

Security Center 5

USER MANUAL

C.Nord

August 7, 2018

Contents

1	What's New	7
1.1	Disabling of Sites, Communication Channels and Events	7
1.2	Site Reclosing	7
1.3	Tooltip	7
1.4	Video confirmations	8
1.5	Cloud Services	8
1.5.1	Remote Programming Interface	8
1.5.2	Mobile Application “MyAlarm”	8
1.5.3	Site Access Control from “MyAlarm” Application	9
1.5.4	Operator Permissions during Alarm Handling	9
2	Introduction	9
2.1	Hardware Requirements for System	10
2.2	Operating System Requirements	10
2.3	Electronic Security Key	10
2.4	Scope of Delivery	10
3	Installation	11
3.1	Selection of Operating System	11
3.2	Configuration of Computer Disk Subsystem	11
3.3	Additional Requirements	11
3.4	Installer	12
3.4.1	Full installation	14
3.4.2	Installation on network workstation	16
3.5	Security Center Removal	16
3.6	Installation Problems	16
4	Getting Started	18
4.1	Security Center Variants	18
4.2	Purpose of Modules	18
4.3	First Start	19
4.4	Admin Password	19
4.5	Data Import	20

5	Event Manager	20
5.1	Module Settings	21
5.1.1	Common	21
5.1.2	Backup	21
5.2	Event Sources	23
5.2.1	Common Event Source Settings	24
5.2.2	Event Source from PimaGuard and Sentinel	25
5.2.3	Event Source via TCP/IP	26
5.2.4	GSM Events Source	27
5.2.5	Sur-Gard events source	28
5.2.6	LONTA-202 Events Source	29
5.2.7	RS-200 Events Source	29
5.2.8	RC 4000 Events Source	30
5.2.9	Multiprotocol Event Source	30
5.3	Event Handlers	31
5.3.1	Common Settings for Event Handler Groups	33
5.3.2	Common Event Handler Settings	34
5.3.3	Event Monitoring	36
5.3.4	Event Chain Monitoring	38
5.3.5	Alarm Entering	40
5.3.6	SMS Message Repeater	41
5.3.7	Site Reclosing	48
5.3.8	Pandora Network	49
5.3.9	Repeater to Cloud	54
5.4	Connection to the Cloud	56
5.4.1	Connection mode	56
5.4.2	Contact information	57
5.4.3	UID of Security Center	58
5.5	About software	58
6	Site Manager	59
6.1	Control Panel	60
6.2	List of Sites	61
6.2.1	Selection of Displayed Columns	61
6.2.2	Sorting of Sites	61
6.2.3	Filtering of Sites during Display	62
6.3	Restoring of Deleted Site	62
6.4	Site	64
6.4.1	Site location on map	64

6.4.2	Site Map	65
6.4.3	Web Link	66
6.4.4	Images of Site	66
6.5	Parts	67
6.6	Zones	68
6.7	Responsible Persons	69
6.8	Arm	70
6.8.1	Long-term arm	70
6.8.2	Site Disabling	71
6.8.3	Arming/Disarming by Duty Operator	71
6.9	Control Time	71
6.10	Arm Schedule	73
6.11	Event Template	75
6.12	Additional Characteristics	77
6.13	Event Handlers	77
6.14	Equipment	78
6.14.1	“Other”	78
6.14.2	“C-Nord GSM (CML)”	78
6.14.3	“Lonta-202”	79
6.14.4	“RS200”	79
6.15	Comment	79
6.16	Videorouters	80
6.17	Service	80
7	System Setup	81
7.1	Event Classes	81
7.2	Event Templates	83
7.2.1	Replacing Event Template	84
7.3	Actions	87
7.4	Alarm Cancellations	88
7.5	Site Types	89
7.6	Site fields	90
8	Personnel Manager	90
8.1	Operators	91
8.1.1	Operator’s Rights in “Event Manager” Module	92
8.1.2	Operator’s Rights in “Duty Operator” Module	92
8.1.3	Operator’s Rights in “Site Manager” Module	93
8.1.4	Operator’s Rights in “Report Manager” Module	94

8.1.5	Operator's Rights in "Site Maps" Module	95
8.1.6	Operator's Rights in "System Setup" Module	96
8.1.7	Operator's Rights in "Nord-LAN Key Configurator" Module	97
8.1.8	Operator's Rights in "Personnel Manager" Module	97
8.2	guards	98
8.3	Computers	99
8.3.1	Allow to run Security Center modules on computers from list only	99
8.3.2	Sites specified for computer	99
8.4	Engineers {# personnel-manager-engineer}	100
9	Site Maps	101
10	Duty Operator	101
10.1	Module Main Window	102
10.2	Quick Access Toolbar	102
10.3	Sites	103
10.3.1	Tooltip {# duty-opertor-tooltip}	104
10.3.2	Site Status	104
10.3.3	Alarm	104
10.3.4	Guards	105
10.3.5	Context Menu	105
10.4	Events	109
10.4.1	All	110
10.4.2	Alarms	111
10.4.3	Events at the Site	111
10.4.4	Status of guards	113
10.5	Alarm handling	113
10.5.1	Call a Guard to the Site	114
10.5.2	Operator's comment	115
10.5.3	Alarm Cancellation	115
10.6	Site Card	116
10.7	Information about Alarms	117
10.8	Module Setup	117
10.8.1	Common	118
10.8.2	Alarm Handling	119
10.8.3	Hot Keys	119
10.8.4	Dialing	120
10.8.5	Security Center - Persona	120

11 Report Manager	121
11.1 Event Reports	121
11.1.1 Events from Undescribed Sites	121
11.1.2 Sites without Events	121
11.1.3 Time Deviation	122
11.1.4 Statistics by Class	122
11.1.5 Sent SMS	122
11.1.6 Statistics by Channels	122
11.1.7 Statistics by Status	122
11.2 Alarm Reports	123
11.2.1 Standard Report and Report by Operator	123
11.2.2 Statistics by Alarm Cancellations	123
11.2.3 Alarms and Events	124
11.3 Reports by Arm Time	124
11.3.1 Arm Time	124
11.3.2 Arm Status	124
11.4 Reports by guards	124
11.4.1 Guard Performance	125
11.4.2 Statistics of Responses	125
11.4.3 Average Number of Calls	125
11.4.4 Response Time	125
11.4.5 Statistics by Cancellations	125
11.5 Site Reports	125
11.5.1 Sites	125
11.5.2 Operators	125
11.5.3 Event Templates	126
11.5.4 Event Handlers	126
12 Database Wizard	126
12.1 Database Check	126
12.2 Backup	127
12.3 Restoring from Backup	128
12.4 Data Import	129
12.4.1 Import from XML File	129
12.5 Data Export	130
12.6 Command Line Options	131
12.6.1 Database Backup	131
12.6.2 Restoring Database from Backup	132
12.6.3 Example of Using Command Line Parameters	132

13 Cloud Services	133
13.1 Engineering Panel	133
14 Technical Support	135

1 What's New

Version 5 of Security Center software has a number of novelties that allow the security company not only to increase the list of services provided to clients, but also to optimize the work of the operator and engineering services.

1.1 Disabling of Sites, Communication Channels and Events

During maintenance or repair of equipment installed on the site, it is convenient to use operation of temporary disabling of the site. After specifying the time and reason for disabling, the duty operator can disable Security Center site so as not to be distracted by receiving and handling messages received from the site. After the expiration of the specified period, the site is turned on automatically, however, the operator can enable the site earlier.

For the period of maintenance or repair of equipment used to provide communication channels with the site, it is possible to disable the communication channels. After specifying the time and reason for disabling, the duty operator can disable one or several site communication channels so as not to be distracted by receiving and handling messages passing through them. Disabling of one or another communication channel do not hinder reception of messages through other site communication channels. After the expiration of the disabling period, the communication channels are turned on automatically, however, the operator can enable the communication channels earlier.

If deliberately false alarms of fire alarm systems occur on the site (due to equipment malfunction, technical vulnerability of the site, movement of animals, etc.), it is possible to use the operation of event temporary disabling. After specifying the time and reason for disabling, the duty operator can disable the site event so as not to be distracted by handling the alarm. After the expiration of the disabling period, the event is turned on automatically, however, the operator can enable the event earlier.

See details on how to disconnect a site, communication channel or event, in the chapter on the “Duty operator” module.

1.2 Site Reclosing

When handling an alarm message received from a site, it may be necessary to reclose the site: to open, inspect and activate security system again after the alarm cause was eliminated. Security Center software provides an opportunity to automatically notify the persons responsible for the site about the need to reclose the sites, as well as about the refusal of the responsible person to reclose.

The responsible person is notified of the need to reclose the site, as well as the refusal of the responsible person to reclose with SMS messages. It is possible to inform the responsible person of this and other situations in the “Site manager” module on [“Responsible Persons”] tab (#site-manager-doorkeys).

The Security Center operator can notify the responsible person about the site reclosing using “Alarm to Guard” application.

In order for the Security Center operator to notify the responsible persons of the site reclosing, such types of actions as “Reclosing request” and “Reclosing failure” shall be allowed. The necessary settings can be set in the “System Settings” module on the “Actions” tab (#system-setup-actions).

Informing the responsible person about the site reclosing is performed with the help of the event handler “Site reclosing”. This handler generates the text of messages corresponding to the type of action in the given format and sends SMS to the responsible persons. See information about the handler settings in the chapter devoted to the [“Event manager”] module (#event-manager-reclosig).

1.3 Tooltip

The “Duty operator” module provides [tooltip](#), which appears when hovering over the site. With the help of the tooltip, the Security Center operator can quickly obtain the required information about the site, namely: number, name and address of the site, state of the site or its sections (under protection or removed from protection), and information about the first and last alarm in case of alarm condition on the site.

1.4 Video confirmations

To reduce the likelihood of response to a false alarm, as well as to coordinate the actions of guards at the site, the operator can view live video from the cameras at the site during alarm handling. To do this, a *video router* shall be installed on the site. It is a special device that can broadcast video from the connected cameras to the Security Center software.

See information on how to add a video router installed on the site to the site card in the chapter on the description of the [“Site Manager”] module (`#site-manager-videorouter`) for information on how to add a video router installed on the site to the site card.

In the chapter about the [“Duty operator”] module (`#duty-opertor-process-alarm`), it is also said about how the operator can view live video from the site during alarm handling.

1.5 Cloud Services

Some new features of the Security Center software of version 5 are implemented as cloud services: “Remote programming interface”, Mobile Application “MyAlarm”, etc. A brief description of the features of these services is given below, and more details about working with them can be found in the chapter “[Cloud Services](#)”.

1.5.1 Remote Programming Interface

“Remote programming interface” service is intended for remote control of equipment installed on the site.

To ensure remote access at the site, the control panel by C.Nord or PIMA Electronic Systems Ltd. shall be installed, and the GSM transmitter “TR-100 GSM III” shall be used as the communicator.

To gain access to the “Remote programming interface” service, it is necessary to [register](#) the engineer in the “Cloud”, and also give him access to the [site management](#).

1.5.2 Mobile Application “MyAlarm”

“MyAlarm” application are intended for clients of private security companies. With its help, it is possible to access the site card, information about its status, and also the list of responsible persons.

The application shall be installed on a mobile device (smartphone or tablet). Android or iOS can be used as the operating system of the mobile device.

The key feature of the “MyAlarm” application is the ability to take the site under protection or to remove the site from protection directly from the application. For this purpose, the control panel by C.Nord or PIMA Electronic Systems Ltd. shall be installed, and the GSM transmitter “TR-100 GSM III” shall be used as the communicator. The application user shall enter the user code that he/she enters on the control panel keypad, this code is translated to the control panel, after that the event of taking or removing is transferred to the “MyAlarm” application. Due to the fact that the events in the “MyAlarm” application are transmitted from the Security Center, after the taking under protection it is not necessary to monitor the signal passage to a private security company.

Ability to view the event log for the site is an important feature of the “MyAlarm” application. Besides, the event log of the “MyAlarm” application displays the actions that the Security Center operator makes during alarm handling.

The Security Center operator can [specify](#) what events and operator actions will be displayed in the event log of the “MyAlarm” application.

It shall be noted that if a video router is installed on the site, in addition to video confirmations in the event log, it is possible to view live video from cameras installed on the site in the “MyAlarm” application. The video stream quality depends on the communication channel bandwidth, which is used for Internet access from the mobile device.

It is necessary to specify the same login and password, which are used to access the “Personal account” services, for authorization in the “MyAlarm” application.

1.5.3 Site Access Control from “MyAlarm” Application

Version 5.3 of the Security Center had only one way to give the responsible person access to the site from the “MyAlarm” application - to assign the responsible person as the administrator of the personal account.

In version 5.4 of the Security Center, a new opportunity appeared: to give access to the responsible persons specified in site card. More information on how to do this can be found in a [separate article](#).

1.5.4 Operator Permissions during Alarm Handling

In version 5.2.855, new operator permissions related to alarm handling in the “Duty Operator” module have been added.

Suppose that the duty operators on the receiver are divided into two groups.

The task of the first group is to make a decision about whether the response requires a response (Guard call) or not. These operators shall be able to start the alarm handling immediately, once it is received. They monitor events from the site, call up the responsible persons, etc. And at some point they decide to cancel the alarm or to react. If it is decided to react, the operator registers the alarm confirmation.

Once the alarm is confirmed, operators from the second group, which task is the response, start their work. They “do not see” those alarms that are not confirmed: the event does not appear in the “Alarms” list, there is no alarm sound, the site does not become alarm. All this happens only at the moment when the alarm is confirmed: the alarm becomes “real”, the reacting operators see it as if it has been just received and begin to react.

Confirm alarms In order for the operator from the first group to confirm the alarm and transmit it to the operators of the second group, he/she shall have the permission “Confirm alarms”.

Manage Guard If the operator has the permission to “Manage Guard”, then he/she has the opportunity to register actions with the type of “Guard Call”, “Guard Arrival” and “Cancel Guard Call”.

If operators from the first group do not really control Guard, then they shall not have this permission. If the operator does not have a permission to manage Guard, then the Guard control actions do not appear in the list of possible actions for the alarm.

The operators of the second group, on the contrary, shall have such permission.

Since this is a new permission, when upgrading to version 5.2.855, all operators of the Security Center who had permission to process alarms will receive it.

Process only confirmed alarms / Cancel only confirmed alarms These are permissions for the operators from the second group. If the operator has permissions only for handling of confirmed alarms, he/she will “see” the alarm only after it has been confirmed.

2 Introduction

Security Center software was developed by the scientific and technical company C.Nord for operation in the complex system of notification transmission “Andromeda”. Security Center software is intended for operating systems Microsoft Windows 7 / 10. It is recommended to run Security Center software on operating system Microsoft Windows Server 2008 / 2012.

It is necessary to note the following features of Security Center software:

- Security Center software consists of independent functional parts (modules), each of which is intended to solve a specific problem. On the one hand, it allows to maximally protect each module against a possible failure of the other, and on the other hand, it allows to install each module on a separate computer in the network.
- Security Center software is oriented for operation on a network that supports TCP/IP protocol. Thus, the changes made to the system on any computer on the network are immediately applied to all the software modules running on that network.

- Operator's rights in Security Center software are defined in relation to a specific action in a specific software module. Thus, operators' access levels are implemented both to the program as a whole, and to its individual components. For example, it is possible to restrict operator's access to both the entire "Site manager" module, and only to the editing function of the site arm schedule.

Receiving equipment of the central station allows receiving and handling events from control panels (concentrators, site units) with built-in communicators (digital message transmission units - specialized modems). Depending on the type of control panel, its functional and service capabilities, it is possible to obtain from it some information about the site state. Most of control panels can transmit a wide range of information. For example, data about the user who performed arming or disarming; place (zone number) of alarm or malfunction (break, short circuit); partial arming with indication of unguarded zones and much more. Due to this, the duty operator has the most complete information on the site status (armed, disarmed, alarmed, etc.) and the equipment technical condition (battery is low, no 220V, telephone line is faulty, etc.).

2.1 Hardware Requirements for System

Minimum configuration: Processor Intel Core i3 2.6 GHz, RAM 2Gb, 17" SVGA monitor, sound card, USB port to install electronic security key.

Recommended configuration: Processor Intel Core i5 3.0 GHz, RAM 4Gb, 19"SVGA monitor, sound card and network card to operate software on the network, USB port to install electronic security key.

2.2 Operating System Requirements

The following operating systems are supported:

- Microsoft Windows XP / Vista / 7 / 8 / 10
- Microsoft Windows Server 2003 / 2008 / 2012 / 2016

Security Center software, version 5 is intended for operation on both 32-bit and 64-bit versions of the listed operating systems.

Before installing Security Center, it is recommended to check that the latest update package offered by Microsoft is installed on the operating system.

2.3 Electronic Security Key

Security Center software is protected from illegal copying by the electronic security key. Before using Security Center, it is necessary to connect the electronic key to USB port of the computer and install its driver.

2.4 Scope of Delivery

Security Center software is delivered in the following package:

- Compact disc containing the following:
 - Distribution package of complete version of Security Center intended for its installation on a new computer where the software was not previously installed.
 - Distribution update package of Security Center intended for updating the already installed Security Center software (or "Andromeda 2.8") to Security Center version 5.
 - Distribution package of drivers for the electronic security key.
- Electronic security key to be inserted into the computer USB port.

3 Installation

3.1 Selection of Operating System

It is recommended to run Security Center software on operating system Microsoft Windows 10.

If you intend to use Security Center software in network, it is preferable to install the server part of Security Center software (full installation) on computer with operating system Microsoft Windows Server 2016.

It is best to use NTFS as the file system.

It is strongly recommended that you update the current operating system by installing the latest service packs provided by Microsoft.

3.2 Configuration of Computer Disk Subsystem

To ensure reliable storage of information and enhance the system performance, it is recommended to install two hard disks on the computer, on which Security Center software will be fully installed. In this case, install the operating system and Security Center executable files on one hard disk and the database directory on the other. If it is impossible to install two hard disks, it is recommended to divide the single hard disk into two partitions and install the operating system on one of them, and the Security Center database on the other.

Besides, regardless of the disk subsystem configuration, you shall configure backup for Security Center software database so that the backup copy is created on an additional hard disk or network resource, which is a physically different storage device.

3.3 Additional Requirements

Before installing Security Center software, you need to make sure that the Andromeda Liberty software or the Andromeda software prior to version 2.8 is not installed on the computer. If one of these programs is detected, delete it before installing Security Center software.

To install Security Center, you need to install Microsoft Internet Explorer 8.0 or higher. It is also recommended that the system has the following components and programs:

- For operating systems Microsoft Windows XP, Microsoft Windows Server 2003 and Microsoft Windows Server 2008:
 - Windows Installer 4.5 or later
 - Microsoft .NET Framework 3.5 SP1
- Microsoft Data Access Components (MDAC) 2.8 or higher
- Microsoft .NET Framework 2.0

Before installing Security Center, you need to make sure that all hardware requirements and operating system requirements are met.

If it is planned to use Security Center with video routers by C.Nord company, then it is necessary to install the latest version of Adobe Flash Player on the computer where you want to run the module “Duty operator”, which can be uploaded from [the Adobe official website](#).

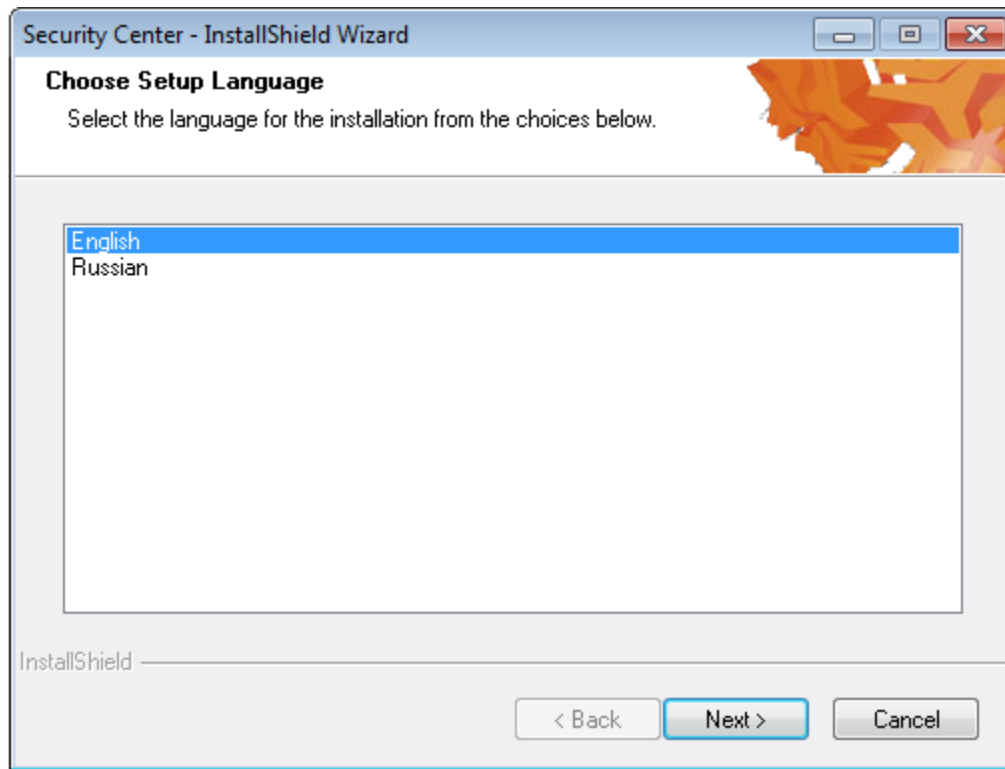


Figure 1: Selecting installer language

3.4 Installer

When installing Security Center software, you need to specify values for several installation options.

Immediately after the installer starts, you need to specify the installer user interface language.

After that, you will need to select the language of the Security Center user interface from the following list:

- English
- Russian

Be careful: Security Center user interface language cannot be changed after installation. If an error is made when selecting the user interface language, to correct it, you will need to remove the Security Center and reinstall it.

Next, the installer will prompt you to specify the directory where the executable files of the Security Center will be located.

After that, you will need to select the type of workstation on which you are installing:

- Select *Full installation* if the computer will act as a server: it will store Security Center database, and will receive events.

Select full installation if it is the only computer on which Security Center will be used.

In case of full installation, Microsoft SQL Server and Security Center database will be installed on the computer. Besides, “Event manager” module will be installed on the computer to receive and process notifications.

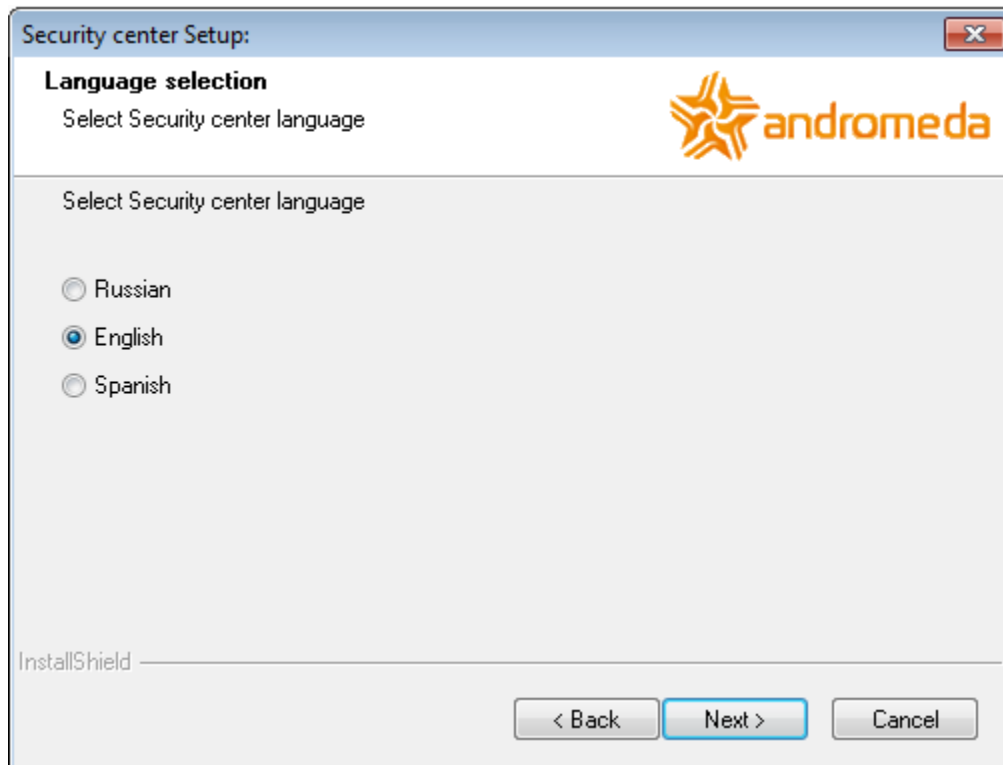


Figure 2: Selecting Security Center language

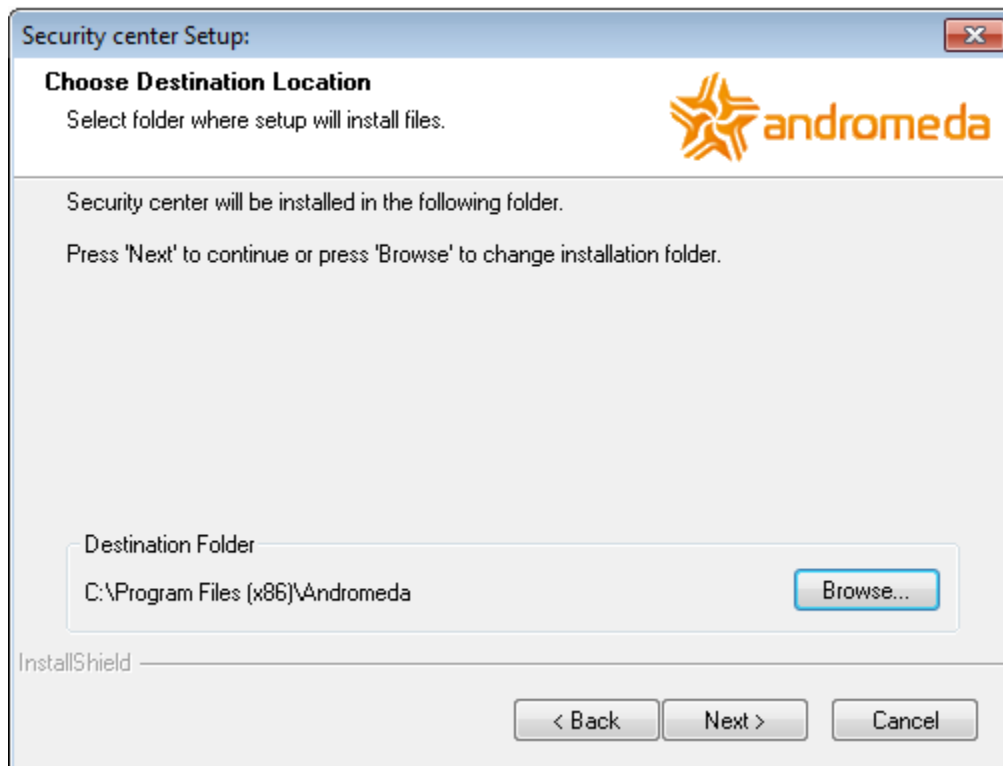


Figure 3: Selecting installation folder

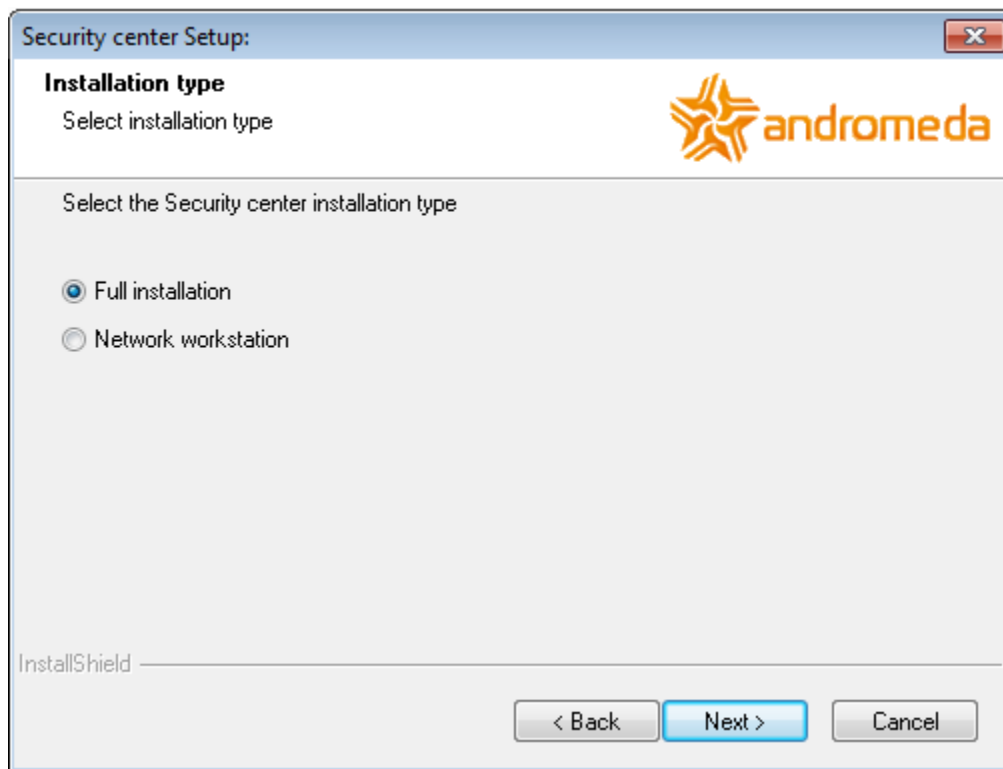


Figure 4: Selecting installation type

- Select installation on *Network workstation* if it is necessary to organize a workplace in the local computer network. Almost all program functions are available to the operator on the network workstation. An exception is a number of service operations, such as changing settings of “Event manager” module and backup management.

When installing on a network workstation, you will need to specify the computer on which the full version was previously installed.

3.4.1 Full installation

When installing the full version, you will need to specify the directory in which Security Center database will be stored.

To increase Security Center performance, it is recommended to place the database files on a separate hard disk or at least on a separate hard disk partition. By default, the installer prompts you to install the database files on a disk partition other than the system one.

You also need to specify the need of BDE setup. The BDE subsystem (“Borland Database Engine”) was used by the Andromeda 1.0 - 2.76, as well as Andromeda Liberty for the database access. BDE subsystem is used by Security Center only when importing data from the databases of the listed programs. If you do not need to import information from the databases of Andromeda 2.6 - 2.76 or Andromeda Liberty, it is not necessary to install the BDE subsystem.

In case of full installation, a named instance of Microsoft SQL Server 2005 Express Edition will appear on the computer. The instance name is “ANDROMEDA”. To perform full installation, the computer shall not have an instance of Microsoft SQL Server with the same name.

Before the installer begins installing SQL Server 2005 and copying the Security Center files to the computer, you can view its settings to make sure that all values for all parameters are set correctly.

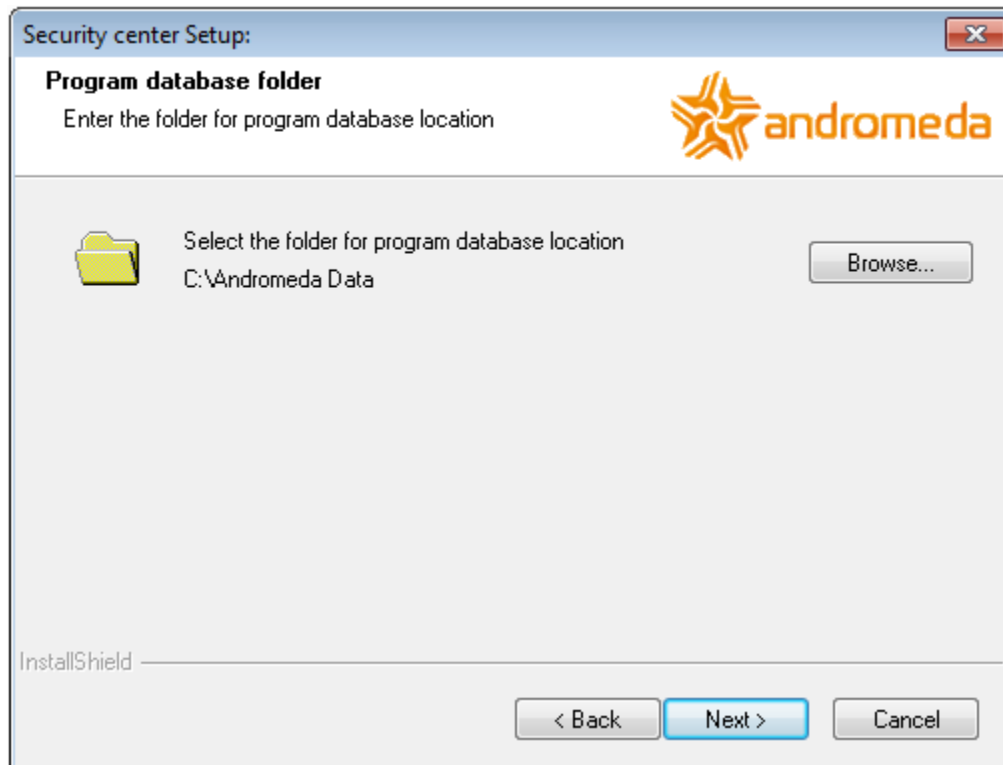


Figure 5: Full installation: selecting database installation folder

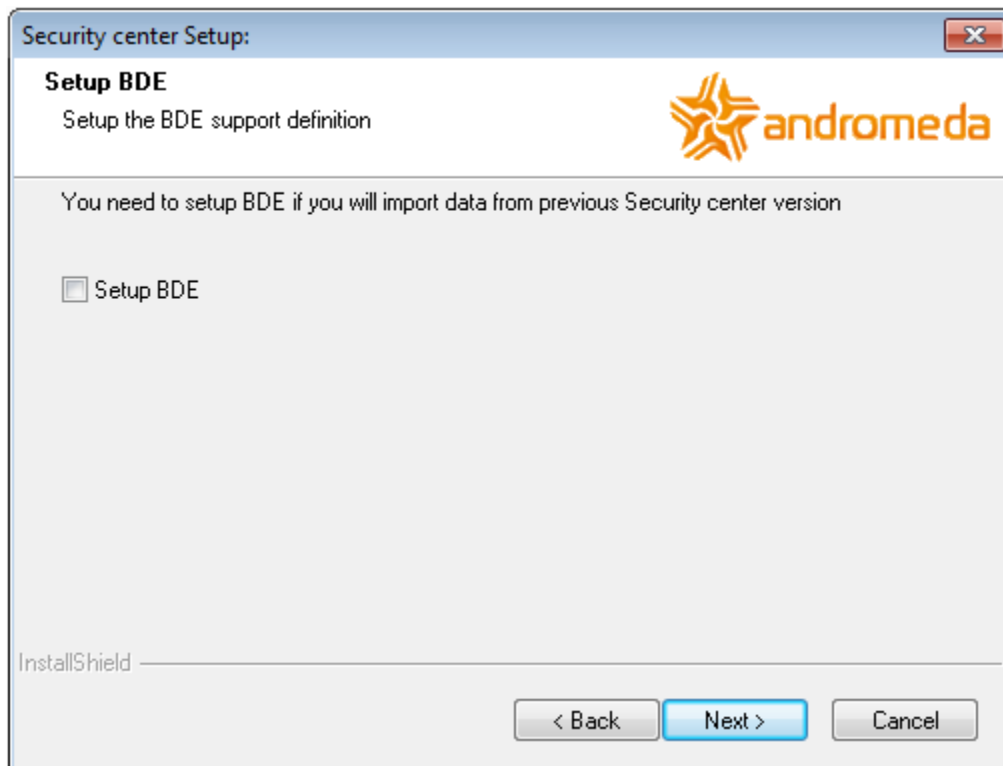


Figure 6: Full installation: selecting BDE setup

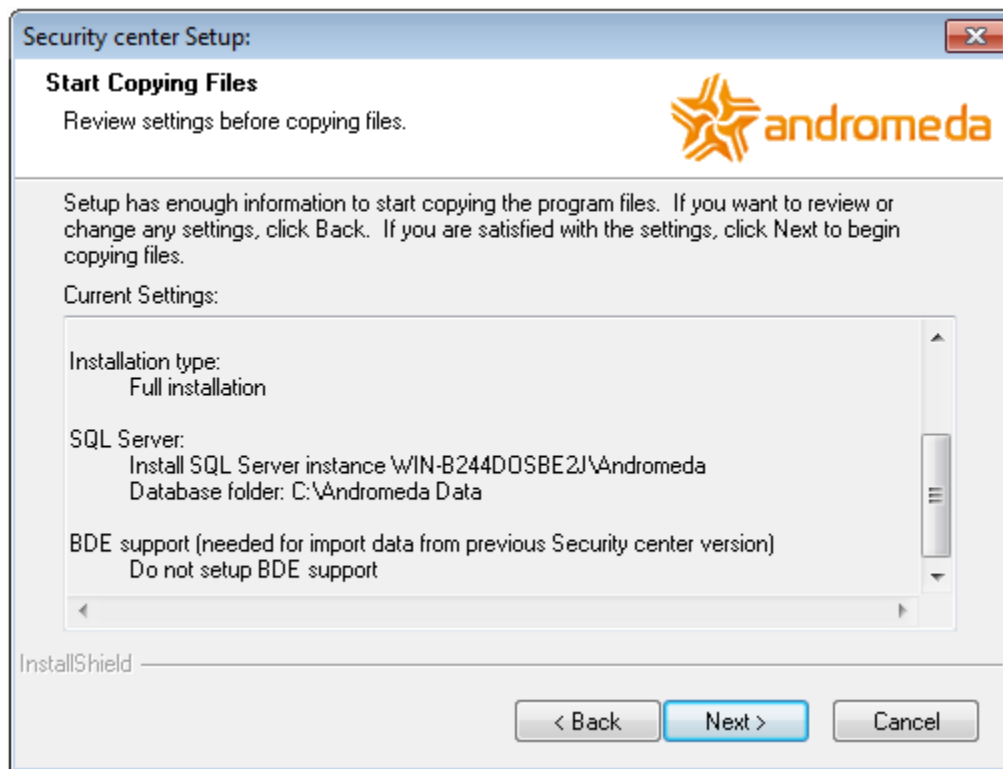


Figure 7: Full installation: list of setup program settings

3.4.2 Installation on network workstation

When installing Security Center on a network workstation, you shall specify an instance of Microsoft SQL Server that is used to store the database.

An instance of Microsoft SQL Server is installed when a full installation of Security Center is performed. The instance name is “ANDROMEDA”. Thus, you need to select a line of the form “**computer name**\ANDROMEDA” in the list, where **computer name** is the name of the computer to which the full installation of Security Center was performed.

If the installer cannot find the instance of Microsoft SQL Server in the local network that is used to store Security Center database, it is recommended to specify the computer name and instance name manually.

After this you need to enter the name or IP address of the computer on which “Event manager” module is started. In most cases, this is the same computer that is used as Security Center server.

Communication with “Event manager” module is necessary for the remaining modules of Security Center to exchange information and synchronize actions.

Before the installer begins copying the files to the computer, you can view its settings to make sure that all values for all parameters are set correctly.

3.5 Security Center Removal

To uninstall Security Center, you shall use the corresponding item in the Windows Control Panel.

3.6 Installation Problems

If there are any problems with Security Center installation, contact the technical support service of C.Nord by e-mail support@cnord.ru.

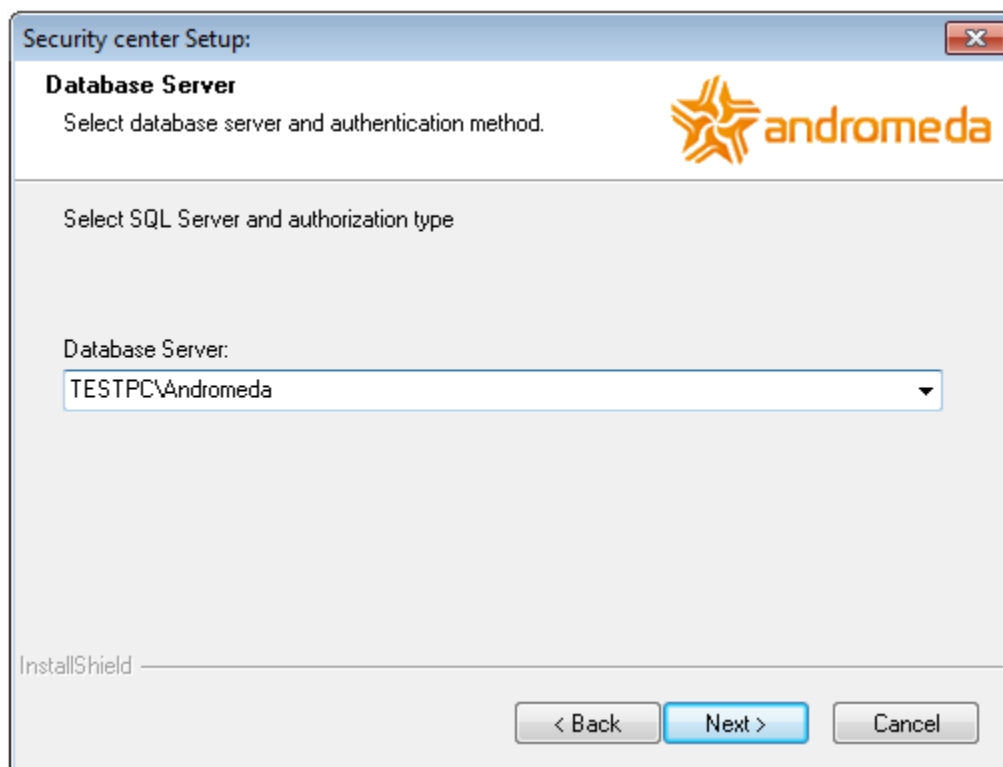


Figure 8: Installation on network workstation: selecting SQL server

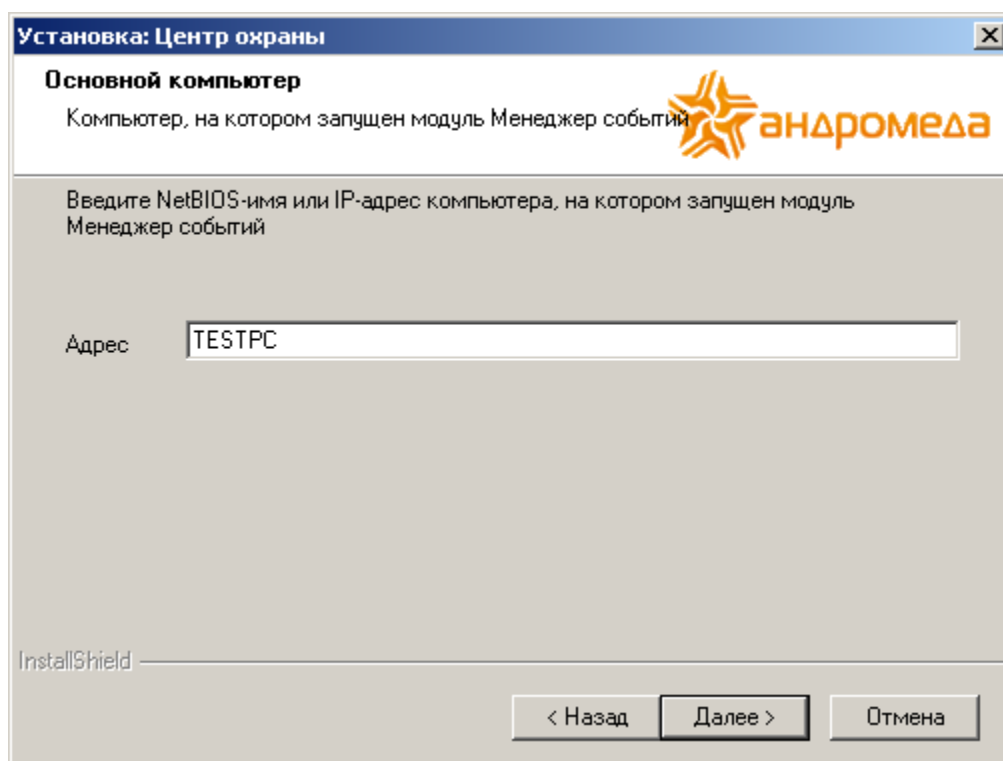


Figure 9: Installation on network workstation: selecting computer with "Event manager" module

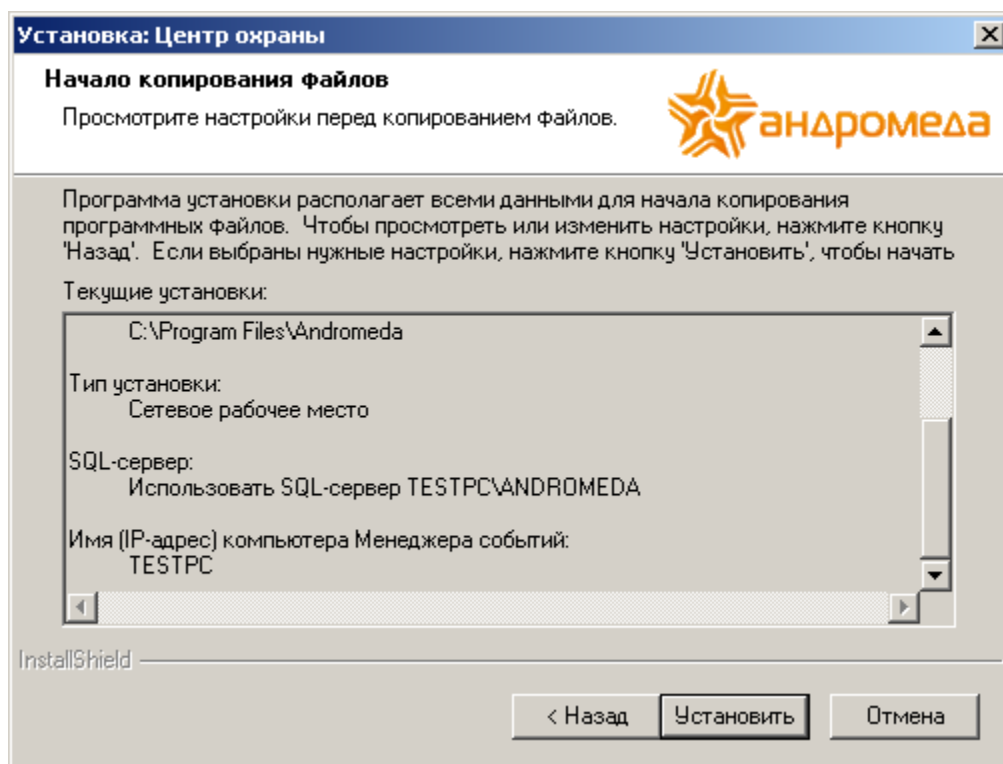


Figure 10: Installation on network workstation: list of installer settings

When contacting technical support, specify Security Center version that is being installed and describe the problem. In case of request by e-mail, it is recommended to attach the archive containing the following files:

- file C:\Andromeda.Install.log - This file contains the log of Security Center installer
- files from folder C:\Andromeda Log - The files contain the logs Security Center modules
- files from folder C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG - The files from this folder and its subfolders contain the logs of Microsoft SQL Server Setup installer

The listed files do not contain personal data or confidential information.

4 Getting Started

4.1 Security Center Variants

Variants of Security Center software differ in the maximum possible number of serviced sites: 1000, 1500, 2000, etc. There are no restrictions on the use of event sources, and the event sources from third-party centralized monitoring panels shall be purchased separately.

Starting variant of Security Center is free of charge and allows to guard up to 1000 sites.

4.2 Purpose of Modules

Security Center software consists of modules, each of which is intended to solve specific problems.

The “**Event Manager**” module is intended for receiving notifications from the receiving equipment of the central station, as well as directly from certain types of site equipment, for example, via GPRS and Ethernet communication channels.

Besides, it is in the “Event manager” module where events are automatically handled: event chains are monitored, SMS messages are sent and events are transmitted to other systems. It shall be noted that the “Event Manager” is the link for all other modules of Security Center: it shall be launched first, because it is with its help that the modules exchange information about new events, operators’ actions and other changes that occurred during the module operation.

The “**Site Manager**” module is used for creation of new sites and changing description of the existing sites.

The “**Duty Operator**” module is used by the operator to handle events. The main functions of the module are monitoring of the site operative state, viewing the latest received events, recording the operator’s actions for handling of the alarm received from sites.

The “**Site Maps**” module is intended for creation of schemes of access to the site, floor plans and location of the protection coverages. Besides, the “Site Maps” module is used to display the site alarm zones on the floor plan during alarm handling.

The list of operators of Security Center, as well as their rights in each of the modules are set in the “**Personnel Manager**”. In the same module, it is possible to change the list of guards, as well as the list of computers on the local network on which the network workstations of Security Center are operated.

The “**Database wizard**” module is intended for the following operations:

- database check and error recovery
- database backup
- database restoration from a backup
- import of data from “Andromeda” software database, “Andromeda Liberty” software, “Strazh” software and “CSM32” software
- export of data from Security Center database for use in other programs

In the **System Setup** module, it is possible to change the directories that are used to describe the sites: list of event templates, event classes and associated actions, site types and list of additional characteristics.

4.3 First Start

To get started, it is necessary to start the “Event manager” module and configure the event sources - special module components, intended to receive events from the central station equipment.

The event sources are configured in the “Event sources” window. To access it, select “Event sources ...” item in the “Event manager” module (right-click on the icon in the system tray of the taskbar).

If Security Center is installed just to get acquainted, then to create events from sites it is possible to use the “Emulation of events ...” item in the “Event Manager” menu.

After the “Event manager” module is started, it is possible to start working with other modules. Sites are entered into the system with the help of the “Site manager” module, and the received events are monitored and alarms are handled with the help of the “Duty operator” module.

4.4 Admin Password

Immediately after installation of the Security Center software, only one operator is present in the list of operators: “Administrator”. The password of the “Administrator” operator by default is **222222**.

4.5 Data Import

The Security Center software implements the function of importing information about sites from databases of the following programs:

- «Andromeda» versions 2.0 — 2.76
- «Tsentravr»
- «PCN6»
- «GuardNet»
- «Strazh»
- «CSM32»
- «Neman»
- «Mirazh»
- «Import from XML»

If before Security Center installation the software from the list above was used, then for a comfortable transition to Security Center, it is possible to import the descriptions of sites from the database of these programs.

If it is intended to import data from the “Andromeda” software version 2.0 - 2.76 or “Andromeda Liberty”, then when installing Security Center, it is necessary to specify the need to install BDE, the subsystem used to access the data of these programs.

Data import is performed with the help of the “Database wizard” module. In the case of import from “Andromeda” software versions 2.0 - 2.76 or “Andromeda Liberty”, all files from the database folder will be required to run it. If there is a backup copy of the database in ZIP format, it is necessary to extract the files from the archive to any folder on the computer hard drive.

5 Event Manager

The “Event manager” module is intended for receiving notifications from the receiving equipment of the central station, as well as directly from certain types of site equipment, for example, via GSM (CSD/GPRS) and Ethernet communication channels.

Events, that constitute the basis of the Security Center software, are a result of handling of notifications received by the “Event manager” module.

The events are automatically handled in the “Event manager” module: event chains are monitored, SMS messages are sent and events are transmitted to other systems. Besides, the “Event Manager” is the link for all other modules of Security Center: it shall be launched first, because it is with its help that the modules exchange information about new events, operators’ actions and other changes that occurred during the module operation.

After the module is started, an icon appears in the system tray of the Windows taskbar, informing you of the module’s operation. After reception of events, the icon color changes, and when you hover over it, information appears on the time of the last event and the total number of events since the module was started.

If you right-click on the mouse button on the module icon, a drop-down menu will appear.

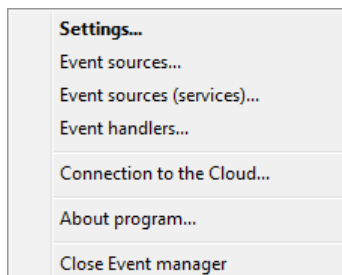


Figure 11: Drop-down menu of the “Event manager” module

5.1 Module Settings

To access the settings select the “Settings ...” item in the module drop-down menu.

To access the “Settings” window and save the changes made in it, the user shall have permission to “Change settings” for the “Event manager” module.

5.1.1 Common

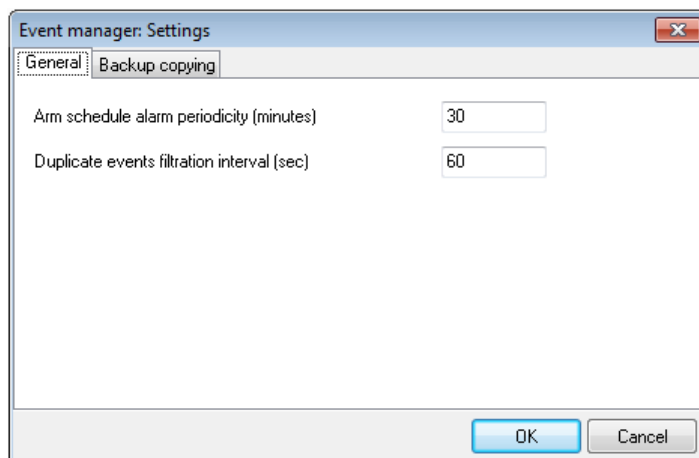


Figure 12: "Settings" window, "Common" tab

The parameter “Arm schedule alarm periodicity” specifies the interval for generating system events with codes ZZXB and ZZXC. The system events with these codes are created when the daily arm schedule of the site is violated and the long-term arm schedule of the site is violated, respectively. Arm schedule and long-term arm schedule of the site are set individually for each site in the “Site Manager” module.

The parameter “Duplicate events filtration interval” specifies the interval during which the second and subsequent identical events received via different communication channels will be considered duplicate. Duplicate events are handled in Security Center modules in a special way. Thus, in the “Duty operator” module they are not displayed in the general list of accepted events. In this case, it is possible to enable their display on the events tab from the site. Besides, duplicate events are not included in the reports unless specifically indicated. The recommended value for this parameter is 60 seconds.

5.1.2 Backup

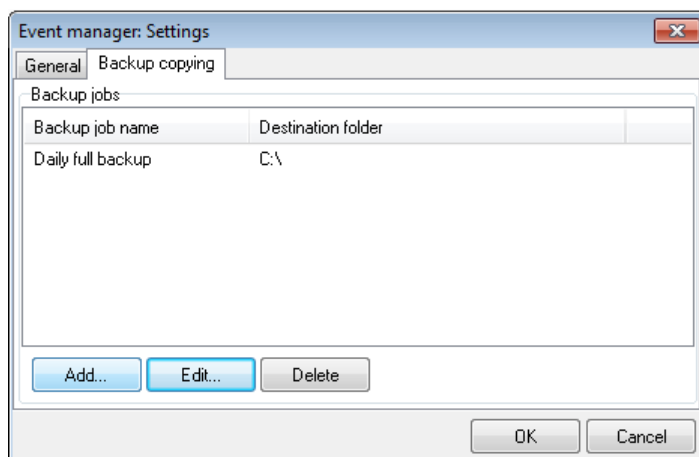


Figure 13: "Settings" window, "Backup" tab

The “Backup” tab of the “Event Manager” settings window is intended for managing backup jobs.

Use the “Add ...” button to create a new backup job, and the “Change ...” and “Delete” buttons to change the settings of the existing job or to delete it.

When creating a new backup job or changing an existing backup job, it is possible to define the job parameters in the “Backup job” window.

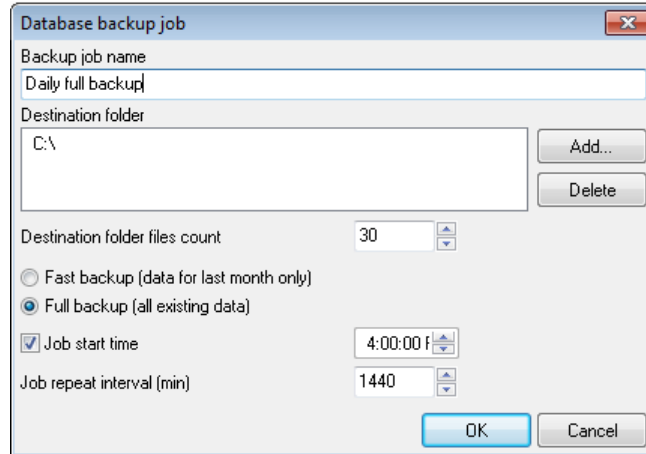


Figure 14: “Backup job” window

The “Job name” parameter allows to specify a name for the backup job to distinguish one job from another in the list.

Use “Destination Folder” parameter to define one or more folders to which the database backup will be copied after it is created. In this case, number of files of the backup copy of the Security Center database in each destination folder will be monitored. If the number of backup files is greater than the number of files in the destination folder, set by “Destination folder files count” when creating a backup, the oldest backup file will be deleted.

There are two types of backup copies of the Security Center database: fast and full.

- *Full* copy of the database contains all information stored in the database at the time of copying, including received events, operator actions and sent SMS messages for the entire period of the software operation.
- The amount of data in the *fast* copy is much smaller: it stores events, operator actions and SMS messages only for the last month.

In general, it is recommended to use fast copies for backup jobs. As for full database backups, they are recommended to be done manually or using Windows Scheduler tasks. See more information about creating a database backup using the Windows Scheduler in the “Database Wizard” section.

The “Job repeat interval” parameter specifies the interval for repeating the backup job.

By checking the box next to the “Job start time” option and specifying the time, it is possible to configure the start of the backup job at the same time. In this case, if the value of the “Job repeat interval” parameter is zero, then the job will be executed once a day. And if the “Job repeat interval” parameter is set to a non-zero value, periodic backups will be run every day at the same time.

Backup copies of the Security Center software database are created using the “Database wizard” module, including those created by backup jobs. To learn more about how to back up the database and perform database restoration from a backup see the “Database Wizard” section of this guide.

5.2 Event Sources

The main purpose of the “Event manager” module is that it receives notifications from the receiving equipment of the central station, as well as directly from certain types of site equipment, for example, via GPRS and Ethernet communication channels. A variety of methods and protocols for transmission of notifications is supported with the help of special components of the “Event manager” module, which are called “event sources”.

To access the settings of event sources select the “Event sources ...” item in the module menu that appears after right-clicking on the module icon in the system tray of the taskbar.

To access the “Event sources” window and save the changes made in it, the user shall have permission to “Change settings” for the “Event manager” module.

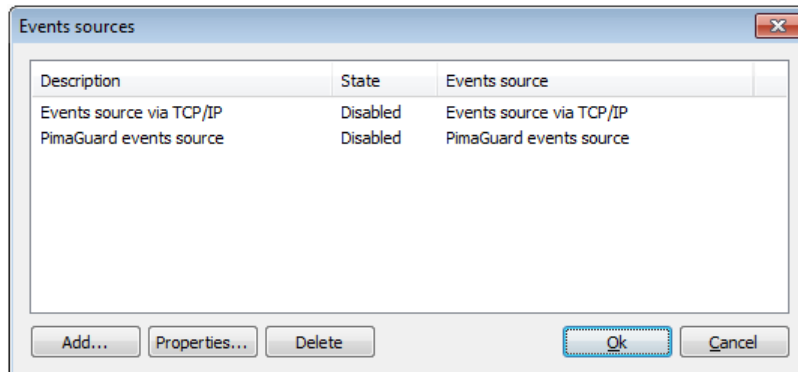


Figure 15: “Event Sources” window

Click on the “Add...” button to select the desired event source from the list of the ones installed in the system.

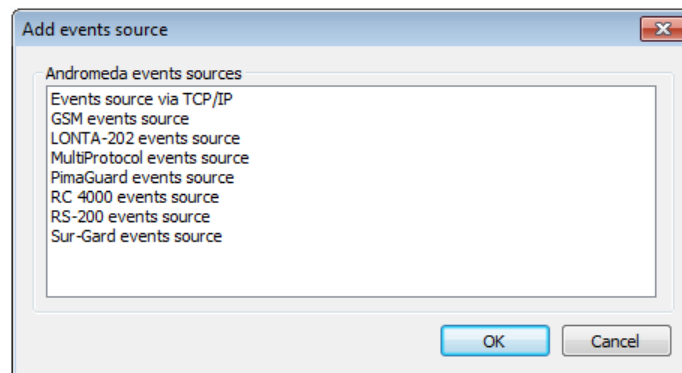


Figure 16: “Add Event Source” window

Use the “Properties ...” button to change the settings of the selected event source.

5.2.1 Common Event Source Settings

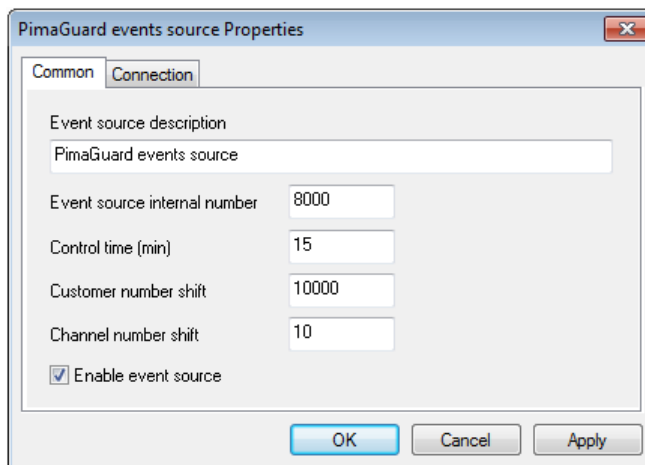


Figure 17: "Event source Properties" window, "Common" tab

Use the "Event source description" parameter to specify the name and important parameters of the event source, in order to see them in the list of used event sources.

The "Event source internal number" parameter is required for its identification by the Security Center and user. First, the number of the event source is used to determine from which source an event is received. Second, when the event source reports something to the user, the event created for this event will have the same site number as the internal source number. It is highly recommended to create sites in the Security Center, the numbers of which correspond to the internal numbers of the event sources - this will allow to monitor the occurrence of errors that occur during the source operation, as well as receive service information about their work.

The "Control time" parameter allows to automatically monitor the fact of receiving events by the source and inform the operator about problems encountered during reception. If, for some reason, no events are received for the event interval specified by this parameter, a system event with "ZZXH" code and the site number corresponding to the internal number of the event source will be created.

Use "Client number shift" parameter to specify a positive integer that will be automatically added to the site number for each event accepted by the event source. It is recommended to use the shift of site numbers if several central monitoring panels, including different panels, are to be connected to one copy of the Security Center software. By setting different shifts of site numbers for different event sources, it is possible to avoid the problem of overlapping of the same numbers of different sites operated on different panels.

For example, two Lonta-202 remote controllers are connected to the Security Center. Ranges of site numbers that can be connected to panels are the same - from 1 to 600. But if the event number shift equal to 1000 is set for one source of events, and 2000 for the other, then we will work with sites 1001-1600 for one panel and 2001-2600 for the other in the Security Center.

"Channel number shift" is a parameter that specifies a positive integer that will automatically be added to the receive channel number. If the channel number shift number is set to zero, then the events received by the event source will use the channel number transmitted by the receiving equipment of the central station or the first channel number if the equipment does not transmit the channel number. By setting different channel number shifts for different event sources, it is possible to distinguish the event sources (and the connected panels) for the received events. The channel number shift is especially relevant when using several identical event sources, since the types and numbers of the communication channels used by these sources will most likely be identical.

It is possible to enable or disable the event source using the "Enable event source" parameter. It shall be noted that if the event source is turned off, then all resources used by it are released.

5.2.2 Event Source from PimaGuard and Sentinel

PimaGuard and Sentinel event source is intended for receiving events via serial port or Ethernet network from the software from the following list:

- “Mcard for MS-DOS”;
- «Pima NetSoft» (transmitters «GSM-200» and communicators «Net4Pro»);
- “Pima IP Receiver” (control panels “AlarmView” “Guardian”);
- “PimaGuard for Windows” (“Andromeda” protocol).

This is the most up-to-date source for receiving events from the receiving equipment of Pima central station, which includes all features of the “Event Source from CMS-420”, which is no longer supplied as part of the Security Center. If it is necessary to support the newest features of the receiving equipment of the central station, as well as the full range of protocols and channels for the transmission of notifications implemented by Pima receiving equipment, it is necessary to use the “Event sources from PimaGuard and Sentinel”.

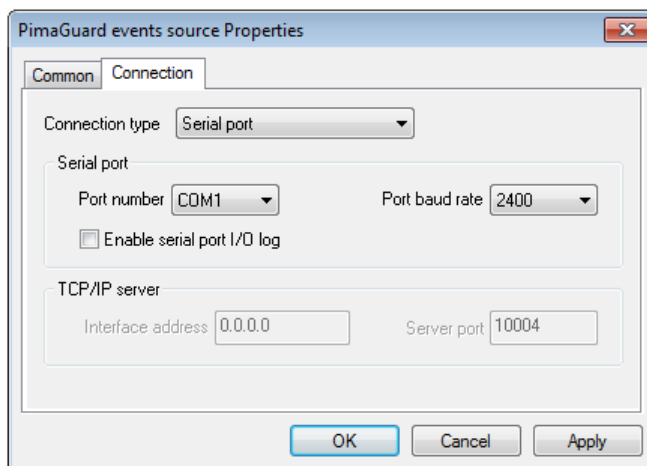


Figure 18: “PimaGuard event sources properties” window, “Connection” tab, “Serial port” connection type

The “Connection Method” parameter specifies the method with which the receiving equipment connects to the Security Center: via serial port or network that supports the TCP/IP protocol.

If serial port is used, use the “Port number” parameter to select the serial port to which the receiving equipment of the central station is connected, and use the “Port baud rate” parameter to set the exchange rate.

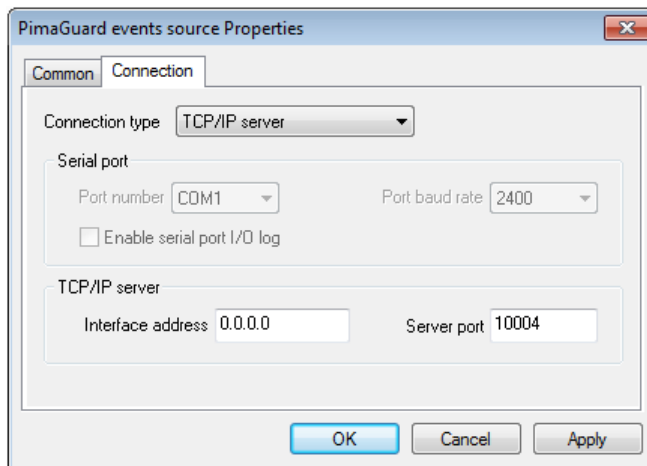


Figure 19: “PimaGuard event sources properties” window, “Connection” tab, “TCP/IP server” connection type

When connecting the receiving equipment via Ethernet, it shall be remembered that the “Event Source from PimaGuard and Sentinel” always acts as TCP/IP server, that is, it waits for incoming connections. If several

network adapters are installed on the computer, or if one adapter uses multiple IP addresses, use the “Interface address” parameter to specify the IP address where the event source shall wait for incoming connections. The “Server port” parameter is intended to indicate the port to which the receiving equipment of the central station will be connected.

When using PimaGuard source in the event receiving mode via Ethernet, it is recommended to use a separate instance of the event source for each instance of the sending software.

5.2.3 Event Source via TCP/IP

“Event source via TCP/IP” is intended for receiving events via TCP/IP-compatible network from the following C.Nord equipment:

- GSM transmitters “TR-100 GSM” and “TR-100 GSM II” - via GPRS
- Panic button “Button” - via GPRS channel
- Repeater “Tsefei” - via Ethernet channel

If this event source is used, the central monitoring panel usually requires a dedicated IP address on the Internet. Besides, it is recommended to connect different types of equipment to different instances of the event source, and when connecting the “Tsefei” repeater, it is best to use a separate instance of the event source for each repeater.

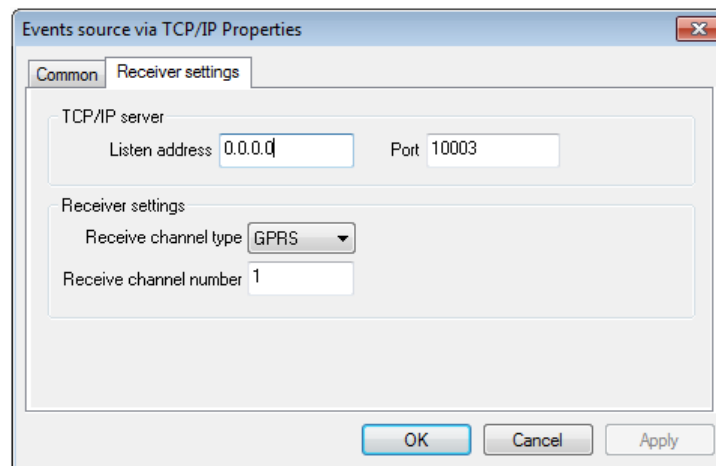


Figure 20: Event source via TCP/IP properties window, "Receiver setting" tab

“Event source via TCP/IP” always acts as a TCP/IP server, that is, it waits for incoming connections. If several network adapters are installed on the computer, or if one adapter uses multiple IP addresses, use the “Interface address” parameter to specify the IP address where the event source shall wait for incoming connections. The “Server port” parameter is used to specify the port to which the connection will be expected.

Use the “Receive channel type” parameter to explicitly specify the type of communication channel that is used when transmitting messages from the site equipment.

For example, the “Event Source via TCP/IP” can receive events from transmitters TR-100 GSM via GPRS channel and from repeaters “Tsefei” via Ethernet. The event source cannot identify the communication channel that is used for transmission. Therefore, when configuring this event source, it is necessary to explicitly specify the type of communication channel that is used for transmission: GPRS if the source is intended for receiving events from TP-100GSM, and Ethernet, if the source receives data from the “Tsefei”.

The “Receive channel number” parameter is used to specify the number that will be used to identify the channel on which the event was received. The parameter value is especially useful if several event sources are used via TCP/IP: to distinguish between sources from which the event was received it is necessary to set different receive channel numbers for them.

5.2.4 GSM Events Source

“GSM Events Source” is intended for reception of events via GSM SMS and CSD channels from the “Nord GSM”, “Soyuz GSM” and “TR-100 GSM IV” - via CSD channel.

It shall be noted that in order to use the GSM event source, it is necessary to connect GSM-modem SonyEricsson GT-47, Siemens MC35, or compatible with them by the command system to the computer.

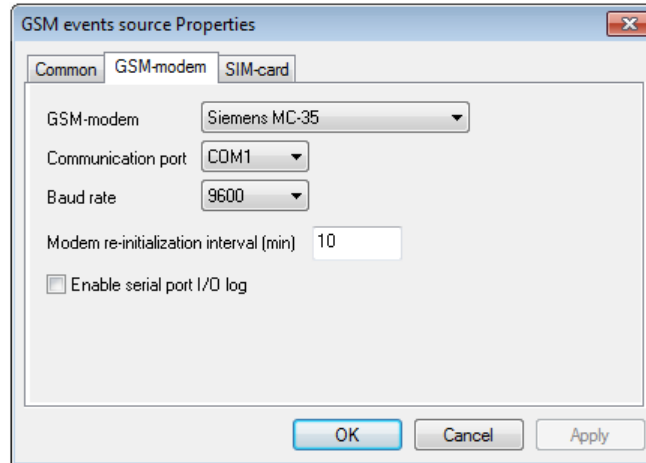


Figure 21: “GSM events source properties” window, “GSM-modem” tab

The “GSM-modem” parameter defines the type of GSM-modem connected to the event source.

Use “Communication port” parameter to select the serial port to which the GSM-modem is connected, and “Baud rate” parameter to set the exchange rate.

The parameter “Modem re-initialization interval” allows to forcefully re-initialize the events of the GSM-modem connected to the source with a specified interval.

Check “Enable serial port I/O log” option to save exchange protocol of the event source with the GSM-modem to the hard disk. This information is useful when finding out the causes of problems when connecting to a GSM-modem or sending SMS messages through it. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

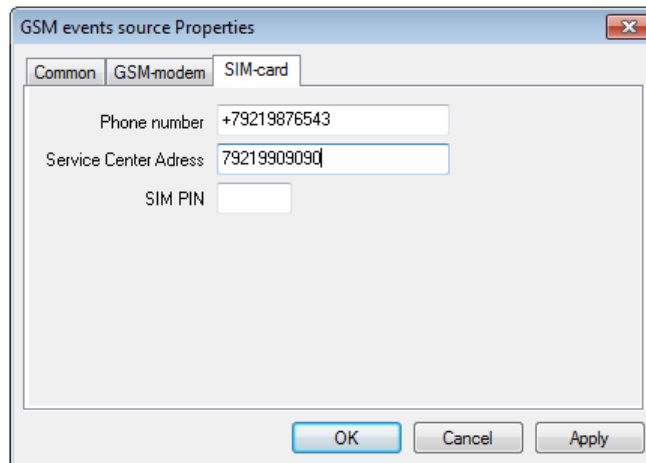


Figure 22: “GSM events source properties” window, “SIM-card” tab

Using the “Phone number” parameter to specify the phone number of the SIM card installed in the GSM-modem. This parameter is required to generate commands for the “PT-300” buttons sent via SMS.

The “Service center address” parameter allows to set the phone number of the SMS-center of the mobile operator, which SIM card is installed in the GSM-modem. Some communication operators require that this parameter be

set so that the function of sending SMS messages works correctly. The phone number that is used as the value of the “Service center address” parameter shall be specified in full, international format. The symbol “+” shall not be used when specifying this number.

If the SIM card installed in the GSM-modem is protected by a personal identification code, it can be set as the value of the “SIM PIN” parameter. It is strongly recommended not to use SIM cards protected by PIN code to avoid problems associated with the loss of set codes.

5.2.5 Sur-Gard events source

It is intended for receiving events via the serial port from the receiving equipment of the Sur-Gard central stations manufactured by DSC up to and including System III. Since the data transmission format used by Sur-Gard central stations is the de facto standard, this event source can be used to receive events from hardware and software from a variety of vendors: “Ritm”, “Proksima”, Jablotron, etc.

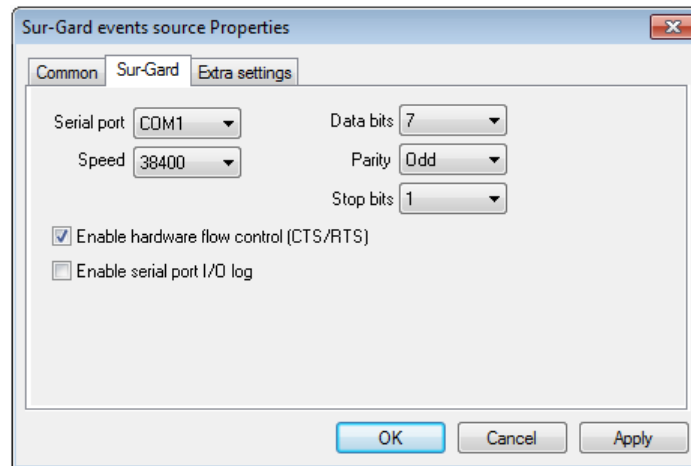


Figure 23: Sur-Gard events source Properties window, “Sur-Gard” tab

Use the “Serial port” parameter to select the serial port to which the receiving equipment of the central station is connected, and use the “Port baud rate” parameter to set the exchange rate. The amount of data bits in the transmitted bytes can be specified with the “Data bits” parameter, the transmission parity can be specified by the “Parity” parameter, and the “Stop bits” parameter is used to determine the amount of stop bits.

If hardware control of the data flow is used when communicating via a serial port, it is necessary to check the “Enable hardware flow control (CTS/RTS)” box.

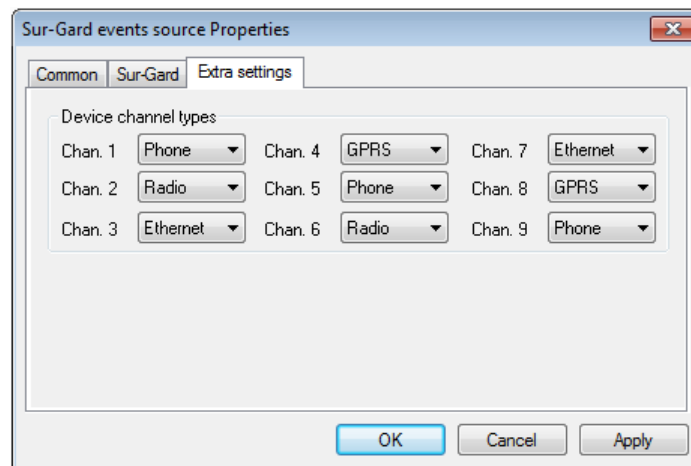


Figure 24: Sur-Gard events source Properties window, “Extra settings” tab

Use the “Extra settings” tab to specify the types of communication channels that are used by the receiving equipment of the central communication when receiving signals from the site equipment.

5.2.6 LONTA-202 Events Source

“LONTA-202 events source” is intended for receiving events via serial port from the central monitoring panels Lonta PRO, Lonta Optima and LONTA-202 manufactured by Altonika.

It shall be noted that if you use the Sentinel software together with any Altonika panel and want to switch to the Security Center software, then you need to know about the possibility of automatic data import from the “Strazh” software. See the description of the “Database wizard” module, with which the data are important, for more information about this function.

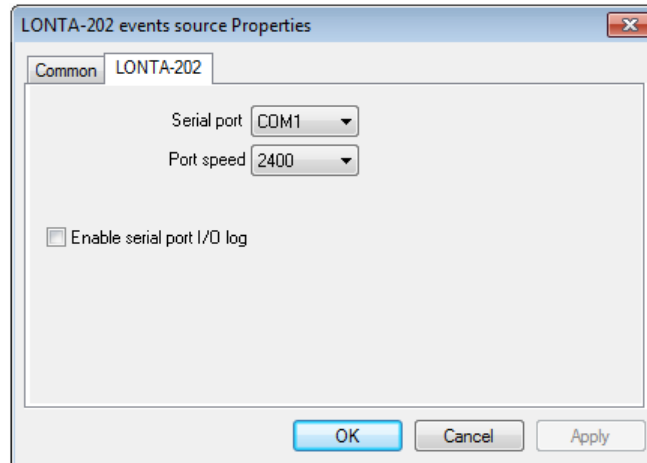


Figure 25: LONTA-202 events source Properties window, "LONTA-202" tab

Use “Serial port” parameter to select the serial port to which the central monitoring panel is connected, and “Port baud rate” parameter to set the exchange rate.

5.2.7 RS-200 Events Source

“RS-200 events source” is intended for receiving events from the central monitoring panel RS-200 manufactured by Altonika. It shall be noted that the event source supports the entire spectrum of equipment that transmits signals to the RS-200 panel.

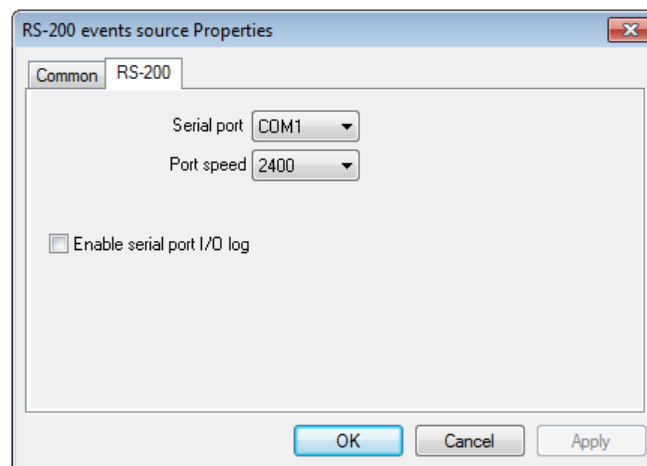


Figure 26: RS-200 events source Properties window, "RS-200" tab

Use “Serial port” parameter to select the serial port to which the central monitoring panel is connected, and “Port baud rate” parameter to set the exchange rate.

Site number shift ”is a positive integer that is automatically added to the site number for each event accepted by the event source.

5.2.8 RC 4000 Events Source

“RC 4000 events source” is intended for receiving events via serial port from the central monitoring panel RC 4000 manufactured by Visonic.

If you use the RC 4000 panel together with CSM32 software and want to switch to the Security Center software, then you need to know about the possibility of automatic data import from the CSM32 software. See the description of the “Database wizard” module, with which the data are important, for more information about this function.

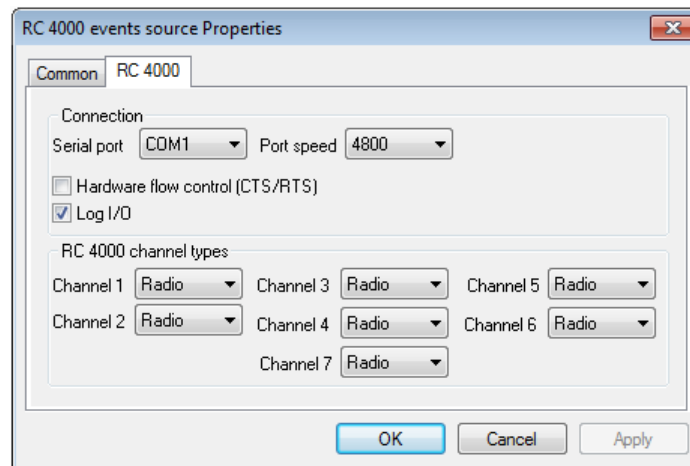


Figure 27: RC 4000 events source Properties window, "RC 4000" tab

Use “Serial port” parameter to select the serial port to which the panel is connected, and “Port baud rate” parameter to set the exchange rate.

If hardware control of the data flow is used when communicating via a serial port, it is necessary to check the “Enable hardware flow control (CTS/RTS)” box.

Check “Log I/O” option to save exchange protocol of the event source with the central monitoring panel to the hard disk. This information is useful when finding out the causes of problems when receiving events from the panel. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

Use the “RC 4000 channel types” tab to specify the types of communication channels that are used by the panel when receiving signals from the site equipment.

5.2.9 Multiprotocol Event Source

“Multiprotocol event source” is intended for receiving events via serial port from the following central monitoring panels

- Silent Knight 9500 (Honeywell)
- RCI4000/RCI5000/DTRCI5000 (KP Electronics)
- Blitz (radio channel) (PKS)
- AES-Intellinet (radio channel)

Besides, this event source supports reception of data via some other common protocols, for example, Ademco 685 protocol.

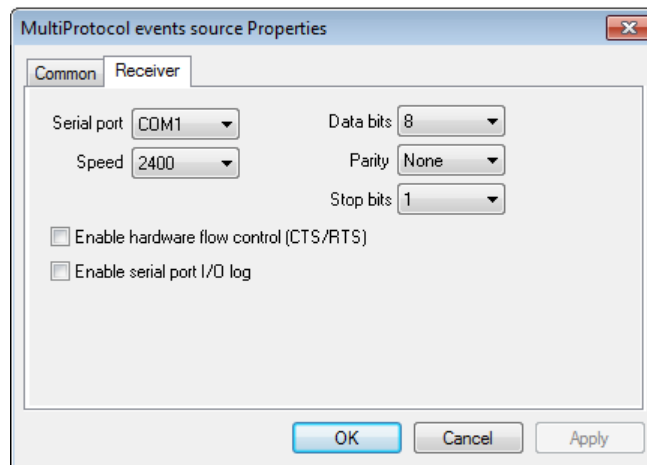


Figure 28: "Multiprotocol events source Properties" window, "Receiver" tab

Use the "Serial port" parameter to select the serial port to which the receiving equipment of the central station is connected, and use the "Port baud rate" parameter to set the exchange rate. The amount of data bits in the transmitted bytes can be specified with the "Data bits" parameter, the transmission parity can be specified by the "Parity" parameter, and the "Stop bits" parameter is used to determine the amount of stop bits.

If hardware control of the data flow is used when communicating via a serial port, it is necessary to check the "Enable hardware flow control (CTS/RTS)" box.

5.3 Event Handlers

After the "Event manager" module accepts notification from the central monitoring or control panel, it decodes and describes the notification in accordance with the event template specified for the site from which the notification was received. The event resulting from the decoding of the notification can be automatically handled in the "Event manager" module with the help of special module components called event handlers.

To access the settings of event sources select the "Event handlers..." item in the module menu that appears after right-clicking on the module icon in the system tray of the taskbar.

To access the "Event handlers" window, the user shall have permission to "View event handlers" for the "Event manager" module.

To save the changes, made in the "Event handlers" window, the user shall have permission to "Edit event handlers" for the "Event manager" module.

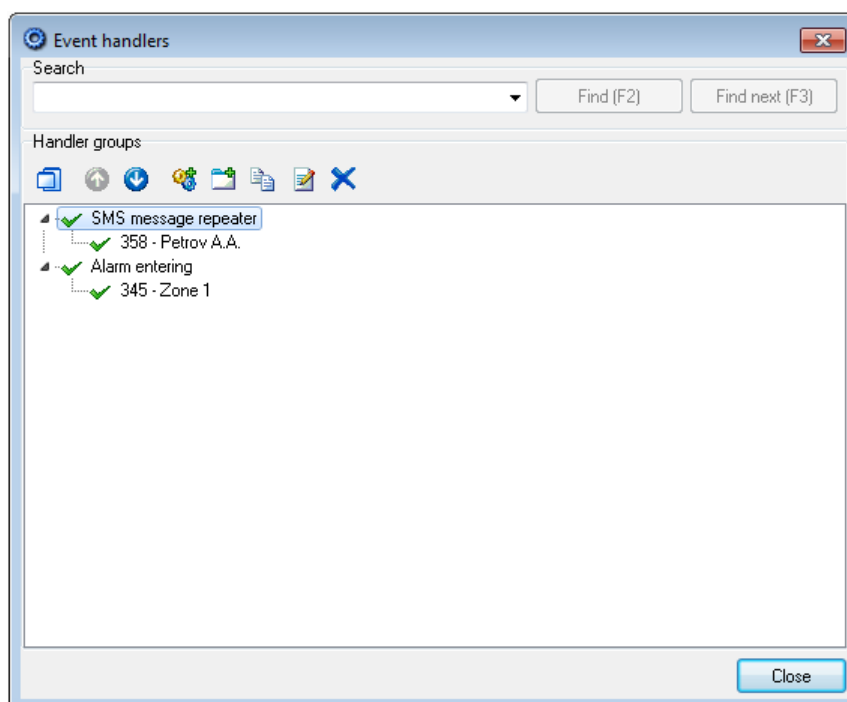


Figure 29: "Event handlers" window

The "Search" area of the "Event Handlers" window is intended to search for a group or event handler in the list. If you click on the "Start" button, the search will be performed from the very beginning of the list. If you click on the "Find next" button, the search will start from the current selected item in the list of handlers.

The Security Center event handlers are controlled with the buttons of the control panel, located at the top of the "Handler groups" area of the "Event Handlers" window.

Click the "Show hidden handler groups" button to display the handlers marked as hidden in the list. To enable display of the hidden event handler groups, the user shall have permission to "View hidden event handlers" for the "Event manager" module. It shall be noted that the permission to "Edit event handlers" applies only to those event handlers that the user can view. Thus, the user can be granted permission to make changes to the handlers of "SMS message repeater" and hide others, critical for the Security Center, such as "Pandora Network" or "Alarm entering".

Use the "Move up the list" and "Move down the list" buttons to change the order of the handlers in the display list. This order is important, since each event is sent to the event handlers in turn, in the order in which the handlers appear in the list. For example, if the "Event chain monitor" handler is configured to monitor the "Alarm reset" event after the "Alarm" event, then it shall be in the list before the "Alarm entering" handler, since the latter can change the class of the received event .

The "Create group" button is intended to add a new group of event handlers to the list. And the button "Create handler" allows to add a new handler to the group. There are no restrictions on the number of groups of handlers in the list or the number of handlers in the group, they can be created as many as necessary. The event handler group defines an algorithm according to which the event will be handled. Besides, the group settings define the resources that will be used during handling. For example, device for SMS sending is specified in the "SMS message repeater" event handler, and this device will be used to send messages to all handlers in the group. As for the handlers in the group, they define the settings for the event handling that is performed with respect to specific sites. In this case, the settings of different handlers do not depend on each other. For example, events from the same site can be handled by different handlers from the same group. Combining of handlers into a group is also useful when event handlers need to be hidden or disabled: the group is hiding together with the handlers that it includes, and if the event handler group is disabled, the handlers included in it will not function, even if they themselves are enabled.

Use "Paste copy of selected item" button to copy the current item selected in the list. If this is an event handler, then its copy will be inserted into the same event handler group, except that the new handler will be disabled. If a

group of handlers is selected in the list, a copy of the group will be inserted into the list. In this case, the state of the group handlers will be preserved, but the new group of event handlers will be turned off.

Click on the “Properties” button to configure the group of event handlers or a separate handler.

The “Delete selected item” button allows to remove the selected group of event handlers or a separate handler in the group from the list. Be careful, when you delete an event handler group, all event handlers included in it will be deleted. Due to the fact that deleting event handlers is accompanied by cleaning the database from their settings, deleting some groups of event handlers can take a long time.

The list of event handlers supports several operations that can be performed with the mouse. For example, it is possible change the order of items in the list, and move event handlers from one group to another.

5.3.1 Common Settings for Event Handler Groups

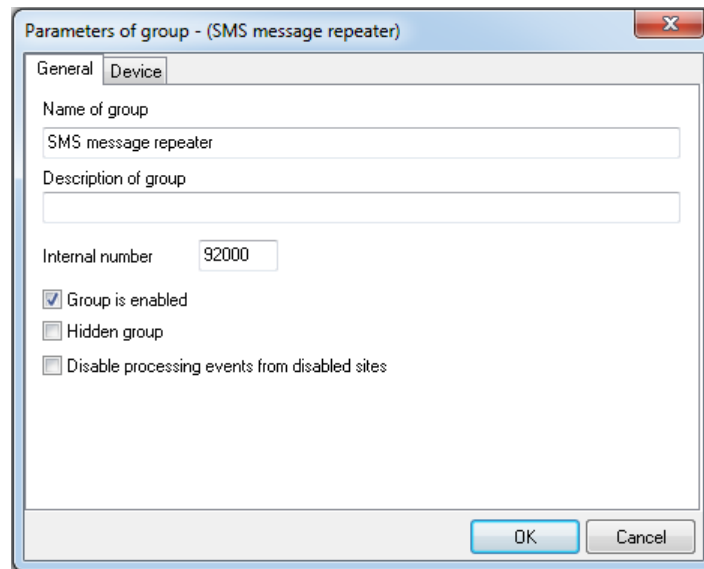


Figure 30: “Parameters of group” window, “Common” tab

As a value for the “Name of group” parameter it is allowed to specify a string that will be displayed in the list of handlers in the “Event Handlers” window. In the group name of event handlers, it is recommended to include key information that characterizes the group to distinguish one group from another, for example, the parameters of the resources used by the group.

The “Description of group” parameter is used to store detailed information about the group of event handlers.

The “Internal number” parameter is required to identify the group of event handlers by Security Center and the user. When the group reports something to the user, the created event will have the same site number as the internal group number. It is highly recommended to create sites in the Security Center, the numbers of which correspond to the internal numbers of the event group - this will allow to monitor the occurrence of errors that occur during the handler operation, as well as receive service information about their work. As an event template for sites which numbers correspond to the internal numbers of the event handler groups, it is recommended to use the “Event Handlers” template.

When searching in the “Event handlers” window, the search query browses the values of the “Name of group”, “Description of group” and “Internal number” parameters.

The group of event handlers can be enabled or disabled by the “Group is enabled” parameter. It shall be noted that if the group of event handlers is disabled, then all resources used by it are released and the event handling by the group is terminated. In this case, the handlers included in the group can be enabled, since the handler state does not influence event handling by the disabled group.

If “Hidden Group” parameter is set for a handler group, it is possible to hide this handler group from the list in the “Event handlers” window for those users who do not have permission to view the hidden groups of event handlers.

Use the “Disable handling events from disabled sites” to disable event handling from sites that are disabled. This function can be useful for almost all handlers, since it allows to automatically exclude disabled sites from handling. The site is disabled in the “Site manager” module on the “Arm” tab. See “Site Manager” section of this manual for more information about disabling sites.

5.3.2 Common Event Handler Settings

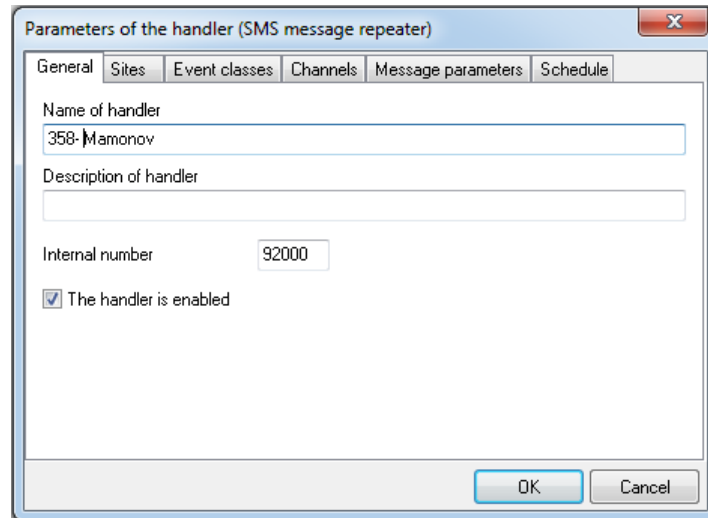


Figure 31: “Parameters of handler” window, “Common” tab

As a value for the “Name of handler” parameter it is allowed to specify a string that will be displayed in the list of handlers in the “Event Handlers” window. In the name of the event handler, it is recommended to include key information that characterizes it and allows to distinguish one handler from another, for example, the number of the site, which events are handled by the handler.

The “Description of handler” parameter is intended for storing detailed information about the event handler.

The “Internal number” parameter is required to identify the handler by Security Center and the user. When the handler reports something to the user, the created event will have the same site number as the internal handler number.

The event handler can be enabled or disabled by the “Handler is enabled” parameter. It shall be noted that for the operation of the event handler, it is necessary that both the handler and the event handler group, into which it is included, are enabled.

Sites

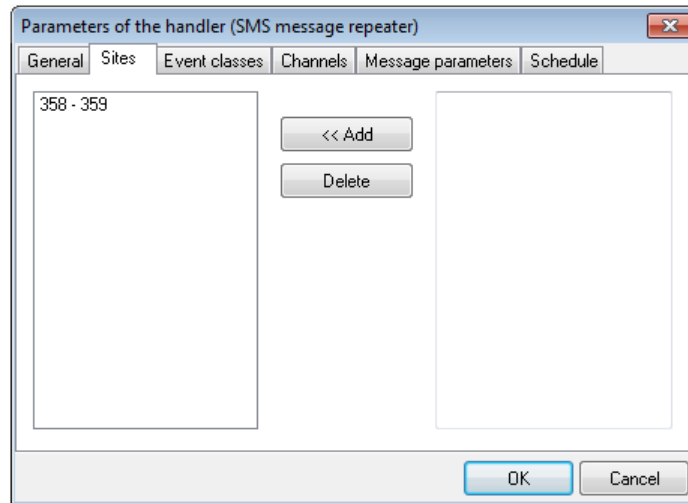


Figure 32: "Parameters of handler" window, "Sites" tab

The "Sites" tab is used to specify the numbers and intervals of the site numbers, which events will be handled. To add a number or an interval of site numbers to the list of handled ones, it is necessary to enter it in the input field in the right part of the window and click on the "Add" button. When entering site numbers, it is allowed to enumerate several numbers or numbers and intervals of numbers separated by commas, for example: "100, 102, 104, 106-100, 200-299". To delete a number or an interval of site numbers from the list of the handled ones, it is necessary to select the line with the value, which shall be deleted in the list, located in the left part of the window, and click on the "Delete" button.

Channels

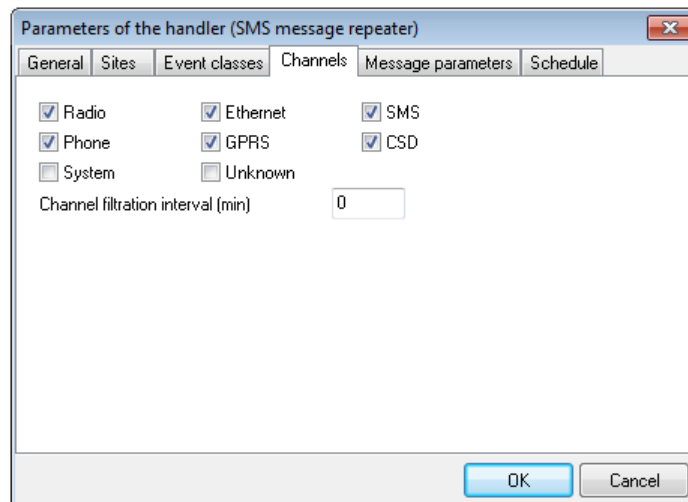


Figure 33: "Parameters of handler" window, "Channels" tab

The "Channels" tab is intended to specify the types of communication channels via which the events to be handled shall be received. To allow the handling of the events received via a particular communication channel, it is necessary to check the appropriate channel name.

The "Channel filtration interval" parameter is intended to exclude from handling the identical events received via different communication channels. If this parameter value is greater than zero, only the first event received will be handled, all other events, received during the specified interval, will be ignored. For example, if two communication channels are used for transmitting messages from the site: radio and telephone and the value of the "Channel filtration interval" parameter is 1 minute, the message received by radio will be handled, and the message received by phone will be ignored (if it comes within one minute). The "Channel filtration interval" parameter is recommended for use in event handlers "SMS message repeater".

Schedule

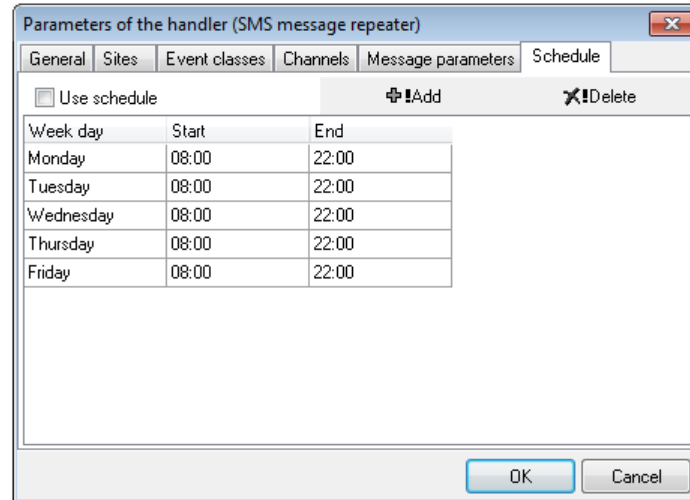


Figure 34: "Parameters of handler" window, "Schedule" tab

If the event handler shall be set up so that event handling is performed only at a specified time, set the handler schedule on the "Schedule" tab.

Click the "Add" button to add the interval of the event handler to the list. For each interval, it is necessary to specify the day of the week to which it relates, as well as the start and end time of its operation.

The "Delete" button is used to delete the interval of the event handler from the list.

Use the "Use schedule" option to enable or disable the use of the schedule by the handler. If the use of the schedule by the event handler is disabled, then it works constantly. If the use of the schedule is enabled, but there is not a single interval for the work, the event handler will never be enabled.

5.3.3 Event Monitoring

This handler monitors periodic reception of the event of a given class and generates a system event in the absence of it.

The handler can be used to solve the following tasks:

- "Guard monitoring". The task of guard monitoring is often reduced to a simple monitoring of the periodic reception of a given event. In this case, despite the fact that the sequence of event reception is not monitored, it is possible to monitor the guards even on a complex route by selecting the intervals for receiving events.
- "Automatic test monitoring" Unlike the control time of a site that implies the arrival of any event from the site via any communication channel, it is possible to monitor the periodic arrival of a particular event, and specify the communication channel via which this event is to be received.

The settings of the "Event monitoring" event handler group completely coincide with the general settings of the event handler groups, which are discussed in detail above.

The settings for the "Event monitoring" event handler also largely coincide with the general settings of the event handlers discussed above, except for the "Event monitoring" tab.

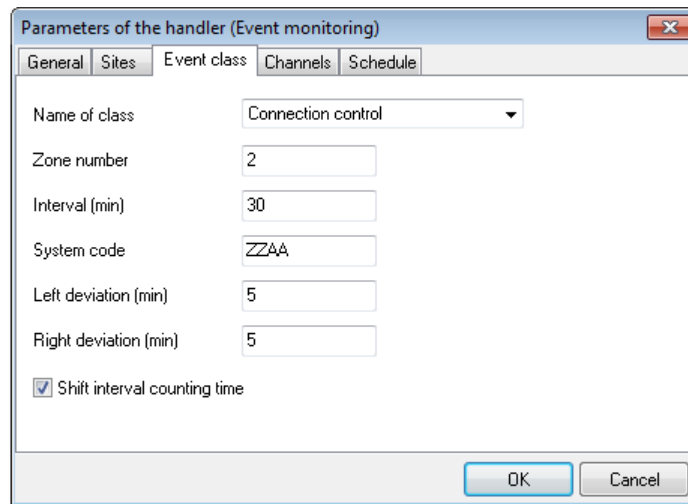


Figure 35: "Parameters of handler (Event monitoring)" window, "Event class" tab

- The event handler, configured as shown in the figure, will monitor the arrival of the "Connection control" event class every 30 minutes. A period from 25 to 34 minutes after receiving the previous event will be considered valid for the next event. *

The "Event class" parameter specifies the event class that the event handler monitors.

Use the "Zone number" parameter to limit the list of events monitored by the handler. If this parameter value is not set or equal to zero, then the handler monitors the reception of any events, which class corresponds to the value of the "Event class" parameter. If the "Zone number" parameter is set to the zone value, only those events that have a zone number corresponding to the specified zone will be monitored.

The "Interval" parameter defines the interval during which the event handler shall receive monitored events.

The "System code" parameter specifies the system event code that will be created if the next event is not received by the handler. When creating a system event, the communication channel "System" and the number of the site, from which the monitored event is not received, are used. The system event will be decoded according to the event template specified for the site on which the event was created.

The "Left deviation" and "Right deviation" parameters are intended to configure the exact monitoring interval for receiving the monitored events. If the value of the "Left deviation" parameter is not equal to zero, then only the event, that is be accepted not earlier than the value of the interval minus the left deviation, will be counted as received. For example, if the event arrival is monitored every 30 minutes and the left deviation is 5 minutes, then only the event, that is received not earlier than 25 minutes after the previous one, will be counted as accepted. If the value of the "Right deviation" parameter is not zero, then the event, that is be received later than the value of the interval plus the right deviation, but not more, will be counted as accepted. For example, if the event is monitored every 30 minutes and the right deviation is 5 minutes, the event, received 34 minutes after the previous one, will be counted as accepted.

If the "Shift interval counting time" parameter is set, then the new timeout interval of the event will be counted from the moment of the previous event reception. If the parameter is not set, then the interval count is related to the moment the handler is enabled. If the events monitored by the handler are created by the person, it is recommended to set the "Shift interval counting time" parameter, so that the event handler ignores inaccuracies and deviations related to the presence of the human factor. If the events created by the equipment are monitored, then it is not necessary to set the "Shift interval counting time" parameter.

Setting the permissible deviations and shifting the beginning of the interval are most often needed for tasks similar to the "Guard monitoring" task: there is an interval during which a round is made, there are permissible deviations. If the monitoring button is pressed ahead of time, it is ignored and it is possible to press it a bit later. At the same time, the new interval will be counted from the moment when the security guard confirmed the completion of the previous one.

5.3.4 Event Chain Monitoring

This handler is intended to monitor the time sequence (chain) of received events and the generation of system messages in case of violation. The handler is intended for solving tasks such as:

- “Monitoring of paired events”. For example, monitoring the restoration of 220V or other faults at the site. Use the “Event chain monitoring” handler for automatic distinguishing between short-term faults from fatal ones, for example, for detection sites where the power supply is not available for too long.
- “Guard monitoring”. The use of this handler allows to monitor the movement of the guard along the route, taking into account the correct sequence of the round.

The settings of the “Event monitoring” event handler group completely coincide with the general settings of the event handler groups, which are discussed in detail above.

The settings for the “Event monitoring” event handler also largely coincide with the general settings of the event handlers discussed above, except for the “Class chain” tab.

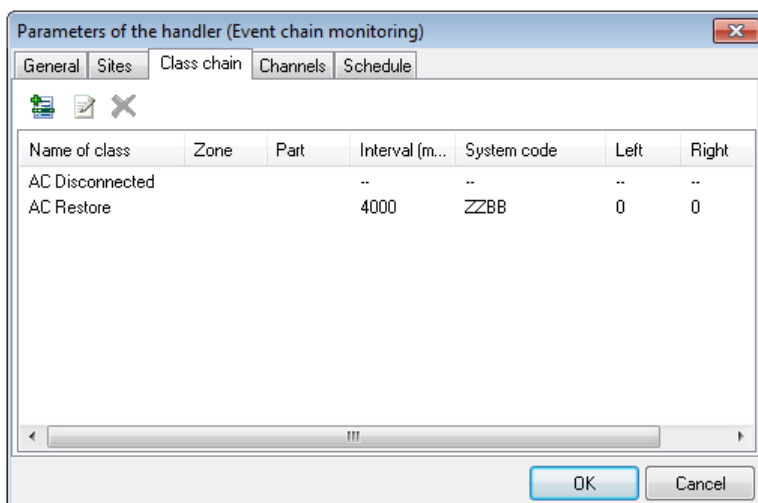


Figure 36: “Parameters of handler (Event chain monitoring)” window, “Class chain” tab

- The event handler, configured as shown in the figure, is waiting for an event with the “AC disconnected” class. If within 5 hours (300 minutes) after receiving it from the site, event with the “AC Restore” class is not received, the handler will create a system event with the “ZZBB” code. The handler configured in this way allows the personnel of the monitoring station to be warned about a prolonged power outage at the site.*

The “Class chain” tab displays a sequence of event classes, the receiving of which is monitored by the handler, and the event handler waits for the events exactly in the order in which they appear in the list.

Unlike the “Event control” event handler, which starts the waiting interval for the monitored event immediately after enabling, the “Event chain monitoring” event handler is enabled only after the first event in the chain is received. The fact of receiving the first event in the chain by the handler is not monitored in any way.

Use the “Add event class to chain” button to add a new event class to the end of the chain of monitored events.

Click on the “Event class properties” button to view and change the parameter values of the selected event class in the list.

The “Delete” button is used to delete an event class from the chain.

Use the “Event class properties” window to view and change the properties of the event class:

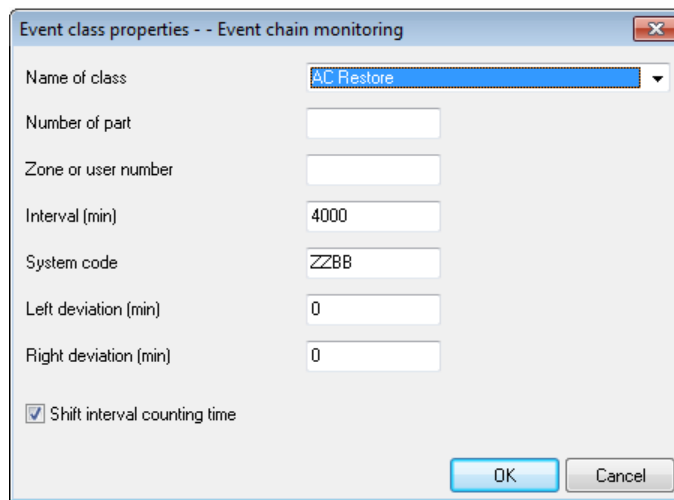


Figure 37: "Event class properties - Event chain monitoring" window

The "Name of class" parameter specifies the event class that the event handler monitors.

Use the "Zone number" parameter to limit the list of events monitored by the handler. If this parameter value is not set or equal to zero, then the handler monitors the reception of any events, which class corresponds to the value of the "Event class" parameter. If the "Zone number" parameter is set to the zone value, only those events that have a zone number corresponding to the specified zone will be monitored.

The "Interval" parameter defines the interval during which the event handler shall receive monitored events.

The "System code" parameter specifies the system event code that will be created if the monitored event is not received by the handler. It shall be noted that it is possible to specify a separate system event code for each event class in the chain. This allows to inform the operator about the details of the violation and offer him different algorithms for handling the situation. When creating a system event, the communication channel "System" and the number of the site, from which the monitored event is not received, are used. The system event will be decoded according to the event template specified for the site on which the event was created.

The "Left deviation" and "Right deviation" parameters are intended to configure the exact monitoring interval for receiving the monitored events. If the value of the "Left deviation" parameter is not equal to zero, then only the event, that is be accepted not earlier than the value of the interval minus the left deviation, will be counted as received. For example, if the event arrival is monitored in 30 minutes and the left deviation is 5 minutes, then only the event, that is received not earlier than 25 minutes after the previous one, will be counted as accepted. If the value of the "Right deviation" parameter is not zero, then the event, that is be received later than the value of the interval plus the right deviation, but not more, will be counted as accepted. For example, if the arrival of the event is controlled after 30 minutes and the deviation to the right is 5 minutes, the event received 34 minutes after the previous one will be counted as received.

If the "Shift interval counting time" parameter is set, then the new timeout interval of the event will be counted from the moment of the previous event reception. If the parameter is not set, then the interval count is related to the moment the handler is enabled. If the events monitored by the handler are created by the person, it is recommended to set the "Shift interval counting time" parameter, so that the event handler ignores inaccuracies and deviations related to the presence of the human factor. If the events created by the equipment are monitored, then it is not necessary to set the "Shift interval counting time" parameter.

Just like the system event code, the values of the permissible deviation parameters and the shift interval counting time can be specified independently for each class in the chain.

Setting the permissible deviations and shifting the beginning of the interval are most often needed for tasks similar to the "Guard monitoring" task: there is an interval during which a round is made, there are permissible deviations. If the monitoring button is pressed ahead of time, it is ignored and it is possible to press it a bit later. At the same time, the new interval will be counted from the moment when the security guard confirmed the completion of the previous one.

Monitoring of connection with C.Nord GSM devices

The “Event chain monitoring” event handler can be used to monitor connection to devices that use “C.Nord GSM (CML)” protocol.

When the device is connected to the event source, a system event with the “ZZWE” code is created, which by default is described with the “Connection established” event class. When the transmitter is disconnected, a system event with the “ZZWF” code is generated, which is described with the “Connection lost” event class.

Thus, there is all necessary information for monitoring the communication channel: if connection with the transmitter is lost and not restored within a given period of time, it is necessary to get information about it.

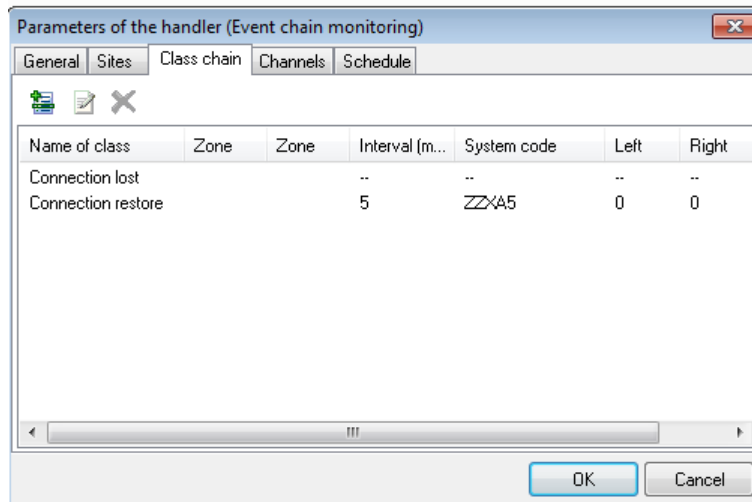


Figure 38: "Parameters of handler (Event chain monitoring) for monitoring connection window

The event handler, which is configured as shown in the figure, will create an event with the “ZZXA5” code (event class - “Connection alarm”, event description - “No events via GPRS”), if connection with the transmitter is not restored within 5 minutes after it has been lost.

5.3.5 Alarm Entering

The “Alarm entering” event handler allows to suspend handling of an alarm event by the “Event Manager” module and wait for disarming, which can be received immediately after the alarm.

The purpose of this event handler is to save the duty operator from having to respond to deliberately false alarms that occur when the sites are disarmed.

This handler shall be used for those sites where security tactics, which excludes entry delay, is used. Besides, the use of this handler is justified for all sites where a staff error is possible during disarming.

The settings of the “Alarm entering” event handler group completely coincide with the general settings of the event handler groups, which are discussed in detail above.

The settings for the “Alarm entering” event handler also largely coincide with the general settings of the event handlers discussed above, except for the “Class chain” tab.

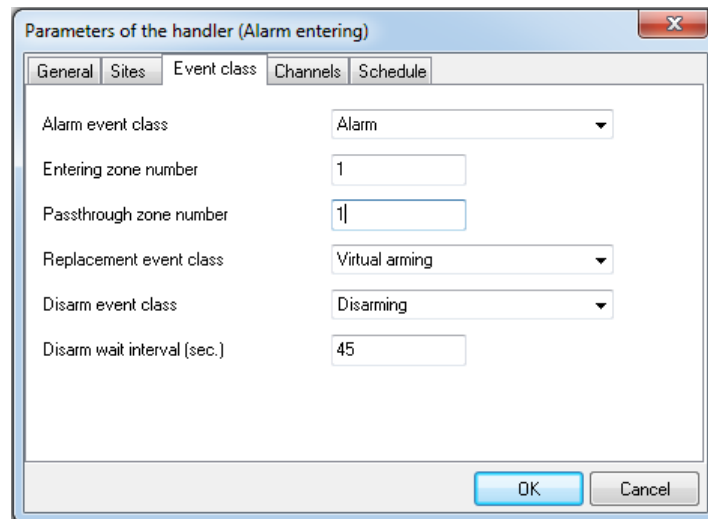


Figure 39: "Parameters of handler (Alarm entering)" window

- If the event handler is configured as shown in the figure, then when an event with the "Alarm" class is received on the first zone, the handler will be enabled and will replace the class for the received event with "Delayed alarm". If after that the event with the class "Disarming" is not received within 45 seconds, the event with the "Alarm" class will be newly created by the handler and sent to the operator for handling. If the event with the class "Disarming" is received, the handler will stop working until the next event with the class "Alarm" is received.*

The "Alarm event class" parameter specifies the class of the event, which handling is suspended by the operator and Security Center.

Use the "Zone number" parameter to determine the event to be handled accurate within a zone: if this parameter value is not set or equal to zero, then any event, which class coincides with the value of the "Alarm event class" parameter, will be accepted for handling. If the "Zone number" parameter is set to the zone value, only the event with the zone number corresponding to the specified one will be handled.

For the event accepted for handling, the event class is replaced. The value of the "Replacement event class" parameter determines which class the event will have after its handling.

After the "Alarm entering" event handler receives an alarm event and replaces the class for it, it starts the countdown of the wait interval for the event which class is set by the value of the "Disarming" event class. If the event with such a class is not received during the interval specified by the value of the parameter "Disarm wait interval", the handler will create a system event, in which the code, class, zone number and description will be copied from the event, which handling was suspended. Only the date and time of the event will differ - they will correspond to the event time of the handler, and the event receiving channel - the value of this event parameter will be set to "System".

5.3.6 SMS Message Repeater

The "SMS message repeater" handler allows to send information about the received events to a mobile phone in the form of SMS messages.

With the help of the "SMS message repeater" handler, it is possible to provide an additional service to the clients of the security company, for example, informing the responsible persons about the site arming and disarming. Besides, with the help of this handler, it is possible to transmit alarms directly to the mobile phone of the Guard in parallel with the work of the duty operator.

Also, this handler can greatly simplify the commissioning of equipment on the connected sites. If the engineer has a personal number of the site that he/she shall use when checking the equipment at the site, and SMS messages for the events received from this site are sent to his/her mobile phone, it will allow to perform the equipment configuration without the duty operators.

Device for Sending SMS Messages

The event handler can send SMS messages using one of the devices connected directly to the operating computer:

- GSM-modems «iRZ TU31»
- GSM-terminals based on GSM-modem “Siemens MC35” or compatible with it
- GSM-modem “SonyEricsson GM-22”
- GSM-modem «SonyEricsson GR-47»
- Nokia mobile phones

To send SMS messages, special device drivers are used, which are called “transceivers”. Each supported device has an appropriate transceiver, which is intended to connect to the device.

In addition to working with hardware devices, the handler can connect to send SMS messages to the “Phoenix” software or directly to the SMS-server of the mobile operator via SMPP protocol. There are also corresponding transceivers for each of these ways of sending SMS messages.

Settings on the “Device” tab allow to determine the way in which SMS messages will be sent, as well as the necessary parameters.

GSM-modem

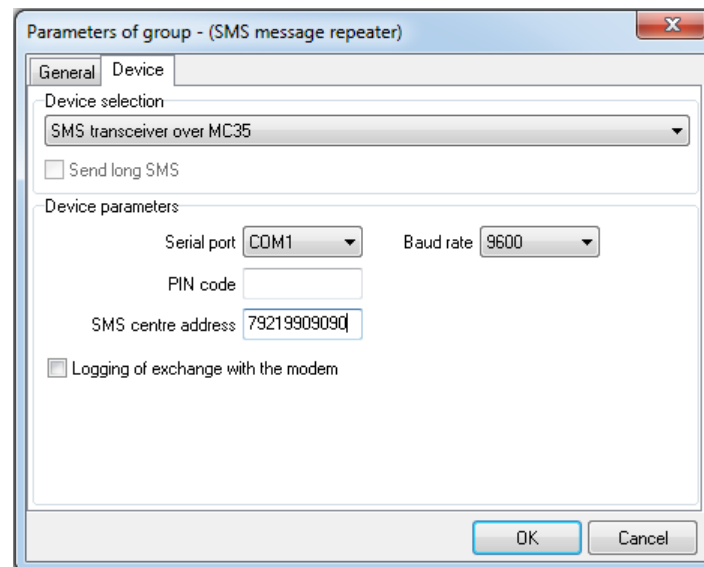


Figure 40: “Parameters of group (SMS message repeater)” window, “Device” tab, parameters of SMS transceiver over modem MC35

Use the “Serial port” parameter to select the serial port to which the GSM-modem is connected, with which SMS messages will be sent, and using the “Baud rate” parameter to set the exchange rate.

If the SIM card installed in the GSM-modem is protected by a personal identification code, it can be set as the value of the “SIM code” parameter. It is strongly recommended not to use SIM cards protected by PIN code to avoid problems associated with the loss of set codes.

The “Service center address” parameter allows to set the phone number of the SMS-center of the mobile operator, which SIM card is installed in the GSM-modem. Some communication operators require that this parameter be set so that the function of sending SMS messages works correctly. The phone number that is used as the value of the “Service center address” parameter shall be specified in full, international format. The symbol “+” shall not be used when specifying this number.

Check “Logging of exchange with the modem” parameter to save the exchange protocol of the event handler with the GSM-modem to the computer hard disk. This information is useful when finding out the causes of problems when connecting to a GSM-modem or sending SMS messages through it. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

The parameters of the transceivers intended for connection to the modems “SonyEricsson GM-22” and “SonyEricsson GR-47” are completely similar to the configuration parameters of the modem “Siemens MC35”.

It shall be noted that several groups of event handlers “SMS message repeater” can use the same GSM-modem for sending SMS messages. Thus, when determining the required number of GSM-modems, take into account only the bandwidth of the used device. For the modem “SonyEricsson GR-47” it is possible to take into account 5-7 SMS messages per minute, and for the modem “Siemens MC35” this value is 10-12 SMS messages per minute.

Phoenix Software

The “Phoenix” software was developed by C.Nord and is intended for organizing a pool of channels for receiving and transmitting SMS messages. It is supplied as part of “Andromeda MS” software and “Andromeda Persona” software. Connection to the “Phoenix” software is carried out over a network that implements the TCP/IP protocol, while a copy of the “Phoenix” software always acts as a TCP/IP server, waiting for connection. The characteristic of the “Phoenix” software is the ability to reserve channels for sending SMS messages, that is why the parameters of the transceiver intended for sending SMS messages over the Phoenix software are divided into two identical groups. One group of parameters is intended for setting the main channel for sending SMS messages, and the second for the backup channel.

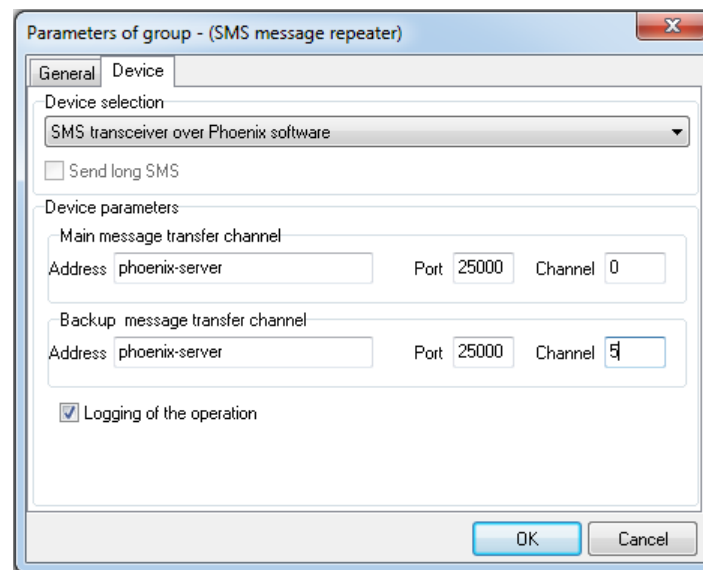


Figure 41: “Parameters of group (SMS message repeater)” window, “Device” tab, parameters of SMS transceiver over Phoenix software

The “Address” parameter is used to specify the NetBIOS name of the computer, on which the instance of the Phoenix software is running, via which it is necessary to send SMS messages. Instead of the NetBIOS name of the computer, it is allowed to specify its IP address. Use the “Port” parameter to specify the port to which you want to connect.

Check “Logging of the operation” parameter to save the exchange protocol of the event handler with the “Phoenix” software to the computer hard disk. This information is useful when finding out the causes of problems when connecting to the “Phoenix” software or sending SMS messages through it. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

Nokia Phones

“SMS transceiver over Nokia phones” is intended for sending SMS messages using some Nokia mobile phone models.

Supported phone models: 1100, 1220, 1260, 1261, 2100, 2270, 2275, 2280, 2285, 2300, 2600, 2650, 3100, 3105, 3108, 3200, 3205, 3210, 3220, 3300, 3310, 3320, 3330, 3350, 3360, 3390, 3395, 3410, 3510, 3510i, 3520, 3530, 3560, 3570, 3585, 3585i, 3586, 3586i, 3587i, 3588i, 3589i, 3590, 3595, 3610, 5100, 5110, 5130, 5140, 5190, 5210, 5510, 6100, 6108, 6110, 6130, 6150, 6190, 6200, 6210, 6220, 6225, 6230, 6250, 6310, 6310i, 6320, 6340, 6340i, 6360, 6370, 6385, 6500, 6510, 6560, 6585, 6590, 6610, 6610i, 6650, 6651, 6800, 6810, 6820, 7110, 7160, 7190, 7200, 7210, 7250, 7250i, 7260, 7600, 8210, 8250, 8290, 8310, 8390, 8810, 8850, 8855, 8890, 8910, 8910i.

Supported methods of connecting mobile phones to computer:

- DAU-9P-compatible cable (FBUS mode);
- DLR-3 cable (DLR-3P) (for the models 6210, 6250, 6310, 6310i, 7110, 7190);
- Infrared port;
- Bluetooth (for models 6310i with firmware version 5.50 and higher, 8910i);
- DKU-5 cable.

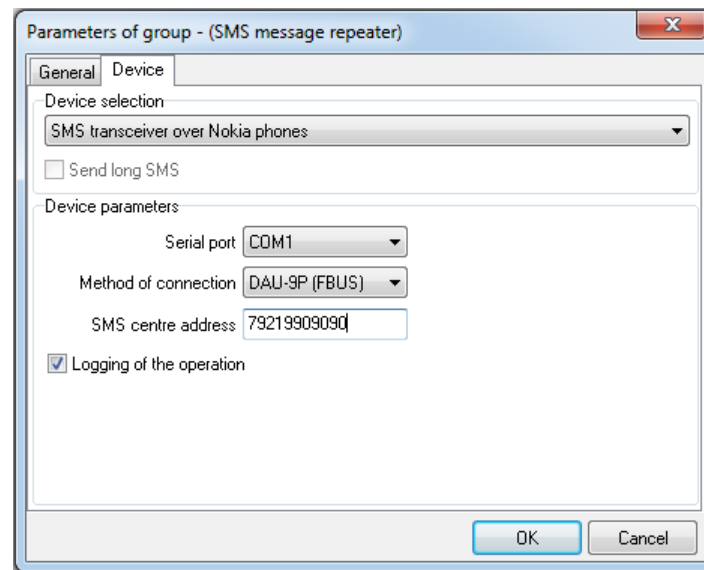


Figure 42: "Parameters of group (SMS message repeater)" window, "Device" tab, parameters of SMS transceiver over Nokia phones

Use the Serial Port option to select the serial port to which the Nokia mobile phone is connected to send SMS messages, and use the "Method of connection" parameter to specify the way that this phone is connected to the computer.

The "Service center address" parameter allows to set the phone number of the SMS-center of the mobile operator, which SIM card is installed in the GSM-modem. Some communication operators require that this parameter be set so that the function of sending SMS messages works correctly. The phone number that is used as the value of the "Service center address" parameter shall be specified in full, international format. The symbol "+" shall not be used when specifying this number.

Check "Logging of the operation" parameter to save the exchange protocol of the event handler with the Nokia phone to the computer hard disk. This information is useful when finding out the causes of problems when connecting to Nokia phone or sending SMS messages through it. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

SMPP Protocol over TCP/IP

"SMS Transceiver over SMPP (TCP/IP)" transmits SMS messages by connecting to SMS-server of the mobile communication operator (SMSC) via SMPP version 3.4. The connection is over a network that supports the TCP/IP protocol.

The “SMSC” tab specifies the parameters required to connect the transceiver to the SMS-server of the mobile operator.

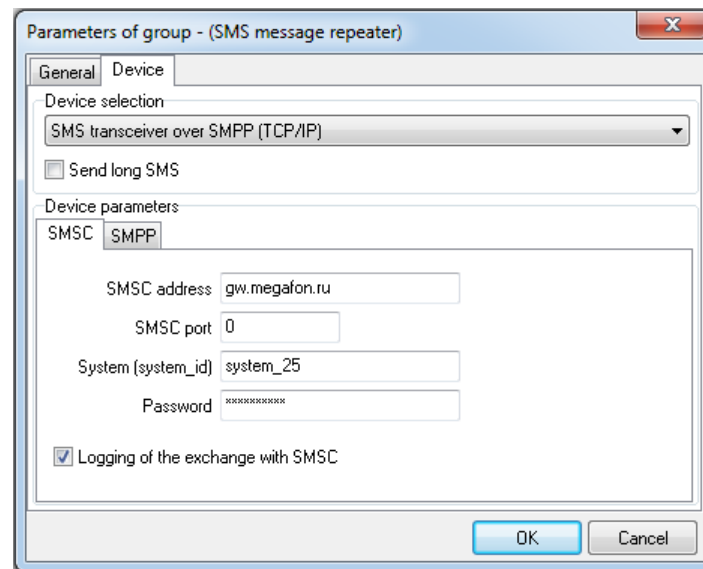


Figure 43: “Parameters of group (SMS message repeater)” window, “Device” tab, parameters of device “SMS transceiver over SMPP (TCP/IP)”, “SMSC” tab

The “SMSC address” parameter allows to set the IP address or DNS name of the computer of the SMS-server of the mobile operator to which you are connecting, and the “SMSC port” parameter allows to specify the TCP/IP port to which it is necessary to connect.

The “System (system_id)” and “Password” parameters are the requisites identifying the system (subscriber) that is connecting to the SMS-server. These requisites are provided by the mobile operator during the preparation of the contract for the organization of connection to their SMS-server.

Check “Logging of the exchange with SMSC” parameter to save the exchange protocol of the event handler with the SMS-server of the mobile communication operator to the computer hard disk. This information is useful when finding out the causes of problems when connecting to the SMS-server of the mobile communication operator or sending SMS messages through it. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

Use the “SMPP” tab to specify the parameters specific to the SMPP protocol. It is recommended to change these parameters only if the mobile communication operator has defined special values for them during the preparation of the contract for the organization of connection to their SMS-server.

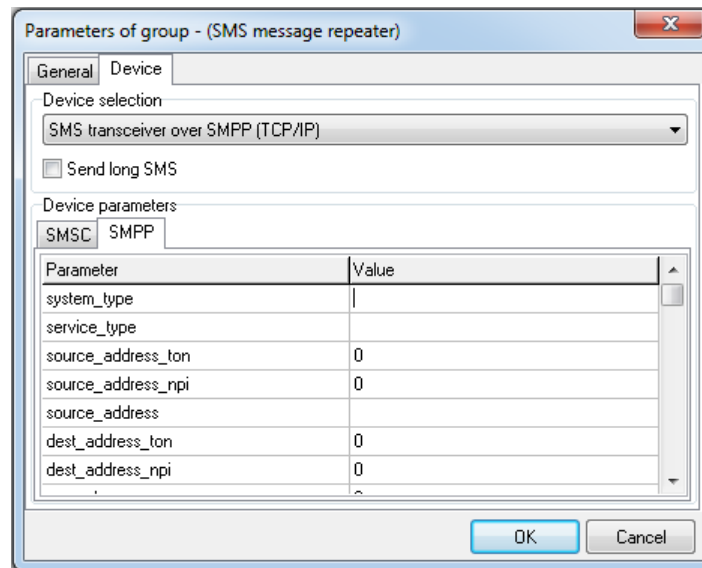


Figure 44: "Parameters of group (SMS message repeater)" window, "Device" tab, parameters of device "SMS transceiver over SMPP (TCP/IP)", "SMPP" tab

The names of all parameters that can be changed on the "SMPP" tab correspond to the fields in the PDU SUBMIT.SM. Detailed description of the parameters and their format can be found in the specification for the SMPP protocol.

"Event Classes" Tab

On the "Event classes" tab, a list of event classes is displayed, upon reception of which the handler will generate SMS message for sending.

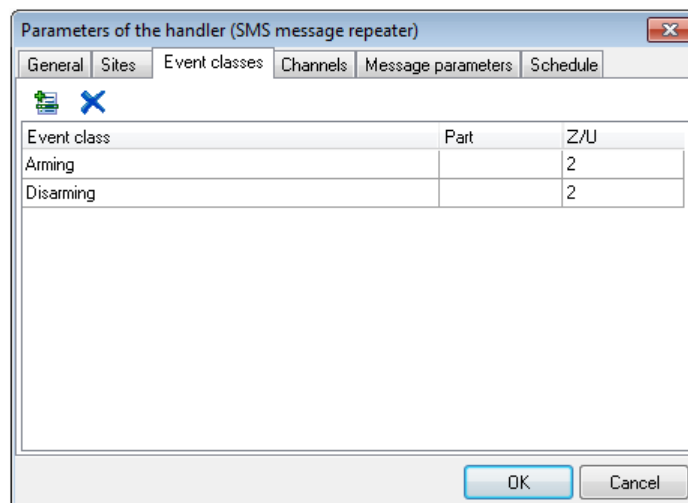


Figure 45: "Parameters of handler (SMS message repeater)" window, "Event classes" tab

For each class of the class in the list it is possible to specify the number of the part, as well as the number of the zone or user - these parameters allow to more accurately determine the events which shall generate SMS messages.

If the value in the "Part" column is not set or equal to zero, then any events, which class corresponds to the one specified in the "Class" column, are handled. If the "Part" column is not set to zero, then SMS messages will be generated only for those events, which part number corresponds to the specified one.

A similar rule applies to the value in the "Z/U" column for specifying the zone number or user that triggered the event.

Use the “Add event class” button to add a new event class to the list of handled event classes.

The “Delete” button is used to delete an event class from the list of the handled events.

“Message Parameters” Tab

Use the “Message parameters” tab to specify the parameters that determine the recipient, as well as the format and content of SMS messages generated by the handler.

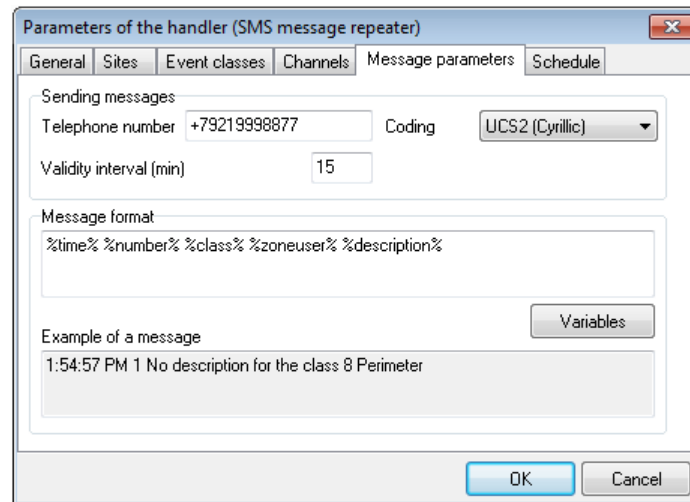


Figure 46: “Parameters of handler (SMS message repeater)” window, “Message parameters” tab

Use the “Telephone number” parameter to set the phone number of the SMS message recipient. When specifying the value for this parameter, it is recommended to specify the phone number in the international format, including the “+” symbol at the beginning of the number.

The “Coding” parameter is used to select the encoding to be used for generating SMS messages. If the value for this parameter is “UCS2 (Cyrillic)”, then the Cyrillic characters that are present in SMS messages will be saved unchanged. If “Translit” is specified as the value for this parameter, the Cyrillic characters in the SMS message will be transliterated, that is, they will be replaced with the corresponding Latin symbols.

It shall be noted that the value of the “Coding” parameter is directly related to the maximum length of the SMS message that can be generated by the event handler: SMS message in the “UCS2” encoding can contain no more than 70 characters, while the maximum length of the message in the “Translit” encoding is 140 characters.

The maximum time during which SMS message is waiting for delivery to the recipient is specified by the parameter “Validity interval”. It shall be noted that this interval is always counted from the moment the SMS message is generated by the handler. Besides, it does not depend on exactly where the SMS message is waiting for delivery to the subscriber: on the waiting list inside the event handler or on the server of the mobile operator: as soon as the validity interval of the SMS message expires, attempts to send it will be stopped.

The “Message format” parameter allows to set a template, according to which SMS messages sent by the handler will be generated. The value corresponding to the fields of the received event, such as the name of the event class or site number, can be substituted into SMS messages using special macros - if a macro is found while handling the message format string, it will be replaced with the value of the corresponding event field.

List of macros supported by the event handler:

- %date% - date of event reception;
- %time% - time of event reception;
- %number% - site number;
- %name% - site name;

- %address% - site address;
- %phone% - site phone numbers;
- %channel% - name of channel via which event was received;
- %code% - event code;
- %lass% - event class name;
- %zoneuser% - number of zone or user that generated event;
- %description% - event description.

Click on the “Variables” button to display the menu, from which to select the contents of the macro that will be added to the value of the “Message format” parameter. Thus, it is not necessary to remember the correct spelling of the desired macro, but simply select it in the list and add it to the format string.

5.3.7 Site Reclosing

The “Site reclosing” handler is intended for informing the responsible persons about site reclosing via SMS messages. With the help of this handler, the responsible persons are informed about the need to reclose the site and about the failure of the responsible persons to reclose.

If it is necessary to reclose the site, the event handler sends SMS message to all the responsible persons, who shall be notified about the need to reclose according to the settings in the “Site manager” module. SMS message is created in the format specified in the “Message parameters” tab of the “Parameters of handler” window. By default, the message about the need to reclose the site contains the site number, name and address.

If the responsible person refuses to reclose the site, the event handler sends SMS message to all responsible persons, who shall be notified about the need to reclose according to the settings in the “Site manager” module. SMS message is created in the format specified in the “Message parameters” tab of the “Parameters of handler” window. By default, the message about the refusal to reclose the site contains the surname and initials of the responsible person, as well as the site number, name and address.

Device for Sending SMS Messages

GSM-modem

The event handler can send SMS messages using the GSM-terminal based on the GSM-modem “Siemens MC35” (or compatible with it). The modem shall be connected directly to the computer with the event handler.

See details on sending SMS messages using the GSM-modem in the chapter on the “SMS message repeater” event handler.

SMPP Protocol over TCP/IP

To send SMS messages it is possible to use the connection to the SMS-server using the SMPP (TCP/IP) protocol.

See details on sending SMS messages over SMPP protocol in the chapter on the “SMS message repeater” event handler.

“Message Parameters” Tab

The “Message parameters” tab of the “Site reclosing” handler is similar to the “SMS message repeater” handler tab of the same name: the parameters defining the format and content of SMS messages generated by the handler are also set here. However, such parameter as “Telephone number” is not specified for the “Site reclosing” event handler. The mobile number of the responsible person is used as the phone number to which the SMS message shall be sent.

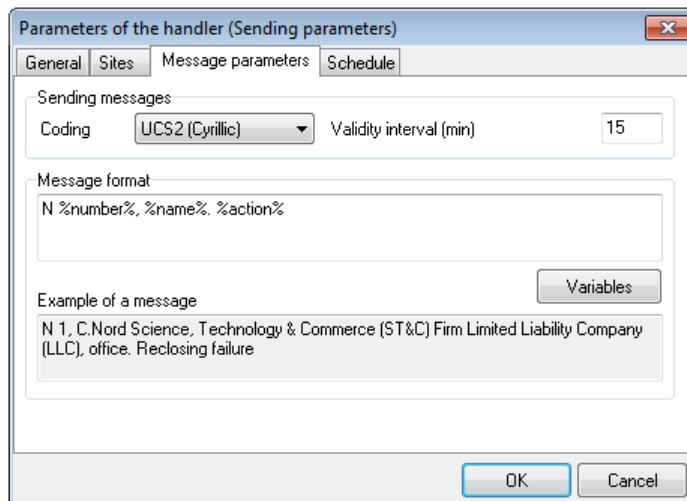


Figure 47: “Site reclosing”, “Parameters of handler (Sending parameters)” window, “Message parameters” tab

See details on other message parameters in the chapter on the “SMS message repeater” event handler.

5.3.8 Pandora Network

The main task of the “Pandora Network” event handler is to organize the information exchange between independent instances of the Security Center software. Events, operator actions and site descriptions can be transmitted from one Security Center to another.

Any channel that supports the TCP/IP protocol can be used as an information transfer channel.

It is possible to precisely describe the amount of information that will be transmitted in the settings of the event handler. For example, it is possible to specify the numbers and intervals of the site numbers, events from which they will be transmitted, event classes required for the transfer, select the actions of the operators, which shall be transmitted. Reciprocal (simultaneous) transmission of information is possible.

First of all, the event handler is used when creating distributed monitoring systems - when several central monitoring panels are combined and it is necessary to collect operational information in a single unified dispatch center.

Parameters of Group

In the settings of the “Pandora network” event handler group it is possible to specify the settings for connection and information transmission, as well as the settings that are applied during handling of the received information.

“Site Numbers” Tab

On the “Site numbers” tab it is possible to specify a list of sites, information on which will be received by the group of handlers, as well as the values of the site number shift.

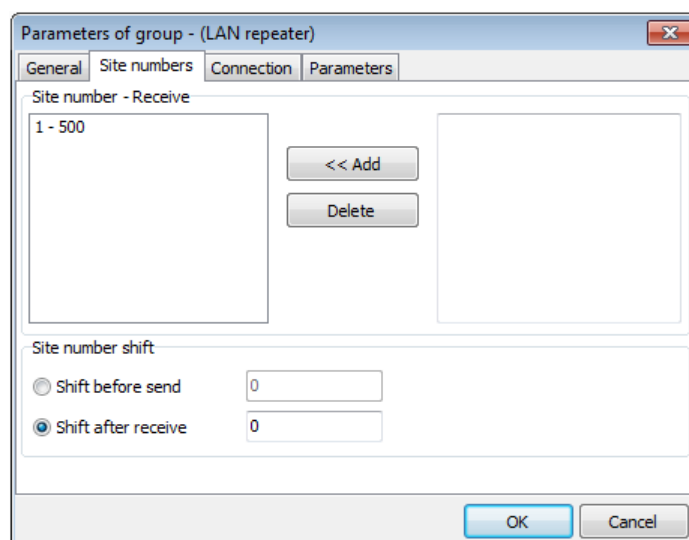


Figure 48: "Parameters of group (Pandora network)" window, "Site Numbers" tab

The "Site number - receive" field is intended for indicating the numbers and intervals of site numbers, information on which will be accepted by the event handler.

To add a number or an interval of site numbers to the list of received ones, it is necessary to enter it in the input field in the right part of the field and click on the "Add" button. To delete a number or an interval of site numbers from the list of received ones, select the line with the value that you want to delete in the list on the left of the field and click on the "Delete" button.

When entering site numbers, it is allowed to enumerate several numbers or numbers and intervals of numbers separated by commas, for example: "100, 102, 104, 106-100, 200-299".

It shall be understood that "site information" means any information transmitted by the "Pandora network" handler: events, site cards, operator actions for alarms. Thus, if it is assumed that the "Pandora network" event handler receives information, then the site numbers, on which information is received, shall be indicated in the "Site number - receive" field.

The "Shift before send" parameter specifies the value of the summand that will be added to the site number, before sending information about the site.

The "Shift after receive" parameter specifies the value of the summand that will be added to the site number, after receiving information about the site.

Negative values can be specified for the "Shift before send" and "Shift after receive" parameters.

The use of site number shifts is especially useful if several central monitoring panels with the same number of protected sites are connected to the unified handling center using the "Pandora network" event handler. In this case, it is necessary to select the appropriate number shift for each panel, for example -10000, 20000, and 30 000, and thus to avoid conflict.

"Connection" Tab

Use the "Connection" tab to specify the connection settings between instances of the "Pandora network" handlers.

Since the "Pandora network" handler uses a TCP/IP network as the communication channel, then to establish connection between the two handler instances, one of them shall act as a server, and the other as a client.

The role in which the handler will act when the connection is made is set by the "Connection initialization mode" parameter.

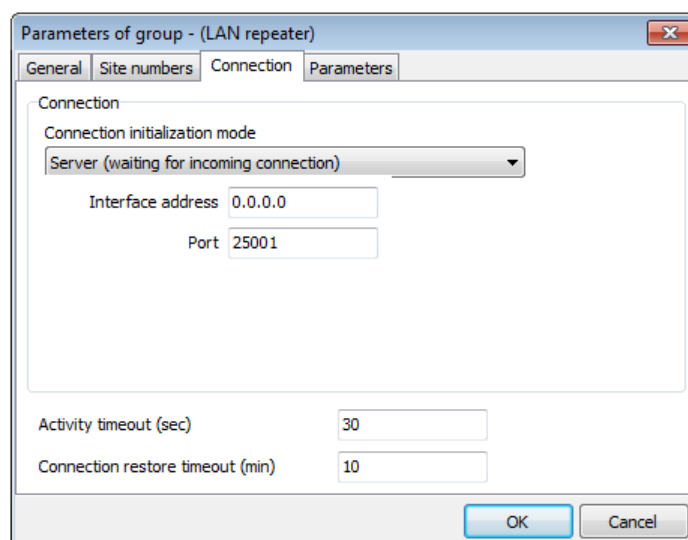


Figure 49: "Parameters of group (Pandora network)" window, "Connection" tab, "Server" mode

If the event handler acts as a server and several network adapters are used with the computer, or if one adapter uses several IP addresses, then using the "Interface address" parameter it is possible to specify the IP address on which the event handler shall wait for the incoming connection. The "Server port" parameter is used to specify the port to which the connection will be expected.

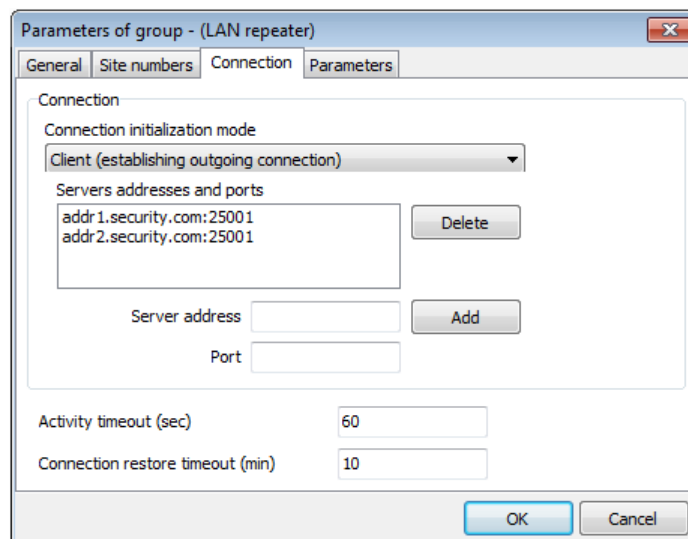


Figure 50: "Parameters of group (Pandora network)" window, "Connection" tab, "Client" mode

If the event handler acts as a client, it is necessary to specify the server address and port to which it is necessary to establish a connection.

It shall be noted that for the "Pandora network" event handler acting as a client, it is possible to specify several server addresses: in the event if it is not possible to establish a connection with the first address in the list, the handler will attempt to connect to the next one and so on.

To add the server address and port to the list, it is necessary to specify them as values for the "Server address" and "Port" parameters and click on the "Add" button.

To remove the server, it is necessary to select it in the server list and click on the "Delete" button.

To monitor the presence of a connection in the absence of information for transmission, the "Pandora network" handler can generate test packets and monitor their reception. In doing so, the test packages are created by the handler, acting as a server, and their reception is monitored by the handler, acting as a client.

The “Activity timeout” parameter is intended for controlling the period of connection monitoring in the absence of information for transmission. If the handler acts as a server, this parameter specifies the interval with which the handler forms the test packet. If the handler acts as a client, the “Activity timeout” parameter specifies the interval during which any packet, including a test packet, shall be received from the server. If there are no packets from the server during the interval specified in the “Activity timeout” parameter, the handler that acts as a client closes the connection.

When configuring the “Pandora network” event handler, it is necessary to select the value for the “Activity timeout” parameter based on the bandwidth of the communication channel and its operation cost. In general, for a handler acting as a client, it is recommended to set the value of the “Activity timeout” parameter approximately two and a half times more than for the handler acting as a server. As for the value of the “Activity timeout” parameter for the handler acting as a server, the recommended value for it shall be within the range of 30-300 seconds.

When connection is established via a communication channel, the “Pandora network” event handler creates a system event with the “ZZYC” code. If connection is lost, a system event with the “ZZYB” code is created. If the value of the “Connection restore timeout” parameter is not equal to zero, then in case of long-term absence of connection, system events with the “ZZYB” code will be created with the period specified by this parameter value.

“Parameters” Tab

Use “Parameters” tab to set the parameters to control reception and transmission of information via communication channel.

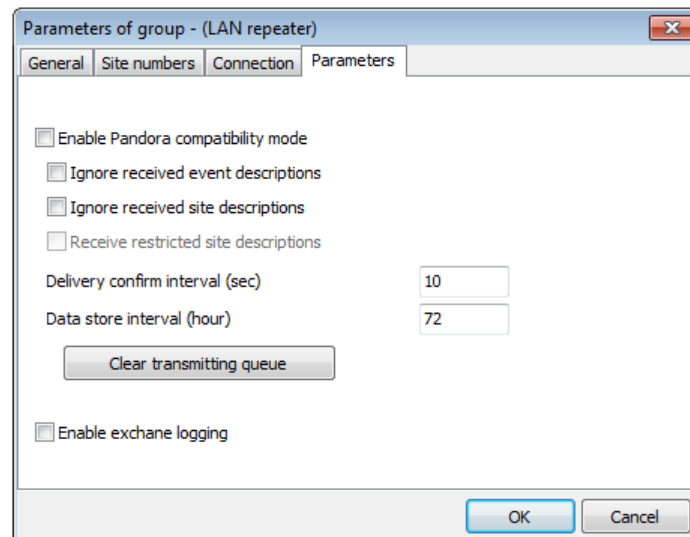


Figure 51: “Parameters of group (Pandora network)” window, “Parameters” tab

If the “Enable Pandora compatibility mode” parameter is selected, then the event handler will use an outdated protocol compatible with the “Pandora” and “Andromeda - Remote Operator” software for the information exchange. This protocol has a number of shortcomings, in particular, it does not guarantee the delivery of information to the recipient. It is strongly recommended not to enable the compatibility mode with “Pandora” when establishing a communication channel between two “Pandora network” handlers.

Use the “Ignore received event descriptions” parameter to control the reception of event descriptions. If this parameter is not selected, decoding is not performed for the events received via the communication channel: event class, part and zone numbers, and description are stored as received. If this parameter is selected, then only the channel and code will be taken from the received event, after which it will be decoded according to the event template set for the site as if it were received from a local event source.

The “Ignore received site descriptions” parameter allows to disable reception via the communication channel and storing in the database of site cards. If this parameter is selected, the site descriptions, that are sent along with the events, as well as their changes on the remote instance of the Security Center, are ignored. If this parameter is not selected, the descriptions of sites, information about which is transmitted via the communication channel, will be synchronized.

If the “Enable Pandora compatibility mode” parameter is not selected, then the “Pandora network” handler guarantees the delivery of information to the recipient. This is achieved with the help of confirmations that are sent from the recipient after the information it has received is registered in the Security Center database. Use the “Delivery confirm interval” parameter to specify the time during which the “Pandora network” handler waits for confirmation from the recipient. If no confirmation is received during the specified interval, then the “Pandora network” handler will send the information, which is not confirmed, again.

The value of the “Delivery confirm interval” parameter depends on the bandwidth of the communication channel used by the “Pandora network” handler and the performance of the computers on which the “Event manager” module is running. For example, if GPRS is used as the communication channel, in order to avoid an avalanche increase in the amount of information in the transmission queue, it is recommended to increase the value of the “Delivery confirm interval” parameter to 90 seconds.

If there is no connection, the “Pandora network” handler accumulates the information in the transmission queue, and after the connection is restored it transfers the information accumulated in the queue. Use the “Data store interval” parameter to control the volume and relevance of the data that are accumulated in the transmission queue. If the period of data storage in the transmission queue is greater than the value of this parameter, then such data will be automatically deleted from the transmission queue. Besides, if the bandwidth of the communication channel has deteriorated and there are data in the queue that cannot be transmitted, click on the “Clear transmitting queue” button to forcefully delete all data accumulated in the queue for transmission at the moment.

Check “Enable exchange logging” parameter to save the exchange protocol of the event handler via TCP/IP network to the computer hard disk. This information is useful when finding out the causes of problems when setting up a connection or sending information via the communication channel. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

“Event Classes” Tab

Use the “Event classes” tab to select event classes to be transmitted by the handler.

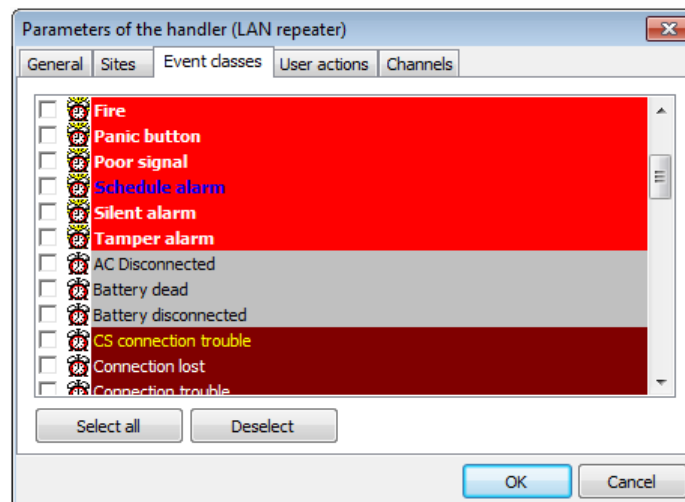


Figure 52: “Parameters of handler (LAN repeater)” window, “Event classes” tab

To select the event class for transmission, check it in the list. Use the “Select All” button to check all event classes in the list. Use the “Deselect” button to deselect all classes in the list that are currently selected for transmission.

“User actions” Tab

Use the “User actions” tab to select the operator actions and cancel the alarms that will be transmitted by the handler. It shall be noted that the actions and cancels that are transmitted by the handler shall relate to those alarms which classes are checked on the “Event classes” tab.

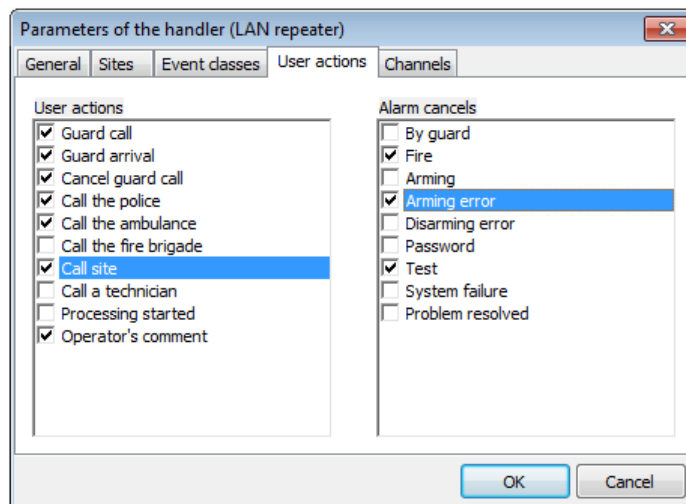


Figure 53: "Parameters of handler (LAN repeater)" window, "User actions" tab

To select the action or cancel for transmission, check them in the list.

5.3.9 Repeater to Cloud

This event handler is intended to transmit information about the Security Center, sites, received events, guards and operator actions, engineers and their permissions, as well as about the video routers installed on the site, to the "Cloud". The "Cloud" is a service that allows to provide web-access to sites and events for owners, installation organizations, operators, and guards.

The "Repeater to Cloud" handler provides operation of such additional services as remote control of the site equipment, mobile Application "MyAlarm" and some others. In more detail, all these services are described in the "Cloud Services" section.

The operation of this handler is important for the proper functioning of all cloud services, that is why editing it is very limited. The "Repeater to Cloud" event handler group and the handler in it are created during the first start of the "Event manager" module and are enabled automatically if the "Cloud Communication" dialog box indicates the need to use cloud services.

Deletion, copying or creating another "Repeater to Cloud" handler is prohibited. It is necessary to change the parameters of connection to the "Cloud" only if "Private Cloud" is used.

"Common" Tab

General settings of the "Repeater to Cloud" event handler group completely coincide with the general settings of the event handler groups, which are discussed in detail above. When a group is created, it is automatically set to "Hidden group".

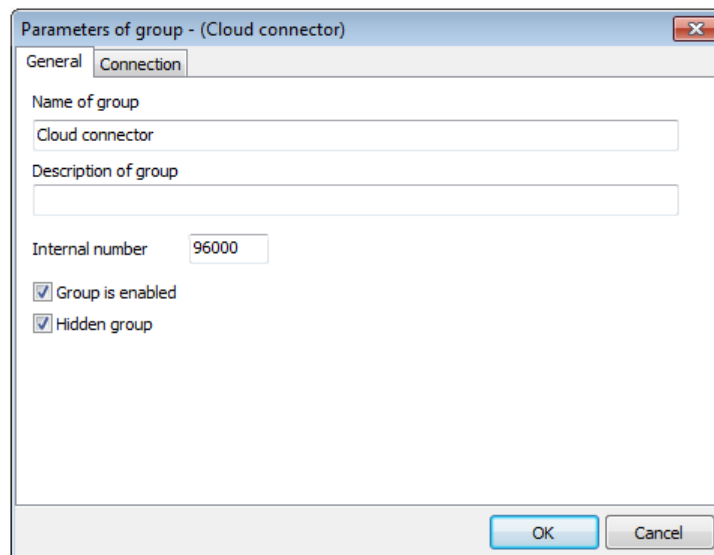


Figure 54: "Parameters of handler (Repeater to Cloud)" window, "Common" tab

"Channel" tab

The "Channel" tab displays the server address and port, which are used for connection to the "Cloud". To connect to the "Cloud" use the following settings: server address - disp.cnord.net, server port - 1025. It is necessary to change the parameters only if "Private Cloud" is used.

Check "Enable exchange logging" parameter to save the exchange protocol of the event handler to the computer hard disk. This information is useful when finding out the causes of problems when setting up a connection or sending information. It is not recommended to include the exchange logging independently, without a request from the technical support service of C.Nord.

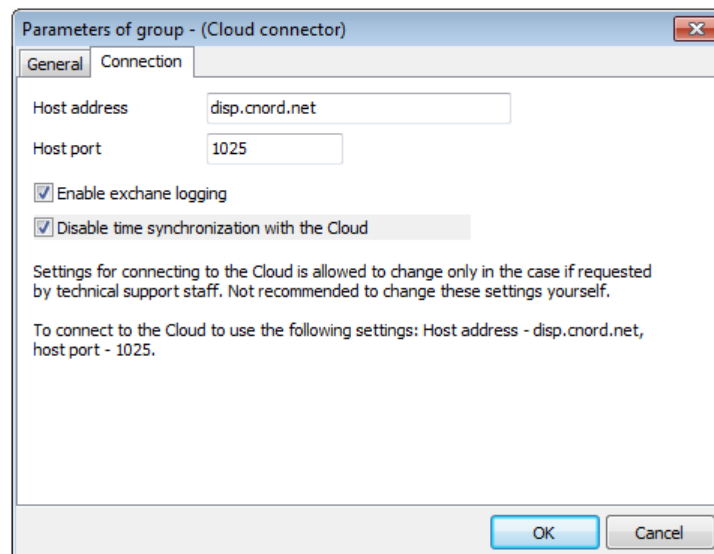


Figure 55: "Parameters of handler (Repeater to Cloud)" window, "Channel" tab

If the user wants to avoid sending unnecessary information to the "Cloud", the user can choose the cloud services that he/she will use, and also ensure that only the information necessary for the selected services is sent to the "Cloud".

To limit the information transmission to the "Cloud" select "Connection to the Cloud" in the Event Manager.

5.4 Connection to the Cloud

When “Connection to the Cloud” option is selected, the drop-down menu of the same name appears in the “Event Manager”.

The “Cloud” icon appears in the status bar of the window. The icon color changes depending on the success of the connection to the Cloud and number of messages in the transmission queue. If the connection to the Cloud is established and the number of messages in the transmission queue does not exceed 100, the Cloud will be green. Otherwise - red.

Besides, the status of the connection to the Cloud is displayed in the “Communication with the Cloud” line, and the number of messages in the transmission queue in the “Messages in the queue” line.

There are three tabs in the window “Connection to the Cloud”: “Connection mode”, “Contact Information”, and “UID of Security Center”.

5.4.1 Connection mode

Select one of the cloud connection modes on the “Connection mode” tab of the “Connection to the Cloud” window. The mode selection determines the cloud services that will be used and the data that will be transmitted to the Cloud.

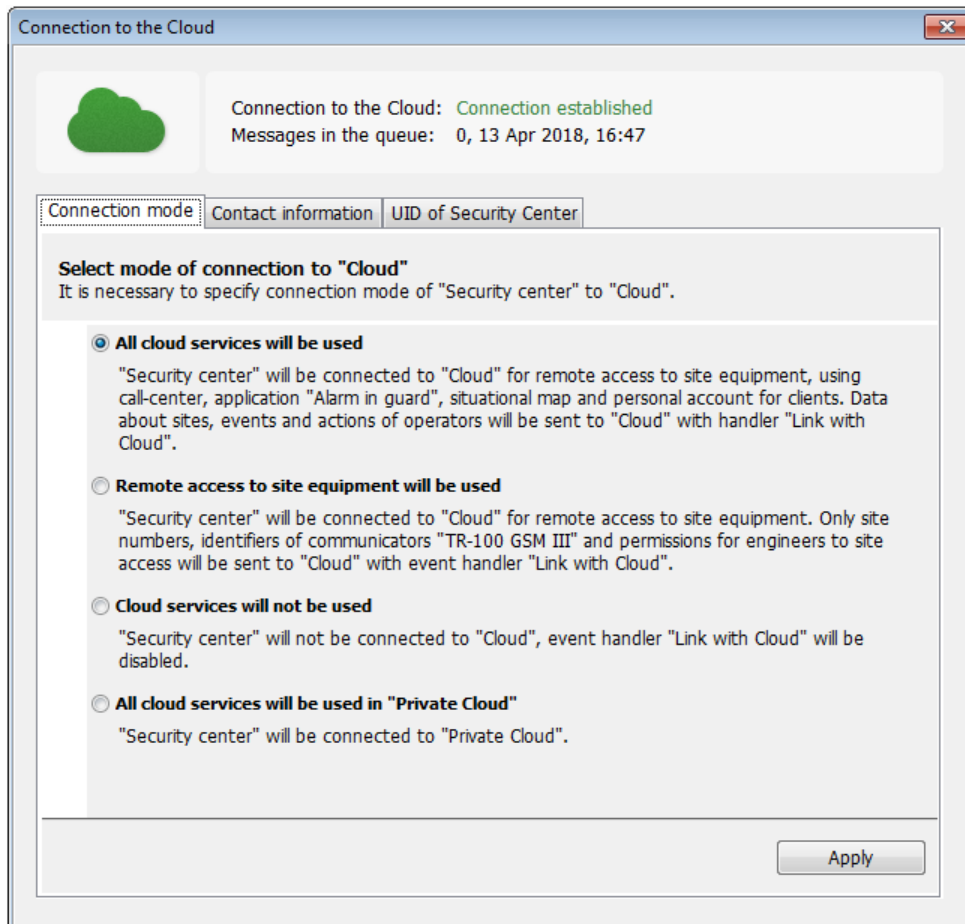


Figure 56: “Connection to the Cloud” window, “Connection mode” tab

Full integration with the Cloud allows to use remote access to site equipment, as well as available cloud services. In this case, all data about sites, events and actions of operators will be transmitted to the “Cloud”.

Connection to the Cloud can only be used for remote access to the site equipment. This connection mode allows to

send only site numbers, communicator identifiers and permissions for engineers to access sites to the Cloud. Other Cloud services will be disabled and information on them will not be transmitted to the Cloud.

It is also possible to disable all cloud services and prohibit the transmission of any data to the Cloud. All services related to the use of the “Cloud” will be unavailable. The “Repeater to Cloud” event handler will be forcibly disabled and cannot be enabled. Access to the registration information and UID of Security Center will not be possible.

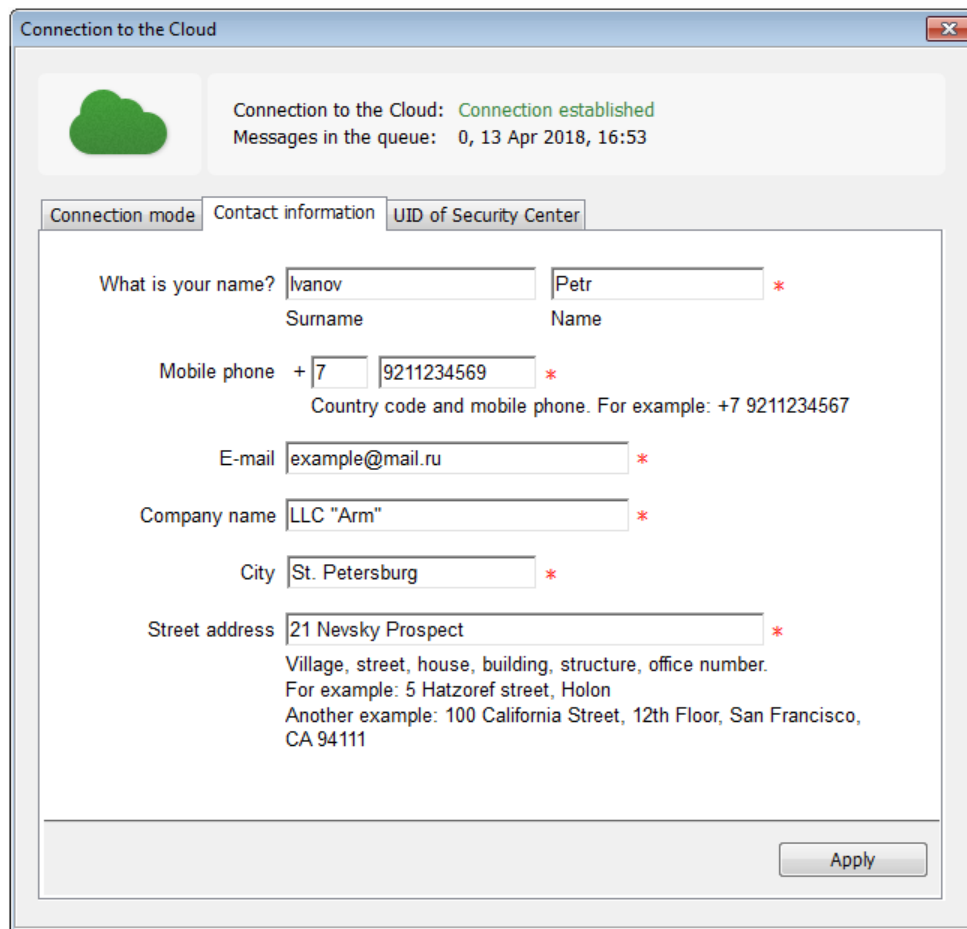
It is also possible to use cloud services in the “Private Cloud”, by selecting the appropriate connection. This provides an increased level of information security due to installation of the software directly on the servers of a private security company. It is possible to specify the address of the “Private Cloud” manager for the “Repeater to Cloud” handler group on the “Channel” tab of the “Parameters of group” window.

5.4.2 Contact information

The “Contact information” tab allows to change the data specified when registering the Security Center in the Cloud.

Use the tab to fill in such fields as “Surname”, “Name”, “Mobile phone”, “E-mail”, “Company name”, “City” and “Street address”. Fields marked with an asterisk are required.

After changing the data, click the “Apply” button. In this case, the information entered will be transmitted to the Cloud.



The screenshot shows a window titled "Connection to the Cloud" with a green cloud icon. At the top, it displays "Connection to the Cloud: Connection established" and "Messages in the queue: 0, 13 Apr 2018, 16:53". Below this are three tabs: "Connection mode", "Contact information" (which is selected), and "UID of Security Center". The "Contact information" tab contains several input fields, each followed by a red asterisk indicating it is required:

- What is your name?** with two sub-fields: "Surname" (containing "Ivanov") and "Name" (containing "Petr").
- Mobile phone** with a country code field (containing "7") and a phone number field (containing "9211234569"). Below this is a note: "Country code and mobile phone. For example: +7 9211234567".
- E-mail** (containing "example@mail.ru").
- Company name** (containing "LLC 'Arm'").
- City** (containing "St. Petersburg").
- Street address** (containing "21 Nevsky Prospect"). Below this is a note: "Village, street, house, building, structure, office number. For example: 5 Hatzoref street, Holon. Another example: 100 California Street, 12th Floor, San Francisco, CA 94111".

An "Apply" button is located at the bottom right of the form area.

Figure 57: "Connection to the Cloud" window, "Contact information" tab

5.4.3 UID of Security Center

It is possible to find out the UID of the used Security Center on the “UID of Security Center” tab. To copy UID select it and click on the “Copy” icon. This is convenient, for example, for the subsequent use of UID when registering a partner account.

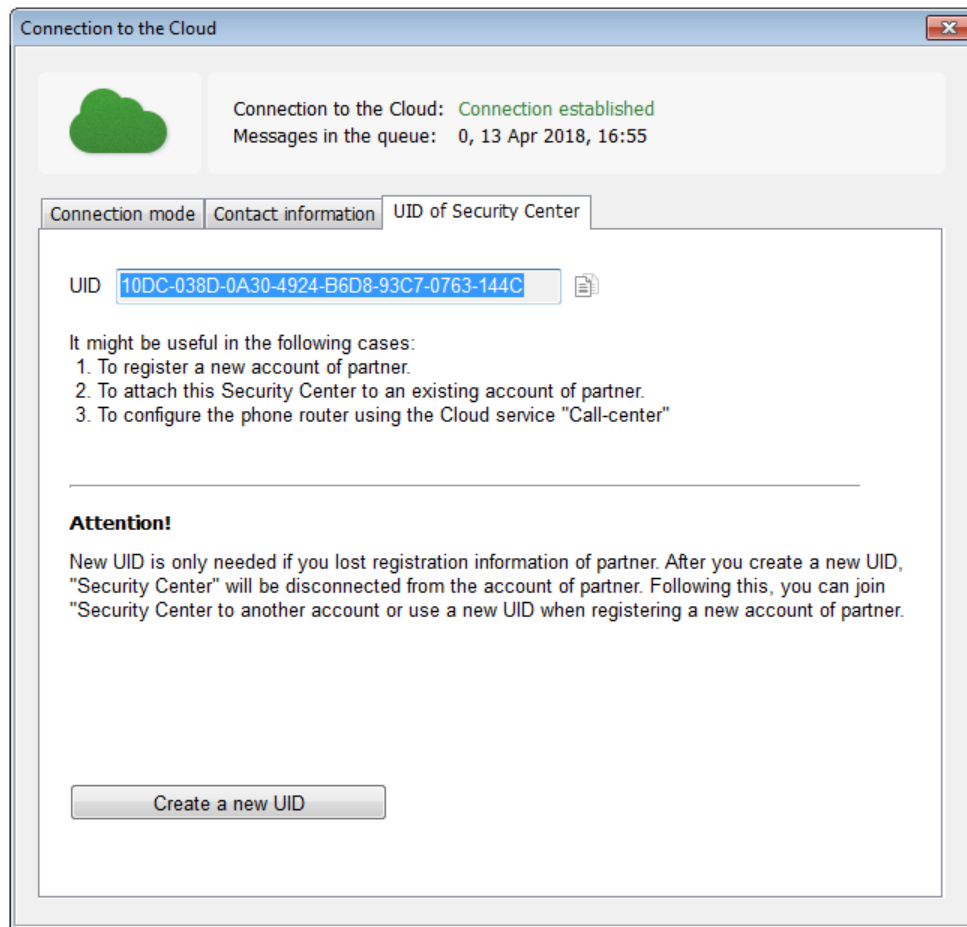


Figure 58: "Connection to the Cloud" window, "UID of Security Center" tab

If it is necessary to re-register the partner account, create a new UID. To do this, click on the “Create a new UID” button. Use the new UID to add this Security Center to another account or create a new partner account. It is allowed to create a new UID no more than once a day.

5.5 About software

When “About software” option is selected, the drop-down menu of the same name appears in the “Event Manager”. It provides information on the version of the Security Center software, as well as information on the operation mode. The Security Center can be used with a security key, temporary license or on a lease basis.

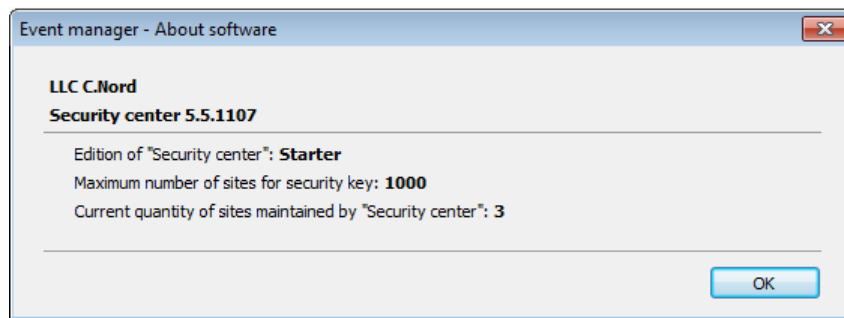


Figure 59: "About software" window

If the security key or license is used, the following is indicated in the "About software" window:

- the Security Center edition;
- maximum number of sites allowed to use;
- current number of sites maintained by the Security Center.

If the Security Center is used with a security key, information on the security key is also displayed in the "About software" window.

If the software is used with a license file, then information on the license is indicated here, as well as the date of its completion.

6 Site Manager

The "Site manager" module is intended to manage the description of sites available in the Security Center software.

To launch the "Site manager" module, the user shall have the "Log in" permission for this module.

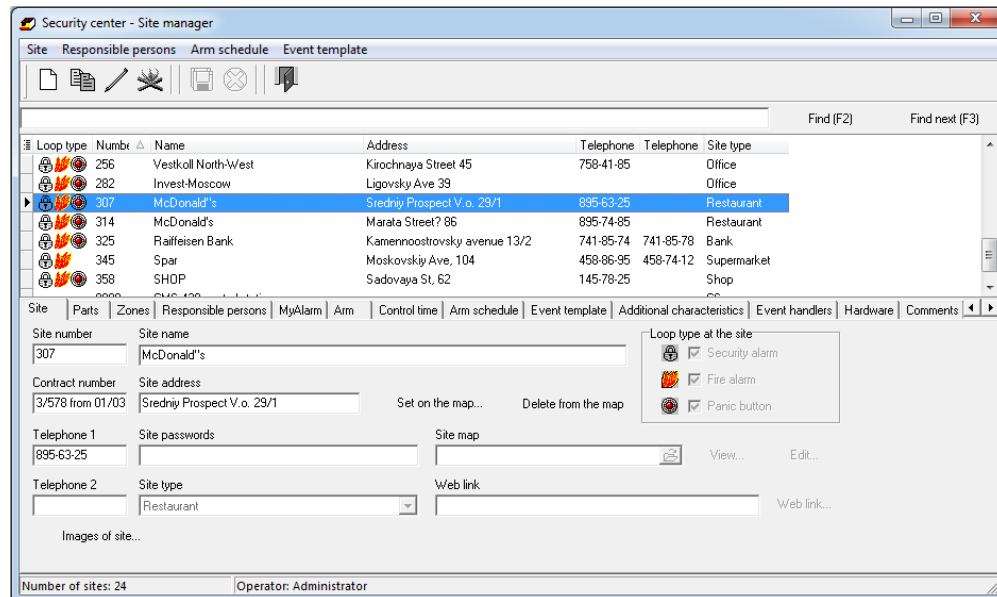


Figure 60: Module main window

[[id-05-01]

The main window of the "Site manager" module displays a list of Security Center sites and a card of the current (selected) site. To perform any operation with the site, select the appropriate item in the menu. The most requested

menu items are duplicated in the control panel of the module and control panels on the tabs on which the fields of the site card are grouped.

6.1 Control Panel



Figure 61: Control Panel

The operations, which are controlled by buttons on the control panel (listed in the order of the buttons):

- Use the “Create site” button to create a new site. The newly created site is assigned the first free site number, which can be changed later.
- The “Copy site” button is intended to create a new site and copy all information from the current (selected) site to it, except for the site number and site number of parts, if any.

For the number of the created site and for the site number of parts, the first available numbers are used, which can be changed when the site is subsequently edited.

- After clicking on the “Edit site” button, the “Site manager” module will switch to the editing mode of the current site card. In the editing mode, it is possible to change the value of the site card fields.

While in the editing mode it is not allowed to select another site from the list of sites - it is necessary to finish editing beforehand, saving the changes made or discarding them.

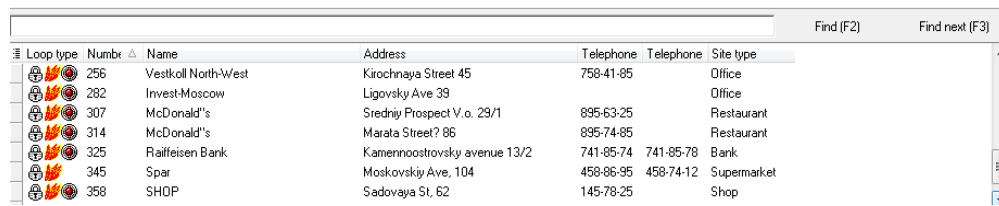
To switch to the editing mode of the site card, the user shall have the “Edit sites” permission for the “Site manager” module. If this is not specified specifically, then this permission is sufficient to make changes to most fields of the site card.

- To delete a site use the button of the same name. When a site is deleted, all information associated with this site is deleted, including description of its parts, zones, responsible persons, etc.

If there is a possibility that the information about the site to be deleted may be needed, it is recommended that the site is not deleted, but instead it shall be changed to the number using a shift to the area of obviously unused site numbers. For example, if site 567 is no longer protected, but the information in the site card or reports on received events may still be needed, it is possible to change the number using the shift of 990000, that is, the new site number will be 990567. To hide such sites from the duty operator, it is possible to use the mechanism of dividing the numbers of sites on computers. See more information about setting up this mechanism, in the chapter on the module “Personnel manager”, section “Computers”.

- The “Save changes” button is only available in site editing mode. Press this button to save all changes to the site card that were made while editing, after which you will exit the editing mode.
- As well as the previous button, the “Undo changes” button is available only in site editing mode. Press this button to cancel all changes made during the site editing, after which you will exit from the editing mode.
- Click on the “Exit program” button to exit the “Site manager” module

6.2 List of Sites



Loop type	Number	Name	Address	Telephone	Telephone	Site type
	256	Vestkoll North-West	Kirochnaya Street 45	758-41-85		Office
	282	Invest-Moscow	Ligovsky Ave 39			Office
	307	McDonald's	Sredniy Prospekt V.o. 23/1	895-63-25		Restaurant
	314	McDonald's	Marata Street? 86	895-74-85		Restaurant
	325	Raiffeisen Bank	Kamennoostrovsky avenue 13/2	741-85-74	741-85-78	Bank
	345	Spar	Moskovskiy Ave, 104	458-86-95	458-74-12	Supermarket
	358	SHOP	Sadovaya St, 62	145-78-25		Shop

Figure 62: List of sites

The main purpose of the list of sites in the “Site manager” module is to find and select a site, information about which shall be viewed or changed.

Search for the site is done using the search bar at the top of the site list. Enter a substring in the input field, then click on the “Start” button to start the search from the beginning of the displayed list of sites. If it is necessary to continue the search, starting with the currently selected site, then click on the “Continue” button. If a site satisfying the search condition is found in the list, it will be selected - it will become the current one. The search for a given substring is performed in all frequently used fields of the site card, such as “Site number”, “Site name”, “Site address”, etc.

6.2.1 Selection of Displayed Columns

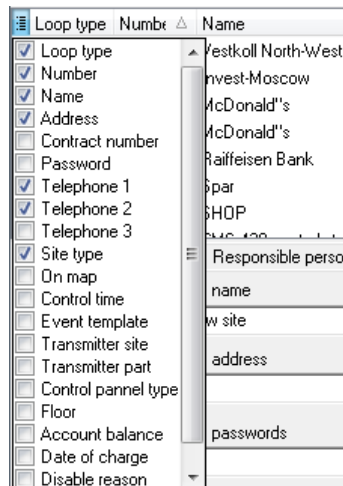


Figure 63: List of sites: selection of displayed columns

It shall be noted that it is possible to select the columns that shall be displayed in the list of sites. To do this, left-click on the special button located in the upper left corner of the list of sites and check the necessary columns in the list that appears.

6.2.2 Sorting of Sites

Sites in the list can be sorted by any of the displayed columns. To do this, left-click on the necessary column. In the header of the column on which the sorting is performed, an icon is displayed, which is a sorting indication, also it specifies the sorting order - ascending or descending. If it is necessary to sort in the reverse order, click on the same column again.

It is possible to sort by several columns. To do this, click on the column header, sorting by which you want to add, and hold down the Control button on the keyboard at the same time.

6.2.3 Filtering of Sites during Display

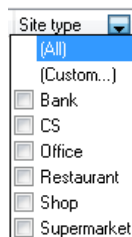


Figure 64: List of sites: filtering button

Another useful function of the list of sites is filtering by a given characteristic. For example, if it is necessary to display only sites of the “store” type, click on the arrow that appears in the column header when the mouse cursor appears over it and select the type of site in the drop-down list.

Or, for example, to make sure that only sites with the word “Dixie” are displayed in the list. To do this, click on the filtering settings arrow on the column and select the “Filter ...” item. In the window it is necessary to choose the comparison rule, let it be “equal”, and enter the reference for comparison - “Dixie”.

Special filtering flexibility is achieved due to the comparison rule “similar to”. Using the rule it is possible to filter the list of sites, ignoring minor discrepancies in the values of fields: to do this, a special symbol “%” can be used in the reference value, indicating the comparison procedure, that instead of it any substring can appear, including an empty one.

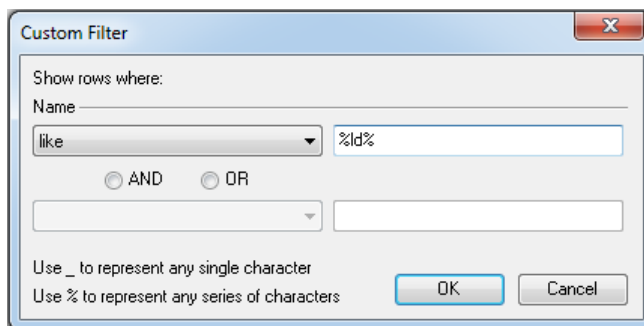
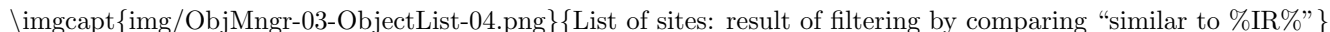


Figure 65: List of sites: filtering settings window

The figure shows the result of filtering by comparison using the rule “similar to %id%”.



6.3 Restoring of Deleted Site

To see the card of the deleted site of the Security Center or generate a report on the events at the deleted site, use the function of restoring a deleted site.

To restore a deleted site, the Security Center operator, who has the appropriate permission, shall select “Restore deleted site...” of the “Site” item in the menu of the “Site manager” module.

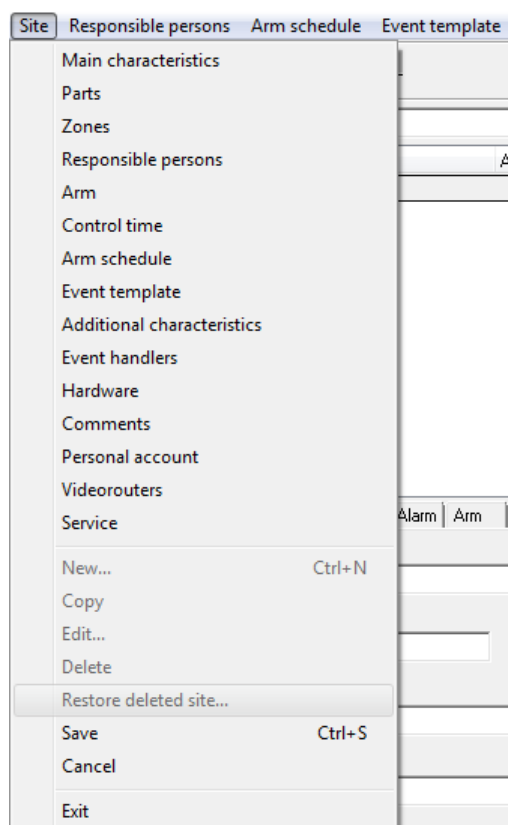


Figure 66: Restore deleted site

The “Select site to restore” window that opens displays the sites that were deleted earlier. For each of them, the number of sites (at the time of the first deletion of the site), name and address of the site, contract number, as well as date and time of deletion of the site are indicated in the corresponding fields. It is convenient to search the site to be restored using these parameters by sorting and filtering sites by a specified characteristic.

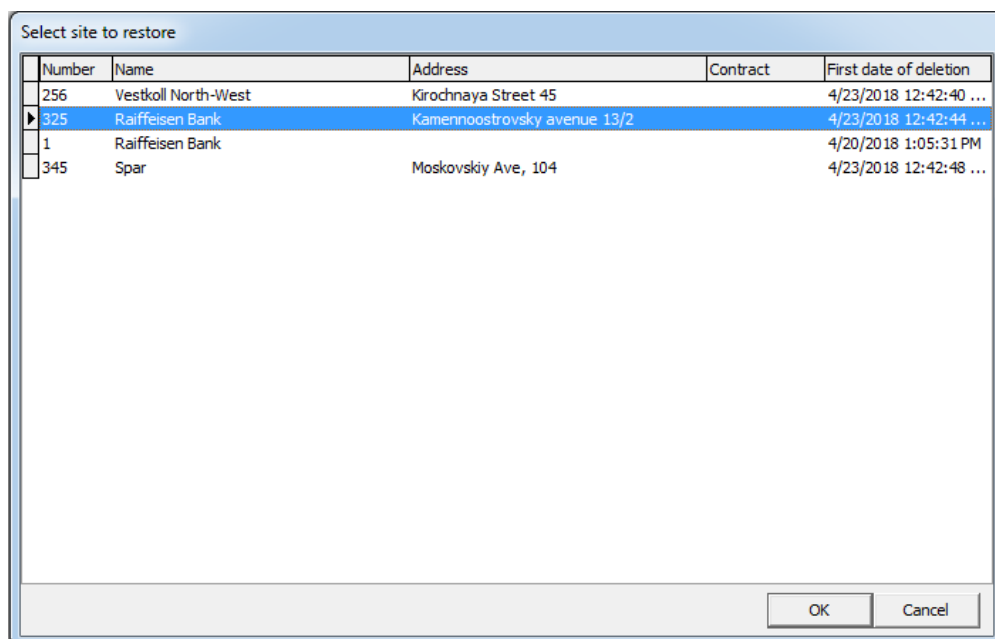


Figure 67: Select site to restore

To restore, select the site in the “Select site to restore” window and click the “OK” button. After that, the site will

be restored and displayed in the list of sites in the main window of the module.

In this case, the number of the restored site changes, if it coincides with the number of already existing site or part. The number change is achieved by adding certain symbols (from “A” to “F”): for example, the site number “314” is changed to “A314”. In the same way, the number of any part of the restored site changes if it coincides with the number of already existing site or part. The number of the restored site and number of its parts are reported in a window that automatically opens immediately after the site is restored.

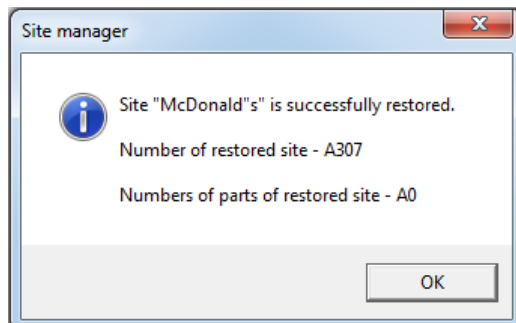


Figure 68: Information on number of restored site and its parts

It shall be noted that for the computer on which the site is being restored, a restriction on the available site numbers can be set. If the number of the site to be restored exceeds the limits of this restriction, the site will be restored, but a message will appear informing the user about the need to change the site number or change the restriction on available site numbers.

For the site, such parameters as identifier of TP-100 GSM III transmitter, identifier and encryption key of the “Yupiter” device are not restored. For the site to be restored, the administrator of the site is also deleted in the “MyAlarm” and subscriptions to event classes and operator actions are deleted, which were available in the “MyAlarm” application before the site deletion. Besides, for the site to be restored, the permissions granted to engineers for remote access to this site are canceled.

It is important to remember that the necessary condition for site restoration is the ability to add a site to the Security Center database in accordance with the available license restrictions. If the maximum possible number of sites is created in the database, an error message is displayed and the procedure for restoring the site is terminated.

6.4 Site

On the “Site” tab it is possible to specify the basic descriptive information about the site: number, name, address, phone numbers and so on.

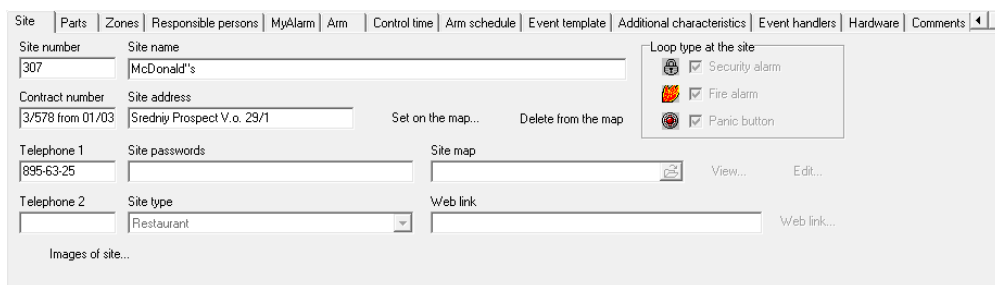


Figure 69: “Site” tab

6.4.1 Site location on map

To locate the site click the “Set on the map...” button next to the “Address” field on the “Site” tab. It is not necessary to switch to editing mode to do this. The “Map” window, called by this action, displays “Google Maps”.

The marker marks the location of the site. The location is determined in accordance with the value of the “City” field specified when registering in the “Cloud” and the “Address” field specified on the “Site” tab. Besides, the window provides a brief information about the site, namely: number, name and address of the site, as well as a comment for the Guard, entered on the “Comment” tab.

By hovering the cursor over it and holding down the left mouse button, it is possible to move the marker to indicate a more accurate location of the site. To zoom in or out use the zoom slider. Move the map with the cursor. The drop-down list allows to change the default type of the map “Scheme” to “Satellite”, “Hybrid”, “Public map”, “Public map + satellite”.

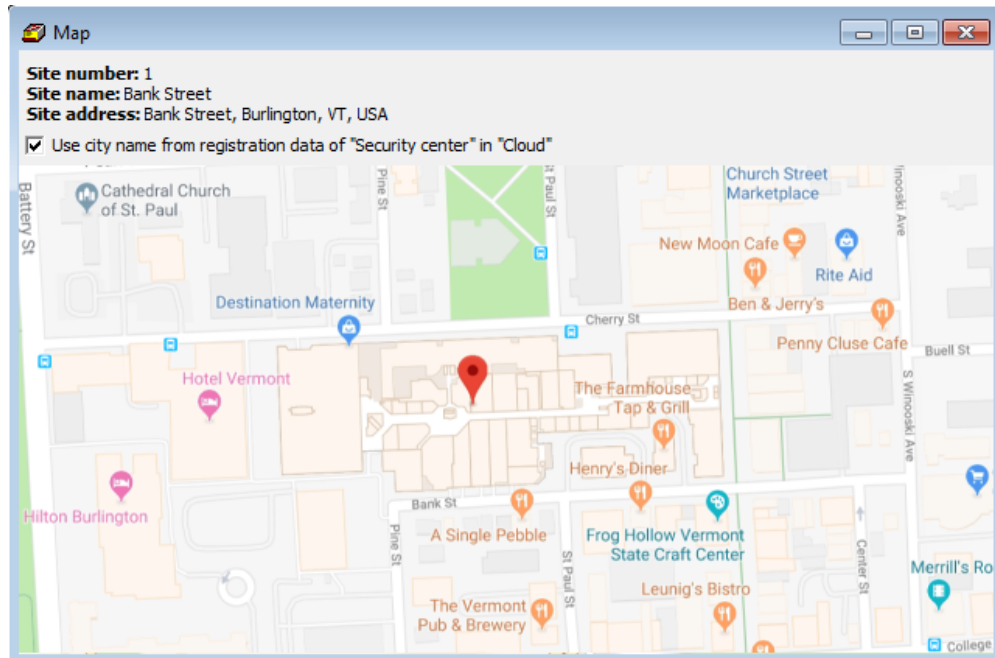


Figure 70: "Site" tab: Set on the map

After the marker is set, click the “Save” button to save the changes. The received site coordinates will be stored in the “Cloud” and in the Security Center database. After the coordinates are successfully saved, the “Delete from map” button will be active. Otherwise, it will be necessary to repeat the operation of setting the site on the map.

Important: setting sites on the map is possible when connecting to the Cloud and when ports 80 and 443 of the TCP protocol for the computer, on which the “Site manager” module is running, are open.

To delete the saved coordinates of the site from the map, click on the “Delete from card” button and confirm the deletion. In this case, information about the coordinates of the site will be deleted both from the Cloud and from the Security Center database.

If it is necessary to find out if the site is set on the map, see the information provided in the list of sites of the “Site manager” module in the “On the map” column. If this column is not displayed in the list, disable it. To do this, check the “On the map” column in the list of columns displayed in the list of sites by left-clicking on the special button located in the upper left corner of the list of sites.

6.4.2 Site Map

It is possible to specify both BMP and JPG file formats, as well as site map files created with the “Site Maps” module as the value for the “Site map” field. The “Change...” button, located next to the “Site map” field, is available for clicking only if the site map file is specified: when it is clicked, the “Site map” module will be launched to change the site map.

When creating and saving site maps using the “Site Maps” module, it is necessary to take into account that copying of information from site map files to the Security Center database is not performed. The source files are used to display the maps. This is important when running the Security Center in the local network, since the map files in

this case shall be stored on a network resource accessible to all network users of the Security Center at least for reading. Besides, when creating backup copies of the Security Center database, a backup copy of the site map files is not created: the user is asked to organize the backup of site map files independently.

See more information about creating site maps using the “Site Maps” module in the section devoted to this module.

6.4.3 Web Link

Despite the name, in the field “Web-link” it is possible to specify *any* file and resource located on the local computer, in the local network or the Internet, which can be opened using the tools installed on the computer.

When clicking the “Link . . .” button in the “Site manager” module, or the “Web link” field in the site card in the “Duty operator” module, the command for opening the specified resource will be executed by the means registered in the operating system on default for this type of resource.

For example, in the “Web link” field it is possible to specify the address (URL) of the web page where video streaming from the camera installed on the site is displayed. Click on the link to run the default browser, in which the specified page will be opened.

Similarly, in the field “Web link” it is possible to specify the path to the description file of the site created in a special format (AutoCad, 3D-Max). Click on the link to launch the program registered in the operating system to open such a file.

6.4.4 Images of Site

In the “Site manager” module, it is possible to download images of the selected site from the hard disk to the Cloud or delete it from the Cloud.

To load and delete images, the operator shall have the permission to “Edit image of site”.

To work with images, it is necessary to click on the “Image of site . . .” button, without switching to the site editing mode. Then the window of the same name is opened for downloading images, as well as for viewing and deleting already uploaded graphics files.

Important: it is possible to download images to the Cloud when connecting to the Cloud and when ports 80 and 443 of the TCP protocol for the computer, on which the “Site manager” module is running, are open.

Use the “Select” button in the “Files” address line to select one or more images of the site in PNG and JPEG formats for download. The image size shall not exceed 5 MB.

To quickly find them on the hard disk and correctly save in the Cloud, it is better to put the images of the site in the folder which name corresponds to the site number. It is also possible to assign the names, that start with the site number.

After selecting the graphic files, click the “Send” button. In this case, the image size will be automatically reduced to the optimal for displaying on the tablet in the “Alarm to Guard” mobile application. The progress bar in the “Progress” field displays the status of loading the selected images. Closing the “Image of site” window or selecting new graphic files for uploading is not possible until the download is complete.

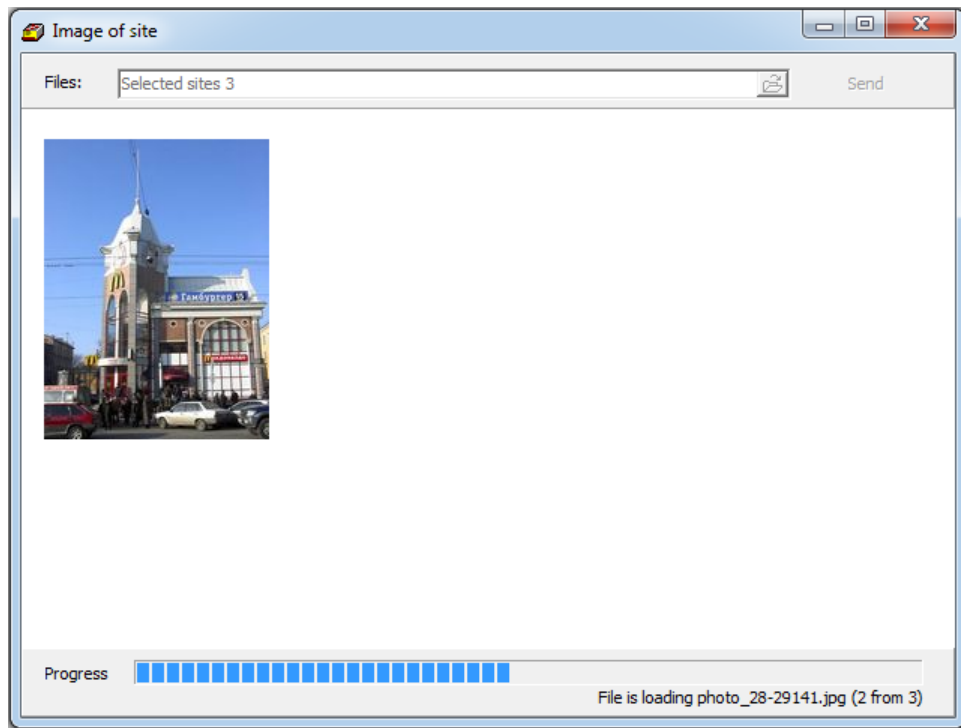


Figure 71: "Site" tab: image of site

Moving or removing of the graphic files, stored in the "Cloud", from the hard disk does not lead to their loss in the Cloud. To delete downloaded image from the Cloud, hover over its thumbnail in the "Image of site" window and click on the "Basket" icon that appears.

6.5 Parts

The "Parts" tab allows to save information about which parts (areas) the site is divided into and what equipment is used to organize parts on the site.

Site	Parts	Zones	Responsible persons	MyAlarm	Arm	Control time	Arm schedule	Event template	Additional characteristics	Event handlers	Hardware	Comments
Add part												
Delete part												
Part	Cust. number	Channels	Description	Arm schedule	Equipment							
4	5	Any	Perimeter	Add	Hunter-Pro							
3	5	P+Eth+GPRS	Safe	View								
2	4	Any	Door	Add	Hunter-Pro							
1	5	Any	Window	View								

Figure 72: "Parts" tab

In a number of cases, the term "Area" is used in the documentation for site devices instead of the term "Part". There is no meaningful difference between these terms, the term "Area" is used for historical reasons: once it was used in one of the translations of the documentation for site devices and since then it is often used as a synonym for the term "Part". Besides, the term "Key" is very common in Russian literature, which is also a synonym of the term "Part".

Sometimes the term "Area" is specially used to emphasize the difference in the method of encoding information transmitted from the site device. For example, the term "Part" is used for site devices transmitting information in the "Contact ID" protocol, which implies one site number for all parts of the device and individual sequence numbers for each part.

In turn, the term “Area” is used for devices transmitting information via the protocols of the “4/2” family (for example, “EPAF”), where there is no separate field for the part number, and to identify the parts it is possible to assign them individual site numbers.

The Security Center software supports any of these methods of identifying parts on the site. When describing parts it is possible to specify both the sequence number and the number of the site (key).

Use the “Add part” and “Delete part” buttons to add a new part to the list of site sections, or delete the selected part from the list.

The “Part” field shall be filled in if the parts in the site device have serial numbers and when sending messages from the site the “Contact ID” protocol is used. As the value for the “Part” field, the sequence number of the part programmed in the site device shall be used.

If there is no part number in the information received from the site, then the value of the “Part” field does not matter for Security Center and can be filled arbitrarily. When a new part is created, it is assigned a number following the maximum number assigned to the existing part.

The “Cust. number” field shall be filled in if individual site numbers are used to identify parts. The value for the “Cust. number” field shall be the site number programmed for the part in the site device.

If individual site numbers are not used to identify parts on the site, the value for the “Cust. number” field can be empty or can be filled with the number of the site to which the site belongs.

The “Channel” field is intended to perform identification of the site from which the event was received in combination with the value in the “Cust. number” field. For example, if you specify the site number in the “Cust. number” field that is different from the site number, and set “Radio” as the value for the “Channels” field, then the event received from the site with such a number over the radio will be treated as an event, received for this site.

Using such a description of parts for sites can be useful in cases when additional communicators (for example, radio transmitters) are installed on already equipped sites, but the numbers of the sites, on which they are installed, are already used in the radio channel. In this case, it is possible to program the panel so that different site numbers are used by telephone and radio, using these numbers and communication channel types when describing the parts of the site.

If the “Channel” field in the section settings is not used to identify the site, it is recommended to use the value “Any” as the value for this field.

In the “Description” field, it is possible to specify an arbitrary line describing the site part for the monitoring center employees. This can be a description of zones or rooms included in the part, or other features of the part organization.

If the Security Center software can identify the part on which the event was received, then the part description will be used to form a description of the events received from the site: the value specified in the “Description” field will be substituted in the description of the event instead of the macro %%part%%.

In the “Arm schedule” field of the “Parts” tab for each of the site parts there are links “Add” or “View”. The “Add interval” link redirects to the “Arm schedule” tab, where the corresponding part for scheduling has already been selected. The “View” link is available when the arm schedule for the part has already been created. Click on the “View” link, to open the schedule created on the “Arm schedule” tab.

As a value for the “Equipment” field, it is possible to specify the type of site equipment that is used to organize the part. This feature is useful if several site devices are installed on the site.

The value for the “Equipment” field can be selected from the list. It is possible to change the contents of this list in the “System setup” module - on the “Site fields” tab, “Customer part equipment” field.

To save the changes made to the description fields of the parts, it is necessary to confirm them by pressing the “Enter” button after completing the entry of the values.

6.6 Zones

On the tab “Zones”, it is possible to describe in detail the protection coverages of the site, including information about the equipment used and distribution of zones in the site parts.

Site	Parts	Zones	Responsible persons	MyAlarm	Arm	Control time	Arm schedule	Event template	Additional characteristics	Event handlers	Hardware	Comments
Add zone		Delete zone										
Zone number	Description	Equipment	Part									
5	Emergency exit door	MCS	314 (1)									
6	Warehouse scope	PIR	314 (1)									
7	Accommodation scope 1 (Car wash)	PIR	314 (1)									
8	Door and main office scope	MCS+PIR	314 (1)									
9	Administrator accommodation scope	PIR	314 (1)									
12	Virtual panic button in tyhe main office		314 (1)									
13	Portable virtual panic button		314 (1)									
14	Fire		315 (2)									

Figure 73: "Zones" tab

Information about zones is a very important part of the site description, since it is used when generating the description of events received from the site. For example, if an alert is received from the site in zone one, the event description, which will be created for handling by the Security Center operator, will be substituted for description of zone one from the site card.

Use the "Add zone" and "Delete zone" buttons to add a new zone to the site zone list, or delete the selected zone from the list.

The "Zone number" field is intended to indicate the number of the described zone. The value for this field shall be the sequence number of the zone programmed in the site device.

In the "Description" field, it is possible to specify an arbitrary line describing the site zone for the monitoring center employees. As a rule, the description contains a name of the room or the protection coverage, to which the zone belongs.

As a value for the "Equipment" field it is possible to specify the list of site equipment that is used to organize the zone.

The value for the "Equipment" field can be selected from the list. It is possible to change the contents of this list in the "System setup" module - on the "Site fields" tab, "Customer zone equipment" field.

As the value for the "Key" field it is possible to specify the part to which this zone belongs. If the site device is divided into several parts, then, by specifying parts in the description of the zones, we will get detailed information on the organization of the protection coverages at the site.

6.7 Responsible Persons

Site	Parts	Zones	Responsible persons	MyAlarm	Arm	Control time	Arm schedule	Event template	Additional characteristics	Event handlers	Hardware	Comments
№	Numbe	Title	Position	Mobile Phone	Work Phone	Address	Display in a private	Reclosing requ	Reclosing failure	PIN cod		
1		Borisova Anna Aleksandrovna	CFD	+89 (112) 371-11-5		Aviacionnaya street, 26	Yes	Yes	Yes	5678		
2		Pavlov Sergei Danilovich	Technical director	+7 (911) 777-81-08	595-54-82	Tipanova street, 15	No	Yes	No	5678		
56		Morozov Petr Konstantinovich	CEO				Yes	No	No			
Comment to the sites												
To call Borisova first handedly!!!												

Figure 74: "Responsible persons" tab

Use the "New" and "Delete" buttons to add a new or delete the selected person from the list.

Use the "Up" and "Down" buttons to change the order of the responsible persons in the list. The order of the responsible persons in the site card in the "Duty operator" module corresponds to the order that can be set on the "Responsible persons" tab.

Click on the "Edit" button in the main panel of the "Site manager" module on the "Responsible persons" tab to edit the field values of the site responsible person.

The “Number” field shall be filled in if the user, who has the personal code of the site arming/disarming, is indicated as the responsible person. In this case, the user number programmed in the site device shall be specified as the value of the “Number” field for the responsible person.

If the described responsible person does not own the personal code of the site arming/disarming, then an empty value can be used for the “Number” field.

In addition to the user number for the responsible person, it is possible to specify other necessary information: name, position, mobile and home phone numbers, address.

If the “Display in a private account” field has “Yes”, the responsible person will be displayed in the list of responsible persons in the “MyAlarm” application.

Configure the automatic notification of the responsible person about the need to reclose the site using the “Reclosing” field. If the value is “Yes”, the responsible person will receive SMS with information about the site that needs to be opened, inspected and taken under protection once the cause of the alarm has been eliminated.

In order for the responsible person to receive SMS with information about the person who refused to arrive for the site reclosing, it is necessary to set the value to “Yes” in the field “Reclosing failure”.

In the field “PIN code”, it is possible to change the PIN code of the responsible person for checking the panic button, as well as to confirm the site arming or disarming (when requesting PIN code). If prior to changing the PIN codes of all site responsible persons were the same, a window will appear asking if it is necessary to change the PIN code for all site responsible persons.

The “Commentary to responsible persons” field is intended to add additional information about the site responsible persons. If necessary, this field can be hidden.

If the responsible persons describe the users with the personal codes of arming/disarming, then information about the user, who performed arming or disarming, will be included in the description of the event handled by the Security Center operator.

6.8 Arm

On the “Arm” tab it is possible to change the parameters associated with the site protection rules and protection.

Figure 75: “Arm” tab

6.8.1 Long-term arm

The field “Put under long-term arm” is intended for enabling long-term protection mode of a site and indication of the mode duration. The long-term protection is intended to control situations when the site for some reason shall be under protection for a long time.

The site long-term protection is monitored as follows:

- at the start of long-term protection, the fact of the site arming is checked;
- if the site is not armed, a system event with the “ZZXC” code is created. If the site continues to be not armed, the system event with the “ZZXC” code will be repeated with the interval specified by the value of the “Arm schedule alarm periodicity” parameter specified in the settings of the “Event manager” module;

- if during the interval specified as the long-term protection time, the site will be disarmed, a system event with the “ZZXE” code will be created, after which the monitoring cycle of the long-term protection will begin anew - with the generation of the system event with the “ZZXC” code and expectation of the site arming.

To change the site long-term protection parameters, the user shall have the “Edit long-term arm” permission for the “Site manager” module.

6.8.2 Site Disabling

The “Disable site” field is intended to disable the site, starting from a certain time. If the site is disabled, the events received from it are handled as follows:

- when receiving any events from the site in the “Duty operator” module, the sound is turned off. That is, all events continue to be displayed, events with types of “Arming” and “Disarming” classes continue to change the state of the site, but there is no sound when receiving events from this site;
- when receiving events with the type of the “Alarm” class, they are automatically canceled. In other words, if the site is disabled and an alarm comes from it, in addition to the fact that there is no alarm sound, this alarm is also automatically canceled.

If the site is disabled, the “Automatically enable the site” parameter allows to turn it on at the specified time without operator intervention.

To disable sites, the user shall have the “Edit disabling” permission for the “Site manager” module.

6.8.3 Arming/Disarming by Duty Operator

If the equipment installed on the site does not imply the possibility of arming or disarming, it may be useful to emulate the events of arming or disarming by the duty operator. To enable this function, set the “Allow conditional arming and disarming by duty operator” parameter in the site settings.

After this parameter is set, an item will appear in the context menu of this site in the “Duty operator” module, allowing to create an event that will change the current state of the site.

For example, if the site is currently armed, the context menu item will be called “Disarm” and when it is selected, a system event will be created that has the default type of the “Disarm” class.

6.9 Control Time

The “Control time” tab is intended for control of one of the most important parameters of site operation control.

Figure 76: “Control time” tab

The site control time is the time interval during which any event shall be received from the site. It shall be understood that the term “Control time” differs in meaning from the term “Autotest control”. During autotest

control it is expected that the site will send quite specific events. But if we are talking about the site control time in the Security Center software, then during its handling, any events received from the site are taken into account.

If it is necessary to control passing of test or any other specific events, it is possible to use “Event monitoring” or “Event chain monitoring” event handlers. More details about the purpose and how to use these event handlers can be found in the section on the “Event manager” module.

It is possible to configure the site control time to separately monitor all communication channels used by the site.

If the “Use common control time for all channels” item is selected, the Security Center software will take into account any events from the site received via any communication channels when handling the site control time.

This approach to setting the site control time is useful if the site uses only one communication channel for transmitting messages or the transmission of signals via backup communication channels is not somehow periodic.

The “Control time” parameter allows to set the hours and minutes during which an event shall be received from the site. If during the specified time no events from the site are received, then a system event with the “ZZXA” code will be created for this site. If any event is received from the site within the specified time, the interval of waiting for events will be restarted.

If 0 is specified as the value for the “Control time” parameter, the handling of the control time for this site will be disabled.

The “Ignore system events” parameter allows to ignore the events created in the Security Center software when handling the control time. It is not recommended to disable this parameter for no particular reason when monitoring received events from real sites.

Select the “Use individual control time for each channel” item if the site is equipped with communicators working via several communication channels and it is necessary to monitor the operation of each communication channel independently of the other. If this item is selected, it is possible to set the control time for each type of communication channel separately. When handling an individual control time, only events received via the controlled communication channel are taken into account. If there are no events within the specified interval for the site, a system event with the “ZZXAx” code will be created, where x will be a figure from 1 to 7 corresponding to the type of the monitored communication channel:

- “ZZXA1” - System
- “ZZXA2” - Radio
- “ZZXA3” - Telephone
- “ZZXA4” - Ethernet
- “ZZXA5” - GPRS
- “ZZXA6” - SMS
- “ZZXA7” - CSD

For events that are created for the site as a result of the operation of the Security Center algorithms, “System” is always specified as the receive channel, that is why the “Ignore system events” parameter is not present when setting the individual control time for each communication channel: the control time for the “System” channel can also be specified.

By default, events with “ZZXA” - “ZZXA7” codes are described in all event templates as alarms, that is, they require registration of operator actions for handling and cancellation. If necessary, it is possible to change the event description. See information about how to do this in the chapter of this description devoted to the “System setup” module.

6.10 Arm Schedule

On the “Arm schedule” tab it is possible to specify the time periods for each day of the week when the site or its parts shall be armed, and also enable monitoring of this rule by the Security Center.

To make changes to the arm schedule settings, the user shall have the “Edit schedule” permission for the “Site manager” module.

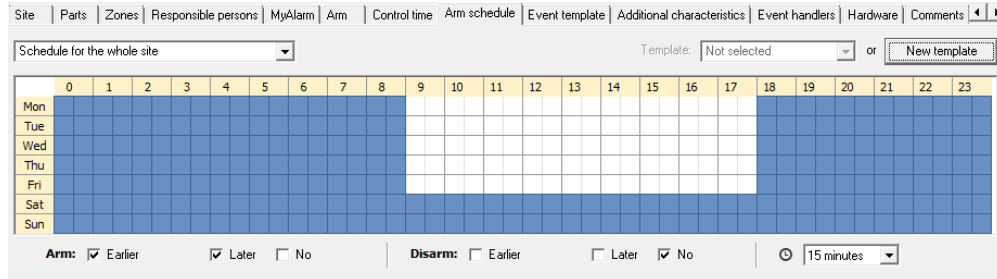


Figure 77: “Arm schedule” tab

It is possible to make arm schedule for the whole site, and for each of its parts. By default, the tab is set to the “Schedule for the whole site” mode. This mode shall be used when making arm schedule for the whole site, that is, for all its parts. If it is necessary to create arm schedule for one or more parts of the site, use the drop-down menu. Here there are all parts created for the site, each of which can be selected to make a separate schedule.

The site or its sections arm schedule is indicated in the table, which lines correspond to the days of the week from Monday to Sunday, and columns to the thirty-minute intervals of the day.

The cells of the table are blue, when they indicate the time when the site or its parts shall be armed. If the cell is white, the site or its parts at the specified time shall be disarmed.

To add an interval during which a site or its parts shall be armed, it is necessary to draw a quadrangle corresponding to the desired interval by the mouse. To delete an interval from the protection time of a site or its parts, do the same operation.

If the drawn interval captures both the blue and white area, a window with two buttons will appear - “Add interval” and “Delete interval”. If the site or its parts are to be armed during the selected time interval, click on the “Add interval” button. If the site or its parts shall be disarmed, click on the “Delete” button.

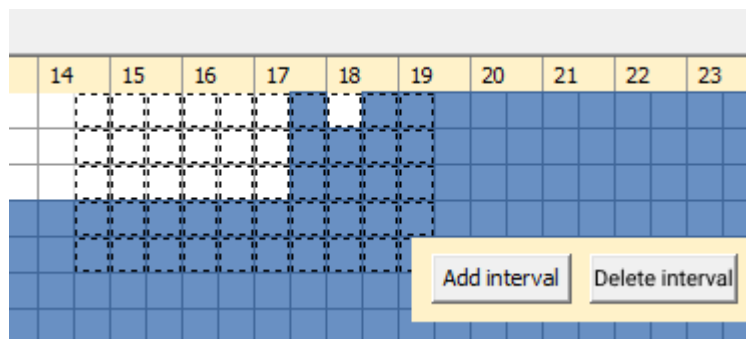


Figure 78: “Arm schedule” tab

It is possible to set the schedule control parameters using check-boxes located at the bottom of the tab. By checking the necessary boxes, specify the monitored states of the armed site.

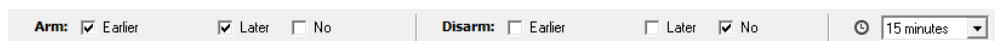


Figure 79: “Arm schedule” tab: site schedule control

Arming control is configured using the following parameters presented in the “Arm” line:

- “Earlier”. This parameter allows to get information about the fact that the site was armed earlier than indicated in the arm schedule. If the site was armed earlier, a system event with the “ZZWA” code is generated. Thus, the head of the protected enterprise can be notified via SMS that the employees left the workplace before the due time.
- “Later”. This parameter allows to get information about the fact that the site was armed later than indicated in the arm schedule. If the site was armed later, a system event with the “ZZWB” code is generated. Thus, the head of a protected enterprise can be notified via SMS about the time delay of employees in the workplace.
- “No”. This parameter allows to get information about the fact that the site is disarmed while according to the arm schedule it shall be armed. In this case, a system event “ZZXB” is created, which will be repeated with an interval specified by the parameter “Arm schedule alarm periodicity”, before the site is armed or until the time when the site can be disarmed. The parameter “Arm schedule alarm periodicity” is set in the settings of the “Event manager” module.

Disarming control is configured using the following parameters presented in the line “Disarm”:

- “Earlier”. This parameter allows to get information about the fact that the site was disarmed earlier than indicated in the arm schedule. If the site was disarmed later, a system event with the “ZZXD” code is generated.
- “Later”. This parameter allows to get information about the fact that the site was disarmed later than indicated in the arm schedule. If the site was disarmed later, a system event with the “ZZWD” code is generated. Thus, the head of the protected enterprise can be notified via SMS about the time of the site disarming, that is, the time of arrival of employees to the workplace.
- “No”. This parameter allows to get information about the fact that the site is armed while according to the arm schedule it shall be disarmed. In this case, a system event with the “ZZWC” code is created. Thus, the head of a protected enterprise can be notified via SMS that employees do not arrive on time to the workplace.

In the field indicated by the timer icon, the time range is set, during which any violations in the schedule of sites are allowed (the maximum value of the parameter is 30 minutes). For example, minus 15 minutes from the arming time and plus 15 minutes from the disarming time in the schedule of sites.

Let’s suppose, that the schedule for the site arming is from 21:45 to 09:15. With an acceptable deviation of 15 minutes, arming is allowed from 21:30 to 21:45, and disarming is allowed from 09:15 to 09:30.

By default, events with “ZZXB” and “ZZXD” codes are described in all event templates as alarms, that is, they require registration of operator actions for handling and cancellation. If necessary, it is possible to change the event description. See information about how to do this in the chapter of this description devoted to the “System setup” module.

If in the previous version of the Security Center the armed site schedule control was set for the site, then when the software is updated, the “No scheduled arming” and “Early disarming” parameters will be enabled for it. The remaining parameters for controlling the site schedule will be disabled.

It is possible to create arm schedule template based on the arm schedule. To do this, create arm schedule for the site or its part and click the “New template” button. It shall be noted that the “New template” button is available for clicking only if at least one time interval is added to the schedule.

In the “New arm schedule template” window that opens, the arm schedule used to create the template is given. Specify the name of the template and click the “Create template” button in this window.

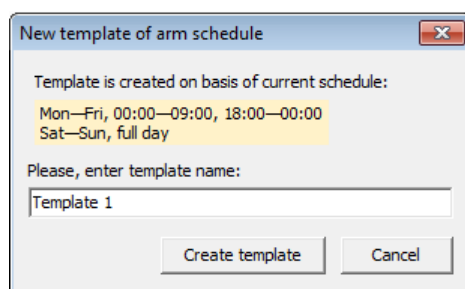


Figure 80: "Arm schedule" tab: new template

To apply a template to the site or its part arm schedule, do the following:

select the required template in the drop-down menu in the "Template" field.

The arm schedule can be edited. To do this, select the "Edit" item in drop-down menu of the "Template" field. All created templates are displayed in the "Arm schedule template edit" window. Click on the line of the required template to enter a new name. Besides, the template can be deleted by clicking on the "Delete" link in the template line and confirming the template deletion.

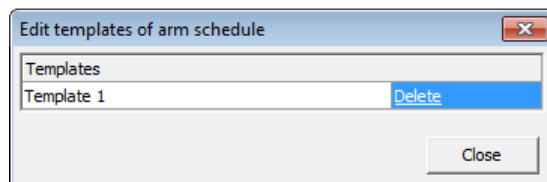


Figure 81: "Arm schedule" tab: template editing

6.11 Event Template

The "Event template" tab is intended for changing the event code template, used for decoding of events received from the site, disabling of alarm events, and for changing the properties of a specific event code for this site.

Site Parts Zones Responsible persons MyAlarm Arm Control time Arm schedule Event template Additional characteristics Event handlers Hardware						
PAF (general) [v] EAPAF Add event Edit event Delete event						
Channel	Code	Event class	Part	Z/U	Event description	
System	ZZXA7	Communication alarm			No CSD-related events	
System	ZZXB	Schedule alarm			Not armed %part%	
System	ZZXC	Schedule alarm			Not armed long-term	
System	ZZXD	Schedule alarm			Premature disarming %part%	
System	ZZXE	Schedule alarm			Prematurely disable long-term arming	
System	ZZXF	Virtual arming			Duty operator	
System	ZZXG	Conditional disarming			Duty operator	
System	ZZXH	CS alarm			Events timed out	
System	ZZXI	System				
System	ZZXJ	CS alarm			Events manager module error	
System	ZZXK	CS alarm			No recovery	

Figure 82: "Event template" tab

The event template that will be used to decode events from the site can be selected from the list in the upper-left corner of the tab.

To change the event template used by the site, the user shall have the "Change event template" permission for the "Site manager" module.

Use the "Add event" button to add a new event to the site event template. Use the "Change event" button to change the description for the selected event. It shall be understood that the changes made will affect only this site and will not be reflected neither in the event code template used by the site nor in any other site.

Click on the "Delete" button to delete an event that was added to the template of this site, or an event, the description of which was changed for this site. Events belonging to the event code template used by the site cannot be deleted.

To change the description of events, the user shall have the “Edit event template” permission for the “Site manager” module. It is not necessary to enter the edit mode to make changes to the description of the event template.

If you change the template events, changes to the database are saved immediately after the user has made changes to the template event. It is not possible to undo changes.

When creating a new event or changing an existing event, it is possible to specify all event attributes in the “Edit event” window.

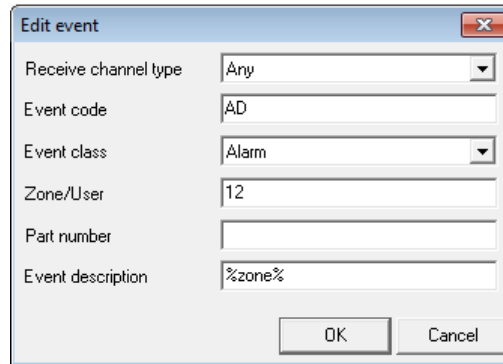


Figure 83: “Edit event” window

A detailed description of the event fields is given in the chapter on the “System setup” module in the section describing the “Event template” tab.

Due to the fact that changes in the event template for a particular site are extremely difficult to control, it is recommended not to use them without special need.

Disabling an alarm event that can be performed using the “Disable event” button, by its value, is very similar to disabling a site, with the only difference being that it is only one event code. When receiving a disabled event in the “Duty operator” module, there is no sound for the event, and “Event manager” creates an automatic cancellation for this alarm. It shall be emphasized that, unlike canceling an alarm for a disabled site, canceling an alarm for a disabled event will cancel only this event - the site arming continues in its entirety, except for the disabled event code.

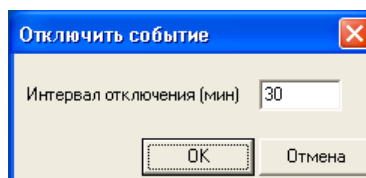


Figure 84: “Disable event” window

The event can be disabled only for a limited time interval, which is indicated when the disabling is performed. After this interval, the event will be automatically enabled. It is possible to enable the disabled event manually at any time by clicking on the “Enable event” button.

All operations for disabling and enabling the event are accompanied by the creation of system events. For example, when an event is disabled, a system event with the “ZZXM” code is generated, when the event is automatically disabled, a system event with the “ZZXN” code is created, and when the event is enabled by the operator (manual enabling), a system event with the “ZZXO” code is generated.

Generating system events allows to accurately track the operations for disabling events.

It shall be noted that the quality of the event templates supplied with the new versions of the Security Center is constantly improving, that is why when describing sites it is recommended to use the latest versions of the event templates.

To replace the outdated event template with its latest version, use the function of replacing the event template implemented in the “System setup” module.

6.12 Additional Characteristics

On the “Additional characteristics” tab it is possible to specify values for additional characteristics of sites (custom fields). Add a new additional characteristic or change an existing one in the “System setup” module, on the “Site fields” tab.

Site	Parts	Zones	Responsible persons	MyAlarm	Arm	Control time	Arm schedule	Event template	Additional characteristics	Event handlers	Hardware	Comment
Field	Value											
Information for engineer												
Communication channel	Radio and Phone											
Keypad	R<150											
Panel	Hunter-Pro											
GMS alarm phone												
Wired phone alarm												
GSM module type	T3-100GSM II											
Connection Date	2010.05.17											
Connected (Organization, Full name)	Special mounting, John Johnson											
State on monitoring date												
Re-enable date												

Figure 85: “Additional characteristics” tab

To save the changes made to the additional characteristics, it is necessary to confirm them by pressing the “Enter” button after completing the entry of the values.

If the value of any additional characteristic for the site is not defined, its value can be left blank. When displaying additional characteristics in the site card, only those which value is indicated are listed in the list of characteristics.

In order for the user to change the values of additional characteristics of the site, he/she shall have the “Edit additional characteristics” permission for the “Site manager” module.

6.13 Event Handlers

The “Event Handlers” tab is intended to display and change the event handlers associated with the site. Read more about the variety and purpose of the event handlers supplied with the Security Center software in the chapter devoted to the “Event manager” module in the “Event handlers” section.

In order for the user to see the groups of handlers and event handlers on this tab, he/she shall have the “View event handlers” permission for the “Event manager” module.



Figure 86: “Event handlers” tab

The purpose of the control panel buttons for the event handlers is the same as in the event handler in the “Event manager” module.

When configuring event handlers in the “Site manager” module, remember that not all groups of event handlers are displayed in the list, but only those handlers in groups which settings include the number of the current site.

In order for the user to make changes to the event handlers associated with the site, he/she shall have the “Edit event handlers” permission for the “Event manager” module.

6.14 Equipment

The “Equipment” tab of the “Site manager” module is intended to indicate the type of equipment used on the site and make the necessary settings. Entering information about the equipment provides the correct support of the Security Center installed on the site devices.

Site	Parts	Zones	Responsible persons	MyAlarm	Am	Control time	Am schedule	Event template	Additional characteristics	Event handlers	Hardware	Comments
Control panel type												
<input type="radio"/> C-Nord GSM (CML)												
<input checked="" type="radio"/> Lonta-202												
<input type="radio"/> RS200												
<input type="radio"/> Ritm												
<input type="radio"/> AlarmView												
<input type="radio"/> Puper type 5												
<input type="radio"/> Other												
Transmitter												
Site number <input type="text" value="318"/>												
Part number <input type="text" value="3"/>												
Signal levels												
Level of warning <input type="text" value="60"/>												
Level of alarm <input type="text" value="30"/>												
<small>If transmitter is used for transmission of signals from several sites that are connected to transmitter for parts, specify number of transmitter and number of part complied with the site for values of parameters "Site number" and "Part number". To control quality of communication with site specify thresholds of transmitter signal level in violation of which system events are created.</small>												

Figure 87: “Equipment” tab

To configure the equipment, select the desired site and switch to the edit mode. From the list of systems presented on the “Equipment” tab, select the type of equipment used on the site: “TR-100 GSM III/Soyuz GSM”, “AlarmView”, “Lonta-202”, “RS200”, “Puper type 5”, or “Neman”. If the equipment of another system is installed on the site, specify the “Other” type.

For the types of equipment “TR-100 GSM III/Soyuz GSM”, “Lonta-202”, and “Other”, specify the parameters for setting up the equipment. Remember that when copying a site for a new site, only the information about the installed equipment type is copied, but not the values of the specified parameters.

6.14.1 “Other”

If the list of equipment types does not include the system used on the site, select the “Other” type. In the “Transmitter” section, set values for the “Site number” and “Part number” parameters.

If the site is one of the parts on the control panel, then in the “Site number” field set the site number of the control panel, and in the “Part number” field - the part number corresponding to the site.

6.14.2 “C-Nord GSM (CML)”

This type of equipment shall be specified for the site if one of the following devices is installed on it:

- “Nord GSM” or “Nord GSM WRL”
- “Serzhant GSM”
- “Soyuz GSM”
- Transmitter “TR-100 GSM IV”

The “ID” field will be automatically filled in after the device connects to the Security Center for the first time.

The device ID is the unique identification number of the processor installed in the device. When receiving events from the site, it is checked that the events are sent from the device which ID is the one assigned to the site. Protection against the equipment substitution is realized in that way.

When replacing the equipment connected to the control panel on the site, delete the value of the “ID” parameter. Do this with the “Delete” button located opposite the “ID” field. After deleting the old value, the ID of the new transmitter will be automatically determined in the “ID” field.

Deletion the value of this parameter is also necessary when the equipment is dismantled at the site or changed.

It is possible to remove the ID and change the type of equipment for one site, as well as for all sites assigned to this identifier. To do this, use the dialog box that appears when changing the type of equipment. When changing all sites assigned to the ID, specify any of the types of equipment listed in the list for the current site, and for other sites the “Other” type is specified by default.

6.14.3 “Lonta-202”

Select the “Lonta-202” type of equipment when using the centralized radio security system “Lonta-202” (formerly called “Rif String RS202”) manufactured by Altonika.

In the “Transmitter” section, set values for the “Site number” and “Part number” parameters. If the site is connected to the radio transmitter as one of the parts, then in the “Site number” field it is necessary to specify the site number of the transmitter, and in the “Part number” field - the parts number corresponding to the site.

The values indicated in the “Site number” and “Part number” fields are priority with respect to the standard numbers of the Security Center sites: when receiving event, the values entered on the “Equipment” tab and first of all values of the site numbers are viewed first.

To control the quality of communication with the site on which the equipment of Lonta-202 system is used, it is necessary to set the threshold levels of the transmitter signal. Do this in the “Signal levels” section, indicating the corresponding parameter values in the “Level of warning” and “Level of alarm” fields.

If the level of the signal received from the site becomes less than the value specified in the “Level of warning” field, a system event with the “ZZXV” code will be created. If the level of the signal received from the site is less than the value specified in the “Level of alarm” field, a system event with the “ZZXU” code will be created. With the help of system events with “ZZXV” and “ZZXU” codes it is possible to automatically monitor the received signal level, attracting the operator’s attention only to those sites where it is required to intervene.

It shall be noted that for sites on which the equipment of Lonta-202 system is installed, the function of viewing the received signal level is available in the “Duty operator” module. The site card has a tab that allows to display the signal level in the form of a graph or as a table of values.

6.14.4 “RS200”

The “RS200” type of equipment shall be selected when using the radio centralized protection system “Rif String RS200” manufactured by Altonika.

6.15 Comment

The “Comments” tab is intended for entering an arbitrary description of the site.

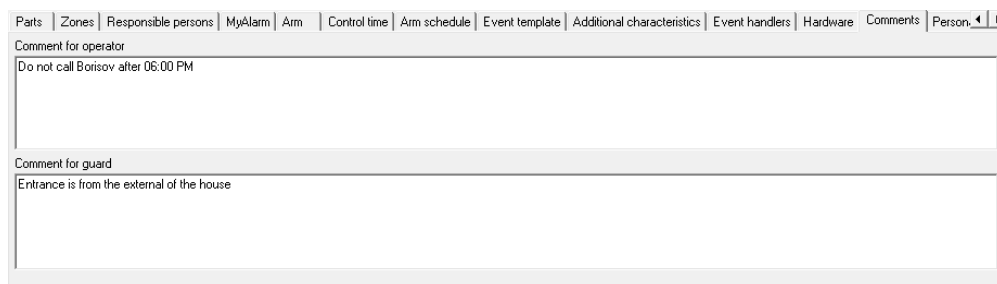


Figure 88: “Comments” tab

In the “Comment for operator” field, the information intended for the Security Center operator is indicated. This information is displayed in the site card in the “Duty operator” module, so it is often used to store notes on the site: requests from the responsible persons, observations of engineers serving the site, recommendations to operators, etc.

6.16 Videorouters

The “Videorouters” tab in the “Site manager” module allows to specify video routers for the site. Video cameras, installed on the site, shall be connected to these video routers.

Thanks to the installation of video cameras, remote monitoring of the site is possible. The surveillance can be conducted both by a responsible person of the protected enterprise by means of the web interface of the “Personal account” or mobile application, and the security company duty operator in the “Duty operator” module while handling an alarm.

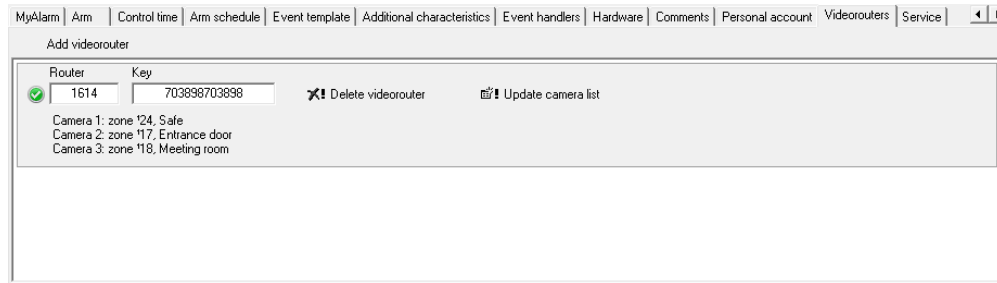


Figure 89: “Videorouters” tab

To add or change data about video routers, as well as view the keys of video routers installed on the site, the user shall have the “Change information about videorouters” permission for the “Site manager” module.

To add the video router installed on the site, click on the “Add videorouter” button on the “Videorouters” tab. In the “Router” field enter the ID of the video router, and in the “Key” field - the password for its authorization. The required data shall be indicated on the device. After that press the “Save” button to save information about the video router or the “Cancel” button to cancel saving. The current status icon of the video router displays the status of its connection.

The site card displays information about the configuration of the added video router. Namely: description of each of the video cameras connected to it and number of zones into their field of vision. This information is stored in the Security Center database and in the “Cloud”.

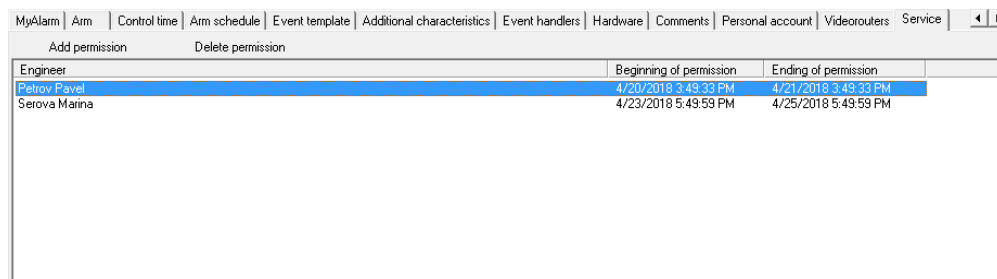
To update the information about video cameras connected to the video router, click on the “Update camera list” button.

To delete information about the video router and the video cameras connected to it, click on the “Delete videorouter” button.

6.17 Service

The “Service” tab is intended to provide engineers with permissions for access to sites. The permission received by the engineer gives him/her the ability to remotely program the control panel on the site during the specified time interval.

When site in the list of sites on the tab is selected, information about engineers, date and time of permission start and end is displayed.



Engineer	Beginning of permission	Ending of permission
Petrov Pavel	4/20/2018 3:49:33 PM	4/21/2018 3:49:33 PM
Serova Marina	4/23/2018 5:49:59 PM	4/25/2018 5:49:59 PM

Figure 90: “Service” tab

Only the user with the corresponding permission can grant site access to engineers.

To issue a permission, select the desired site in the site list and click the “Add permission” button.

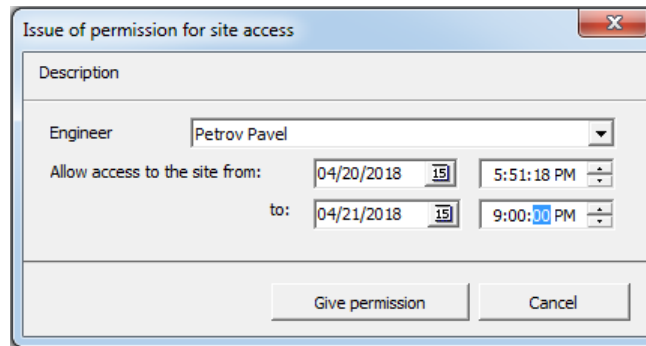


Figure 91: "Issue permission for site access" window

In the “Issue permission for site access” window fill in the following fields:

- “Engineer” - engineer from the drop-down list. The list displays the engineers created in the “Personnel manager” module. Engineers who have not confirmed the e-mail address for registration in the Cloud can also be selected from the list, but they will only gain access to sites after the registration is completed;
- “Allow access to the site from” and “to” - date and time of permission start and end, respectively. Permission to access the site can be issued for no more than thirty days. When issuing a permission for more than three days, the application will ask for confirmation. Besides, granting an engineer permission to access the site will cancel the permission granted to him/her for access to this site earlier.

After entering the data, click on the “Give permission” button to complete the operation. To cancel it, click on the “Cancel” button.

To remove the permission to access the site, select the permission in the list and click on the “Delete permission” button.

7 System Setup

The “System setup” module is intended to change the service directories of the Security Center, for example, event templates or site types.

7.1 Event Classes

In the Security Center software, the created events are divided into several types:

- Alarm
- Warning
- Arming
- Disarming
- Fault
- Restore
- Exception
- Test
- Other
- Alarm reset

The event type determines the handling. For example, events of the “Alarm” type require obligatory operator’s actions, called alarm handling. Besides, alarms, which handling is not started or completed, change the current status of sites. When handling events that have the “Arming” or “Disarming” type, the site status also changes.

The list of event types is predefined and cannot be changed by the user. Event classes are intended to group the events and manage them. The event class defines its type, in this case it is possible to create several classes with the “Alarm” type and define individual action lists and cancellations for each alarm.

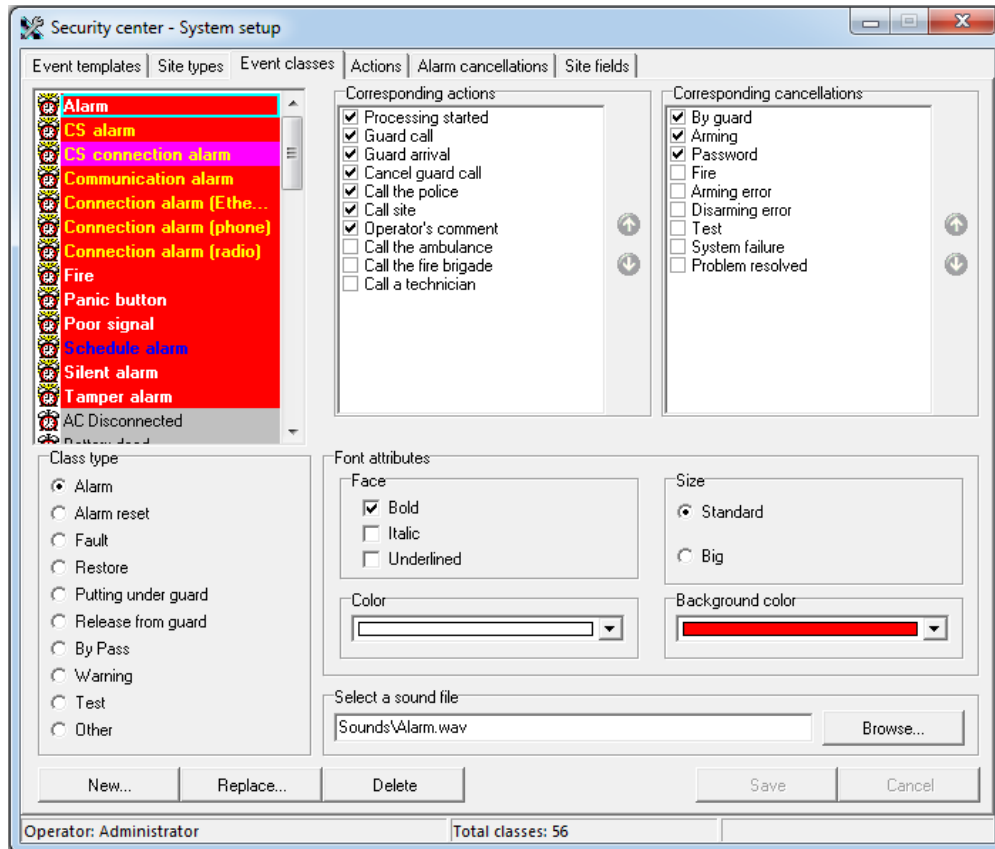


Figure 92: “Event classes” tab

Use the “Event classes” tab to change the list of used event classes.

To save the changes made on this tab, the user shall have the “Edit event classes” permission for the “System setup” module.

The event class defines the appearance of the event in the list of received events of the “Duty operator” module. Color, font, background color - all these properties of the event class can be changed in the “System setup” module.

In addition to the attributes responsible for displaying events, it is possible to specify an audio file that will be played when an event is received.

For event classes of the “Alarm” type, there are action lists and cancellations, which the operator can register during alarm handling. It is important that it is possible to define not only the list of actions, but also their sequence during display.

Since event classes define appearance, sound and alarm script, the Security Center ensures that these parameters remain unchanged for already registered events. In other words, any changes and even deletion of event classes do not affect events that are already accepted and registered in the database. If the color or size of the font, used to display the event or the type of the event, is changed, these changes will only apply to new events, those that will be registered in the database after the changes are made.

Replacing Event Class

If the Security Center has been in operation for a long time, then there is a possibility that the list of event classes is littered. For example, it contains duplicate classes or information about classes that are no longer used. However, it is impossible to remove these classes, because there are events that are described by these classes. To cope with this problem, it is possible to replace duplicates or unused event classes with their current analogs. To replace the obsolete event class with the one currently in use, use the “Replace...” button.

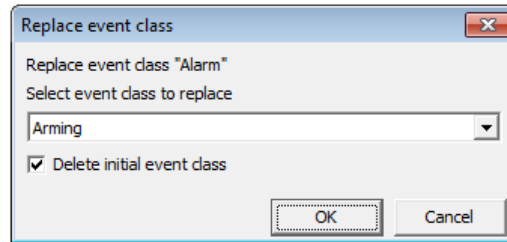


Figure 93: "Replace event class" window

In the window that appears, select the event class that will be used instead of the replaced one, and also specify the need to delete the event class that is being replaced.

7.2 Event Templates

The same event that occurred on the site can be transmitted to the Security Center in different ways. The notification format, in which information about the event will be received, depends on the type of the transmitting equipment and communication channel.

An event template is a list of events that can be received when decoding notifications from a site.

The event template is an integral characteristic of the site. It is possible to specify the event template that shall be used for the site in the “Site manager” module.

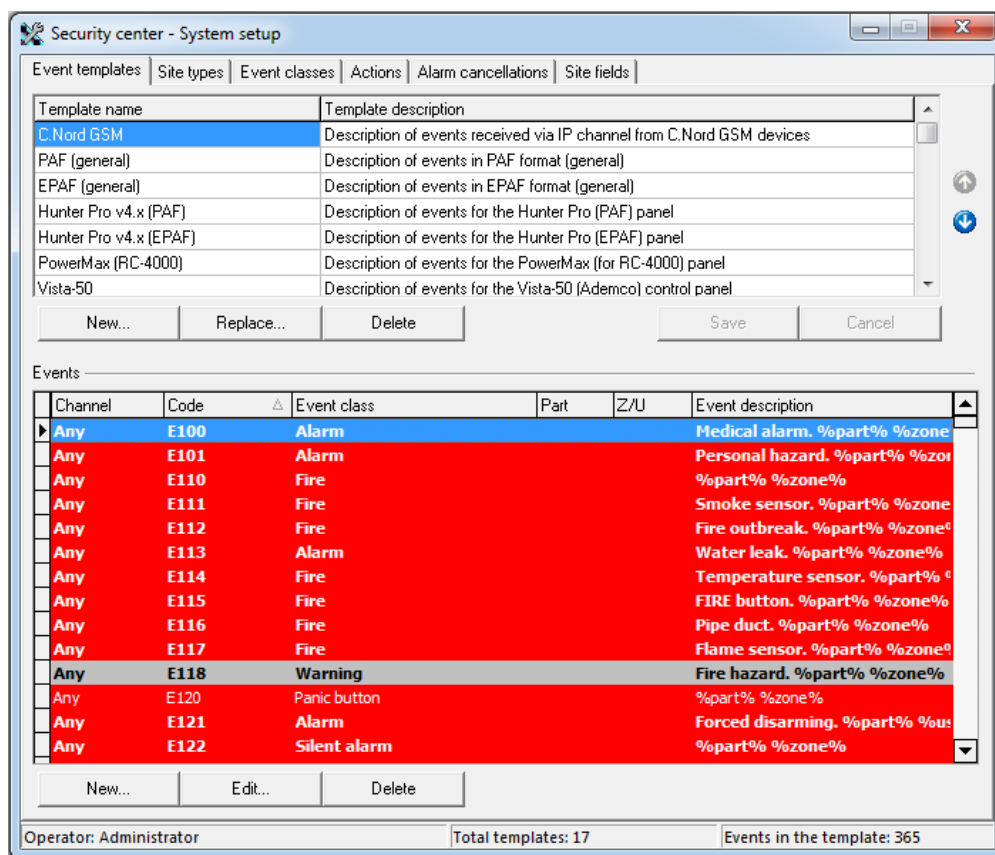


Figure 94: "Event templates" tab

Use the "Event templates" tab to change the list of templates used by the Security Center. Besides, it is possible to change the description of the events in the template.

To save the changes made on this tab, the user shall have the "Edit event templates" permission for the "System setup" module.

Changes that are made to the description of the template events on the System setup tab affect all sites that use this event template. It is strongly recommended not to make changes to the site event template without a valid reason.

It is impossible to delete the event template used in site description. If the template that the user wants to delete is used as an event template for a site, the attempt to delete will be completed with an error.

7.2.1 Replacing Event Template

It shall be noted that the quality of the event templates supplied with the Security Center is constantly improving, that is why when describing sites it is recommended to use the latest versions of the event templates. To replace the obsolete template for sites with another, more relevant, use the function of replacing event templates. To replace the obsolete event template with the one currently in use, use the "Replace..." button.

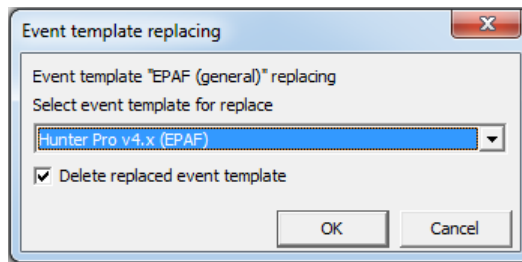


Figure 95: "Event template replacing" window

In the window that appears, select an event template that shall be used instead of the replaced one, and also specify the need to delete the obsolete event template.

Event Editing

If you change the template events, changes to the database are saved immediately after the user has made changes to the template event. It is not possible to undo changes.

When creating a new event or changing an existing event, it is possible to specify all event attributes in the "Edit event" window.

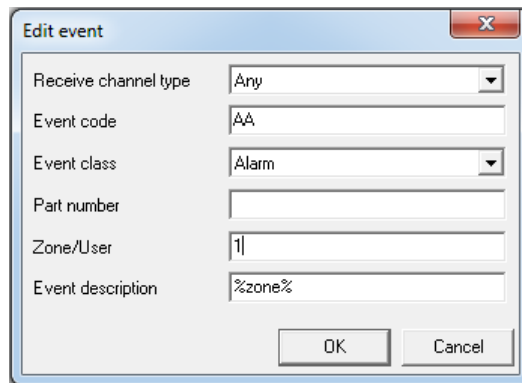


Figure 96: "Edit event" window

- "Receive channel type" - when decoding an event, it is important which channel was used when it was received by the Security Center. For example, the same event code can be decoded in different ways, for events received via radio and phone. If the event code is defined for both specific communication channels and for "Any" communication channel, the decoding for the "Any" communication channel is applied only if the decoding for a specific communication channel is not found.
- "Event code" is the significant part of the message sent from the site. It is the code that identifies the change that has occurred to the control panel on the site. Event codes can be of different lengths, it depends on the format (protocol) and communication channel used during information transmission from the site device to the central station. The Security Center supports event codes up to 25 characters in length.
- "Event class" is an event class that will be mapped to the received code when decoding an event. The event class defines the appearance of the event in the event list, as well as a list of possible actions for handling, if the event class is "Alarm".
- "Part number" is an attribute that can be used to further identify the event during decoding. If the protocol of exchange with the site device contains the number of the part to which the event relates, then the event will be identified not only by the code and the receiving channel, but also by the part number. Besides, the part number is used when generating the event description automatically: if the part number is not a zero, and the event description contains the macro `%part%`, then instead of the macro, the description of the site part corresponding to the part number received from the site will be inserted.

- “Zone/User” is an attribute that can be used depending on how the informative format (protocol) is used to transmit information from the control panel to the Security Center.

Let’s suppose that the panel, when transmitting to the station, uses the ContactID protocol, which, among other things, sends the number of the tripped zone or the number of the user who performed the site disarming. In this case, the Security Center ignores the zone or user number specified in the event description and always uses the value received from the panel: the zone number, which was sent from the panel, will be used to decode the event.

Now let’s consider the situation when the panel, when transmitting to the station, uses the EPAF protocol, in which only the site number and event code are transmitted. The zone or user numbers are not explicitly transmitted, but the relationship between the event code and zone or user number is known. In this case, the zone or user number is specified in the event template - according to the event code, and it is the value specified in the template that will be used to form the event description.

As an example, let’s consider an alarm message in the first zone transmitted via different protocols. In the ContactID protocol, this message will be transmitted in the form of E130 code and zone number 1. When forming the description, the Security Center will immediately perform the substitution of the description of the first zone in the event description. While in the EPAF protocol the same message will be transmitted only in the form of AA code and to get the number of the zone corresponding to this code, the Security Center will have to look into the event template.

- “Event description” is an arbitrary text string describing the event.

When describing events, it is recommended to use the macros `%user%` and `%zone%`. If a macro is found in the description of the event during its decoding, a value corresponding to the name of the zone (macro `%zone%`) or the name of the responsible person (macro `%user%`) will be inserted in the description. In this case, the zone or user number will be taken from the event itself. Information about zones and responsible persons on the site is very important. It is possible to enter this information for the site in the “Site manager” module.

7.3 Actions

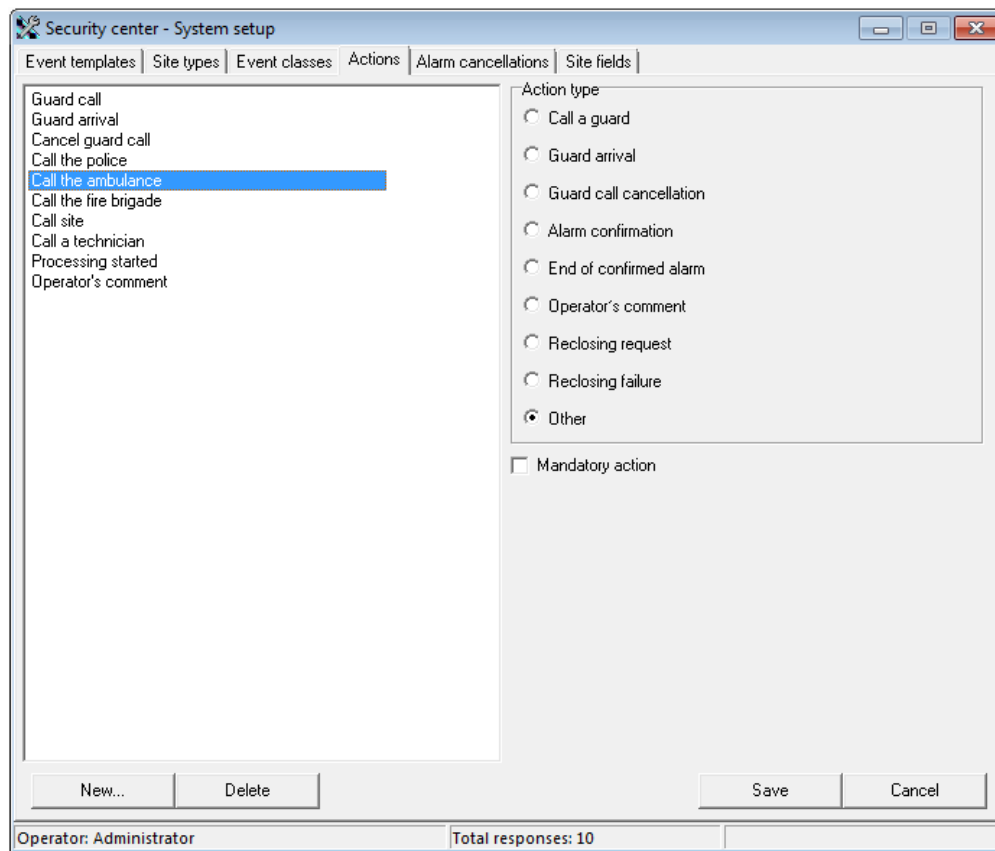


Figure 97: "Actions" tab

The "Actions" tab is intended for changing the list of actions that an operator can register during alarm handling. To save the changes made on this tab, the user shall have the "Edit operator actions" permission for the "System setup" module.

The following types of actions are defined in the Security Center software:

- "Call a guard" - when registering this type of action, the operator will have to specify the guard that was called to the site. If a guard has been called to the site, then the site alarm can be canceled only after the guard's arrival to the site or the cancellation of its call is registered. The list of guards used by the Security Center can be changed in the "Personnel manager" module.
- "Guard arrival" - action of the "Guard arrival" type is available for registration only after the guard call to the site is registered. When registering an action with the "Guard arrival" type, the operator will have to select the guard, the arrival of which he/she is registering.
- "Guard call cancellation" - registration of cancellation of a guard call is available only after its call to the site is registered. When registering a call cancellation, the operator will have to select the guard which call cancellation is being performed by the operator.
- "Operator's comment" - this type of action allows the operator to enter arbitrary text associated with the alarm handling. Actions of this type can be registered at any stage of alarm handling. It is recommended to include this type of action in action lists for all alarms that are available in the Security Center.
- "Reclosing request" - this type of action allows the operator to automatically inform the responsible persons about the need to reclose the site. When registering this type of action, SMS message is sent to the responsible persons, for whom an alert about reclosing request is set in the "Site manager" module. The SMS contains

the number, name and address of the site to be opened, inspected and reclosed once the cause of the alarm has been eliminated.

- “Reclosing failure” - this type of action allows the operator to automatically inform the responsible persons about the refusal of the person responsible to reclose. When registering an action of this type, the operator shall select the responsible person of the site who has refused to come for reclosing. List contains only those responsible persons, who are notified about the need to reclose according to the “Site Manager” module setting. In this case, the full name the responsible person, who refused to reclose, is displayed in the “Note” field when the action is written to the event log. When registering this type of action, SMS message is sent to the responsible persons, for whom an alert about reclosing refusal is set in the “Site manager” module. The SMS contains the name of the responsible person, who refused to reclose, as well as the site number, name and address.
- “Other” - actions of the “Other” type are informational in nature and are used for quick registration of actions often used during alarm handling (call to the responsible person, call to police, etc.). Actions of this type can be registered at any stage of alarm handling.

The list of actions with the “Other” type is recommended to be constantly updated, so that they correspond to the tactics of the guard used at the moment. A good source for new actions with the “Other” type can be registered operator comments.

Action of any type can be made mandatory for execution during alarm handling. To do this, select the action in the list and check the “Mandatory action” box.

7.4 Alarm Cancellations

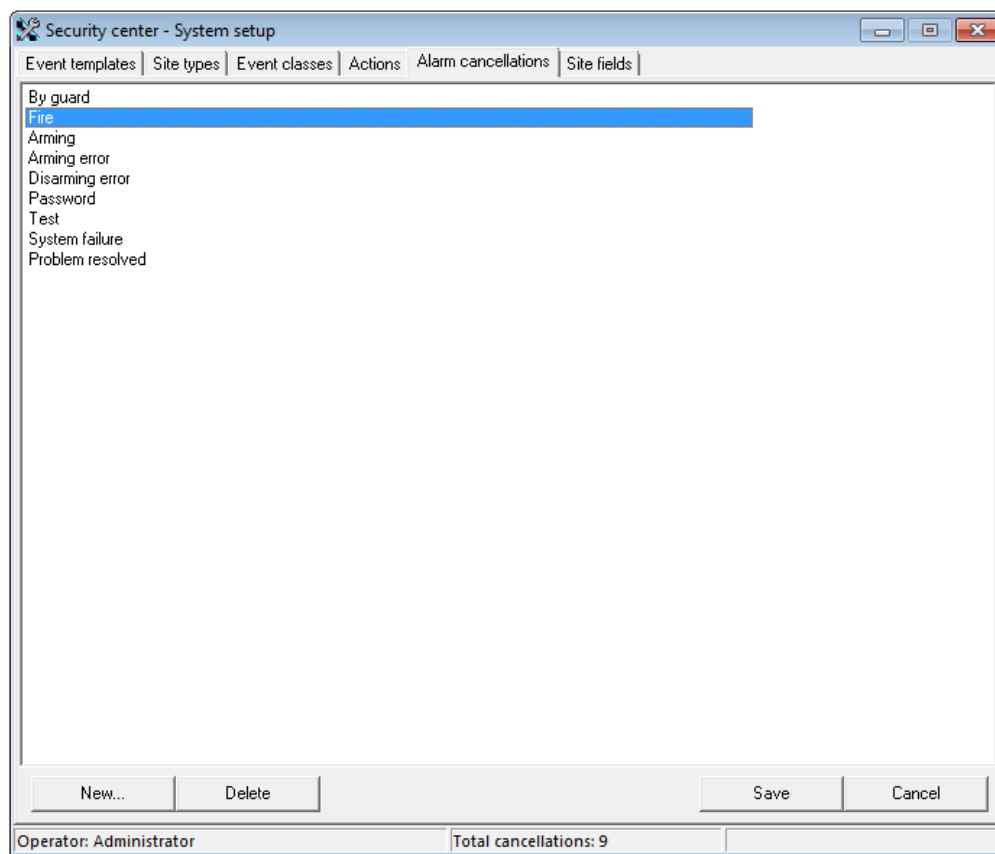


Figure 98: "Alarm cancellation" tab

Use the “Alarm cancellation” tab to edit the list of reasons recorded when canceling alarms.

To save the changes made on this tab, the user shall have the “Edit alarm cancellations” permission for the “System setup” module.

The list of available alarm cancellations is closely related to the site protection tactics and is of great importance in analyzing the company performance.

The Security Center software contains several analytical reports ensuring evaluation of the most common causes for canceling alarms, including in the context of sites. To use these reports, it is necessary to maintain a list of cancellations of alarms in the current state and clearly regulate the use of each cancellation in the operator’s instructions.

7.5 Site Types

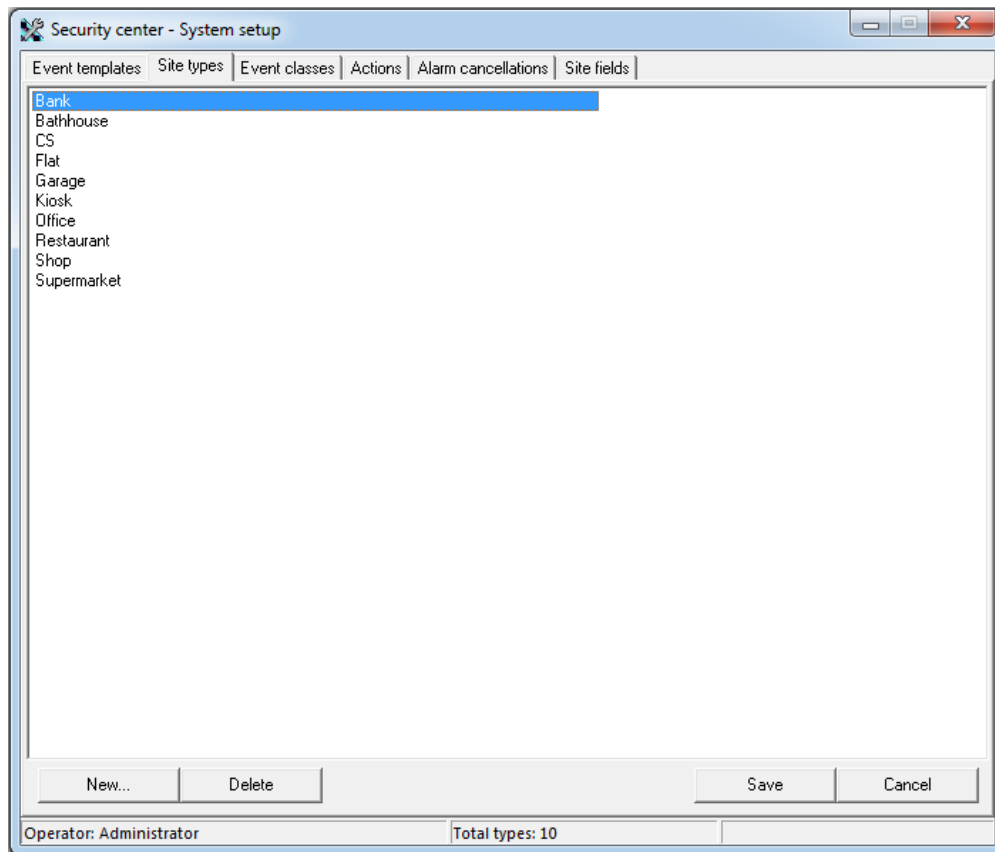


Figure 99: "Site types" tab

The “Site types” tab is used to manage the list of site types.

To save the changes made on this tab, the user shall have the “Edit site types” permission for the “System setup” module.

The site type is a mandatory property of a site. The site type is used for the convenience of organizing (sorting, grouping) the list of sites, for example, when viewing site properties or creating reports. It is possible to specify the type for a site in the “Site manager” module.

7.6 Site fields

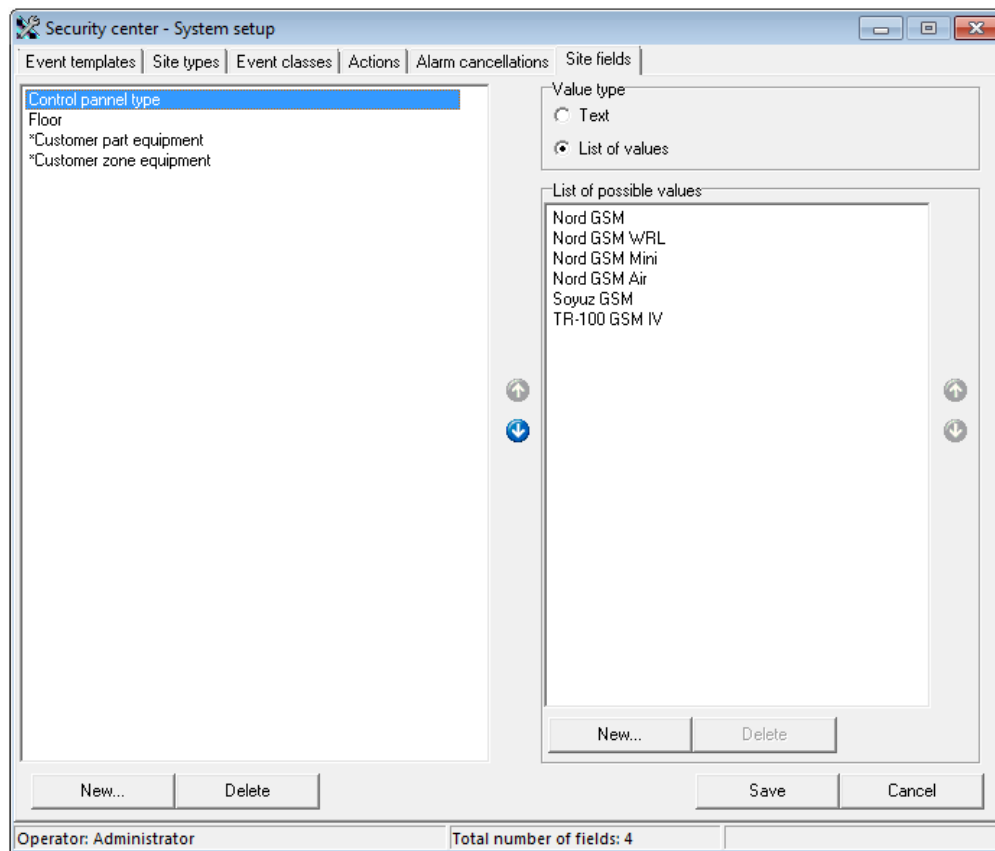


Figure 100: "Site fields" tab

Use the "Site fields" tab to change the list of additional fields that will be available when filling the site card.

To save the changes made on this tab, the user shall have the "Edit site fields" permission for the "System setup" module.

When creating a list of fields, it is possible to set their sequence when they are displayed in the site card.

If the values of a field are a list of previously known values, then it is possible to fill this list by specifying the appropriate type for the field. In this case, the list of values does not limit the ability to specify a value for the site field manually, if necessary.

There are two fields in the list of site fields, for which it is recommended to change only the list of possible values. These fields are "*Customer part equipment*" and "*Customer zone equipment*". As their names suggest, they are intended so that it was more convenient to fill in the values for the "Equipment" field when editing parts and zones of sites in the "Site manager" module.

8 Personnel Manager

In the "Personnel manager" module, it is possible to edit the list of operators and their rights - in the Security Center modules, guards, that are used in the Security Center, as well as the list of computers on the local network, on which the Security Center network workplaces are allowed.

8.1 Operators

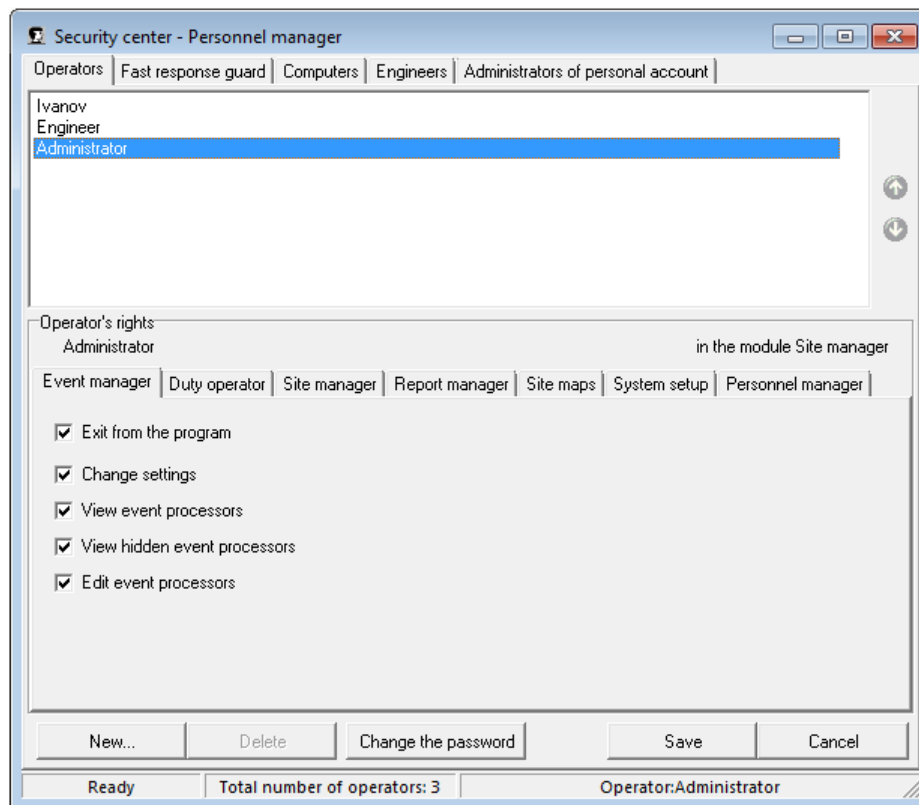


Figure 101: Operators tab

The “Operators” tab is intended for editing the list of software operators and their rights in the Security Center modules.

To save the changes made on this tab, the user shall have the “Edit Groups” permission for the “Personnel manager” module.

Operator rights are individual for each Security Center module. Availability of this or that right determines the list of operations that can be performed in the module.

Before determining the operator’s rights in the module, allow the operator to enter this module.

When creating a new operator, it is possible to assign him/her the same rights as one of the existing ones. To do this, before creating a new operator, in the list of operators select the user, whose rights shall be copied.

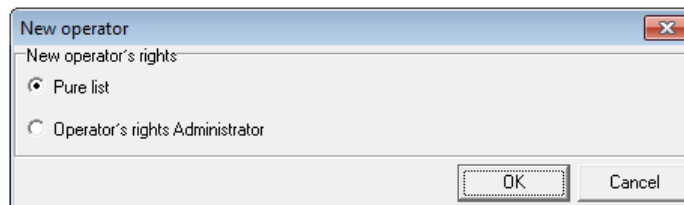


Figure 102: Selecting list of rights for new operator

It is forbidden to edit the name and rights of the operator, who entered the module, as well as “Administrator” in the module “Personnel Manager”.

For the current operator of the “Personnel manager” module and the “Administrator”, only password changing is allowed.

8.1.1 Operator's Rights in "Event Manager" Module

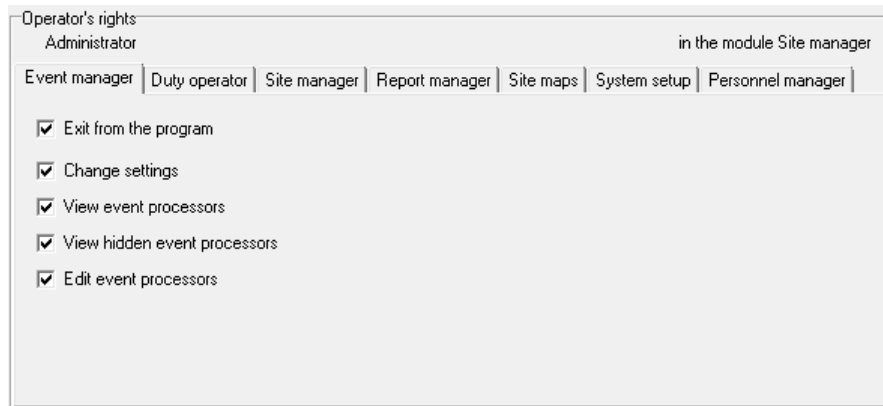


Figure 103: Operator's rights in the "Event manager" module

- "Exit from the program" - permission to shut down the "Event manager" module.
- "Change settings" - permission to make changes to the settings of the "Event manager" module.
- "View event handlers" - permission to view (but not to change) the settings of event handlers. This permission also applies to the "Event handlers" module.
- "View hidden event handlers" - permission to view (but not to change) the settings of *hidden* event handlers. This permission also applies to the "Event handlers" module.
- "Edit event handlers" - permission to make changes to the settings of those event handlers that are allowed to view. This permission also applies to the "Event handlers" module.

8.1.2 Operator's Rights in "Duty Operator" Module

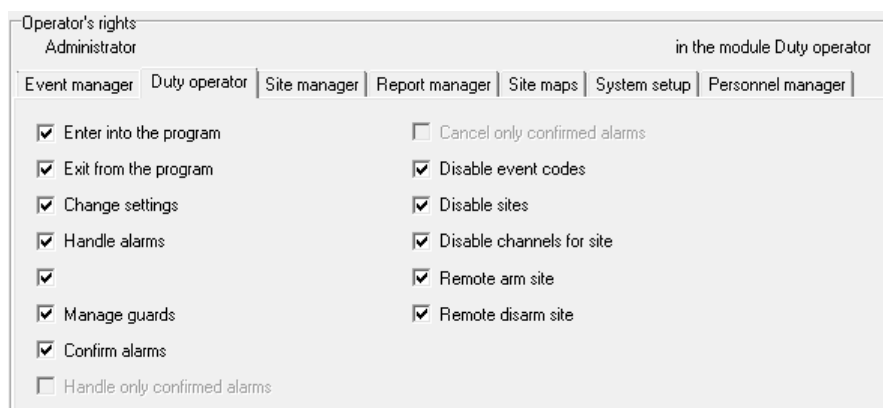


Figure 104: Operator's rights in the "Duty operator" module

- "Enter into the program" - permission to enter the "Duty operator" module. If the operator has to handle the alarms, then he/she shall have this permission.
- "Exit from the program" - permission to close the "Duty operator" module. Ban on closing of the "Duty operator" module can be useful for inexperienced operators, as a warning about exiting the module by mistake.
- "Change settings" - permission to make changes to the settings of the "Duty operator" module. It is not recommended to grant this permission to the duty operators, especially since the settings of the "Duty

operator” module are associated with the computer on which the module is being executed, and not with the operator who launched the program. Thus, the administrator can perform all the necessary settings of the module on the computer and any operator, who launched the “Duty operator” module, will work with these settings.

- “Handle alarms” - permission to handle an alarm. The Security Center operator with this right can call the “Alarm handling” window and perform all possible actions to handle the alarm. To cancel the alarm, the operator shall also have the right to “Cancel alarm”.
- “Cancel alarm” - permission to cancel alarm. The Security Center operator with this right can call the “Alarm handling” window and cancel the alarm. To handle an alarm, the operator shall also have the right to “Handle alarms”.
- “Disable event codes” - permission to disable events. The Security Center operator with this right can call the “Disable event” window and disable the event, specifying the time during which the event shall be disabled and the reason for disabling.
- “Disable sites” - permission to disable sites. The Security Center operator with this right can call the “Site disabling” window and disable the site, specifying the time during which the site shall be disabled and the reason for disabling.
- “Disable channels for site” - permission to disable communication channels for the site. The Security Center operator with this right can call the window “Site channels disabling” and disable one or several communication channels, specifying the time during which the communication channels shall be disabled, and the reason for disabling.
- “Remote arm site/remote disarm site” - permission for remote arming/disarming of sites. The Security Center operator with this right can arm/disarm the site, if the equipment with the type of the transmitter “TR-100 GSM III” is installed on the site.

8.1.3 Operator’s Rights in “Site Manager” Module

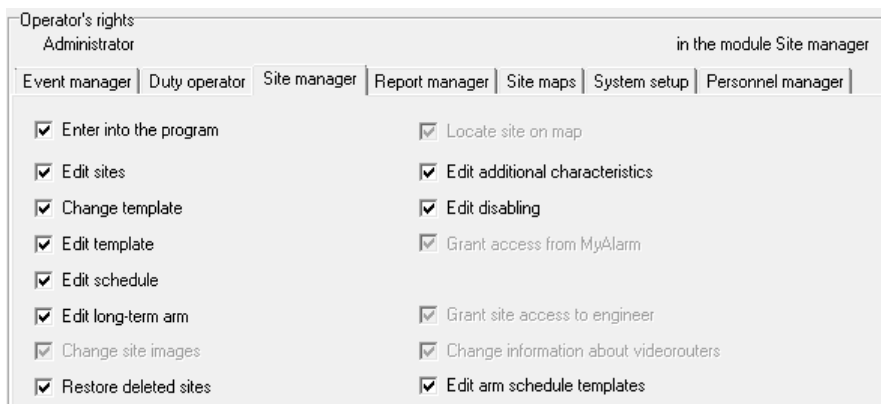


Figure 105: Operator’s rights in the “Site manager” module

- “Enter into the program” - permission to enter the “Site manager” module. If the operator shall be able to view and edit site cards, then he/she shall have this permission.
- “Edit sites” - permission to edit site cards. This permission applies to most fields of the site card, with the exception of those fields for which changes additional permissions described below are required. With the help of additional permissions it is possible to protect important or rarely changed card fields from accidental changes.
- “Change template” - permission to change the site event template. The event template determines how messages received from the site equipment will be decoded: which messages shall be considered alarm ones,

which messages shall be considered as armings, etc. Which particular event template shall be used for a site depends on the equipment installed on the site, as well as on the communication channels via which messages from the site are transmitted. For most modern site devices, the event template “Radio (EPAF), DTMF, GPRS”, which is included in the Security Center package, is suitable and recommended for use.

- “Edit template” - permission to edit descriptions of events included in the event template set for the site. It shall be noted that the changes will be applied only to the site for which changes are made and the event template itself won’t be affected in any way. It is strongly recommended not to make changes to the site event template without a valid reason.
- “Edit schedule” - permission to edit the parameters of the site arm schedule. If the arm schedule is set for the site and its monitoring is enabled, then, if the schedule is violated, the Security Center will create the appropriate system events (alarms).
- “Edit long-term arm” - permission to edit the parameters of long-term arm of the site. If the long-term arm is enabled for the site, then when you try to disarm the site, the Security Center will create a system event (alarm).
- “Change site images” - permission to change the site images.
- “Restore deleted sites” - permission to restore deleted sites.
- “Locate site on map” - permission to change the location of the site on the map.
- “Edit additional characteristics” - permission to change the values of additional characteristics of the site. Important information can be indicated in the additional characteristics of the site.
- “Edit disabling” - permission to change the disabling parameters of the site. For disabled sites, Security Center performs automatic cancellation of alarms, without notification of the duty operator about them.
- “Grant site access to engineer” - permission to grant remote access to sites to engineers.
- “Change information about videorouters” - permission to change information about video routers. This permission allows to add and remove video routers, to which the cameras on the site are connected.
- “Edit arm schedule templates” - permission to edit arm schedule templates. With this permission, it is possible to create, edit and delete templates based on the selected arm schedule.

8.1.4 Operator’s Rights in “Report Manager” Module

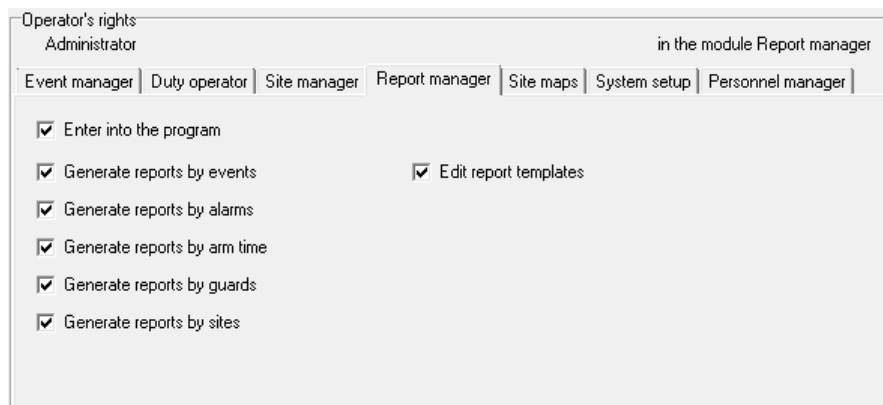


Figure 106: Operator’s rights in the “Report manager” module

- “Enter into the program” - permission to enter the “Report manager” module. If the operator shall be able to create reports, then he/she shall have this permission.

- “Generate reports by events” - permission to create reports on the received events. When creating these reports, the operator has access to the list of sites, as well as to the list of event classes. The generated reports contain information about the events that were received during a given period, events from undescribed sites, and sent SMS messages.
- “Generate reports by alarms” - permission to create report on alarms. When creating these reports, the operator has access to the list of sites, as well as to the list of event classes and operator’s actions. The generated reports contain information about the received events, operator’s actions for handling alarms and guard responses. Besides, some of the alarm reports provide information on the basis of which it is possible to identify problematic sites and analyze the causes of the alarms.
- “Generate reports by arm time” - permission to create alarm reports. When creating these reports, the operator has access to the list of sites, as well as to the list of event classes. The created reports contain information about the time during which the sites were to be protected in accordance with their arm schedule, as well as the time during which the sites were actually armed.
- “Create reports by guards” - permission to create reports on guards. When creating these reports, the operator has access to a list of sites, as well as to lists of event classes and guards. The generated reports contain information about the received events, operator’s actions for handling alarms and guard responses.
- “Generate reports by sites” - permission to create reports by sites. When creating these reports, the operator has access to the list of sites. The created reports can contain all the information available in the site cards.
- “Edit report templates” - permission to create new and edit existing forms, on the basis of which reports in the “Report manager” module can be created. It is strongly recommended not to grant this permission to operators, and also to make changes to report templates without backing up the modified data.

8.1.5 Operator’s Rights in “Site Maps” Module

Operator's rights	
Administrator	in the module Site maps
Event manager	Duty operator
Site manager	Report manager
Site maps	System setup
Personnel manager	
<input checked="" type="checkbox"/> Enter into the program <input checked="" type="checkbox"/> Edit site maps	

Figure 107: Operator’s rights in the “Site maps” module

- “Enter into the program” - permission to enter the “Site maps” module. If the operator shall be able to view or edit site maps, including - to view the maps of sites when handling an alarm, then he/she shall have this permission.
- “Edit site maps” - permission to create new and edit the existing site maps.

8.1.6 Operator's Rights in "System Setup" Module

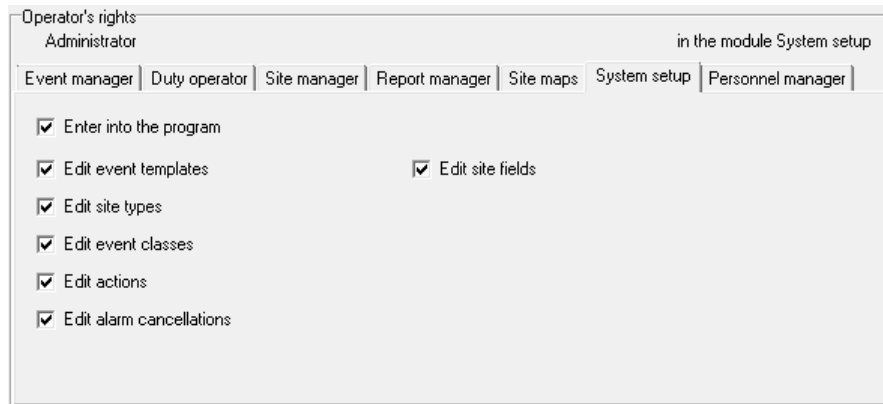


Figure 108: Operator's rights in the "System setup" module

- "Enter into the program" - permission to enter the "System setup" module. If the operator shall be able to view or change the settings of the system directories of the Security Center, then he/she shall have this permission.
- "Edit event templates" - permission to create new and edit the existing event templates. The event template determines how messages received from the site equipment will be decoded: which messages shall be considered alarm ones, which messages shall be considered as armings, etc. Changes that are made to the description of the template events in the "System setup" module will affect all sites that use the edited event template. It is strongly recommended not to make changes to the site event template without a valid reason.
- "Edit site types" - permission to create new and edit the existing site types. Types are the mechanism for grouping and filtering sites in the list. If you change, for example, rename a site type in the "System setup" module, this change will affect all sites for which the changed type is set.
- "Edit event classes" - permission to create new and edit the existing event classes. The event class is a key entity for all processes of the Security Center software related to the handling of the received events. Introduction of changes to event classes shall be done carefully and with great attention.
- "Edit actions" - permission to create new and edit the existing operator's actions, performed during alarm handling. To create and edit alarm handling scripts, the user shall have this permission.
- "Edit alarm cancellation" - permission to create new and edit the existing causes for canceling alarms. To create and edit alarm handling scripts, the user shall have this permission.
- "Edit site fields" - permission to edit the site fields (additional characteristics). Additional characteristics of the sites are useful in the event, when it is necessary to add information to the site card for which there is no special field, and it is not advisable to enter it into notes. This permission may be necessary for those users of the Security Center, whose task is to maintain the database of the site cards.

8.1.7 Operator's Rights in "Nord-LAN Key Configurator" Module

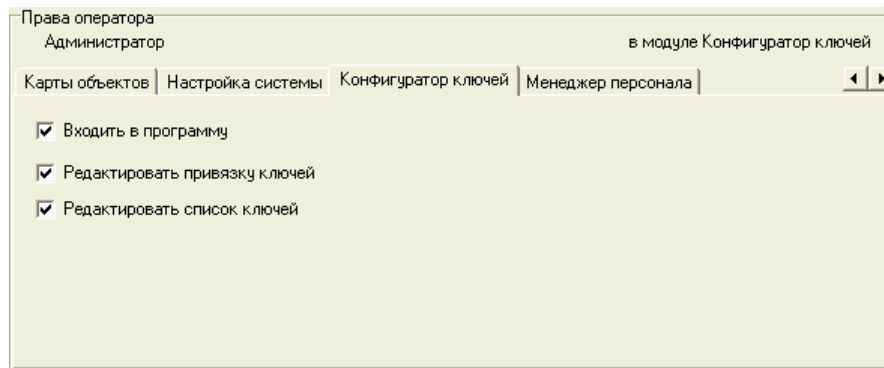


Figure 109: Operator's rights in the "Nord-LAN key Configurator" module

- "Enter into the program" - permission to launch the "Nord-LAN keys Configurator" module.
- "Edit key mapping" - permission to change the list of keys that allow you arm or disarm a specific site.
- "Edit list of keys" - permission to edit the general list of keys Touch-memory, intended for arming and disarming sites equipped with site devices "Nord-LAN".

8.1.8 Operator's Rights in "Personnel Manager" Module

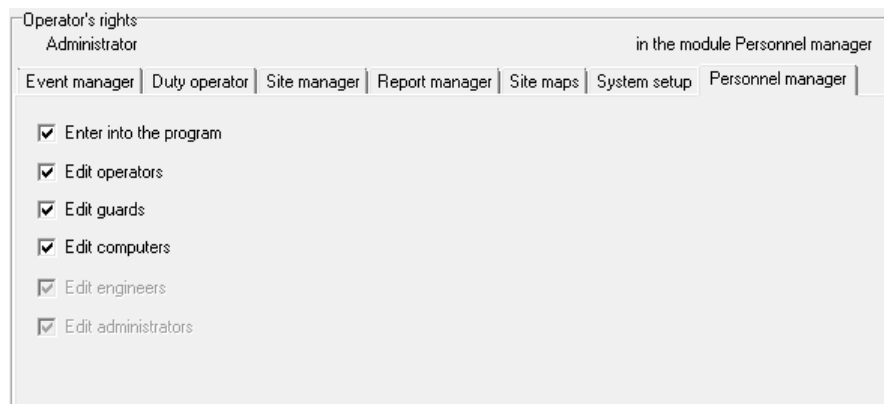


Figure 110: Operator's rights in the "Personnel manager" module

- "Enter into the program" - permission to launch the "Personnel manager" module.
- "Edit operators" - permission to indicate details for new operators, as well as to change the password and rights of the existing operators. A user with this permission cannot change his/her own rights in the Security Center modules, as well as the rights of the "Administrator".
- "Edit guards" - permission to change the list of guards. Guards are used for alarm handling - when registering activities related to a guard, the operator selects the guard, in relation to which the action is registered, from the list.
- "Edit computers" - permission to edit the list of computers on which the Security Center modules can be launched.
- "Edit engineers" - permission to edit the list of engineers for granting them remote access to sites.

8.2 guards

Guard name	Phone 1	Phone 2	Phone 3	Guard chief
East				
North				
West				
South				

New... Delete Save Cancel

Ready Total number of guards: 4 Operator:Administrator

Figure 111: "Guards" tab

On the "Guards" tab it is possible to edit the list of guards that are used in the Security Center software.

To save the changes made on this tab, the user shall have the "Edit Groups" permission for the "Personnel manager" module.

8.3 Computers

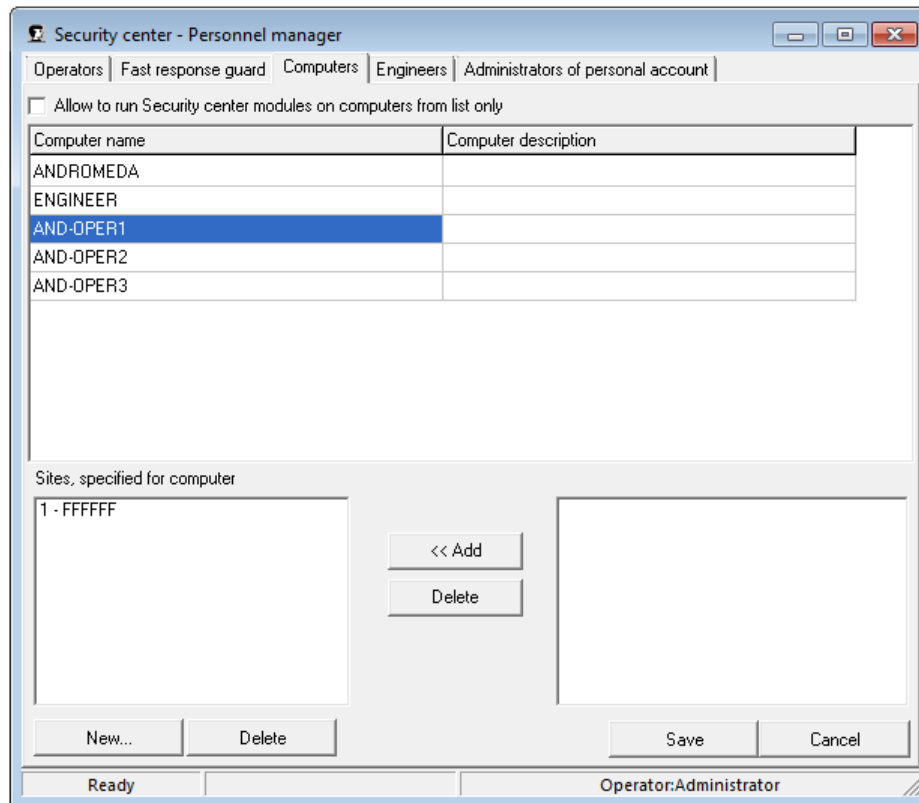


Figure 112: "Computers" tab

The "Computers" tab is intended to manage the list of computers on which the network workplaces of the Security Center software are allowed, and to manage the list of sites available on these computers.

To save the changes made on this tab, the user shall have the "Edit computers" permission for the "Personnel manager" module.

8.3.1 Allow to run Security Center modules on computers from list only

If this option is disabled, the Security Center modules can be run on any computer on the network. In this case, if the computer on which the Security Center modules are launched is not included in the list, it will be added there automatically.

If the restriction that allows the network workstations of the Security Center to be used only on those computers, that are included in the list, is included, then the attempt to launch any module of the Security Center on a computer that is not on the list will be rejected. Computers shall be added to the list manually.

8.3.2 Sites specified for computer

If necessary, for each computer it is possible to define a list of site numbers that are allowed to be downloaded by the Security Center modules, that are launched on this computer.

This function is useful, when the duty operators use the scheme of dividing sites between network workplaces. For example, on one computer, the operator works with sites from the first number to the third hundredth, on the next - from the three hundred first number to the six hundredth and so on.

8.4 Engineers {# personnel-manager-engineer}

[“Engineers” tab]id-07-13

The “Engineers” tab is used to manage the list of engineers that can be granted permissions to access remote site management.

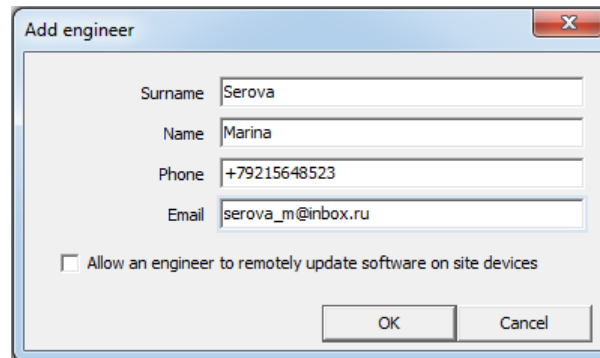


Figure 113: Add engineer

The list of engineers can be edited by the user who has the right to “Edit engineers”.

To add an engineer to the list, click the “New...” button. This opens the “Add engineer” window, in which the following fields shall be filled:

- “Surname” is the engineer surname. The surname and the name of the engineer shall be entered in Russian or Latin letters;
- “Name” - the engineer name;
- “Phone” - mobile phone number in international format;
- “Email” - the email address of the engineer.

After entering the data, click the “Add” button to add the engineer. At the same time, the surname, name and email of the created engineer will be displayed in the list of engineers. To cancel the changes, click the “Cancel” button.

After creating the engineer account, a letter will be sent to his/her email address. The engineer shall confirm the e-mail address to complete the registration in the Cloud by following the link in the letter, and then create and confirm the password for accessing the web interface for remote site programming.

To change information about the engineer, select him/her in the list and click “Change”. This opens the “Edit engineer” window. Changing the engineer email after creating an account in the system is impossible.

To remove the engineer, select him/her in the list and click “Delete”, after that confirm the deletion in the new window.

Save changes in the list of engineers by clicking the “Save” button. Otherwise, click on the “Cancel” button.

Information about the permissions granted to the engineer for access to sites is displayed in the list of “Permissions for engineer”. When selecting an engineer, the list contains information about the site number, its name, and date and time of the beginning and ending of the permission to access it.

To cancel the permission granted to the engineer for access to a site, select the permission in the list and click the “Delete permission” button.

9 Site Maps

With the help of the “Site maps” module, it is possible to create graphical schemes describing the site: terrain map with a map of possible ways of approaching the site, site photos, floor plans, etc.

After the plan of the site premises is developed, it is possible to place a diagram of the protection coverages.

When handling an alarm it is possible to view alarm zones on site maps in the “Duty operator” module.

There is no built-in graphic editor in the “Site maps” module, therefore it is recommended to create schemes using third-party tools. Ready images can be inserted into the map from BMP or JPG files as a background image. When preparing a background picture, select its size and resolution, taking into account the possible printing of the site map: no transformations are made, the background picture is printed in accordance with its parameters.

After the background picture is selected for the map, it is possible to place zones on it. For each zone, select the location and dimensions, as well as the way it is displayed in the active and passive state. After that associate the event code with the zone, the registration of which will mean the transition of the zone to the active state. Typically, this code is selected as the alarm code corresponding to the zone.

When the alarm site file is opened from the “Duty operator” module, the card containing the zone on which the alarm was received is active. Besides, the alarm zone can change visually - displayed alternately in the passive and active state.

It is also possible to specify a file for the zone. When the alarm site file is opened, the associated file will also be opened by means provided in the operating system for its file type. For example, if you specify a document containing important information about the site as the file, this document will be opened together with the map file.

If the Security Center software is used on the network, then the site map file shall be saved to a folder that is accessible to all users on the network. It shall be remembered that even if this folder is local for the computer where the site maps are edited, it is still necessary to use the absolute path to the folder when saving.

When saving a new site map file or saving it with a different name, the “Site map” field - its value can be viewed and changed in the “Site manager” module - is updated automatically.

10 Duty Operator

The “Duty operator” module is intended to monitor the operational status of the sites, view incoming events and record the operator’s actions while handling alarms.

Before starting working in the “Duty operator” module, make sure that the “Event manager” module is running. If during the operation of the “Duty operator” module a connection error occurs with the “Event manager” module, a window with the error appears.

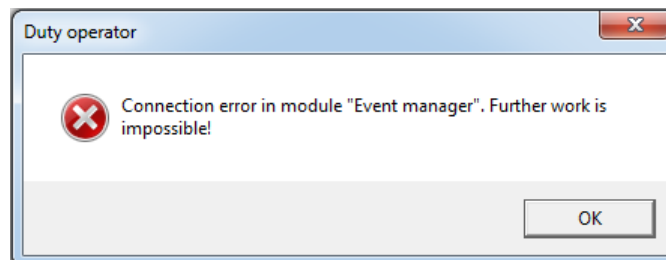


Figure 114: Message of connection error with “Event manager” module

To launch the “Duty operator” module, the user shall have the “Enter into the program” permission for this module.

Just like the rest of the Security Center modules, the “Duty operator” module downloads only those sites, the use of which is allowed on the computer on which it is running. It is possible to specify the intervals of site numbers that can be used on a particular network workplace in the “Personnel manager” module.

10.1 Module Main Window

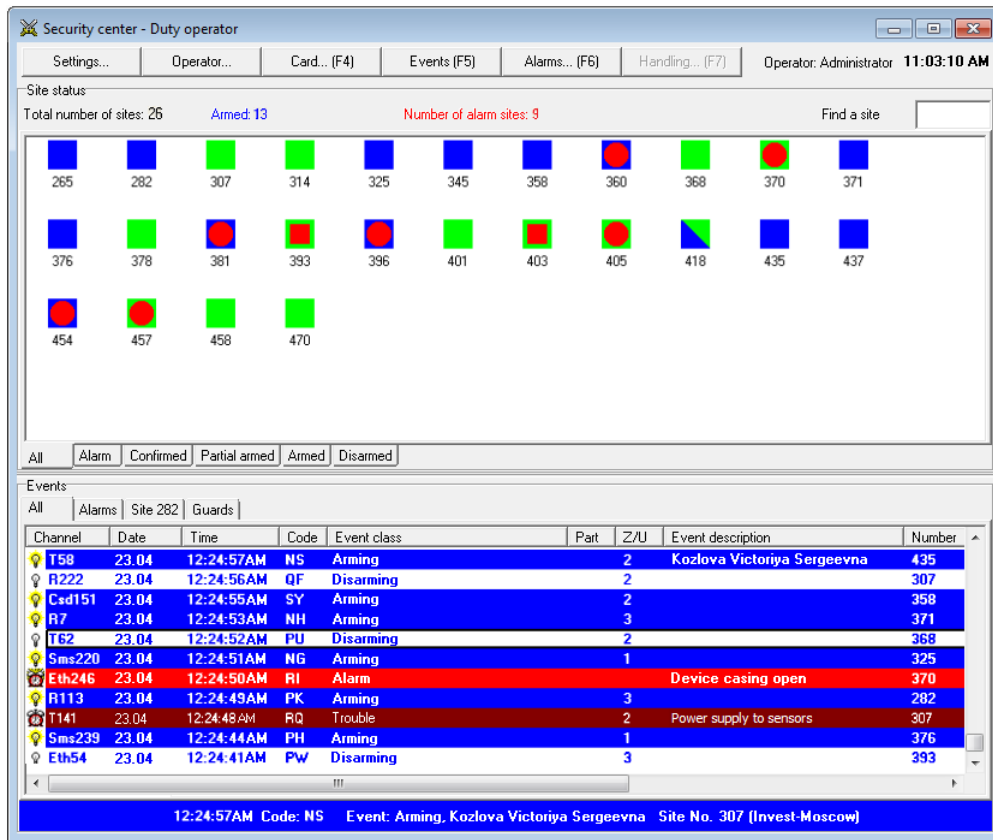


Figure 115: Module main window

The main window of the “Duty operator” module is divided into two parts. The upper part is intended for displaying sites, the lower one for displaying the received events.

10.2 Quick Access Toolbar

The toolbar contains buttons that allow to access the most requested functions of the “Duty operator” module. In addition to the name of the function, a key or a combination of keys is given in parentheses to access the function from the keyboard.



Figure 116: Quick Access Toolbar

Click on the “Settings” button to open the settings window of the “Duty operator” module. In order for the user to make changes to the module settings, he/she shall have the “Change settings” permission for the “Duty operator” module.

Click on the “Operator...” button to change the operator registered in the “Duty operator” module. After the button is clicked, the operator registration window will be displayed in the module, the “Duty operator” module will not be stopped: the reception of events will continue, and when an alarm is received, the alarm handling window will be displayed.

Click on the “Card...” button to access the “Site card” window. The window of the current site will be displayed. The current site will be the site selected in the site list, or the site which event is selected in the event list, depending on the focused window.

Click on the “Events” button to activate the “Events from site” tab in the event window and to display the events from the current site in the list of events on this tab. The rules for selecting the current site will be the same as when clicking on the “Card...” button.

Click on the “Alarms...” button to access the “Alarm information” window. After the window is opened, the card of the current site and the handling log of the last alarm from this site will be loaded into it.

Click on the “Handling...” button to open the “Alarm handling” window. The button is active if the operator, who launched the module, has permission to “Handle alarms” or “Cancel alarm”. Besides, the button is only available if the current site is an alarm site.

10.3 Sites

At the top of the “Site status” window, the total number of sites loaded by the module, number of sites that are currently armed, and number of sites which alarm handling has not yet been completed, is given.

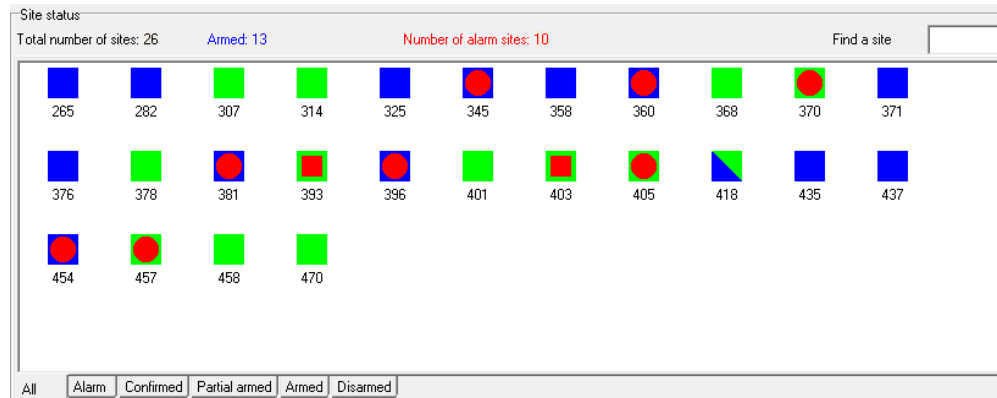


Figure 117: “Site status” window, “All” tab

Protected sites are displayed in the “Duty operator” module in the form of icons in the “Site status” window. The icon color displays the current status of the site. If it is blue, then the site is armed, green is disarmed, gray - the site is disabled. If one part of the icon is blue and the other is green, the site is partially armed. A red circle or square means that there is an alarm on the site, which has not yet been completed, while a red circle indicates that no action has been recorded for this alarm.

It shall be remembered that alarms received from disabled sites are handled by the system automatically, immediately after reception. The arming and disarming events received from disabled sites also do not change their status. Thus, the disabled site cannot be alarming, armed, or disarmed. It is always displayed with a gray icon.

The site icons are displayed on tabs that group sites by basic states. The purpose of tabs is easy to guess by their names:

- the “All” tab displays all sites that are allowed to be used in this workplace;
- on the “Alarms” tab, the sites for which there are unhandled alarms are displayed;
- the “Partial armed” tab displays sites that were partially armed. In this case, not the whole site is protected, but only its particular zones;
- the “Armed” tab displays sites that are currently armed;
- the “Disarmed” tab displays sites that are currently disarmed, or sites which status is not defined, because they have never sent any events about arming or disarming.

To quickly find a site by number, use the field to search for a site in the upper right corner of the “Site status” window. Search for a site is carried out on the same tab that is currently active and is executed “on the fly”, as the digits of the site number are entered in the search field.

10.3.1 Tooltip {# duty-opertor-tooltip}

When you hover over a site in the “Site status” window, a tooltip appears, with which the Security Center operator can quickly obtain the information about the required site. The tooltip contains the following information:

- number, name and address of the site;
- status of the site or its parts (armed or disarmed);
- description of the alarm situation at the site;
- information about the guards called to the site.

10.3.2 Site Status

The tooltip contains information about the site status if at least one site is armed or disarmed.

282, Invest-Moscow Ligovsky Ave 39		
14:56	Window	Morozov Ivan S...
14:54	Door	Petrenko Vadim F...
14:55	Safe	User 4
	Cashbox	No information

Figure 118: "Site status" window, tooltip, Site status

The tooltip indicates the time of the site arming or disarming if the event occurred within the last 24 hours, or the date if the event occurred earlier. The background color indicates the site current status: blue - the site is armed, green is disarmed. It shall be noted that when the “Show status color in reverse” parameter is selected, the colors that show the status of the protected sites are inverted. Besides, the tooltip informs about the user who completed the site arming or disarming.

If the site is divided into sections, the tooltip provides information about the status of each site part. In this case, the tooltip contains the following information: time of the last arming or disarming, part description, and the user who performed the operation. The last registered event is displayed in bold.

10.3.3 Alarm

If an alarm situation is registered at the site, the tooltip contains information about the alarm. If several alarm events are registered at the site, the tooltip displays information about the first and last registered alarm.

282, Invest-Moscow Ligovsky Ave 39		
15:03	Door and main office scope	
15:03	Window	Morozov Ivan Ser...
14:54	Safe	Petrenko Vadim F...
15:03	Door	User 4
	Cashbox	No information

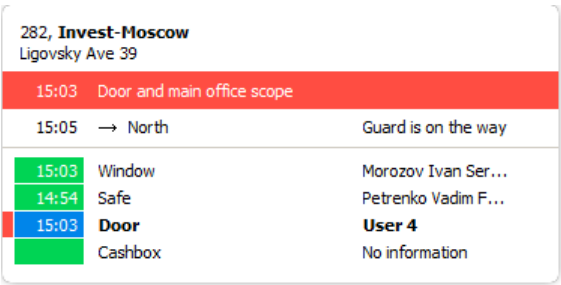
Figure 119: "Site status" window, tooltip, Alarm

The tooltip indicates the time of the alarm if the event occurred within the last 24 hours, or the date if the event occurred earlier. The red background indicates an alarm situation at the site.

If the site is divided into parts, the alarm parts are red.

10.3.4 Guards

The tooltip contains information about the Guard, if the Guard is called to the site (“Guard en route”) or is present at the site (“Guard on site”). If the Guard call to the site is canceled, the call information is not displayed.



282, Invest-Moscow Ligovsky Ave 39		
15:03	Door and main office scope	
15:05	→ North	Guard is on the way
15:03	Window	Morozov Ivan Ser...
14:54	Safe	Petrenko Vadim F...
15:03	Door	User 4
	Cashbox	No information

Figure 120: "Site status" window, tooltip, Guard

The tooltip indicates the time of the Guard call or arrival to the site, if the event occurred within the last 24 hours, or the date if the event occurred earlier.

10.3.5 Context Menu

When you right-click on the site icon, a context menu is displayed, with which you can quickly access information about the site.

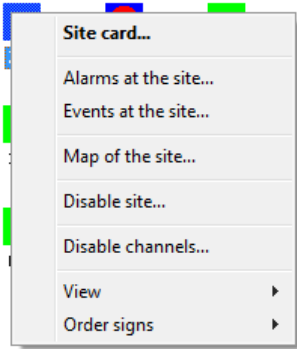


Figure 121: "Site status" window, context menu

Selecting the “Site card...” menu item to access the window displaying the card fields of the selected site. The window appearance and its description are presented below, in the section “Site Card” Window”.

The “Alarms at the site...” item is intended for access to the window, displaying information about the alarms at the site, which handling is completed. In addition to the alarms themselves, this window displays the operator’s alarm handling log. See more information about this window below, in section “Alarms” Window”.

Select the “Events at the site” menu item, to activate the “Site” tab at the bottom of the main window of the “Duty operator” module. The tab is intended to display events for a particular site and events from the selected site will be loaded into it.

Use the “Map of the site...” item to open the map file (graphic plan) of the site. If a graphic format file (BMP or JPG) is specified as the site map, it will be opened for viewing in the special window of the “Duty operator” module. If the site map is created with the help of the “Site maps” module, this module will be opened for viewing it.

The “Disable site” item in the context menu allows to temporarily disable any Security Center site, saving all information about the site in the system. This feature is convenient during routine maintenance or repair of equipment installed at the site.

The Security Center sites can be disabled by the operator with the corresponding permission. Select the “Disable site” item to view the “Site disabling” window, which contains information about the site number and name. Enter

the time during which the site shall be disabled in the “Disable for” field of this window. After this time, the site will be enabled automatically. Enter the time in minutes, the maximum allowed value is 180 minutes. Specify the reason for the site temporary disabling in the “Reason for disconnection” field. This field is required. Before clicking on the “Disable site” button, study the warning that automatically alerts about the time when the site is disabled automatically (for example, “The site will be enabled automatically in 120 minutes, today at 22:16”).

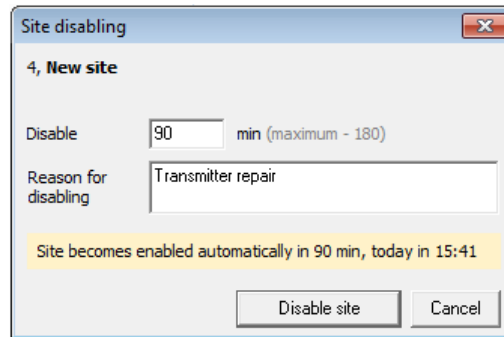


Figure 122: “Site status” window, “Site disabling” window

The event log displays information about the site disabling, namely: date and time of the site disabling; operator who performed disabling; time and reason for disabling.

The “Enable site” item allows to enable the previously disabled Security Center site before the expiration of the time specified during disabling.

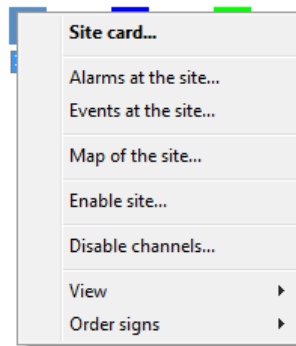


Figure 123: “Site status” window, context menu, “Enable site” item

Select the “Enable site” item to view the “Site enabling” window, which contains information about the site number and name and time of the site automatic disabling. To enable the site, click the “Enable site” button of this window.

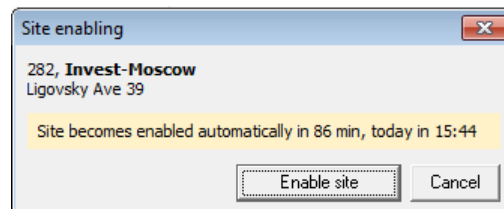


Figure 124: “Site status” window, “Site enabling” window

The event log displays information about the site enabling, namely: date and time of the site enabling; enabling mode (automatic or manual). If the site is manually enabled, the operator who performed the operation is specified for the event.

The “Disable channels” item in the context menu allows to temporarily disable any site channel, saving all information about the channel in the system. This function is convenient in case of a malfunction of the equipment used to for the communication channels.

The communication channel can be disabled by the operator, who has the right to “Disable channels for site”. Select the “Disable channels” item to view the “Site channels disabling” window, which contains information about the site number and name. Select one or several communication channels for disabling in the “Channels that can be disabled” section: Radio, Phone, System, Ethernet, GPRS, SMS, and CSD. Enter the time during which the channels shall be disabled in the “Disable for” field of this window. After this time, the channels will be enabled automatically. Enter the time in minutes, the maximum allowed value is 180 minutes. Specify the reason for the channel temporary disabling in the “Reason for disconnection” field. This field is required. Before clicking on the “Disable channels” button, study the warning that automatically alerts about the time when the channels are disabled automatically (for example, “The channel will be enabled automatically in 120 minutes, today at 16:31”).

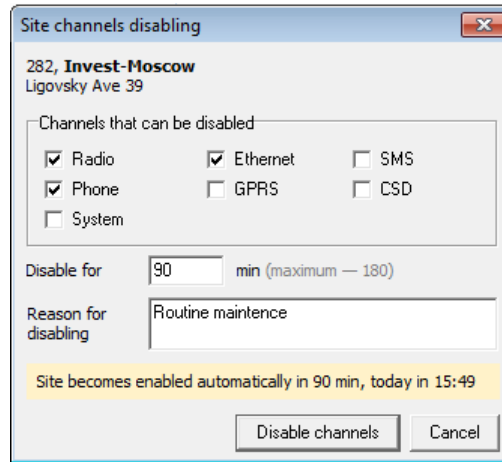


Figure 125: “Site status” window, “Site channels disabling” window

The event log displays information about the channel disabling, namely: date and time of the channel disabling; channel name; period and reason for disabling.

The “Enable channels” item allows to enable the previously disabled channels before the expiration of the time specified during disabling.

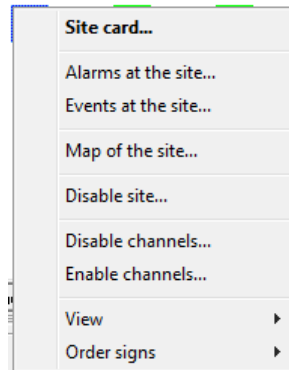


Figure 126: “Site status” window, context menu, “Site channels enabling” item

Select the “Enable channels” item to view the “Site channels enabling” window, which contains information about the site number and name. Select one or several communication channels for enabling in the “Channels that can be disabled” section and click on the “Enable channels” button:

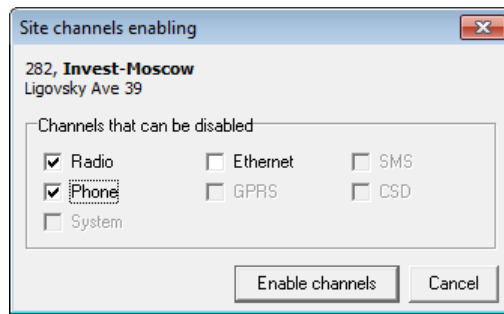


Figure 127: "Site status" window, "Site channels enabling" window

The event log displays information about the channel enabling, namely: date and time of the channel enabling; enabling mode (automatic or manual). If the channel is manually enabled, the operator who performed the operation is specified for the event.

The "View" item is intended to change the way the list of sites is displayed.

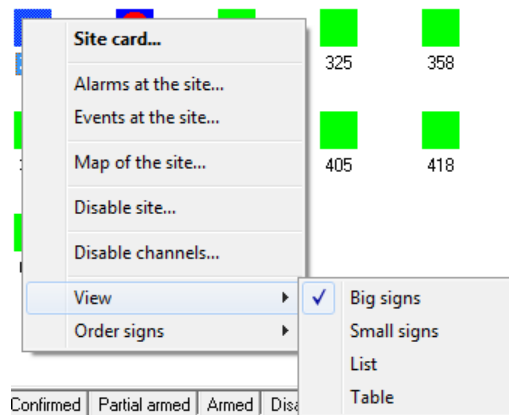


Figure 128: "Site status" window, context menu, "View" item

"Large icons", "Small icons", "List" items differ only in the size of the site icon and the way items are scrolled in the window. As for the "Table" item, if it is selected in the "Site status" window, a list of sites similar to the list of sites used in the "Site manager" module will be displayed.

Site status						
Total number of sites: 26			Number of alarm sites: 10			
		Find (F2)	Find next (F3)			
	Number	Name	Address	Telephone	Telephone	On map
	282	Invest-Moscow	Ligovsky Ave 39			No
	314	McDonolde	Marata Street? 86	895-74-85		No
	358	SHOP	Sadovaya St. 62	145-78-25		No
	381	McDonald's	Sredniy Prospekt V.o. 29/1	895-63-25		Yes
	393	Raiffeisen Bank	Kamennostrovsky avenue 13/2	741-85-74	741-85-78	No

Figure 129: "Site status" window, "All" tab, "Table" view

A detailed description of functions of such list of sites is given in the chapter devoted to the "Site manager" module. It shall be noted here that this list of sites allows to search for a site using the majority of significant fields, and not only by number, and in addition, the operator can see the fields of the site necessary to him/her without opening a separate window with the site card.

The "Arrange icons" context menu item is intended to change the way the icons of the sites are sorted when displayed.

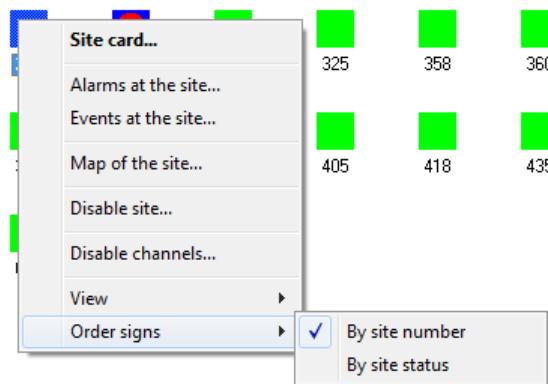


Figure 130: "Site status" window, context menu, "Arrange icons" item

If you select sorting by site number, the site icons in the list will be displayed in ascending order of the site numbers. If you select sorting by site status, the site status will be taken into account in the first instance.

In this case, first, sites will be displayed for which there are undefined alarms, and the first ones in the list will be those sites which alarm handling has not yet begun. After the alarm sites, sites that are armed will be displayed. The most recently disarmed and disabled sites will be displayed in the list as last, as well as sites which state is not defined.

It shall be noted that the item highlighted in the context menu in bold is the default item and will be executed in case of double clicking on the site with the left mouse button. If there are no undefined alarms for the selected site, then the item "Site card..." is the default item. If the alarm site is selected, then the default item is "Alarm handling...", after it is selected a window intended for the site alarm handling is opened:

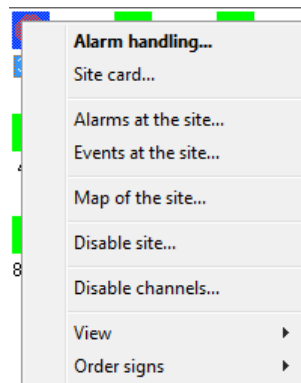


Figure 131: "Site status" window, context menu, "Enable site" item

10.4 Events

At the bottom of the main window of the "Duty operator" module, the received events and the status of the guards are displayed.

Events are divided into three categories, each of which is displayed on a separate tab.

10.4.1 All

Channel	Date	Time	Code	Event class	Part	Z/U	Event description	Number
S	12.09	3:28:01 PM	ZZ...	Connection alarm (phone)			No phone-related events	345
T58	12.09	3:27:54 PM	NS	Arming	2		Kozlova Victoriya Sergeevna	435
R222	12.09	3:27:51 PM	QF	Disarming	2			307
Csd151	12.09	3:27:24 PM	SY	Arming	2		Arming	358
R7	12.09	3:27:15 PM	NH	Arming	3			371
T62	12.09	3:25:57 PM	PU	Disarming	2		Temporary code	368
Sms220	12.09	3:25:51 PM	NG	Arming	1			325
Eth246	12.09	3:25:50 PM	RI	Tamper alarm	1		Equipment unsealed	370
R113	12.09	3:25:47 PM	PK	Arming	3			282
T141	12.09	3:19:31 PM	RQ	Trouble	2		Power supply to sensors	307
Sms239	12.09	3:15:47 PM	PH	Arming	1			376

Figure 132: "Events" window, "All" tab

The "All" tab displays all the significant events received from the sites loaded by the "Duty operator" module. In order to clarify what events are considered significant, it shall be mentioned that a filtering mechanism for test and duplicate events, which allows the operator of the Security Center to be released from handling information that does not matter to him/her, has been implemented in the Security Center software. The event filtering mechanism is controlled with the settings in the "Event manager" module. See the chapter devoted to this module to get acquainted with the details of this mechanism. Here it shall be mentioned that events that the significant events are those, that are not test or repeated, and only they are displayed on the "All" tab. If the duty operator for some reason needs to see all events received from a particular site, then he/she can do it using the "Events from site" tab, which is described below.

The following information is displayed in the columns of the table of the "Events" window:

- "Channel" - type and number of the channel via which the event is accepted. The value of this parameter is determined by the event source with which the event was received. See more information about existing sources of events and their settings in the chapter on the module in the section "Event sources".
- "Date", "Time" - date and time of the event reception by the monitoring station equipment. If the information transmitted by the receiving equipment of the monitoring station does not contain the date and time of the event reception, then this column will display the date and time of recording the event in the database of the Security Center software.
- "Code", "Event class", "Part", "Z/U", "Event description" are the parameters obtained as a result of decoding of the received event in accordance with the site description. See more details about the parameters in the chapters on the "System setup" and "Site manager" modules, in the sections that describe the event templates.
- "Number", "Name", "Address" are the fields of the same name of the site card from which the event was received.

Events in the list can be sorted by any of the displayed columns. To do this, left-click on the necessary column.

When you right-click on the event, a context menu is displayed, with which you can quickly access information about the site.

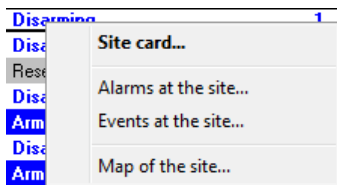
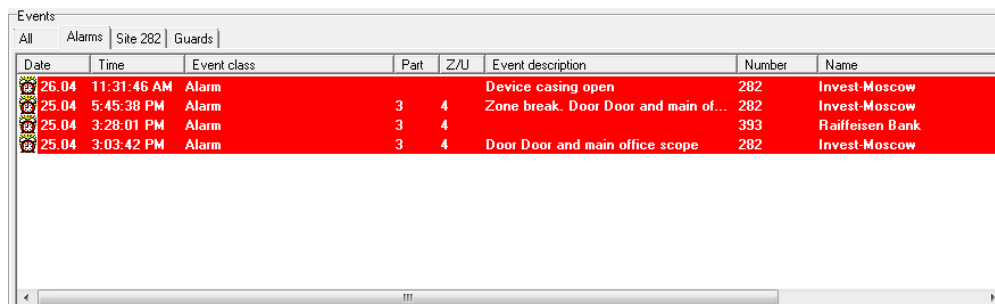


Figure 133: "Events" window, context menu

The purpose of the menu items is completely similar to that in the context menu displayed when clicking on the site icon in the "Site status" window.

10.4.2 Alarms

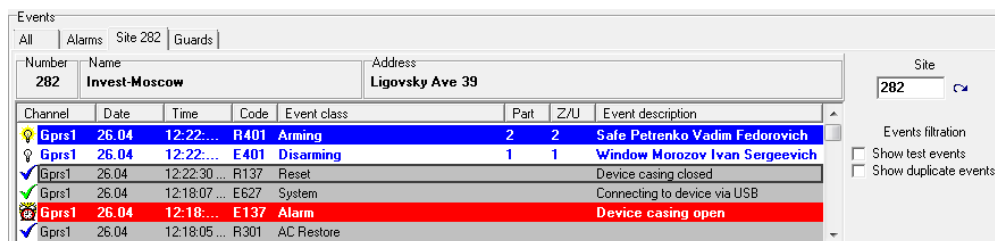


Date	Time	Event class	Part	Z/U	Event description	Number	Name
26.04	11:31:46 AM	Alarm			Device casing open	282	Invest-Moscow
25.04	5:45:38 PM	Alarm	3	4	Zone break. Door Door and main of...	282	Invest-Moscow
25.04	3:28:01 PM	Alarm	3	4	Door Door and main office scope	393	Raiffeisen Bank
25.04	3:03:42 PM	Alarm	3	4	Door Door and main office scope	282	Invest-Moscow

Figure 134: "Events" window, "Alarms" tab

The "Alarms" tab displays alarm events that have not yet been completed.

10.4.3 Events at the Site



Channel	Date	Time	Code	Event class	Part	Z/U	Event description
Gprs1	26.04	12:22:00	R401	Arming	2	2	Safe Petrenko Vadim Fedorovich
Gprs1	26.04	12:22:00	E401	Disarming	1	1	Window Morozov Ivan Sergeevich
Gprs1	26.04	12:22:30	R137	Reset			Device casing closed
Gprs1	26.04	12:18:07	E627	System			Connecting to device via USB
Gprs1	26.04	12:18:00	E137	Alarm			Device casing open
Gprs1	26.04	12:18:05	R301	AC Restore			

Figure 135: "Events" window, "Events at the site" tab

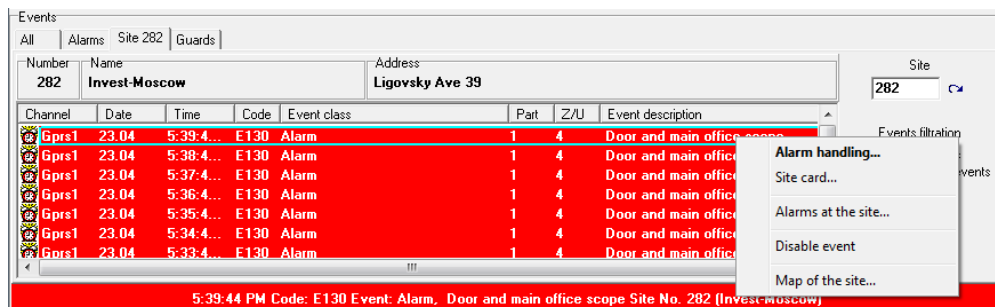
The "Events at the site" tab displays a summary of the selected site, as well as the events received from it.

To change a site, which events are displayed on the "Events at the site" tab, enter its number in the "Change site" field and press the "Enter" key or the arrow button.

Use the "Show tests" parameter to enable or disable display of filtered test events received from the site. Similarly, use the "Show duplicates" parameter to enable or disable display of filtered duplicate events received from the site.

Right-click on the event to display the context menu, with which you can temporarily disable the event.

Events can be disabled by the operator with "Disable event codes" permission. If you select the "Disable event" option, a dialog box with information about the number, name and address of the site appears. Besides, the following is indicated: event code; event class; number of the part in which the event occurred; number of the zone in which the event occurred; description of the event.



Channel	Date	Time	Code	Event class	Part	Z/U	Event description
Gprs1	23.04	5:39:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:38:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:37:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:36:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:35:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:34:40	E130	Alarm	1	4	Door and main office scope
Gprs1	23.04	5:33:40	E130	Alarm	1	4	Door and main office scope

Figure 136: "Events" window, context menu, "Disable event" item

Enter the time during which the event shall be disabled in the "Disable for" field of this window. After this time, the event will be enabled automatically. Enter the time in minutes, the maximum allowed value is 90 minutes.

Specify the reason for the event temporary disabling in the “Reason for disconnection” field. This field is required. Before clicking on the “Disable event” button, study the warning that automatically alerts about the time when the event is disabled automatically (for example, “The event will be enabled automatically in 45 minutes, today at 21:51”).

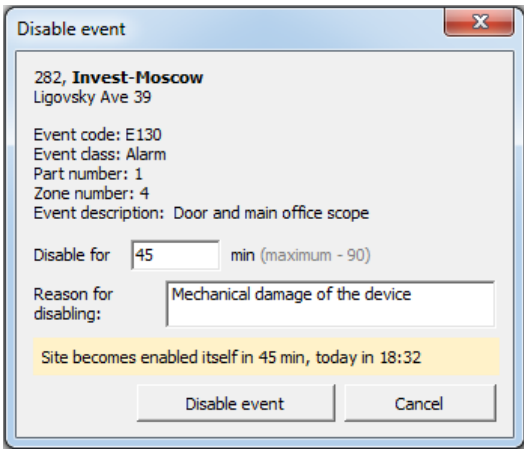


Figure 137: “Events” window, “Disable event” window

The event log displays information about the event disabling, namely: date and time of the event disabling; event code; part and zone numbers, period and reason for disabling.

The “Enable event” item in the context menu allows to enable a previously disabled event before the expiration of the period, specified for disabling.

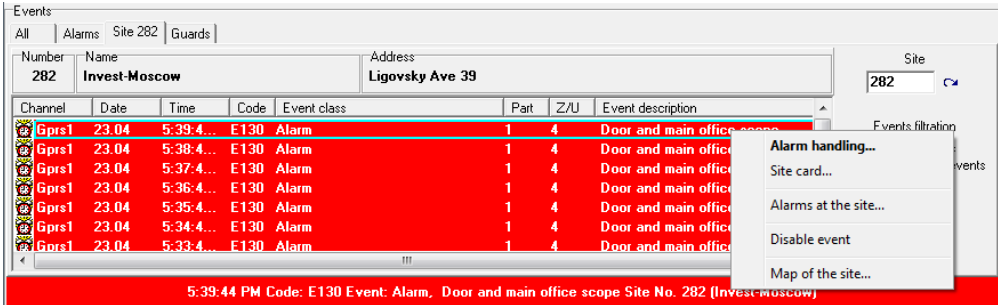


Figure 138: “Events” window, context menu, “Enable event” item

If you select the “Enable event” item, a dialog box with information about the number and name of the site appears. Besides, the following is indicated: event code; event class; number of the part; number of the zone; description of the event. The window also indicates the time of the event automatic enabling. To enable the event, click on the “Enable event” button of this window.

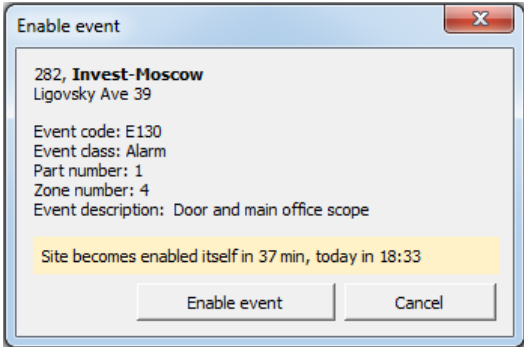
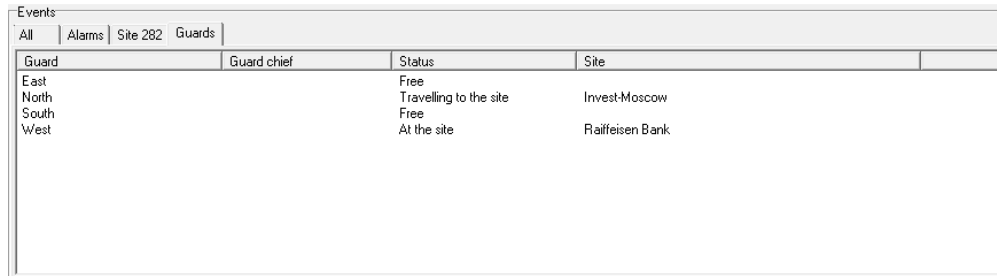


Figure 139: “Events” window, “Enable event” window

The event log displays information about the event enabling, namely: date and time of the event enabling; event

code; part and zone numbers; enabling mode (automatic or manual). If the event is manually enabled, the operator who performed the operation is specified for the event.

10.4.4 Status of guards



Guard	Guard chief	Status	Site
East		Free	
North		Travelling to the site	Invest-Moscow
South		Free	
West		At the site	Raiffeisen Bank

Figure 140: "Events" tab, "Guard" tab

The "Guards" tab displays the guards used by the Security Center. In addition to the general information about the guards on the tab, their current status is displayed ("Free", "Travelling to the site", "At the site"), and the name of the site to which the guard is called, if it is currently occupied.

10.5 Alarm handling

The window is intended to handle an alarm by the operator, who has "Handle alarm" permission. Alarm handling means recording the actions performed by the operator in the alarm log. This log is maintained in the "Duty operator" module, information from it can be printed in the "Report manager" module.

When the alarm event is received, the "Alarm handling" window opens automatically. This feature can be disabled in the settings of the "Duty operator" module. If you need to re-open the "Alarm handling" window, double-click on the alarm site or alarm event that you need to handle.

When handling an alarm, it is important to understand that if another alarm is received from the site during the alarm process, both these alarms will be combined into a group and then they will be handled together. In the same way, these events will be displayed together when viewing handled alarms and when creating alarm reports in the "Report manager" module.

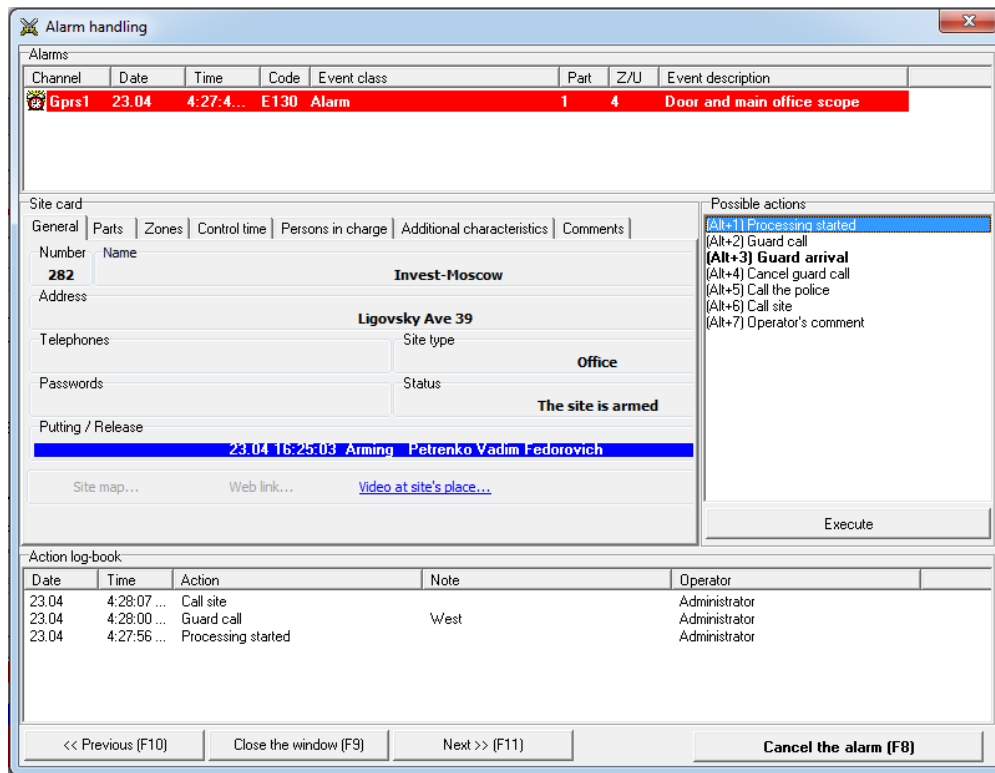


Figure 141: "Alarm handling" window

At the top of the "Alarm handling" window, all site alarms, which shall be handled, are displayed.

In the middle part of the window there is a site card, on different tabs of which information about the site is displayed. The purpose of the displayed site fields is discussed in detail in the chapter devoted to the "Site manager" module.

The link "Video at site's place" allows the operator to view the video transmitted by the cameras installed on the site. When the link is clicked, a window opens, where live video is displayed from all cameras installed on the site connected to the video router.

To view video from the cameras, you shall have Adobe Flash Player installed on the computer with the latest available version that can be downloaded from the [official Adobe website](#).

A list of actions, that the operator can perform during an alarm handling, is located to the right of the site card. This list includes the actions that are assigned to the classes of the events that shall be handled. Thus, for different alarms, the operator sees various possible actions, which allows to help and manage the operator's work.

The first ten actions in the list can be registered using the numeric keys on the keyboard as shortcut keys. If necessary, instead of pressing a single number key, it is possible to press it in combination with the "Alt" key. The option with which it is possible to enable or disable the use of the "Alt" key for quick access to actions is in the program settings.

See more information on how to create possible actions during alarm handling, as well as how to assign actions to event classes, in the chapter devoted to the "System setup" module.

10.5.1 Call a Guard to the Site

When registering an action with the "Call a guard" type, a window is displayed in which the operator shall select the guard that he/she called on the site.

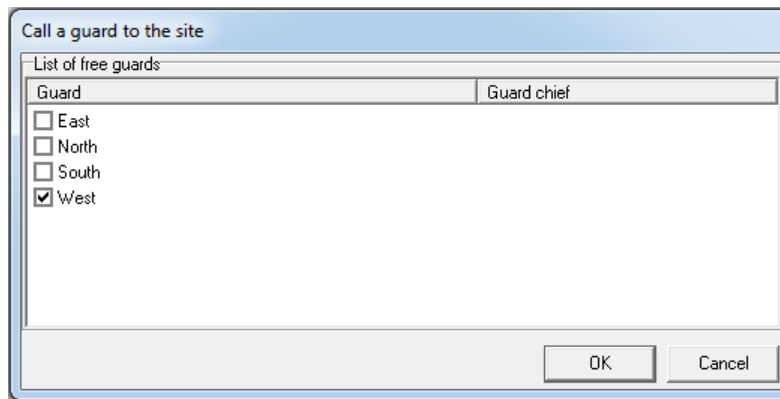


Figure 142: "Call a guard to the site" window

To register a guard call, check it in the list of guards and press the "OK" button. It is possible to check a guard in the list in two ways: by left-clicking the check box to the left of the group name, or by double-clicking the left mouse button anywhere on the line, in which the guard name and its senior are displayed.

If the operator registers the guard's arrival to the site or the cancellation of the guard call, the same window is displayed, but only the guards that were called to the site will be displayed in the list.

It is possible to change the list of guards in the "Personnel manager" module. See more information on how to do this in the chapter devoted to this module.

10.5.2 Operator's comment

If the operator registers an action with the type "Operator's comment", then the text of the comment can be entered in a special window.

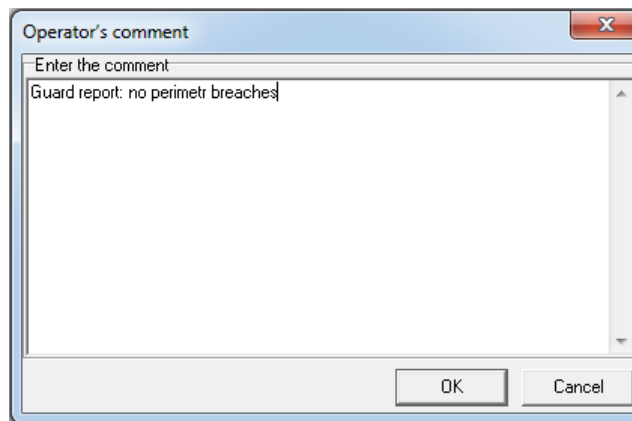


Figure 143: "Operator's comment" window

The maximum length of the operator's comment is limited to four thousand characters.

To finish entering the comment from the keyboard, click on the "Enter" button. To enter a new line when entering a comment, press the key combination "Control" + "Enter".

10.5.3 Alarm Cancellation

If the alarm handling is completed and the operator shall register this, then he/she shall press the "Cancel the alarm (F8)" button. The alarm can be canceled by the Security Center operator with the corresponding permission.

The operator can select the brief result of the alarm handling or cause for canceling it in the "Alarm cancellation" window.

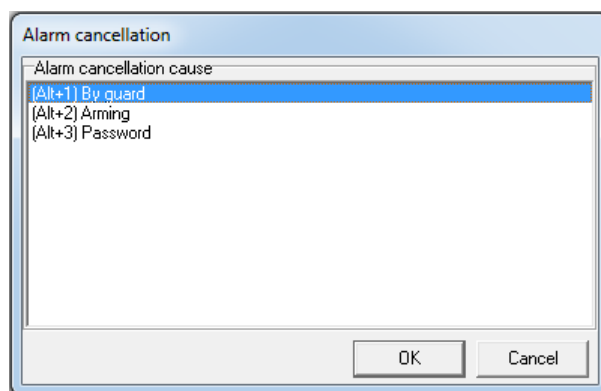


Figure 144: "Alarm cancellation" window

Reasons for alarm cancellation, displayed in the list, are assigned to the alarm event classes, for which the alarm cancellation is registered.

Also, as in the list of possible actions, the first ten reasons for alarm cancellation can be selected with the help of numeric keys or their combination with the "Alt" button.

To analyze the causes of alarms and make decisions intended to optimize the work of the monitoring station personnel, it is recommended to maintain a list of possible cancellations of alarms in the current state for each type of alarm. Besides, for the reliability of the analysis, the operator shall correctly register the actual reasons for canceling alarms. An instruction for the operator, which includes typical alarms and situations that lead to them, recommended scheme for handling typical alarms and an explicit indication of the reason for canceling the alarm, which the operator shall register in each case, is extremely useful for the analysis reliability, especially at first.

10.6 Site Card

The "Site card" window is intended for access to information about the site. To open it, double-click on the icon of a site that is not alarming, or right-click on the icon of any site and select the "Site card..." item in the menu, that appears.

Besides, the site card can also be opened from the menu that appears when you right-click on any events from the site. Double-clicking the left mouse button on any event that is not alarming will result in a similar result.

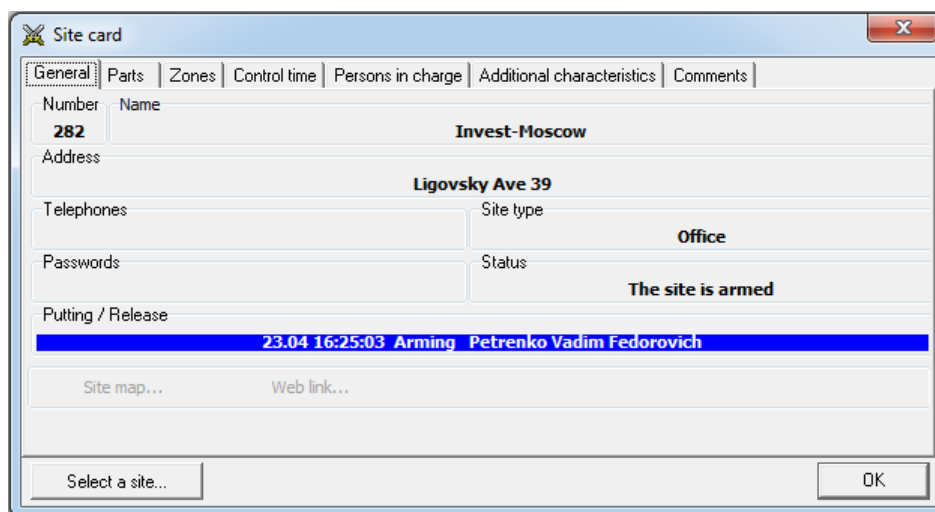


Figure 145: "Site card" window

All information about the site that the duty operator may need is displayed on the tabs of the "Site card" window.. The purpose of the displayed site fields is discussed in detail in the chapter devoted to the "Site manager" module.

10.7 Information about Alarms

The “Information about alarms” window allows the operator to view the log of handling alarms, which were canceled.

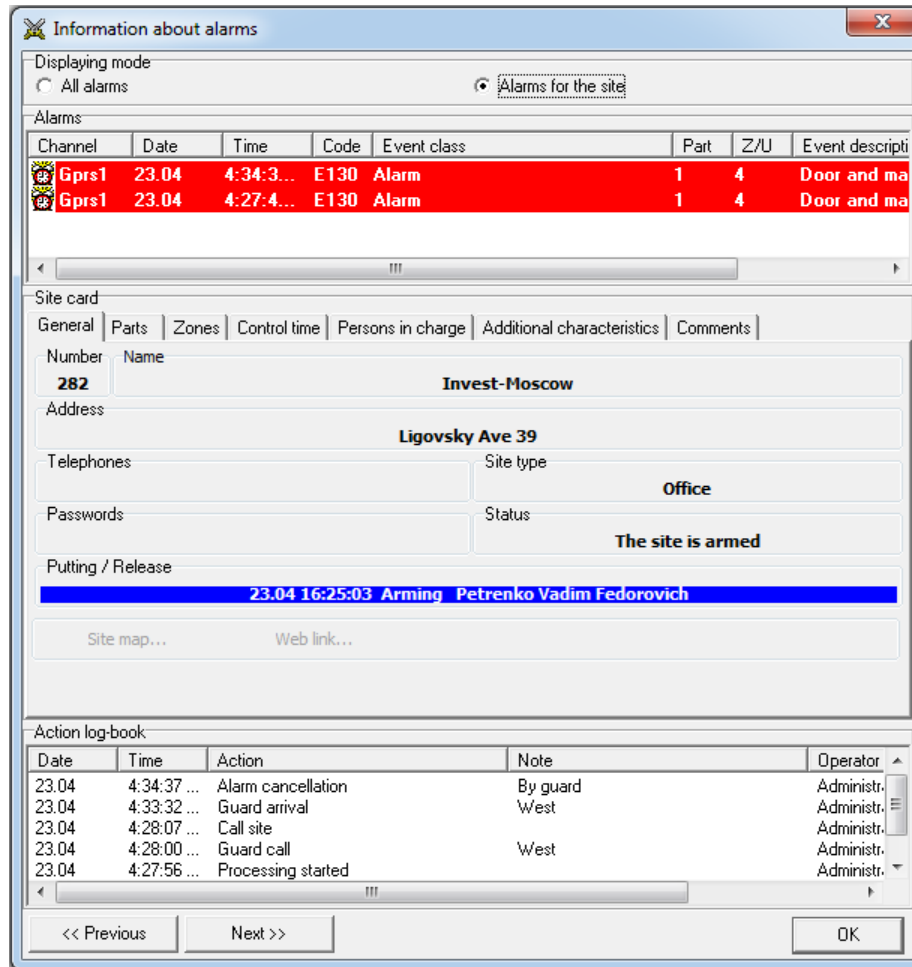


Figure 146: “Information about alarms” window

Switch of information display mode when moving to the next or previous alarm is located in the upper part of the window. In the “All alarms” mode, if you press “<< Previous” or “Next >>” button, the program will switch to the previous or next alarm in chronological order. In the “Alarms for the site” mode, the program will switch to the alarms for the site that is displayed in the window.

The list of alarms, for which the log is displayed, is located below the information display switch. See more information about assigning fields in the alarm list above, in the section on the “Event list” window.

The site card is displayed below the list, in the middle of the screen. The purpose of the displayed site fields is discussed in detail in the chapter devoted to the “Site manager” module.

The list of actions registered by the operator during alarm handling is displayed at the bottom of the screen. The list is displayed in chronological order and includes the actions registered by all operators who participated in the alarm handling.

10.8 Module Setup

Access to the settings of the “Duty operator” module is regulated by rights that can be set in the “Personnel manager” module. Besides, that it is possible to limit an operator access to the module settings, it is also possible to prohibit the operator from closing the “Duty operator” module. These restrictions can be useful not only for

inexperienced operators, but also for all duty operators, since accidentally closing the module or blocking the main window of the module with the settings window can negatively affect the process of alarm handling.

10.8.1 Common

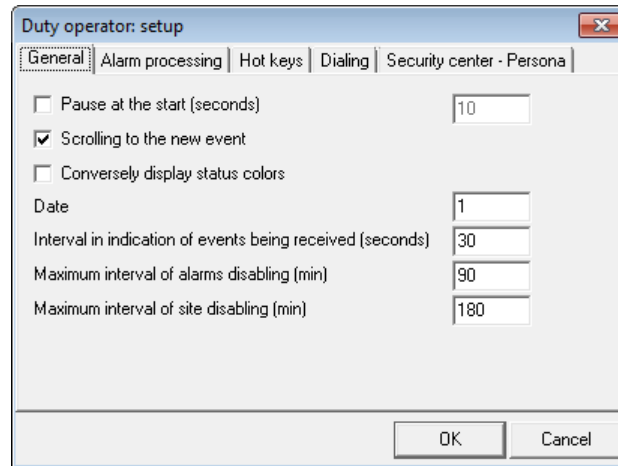


Figure 147: "Setup" window, "Common" tab

The "Pause at the start" parameter sets a pause, during which the "Duty operator" module will be delayed at the start. The parameter can be useful, if the icons of the "Event manager" and "Duty operator" modules are located in the "Startup" folder or if they are downloaded automatically at the start of the operating system in another way. To start the "Duty operator" module, the running "Event manager" module is needed, and it may take some time to start and fully initialize the module.

If the value for the "Scrolling to the new event" parameter is set, then when you receive new events from sites, the list of events in the "All events" window will automatically scroll so that the new event is visible.

The "Conversely display status colors" parameter allows to invert the colors of the icons, representing the protected site status. By default, the Security Center site that is armed is blue and the disarmed site is green. If before the work with the Security Center the operator used the software for protection and monitoring of sites with the settings inverse to the proposed ones, he/she can apply this parameter. In this case, the site icons will be displayed in the colors inverted to the original ones: the armed site will be green, and the disarmed site will be blue. To apply the "Conversely display status colors" parameter, reload the "Duty operator" module.

It is possible to adjust the total number of events displayed in the "Duty operator" module using the "Date" parameter. It shall be remembered that the longer the interval of events is set, the longer the "Duty operator" module will be initialized and the more the requirements of this module will be to the resources of the computer.

With the "Interval of event reception indication" parameter the operator can continuously monitor the software operation, which is necessary for the timely detection of its malfunction. This parameter provides reliable control of the Security Center operator, including the "Duty operator" module, with the help of the sound indication of event reception. In order for the operator to be confident in the stable functioning of the system, event reception not subject to filtration is accompanied by a sound signal. If there are no unfiltered events during the time interval set by the parameter, the sound signal is accompanied by the reception of the filtered event. This event is displayed in the line of the last received event, but there is no information about it in the general list of received events, either in the list of alarm events or in the list of events for the site (to display the filtered event in the list of events for site enable "Show duplicates" mode). Besides, the received filtered event is not displayed in the site card or in the alarm handling window. To enable the display, set the "Interval of event reception indication" parameter to a value greater than zero. If this parameter is set to zero, the event reception indication is disabled. The default display interval is 30 seconds.

The maximum time for disabling events is set in minutes using the parameter "Maximum interval of alarms disabling". By default, time of event disabling shall not exceed 90 minutes.

The maximum time for disabling the Security Center sites is set in minutes using the “Maximum interval of site disabling” parameter. By default, time of site disabling shall not exceed 180 minutes.

10.8.2 Alarm Handling

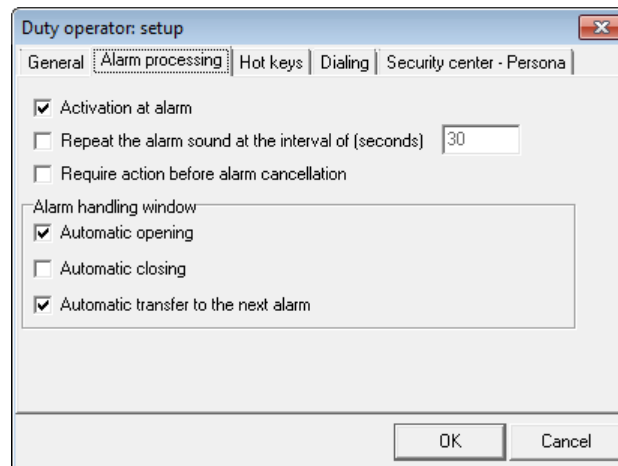


Figure 148: "Setup" window, "Alarm handling" tab

If, when receiving a new alarm event, it is necessary for the “Duty operator” module to attract the attention of the operator, it is necessary to set the value for the “Activation at alarm” parameter.

In a situation where there is an alarm in the “Duty operator” module, for which no actions are registered for too long, the parameter “Repeat the alarm sound at the interval of” may be useful. If this parameter is set to a non-zero value, then if there are no alarm actions during the specified time, the “Duty Operator” behaves as if this alarm had just been received: it will again play the alarm sound and open the alarm window if this is enabled by the “Automatic opening” parameter in the alarm handling window.

The checked “Automatic opening” item of the “Alarm handling” window allows the alarm window to be opened automatically in case of alarm. The “Automatic closing” and “Automatic transfer to the next alarm” parameters determine the behavior of the alarm handling window, at the moment when the current alarm handling is completed. If the value of the first parameter is set, the alarm handling window will be closed. If a value for the second parameter is set, the next received alarm will be loaded into the alarm handling window. If values for both parameters are set, then the next alarm will be attempted first, and if it is not, the alarm handling window will be closed.

10.8.3 Hot Keys

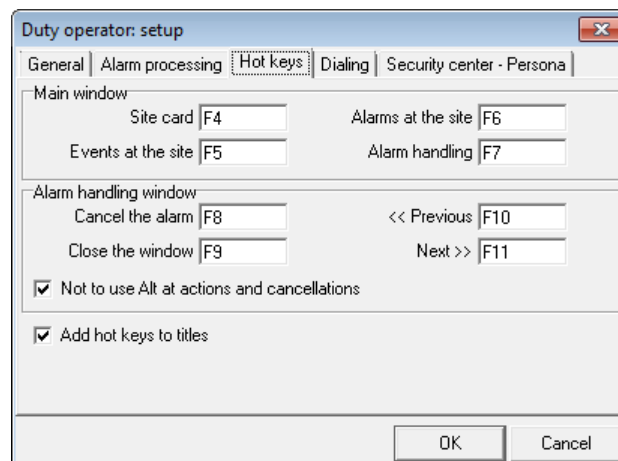


Figure 149: "Setup" window, "Hot keys" tab

Use the “Hot keys” tab to assign keyboard shortcuts for quick access to the main functions of the “Duty operator” module.

It shall be noted that hot keys for actions and cancellations are assigned automatically, when their list is formed. But with the “Not to use Alt at actions and cancellations” parameter it is possible to prohibit the combination of “Alt + Digit” for fast registration of actions or cancellations and use only digits.

The “Add hot keys to titles” parameter allows to display the hot keys assigned to operations in the button titles.

10.8.4 Dialing

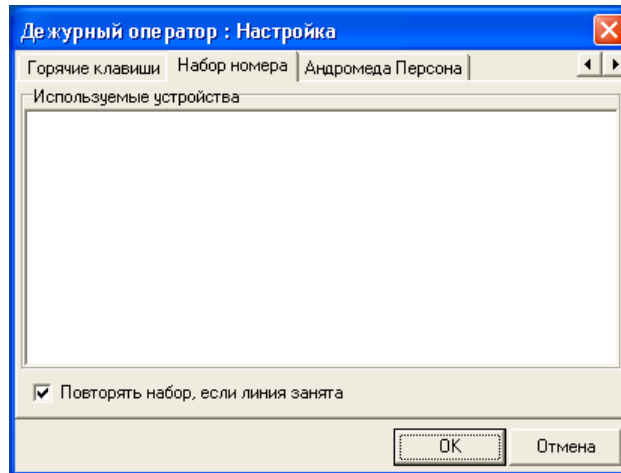


Figure 150: "Setup" window, "Dialing" tab

If there is a modem or any device that supports dialing via TAPI interface connected to the computer, it is possible to specify the list of devices that the “Duty operator” module can use to dial on the “Dialing” tab.

To start dialing, left-click on any phone number of the site that is displayed in the site card.

If the dialed number is busy, the “Duty operator” module can dial it again if the value for “Repeat dialing, if the line is busy” is set.

10.8.5 Security Center - Persona

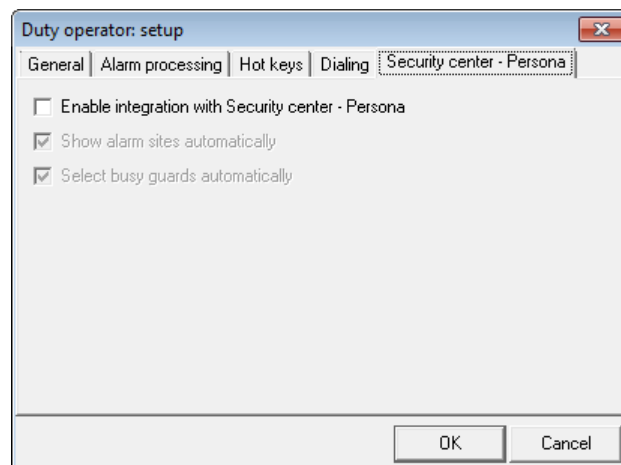
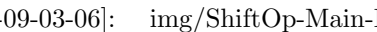
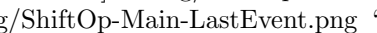



Figure 151: "Setup" window, "Security center - Persona" tab

The Security Center software can be used in conjunction with the “Andromeda Persona” software. In particular, it is possible to download a list of sites of the Security Center to the “Persona”, after which they can be placed on the terrain map.

Besides, changes in the status of sites and guards can be transferred from the Security Center to “Persona” so that the “Persona” can automatically display alarm sites on the map and also display the status of guards that are called to sites.

On the “Andromeda Persona” tab, it is possible to enable the “Duty operator” module integration with the “Andromeda Persona” software, and also allow automatic display of alarm sites and the status of guards in the “Persona”.

[id-09-03-06]:  “Events” window, context menu of alarm site” [id-09-04]:  “Line of last received event” [id-09-10]:  ” “Select site” window”

11 Report Manager

The “Report manager” module is intended to create reports on the operation of sites, Security Center and security company personnel.

A report form generator is built in the “Report manager” module, with which it is possible to modify the existing reports or create new ones.

11.1 Event Reports

When creating event reports, remember about the filtering algorithms that are used when registering events. See more information about filtering events in the section on the “Event manager” module, here it shall be noted that if necessary, it is possible to include the filtered events in the generated reports.

Unless otherwise specified, all event reports , are created taking into account the selected sites and event classes. Due to this, reports can be created for solving various tasks, including those specific for a particular security company.

The first three event reports (“01 - Sort by time”, “02 - Sort by sites” and “03 - Grouping by sites”) are intended for viewing the events received from sites in different views. It shall be noted that if parts with their own site numbers are created for a site, the events from these parts are displayed in the event reports. In this case the site number of the part is indicated in parentheses after the site number.

11.1.1 Events from Undescribed Sites

The report “04 - From undescribed sites” is intended for viewing events that the Security Center failed to associate with any of the existing sites. Like the “Events from undescribed sites” module, this report is intended to identify errors made during programming of site equipment, or when describing sites in the Security Center. For obvious reasons, the sites and event classes selected during its creation do not matter for this report.

11.1.2 Sites without Events

The purpose of the report “05 - List of sites without events” is twofold. It used to get a list of sites from which no events were received within a given period of time in the simplest way. To do this, select all sites from the list of sites, and in the list of event classes select all event classes.

Another more interesting task, for which the report can be used, is to find, for example, all sites of the “Bank” type, from which there have not been any faults during the last month. To do this, select all sites of the desired type and event classes that have the “Fault” type. The report created on the basis of such parameters will contain only the desired sites.

11.1.3 Time Deviation

Using the report “06 - By time deviation” to check the correct programming of the interval of the automatic test on the site and correct filling of the “Control time” field in the site card. When creating the report, the average time interval between events from the site is calculated, after which it is compared with the target time of the site.

If the difference of values is greater than the threshold specified at the time of report creation, then such site will be highlighted in the list. Depending on the algorithms used by the control panels to calculate time for creation of the next automatic test, it is possible to exclude all events which class type is not “Test” when creating the report.

11.1.4 Statistics by Class

The report “07 - Statistics” is needed to calculate the number of events of the given classes that were received from the site over a period. First of all, the report is useful for identifying sites with faults of various kinds. For example, if you select the event class “AC Fault” when creating the report, you can calculate how many times over the given period the site had power supply problems. To include only those sites that you really need to pay attention to in the report, when creating a report, it is possible to set the minimum number of events for each of the specified classes that shall be received for the site to be included in the report.

It shall be noted that for the effective use of this report, the user shall create separate classes for those events, which are of interest to him/her.

11.1.5 Sent SMS

Reports that belong to the group “08 - Sent SMS” - “12 - SMS, grouping by sites” are intended for monitoring the operation of the event handler “SMS message repeater”. Use these reports to get information about SMS messages that were created when handling events by sites, as well as the time of delivery of these SMS messages to the recipient.

11.1.6 Statistics by Channels

Depending on the settings with which the report “13 - Via communication channels” will be created, it can be used to solve several tasks. First, it is possible to estimate which communication channels are used by the site and to what extent, after calculating how many events are received from it on each of the communication channels. Second, it is possible to estimate the load of a separate communication channel by counting the number of events received from it from all selected sites.

11.1.7 Statistics by Status

Use the report “14 - Site status” to calculate the number and duration of situations when the site has a certain status. Each status of a site within this report is characterized by two events: the first event signals that the site has passed to a known state, when the second event is received, it is considered that the site is not already in this state. Good examples of site status are power or communication channel failures.

For example, if there is a power failure at the site, an event will be created that records failure, and after the failure is eliminated, an event about power supply restoration will be created. If it is necessary to calculate how many times the site was in a “power failure” state, and in addition - what is the total duration of this state, then when creating this report, specify the event classes corresponding to the failure and restoration of the power supply.

The states of interest to users of the Security Center can be very different. In order for this report to be actively used when working with the Security Center, it is necessary to create separate classes for those events that register the beginning and completion of state, which of interest to the user.

11.2 Alarm Reports

All alarm events registered by the Security Center require mandatory handling by the operator. If an alarm event is registered for the site at the moment when there is another unhandled event on the same site, then such events are combined into a group and further handled together. The alarms are handled in the “Duty operator” module. When handling an alarm, the operator registers the actions that he/she performed during the alarm handling in the Security Center. After the handling, the operator cancels the alarm by registering the handling time and result.

During creation, most alarm reports allow to specify whether to include data on the alarms for which there were no calls from the guards. This is due to the fact that such alarms are considered temporary or false by many security companies. Therefore, in some reports there shall not be such alarms, and in some, on the contrary, there shall only be such alarms.

When creating alarm reports, select sites and alarm event classes to be included in the report. If, when creating a report, it is important to select only those alarms for which certain actions were registered, it is possible to explicitly specify the actions of the operators that are required.

11.2.1 Standard Report and Report by Operator

The report “01 - By operator” is intended for viewing alarms, which were handled by a certain operator. And with the help of the report “02 - Standard” it is possible to see all registered alarms and actions for them. Additionally, when creating this report, it is possible to display only those alarms for which there were no guard calls.

11.2.2 Statistics by Alarm Cancellations

When creating the report “03 - By number of cancellations”, it is possible to specify the minimum number of cancellations that shall be registered over a period. If you select any specific cancellation, for example, “Equipment fault”, and specify that there shall be at least 5 such cancellations, you can get a report that will include all sites which alarms have been canceled at least 5 times since indicating the cause of “Equipment fault”.

The report “03a - Statistics by cancellations” is intended for calculating the number of selected cancellations registered over a given period. With its help, it is possible to see what causes of alarm cancellation are registered more often than others and how much. For example, it is possible to see what percentage of the alarms that were canceled are false. In addition to counting the total number of cancellations for all selected sites, the report allows to detail site cancellations in order to see on which particular sites there were more false alarms or alarms on which there were guard calls.

With the help of the report “03b - Summary by cancellations”, it is possible to see one more option for detailing site cancellations. It is more convenient to view the report than the previous one, but there is a limit - it can include no more than four cancellations. Just like the previous one, this report allows to know which sites are highlighted in the common list by the causes of the alarms that occur on them.

The report “03c - Summary by cancellations with comment” allows to select one cause for canceling an alarm, to calculate the number of alarms, during which cancellation the cause was indicated, and besides - to display all the comments that the operators registered when during handling of these alarms. If the algorithm for handling alarms by operators requires comments when registering situations accompanying handling, this report will be very useful in analyzing the causes of alarms, as well as the problems that arise when they are handled.

The last of the summary alarms cancellation reports, “05 - Cancellations by day” allows to select one cause for canceling an alarm and calculate how many times this cause was used on each day over the selected period. Besides, the report allows to select one additional characteristic of the site, which will also be included in the report.

Suppose that with the help of previous reports it was discovered that there were a lot of false alarms for the site during a month. Using the report “05 - Cancellations by day” it is possible to find out how these alarms were distributed by the days of the month: they occurred every day or during someone’s specific shifts.

11.2.3 Alarms and Events

The report “04 - With events” is a combination of two reports - event report and alarm report. When creating this report, it is possible to select not only event classes with the “Alarm” type, but also others. In this case, it is the events with the type of the “Alarm” class and the actions that were registered during their handling, that determine which sites will be included in the report. Events with other types of classes will be included in the report after the standard alarm report is created.

Events that were received before and after an alarm can be useful in finding out the causes for the occurrence of an alarm, so this report is most often used for this purpose.

11.3 Reports by Arm Time

The purpose of this group of reports is to provide information about the time during which the site was armed, or to specify whether the site was armed at a specified time.

11.3.1 Arm Time

The report “01 - With the amount of time” allows to see the daily site arming and disarming over a period, the time during which the site armed, and also the time during which the site had to be armed in accordance with arm schedule.

When displaying the site arming and disarming, these events are mandatory filtered: if several armings are received one by one, only the first one will be included in the report. If several disarmings are received one by one, only the last disarming will be included in the report.

The time, over which the site was supposed to be armed according to the schedule, does not depend on whether the monitoring of the arm schedule is included for the site. Thus, even if the site arm schedule is not monitored, it can still be used to compare the estimated and actual period of the site arming.

With the help of the report “02 - Briefly” it is possible to get simply the amount of the time during which the site was armed over a given period. This report can be useful in cases when payment for security services depends on the time during which the site was armed.

11.3.2 Arm Status

Often there are situations when it is necessary to find out in which state the site was on a particular day and time. To solve this problem, the report “03 - Arm Status” is used. When creating a report, select the date, time and arm status of the required site.

11.4 Reports by guards

The analysis of the guard operation allows to assess the quality of the security services provided and reliability of guards. Besides, by linking guard calls to sites, it is possible to highlight the sites to which the guards are called more often than to the rest and make some organizational conclusions with respect to these sites.

The report on the guards resembles alarm reports, except that they are focused on the specifics associated with the work of guards – counting the arrival time, average time of arrival, number of calls, etc.

In order for alarm reports and reports by guards to be truly useful, the alarm handling procedure shall be linked to the actions and causes for canceling the alarms that are registered by operators. First, it is necessary to identify the typical situations that are the cause of alarms. Second, to handle these situations, it is necessary to create actions and alarm cancellations. Third, it is necessary to train the operator to identify typical situations, to act in accordance with the rules developed for them and to register exactly those actions and cancellations that correspond to a certain situation.

11.4.1 Guard Performance

The report “01 - Guard Performance” is intended for displaying all alarms over the period for which calls of selected guards were registered.

11.4.2 Statistics of Responses

The next report, “02 - Statistics of responses”, shows the main statistics related to the performance of guards over a period: total number of group calls, number of calls that were canceled, time which the guard spent on calls, and average arrival time of the guard. The report can be useful for estimating the workload of a guard, as well as for identifying the most and least loaded guards.

11.4.3 Average Number of Calls

Use the report “03 - Average number of calls” to calculate the total number of calls for guards to sites, as well as the average number of guard calls to site per month. This report is used to identify the sites to which the guards are called most often.

11.4.4 Response Time

The purpose of the report is “04 - Response time” is to estimate the time that elapses from the time the alarm is received to the call of the guard and its arrival at the site. When creating a report, it is possible to specify the maximum allowed values for these intervals, so that only those alarms are included in the report, where these values were exceeded.

11.4.5 Statistics by Cancellations

Just like the similar alarm report, the report “05 - Statistics by cancellations” allows to calculate the number of registered causes of alarm cancellation over a period, but only for the selected guards. With the help of this report, it is possible to estimate how many of the alarms to which the guard was called were false and why.

11.5 Site Reports

A set of site reports is intended to create a hard copy for the main data of the Security Center: sites, operators, event templates and event handlers.

11.5.1 Sites

The reports “01 - List of sites”, “02 - Minimal card”, “03 - Short card” and “04 - Full card” are intended for viewing and printing information about sites in different views and in different volumes.

The report “06 - Control time” allows to display sites which control time is within the limits defined during the report creation. The report can be useful when ranking sites, if the control time for the site is set according to its importance.

11.5.2 Operators

Use the report “05 - Operators” to print a list of users of the Security Center software and their rights in the modules.

11.5.3 Event Templates

A variety of information about using event templates can be obtained using the report “07 - List of event templates”. Depending on the parameters that were specified when creating the report, it is possible to find out which templates are used for sites, and which ones are not. For those templates that are used, it is possible to count the number of sites that use them.

If in addition to the list of event templates it is possible to get descriptions of events that are included in a particular template, then use the report “08 - Event template codes”.

11.5.4 Event Handlers

The report “09 - SMS message repeaters” is intended for viewing and printing information about the settings of the event handlers “SMS message repeaters”. It is used to get information about all handlers that are used for the selected sites, or only those that have a specific recipient number.

12 Database Wizard

The “Database wizard” module is intended to perform the following operations:

- database check
- operation with database backups
- data import and export

After starting the “Database wizard” module, select the required operation:

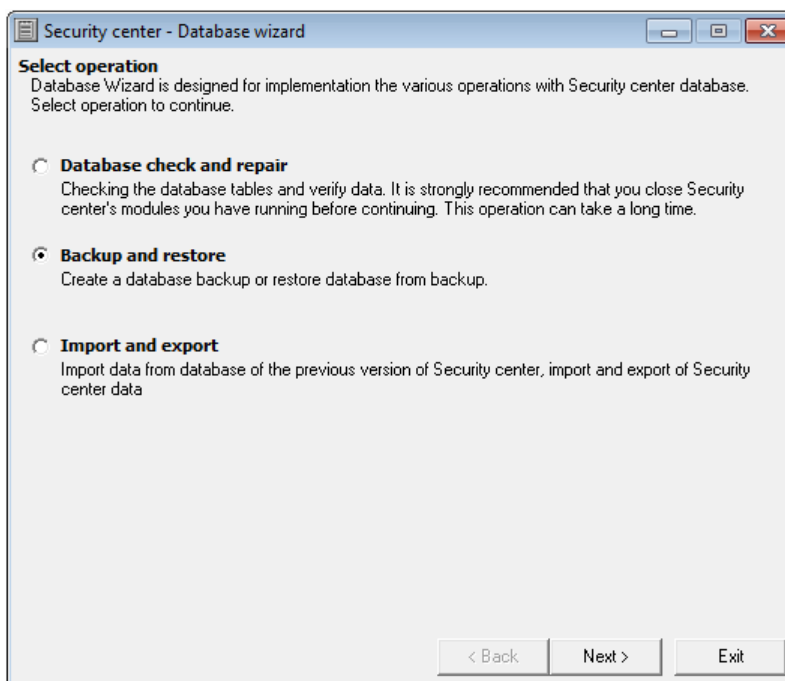


Figure 152: Start window of the "Database wizard" module

12.1 Database Check

It is recommended to perform database check operation at least once a month. Procedures included in the database check do not have any settings and are performed automatically.

During a database check, it is not necessary to stop operation of other modules. After the check is completed, it is recommended to restart the “Duty operator” module.

12.2 Backup

Database backup can be performed only on the computer on which the full installation of the Security Center was performed.

The backup procedure does not have a critical impact on the operation of other Security Center modules. However, when performing a database backup, there may be some performance degradation of the computer as a whole. This fact shall be taken into account when choosing the time to perform a backup.

When creating a database backup, set the values for the parameters that control the backup operation.

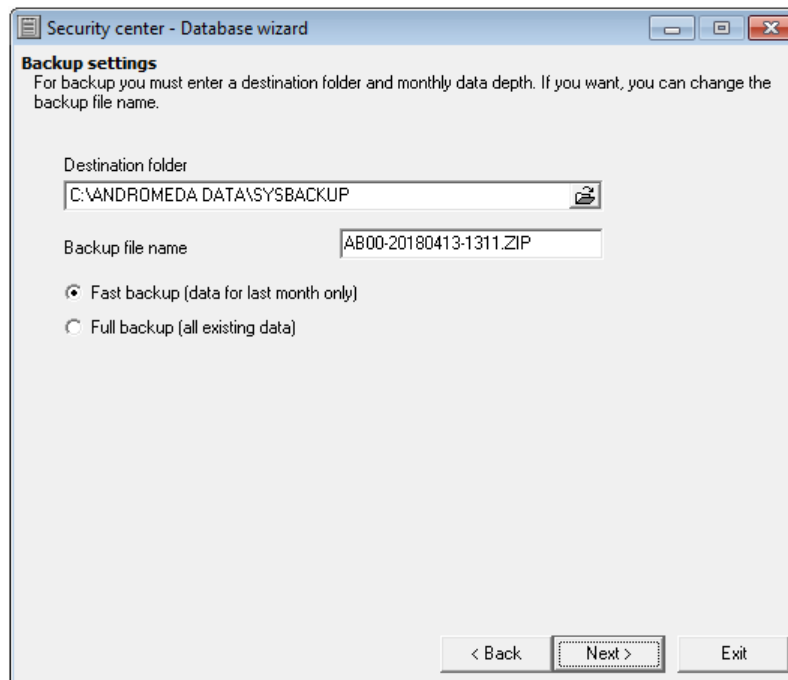


Figure 153: Backup settings window

The Destination folder option specifies the folder on the hard disk of the computer or network resource in which the database backup will be saved.

The backup file name can be specified using the parameter of the same name. Despite the fact that there are no restrictions on naming the backup file, it is necessary to remember that to restore the Security Center database from the backup using the GUI of the “Database wizard” module, the file name shall begin with the Latin characters “AB”.

Note that the backup copy of the Security Center software database is created in the form of a ZIP archive, in which several files containing backup data can be included. If the archive file size exceeds 4Gb, a multi-volume archive will be created, all files of which will be needed for restoration the database from the backup.

In addition to the name of the backup file and the folder name for its location, specify the backup type that you want to create. The backup type determines the amount of information that will be included in the backup.

In case of *full backup*, all information stored in the database at the time of copying, including received events, operator actions, and sent SMS messages over the entire period of the Security Center operation will be included in the database backup.

In case of *fast backup*, the amount of data in the backup will be significantly less: it will save events, operator actions and SMS messages only for the last month.

Based on the amount of information stored during backup, it is recommended to perform a full backup at least once a month, and fast backups - at least once a day.

To store backups, it is recommended to use not one but several media, and those that are not physically connected with the disk subsystem of the computer on which the Security Center database is stored. For example, it can be a separate hard drive, flash drive, or a network resource.

To increase the system reliability as a whole, the Security Center performs automatic backup. Fast copies of the database are stored in the “ANDROMEDA DATA\SYSDBACKUP” folder, the interval for creating automatic backups is 24 hours by default.

12.3 Restoring from Backup

Restoring the database from a backup can only be performed on the computer on which the complete installation of the Security Center software was performed.

Before restoring the database from a backup, stop all modules of the Security Center, including the “Event manager” module.

The version of the database from which the restore is performed does not matter: immediately after the restore, the “Database wizard” module will check the version of the recovered data and, if necessary, perform the update.

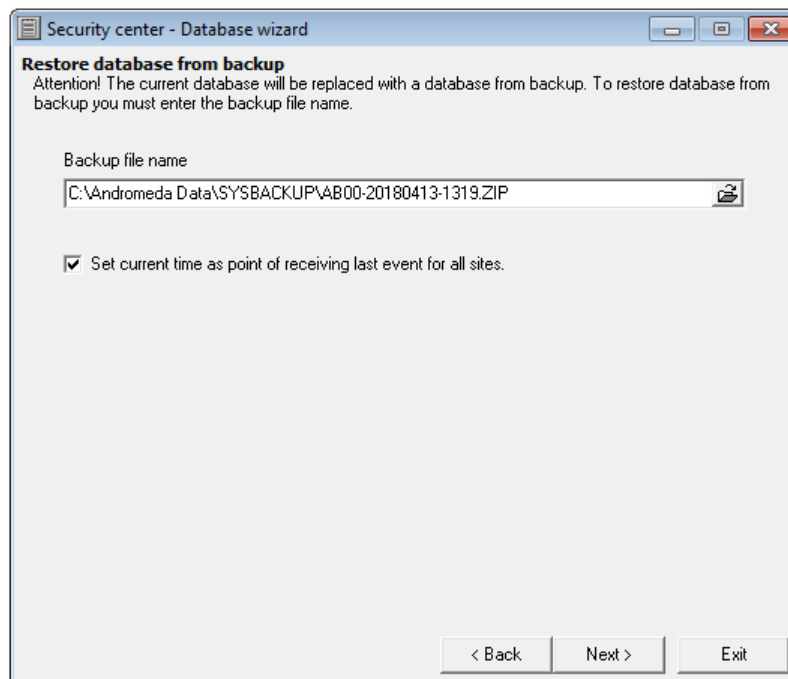


Figure 154: Configuration window for restore from a backup

The name of the backup file from which it is necessary to restore the database can be specified using the same parameter. If a database backup was created in a multi-volume archive, then all archive files are required when recovering from such a copy.

The “Set current time as point of receiving last event for all sites” parameter is intended to prevent generation of events about the absence of a control event immediately after the database is restored from the backup. If this flag is set when restoring a database from a backup, then for all sites in the database of the Security Center software the reference time starts counting from the moment the database is restored from the backup.

See more information about the “Site control time” parameter in the chapter describing the “Site manager” module, section “Control time”.

It is recommended to restore the database in two steps: first, restore from the most recent full copy of the database, and then from the current fast copy. Thus, at the first stage, the entire existing history will be restored, and at the second stage, constantly changing information will be updated.

When database restoration from a backup is complete, it is recommended to perform a database check. It shall be remembered that the database check does not block the operation of other Security Center modules, so it can be performed after the “Event manager” and “Duty operator” are started.

12.4 Data Import

It is possible to import data only on the computer on which the full installation of the Security Center software was performed.

Before starting data import, stop all modules of the Security Center, including the “Event manager” module.

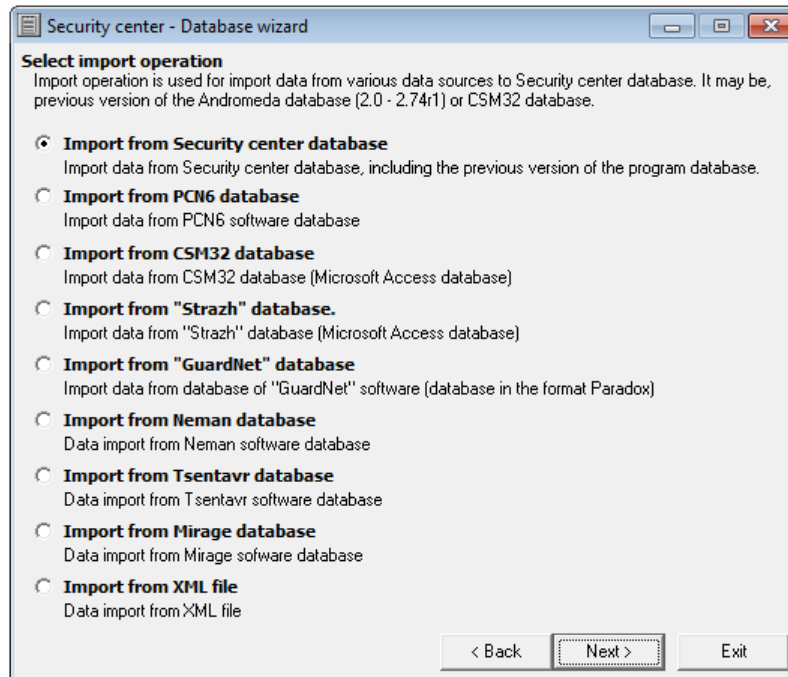


Figure 155: Window for selecting data source for import operation

In the Security Center, in addition to other sources, it is possible to import from an XML file.

12.4.1 Import from XML File

By importing from an XML file, it is possible to import a site database of Cobra software to the Security Center.

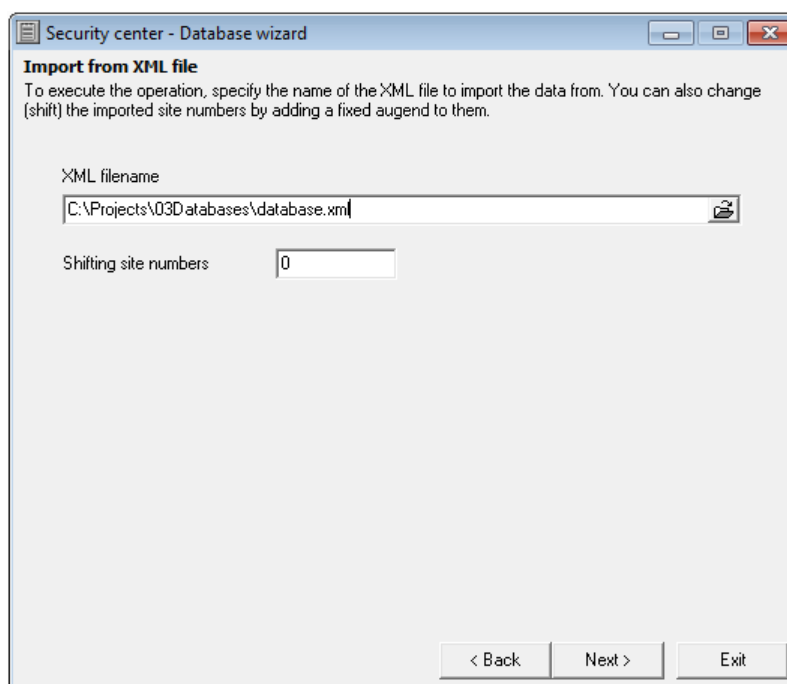


Figure 156: Window for setting import from XML file

Use the “XML filename” parameter to select the database file by specifying the path to it.

When importing from an XML file, it is possible to move the numbers of the imported sites. The shift is performed because summand, specified during import setup, is added to the site numbers, information about which is transferred to the Security Center. For example, if the value of the “Shifting site numbers” parameter is set to 10000, and the site numbers in the XML file are within the range from 1 to 2000, then in the Security Center database, these sites will have numbers within the range from 10001 to 12000.

See more information about the function of shifting site numbers in event sources in the chapter on the “Event manager” module in the section “Event sources”.

12.5 Data Export

The Security Center supports exporting information about sites to a text file with a value separator.

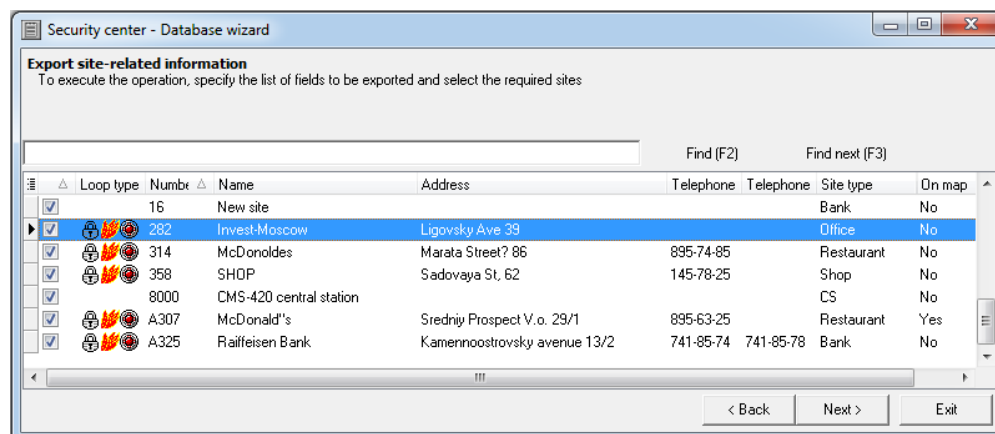


Figure 157: Window for selecting sites and fields when setting up site information export

For export, select sites and fields (columns) which information will be written to the export file. Select the sites, information about which shall be exported, by checking the boxes in the first column of the line near the site. Select

fields, information from which will be written to the export file, by enabling or disabling their display. The export file will include information only from those fields (columns) that are displayed in the table.

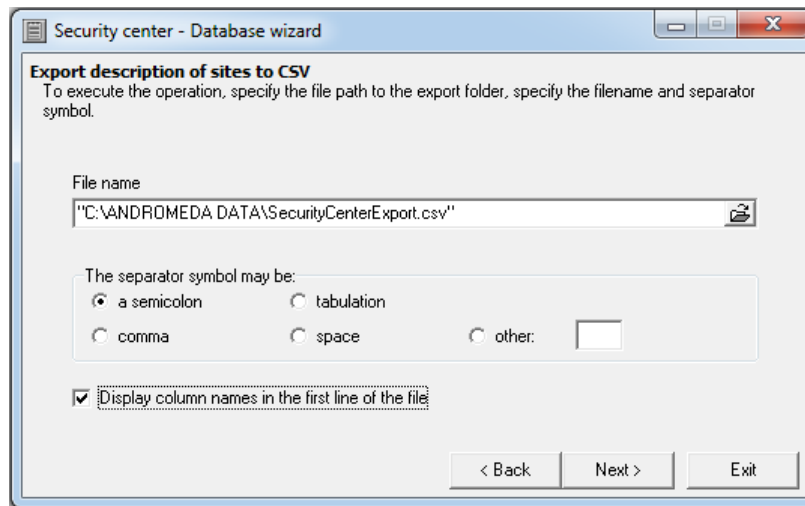


Figure 158: Window for setting exporting information about sites

Use the “File name” parameter to specify the folder and name of the export file.

Use the “Separator symbol” parameter to select the character that will be used as a field separator in one line of the export file. It shall be remembered that the line field values in the export file are enclosed in double quotes, which excludes the possibility of incorrect recognition of the separator when opening the export file.

12.6 Command Line Options

Along with the graphical user interface, the “Database wizard” module can be used for control with the command line.

This feature can be useful if the Windows Scheduler, which has more advanced capabilities than the scheduler built into the “Event manager” module, is used as the task scheduler for backing up a database or restoring from a backup.

12.6.1 Database Backup

```
AnDBWiz.exe
  /BACKUPDB
  /FOLDER: <Destination folder 1>; <Destination folder 2>
  /TYPE:<Backup type>
  /BACKUPCOUNT: <Number of files in the destination folder>

/BACKUPDB
```

This parameter specifies that the “Database wizard” module shall perform a database backup. The backup procedure settings are set by the command line parameters following it.

```
/FOLDER: <Destination folder 1>; <Destination folder 2>
```

One or several folders to which the database backup will be saved. At least one folder shall be specified. The names of the folders shall be enclosed in quotation marks. If section folders are specified, they shall be separated by a semicolon. It is allowed to use absolute paths in folder names.

`/TYPE:<Backup Type>`

The type of backup to be created. If this parameter is set to “0”, it indicates fast backup. If this parameter is set to “1”, it indicates full backup. The parameter is optional. If the parameter value is not set, fast backup will be created.

`/BACKUPCOUNT: <Number of files in the destination folder>`

This parameter specifies the maximum number of database backup files in the destination folder. If you find that the number of backup files of the same type exceeds the maximum possible number when creating a backup, the oldest backup file will be deleted. The parameter is optional. If the parameter value is not specified, the value for this parameter will be 10.

12.6.2 Restoring Database from Backup

```
AnDBWiz.exe
  /RESTOREDB
  /FOLDER: <Source folder>
  /TYPE:<Backup type>
```

`/RESTOREDB`

This parameter specifies that the “Database wizard” module shall restore the database from a backup. The database restoration settings are set by the command line parameters following it.

`/ FOLDER: <Source folder>`

The folder to which the backup of the database will be restored. If several backup files of the specified type are found in the specified folder, then the restoration from the most recent file creation will be performed.

`/TYPE: <Backup Type>`

The type of backup from which the database shall be restored. If this parameter is set to “0”, it indicates fast backup restoration. If this parameter is set to “1”, it indicates full backup restoration. The parameter is optional. If the value of the parameter is not set, then the restoration from the fast backup will be performed.

12.6.3 Example of Using Command Line Parameters

```
AnDBWiz.exe
  /BACKUPDB
  /FOLDER:"E:\Backup Data\Operational";"\\Storage\Andromeda Backup\Operational"
  /BACKUPCOUNT:25
```

The above mentioned set of command-line parameters means that the “Database wizard” module shall create a fast copy of the database and copy it to the folders `E:\Backup Data\Operational` and `\\Storage\Andromeda Backup\Operational`.

When copying a backup to the destination folder, the “Database wizard” module shall check that the total number of online backup files in the destination folder does not exceed 24, and if there are more, the oldest backup file shall be deleted.

13 Cloud Services

The cloud is an infrastructure software and hardware complex. It provides services to improve the quality of services offered by the private security company.

“Alarm to Guard” is also a cloud service. This application provides fast interaction between the Security Center operator and Guard employees. Besides, it allows the Guard to get the necessary information about the site and its status.

In addition to these services, various web-interfaces are available. For example, with the help of the “Partner interface” a private security company can manage the Cloud services. It is possible to configure one of the cloud services, for example, “Alarm to Guard.”

The “Engineer Interface” displays a site available for control and provides the ability to remotely control the equipment on it.

The Security Center user can select one of the modes of operation with cloud services, depending on the degree of integration with the Cloud. Full integration allows to use all cloud services. Partial means only a service that provides remote access to equipment on a site. By prohibiting transfer of any data to the Cloud, the user refuses to use all cloud services.

13.1 Engineering Panel

The “Engineering panel” application is intended for remote configuration of equipment installed on the site, as well as for updating the software version of the devices.

In order for the engineer to remotely change the settings, one of the following devices shall be installed on the site:

- **Nord GSM or Nord GSM WRL**
- **Nord GSM Mini or Nord GSM Air**
- **Soyuz GSM**
- **TR-100 GSM IV**

In order for an engineer to access the service, an account shall be created for him/her.

It is possible to create engineer account on the “Engineers” tab of the “Personnel manager” module. When creating an account, an email is sent to the engineer’s email address. The engineer shall click on the link in the letter and create and confirm the password for accessing the “Engineering panel” on the page that opens. After entering the data, it is necessary to click the “Register” button to complete the registration in the Cloud.

In order for the Security Center operator to create an account for the engineer or change its settings, he/she shall be given permission to edit the engineers.

After successful registration, a link will be displayed on the page to the main page of the “Engineering panel”. On this page, links to remote programming interfaces of sites will be given in “Available sites”, access to which is allowed to the engineer. Each link specifies the site number and the allowed access time to the site (for example, “Site No. 314, access to the site is allowed from 15:55 25.08.2013 till 16:55 25.08.2013”).

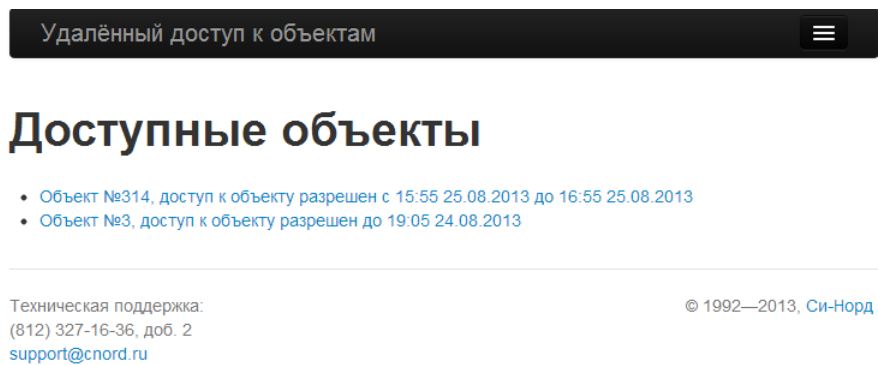


Figure 159: Engineering panel

The Security Center user, who has the corresponding permission, can grant the engineer access to sites using the “Maintenance” tab of the “Site manager” module.

The engineer can go to any of the links specified in the web interface only at the time that is allowed to him/her to access the site. At the same time, he/she enters the “Remote keyboard” page. The page contains the interface of the web-keyboard, which is identical to the one installed on the site. Thus, the remote programming interface implements the behavior of the real keyboard connected to the device. Information on how the buttons are duplicated on the keyboard is shown in the web interface to the right of the keyboard.

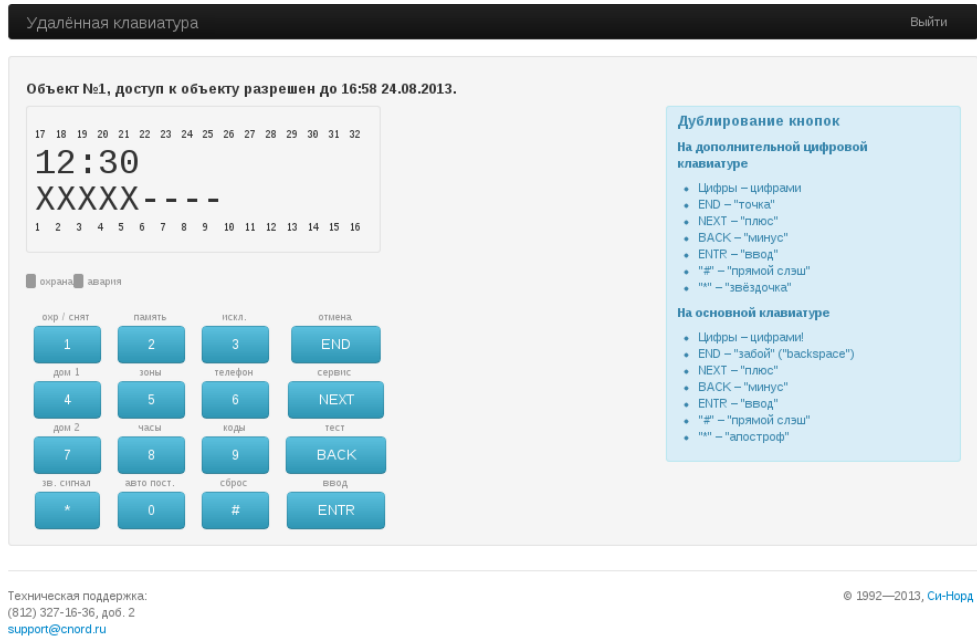


Figure 160: Web keyboard

It shall be noted that if an error occurs while working with the web keyboard, the error text is displayed and the interface goes to the main page with a list of sites. For example, if the web keyboard is not used for more than five minutes, the communication session with the site is completed. At the same time, the following message is displayed: “The waiting period for actions to configure the device has expired. To ensure security, the communication session with site No. 314 is completed”.

If the connection to the site is lost for any reason, the keypad on the site is disabled. In this case, the error text is as follows: “The waiting period for the response from the device has expired. To ensure security, the communication session with site No. 314 is completed”.

If when the web keyboard is opened or used it turns out that the site is armed, the following message is displayed: “Site No. 314 is currently armed. To access the web keyboard disarm the site”.

After the work is finished, the engineer shall exit the system by clicking on the “Exit” link located on the main panel of the page.

To log in to the web-interface, go to keyboard.cnord.net and enter the e-mail address and password created at registration. After that, click the “Login” button. To recover a password, click on the link “Forgot your password?”. In the appeared window it is necessary to enter the e-mail address and press the button “Restore password”. At the same time, a letter containing a link for password restoration will be sent to the specified address.

14 Technical Support

If problems arise during the operation of the Security Center software, or if you want to improve it, contact the technical support service of C.Nord by e-mail [\[support@cnord.ru\]](mailto:support@cnord.ru)(mailto:support@cnord.ru).

When contacting technical support about a problem, specify Security Center version that is being installed and describe the problem.

In case of request by e-mail, it is recommended to attach the archive containing the following files:

- file `C:\Andromeda_Install.log` - This file contains the log of Security Center installer
- files from folder `C:\Andromeda Log` - The files contain the logs Security Center modules
- files from folder `C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG` - The files from this folder and its subfolders contain the logs of Microsoft SQL Server Setup installer

The listed files do not contain personal data or confidential information.