https://glab.com.ua

Communication device for one or two SIM cards easyDTMFv9.05 (DUAL SIM) (ContactID™ or AdemcoExpress™ communicator) Installation and usage manual

Lviv 2023

Contents

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 backup channel in case of issues with the mobile network.
- Optional push notifications for the GMonitor mobile application.
- In-browser console that logs status and possible errors when programming or operating.
- Checks connection to the monitoring station before starting operation.
- 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.
- 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 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**.

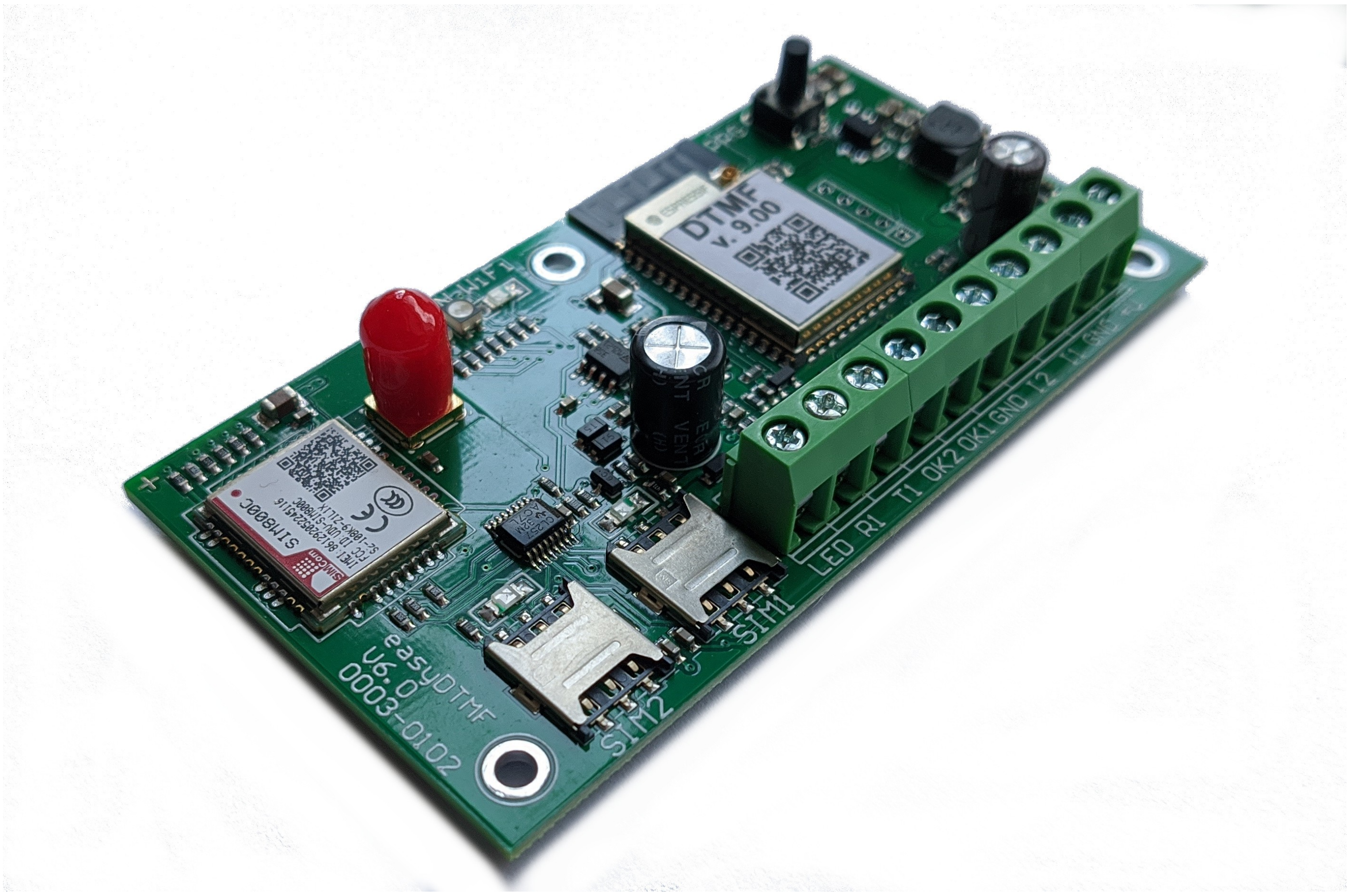


Figure 1

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	**+3ºC...+45ºC**

Electrical specifications

Name	*Parameter*	*Unit*	*Value*
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**

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 main SIM card, "SIM2" – for the backup card.

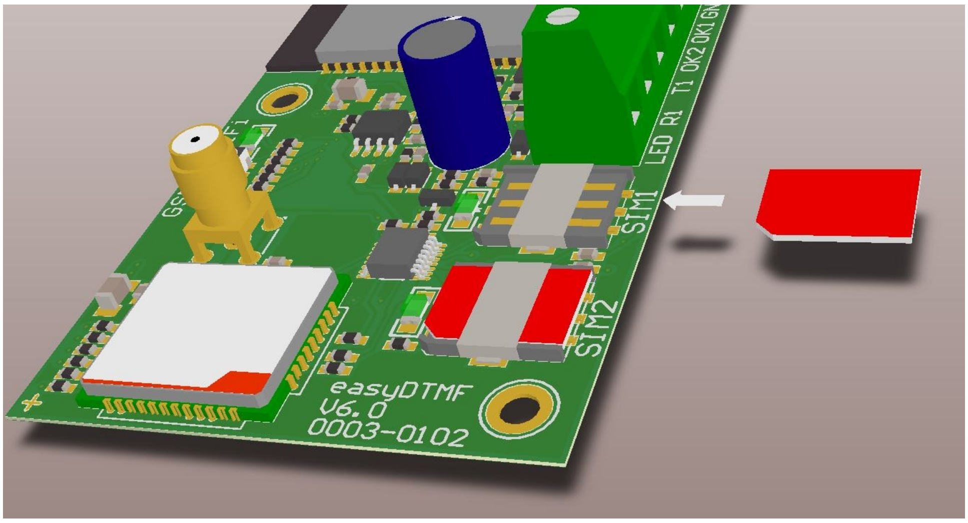


Figure 2

If only one SIM card is used, it has to be installed into the main SIM holder (SIM1). In this case the device will send a backup channel malfunction message to the monitoring station (See **Appendix 2**).

Circuit board overview

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

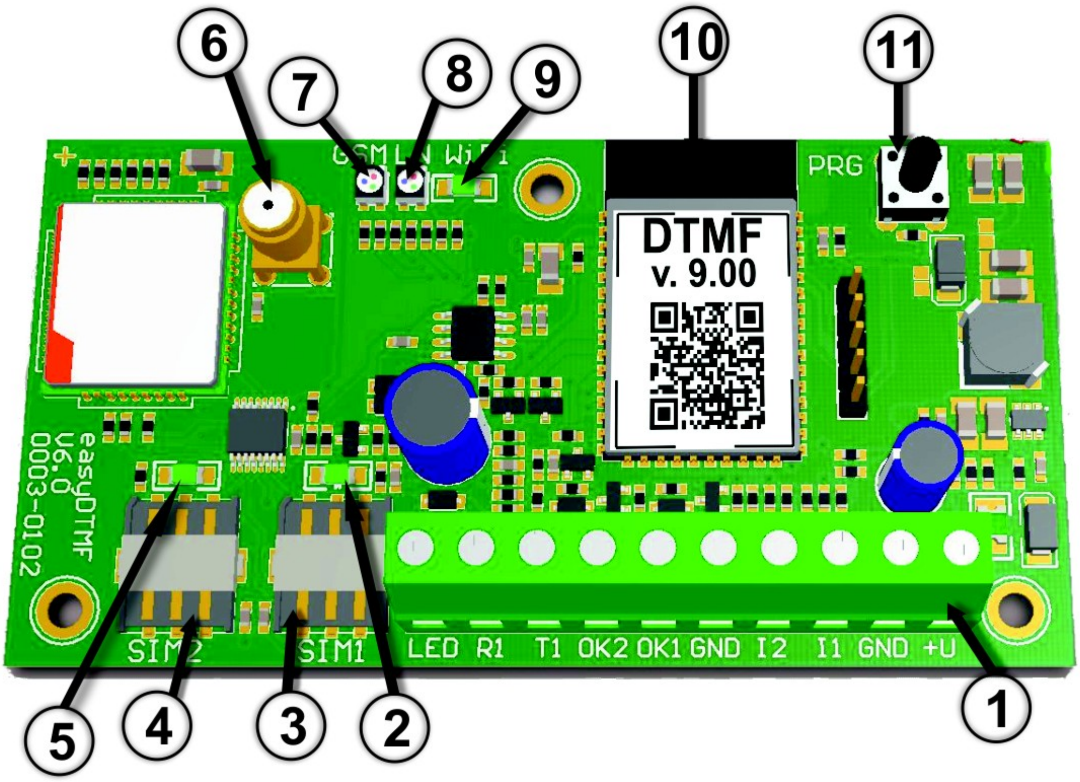


Figure 3

① – Terminals with the inputs and outputs for the alarm control panel. The description of terminals can be found in **table 1**.

② – Green indicating LED for the main SIM card (SIM1). See section “LED indication”.

③ – NanoSIM holder for the main SIM card.

④ – NanoSIM holder for the backup SIM card.

⑤ – Green indicating LED for the backup 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 indicating LED for the WiFi module. See section “LED indication”.

⑩ – WiFi module antenna.

⑪ – Multipurpose button. See section “Multipurpose button”.

Table 1. Description of terminals.

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

Connecting to the alarm control panel

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

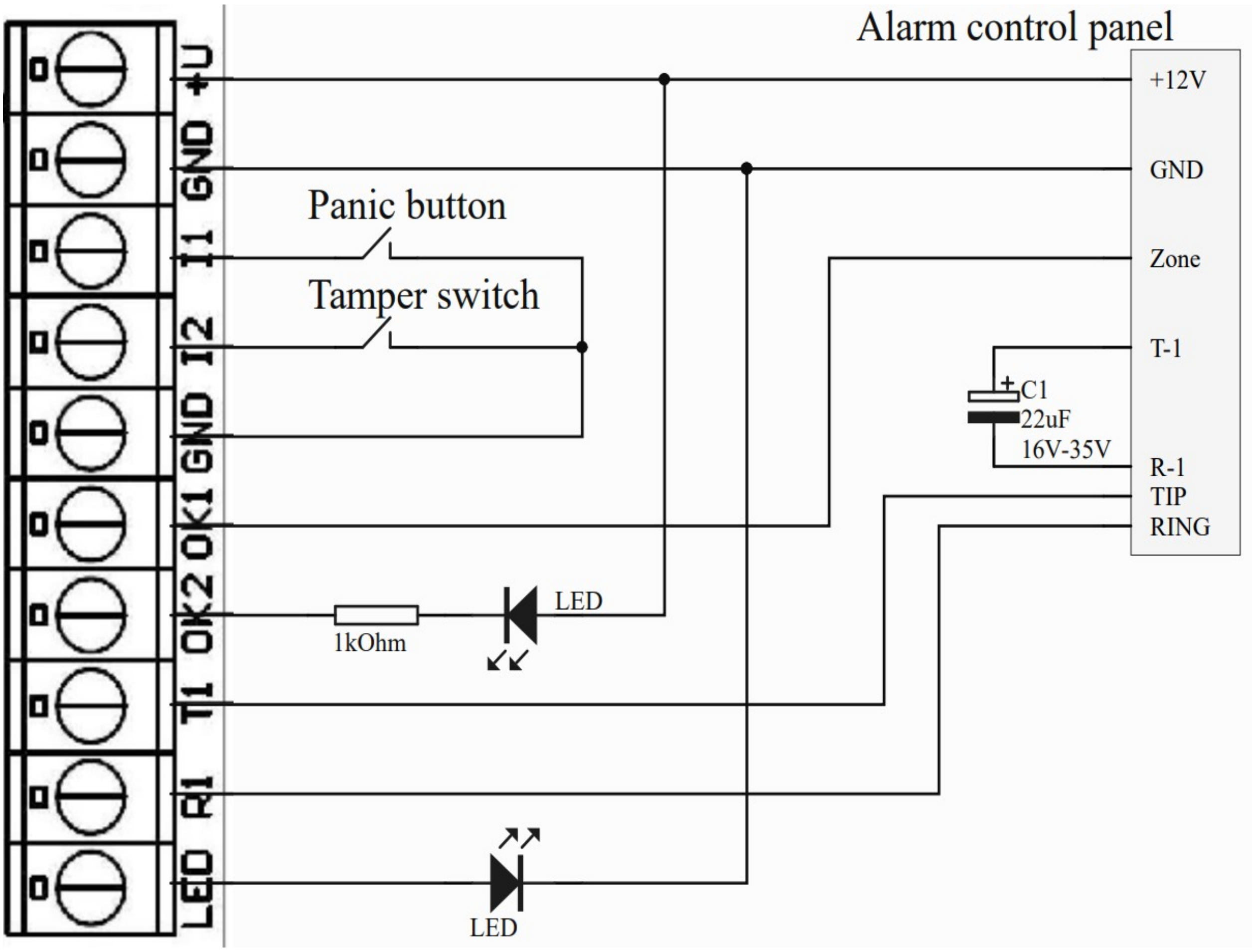
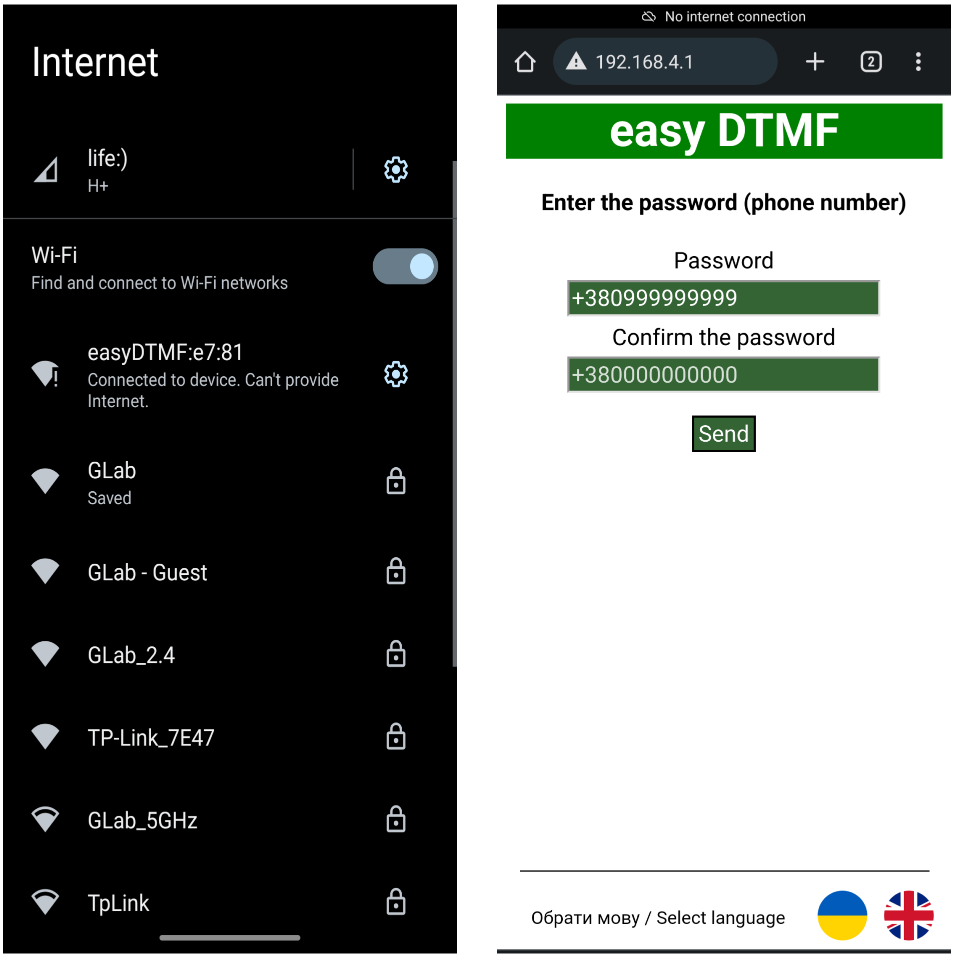


Figure 4

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 main ("SIM1") and backup ("SIM2") SIM cards.
Insert the SIM cards into the device.
If the device was used before, it needs to be reset 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 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.



Internet

life:)
H+

Wi-Fi
Find and connect to Wi-Fi networks

easyDTMF:e7:81
Connected to device. Can't provide Internet.

GLab
Saved

GLab - Guest

GLab_2.4

TP-Link_7E47

GLab_5GHz

TpLink

No internet connection

192.168.4.1

easy DTMF

Enter the password (phone number)

Password
+380999999999

Confirm the password
+380000000000

Send

Обрати мову / Select language

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 (see **figure 5**). Press "Send" when done.

ATTENTION!

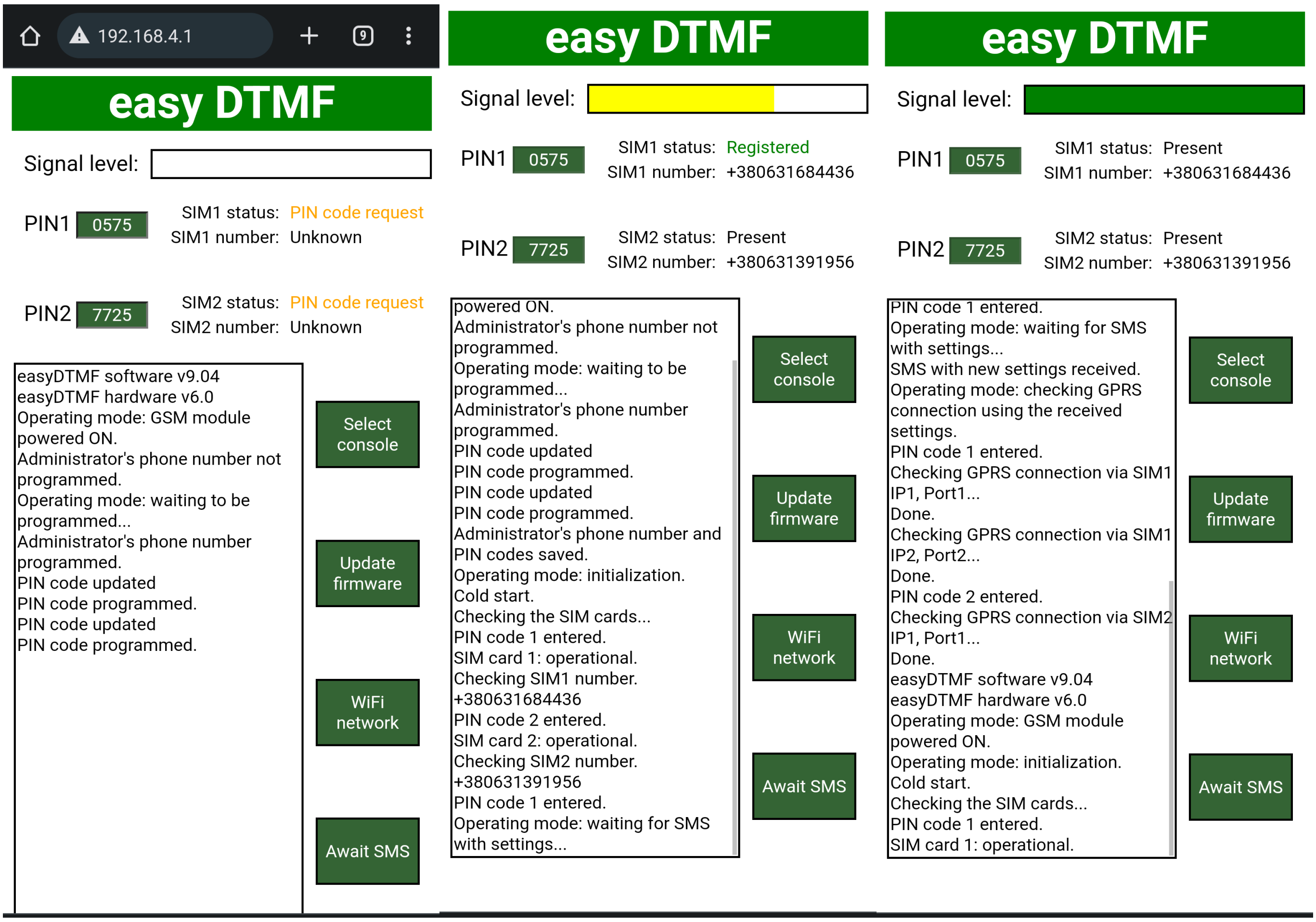
Do not share the password with unauthorized persons. Furthermore, the password can only be changed by resetting the device to factory settings.

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


192.168.4.1

easy DTMF

Signal level:

PIN1 0575 SIM1 status: PIN code request
SIM1 number: Unknown

PIN2 7725 SIM2 status: PIN code request
SIM2 number: Unknown

```
easyDTMF software v9.04
easyDTMF hardware v6.0
Operating mode: GSM module
powered ON.
Administrator's phone number not
programmed.
Operating mode: waiting to be
programmed...
Administrator's phone number
programmed.
PIN code updated
PIN code programmed.
PIN code updated
PIN code programmed.
```

easy DTMF

Signal level:

PIN1 0575 SIM1 status: Registered
SIM1 number: +380631684436

PIN2 7725 SIM2 status: Present
SIM2 number: +380631391956

```
powered ON.
Administrator's phone number not
programmed.
Operating mode: waiting to be
programmed...
Administrator's phone number
programmed.
PIN code updated
PIN code programmed.
PIN code updated
PIN code programmed.
Administrator's phone number and
PIN codes saved.
Operating mode: initialization.
Cold start.
Checking the SIM cards...
PIN code 1 entered.
SIM card 1: operational.
Checking SIM1 number.
+380631684436
PIN code 2 entered.
SIM card 2: operational.
Checking SIM2 number.
+380631391956
PIN code 1 entered.
Operating mode: waiting for SMS
with settings...
```

easy DTMF

Signal level:

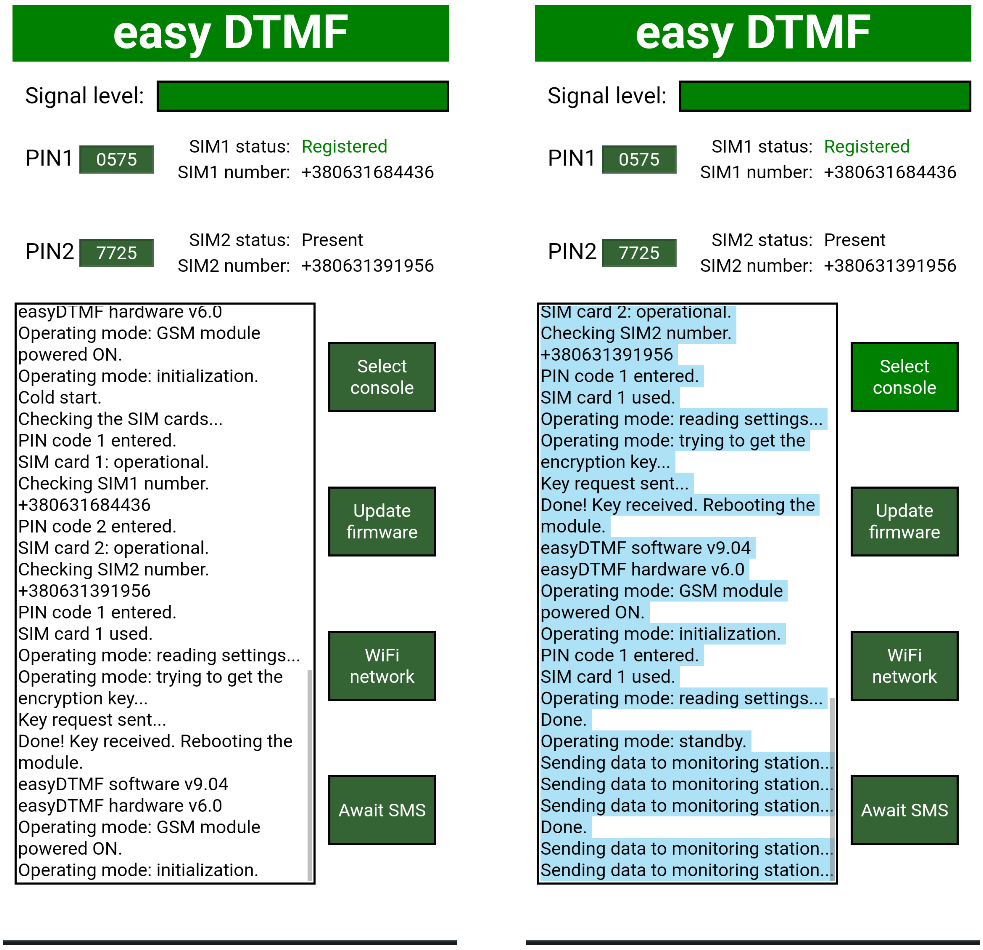
PIN1 0575 SIM1 status: Present
SIM1 number: +380631684436

PIN2 7725 SIM2 status: Present
SIM2 number: +380631391956

```
PIN code 1 entered.
Operating mode: waiting for SMS
with settings...
SMS with new settings received.
Operating mode: checking GPRS
connection using the received
settings.
PIN code 1 entered.
Checking GPRS connection via SIM1
IP1, Port1...
Done.
Checking GPRS connection via SIM1
IP2, Port2...
Done.
PIN code 2 entered.
Checking GPRS connection via SIM2
IP1, Port1...
Done.
easyDTMF software v9.04
easyDTMF hardware v6.0
Operating mode: GSM module
powered ON.
Operating mode: initialization.
Cold start.
Checking the SIM cards...
PIN code 1 entered.
SIM card 1: operational.
```

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). 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.



easy DTMF

Signal level:

PIN1 0575 SIM1 status: Registered
SIM1 number: +380631684436

PIN2 7725 SIM2 status: Present
SIM2 number: +380631391956

```
easyDTMF hardware v6.0
Operating mode: GSM module
powered ON.
Operating mode: initialization.
Cold start.
Checking the SIM cards...
PIN code 1 entered.
SIM card 1: operational.
Checking SIM1 number.
+380631684436
PIN code 2 entered.
SIM card 2: operational.
Checking SIM2 number.
+380631391956
PIN code 1 entered.
SIM card 1 used.
Operating mode: reading settings...
Operating mode: trying to get the
encryption key...
Key request sent...
Done! Key received. Rebooting the
module.
easyDTMF software v9.04
easyDTMF hardware v6.0
Operating mode: GSM module
powered ON.
Operating mode: initialization.
```

easy DTMF

Signal level:

PIN1 0575 SIM1 status: Registered
SIM1 number: +380631684436

PIN2 7725 SIM2 status: Present
SIM2 number: +380631391956

```
SIM card 2: operational.
Checking SIM2 number.
+380631391956
PIN code 1 entered.
SIM card 1 used.
Operating mode: reading settings...
Operating mode: trying to get the
encryption key...
Key request sent...
Done! Key received. Rebooting the
module.
easyDTMF software v9.04
easyDTMF hardware v6.0
Operating mode: GSM module
powered ON.
Operating mode: initialization.
PIN code 1 entered.
SIM card 1 used.
Operating mode: reading settings...
Done.
Operating mode: standby.
Sending data to monitoring station...
Sending data to monitoring station...
Sending data to monitoring station...
Done.
Sending data to monitoring station...
Sending data to monitoring station...
```

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.

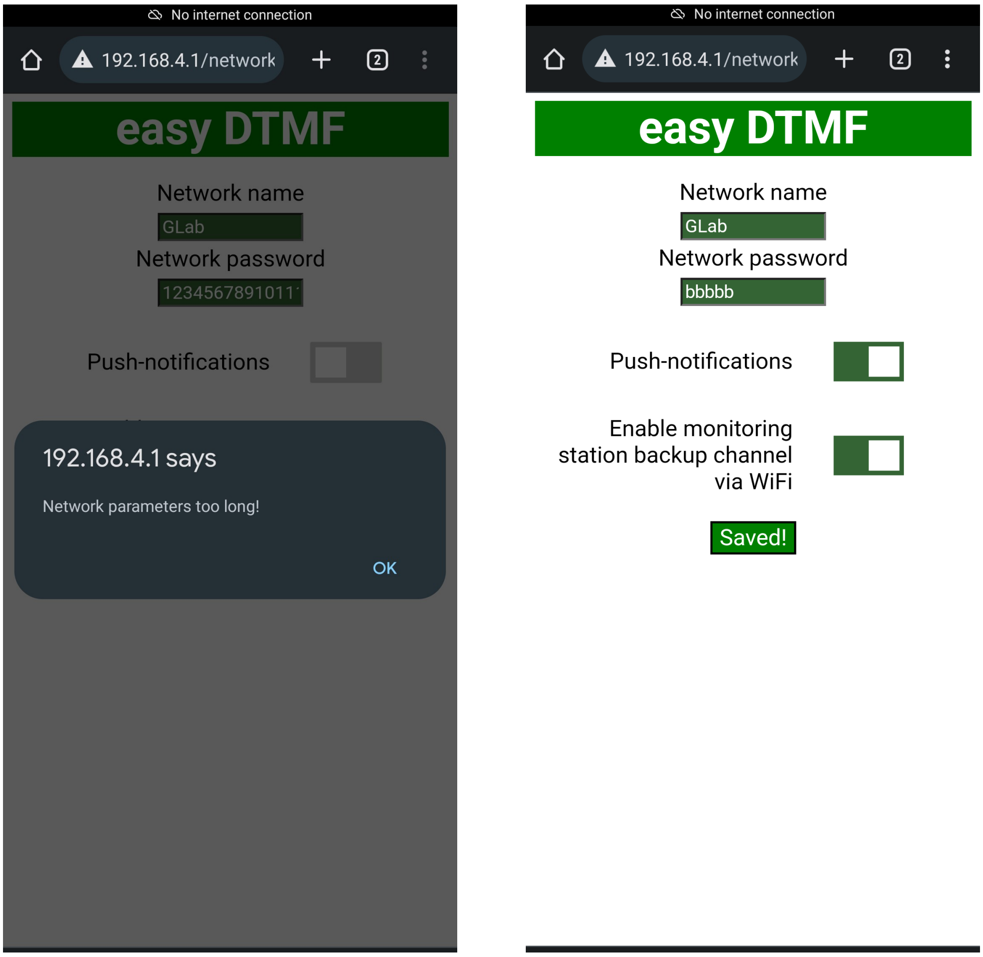
The current SIM card phone number is displayed under the SIM card status. If the device shows an error instead of the phone number, the SIM card is either not activated, or does not support the USSD phone number request. While in factory settings, the SIM cards are not yet registered with the mobile 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 backup 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.



No internet connection

192.168.4.1/network

easy DTMF

Network name: GLab

Network password: 12345678910111

Push-notifications

192.168.4.1 says

Network parameters too long!

No internet connection

192.168.4.1/network

easy DTMF

Network name: GLab

Network password: bbbbb

Push-notifications

Enable monitoring station backup channel via WiFi

Saved!

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 «ОК1» or «ОК2».

Values sent in SMS	*Operating mode description*
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 ОК1, ОК2».**
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 ОК1, ОК2».**
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.**

LED indication

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

Table 3. Indicating LED "GSM" ⑦.

Color	*Timing*	*Description*
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 "**Programming the device**").
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 **table 4**).
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 **table 4**).
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 **table 4**).

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

Color	*Signal strength*	*Notes*
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.

Color	*Timing*	*Description*
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

Color	***Timing***	***Description***
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 ●	Two short (72 ms) flashes once per second.	Connected to the programmed WiFi access point in station mode. The push notification server and/or the backup WiFi 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 the push notification server. If this persists for a few minutes, check the diagnostic console log for additional details.

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

LED	***Timing***	***Description***
②	Turned off.	Main SIM card not found.
② ●	On for 72 ms, off for 672 ms. Looks like a short flash once per second.	Main SIM card is present but not used.
② ●	On for 422 ms, off for 422 ms. Looks like a long flash once per second.	Main SIM card is registered with the mobile network.
② ●	Solid on.	Connected to the GRAPH server using the main SIM card.
② ●	On for 72 ms, off for 72 ms. Looks like frequent blinking.	Attempting data transmission to the monitoring station using the main SIM card.
⑤	Turned off.	Backup SIM card not found.
⑤ ●	On for 72 ms, off for 672 ms. Looks like a short flash once per second.	Backup SIM card is present but not used.
⑤ ●	On for 422 ms, off for 422 ms. Looks like a long flash once per second.	Backup SIM card is registered with the mobile network.
⑤ ●	Solid on.	Connected to the GRAPH server using the backup SIM card.
⑤ ●	On for 72 ms, off for 72 ms. Looks like frequent blinking.	Attempting data transmission to the monitoring station using the backup 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 access point mode will change to the opposite (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.

Command	*Example*	*Description*
0XX	***010***	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.
1X	***10***	OK1 operating mode. 0 – monostable, 1 – bistable, 2– arm confirmation, 3 – security service fee notification/arm blocking .
2X	***20***	OK2 opearating mode. 0 – monostable, 1 – bistable, 2– arm confirmation, 3 – security service fee notification/arm blocking.
3XXXX	***31111***	Customer identifier (number) for the monitoring station. 4 digits.
4xxx.xxx.xxx.xxx	***4192.168.1.1***	IP address of the GRAPH receiver first channel (line).
5xxxxx	***510000***	IP port (socket) number of the GRAPH receiver first channel (line). Must contain 5 digits.
6xxx.xxx.xxx.xxx	***6192.168.1.2***	IP address of the GRAPH receiver second channel (line).
7xxxxx	***710000***	IP port (socket) number of the GRAPH receiver second channel (line). Must contain 5 digits.
8xxxxxxxxxx	***8internet***	Name of GPRS access point for the main SIM card (SIM1).
9xxxxxxxxxx	***9www.umc.ua***	Name of GPRS access point for the backup SIM card (SIM2).
Ax	***A0***	Input operating mode. Placeholder for future software versions.
Dxx	***D11***	Open collector management (see **Managing outputs OK1, OK2**).
E	***E***	Reset the settings.
F	***F***	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.

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

Command (*DXX*DYY)	***Description***
D10	Deactivate OK1
D11	Activate OK1
D20	Deactivate OK2
D21	Activate OK2

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

Command (*DXXX*DYYY*)	***Description***
D1XX	Activate OK1 for XX seconds* **
D2YY	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.

✋**ATTENTION!**

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

Management commands are sent exclusively to the main SIM card phone number.

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 2: missing.” The device is unable to detect a backup 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 settings field is 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 main SIM card.

"Error in settings: SIM2 access point name" — error in GPRS access point name for the backup 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 main SIM card PIN code.

"Error in settings: SIM2 PIN" — error in the backup 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. This error is critical and requires action. The error can occur due to the SIM card 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 SIM1."

"Service may be inactive, or the account has insufficient funds."
"Resetting all settings."
Or:
"No communication via SIM1. 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 1: PIN code error or missing" PIN code error (or a wrong PIN code was entered) for the main SIM card. The SIM card may be deactivated.

"SIM 2: BLOCKED." The backup SIM card is blocked. A mobile phone and a PUK code is needed to unlock it.

"SIM 2: PIN code error or missing" PIN code error (or a wrong PIN code was entered) for the backup SIM card. The SIM card may be deactivated.

"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 1: unable to register. Rebooting the module." Unable to register the main SIM card with the mobile network. Check the SIM card.

"SIM 2: unable to register. Rebooting the module." Unable to register the backup SIM card with the mobile network. Check the SIM card.

"SIM 2: card error. Rebooting the module." Backup SIM card fault. Check the SIM card.

"PIN code 1 not entered but required." The device detected that the main SIM card PIN code has not been submitted but is required to register with the network. Program the PIN code.

"PIN code 1 mismatch, reset to factory settings." The device detected that the main 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 1. Check SIM card 1." No response from the main SIM card after the PIN code was entered. The SIM card may be faulty.

"PIN code 2 not entered but required." The device detected that the backup SIM card PIN code has not been submitted but is required to register with the network. Program the PIN code.

"PIN code 2 mismatch, reset to factory settings." The device detected that the backup 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 2. Check SIM card 2." No response from the backup 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.

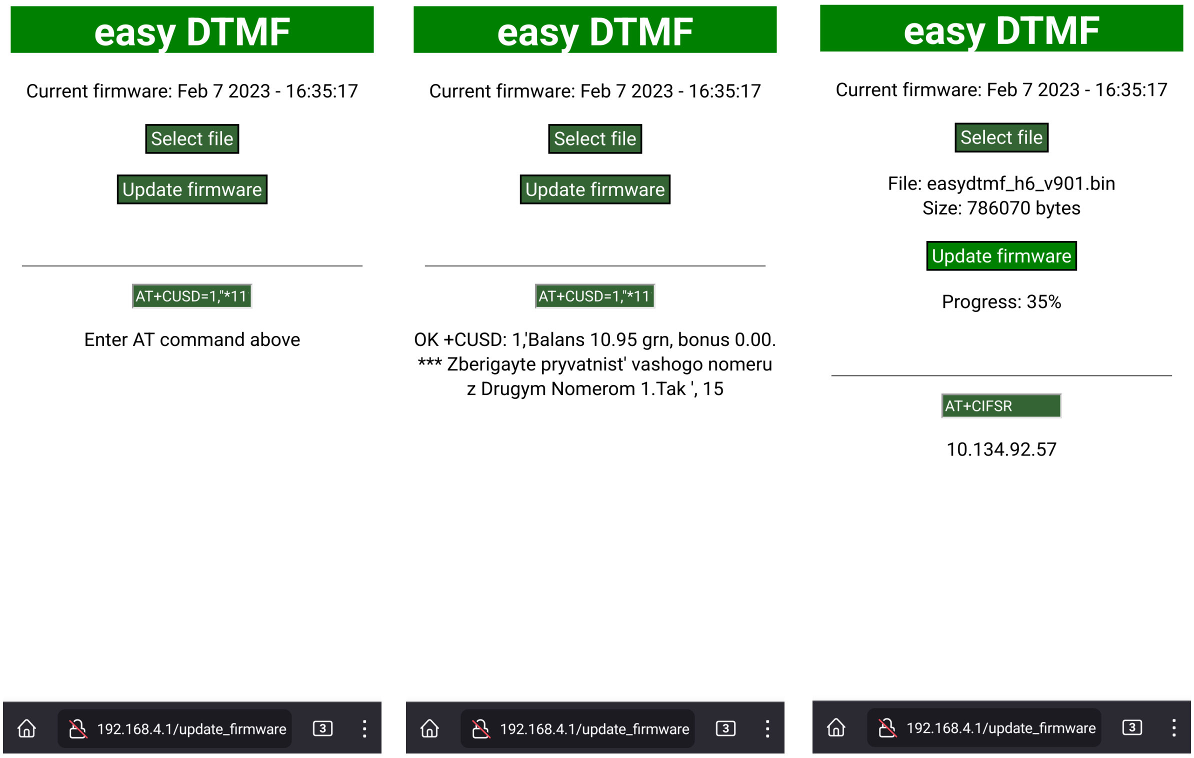
"Unable to connect to WiFi AP! Check the SSID / password." The WiFi network with the provided name cannot be found or the password does not match. Make sure that the network requisites are correct.

"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.
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 8**).
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 while 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.



Current firmware: Feb 7 2023 - 16:35:17

AT+CUSD=1,"*11

Enter AT command above

Current firmware: Feb 7 2023 - 16:35:17

AT+CUSD=1,"*11

OK +CUSD: 1,'Balans 10.95 grn, bonus 0.00. *** Zberigayte pryvatnist' vashogo nomeru z Drugym Nomerom 1.Tak ', 15

Current firmware: Feb 7 2023 - 16:35:17

File: easydtmf_h6_v901.bin
Size: 786070 bytes

Progress: 35%

AT+CIFSR

10.134.92.57

Figure 8

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 8**). 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.

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

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

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

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

E603 – periodic radio test. Transmission frequency 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).
E315 – backup channel fault (SIM card 2 not found).
E316 – switching to the main transmission channel (SIM1).
E317 – switching to the backup transmission channel (SIM2).
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 of the main (group code) or the backup (zone code) SIM card (see **table 12**).

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

Group code (main SIM)	**Zone code (backup SIM)**	**Error description**
3		Unable to establish connection to the GRAPH server via the first IP address/port number. Check the GPRS access point settings, the IP address and the IP port (socket) number.
4		Unable to transmit a test message to the GRAPH server via the first IP address/port number. Check the GRAPH software settings.
5		Unable to establish connection to the GRAPH server via the second IP address/port number. Check the GPRS access point settings, the IP address and the IP port (socket) number.
6		Unable to transmit a test message to the GRAPH server via the second IP address/port number. Check the GRAPH software settings.
	2	Backup SIM card not found (not responding). Clear the SIM card contacts or replace the card if it is out of order.

Group code (main SIM)	Zone code (backup SIM)	Error description
	3	Unable to establish connection to the GRAPH server via the first IP address/port number. Check the GPRS access point settings, the IP address and the IP port (socket) number.
	4	Unable to transmit a test message to the GRAPH server via the first IP address/port number. Check the GRAPH software settings.