GUARDX

Supervision and administration software for INTEGRA and INTEGRA Plus alarm control panels

User manual

Version 1.18

guardx_en 06/20

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.eu

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.
Please visit us at:
http://www.satel.eu

Default codes:
Service code: 12345
Administrator code - Object 1: 1111

The following symbols may be used in this manual:

ℹ - note;
⚠ - caution.

CONTENTS

1. Introduction

The GUARDX program is intended for supervision and management of security systems based on the INTEGRA (firmware version 1.03 or newer) and INTEGRA Plus alarm control panels.

Communication between the program and the control panel takes place:

- locally: via the COM port of computer connected to the RS-232 port of control panel or to the RS-232 port of keypad connected to the control panel,
- remotely, via:
  - Ethernet, provided that ETHM-1 Plus / ETHM-1 module is connected to the control panel,
  - GPRS:
    - if the SATEL GSM module is connected to the INTEGRA 24 / INTEGRA 32 / INTEGRA 64 / INTEGRA 128 control panel as an external modem,
    - for INTEGRA 128-WRL,
  - SATEL server, provided that ETHM-1 Plus module is connected to the control panel.

For remote communication, the computer on which the GUARDX program is installed must have a permanent Internet access.

2. Features

- System state visualization on the map of protected object / premises.
- System control from the map level: activating / deactivating outputs, bypassing / unbypassing zones, arming / disarming partitions.
- Real-time information about alarm situations.
- System control from the keypad on computer screen.
- Adding, editing and deleting system users.
- Access to control panel event history.

3. Installation and system requirements

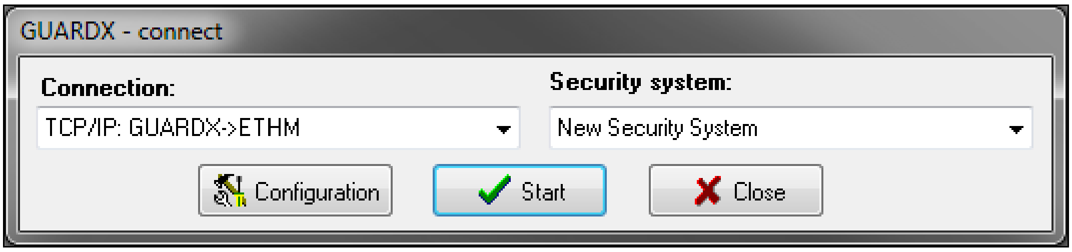
The GUARDX program installation file is available for download at www.satel.eu. The program can be installed on computers with Windows XP/VISTA/7/8/10 operating system.

4. First-time start-up of the GUARDX program

1. Launch the program using the shortcut icon on desktop or selecting the program in the “Start” menu of your Windows operating system.
2. The GUARDX program startup window will be displayed (see “Startup window”).
3. Configure the settings required to establish connection with the alarm system (see “Adding a new alarm system”).
4. Open the program main menu (see “Opening the main menu”).

5. Startup window

The startup window opens when the program is being launched. If it will not open on launching the program, but the authorization window opens at once instead, it means that the "Auto-Connect (no CONNECTION menu)" option is enabled (see "Menu options").



GUARDX - connect

Connection: TCP/IP: GUARDX->ETHM

Security system: New Security System

Fig. 1. GUARDX program startup window.

Connection – the method of communication with the control panel (see "Method of communication").

Security system – name of the alarm system you can connect to (see "Adding a new alarm system").

Configuration – click to open the "Connection" window (see "Connection").

Start – click to open the main menu (see "Opening the main menu").

Close – click to close the startup window.

5.1 Adding a new alarm system

1. In the startup window, in the "Security system" field, select "New Security System".
2. Click on "Configuration" or "Start".
3. The "System name" window will be displayed.
4. Enter the alarm system name in the "New Security System" field.
5. Click "OK".
6. The "Connection" window will be displayed.
7. Enter the data required to establish communication with the control panel (see "Connection").
8. Click "OK".

5.2 Opening the main menu

1. In the startup window, in the "Security system" field, select an alarm system.
2. In the "Connection" field select the method of communication (see "Method of communication").
3. Click "Start".
4. The program will connect to the control panel (if you selected "Off-line" in the "Connection" field, the main menu will be displayed).
5. After establishing connection with the control panel, the authorization window will be displayed.
6. In the "Enter code" field, enter the control panel access code. You can enter the service code (by default: 12345), administrator code (by default for Object 1: 1111) or user code (the user must have the "Start GUARDX connection" authority level).
7. Click "OK".

8. The main menu will be displayed.

When running the program for the first time, use the administrator password to log in.

Entering a wrong code twice will take you back to the startup window.

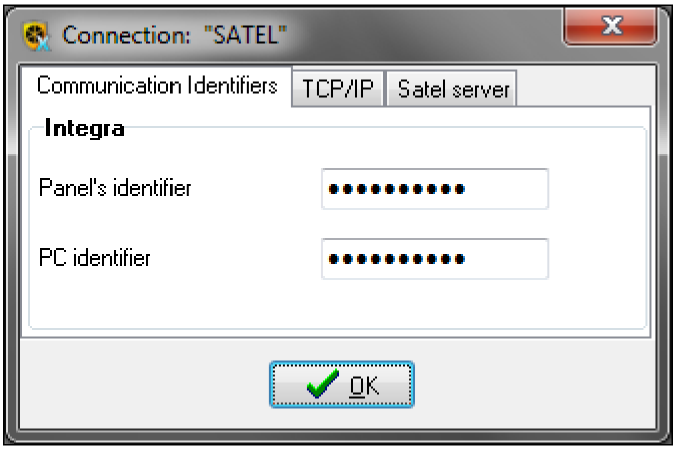
The GUARDX program has been developed for the alarm system administrator. Because all data are downloaded from the control panel each time when you run the program, it is advisable to keep the program running all the time. It is recommended that you run the functions of downloading the data and configuration settings from the control panel at predefined intervals, as well as each time after making changes to the alarm system (e.g. using the "Refresh panel data" button – see "Configuration menu").

Using the GUARDX program on one computer, you can start several connections to the control panels, each one to a different alarm system.

5.3 Connection

5.3.1 Communication identifiers

The GUARDX program will be able to establish communication with the control panel if the communication identifiers in program and control panel are identical.



Panel's identifier ●●●●●●●●●●

PC identifier ●●●●●●●●●●

Fig. 2. "Communication identifiers" tab in the "Connection" window.

Panel's identifier – identifier of the alarm control panel. It must have 10 characters (digits or letters from A to F). It makes possible recognition of the control panel and adjustment of the data file to it, provided it has been saved on the computer. Having entered the value, you can click 👓 to see the sequence of characters.

PC identifier – identifier of the computer running the GUARDX program. It must have 10 characters (digits or letters from A to F). The control panel will only establish connection with the program using the correct identifier. Having entered the value, you can click 👓 to see the sequence of characters.

The communication identifiers you can program in the control panel using:

- *LCD keypad ([service code]✱ ▶"Service mode" ▶"SM settings"),*
- *DLOADX program ("Connection settings" window – the command for opening this window is available in the "Communication" menu; you can also use the Ctrl+R key combination).*

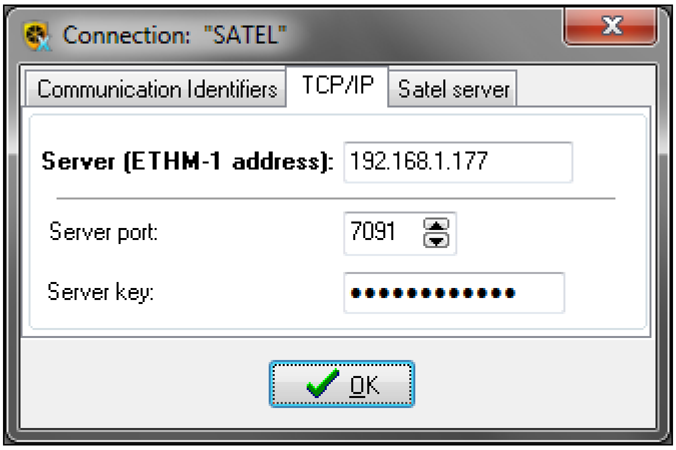
5.3.2 TCP/IP

The settings below apply to direct communication with the ETHM-1 Plus / ETHM-1 module.

Server (ETHM-1 address) – address of the Ethernet module. If the Ethernet module is not in the same local network as the computer with GUARDX program, it must be a public address. You can enter either the IP address or the domain name.

Server port – number of the TCP port used during communication between the control panel and the computer with GUARDX program via Ethernet. You can enter values from 1 to 65535. Default: 7091.

Server key – a string of up to 12 alphanumeric characters (digits, letters and special characters) to be used for data encryption during communication between the control panel and the computer with GUARDX program via Ethernet. Click 👓 to see the sequence of characters.



Server (ETHM-1 address): 192.168.1.177

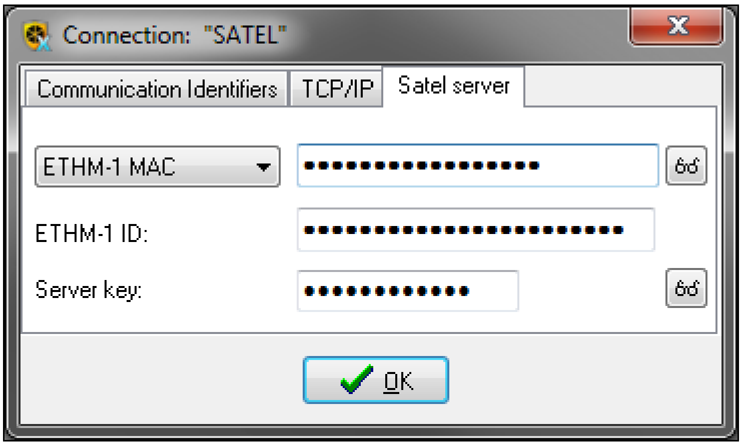
Server port: 7091

Server key: ●●●●●●●●●●●●

Fig. 3. “TCP/IP” tab in the “Connection” window.

5.3.3 Satel sever

The settings below apply to communication via the SATEL server. You can select communication via Ethernet (“ETHM-1 MAC”) or GPRS (“INT-GSM IMEI”). Click on the communication variant if you want to change it.



ETHM-1 MAC: ●●●●●●●●●●●●●●●●●●

ETHM-1 ID: ●●●●●●●●●●●●●●●●●●●●●●●●●

Server key: ●●●●●●●●●●●●

Fig. 4. “Satel server” tab in the “Connection” window.

ETHM-1 MAC – select this variant if the ETHM-1 Plus module is connected to the control panel. In the field beside, enter the hardware address of the Ethernet module. Click 👓 to see the sequence of characters.

ETHM-1 ID – individual ID number assigned to the ETHM-1 Plus module by the SATEL server. Having entered the value, you can click 👓 to see the sequence of characters.

INT-GSM IMEI – select this variant if the INT-GSM module is connected to the control panel. In the field beside, enter the ID number of the INT-GSM module GSM telephone. Click 👓 to see the sequence of characters.

INT-GSM ID – individual ID number assigned to the INT-GSM module by the SATEL server. Having entered the value, you can click 👓 to see the sequence of characters.

*You can check the MAC address, IMEI number and ID using the DLOADX program or LCD keypad ([*code*]✱ ▶“Tests” ▶“IP/MAC/IMEI/ID”).*

Server key – a string of up to 12 alphanumeric characters (digits, letters and special characters) to be used for data encryption during communication between the control panel and the computer with GUARDX program. Click 👓 to see the sequence of characters.

5.4 Method of communication

5.4.1 COM port

If the:

- RS-232 port of the control panel,
- USB MINI-B connector of the control panel,
- RS-232 port of the keypad with mechanical keys (PIN-5 connector), connected to the control panel,
- RS-232 port of the INT-RS / INT-RS Plus system integration interface (DB-9 male connector), connected to the keypad bus on the control panel mainboard,

is connected to the computer, communication between the GUARDX program and the control panel can be established via the COM port. This enables the alarm system to be administered locally.

5.4.1.1 Connecting computer to control panel RS-232 port

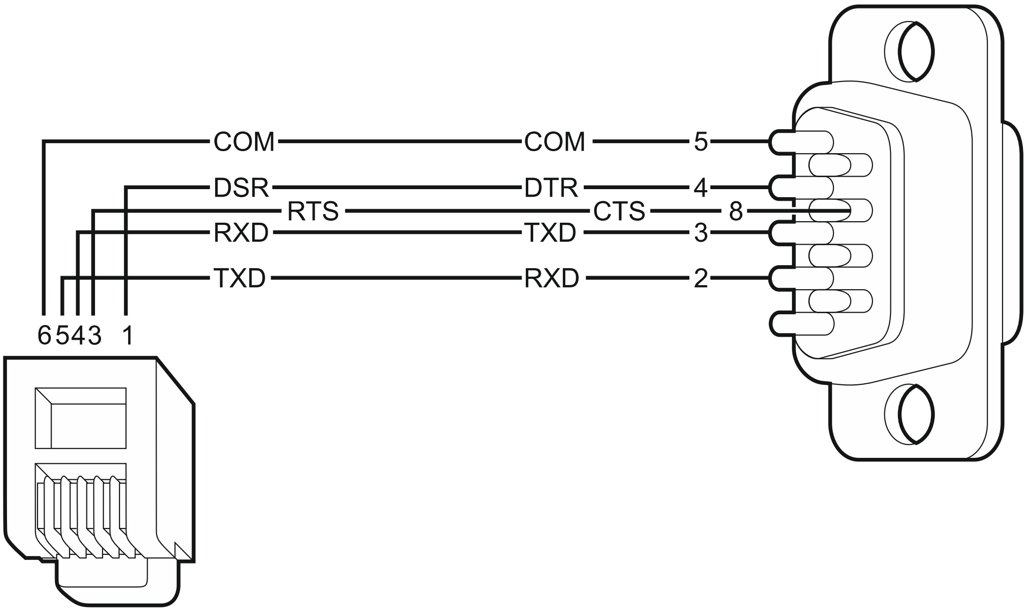


Fig. 5. Computer connection to control panel RS-232 port. Shown on the left is RJ connector to be plugged into the control panel mainboard socket. Shown on the right is DB-9 female connector (solder side view).

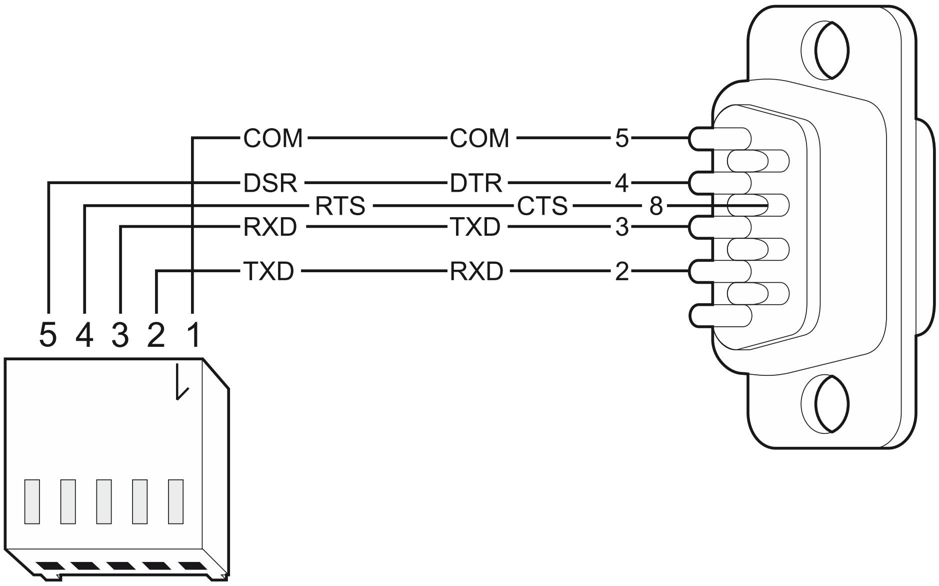


Fig. 6. Computer connection to control panel RS-232 port – control panel with PIN-5 connector. Shown on the left is PIN-5 plug. Shown on the right is DB-9 female plug (solder side view).

5.4.1.2 Connecting computer to control panel USB MINI-B connector

If the control panel is connected to the computer with the USB cable, the Windows system will automatically detect connection of a new device and display a window of the wizard that will lead the you through the procedure of installation of drivers for the new hardware. You can download the drivers from the www.satel.eu website. Some versions of the Windows operating system may give a warning that the driver has not passed the tests for conformity. Despite these warnings, continue the installation of drivers.

Connecting the USB port to the computer will block the RS-232 port.

5.4.1.3 Connecting computer to keypad RS-232 port

To make this type of connection, it is advisable to use unshielded non-twisted cable (using the “twisted pair” type of cable, e.g. UTP, STP, FTP, is not recommended). Distance between the computer and the keypad can be up to 10 m.

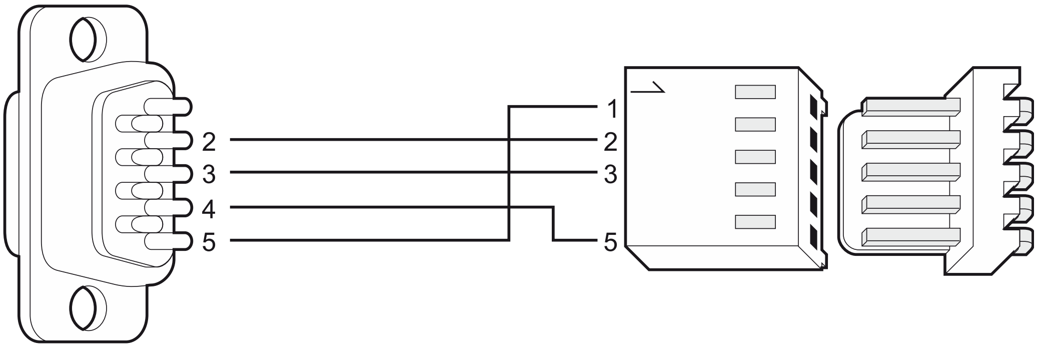


Fig. 7. Computer connection to the keypad RS-232 port. Shown on the right is keypad interface. Shown on the left is DB-9 female connector (solder side view).

On the keypad to which the computer with the GUARDX program is connected, enable the “Communication RS” option (DLOADX program →“Structure” window

→"Hardware" tab →"Keypads" item →[keypad name] →"Keypad" tab). Starting the GUARDX program automatically begins the data exchange.

5.4.1.4 Connecting computer to RS-232 port of INT-RS / INT-RS Plus interface

The DB-9 male connector (RS-232 port) located on the interface PCB makes possible its connection to the computer. To make this type of connection, use the so-called null modem cable. Operating mode of the device is selected using switches 4 to 10 (see the INT-RS / INT-RS Plus interface manual).

5.4.1.5 Starting local administration of the system

Communication identifiers in the control panel and the program must be identical (see "Connection").

1. In the startup window, "Connection" field, select "COMn" (where n is the number of the COM port to which the control panel / keypad / INT-RS / INT-RS Plus interface is connected).
2. In the "Security system" field, select the system to which you want to connect, and then click "Start".
3. If the keypad RS-232 port is connected to the computer COM port, proceed to step 7.
4. If the RS-232 port of the control panel / INT-RS / INT-RS Plus interface or the control panel USB MINI-B connector is connected to the computer COM port, enter the service code (by default 12345) on the keypad connected to the control panel and press the ✱ key.
5. Use the arrow keys to find "Downloading" on the function list and press **#**.
6. When the arrow indicates the "Start DWNL-RS" function, press **#**.

To run the "Start DWNL-RS" function you can use the [service code]✱01 key shortcut.

7. The authorization window will be displayed.
8. Enter the service / administrator / user code (the user must have the "Start GUARDX connection" authority level) and click "OK".
9. The GUARDX program will display a message to inform you that connection has been established. Click "OK".

5.4.2 Off-line

Select "Off-line" if you want to open the main menu of the program without establishing connection with the control panel. When the program is running in the "Off-line" mode:

- you can edit the maps,
- you can export the data to transfer them to the disk drive of another computer,
- you can import the data to transfer them from the disk drive of another computer,
- you can view the list of users and their authority level if you enter the administrator code,
- you can load from file the alarm system data exported from the DLOADX program,
- you have no access to events.

5.4.2.1 Opening the main menu

1. In the startup window, "Connection" field, select "Off-line".
2. In the "Security system" field, select the system and click "Start".

5.4.3 Remote communication

Remote communication between the program and the control panel can take place:

- over Ethernet – when the ETHM-1 Plus / ETHM-1 Ethernet module is connected to the control panel,
- via GPRS – in the case of INTEGRA 128-WRL or any other control panel, when the INT-GSM module is installed in the alarm system, or the SATEL GSM module is connected to the control panel.

5.4.3.1 Connecting the RS-232 ports of control panel and communication module

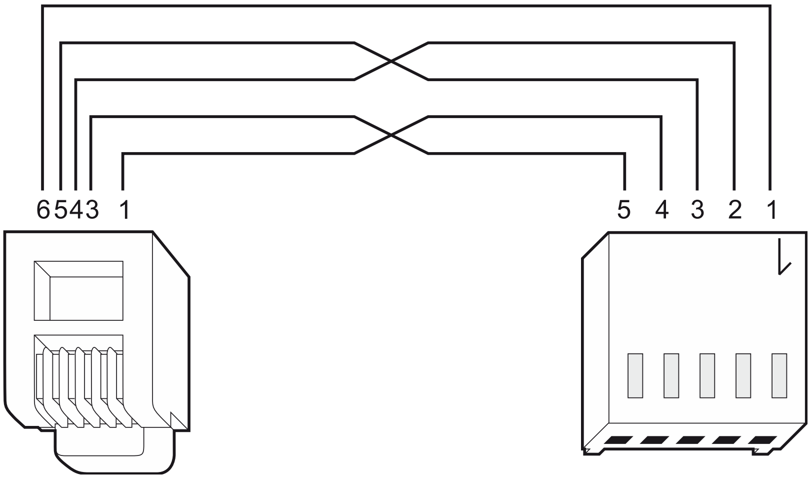


Fig. 8. Connection of the RS-232 ports of control panel and communication module (ETHM-1 Plus / ETHM-1 / INT-GSM module or SATEL GSM module). Shown on the left is RJ connector plugged into control panel mainboard socket. Shown on the right is PIN-5 connector. Ready-to-use cable is offered by SATEL (RJ/PIN5).

If the SATEL GSM module is to work as an external modem with the INTEGRA, INTEGRA Plus control panel, do not enable the "Fax/Modem" option in it.

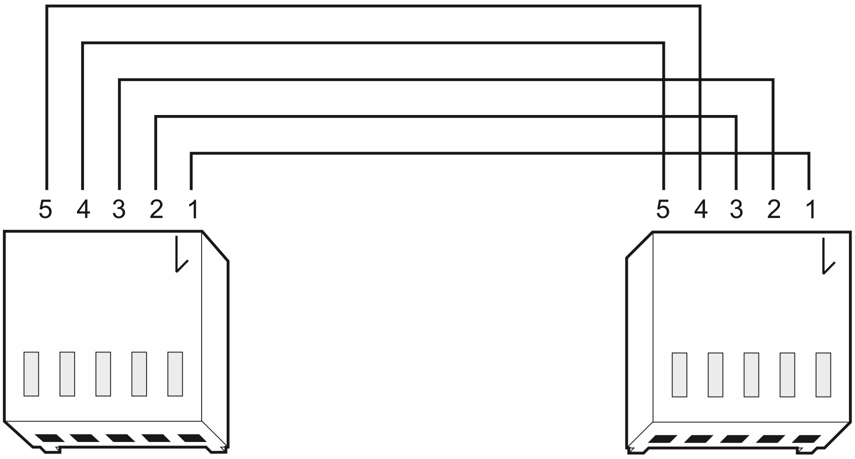


Fig. 9. Connection of the RS-232 ports of control panel with PIN-5 connector and communication module (ETHM-1 Plus / ETHM-1 / INT-GSM module or SATEL GSM module). Ready-to-use cable is offered by SATEL (PIN5/PIN5).

5.4.3.2 TCP/IP: GUARDX->ETHM

Select “TCP/IP: GUARDX->ETHM” if the GUARDX program is to connect to the control panel via ETHM-1 Plus / ETHM-1 module. The communication between the module and the control panel is possible in two ways:

1. via RS-232 port on the control panel mainboard,
2. using the control panel keypad bus.

If the RS-232 ports of control panel and Ethernet module are connected (see “Connecting the RS-232 ports of control panel and communication module“), the communication will be established via the RS-232 port. If however the DLOADX program will connect to the module, it will take over the connection via the RS-232 port, and the GUARDX program will use the control panel keypad bus for communication. This type of connection is slower and less effective than communication via the RS-232 port on the control panel mainboard.

If communication takes place in the WAN network, the Ethernet module must have a public IP address.

Communication identifiers in the control panel and the program must be identical (see “Connection”).

The ETHM-1 Plus / ETHM-1 module enables just one connection at a time. If the connection, e.g. with the DLOADX program, ACCO NET or INTEGRUM system, is already established, the “Server busy, disconnected” message will be displayed at any attempt to establish another connection.

Initiating connection from GUARDX program

Control panel settings

You can configure the settings using LCD keypad or the DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering ETHM/GSM” options.

Ethernet module settings (ETHM-1, ETHM-1 Plus)

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ETHM-1” tab):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enter the TCP port number if it is to be different than 7091,
- configure the network settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server (ETHM-1 address)” field, address of the Ethernet module,
- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX->ETHM”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.

3. The “Connection TCP/IP: GUARDX->ETHM-1” window will open with information about establishing connection.
4. The authorization window will be displayed.
5. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
6. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

5.4.3.3 TCP/IP: GUARDX<-ETHM/INT-GSM

Select “TCP/IP: GUARDX<-ETHM/INT-GSM” if the control panel is to connect to the GUARDX program via ETHM-1 Plus / ETHM-1 / INT-GSM module. The communication between the module and the control panel is possible in two ways:

1. via RS-232 port on the control panel mainboard,
2. using the control panel keypad bus.

If the RS-232 ports of control panel and module are connected (see “Connecting the RS-232 ports of control panel and communication module“), the communication will be established via the RS-232 port. If however the DLOADX program will connect to the module, it will take over the connection via the RS-232 port, and the GUARDX program will use the control panel keypad bus for communication. This type of connection is slower and less effective than communication via the RS-232 port on the control panel mainboard.

> *If communication takes place in the WAN network, the Ethernet module must have a public IP address.*
>
> *Communication identifiers in the control panel and the program must be identical (see “Connection”).*
>
> *The ETHM-1 Plus / ETHM-1 module enables just one connection at a time. If the connection, e.g. with the DLOADX program, ACCO NET or INTEGRUM system, is already established, the “Server busy, disconnected” message will be displayed at any attempt to establish another connection.*

Initiating a connection via the ETHM-1 Plus / ETHM-1 module from the keypad

> *If the INT-GSM module is connected to the ETHM-1 Plus module and connection over Ethernet cannot be established, an attempt will be made to establish connection via GPRS.*

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

ETHM-1 Plus / ETHM-1 module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ETHM-1” tab):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enter address of the computer running the GUARDX program (“GUARDX server”),
- enter the TCP port number if it is to be different than 7091,
- configure the network settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-ETHM/INT-GSM”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<-ETHM-1” window will open with information about establishing connection.
4. Ask the user to start the “ETHM-1 →GUARDX” function on the keypad ([code]✱ ▶“Downloading” ▶“ETHM-1 →GUARDX”). The function is available to the service, administrator and user having the “Downloading starting” right.
5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

Initiating a connection via the ETHM-1 Plus module using SMS message

> *The INT-GSM module must be connected to the ETHM-1 Plus module. If connection via Ethernet cannot be established, an attempt will be made to establish communication via GPRS.*

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

ETHM-1 Plus + INT-GSM module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ETHM-1” and “INT-GSM functions” tabs):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enter address of the computer running the GUARDX program (“GUARDX server”),
- enter the TCP port number if it is to be different than 7091,
- program the control command, which, if sent in the SMS message, will initiate connection with the GUARDX program (“SMS initiating GUARDX connection”),
- configure the network settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-ETHM/INT-GSM”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<-ETHM-1” window will open with information about establishing connection.
4. Send to the INT-GSM module the following SMS message:

   xxxx= (“xxxx” – the control command to initiate establishment of communication with GUARDX program) – the module is to connect to the computer whose address is programmed in the module,

   xxxx=aaaa:p= (“xxxx” – the control command to initiate establishment of communication with GUARDX program; “aaaa” – address of the computer with GUARDX program (IP address or domain name); “p” – TCP port) – the module is to connect to the computer whose address has been given in the SMS message and use for communication the TCP port given in the SMS message.
5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

Initiating a connection via the INT-GSM module from the keypad

The method of establishing communication, as described below, applies to the INT-GSM module connected directly to the alarm control panel. If the INT-GSM module is connected to the ETHM-1 Plus module, see description of initiating a connection via the ETHM-1 Plus module.

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

INT-GSM module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“INT-GSM” and “INT-GSM functions” tabs):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enter address of the computer running the GUARDX program (“GUARDX server”),
- enter the TCP port number if it is to be different than 7091,
- configure the GPRS settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-ETHM/INT-GSM”.

2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<-ETHM-1” window will open with information about establishing connection.
4. Ask the user to start the “INT-GSM →GUARDX” function on the keypad ([code]✱ ▶“Downloading” ▶“INT-GSM →GUARDX”). The function is available to the service, administrator and user having the “Downloading starting” right.
5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

Initiating a connection via the INT-GSM module by using SMS message

> *The method of establishing communication, as described below, applies to the INT-GSM module connected directly to the alarm control panel. If the INT-GSM module is connected to the ETHM-1 Plus module, see description of initiating a connection via the ETHM-1 Plus module.*

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

INT-GSM module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ INT-GSM” and “INT-GSM functions” tabs):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enter address of the computer running the GUARDX program (“GUARDX server”),
- enter the TCP port number if it is to be different than 7091,
- program the control command, which, if sent in the SMS message, will initiate connection with the GUARDX program (“SMS initiating GUARDX connection”),
- configure the GPRS settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-ETHM/INT-GSM”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<-ETHM-1” window will open with information about establishing connection.

4. Send to the INT-GSM module the following SMS message:

   xxxx= ("xxxx" – the control command to initiate establishment of communication with GUARDX program) – the module is to connect to the computer whose address is programmed in the module,

   xxxx=aaaa:p= ("xxxx" – the control command to initiate establishment of communication with GUARDX program; "aaaa" – address of the computer with GUARDX program (IP address or domain name); "p" – TCP port) – the module is to connect to the computer whose address has been given in the SMS message and use for communication the TCP port given in the SMS message.
5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the "Start GUARDX connection" authority level) and click "OK".
7. The GUARDX program will display a special message to inform you that connection has been established. Click "OK".

5.4.3.4 TCP/IP: GUARDX<-GPRS INTEGRA WRL

Select "TCP/IP: GUARDX<-GPRS INTEGRA WRL" if GPRS connection is to be established with INTEGRA 128-WRL control panel.

> *Communication identifiers in the control panel and the program must be identical (see "Connection").*

Initiating a connection from the keypad

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →"Structure" window →"Hardware" tab →"GSM phone" tab):

- enter address of the computer running the GUARDX program,
- enter the TCP port number,
- configure the GPRS settings,
- configure the built-in GSM module.

GUARDX program settings

To configure the settings, click on the "Configuration" button in the GUARDX startup window. In the window that will open, select the "TCP/IP" tab and enter:

- in the "Server port" field, number of the TCP port that will be used during communication.

Establishing communication

1. In the startup window, "Connection" field, select "TCP/IP: GUARDX<-GPRS INTEGRA WRL".
2. In the "Security system" field, select the system you want to connect to and click "Start".
3. The "GPRS -> GUARDX, TCP/IP Server" window will open. Click "Start". This will activate the server for GPRS connection.

> *If the number of TCP port to be used during communication has not been predefined, click "Stop" in the "GPRS -> GUARDX, TCP/IP Server" window. In the "Server port" field, enter the port number and click "Start".*

4. Ask the user to start the "Start DWNL-GPRS" function on the keypad ([code]✱ ▶"Downloading" ▶"Start DWNL-GPRS"). The function is available to the service, administrator and user having the "Downloading starting" right.
5. The authorization window will be displayed.

6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

Initiating a connection by using SMS message

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“GSM phone” tab):

- enter address of the computer running the GUARDX program,
- enter the TCP port number,
- program the control command, which, if sent in the SMS message, will initiate connection with the GUARDX program,
- configure the GPRS settings,
- configure the built-in GSM module.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication.

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-GPRS INTEGRA WRL”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “GPRS -> GUARDX, TCP/IP Server” window will open. Click “Start”. This will activate the server for GPRS connection.

> *If the number of TCP port to be used during communication has not been predefined, click “Stop” in the “GPRS -> GUARDX, TCP/IP Server” window. In the “Server port” field, enter the port number and click “Start”.*

4. Send to the INTEGRA 128-WRL control panel the following SMS message:

   xxxx=gprs= (“xxxx” – control command to initiate establishing communication with GUARDX program) – the control panel is to connect to the computer whose address is programmed in the control panel,

   xxxx=aaaa:p= (“xxxx” – control command to initiate establishing communication with GUARDX program; “aaaa” – address of the computer with GUARDX program (IP address or domain name); “p” – TCP port number) – the control panel is to connect to the computer whose address has been given in the SMS message and use for communication the TCP port given in the SMS message.
5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

5.4.3.5 TCP/IP: GUARDX<-GSM4/5/LT/X

Select “TCP/IP: GUARDX<-GSM4/5/LT/X” if GPRS connection is to be established with a control panel to which a SATEL GSM module is connected (see “Connecting the RS-232 ports of control panel and communication module”). **GSM-X** module or module with LEON telephone is required:

- GSM LT-1 with firmware 1.14 (or newer),

- GSM LT-2 with firmware 2.14 (or newer),

- GSM-4 with firmware 4.14 (or newer),

- GSM-5 with firmware 5.14 (or newer).

> *Communication identifiers in the control panel and the program must be identical (see “Connection”).*

Initiating a connection by using SMS message

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

GSM module settings

You can configure the settings as described in the GSM module manual:

- enter address of the computer running the GUARDX program,
- enter the TCP port number,
- enter the data encryption key,
- program the control command, which, if sent in the SMS message, will initiate connection with the GUARDX program,
- configure the GPRS settings,
- additionally, you can enable the option that will enable connection to be established with the computer whose network address will be given in the SMS message initiating the connection.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, select the “TCP/IP” tab and enter:

- in the “Server port” field, number of the TCP port that will be used during communication,
- in the “Server key” field, the data encryption key (identical to that in the module).

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: GUARDX<-GSM4/5/LT/X”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “GSM->GUARDX, TCP/IP Server” window will open. Click “Start”. This will activate the server for GPRS connection.

> *If the number of TCP port to be used during communication has not been predefined, click “Stop” in the “GSM->GUARDX, TCP/IP Server” window. In the “Server port” field, enter the port number and click “Start”.*

4. Send to the GSM module the following SMS message:

   zzzzzz. or **zzzzzz=** (“zzzzzz” – control command programmed in the GSM module that initiates establishing GPRS communication with the GUARDX program) – the GSM module will connect the control panel to the computer whose address is programmed in the module,

zzzzzz=aaaa:p. or **zzzzzz=aaaa:p=** (“zzzzzz” – control command programmed in the GSM module that initiates establishing GPRS communication with the GUARDX program; “aaaa” – address of the computer with GUARDX program (IP address or domain name); “p” – TCP port) – the GSM module will connect the control panel to the computer whose address is indicated in the SMS message.

5. The authorization window will be displayed.
6. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
7. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

5.4.3.6 TCP/IP: SATEL server

Select “TCP/IP: SATEL server” if communication between the GUARDX program and the control panel is to be established via the SATEL server. The ETHM-1 Plus or INT-GSM module must be connected to the control panel.

> *No public IP address is required for the control panel or for the computer running the GUARDX program.*
>
> *Communication identifiers in the control panel and the program must be identical (see “Connection”).*
>
> *For communication via the SATEL server, the ports of 1024-65535 range are used as outgoing ports. These ports must not be blocked.*

Initiating a connection in the case of communication via the ETHM-1 Plus module

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

ETHM-1 Plus module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ETHM-1” tab):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enable the “Communication via SATEL server” option,
- configure the network settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, in the “Satel sever” tab:

- select the “ETHM-1 MAC” variant,
- enter MAC address of the ETHM-1 Plus module,
- enter identification number assigned to the ETHM-1 Plus module by the SATEL server (“ETHM-1 ID”),
- enter the data encryption key (“Server key”).

> *You can check the MAC address and ID using the DLOADX program or LCD keypad ([*code*]✱ ▶“Tests” ▶“IP/MAC/IMEI/ID”).*

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: SATEL server”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<->ETHM-1” window will open with information about establishing connection.
4. The authorization window will be displayed.
5. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
6. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

Initiating a connection in the case of communication via the INT-GSM module

> *The method of establishing communication, as described below, applies to the INT-GSM module connected directly to the alarm control panel. If the INT-GSM module is connected to the ETHM-1 Plus module, see description of initiating a connection via the ETHM-1 Plus module.*

Control panel settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Options” window →“Telephone” tab):

- enable the “External modem”, “Modem ISDN/GSM/ETHM” and “Answering – ETHM/GSM”.

INT-GSM module settings

You can configure the settings using LCD keypad or DLOADX program (DLOADX program →“Structure” window →“Hardware” tab →“Keypads” item →[module name] →“ INT-GSM” and “INT-GSM functions” tabs):

- enable the “GUARDX” option,
- enter the data encryption key (“GUARDX key”),
- enable the “Communication via SATEL server” option,
- configure the GPRS settings.

GUARDX program settings

To configure the settings, click on the “Configuration” button in the GUARDX startup window. In the window that will open, in the “Satel sever” tab:

- select the “INT-GSM IMEI” variant,
- enter IMEI number of the INT-GSM module,
- enter identification number assigned to the INT-GSM module by the SATEL server (“INT-GSM ID”),
- enter the data encryption key (“Server key”).

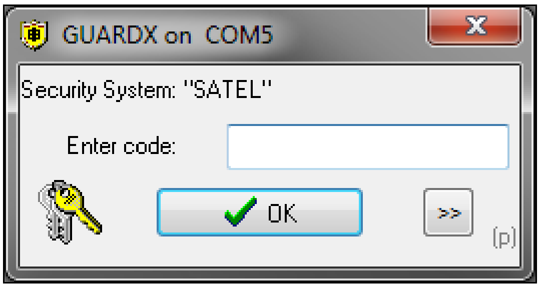
> *You can check the IMEI number and ID using the DLOADX program or LCD keypad (*[code]*✱ ▶“Tests” ▶“IP/MAC/IMEI/ID”).*

Establishing communication

1. In the startup window, “Connection” field, select “TCP/IP: SATEL server”.
2. In the “Security system” field, select the system you want to connect to and click “Start”.
3. The “Connection TCP/IP: GUARDX<->ETHM-1” window will open with information about establishing connection.
4. The authorization window will be displayed.

5. Enter the service / administrator / user code (the user must have the “Start GUARDX connection” authority level) and click “OK”.
6. The GUARDX program will display a special message to inform you that connection has been established. Click “OK”.

6. Authorization window



Security System: "SATEL"

Enter code:

Fig. 10. Authorization window.

The authorization window is displayed when you have to enter the control panel access code. To enter the code, you can use either the keyboard or the mouse (click on >> to display the buttons for entering the code).

You can enter the service code (by default: 12345), administrator code (by default for Object 1: 1111) or user code (the user must have the “Start GUARDX connection” authority level).

ℹ *Access to some functions in the program depends on what type of code you use.*

Having entered the code, press ENTER or click “OK”.

If you click “Write” in the “Users” window, the “Remember access code” option will be available in the authorization window. If you enable the option, the code will be remembered until the “Users” window is closed, i.e. after you click “Write”, the authorization window will not reappear.

7. Main menu

Buttons:

- SATEL logo – click to display additional menu (see “Additional menu”).
- communication – click to display communication menu (see “Communication menu”).
- system state – click to display the list of maps. Click on the map name to view it (see “Map”). If there was an alarm in the system, the button flashes alternately with the button.
- keypad – click to display virtual keypad (see “Keypad”).
- users – click to open “Users” window (see “Users”).

- event log – click to open "Event log" window (see "Event log").

- quit – click to stop the process of downloading events from the control panel (see "Stop reading events").

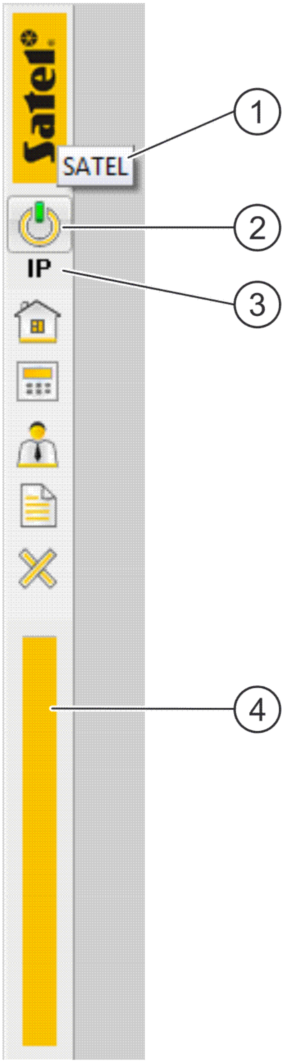


Fig. 11. GUARDX program main menu.

1 alarm system name.

2 icon indicating current status of communication with the alarm control panel:
alternating green and yellow – the program is connected to the control panel,
gray – no connection to the control panel.

3 information about method of communication with the alarm control panel:
[COM port number] – communication via RS-232 port,
IP – communication via Ethernet or GPRS.

4 information about data downloading progress.

7.1 Additional menu

The additional menu is displayed:

- after you click on the SATEL logo in the main menu,
- after you right click on the program icon in the tray.

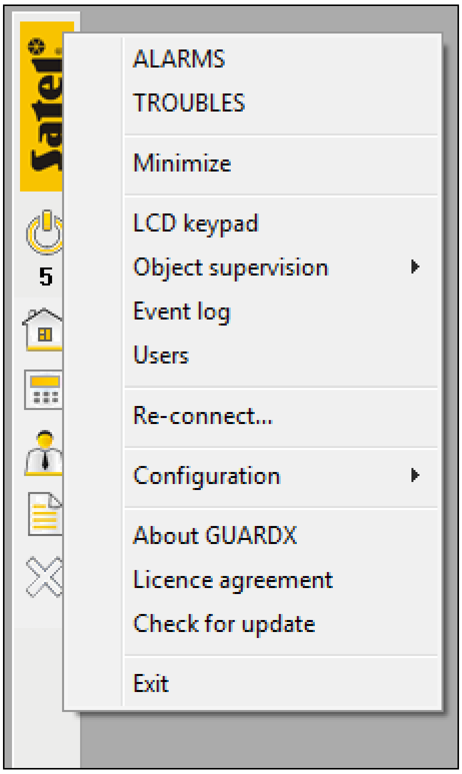


Fig. 12. Additional menu.

ALARMS – click to display “ALARM” window (see “ALARM”). The command is displayed if there is an alarm condition in the alarm system.

TROUBLES – click to display “TROUBLE” window (see “TROUBLE”). The command is displayed if there is a trouble condition in the alarm system.

Minimize – click to minimize the main menu and all open windows (see “Icon in the tray”).

LCD keypad – click to display virtual keypad (see “Keypad”).

Object supervision – hover the cursor over the command to display the list of maps. Click on the map name to view it (see “Map”).

Event log – click to open “Event log” window (see “Event log”).

Users – click to open “Users” window (see “Users”).

Re-connect... – click to restart the connection with the control panel. The startup window will be displayed (see “Startup window”). The command is NOT displayed if the “Auto-Connect (no CONNECTION menu)” option is enabled (see “Menu options”).

Log in again – click to log in again. The authorization window will be displayed (see “Authorization window”). The command is displayed if the “Auto-Connect (no CONNECTION menu)” option is enabled (see “Menu options”).

Configuration – hover the cursor over the command to display the configuration menu (see “Configuration menu”).

About GUARDX – click to display information about the program.

Licence agreement – click to view the licence agreement.

Check for update – click to open the window with information about the updates (see “Information about the updates”).

Exit – click to exit the program.

7.2 Communication menu

The communication menu is displayed after you click on ⏻ in the main menu (see “Main menu”).

TCP/IP, RS-232 – click to open “Connection” window (see “Connection”).

On – click to start local communication (via the COM port) with the control panel.

Off – click to terminate local communication (via the COM port) with the control panel.

7.3 Configuration menu

The configuration menu is displayed after you hover the cursor over the “Configuration” command in the additional menu (see “Additional menu”).

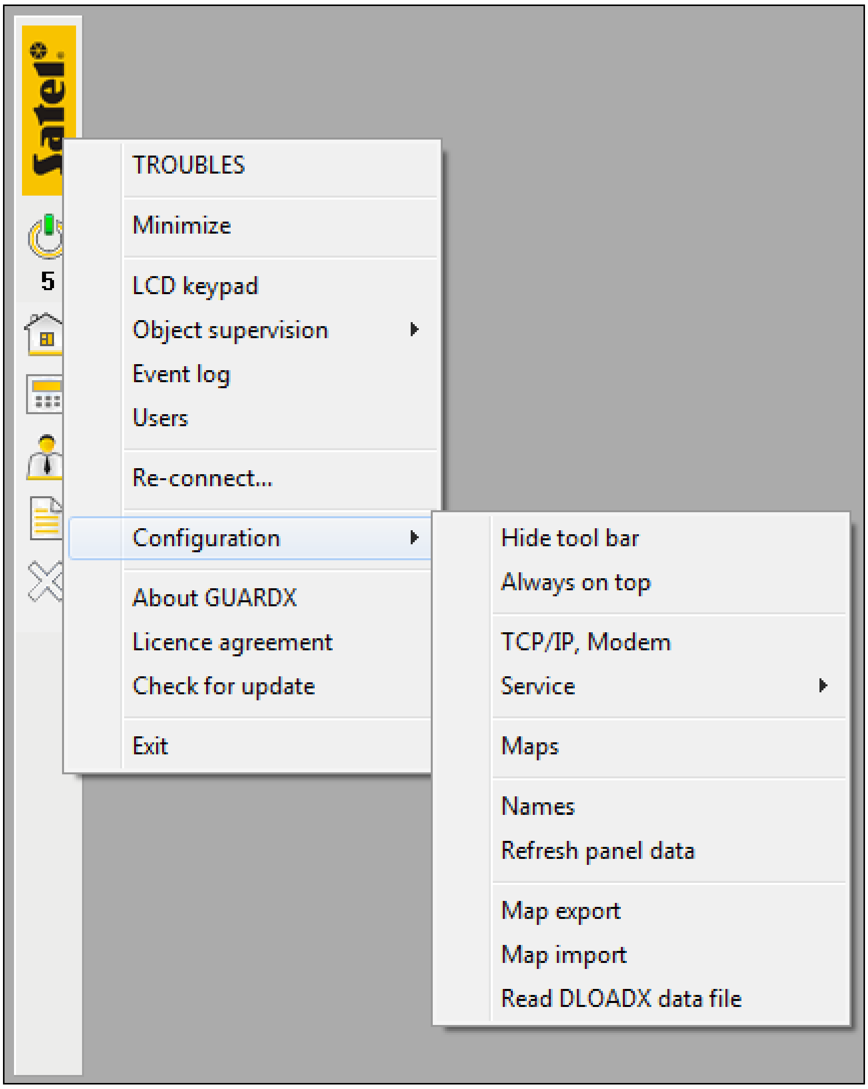


Fig. 13. Configuration menu.

Hide tool bar – click to hide the program main menu.

Show tool bar – click to display the program main menu (the configuration menu is available after you right-click on the program icon in the tray).

Always on top – click if the program main menu is to be always displayed on top. If the program main menu is always displayed on top, click on the command to restore the normal mode of displaying the main menu.

TCP/IP, Modem – click to open the “Connection” window (see “Connection”).

Service – hover the cursor over the command to display a menu containing two commands:

Options – click to open “GUARDX Service” window (see “GUARDX Service”).

Save window size/position – click to save the size and position of the main menu as well as open windows.

Maps – click to open the “Maps” window (see “Maps”).

Names – click to open the “Names” window (see “Names”).

Refresh panel data – click to read data from the control panel.

Map export – click to export the alarm system data to file.

SATEL recommends that you regularly export the system data to file. The file should be stored on a different disk than the one on which the GUARDX program is installed, or on another data carrier. These precautions will enable you to recover the data in the case of the operating system failure, disk damage, etc.

Map import – click to import the alarm system data from file.

Read DLOADX data file – click to read the alarm system data from the DLOADX data file (see “Reading DLOADX data file”).

8. Map

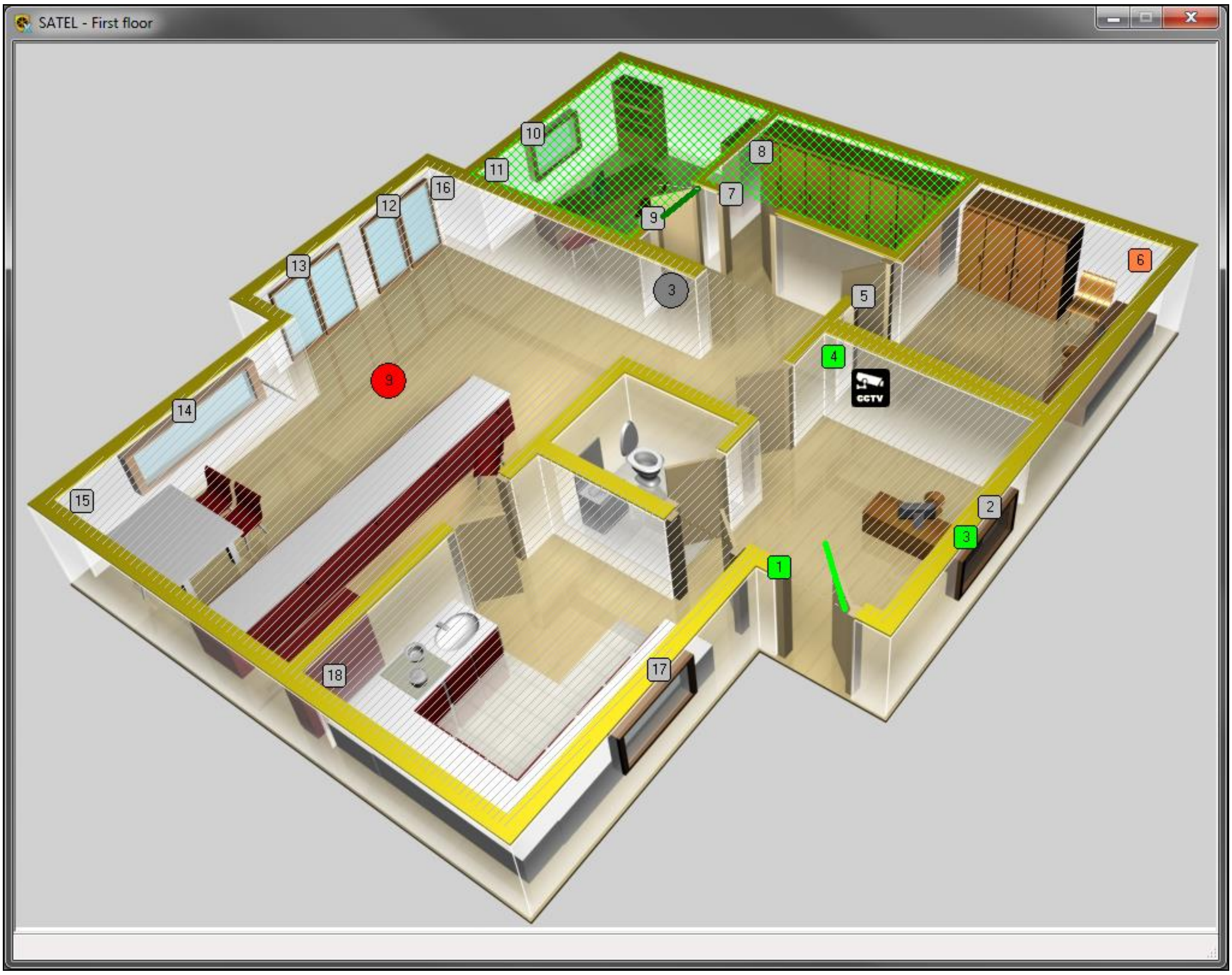


Fig. 14. Window with a map (example).

In this window you can:

- supervise the current state of partitions, doors, and also zones and outputs of the control panel as well as expansion modules connected to it,
- arm / disarm partitions,
- bypass / unbypass zones,
- activate / deactivate outputs,
- open the window with another map,
- check where the IP camera is installed and view the image from the camera,
- display the on-screen keypad,
- edit the map (see “Editing the map”).

The map creating procedure is described in section “Creating a new map”.

The following objects may be on the map:

- area (partition) – polygon. The color and pattern of the polygon indicate the partition state. Default settings are shown in Fig. 15 (you can change these settings when editing the map):

  A (diagonal gray lines) – partition disarmed.

  B (intersecting diagonal light-green lines) – partition armed.

  C (diagonal green lines) – exit delay countdown.

  D (yellow background) – entry delay countdown.

  E (red background) – alarm.

  F (diagonal red lines) – alarm memory when partition is disarmed.

  G (intersecting diagonal red lines) – alarm memory when partition is armed.

  H (dark rose background) – fire alarm.

  I (diagonal purple lines) – fire alarm memory when partition is disarmed.

  J (intersecting diagonal purple lines) – fire alarm memory when partition is armed.

  Hovering the cursor over a partition will display its name, number and information about its state in the window title.

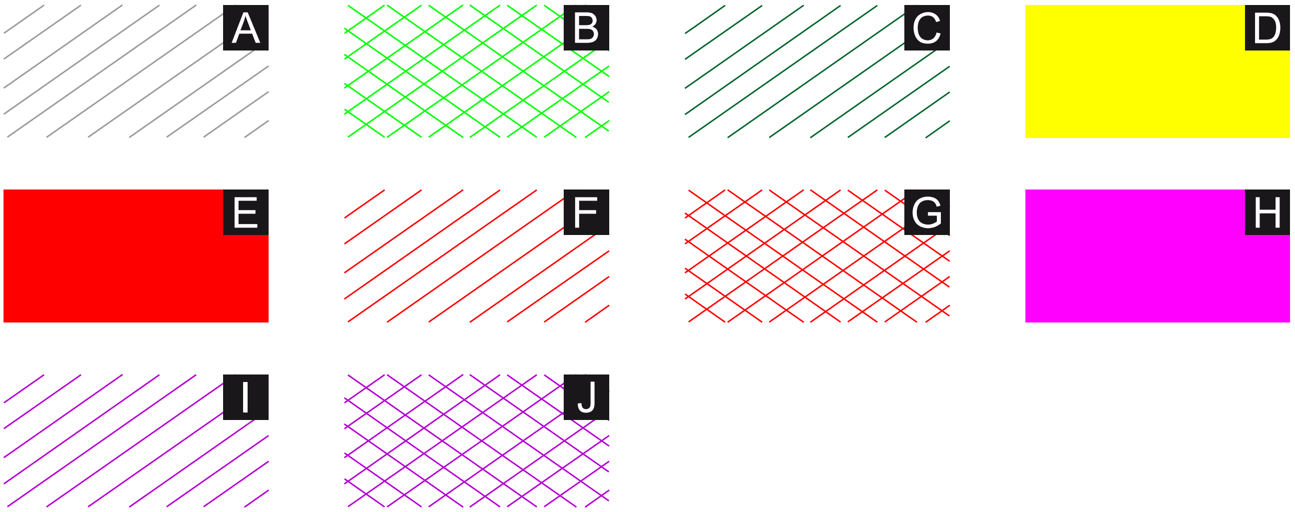


Fig. 15. Default colors and patterns indicating the partition state.

- detector (zone) – by default, it is a square with rounded corners and zone number in the center. The color indicates the zone state:

  gray – normal state,

light-green – violated,

rose – tamper / tamper alarm / tamper alarm memory,

red – alarm / alarm memory,

orange – bypassed,

yellow – trouble (long violation or no violation),

light-orange – masking.

You can change the object settings (including its colors) when editing the map.

Hovering the cursor over a zone will display its name, number and information about its state.

- output – by default, it is a circle with the output number in the center. The color indicates the state of output:

  grey – output turned off,

  red – output turned on.

  You can change the object settings when editing the map.

  Hovering the cursor over an output will display its name in the window title.
- link to another map – by default it is the name of the map the link points to. You can change the object settings when editing the map. Hovering the cursor over a link will display in the window title the name of the map the link will lead you to. Click on the link to open the window with the map.
- door – symbol.
- IP camera (link to the camera image) – by default it is the CCTV icon. You can change the icon when editing the map. Hovering the cursor over the link will display the camera name in the window title. Click on the link to display the image from the camera.

The image from camera will be displayed if a camera image viewing application is installed in the system.

If you click the right mouse button in the window, a context menu will be displayed with the following commands:

LCD keypad – click to display virtual keypad (see “Keypad”).

Map edit – click to edit the map (see “Editing the map”).

Save window size/position – click to save the size and position of the window.

If you click the right mouse button on an area (a partition), the following commands can be additionally available:

Arm – click to arm the partition.

Disarm – click to disarm the partition..

Clear alarm – click to clear alarm.

If you click the right mouse button on a detector (a zone), one of the following commands can be additionally available:

Bypass zone – click to bypass the zone.

Unbypass zone – click to unbypass the zone.

If you click the right mouse button on an output, the following commands will be additionally available:

Output ON – click to turn the output ON.

Output OFF – click to turn the output OFF.

8.1 Editing the map

You can edit the map immediately after creating it (see “Creating a new map”) or at any time, by doing the following steps.

1. Click the right mouse button in the “Map” window.
2. Click “Map edit” in the context menu.
3. The authorization window will be displayed.
4. Enter the code of access to the control panel and click “OK”.
5. The menu with map editing buttons will be displayed.

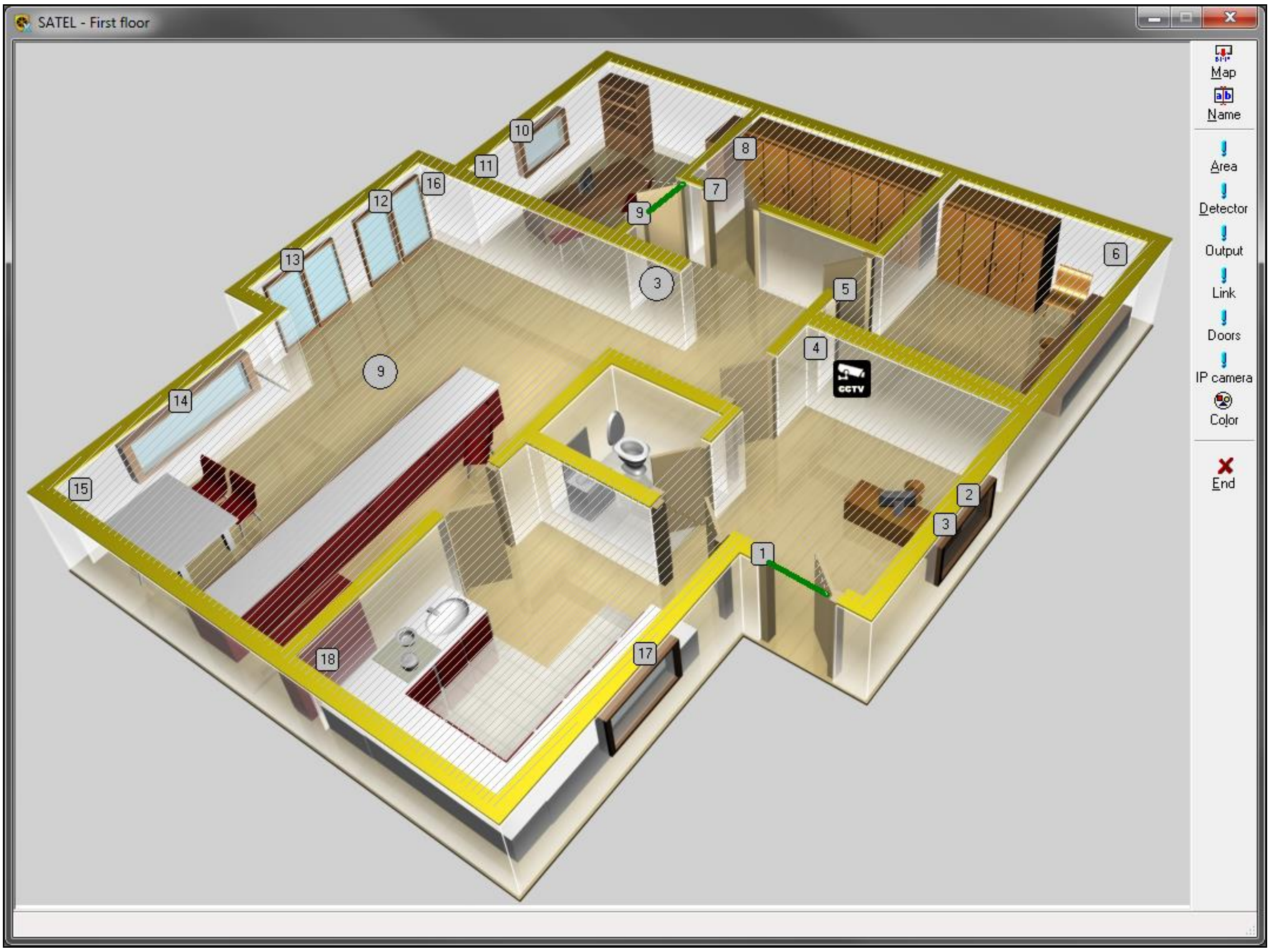


Fig. 16. Window with a map during edition (example).

8.1.1 Buttons

Map – click to add a site plan (see “Adding a site plan”).

Name – click to change the map name (see “Changing the map name”).

Area – click to place a partition on the map (see “Placing area (partition) on the map”).

Detector – click to place a zone on the map (see “Placing detector (zone) on the map”).

Output – click to place an output on the map (see “Placing output on the map”).

Link – click to place a link to another map on the map (see “Placing link to another map on the map”).

Doors – click to place a door on the map (see “Placing door on the map”).

IP camera – click to place a link to the IP camera image on the map (see “Placing link to the IP camera image on the map”).

Color – click to open the “Color” window (see “Color”).

End – click to finish editing the map.

8.1.2 Context menu when editing the map

Right-click on the window with map being edited to display the context menu containing the following commands:

Properties – click to edit the object properties (see “Object properties”). The command is available after you right-click on the object.

LCD keypad – click to display virtual keypad (see “Keypad”).

Map edit – click to finish editing the map.

Save window size/position – click to save the size and position of the window.

New area – hover the cursor over the command to display the list of partitions in the alarm system. Click on the partition you want to place on the plan and then follow the procedure described in section “Placing area (partition) on the map”.

New detector – hover the cursor over the command to display the list of zones in the alarm system. Click on the zone you want to place on the plan and then follow the procedure described in section “Placing detector (zone) on the map”.

New link – hover the cursor over the command to display the list of available maps (see “Creating a new map”). Click on the map, the link to which you want to place on the map and then follow the procedure described in section “Placing link to another map on the map”.

New output – hover the cursor over the command to display the list of outputs in the alarm system. Click on the output you want to place on the plan and then follow the procedure described in section “Placing output on the map”.

Delete – click to remove an object from the map (see “Removing an object from the map”). The command is available after you right-click on the object.

Send to back – click to send the object to back. The command is available after you right-click on the object.

Bring to front – click to bring the object to front. The command is available after you right-click on the object.

Additionally, a right-click on the door will display the following command:

Invert – click to change the direction of door opening on the map.

8.1.3 Adding a site plan

1. Click on the “Map” button in the menu.
2. In the window that will open, indicate location of the site plan (BMP file).
3. The window will be displayed in which you must decide if the plan is to be transparent or not. If you click “Yes”, the plan will be located above the areas (partitions) and will be transparent in those places where the color is the same as in the lower left corner of the plan. If you click “No”, the plan will be located under the areas (partitions) and will not be transparent.
4. The plan will be displayed in the window.

If you want to remove the transparency from the map, you must load the graphic file again.

Swapping the image will have no effect on the elements placed on the map.

If you want to delete the image, you must remove it from the program folder.

8.1.4 Changing the map name

1. Click on the “Name” button in the menu.
2. The “Map name” window will be displayed.
3. Enter a new name of the map.
4. Click “OK”.
5. The changed name will be displayed in the title of the map window.

8.1.5 Placing area (partition) on the map

1. Click on the “Area” button in the menu.
2. The list of partitions in the alarm system will be displayed.
3. Click on the partition you want to place on the map.
4. Hover the cursor over the map. The cursor shape will change to ✎ .
5. Click where one of the corners of the area being drawn is to be located. A point will be drawn.
6. Click where another corner of the area being drawn is to be located. Another point will be drawn as well as the line connecting it with the previous point. The line will be one of the sides of the area being drawn.
7. Continue drawing until the expected shape is obtained.
8. Finally, click again on the first point drawn to close the curve (when the cursor is over the point, its shape will change to ✛). The polygon drawn will be filled with diagonal lines. You can use the “drag and drop” method to move the polygon to another place. If you want to change the position of any point, move the cursor over it (the cursor shape will change to ⌖) and then use the “drag and drop” method.

8.1.6 Placing detector (zone) on the map

1. Click on the “Detector” button in the menu.
2. The list of zones in the alarm system will be displayed.
3. Click on the zone you want to place on the map.
4. A zone type object will appear on the map.
5. Use the “drag and drop” method to place the object at the required place on the map.

8.1.7 Placing output on the map

1. Click on the “Output” button in the menu.
2. The list of outputs in the alarm system will be displayed.
3. Click on the output you want to place on the map.
4. An output type object will appear on the map.
5. Use the “drag and drop” method to place the object at the required place on the map.

8.1.8 Placing link to another map on the map

1. Click on the “Link” button in the menu.
2. The list of available maps will be displayed (see “Creating a new map”).
3. Click on the map the link to which you want to place on the map.
4. A link type object will appear on the map.
5. Use the “drag and drop” method to place the object at the required place on the map.

8.1.9 Placing door on the map

1. Click on the “Door” button in the menu.

2. The list of access control devices in the alarm system will be displayed.
3. Click on the device supervising the door which you want to place on the map.
4. The door symbol will appear on the map.
5. Use the “drag and drop” method to place the object at the required place on the map.
6. If you want to change the size of the object or turn it, move the cursor over one of its ends (the cursor shape will change to ⌖) and use the “drag and drop” method.
7. If you want change direction to which the door on the map opens, right-click on the object and then click “Invert” in the context menu.

8.1.10 Placing link to the IP camera image on the map

1. Click on the “IP camera” button in the menu.
2. The CCTV icon will appear on the map.
3. Use the “drag and drop” method to place the object at the required place on the map.
4. Right-click on the object.
5. Click “Properties” in the context menu.
6. A window with the object properties will open (see “Camera properties”).
7. Configure settings of the link to the camera image.

8.1.11 Color

In this window, you can select colors that will be used for presentation of the state of partitions and zones.

ℹ *You can define the set of colors individually for each map.*

8.1.12 Object properties

Content of the window displayed by clicking on the “Properties” command in the context menu depends on the type of object.

8.1.12.1 Area properties

Partition – partition whose state is presented by the object. Click on the field if you want to select another partition.

Show partition name – select the option if the partition name is to be displayed.

Show text – select the option if the partition description is to be displayed. Enter the description text in the adjacent field.

No text – select this option if NO text is to be displayed.

Text

Font – click to configure settings of the font used to display the name or description of the partition.

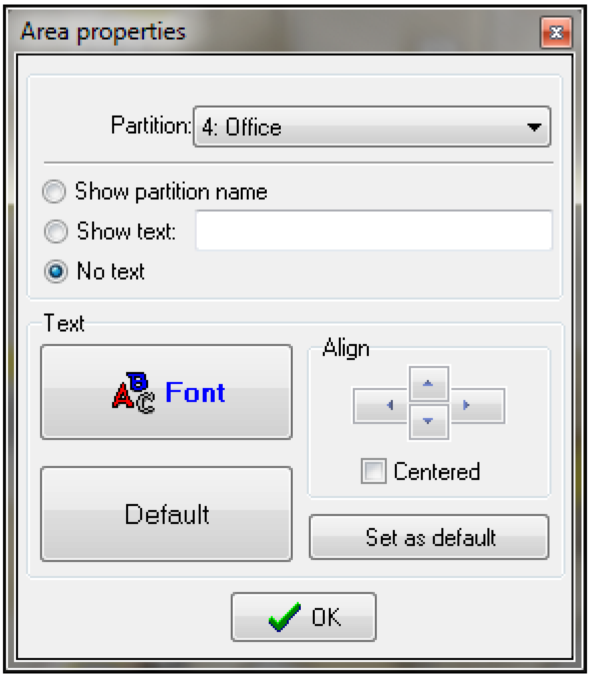
Default – click if the default font is to be used to display the name or description of the partition.

Align – using the arrow keys, you can change position of the text (name / description).

Centered – click to center the text (name / description).

Set as default – click to save the text settings.

OK – click to save the changes made and close the window.



Area properties

Partition: 4: Office

○ Show partition name

○ Show text:

● No text

Text

Font

Default

Align

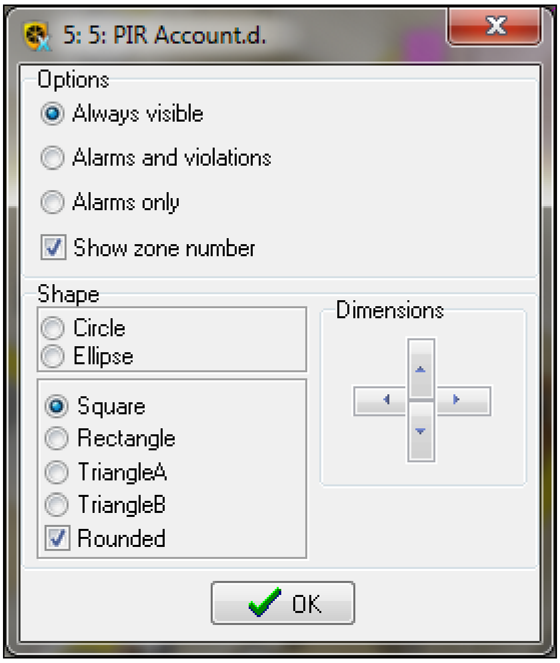
☐ Centered

Set as default

OK

Fig. 17. “Area properties” window.

8.1.12.2 Detector (zone) properties



5: 5: PIR Account.d.

Options

● Always visible

○ Alarms and violations

○ Alarms only

☑ Show zone number

Shape

○ Circle

○ Ellipse

● Square

○ Rectangle

○ TriangleA

○ TriangleB

☑ Rounded

Dimensions

OK

Fig. 18. Detector (zone) properties.

Options

Always visible – select the option if the object is to be always visible.

Alarms and violations – select this option if the object is NOT to be visible when the zone state is normal.

Alarms only – select this option if the object is NOT to be visible when the zone is in its normal state or is violated.

Show zone number – if the option is enabled, the zone number is displayed.

Shape

You can select the object shape (circle, ellipse, square, rectangle or triangle).

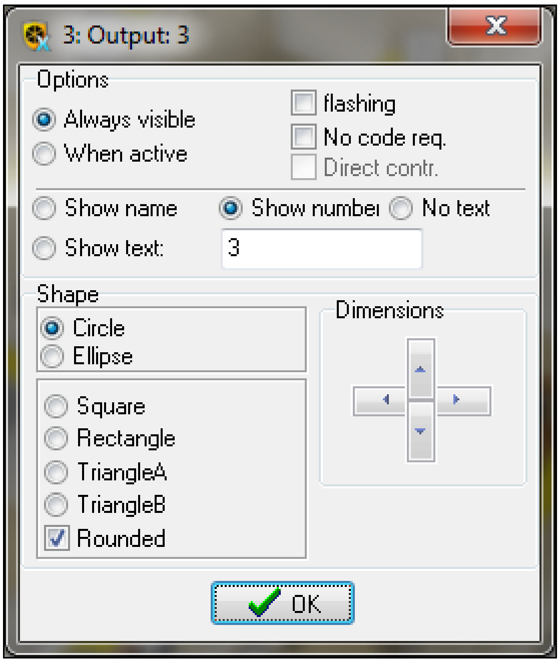
Rounded – if the option is enabled, the corners of the selected figure are rounded.

Dimensions

You can use the arrow keys to change the object size.

OK – click to save the changes made and close the window.

8.1.12.3 Output properties



3: Output: 3

Options

● Always visible
○ When active
□ flashing
□ No code req.
□ Direct contr.

○ Show name
● Show numbei
○ No text
○ Show text: 3

Shape

● Circle
○ Ellipse
○ Square
○ Rectangle
○ TriangleA
○ TriangleB
☑ Rounded

Fig. 19. Output properties.

Options

Always visible – select the option if the object is to be always visible.

When active – select the option if the object is to be visible only when the output is active.

flashing – if the option is enabled, the object is to flash when the output is active.

No code req. – if this option is enabled, you can control the output from the map without entering the code.

Direct contr. – if this option is enabled, left-click on the object will change the output state. The option is available if the “No code req.” option is enabled.

Show partition name – select the option if the output name is to be displayed.

Show text – select the option if the output description is to be displayed. Enter the description text in the adjacent field.

Show number – select the option if the output number is to be displayed.

No text – select this option if NO text is to be displayed.

Shape

You can select the object shape (circle, ellipse, square, rectangle or triangle).

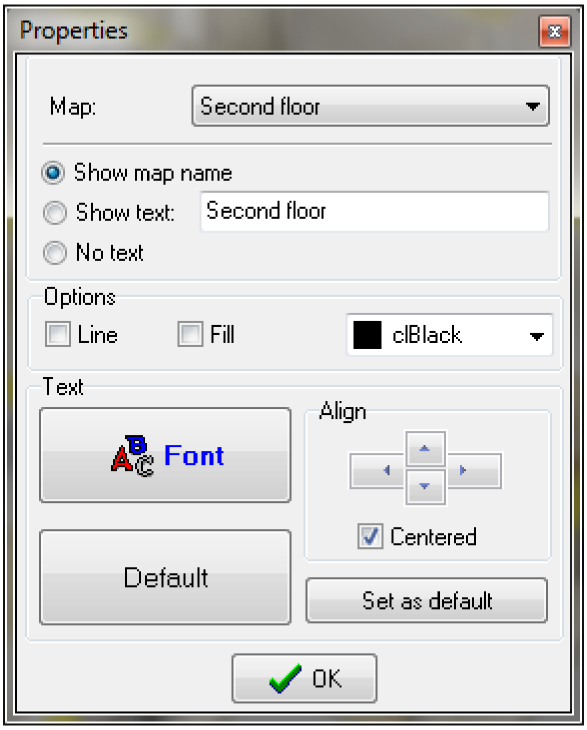
Rounded – if the option is enabled, the corners of the selected figure are rounded.

Dimensions

You can use the arrow keys to change the object size.

OK – click to save the changes made and close the window.

8.1.12.4 Link properties



Properties

Map: Second floor

● Show map name

○ Show text: Second floor

○ No text

Options

□ Line □ Fill ■ clBlack

Text

Fig. 20. Link properties.

Map – the map to which the link points. Click on the field, if you want to select another map.

Show map name – select the option if the map name is to be displayed.

Show text – select the option if the map description is to be displayed. Enter the description text in the adjacent field.

No text – select this option if NO text is to be displayed (if this option is enabled and the "Line" and "Fill" options are disabled, the object is not visible).

Options

Line – if this option is enabled, the object perimeter line is displayed.

Fill – if this option is enabled, the object filling is displayed.

[color] – you can select the color of perimeter line and filling.

Text

Font – click to configure settings of the font used to display the name or description of the map.

Default – click if the default font is to be used to display the name or description of the map.

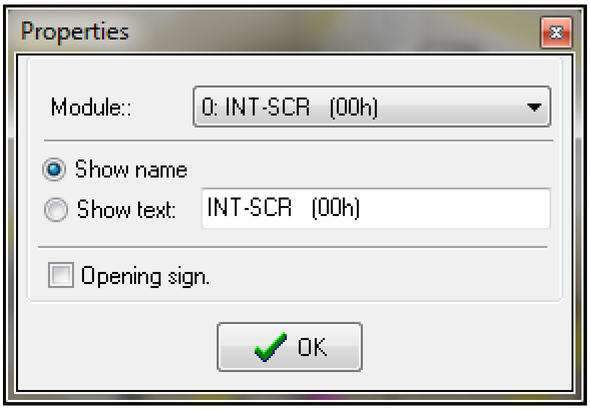
Align – you can use the arrow keys to change position of the text (name / description).

Centered – click to center the text (name / description).

Set as default – click to save the text settings.

OK – click to save the changes made and close the window.

8.1.12.5 Door properties



Properties

Module:: 0: INT-SCR (00h)

● Show name

○ Show text: INT-SCR (00h)

□ Opening sign.

Fig. 21. Door properties.

Module – you can select an access control device.

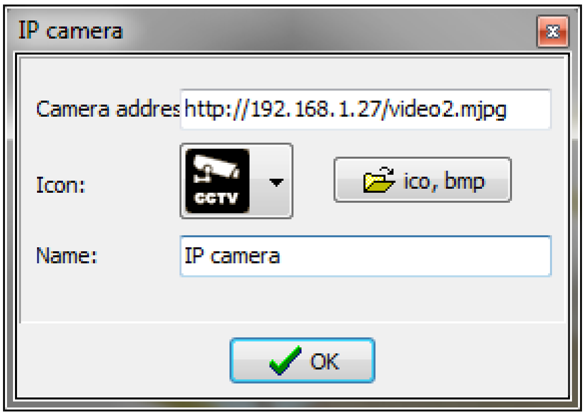
Show map name – select the option if the name of access control device is to be displayed.

Show text – select the option if the door description is to be displayed. Enter the description text in the adjacent field.

Opening sign. – if this option is enabled, opening the door is audibly signaled.

OK – click to save the changes made and close the window.

8.1.12.6 Camera properties



IP camera

Camera addres http://192.168.1.27/video2.mjpg

Icon:

Name: IP camera

Fig. 22. Properties of the link to the camera image

Camera address – system command to run the camera image viewing application. If the image is to be viewed through a web browser, enter the camera address.

Icon – click to select the camera icon from the list of icons available in the program.

ico, bmp – click to select your own icon. A window will open in which you can indicate location of the ICO or BMP file.

Name – camera name.

OK – click to save the changes made and close the window.

8.1.13 Removing an object from the map

1. Click the right mouse button on the object you want to delete.
2. Click “Delete” in the context menu.

9. Keypad

The keypad displayed on screen is a fully functional keypad. It can be used to operate the control panel in the same way as the LCD keypad connected to the control panel.

Operation of the system from the virtual keypad is available when the program is communicating with the control panel.

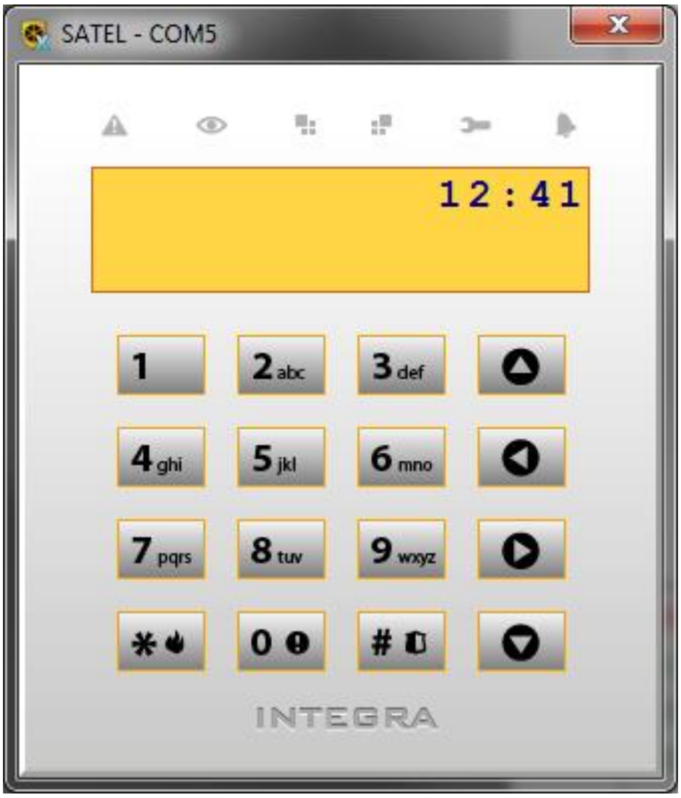


Fig. 23. GUARDX program virtual keypad.

If you use a computer keyboard to operate the virtual keypad:

- you can enter digits, letters and special characters from the keyboard,
- ENTER key acts as the keypad # key,
- ESC and DELETE keys act as the keypad * key,
- arrow keys act as the keypad arrow keys,
- functions which are run by a long-press on a keypad key can be run by long pressing the corresponding keyboard key.

The settings of the virtual keypad displayed in the GUARDX program you can configure in the control panel using an LCD keypad or the DLOADX program.

10. Users

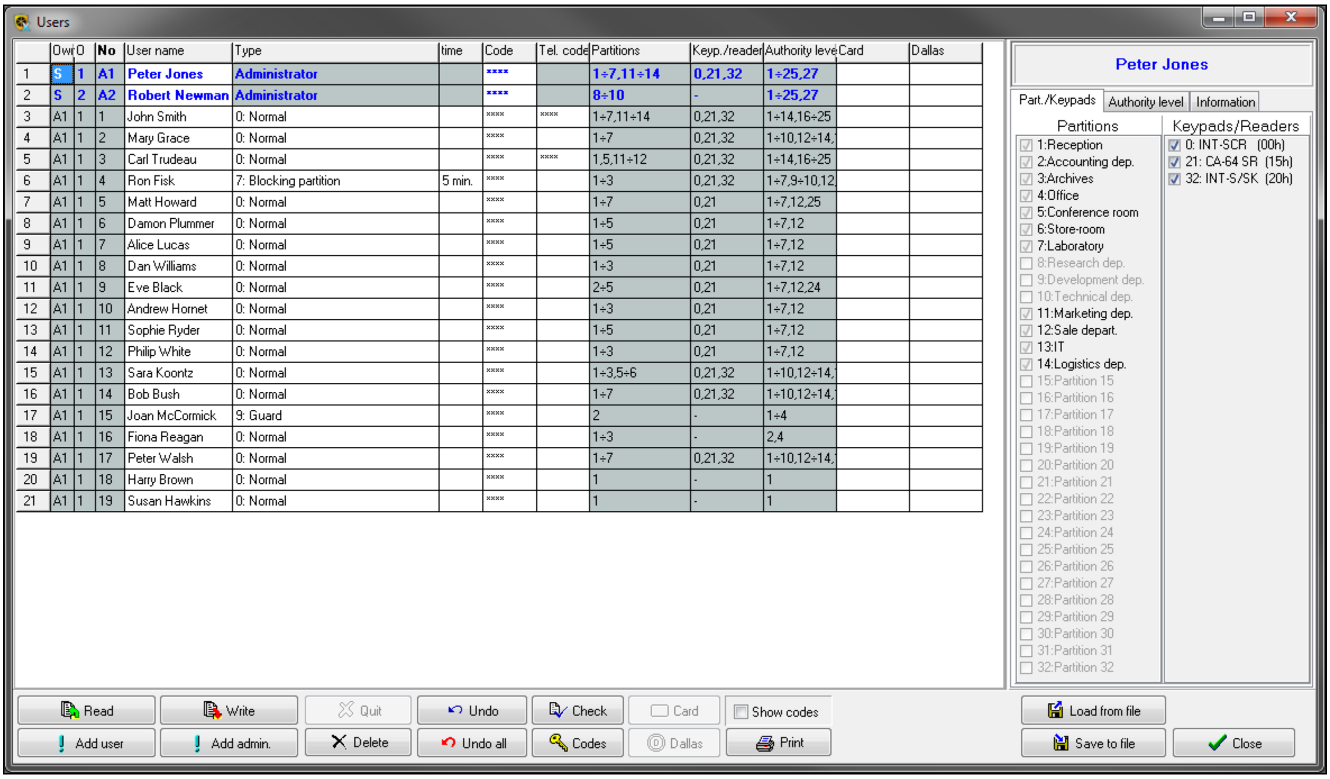
The data about administrators and users are presented in the table.

Owner – information on who has created and can remove the given user from the system:

S – service technician (installer). The service technician is owner of all administrators, i.e. can add them to or remove from the system. If the service technician has added a user, the owner of such user will be the administrator of the given object.

A1, A2 … – administrator of the given object (A1 – administrator of object 1, A2 – administrator of object 2, etc.). The administrator can edit and remove all users of his partition.

U1, U2 … – user, who has created the given user.



	Owr	O	No	User name	Type	time	Code	Tel. code	Partitions	Keyp./reader	Authority leve	Card	Dallas
1	S	1	A1	Peter Jones	Administrator		****		1÷7,11÷14	0,21,32	1÷25,27		
2	S	2	A2	Robert Newman	Administrator		****		8÷10	-	1÷25,27		
3	A1	1	1	John Smith	0: Normal		****	****	1÷7,11÷14	0,21,32	1÷14,16÷25		
4	A1	1	2	Mary Grace	0: Normal		****		1÷7	0,21,32	1÷10,12÷14,		
5	A1	1	3	Carl Trudeau	0: Normal		****	****	1,5,11÷12	0,21,32	1÷14,16÷25		
6	A1	1	4	Ron Fisk	7: Blocking partition	5 min.	****		1÷3	0,21,32	1÷7,9÷10,12,		
7	A1	1	5	Matt Howard	0: Normal		****		1÷7	0,21	1÷7,12,25		
8	A1	1	6	Damon Plummer	0: Normal		****		1÷5	0,21	1÷7,12		
9	A1	1	7	Alice Lucas	0: Normal		****		1÷5	0,21	1÷7,12		
10	A1	1	8	Dan Williams	0: Normal		****		1÷3	0,21	1÷7,12		
11	A1	1	9	Eve Black	0: Normal		****		2÷5	0,21	1÷7,12,24		
12	A1	1	10	Andrew Hornet	0: Normal		****		1÷3	0,21	1÷7,12		
13	A1	1	11	Sophie Ryder	0: Normal		****		1÷5	0,21	1÷7,12		
14	A1	1	12	Philip White	0: Normal		****		1÷3	0,21	1÷7,12		
15	A1	1	13	Sara Koontz	0: Normal		****		1÷3,5÷6	0,21,32	1÷10,12÷14,		
16	A1	1	14	Bob Bush	0: Normal		****		1÷7	0,21,32	1÷10,12÷14,		
17	A1	1	15	Joan McCormick	9: Guard		****		2	-	1÷4		
18	A1	1	16	Fiona Reagan	0: Normal		****		1÷3	-	2,4		
19	A1	1	17	Peter Walsh	0: Normal		****		1÷7	0,21,32	1÷10,12÷14,		
20	A1	1	18	Harry Brown	0: Normal		****		1	-	1		
21	A1	1	19	Susan Hawkins	0: Normal		****		1	-	1		

Peter Jones

Part./Keypads | Authority level | Information

Partitions

☑ 1:Reception
☑ 2:Accounting dep.
☑ 3:Archives
☑ 4:Office
☑ 5:Conference room
☑ 6:Store-room
☑ 7:Laboratory
☐ 8:Research dep.
☐ 9:Development dep.
☐ 10:Technical dep.
☑ 11:Marketing dep.
☑ 12:Sale depart.
☑ 13:IT
☑ 14:Logistics dep.
☐ 15:Partition 15
☐ 16:Partition 16
☐ 17:Partition 17
☐ 18:Partition 18
☐ 19:Partition 19
☐ 20:Partition 20
☐ 21:Partition 21
☐ 22:Partition 22
☐ 23:Partition 23
☐ 24:Partition 24
☐ 25:Partition 25
☐ 26:Partition 26
☐ 27:Partition 27
☐ 28:Partition 28
☐ 29:Partition 29
☐ 30:Partition 30
☐ 31:Partition 31
☐ 32:Partition 32

Keypads/Readers

☑ 0: INT-SCR (00h)
☑ 21: CA-64 SR (15h)
☑ 32: INT-S/SK (20h)

Fig. 24. “Users” window.

O – number of the object to which the given user belongs. Click on the column heading to change the way of data sorting in the table (the users are sorted by objects, or not).

No – user number. Click on the column heading to sort users in the table by their number.

User name – individual user name (up to 16 characters). Click on the column heading to sort users in the table by their name.

Type – user type (see: “User types”).

time – additional parameter for some types of users:

- validity for the “Renewable” and “Temporary” type of user,
- blocking time for the “Blocking partition” type of user,
- time schedule (first number) and validity (second number) for the “Scheduled” type of user.

Code – a string of 4 to 8 digits for user authentication in the alarm control panel (the minimum length of the code can be defined in the control panel settings). The codes are presented as a sequence of asterisks, unless the “Show codes” option is enabled. If the code is presented against yellow background, it means that another user has accidentally entered this code during code changing, and, therefore, it must be changed.

Tel. code – a string of 4 digits for authentication of the user when using the functions of telephone call answering and telephone control.

Partitions – numbers of partitions to which the user has access (i.e. can arm / disarm them, clear alarm, etc.). To select the partitions, use the “Part./keypads” tab on the right side of the window (see “Part./Keypads”).

Keyp./reader – addresses of additional modules from which the user can operate the system (proximity card arm/disarm devices, partition keypads, code locks, proximity card reader expansion modules and DALLAS chip expansion modules) and to which the user has access. To select the partitions, use the “Part./keypads” tab on the right side of the window (see “Part./Keypads”).

Authority level – numbers of user rights. To select a right, use the “Authority level” tab on the right side of the window (see “Authority level”).

Card – number of the user's proximity card.

Dallas – number of the user's DALLAS iButton.

Buttons and options

If the program is not connected to the control panel, some buttons are not available.

Read – click to read the user data from the control panel.

Write – click to write the changes to the control panel.

Clicking on the “Write” button will display the authorization window (see “Authorization window”). If you select the “Remember access code” option in the window, the code will be remembered until the “Users” window is closed, and the authorization window will not reappear.

Quit – click to stop reading/writing data.

Undo – click to undo the changes made to the selected user (settings read from the control panel will be restored).

Check – click to check whether the user names do not repeat themselves.

Card – click to add a proximity card to the user (see “Adding proximity card”). The button is available after you click in the “Card” column.

Show codes – if the option is enabled, codes of the users who have not changed their codes are shown in the “Code” column

Add user – click to add new users (see “Adding user”).

Add admin. – click to add new administrator (see “Adding administrator”).

Delete – click to remove selected administrator or user (see “Removing administrator / user”).

Undo all – click to undo all the changes made that have not been saved yet.

Codes – click to generate new codes for users (see “Codes”).

Dallas – click to add a DALLAS iButton to the user (see “Adding DALLAS iButton”). The button is available after you click in the “Dallas” column, provided that a DALLAS iButton supporting expander is installed in the system.

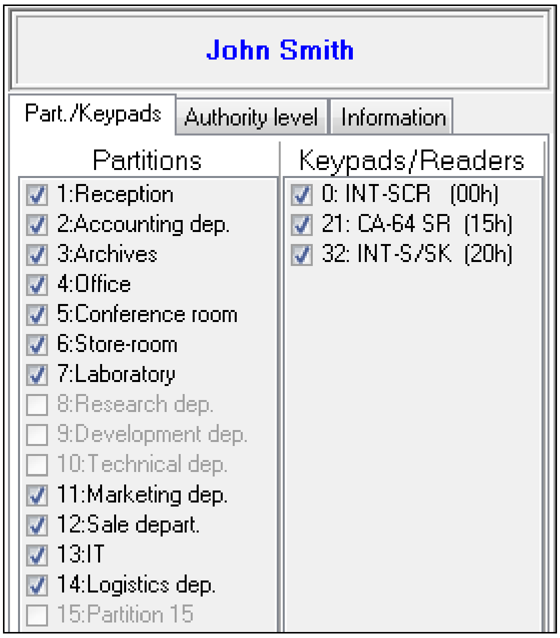
Print – click to print information about users.

Load from file – click to load data from a UDT file.

Save to file – click to save data to a UDT file.

Close – click to close the window.

10.1 Part./Keypads



John Smith

Part./Keypads | Authority level | Information

Partitions

☑ 1:Reception
☑ 2:Accounting dep.
☑ 3:Archives
☑ 4:Office
☑ 5:Conference room
☑ 6:Store-room
☑ 7:Laboratory
□ 8:Research dep.
□ 9:Development dep.
□ 10:Technical dep.
☑ 11:Marketing dep.
☑ 12:Sale depart.
☑ 13:IT
☑ 14:Logistics dep.
□ 15:Partition 15

Keypads/Readers

☑ 0: INT-SCR (00h)
☑ 21: CA-64 SR (15h)
☑ 32: INT-S/SK (20h)

Fig. 25. “Part./Keypads” tab.

Partitions – list of partitions in the system. Select the partitions to which the user is to have access. Numbers of the selected partitions are shown in the “Partitions” column.

Keypads/Readers – list of partition keypads, code locks, proximity card reader expansion modules and DALLAS expansion modules in the system. Select the modules to which the user is to have access. Addresses of the selected modules are shown in the “Keyp./reader” column.

10.2 Authority level

The tab presents the list of all rights. Select which rights the user is to have. The numbers of selected rights are presented in the “Authority level” column.

Arming – the user can arm the system.

Disarming – the user can disarm the system.

Disarm, when other user arm – the user can disarm, if other user has armed. If the user does not have this right, he can only disarm if he has armed.

Partition alarm canceling – the user can clear alarms in partitions to which he has access.

Object alarm canceling – the user can clear alarms in the object to which he belongs.

Other partitions alarm canceling – the user can clear alarms in other objects.

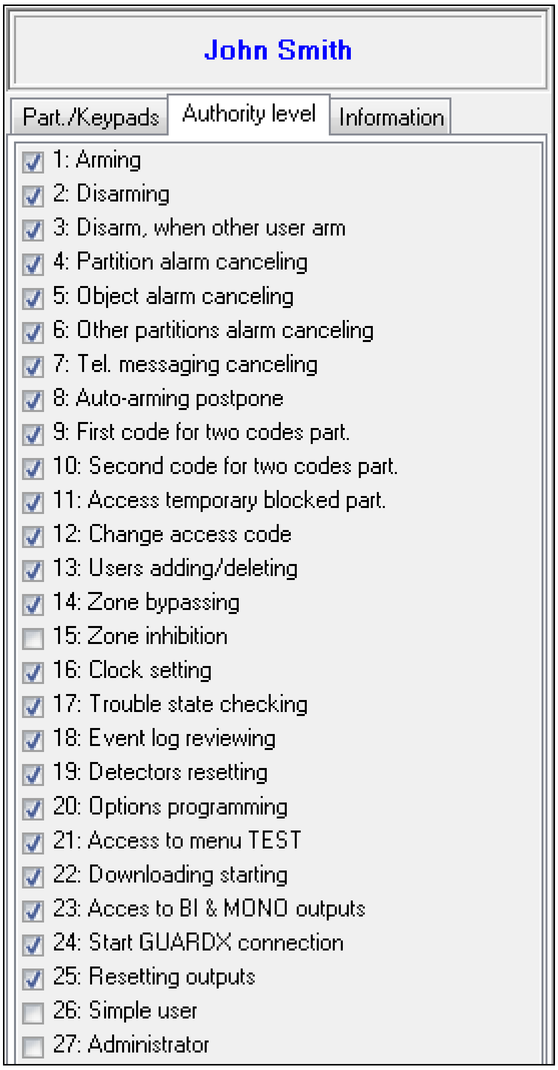
Tel. messaging canceling – the user can cancel telephone messaging.

Auto-arming postpone – the user can defer arming by the timer.

First code for two codes part. – the user can enter the first code, if 2 codes are needed to arm / disarm.

Second code for two codes part. – the user can enter the second code, if 2 codes are needed to arm / disarm.

Access temporary blocked part. – the user can disarm temporary blocked partitions (“With temporary blocking” type partition).



John Smith

☑ 1: Arming
☑ 2: Disarming
☑ 3: Disarm, when other user arm
☑ 4: Partition alarm canceling
☑ 5: Object alarm canceling
☑ 6: Other partitions alarm canceling
☑ 7: Tel. messaging canceling
☑ 8: Auto-arming postpone
☑ 9: First code for two codes part.
☑ 10: Second code for two codes part.
☑ 11: Access temporary blocked part.
☑ 12: Change access code
☑ 13: Users adding/deleting
☑ 14: Zone bypassing
□ 15: Zone inhibition
☑ 16: Clock setting
☑ 17: Trouble state checking
☑ 18: Event log reviewing
☑ 19: Detectors resetting
☑ 20: Options programming
☑ 21: Access to menu TEST
☑ 22: Downloading starting
☑ 23: Acces to BI & MONO outputs
☑ 24: Start GUARDX connection
☑ 25: Resetting outputs
□ 26: Simple user
□ 27: Administrator

Fig. 26. “Authority level” tab.

Change access code – the user can change own access code.

Users adding/deleting – the user can add, edit and delete users.

Zones bypassing – the user can inhibit the zones.

Zone isolation – the user can isolate the zones.

Clock setting – the user can program the control panel clock.

Trouble state checking – the user can view the current troubles.

Event log reviewing – the user can view the event log.

Detectors resetting – the user can reset the “43. Resetable power supply” type outputs (the user has access to “Reset zones” user function).

Options programming – the user has access to the user functions in the “Change options” submenu.

Access to menu TEST – the user has access to the user functions in the “Tests” submenu.

Downloading starting – the user can initiate remote programming of the control panel from the keypad..

Access to BI & MONO outputs – the user can control the outputs.

Start GUARDX connection – the user can use the GUARDX program to operate the system.

Resetting outputs – the user can clear latched outputs (the user has access to “Clr.latch.outs” user function).

Simple user – having entered the code, confirmed with the # key, the user never selects the partitions which are to be armed / disarmed. All partitions the user has access will be armed / disarmed.

Administrator – the user has access to the menu functions which are reserved for the administrator.

10.3 Information

In this tab, you can assign an image to the user, as well as enter additional information. These data are only stored in the GUARDX program (they are not written to the control panel).

... – click to add user picture (see “Adding user picture”).

10.3.1 Adding user picture

1. Click ....
2. In the window that will open, indicate location of the picture. The program supports JPG, JPEG, BMP, TIF, TIFF, ICO, EMF or WMF file formats.
3. Click “Open”.
4. The picture will be displayed in the tab.

10.3.2 Deleting user picture

1. Right-click on the picture.
2. Click “Delete” in the context menu.

10.3.3 Entering additional information about user

1. Click in the lower part of the “Information” tab.
2. Enter additional information about the user.

10.4 User types

The description includes only the codes, but the information provided below applies to all identifiers assigned to the user.

0 Normal – basic type of user.

1 One-time – the user will get one-time access.

2 Renewable – the user has access to the system for a defined period of time. The user validity time should be entered in the “Time” column. Before the validity time expires, the control panel will prompt the user to change the code. After the code has been changed, the validity time will run from the beginning.

3 Temporary – the user has access to the system for a defined period of time. The user validity time should be entered in the “Time” column. After the validity time expires, the user will have no access to the system.

4 Duress – code to be used in hold-up and duress situations. If the code is used, the silent alarm is triggered and the monitoring station can be notify about the situation.

5 “Mono” output operating – code for control of the “24.MONO switch” type outputs.

6 “Bi” output operating – code for control of the “25.BI switch” type outputs.

7 Blocking partition – the code enables access to the armed partitions. Using the code will block the armed partition(s) (the partition zones will not trigger the burglary alarm). The blocking time is defined individually for each user within the range from 1 to 109 minutes.

If, however, the time of blocking for guard round is defined for the partition and its duration is longer, the blocking will last longer.

8 Cash machine zones bypassing – the code to be used to unblock access to the cash dispenser (the “24H Cash machine” type zones will be temporarily bypassed in the partition).

9 Guard – using this code means having made the round (additionally, it can result in the partition being temporarily bypassed for the duration of guard round). The installer defines the modules which are used to confirm making the round and determines the time interval between successive rounds. If such a user is granted access to the partition, he/she will have the same possibilities as the “Normal” type user.

10 Scheduled – the user has access to the system as per the time schedule for a specified period of time. The schedule number (time schedule you can configure using the LCD keypad or DLOADX program) and user validity time should be entered in the “Time” column.

10.5 Managing users

You can manage the users in the “Users” window (see “Users”) if the program is connected to the control panel.

The administrators can be added, edited and removed by the installer (service technician).

The installer (service technician) can edit users of the given object, if the “Serv. can edit” option is enabled by the administrator of this object.

The user can edit and remove the users in relation to which he/she is the superior. For example, if the user A has created the user B, and the user B has created the user C, then the user A can edit the users B and C.

10.5.1 Adding administrator

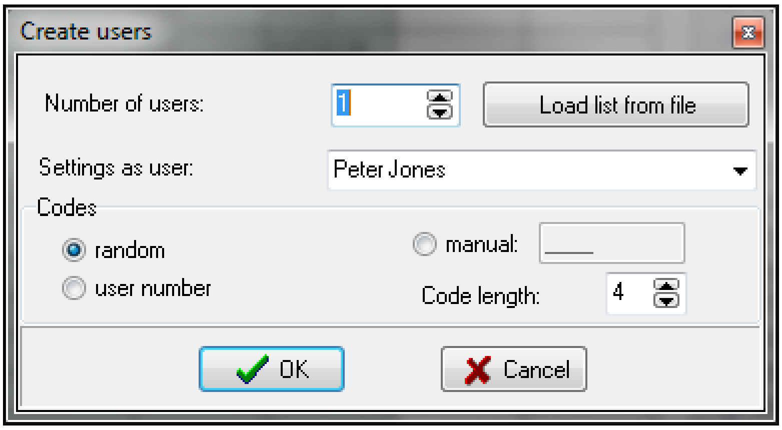
You can add an administrator only when there is an object to be managed by the administrator. There can be 1 administrator in each object. The administrator has access to all partitions in the object and also specifies how the system can be accessed by using the service code.

1. Click “Add admin.”.
2. The new administrator will appear in the table.
3. Enter individual name of the new administrator.
4. Enter a new code instead of the default factory code.
5. Click on the “Authority level” tab and define the authority level of the new administrator.
6. Click “Write” to save changes to the control panel.

10.5.2 Adding user

The new user cannot have a higher authority level than that of the person who is adding him/her to the system.

1. Click “Add user”.
2. The “Create users” window will open.



Number of users: 1

Settings as user: Peter Jones

Codes

● random

○ user number

○ manual:

Code length: 4

Fig. 27. “Create users” window.

3. In the “Number of users” field, define how many users are to be added to the system.

> *On clicking the “Load list from file” button, you can load a text file with a list of names of users to be created (the first 16 characters from each line will be loaded, without the initial spaces and digits).*

4. In the “Settings as user” field, select the user, based on whose settings the new user(s) will be created. The new user(s) will be assigned to the same object as the model user.
5. Define how the code of the new user(s) is to be created. The code can be random generated, created on the basis of user number, or entered manually.
6. Enter the number of digits in the code to be created.
7. Click “OK”. The new user(s) will appear in the table.
8. Enter individual name of the new user(s).
9. In the “Type” column, select the user type.
10. If the “Renewable”, “Temporary”, “Partition blocking” or “Scheduled” user type is selected, define additional parameters in the “Time” column.
11. If the user is to use the answering and remote control functions, enter the telephone code.
12. Click on “Part./keypads” tab and define to which partitions and modules the user is to have access (by default, the new user is granted access to partitions and modules to which the user whose settings served as a model for creating the new user has access).
13. Click on the “Authority level” tab and define the authority level for the new user.
14. Optionally, in the “Information” tab, you can assign an image to the user and enter additional related information.
15. Click “Write” to save changes to the control panel.

10.5.3 Removing administrator / user

1. Click on the administrator / user you want to remove.
2. Click “Delete”.
3. The “Confirm” window will open.
4. Click “Yes”.
5. The “Confirm” window will be closed, and the administrator / user will be highlighted in red in the table.
6. Click “Write” to save changes to the control panel.

10.5.4 Adding proximity card

You can add a proximity card by entering its number manually or reading its number by means of a device provided with proximity card reader.

10.5.4.1 Entering the number manually

1. In the “Card” column, click on the field of the user to whom you want to assign a card.
2. Enter the card serial number and confirm by pressing ENTER.
3. Click “Write” to save changes to the control panel.

10.5.4.2 Reading the number

1. In the “Card” column, click on the field of the user to whom you want to assign a card.
2. Click “Card”.
3. The card adding window will be opened.
4. In the “Reader” field, select the device (keypad with built-in reader, proximity card arm/disarm device, expansion module for proximity card readers, etc.) to be used for reading the card number.
5. Click “Add” button.
6. According to the prompts displayed in the window, present the card twice to the proximity card reader.
7. When the “Card read” message is displayed, and the number of the card appears in the “Card code” field, click “Close” button.
8. The card adding window will be closed. The card number will appear in the “Card” column.
9. Click “Write” to save changes to the control panel.

10.5.5 Removing proximity card

1. In the “Card” column, double click on the field of the user whose card you want to remove.
2. Press the DELETE key to clear the card number.
3. Click “Write” to save changes to the control panel.

10.5.6 Adding DALLAS iButton

You can add a DALLAS iButton by entering its number manually or reading its number by means of a DALLAS iButton reader.

10.5.6.1 Entering the number manually

1. In the “Dallas” column, click on the field of the user to whom you want to add an iButton.
2. Enter the iButton number and confirm by pressing ENTER.
3. Click “Write” to save changes to the control panel.

10.5.6.2 Reading the number

1. In the “Dallas” column, click on the field of the user to whom you want to add an iButton.
2. Click “Dallas”.
3. The DALLAS iButton adding window will be opened.
4. In the “Reader” field, select the DALLAS reader expansion module to be used for reading the DALLAS iButton number.
5. Click “Add”.
6. According to the prompts displayed in the window, read in the iButton twice.
7. When the “Dallas read” message is displayed, and the number of the DALLAS iButton appears in the “Card code” field, click “Close”.

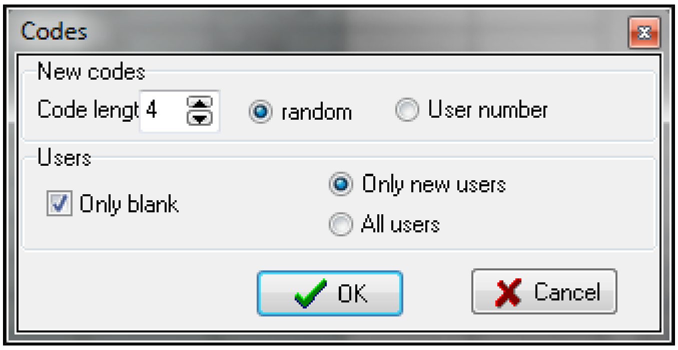
8. The DALLAS iButton adding window will be closed. The iButton number will appear in the “Dallas” column.
9. Click “Write” to save changes to the control panel.

10.5.7 Removing DALLAS iButton

1. In the “Dallas” column, double click on the field of the user whose iButton you want to remove.
2. Press the DELETE key to clear the iButton number.
3. Click “Write” to save changes to the control panel.

10.6 Codes

The window allows you to generate new user codes.



Codes

New codes

Code lengt 4

● random ○ User number

Users

☑ Only blank

● Only new users

○ All users

Fig. 28. “Codes” window.

New codes

Code length – define how many digits are the new codes to have (from 4 to 8).

random – select the option if the codes are to be randomly generated by the program.

User number – select the option if the codes are to be created based on the user numbers.

Users

Only blank – if the option is enabled, the codes will be created only for the for users who have no code.

Only new users – select the option if the codes are to be generated only for new users (users who are not saved to the control panel).

All users – select the option if the codes are to be generated for all users.

Cancel – click to close the window without generating any codes.

OK – click to generate new codes.

11. Event log

Presented in the window is a list of alarm system events.

No. – event number on the list.

Date – date the event occurred.

Time – time the event occurred.

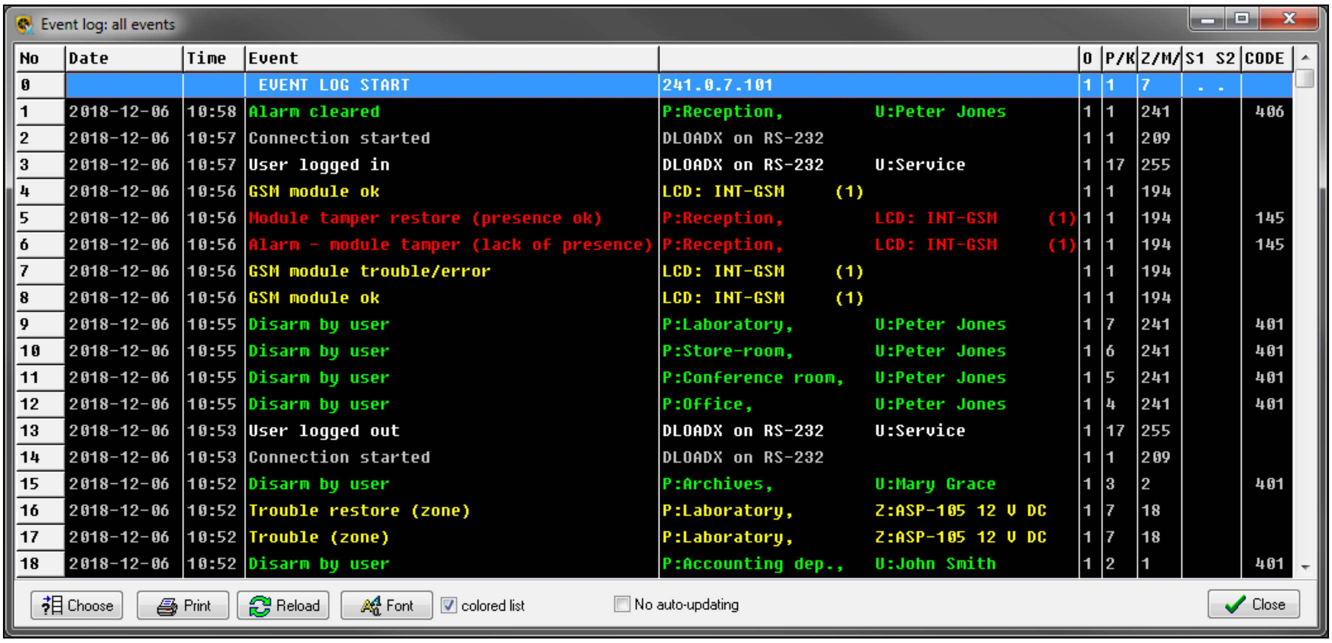
Event – description of the event.

[Details] – additional information on the event, e.g. type of connection, name of device, partition, zone, user etc., the event relates to.

O – object number.

P/K – partition number, module address or output number (for events providing information about output trouble).

Z/M/U – number of zone, module or user.



No	Date	Time	Event		O	P/K	Z/M/	S1	S2	CODE
0			EVENT LOG START	241.0.7.101	1	1	7	.	.	
1	2018-12-06	10:58	Alarm cleared	P:Reception, U:Peter Jones	1	1	241			406
2	2018-12-06	10:57	Connection started	DLOADX on RS-232	1	1	209			
3	2018-12-06	10:57	User logged in	DLOADX on RS-232 U:Service	1	17	255			
4	2018-12-06	10:56	GSM module ok	LCD: INT-GSM (1)	1	1	194			
5	2018-12-06	10:56	Module tamper restore (presence ok)	P:Reception, LCD: INT-GSM (1)	1	1	194			145
6	2018-12-06	10:56	Alarm – module tamper (lack of presence)	P:Reception, LCD: INT-GSM (1)	1	1	194			145
7	2018-12-06	10:56	GSM module trouble/error	LCD: INT-GSM (1)	1	1	194			
8	2018-12-06	10:56	GSM module ok	LCD: INT-GSM (1)	1	1	194			
9	2018-12-06	10:55	Disarm by user	P:Laboratory, U:Peter Jones	1	7	241			401
10	2018-12-06	10:55	Disarm by user	P:Store-room, U:Peter Jones	1	6	241			401
11	2018-12-06	10:55	Disarm by user	P:Conference room, U:Peter Jones	1	5	241			401
12	2018-12-06	10:55	Disarm by user	P:Office, U:Peter Jones	1	4	241			401
13	2018-12-06	10:53	User logged out	DLOADX on RS-232 U:Service	1	17	255			
14	2018-12-06	10:53	Connection started	DLOADX on RS-232	1	1	209			
15	2018-12-06	10:52	Disarm by user	P:Archives, U:Mary Grace	1	3	2			401
16	2018-12-06	10:52	Trouble restore (zone)	P:Laboratory, Z:ASP-105 12 V DC	1	7	18			
17	2018-12-06	10:52	Trouble (zone)	P:Laboratory, Z:ASP-105 12 V DC	1	7	18			
18	2018-12-06	10:52	Disarm by user	P:Accounting dep., U:John Smith	1	2	1			401

Fig. 29. “Event log” window.

S1 S2 – reporting status (S1 – monitoring station 1, S2 – monitoring station 2):

no symbol – event is not reported.

+ – event successfully reported to the monitoring station.

. – event waiting to be reported to the monitoring station.

! – event not reported yet because of failure of communication with the monitoring station (the station has not acknowledged receiving the event).

Code – internal code assigned to an event in the control panel (consistent with the Contact ID format code for events that are reported in this format).

If, since the last readout, the number of events has exceeded the capacity of control panel memory, part of the older events will be erased. In such a case, a message about lack of continuity of the event log will be displayed in the window.

Buttons and options

Choose – click to open the “Choose” window (see “Choose”).

Print – click to open the “Print” window (see “Print”).

Reload – click to read events from the control panel / update the event log.

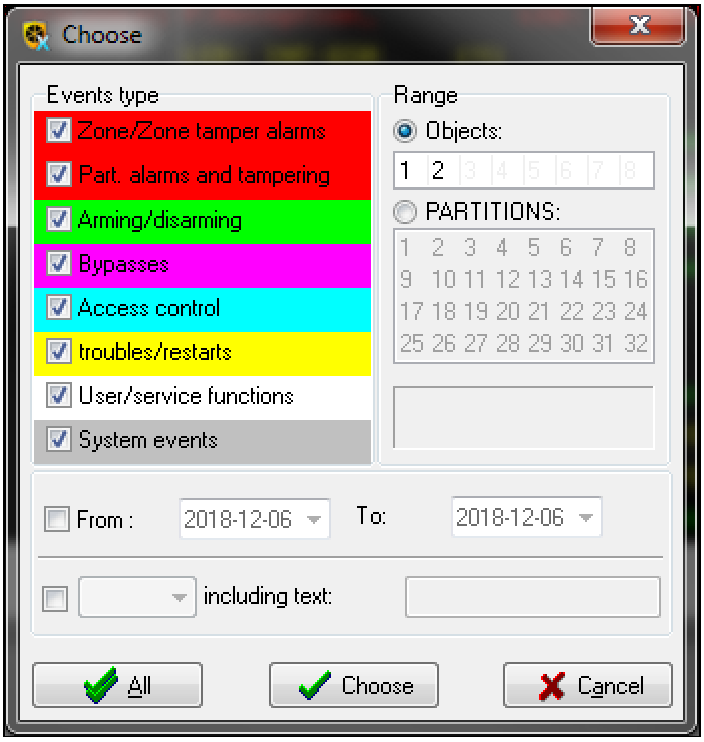
Font – click to configure settings of the font used to present events.

colored list – if this option is enabled, events are displayed in colors that can be defined in the “Choose” window.

No auto-updating – if this option is enabled, events are not automatically read from the control panel (click “Reload” to read events from the control panel).

Close – click to close the window.

11.1 Choose



Events type

☑ Zone/Zone tamper alarms

☑ Part. alarms and tampering

☑ Arming/disarming

☑ Bypasses

☑ Access control

☑ troubles/restarts

☑ User/service functions

☑ System events

Range

● Objects:

1 2 3 4 5 6 7 8

○ PARTITIONS:

1 2 3 4 5 6 7 8
9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32

□ From : 2018-12-06 To: 2018-12-06

□ including text:

Fig. 30. “Choose” window.

In the “Choose” window, you can assign colors to different event types and filter the events.

Events type – types of events that are to be displayed. If the “Colored list” option is selected in the “Event log” window, the event types will be highlighted in color.

Range – the range of displayed events can be limited to the selected objects or partitions:

Objects – events will be filtered by objects. The numbers of fields in the table correspond to the numbers of objects. The field color has the following meaning:

- white – events from the object will not be displayed,
- orange – events from the object will be displayed.

Double-click on the field to change its color.

If no object is highlighted (all fields remain white), events from all objects will be displayed.

PARTITIONS – events will be filtered by partitions. The numbers of fields in the table correspond to those of partitions. The field color has the following meaning:

- white – events from the partition will not be displayed,
- orange – events from the partition will be displayed.

Double-click on the field to change its color.

If no partition is highlighted (all fields remain white), events from all partitions will be displayed.

From – enter a date in this field, if events that occurred after this date are to be displayed.

To – enter a date in this field, if events that occurred before this date are to be displayed.

only including text – if you select this option, you can define the text that must be included in event description for the event to be displayed.

and including text – if you select this option, you can define the text that, if included in the event description, will cause the event to be displayed next to the events that have been selected by other criteria (event type, range, etc.).

without including text – if you select this option, you can define the text that, if included in the event description, will cause the event not to be displayed.

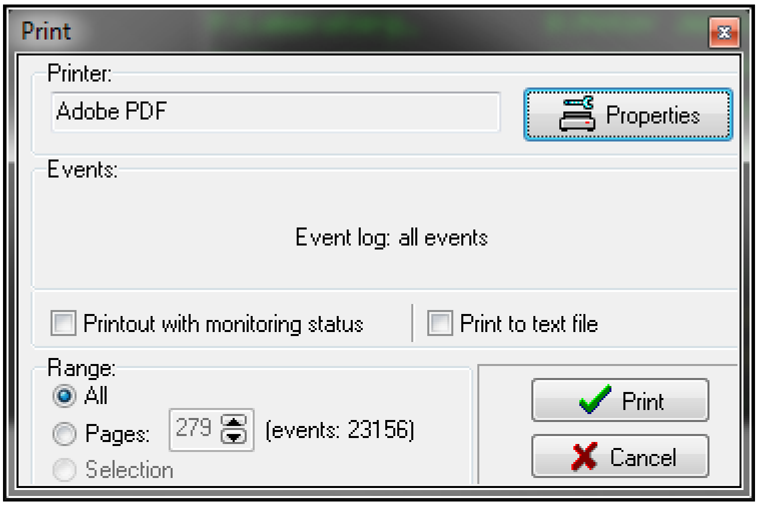
Buttons

All – click on the button to close the window and display all events in the "Event log" window (without taking into account the criteria defined in the "Choose" window).

Choose – click on the button to close the window and display events in the "Event log" window according to the criteria defined in the "Choose" window.

Cancel – click to close the window, disregarding operations performed in it.

11.2 Print



Print

Printer: Adobe PDF

Events: Event log: all events

□ Printout with monitoring status

□ Print to text file

Range:
● All
○ Pages: 279 (events: 23156)
○ Selection

Fig. 31. "Print" window.

The window allows you to define parameters of a printout containing the event log.

Printer – information on the selected printer.

Events – information on events to be printed.

Printout with reporting status – if the option is enabled, reporting status information will be included in the printout.

Print to text file – if the option is enabled, the event log will be exported to a text file.

Range – you can define a printout range:

All – all events.

Pages – defined number of event pages. The number of events is shown in parentheses.

Selection – the events selected in the "Event log" window.

Buttons

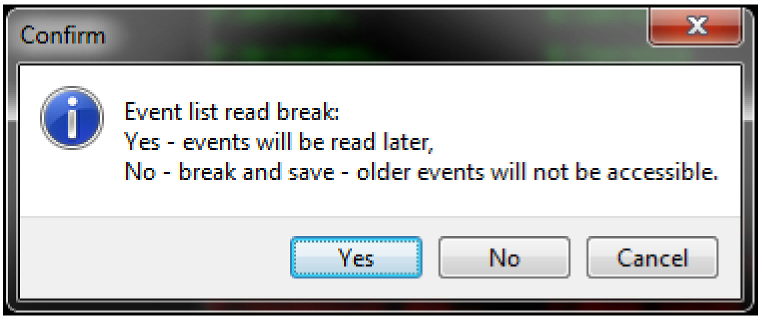
Properties – click to configure the printer.

Print – click to print / export to file the event log.

Cancel – click to close the window.

12. Stop reading events

1. Click on ✕ in the main menu.
2. The “Confirm” window will be displayed



Confirm

Event list read break:
Yes - events will be read later,
No - break and save - older events will not be accessible.

Fig. 32. “Confirm” window.

3. Click on one of the buttons:

   Yes – event reading will be stopped and events will be read later.

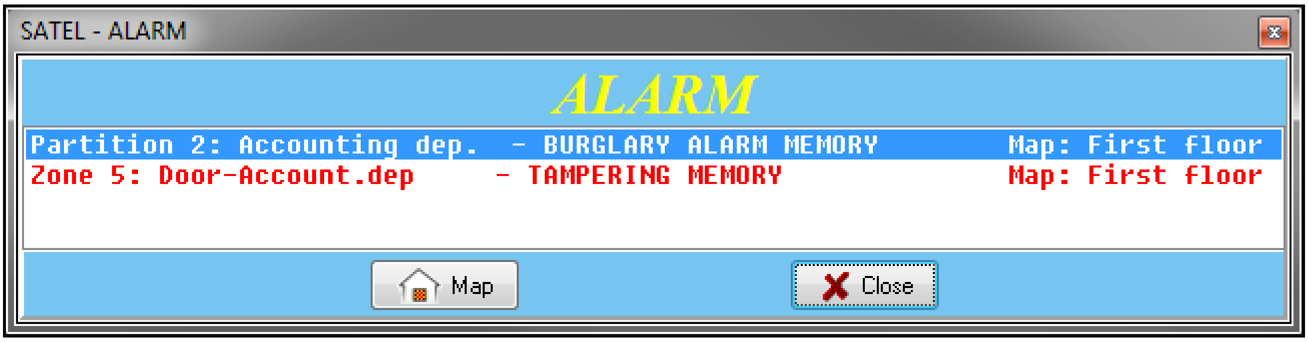
   No – event reading will be stopped and older events will not be accessible any more.

   Cancel – event reading will be continued.

13. ALARM

“ALARM” is the default window title. You can change it (see “ALARM window messages”).

The window displays information about alarms in the alarm system. The name of the alarm system is displayed in the window title. The “ALARM” window settings you can configure in the “GUARDX Service” window, “ALARM window messages” tab (see “ALARM window messages”).



SATEL - ALARM

ALARM

```
Partition 2: Accounting dep.  - BURGLARY ALARM MEMORY     Map: First floor
Zone 5: Door-Account.dep     - TAMPERING MEMORY          Map: First floor
```

Fig. 33. “ALARM” window (example).

Partition / zone – number and name of the partition / zone.

[information] – message indicating the type of alarm (burglary, fire, tamper) and whether the alarm is still active or not.

Map – name of the map on which partition / zone is placed.

Buttons

Map – highlight a selected alarm on the list and click on the button to open the “Map” window (see “Map”). You can also double-click on the selected item on the list to open the window.

Close – click to close the window.

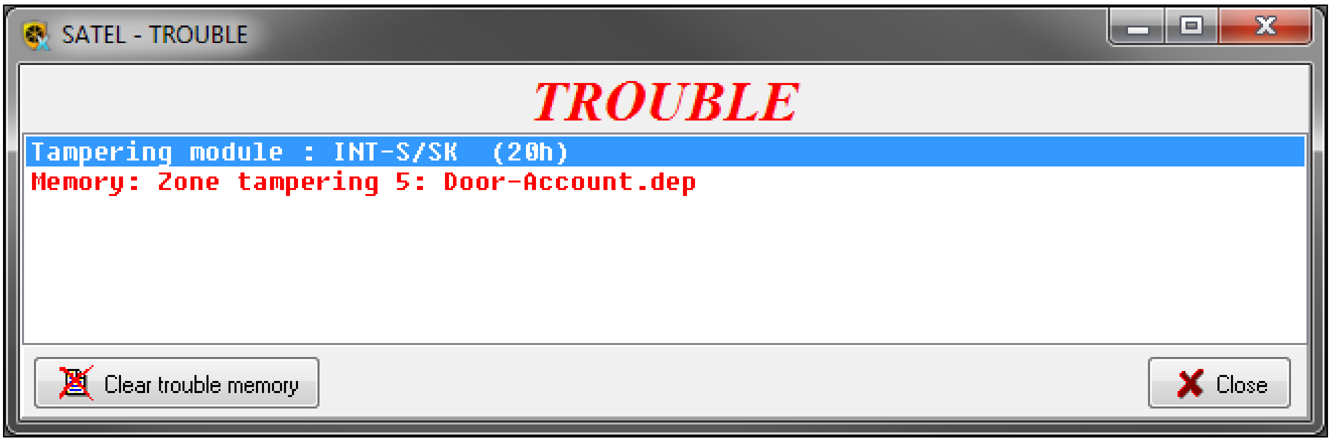
14. TROUBLE

The window shows information about troubles in the alarm system. The name of the system is displayed in the window title.

Buttons

Clear trouble memory – click to clear the trouble memory. The button is available if the “Trouble memory until review” option is enabled in the control panel.

Close – click to close the window.



```
Tampering module : INT-S/SK  (20h)
Memory: Zone tampering 5: Door-Account.dep
```

Fig. 34. “TROUBLE” window (example).

15. Icon in the tray

If the program is minimized, the program icon is displayed in the tray. The icon provides the following information:

– not flashing – no communication with the control panel,

– flashing alternately blue and yellow – the program receiving data from the control panel,

– flashing alternately red and yellow – the program receiving data from the control panel in which alarm was triggered.

Click on the icon to restore the main menu and windows of the program. Right-clock on the icon to display the additional menu (see “Additional menu”).

16. GUARDX Service

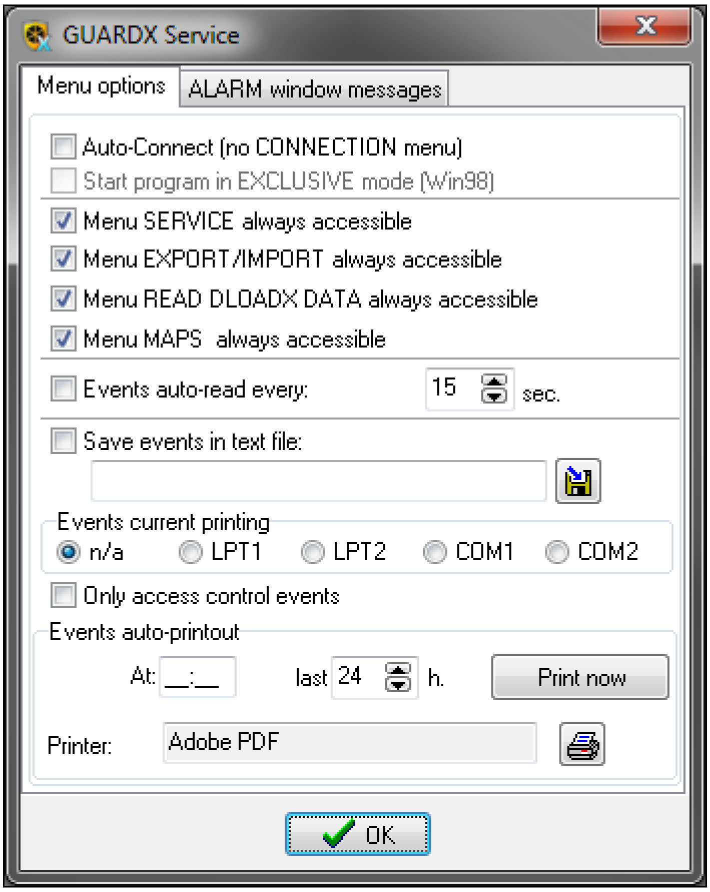
16.1 Menu options

Auto-Connect (no CONNECTION menu) – if this option is enabled, the program connects, immediately after start, to the alarm system (to the control panel it was recently connected to, or to the control panel the shortcut points to – see “Creating a shortcut to the alarm system”). The startup window is not displayed.

Menu SERVICE always accessible – if this option is enabled, the “Service” command is always shown in the configuration menu. The option is available to the installer (service technician).

Menu EXPORT/IMPORT always accessible – if this option is enabled, the “Map export” and “Map import” commands are always displayed in the configuration menu. If the option is disabled, the commands are only available to the installer (service technician).

Menu READ DLOADX DATA always accessible – if this option is enabled, the “Read DLOADX data file” command is always displayed in the configuration menu. If the option is disabled, the command is only available to the installer (service technician).



□ Auto-Connect (no CONNECTION menu)
□ Start program in EXCLUSIVE mode (Win98)
☑ Menu SERVICE always accessible
☑ Menu EXPORT/IMPORT always accessible
☑ Menu READ DLOADX DATA always accessible
☑ Menu MAPS always accessible
□ Events auto-read every: 15 sec.
□ Save events in text file:

Events current printing
● n/a ○ LPT1 ○ LPT2 ○ COM1 ○ COM2

□ Only access control events

Events auto-printout
At: __:__ last 24 h.
Printer: Adobe PDF

Fig. 35. “Menu options” tab in the “GUARDX Service” window.

Menu MAPS always accessible – if this option is enabled, the “Maps” command is always displayed in the configuration menu. If the option is disabled, the command is only available to the installer (service technician).

Events auto-read every – if this option is enabled, events (including troubles) are read from the control panel automatically at preset intervals (enter the time in the field beside).

Save events in text file – if this option is enabled, events read from the control panel are written to text file. Click 💾 to indicate location of the text file and name it.

Events current printing – if events are to be printed after reading from the control panel, select the computer port to which the printer is connected: **n/a** (real-time printing not available), **LPT1**, **LPT2**, **COM1** or **COM2**.

Only access control events – if this option is enabled, access control events only will be saved / printed.

Events auto-printout – events can be printed automatically at specified time:

At – define the time at which events are to be printed.

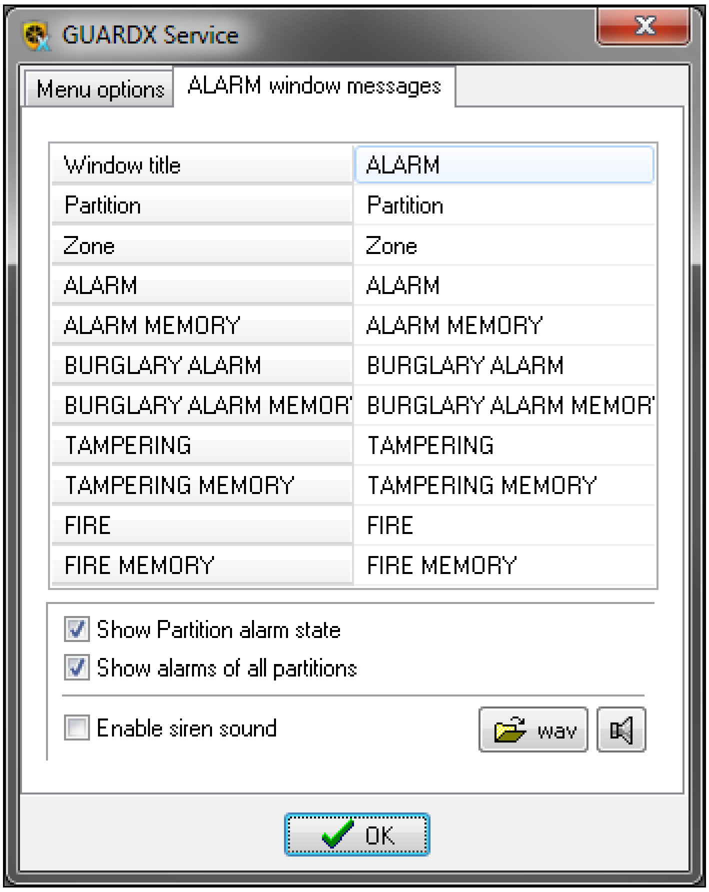
last – define events from how many last hours are to be printed.

Print now – click to print the events.

Printer – printer to be used for printing events. Click 🖨 to open window with print properties.

OK – click to confirm the changes and close the window.

16.2 ALARM window messages



Window title	ALARM
Partition	Partition
Zone	Zone
ALARM	ALARM
ALARM MEMORY	ALARM MEMORY
BURGLARY ALARM	BURGLARY ALARM
BURGLARY ALARM MEMOR'	BURGLARY ALARM MEMOR'
TAMPERING	TAMPERING
TAMPERING MEMORY	TAMPERING MEMORY
FIRE	FIRE
FIRE MEMORY	FIRE MEMORY

☑ Show Partition alarm state

☑ Show alarms of all partitions

□ Enable siren sound

Fig. 36. “ALARM window messages” tab in the “GUARDX Service” window.

In the tab, you can configure the “ALARM” window settings (see “ALARM”).

Window title – title of “ALARM” window (preceded by alarm system name).

Partition – way of partition naming in the alarm system.

Zone – way of zone naming in the alarm system.

ALARM – alarm message.

ALARM MEMORY – alarm memory message.

BURGLARY ALARM – burglary alarm message.

BURGLARY ALARM MEMORY – burglary alarm memory message.

TAMPERING – tamper alarm message.

TAMPERING MEMORY – tamper alarm memory message.

FIRE – fire alarm message.

FIRE MEMORY – fire alarm memory message.

Show Partition alarm state – if this option is enabled, the window shows alarms from partitions to which the current user has access.

Show alarms of all partitions – if this option is enabled, the window shows alarms from all partitions.

Enable siren sound – if this option is enabled, alarms are signaled acoustically.

wav – click to indicate location of the WAV file which is to be played back if an alarm is triggered.

🔈 – click to play back the sound file.

🔇 – click to end playing back the sound file.

OK – click to confirm the changes and close the window.

17. Maps

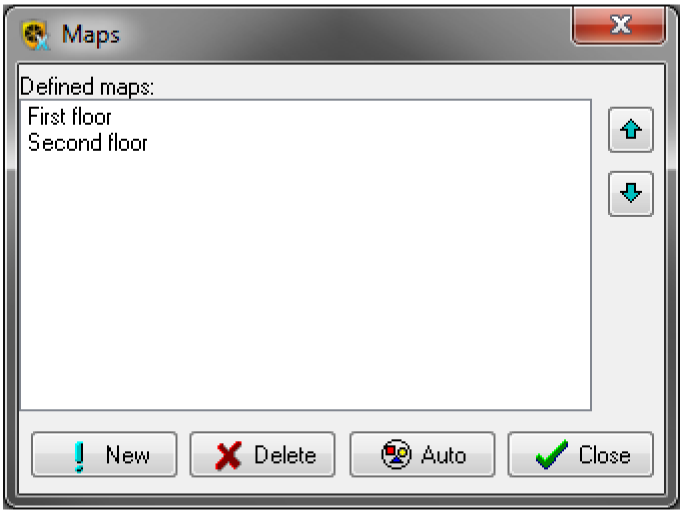


Fig. 37. “Maps” window.

Defined maps – list of maps created for the given alarm system. The order of map arrangement affects the:

- sequence in which the maps are displayed in the case of alarm on several maps (the map which is first in the sequence is displayed first),
- sequence in which the maps are displayed when you click on the 🏠 button in the main menu,
- sequence in which the maps are displayed by hovering the cursor over the “Object supervision” command in the additional menu (see “Additional menu”).

⇧ – click to move the selected map up.

⇩ – click to move the selected map down.

New – click to create a new map without objects (see “Creating a map without objects”).

Delete – click to delete the highlighted map (see “Deleting map”).

Auto – click to create a new map with objects (see “Creating a map with objects”).

Close – click to close the window.

17.1 New map

To display the “New map” window, click in the “Maps” window on “New” or “Auto”. Clicking on “New” will only display the “Name” field and the “OK” and “Cancel” buttons.

Name – name of the new map.

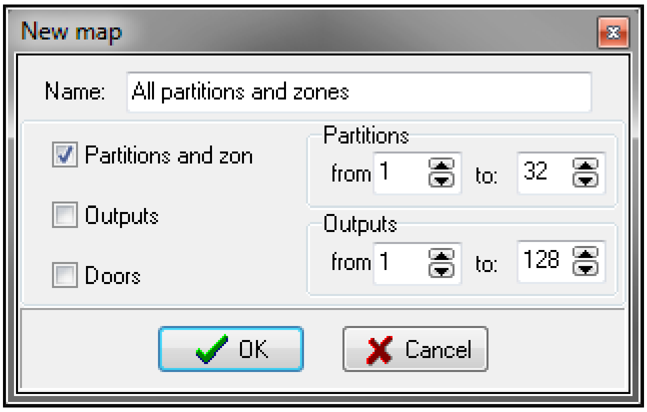
Partitions and zones – if this option is enabled, partitions and zones will be automatically placed on the map. Define in the “from” and “to” fields which partitions are to be placed on the map (zones belonging to these partitions will be placed on the map).

Outputs – if this option is enabled, outputs will be automatically placed on the map. Define in the “from” and “to” fields which outputs are to be placed on the map.

Doors – if this option is enabled, all doors supervised by the access control devices in the alarm system will be automatically placed on the map.

OK – click to create a map.

Cancel – click to cancel creating the map.



New map

Name: All partitions and zones

☑ Partitions and zon

□ Outputs

□ Doors

Partitions: from 1 to: 32

Outputs: from 1 to: 128

Fig. 38. “New map” window displayed by clicking on the “Auto” button.

17.2 Managing maps

The procedures described below apply to working with the program connected to the control panel. If the program is not connected to the control panel, the authorization window will not be displayed.

17.2.1 Creating a new map

1. Click on the SATEL logo in the main menu or right-click on the program icon in the tray.
2. The additional menu will be displayed.
3. Hover the cursor over the “Configuration” menu to display the configuration menu.
4. Click “Maps”.

17.2.1.1 Creating a map without objects

1. Click “New”.
2. The “New map” window will be displayed.
3. Enter the name of the map in the “Name” field.
4. Click “OK”.
5. The authorization window will be displayed.
6. Enter the control panel access code and click “OK”.
7. The “Map” window will be displayed in the edit mode (see “Editing the map”).

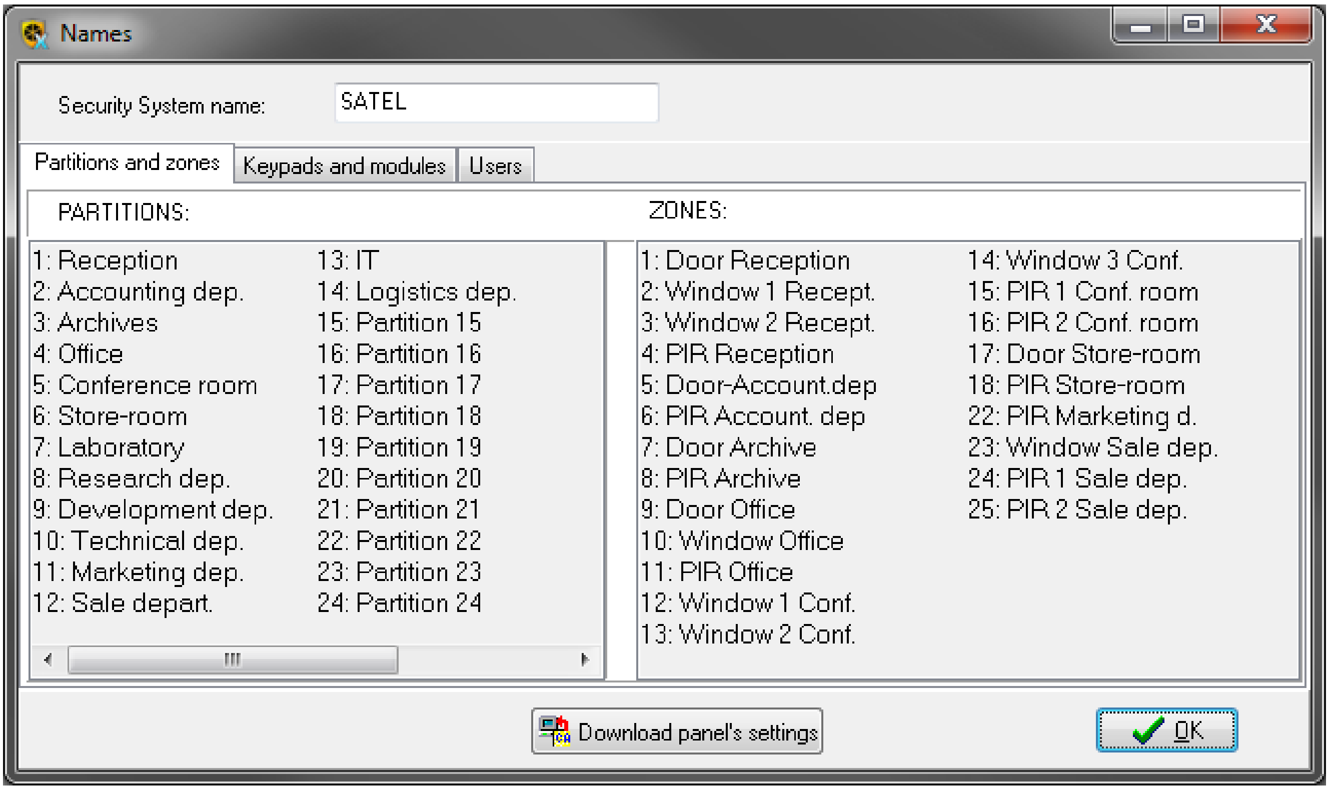
17.2.1.2 Creating a map with objects

1. Click “Auto”.
2. The “New map” window will be displayed.
3. Enter the name of the map in the “Name” field.
4. Define which objects are to be placed on the map (see “New map”).
5. Click “OK”.
6. The authorization window will be displayed.
7. Enter the control panel access code and click “OK”.
8. The “Map” window will be displayed, showing the pre-selected objects.

17.2.2 Deleting map

1. Click on the SATEL logo in the main menu or right-click on the program icon in the tray.
2. The additional menu will be displayed.
3. Hover the cursor over the “Configuration” menu to display the configuration menu.
4. Click “Maps”.
5. Click on the map you want to delete.
6. Click “Delete”.
7. The authorization window will be displayed.
8. Enter the control panel access code and click “OK”.
9. The map will be removed from the list.

18. Names



Security System name: SATEL

PARTITIONS:

1: Reception
2: Accounting dep.
3: Archives
4: Office
5: Conference room
6: Store-room
7: Laboratory
8: Research dep.
9: Development dep.
10: Technical dep.
11: Marketing dep.
12: Sale depart.
13: IT
14: Logistics dep.
15: Partition 15
16: Partition 16
17: Partition 17
18: Partition 18
19: Partition 19
20: Partition 20
21: Partition 21
22: Partition 22
23: Partition 23
24: Partition 24

ZONES:

1: Door Reception
2: Window 1 Recept.
3: Window 2 Recept.
4: PIR Reception
5: Door-Account.dep
6: PIR Account. dep
7: Door Archive
8: PIR Archive
9: Door Office
10: Window Office
11: PIR Office
12: Window 1 Conf.
13: Window 2 Conf.
14: Window 3 Conf.
15: PIR 1 Conf. room
16: PIR 2 Conf. room
17: Door Store-room
18: PIR Store-room
22: PIR Marketing d.
23: Window Sale dep.
24: PIR 1 Sale dep.
25: PIR 2 Sale dep.

Fig. 39. “Names” window.

Security System name – name given to the alarm system in the GUARDX program.

Partitions and zones – the tab displays the names of alarm system partitions and zones.

Keypads and modules – the tab displays the names of devices connected to the control panel communication buses.

Users – the tab displays the names of administrators and users.

Download panel’s settings – click to read data from the control panel.

OK – click to close the window.

19. Reading DLOADX data file

You can read the alarm system information from the file exported from the DLOADX program.

1. Click on the SATEL logo in the main menu or right-click on the program icon in the tray.
2. The additional menu will be displayed.
3. Hover the cursor over the “Configuration” menu to display the configuration menu.
4. Click “Read DLOADX data file”.
5. In the window that will open, indicate location of the file exported from the DLOADX program.
6. If the file is encrypted, a window will be displayed in which you can enter the data encryption key.
7. The program will inform you that the alarm system data have been read.

20. Information about the updates

To open the window with information about available updates, click on the “Check for update” command in the additional menu (see “Additional menu”).

Check for update automatically – if this option is enabled, the program will automatically check for and inform you about available updates.

Download – click to visit the www.satel.eu website and download the latest version of the program. The button is displayed when a newer version of the program is available.

OK – click to close the window.

21. Information about alarms

If an alarm occurs in the alarm system:

- the “ALARM” window will be displayed (see “ALARM”), possibly accompanied by a sound signal (see “ALARM window messages”),
- if the element which triggered the alarm (partition, zone) is placed on the map, the “Map” window will be displayed (see “Map”).

22. Creating a shortcut to the alarm system

You can create a shortcut to the alarm system if:

- the settings required to establish connection with the alarm system are configured (see “Adding a new alarm system”),
- the “Auto-Connect (no CONNECTION menu)” option is enabled (see “Menu options”).

1. Create a shortcut to the GUARDX program (e.g. on the desktop).
2. Click the right mouse button on the shortcut.
3. Click “Properties” in the context menu.
4. In the “Properties” window, “Shortcut” tab, “Target” field, after the GUARDX program access path (e.g. "C:\Program Files (x86)\Satel\GUARDX\GuardX.exe"), enter in turn:
   - space
   - communication method – if the COM port is to be used, do not use quotation marks (e.g. for COM5 port, enter com5); for another method of communication, use quotation marks (e.g. "TCP/IP: GUARDX->ETHM")
   - space
   - alarm system name – if the name contains no space, do not use quotation marks (e.g. Company); if the name contains a space, use quotation marks (e.g. "Building company")

- – space
- – PASS:
- – code for access to the control panel

If the code is not to be entered automatically, skip the last three elements, i.e. space, PASS: and code. The person launching the program by using a shortcut will have to enter the code for access to the control panel.

Example 1:

"C:\Program Files (x86)\Satel\GUARDX\GuardX.exe" com5 Company PASS:12345 [the program is to connect via the COM5 port to the “Company” system; the 12345 code will be used]

Example 2:

"C:\Program Files (x86)\Satel\GUARDX\GuardX.exe" "TCP/IP: GUARDX->ETHM" "Building company" PASS:1111 [the program is to connect via ETHM-1 Plus / ETHM-1 module to “Building company” system; the 1111]

Example 3:

"C:\Program Files (x86)\Satel\GUARDX\GuardX.exe" "TCP/IP: SATEL server" Company [the program is to connect via SATEL server with “Company” system; entering the control panel access code will be required]

5. Click “OK”.

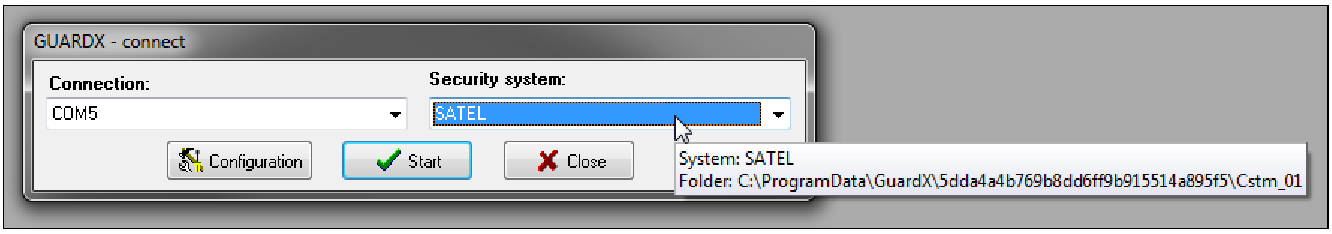
If you make a mistake when entering additional parameters of the shortcut, these parameters will be disregarded when launching the program.

23. Alarm system data

The data downloaded from the control panel are saved to files on the computer hard disk.

23.1 Checking data location

1. In the startup window, “Security system” field, select the alarm system.
2. Hover the cursor over the name.
3. Access path to the selected alarm system data will be displayed.

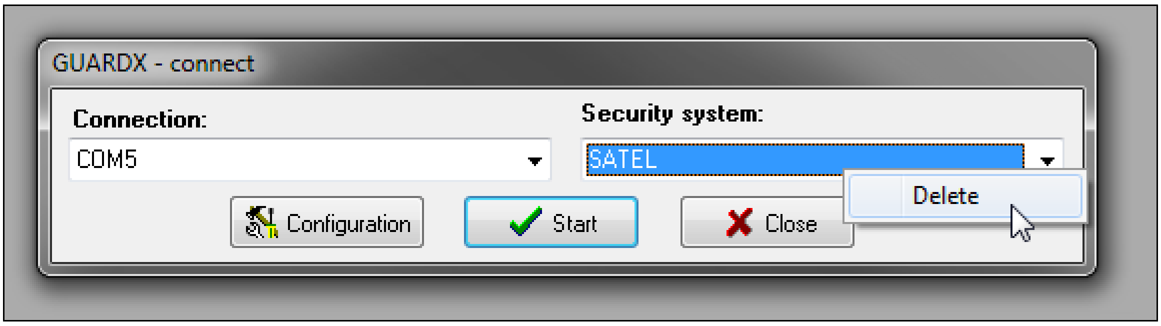


System: SATEL
Folder: C:\ProgramData\GuardX\5dda4a4b769b8dd6ff9b915514a895f5\Cstm_01

Fig. 40. Access path to alarm system data (example).

23.2 Deleting data

1. In the startup window, “Security system” field, select the alarm system.
2. Right-click on the alarm system name.
3. When the “Delete” command appears, click on it.
4. When the “Confirm” window will be displayed, click “Yes”.



GUARDX - connect

Connection: COM5

Security system: SATEL

Fig. 41. Deleting the alarm system data (example).