



<https://glab.com.ua>

**Communication device  
easyDTMFv9.12 (DUAL SIM)  
(ContactID™ or AdemcoExpress™ communicator)  
Installation and usage manual**

Lviv 2025

# Contents

Features.....	3
Purpose.....	4
Specifications.....	4
General operational characteristics.....	4
Electrical specifications.....	5
GSM modem.....	5
WiFi characteristics.....	5
Preparations, programming and powering on.....	5
SIM card requirements.....	5
Installing the SIM cards.....	6
Circuit board overview.....	7
Connecting to the alarm control panel.....	8
Programming the device.....	9
Programming the security alarm system.....	13
Connecting the outputs.....	13
Operating modes of outputs.....	13
LED indication.....	14
Multipurpose button.....	16
SMS command format.....	16
Programming the settings.....	16
Managing outputs OK1, OK2.....	17
Service commands.....	18
Errors when programming or operating and how to resolve them.....	18
Updating the firmware.....	21
Warranty.....	23
Scope of delivery.....	23
Appendix 1: AdemcoExpress™ to ContactID™ protocol conversion table.....	24
Appendix 2: Additional ContactID codes transmitted to the monitoring station.....	28

## Features

- In-browser programming via WiFi.
- Transmits all events supported by the security alarm system to the monitoring station.
- Uses the nanoSIM card format.
- Can be used with two SIM cards from different mobile network operators.
- Can be used with just one SIM card.
- Can use the programmed WiFi access point as a transmission channel to the monitoring station.
- Optional push notifications for the GMonitor mobile application.
- In-browser console that logs status and possible errors when programming or operating.
- Recurrent checks for connection to the monitoring station using all provided channels.
- Cellular network signal strength indication.
- Works with any security alarm systems that support ContactID™ or AdemcoExpress™ telephone protocols.
- 2 potential inputs for «panic button» and «tamper» event transmission.
- 2 open collector outputs, each can be managed from the monitoring station phone number or from the GMonitor mobile application.
- Programmable «life pulse» re-transmission time.
- Communicates with the monitoring station using the **Glab-crypto** encrypted protocol.
- Transmits a «device reboot» event to the monitoring station when previously powered off.
- Can notify the user if the security service fee has not been paid.
- Can block arming the system if the security service fee has not been paid.

## Purpose

EasyDTMF communicator is designed to transmit an alarm signal from security alarm systems that support the ContactID™ or AdemcoExpress™ telephone protocols to the monitoring station via the Glab-crypto™ protocol. The device is shown on **figure 1**.

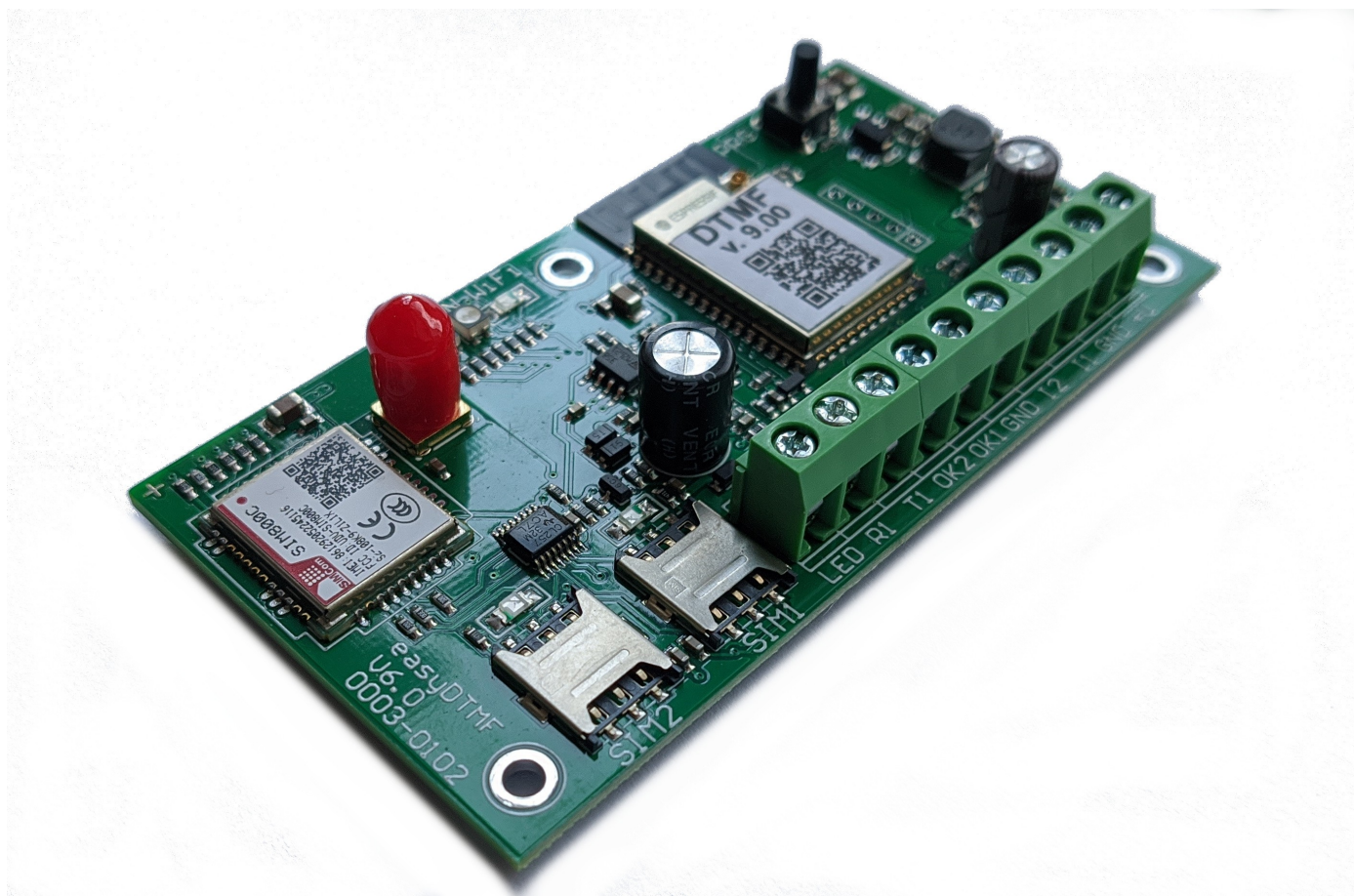


Figure 1

## Specifications

### *General operational characteristics*

Number of inputs	2
Number of open collector outputs	2
Supported nanoSIM card standard	GSM
Supported number of nanoSIM cards	2
Data format used for transmission to the monitoring station	Glab-crypto
Supports backup monitoring station server address	Yes
Real-time clock	Yes
Power-on to operational time, seconds (not more than)	50
Operating temperature range	+3°C...+45°C

## Electrical specifications

<i>Name</i>	<i>Parameter</i>	<i>Unit</i>	<i>Value</i>
Supply voltage	$U_{pwrdc}$	V	+10...+15
Max. current consumption	$I_{pwrmax}$	mA	1000
Standby current consumption (WiFi off), approx.	$I_{pwravg}$	mA	25
Standby current consumption (WiFi on), approx.	$I_{pwravg}$	mA	50
Max. voltage of log. «1» at the inputs I1 – I2	$U1_{max}$	V	$U_{pwrdc}+1$
Min. voltage of log. «1» at the inputs I1 – I2	$U1_{min}$	V	6
Max. voltage of log. «0» at the inputs I1 – I2	$U0_{max}$	V	1,6
Min. voltage of log. «0» at the inputs I1 – I2	$U0_{min}$	V	0
Max. load current from the outputs OK1 and OK2 (not protected)	$I_{okmax}$	mA	100
Max. DC voltage at the outputs OK1 and OK2	$U_{okmax}$	V	15

## GSM modem

Frequency range	GSM 850/EGSM 900/ DCS 1800/ PCS1900, auto selection
GSM class	Small MS
Transmitter power	Class 4 (2W @ 850/900MHz) Class 1 (1W @ 1800/1900MHz)
SIM interface	Support SIM card: 1,8V, 3V
Antenna interface	SMA female

## WiFi characteristics

Frequency range		2412 – 2484 MHz
WiFi standard		IEEE 802.11b/g/n
Data rate	20 MHz	802.11b: 1, 2, 5.5 and 11 Mbps 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n: MCS0-7, 72.2 Mbps (Max)
	40 MHz	802.11n: MCS0-7, 150 Mbps (Max)

## Preparations, programming and powering on

### SIM card requirements

The device supports standard GSM Phase1, GSM Phase2+ nanoSIM cards with 1.8 and 3 Volts supply voltage. This means that any SIM card manufactured not earlier than 2004 will work.

The SIM cards must be activated. Also canceling the PIN request on boot is not required but strongly recommended – this speeds up the loading time.

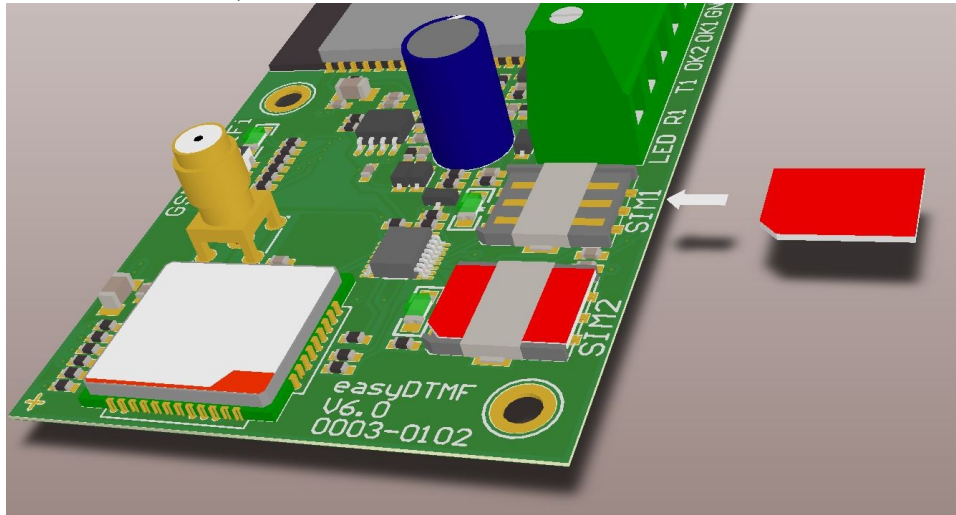
## Installing the SIM cards

Connect the antenna to the SMA connector of the device.

### ⚠ATTENTION!

*Using the device without the GSM antenna causes the GSM module to malfunction. Note that the manufacturer's warranty does not apply to the GSM module.*

Insert the SIM cards into the device from the outer side (see **figure 2**). The “SIM1” holder is intended for the first SIM card, “SIM2” – for the second card.



**Figure 2**

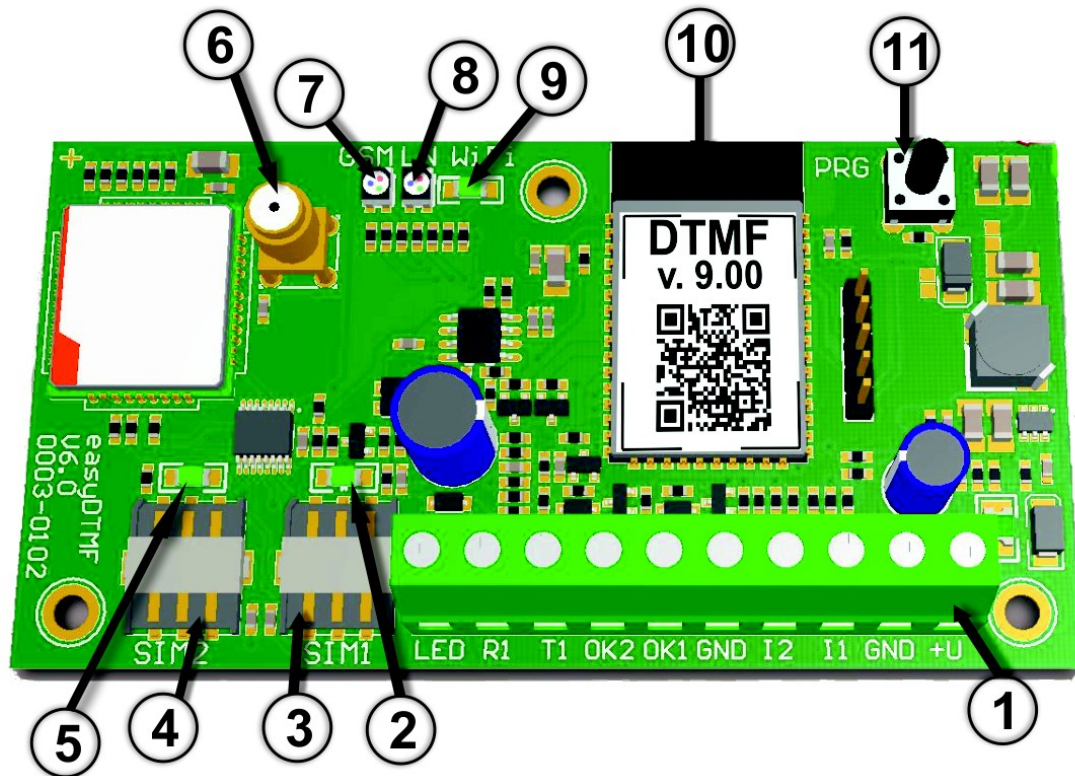
If only one SIM card is used, it can be installed into either SIM holder (SIM1 / SIM2). In this case the device will send a channel malfunction message (for the remaining channel) to the monitoring station when powered on (See **Appendix 2**).

### ⚠ATTENTION!

*Inserting or removing the SIM cards while the device is powered can damage both the SIM cards and the GSM module. Note that the manufacturer's warranty does not apply to the GSM module.*

## Circuit board overview

All of the needed circuit board elements are shown on **figure 3**.



**Figure 3**

- ① – Terminals with inputs and outputs for the alarm control panel. The description of terminals can be found in **table 1**.
- ② – Green indicating LED for the first SIM card (SIM1). See section “LED indication”.
- ③ – NanoSIM holder for the first SIM card.
- ④ – NanoSIM holder for the second SIM card.
- ⑤ – Green indicating LED for the second SIM card (SIM2). See section “LED indication”.
- ⑥ – SMA connector for the GSM antenna.
- ⑦ – RGB LED indicating the GSM module/device operating mode. See section “LED indication”.
- ⑧ – RGB LED indicating the telephone receiver (“LN”) status. See section “LED indication”.
- ⑨ – Green LED indicating the WiFi operating mode. See section “LED indication”.
- ⑩ – WiFi module antenna.
- ⑪ – Multipurpose button. See section “Multipurpose button”.

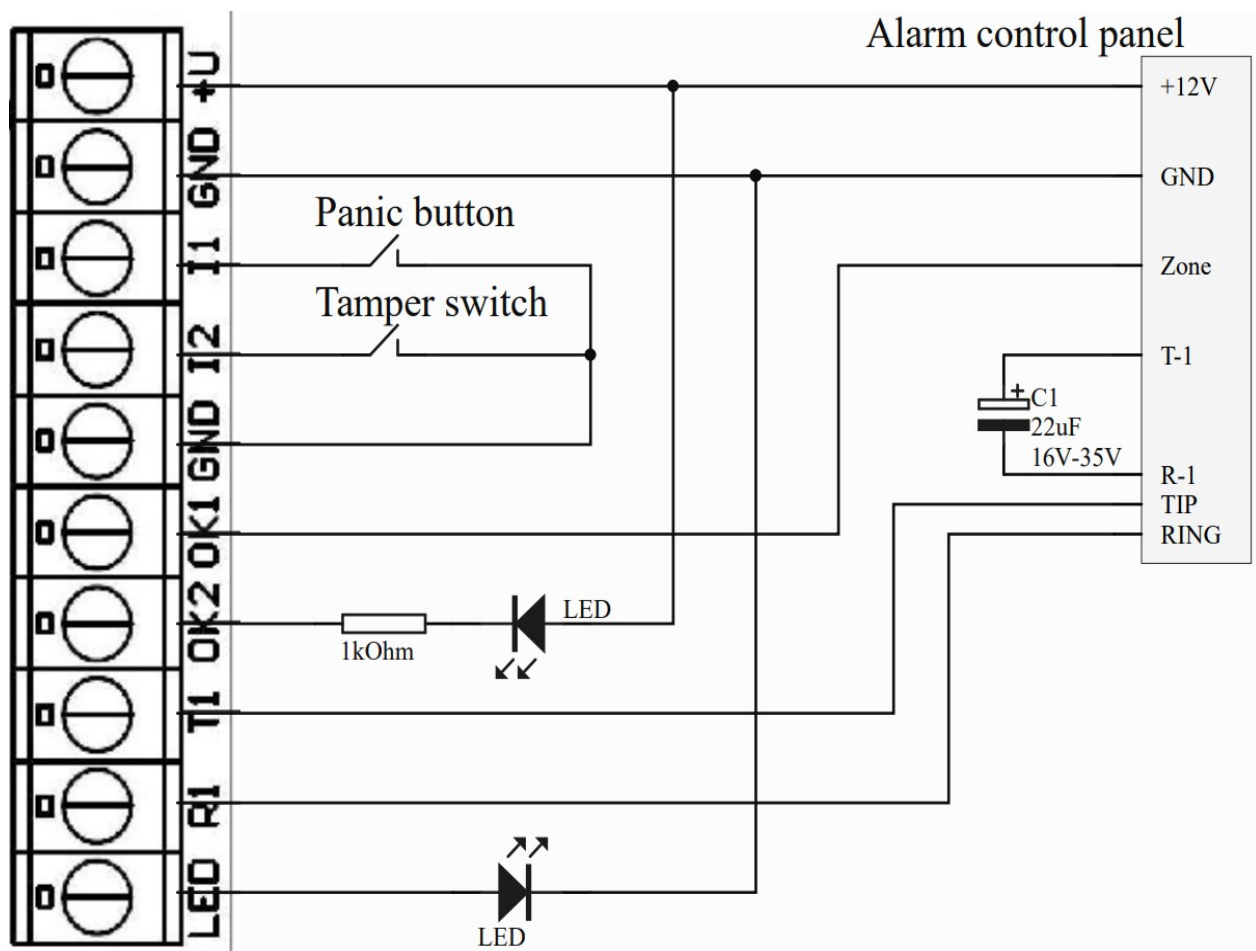


**Table 1. Description of terminals.**

<i>Terminal</i>	<i>Description</i>
<b>+U</b>	<b>Power supply «+». Operating voltage 10-15 V DC.</b>
<b>GND</b>	<b>Power supply «-», common terminal.</b>
<b>I1</b>	<b>Input for a panic button. Active level «1», must be connected to «GND» if unused.</b>
<b>I2</b>	<b>Tamper switch input. Active level «1», must be connected to «GND» if unused.</b>
<b>GND</b>	<b>Power supply «-», common terminal. Unused inputs I1 and I2 (also an arm confirmation LED «-») can be connected to this terminal.</b>
<b>OK1</b>	<b>Programmable open collector output, switching to the power supply «-».</b>
<b>OK2</b>	<b>Programmable open collector output, switching to the power supply «-».</b>
<b>T1</b>	<b>Input for the telephone line from the alarm control panel.</b>
<b>R1</b>	<b>Input for the telephone line from the alarm control panel.</b>
<b>LED</b>	<b>Output for an arm confirmation LED «+».</b>

## Connecting to the alarm control panel

A typical wiring diagram is displayed on **figure 4**.



**Figure 4**



## Programming the device

Before programming the device make sure that the device's SIM cards are activated and have mobile data services turned on. If necessary, write down the PIN codes for the first ("SIM1") and second ("SIM2") SIM cards.

Insert the SIM cards into the device while it is powered off.

If the device was used before, it needs to be reset to factory settings. In order to do so, hold the multipurpose button ⑩ and power the device. A blue light will start to blink on LED ⑦. After 15 seconds all the LEDs will turn on, meaning that the reset is complete, the button can be released and power can be turned off.

If the device is new, factory reset is not necessary.

Power the device. The LED ⑦ "GSM" will light up in red. The green LED ⑨ "WiFi" will flash once per second, indicating that a WiFi access point named "easyDTMF:XX:XX" is activated. "XX:XX" in the access point name are the last four digits from the MAC address of the WiFi module.

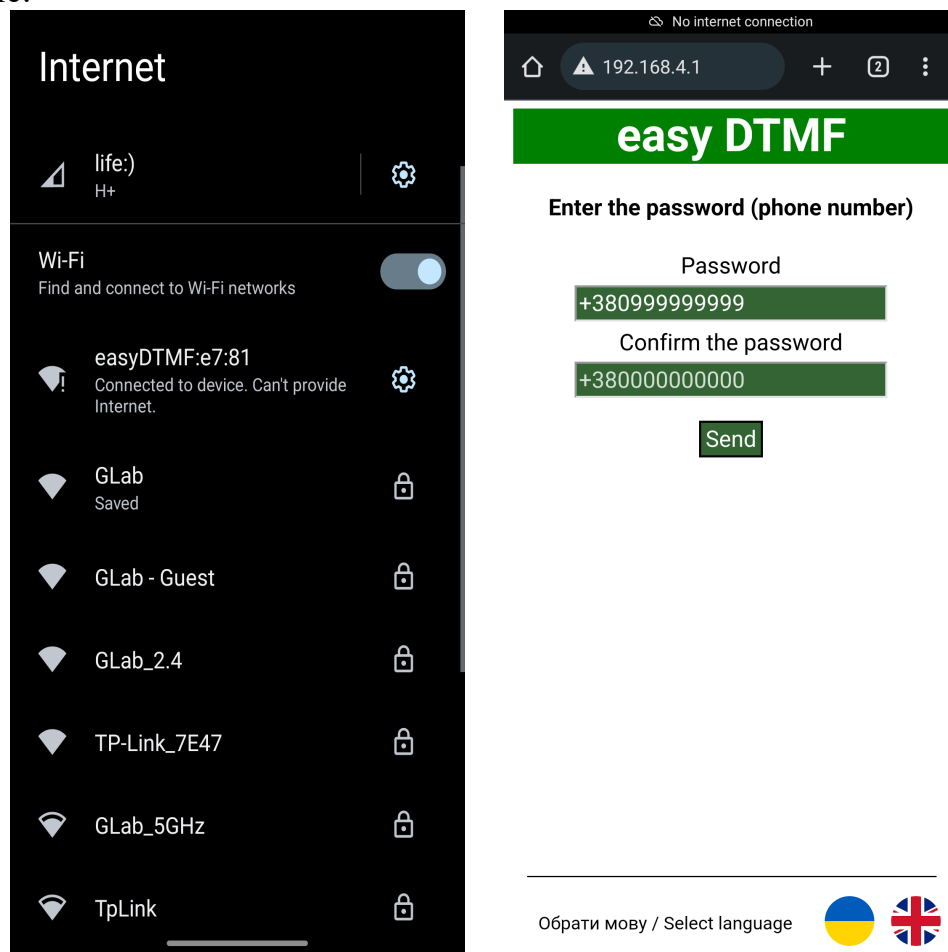


Figure 5

Connect to the WiFi access point using a smartphone/computer (see figure 5). The WiFi password is **easyDTMF** (case sensitive). The smartphone may offer to change the WiFi network or use mobile data for internet access – decline if asked. Open an internet browser and load a page with the device's IP address: **192.168.4.1** (see figure 5).

On the page, a password needs to be programmed and confirmed. A password is always a phone number (in international format), which is then used to send an SMS message with the settings for the device (see figure 5). Press "Send" when done.

## ATTENTION!

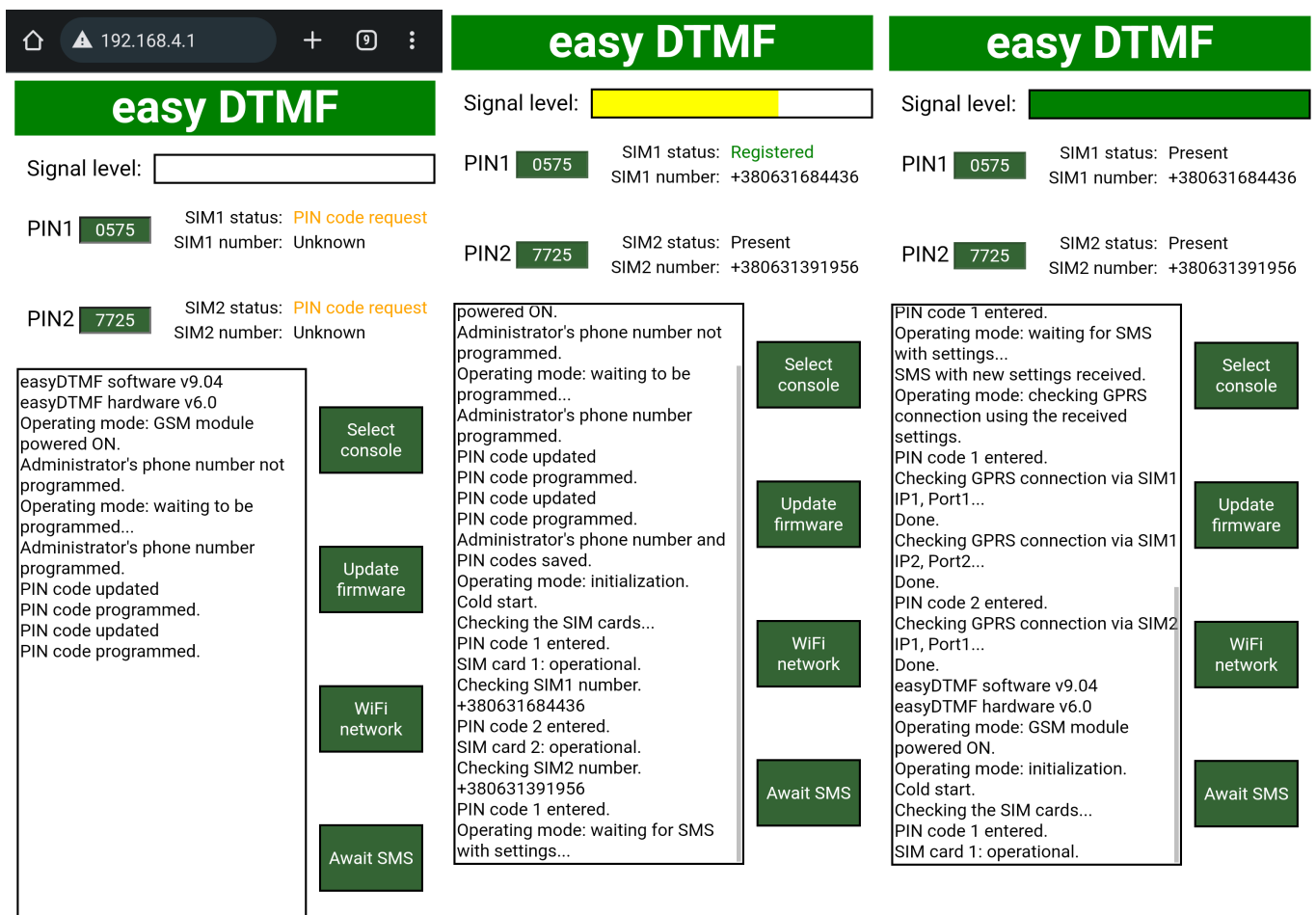
***Do not share the password with unauthorized persons. The password can only be changed by confirming the old one in the corresponding window during authorization or by resetting the device to factory settings.***

Then the diagnostics and programming web page will open in the browser (see **figure 6**). Here SIM card PIN codes should be programmed, but only if SIM1 or SIM2 status shows “PIN code request”. Otherwise the PIN code change field is unavailable.

To change the PIN code, enter 4 digits in the corresponding input field and then click elsewhere on the web page — for instance on the diagnostic console (where “easyDTMF software v9.0X” is written). The device will react with the following message: “PIN code updated. PIN code is programmed.”, else retry entering the PIN code.

When the PIN codes are programmed or not needed, click the “Await SMS” button. The diagnostic console will show logs similar to the second picture of **figure 6**. In general, after receiving the “Operating mode: waiting for SMS with settings...” log entry, the engineer at the monitoring station can send an SMS with the settings since the device is ready to receive and process it. (See the manual to GRAPH software at [glab.com.ua](http://glab.com.ua)).

When the device receives an SMS with the settings, it will print the following: “SMS with new settings received”.

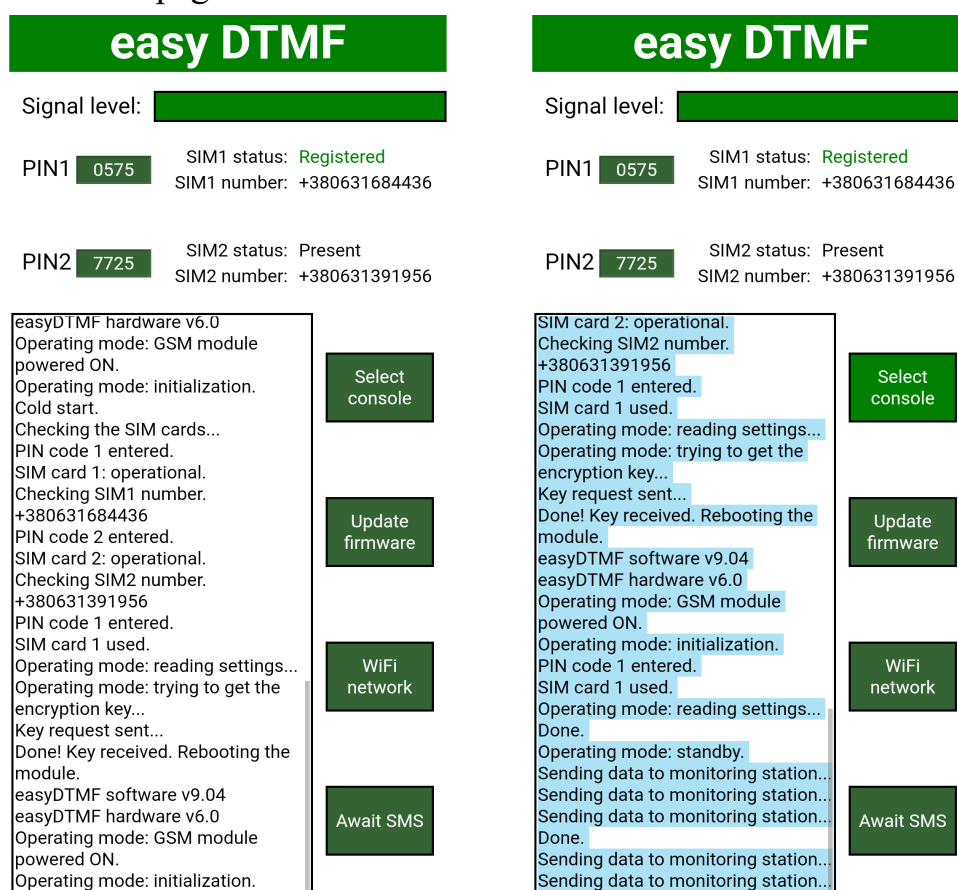


**Figure 6**

After receiving an SMS with valid settings, the device will attempt to connect to the GRAPH server using IP addresses and port numbers provided in the SMS. This operation is accompanied by console log message “Checking the GPRS connection on SIMX IPX PortX”, where X can be 1 or 2. If connection to the GRAPH server is established, the device sends an encryption key request to the monitoring station operator and awaits the encryption key (See the manual to GRAPH software at [glab.com.ua](http://glab.com.ua)). All the actions regarding the key request and response will be logged to the diagnostic console (see **figure 7**).

When the operator responds to the encryption key request, the device reboots and starts the main operation mode (sending data to the monitoring station). This is indicated by the console log entry “Operating mode: standby” (see **figure 7**). If the diagnostic console log differs from the one shown on **figure 7** (error messages appear), the console text can be selected with the “Select console” button and then copied to clipboard for further analysis. In case of errors refer to section “Errors when programming or operating and how to resolve them”.

If the diagnostic console has printed the message “Connection error: 0”, press the multipurpose button to reactivate the WiFi access point and then reconnect to the WiFi network, reload the web page.



**Figure 7**

The web page has a cellular network signal level bar, equivalent to the color of LED ⑦ “GSM”, as seen in **table 4**. An empty bar indicates that the signal level detection is unavailable.

The current SIM card phone number is displayed under the SIM card status. If the device shows an error instead of the phone number, the SIM card is either not activated, or does not

support the USSD phone number request. While in factory settings, the SIM cards are not yet registered with the mobile network, so the phone number is set to “Unknown”.

## 👉 ATTENTION!

*In order to receive the encryption key request, the **GRAPH** client (or the **GRAPH** agent) software must be running on the monitoring station operator’s workstation.*

In case you want to enable the WiFi transmission channel and/or the GMonitor push notifications, click the “WiFi network” button. The web browser will display a page with the WiFi settings (see **figure 8**).

Make sure to enter the correct WiFi network name (SSID) and password there. Also in order to connect to the push notification server and the monitoring station the WiFi network needs to have internet access and the configured ports (see **table 8**) need to be open in the router. Tick the necessary features below and press “Save”, the button will update to “Saved!” if successful. Otherwise a popup window will notify about the problem (see **figure 8**). To learn more about push notifications, see the manual for the **GMonitor** mobile application.

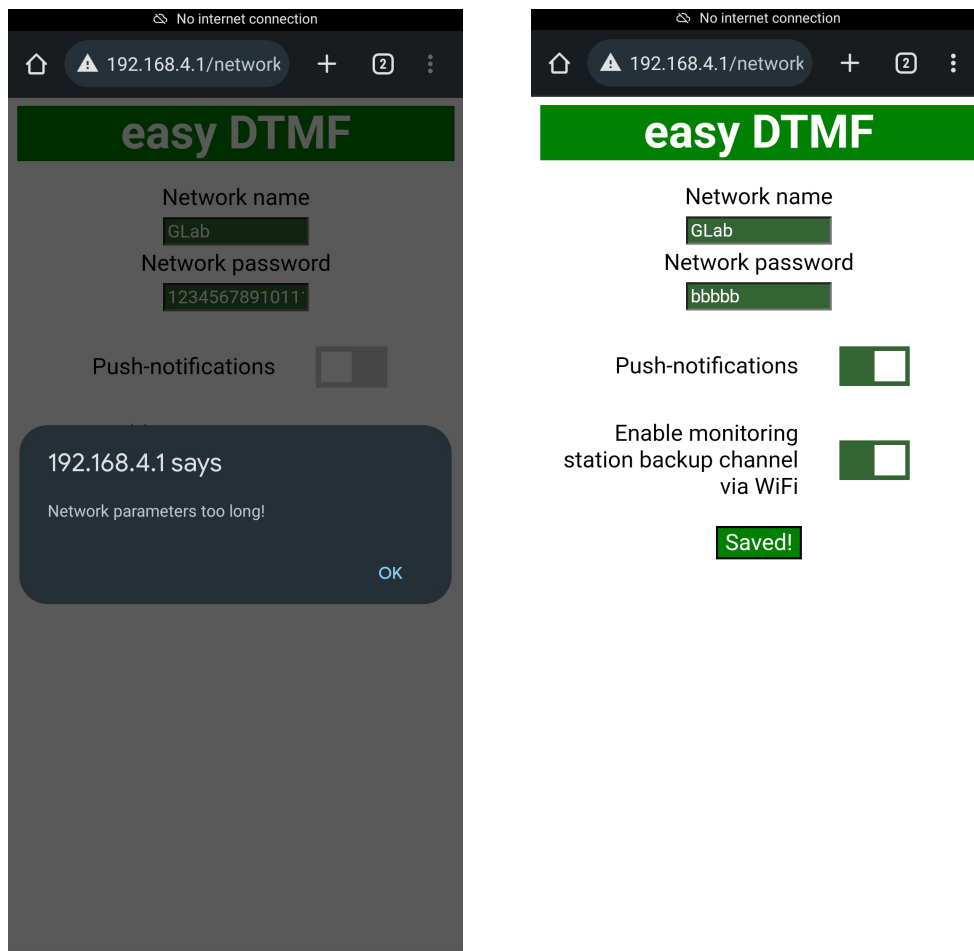


Figure 8

## Programming the security alarm system

In general the security alarm system needs to have the telephone monitoring (number to dial -"1") enabled, the ContactID or AdemcoExpress transmission format selected and alarm customer identifier (number) programmed. This identifier may match the device identifier. Otherwise it is possible to control the connection to the security alarm system separately and use the device inputs as zones from an extra site. It is worth noting that in such case the monitoring station database will need to store two different objects.

### **ATTENTION!**

*The phone number to be programmed in the security alarm system is «1».  
The protocol is ContactID or AdemcoExpress.*

The necessary AdemcoExpress codes for programming in the security alarm system are provided in **Appendix 1**. It is needed for correct conversion to ContactID protocol.

## Connecting the outputs

The device has two open collector outputs that are switching to the common ground. The outputs can be used by the monitoring station operator to remotely manage various equipment, control the security panel status, light an arm confirmation LED or block arming the system if the security service fee has not been paid.

### **ATTENTION!**

*The device outputs have limited load capacity. Output current **MUST NOT EXCEED 100 mA!***

## Operating modes of outputs

Each of the device outputs has 4 independent operating modes (see **Table 2**).

**Table 2. Operating modes of outputs «OK1» or «OK2».**

<i>Values sent in SMS</i>	<i>Operating mode description</i>
0	The according output works in monostable mode. The output can be activated or deactivated with an SMS command*. See the command format in section «Managing outputs OK1, OK2».
1	The according output works in bistable mode. The output can be activated for up to 99 seconds with an SMS command*. See the command format in section «Managing outputs OK1, OK2».
2	The according output controls an arm confirmation LED. In case the arm event message is successfully sent to the monitoring station, the output will be activated for 60 seconds.
3	The according output controls end-user notifications about the unpaid security service fee or inability to arm the system.

\* Instead of sending SMS commands, outputs can be managed from the GMonitor application but only if the administrator grants a permission.

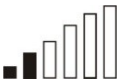
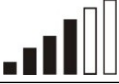

## LED indication

The description of all the indicating LEDs is provided in **tables 3 – 7**.

**Table 3. Indicating LED “GSM” ⑦.**

<i>Color</i>	<i>Timing</i>	<i>Description</i>
None	Turned off.	“GSM” LED being off for several seconds indicates that the device is rebooting the GSM module. If the “GSM” LED is not turning on at all, contact the manufacturer’s service.
Red ●	Solid on.	An error occurred. Activate the WiFi access point, connect to the device’s WiFi network and read the error log (see “ <b>Programming the device</b> ”).
Red ● Yellow ● Green ●	On for 64 ms, off for 800 ms. Looks like a short flash once per second.	The device is trying to register with the cellular network. LED color shows the last tracked signal strength level of the cellular network (see <b>table 4</b> ).
Red ● Yellow ● Green ●	On for 64 ms, off for 3000 ms. Looks like a short flash once per 3 seconds.	The device is registered with the cellular network. LED color shows the signal strength level of the cellular network (see <b>table 4</b> ).
Red ● Yellow ● Green ●	On for 64 ms, off for 300 ms. Looks like blinking three times per second.	GPRS data transfer service is active. LED color shows the signal strength level of the cellular network (see <b>table 4</b> ).

**Table 4. Approximate cellular network signal strength level and the corresponding color of LED ⑦ “GSM”.**

<i>Color</i>	<i>Signal strength</i>	<i>Notes</i>
Red ●		The signal is not strong enough for normal operation. An external antenna with greater sensitivity is needed.
Yellow ●		The signal is at about 50% strength. Enough for normal operation.
Green ●		Maximum signal level.

### **ATTENTION!**

*The LEDs indicate an error only for 30 seconds. Afterwards the device reboots the GSM modem and attempts to start the main operation. This does not apply to waiting for the encryption key or an SMS with the settings.*

**Table 5. Indicating LED “LN” ⑧.**

<b><i>Color</i></b>	<b><i>Timing</i></b>	<b><i>Description</i></b>
None	Turned off.	Telephone line in standby mode.
Red ●	Solid on.	Telephone line fault, no connection to the alarm control panel.
Yellow ●	Turned on for a couple of seconds, then off.	The alarm control panel is setting up a telephone line communication with the device. LED turning off means that the device detected a dialed number “1”.
Yellow ●	Turned on for a longer time, then off.	The alarm control panel is trying to set up a telephone line communication with the device. LED not turning off can indicate: - no connection to the monitoring station; - insufficient telephone line signal level from the alarm control panel.
Green ●	Blinks 2 times.	The device sent a “HANDSHAKE” signal to the alarm control panel.
Green ●	Turned on for one second.	The device sent a “KISSOFF” signal to the alarm control panel.
Blue ●	Short flash.	The device successfully detected a DTMF signal from the alarm control panel.

**Table 6. Indicating LED “WiFi” ⑨**

<b><i>Color</i></b>	<b><i>Timing</i></b>	<b><i>Description</i></b>
None	Turned off	WiFi access point and station is off.
Green ●	On for 72 ms, off for 672 ms. Looks like a short flash once per second.	WiFi access point activated. If no client is connected, the access point will remain active for 15 minutes and will turn off later.
Green ●	Once per second: two short (72 ms) flashes and a pause.	Connected to the programmed WiFi access point in station mode. The push notification server and/or the WiFi transmission channel is active.
Green ●	Three short (72 ms) flashes once per second. Looks like frequent blinking.	Unable to connect to the programmed WiFi access point or having trouble connecting to the internet. If this persists for a few minutes, check the diagnostic console log for additional details.



**Table 7. Indicating LEDs ② («SIM1») and ⑤ («SIM2»).**

<b>LED</b>	<b>Timing</b>	<b>Description</b>
②	Turned off.	First SIM card not found.
② ●	On for 72 ms, off for 672 ms. Looks like a short flash once per second.	First SIM card is present but not used.
② ●	On for 422 ms, off for 422 ms. Looks like a long flash once per second.	First SIM card is registered with the mobile network.
② ●	Solid on.	Connected to the GRAPH server using the first SIM card.
② ●	On for 72 ms, off for 72 ms. Looks like frequent blinking.	Attempting data transmission to the monitoring station using the first SIM card.
⑤	Turned off.	Second SIM card not found.
⑤ ●	On for 72 ms, off for 672 ms. Looks like a short flash once per second.	Second SIM card is present but not used.
⑤ ●	On for 422 ms, off for 422 ms. Looks like a long flash once per second.	Second SIM card is registered with the mobile network.
⑤ ●	Solid on.	Connected to the GRAPH server using the second SIM card.
⑤ ●	On for 72 ms, off for 72 ms. Looks like frequent blinking.	Attempting data transmission to the monitoring station using the second SIM card.

## Multipurpose button

Multipurpose button is designed for the following:

- Resetting the device to factory settings. In order to do so, hold the multipurpose button ⑪ and power the device. A blue light will start to blink on LED ⑦. After 15 seconds all the LEDs will turn on, meaning that the reset is complete, the button can be released.
- Turning on/off the WiFi access point. Press the multipurpose button ⑪ while the device is operational. The WiFi mode will change to the opposite (access point – station, see table 6). The WiFi access point will stay on for 15 minutes if no client connection is active.

## SMS command format

### Programming the settings

A text SMS message is used for programming the settings with commands «\*1XX\*AYYY\*» in the message body. An SMS message must be sent from the phone number set as the password for the device web page. The list of supported commands is provided in table 8.

**Table 8.**

<b>Command</b>	<b>Example</b>	<b>Description</b>
<b>*0XX*</b>	<b>*010*</b>	Delay between the test messages sent to the monitoring station. Entered number XX is multiplied by 30 seconds. Enter 00 to disable the test message transmission.
<b>*1X*</b>	<b>*10*</b>	OK1 operating mode. 0 – monostable, 1 – bistable, 2 – arm confirmation, 3 – security service fee notification/arm blocking.
<b>*2X*</b>	<b>*20*</b>	OK2 operating mode. 0 – monostable, 1 – bistable, 2 – arm confirmation, 3 – security service fee notification/arm blocking.
<b>*3XXXX*</b>	<b>*31111*</b>	Customer identifier (number) for the monitoring station. 4 digits.
<b>*4xxx.xxx.xxx.xxx*</b>	<b>*4192.168.1.1*</b>	IP address of the GRAPH receiver first channel (line).
<b>*5xxxxx*</b>	<b>*510000*</b>	IP port (socket) number of the GRAPH receiver first channel (line). Must contain 5 digits.
<b>*6xxx.xxx.xxx.xxx*</b>	<b>*6192.168.1.2*</b>	IP address of the GRAPH receiver second channel (line).
<b>*7xxxxx*</b>	<b>*710000*</b>	IP port (socket) number of the GRAPH receiver second channel (line). Must contain 5 digits.
<b>*8xxxxxxxxxxx*</b>	<b>*8internet*</b>	Name of GPRS access point for the first SIM card (SIM1).
<b>*9xxxxxxxxxxx*</b>	<b>*9www.umc.ua*</b>	Name of GPRS access point for the second SIM card (SIM2).
<b>*AX*</b>	<b>*A0*</b>	Input operating mode. Placeholder for future software versions.
<b>*Dxx*</b>	<b>*D11*</b>	Device management commands, notably open collector management (see <b>Managing outputs OK1, OK2 and Service commands</b> ).
<b>*E*</b>	<b>*E*</b>	Reset the settings.
<b>*F*</b>	<b>*F*</b>	Reboot the device remotely.

A sample SMS with the settings:

**\*010\*10\*21\*31234\*4192.168.1.1\*502050\*6abc.com\*702051\*8internet\*9www.umc.ua\*A0\***

## **ATTENTION!**

***The IP addresses and access point names above are provided only for demonstration purposes!***

Note that the device does not support non-latin characters in the SMS message.

Furthermore, if the security alarm system and the device have different alarm customer identifiers (numbers), easyDTMF will not change the identifier when transmitting to the monitoring station. In such case it is necessary to create as many objects in the monitoring station database as the security alarm system uses plus one for the device.

## **Managing outputs OK1, OK2**

Managing the outputs is done via a text SMS message with commands «\*DXX\*DYYY\*» in the message body. Commands are listed in **tables 9 and 10**. The message body can contain several commands separated with the «space» symbol.

Alternatively, outputs can be managed from the GMonitor mobile application, but all management commands require a granted permission from the administrator (see the **GMonitor manual**).

**Table 9. Commands for SMS output management in mode «0». Monostable mode.**

<b>Command (*DXX*DYY)</b>	<b>Description</b>
<b>*D10*</b>	Deactivate OK1
<b>*D11*</b>	Activate OK1
<b>*D20*</b>	Deactivate OK2
<b>*D21*</b>	Activate OK2

**Table 10. Commands for SMS output management in mode «1». Bistable mode.**

<b>Command (*DXXX*DYYY*)</b>	<b>Description</b>
<b>*D1XX*</b>	Activate OK1 for XX seconds* **
<b>*D2YY*</b>	Activate OK2 for YY seconds* **

\* maximum output activation duration is 99 seconds.

\*\* if XX or YY are equal to 00, the output will remain activated for 2 seconds.

## Service commands

Service management commands are similar to **Managing outputs OK1, OK2** but use the format «\*D0X\*» and currently consist of:

- **\*D01\*** – automatic firmware update command. The device must be connected to a WiFi network with internet access. By default it downloads the latest firmware from the official website [glab.com.ua](http://glab.com.ua), however an optional valid reference to an HTTP(S) server with a correct encrypted firmware image can be specified. For instance, **\*D01\*** or **\*D01\*http://192.168.1.69/OlderVersion.bin\***. The **GMonitor** application can execute this command from the appropriate sub-menu provided that permission from the administrator was granted. On update end the device generates an event, depending on if the update was successful (and specifies the reason in an error code if not).

### **ATTENTION!**

*The device ignores invalid commands and commands with non-latin characters inside the message body.*

*SMS commands have to be sent to the currently active SIM card phone number. The active SIM card can be determined from the latest channel switch event (see Appendix 2). In case WiFi is the active channel, the default active SIM card is SIM1 (provided that it is present and operational – no first channel fault event was received).*

## **Errors when programming or operating and how to resolve them**

### **ATTENTION!**

*Device programming can be started only when the **GRAPH** server software is installed, configured, tested and running on the monitoring station server. **GRAPH** installation and usage manual can be found on the following web page:*

*<https://glab.com.ua/en/downloads.html>.*

**All LEDs remain off when powering the device** — make sure that the supply voltage is present between the terminal inputs of the device. If it is present, the device is likely broken or damaged, contact the manufacturer's service.

**Red GSM LED stays on** — turn on the WiFi access point (if deactivated), connect to it, open the main web page in browser and read the error log (see section "Programming the device").

List of possible error messages in the web diagnostic console:

**"ERROR! No response to power-OFF pulse."** or **"ERROR! No response to power-ON pulse."** The SIM800C GSM module is out of order. The device is not operational, contact the manufacturer's service.

**"SIM card X: missing."** The device is unable to detect the mentioned SIM card. If it is present, delete the SIM card contacts or replace the card. If the backup SIM card is not used, ignore this message.

**"Settings incomplete."** The device has not detected some of the needed settings (setting missing or contains invalid characters) and is waiting for another SMS with the settings. After this message the device will specify which setting fields are invalid:

*"Error in settings: administrator's phone number"* — error in the administrator's phone number (password).

*"Error in settings: life pulse"* — error in the period of test messages, sent to the monitoring station. Recommended value — \*005\* (2.5 min.).

*"Error in settings: OK1 mode"* — error in OK1 operating mode.

*"Error in settings: OK2 mode"* — error in OK2 operating mode.

*"Error in settings: customer number"* — error in the alarm customer identifier (number).

*"Error in settings: IP address 1"* — error in the main IP address.

*"Error in settings: TCP port 1"* — error in the main TCP port.

*"Error in settings: IP address 2"* — error in the backup IP address.

*"Error in settings: TCP port 2"* — error in the backup TCP port.

*"Error in settings: SIM1 access point name"* — error in GPRS access point name for the first SIM card.

*"Error in settings: SIM2 access point name"* — error in GPRS access point name for the second SIM card.

*"Error in settings: input operating mode"* — error in input operating mode.

*"Error in settings: encryption key"* — error in the encryption key.

*"Error in settings: SIM1 PIN"* — error in the first SIM card PIN code.

*"Error in settings: SIM2 PIN"* — error in the second SIM card PIN code.

**"No response from the GSM module. Rebooting the module."** The device received no response when trying to read an SMS message. No actions are required.

**"No registration with the cellular network for more than 2 minutes. Rebooting the module."** The device is unable to register with the mobile network for several minutes and tries rebooting the GSM module. If this message appears often, try replacing the GSM antenna with a more sensitive one or replace the SIM card with another from a different mobile network operator that has better mobile coverage over the site where the device is installed.

**"Key request failed!"** or **"Key request timed out after 30 seconds!"** The device has not received a response to the encryption key request. Make sure that the monitoring station administrator is ready to approve sending the encryption key via GRAPH.

**"GPRS connection error."** The device cannot connect to the GPRS data transfer service using the new settings. This error is critical and requires action. The error can occur due to the SIM cards not being activated, having low SIM card account balance or the mobile network operator not activating the mobile data services. Afterwards the device usually prints the following:

*"No GPRS on SIM cards."*

*"Service may be inactive, or the account has insufficient funds."*

*"Resetting all settings."*

Or:

*"No communication via SIM cards. The remote server may be down."*

*"Resetting all settings."*

In any case make sure that the GRAPH server is operational.

**"Data transmission error."** The device is unable to send a message to the monitoring station. If this error occurs often, try replacing the GSM antenna with a more sensitive one or replace the SIM card with another from a different mobile network operator that has better mobile coverage over the site where the device is installed.

**"SIM X: PIN code error or missing"** PIN code error (or a wrong PIN code was entered) for the mentioned SIM card. The SIM card may be deactivated.

**"SIM X: BLOCKED."** The mentioned SIM card is blocked. A mobile phone and a PUK code is needed to unlock it.

**"SIM800 module did not respond. Rebooting the module."** No response from the SIM800C GSM module. If this message appears often, contact the manufacturer's service.

**"Unknown response from SIM800 module. Rebooting the module."** Unexpected response from the SIM800C module. If this message persists, contact the manufacturer's service.

**"SIM X: unable to register. Rebooting the module."** Unable to register the mentioned SIM card with the mobile network. Check the SIM card.

**"SIM X: card error. Rebooting the module."** Mentioned SIM card fault. Check the SIM card.

**"PIN code X not entered but required."** The device detected that the mentioned SIM card PIN code has not been submitted but is required to register with the network. Program the PIN code.

**"PIN code X mismatch, reset to factory settings."** The device detected that the mentioned SIM card PIN code is invalid. Reset the device to factory settings and enter the correct PIN code. Resetting is necessary to avoid blocking the SIM cards.

**"Error entering PIN code X. Check SIM card X."** No response from the mentioned SIM card after the PIN code was entered. The SIM card may be faulty.

**"FLASH MEMORY ERROR! Contact the manufacturer!"** The device memory is corrupted. Contact the manufacturer's service.

**"Unable to connect to WiFi AP! Check the SSID / password."** The WiFi network with the provided name cannot be found or the password does not match. Make sure that the network requisites are correct.

**"Unable to find the notification server domain!"** or **"Unable to find the monitoring station domain!"** The provided WiFi network may not have access to the internet or there might be

issues with DNS servers. If those problems are ruled out, the notification server may be down (Notify the manufacturer) / monitoring station may be down (Contact the security service provider).

**"Unable to connect to the notification server!"** or **"Unable to connect to the monitoring station!"** Equivalent to the former but instead of the DNS server issues, the necessary port might be closed in the WiFi router / network interface.

**"Device IMEI is not registered at the notification server!"** Contact the manufacturer's service and send the device IMEI for registration. The IMEI can be found on the SIM800 GSM module (**figure 3**, upper left).

All the internal error messages that cannot be caused or resolved by user's action are not listed here. If you encounter one of such errors that impacts the device operation, contact the manufacturer's service and provide the description of error.

## Updating the firmware

In order to update the device firmware, first download the latest firmware file using the web address: <https://glab.com.ua/en/downloads.html>. The firmware file must be named "easydtmf\_h6\_v**XXX**.bin", where **XXX** is the firmware version inside. The current device firmware version can be seen in the diagnostic console and on the update page (see **figure 9**). Afterwards activate the WiFi access point using the multipurpose button and connect the device with the firmware file downloaded to the easyDTMF WiFi network.

Launch a web browser and enter **192.168.4.1** in the address field.

If the user is unauthorized, the device will display a login page — enter the password there. When on the main page, click the "Update firmware" button (see **figure 6**), or enter the following directly in the browser address field: **192.168.4.1/update\_firmware** (see **figure 9**).

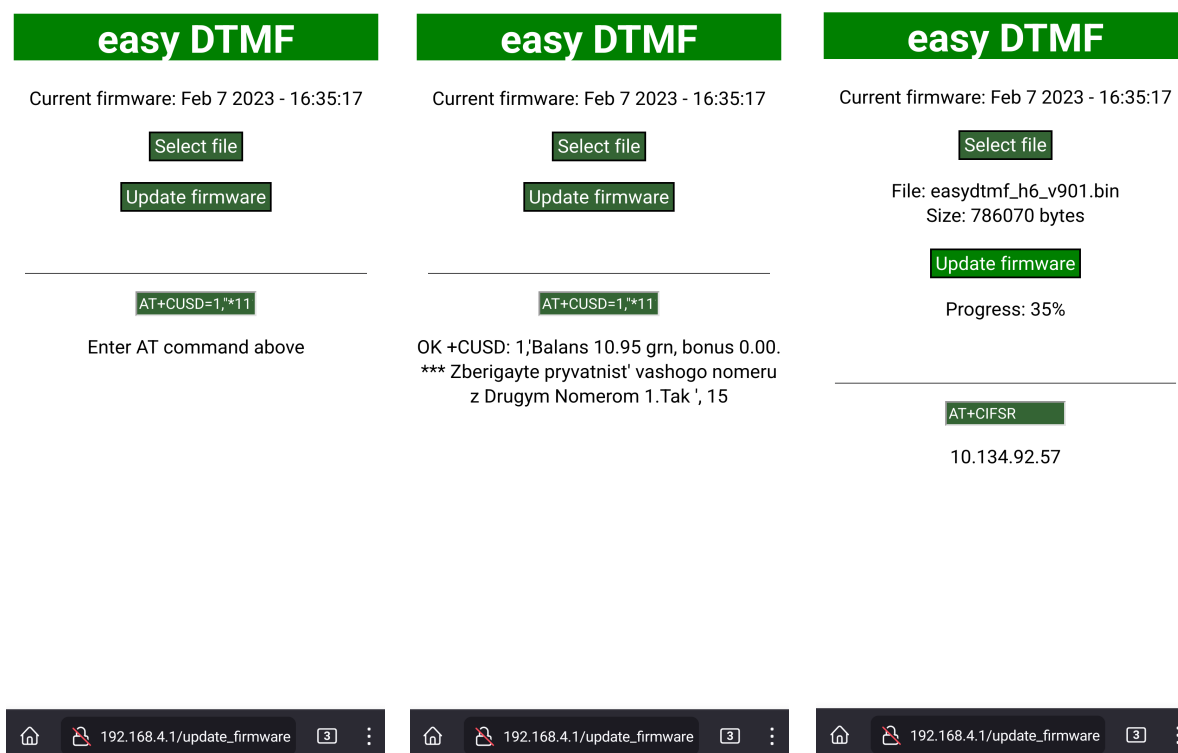
The web browser will then load the firmware update page.

Click the **"Select file"** button and find the downloaded firmware file (for example *easydtmf\_h6\_v901.bin*).

Then click the **"Update firmware"** button and wait until the file is uploaded. In case of successful update the device will print: **"Uploaded, reboot in 5 seconds"**. The firmware update is finished after the device reboots.

Alternatively the device can be updated remotely without needing any physical access using the automatic update command (see section **Service commands**). In order to execute this command the device must be connected to a WiFi network with internet access at the installation site. The command is issued either from the administrator's phone in an SMS message or from the **GMonitor** application if the administrator granted such permission.





**Figure 9**

Additionally the device can issue AT commands from the user to the GSM modem. This can be done by entering the AT command in the corresponding input field and then clicking elsewhere on the web page. The GSM modem will then process the command, response will be displayed in the line below (see **figure 9**). The maximum processing time for the user AT commands is set to 15 seconds, so all the commands with longer response time will return an error. Some example AT commands:

- AT+CUSD=1,"\*111#",15 — check the SIM card account balance (default AT command);
- AT+CIFSR — get the current modem IP address when the GPRS data transfer service is active;
- AT+CUSD=1,"\*161#",15 — get the current SIM card phone number.

The complete list of AT commands can be found in the GSM modem manual using the web address: [https://microchip.ua/simcom/2G/SIM800%20Series\\_AT%20Command%20Manual\\_V1.12.pdf](https://microchip.ua/simcom/2G/SIM800%20Series_AT%20Command%20Manual_V1.12.pdf).



## **Warranty**

ATTENTION! The product manufacturer is liable only within the limits of warranty obligation for the operation of the device itself and is not responsible for the device installation quality, the coverage and service of the GSM operator, the quality of radio signal, etc.

The manufacturer is not responsible for any accident, caused by the use of the device by both the owner and the third party.

All responsibility for using the device falls on the user.

The manufacturer is liable for warranty repair of the device during 12 month starting from the time the product was sold.

The warranty does not apply to devices that are out of order due to the user's fault, in particular in case of violation of the exploitation and installation rules, in case of the damaged warranty seals, in case of mechanical damage presence, as well as in case of malfunctions, caused by lightning strike, short circuit in the electrical grid and so on.

Also the warranty does not apply to the SIM800C module, being a part of the device

## **Scope of delivery**

- |                                  |          |
|----------------------------------|----------|
| 1. EasyDTMF communication device | – 1 pcs. |
| 2. JCG-017 antenna               | – 1 pcs. |
| 3. Plastic mounting racks        | – 3 pcs. |
| 4. Capacitor 22uF 35v            | – 1 pcs. |

# Appendix 1: AdemcoExpress™ to ContactID™ protocol conversion table

## ATTENTION!

*The Ademco identifier and the subscriber's phone number cannot contain «0». When a «0» occurs in the Ademco identifier, the message E35900000 (Contact ID) is transmitted, the same applies to the subscriber's phone number but the transmitted message is E35800000.*

**Table 11. AdemcoExpress™ to ContactID™ code to event conversion.**

Ademco	Contact ID event	Ademco	Contact ID event
11	alarm zone 1	2D	time/date reset
12	alarm zone 2	2E	memory checksum error
13	alarm zone 3	2F	reset to factory settings
14	alarm zone 4	31	restore zone 1
15	alarm zone 5	32	restore zone 2
16	alarm zone 6	33	restore zone 3
17	alarm zone 7	34	restore zone 4
18	alarm zone 8	35	restore zone 5
19	alarm zone 9	36	restore zone 6
1A	alarm zone 10	37	restore zone 7
1B	alarm zone 11	38	restore zone 8
1C	alarm zone 12	39	restore zone 9
1D	alarm zone 13	3A	restore zone 10
1E	alarm zone 14	3B	restore zone 11
1F	alarm zone 15	3C	restore zone 12
21	alarm zone 16	3D	restore zone 13
22	preliminary alarm	3E	restore zone 14
23	restore zone 16	3F	restore zone 15
24	code crack alarm	41	arm group 1 user 1
25	duress alarm	42	arm group 1 user 2
26	partial arm	43	arm group 1 user 3
27	partial arm	44	arm group 1 user 4
28	quick arm	45	arm group 1 user 5
29	alarm cancel	46	arm group 1 user 6
2A	enter programming mode	47	arm group 1 user 7
2B	exit programming mode	48	arm group 1 user 8
2C	enter download mode	49	arm group 1 user 9
4A	arm group 1 user 10	73	arm group 4 user 3

<b>Ademco</b>	<b>Contact ID event</b>	<b>Ademco</b>	<b>Contact ID event</b>
<b>4B</b>	arm group 1 user 11	<b>74</b>	arm group 4 user 4
<b>4C</b>	arm group 1 user 12	<b>75</b>	arm group 4 user 5
<b>4D</b>	arm group 1 with key (zone)	<b>76</b>	arm group 4 user 6
<b>4E</b>	arm group 1 user 14	<b>77</b>	arm group 4 user 7
<b>4F</b>	arm group 1 user 15	<b>78</b>	arm group 4 user 8
<b>51</b>	arm group 2 user 1	<b>79</b>	arm group 4 user 9
<b>52</b>	arm group 2 user 2	<b>7A</b>	arm group 4 user 10
<b>53</b>	arm group 2 user 3	<b>7B</b>	arm group 4 user 11
<b>54</b>	arm group 2 user 4	<b>7C</b>	arm group 4 user 12
<b>55</b>	arm group 2 user 5	<b>7D</b>	arm group 4 with key (zone)
<b>56</b>	arm group 2 user 6	<b>7E</b>	arm group 4 user 14
<b>57</b>	arm group 2 user 7	<b>7F</b>	arm group 4 user 15
<b>58</b>	arm group 2 user 8	<b>81</b>	zone bypass by user 1
<b>59</b>	arm group 2 user 9	<b>82</b>	zone bypass by user 2
<b>5A</b>	arm group 2 user 10	<b>83</b>	zone bypass by user 3
<b>5B</b>	arm group 2 user 11	<b>84</b>	zone bypass by user 4
<b>5C</b>	arm group 2 user 12	<b>85</b>	zone bypass by user 5
<b>5D</b>	arm group 2 with key (zone)	<b>86</b>	zone bypass by user 6
<b>5E</b>	arm group 2 user 14	<b>87</b>	zone bypass by user 7
<b>5F</b>	arm group 2 user 15	<b>88</b>	zone bypass by user 8
<b>61</b>	arm group 3 user 1	<b>89</b>	zone bypass by user 9
<b>62</b>	arm group 3 user 2	<b>8A</b>	zone bypass by user 10
<b>63</b>	arm group 3 user 3	<b>8B</b>	zone bypass by user 11
<b>64</b>	arm group 3 user 4	<b>8C</b>	zone bypass by user 12
<b>65</b>	arm group 3 user 5	<b>8D</b>	zone bypass by user 13
<b>66</b>	arm group 3 user 6	<b>8E</b>	zone bypass by user 14
<b>67</b>	arm group 3 user 7	<b>8F</b>	zone bypass by user 15
<b>68</b>	arm group 3 user 8	<b>91</b>	partial arm by user 1
<b>69</b>	arm group 3 user 9	<b>92</b>	partial arm by user 2
<b>6A</b>	arm group 3 user 10	<b>93</b>	partial arm by user 3
<b>6B</b>	arm group 3 user 11	<b>94</b>	partial arm by user 4
<b>6C</b>	arm group 3 user 12	<b>95</b>	partial arm by user 5
<b>6D</b>	arm group 3 with key (zone)	<b>96</b>	partial arm by user 6
<b>6E</b>	arm group 3 user 14	<b>97</b>	partial arm by user 7
<b>6F</b>	arm group 3 user 15	<b>98</b>	partial arm by user 8
<b>71</b>	arm group 4 user 1	<b>99</b>	partial arm by user 9
<b>72</b>	arm group 4 user 2	<b>9A</b>	partial arm by user 10

<b>Ademco</b>	<b>Contact ID event</b>	<b>Ademco</b>	<b>Contact ID event</b>
<b>9B</b>	partial arm by user 11	<b>C4</b>	disarm group 3 user 4
<b>9C</b>	partial arm by user 12	<b>C5</b>	disarm group 3 user 5
<b>9D</b>	partial arm by user 13	<b>C6</b>	disarm group 3 user 6
<b>9E</b>	partial arm by user 14	<b>C7</b>	disarm group 3 user 7
<b>9F</b>	partial arm by user 15	<b>C8</b>	disarm group 3 user 8
<b>A1</b>	disarm group 1 user 1	<b>C9</b>	disarm group 3 user 9
<b>A2</b>	disarm group 1 user 2	<b>CA</b>	disarm group 3 user 10
<b>A3</b>	disarm group 1 user 3	<b>CB</b>	disarm group 3 user 11
<b>A4</b>	disarm group 1 user 4	<b>CC</b>	disarm group 3 user 12
<b>A5</b>	disarm group 1 user 5	<b>CD</b>	disarm group 3 with key (zone)
<b>A6</b>	disarm group 1 user 6	<b>CE</b>	disarm group 3 user 14
<b>A7</b>	disarm group 1 user 7	<b>CF</b>	disarm group 3 user 15
<b>A8</b>	disarm group 1 user 8	<b>D1</b>	disarm group 4 user 1
<b>A9</b>	disarm group 1 user 9	<b>D2</b>	disarm group 4 user 2
<b>AA</b>	disarm group 1 user 10	<b>D3</b>	disarm group 4 user 3
<b>AB</b>	disarm group 1 user 11	<b>D4</b>	disarm group 4 user 4
<b>AC</b>	disarm group 1 user 12	<b>D5</b>	disarm group 4 user 5
<b>AD</b>	disarm group 1 with key (zone)	<b>D6</b>	disarm group 4 user 6
<b>AE</b>	disarm group 1 user 14	<b>D7</b>	disarm group 4 user 7
<b>AF</b>	disarm group 1 user 15	<b>D8</b>	disarm group 4 user 8
<b>B1</b>	disarm group 2 user 1	<b>D9</b>	disarm group 4 user 9
<b>B2</b>	disarm group 2 user 2	<b>DA</b>	disarm group 4 user 10
<b>B3</b>	disarm group 2 user 3	<b>DB</b>	disarm group 4 user 11
<b>B4</b>	disarm group 2 user 4	<b>DC</b>	disarm group 4 user 12
<b>B5</b>	disarm group 2 user 5	<b>DD</b>	disarm group 4 with key (zone)
<b>B6</b>	disarm group 2 user 6	<b>DE</b>	disarm group 4 user 14
<b>B7</b>	disarm group 2 user 7	<b>DF</b>	disarm group 4 user 15
<b>B8</b>	disarm group 2 user 8	<b>E1</b>	alarm cancel user 1
<b>B9</b>	disarm group 2 user 9	<b>E2</b>	alarm cancel user 2
<b>BA</b>	disarm group 2 user 10	<b>E3</b>	alarm cancel user 3
<b>BB</b>	disarm group 2 user 11	<b>E4</b>	alarm cancel user 4
<b>BC</b>	disarm group 2 user 12	<b>E5</b>	alarm cancel user 5
<b>BD</b>	disarm group 2 with key (zone)	<b>E6</b>	alarm cancel user 6
<b>BE</b>	disarm group 2 user 14	<b>E7</b>	alarm cancel user 7
<b>BF</b>	disarm group 2 user 15	<b>E8</b>	alarm cancel user 8
<b>C1</b>	disarm group 3 user 1	<b>E9</b>	alarm cancel user 9
<b>C2</b>	disarm group 3 user 2	<b>EA</b>	alarm cancel user 10
<b>C3</b>	disarm group 3 user 3	<b>EB</b>	alarm cancel user 11

<b>Ademco</b>	<b>Contact ID event</b>	<b>Ademco</b>	<b>Contact ID event</b>
<b>EC</b>	alarm cancel user 12	<b>F7</b>	output 2 fault
<b>ED</b>	alarm cancel user 13	<b>F8</b>	output 2 restore
<b>EE</b>	alarm cancel user 14	<b>F9</b>	output 3 fault
<b>EF</b>	alarm cancel user 15	<b>FA</b>	output 3 restore 3
<b>F1</b>	AC power fail	<b>FB</b>	tamper switch input alarm
<b>F2</b>	AC power restore	<b>FC</b>	tamper switch input restore
<b>F3</b>	battery fail	<b>FD</b>	lost connection with the communicator
<b>F4</b>	battery restore	<b>FE</b>	wrong time/date
<b>F5</b>	output 1 fault	<b>FF</b>	periodic test message
<b>F6</b>	output 1 restore		

Note: The device automatically detects the type of input protocol and converts the message for the monitoring station if needed.

## ***Appendix 2: Additional ContactID codes transmitted to the monitoring station***

The ContactID codes, which the device sends to the monitoring station depending on certain conditions, are displayed below.

- E603 – periodic radio test. Transmission interval is programmed with the \*0XX\* command.
- E552 – no connection to the security alarm system.
- R552 – connection to the security alarm system restored.
- E305 – device reboot (the device firmware version is specified in the Zone field).
- E359 – forbidden symbol (0) in AdemcoExpress protocol.
- E358 – error in the alarm customer number (programmed as 0000).
- E356 – DTMF package checksum error.
- E353 – no messages from the security alarm system for 25 h.
- R353 – received a message from the security alarm system after a break for more than 25 h.
- E354 – invalid phone number programmed in the security alarm system.
- R354 – restored a valid phone number in the security alarm system.
- E753 – connection to the security alarm system is blocked due to unpaid security service fee.
- E752 – arming the system is blocked due to unpaid security service fee.
- E751 – warning that arming the system can be blocked due to unpaid security service fee.
- E750 – arming the system is unlocked.
- E760 – error in settings for the first (group code) and / or the second (zone code) SIM card (see **table 12**).
- E761 – unable to connect to WiFi network.
- R761 – restored the connection to WiFi network.
- E762 – the remote update is finished, the last digit in the Zone field shows the resulting status, where: 0 — success, everything else — an error code (see **table 13**).
- E360 – first channel fault (SIM1 missing or out of order).
- R360 – first channel restored.
- E361 – first channel first subchannel fault (no connection to the security station using IP1 Port1 via SIM1).
- R361 – first channel first subchannel restored.
- E362 – first channel second subchannel fault (no connection to the security station using IP2 Port2 via SIM1. If both events E361, E362 are present – check the SIM1 account balance).
- R362 – first channel second subchannel restored.
- E363 – second channel fault (SIM2 missing or out of order).
- R363 – second channel restored.
- E364 – second channel first subchannel fault (no connection to the security station using IP1 Port1 via SIM2).
- R364 – second channel first subchannel restored.
- E365 – second channel second subchannel fault (no connection to the security station using IP2 Port2 via SIM2. If both events E364, E365 are present – check the SIM2 account balance).
- R365 – second channel second subchannel restored.
- E366 – third channel fault (unable to register with the WiFi network or get the IP address).
- R366 – third channel restored.

E367 – third channel first subchannel fault (no connection to the security station using IP1 Port1 via WiFi).

R367 – third channel first subchannel restored.

E368 – third channel second subchannel fault (no connection to the security station using IP2 Port2 via WiFi. If both events E367, E368 are present – the WiFi network may not have internet access).

R368 – third channel second subchannel restored.

E316 – first transmission channel is active (SIM1).

E317 – second transmission channel is active (SIM2).

E318 – third transmission channel is active (WiFi).

E764 – switched to the subchannel specified in the Zone field\*.

E770 – activated the output specified in the Zone field (last digit).

R770 – deactivated the output specified in the Zone field (last digit).

\* For the event 764, channel information is stored in the last two digits of the Zone field, where the second last digit is the channel number (1 — SIM1, 2 – SIM2, 3 – WiFi) and the last digit is the sub-channel number (1 — IP1 Port1; 2 – IP2 Port2).



**Table 12.** Description of errors, transmitted with the event code «E760».

<b>Group (SIM1) / Zone (SIM2) code</b>	<b>Error description</b>
0	No errors.
1	SIM card not found (not responding). Clear the SIM card contacts or replace the card if it is out of order.
2	Unable to register SIM card with the mobile network. SIM card may be deactivated by the mobile network operator, replace the card.
3	Unable to establish connection to the GRAPH server using the first IP address/port number. Check the GPRS access point settings, the first IP address and IP port (socket) number, also make sure the SIM card has the mobile data service enabled and the account balance is sufficient.
4	Unable to transmit a test message to the GRAPH server using the first IP address/port number. Check the GRAPH program settings.
5	Unable to establish connection to the GRAPH server using the second IP address/port number. Check the second IP address and IP port (socket) number.
6	Unable to transmit a test message to the GRAPH server using the second IP address/port number. Check the GRAPH program settings.

**Table 13.** Description of errors, transmitted with the event code «E762» - remote update.

<b>Last Zone digit</b>	<b>Error description</b>
0	Update successfully installed.
1	Failed to start an HTTP session.
2	Failed to open HTTP connection to the remote server.
3	Failed to allocate memory for the update or the firmware file is too large.
4	HTTP request error, connection closed by the server.
5	Unexpected end of data stream, empty response from the server.
6	Failed to begin the update or to configure boot from the new firmware, possible flash memory issues.
7	Firmware writing error, likely an invalid firmware file from the server.
8	Firmware checksum does not match, likely a damaged firmware file.
9	Failed to validate and save the new firmware.