STEMAX

STEMAX ML

COMMUNICATION SERVER

6.0

USER MANUAL

CONTENTS

1 ABOUT STEMAX ML

The STEMAX ML communication server (hereafter referred to as STEMAX ML) is designed to transfer data from STEMAX controllers and Livicom sites to any third-party central monitoring system in the Contact ID (DSC Sur-Gard) protocol.

STEMAX ML receives events from STEMAX controllers and Livicom sites encrypted by the MSRV protocol and re-encrypts them using the standard Contact ID (Sur-Gard) protocol. The event transmission module is built directly into the STEMAX ML server. STEMAX ML buffers all events until the third-party monitoring system receives them to ensure the reliable delivery.

STEMAX ML is designed as a Windows service. STEMAX ML does not have any database and that speeds up event processing and transfer to the third-party monitoring system. It also simplifies the STEMAX ML installation and maintenance. Supported operating systems — Windows Vista, 7, 8 and 10.

STEMAX ML features:

- STEMAX ML receives data from the Livicom cloud platform and directly from Livi Smart Hub / Livi Smart Hub 2G hubs (hereafter referred to as the hubs),
- STEMAX ML receives data directly from STEMAX controllers (hereafter referred to as the controllers),
- The correspondence of events in the MSRV format to events in the Contact ID format can be set by default or configured manually (see 7.2).
- STEMAX ML selectively tests site communication channels for quick detection of failures or possible suppression.
- The GSM signal strength is analyzed and displayed in real time.
- All changes in the server configuration are applied automatically without restarting the server.

Note that STEMAX ML cannot be used as an independent monitoring system, since it does not have any database.

2 SELECT PC FOR STEMAX ML

STEMAX ML is designed for installation on a personal computer (PC) running under 7/ 8 or 10. The recommended PC configuration is shown in the table 2.1.

Table 2.1 – Recommended PC configuration

Configuration parameter	**Recommended value**
Processor speed	2400 MHz or more
RAM	2 GB or more
HDD	500 GB or more
Video card	1 GB or more
Network card	10 MB/s or more
Ethernet bandwidth	5 Mbps or more
Screen diagonal	19” or more
Uninterruptible power supply	required

The configuration above is given for reference. STEMAX ML can run on both lower and higher performance PCs. PC performance requirements are also determined by the number of connected sites and types of their communication channels.

3 OBTAIN LICENSE

STEMAX ML is a proprietary software, which is distributed under a free license. Security companies have to go through the licensing procedure to use STEMAX ML.

Follow these steps to obtain the license:

- Send an official license request to the Stels research and development company (hereafter referred to as STELS) by e-mail to support@nppstels.ru.
- STELS provides you the STEMAX ML installation file and the user manual, if the request has been accepted.
- Launch the STEMAX_Server_ML_X.exe installation file (where X is the software version number) to install STEMAX ML.

NOTES

1 – We recommend running executable files **as Administrator** in Windows 7 and above. Right-click on the file and select *Run as Administrator* in the menu.

2 – The license binds STEMAX ML to the PC, on which it is installed. Make sure that the PC fits the configuration requirement (see table 2.1) before launching the installation file.

- Find the file LicenseQuery in the STEMAX ML installation folder and run it as Administrator.
- Click the Create request file button in the window that opens.
- Select the folder to save the license query file (*.liq) and click the *Save* button.
- Send the saved license query file (*.liq) to support@nppstels.ru.

You will receive the license **(***.reg file**). Download it from the e-mail and copy it to the STEMAX ML installation folder** (by default C:\Program Files\MS_System_ML).

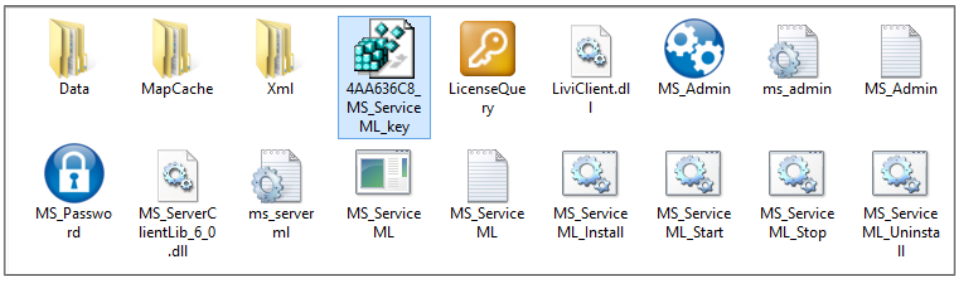


Figure 3.1 – License file in the STEMAX ML installation folder

Note – If the STEMAX ML service is running, then stop it and launch again after you have saved the license (see 4.4). You will not be able to create receiver-transmitters in STEMAX ML without the license.

The license binds STEMAX ML to the PC, on which it is installed. If you are going to run another copy of STEMAX ML on a different PC, then you will have to follow the same licensing procedure for the second PC again.

4 INSTALL AND RUN STEMAX ML

4.1 INSTALL STEMAX ML

STEMAX ML is designed as a Windows service. Run the *MS_ServiceML_Install.bat* file as Administrator to install the service. The file is located in the STEMAX ML installation folder (by default C:\Program Files\MS_System_ML).

The STEMAX ML service will be installed on your PC, but not started. Set the superuser name and password as described below before starting the service.

4.2 CREATE SUPERUSER

Superuser is the STEMAX ML user with the complete set of rights, including the right to create and delete other user and set access rights for them.

Follow these steps to create the superuser:

1. Open the STEMAX ML installation folder (by default C:\Program Files\MS_System_ML).
2. Run the *MS_Password.exe* file as Administrator.
3. Enter the superuser name and password in the open window and click “Set”.
4. Click *ok* to close the confirmation window.

We recommend restricting access to the *MS_Password.exe* file for security purposes, when the superuser has been created. For example, you can put it in a password-protected archive.

4.3 START STEMAX ML

Run the *MS_ServiceML_Start.bat* file as Administrator to initiate the service. The file is located in the STEMAX ML installation folder (by default C:\Program Files\MS_System_ML).

The service runs in the background in Windows after it has been started. The service starts automatically with Windows when you turn on the PC.

4.4 STOP AND RESTART STEMAX ML

The STEMAX ML service should be stopped in the following cases:

- To change the superuser name or password using the *MS_Password.exe* program.
- To change the STEMAX ML operational parameters in the *ms_serverml.ini* file.

Changed settings are applied only when the service is restarted (stopped and started again).

Run the *MS_ServiceML_Stop.bat* file as Administrator to stop the service. Then run again the *MS_ServiceML_Start.bat* file as Administrator to restart the service. The files are located in the STEMAX ML installation folder (by default C:\Program Files\MS_System_ML).

Note – You can also stop and start the service using the Windows Task Manager.

4.5 RUN STEMAX ADMINISTRATOR

Run the *MS_Admin.exe* file as Administrator. The file is located in the STEMAX ML installation folder (by default C:\Program Files\MS_System_ML).

When the *STEMAX Administrator* is launched, the main window opens in an inactive state with the *Server connection* window on top (the authorization window – see figure 4.1).

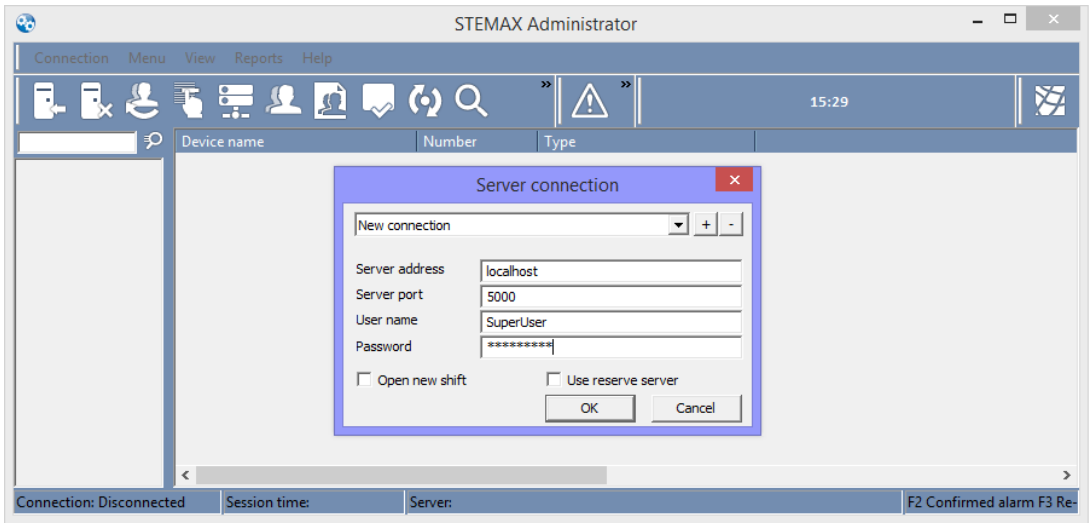


Figure 4.1 – Launching the *STEMAX Administrator*

Log in to the *STEMAX Administrator* as the Superuser (see 4.2): enter the data according to the table 4.1 in the authorization window and click *OK* .

Table 4.1 – *STEMAX ML* connection parameters

Parameter	**Value**
Server address	- localhost, if the *STEMAX Administrator* is launched on the server PC (on the PC where the STEMAX ML service is running). - local IP address of the server PC, if the *STEMAX Administrator* is connecting to the STEMAX ML service using LAN. - external static IP address of the server PC, if the *STEMAX Administrator* should connect to STEMAX ML through the Internet.
Server port	TCP/IP port, which is dedicated for connection to the STEMAX ML server (by default 5000).
Username	Superuser name
Password	Superuser password

If you have entered any incorrect data, then retry to log in. Open the *Connection* menu in the main window of the *STEMAX Administrator* and select *Connect to server* (see figure 4.2). The authorization window will open again.

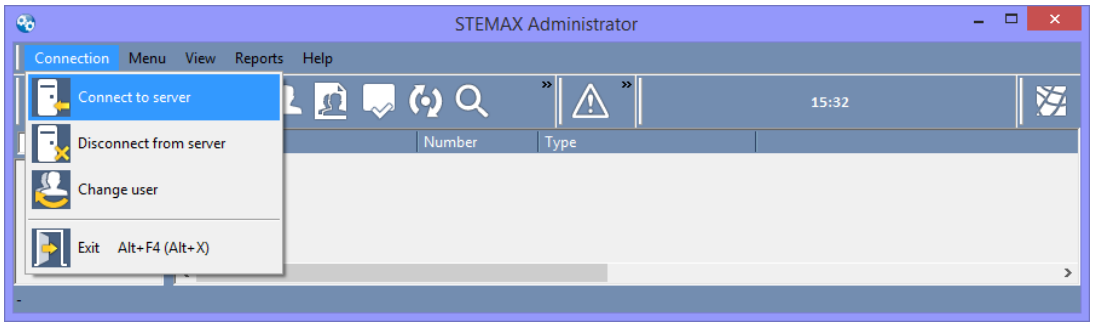


Figure 4.2 – Reconnecting to STEMAX ML

You can save the log in details for auto-fill. Enter the log in details and click the button + at the top of the authorization window to save them (see figure 4.3).

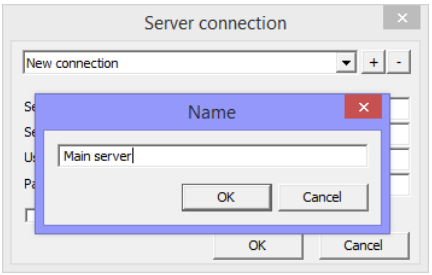


Figure 4.3 – Adding the log in profile

Enter a name for the log in profile in the *Name* window and click *OK*. The log in profile is saved in the program memory. Later you will be able to select the profile from the drop-down list at the top of the authorization window (see figure 4.4).

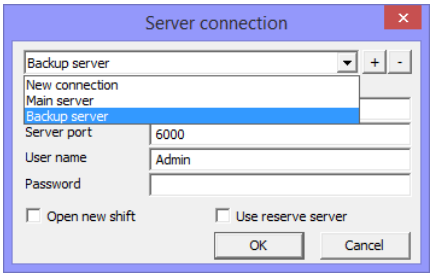


Figure 4.4 – Selecting the log in profile

To delete the selected log in profile, click on the button -

Check boxes *Open new shift* and *Use reserve server* can be hidden in some versions of STEMAX ML (see figure 4.1). They are not intended to be used in STEMAX ML (a reserve server and shifts are used in the full version of the STEMAX software).

5 SET UP INTERACTION WITH LIVICOM SYSTEM

Livicom Smart Homes are the sites where Livi Smart Hub or Livi Smart Hub 2G is used as the controller (hereafter referred to as the Livicom sites). The Livicom sites register in STEMAXL ML automatically as the result of the procedure described below (see 8).

Follow these steps to set up the interaction between the Livicom sites and your monitoring system with the help of STEMAX ML:

1. Go through the authorization procedure to become a Livicom partner.

The security company should perform the actions described on p. 5.1 to obtain the Livicom partner status.

2. Configure STEMAX ML to receive events from the Livicom cloud platform and from the hubs.

The STEMAX ML administrator creates receiver-transmitters so that the STEMAX ML server could receive events from the Livicom cloud platform and from the hubs (see 5.2).

3. Receive and process security service requests from Livicom clients.

The security company receives security service requests from Livicom sites by e-mail and processes them to accept sites for protection (see 8).

The hubs, which are connected to STEMAX ML, will send events in real time to the STEMAX ML server via a TCP-IP channel (GPRS or Ethernet). The hub will simultaneously send alarm alerts to the Livicom platform and to STEMAX ML as the hub can support four active IP-connections.

The structure of the interaction between the Livicom sites and STEMAX ML is shown on the figure 5.1.

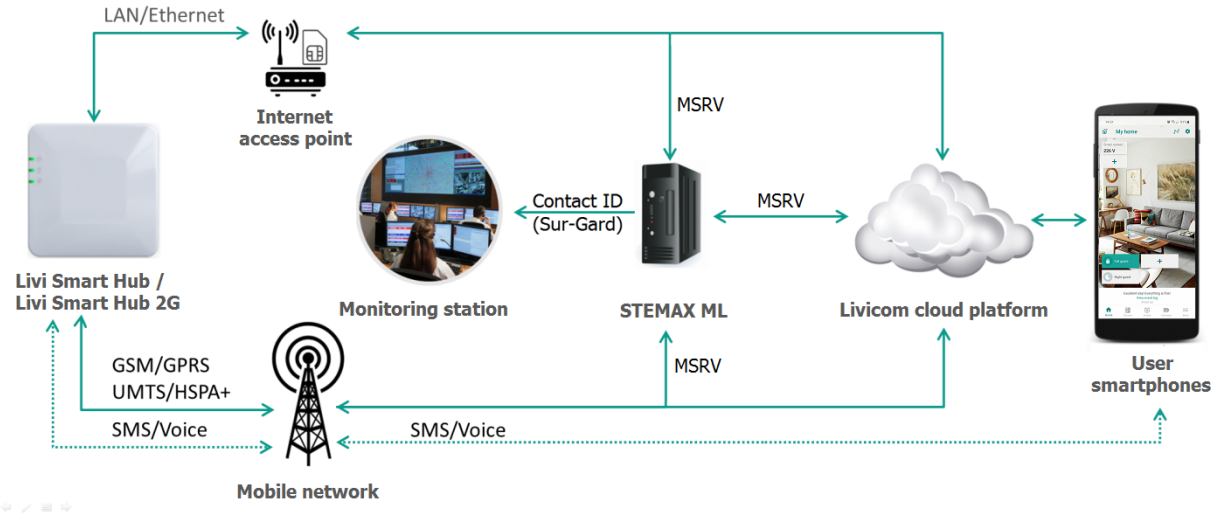


Figure 5.1 – The structure of the integration between the Livicom system and STEMAX ML

Only the security company can disconnect the Livicom sites from the STEMAX ML server. But Livicom clients can initiate the disconnection by sending the service termination request from the Livicom app (see 9.5).

5.1 BECOME LIVICOM PARTNER

Any security company can be authorized as the Livicom partner. The authorization requirements are:

- ✓ To have any central monitoring station, which is able to receive events in the standard Contact ID (DSC Sur-Gard) protocol.
- ✓ To purchase any Livicom starter kit to study the Livicom system features.
- ✓ To install and set up STEMAX ML (version 6.0 or higher).

If the authorization requirements are met, then the security company can send an authorization request to STELS by e-mail (mail-to: support@nppstels.ru).

The request should contain the information listed in the table 5.1

Table 5.1 – Authorization request contents

Information	Description
Company info	Full name of the security company, its requisites, names and contacts of the director and STEMAX ML administrator
E-mail	Select the e-mail that is dedicated to interact with clients and to receive technical reports
STEMAX ML server address	The external static IP address or the DNS address of the PC where the STEMAX ML service is running
STEMAX ML server	TCP/IP port on the server PC, which is dedicated to connect the hubs to

Information	Description
Company info	Full name of the security company, its requisites, names and contacts of the director and STEMAX ML administrator
E-mail	Select the e-mail that is dedicated to interact with clients and to receive technical reports
port	STEMAX ML (by default 5000)
Contacts	Web-site of the security company, contact info clients, the list of cities, in which the company provides security services

The authorization request should be written on the letterhead of the security company, signed by the director and sealed.

STELS processes the request received from the security company. If the request is accepted, STELS registers the security company on the Livicom cloud platform.

Then STELS provides to the security company the following data (by e-mail):

- Livicom cloud platform DNS address.
- TCP/IP port for connecting STEMAX ML to the platform.
- Username of the security company account on the platform.
- Password of the account on the platform.
- The unique identifier of the security company in the Livicom system (*Provider ID*).
- The unique key for connecting the security company to the Livicom system (*Provider secret key*).

STELS requires the authorized partner to adapt the security contract form, to post on the main page of its website information about the Livicom system and to instruct sales managers on how to connect Livicom sites to STEMAX ML.

Then the security company can proceed by configuring STEMAX ML to receive events from the Livicom system.

5.2 CONFIGURE STEMAX ML TO RECEIVE EVENTS FROM LIVICOM SITES

The security company should create two receiver-transmitters in STEMAX ML:

1. A *Livicom Server* receiver-transmitter for data exchange between STEMAX ML and Livicom cloud platform (see 5.2.1).
2. A *TCP/IP* receiver-transmitter for direct data exchange between STEMAX ML and the hubs (see 5.2.2).

5.2.1 CREATE AND LAUNCH LIVICOM SERVER RECEIVER-TRANSMITTER

Follow these steps to create and launch the *Livicom Server* receiver-transmitter:

1) Click the button  on the toolbar **or** select *System devices* in the *Menu* in the main window of the *STEMAX Administrator* (see figure 5.2).

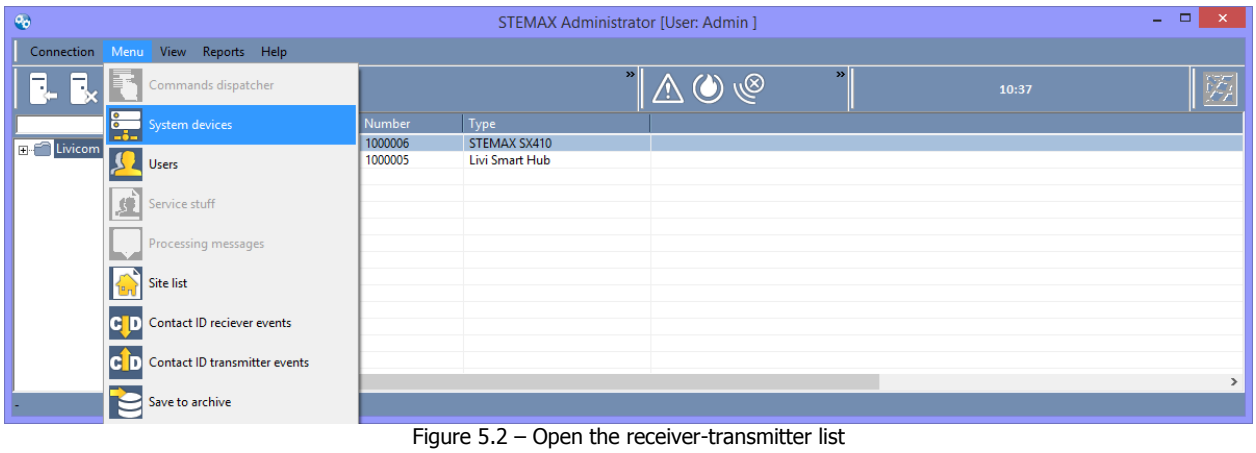


Figure 5.2 – Open the receiver-transmitter list

2) Right-click on the empty space in the *System devices* window and select *Create* (see figure 5.3).

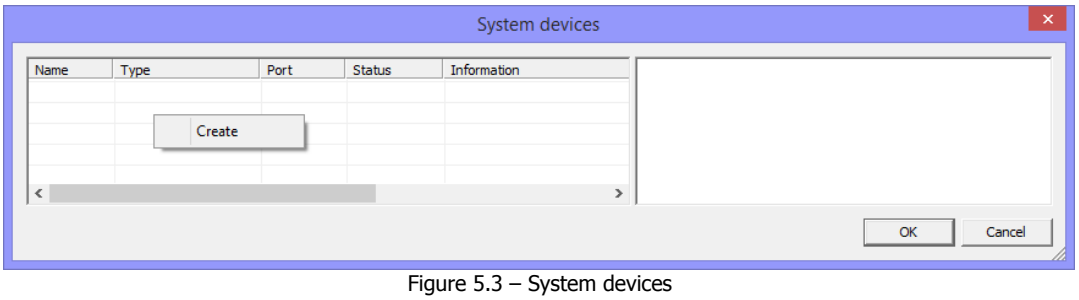


Figure 5.3 – System devices

3) Select the *Livicom Server* type and click OK (see figure 5.4).

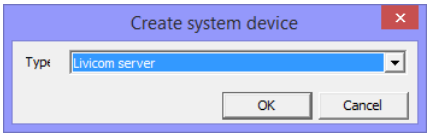


Figure 5.4 – Creating the *Livicom Server* receiver-transmitter card

4) The created *Livicom Server* receiver-transmitter card opens (see figure 5.5).

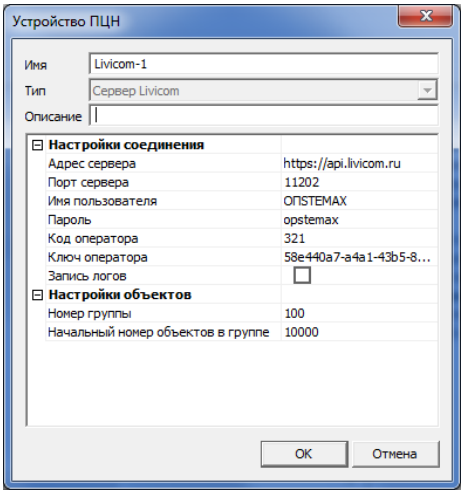


Figure 5.5. – System devices

For connecting to the Livicom platform, use the data provided by STELS to the authorized Livicom partner (see 5.1). Enter the following data in the receiver-transmitter card:

- *Server address* – the DNS-address of the Livicom cloud platform.
- *Server port* – the TCP/IP port for connecting the security company to the Livicom system.
- *Username* of the security company account on the Livicom platform.
- *Password* of the security company account on the Livicom platform.
- *Provider ID* – the unique identifier of the security company in the Livicom system.
- *Provider secret key* – the unique key for connecting the security company to the Livicom system.

- *Group number* - the number of the site group in STEMAX ML, to which the Livicom sites will be added automatically. The group with this number will be created automatically when the first Livicom site is connected to Stemax ML.
- *Initial site's number in group* – the number of the site in STEMAX ML, which will be assigned automatically to the first connected Livicom site. We recommend choosing the site number with a large offset relative to the numbers of already existing sites, e.g. 10000.

Click *OK* to save the data.

Then launch the receiver-transmitter that you've created. Right-click on the name of the receiver-transmitter and select *Start* in the context menu to launch it (see figure 5.6).

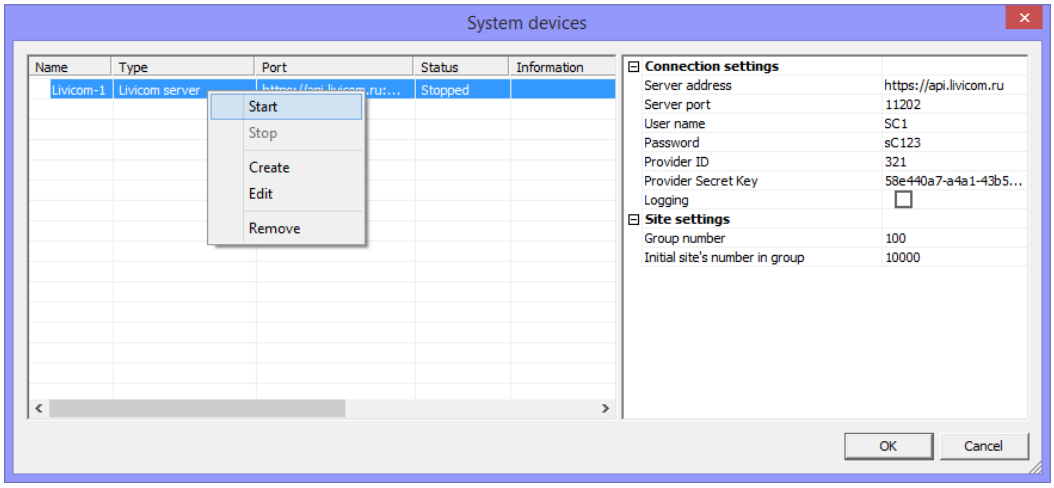


Figure 5.6 – System devices

Make sure that the *Livicom Server* receiver-transmitter is operating: the indicator next to the receiver-transmitter's name is green (see figure 5.7).

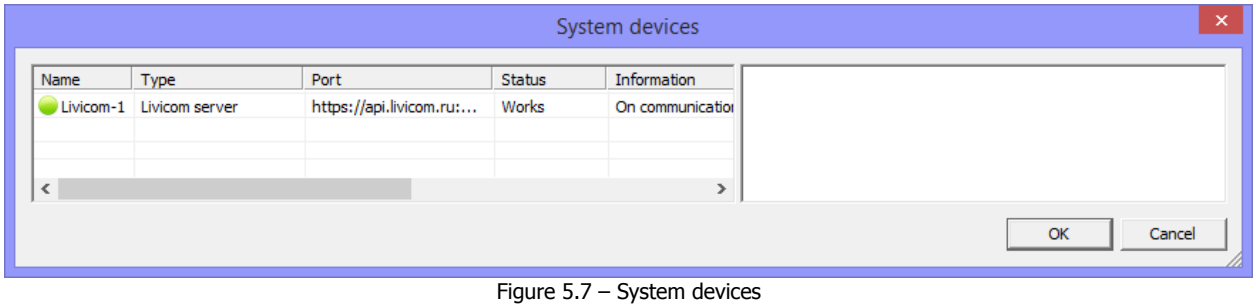


Figure 5.7 – System devices

We recommend creating and launching only one *Livicom Server* receiver-transmitter. Create two or more *Livicom Server* receiver-transmitters, if you need to configure data exchange between STEMAX ML and several cloud platforms.

5.2.2 CREATE AND LAUNCH TCP/IP RECEIVER-TRANSMITTERS

Thr 2G hubs can transmit alarm alerts and some auxiliary events directly to STEMAX ML (see *Appendix A* for the list of such events – p. 36). Follow these steps to set up the data exchange between the hubs and STEMAX ML:

1. Click the button  on the toolbar **or** select *System devices* in the *Menu* in the main window of the *STEMAX Administrator* (see figure 5.2).
2. Right-click on the empty space in the *System devices* window and select *Create* (see figure 5.3).

5) Select the *TCP/IP* type and click *OK* (see figure 5.8).

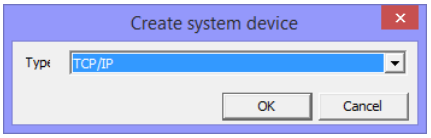


Figure 5.8 – Creating the *TCP/IP* receiver-transmitter card

The TCP/IP receiver-transmitter card is created. In the *Port* line (see figure 5.9), enter the *TCP/IP port*, which is dedicated to connect the hubs to STEMAX ML. Make sure that it's the same port that you provided to STELS during the authorization procedure (see 5.1).

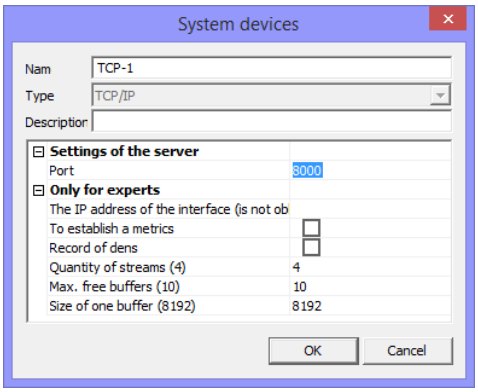


Figure 5.9 – the TCP/IP receiver-transmitter card

Click *OK*.

Then launch the *TCP/IP* receiver-transmitter that you've created. Right-click on the name of the receiver-transmitter and select *Start* in the context menu to launch it (see figure 5.6).

Make sure that the *TCP/IP* receiver-transmitter is operating: the indicator next to the receiver-transmitter's name is green.

Note – The data exchange between hubs and STEMAX ML will continue even if the connection between the Livicom platform and STEMAX ML has been interrupted. Lists of events transmitted by the Livicom platform and transmitted by the hub directly are given in the *Appendix A* (p. 36).

The interaction between the Livicom sites and STEMAX ML is set up. The connected hubs will be added to STEMAX ML automatically in the *Deactivated* state (connect the hubs as described in 8). All site data (name, address, devices and users) will also be loaded into the site card automatically.

6 SET UP INTERACTION WITH STEMAX CONTROLLERS

Follow these steps to set up the interaction between the STEMAX controllers and your monitoring system with the help of STEMAX ML:

1. Configure STEMAX ML to receive events from the STEMAX controllers.

The STEMAX ML administrator creates receiver-transmitters so that the STEMAX ML server could receive events from the controllers (see 6.1).

2. Configure STEMAX controllers to send events to the STEMAX ML.

Install a Stemax Configurator program and write connection settings to the controller (see 6.2).

After that the controllers will send events in real time to the STEMAX ML server via a TCP-IP channel (GPRS or Ethernet/Wi-Fi).

The structure of the interaction between the controllers and STEMAX ML is shown on the figure 5.1.

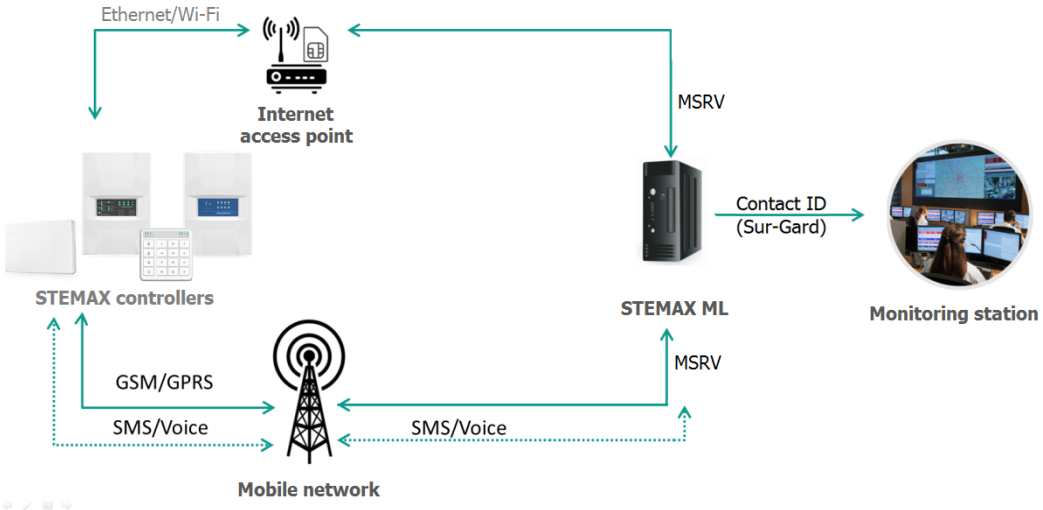


Figure 6.1 – The structure of the integration between the Livicom system and STEMAX ML

6.1 CREATE AND LAUNCH TCP/IP RECEIVER-TRANSMITTERS

Follow these steps to set up the data exchange between the controllers and STEMAX ML:

1. Click the button  on the toolbar **or** select *System devices* in the *Menu* in the main window of the *STEMAX Administrator* (see figure 5.2).
2. Right-click on the empty space in the *System devices* window and select *Create* (see figure 5.3).
3. Select the *TCP/IP* type and click *OK* (see figure 5.8).

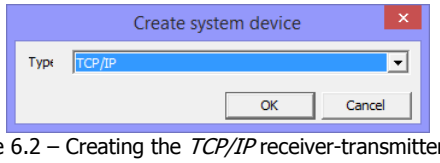


Figure 6.2 – Creating the *TCP/IP* receiver-transmitter card

The TCP/IP receiver-transmitter card is created. In the *Port* line (see figure 5.9), enter the *TCP/IP port*, which is dedicated to connect the controllers to STEMAX ML. Make sure that it's **NOT** the same port that you used for the hubs (see 5.2.2).

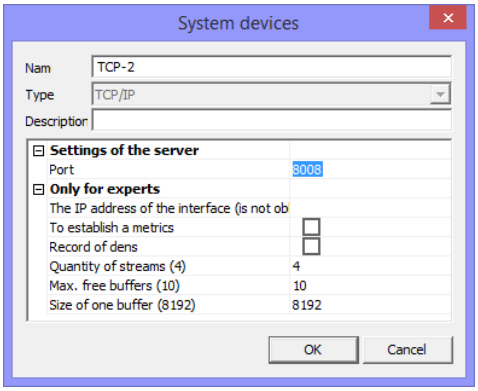


Figure 6.3 – the TCP/IP receiver-transmitter card

4. Click *OK*.

Then launch the *TCP/IP* receiver-transmitter that you've created. Right-click on the name of the receiver-transmitter and select *Start* in the context menu to launch it (see figure 5.6).

Make sure that the *TCP/IP* receiver-transmitter is operating: the indicator next to the receiver-transmitter's name is green.

Note – We recommend creating at least three TCP/IP receiver-transmitters so the controllers could stay online if one of the receiver-transmitters fails or becomes unavailable.

6.2 CONFIGURE STEMAX CONTROLLERS TO SEND EVENTS TO THE STEMAX ML.

The STEMAX Configurator program helps to configure the controllers and monitor their statuses. The Configurator is designed for personal computers running Windows OS. When installing the program for the first time on a PC, you must also install the following components:

- USB driver (required for correct connection of STEMAX controllers to a PC via USB interface);
- .NET Framework version 4.5.2 (required for the correct operation of the Configurator program).

Follow these steps to install all required components:

1. Download the installation package of the Configurator https://disk.yandex.ru/d/YHCoG8jGtQSIJQ.
2. After downloading, extract the installation file from the archive.
3. Run the installation file Configurator_pro_setup_4.31_En.exe. In some versions of Windows OS, it is recommended to run installation files as a system administrator to ensure correct installation.
4. In the installation dialogue leave all the checkboxes selected and click *Next*.

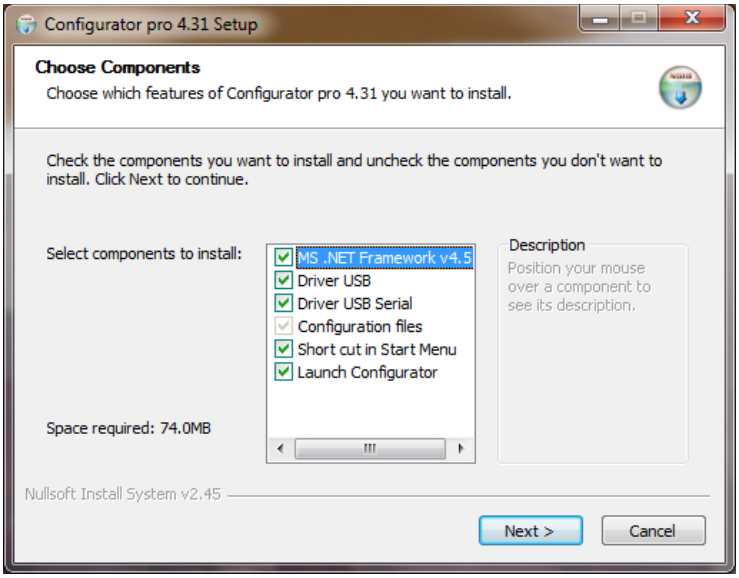


Figure 6.4 – Installation process

5. Specify the installation folder and click *Install*.

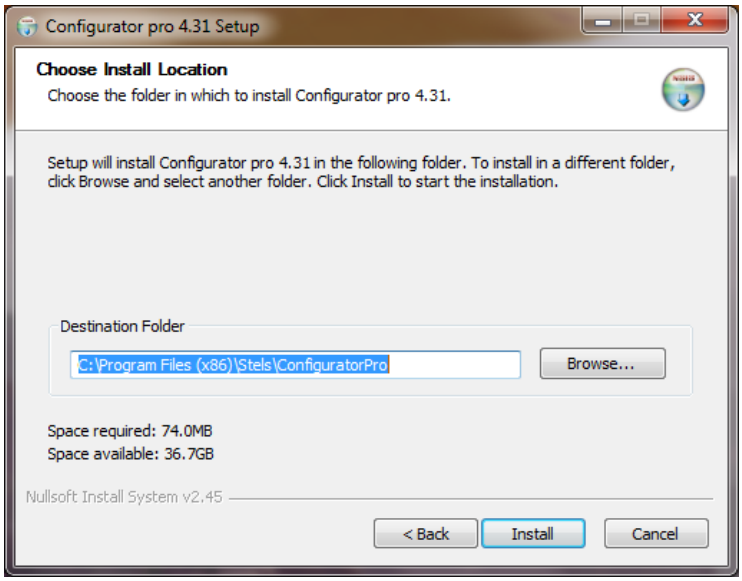


Figure 6.5 – Installation process

When running, the Configurator program will create files and subfolders in the folder in which its executable file is located. Make sure that writing to the selected folder is allowed.

Prepare the controller for configuration:

1) Supply the controller with power from a 230 V AC network or a 12 V battery. The battery can be purchased separately.

2) Connect the controller to a PC with the Configurator running using a USB cable.

The «New Connection Found» window will automatically open, displaying the type and serial number of the connected controller. Click ok to add the controller to the Configurator.

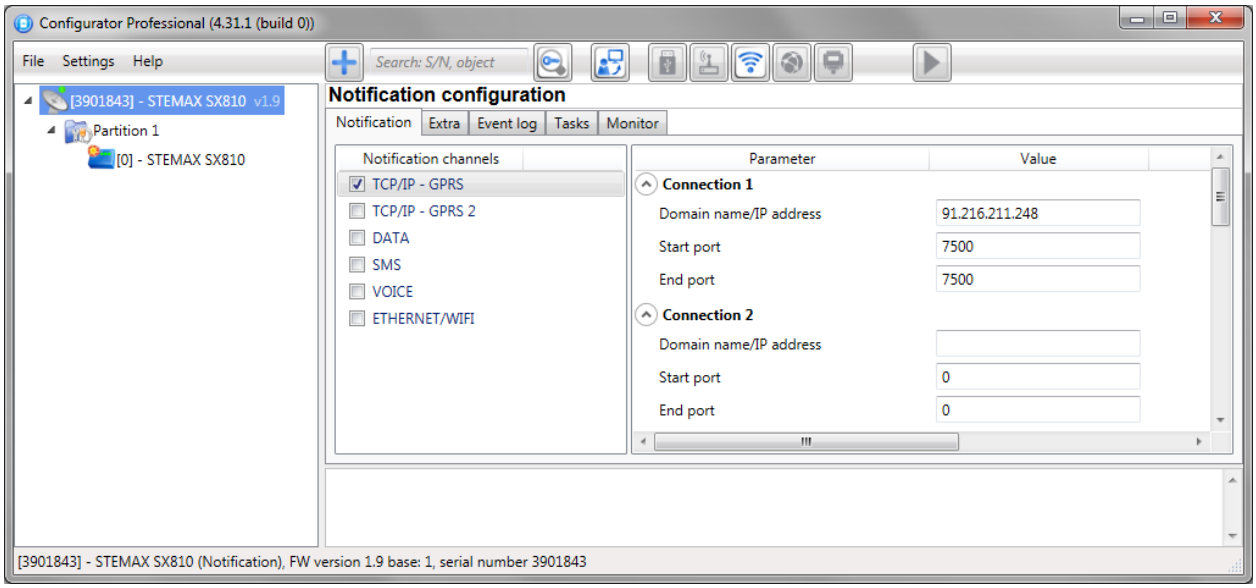


Figure 6.6 – Main window of the Configurator

Make sure that the connected controller is displayed on the left. Green dot near the serial number indicates that the connection between your PC and the controller is established.

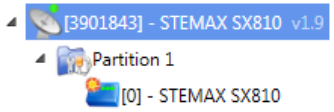


Figure 6.7 – Connection indicator

Press F5 to read the controller's configuration or use a context menu of the controller.

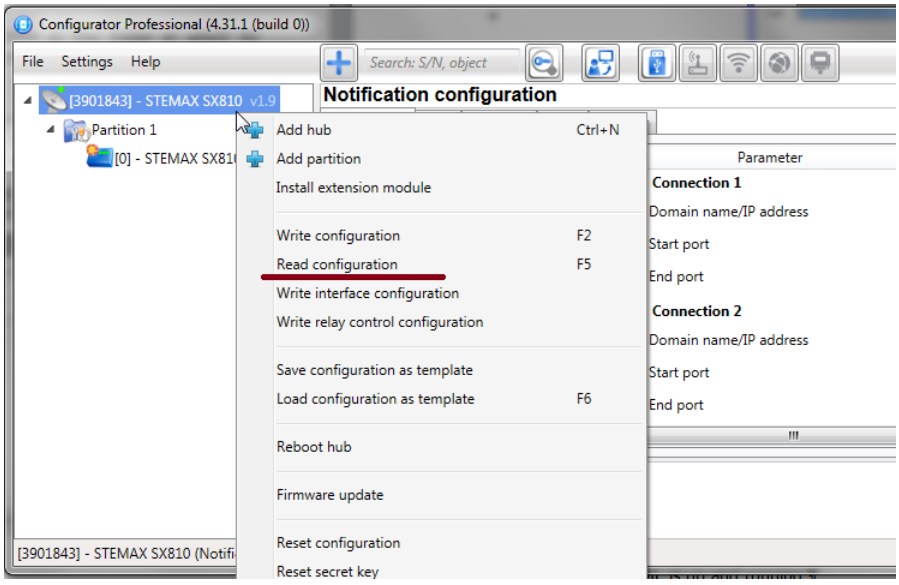


Figure 6.8 – Context menu of the controller

Next fill in the parameters on the "Notification" tab to connect the controller to the STEMAX ML.

6.2.1 NOTIFICATION CONFIGURATION

"Notification" tab allows to select and configure channels for sending notifications to the STEMAX ML server. The controllers have built-in 2.5G GSM / GPRS modems, in which two SIM cards should be installed. We recommend to choose sim-cards of different providers. SIM 1 will serve for the main communication channel and SIM 2 will serve as the backup. **Please, make sure that the controller carries no voltage before installing SIMs in their slots**.

Then you should activate the preferred transmission channel by checking its box in the "Notification channels" list. If the channel's name is not checked, then the channel can't be activated, even if all parameters are filled.

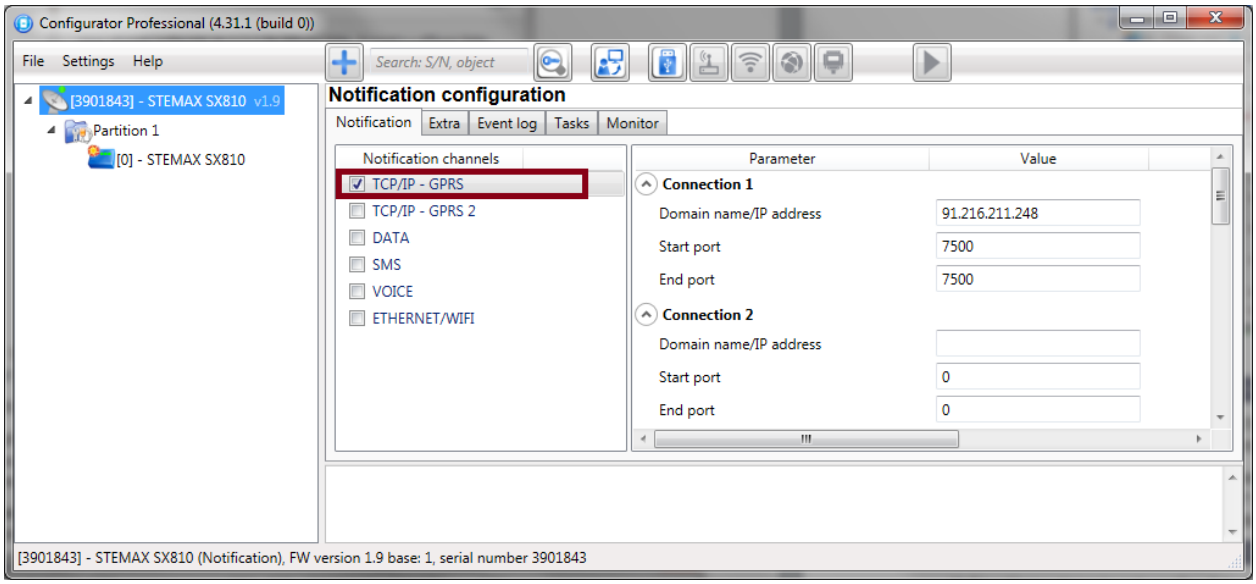


Figure 6.9 – Main window of the Configurator

The controllers support the following notification channels:

- **TCP/IP-GPRS**: data transmission to the Internet using the TCP/IP protocol via GSM wireless network ("mobile Internet").

  TCP/IP-GPRS is an **online** data transfer method. It allows to establish and maintain a constant connection between the controller and the server via "mobile Internet". The controller sends test events to the server regularly in order to check that the connection stays active. The test period is set on this tab in the "Test period, sec" parameter. The TCP/IP-GPRS is a **confirmable** channel: the STEMAX ML server sends a confirmation of successful data receipt to the controller.

- **SMS**: data transmission in SMS format via GSM wireless network.

SMS is an **offline** data transfer method. The SMS is a **non-confirmable** channel: no confirmation of successful data receipt can be sent over this channel.

- **VOICE**: voice calls from the controller to the GSM modem of the STEMAX ML server.

Note that no voice message can be provided during the call. The VOICE channel is aimed to confirm that the controller is on and operating in a situation when the server has stopped receiving test events from the controller via TCP/IP-GPRS channel (jamming control). The VOICE channel activation setting are also defined on this tab (check "VOICE" box in the "Notification channels" list).

If all three notification channels are checked on this tab, then the controller will follow two basic notification algorithms. The algorithms are designed according to the priority of event delivery. The first algorithm is designed for transmission of alarm events:

First round: TCP/IP-GPRS 1 -> SMS 1 -> SMS 2 -> TCP/IP-GPRS 2 -> Second round -> and so on.

Where 1 is for SIM 1, 2 is for SIM 2.

The execution of the algorithm stops once the controller receives the confirmation of successful data receipt from the server. Since the SMS channel is non-confirmable, the controller continues to execute the algorithm regardless SMS delivery state.

If during the first round the notification has not been delivered, then the second round starts with 120 seconds delay. The interval between subsequent rounds is prolonged (each time extended by 120 seconds) in order to save money. When the interval reaches 32 minutes, it stops expanding. New rounds repeat with the same interval until the delivery receipt is received.

For the first algorithm the priority is to ensure the data delivery in the shortest time possible. Alarm events include:

- Security alarm;
- Fire alarm;
- Arm / Disarm under duress;
- Possible jamming of the controller's communication channels.

All other events recorded by the controller are called system events. For system events, the second algorithm is designed:

First round: TCP/IP-GPRS 1 -> TCP/IP-GPRS 2 -> SMS 2 ->Second round -> and so on.

The controller sends SMS only via SIM 2 when notifying about system events. The interval between rounds is prolonged (each time extended by 120 seconds) in order to save money. When the interval reaches 32 minutes, it stops expanding. New rounds repeat with the same interval until the delivery receipt is received.

The implementation of algorithms in each situation depends on the settings recorded for the controller on this tab.

The controller switches to SIM 2 once a month to keep the SIM active and avoid its blocking by the provider. The controller returns to SIM 1 after transmitting one test event to the server and receiving the confirmation receipt.

6.2.2 TCP/IP – GPRS

Check the "TCP/IP - GPRS" box in the "Notification channels" list and fill in the parameters described below, if you want to activate the TCP/IP - GPRS channel.

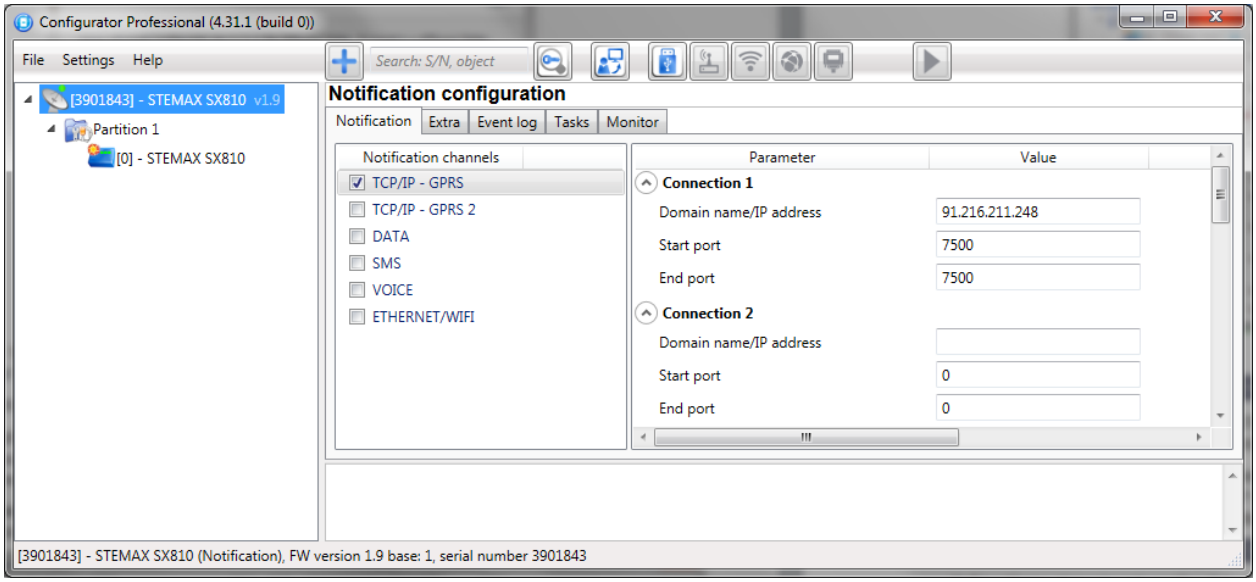


Figure 6.10 – Main window of the Configurator

Connection 1 and Connection 2: these blocks contain the parameters of the main and backup connections to the STEMAX server via the Internet.

Note that the main and backup connections can be implemented as separate connections to different server computers (main and backup STEMAX servers) or as separate connections to one server computer with two Internet access points.

Domain name / IP address: DNS address or external static IP address of the STEMAX server (if connected via external networks) **or** local static IP address of the STEMAX server (if connected via LAN).

Start port: the first TCP/IP port from the range used to connect controllers to the server.

End port: the last TCP/IP port from the range used to connect controllers to the server.

Note that the use of several TCP/IP ports helps to ensure the notification delivery. We recommend to open 2 to 4 TCP/IP ports on the server computer for data exchange with controllers. For each of these TCP/IP ports, you should to create a dedicated system device in the STEMAX Administrator program.

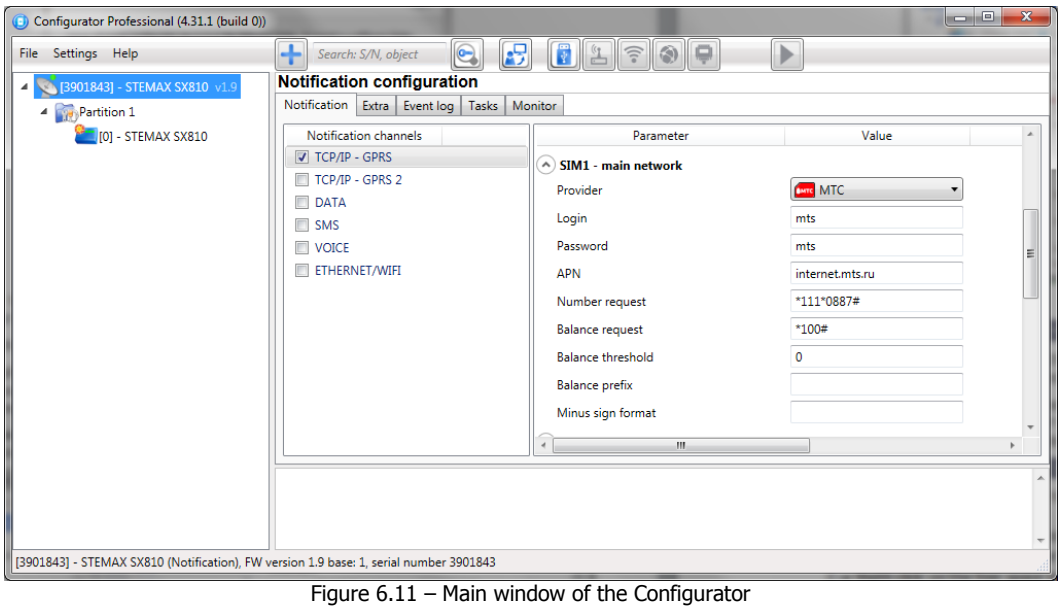


Figure 6.11 – Main window of the Configurator

SIM1 - main network and SIM2 - backup network: these blocks contain the parameters for connecting to the GPRS service on the SIM cards and for setting up SIM card balance control.

Provider: a drop-down list that allows you to quickly set up the access to the GPRS service ("mobile Internet") for the well-known providers. If you use services of the provider that is not in the list, then you should fill all the parameters below manually. Ask your provider for correct values.

Login: login for access to the "mobile Internet" service.

Password: password for access to the "mobile Internet" service.

APN: URL of the access point to the "mobile Internet" service.

Number request: the command for requesting the phone number of the SIM card (USSD request). Click the "+" button to see the default USSD request for the selected provider.

For setting up SIM card balance control, fill in the following parameters for each SIM:

Balance request: the command for requesting financial balance of the SIM card (USSD request). Click the "+" button to see the default USSD request for the selected provider.

Balance threshold: specify the level of the financial balance (in tariff monetary units). Each time the controller requests the financial balance, it will compare the value to the threshold. Once the value drops below the threshold, a notification will be sent to the STEMAX server.

Note that the controller requests the financial balance once a day, so we recommend taking into account the average daily costs when setting the balance threshold.

If the controller is rebooted / restarted, the controller will send the first balance request in 5 minutes (5 min after switching on).

Balance prefix (optional): a part of the SMS sent by the provider in response to the balance request. Enter the symbols that are shown right before the balance value (helps to identify the value in non-standard texts).

Minus sign format (optional): enter the symbols that show negative value of the financial balance (helps to identify a negative value in non-standard texts).

Connection control block contains parameters for the connection activity control.

Test period, sec: period for sending test events via TCP/IP-GPRS channel.

Jamming control: enabling/disabling the jamming control of the controller's communication channels. Enable the jamming control function, if you want to quickly detect signal loss from the controller over all activated communication channels. If the function is enabled, the controller makes test calls via the VOICE channel when test events can no longer be delivered via TCP/IP-GPRS channel using SIM 1 - main network. If the server does not receive any VOICE calls from the controller, then a "Possible Jamming" event is generated.

Note that the "Possible Jamming" event cannot be generated if you haven't filled in the "Create event "Possible jamming" parameter in the STEMAX Administrator program for the corresponding Site ("Additional parameters" tab).

Return on main network: the period for return to the main GSM network. When the controller cannot send test events via SIM 1, it switches to SIM 2 to establish and maintain the connection using backup network. But the controller will try to switch back to the main network regularly. Set the period for such tries in this parameter (e. g. every 2 hours).

6.2.3 SMS

Check the "SMS" box in the "Notification channels" list and fill in the parameters described below, if you want to activate the SMS channel.

SIM1 - main network -> Phone 1: telephone number of the GSM modem of the STEMAX server, which is dedicated to receive data from the controller's SIM 1.

SIM2 - backup network -> Phone 1: telephone number of the GSM modem of the STEMAX server, which is dedicated to receive data from the controller's SIM 2.

6.2.4 VOICE

Check the "VOICE" box in the "Notification channels" list and fill in the parameters described below, if you want to use voice calls from the controller to the STEMAX server to detect possible jamming.

SIM1 - main network -> Phone 1, Phone 2: telephone numbers of the GSM modems which are dedicated to receive test calls from the controller's SIM 1. If STEMAX server has only one GSM modem for test calls, then enter its number in the Phone 1 parameter.

SIM2 - backup network -> Phone 1, Phone 2: telephone numbers of the GSM modems which are dedicated to receive test calls from the controller's SIM 2 (the calls are performed only if SIM 1 cannot be used).

Connection control -> Test period, min: period of VOICE test calls.

6.2.5 RECORDING SETTINGS TO THE CONTROLLER

Record the new parameters to the controller's memory after filling this tab. Make sure that the controller is connected to your PC via the USB (locally). Then press the F2 key on your keyboard and wait for the Configurator to transfer new setting to the controller.

Disconnect USB interface from the controller. If TCP/IP-GPRS channel is enabled and configured, then the communication indicator on the front panel of the controller will stay green. If only SMS channel is activated, then the communication indicator will flash red (2 red blinks (0.25 s / 0.25 s), then pause for 3 s).

You can also check the GSM signal strength for the controller's active SIM. Open the controller's enclosure and press twice on the tamper button. The communication indicator and 1 - 4 indicators will display the signal strength by rapid blinks. Display scheme: one indicator blinks quickly - bad signal level; two indicators blink quickly - low level; three indicators blink - good level; four indicators blink - excellent level.

Double-click the tamper again to exit the display mode.

7 SET UP INTERACTION WITH MONITORING STATION

STEMAX ML receives events from STEMAX and Livicom sites encrypted in the MSRV protocol and re-encrypts them using the standard Contact ID (Sur-Gard) protocol.

Create and launch a Contact ID transmitter to set the data transfer to the third-party monitoring station (see 7.1). Set the correspondence of the events received from STEMAX and Livicom sites to the events sent to the third-party monitoring station in the *Contact ID transmitter events* table (see 7.2).

7.1 CREATE AND LAUNCH CONTACT ID TRANSMITTER

Follow these steps to set up the data transfer to the third-party monitoring station:

1. Click the button  on the toolbar **or** select *System devices* in the *Menu* in the main window of the *STEMAX Administrator* (see figure 5.2).

2. Right-click on the free space in the *System devices* window and select *Create* (see figure 5.3).
3. Select the *Contact ID transmitter* type and click *OK* (see figure 7.1).

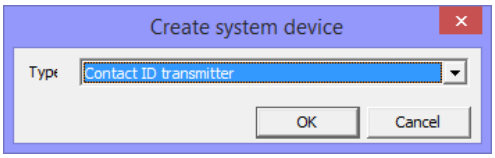


Figure 7.1 – Creating the *Contact ID transmitter* card

The *Contact ID transmitter* card is created. Fill the parameters described below and click *OK* in the *System device* window.

- *Name*: the name of the transmitter.
- *Description*: any user description of the transmitter.
- *Transport*: protocol for connecting the transmitter to STEMAX ML (TCP/IP or RS-232).
- For RS-232 connection protocol:
  - *Port*: number of the COM port to which the transmitter is connected.
  - *Speed*: the baud rate for the COM port.
  - *Data bits*: select 8.
  - *Evenness*: select *Empty*.
  - *Stop bits*: select 1.
- For TCP/IP connection protocol:
  - *Server address* – the IP-address of the third-party monitoring system server.
  - *Port*: the TCP/IP port for connecting to the monitoring system server.
- *Logging:* check the box if you want the operation protocol of the Contact ID transmitter to be kept. The operation protocol will be saved in the MS_ServerCOMX.log file (where X is the number of the COM port to which the transmitter is connected). The file can be found in the STEMAX ML installation folder. The protocol can be useful for troubleshooting.
- Protocol type: Contact ID protocol type: DCS Sur-Gard or Altonika-RS202BS.
- *Events table name:* the name of the table where the correspondence of Contact ID events and STEMAX ML events is set (see 7.2, p. 21).
- *Station testing period, sec:* the period of sending a test event to the receiving side to show that STEMAX ML is up and running.
- *Sites testing period [602], min:* the period of *the Contact ID Periodic test report (602) event formation.* The event informs the receiving side that the site is online.
- *Pause between site tests, msec:* the pause between sending two events *Periodic test report* (the function allows you to distribute the sending of events in time if they are simultaneously generated for a large number of sites).
- *Events queue length* (*It is not limited| 10 | 100 | 1000 | 10000*): maximum queue length of the events awaiting to be sent by the *Contact ID transmitter*. If the events queue length is exceeded, then old events will be deleted.
- *Replace partition 0 with partition No.:* the number of the partition that will represent partition 0.

Examples of the *Contact ID transmitter* settings are shown on the figure 7.2.

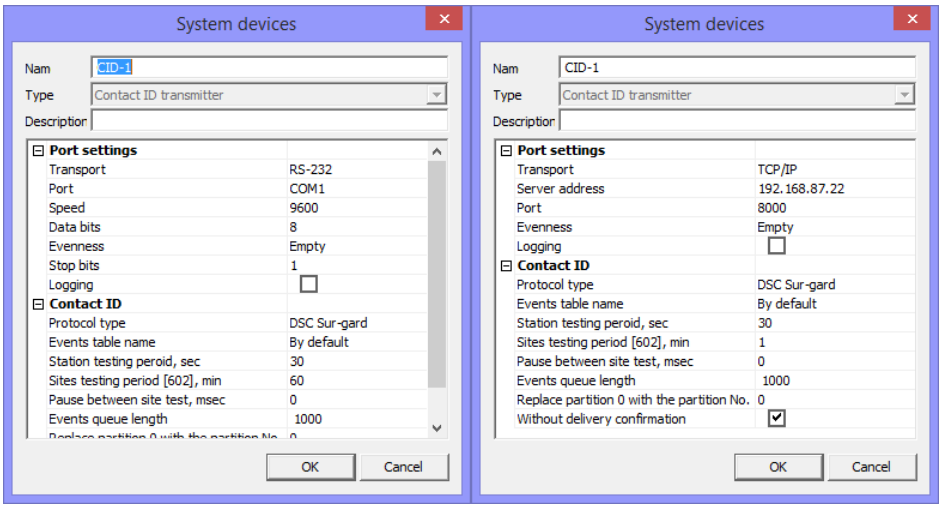


Figure 7.2 – System devices

Then launch the transmitter that you've created. Right-click on the name of the transmitter and select *Start* in the context menu to launch it (see figure 5.6).

We recommend creating and launching as many Contact ID transmitters as many third-party monitoring stations should receive events from STEMAX ML.

7.2 FILL IN CONTACT ID TRANSMITTER EVENTS

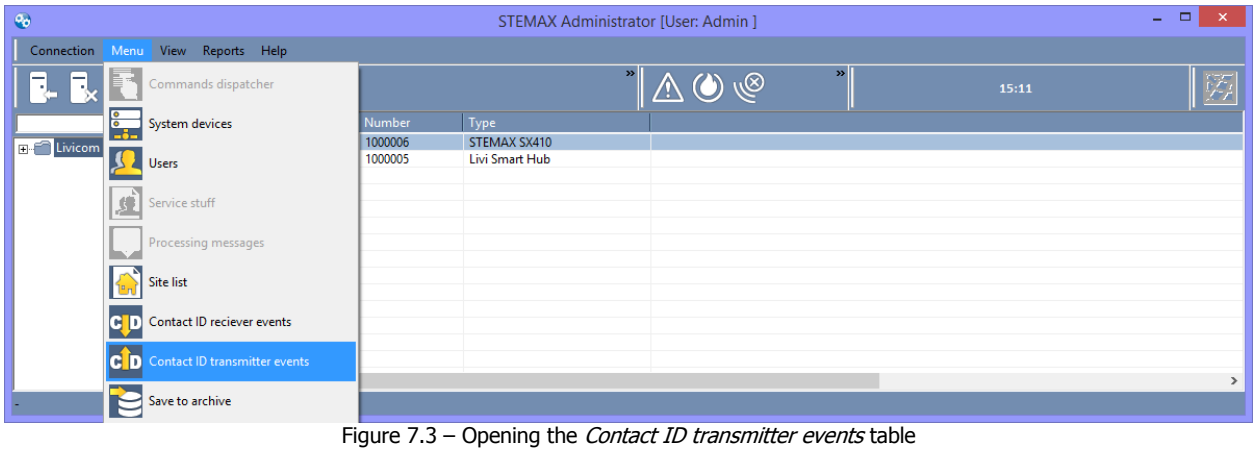


Figure 7.3 – Opening the *Contact ID transmitter events* table

Select *Contact ID transmitter events* in the *Menu* in the main window of the *STEMAX Administrator*.

The *Table* drop-down list allows you to choose between the available Contact ID transmitter events tables. You can make changes to the first table (*Default*) and create other tables (see figure 7.4).

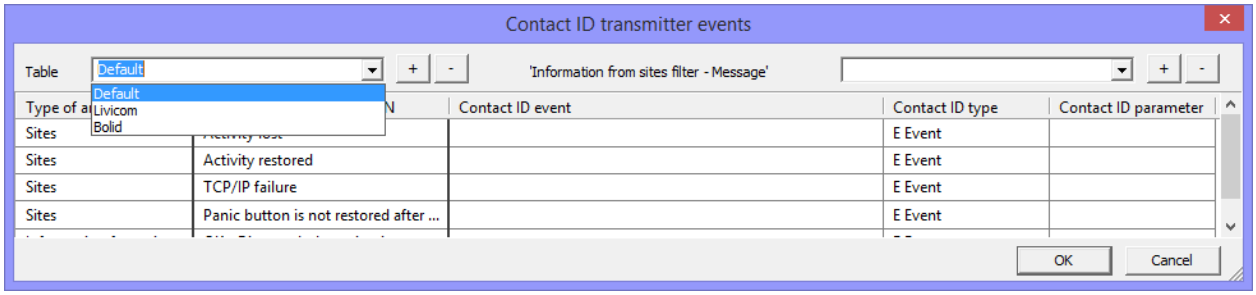


Figure 7.4 – Contact ID transmitter events table

In the *Table* field, it is displayed the name of the table, which you are editing. Click the button + to create a new table. Enter the name for the new table and click *OK* (see figure 7.5). The new *Contact ID transmitter* events table is created.

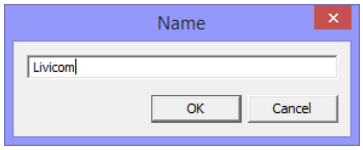
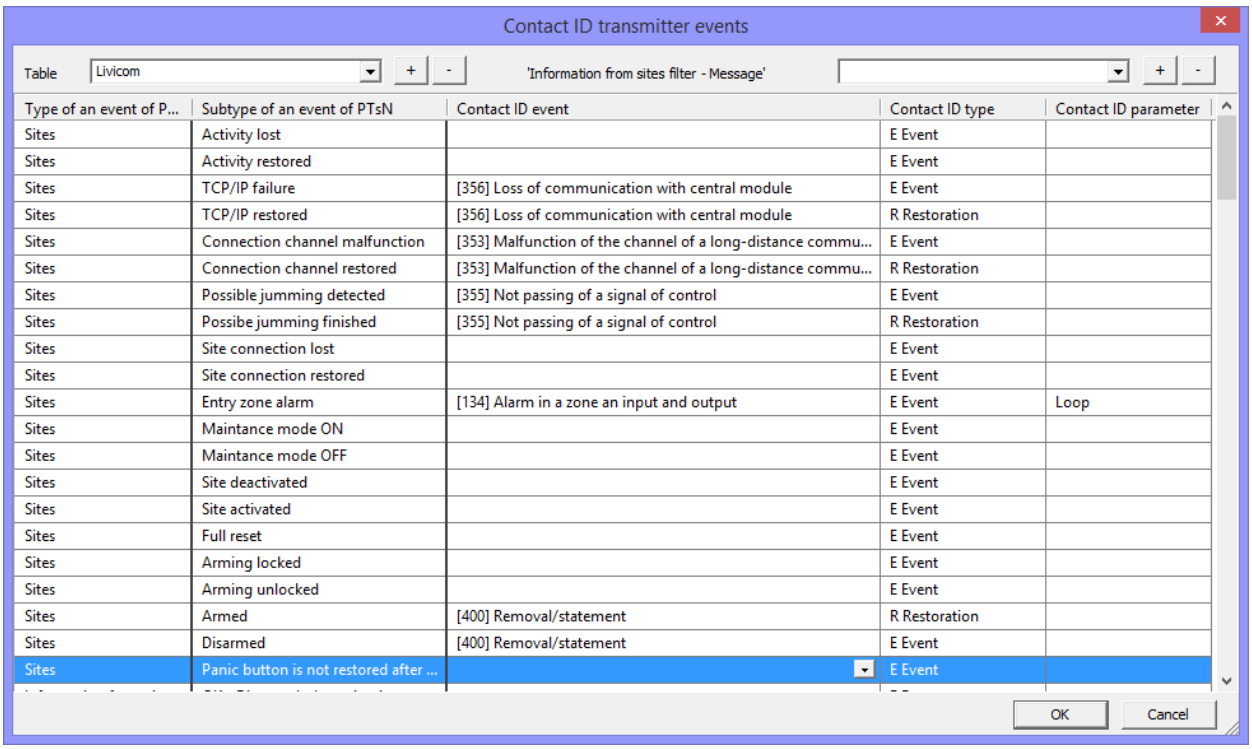


Figure 7.5 – Creating a new Contact ID transmitter events table

Click the button - to delete the table, which is currently open.

The appearance of the *Contact ID transmitter events* table is shown on the figure 7.6. The table contains the following columns:

- *Type of an event of PTsN:* STEMAX ML event type.
- *Subtype of an event of PTsN:* STEMAX ML event subtype.
- Cells in the columns *Contact ID event*, *Contact ID type*, *Contact ID parameter* are drop-down lists. Left-click on them to select one of the proposed values or no value (empty value).
  - *Contact ID event:* number and description of the Contact ID event.
  - *Contact ID type:* Contact ID event type (event or recovery).
  - *Contact ID parameter*: the parameter to which the event belongs (*Key* / *Loop* / *Section* / not selected).



Type of an event of P...	Subtype of an event of PTsN	Contact ID event	Contact ID type	Contact ID parameter
Sites	Activity lost		E Event	
Sites	Activity restored		E Event	
Sites	TCP/IP failure	[356] Loss of communication with central module	E Event	
Sites	TCP/IP restored	[356] Loss of communication with central module	R Restoration	
Sites	Connection channel malfunction	[353] Malfunction of the channel of a long-distance commu...	E Event	
Sites	Connection channel restored	[353] Malfunction of the channel of a long-distance commu...	R Restoration	
Sites	Possible jumming detected	[355] Not passing of a signal of control	E Event	
Sites	Possibe jumming finished	[355] Not passing of a signal of control	R Restoration	
Sites	Site connection lost		E Event	
Sites	Site connection restored		E Event	
Sites	Entry zone alarm	[134] Alarm in a zone an input and output	E Event	Loop
Sites	Maintance mode ON		E Event	
Sites	Maintance mode OFF		E Event	
Sites	Site deactivated		E Event	
Sites	Site activated		E Event	
Sites	Full reset		E Event	
Sites	Arming locked		E Event	
Sites	Arming unlocked		E Event	
Sites	Armed	[400] Removal/statement	R Restoration	
Sites	Disarmed	[400] Removal/statement	E Event	
Sites	Panic button is not restored after ...		E Event	

Figure 7.6 – Contact ID transmitter events *table*

8 CONNECT LIVICOM SITES TO STEMAX ML

The contacts of the security company are posted in the Livicom app and on www.smartlivi.com, when the company has been authorized as the Livicom partner (see 5.1). Livicom clients can form a request for the security service in the Livicom app and send it to the selected security company. The procedure for selecting the security company, filling and sending the request is described in 8.1.

The security company receives the requests of the Livicom clients by e-mail and processes them. The company might carry out audits of the sites, install some additional equipment and take other actions that are traditionally taken by the company's specialists for new clients. If the agreement is reached, then the security company can accept the site for protection and activate the security service in the Livicom system as described in 8.3.

8.1 RECEIVE SECURITY SERVICE REQUESTS

The user of the Livicom app with the "*Owner*" role[1] initiates the connection of the security service directly in the Livicom app.

Open the home screen of the site, tap on the ⚙ icon in the upper right corner and then tap on the *Guard* to select the security company to connect to (see figure 8.1).

[1] The owner of the site is the Livicom app user who have registered the hub in the app.

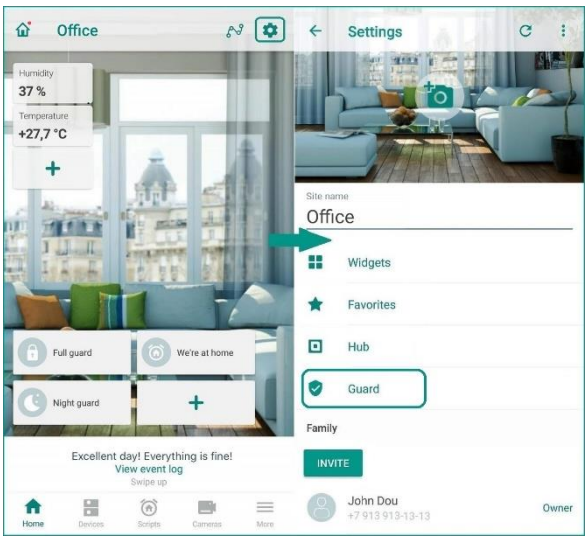


Figure 8.1 – Selecting the security company

You will see the City of service delivery and the list of security companies that offer security services for Livicom sites in the city (see figure 8.2).

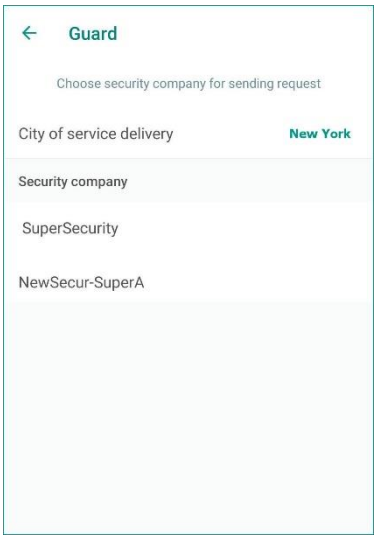


Figure 8.2 – Guard screen

The city of service delivery is detected automatically by the geolocation of the hub when the site's owner registers the hub on the Livicom server (and creates the site).

If the city is detected incorrectly, then tap on the "City of service delivery" line to change it. Start taping the name of your city in the field at the top of the screen. Then select your city from the filtered list and you'll be redirected back to the "Guard" screen.

The list on the "*Guard*" screen will be updated to display all the security companies that offer the security service for Livicom sites in your city. Select one of the companies and tap on its name to proceed with the service request.

You will see the pre-filled request form that will allow you to request the connection to the security company (see figure 8.3).

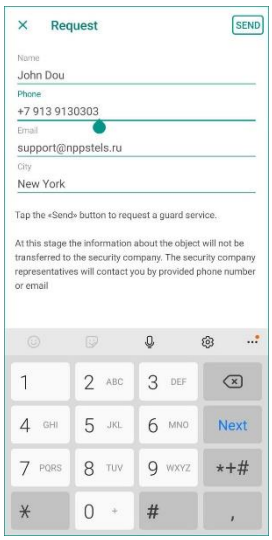


Figure 8.3 – Sending the security service request

The data is imported automatically from your Livicom account. You can edit the data if something has changed. Check thoroughly your email and phone number and tap on "*SEND*" in the upper right conner to send the request.

The request will be sent to the security company by email. In the event log, you will see the entry, which will contain the name of the security company and the date when you have sent the request (see figure 8.4).

Figure 8.4 – Site event log

You can send requests to as many security companies as you like.

The security company receives security service requests from Livicom clients by e-mail (the e-mail that has been provided to STELS during the authorization procedure - see 5.1).

The email will contain the following information:

- Name of the Livicom site's owner and contact info (e-mail and phone).
- City, in which the site is located.
- *Refuse to provide the security service for the site* button. The client request will be rejected, if an employee of the security company clicks on this button. The client will receive the push-notification about the rejection (see 8.2).
- *Agree to provide the security service for the site* button. The company can confirm that it is ready to protect the site by clicking on this button (see 8.3).

8.2 REJECT REQUESTS

The client request will be rejected, if an employee of the security company clicks on the *Refuse to provide the security service for the site* button. The client will receive the push-notification about the rejection (see figure 8.5).

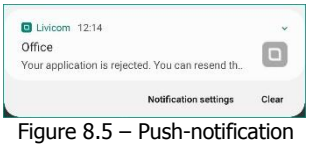


Figure 8.5 – Push-notification

The corresponding entry will appear in the event log. The entry will contain the date and time of the reply (see figure 8.6).

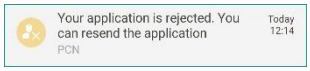


Figure 8.6 – Site event log

The request sent to this company will be canceled.

8.3 ACCEPT SITES FOR PROTECTION

The security company receives the requests of the Livicom clients by e-mail and processes them according to the internal regulations of the company. For example, the company might carry out audits of the sites, install some additional equipment and take other actions that are traditionally taken by the company's specialists for new clients.

If the agreement is reached, then the security company can accept the site for protection. Open the e-mail with the request of the Livicom client and click the button to confirm that the company is ready to protect the site (see 8.1).

The client receives the push-notification in the Livicom app (see figure 8.7).

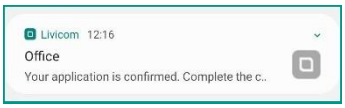


Figure 8.7 – Request confirmation push-notification

The corresponding entry will appear in the event log. The entry will contain the date and time of the reply (see figure 8.8).

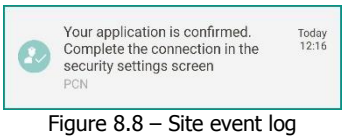


Figure 8.8 – Site event log

The client goes to the "*Guard*" screen in the Livicom app, opens the confirmed request and clicks the *Connect* button to connect the site to the server of the security company (see figure 8.9).

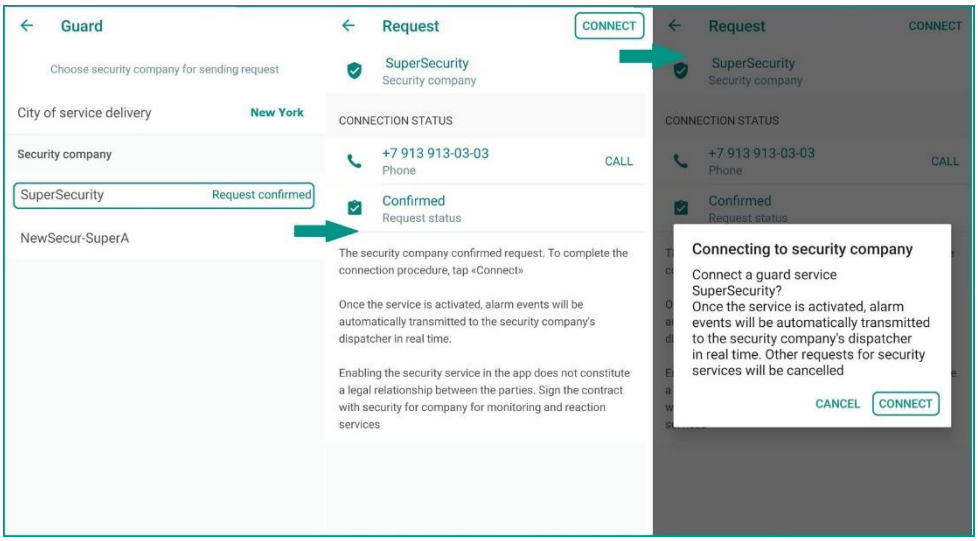


Figure 8.9 – Connecting to the security company

In the pop-up window, tap again on the "*Connect*" (see figure 8.9). The hub will establish the connection to the server of the security company. During the connection process, the hub receives and saves the IP-address and TCP/IP port of the STEMAX ML server, which were provided by the security company during the authorization procedure as the Livicom partner (see p. 5.1).

Note – The Livicom platform will not be able to provide automatic connection of the hub to the security company, if the server of the security company is not online at the moment of the connection establishment. In this case, the request for the security service will return to the "*Confirmed (awaiting user connection)*" status. Contact the security company to resolve the connection problem. Wneh the connection with the main STEMAX server is restored, the client opens the confirmed request in the *Livicom app* and clicks the *Connect* button again (see figure 8.9).

Then your requests for the security service in other companies will be canceled automatically, and the security service will go into the "*Waiting for activation*" status.

The corresponding entry will appear in the event log. The entry will contain the date and time of the connection (see figure 8.10).

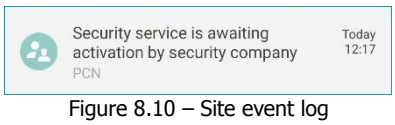


Figure 8.10 – Site event log

An e-mail is automatically sent to the security company with the following information about the new site:

- Hub serial number;
- Site ID in STEMAX ML;
- User name in the Livicom app;
- User phone number;
- User e-mail;
- City, in which the site is located.

Two linked cards are automatically created in STEMAX ML:

1. Device card for the hub (see figure 8.11).
2. Site card for the Livicom Smart Home (see figure 8.12).

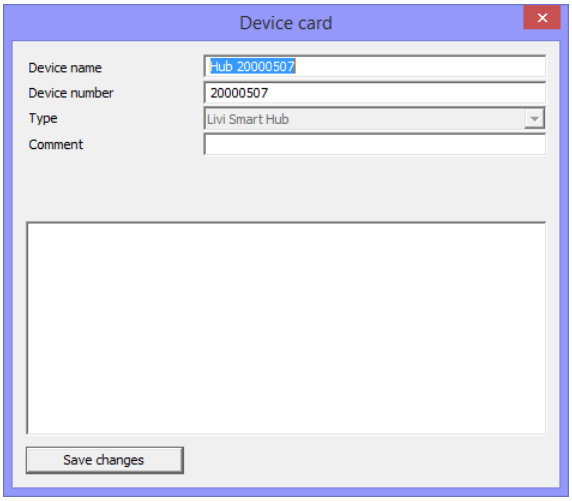


Figure 8.11 – Device card

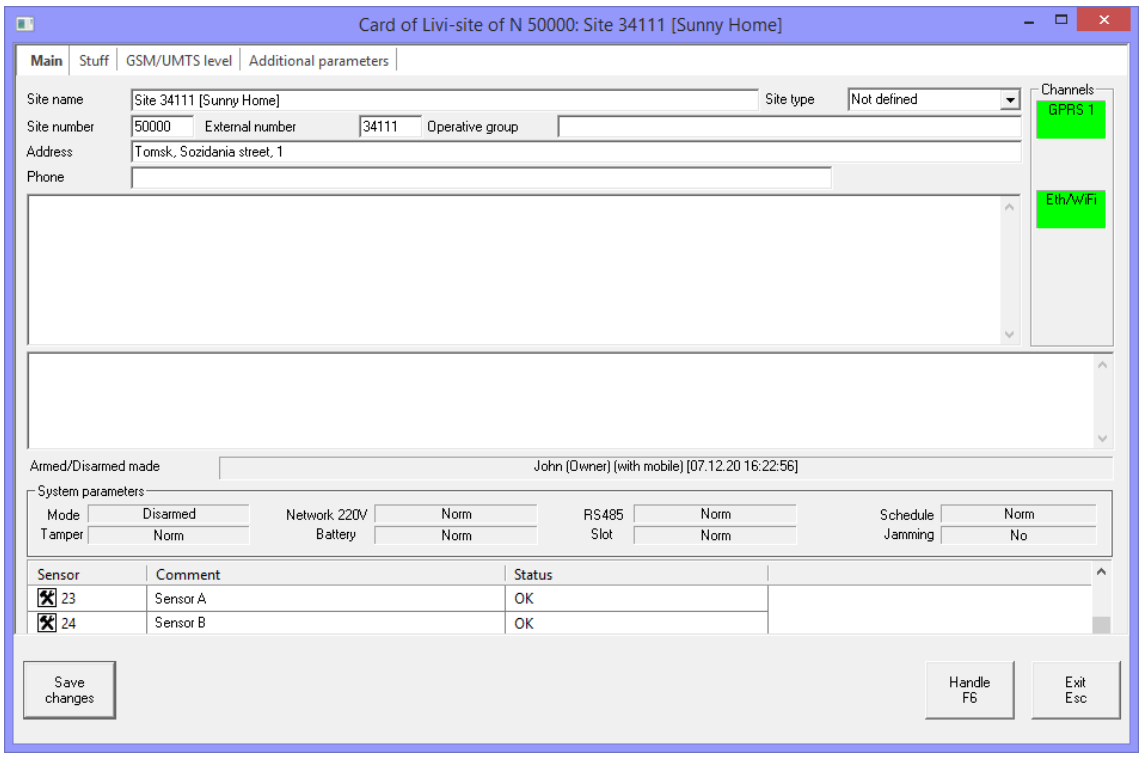


Figure 8.12 – Site card

Note – The new site is added to STEMAX ML in a deactivated state.

9 WORK WITH LIVICOM SITES

9.1 ACTIVATE LIVICOM SITES

Perform the following actions to activate the new site:

1. Run the *STEMAX Administrator* (MS_Admin.exe) as Administrator and connect it to the STEMAX server.
2. Find the Livicom group in the site tree (on the left side of the STEMAX Administrator main window).
3. In the group, find the site, whose identifier was specified in the e-mail.
4. Right-click on the site name and selects "*Activate*" in the context menu (see figure 9.1).

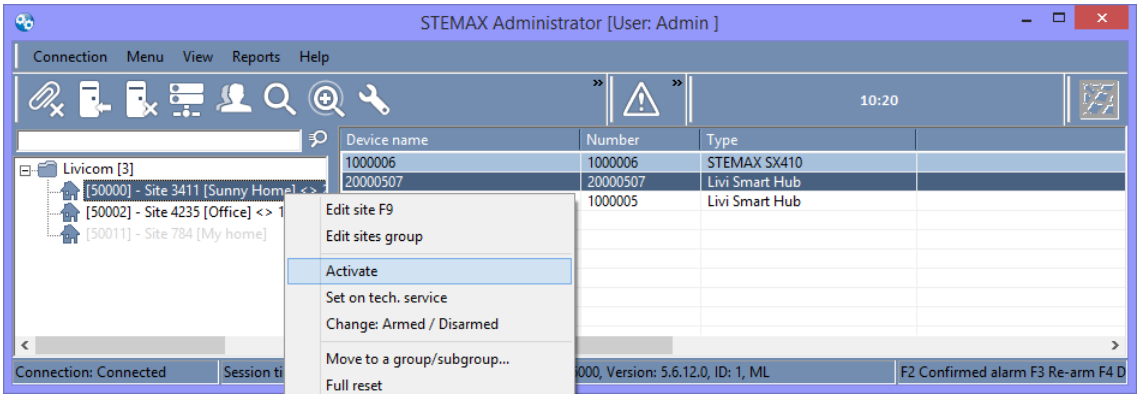


Figure 9.1 – Activating the site

The client will receive the push-notification that the security service is activated (see figure 9.2).

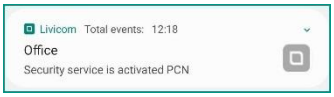


Figure 9.2 – Service activation push-notification

The corresponding entry will appear in the event log. The entry will contain date and time of the service activation (see figure 9.3).

Figure 9.3 – Site event log

The security service will switch to the *Active* status (see figure 9.4).

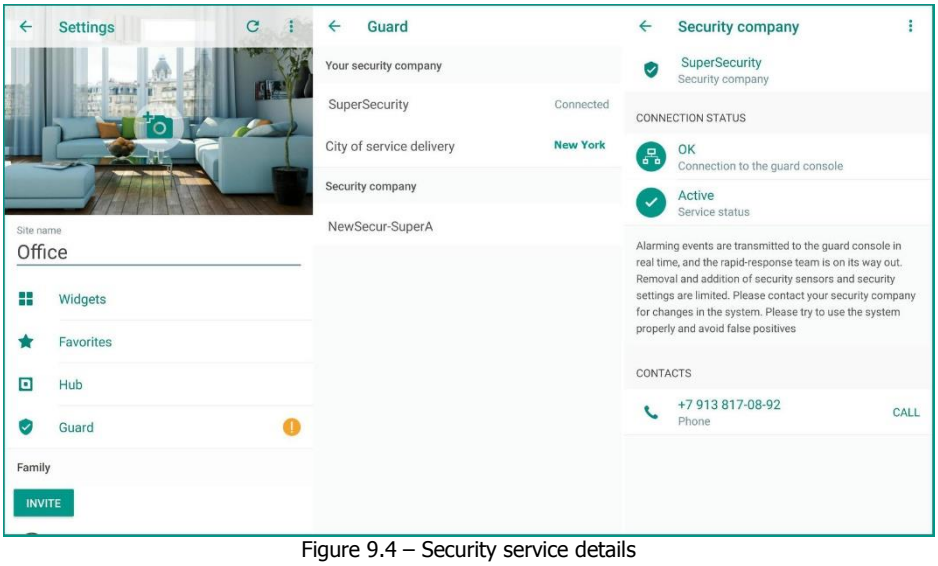


Figure 9.4 – Security service details

The name of the security company to which the site is connected will be displayed at the top of the security companies list in the Livicom app.

Note – Once the site is activated in STEMAX ML, the site users will not be allowed to add, remove or change settings of security, fire and emergency sensors in the Livicom app. To let the users perform the changes, put the site into the maintenance mode (see 9.3).

In case of an emergency at the site, the alarm signal will go to users' smartphones and to the security company at the same time (if the security service has the "Active" status). The list of transmitted alarm events is given in the *Appendix A* (p. 36).

9.2 CHECK SITE CARD

Each Livicom site has its card in STEMAX ML if it has been accepted for protection. The card contains the following information:

- general description of the site (its name in the Livicom system, address, etc),
- the list of devices connected to the hub,
- user list.

Open the site card by double-clicking the left mouse button on the site name in the site tree (on the left side of the STEMAX Administrator main window).

9.2.1 MAIN TAB

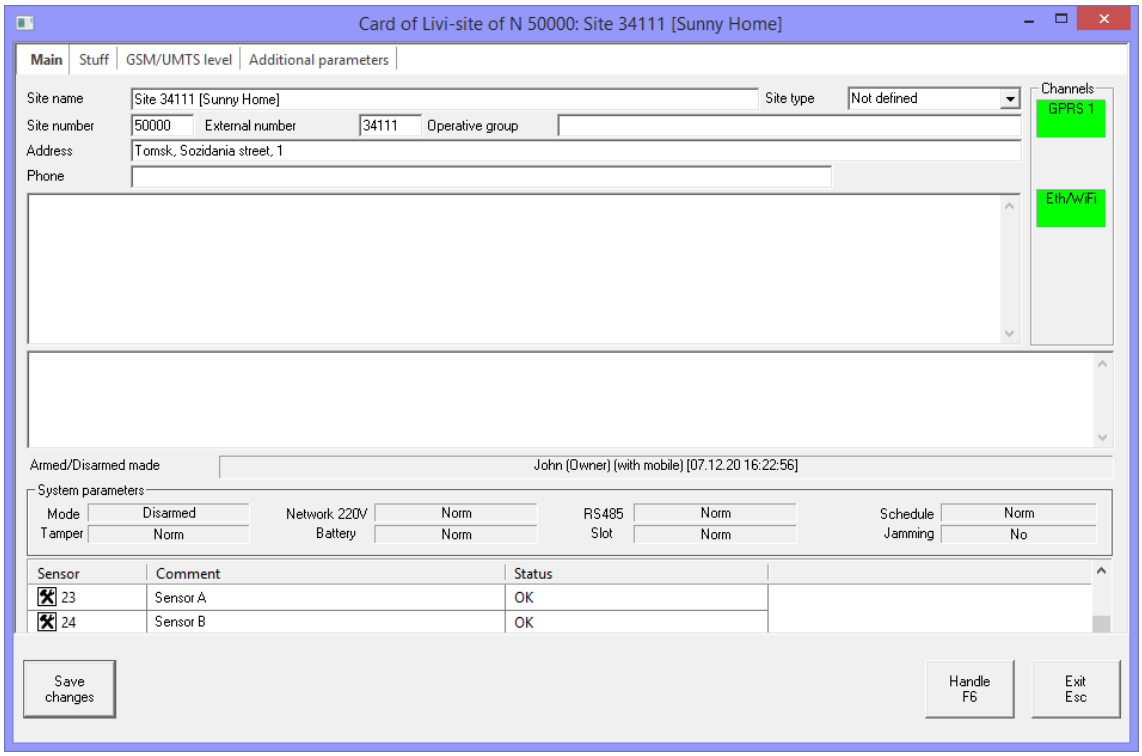


Figure 9.5 – Site card

The Main tab of the site card contains the following data:

- *Site name*: the name that the site's owner entered in the Livicom app. The name can be changed in STEMAX ML to make the site's identification easier: enter the new name and click on the *Save changes* button to save it.
- *Site type*: optional, the type can be set for information purposes.
- *Site number*: the number of the site in STEMAX ML.
- *External number*: the number of the site on the Livicom platform.
- *Operative group*: optional, a rapid response team can be appointed to the site.
- *Address*: the address that the site's owner entered in the Livicom app. The address can be changed or updated in STEMAX ML: enter the new address and click on the *Save changes* button to save it.
- *Phone*: primary contact of the site owner.
- *Description*: optional , any information about the site.
- *Comments*: optional, any information about the site.

The *Channels* block contains the **indicators of the hub communication channels statuses** (GPRS and Ethernet). If you want to hide or add one of the indicators, then configure its use on the *Additional parameters* tab (see 9.2.4).

The indicators can have the following colors:

- **green**: the connection is established;
- **red**: the connection is broken;
- **orange**: a failure is detected;
- **gray**: no data is being transmitted over the channel (or the parameters for detecting channel activity are configured incorrectly - see 9.2.4).

In the *Armed / disarmed made* field, the name of the user, who has been the last to enable/disable the guard of the site, and the time of this operation are displayed.

The *System parameters* block contains the following indicators of the hub current state:

- *Mode*: the current state of the site's guard (Armed / Disarmed).
- *Tamper*: the state of the hub enclosure (Norm / Failure)
- *Network 220 V*: the state of the hub 220 V power suppy (Norm / Failure).
- *Battery*: the state of the backup battery (Norm / Failure if the battery is absent or low).
- *RS-485*: RS-485 interface status (this indicator is always Norm for the hub).
- *Slot*: extension unit slot status (this indicator is always Norm for the hub).
- *Schedule:* this indicator is always Norm for the hub
- *Jamming*: suppression of communication channels at the site (No / Possible).

The lower part of the tab displays the list of devices installed at the site and their current state.

9.2.2 STUFF TAB

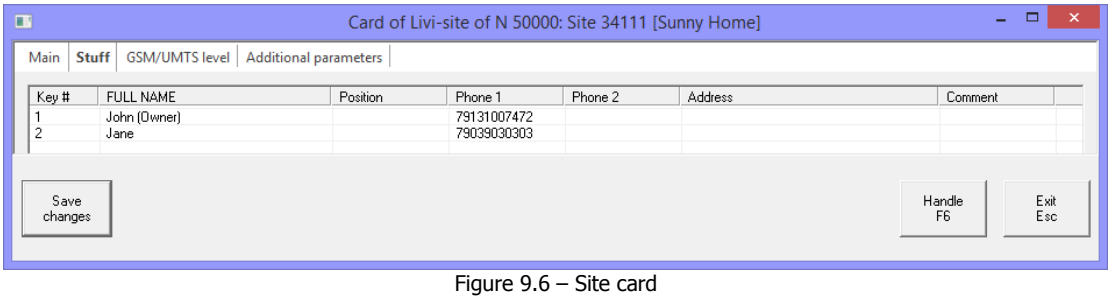


Figure 9.6 – Site card

The *Stuff* tab contains the list of users invited by the site's owner to control the site together:

- *Key #*: the number of the entry
- *Full Name*: the name of the user as recorded by the site's owner in the Livicom app.
- *Position*: the short description of the user's role.
- *Phone 1*: the user's first contact phone number.
- *Phone 2*: the user's second contact phone number.
- *Address*: the address of the user.
- *Comment*: any information about the user.

9.2.3 GSM/UMTS LEVEL TAB

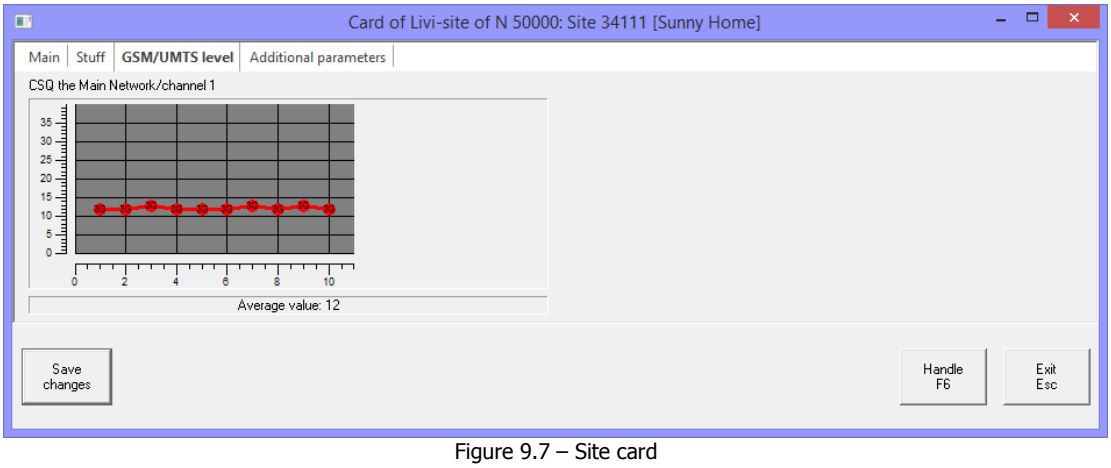


Figure 9.7 – Site card

The *GSM/UMTS level* tab graphically displays the strength of the GSM signal at the site (if a sim-card is installed in the hub).

9.2.4 ADDITIONAL PARAMETERS TAB

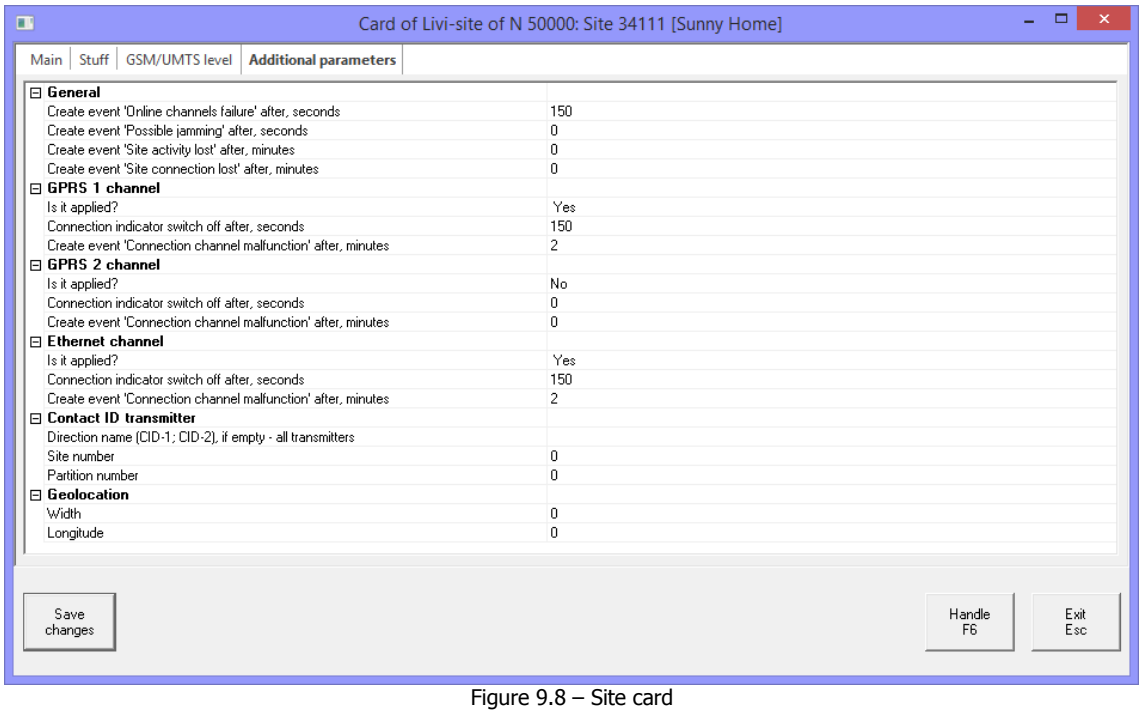


Figure 9.8 – Site card

General block

You can set the parameters for monitoring the status of both communication channels. Fill the parameters if you need to detect possible GSM suppression at the site.

Note – If the parameter is set to 0, then it is disabled (the events will not be generated).

- *Create event 'Online channels failure' after, seconds*: if STEMAX ML does not receive any test events from the hub during the time specified in this parameter, then the 'Online channels failure' event will be generated and sent to your monitoring station. The period should be 2–4 times longer than the test period for the communication channel. For example, the hub sends test events via Ethernet every 10 seconds, so the event might be useful to be generated in 35 seconds. For the GPRS channel, the test period is 25 seconds and the event should be generated in 90 seconds.
- *Create event 'Possible jamming' after, seconds*: if STEMAX ML has generated 'Online channels failure' event and the test events from the hub are still absent during the time specified in this parameter, then the 'Possible jamming' event will be generated and sent to your monitoring station. The period should be specified in seconds.
- *Create event 'Site activity lost' after, minutes:* if STEMAX ML has generated 'Possible jamming' event and the test events from the hub are still absent during the time specified in this parameter, then the 'Site activity lost' event will be generated and sent to your monitoring station. The period should be 2–4 times longer than the time period specified in the 'Create event 'Possible jamming' parameter. The period should be specified in minutes.
- *Create event 'Site connection lost' after, minutes*: control time of long-term communication losses on all channels. If during this time no events is received from the site via any of the used channels, then the 'Site connection lost' event is generated. The period should be 20–200 times longer than the test period for the communication channel. The exact time period of this parameter should be determined individually for each site, since this event might require the security company to respond (e.g. to send someone to the site to eliminate the malfunction). The period should be specified in minutes.

GPRS 1 channel, GPRS 2 channel, ETHERNET channel blocks

- *Is it applied?:* If the value *Yes* is selected, the status indicator of the channel is displayed on the *Main* tab.

- *Connection indicator switch off after, seconds:* timer for monitoring short-term communication losses for each channel. The connection state is shown by the indicator in real time. The period should be 2–4 times longer than the test period for the communication channel (25 seconds for GPRS and 10 seconds for Ethernet).
- *Create event 'Connection channel malfunction' after, minutes:* timer for monitoring long-term communication losses for each channel. The state is shown by the color of the card frame in the object field. The period should be 20–200 times longer than the test period for the communication channel.

Contact ID transmitter block

- *Direction name:* the name of the Contact ID transmitter, which will be used to send events from this site (see 7.1). Leave the parameter empty if you use only one Contact ID transmitter or if all Contact ID transmitters should send events from this site.
- *Site number*: the number of the site's controller to be transmitted to the third-party monitoring station.
- *Partition number*: the number of the controller's partition to be transmitted to the third-party monitoring station.

Geolocation block

- *Width*: the latitude of the site's location.
- *Longitude*: the longitude of the site's location.

Latitude and longitude of the site's location are determined by the Livicom system automatically. Click the Save changes button after making changes to save them.

9.3 PUT SITES INTO MAINTENANCE MODE

If the security service is in the *Active* status, then the users cannot connect new security, fire and auxiliary sensors to the hub or remove the connected ones. To let the users perform the changes, the dispatcher puts the site into the maintenance mode.

Follow these steps to put the site into the maintenance mode:

1. Find the site in the site tree (on the left side of the *STEMAX Administrator* window).
2. Right-click on the site name and select "*Set on tech.service*" in the context menu.

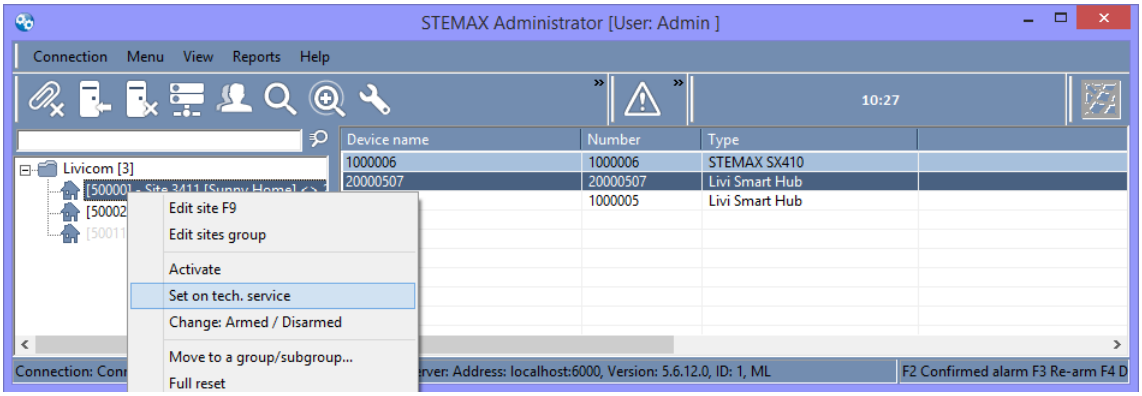


Figure 9.9 – Putting the site into the maintenance mode

The client will receive the push-notification that the security service is suspended for maintenance (see figure 9.10).

Figure 9.10 – Push-notification about the maintenance

The corresponding entry will appear in the event log. The entry will contain the name of the security company, date and time of the suspension for maintenance (see figure 9.11).

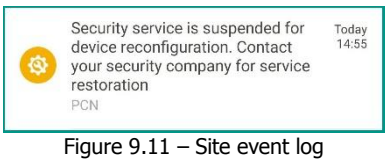


Figure 9.11 – Site event log

The user will be able to add and remove sensors and change the configuration of the security system. Information about all changes will be automatically uploaded to the site card in STEMAX ML.

Put the site back into the active mode using the context menu in the site tree of the *STEMAX Administrator* (see figure 9.12).

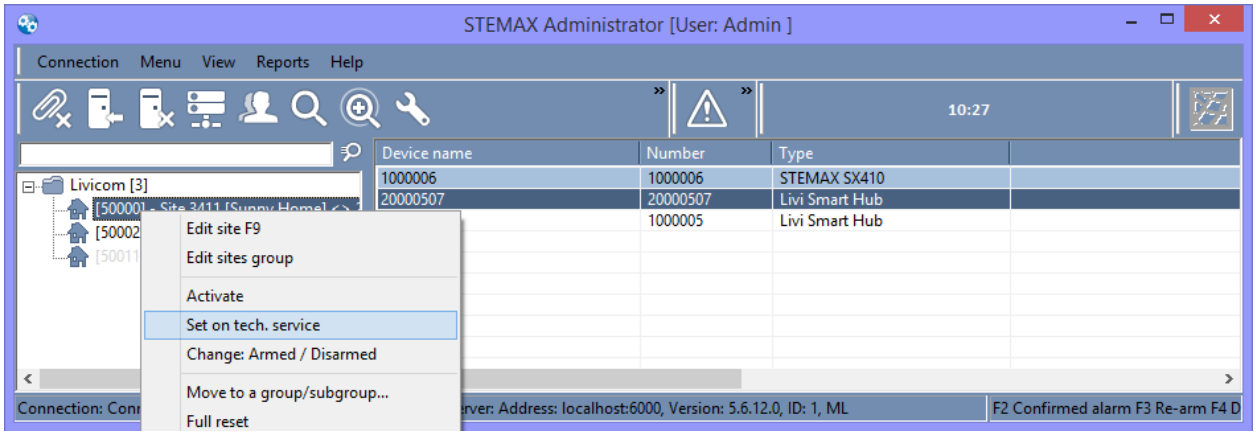


Figure 9.12 – Taking the site out of the maintenance mode

The client will receive the push-notification in the Livicom app that the security service is activated again, and a corresponding entry will appear in the event log in the app.

9.4 SUSPEND SECURITY SERVICE

Follow these steps to suspend the security service (e.g. in case of non-payment):

1. Run the *STEMAX Administrator* (MS_Admin.exe) as Administrator and connect it to STEMAX ML.
2. Find the site in the site tree (on the left side of the STEMAX Administrator main window).
3. Right-click on the site name and select "*Deactivate*" in the context menu.

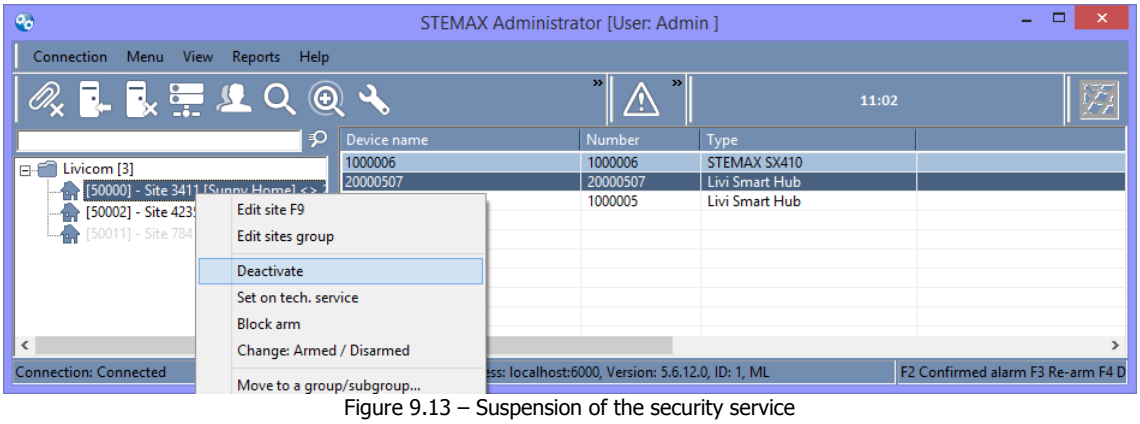


Figure 9.13 – Suspension of the security service

The client will receive the push-notification that the security service is suspended (see figure 9.14).

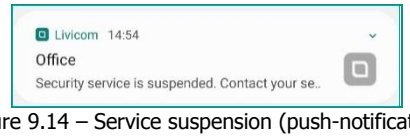


Figure 9.14 – Service suspension (push-notification)

The corresponding entry will appear in the event log. The entry will contain the name of the security company, date and time of the suspension (see figure 9.15).

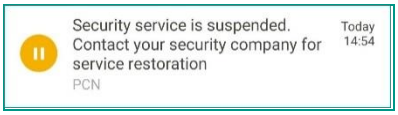


Figure 9.15 – Site event log

Put the site back into the active mode using the context menu in the site tree of the STEMAX Administrator (see figure 9.16).

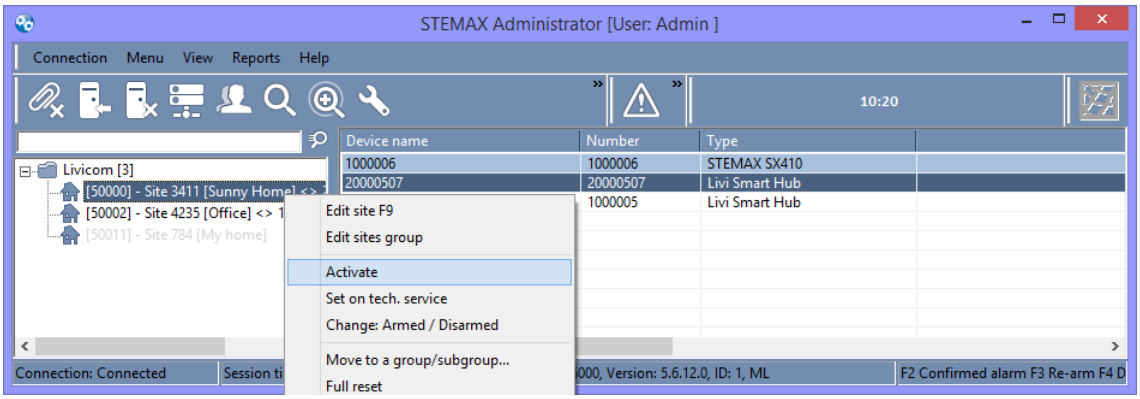


Figure 9.16 – Activating the site

The client will receive the push-notification in the Livicom app that the security service is activated again, and the corresponding entry will appear in the event log in the app.

9.5 DISABLE SECURITY SERVICE

9.5.1 THE CLIENT INITIATES THE SECURITY SERVICE DISABLING

Client follows these steps to initiate the security service disabling:

1. Opens the "Guard" screen in the Livicom app, taps on the 3-dots button ⋮ in the upper right corner of the screen and select "*Disconnect*" in the popup menu (see figure 9.17).

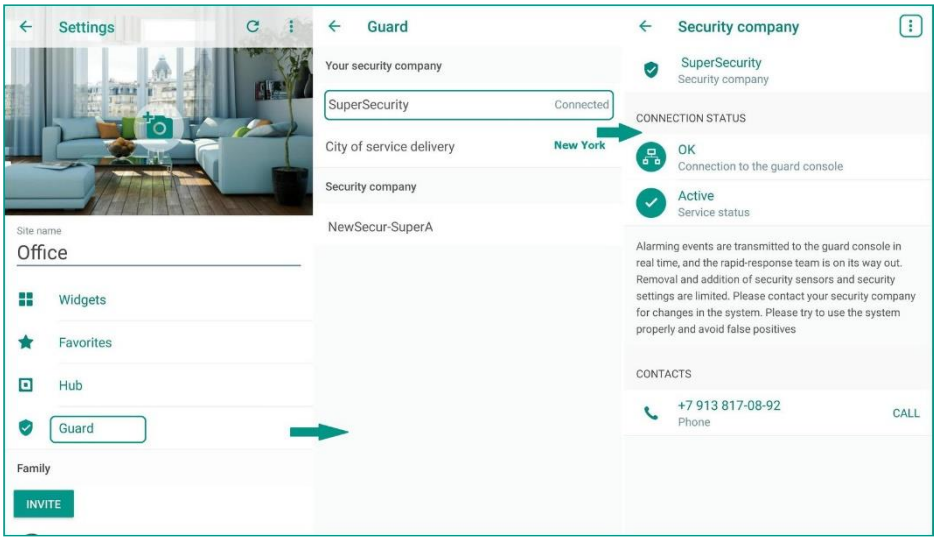


Figure 9.17 – Disconnecting from security company

2. Then confirm that you want to send the service termination request by tapping on the "*Send*" button in the pop-up window.

The request will be sent to the security company by email. In the event log, you will see the entry, which will contain the name of the security company and the date when you have sent the request (see figure 9.19).

The security company receives service termination requests from Livicom clients by e-mail (the e-mail that was provided to STELS during the authorization procedure - see 5.1).

The email will contain:

1. Information about the Livicom client and their contact details (e-mail and phone).
2. Site ID and hub serial number.
3. *Confirm service termination* button. Click this button if you agree to disconnect the Livicom site from Stemax server.

The security company will process the termination request according to the company's internal regulations. Then the security company can proceed by disconnecting the site from the company's server. Open the e-mail with the request of the Livicom client and click the button to confirm that the company agrees to terminate the service.

Then the following actions are automatically performed:

- the connection between the hub and the STEMAX software is broken,
- information about the hub is deleted from the STEMAX server,
- the site is switched to the *Deactivated* state[2]. The site users will receive the push-notification about the security service termination (see figure 9.18).

Figure 9.18 – Service termination push-notification

The corresponding entry will appear in the event log. The entry will contain date and time of the service termination (see figure 9.19).

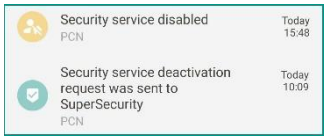


Figure 9.19 – Site event log

The message about the disabling of the security service is sent to the e-mail of the security company.

9.5.2 THE SECURITY COMPANY DISABLES THE SECURITY SERVICE

Delete the site from the STEMAX server to disable the security service. Follow these steps to delete the site:

1. Run the *STEMAX Administrator* (MS_Admin.exe) as Administrator and connect it to the STEMAX server.
2. Find the site in the site tree (on the left side of the STEMAX Administrator main window).
3. Right-click on the site name and select "*Delete site*" in the context menu (see figure 9.20).

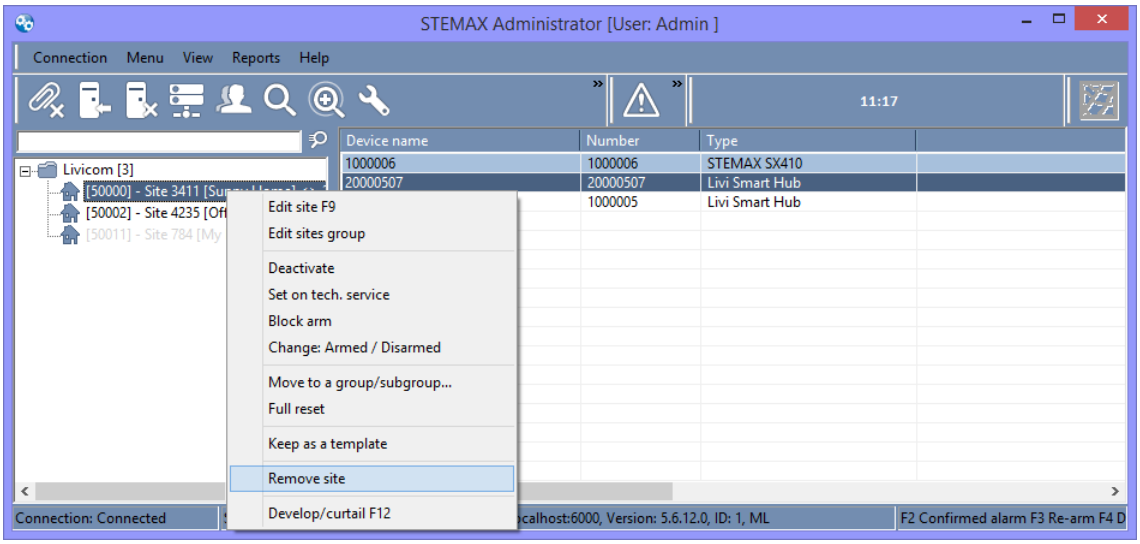


Figure 9.20 – Disabling the security service

The site users will receive the push-notification that the security service is disabled by the security company. The corresponding entry will appear in the event log. The entry will contain the name of the security company, date and time of the suspension.

[2] If the Livicom client connects to the security company again, the hub card will automatically link to the site card.

10 UPDATE STEMAX ML

Follow these steps to update STEMAX ML if you are using an outdated version of the software (STEMAX ML 5.6 or lower):

1. Run the *MS_ServiceML_Stop.bat* file as Administrator to stop the server. The file is located in the STEMAX ML installation folder (by default *C:|Program Files|MS_System_ML*).
2. Then run again the *MS_ServiceML_Uninstall.bat* file as Administrator to delete the old server.
3. Rename the *MS_System_ML* folder. Pick any different name for it. For example: *MS_System_ML_1*.
4. Install the new version of STEMAX ML as described in 3 (p. 4).
5. Then copy the following subfolders and files from the old STEMAX ML folder (from the renamed folder) to the new STEMAX ML installation folder (by default C:\Program Files\MS_System_ML):
   - *Data* and *XML* folders;
   - Licence (**.reg* file);
   - *ms_serverml.ini and ms_admin.ini* files.
6. Run the *MS_ServiceML_Start.bat* file as Administrator to initiate the service.
7. Launch *MS_Admin.exe*.

STEMAX ML is updated and running.

APPENDIX A – TRANSMITTED EVENTS

Events transmitted from the Livicom platform to STEMAX ML:

- Site add / edit / delete
- Stuff add / edit / delete
- Device add / edit / delete

Events transmitted from STEMAX ML to the Livicom platform:

- Site under maintenance
- Site deactivated
- Site activated (including removed from maintenance)
- Site deleted

Events transmitted directly from the hub to STEMAX ML:

- Livi MS motion sensor alarm / ok / connection lost / low battery
- Livi MSW motion sensor alarm / ok / connection lost / low battery
- Livi FS smoke sensor alarm / ok / connection lost / main battery low / backup battery low
- Livi CS opening sensor alarm / ok / connection lost / low battery
- Livi CSM opening sensor alarm / ok / connection lost / low battery
- Livi GS glass break sensor alarm / ok / connection lost / low battery
- Livi VS impact sensor alarm / ok / connection lost / low battery
- Livi Key Fob control panel "Punic button" alarm / ok / low battery
- Livi RFID security control panel "Punic button" alarm / ok / connection lost / low battery
- Livi US universal sensor (with fire and/or security sensors) alarm / ok / connection lost / low battery

The *Alarm* and *Ok* events are generated and transmitted immediately. The *Connection lost* event is generated if the hub has not received test events from the device during five test periods. The *Low battery* event is generated if the battery voltage remains at 2.3 V or less for the period specified in the table below.

Livi radio device	Test period, minutes	Connection lost, minutes	Low battery, hours
Livi CS opening sensor	2	from 10 to 12	4
Livi FS smoke sensor	2	from 10 to 12	4
Livi GS glass break sensor	2	from 10 to 12	4
Livi Key Fob control panel	no tests	not tracked	4
Livi MS motion sensor	2	from 10 to 12	4
Livi MSW curtain type motion sensor	2	from 10 to 12	4
Livi RFID security control panel	10	from 50 to 60	4
Livi US universal sensor	2	from 10 to 12	4
Livi VS impact sensor	2	from 10 to 12	4

The events about hub state, that are transmitted directly from the hub to STEMAX ML:

Generated event	Minimum fixation time	Recovery event	Event is directed to
Ethernet failure (if the hub continues to operate via mobile internet)	40 seconds	Ethernet restored	Mobile app and STEMAX ML

Generated event	Minimum fixation time	Recovery event	Event is directed to
220 V failure (if the hub continues to operate on battery)	3 minutes	220 V restored	Mobile app and STEMAX ML

Events, which are generated in case the connection is lost, are shown in the table below**.**

Generated event	Minimum disconnection time	Connection recovery event	Event is directed to
If the connection between the hub and STEMAX ML* is lost			
Loss of communication with the monitoring station	3 minutes	Communication with the monitoring station restored	Mobile app
If the connection between the hub and Livicom platform* is lost			
Loss of communication with the site	3 minutes	Communication with the site restored	Mobile app and STEMAX ML

* If the connection is lost between the hub and STEMAX ML or between the hub and the Livicom platform, all generated events are queued by the hub for sending. The hub will send all accumulated events after the connection is restored.

APPENDIX B – STELS technical support contacts

If you have not found the answer to your question in this manual, then STELS contact technical support.

e-mail:

support@nppstels.ru

phones:

+7 (3822) 488-508, 488-507,

+7-923-414-0144.

Technical support schedule:

on weekdays from 8:00 to 20:00 Tomsk time (GMT + 7)