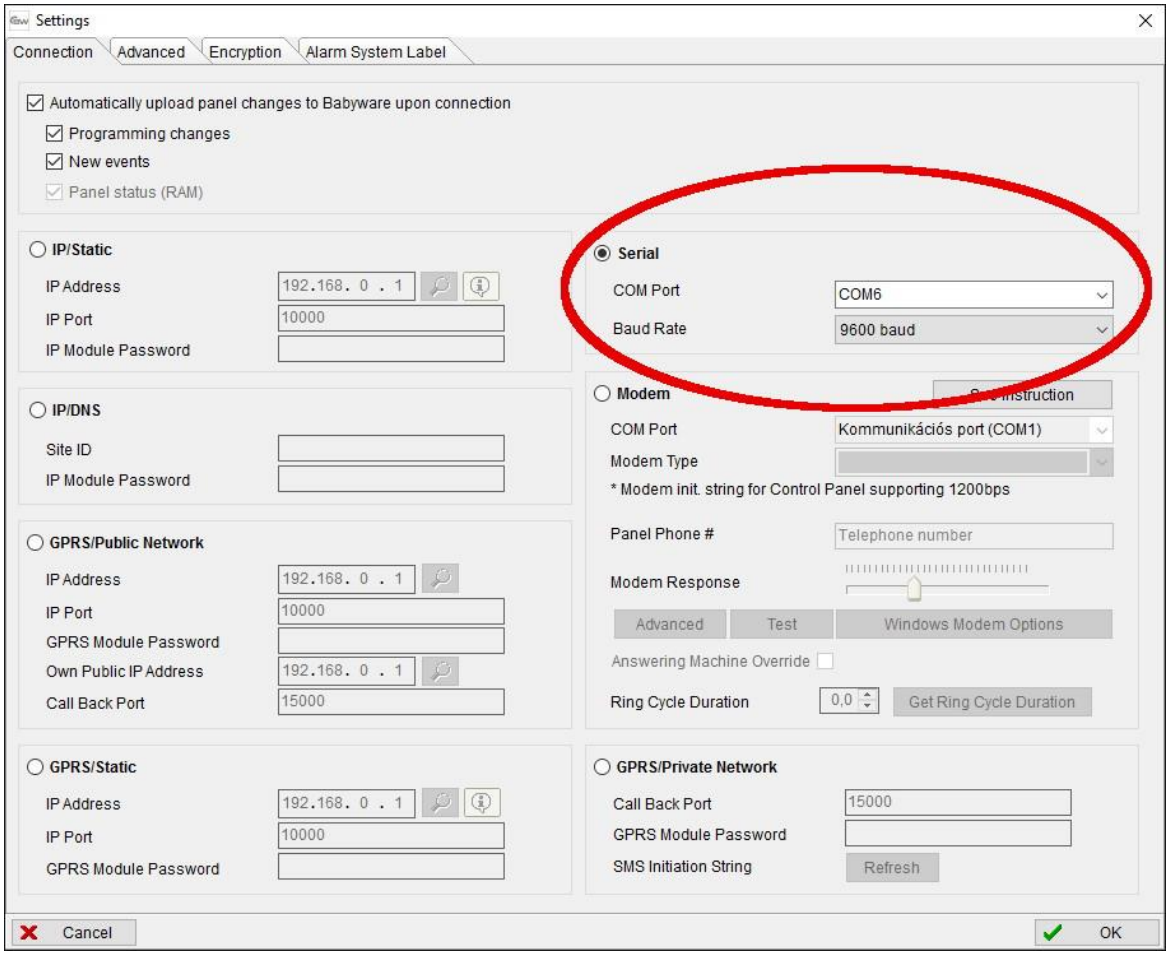
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***ecoLINE PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains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

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

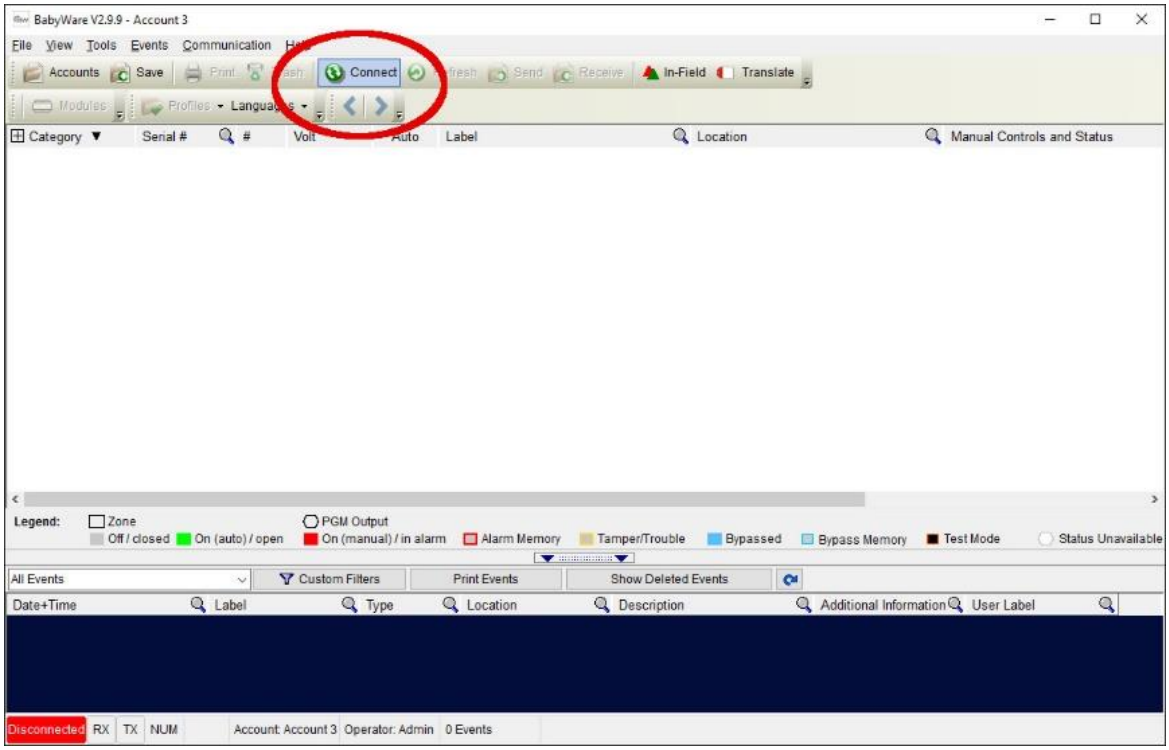
System logs: shows information about program operation and displays data received through the serial port.

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

Example for selecting the serial communication port in the ***Babyware*** programming software:
For Spectra alarm control panels: Baud rate=9600 baud
For EVO alarm control panels: Baud rate=57600 baud

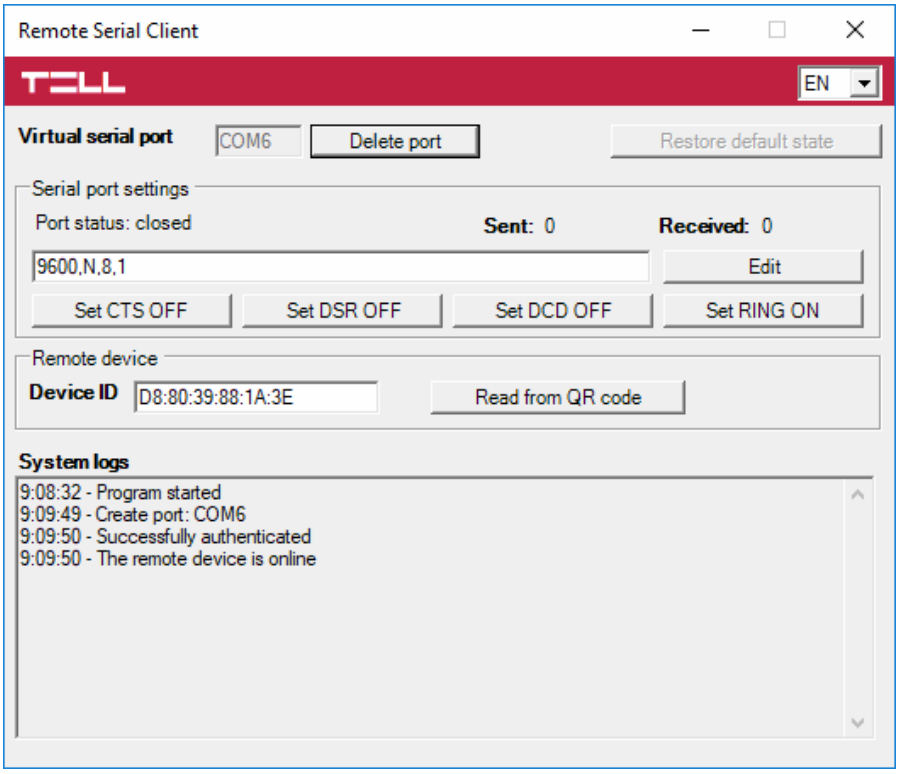


Start connecting:



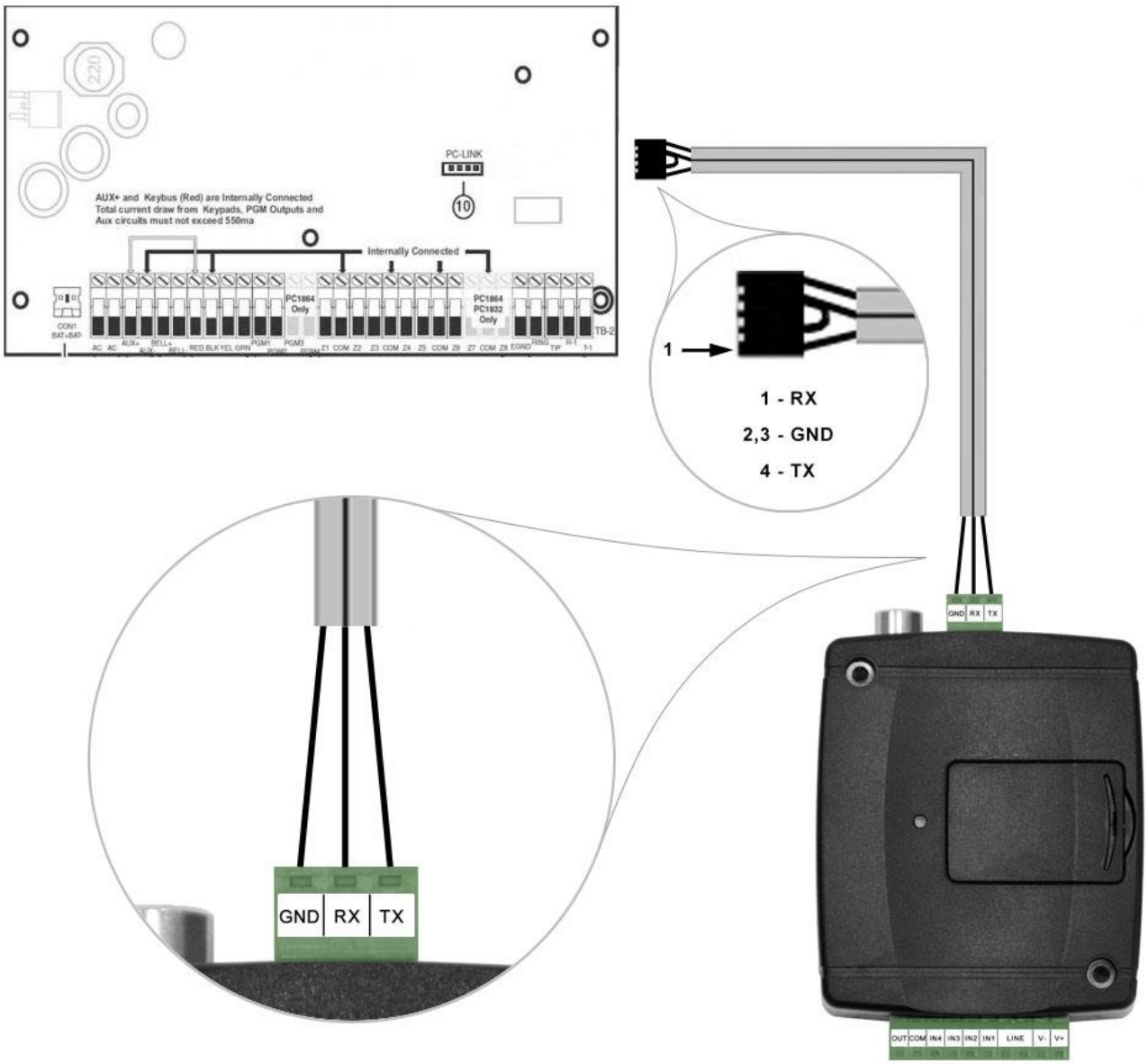
Then the programming software will open the serial port and will establish the connection with the alarm control panel.

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



5.1.2 DSC alarm systems

- **Installation:**



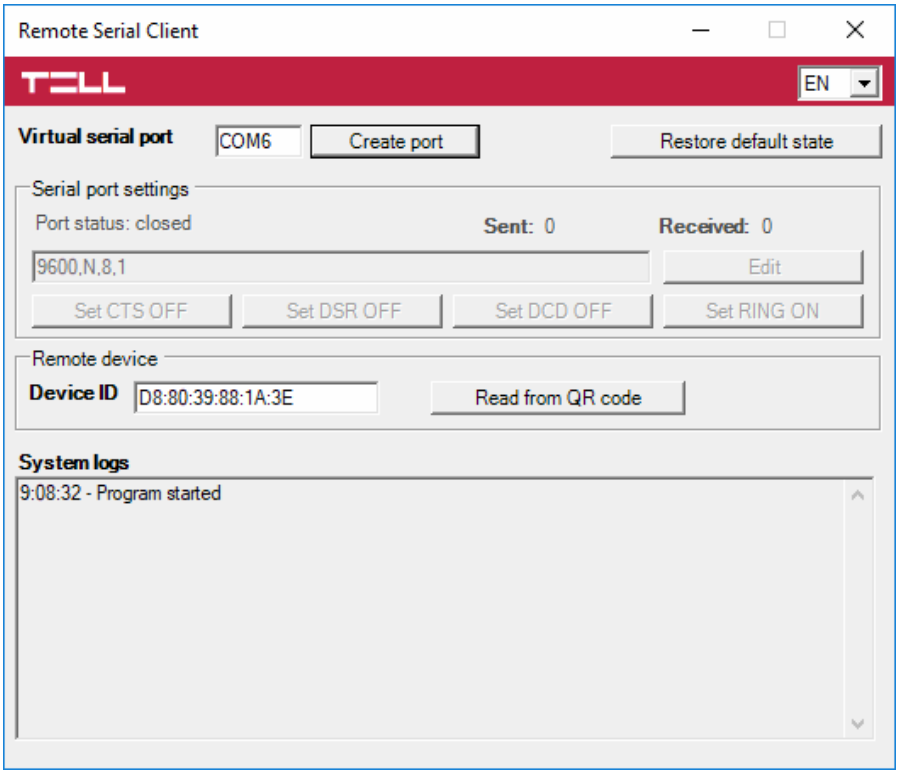
Wiring diagram for DSC alarm systems

Connect the supplied special cable to the serial port of the ***ecoLINE PRO*** device as shown in the figure above, then plug it onto the alarm control panel.

- **Software settings:**

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

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



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

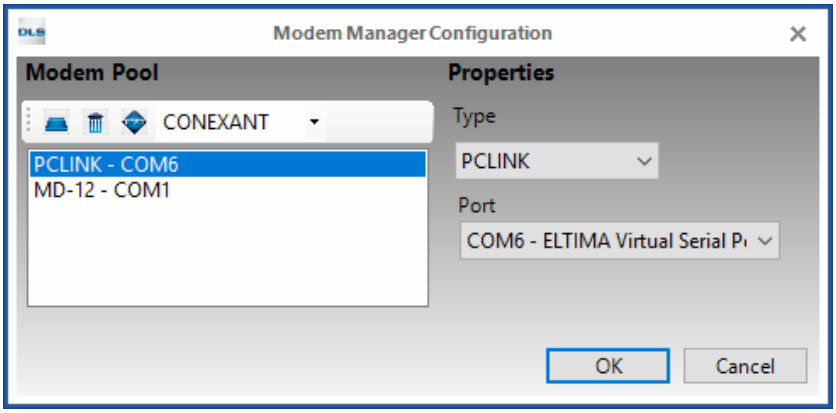
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***ecoLINE PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains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

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

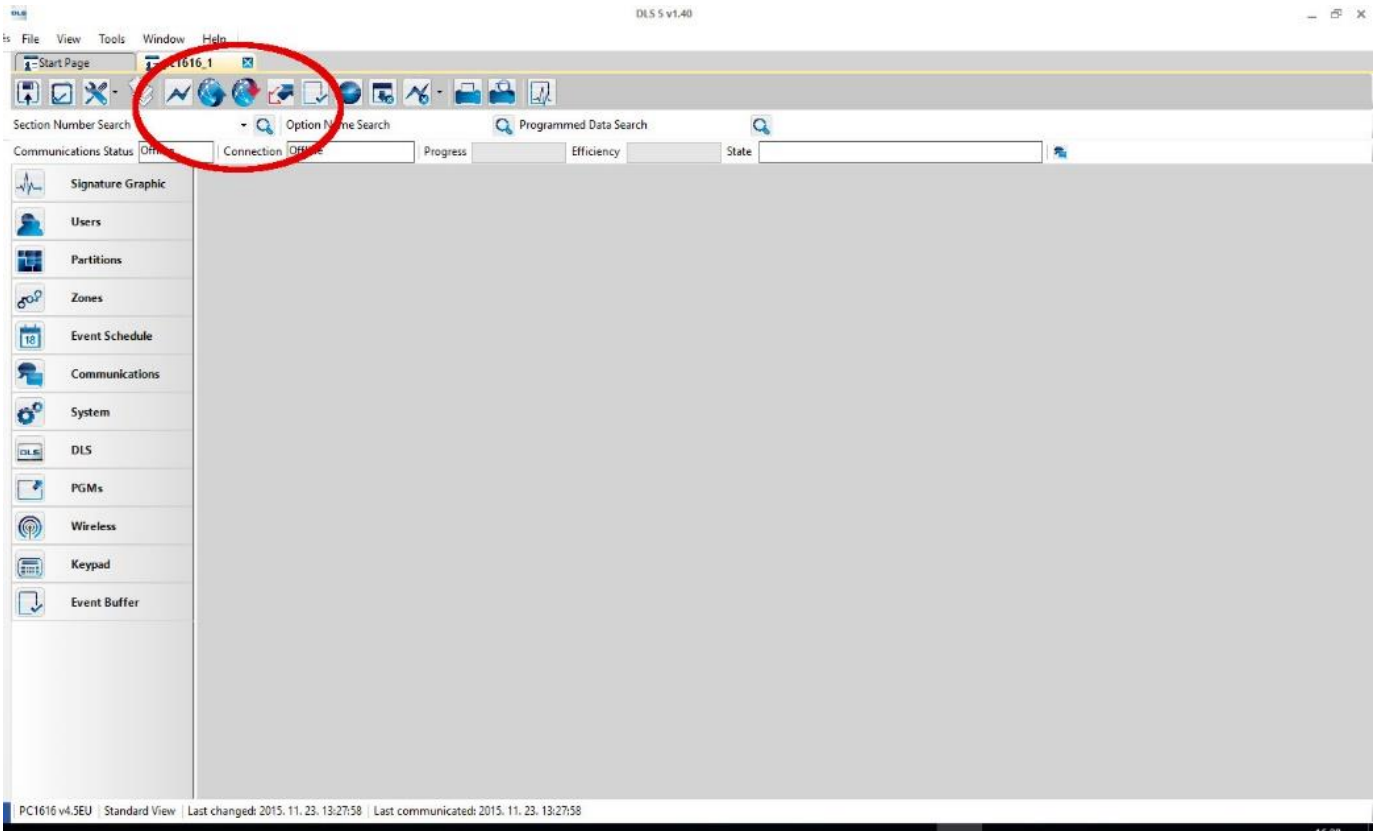
System logs: shows information about program operation and displays data received through the serial port.

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

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

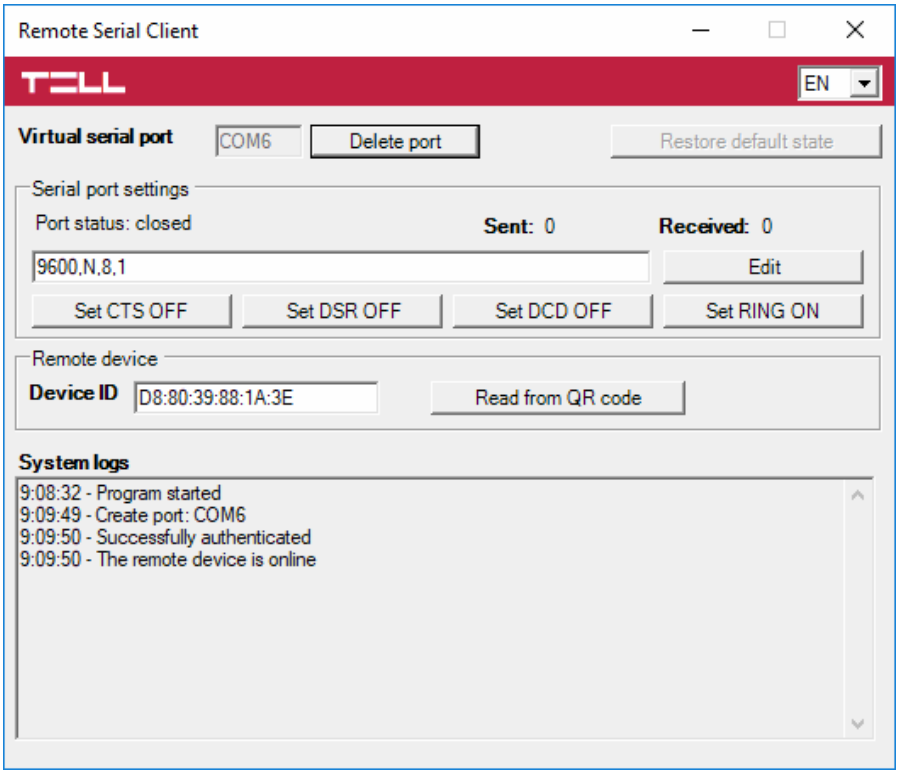


Start connecting:



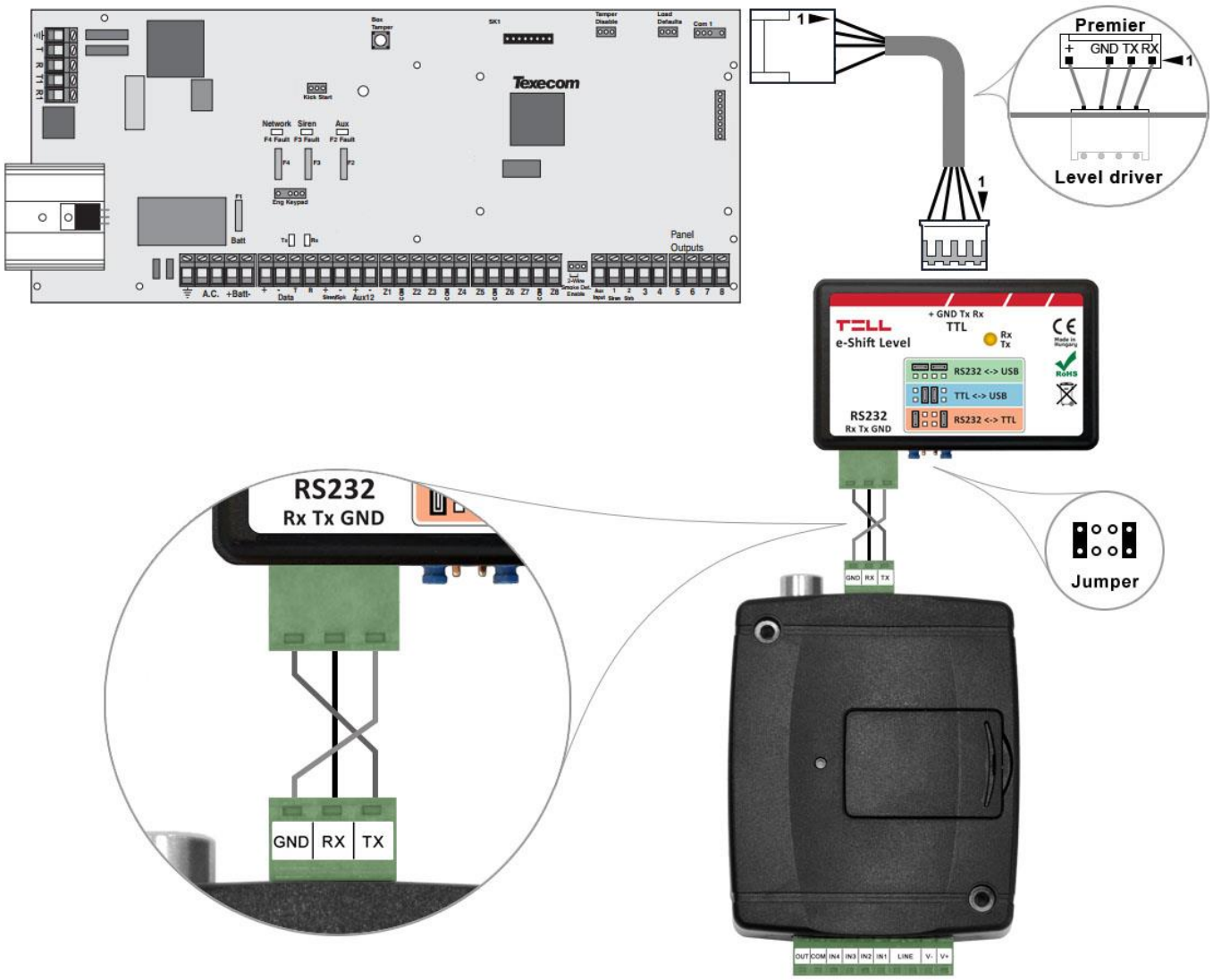
Then the programming software will open the serial port and will establish the connection with the alarm control panel.

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



5.1.3 Premier and Premier Elite alarm systems

- **Installation:**



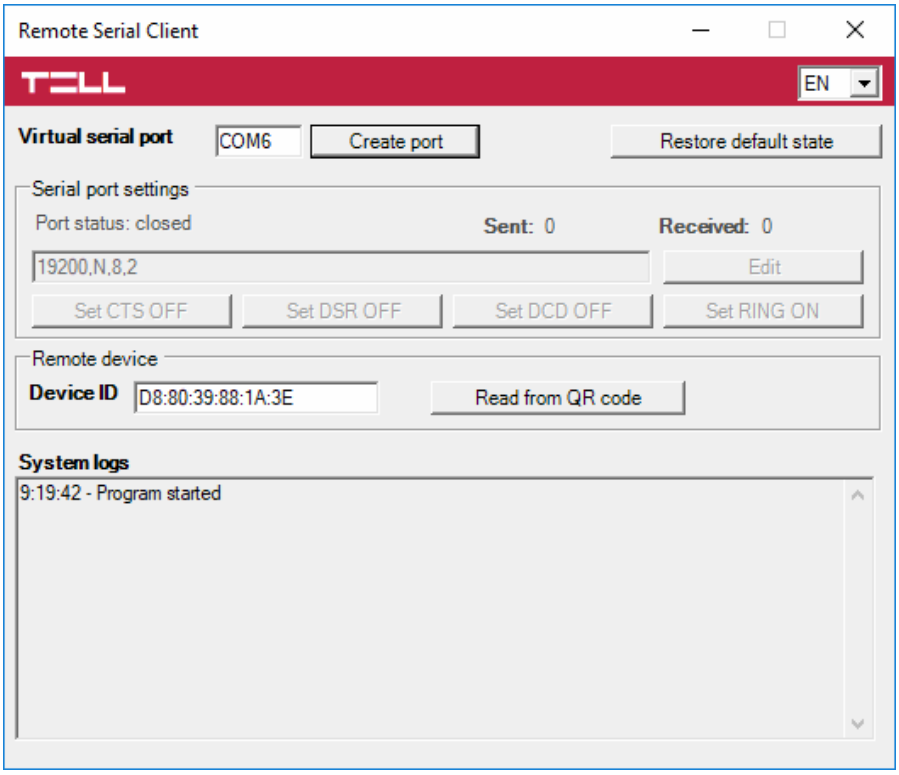
Wiring diagram for Premier alarm systems

For Premier alarm control panels a level driver interface is needed to establish the serial link. TELL offers its own level driver interface produced for this purpose. Connect the serial port output of the level driver interface to the serial port of the ***ecoLINE PRO***, then link the level driver interface with the alarm control panel using the supplied special cable, as shown in the figure above. Configure the jumpers of the driver level interface as well as shown in the figure above.

- **Software settings:**

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

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



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

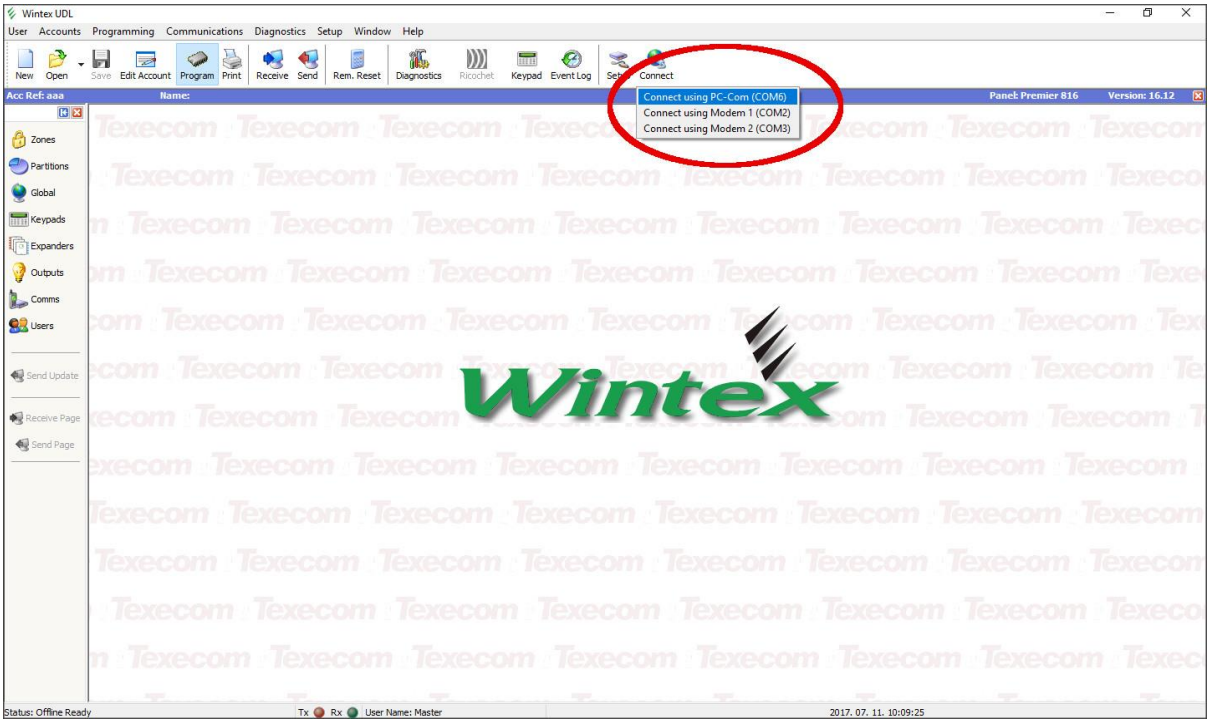
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***ecoLINE PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains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

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

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

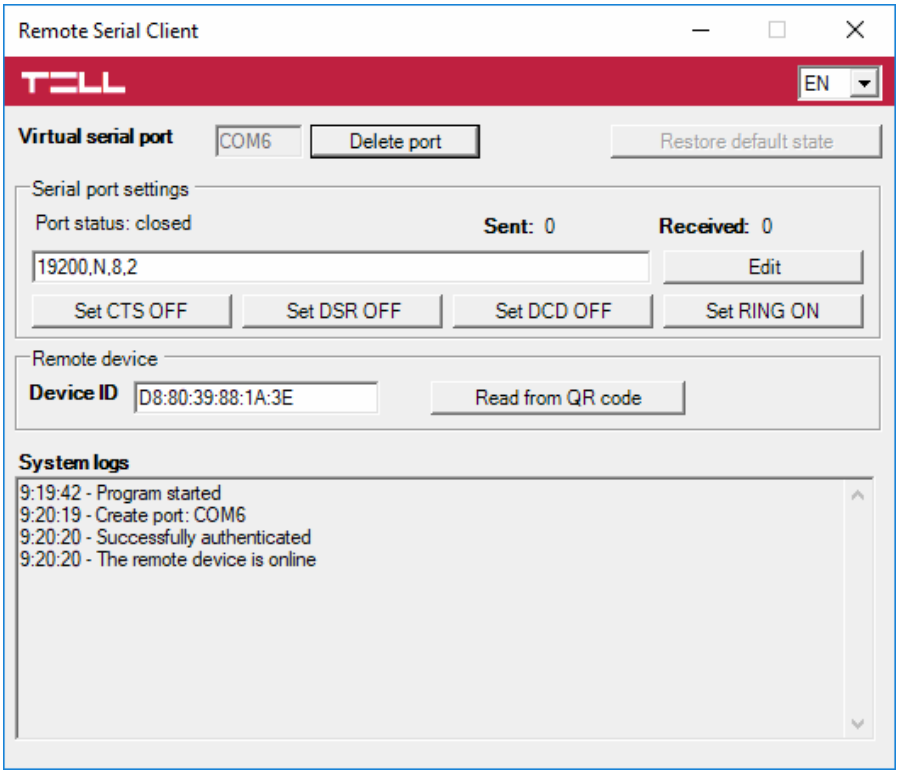
Create port: click on this button to create the configured virtual serial port, then select the created port in at the serial communication settings in the programming software of the alarm system. Please note that the ***ecoLINE PRO*** device should be online in order to create the virtual serial port.

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



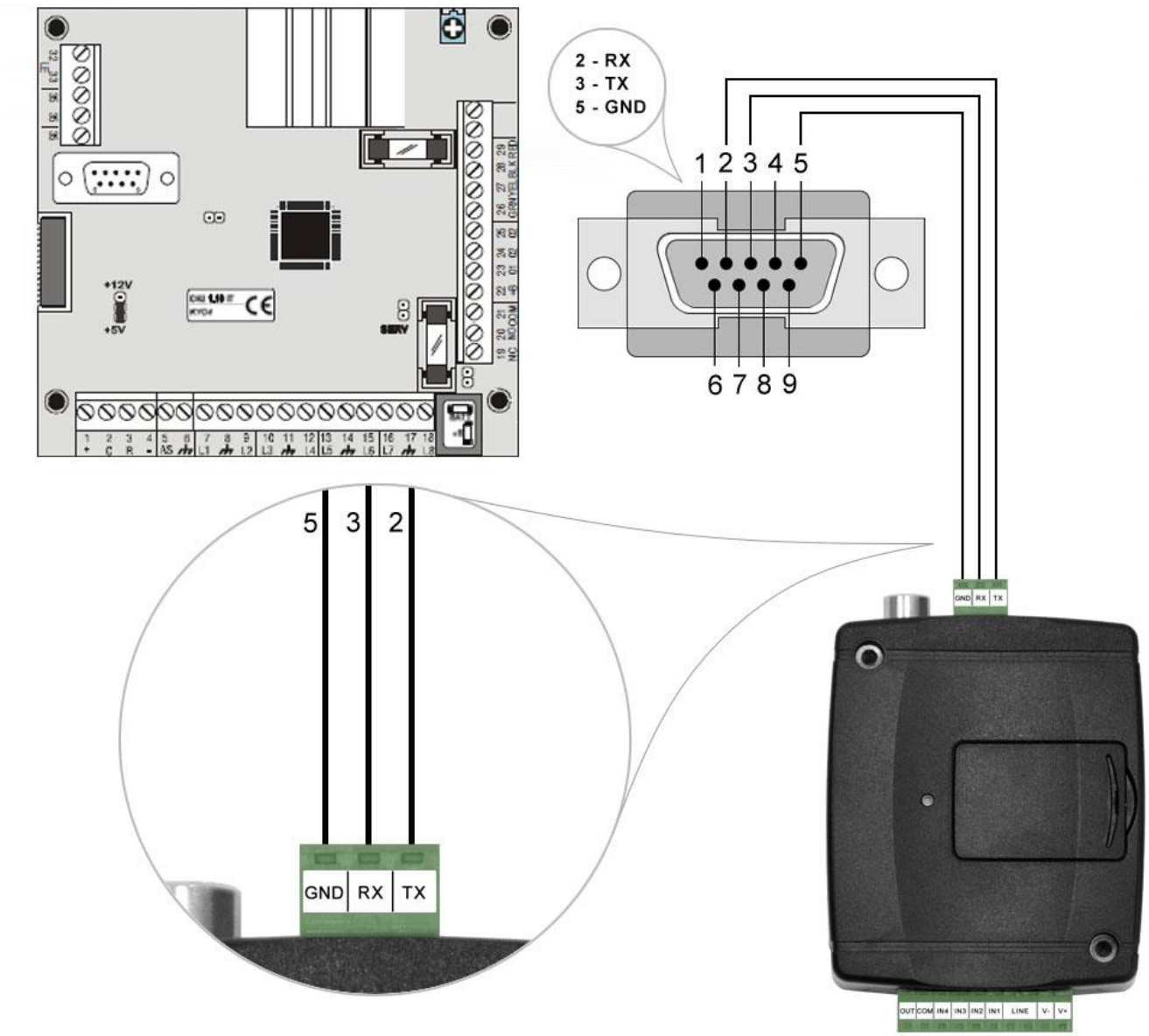
Then the programming software will open the serial port and will establish the connection with the alarm control panel.

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



5.1.4 Bentel alarm systems

- **Installation:**



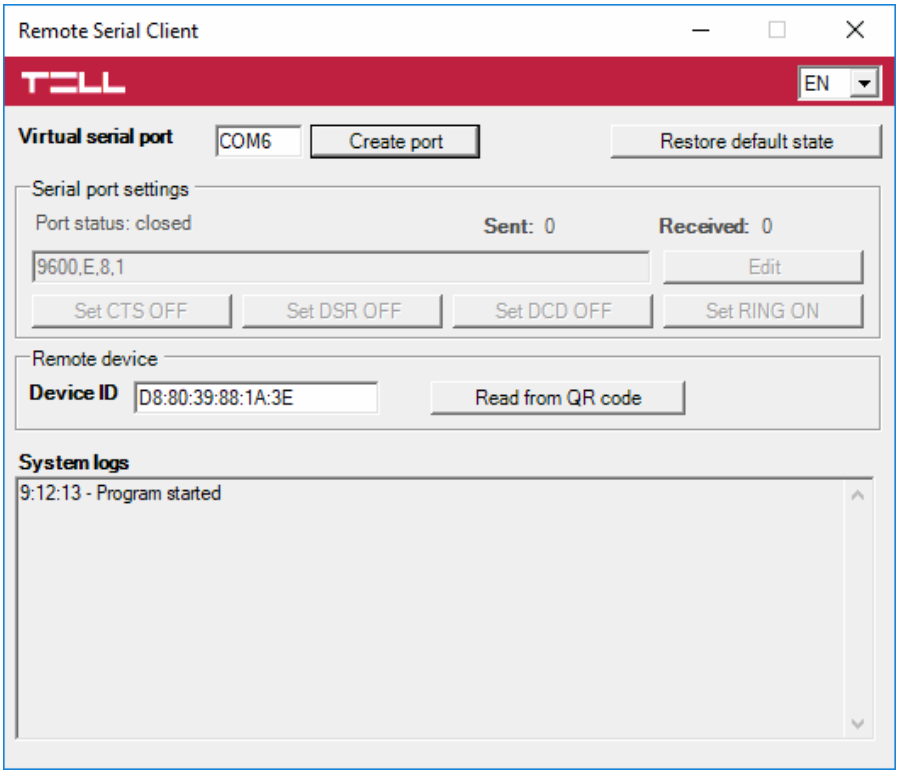
Wiring diagram for Bentel alarm systems

Connect the supplied special cable to the serial port of the ***ecoLINE PRO*** device as shown in the figure above, then plug it onto the alarm control panel.

- **Software settings:**

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

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



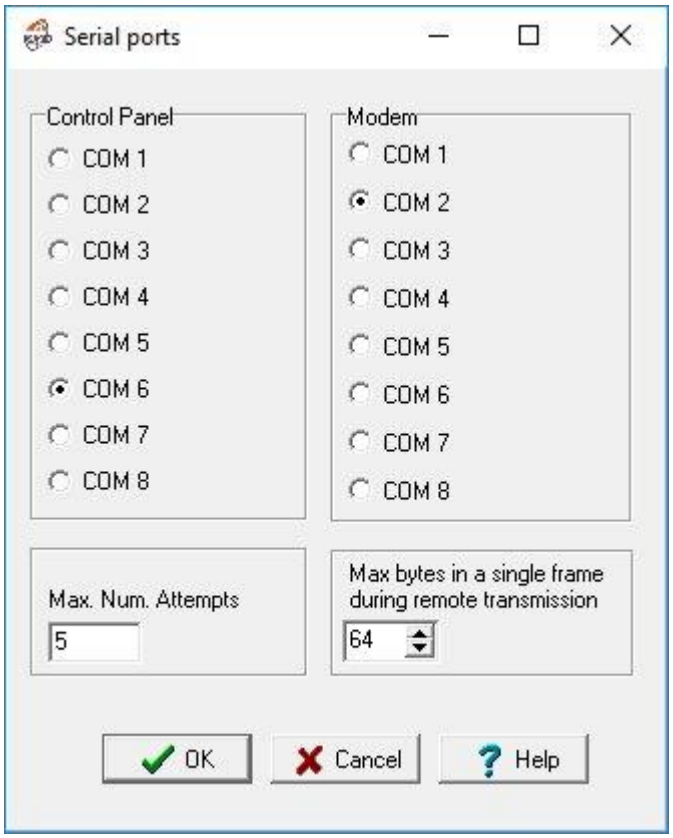
Open the ***Remote Serial Client*** software and configure the settings in the order below:

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

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

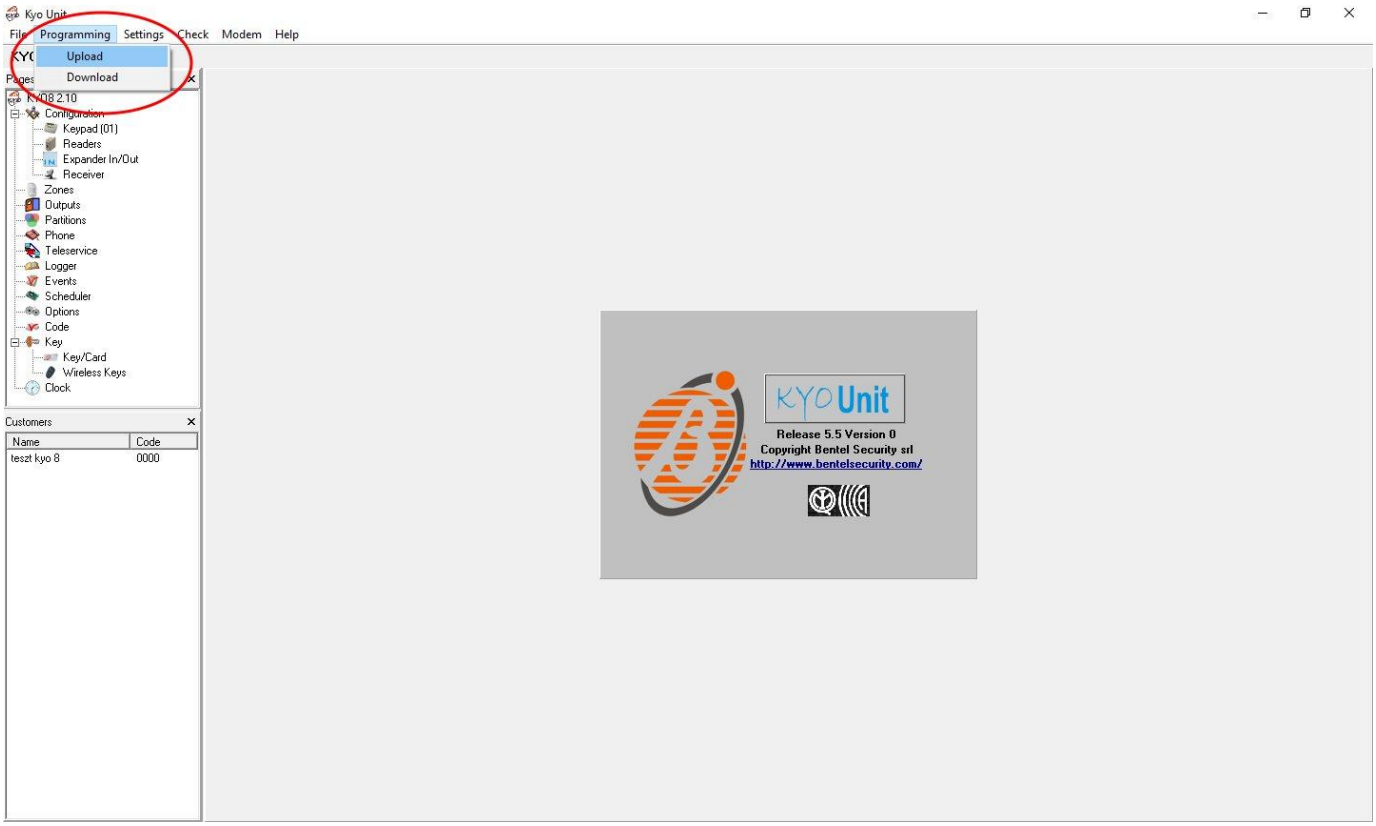
System logs: shows information about program operation and displays data received through the serial port.

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



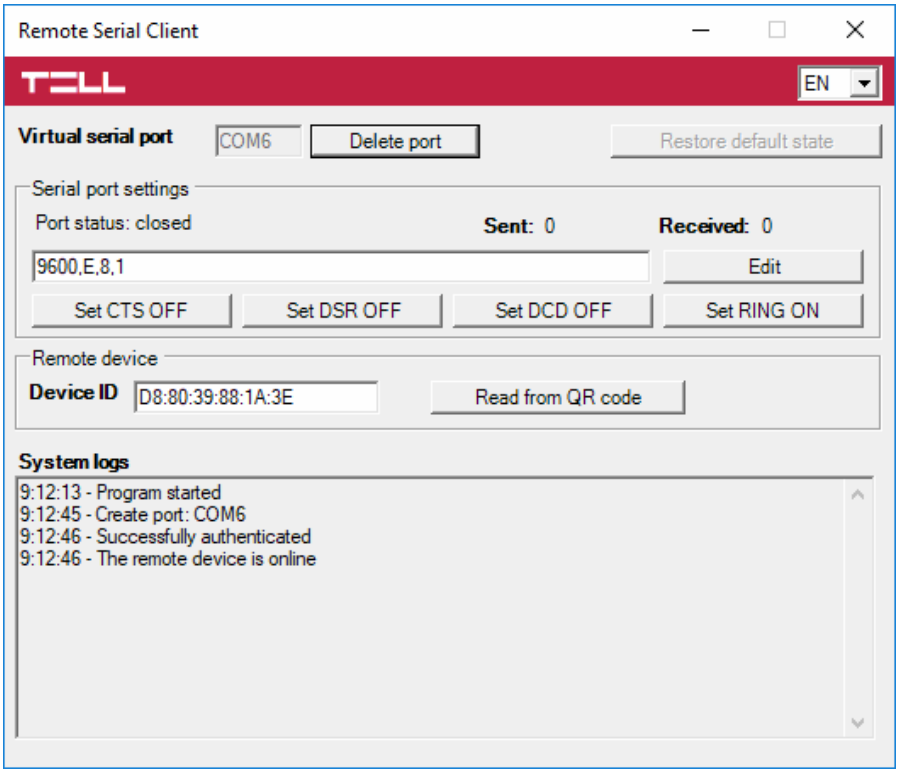
Example for selecting the serial communication port in the ***Bentel Security Suite*** programming software (see the figure on the right hand side).

Start connecting:



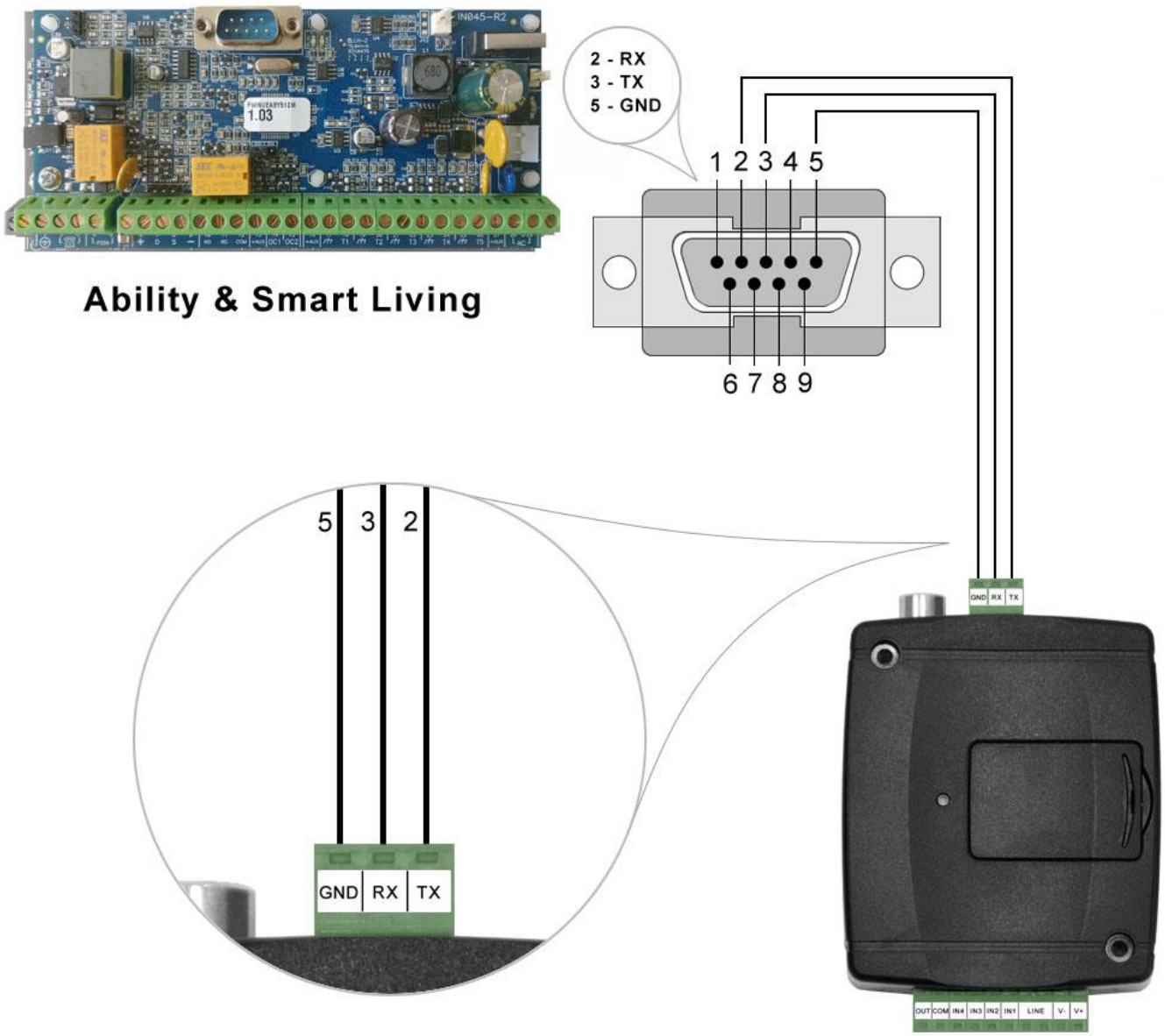
Then the programming software will open the serial port and will establish the connection with the alarm control panel.

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



5.1.5 Inim alarm systems

- **Installation:**



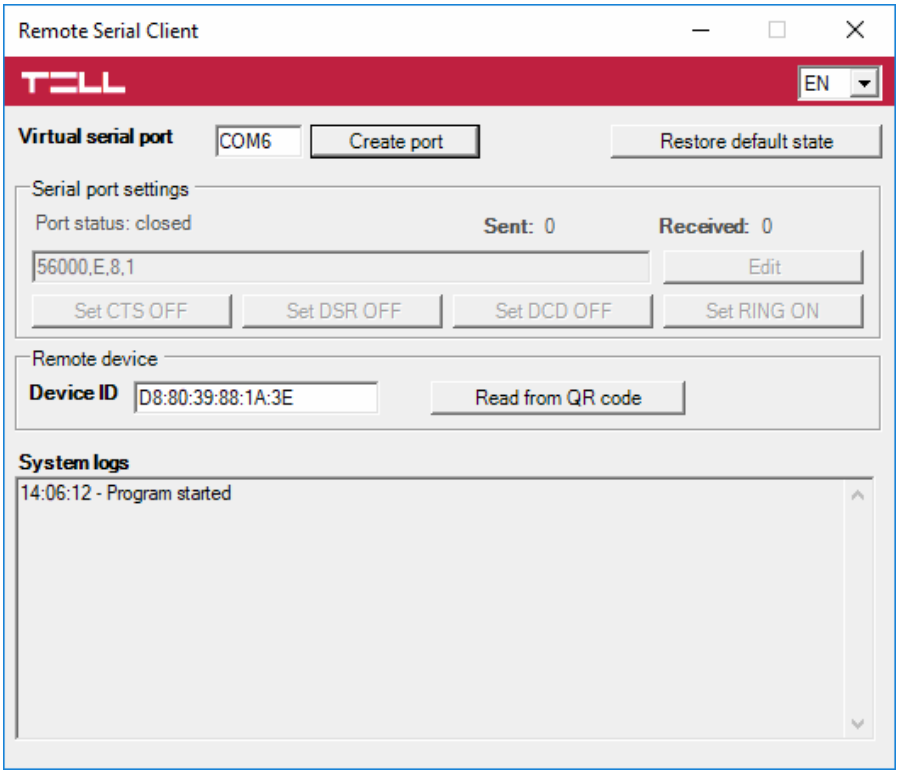
Wiring diagram for Inim alarm systems

Connect the supplied special cable to the serial port of the ***ecoLINE PRO*** device as shown in the figure above, then plug it onto the alarm control panel.

- **Software settings:**

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

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



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

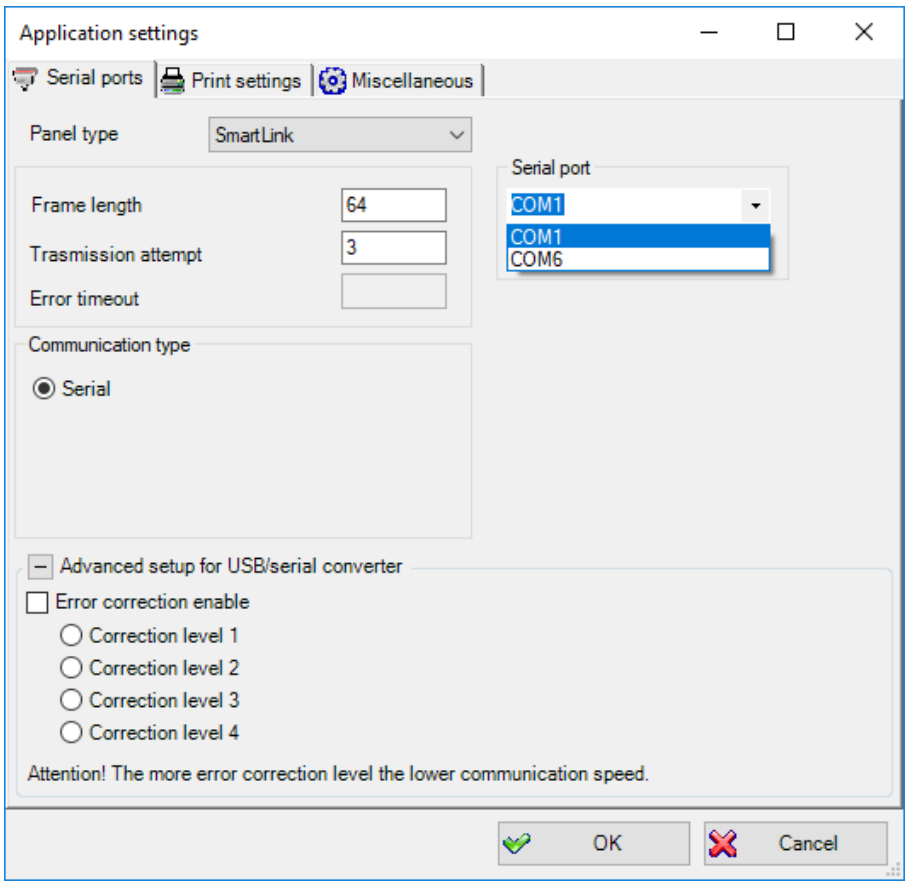
Device ID: enter the device identifier (6x2 hexadecimal characters separated by colons) of the ***ecoLINE PRO*** device connected to the alarm control panel.
Using the "***Read from QR code***" button, you can also read the device ID from the image file saved from the programming software, that contains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

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

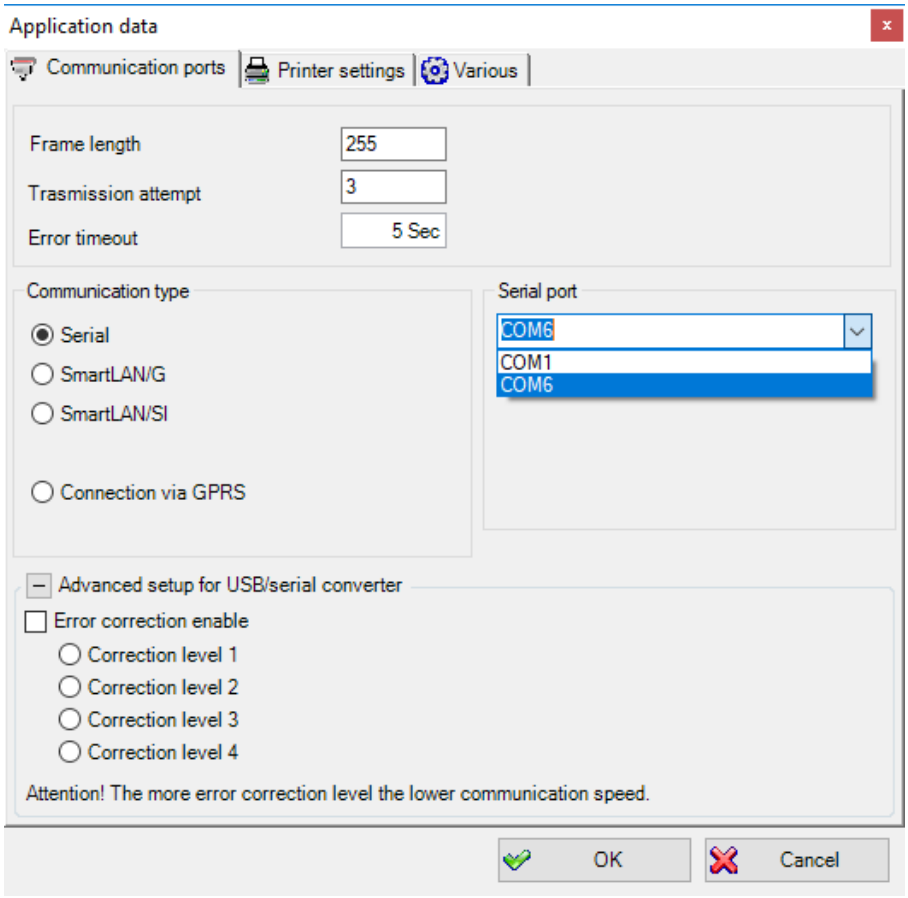
System logs: shows information about program operation and displays data received through the serial port.

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

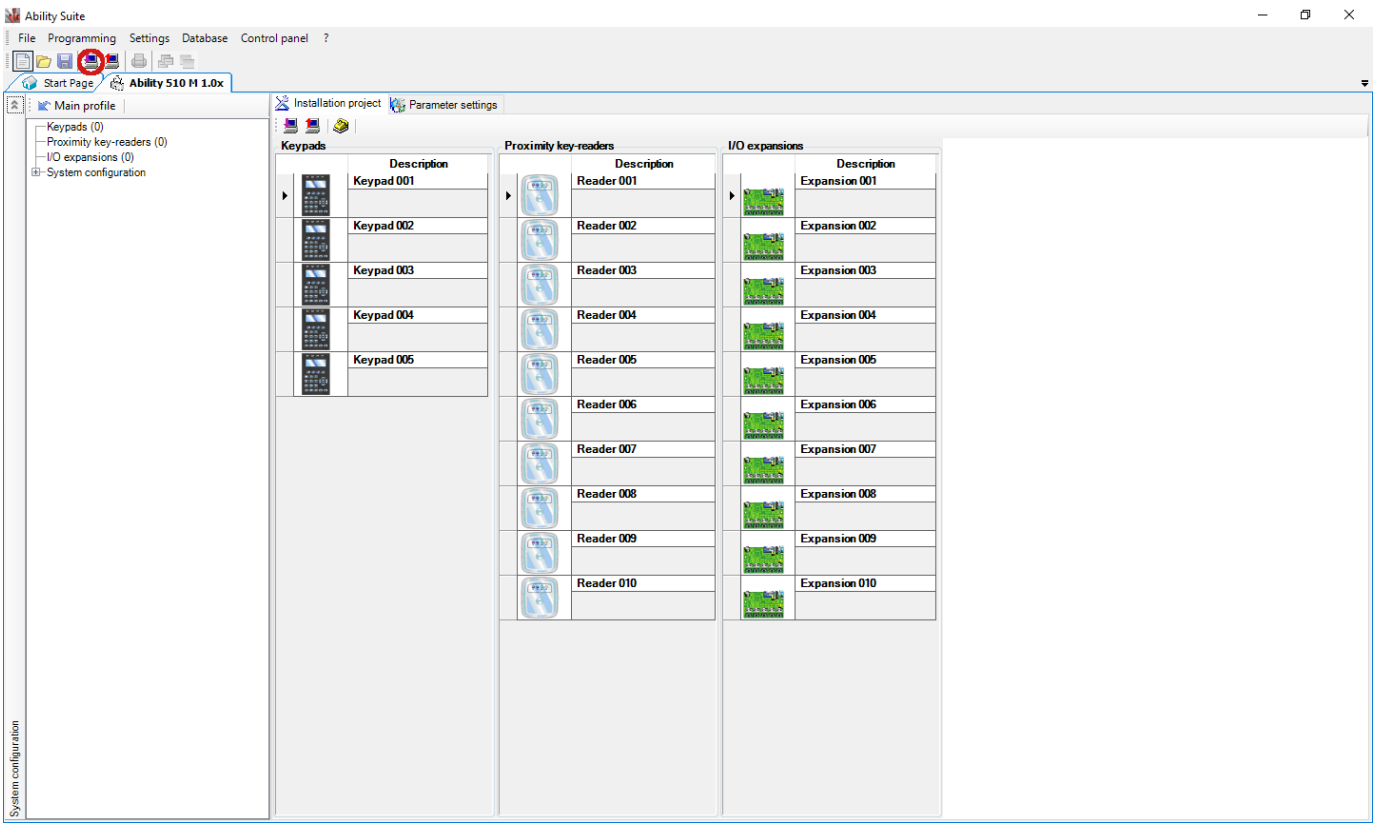
Example for selecting the serial communication port in the ***Ability Suite*** programming software, in the "***Settings / Application settings***" menu:



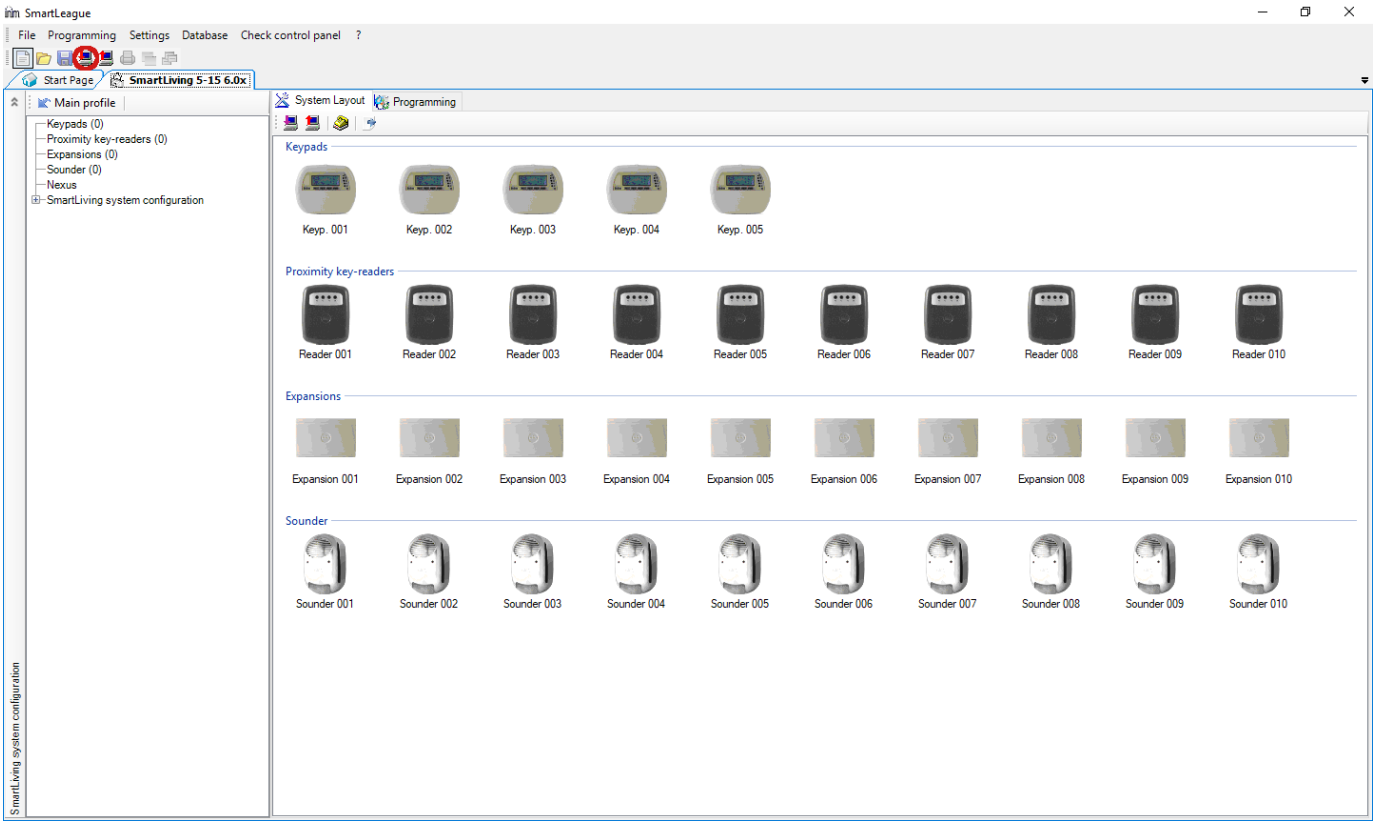
Example for selecting the serial communication port in the ***Smart League*** programming software, in the "***Settings / Application settings***" menu:



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

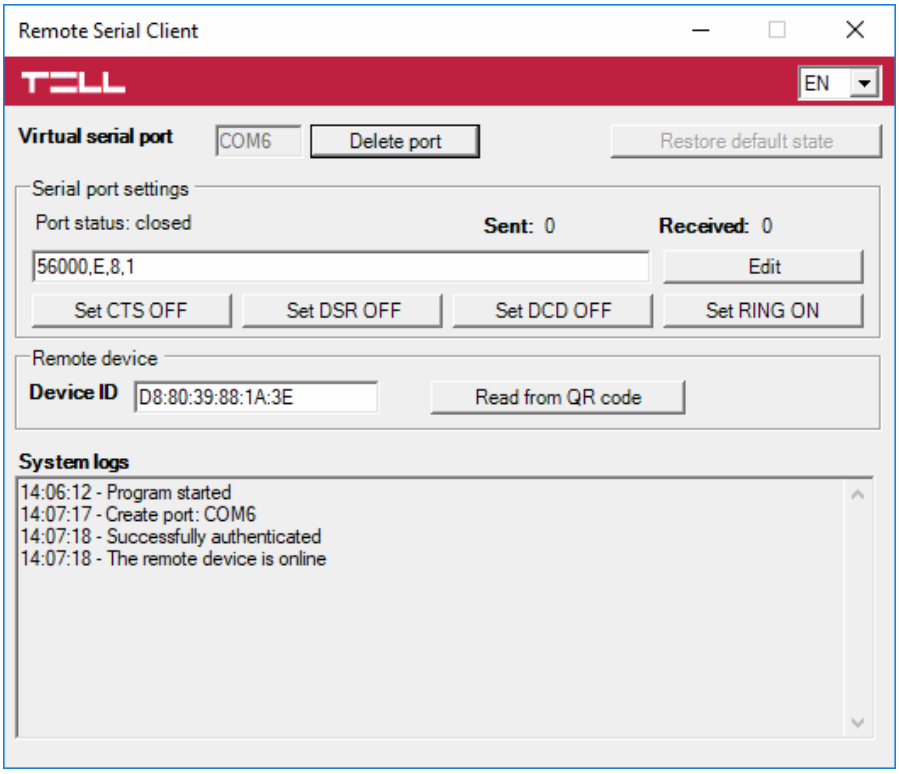


Start connecting with the ***Smart League*** programming software:



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

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



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

It is possible to arm and disarm a partition in the connected alarm system via the mobile application, if the given alarm control panel can be armed and disarmed by dry relay contact pulses through one of its inputs. To use this feature, connect the relay output (**OUT** and **COM**) of the ***ecoLINE PRO*** to the alarm control panel's input used for arming and disarming, set the given input in the alarm control panel to normally open (**NO**) pulse control, and then configure the control mode of the device's output in the ***Output*** menu. Select the ***Monostable*** option (you can leave the pulse duration setting on the factory default value of 1500 milliseconds), and set the number of the ***Controlled partition***.

After doing the wiring and configuring the settings correctly, to arm and disarm the alarm system, activate the output of the ***ecoLINE PRO*** in the mobile application using the button provided with the padlock symbol. Each output activation action will close the **OUT** and **COM** terminals for the configured period of time (1.5 seconds), and then will revert to default open state automatically. The contact pulses generated this way will arm and disarm the alarm system through the alarm control panel's input appropriate for this. As soon as the alarm system reports the arming or disarming event, this will trigger the color and status change of the control button in the mobile application, which is intended to indicate the partition status change.

For this function to work, and in order to receive state messages on arming and disarming in the mobile application, reporting of arming and disarming events should be enabled in the alarm control panel, and the number of the controlled partition should be set correctly in the output settings of the ***ecoLINE PRO*** device.

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.

You can update the ***ecoLINE PRO*** firmware 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 application or the programming software.

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

- **Updating via USB using the programming software:**
  - Download the latest firmware file (that has the **.tf3** extension) necessary for updating, from the manufacturer's website.
  - Click on the "***General***" device settings 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 a few seconds later, running on the new firmware.

7.2 Updating remotely over the internet

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

8 Restoring the factory default settings

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

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

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

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 passwords, but the settings cannot be restored if the device lock option has been enabled in the settings.

9 Contents of the package

- ***ecoLINE PRO*** + terminal connector
- GSM antenna
- Installation and application manual
- 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