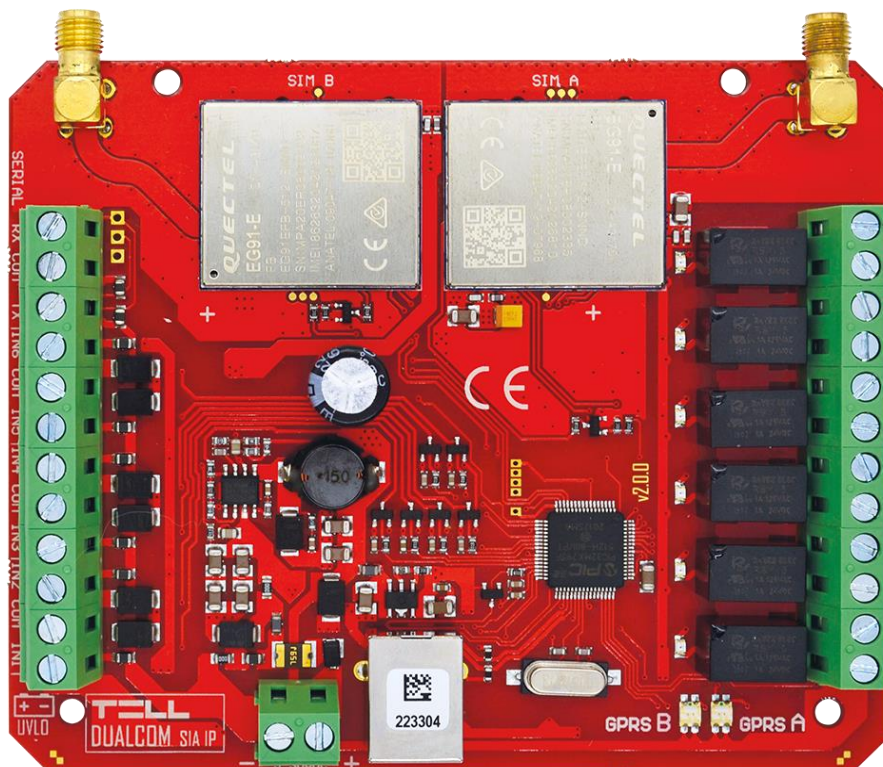


DUALCOM

INSTALLATION AND APPLICATION MANUAL

for device version V3.04

Document version: 3.71 30.03.2023



Product models:

- DUALCOM - 2G.IN6.R6
- DUALCOM - 4G.IN6.R6
- DUALCOM - 2G.IN6.R6 KIT
- DUALCOM - 4G.IN6.R6 KIT

Table of contents

1	Application	4
2	Functions	4
3	Difference between the 2G, 4G and KIT models	4
4	Device overview	5
5	Wiring and putting in operation	6
5.1	Under Voltage Lock Out (UVLO) function	6
5.2	Input wiring	6
5.3	Output wiring	7
5.4	EXT24-D expansion module	7
5.5	SIM card holders	8
5.6	Connecting the antenna	9
5.7	Signals of the status LEDs (GPRS A and GPRS B)	9
5.8	Installation	9
5.9	Putting into operation	9
5.10	Technical specification	10
6	General logic of reporting for fire alarm systems	11
6.1	Estimated data usage	11
7	Configuring the DUALCOM	12
7.1	The user interface and configuration options of the software	12
7.2	Methods for connecting to the device	13
7.2.1	TELL servers and receivers	13
7.2.2	Configuring directly via USB	14
7.2.3	Remote connecting to devices via cloud service	15
7.2.4	Remote connecting to devices which are using the TEX protocol	18
7.2.5	Remote connecting to devices which are using the TELLMon protocol	19
8	DUALCOM SIA IP programming software usage and feature descriptions	21
8.1	Connection menu	21
8.1.1	Viewing the settings options and configuring offline	21
8.1.2	Connection type	22
8.1.3	Device register	24
8.1.4	Server register	26
8.2	Device settings menu	29
8.2.1	General	29
8.2.2	Reporting channels	33
8.2.3	Notification templates	36
8.2.4	Inputs	38
8.2.5	Input events	40
8.2.6	Tamper events	45
8.2.7	Service events	49
8.2.8	Advanced settings	55
8.3	Device status menu	56
8.3.1	Status monitoring	56
8.3.2	Event logs	58
8.3.3	System event logs	60
8.3.4	System logs	61
8.4	Software settings menu	62
8.4.1	Settings	62
8.4.2	About	63

9	Configuring by SMS commands	64
10	Updating the firmware	67
10.1	Updating via USB	67
10.2	Updating remotely over the internet	68
11	Restoring the factory default settings	68
12	Contents of the package	68
13	About the manufacturer	68

1 Application

Communicator for fire alarm control panels, that reports the activity of the connected fire alarm control panel's outputs to CMS receivers, through IP channel over the mobile Internet. It can be used for any control panel which has contact outputs, or where contact outputs can be obtained using relays. The device supports the following protocols for reporting to CMS:

- **SIA IP** protocol based on **ANSI/SIA DC-09-2007** standard
- **TELLMon** protocol (custom TELL protocol)
- **TEX** protocol (custom TELL protocol)

The device works with the following receiver models: **TELLMon**, **MVP.next**, **AMR-08**, **ENIGMA II**, **TEX-MVP**, **TEX BASE/PRO**, and all receivers that support the **SIA DC-09** protocol.

2 Functions

- Parallel usage of two independent GSM modems.
- Reporting up to 4 IP addresses, which means 2 primary IP addresses per network.
- 6 NO/NC/EOL contact inputs.
- 6 alarm-activated NO relay outputs.
- Programmable by PC software and by SMS.
- Supervision message with configurable sending interval for automatic supervision of transmission channels.

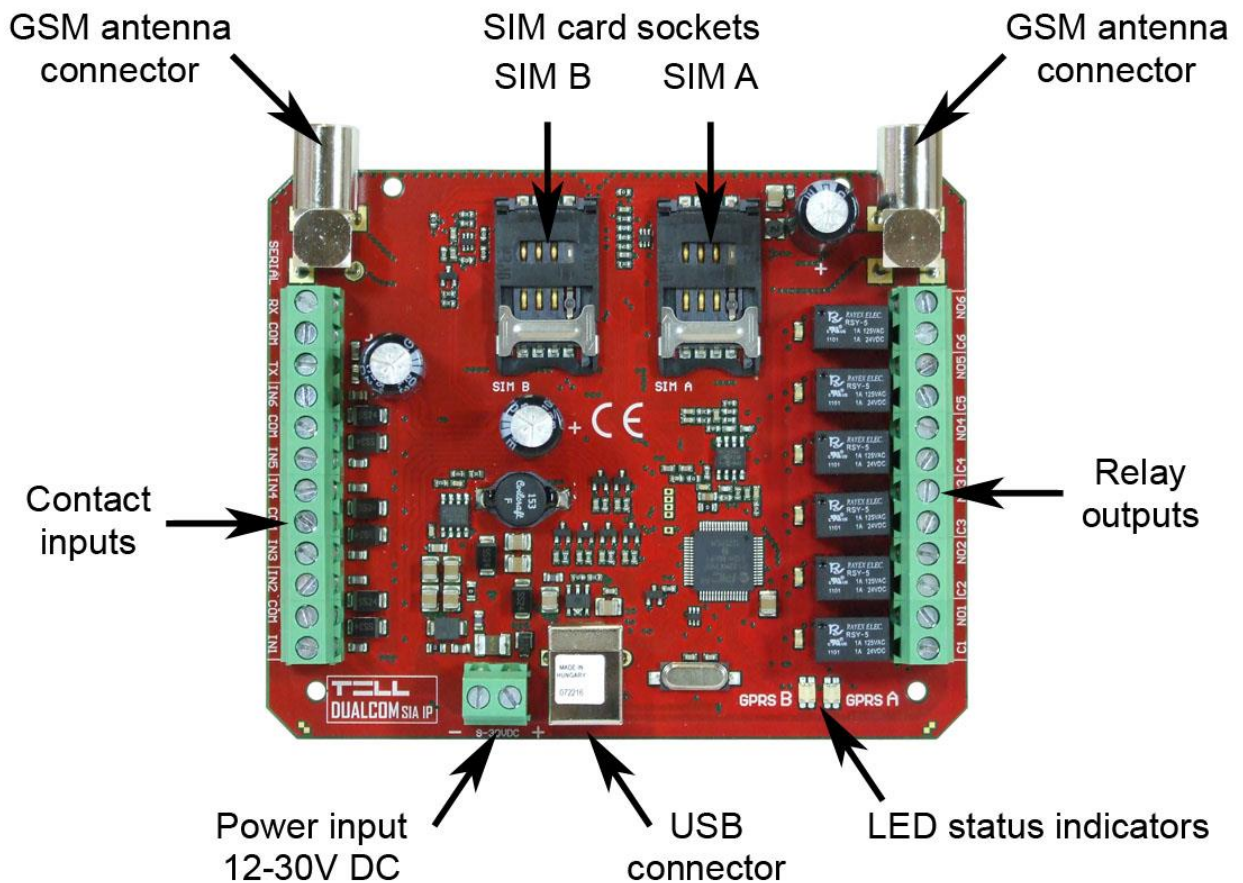
3 Difference between the 2G, 4G and KIT models

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

The **KIT** models include a metal box and a power supply in addition to the device.

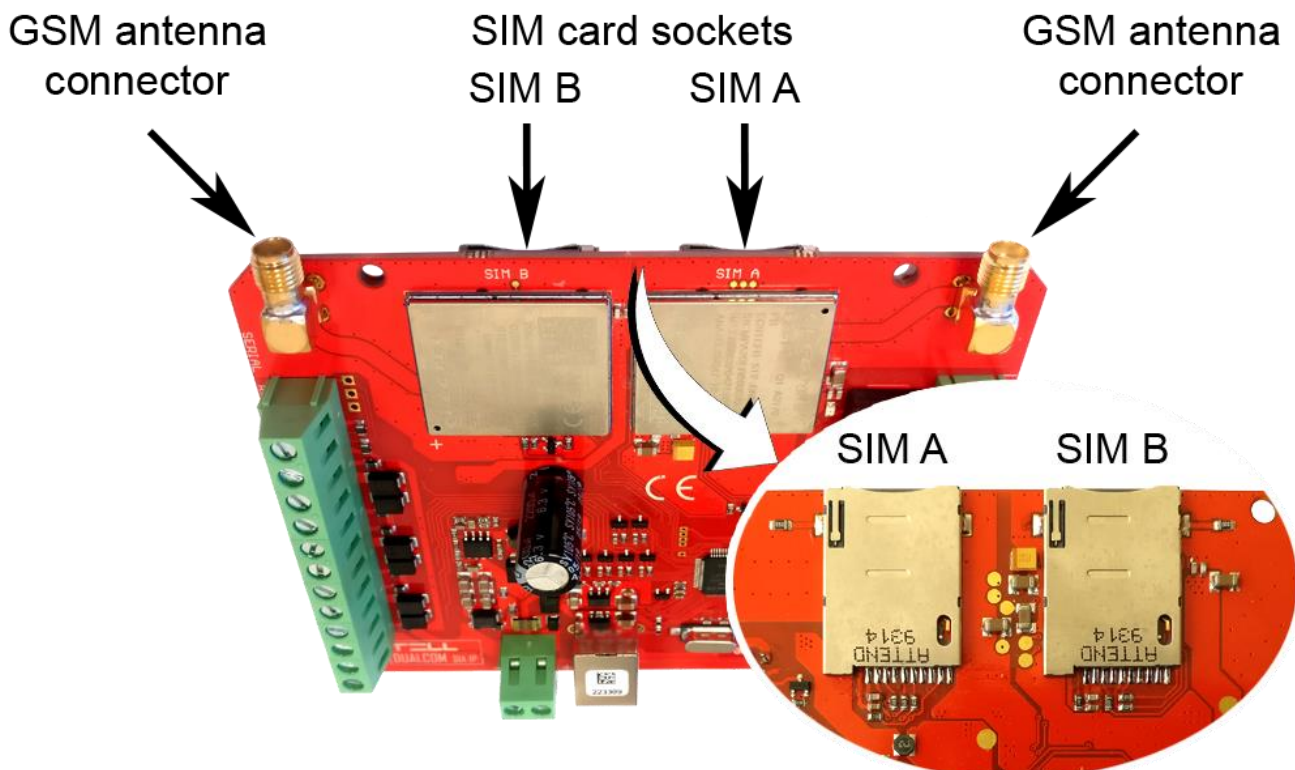
4 Device overview

a) 2G product variant:



b) 4G product variant:

Unlike the 2G product variant, the 4G variant has the SIM card holders on the back of the panel, and uses SMA type antenna connectors.



5 Wiring and putting in operation

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

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

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

- Recommended TELL power supply: TT25VA-12V5.

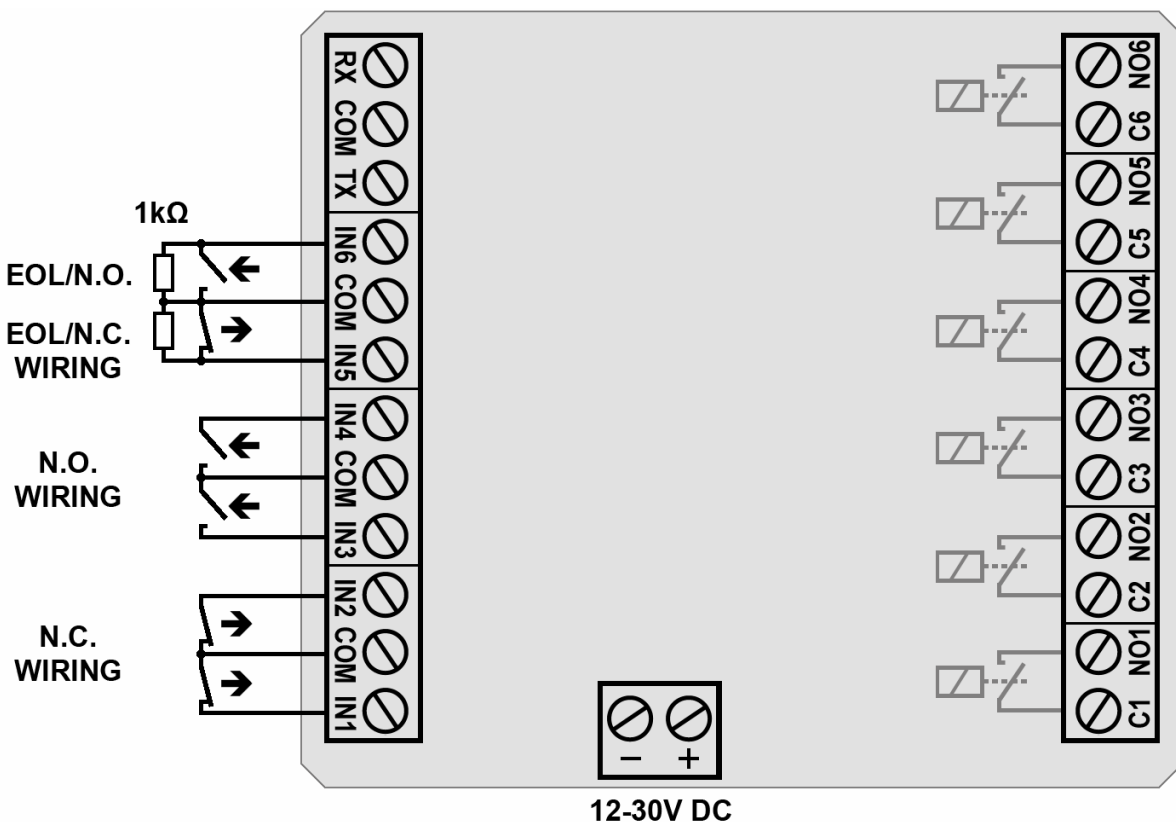
5.1 Under Voltage Lock Out (UVLO) function



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

5.2 Input wiring

The normally open or normally closed dry contacts should be connected between the selected input (**IN1...IN6**) and the **COM** terminal placed next to the input. In case of using an end-of-line (**EOL**) resistor, the **1kΩ** resistor should be connected to the end of the loop, in a parallel connection with the dry contact.



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...IN6**) and 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...IN6**) and the **COM** terminal becomes open.

In case of using an end-of-line resistor for an input, enable the **EOL** option in the settings for the given input.

Attention! If an input is not used, but you configure it as normally closed (**NC**), you have to close the given input according to the settings with a short wire. Otherwise, the given input may cause false alarms.

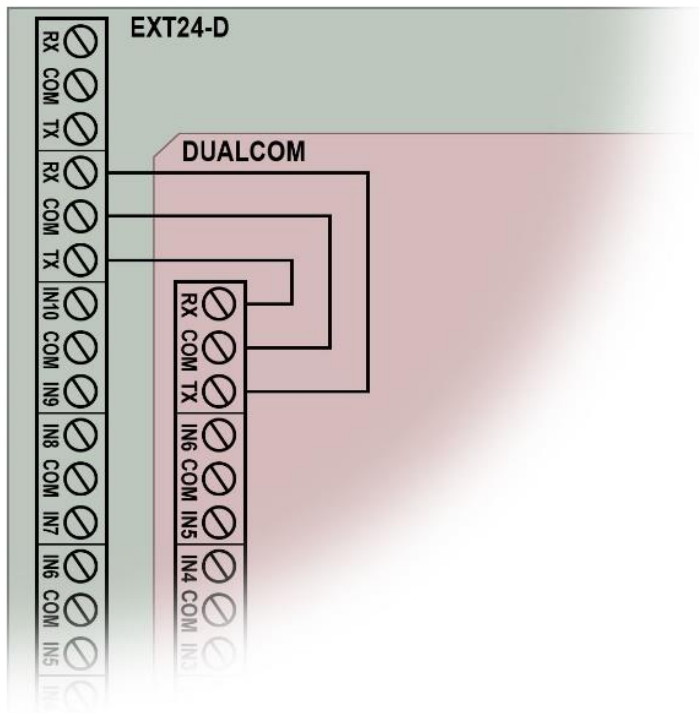
5.3 Output wiring

The outputs provide normally open (N.O.) dry (potential free) relay contacts by default and closed contacts upon control.

5.4 EXT24-D expansion module

Using the **EXT24-D** expansion module, you can expand the 6 onboard inputs of the **DUALCOM** with further 24 inputs.

- **Connecting the EXT24-D expansion module:**



In order to connect the **EXT24-D** expansion module, do the wiring of the terminals as shown in the figure at the side.

DUALCOM		EXT24-D	
<i>RX</i>	->	<i>TX</i>	RX/TX terminal block next to input IN10
<i>COM</i>	->	<i>COM</i>	
<i>TX</i>	->	<i>RX</i>	

The wiring of the expansion module inputs should be done the same way as for the inputs of the **DUALCOM** device.

5.5 SIM card holders

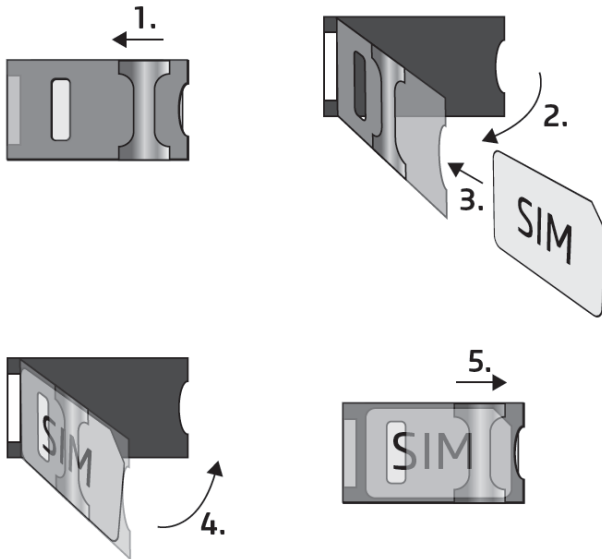
- **Inserting the SIM cards:**

The device requires **Mini (2FF) size SIM cards**.

Attention! Inserting or removing the SIM card when the device is powered up is strictly prohibited! In this case both the SIM card and the device may suffer a damage that automatically implies loss of warranty!

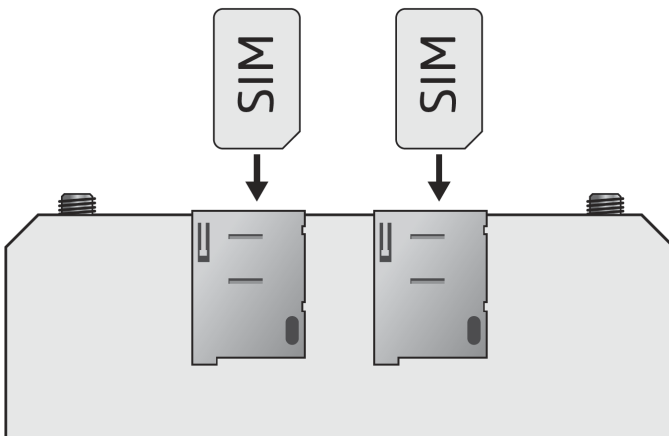
Insert the SIM cards into sockets **SIM A** and **SIM B**.

a) For the 2G product variant:



- 1. Pull the metal security lock of the SIM holder towards the upper edge of the panel, 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.
- 4. Fold back the opened part together with the SIM card.
- 5. Secure the SIM card by pressing down carefully the metallic security lock and pulling it towards the USB connector, until you hear a click.

b) For the 4G product variant:



- Slide the SIM card into the holder as shown in the figure, with the contacts facing the panel, and then push it all the way in against the spring until you hear a click.
- If you want to remove the SIM card from the holder, push the card again against the spring until you hear a click. This will eject the card, and you can pull it out from the holder.

5.6 Connecting the antenna

Connect the GSM antennas to the antenna sockets. The 2G product variant has FME-M connectors, while the 4G variant uses SMA type connectors. The device comes with antennas that provide good transmission under normal reception circumstances. In case of experiencing signal strength problems or/and wave interference (fading), use directed antennas, or find a more advantageous mounting place for the antennas. In case of installing the unit into a metal box, the antennas should be mounted outside the box, in a place where the measured GSM signal is the highest available.

5.7 Signals of the status LEDs (GPRS A and GPRS B)

Slow flashing green	Connected to the mobile Internet, idle state
Quick flashing green	Reporting is in progress
Flashing red	System startup/restart is in progress
Permanent red	Error

5.8 Installation

Please check the environment before installing the device.

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

5.9 Putting into operation

- **Disable the voicemail service and SMS notification about missed calls on the SIM card installed in the device.**
- **The device can handle the SIM card's PIN code. If you want to use the PIN code management, configure the SIM card's PIN code in the programming software in the "General" device settings menu. Otherwise disable PIN code request on the SIM card.**
- Make sure that the mobile Internet service is available on the SIM cards.
- Make sure that the SIM cards are installed properly.
- Make sure that the antennas are connected to the FME-M connectors.
- You can power up the device (12...30V DC). Make sure that the power source is sufficient for the operation of the device. The nominal current consumption of the device is 70mA, however, it may increase up to 400mA during communication and output control. If the used power source is not sufficient for the operation of the device, this may cause malfunctions.

5.10 Technical specification

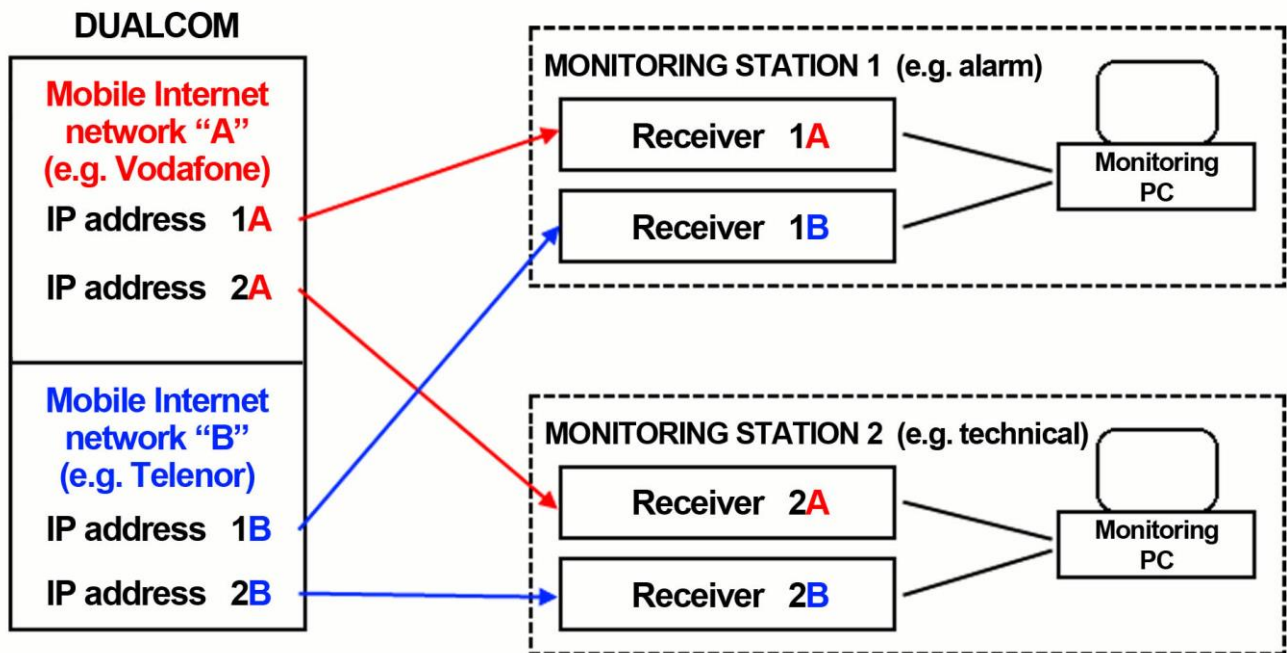
Supply voltage range:	12-30V DC
Nominal current consumption:	70mA @ 12V DC, 40mA @ 24V DC
Maximum current consumption:	400mA @ 12V DC, 200mA @ 24V DC
Operating temperature:	-20°C to +70°C
Transmission frequency:	
2G model:	850/900/1800/1900 MHz
4G model:	900/1800 MHz@GSM/EDGE, B1/B8@WCDMA, B1/B3/B7/B8/B20/B28A@LTE
Antenna connector type:	
2G model:	FME-M
4G model:	SMA
Highest load supported on outputs:	1A @ 24VAC/DC
Dimensions:	116 x 100 x 25mm
Net weight:	280g
Gross weight (packed):	300g

6 General logic of reporting for fire alarm systems

The reporting scheme shown below illustrates the general use and recommended operation for fire alarm systems. Of course, it is also possible to configure a different operating mode using custom notification templates. You can read more about this in chapter “[Notification templates](#)”. The device reports the events generated by triggering the contact inputs simultaneously to the configured receiver IP addresses, through both independent mobile Internet channels. The requirement for the simultaneous operation is a pair of receivers operating on two different networks, on the remote monitoring station side.

The logical scheme in the figure below illustrates the method of reporting. The legend for the IP address markings is the following:

Monitoring station numbering	Mobile service provider marking
1	A= e.g. Vodafone B= e.g. Telenor
2	A= e.g. Vodafone B= e.g. Telenor



After an event occurs, the device establishes IP connection with the configured receivers through both networks (A and B) at the same time. The reports are sent through the different networks and to the different remote monitoring stations in parallel. Due to the parallel operation, ideally each receiver receives the event roughly at the same time (in about 5 seconds in average). If sending fails through a network on the device side, or delay occurs, the other network’s transfer rate and availability will still be provided. The system provides possibility for use with two remote monitoring stations. The two monitoring stations shown in the figure above can be completely equivalent, or functionally separated (e.g. alarm and technical). If reporting to only one remote monitoring station is required, then it is enough to configure receivers 1A and 1B only.

6.1 Estimated data usage

- **CMS communication:** in case of using the TCP protocol, by a supervision message interval of 60 seconds, the expected data usage is about 25MB/month per each configured IP address. For the UDP protocol, the expected data usage is about 9MB/month.
- **Cloud usage:** if the service is enabled, maintaining a permanent connection with the cloud uses about 12MB/month.

7 Configuring the DUALCOM

The device can be configured the following ways:

- By computer via USB, using the programming software.
- By computer over the Internet, using the programming software.
- Main parameters can also be configured remotely via SMS commands.

The **DUALCOM SIA IP** programming software is compatible with the following operating systems:

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

Earlier Windows operating systems are not supported by the software.

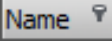

Installing the programming software: open the software setup application and follow the instructions of the installation wizard to complete the installation. The latest version of the programming software is available on the manufacturer's website (<http://www.tell.hu>).

7.1 The user interface and configuration options of the software

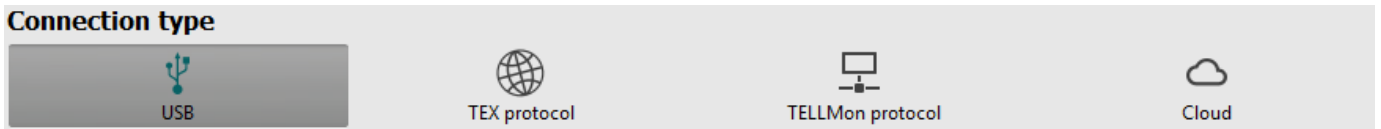
The user interface language can be selected during installation.

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

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

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

7.2 Methods for connecting to the device



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

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

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

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

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

- MVP.next server;
- TELLMon receiver.

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

7.2.1 TELL servers and receivers

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







7.2.2 Configuring directly via USB

To start programming the device, follow the instructions below:

- Open the **DUALCOM SIA IP** programming software.
- Select the USB option in the “**Connection type**” menu, power up the device and connect it to the computer using a USB-A to USB-B cable.

Connection parameters

Device password

- Enter the device password.
 - Super administrator permission: full access to all settings. (Default password: **1234**).
 - Administrator permission: full access to all settings except device identification settings.
 - 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.
- To close the connection, click on “**Disconnect**”  button.

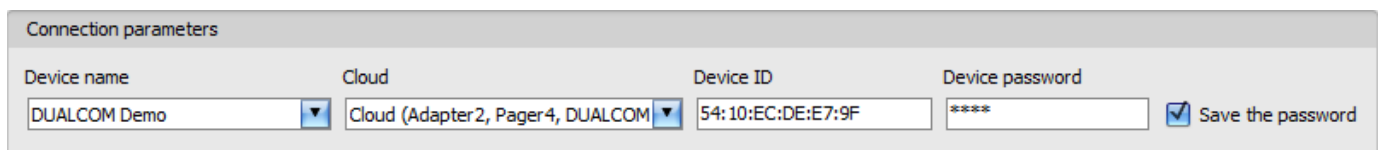
7.2.3 Remote connecting to devices via cloud service

This connection type can be used if the **DUALCOM** device is connected to the cloud. In case that you use a SIM card in the device, that works in a private APN, you have to arrange with the mobile service provider to open the given private APN for accessing the cloud server IP address at 54.75.242.103, port: 2020.

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

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

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



Device name	Cloud	Device ID	Device password	
DUALCOM Demo	Cloud (Adapter2, Pager4, DUALCOM)	54:10:EC:DE:E7:9F	*****	<input checked="" type="checkbox"/> Save the password

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

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


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

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

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

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

Connecting to the device through the cloud:

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

Entering the device password.

- Super administrator permission: full access to all settings. (Default password: **1234**).
- Administrator permission: full access to all settings except device identification settings.
- Connecting remotely without a password is not possible.
- If cloud usage is enabled in the settings of the given device, the device keeps continuous connection with the cloud server. In this case skip the SMS sending process mentioned below. Cloud usage can be enabled in the “**General**” settings menu. If cloud usage is disabled, the device will not keep continuous connection with the cloud, it will only connect upon request. Therefore, if this is the case, before trying to connect remotely to the device, the request for connecting to the server should be sent by SMS to the phone number of the SIM card installed into the device. The device accepts the request for connecting to the cloud server from the “**Admin phone number**” configured in the “**General**” device settings menu, or from any phone number, if the valid device password is specified at the beginning of the message. You can specify the device password in the message using the “**PWD**” parameter, as shown below. Commands sent from unauthorized phone numbers with a missing device password or a wrong password, will be ignored by the device and it will not send any reply to these numbers.

Commands should always be typed using capital letters.

If you want the device to use interface **SIM B** to connect to the cloud instead of the default interface **SIM A**, first change the interface used for this to **SIM B** using the following command:

When sent from the **Admin phone number**: **CLOUD=SIMB#**

When sent from **other phone number**: **PWD=device password#CLOUD=SIMB#**

The request command for connecting to the server is:

When sent from the **Admin phone number**: **CONNECT#**

When sent from **other phone number**: **PWD=device password#CONNECT#**

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

Example on the usage of the command, with the default password: **PWD=1234#CONNECT#**

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

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

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

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

Possible error messages:

Message	Specification
Missing APN	The APN is not configured.
Network connection error	The device is unable to connect to the Internet due to an error, faulty settings, or missing Internet service.
CLOUD syntax error	The parameter specified for the CLOUD command is wrong.

It is also possible to configure the cloud settings using the commands below, but normally the factory default values are already configured for this. The following commands will set the cloud server address and port number, and then the device will initiate a cloud connection automatically.

When sent from the **Admin phone number**:

CONNECT=server address:port nr#

When sent from **other phone number**:

PWD=device password#CONNECT=server address:port nr#





Example on the usage of the commands mentioned above:

CONNECT=54.75.242.103:2020#

PWD=1234#CONNECT=54.75.242.103:2020#

If the APN settings are not configured in the device, or if they are wrong, you can configure this too along with selecting the default interface for cloud usage, using the commands found in chapter "[Configuring by SMS commands](#)".

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

- Click on the "**Connect**"  button and wait for the connection to establish. The process of connecting may take a few seconds.
- The connection status is indicated by the status icon in the top left corner of the program window:
 -  disconnected (green)
 -  connected (gray)
- After connecting using the valid password, you can configure the device, change settings, download event logs, and monitor system status.
- To disconnect from the device, click on the "**Disconnect**"  button.

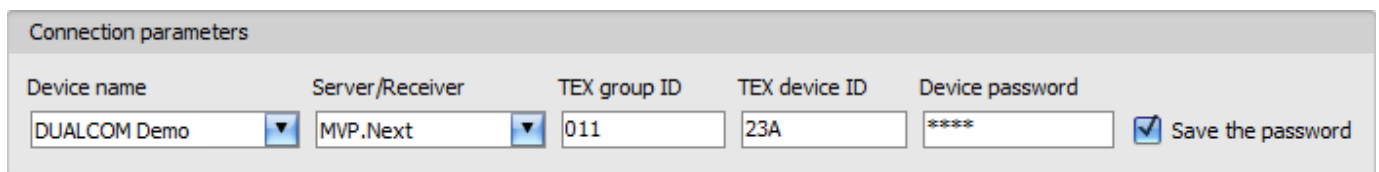
7.2.4 Remote connecting to devices which are using the TEX protocol

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

Further details on the remote access of devices via the MVP.next server you can find in chapter "[Server register / Remote access of devices via the MVP.next server](#)".

Connection between the device and the *DUALCOM* programming software can be established through the server/receiver on which the device is online.

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



Device name	Server/Receiver	TEX group ID	TEX device ID	Device password	
DUALCOM Demo	MVP.Next	011	23A	****	<input checked="" type="checkbox"/> Save the password

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

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


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

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

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


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

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


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

Entering the device password.

- Super administrator permission: full access to all settings. (Default password: **1234**).
- Administrator permission: full access to all settings except device identification settings.
- 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:



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

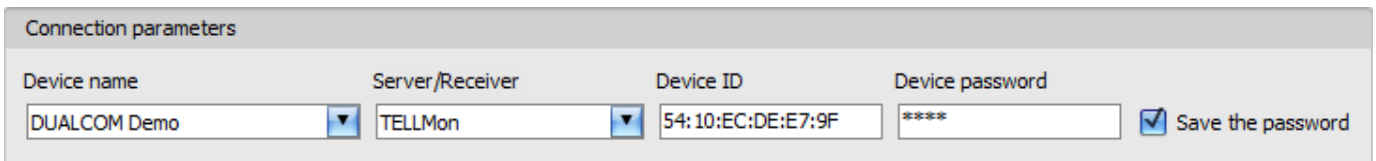
7.2.5 Remote connecting to devices which are using the TELLMon protocol

This connection type can be used if the *DUALCOM* device you want to access remotely is connected to a TELLMon receiver or an MVP.next server, and it has been configured to communicate with the given server or receiver using the TELLMon protocol.

Further details on the remote access of devices via the MVP.next server you can find in chapter “[Server register / Remote access of devices via the MVP.next server](#)”.

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

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



Device name	Server/Receiver	Device ID	Device password	
DUALCOM Demo	TELLMon	54:10:EC:DE:E7:9F	****	<input checked="" type="checkbox"/> Save the password

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

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


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

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

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


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

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

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

Entering the device password.


- Super administrator permission: full access to all settings. (Default password: **1234**).
- Administrator permission: full access to all settings except device identification settings.
- Connecting remotely without a password is not possible.

- Click on the “**Connect**”  button.
- **The DUALCOM device that communicates using the TELLMon protocol is not online continuously. The device connects to the server or receiver only when it sends a supervision message or reports an event. Therefore, after clicking on the “Connect” button, you will have to wait for the device until it next connects to the server or receiver to send a supervision message or report an event. This is the moment when the programming software can connect to the device. Therefore, if the device is configured to rarely send supervision messages to the server or receiver, the programming software can connect to the device after a long time only (depending on the configured supervision message sending interval).**

- The connection status is indicated by the status icon in the top left corner of the program window:

 disconnected

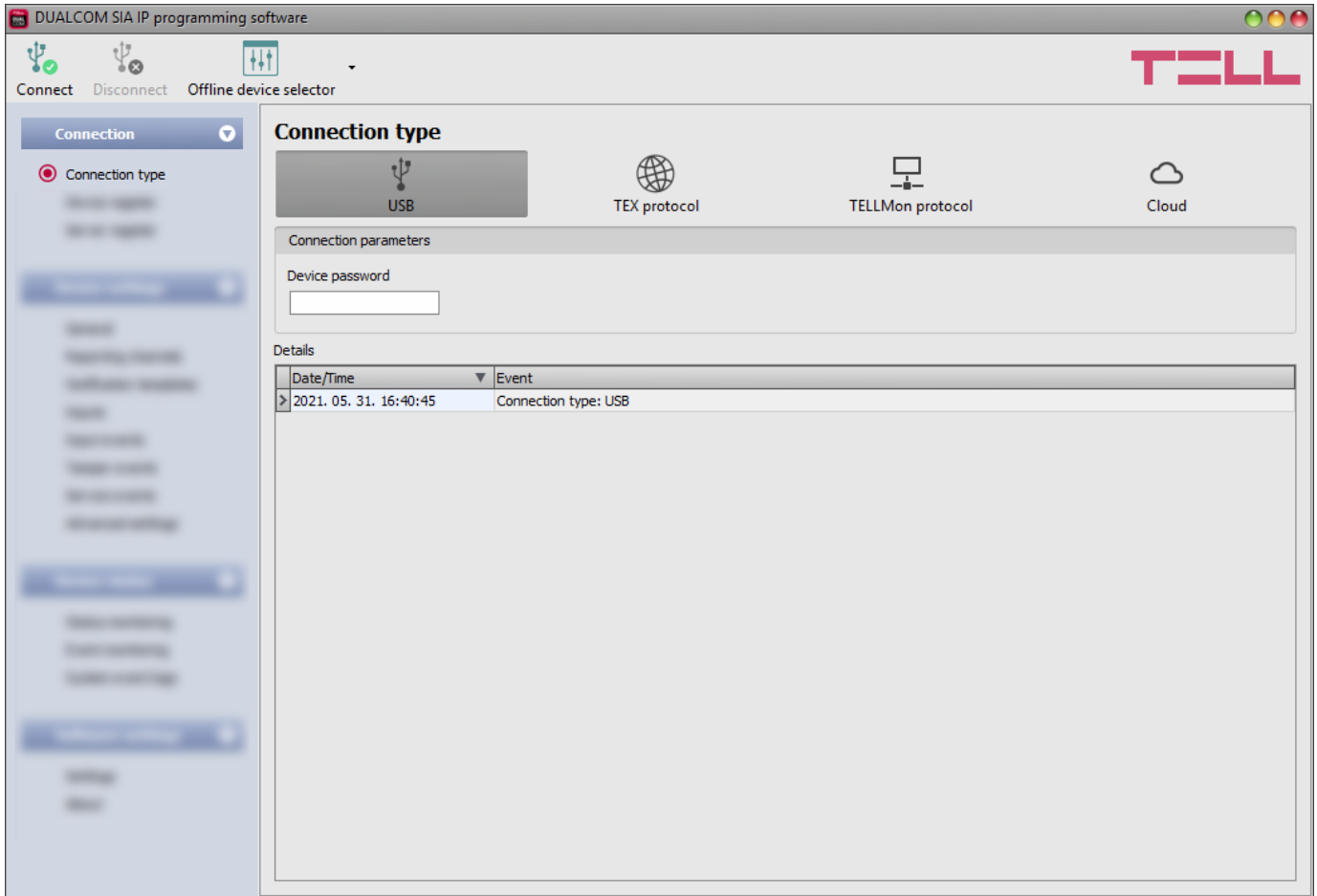
 connected

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


8 DUALCOM SIA IP programming software usage and feature descriptions

8.1 Connection menu

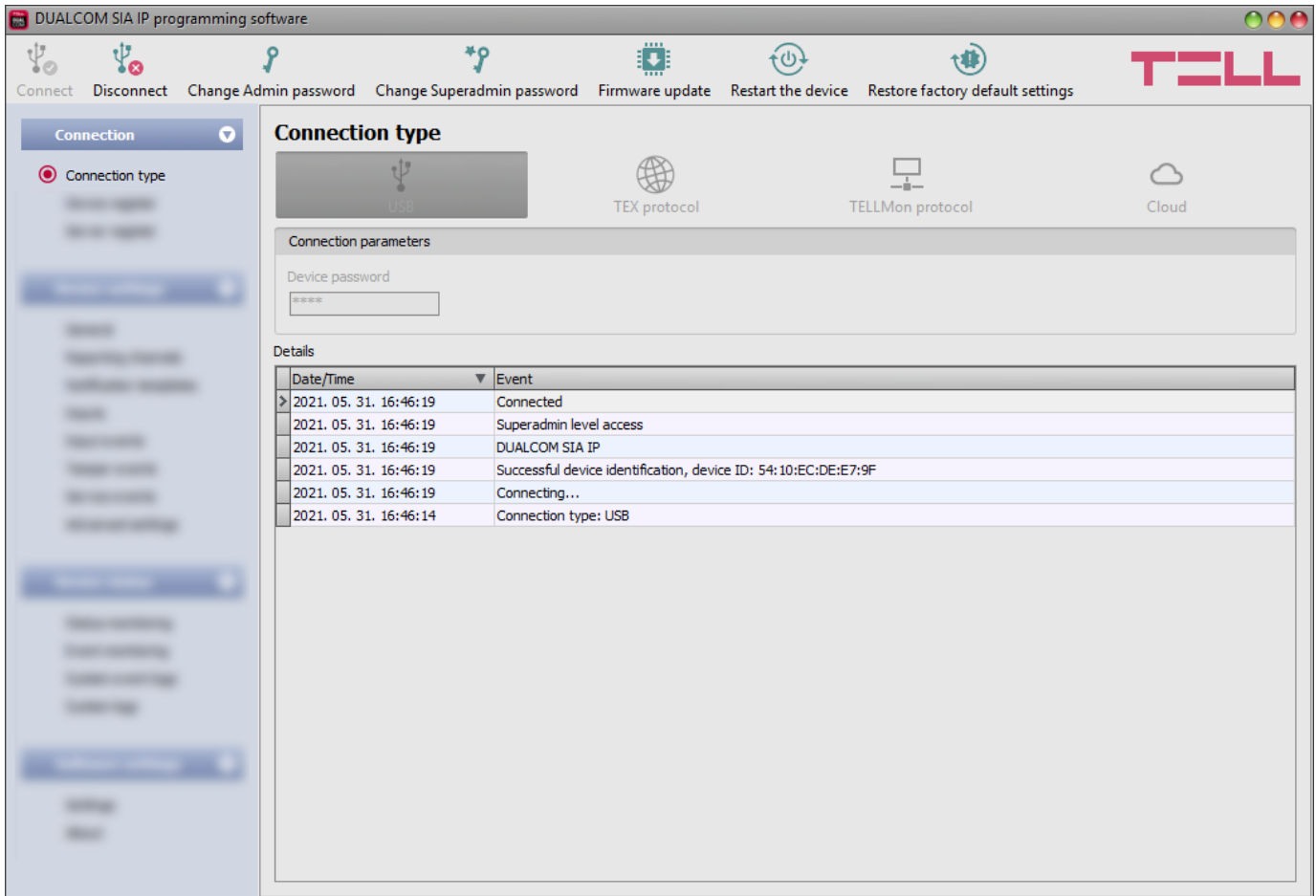
8.1.1 Viewing the settings options and configuring offline



The “**Offline device selector**” enables you to view the settings options of the **DUALCOM** device, and to configure and save the settings in advance offline, without connecting the device.

If you want to configure and save the settings of a **DUALCOM** device model, click on the “**Offline device selector**”  button.

8.1.2 Connection type




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

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


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

Available options:

- **Change Admin password:**

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

- **Change Superadmin password:**

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

The dialog box titled 'Changing the Superadmin password' contains three input fields: 'Actual password', 'New password', and 'Confirm new password'. Below the fields is a warning message: 'The following characters are not supported: ^ ~ < > = | \$ % " , ^'. At the bottom are 'OK' and 'Cancel' buttons.

Enter the actual password, then the new password and its confirmation, then click “**OK**”. The password should consist of at least 4, but not more than 8 characters. Accepted characters are: numbers (0...9), lower case letters (a...z), and capital letters (A...Z).

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

- Updating the firmware:



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

- Restart the device:



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

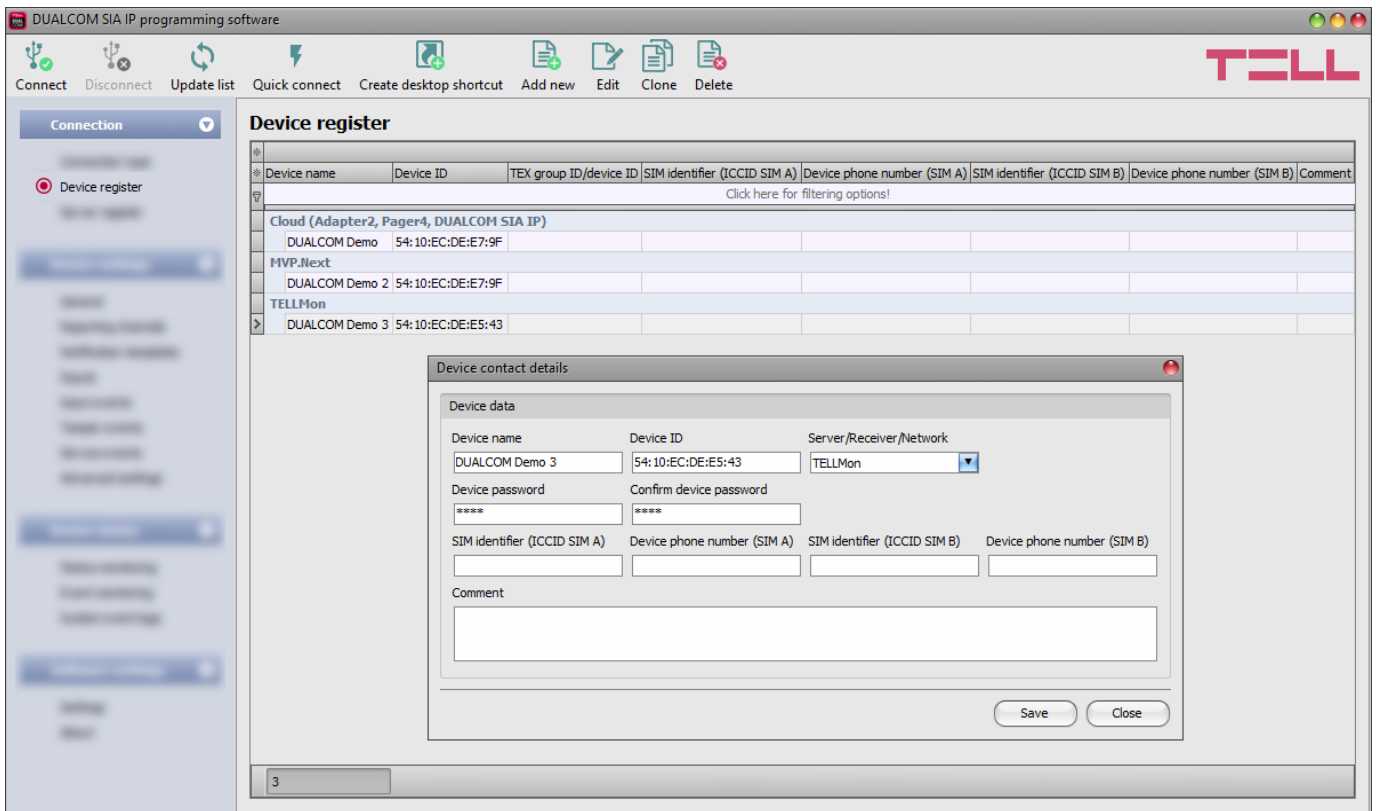
- Restore factory default settings:



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

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


8.1.3 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, from the “**Device name**” drop-down menu, from the devices added to the database. You can also connect remotely to a device directly from the device register, by selecting the device, and

then clicking on the **Quick connect**  button.

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

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

If needed, you can import a database exported from an earlier version of the program using the **MMTool** software which is included in the setup of the **DUALCOM** programming software.

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

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



: update the records from database



: quick remote connect to the selected device



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



: add new device



: clone entry (duplicate)



: edit entry



: delete entry

Data stored in the device register:

Device name: custom device name

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

The format of the device identifier is: **FF:FF:FF:FF:FF:FF** (6x2 hexadecimal characters).

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

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

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

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

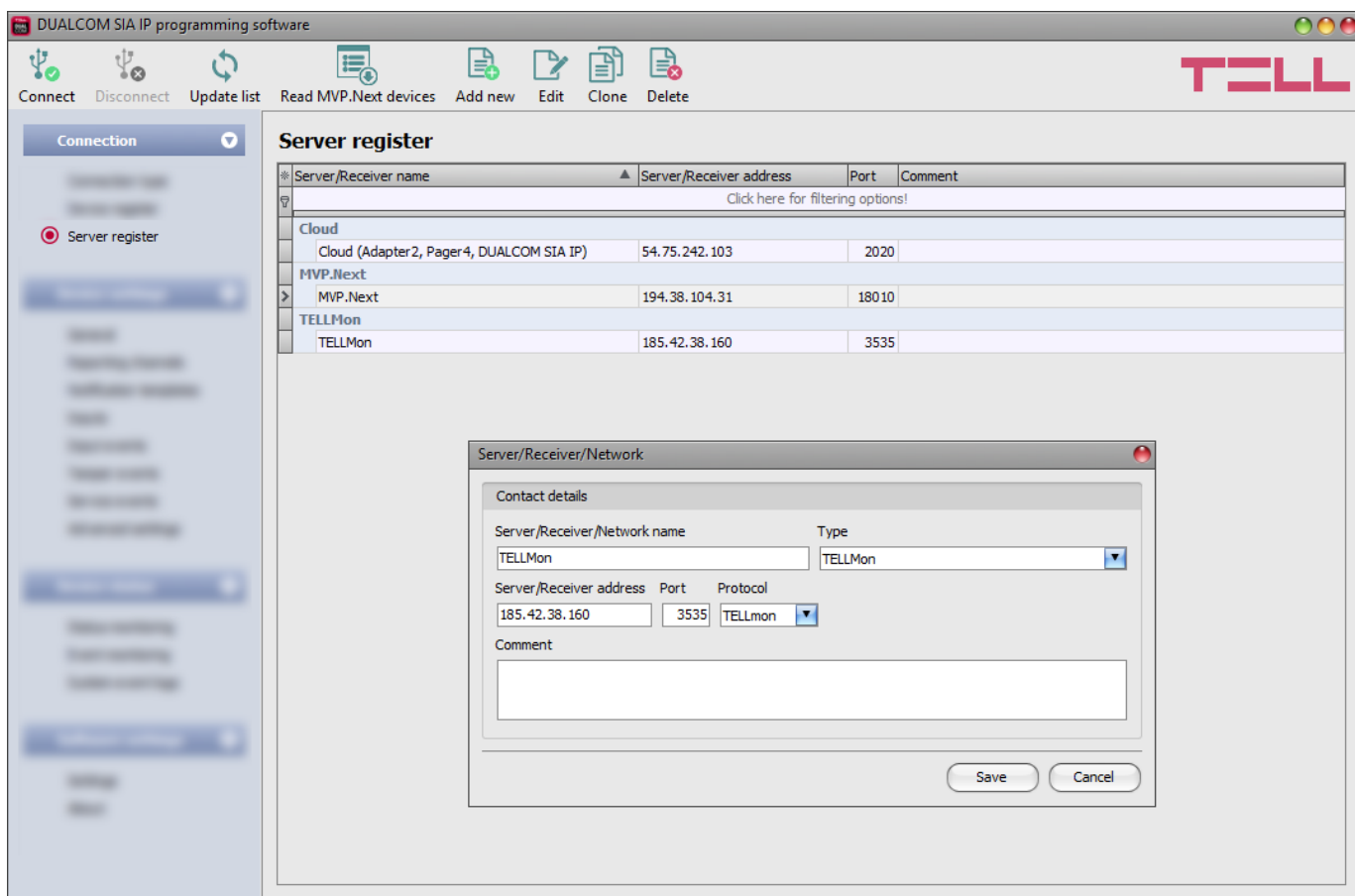
Device password/Confirm device password: the superadmin or admin password configured in the given device, depending on which one you want to use for connecting to the device.

SIM identifier (ICCID SIM A/B): the identifiers of the SIM cards installed in the device. If the device is connected via USB, and the SIM cards are installed, the software will read the ICCIDs automatically from the device and will insert the data in these fields when you add a record with new device contact details. If automated reading fails, you can enter the IDs manually, or copy from the “**Status monitoring**” menu. The ICCIDs have no specific function, their purpose is informational.

Device phone number (SIM A/B): in these fields you can enter the phone numbers of the SIM cards installed in the device. They have no specific function, their purpose is informational.

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

8.1.4 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 them with your devices in the “**Device register**” menu, when recording the contact details of your devices. You can add new server or receiver contact details to the database, and also edit, delete, and clone entries for easy adding of servers or receivers with similar contact details.

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

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



: update the records from database



: read devices from MVP.next server



: add new server, receiver or network



: clone entry (duplicate)



: edit entry



: delete entry

Data stored in the server register:

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

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

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

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

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

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

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

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

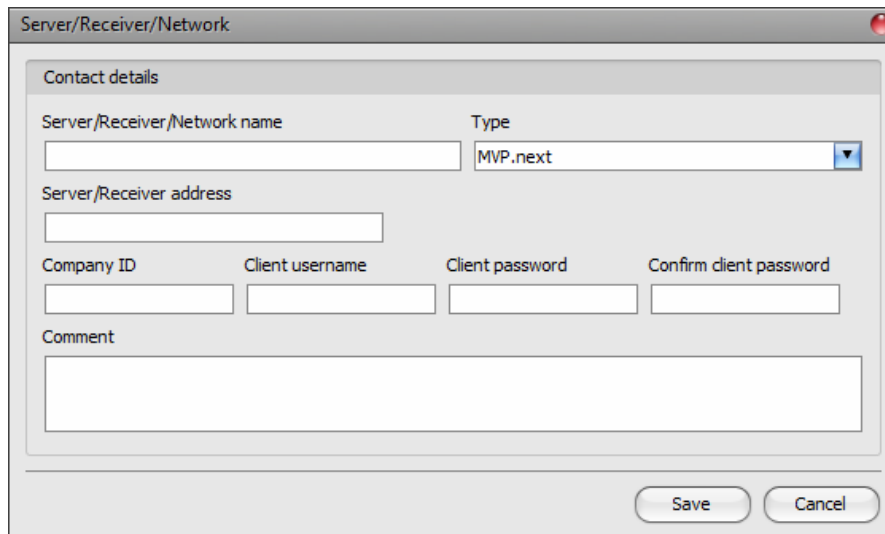
Comment: in this field you can enter custom comments related to the given server, receiver, or network.

Remote access of devices via the MVP.next server:


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

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

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









The screenshot shows a dialog box titled "Server/Receiver/Network". It has a "Contact details" section with the following fields: "Server/Receiver/Network name" (text input), "Type" (dropdown menu showing "MVP.next"), "Server/Receiver address" (text input), "Company ID" (text input), "Client username" (text input), "Client password" (text input), and "Confirm client password" (text input). Below these is a "Comment" text area. At the bottom right, there are "Save" and "Cancel" buttons.

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

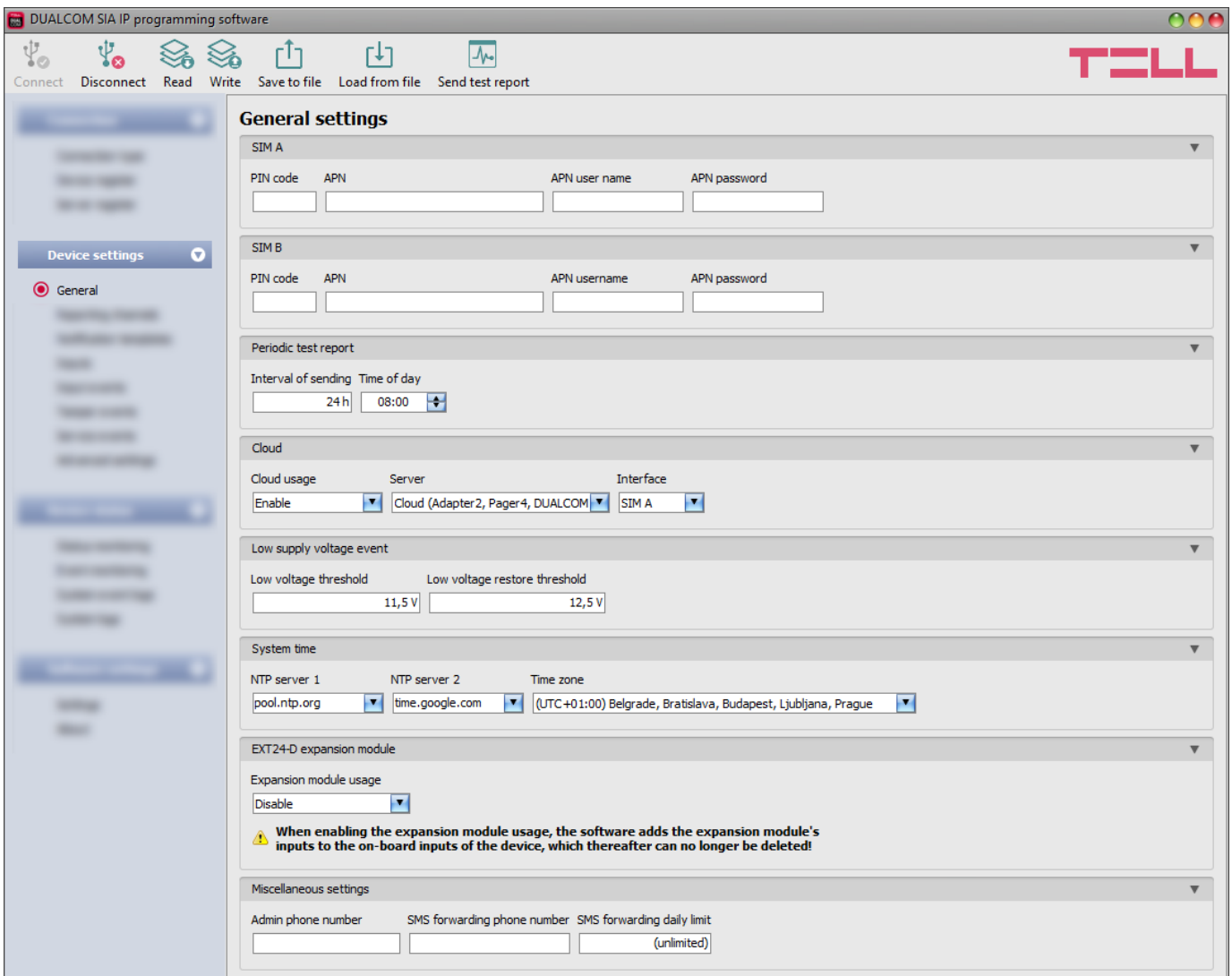
Attention! You can use the registered client username and password in any other programming software that supports the MVP.next, but you can connect to the server with one software only at the same time, using the same username. If you want to use more than one programming software simultaneously, you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

8.2 Device settings menu

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

- **Changing the device settings:** To change the device settings, first you must read the actual settings from the device by clicking on the “**Read**”  button in any submenu in the “**Device settings**” menu. Writing the settings into the device using the “**Write**”  button is not possible until the settings are read. After making changes in the settings, write the settings into the device by clicking on the “**Write**”  button.
- **Overwriting the device settings:** If you want to completely overwrite the settings, you can import and write data from a previously made system backup. To create a system backup file, configure the desired settings in the submenus, and then click on the “**Save to file**”  button in the “**General**” device settings menu. You can import the saved backup into the program using the “**Load from file**”  button, and then write imported settings into the device by clicking on the “**Write**”  button. This is useful when you want to configure many devices with the same settings.

8.2.1 General



The screenshot displays the 'General settings' window in the DUALCOM SIA IP programming software. The interface includes a top toolbar with icons for Connect, Disconnect, Read, Write, Save to file, Load from file, and Send test report. The 'General settings' panel is divided into several sections:

- SIM A:** Fields for PIN code, APN, APN user name, and APN password.
- SIM B:** Fields for PIN code, APN, APN username, and APN password.
- Periodic test report:** Fields for Interval of sending (24 h) and Time of day (08:00).
- Cloud:** Cloud usage (Enable), Server (Cloud (Adapter2, Pager4, DUALCOM)), and Interface (SIM A).
- Low supply voltage event:** Low voltage threshold (11,5 V) and Low voltage restore threshold (12,5 V).
- System time:** NTP server 1 (pool.ntp.org), NTP server 2 (time.google.com), and Time zone ((UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague).
- EXT24-D expansion module:** Expansion module usage (Disable). A warning message states: "When enabling the expansion module usage, the software adds the expansion module's inputs to the on-board inputs of the device, which thereafter can no longer be deleted".
- Miscellaneous settings:** Admin phone number, SMS forwarding phone number, and SMS forwarding daily limit (unlimited).

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

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read**” button. This will read all settings in all menus.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the “**Write**” button. This will write the changes only, but all changes made in any menu.

- Saving settings to file:



To save all device settings to file, click on the “**Save to file**” button.

- Loading settings from file:



To load saved settings from file, click on the “**Load from file**” button.

- Send test report:



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

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

SIM A: settings of the SIM card marked with “**A**”, found on the right-hand side of the board.

SIM B: settings of the SIM card marked with “**B**”, found on the left-hand side of the board.

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

APN: the access point name necessary to connect to the Internet. Ask this from the mobile service provider of the SIM card installed in the device. If no APN is configured, the device will not be able to connect to the Internet, and thereby it cannot operate.

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

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

Periodic test report:

Interval of sending (1 to 24h): the interval of periodic test report sending. When the 24h value is selected, you can also configure the time of day for periodic test report sending.

Time of day (hh:mm): the time of day for periodic test report sending (only for the 24h interval!).

In order to generate and report periodic test report events, the “**Periodic test report**” service event should be configured in the “**Service events**” menu.

Cloud:

Cloud usage: if this option is enabled, the device will connect to the cloud server operated by the manufacturer and will stay connected permanently. To ensure a continuous connection and availability, the device sends supervision messages that use about **12 MB data per month** on its own. Using the cloud server, special services become available, such as remote programming, control and monitoring of your device over the cloud. This is useful when you are using the device with the SIA DC-09 protocol, which does not support remote access, or when it is not possible to access the device for the moment via the CMS server or receiver (e.g. if the server or receiver is down due to a network or other error, or the settings in the device are wrong). If this option is enabled, the device will always be online and thereby accessible remotely anytime. If this option is disabled, you can still initiate a temporary cloud connection manually, by sending a command via SMS to the phone number of the device. You can read more about this in the [“Remote connecting to devices via cloud service”](#) paragraph. In case of using a SIM card that uses a private APN, the given private APN should be opened at the mobile service provider to access the cloud server IP address at 54.75.242.103, port: 2020.

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

Interface: in this section you can select the SIM card which the device will use for the cloud service. The selected SIM card will bear the data usage arising from cloud usage.

Low supply voltage event:

Low voltage threshold: the device has built-in supply voltage monitoring function. In this section you can configure the threshold from 10V to 30V, at which the device will generate the **“Low supply voltage”** event. The event will be generated if the supply voltage is continuously at, or below the configured level for at least 30 seconds.

Low voltage restore threshold: In this section you can configure the threshold from 10 to 30V, at which the device will generate the **“Low supply voltage”** restore event. The event will be generated if the supply voltage is continuously at, or above the set level for at least 30 seconds after a **“Low supply voltage”** event.

In order to generate and report low supply voltage and voltage restore events, the **“Low supply voltage”** new and restore service events should be configured in the **“Service events”** menu.

System time:

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

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

EXT24-D expansion module:

Expansion module usage: using the **EXT24-D** expansion module, you can expand the 6 onboard inputs of the **DUALCOM** device with further 24 inputs. Enable this option if you connect the expansion module to the device. When you enable this option, the program will add the inputs of the expansion module to the inputs of the device in the settings.

Attention! After enabling this option, it is no longer possible to remove the expansion module inputs from the settings!

Miscellaneous settings:

Admin phone number: it is possible to configure the device by sending commands in SMS to the phone number of the device. The device accepts SMS commands only from the Superuser phone number. You can enter the superuser phone number here, or can register it by SMS. You can find the list of the available SMS commands in chapter "[Configuring by SMS commands](#)".

SMS forwarding phone number: the device forwards the messages received by its SIM cards to the phone number configured in this section. The received messages are deleted automatically after forwarding. If no phone number is configured, the device deletes all incoming messages without forwarding.

SMS forwarding daily limit: with this setting you can limit the number of SMS messages to be forwarded per day. When the configured limit is reached, the device will not forward new incoming SMS messages for 24 hours. After 24 hours the message counter resets automatically, and incoming messages will be forwarded again up to the configured limit. The SMS forwarding daily limit can be disabled and set to unlimited by deleting the entered value.

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

8.2.2 Reporting channels

The screenshot shows the 'Reporting channels' configuration window in the DUALCOM SIA IP programming software. The window has a title bar with 'DUALCOM SIA IP programming software' and a 'TELL' logo. Below the title bar are four buttons: 'Connect', 'Disconnect', 'Read', and 'Write'. The main area is titled 'Reporting channels' and contains two sections for 'CID reporting to CMS over IP'.

CID reporting to CMS over IP - SIM A interface

Name	IP address	Port	Protocol	User account ID	Supervision message	Supervision message interval	Time zone
1A		3535	TELLMON	0000	Enable	90 s	UTC

IP1A
Network protocol: TCP

Name	IP address	Port	Protocol	SIA account prefix	User account ID	Supervision message	Supervision message interval	Time zone
2A		9999	SIA IP		0000	Enable	90 s	Local

IP2A
Network protocol: TCP
AES key:
 Send each message in a new session

CID reporting to CMS over IP - SIM B interface

Name	IP address	Port	Protocol	User account ID	Supervision message	Supervision message interval	Time zone
1B		3535	TELLMON	0000	Enable	90 s	UTC

IP1B
Network protocol: TCP

Name	IP address	Port	Protocol	SIA account prefix	User account ID	Supervision message	Supervision message interval	Time zone
2B		9999	SIA IP		0000	Enable	90 s	Local

IP2B
Network protocol: TCP
AES key:
 Send each message in a new session

In this section, you can configure the server/receiver availabilities for reporting to CMS.

Attention! For higher security, when using the device with a fire alarm system, it is mandatory to configure the IP addresses in pairs, which means that **IP1A** shall be configured along with **IP1B**, and **IP2A** with **IP2B**, and vice versa!

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read**” button. This will read all settings in all menus.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the “**Write**” button. This will write the changes only, but all changes made in any menu.

Please note that the settings must be written in the device to be applied after a change

is made. For this, click on the “Write”  **button.**

CID reporting to CMS over IP:

You can configure up to 4 CMS servers or receivers, 2 IP addresses for each modem (interface SIM A and SIMB) with the following parameters:

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

IP address: CMS server or receiver IP address. The system works with static IP address only! The device does not support domain name usage, because it happens that domain resolution does not work due to the instability of the service. This could lead to delays in reporting or even to reporting failure, which is not acceptable on reporting of fire alarm events. 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 arrange with the mobile service provider to open the given private APN for accessing the given server/receiver IP address.

Port: CMS server or receiver communication port number.

Default port numbers:

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

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

Available protocols:

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

SIA account prefix: in case of using the **SIA IP** (DC-09) protocol, you can configure a prefix of up to 2 hexadecimal characters, which the device will add in front of the 4-character user account ID in supervision messages. Thereby, supervision messages will be sent towards CMS servers or receivers with an up to 6-character long identifier. The following characters can be used: 0..9, A, B, C, D, E, F.

User account ID: the user account ID necessary for Contact ID reporting to CMS. The events and the supervision messages too, are sent to the configured servers or receivers using the user account ID configured in this section. In case of using the **SIA IP** protocol, the **SIA account prefix** will be added in front of the user account ID. The user account ID length is 4 hexadecimal characters, and the following characters can be used: 0..9, A, B, C, D, E, F.

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.

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

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

Attention! The lower the value, the higher the data usage!

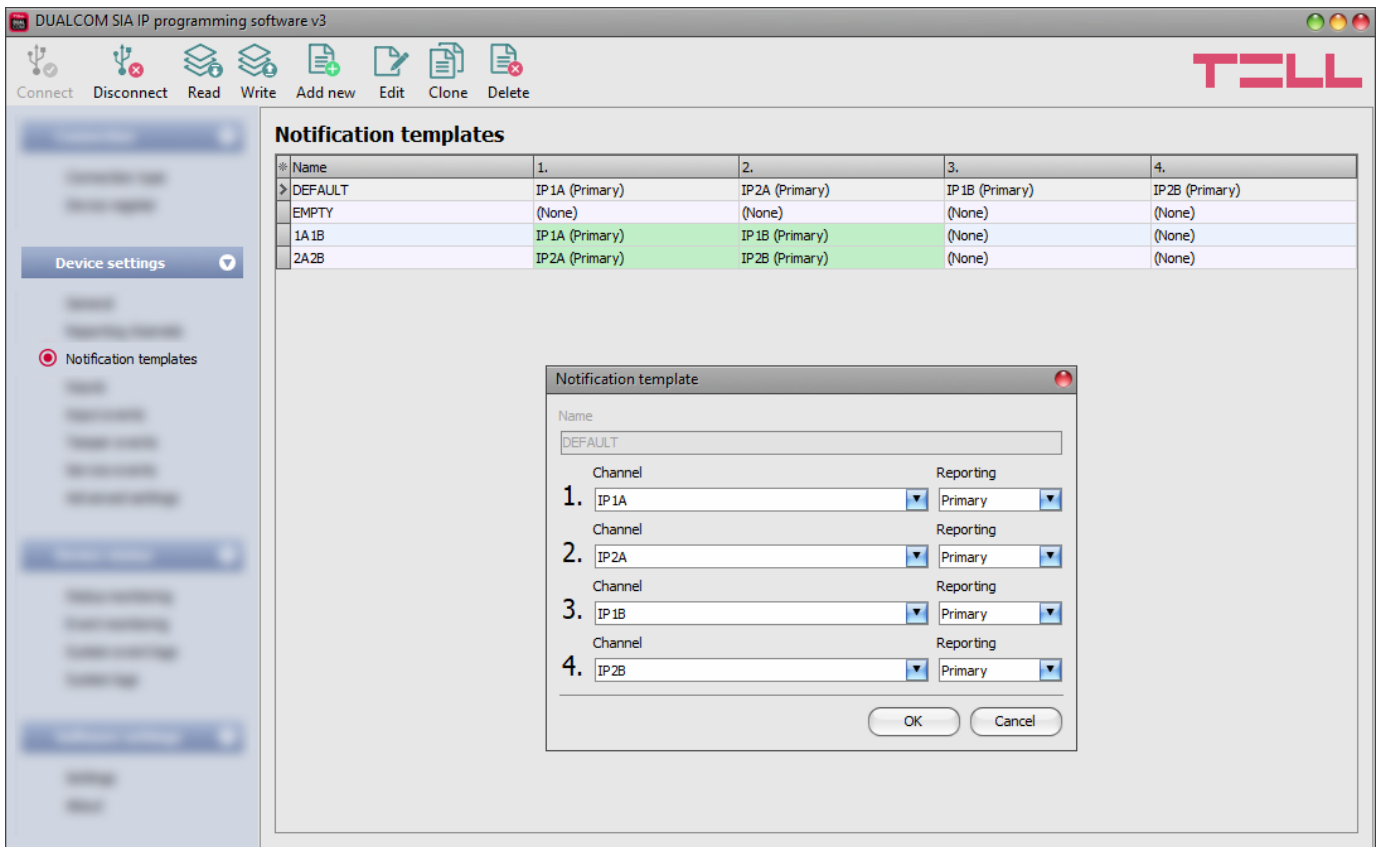
Time zone: in this section you can select whether the given server or receiver sends the timestamp used for synchronizing the system time in **UTC** or **local time**. It is important to select the appropriate option for each server and receiver, since if the system time is set incorrectly, events will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

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

AES key: the custom AES encryption key can be used for the **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, for the **SIA IP** protocol it can be enabled to send each message in a new TCP session. In case of using UDP, the device will open a new port for each message, if this option is enabled.

8.2.3 Notification templates



In this menu you can configure different templates according to which the device will send reports to CMS servers and receivers. For quick and easy setup, the device contains 4 built-in templates, named as “**EMPTY**” and “**DEFAULT**”, “**1A1B**” and “**2A2B**”, which cannot be deleted, but their configuration can be changed if needed.

The device will report the events associated with the “**DEFAULT**” notification template to all configured receivers (IP addresses **1A**, **1B**, **2A** and **2B**).

By associating the “**1A1B**” or the “**2A2B**” with events, you can configure which pair of receivers (IP addresses **1A+1B** or **2A+2B**) should the given events be reported to, via the two separate modems (**A** and **B**). With this, you can separate e.g. alarm events and technical events (reporting alarm events to the alarm monitoring station only, and technical events to the technical monitoring station only) – as described in chapter “[General logic of reporting for fire alarm systems](#)”.







If you wish to add new notification templates, this should be done prior to configuring events. Any template can be assigned to any event, thus reports can be directed to the desired servers and receivers, with the desired priorities. Servers/receivers are classified into two groups, primary and backup. When an event occurs, the given report will be sent to all servers and receivers configured as primary in the notification template associated with the given event. In case that none of the primary servers/receivers are available, the device will try to report to the servers/receivers configured as backup.

The order of reporting to servers and receivers configured as backup in a template corresponds to the numbering (1 to 6) of the channels in the template.

The priority depends on the classification of the configured servers/receivers (primary or backup). Primary servers/receivers will be notified first. Reports will be sent to all primary servers/receivers, while backup servers/receivers will only be notified if reporting to all primary ones fail. In this case, the device will try to report to the first highest priority backup server/receiver, and then, if this fails, to the second one, and so on. Additionally, if a reporting channel fails, the devices will keep sending supervision messages to the given server/receiver by the configured supervision sending interval to check its availability, and will send the report as soon as it becomes available. The device will no longer try to report events for which reporting failed for more than 10 minutes.



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

Available options:

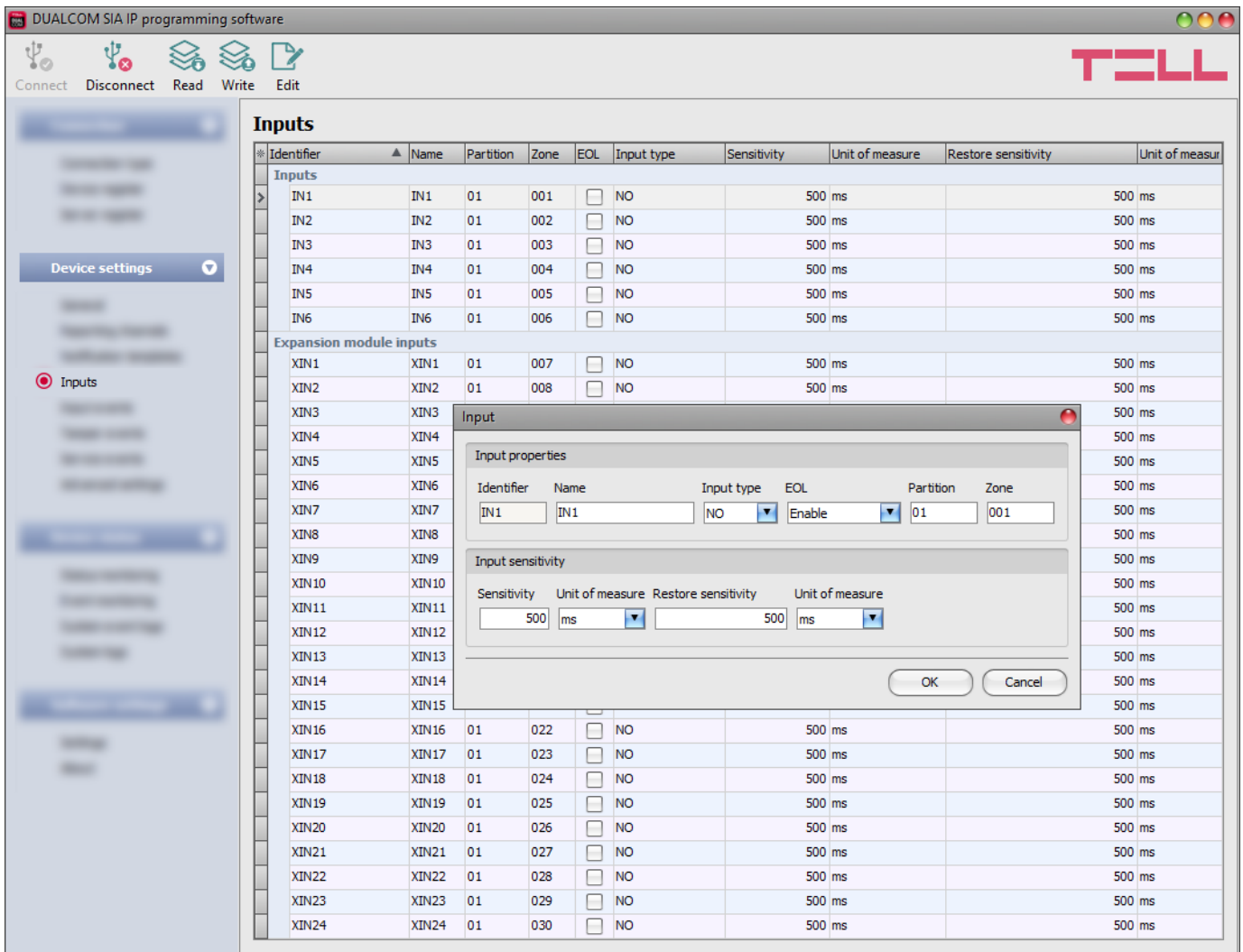
- Reading the settings from the device:
 To read the settings from the device click on the “**Read**” button. This will read all settings in all menus.
- Writing the settings into the device:
 After changing the settings or entering new settings, to take effect, it is necessary to write the new settings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

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

Creating a new notification template:

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

8.2.4 Inputs






The screenshot shows the 'Inputs' configuration window in the DUALCOM SIA IP programming software. The window title is 'DUALCOM SIA IP programming software' and it features the TELL logo in the top right corner. The interface includes a toolbar with 'Connect', 'Disconnect', 'Read', 'Write', and 'Edit' buttons. A sidebar on the left shows 'Device settings' and 'Inputs' selected. The main area contains a table of inputs:

Identifier	Name	Partition	Zone	EOL	Input type	Sensitivity	Unit of measure	Restore sensitivity	Unit of measur
Inputs									
IN1	IN1	01	001	<input type="checkbox"/>	NO	500 ms			500 ms
IN2	IN2	01	002	<input type="checkbox"/>	NO	500 ms			500 ms
IN3	IN3	01	003	<input type="checkbox"/>	NO	500 ms			500 ms
IN4	IN4	01	004	<input type="checkbox"/>	NO	500 ms			500 ms
IN5	IN5	01	005	<input type="checkbox"/>	NO	500 ms			500 ms
IN6	IN6	01	006	<input type="checkbox"/>	NO	500 ms			500 ms
Expansion module inputs									
XIN1	XIN1	01	007	<input type="checkbox"/>	NO	500 ms			500 ms
XIN2	XIN2	01	008	<input type="checkbox"/>	NO	500 ms			500 ms
XIN3	XIN3					500 ms			500 ms
XIN4	XIN4					500 ms			500 ms
XIN5	XIN5					500 ms			500 ms
XIN6	XIN6					500 ms			500 ms
XIN7	XIN7					500 ms			500 ms
XIN8	XIN8					500 ms			500 ms
XIN9	XIN9					500 ms			500 ms
XIN10	XIN10					500 ms			500 ms
XIN11	XIN11					500 ms			500 ms
XIN12	XIN12					500 ms			500 ms
XIN13	XIN13					500 ms			500 ms
XIN14	XIN14					500 ms			500 ms
XIN15	XIN15					500 ms			500 ms
XIN16	XIN16	01	022	<input type="checkbox"/>	NO	500 ms			500 ms
XIN17	XIN17	01	023	<input type="checkbox"/>	NO	500 ms			500 ms
XIN18	XIN18	01	024	<input type="checkbox"/>	NO	500 ms			500 ms
XIN19	XIN19	01	025	<input type="checkbox"/>	NO	500 ms			500 ms
XIN20	XIN20	01	026	<input type="checkbox"/>	NO	500 ms			500 ms
XIN21	XIN21	01	027	<input type="checkbox"/>	NO	500 ms			500 ms
XIN22	XIN22	01	028	<input type="checkbox"/>	NO	500 ms			500 ms
XIN23	XIN23	01	029	<input type="checkbox"/>	NO	500 ms			500 ms
XIN24	XIN24	01	030	<input type="checkbox"/>	NO	500 ms			500 ms

An 'Input' dialog box is open, showing configuration options for a selected input (IN1). The dialog has two sections: 'Input properties' and 'Input sensitivity'. In the 'Input properties' section, the Identifier is 'IN1', Name is 'IN1', Input type is 'NO', EOL is 'Enable', Partition is '01', and Zone is '001'. In the 'Input sensitivity' section, Sensitivity is '500', Unit of measure is 'ms', Restore sensitivity is '500', and Unit of measure is 'ms'. The dialog has 'OK' and 'Cancel' buttons.

In this menu you can configure the properties and options of the dry contact inputs. If you want to use the **EXT24-D** expansion module, enable the “**Expansion module usage**” option in the “**General**” device settings menu, to display the expansion module’s inputs too.

Available options:

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

Please note that the settings must be written in the device 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 for identification of the inputs in the program.

Name: you can add a custom name to events, according to their use. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " '.

Input type: the input can be normally open (**NO**), or normally closed (**NC**).

When set to **NO**, an input event will be generated when the open contact between the given input (**IN1...IN6**) and the **COM** terminal placed next to the input becomes closed.

When set to **NC**, an input event will be generated when the closed contact between the given input (**IN1...IN6**) and the **COM** terminal placed next to the input becomes open.

EOL: if enabled, tamper protection function is automatically activated for the given input. In this case, the given input must be provided with a **1k Ω** end-of-line resistor at the end of the loop, directly at the controlling contact (see wiring diagram).

Partition: in this section you can configure the partition number you wish to assign to the given event. The default configuration for partition is 01.

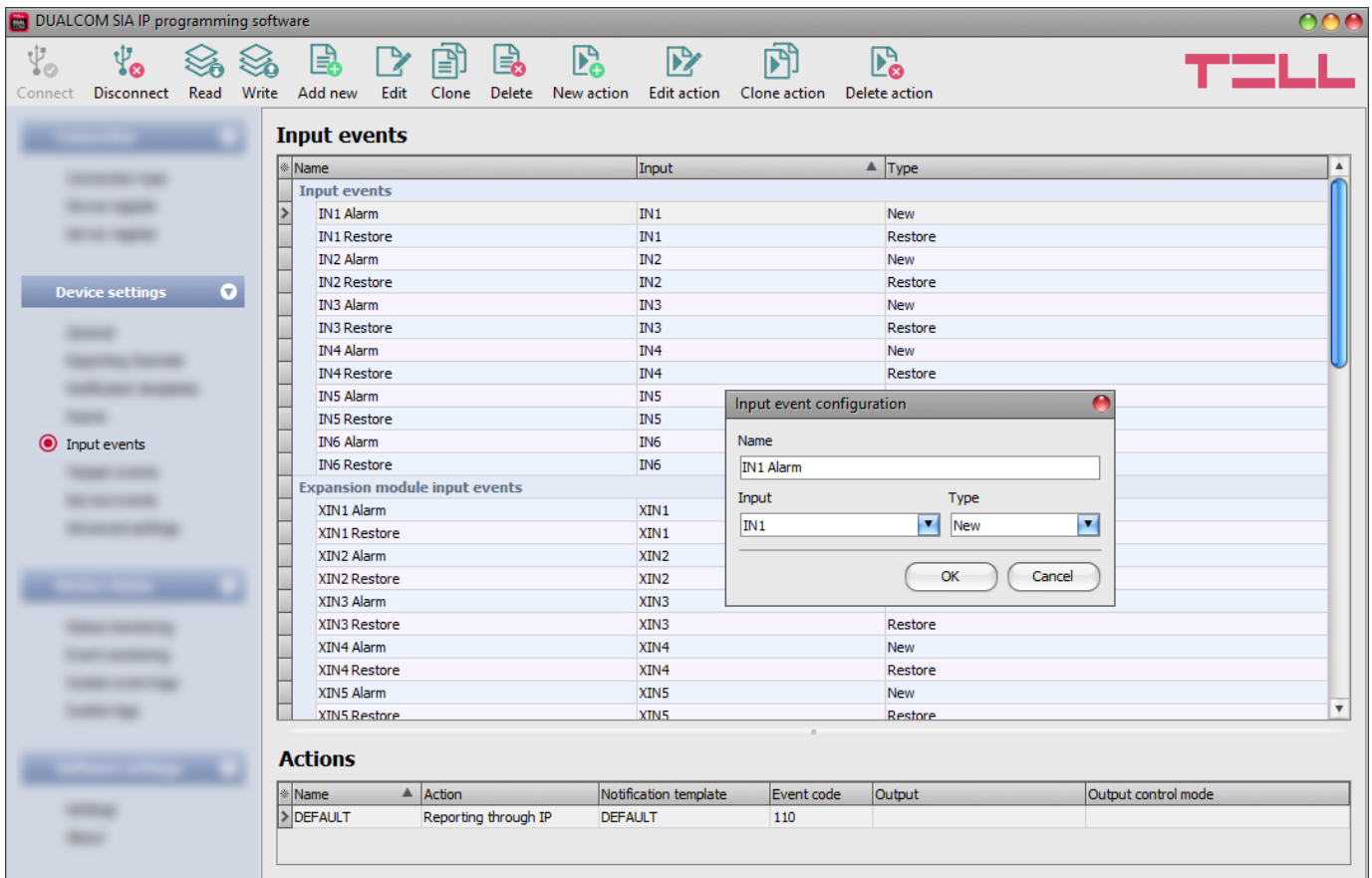
Zone: in this section you can configure the zone number you wish to assign to the given event. The default configuration for zones is in accordance with the number of the inputs (001 to 006).

Input sensitivity:

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

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

8.2.5 Input events



In this menu you can configure the input events generated by the contact inputs. You can add one new and one restore event for each input. If you want to use the **EXT24-D** expansion module, enable the “**Expansion module usage**” option in the “**General**” device settings menu, to display the expansion module’s input events too.

A reporting action should be associated with input events for reporting to CMS, and an output control action, for controlling outputs by events.

When you connect to a new **DUALCOM** device, which has not been configured yet, all input events will be shown in this menu after reading the settings from the device. A CMS reporting action is associated by default with each event, with the default Contact ID event code, with the zone number that corresponds to the number of the given input, and with the “**DEFAULT**” notification template, based on which the event will be reported to all configured receivers.

You can associate one reporting action, and any number of output control actions with each input event.

The events are shown in the “**Input events**” window, while actions associated with the selected event are shown in the “**Actions**” window.

If needed, you can delete the unused input events, or add missing/deleted events as new. If there is no input event added and configured for an input, state changes on the given input will not generate input events and will not send reports.

Available options:

- Reading the settings from the device:



To read the settings from the device click on the “**Read**” button. This will read all settings in all menus.

- Writing the settings into the device:



After changing the settings or entering new settings, to take effect, it is necessary to write the new settings into the device by clicking on the “**Write**” button. This will write the changes only, but all changes made in any menu.

- Adding a new input event:



To add a new input event, click on the “**New**” button.

- Creating a copy of an existing input event:



To create a copy of the selected input event, click on the “**Clone**” button. Please note that the new copy should have a different unique name.

- Editing input event settings:



To edit the settings of the selected input event, click on the “**Edit**” button.

- Deleting an input event:



To delete the selected input event, click on the “**Delete**” button.

- Adding a new action:



To add a new action, click on the “**New action**” button.

- Creating a copy of an existing action:



To create a copy of the selected action, click on the “**Clone action**” button. Please note that the new copy should have a different unique name.

- Editing action settings:



To edit the settings of the selected action, click on the “**Edit action**” button.

- Deleting an action:



To delete the selected action, click on the “**Delete action**” button.

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

Input event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 40 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .

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

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

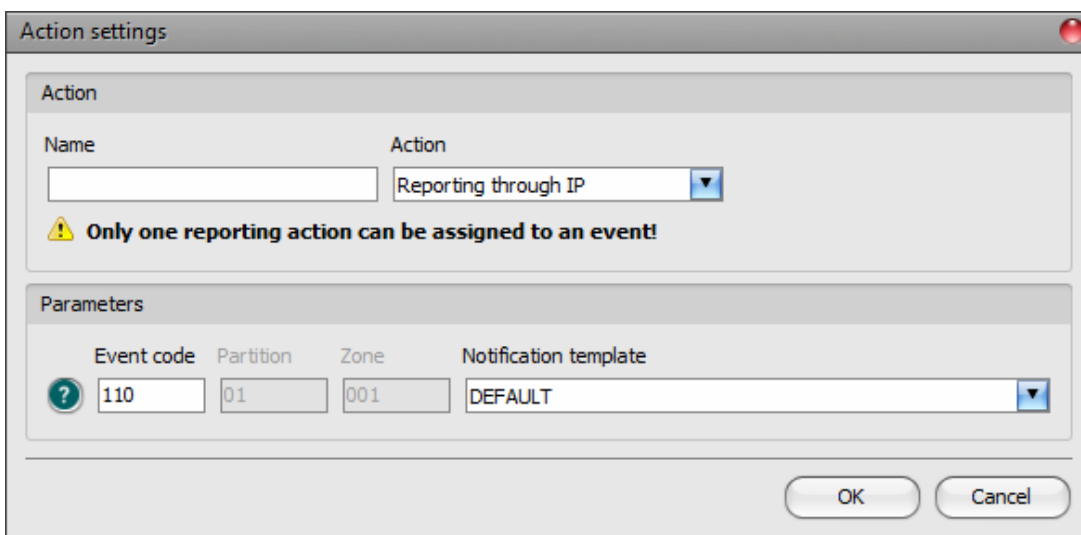
Action settings:

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

Action: you can select the action to be performed from the drop-down menu.


Available actions:

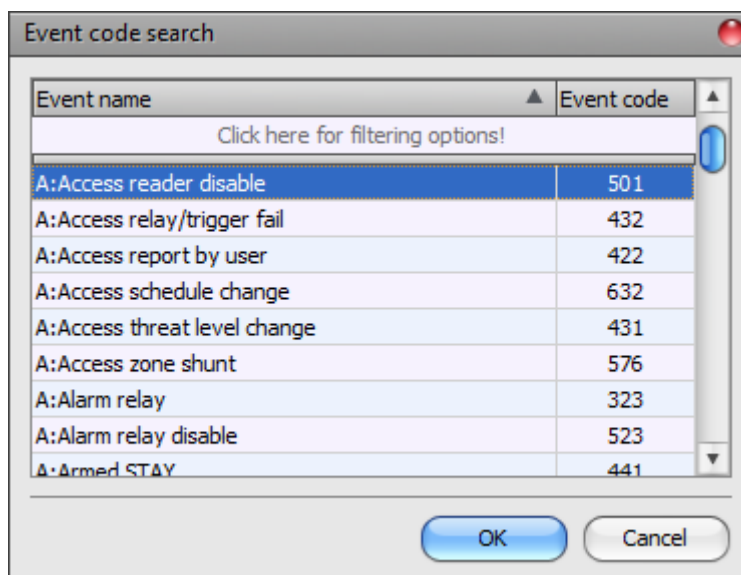
- **Reporting through IP:** this type of action will send a report to CMS with the configured event code, according to the associated notification template, when the given event occurs. Only one reporting action can be assigned to an event.



Parameters:

Event code: in this section you can configure the 3-digit Contact ID event code, which you want to assign to the given event (e.g. 110 = fire alarm). The event code consists of hexadecimal characters (0...9,A,B,C,D,E,F). You can configure the partition and zone number in the input settings.

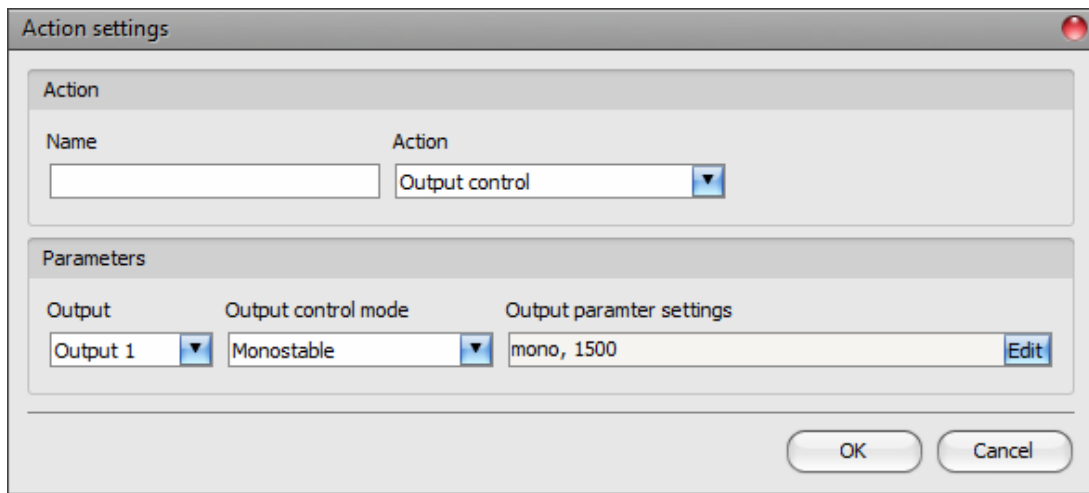
The software includes a built-in event code search tool which contains the list of standard Contact ID codes. The search tool opens by clicking on the  icon with the question mark symbol placed in front of the event code input field.



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

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events.

- **Output control:** this type of action will perform an output control according to the configured parameters when the given event occurs. You can add any number of output control action to an event.



The screenshot shows a dialog box titled "Action settings". It is divided into two main sections: "Action" and "Parameters".

- Action section:** Contains a "Name" field with the text "Action" and a dropdown menu currently showing "Output control".
- Parameters section:** Contains three sub-sections:
 - Output:** A dropdown menu showing "Output 1".
 - Output control mode:** A dropdown menu showing "Monostable".
 - Output parameter settings:** A text field containing "mono, 1500" and an "Edit" button.

At the bottom right of the dialog box, there are two buttons: "OK" and "Cancel".

Parameters:



Output: in this section you can select the output to be controlled when the given input event occurs.

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




- **Monostable:** the output will be activated for the time configured in the “**Duration**” section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 60 minutes.
- **Bistable ON:** the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF:** the output will become deactivated.
- **State change:** the output will change state (if deactivated, it will become activated, and if activated, it will become deactivated).
- **Pulse series:** the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes too.

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

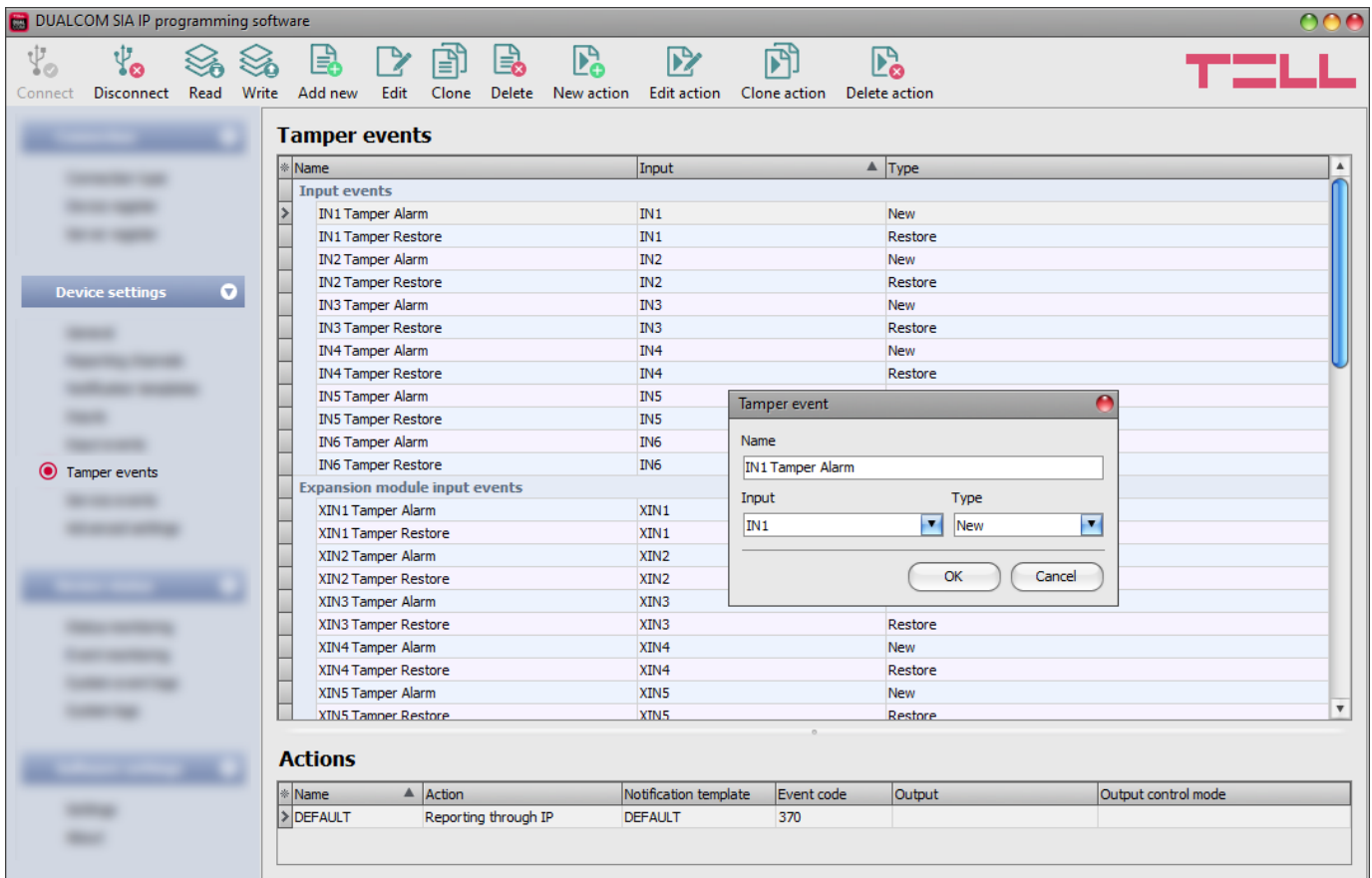
Adding a new action to an event:

- Select the input event, which you want to configure, by clicking on it in the “**Input events**” window.
- Click on the “**New action**”  button.
- Enter a name for the action. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .
- Select the action you want to add, using the “**Action**” drop-down menu.
- Configure the action in the “**Parameters**” section.
- Click on the “**OK**” button. The action will be added in the “**Actions**” window.
- Click on the “**Write**”  button.

Editing, cloning, or deleting an action:

- Select the input event for which you want to edit, clone, or delete an action, by clicking on it in the “**Input events**” window.
- Select the action, which you want to edit, clone, or delete, by clicking on it in the “**Actions**” window.
- Click on the “**Edit action**”  , “**Clone action**”  , or the “**Delete action**”  button.

8.2.6 Tamper events



In this menu you can configure the tamper events generated by the contact inputs.

Attention! Regardless of the settings configured in the "**Tamper events**" menu, the tamper protection function will only work, and a tamper event will only be generated on an input if the "**EOL**" option is enabled in the settings of the given input, and the end-of-line resistor has also been installed on that input.

A new and a restore tamper event belongs to each input.

If you want to use the **EXT24-D** expansion module, enable the "**Expansion module usage**" option in the "**General**" device settings menu, to display the expansion module's tamper events too.

A reporting action should be associated with tamper events for reporting to CMS, and an output control action, for controlling outputs by events.











When you connect to a new **DUALCOM** device, which has not been configured yet, all tamper events will be shown in this menu after reading the settings from the device. A CMS reporting action is associated by default with each event, with the default Contact ID event code, with the zone number that corresponds to the number of the given input, and with the "**DEFAULT**" notification template, based on which the event will be reported to all configured receivers.

You can associate one reporting action, and any number of output control actions with each tamper event.

The events are shown in the "**Tamper events**" window, while actions associated with the selected event are shown in the "**Actions**" window.

If needed, you can delete the unused tamper events, or add missing/deleted events as new. If there is no tamper event added and configured for an input, tamper related state changes on the given input will not generate events and will not send reports.

Available options:

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

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

Tamper event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 40 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .

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

Type: the type of the event, which can be new or restore. New event will be generated when tamper occurs, and restore event will be generated when the tamper restores. In the Contact ID protocol, new events are indicated with 1 (or E), and event restorals are indicated with 3 (or R).

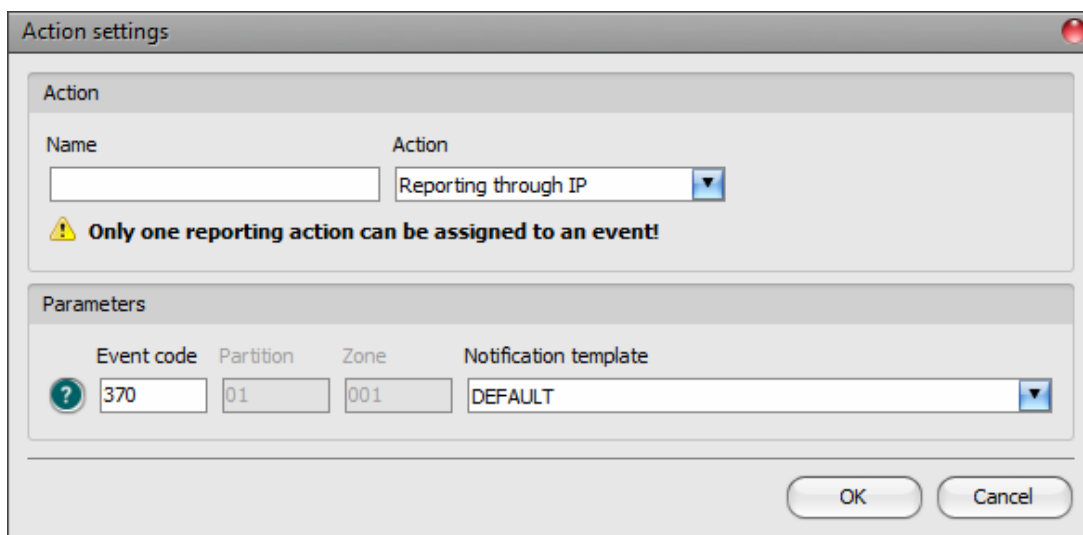
Action settings:

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

Action: you can select the action to be performed from the drop-down menu.


Available actions:

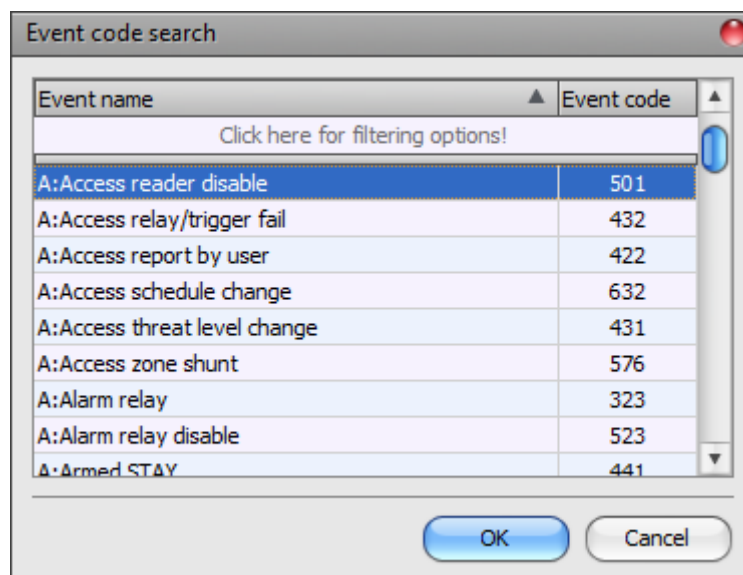
- **Reporting through IP:** this type of action will send a report to CMS with the configured event code, according to the associated notification template, when the given event occurs. Only one reporting action can be assigned to an event.



Parameters:

Event code: in this section you can configure the 3-digit Contact ID event code, which you want to assign to the given event (e.g. 370 = protection loop trouble). The event code consists of hexadecimal characters (0...9,A,B,C,D,E,F). You can configure the partition and zone number in the input settings.

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



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

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events.

- **Output control:** this type of action will perform an output control according to the configured parameters when the given event occurs. You can add any number of output control action to an event.

The screenshot shows a dialog box titled "Action settings". It is divided into two main sections: "Action" and "Parameters".

- Action section:** Contains a "Name" label and a text input field. To its right is a dropdown menu labeled "Action" with "Output control" selected.
- Parameters section:** Contains three fields:
 - "Output": A dropdown menu with "Output 1" selected.
 - "Output control mode": A dropdown menu with "Monostable" selected.
 - "Output parameter settings": A text input field containing "mono, 1500" and an "Edit" button to its right.

At the bottom right of the dialog are "OK" and "Cancel" buttons.

Parameters:

Output: in this section you can select the output to be controlled when the given input event occurs.



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

Available options:




- **Monostable:** the output will be activated for the time configured in the “**Duration**” section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 60 minutes.
- **Bistable ON:** the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF:** the output will become deactivated.
- **State change:** the output will change state (if deactivated, it will become activated, and if activated, it will become deactivated).
- **Pulse series:** the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes too.

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

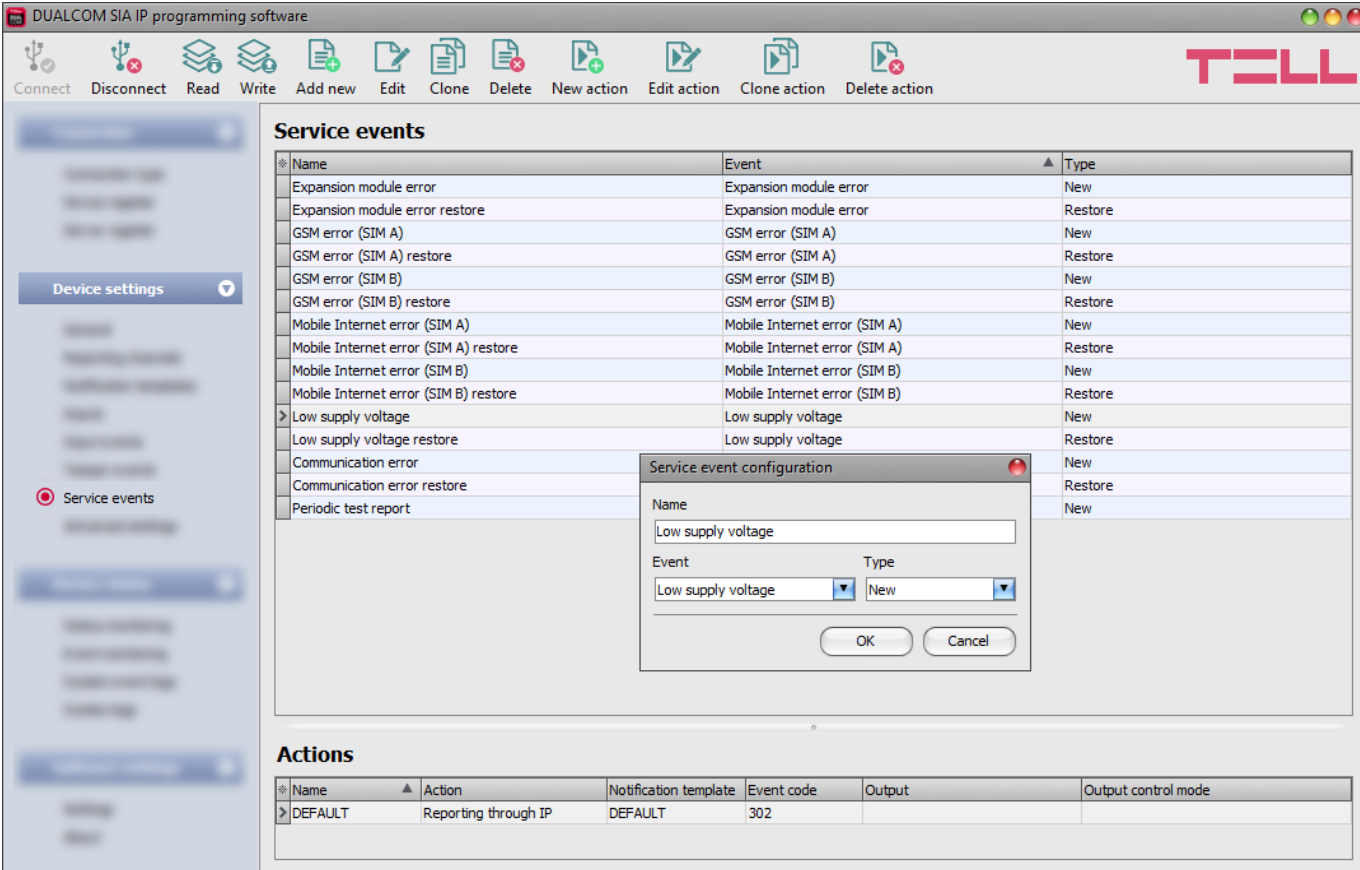
Adding a new action to an event:

- Select the tamper event, which you want to configure, by clicking on it in the “**Tamper events**” window.
- Click on the “**New action**”  button.
- Enter a name for the action. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .
- Select the action you want to add, using the “**Action**” drop-down menu.
- Configure the action in the “**Parameters**” section.
- Click on the “**OK**” button. The action will be added in the “**Actions**” window.
- Click on the “**Write**”  button.

Editing, cloning, or deleting an action:

- Select the tamper event for which you want to edit, clone, or delete an action, by clicking on it in the “**Input events**” window.
- Select the action, which you want to edit, clone, or delete, by clicking on it in the “**Actions**” window.
- Click on the “**Edit action**” , “**Clone action**” , or the “**Delete action**”  button.

8.2.7 Service events



The screenshot shows the DUALCOM SIA IP programming software interface. The main window displays a list of service events under the heading "Service events". A dialog box titled "Service event configuration" is open, allowing the user to configure a specific event. The dialog box has a "Name" field with the text "Low supply voltage", an "Event" dropdown menu set to "Low supply voltage", and a "Type" dropdown menu set to "New". There are "OK" and "Cancel" buttons at the bottom of the dialog box.

Name	Event	Type
Expansion module error	Expansion module error	New
Expansion module error restore	Expansion module error	Restore
GSM error (SIM A)	GSM error (SIM A)	New
GSM error (SIM A) restore	GSM error (SIM A)	Restore
GSM error (SIM B)	GSM error (SIM B)	New
GSM error (SIM B) restore	GSM error (SIM B)	Restore
Mobile Internet error (SIM A)	Mobile Internet error (SIM A)	New
Mobile Internet error (SIM A) restore	Mobile Internet error (SIM A)	Restore
Mobile Internet error (SIM B)	Mobile Internet error (SIM B)	New
Mobile Internet error (SIM B) restore	Mobile Internet error (SIM B)	Restore
Low supply voltage	Low supply voltage	New
Low supply voltage restore	Low supply voltage	Restore
Communication error		New
Communication error restore		Restore
Periodic test report		New

Name	Action	Notification template	Event code	Output	Output control mode
DEFAULT	Reporting through IP	DEFAULT	302		

In this menu you can configure the internal service events generated by the device.

A new and a restore event belongs to each service event, except for the periodic test report, which has a fixed type.

A reporting action should be associated with service events for reporting to CMS, and an output control action, for controlling outputs by events.











When you connect to a new **DUALCOM** device, which has not been configured yet, all service events will be shown in this menu after reading the settings from the device. A CMS reporting action is associated by default with each event, with the default Contact ID event code, and with the “**DEFAULT**” notification template, based on which the event will be reported to all configured receivers.

You can associate one reporting action, and any number of output control actions with each service event.

The events are shown in the “**Service events**” window, while actions associated with the selected event are shown in the “**Actions**” window.

If needed, you can delete the unused service events, or add missing/deleted events as new. If a service event is not added and configured, the device will not generate the given event, and will not send reports on that event.

Available options:

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

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

Service event:

Name: custom name of the event. The name entered in this section is used for identification of the given event within the program and in the event logs. The name should not be longer than 40 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .

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

Available service events:

- **Communication error:** this type of event is generated if the device cannot connect to the receivers through any of the configured channels for 100 seconds. A restore event is generated when the connection restores on at least one channel. This event is used to locally indicate the communication error through a relay output.
- **Expansion module error:** this type of event is generated when there is a connection loss between the device and the **EXT24-D** expansion module. A restore event is generated when the connection restores.
- **GSM error (SIM A / SIM B):** this type of event is generated if the device loses the connection with the GSM network, or it is unable to register on the GSM network for at least 60 seconds. A restore event is generated upon successful registration on the GSM network. The device generates a separate error event for each interface (SIM A and SIM B). Most common reasons for this type of error are the following: there is no SIM card installed in the device, or the card is not installed properly, the card is damaged, or the service is not available on the SIM card, low GSM signal, the GSM antenna is not connected, insufficient supply voltage/current.
- **Mobile Internet error (SIM A / SIM B):** this type of event is generated if the device is unable to establish the Internet connection for at least 60 seconds. A restore event is generated when the Internet connection restores. Most common reasons for this type of error are the following: wrong APN configured, or the mobile Internet service is not enabled on the SIM card.
- **Low supply voltage:** the device has built-in supply voltage monitoring function. Low supply voltage event is generated if the supply voltage drops below the configured low supply voltage threshold for at least 30 seconds. Low supply voltage restore event is generated when the supply voltage returns above the configured low supply voltage restore threshold for at least 5 seconds, after a "**Low supply voltage**" event. You can configure the threshold values in the "**General**" settings menu.
- **Periodic test report:** this type of event is generated according to the periodic test report settings configured in the "**General**" device settings menu.

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

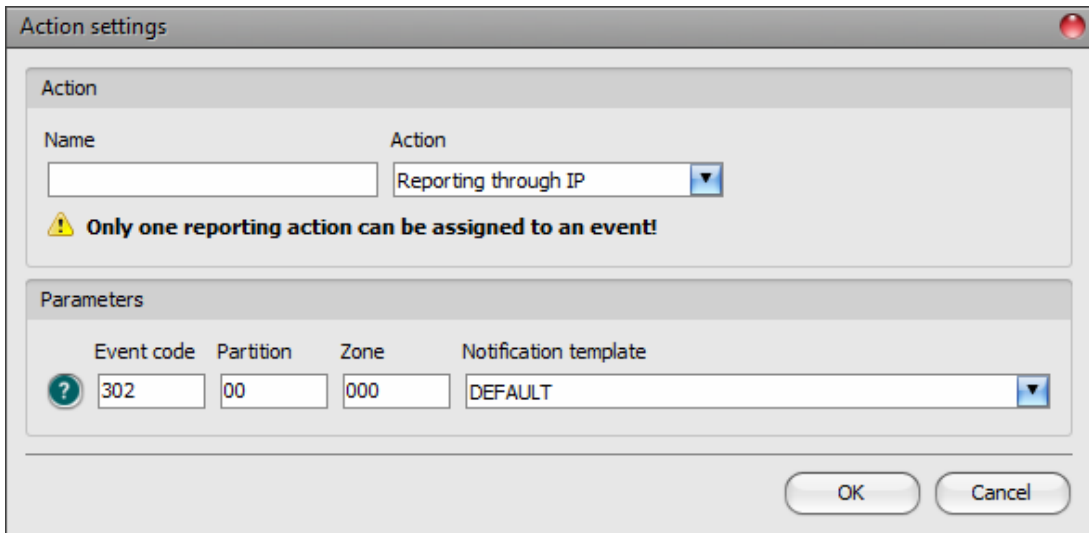
Action settings:

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

Action: you can select the action to be performed from the drop-down menu.


Available actions:

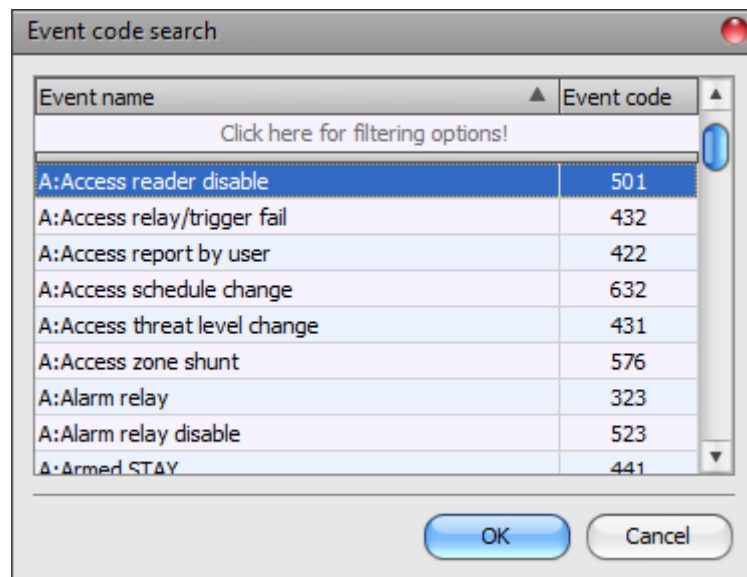
- **Reporting through IP:** this type of action will send a report to CMS with the configured event code, according to the associated notification template, when the given event occurs. Only one reporting action can be assigned to an event.



Parameters:

Event code: in this section you can configure the 3-digit Contact ID event code, which you want to assign to the given event (e.g. 302 = low system battery). The event code consists of hexadecimal characters (0...9,A,B,C,D,E,F). You can configure the partition and zone number in the input settings.

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



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

Partition: in this section you can configure the partition number that you want to assign to the given event. The default configuration for the partition number of service events is 00.

Zone: in this section you can configure the zone number that you want to assign to the given event. The default configuration for the zone number of service events is 000.

Notification template: in this section you can select a preconfigured notification template which you want to use for the given event. If you want to use additional notification templates, these should be added prior to configuring the events.

- **Output control:** this type of action will perform an output control according to the configured parameters, when the given event occurs. You can add any number of output control action to an event.

The screenshot shows a dialog box titled "Action settings". It is divided into two main sections: "Action" and "Parameters".
In the "Action" section, there is a "Name" label followed by an empty text input field and a dropdown menu currently showing "Output control".
In the "Parameters" section, there are three fields: "Output" with a dropdown menu showing "Output 1", "Output control mode" with a dropdown menu showing "Monostable", and "Output parameter settings" with a text input field containing "mono, 1500" and an "Edit" button to its right.
At the bottom right of the dialog box, there are "OK" and "Cancel" buttons.

Parameters:

Output: in this section you can select the output to be controlled when the given input event occurs.



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

Available options:



- **Monostable:** the output will be activated for the time configured in the “**Duration**” section of the output parameter settings, then it will revert to normal state automatically. The duration can be configured from 5 milliseconds to 60 minutes.
- **Bistable ON:** the output will be activated permanently and will change state only upon receiving a different command or upon power loss.
- **Bistable OFF:** the output will become deactivated.
- **State change:** the output will change state (if deactivated, it will become activated, and if activated, it will become deactivated).
- **Pulse series:** the output can be controlled by pulse series as well. The number of pulse series can be configured from 1 up to 3. For each pulse it can be configured how long the output should be activated, how long should be deactivated, the number of repetitions and the pause between repetitions. The active periods can be configured from 5 milliseconds to 60 minutes and the number of repetitions can be configured from 1 to 10, and the pause between pulses can be configured from 5 milliseconds to 60 minutes too.

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

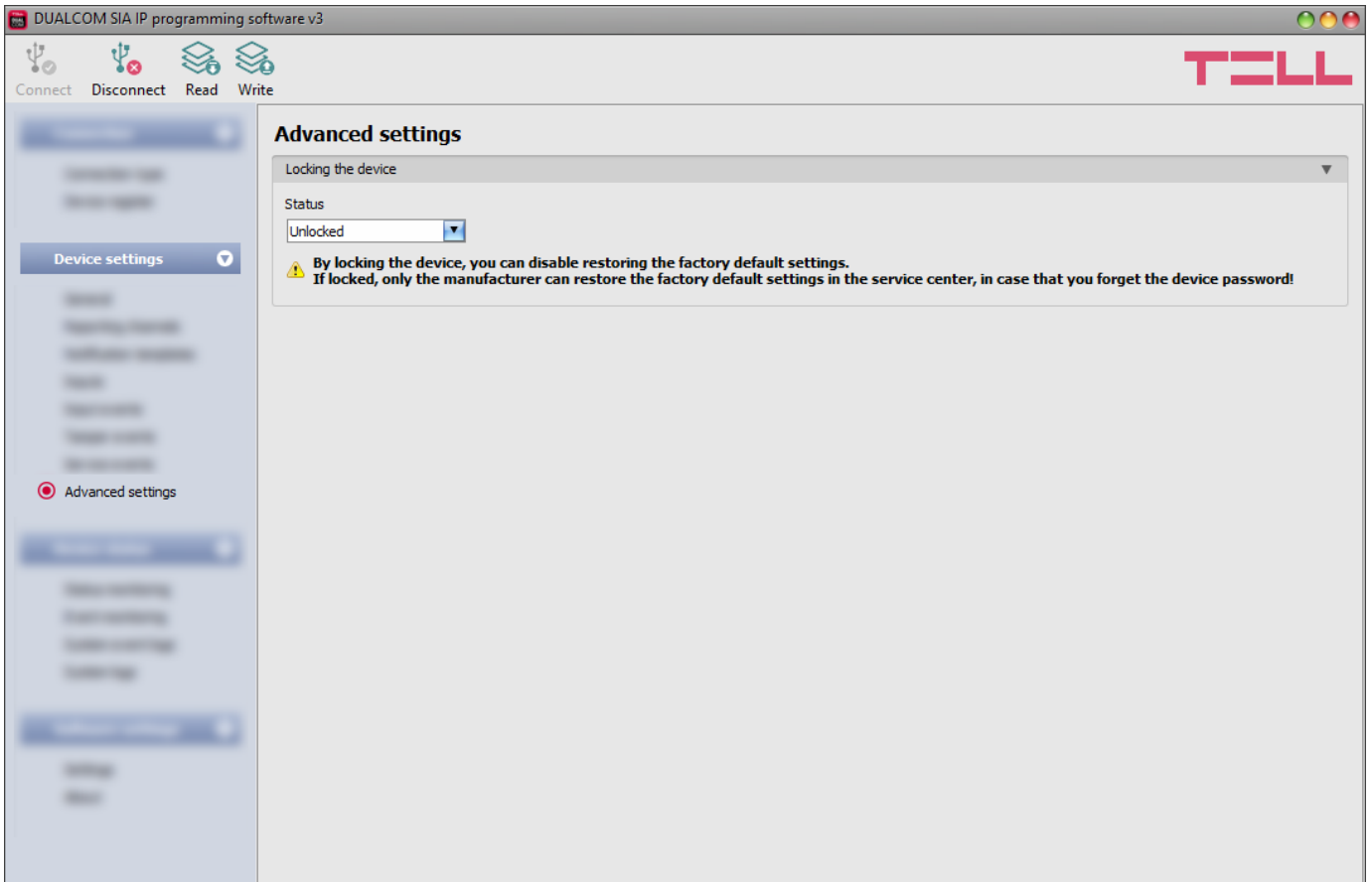
Adding a new action to an event:

- Select the service event, which you want to configure, by clicking on it in the “**Service events**” window.
- Click on the “**New action**”  button.
- Enter a name for the action. The name should not be longer than 20 characters, and the following characters cannot be used: ^ ~ < > = | \$ % " ' .
- Select the action you want to add, using the “**Action**” drop-down menu.
- Configure the action in the “**Parameters**” section.
- Click on the “**OK**” button. The action will be added in the “**Actions**” window.
- Click on the “**Write**”  button.

Editing, cloning, or deleting an action:



- Select the service event for which you want to edit, clone, or delete an action, by clicking on it in the “**Input events**” window.
- Select the action, which you want to edit, clone, or delete, by clicking on it in the “**Actions**” window.
- Click on the “**Edit action**”  , “**Clone action**”  , or the “**Delete action**”  button.

8.2.8 Advanced settings



In this menu you can configure the device lock settings.

Available options:

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

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.

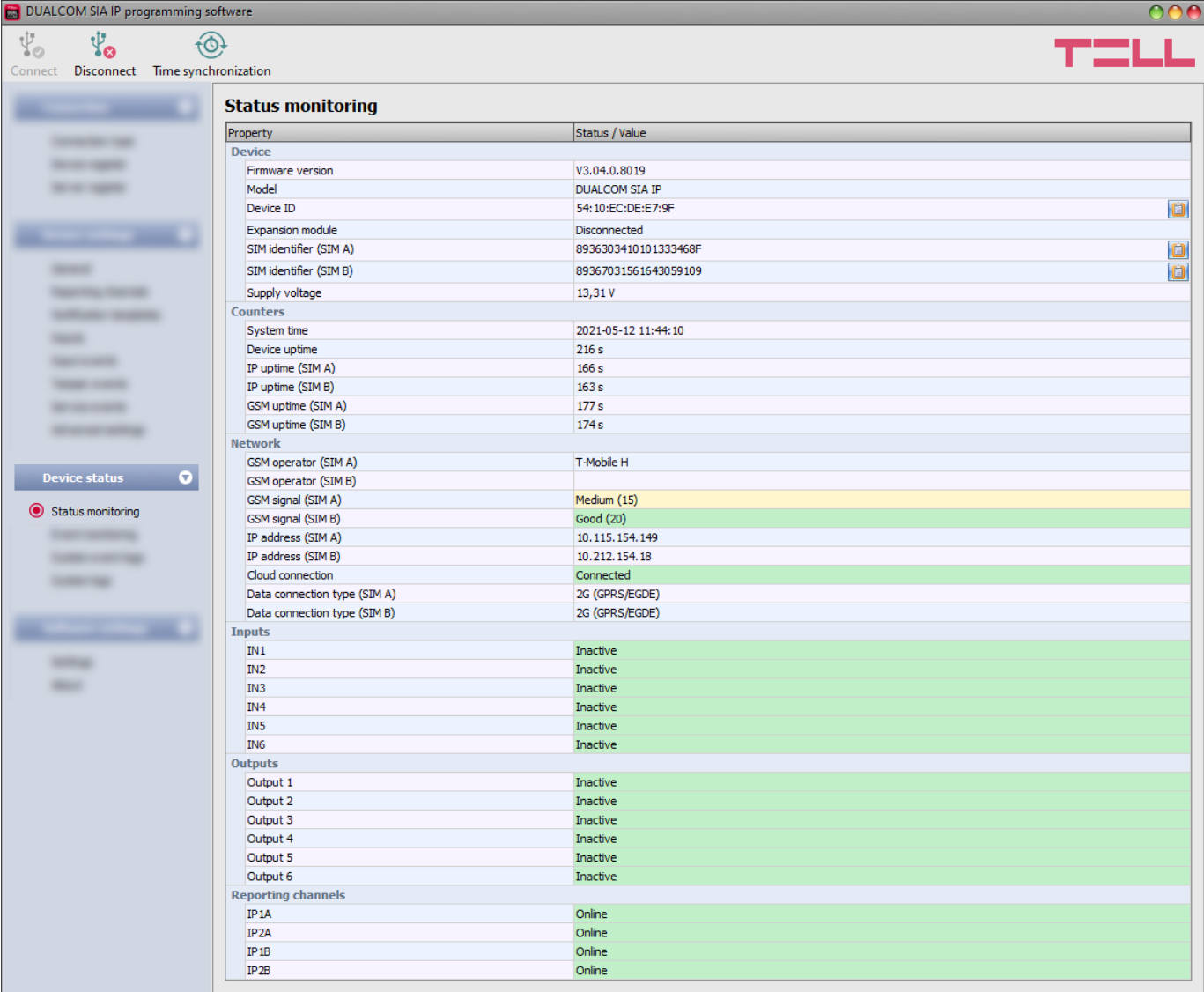
Locking the device:

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

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

8.3 Device status menu

8.3.1 Status monitoring



The screenshot shows the 'Status monitoring' window in the DUALCOM SIA IP programming software. The window title is 'DUALCOM SIA IP programming software'. The interface includes a top bar with 'Connect', 'Disconnect', and 'Time synchronization' buttons, and a 'TELL' logo. The main window displays a table of system properties and status.

Property	Status / Value
Device	
Firmware version	V3.04.0.8019
Model	DUALCOM SIA IP
Device ID	54:10:EC:DE:E7:9F
Expansion module	Disconnected
SIM identifier (SIM A)	8936303410101333468F
SIM identifier (SIM B)	89367031561643059109
Supply voltage	13,31 V
Counters	
System time	2021-05-12 11:44:10
Device uptime	216 s
IP uptime (SIM A)	166 s
IP uptime (SIM B)	163 s
GSM uptime (SIM A)	177 s
GSM uptime (SIM B)	174 s
Network	
GSM operator (SIM A)	T-Mobile H
GSM operator (SIM B)	
GSM signal (SIM A)	Medium (15)
GSM signal (SIM B)	Good (20)
IP address (SIM A)	10.115.154.149
IP address (SIM B)	10.212.154.18
Cloud connection	Connected
Data connection type (SIM A)	2G (GPRS/EGDE)
Data connection type (SIM B)	2G (GPRS/EGDE)
Inputs	
IN1	Inactive
IN2	Inactive
IN3	Inactive
IN4	Inactive
IN5	Inactive
IN6	Inactive
Outputs	
Output 1	Inactive
Output 2	Inactive
Output 3	Inactive
Output 4	Inactive
Output 5	Inactive
Output 6	Inactive
Reporting channels	
IP1A	Online
IP2A	Online
IP1B	Online
IP2B	Online

The “**Status monitoring**” menu provides information on actual system status. Please note that for faster communication, in case of remote connection some of the options are not available. Status information loads and refreshes automatically only when connected through USB. In case of remote connection, status information can be loaded or updated by clicking on the

“**Query**”  button.

Device:

- **Firmware version:** the firmware version of the device.
- **Model:** the device type/model.
- **Device ID:** the unique identifier of the device (6x2 hexadecimal characters). This identifier is burned-in during production and thereby it is unchangeable. You can copy the ID to clipboard by clicking the notepad icon on the right-hand side.
- **Expansion module:** shows the connection status of the **EXT24-D** expansion module.
- **SIM identifier (SIM A / SIM B):** the identifier (ICCID) of the SIM cards installed in the device, for both interfaces. You can copy the ID to clipboard by clicking the notepad icon on the right-hand side.
- **Supply voltage:** value of measured supply voltage.

Counters:

- **System time:** the system date and time.
- **Device uptime:** elapsed time since the device has been powered up.
- **IP uptime (SIM A / SIM B):** elapsed time for both interfaces since the device has last connected to the Internet.
- **GSM uptime (SIM A / SIM B):** elapsed time for both interfaces since the device has last connected to the GSM network.

Network:

- **GSM operator (SIM A / SIM B):** the name of the GSM operator used.
- **GSM signal (SIM A / SIM B):** actual GSM signal level for both interfaces: None/Very low, Weak, Medium, Good, Excellent.
- **IP address (SIM A / SIM B):** the actual IP address of the device for both interfaces.
- **Cloud connection:** the cloud connection status.
- **Data connection type (SIM A / SIM B):** the current data connection type for both interfaces: 4G (E-UTRAN), 3G (UTRAN), 2G (GPRS/EGDE).

Inputs:

- **IN1...IN6:** the actual state of the contact inputs:
 - **Inactive:** the input is in idle state.
 - **Active:** the input is triggered.
 - **Tamper:** in case of using EOL – protection loop trouble on the given input (loop open).

Expansion module inputs:

- **XIN7...XIN30:** the actual state of the **EXT24-D** expansion module's contact inputs.

Outputs:

- **Output1...Output6:** the actual state of the outputs:
 - **Inactive:** the output is in idle state.
 - **Active:** the output is triggered.

Reporting channels:

- **IP1A, IP2A, IP1B, IP2B:** connection status of the configured servers and IP receivers:
 - **Connecting...:** connecting is in progress.
 - **Online:** connected to server/receiver, ready.
 - **Failed to connect or auth error:** no response received from the configured IP address (no receiver on the configured IP address, or authentication error).
 - **Rejected by server/receiver:** the given server/receiver has rejected the device.
 - **Not configured:** no IP address configured for the given channel.

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

- **Query:**



This button appears in case of remote connection only. By clicking on it, status information will be downloaded from the device. This is not needed for USB connection, since in that case the data is downloaded automatically.

- **Time synchronization:**



This button is used to synchronize the device system time with the PC system time, or set custom time, according to your choice.







8.3.2 Event logs

Event							Reporting			
#	Date/Time	Event	Category	Type	Source	Event code	1A	2A	1B	2B
15	2020. 03. 02. 12:53:57	IN4 restore	Input	restore	IN4	18311001004	?	?	*	*
14	2020. 03. 02. 12:53:56	IN4 alarm	Input	New	IN4	18111001004	*	*	*	*
13	2020. 03. 02. 12:52:21	Periodic test report	Service	New	Periodic test report	18160200000	*	*	*	*
12	2020. 03. 02. 12:51:41	IN6 restore	Input	restore	IN6	18311001006	*	*	*	*
11	2020. 03. 02. 12:51:40	IN6 alarm	Input	New	IN6	18111001006	*	*	*	*
10	2020. 03. 02. 12:50:49	IN3 restore	Input	restore	IN3	18311001003	*	*	*	*
9	2020. 03. 02. 12:50:47	IN3 alarm	Input	New	IN3	18111001003	*	*	*	*
8	2020. 03. 02. 12:50:32	IN1 restore	Input	restore	IN1	18311001001	*	*	*	*
7	2020. 03. 02. 12:50:30	IN1 alarm	Input	New	IN1	18111001001	*	*	*	*
6	2020. 03. 02. 12:50:22	IN5 restore	Input	restore	IN5	18311001005	*	*	*	*
5	2020. 03. 02. 12:50:21	IN5 alarm	Input	New	IN5	18111001005	*	*	*	*
4	2020. 03. 02. 12:50:14	IN2 restore	Input	restore	IN2	18311001002	*	*	*	*
3	2020. 03. 02. 12:50:13	IN2 alarm	Input	New	IN2	18111001002	*	*	*	*
2	2020. 03. 02. 12:50:08	IN1 restore	Input	restore	IN1	18311001001	*	*	*	*
1	2020. 03. 02. 12:50:07	IN1 alarm	Input	New	IN1	18111001001	*	*	*	*

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

You can follow the events and the reporting progress in the “**Events**” window, while the configured actions performed by events are shown in the “**Actions**” window. To view the actions associated with 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 you want to see in the list: last 10, 20, 50, 100 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.

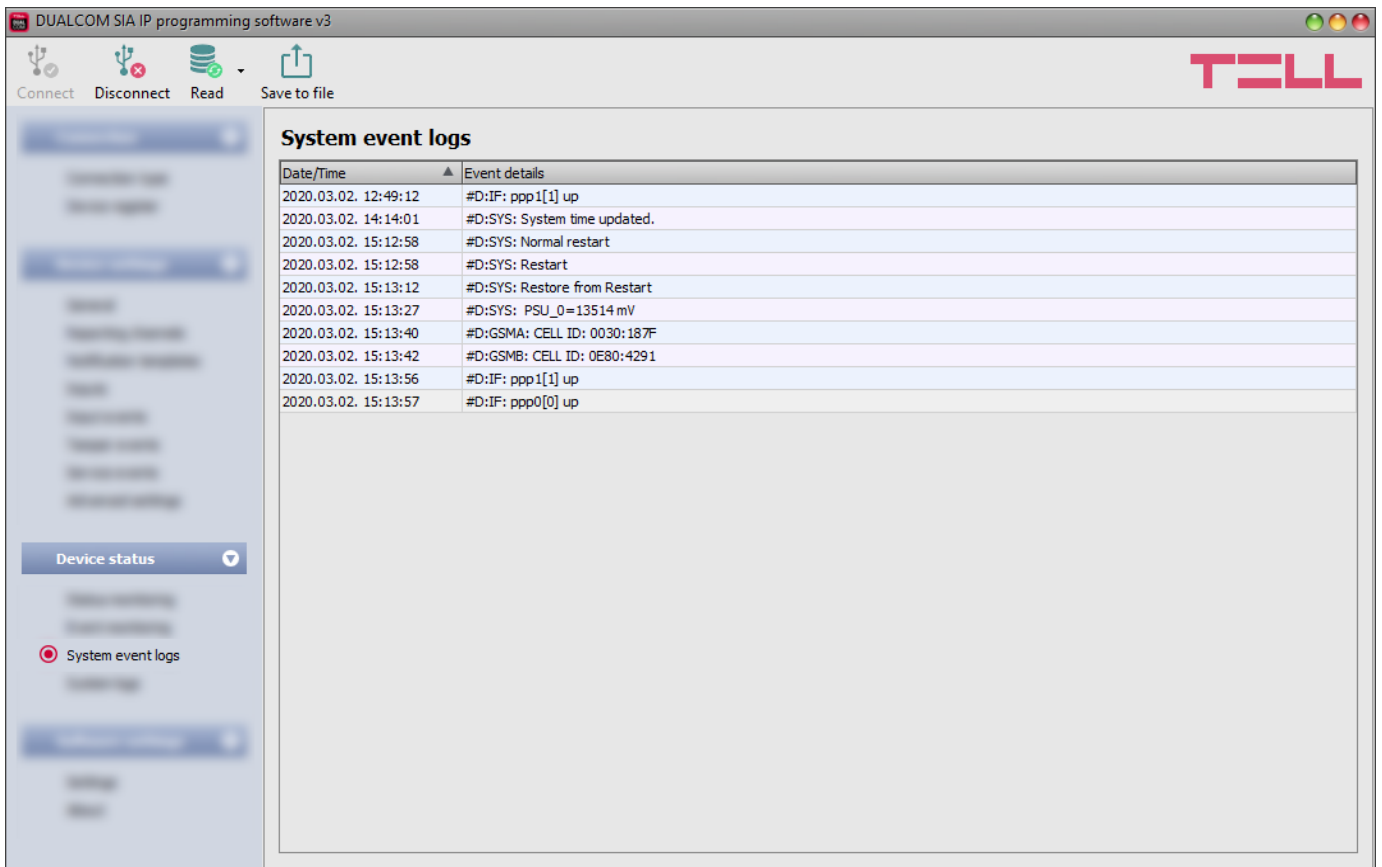
Elements of the event log:

- **#:** the ordinal number of the event in the list.
- **Date/Time:** event occurrence date and time.
- **Event:** the name of the event.
- **Category:** event category (input or service).
- **Type:** event type (new / restore).
- **Source:** event source (input number or service event name).
- **Event code:** the event’s Contact ID event code.
- **IP1A, IP2A, IP1B, IP2B:** reporting to the configured servers and IP receivers.



Legend of reporting status shown in the **IP1A, IP2A, IP1B** and **IP2B** columns:


?	New event reporting is in progress.
R	No need to report, because reporting to an alternative reporting channel was successful.
*	Reported successfully.
E	Reporting failed, the given server/receiver is not available.
-	No reporting action or server/receiver IP address configured.
T	Timeout, the notification could not be delivered in time.

8.3.3 System event logs



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

To download the system event logs from the device, open the “**Read**”  drop-down menu, select how many events you want to download (last 10, 20, 50, 100 or all), and then click on the “**Read**”  button.

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

8.3.4 System logs

System logs

General

Date/Time	Type	Identifier	Event
2020.03.02.14:41:20	DEBUG	1513832	D: [DualCom] <2A> (14:38:20)Send LifeSign
2020.03.02.14:41:20	DEBUG	1514206	D: [UserLevelEvObs] <2A> (14:38:20)Receiver time: 14:56:06,02-27-2020
2020.03.02.14:41:20	DEBUG	1514233	D: [UserLevelEvObs] <2A> (14:38:20)Response: ACK
2020.03.02.14:41:20	DEBUG	1514238	D: [DualCom] <2A> (14:38:20)Lifesign OK
2020.03.02.14:41:21	DEBUG	1514245	D: [DualCom] <1B> (14:38:20)Disconnect...
2020.03.02.14:41:21	DEBUG	1514250	D: [DualCom] <1B> (14:38:20)OnClosed...
2020.03.02.14:41:21	DEBUG	1514378	D: [DualCom] <2B> (14:38:21)Disconnect...
2020.03.02.14:41:21	DEBUG	1514385	D: [DualCom] <2B> (14:38:21)OnClosed...
2020.03.02.14:41:25	DEBUG	1519125	D: [DualCom] <1A> (14:38:25)Disconnect...
2020.03.02.14:41:25	DEBUG	1519130	D: [DualCom] <1A> (14:38:25)OnClosed...
2020.03.02.14:41:31	DEBUG	1524793	D: [DualCom] <2A> (14:38:31)Disconnect...
2020.03.02.14:41:31	DEBUG	1524797	D: [DualCom] <2A> (14:38:31)OnClosed...

SIM A interface

Date/Time	Event
2020.03.02.14:38:24	D: [DualCom] <1A> (14:35:24)OnClosed...
2020.03.02.14:38:30	D: [DualCom] <2A> (14:35:30)Disconnect...
2020.03.02.14:38:30	D: [DualCom] <2A> (14:35:30)OnClosed...
2020.03.02.14:41:13	D: [DualCom] <1A> (14:38:13)Lifesign Send...
2020.03.02.14:41:14	D: [DualCom] <1A> (14:38:14)Send LifeSign
2020.03.02.14:41:15	I: [UserLevelEvObs] <1A> (14:38:15)Response: ACK
2020.03.02.14:41:15	D: [DualCom] <1A> (14:38:15)Lifesign OK
2020.03.02.14:41:19	D: [DualCom] <2A> (14:38:19)Lifesign Send...
2020.03.02.14:41:20	D: [DualCom] <2A> (14:38:20)Send LifeSign
2020.03.02.14:41:20	D: [UserLevelEvObs] <2A> (14:38:20)Receiver time: 14:56:06,02-27-2020
2020.03.02.14:41:20	D: [UserLevelEvObs] <2A> (14:38:20)Response: ACK
2020.03.02.14:41:20	D: [DualCom] <2A> (14:38:20)Lifesign OK
2020.03.02.14:41:25	D: [DualCom] <1A> (14:38:25)Disconnect...
2020.03.02.14:41:25	D: [DualCom] <1A> (14:38:25)OnClosed...
2020.03.02.14:41:31	D: [DualCom] <2A> (14:38:31)Disconnect...
2020.03.02.14:41:31	D: [DualCom] <2A> (14:38:31)OnClosed...

SIM B interface

Date/Time	Event
2020.03.02.14:38:19	D: [DualCom] <1B> (14:35:19)OnClosed...
2020.03.02.14:38:20	D: [DualCom] <2B> (14:35:20)Disconnect...
2020.03.02.14:38:20	D: [DualCom] <2B> (14:35:20)OnClosed...
2020.03.02.14:41:08	D: [DualCom] <1B> (14:38:07)Lifesign Send...
2020.03.02.14:41:09	D: [DualCom] <1B> (14:38:08)Send LifeSign
2020.03.02.14:41:09	I: [UserLevelEvObs] <1B> (14:38:09)Response: ACK
2020.03.02.14:41:09	D: [DualCom] <1B> (14:38:09)Lifesign OK
2020.03.02.14:41:09	D: [DualCom] <2B> (14:38:09)Lifesign Send...
2020.03.02.14:41:10	D: [DualCom] <2B> (14:38:10)Send LifeSign
2020.03.02.14:41:10	D: [UserLevelEvObs] <2B> (14:38:10)Receiver time: 14:55:56,02-27-2020
2020.03.02.14:41:10	D: [UserLevelEvObs] <2B> (14:38:10)Response: ACK
2020.03.02.14:41:10	D: [DualCom] <2B> (14:38:10)Lifesign OK
2020.03.02.14:41:21	D: [DualCom] <1B> (14:38:20)Disconnect...
2020.03.02.14:41:21	D: [DualCom] <1B> (14:38:20)OnClosed...
2020.03.02.14:41:21	D: [DualCom] <2B> (14:38:21)Disconnect...
2020.03.02.14:41:21	D: [DualCom] <2B> (14:38:21)OnClosed...

This menu shows information about the internal processes of the device and communication. These details help troubleshooting if a malfunction occurs. **This option is only available when connected through USB!**

Based on their nature, information are splitted into different channels. You can view the entries related to the general operation of the device, and entries of interfaces SIM A and SIM B, in separate windows. The program stores the logs automatically in the folder named “**Logs**”, found in the data folder which you can open by clicking on the link available in the “**About**” menu.

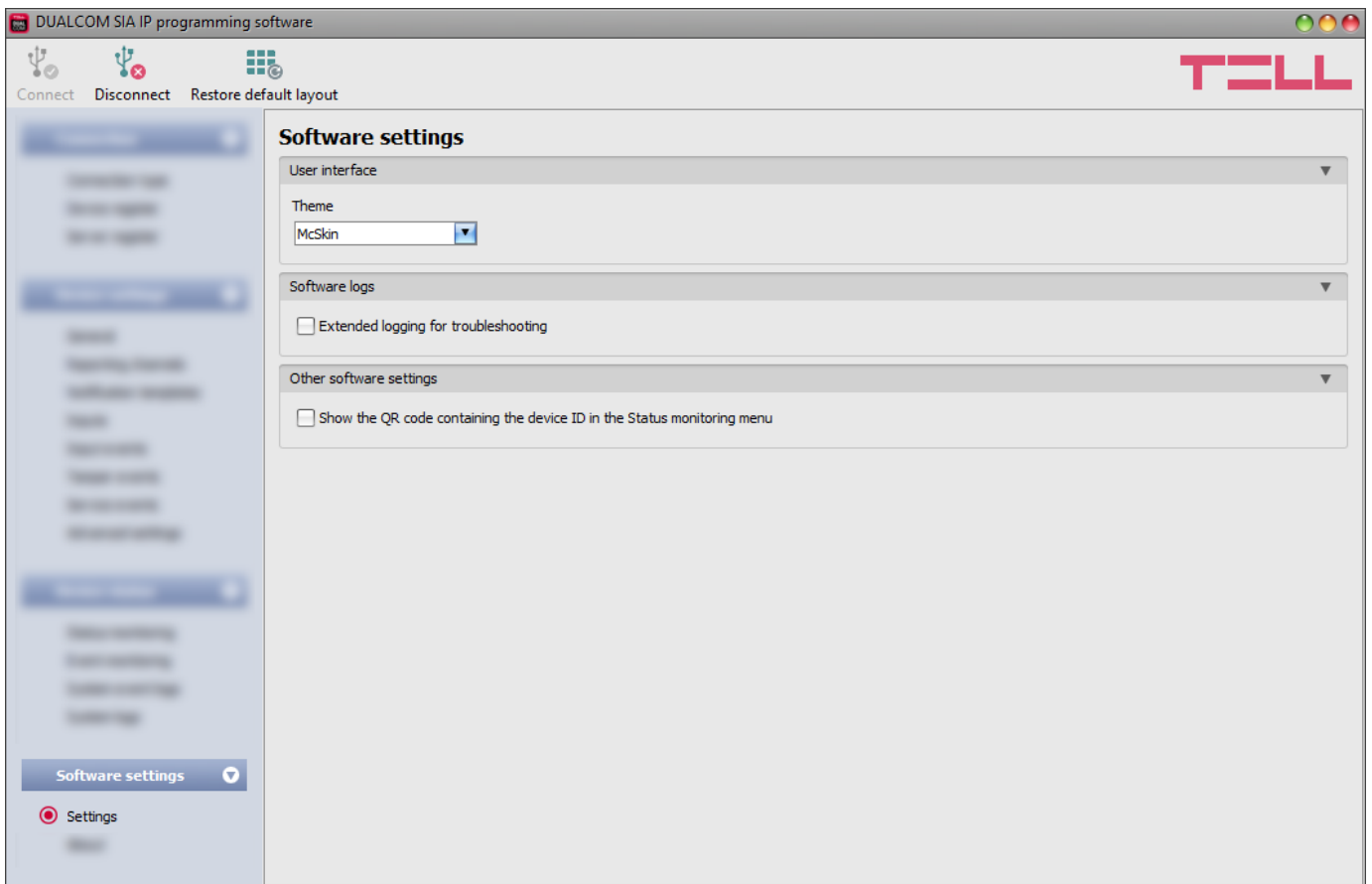
The “**AT log (SIM A)**” and “**AT log (SIM B)**” buttons are used to enable and disable logging of AT commands, separately for each interface. This serves for troubleshooting, for viewing detailed information on the operation of the modems.

Elements of the system logs window:

- **Date/Time:** date and time of entry.
- **Identifier:** entry identification number.
- **Type:** information channel type.
- **Event:** event details.

8.4 Software settings menu

8.4.1 Settings



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

Available options:

- **Restore default layout:**



To restore the user interface default layout, click on the “**Restore default layout**” button, and then close and restart the program.

User interface:

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

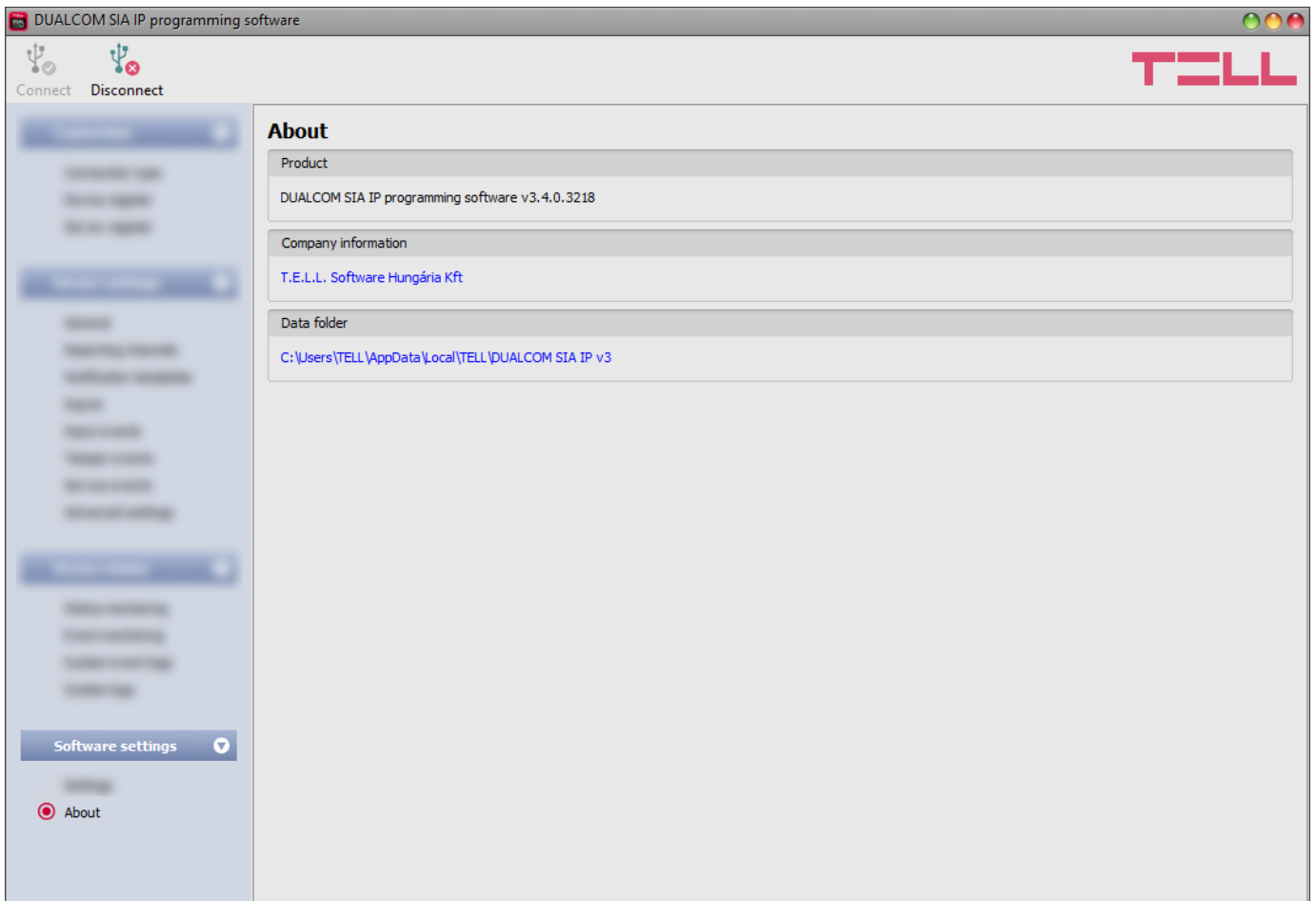
Software logs:

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

Other software settings:

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

8.4.2 About



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

9 Configuring by SMS commands

The tables below contain the SMS commands which can be used to configure the essential settings needed for the device to connect to the mobile Internet, and to a receiver. You can send SMS commands to either phone numbers of the SIM cards installed in the device. After successfully configured, you can access the device for further detailed configuring, using the programming software over the cloud or via the receiver (in case of using a TELLMon receiver).

The device accepts SMS commands from the **Admin phone number** configured in advance, or from any phone number, if you specify the valid device password at the beginning of the message. You can specify the device password in the message using the “**PWD**” parameter, as shown below. Commands sent from unauthorized phone numbers with a missing device password or a wrong password, will be ignored by the device and it will not send any reply to these numbers.

Commands should always be typed using capital letters.

SMS command, when sent from the ADMIN PHONE NUMBER	Specification
APNA=APN# APNB=APN# Example: APNA=internet#	Configuring the APN for interfaces SIM A and SIM B.
APNA=APN,username,password## APNB=APN,username,password## Example: APNB=net,guest,guest#	Configuring the APN along with the username and password belonging to it.
IP1A=IP address,port number,user account ID# Example: IP1A=185.45.23.129,3535,4321#	Configuring the receiver IP address, port number, and the user account ID for channel IP1A.
IP1B=IP address,port number,user account ID#	Configuring the receiver IP address, port number, and the user account ID for channel IP1B.
CLOUD=SIMA# CLOUD=SIMB#	Configuring the default interface (SIM A or SIM B) for cloud usage.
CONNECT=cloud IP address:port number# Example: CONNECT=54.75.242.103:2020#	Configuring the cloud IP address and port number, and then connecting to the cloud.

It is possible to send multiple commands in one SMS, but the message length should not exceed 140 characters. Each command must end with the # character, e.g.:

APNA=internet#APNB=net,guest,guest#IP1A=185.45.23.129,3545,4321#

SMS command, when sent from OTHER PHONE NUMBER	Specification
PWD=device password#APNA=APN# PWD=device password#APNB=APN# Example: PWD=1234#APNA=internet#	Configuring the APN for interfaces SIM A and SIM B.
PWD=device password#APNA=APN,username,password# PWD=device password#APNB=APN,username,password# Example: PWD=1234#APNB=net,guest,guest#	Configuring the APN along with the username and password belonging to it.
PWD=device password#IP1A=IP address,port number,user account ID# Example: PWD=1234#IP1A=185.45.23.129,3535,4321#	Configuring the receiver IP address, port number, and the user account ID for channel IP1A.
PWD=device password#IP1B=IP address,port number,user account ID#	Configuring the receiver IP address, port number, and the user account ID for channel IP1B.
PWD=device password#CLOUD=SIMA# PWD=device password#CLOUD=SIMB# Example: PWD=1234#CLOUD=SIMA#	Configuring the default interface (SIM A or SIM B) for cloud usage.
PWD=device password#CONNECT=cloud IP address:port number# Example: CONNECT=54.75.242.103:2020#	Configuring the cloud IP address and port number, and then connecting to the cloud.

PWD: the device password can be specified using this parameter, which is necessary when the command is sent from an unauthorized phone number. The superadmin and admin passwords are both accepted (default superadmin password: 1234).

It is possible to send multiple commands in one SMS, but the message length should not exceed 140 characters. Each command must end with the # character, e.g.:

PWD=1234#APNA=internet#APNB=net,guest,guest#IP1A=185.45.23.129,3535,4321#

The device will send a reply when configuring is successful, or if there are errors in the parameters sent. Possible replies:

Message	Specification
APNA changed	APN successfully configured for interface SIM A.
APNB changed	APN successfully configured for interface SIM B.
IP1A changed	Receiver availabilities successfully configured for channel IP1A.
IP1B changed	Receiver availabilities successfully configured for channel IP1B.
CLOUD changed	The default interface for cloud usage successfully configured.
IP1A: Admin access denied	You have specified the admin password for the IP1A command, which is unauthorized to change receiver settings.
IP1B: Admin access denied	You have specified the admin password for the IP1B command, which is unauthorized to change receiver settings.
IP1A: user account ID error	The user account ID specified for the IP1A settings is wrong.
IP1B: user account ID error	The user account ID specified for the IP1B settings is wrong.
IP1A: port range error	The port number specified for the IP1A settings is wrong.
IP1B: port range error	The port number specified for the IP1B settings is wrong.
IP1A: IP address format error	The IP address specified for the IP1A settings is wrong.
IP1B: IP address format error	The IP address specified for the IP1B settings is wrong.
IP1A: syntax error	You have specified more, or less parameters for the IP1A command.
IP1B: syntax error	You have specified more, or less parameters for the IP1B command.
CLOUD syntax error	The parameter specified for the CLOUD command is wrong.

In case that you send the wrong command, the device cannot interpret your message, and therefore it will not send a reply!

10 Updating the firmware

TELL always releases its products with the latest firmware version. However, as our products are being continuously improved, new firmware updates may occasionally be released for the products, which may include new features along with bug fixes. Therefore, it is recommended that you always upgrade your product to the latest firmware version available. All released firmware versions are available on the TELL website, including older versions.

ATTENTION! Downgrading to an earlier version is not supported! Always upgrade your product to the latest version. Otherwise, your settings could get wiped due to differences in functionality between versions, or the product may become unusable due to unsupported components. (A newer hardware may contain new components, e.g., a new flash memory, modem, etc., which are not supported by an earlier firmware.)

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


10.1 Updating via USB

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

- **Updating via USB using the desktop update application:**

- Download the latest update tool (application with **.exe** extension) from the manufacturer's website. The update tool includes the firmware as well, therefore the file name is the same as the firmware version number.
- Open the update tool and click on the "**FIRMWARE**" button.
- 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 tool when the progress bar shows that the process has completed.
- Wait until the LED status indicator on the device shows activity. You can then connect to the programming software and check the functioning.

- **Updating via USB using the programming software:**

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

10.2 Updating remotely over the internet

The following methods are available for updating the **DUALCOM** device's firmware remotely:


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

After establishing the remote connection, the steps for remote update are the same as the steps for updating through USB, as specified above.

11 Restoring the factory default settings

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

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

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

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

12 Contents of the package

- **DUALCOM** device
- 2pcs GSM 900/1800MHz antenna
- Plastic spacer support / snap fasteners
- Quick start guide, warranty card

13 About the manufacturer

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