



<https://play.google.com/store/apps/details?id=ua.com.glab.easygsmv40>
www.glab.com.ua

**Notification device
for one or two SIM cards
easyDTMFv8.0 (DUAL SIM)
(ContactID™ or AdemcoExpress™ communicator)
Installation and user guide**

Contents

Review of functions.	3
Purpose.	3
Specifications.	4
Work preparation, connection and programming.	4
Requirements for SIM cards of GSM operator.	4
SIM card installation.	5
Purpose of inputs.	5
Connection to security alarm.	5
Template recording.	5
Programming.	6
Connecting the outputs.	6
LED indication.	7
Working modes of outputs.	9
SMS command format.	10
Programming the settings.	10
Output OK1, OK2 management.	11
Warranty.	11
Scope of delivery.	12
Appendix 1: Example of the device connection.	12
Appendix 2: The GRAPH server program usage.	13
Appendix 3: Table of recoding AdemcoExpress™ to ContactID™.	16
Appendix 4: List of additional ContactID codes, which are transmitted to the security monitoring station.	20

Review of functions

- Programming without a computer.
- Usage of two SIM cards from different operators.
- Possibility to use with one SIM card.
- Error indication while programming and working.
- Check of connection to the security monitoring station before start of work.
- Cellular network signal strength indication.
- Work with any security alarms that support ContactID™ or AdemcoExpress™ telephone protocols.
- 2 potential inputs for «alarm button» and «tamper» event transmission.
- 2 «open collector» type outputs, each of them can be managed from the security monitoring station phone.
- Programmable «life pulse» transmit time.
- Work with the security monitoring station using the encrypted protocol **GLab-crypto**.
- Security monitoring station notification of «power off» by transmitting a «device reboot» event.

Purpose

EasyDTMF communicator is a device of alarm signal transmission from centrals that support the ContactID™ or AdemcoExpress™ telephone protocols to the security monitoring station, using the GLab-crypto™ protocol. External view of the device is shown on **figure 1**.



Figure 1.

Specifications

Performance characteristics

Quantity of inputs	2
Quantity of «open collector» type outputs	2
SIM card standard that is supported	GSM
Quantity of SIM cards that is supported	2
Format of information transmission to the security monitoring station	Glab-crypto
Max. quantity of the security monitoring station server addresses	2
Real-time clock	Yes
Power on ready time, seconds, not more than	60

Electrical specifications

Name	Parameter	Unit	Value
Device supply voltage	U_{pwrdc}	V	+10...+15
Max. current consumption	I_{pwrmax}	mA	1000
Current consumption in stand-by mode, around	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	$U_{pwrdc}*0,75$
Max. voltage of log. «0» at the inputs I1 – I2	$U0_{max}$	V	$U_{pwrdc}*0,25$
Min. voltage of log. «0» at the inputs I1 – I2	$U0_{min}$	V	0
Max. load current on OK1 and OK2 outputs (not protected)	I_{okmax}	mA	100
Max. allowed DC voltage on OK1 and OK2 outputs	U_{okmax}	V	15

GSM modem

Frequency range	GSM 850/EGSM 900/ DCS 1800/ PCS1900, automatic selection
GSM class	Small MS
Transmitter power	Class 4 (2W) at EGSM900/GSM850 Class 1 (1W) at DCS1800/PCS1900
SIM interface	Support SIM card: 1,8V, 3V

Work preparation, connection and programming

Requirements for SIM cards of GSM operator.

The device supports standard GSM Phase1, GSM Phase2+ SIM cards with 1,8 and 3 Volts supply voltage. This means that any operator SIM card manufactured not earlier than 2004 will work.

All SIM cards must be activated, also the PIN request when turning on the phone must be cancelled for both cards.

SIM card installation.

Connect the antenna to the SMA connector of the device.

ATTENTION!

Turning on 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 card into the device from the external side (see **figure 1**). The upper SIM holder is intended for the main SIM card, the lower one – for the backup card.

When using only one SIM card the device works only with the main SIM card. In this case the device will send a message to the monitoring station about a malfunction of the backup channel. (See Appendix 4).

Purpose of inputs.

Table 1. Purpose of the device inputs.

<i>Input</i>	<i>Purpose</i>
+U	«+» device power supply. Possible voltage from 10 to 15 Volts DC.
GND	«-» device power supply. Common.
I1	Input for connection of the alarm button. Active level «1». If not used, must be connected to «GND».
I2	Tamper input. Active level «1». If not used, must be connected to «GND».
GND	«-» device power supply. Common.
OK1	«Open collector» type output which is commutated to «-» device power supply.
OK2	«Open collector» type output which is commutated to «-» device power supply.
T1	Input for connecting the telephone line from the security alarm.
R1	Input for connecting the telephone line from the security alarm.
LED	Output for connecting the anode («+») of LED indicating arming confirmation.

Connection to security alarm.

The (typical) example of device connection is displayed in Appendix 1.

Template recording.

An automatic recording of the necessary for the device to work monitoring station administrator's phone number is possible to the phone book of the main SIM card.

In order to do so you need to delete an entry named «GBGPRS001» from the main SIM card phone book (if the card has already been used in the device), install the SIM cards (main and backup) with removed PIN request into the device and power the device. In around 60 seconds the red LED «7» will light up – the template has been recorded into the main SIM card phone book. Turn off the power, remove the main SIM card. See section *LED indication* for more specific information on LED indication.

Programming.

Before the programming start, write down the phone number of the security monitoring station (the operator's mobile phone number) to the main SIM card cell named «GBGPRS001» using your cell phone.

Insert the main SIM card into the device. Power the device. In around 60 seconds the LED «7» (red) will blink 1 time with a 2 second pause. It means that the device is in the standby mode, awaiting an SMS with programming settings. The SMS format is described in section *SMS command format*.

After receiving an SMS with the correct settings the device reboots and tries to establish connection with the GRAPH server, IP addresses and port numbers of which were written in the SMS. This mode is indicated by double blink of the LED «7» (red) with a 2 second pause. After a successful connection with the GRAPH server is established, the device will reboot and enter the standby mode, sending a request for an encryption key to the security monitoring station operator and waiting for response. (See Appendix 2: The GRAPH server program usage). Triple blink of the LED «7» (red) with a 2 second pause indicates this state. If the LED indication in mentioned above modes differs from the one described, see section *LED indication*.

ATTENTION!

The GRAPH client must be running at the monitoring station operator's workplace in order for him to receive an encryption key request.

After obtaining a permission to receive the key, given by the operator, the device reboots and enters the main working mode (information transmission to the monitoring station). (See section *LED indication*).

ATTENTION!

Phone number for security alarm programming is «1». Protocol ContactID or AdemcoExpress.

Connecting the outputs.

The device outputs are of «open collector» type and are commutated to the common ground. The outputs can be used for remote management of various equipment, control of security panel operation or arming confirmation indicating LED management by the security monitoring station operator.

ATTENTION!

The device outputs have limited loaded capability. Output current MUST NOT EXCEED 100mA!

LED indication.

The LED indication (see **figure 2**) of the device works in **five modes**.

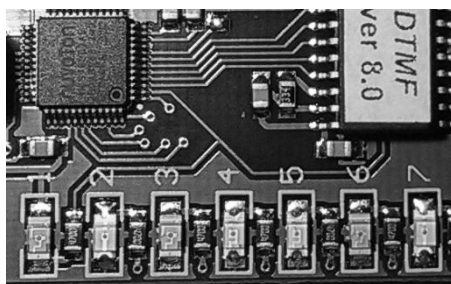


Figure 2.

Mode 1– error indication (red LED «7» glows constantly).

This mode is often used while the device is turning on to inform the user of the device's inability to work properly. The yellow LED «6» shows the error code. The green LEDs «4» and «5» show the entry number where a mistake is found. For example, if LED «5» blinks 7 times in a row after a pause, it means that the error is in entry №7 (see **Table 2**).

Table 2. Error codes of the device.

<i>LED «6», number of impulses</i>	<i>Error description</i>
1	Error in the programming entry. Read the error code and change the SMS with the programming settings.
2	SIM card error. Clear all the SIM card contacts or replace the card.
3	PIN code error. Turn off the PIN code request in the security settings.
4	No connection to the GSM modem. Contact the manufacturer's service.
5	Backup SIM card or backup SIM card settings error. The error code will be transmitted to the security monitoring station as soon as possible. (See Appendix 4).

ATTENTION!

The device indicates errors only for 60 seconds. Afterwards the device will reboot the GSM modem and perform another attempt to enter the working mode. This does not concern the standby mode while waiting for the encryption key or an SMS with settings.

Mode 2 (red LED «7» blinks 1 time per two seconds) – **awaiting an SMS with settings**.

Yellow LED «6» is used to indicate the operation of the GSM modem. If the LED «6» blinks 1 time per second, it means that the modem is being registered at the GSM operator network. If the LED «6» blinks 1 time per 3 seconds, the modem is registered in the network. The green LEDs «5», «4» are used to display signal strength of the cellular network operator. Approximate signal level values are displayed in **Table 3**. The green LEDs «8» («S1») and «9» («S2») are used to indicate the device working mode with SIM cards (see **Table 4**).

Mode 3 (red LED «7» blinks 2 times per two seconds) – **GPRS connection to the GRAPH program check on all IP addresses and SIM cards.**

Yellow LED «6» is used to indicate the operation of the GSM modem. If the LED «6» blinks 1 time per second, it means that the modem is being registered in the GSM operator network. If the LED «6» blinks 1 time per 3 seconds, the modem is registered at the network. If the LED «6» blinks 2 times per second, the GPRS connection to the GRAPH program is established. The green LEDs «5», «4» are used to display signal strength of the cellular network operator. Approximate signal level values are displayed in **Table 3**. The green LEDs «8»(«S1») and «9»(«S2») are used to indicate the device working mode with SIM cards (see **Table 4**).

Mode 4 (red LED «7» blinks 3 times per two seconds) – **an attempt to receive the encryption key from the monitoring station operator.**

Yellow LED «6» is used to indicate the operation of the GSM modem. If the LED «6» blinks 1 time per second, it means that the modem is being registered in the GSM operator network. If the LED «6» blinks 1 time per 3 seconds, the modem is registered at the network. If the LED «6» blinks 2 times per second, the GPRS connection to the GRAPH program is established. The green LEDs «5», «4» are used to display signal strength of the cellular network operator. Approximate signal level values are displayed in **Table 3**. The green LEDs «8»(«S1») and «9»(«S2») are used to indicate the device working mode with SIM cards (see **Table 4**).

Mode 5 (red LED «7» does not glow) – **working mode.**

Yellow LED «6» is used to indicate the operation of the GSM modem. If the LED «6» blinks 1 time per second, it means that the modem is being registered in the GSM operator network. If the LED «6» blinks 1 time per 3 seconds, the modem is already registered at the network. If the LED «6» blinks 2 times per second, the GPRS connection to the GRAPH program is established. The green LEDs «5», «4» are used to display signal strength of the cellular network operator. Approximate signal level values are displayed in **Table 3**. The green LEDs «8»(«S1») and «9»(«S2») are used to indicate the device working mode with SIM cards (see **Table 4**).

Table 3. Approximate level values of the cellular network operator signal.

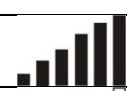



<i>Level</i>			<i>Notes</i>
«4»	«5»		
Glow	Glow		Maximum signal strength.
Does not glow	Glow		At about 50% signal strength. Enough for normal device operation.
Does not glow	Blinks 2 times per second		Signal strength is not enough for normal device operation. External antenna is needed.
Does not glow	Blinks 4 times per second		The device cannot operate. External antenna is needed.

Table 4. LED «8»(«S1») and «9»(«S2») indication.

<i>LED</i>	<i>Indication</i>	<i>Description of indication</i>
«8» («S1»)	Does not glow.	The main SIM card not found.
«8» («S1»)	Short blink 1 time per second.	The main SIM card is present but not used.
«8» («S1»)	Long blink 1 time per second.	The main SIM card is registered at the network.
«8» («S1»)	Glowes constantly.	The connection to the GRAPH program is established using the main SIM card.
«8» («S1»)	Blinks often.	Attempting transmission to the monitoring station using the main SIM card.
«9» («S2»)	Does not glow.	The backup SIM card not found.
«9» («S2»)	Short blink 1 time per second.	The backup SIM card is present but not used.
«9» («S2»)	Long blink 1 time per second.	The backup SIM card is registered at the network.
«9» («S2»)	Glowes constantly.	The connection to the GRAPH program is established using the backup SIM card.
«9» («S2»)	Blinks often.	Attempting transmission to the monitoring station using the backup SIM card.

LED «1» (yellow) – indication of «picked up handset» signal (opposite to HUP signal).

LED «2» (red) – security alarm transmission line emergency (breach).

LED «3» (yellow) – indication of «HANDSHAKE» and «KISSOFF» signals.

Working modes of outputs.

Every output of the device has 3 independent working modes (see **Table 5**).

Table 5. Working modes of outputs «OK1» or «OK2».

<i>Values sent in SMS</i>	<i>Working 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 «Output OK1, OK2 management».
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 «Output OK1, OK2 management».
2	The according output controls the LED that is indicating arming confirmation. In case of successful transmission of the «armed» message to the monitoring station, this output becomes activated for 60 seconds.

SMS command format

Programming the settings.

A text SMS with commands «*1XX*CYYY*» inside the message body is used to program the settings. List of commands is displayed in **Table 6**.

Table 6.

<i>Command</i>	<i>Example</i>	<i>Note</i>
0XX	*010*	Frequency of sending the test message to the security monitoring station. Number x 30 seconds. In case of 00 the test message will not be sent.
1X	*10*	OK1 working mode. 0 – monostable, 1 – bistable, 2– arming confirmation (receipt).
2X	*20*	OK2 working mode. 0 – monostable, 1 – bistable, 2– arming confirmation (receipt).
3XXXX	*31111*	Object number for transmission to the monitoring station. 4 digits.
4xxx.xxx.xxx.xxx	*4192.168.1.1*	IP address of the GRAPH receiver first line.
5xxxxx	*510000*	IP port number (socket) of the GRAPH receiver first line. Must contain 5 digits.
6xxx.xxx.xxx.xxx	*6192.168.1.2*	IP address of the GRAPH receiver second line.
7xxxxx	*710000*	IP port number (socket) of the GRAPH receiver second line. Must contain 5 digits.
8xxxxxxxxxxx	*8internet*	Name of the GPRS access point for the main SIM card (SIM1).
9xxxxxxxxxxx	*9www.umc.ua*	Name of the GPRS access point for the backup SIM card (SIM2).
Ax	*A0*	Input working mode. Reserved for the following program versions.
Dxx	*D11*	Open collector management (see section Output OK1, OK2 management).
E	*E*	Settings reset.
F	*F*	Remote device reboot.

An example of SMS for settings programming:

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

ATTENTION!

All of the IP addresses and access point names in the example above are given only for understanding the SMS format!

Note that the usage of the Cyrillic alphabet inside the SMS is unacceptable.

Output OK1, OK2 management.

A text SMS with commands «*DXX*DYYY*» inside the message body are used to manage outputs. List of commands is displayed in **Table 7** and **Table 8**.

There can be several commands in the message body separated by the «space» symbol.

Table 7. Commands for SMS managing the outputs in mode «0». Monostable mode.

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

Table 8. Commands for SMS managing the outputs in mode «1». Bistable mode.

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

* Maximum time for the output to be active is 99 seconds.

** If XX or YY equal 00, the output will be activated for minimum 2 seconds.

ATTENTION!

The device ignores incorrect commands or commands which contain Cyrillic letters in the message body.

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

Warranty

ATTENTION! The manufacturer of the product is liable only within the limits of the warranty obligation for the operation of the device itself and is not responsible for the installation quality of the device, the coverage and service of the GSM operator, the quality of the 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 the exploitation and installation rules violation, 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 network and so on. Also the warranty does not apply to the SIM900 module which is a part of the device.

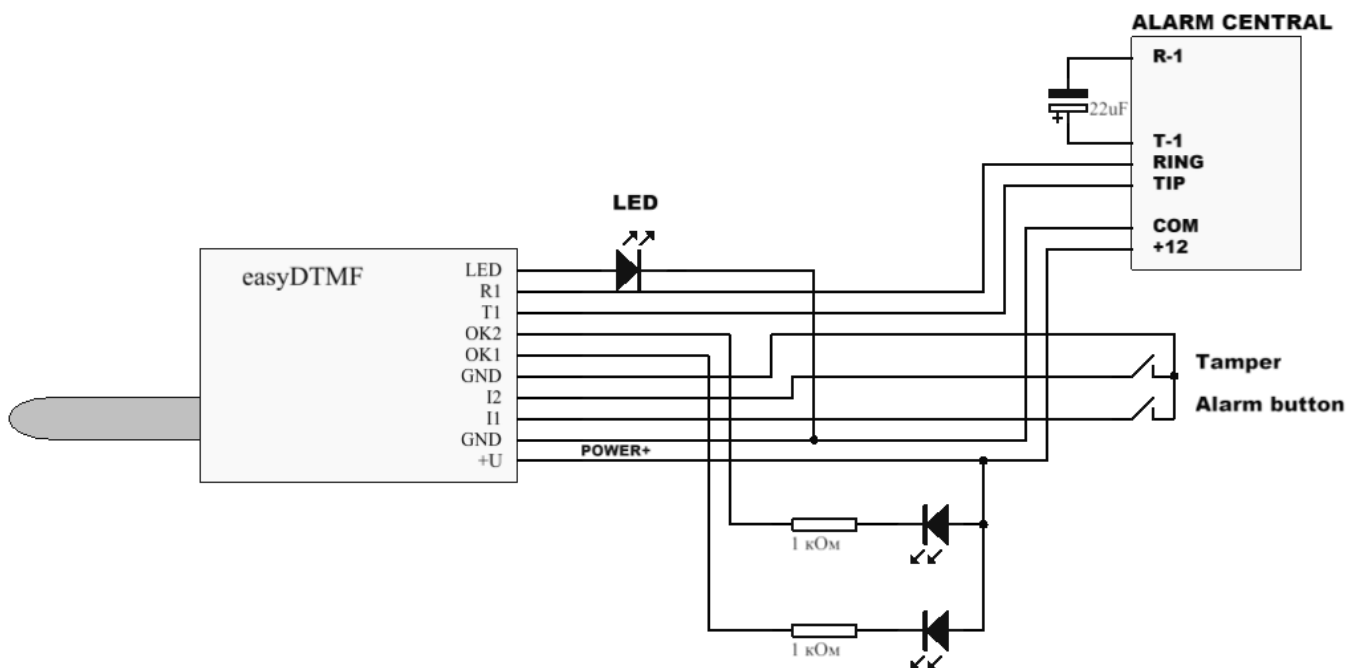
Scope of delivery

1.EasyDTMF communicator	– 1 pcs.
2.ADA-0068 antenna	– 1 pcs.
3.Mounting racks	– 4 pcs.
4.Installation and user guide	– 1 pcs.
5.Capacitor 22uF 35v	– 1 pcs.

Appendix 1: Example of the device connection.

An example of device connection to the security alarm is displayed below (figure 3).

Figure 3. An example of easyDTMF connection to the security alarm.



Appendix 2: The GRAPH server program usage.

The server part of software is designed to receive and decrypt messages in GLab-crypto protocol and to register new transmission devices while giving them an encryption key (for protection against substitution). Decrypted messages in Shur-GARD ContactID format are forwarded to a COM port in an existing system or to the other IP address.

The GRAPH system service will automatically launch after the program has been installed.

In order to launch a client part of the server:

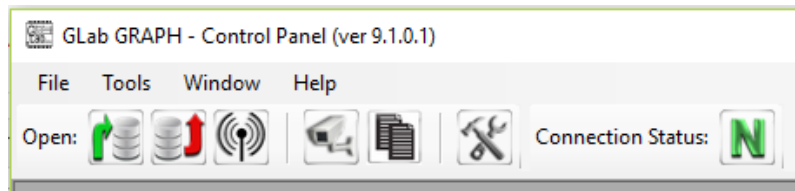
Click the «GRAPH Client» icon.

In the dialogue window select the IP address of a computer where the server is running, select the port number for connection and press the «Connect» button:

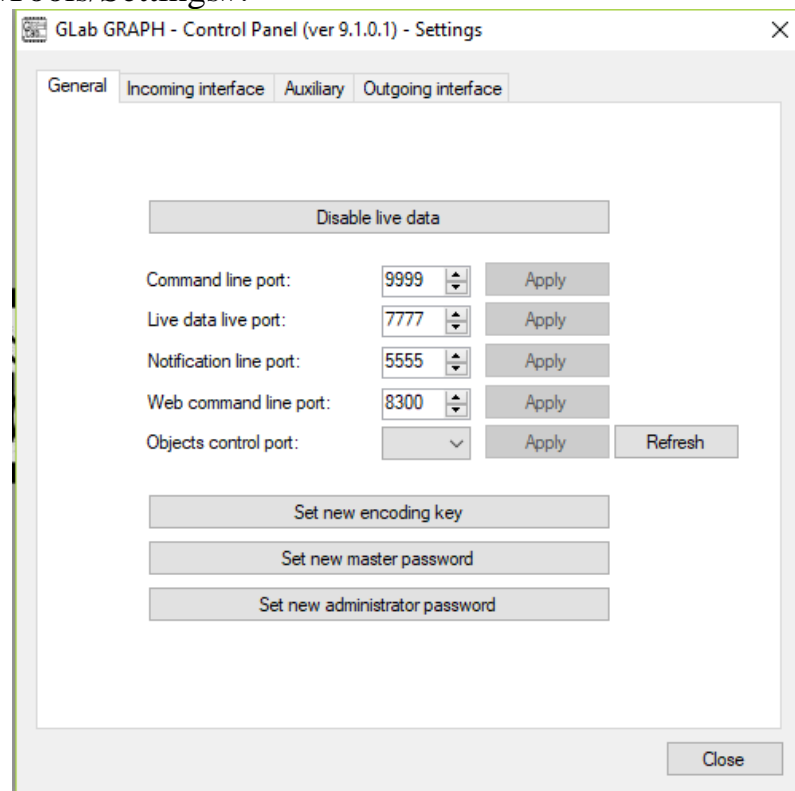
The default password in the program is «master».

The default password for access settings is «admin».

In the following pop-up window click «Tools/Language» and choose a preferable interface language.



Afterwards open «Tools/Settings»:



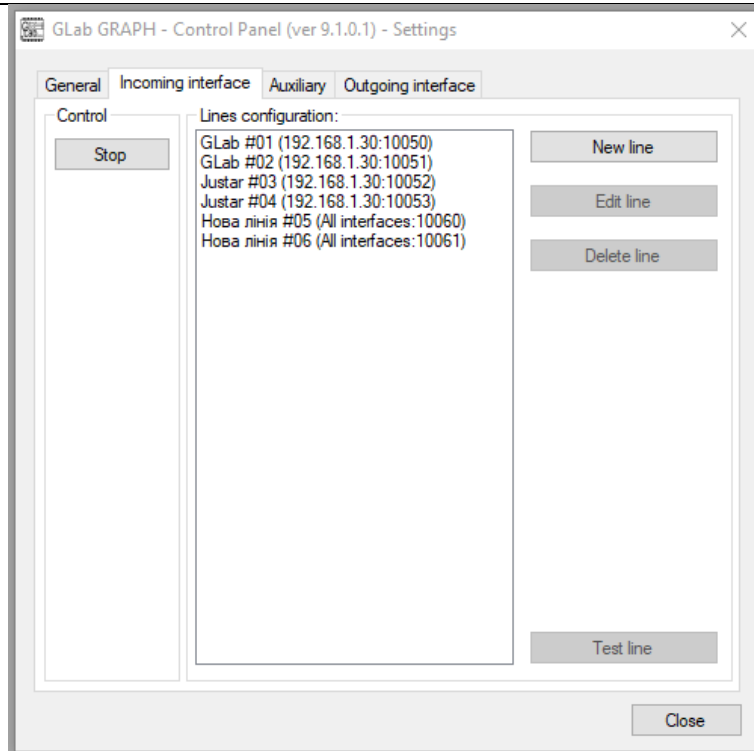
Tab «General»:

- «Disable live data» - serves to allow or forbid viewing data that is received and processed by the server in real time.
- «Command line port» - the connection between the client side and the server is established through that port.

- «Live data live port» - the data to the real time event window is transmitted through that port.
- «Notification line port» - a message about a key request by the object device is displayed through that port.
- «Set new encoding key» - a code phrase (no less than 8 symbols), based on which the program generates the encryption key.

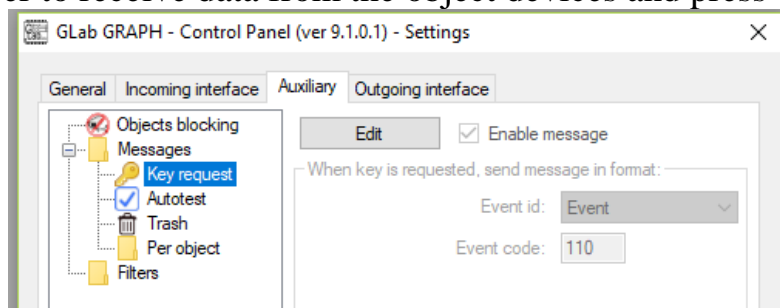
ATTENTION!

The entered code phrase should be written and hidden. If you do not remember a code phrase, after installation to a new computer none of the previously connected devices will work.



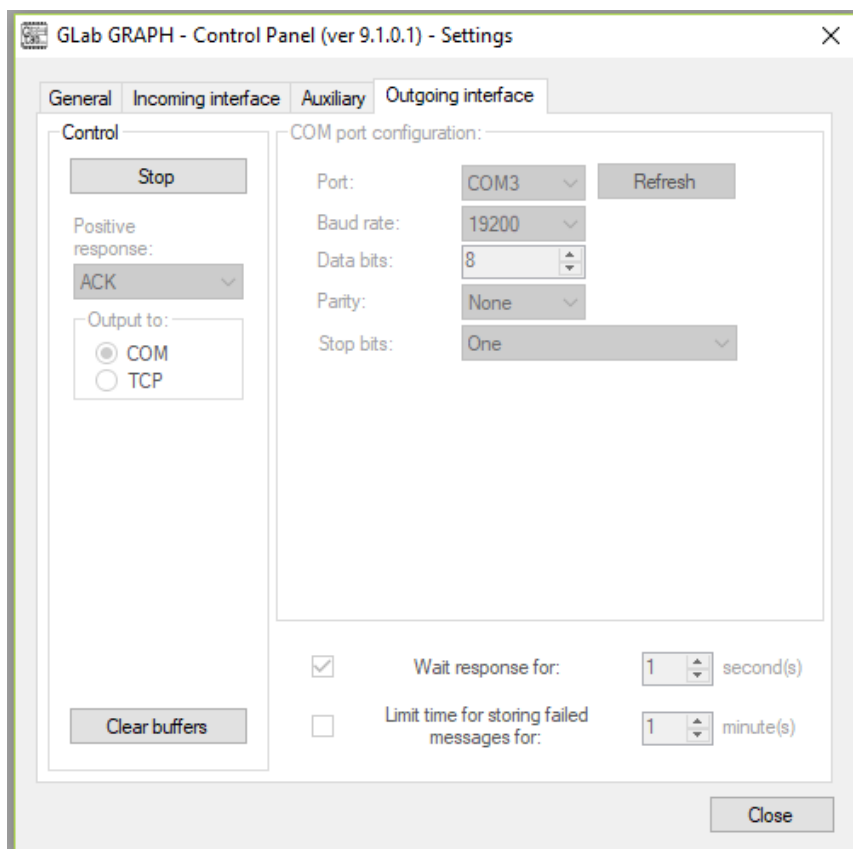
Tab «Incoming interface»:

Here you should add a «New line», choose the IP address and the port number which will be used by the server to receive data from the object devices and press «Start».



Tab «Auxiliary»:

- «Key request». A message in the standard Shur-GARD ContactID format, which is forwarded to the output interface after receiving an encryption key request from the object.
- «Auto test». A message like «5000 18YYYYE60200000[0x14]» (a chosen object number will be written instead of YYYY) will be transmitted with a certain period (in minutes), granted that the checkbox has been marked.



Tab «Outgoing interface» - here it is possible to set the output for received and decrypted messages to COM port of a computer or to an IP address.

If the station software understands the Sur-GARD receiver on the COM port, a free program com0com (<http://com0com.sourceforge.net>) can be used to create a pair of virtual serial ports. Install one of the com0com ports as a Sur-GARD port in the station software. Then choose the second port from the pair in the «Output interface» tab, set the speed, bit quantity, parity control, quantity of stop bits, presence of positive response from the station software and press the «Start» button. If everything was done correctly, the program should be ready for work.

For administrative convenience it is possible in the program to browse input and output interface history files, as well as real time data. (Tab «File/Open»).

Appendix 3: Table of recoding AdemcoExpress™ to ContactID™.

ATTENTION!

The Ademco identifier and the subscriber's phone number cannot equal «0». When a «0» occurs in the Ademco identifier, the message E35900000 (Contact ID) is transmitted, and when a «0» occurs in the subscriber's phone number, the message is E35800000.

Table 9. Recoding AdemcoExpress™ to ContactID™.

Ademco	Event Contact ID	Ademco	Event Contact ID
11	zone 1 alarm	2D	reset time /date
12	zone 2 alarm	2E	memory checksum error
13	zone 3 alarm	2F	reset to factory settings
14	zone 4 alarm	31	zone 1 restore
15	zone 5 alarm	32	zone 2 restore
16	zone 6 alarm	33	zone 3 restore
17	zone 7 alarm	34	zone 4 restore
18	zone 8 alarm	35	zone 5 restore
19	zone 9 alarm	36	zone 6 restore
1A	zone 10 alarm	37	zone 7 restore
1B	zone 11 alarm	38	zone 8 restore
1C	zone 12 alarm	39	zone 9 restore
1D	zone 13 alarm	3A	zone 10 restore
1E	zone 14 alarm	3B	zone 11 restore
1F	zone 15 alarm	3C	zone 12 restore
21	zone 16 alarm	3D	zone 13 restore
22	preliminary alarm	3E	zone 14 restore
23	zone 16 restore	3F	zone 15 restore
24	Attempt to crack code 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	fast arm	45	arm group 1 user 5
29	cancel alarm	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 boot mode	49	arm group 1 user 9

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

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

Ademco	Event Contact ID	Ademco	Event Contact ID
F1	alternating voltage 230V breakdown	F9	output 3 breakdown
F2	alternating voltage 230V restore	FA	output 3 restore
F3	accumulator breakdown	FB	tamper input alarm
F4	accumulator restore	FC	tamper input restore
F5	output 1 breakdown	FD	lost connection to communicator
F6	output 1 restore	FE	incorrect time/date
F7	output 2 breakdown	FF	periodic test
F8	output 2 restore		

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

Appendix 4: List of additional ContactID codes, which are transmitted to the security monitoring station.

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

E603 – periodic radio test. The transmission frequency is programmed with the *0XX* command.

E552 – no connection to the security alarm.

R552 – connection to the security alarm restored.

E305 – device reboot (the software version of the device is specified in the zone field).

E357 – GSM module reboot.

E315 – backup channel breakdown (absence of SIM card 2).

E316 – the main transmission channel is used (SIM1).

E317 – the backup transmission channel is used (SIM2).

E358 – error in programming the object number (programmed 0000).

E760 – error in settings of the main (group code) or the backup (zone code) SIM card. (See **Table 10**).

Table 10. Description of errors transmitted in code «E760».

Group code (main SIM)	Zone code (backup SIM)	Error description
3		Cannot establish connection with the GRAPH program on the first IP address / port number. Check the settings of the GPRS access point, IP address, number of IP port (socket).
4		Cannot transmit a test message to the GRAPH program on the first IP address/ port number. Check the GRAPH program settings.
5		Cannot establish connection with the GRAPH program on the second IP address / port number. Check the settings of the GPRS access point, IP address, number of IP port (socket).
6		Cannot transmit a test message to the GRAPH program on the second IP address/ port number. Check the GRAPH program settings.
	2	The backup SIM card is not installed (The PIN request when registering in the network is not cancelled). Cancel the PIN-code request. Clear all the contacts from the SIM card, or replace it if the SIM card is defective.
	3	Cannot establish connection with the GRAPH program on the first IP address / port number. Check the settings of the GPRS access point, IP address, number of IP port (socket).
	4	Cannot transmit a test message to the GRAPH program on the first IP address/ port number. Check the GRAPH program settings.