

# Nord GSM Air

## OPERATION MANUAL



**C.Nord**

December 8, 2018

# Contents

<b>1</b>	<b>Technical Description</b>	<b>4</b>
1.1	Purpose and Capabilities . . . . .	4
1.2	Power Supply . . . . .	4
1.3	Communication channels . . . . .	4
1.4	Functionality . . . . .	5
1.5	Main Technical Characteristics . . . . .	5
1.6	Scope of Delivery, Marking and Package . . . . .	6
1.6.1	Scope of Delivery . . . . .	6
1.6.2	Marking . . . . .	6
1.6.3	Packing . . . . .	6
<b>2</b>	<b>Device Control</b>	<b>7</b>
2.1	TM-Key . . . . .	7
2.1.1	Reading Indication . . . . .	7
2.1.2	Error Indication . . . . .	7
2.1.3	Disarming Indication . . . . .	8
2.1.4	Arming Indication . . . . .	8
2.1.5	Standby Mode Indication . . . . .	8
2.2	Built-In Keypad . . . . .	9
2.2.1	Arming and Disarming . . . . .	10
2.2.2	Getting Information about Status . . . . .	11
2.2.3	Panic Button . . . . .	12
2.2.4	Backlight and Sound Turning Off . . . . .	12
2.3	CN-Keypad Wireless Keypad . . . . .	12
2.3.1	Arming and Disarming . . . . .	13
2.3.2	Getting Information about Status . . . . .	15
2.3.3	Panic Button . . . . .	15
2.3.4	Backlight and Sound Turning Off . . . . .	15
2.4	Wireless Keyfob . . . . .	15
2.4.1	MyAlarm Mobile Application . . . . .	16
<b>3</b>	<b>Installation and First Start</b>	<b>17</b>
3.1	Device Wiring Diagram . . . . .	17
3.2	Connection of Wired Zones . . . . .	18
3.2.1	Normally Closed and Normally Open Zone . . . . .	18
3.2.2	Terminating Resistors . . . . .	18
3.2.3	Zone without Terminating Resistors . . . . .	18

3.2.4	Zone with One Terminating Resistor . . . . .	19
3.2.5	Zone with Two Terminating Resistors . . . . .	19
3.2.6	Wired Zones in Configurator . . . . .	20
3.3	Connection of Temperature Sensors . . . . .	21
3.4	GSM Channel Setting . . . . .	21
3.4.1	SIM Card Installation . . . . .	22
3.4.2	Connection of Remote GSM Antenna . . . . .	22
3.5	Connection of Touch Memory Reader . . . . .	23
<b>4</b>	<b>Software Update</b>	<b>24</b>
4.1	Device Connection to computer . . . . .	24
4.2	Driver Installation in Windows XP and Windows 7 . . . . .	24
4.3	Driver Installation in Windows 8 . . . . .	29
4.4	Utility to update software . . . . .	32
<b>5</b>	<b>Device Configuration</b>	<b>34</b>
5.1	Control Panel and Tab Panel . . . . .	34
5.2	Control Panel . . . . .	34
5.2.1	Tab Panel . . . . .	36
5.3	Zones . . . . .	37
5.3.1	Zones Numbering . . . . .	37
5.3.2	Turning Zone On and Off . . . . .	37
5.3.3	Zone Type . . . . .	37
5.3.4	Zone Normal State . . . . .	39
5.3.5	Terminating Resistors . . . . .	39
5.3.6	Entry Delay . . . . .	39
5.3.7	Exit Delay . . . . .	40
5.4	Users . . . . .	41
5.5	Partitions . . . . .	43
5.5.1	Partition Management . . . . .	43
5.6	Miscellaneous . . . . .	44
5.6.1	Intervals . . . . .	44
5.6.2	Siren . . . . .	46
5.6.3	Backup Power Supply . . . . .	47
5.6.4	Arm and Disarm . . . . .	48
5.6.5	Control and Indication . . . . .	49
5.6.6	Configuration Protection . . . . .	49
5.7	Security Center . . . . .	52
5.7.1	Device Identification . . . . .	52

5.7.2	GPRS Transmission Parameters . . . . .	53
5.7.3	Transmission Parameters via GSM voice channel . . . . .	54
5.7.4	SMS Transmission Parameters . . . . .	55
5.7.5	Communication Channel Switching . . . . .	55
5.8	Cloud . . . . .	57
5.9	Ethernet . . . . .	58
5.10	GSM operators . . . . .	59
5.11	Automatic Controls . . . . .	60
5.11.1	Light Indicator . . . . .	60
5.11.2	Siren . . . . .	62
5.11.3	Miscellaneous . . . . .	62
5.12	Event History . . . . .	65
5.13	State Panel . . . . .	66
5.13.1	Communication Channels . . . . .	66
5.13.2	Wired Zones . . . . .	66
<b>6</b>	<b>Remote Access to Device</b>	<b>68</b>
6.1	Description of Remote Access Technology . . . . .	68
6.1.1	Communication Channel Device $\longleftrightarrow$ Receiver . . . . .	68
6.1.2	Communication Channel Device $\longleftrightarrow$ “Cloud” . . . . .	69
6.1.3	Communication Channel Receiver $\longleftrightarrow$ “Cloud” . . . . .	69
6.2	Remote Access Setting . . . . .	69
6.2.1	Creating Engineer . . . . .	69
6.2.2	Granting Permissions to Engineer . . . . .	71
6.3	Device Remote Configuration . . . . .	71
6.3.1	Selection of Site to Configure . . . . .	71
6.3.2	Working with Configuration . . . . .	72
6.3.3	Work Features . . . . .	73
6.4	Remote Software Update on Device . . . . .	73
6.4.1	Information about Sites on Receiver . . . . .	73
6.4.2	Process of Remote Software Update on Device . . . . .	74
6.4.3	Updating Software on Selected Site . . . . .	75
6.4.4	Updating Software on all Sites . . . . .	75
6.4.5	Update Process Stopping . . . . .	76
<b>7</b>	<b>Event codes</b>	<b>77</b>

# 1 Technical Description

## 1.1 Purpose and Capabilities

The “Nord GSM Air” device is wireless control panel with built-in keypad for security systems.

The “Nord GSM Air” device is intended for operation as the head unit of the security system - the receiving and monitoring security alarm device, installed in the premises at the protected sites.

Various wireless security and process detectors and devices can be connected to “Nord GSM Air”.

The device can generate and transmit to the control panel messages about events occurring during its operation and related to:

- the device arming or disarming;
- changes in the state of its security zones;
- changes in the state of its power sources (main and backup);
- disruptions in the operation of communication channels used by the product and other malfunctions;
- activation and restoration of the state of the housing tamper switch.

The device transmits notifications to the receiver using the built-in GSM/GPRS-communicator via voice channel, SMS or GPRS.

The device is equipped with uninterrupted power supply and automatically maintains its backup power source installed in its case during its entire operating life. The product is capable of providing power supply to the connected communication modules (communicators) and devices for expanding its functionality within the limits of permissible consumed capacities.

## 1.2 Power Supply

The main power source of the product is a DC power adapter with  $(10\div 14)$  V output.

The Li-Ion 18650 battery with 3.7 V rated voltage can be used as a backup power source.

The product provides automatic maintenance of the installed battery, which includes the following:

- subsequent charge of the discharged battery with a current of  $(100\pm 25)$  mA;
- ability to automatically turn off the discharged battery in the absence of the main power supply when the voltage on it reaches  $(3.5\pm 0.1)$  V;
- stability to both the break and short circuit in the battery circuit is unlimited in time, while the product will be powered from the main source;
- protection against “reverse polarity” in case of wrong connection to the battery terminals or external UPS.

If an external UPS is used as a backup power source. External UPS must be connected instead of main power source. The product continues to periodically monitor the fact of its connection, but does not monitor the presence, condition and charge of its backup battery.

## 1.3 Communication channels

The product events can be sent by the GSM 900/1800 cellular networks of two different carriers through the built-in GSM-modem.

The product is equipped with a internal GSM-antenna. It is possible to connect a external dipole antenna (with a MMCX-male connector type) to improve the communication quality with the base station of the carrier.

To transmit events to the monitoring panel, the device can use the following communication channels:

- GPRS;
- VOICE (voice channel with DTMF-encoding);
- SMS.

In the mode of packet transmission of notifications (GPRS), the content is encrypted.

The device has a two-tier SIM-card holder, in which it is possible to install two SIMs of different carriers. The active SIM is selected automatically, in accordance with the established algorithm of the cellular communication module.

The device can estimate the signal level in the carrier networks at the device installation site separately for each of the two SIMs and display the received result in the configurator interface.

## 1.4 Functionality

- configuration of 2 alarm wired zones intended for receiving notifications from analogue manual and automatic security and fire detectors, security and fire alarm system units through the outputs of the central security panel relays;
- – connection of up to 31 wireless devices;
- configuration of up to 32 partitions with the possibility of their independent arming and disarming.
- control of actuators and automation facilities using open-collector control outputs;
- control of the product operation mode using electronic keys Touch Memory, proximity card reader and wireless keyfobs;
- sound and light alarm in “Alarm” and “Fire” modes;
- control of the zone operability with automatic detection of an open or short circuit, light and sound alarm signaling, formation of notifications for the receiver about the fault;
- sound and light indication when the product is armed and disarmed;
- storing of information to the event log.

## 1.5 Main Technical Characteristics

- The minimum number of the product wired security zones, designed to connect different detectors, is 2;
- The maximum allowable total resistance of two wires of each zone - no more than 330 Ohm;
- The maximum number of wired zone states controlled by the product is two (“normal”, “alarm”). In this case, the type of each of the organized zones is normally closed or normally open is set by the user when configuring the product;
- The maximum current consumption of all wired sensors connected to the product is limited by the value of self recovering thermal switch and shall not exceed 200 mA;
- The product has non-volatile memory for storing messages generated by it;
- The product provides support for the 1-Wire protocol in the rank of “master” on the connector of the corresponding interface, allowing its arming and disarming, for example, with the help of devices of the DS1990A series, connecting remote temperature sensors, hardware devices for expanding the controller ports, etc. (support of different device on the 1-Wire bus is determined by the software version of the product controller). The “LED” line of the 1-Wire interface is short-circuit protected and is designed to connect an external LED indicating the product status, with a current consumption of up to 8 mA (for example, LED located in the TM reader);
- A piezoelectric siren can be connected to the product for sound confirmation of the “Alarm” state with a current consumption up to 200 mA, at the same time the product detects such malfunctions in its connection circuit as a break and short circuit, both in the absence and in the presence of “Alarm” signal. The output for the siren connection is protected by the self recovering thermal switch;

- The product's wired zones can be configured as discrete outputs of "open collector" type, allowing connecting the switched load to the product, for example, electromagnetic relays, acoustic or electrooptical devices. The maximum allowable sink load current of discrete outputs is 500 mA; the maximum permissible DC voltage supplied to the outputs is plus 50 V;
- The product is equipped with a vertical connector of the "mini USB B" type for its configuration after connecting to the computer USB port;
- By means of special software it is possible to remotely change the product configuration parameters, as well as update the controller software;
- The product is designed for continuous (twenty-four-hour) operation in the operating temperature range (without taking into account the temperature limitations of the backup power supply) from -20°C to +50°C;

The permissible product operating temperature range with a backup source is determined by the characteristics of the battery installed in it, and first of all by the maximum permissible temperature values during charging.

- Overall dimensions of the plastic case, mm, maximum, - 150x96x32;
- The product weight in a plastic case (without a backup power source, power cord and packaging), kg, maximum, - 0,2;

## 1.6 Scope of Delivery, Marking and Package

### 1.6.1 Scope of Delivery

Receiving and monitoring security and fire alarm device "Nord GSM Air"	1 pc.
Battery with dimension 18650	1 pc.
Power supply adapter	1 pc.
Technical specification	1 pc.
Package	1 pc.

### 1.6.2 Marking

The product printed circuit board has a marking indicating the polarity of the terminals of the terminal blocks and their purpose.

The product is marked in the form of labels with the name of the product and bar code. The labels are glued on the front side of the product printed circuit board and case. In addition, the label is glued in the product certificate.

### 1.6.3 Packing

The product is delivered in a separate cardboard box. Before placing in a box, the product in a plastic case is packed in a polyethylene air-bubble bag, providing the product additional protection from damage and increased humidity during storage and transportation. The accessories are shipped with the product in accordance with the scope of delivery.

## 2 Device Control

The following control devices can be used to for the device arming/disarming:

- built-in keypad;
- wireless keypad “CN-Keypad”;
- wireless keyfob “CN-Keyfob”;
- TouchMemory key;
- mobile application “MyAlarm”.

### 2.1 TM-Key



*Figure 1: TM-reader and TM-key*

The device has a built-in interface for connecting the TM-key readers. In addition, the device provides the ability to connect the LED indicator, which is located directly in the case of some models of TM-key readers.

The LED indicator located in the TM-reader case is intended for indication of the TM-key reading, arming and disarming, and also for indicating the device current state.

With a single TM-key it is possible to arm or disarm one partition. If one user has to be able to arm or disarm several partitions at the same time, then the appropriate rules shall be set in the “Automatic controls” section.

#### 2.1.1 Reading Indication

If the key reading operation has completed successfully, the device indicates this fact, regardless of whether the key is found in the device memory or not. In other words, if the reading is successful, the device simply confirms that a key has been brought to the reader and this key has been read.

Indication of successful reading of the TM-key: the LED “flashes” (turns on for 0.1 sec., then turns off for 0.1 sec.) for 1 second.

#### 2.1.2 Error Indication

The following errors are possible during a key reading:

- key is not found in the device memory;
- arming rejection.

Error indication: the LED “flashes” (turns on for 0.5 s, then turns off for 0.5 s.) for 3 seconds.



### 2.1.3 Disarming Indication

If the key, with which you can change the partition status and this partition is armed, is read, then the partition is disarmed.

The disarming is indicated after the reading is completed.

Disarming indication: the LED turns on for 5 seconds and turns off.

After the disarming indication is displayed, the standby mode indicator is enabled.

### 2.1.4 Arming Indication

If a key, with which it is possible to change the partition status, is read, then if there are no zones in the partition with exit delay, the partition is armed. If there are zones with exit delay, then the delay interval counting starts; arming is performed after the exit delay expires.

The arming indication depends on how many partitions are configured in the device.

#### One Partition

If only one partition is configured in the device, then after it has been armed, the LED turns on and remains lit: the standby mode indicator with the only partition armed is enabled.

#### Several Partitions

If several partitions are configured in the device, then the indication after the current one is armed depends on whether the disarmed partitions remained or not.

If all partitions are armed, the LED turns on and remains lit: the standby mode indicator with several partitions is activated, all partitions are armed.

If there is at least one not armed partition, the LED turns on and is glowing for 20 seconds. After that, the indication of the standby mode with several partitions is enabled, some of which are disarmed.

#### Arming Rejection

“Arming rejection” is the impossibility to arm the site, if the security alarm on the site is faulty, or arming is prohibited due to lack of payment for security services.

There are the following reasons for arming rejection:

- malfunction of one or more zones;
- alarm in one or more zones;
- no communication with the panel program via IP channel;
- absence of 220V on the site;
- no payment for security services;
- the device case is opened.

### 2.1.5 Standby Mode Indication

At the time of the reading indication, arming/disarming errors, arming and disarming the indication of the standby mode is interrupted.

The standby mode indication depends on how many partitions are configured in the device.

## One Partition

If only one partition is configured in the device, then the LED indicates the partition status, the presence of an alarm during protection and faulty zones:

- LED is on continuously if the partition is armed;
- LED is not on if the partition is disarmed;
- the LED “flashes” (blink), if there are faults in the zones;
- the LED “flashes”, if after the partition was armed, there was an alarm and the partition was not disarmed.

“Flashing” means that the LED turns on for 1 second, then turns off for 1 second, then turns on again for 1 second, etc.

## Several Partitions

If several partitions are configured in the device, then only the following is indicated: the entire device arming, presence of an alarm, when the entire device was under protection, and also the zone faults.

- LED is on continuously if all device partitions are armed;
- LED is off if at least one of the partitions is disarmed;
- LED “flashes” if there are faults in the zones;
- LED “flashes”, if after the device was armed, there was an alarm and the alarmed partition was not disarmed.

## 2.2 Built-In Keypad



*Figure 2: CN-Keypad*

The device state can be controlled or its status can be recognized using the built-in keypad.

### 2.2.1 Arming and Disarming

The device has the ability to arm and disarm several partitions with one user code. The partitions that can be armed or disarmed with a specific code are configured during the device configuration.

#### Arming

To arm a partition, it is necessary to press the “house” icon and enter the user code.

- if the code is correct, then the site (partition) will be armed, the keypad will confirm the arming by turning on the red LED. Or the countdown of the exit delay will start, which will be accompanied by a sound and LED indication.
- if the code is incorrect or the user who owns this code has more than one partition, the keypad will display an error.
- if arming is not possible, the keypad will display an error.



Figure 3

If several partitions are assigned to the user, then first the user shall click the “house” button, select the partition, which state he/she wants to change, and then type the code.



Figure 4: Example of arming of partition No. 1 with code 1234

#### Arming Rejection

“Arming rejection” is the impossibility to arm the site, if the security alarm on the site is faulty, or arming is prohibited due to lack of payment for security services.

There are the following reasons for arming rejection:

- malfunction of one or more zones;
- alarm in one or more zones;
- no communication with the panel program via IP channel;
- absence of 220V on the site;
- no payment for security services;
- the device case is opened.

#### Disarming

If the user can control only one partition, to disarm it is necessary to enter the user code.

- if the code is correct, then the site (partition) will be disarmed. The keypad will confirm disarming by turning on the green LED;

- if the code is incorrect or the user, who owns this code, can control several partitions, the keypad will display an error.



Figure 5

If the user can control several partitions, to disarm them, it is necessary to type the partition number, then # and enter the user code.

- If the code is correct, then the partition will be disarmed. The keypad will confirm disarming by turning on the green LED.
- In case of repeated disarming of the same partition, the keypad will display its status: the green LED will turn on.



Figure 6: Example of disarming of partition No. 1 with code 1234

The exit or entry delay countdown is indicated by the intermittent sound, which is reproduced during the entire delay interval. The sound indication of the exit or entry delay is disabled when any button on the keypad is pressed.

## 2.2.2 Getting Information about Status

The K14-LED keypad has green and red LEDs:

- Red LED is lighted when a partition is armed.
- If the partition is disarmed, the green LED is lighted.
- Red and green LEDs flash simultaneously if an error occurs. For example, if an incorrect user code is entered or in case of arming rejection.

### Getting Information about Site Status

To get information about a site status press **i** button:

- if all device partitions are disarmed, then green LED is lighted;
- if some partitions are armed, and others are disarmed, the keypad will display error, since it is necessary to clearly specify the number of the partition, which status shall be received;
- if the device configuration does not have partitions, then the device will display an error;

### Getting Information about Partition Status

To get information about a partition status press the partition number button and **i** button:

- if the partition is armed, then red LED will be lighted;
- if the partition is disarmed, then green LED will be lighted;
- if the device configuration does not have a partition with such a number, an error is displayed.

### 2.2.3 Panic Button

If the device configuration permits the use of the keypad as a panic button, then for activation it is necessary to press and hold the “houses” button for 3 seconds. The panic button pressing is confirmed by turning on of green and red LEDs for 1 second accompanied by sound.

If the device configuration prohibits the use of the keypad as a panic button, then the keypad will display an error.

### 2.2.4 Backlight and Sound Turning Off

Buit-in can turn on and off the sound and backlight.

To turn on or turn off the sound confirmation of pressing the buttons, simultaneously press and hold “#” and “9” buttons. To turn the backlight on or off, simultaneously press and hold “#” and “0” buttons.

## 2.3 CN-Keypad Wireless Keypad



*Figure 7: CN-Keypad*

The device state can be controlled or its status can be recognized using the “CN-Keypad” wireless keypad. To add a keypad to the device configuration, it is necessary to do the following.

- Remove the cover from the keypad.

- Power up - the keypad is powered by two lithium batteries type CR123A (main and backup). To replace the batteries, it is necessary to open the battery cover of the keypad, install the backup battery first, and then the main battery.
- In the device's configurator, go to the "Wireless devices" tab and click on "Add wireless device".
- Switch the keypad to the "Connection" mode. To do this, close the "Reset" contacts located on the device board. The green LED of "CN-Keypad" confirms the transition to the connection mode.

(For more details, see Section 5.3. Wireless devices)

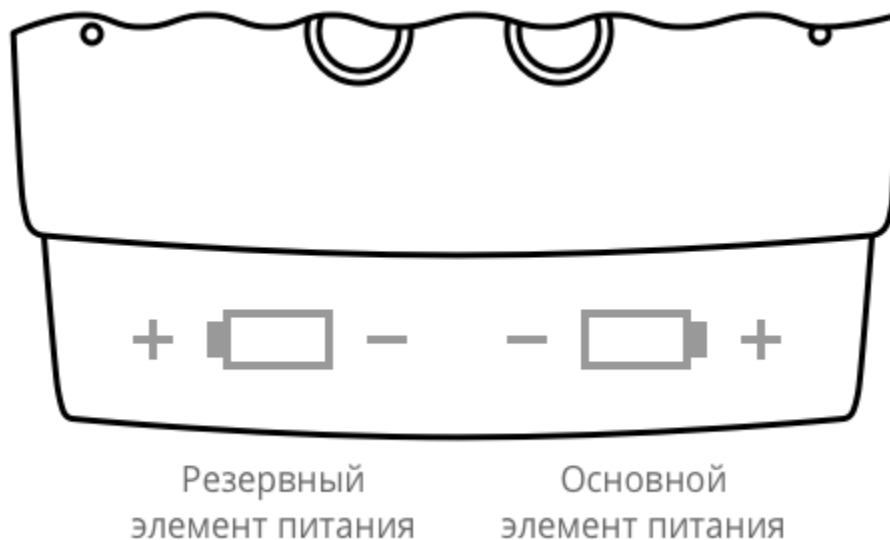


Figure 8: Battery compartment of the CN-Keypad keypad

The device can connect no more than four wireless keypads, and the device can work with all simultaneously.

### 2.3.1 Arming and Disarming

The device has the ability to arm and disarm several partitions with one user code. The partitions that can be armed or disarmed with a specific code are configured during the device configuration.

#### Arming

To arm a partition, it is necessary to press the "house" icon and enter the user code.

- if the code is correct, then the site (partition) will be armed, the keypad will confirm the arming by turning on the red LED. Or the countdown of the exit delay will start, which will be accompanied by a sound and LED indication.
- if the code is incorrect or the user who owns this code has more than one partition, the keypad will display an error.
- if arming is not possible, the keypad will display an error.

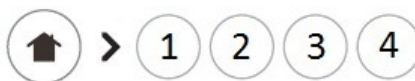


Figure 9

If several partitions are assigned to the user, then first the user shall click the “house” button, select the partition, which state he/she wants to change, and then type the code.



Figure 10: Example of arming of partition No. 1 with code 1234

### Arming Rejection

“Arming rejection” is the impossibility to arm the site, if the security alarm on the site is faulty, or arming is prohibited due to lack of payment for security services.

There are the following reasons for arming rejection:

- malfunction of one or more zones;
- alarm in one or more zones;
- no communication with the panel program via IP channel;
- absence of 220V on the site;
- no payment for security services;
- the device case is opened.

### Disarming

If the user can control only one partition, to disarm it is necessary to enter the user code.

- if the code is correct, then the site (partition) will be disarmed. The keypad will confirm disarming by turning on the green LED;
- if the code is incorrect or the user, who owns this code, can control several partitions, the keypad will display an error.



Figure 11

If the user can control several partitions, to disarm them, it is necessary to type the partition number, then # and enter the user code.

- If the code is correct, then the partition will be disarmed. The keypad will confirm disarming by turning on the green LED.
- In case of repeated disarming of the same partition, the keypad will display its status: the green LED will turn on.



Figure 12: Example of disarming of partition No. 1 with code 1234

The exit or entry delay countdown is indicated by the intermittent sound, which is reproduced during the entire delay interval. The sound indication of the exit or entry delay is disabled when any button on the keypad is pressed.

### 2.3.2 Getting Information about Status

The K14-LED keypad has green and red LEDs:

- Red LED is lighted when a partition is armed.
- If the partition is disarmed, the green LED is lighted.
- Red and green LEDs flash simultaneously if an error occurs. For example, if an incorrect user code is entered or in case of arming rejection.

### Getting Information about Site Status

To get information about a site status press **i** button:

- if all device partitions are disarmed, then green LED is lighted;
- if some partitions are armed, and others are disarmed, the keypad will display error, since it is necessary to clearly specify the number of the partition, which status shall be received;
- if the device configuration does not have partitions, then the device will display an error;

### Getting Information about Partition Status

To get information about a partition status press the partition number button and **i** button:

- if the partition is armed, then red LED will be lighted;
- if the partition is disarmed, then green LED will be lighted;
- if the device configuration does not have a partition with such a number, an error is displayed.

### 2.3.3 Panic Button

If the device configuration permits the use of the keypad as a panic button, then for activation it is necessary to press and hold the “houses” button for 3 seconds. The panic button pressing is confirmed by turning on of green and red LEDs for 1 second accompanied by sound.

If the device configuration prohibits the use of the keypad as a panic button, then the keypad will display an error.

### 2.3.4 Backlight and Sound Turning Off

“CN-Keypad” can turn on and off the sound and backlight.

To turn on or turn off the sound confirmation of pressing the buttons, simultaneously press and hold “#” and “9” buttons. To turn the backlight on or off, simultaneously press and hold “#” and “0” buttons.

## 2.4 Wireless Keyfob

Wireless keyfob, as a TouchMemory key, is assigned to a user. With a single TouchMemory key it is possible to arm or disarm only one partition. If one user has to be able to arm or disarm several partitions at the same time, then the appropriate rules shall be set in the “Automatic controls” section.

The keyfob is equipped with a panic button. If the button is pressed, the device will create an panic button alarm event.



### 2.4.1 MyAlarm Mobile Application

**MyAlarm** – is a mobile application for working with security alarm.

The MyAlarm application is available only to security company customers.

With the help of the mobile application, it is possible to control the state of “Nord GSM” devices, operating over GPRS or Ethernet. To do this, it is necessary to give access to the site in the Security Center software to the person in charge.

To arm or disarm from the application, click the lock icon. After that, enter the user code. More detailed information can be found in section «**MyAlarm**» on the technical support site.

### 3 Installation and First Start

#### 3.1 Device Wiring Diagram

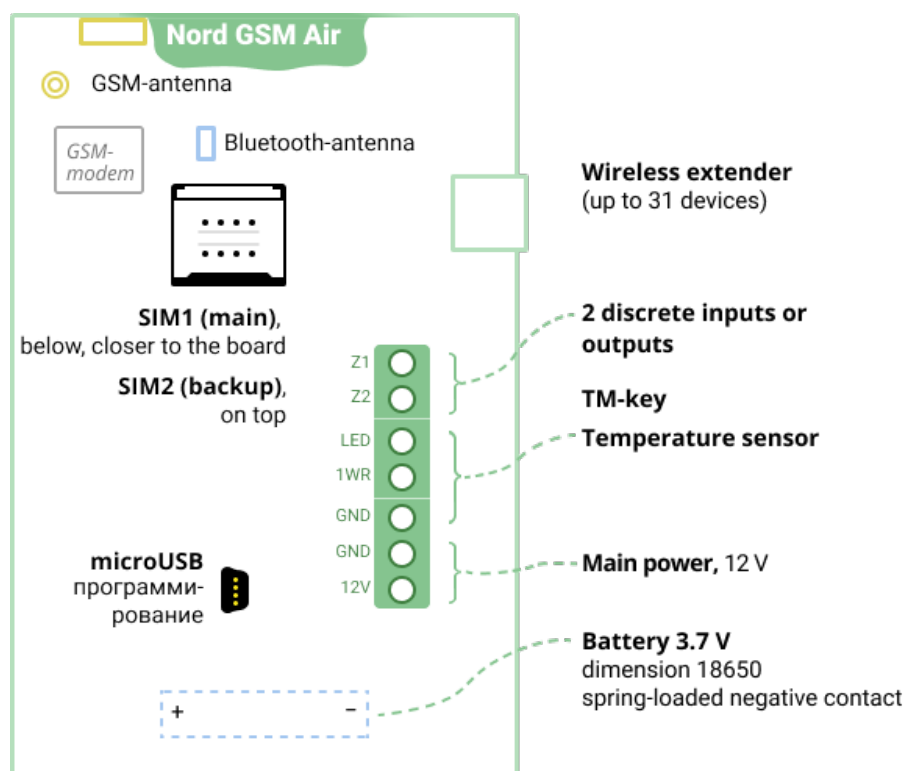


Figure 13

## 3.2 Connection of Wired Zones

The signal cables of the zones are connected to the terminals “Z1”-“Z4”.

The common zone cables are connected to the “GND” terminals.

The plus power supply cables of the security zones (12 V) are connected to the “S\_PWR” terminals.

### 3.2.1 Normally Closed and Normally Open Zone

The normal state of the zone is determined by its detectors:

- if the normal state for the zone is defined as *closed*, then there shall be detectors in this zone, which also have *closed* contacts of their output relay in the normal state. In case of alarm, these detectors shall *open* the contacts of the output relay;
- if the normal state for the zone is defined as *open*, then there shall be detectors in this zone, which have *open* contacts of their output relay in the normal state. In case of alarm, these detectors shall *close* the contacts of the output relay;

It shall be noted that the vast majority of modern infrared and magnetic contact detectors have *normally closed* contacts of their output relay. Thus, for zones with these detectors, the normal state shall be defined as *closed*.

Normally open detectors are connected to the zone in parallel, and normally closed - in series.

One zone can include detectors of only one type: either normally closed, or normally open.

### 3.2.2 Terminating Resistors

If the terminating resistors are not used when connecting the zone, then for this zone the device can determine only one of two states: “Alarm” or “Norm”. This zone is very vulnerable: if the normal state for the zone is defined as *open*, then it is very simple to cut the zone cable in any accessible location, and the zone will remain in the normal state forever, there will never be any alarms on such a zone. The zone, which normal state is defined as *closed*, does not look any better: if one can short-circuit the signal cables of the zone, then there will never be any alarms on it.

One terminating resistor, installed in the zone, allows to distinguish the failure in the zone from the alarm. What kind of fault can be detected - break or short circuit - depends on the normal state of the zone: for the zone *open* normal state, one terminating resistor allows to determine the zone break, and for the *closed* normal state – short circuit.

Two terminating resistors allow to determine both break and short circuit for a zone with any normal state.

For *minimum* counteraction against the alarm zone disabling, it is recommended to include at least one terminating resistor in the zones.

### 3.2.3 Zone without Terminating Resistors

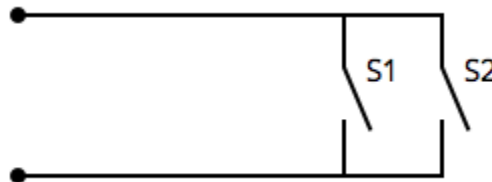


Figure 14: Normally open zone

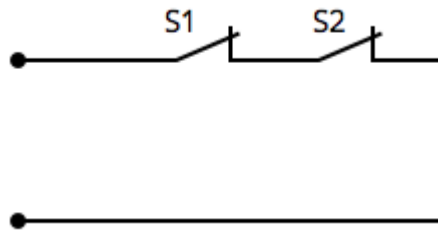


Figure 15: Normally closed zone

### 3.2.4 Zone with One Terminating Resistor

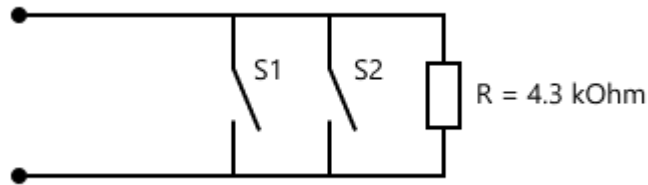


Figure 16: Normally open zone

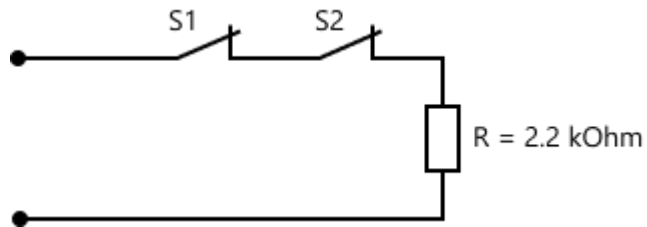


Figure 17: Normally closed zone

### 3.2.5 Zone with Two Terminating Resistors

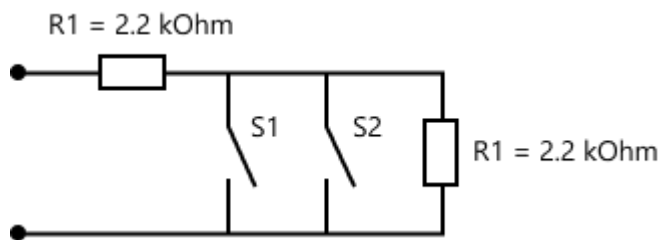


Figure 18: Normally open zone

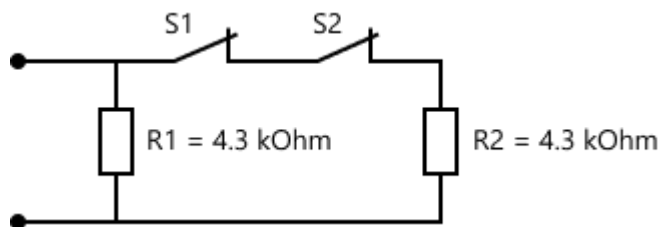


Figure 19: Normally closed zone

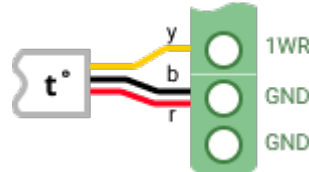
### 3.2.6 Wired Zones in Configurator

When configuring the device, it is necessary to explicitly specify the rate for the wired zone, and the number of terminating resistors. It is possible to do this on the “[Zones](#)” tab.

### 3.3 Connection of Temperature Sensors

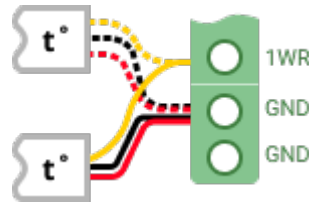
The wired temperature sensor is connected to the 1-Wire terminal group. The black and red wires coming from the sensor shall be twisted together and connected to the “GND” terminal, and the yellow wire to the “1WR” terminal - as shown in the picture below. If it is necessary to connect several wired temperature sensors, then all of them shall be connected in parallel to each other.

In order for the device to detect a wired temperature sensor, it is necessary to turn on the mode of constant polling of the 1-Wire interface in the device settings. It is possible to do this on the “Miscellaneous” tab in the [Control and indication](#) section.



*Figure 20: Diagram of wired temperature sensor connection to device*

It is possible to connect several wired temperature sensors to the device.



*Figure 21: Diagram of several wired temperature sensors connection to the device*

### 3.4 GSM Channel Setting

The device is equipped with an built-in GSM-modem, which can work alternately with one of the two installed SIM-cards.

### 3.4.1 SIM Card Installation

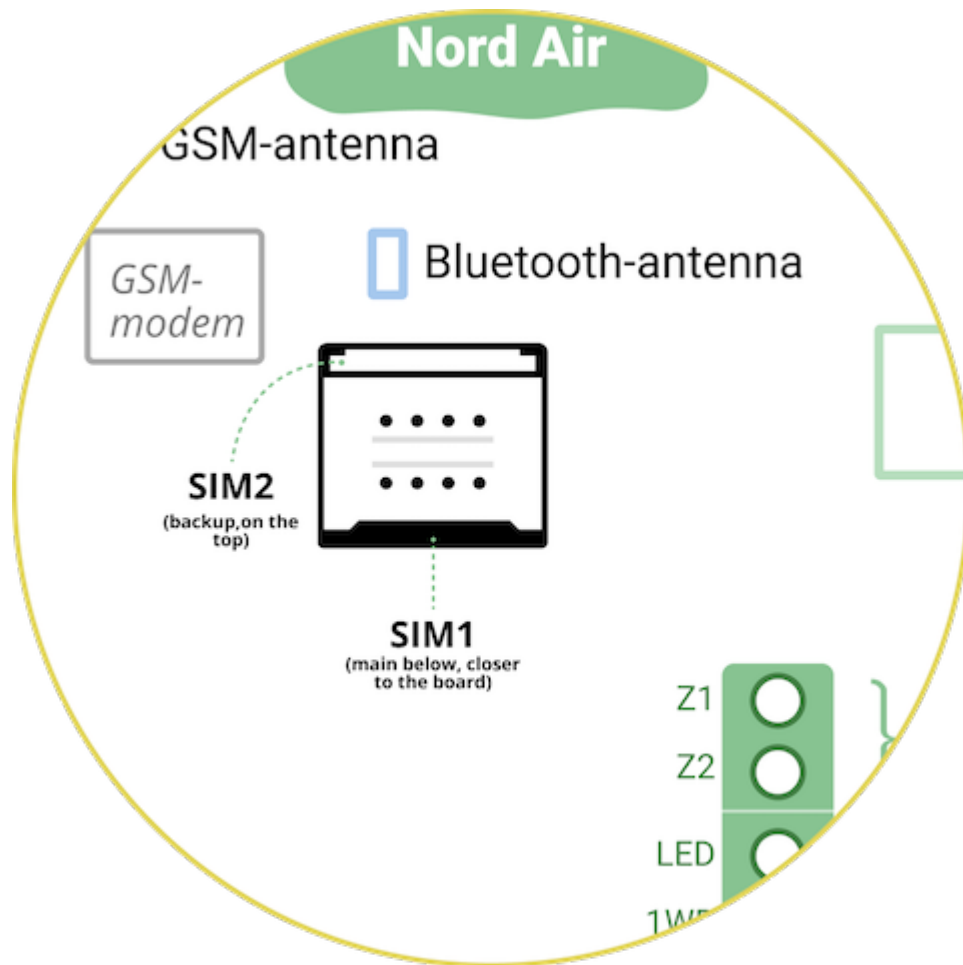


Figure 22: SIM Cards Installation

The SIM card holder is located on the middle part of the device board.

The main SIM-card (SIM1) is below, the reserve on (SIM2) is on top. SIM-cards are installed in the holder with the contact pad towards the board. Before installing SIM-cards in the device, completely disconnect it, otherwise the SIM-card can be disabled by static electricity.

Do not forget to turn off the PIN code request. If the PIN code is not disabled: firstly, the device will not be able to use this SIM card; secondly, the SIM card can be blocked after several activation attempts.

If you use only one SIM card, be sure to install it in the slot for the main SIM card - closer to the card.

### 3.4.2 Connection of Remote GSM Antenna

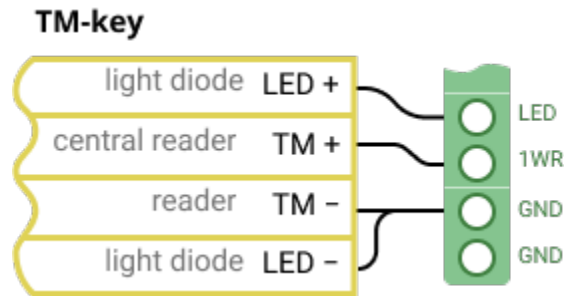
Recommendations for installation of the external antenna:

- move away from the device at a distance of at least 50 cm;
- do not coil the antenna feeder;
- mount the antenna on the dielectric surface;
- mount the antenna in a vertical position.

### 3.5 Connection of Touch Memory Reader

The device has a built-in interface for connecting the TM-key readers. It is possible to add up to 32 TM keys to the device.

Touch Memory reader is connected to the device to LED, DATA and GND terminals of the “Reader” group.



*Figure 23: Touch Memory card reader connection diagram*

Instead of the TM-reader, it is possible to connect any reader with the Dallas Touch Memory protocol emulation (DS1990A). For example, Proximity-readers (“PS-01”, “CP-Z2B”).

It shall be taken into account that to connect some readers that emulate the DS1990A protocol, it is necessary to disable the mode of constant polling of the 1-Wire interface, which is enabled by default. To do this, go to the [Miscellaneous](#) tab in the configurator and uncheck the “Enable constant polling of the 1-Wire interface” option.



## 4 Software Update

Before setting the device, it is necessary to make sure that the version of the software that is installed on it is up-to-date. For this connect the device to the computer and run the utility to update the firmware of the device via USB.

The software package that will be required to connect the device to the computer and update the software version can be downloaded from the official support site of C.Nord company([support.cnord.ru](http://support.cnord.ru)), from page «[Files for download](#)».

The package for updating the software version of the devices comes in the form of a zip-archive with the name of type **CnordFirmware-YYYYMMDD-XX.XX.zip**, where **YYYYMMDD** is the release date of the software, and **XX.XX** is a version of the software in the archive. The contents of the archive shall be unpacked in a folder on the hard disk of the computer. The following programs are included in the archive:

- driver for connecting the device to the computer;  
The driver is located in the folder **Driver**
- utility program, intended to update the software version of the device;  
The executable utility file is called **CnordFirmware.exe**, this file shall be run to update the software version of the device.

The package for updating the software version of the device includes the latest firmware versions for the following devices:

- Nord GSM, Nord GSM WRL, Nord LAN, Nord RF;
- Nord GSM Mini;
- Nord GSM Air;
- TR-100 GSM IV;
- Serzhant GSM;
- Soyuz GSM;
- Soyuz PCB GSM.

### 4.1 Device Connection to computer

The operating system of the Windows family (XP/7/8/10) shall be installed on the computer to which the device is connected. The operating system bitness (32 or 64 bits) does not matter.

Before connecting the device to the computer, *it is strongly recommended* to supply the main or backup power to it. If the device is powered by *only* USB, then its operation may be unstable.

Before you start working with the device, install the driver. The device is connected to the computer using a USB-Mini cable, and the driver is a special software that allows programs with which the user interacts to exchange data with the device.

The same driver is supplied for all operating systems.

### 4.2 Driver Installation in Windows XP and Windows 7

When you first connect the device to the computer, a notification will appear in the system tray of the taskbar that new hardware has been found. You can install the driver through Device Manager. To do this, go to the “Start” menu, right-click “Computer” and select Manage, then in the left menu select “Device Manager”.

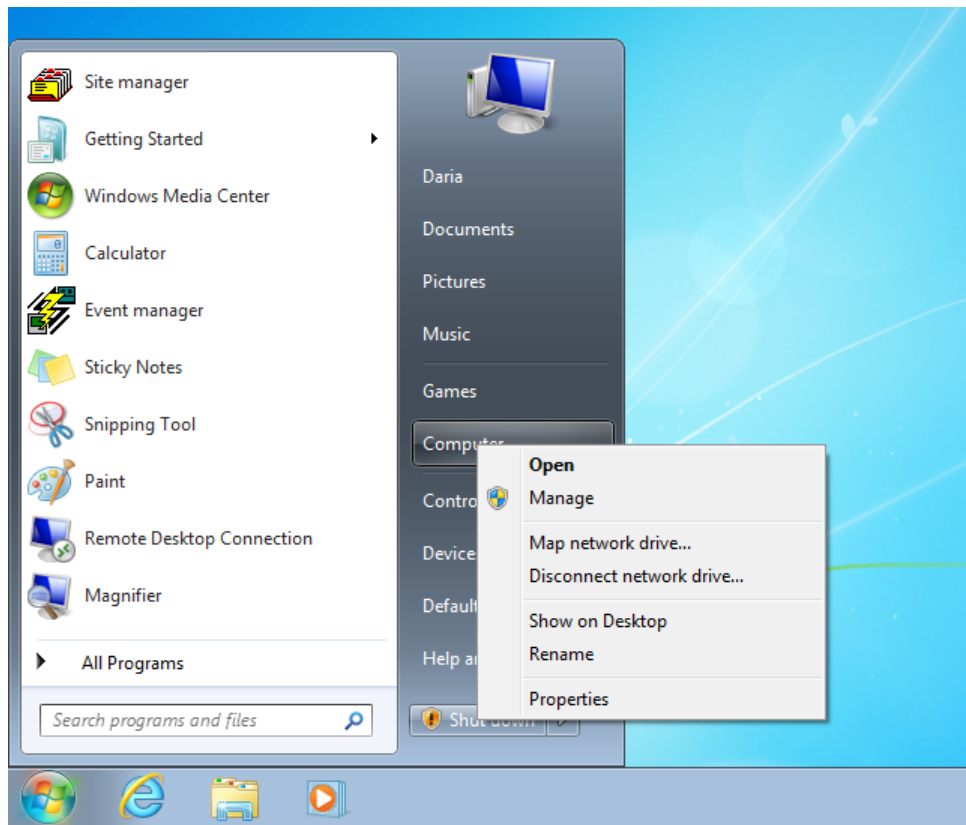


Figure 24

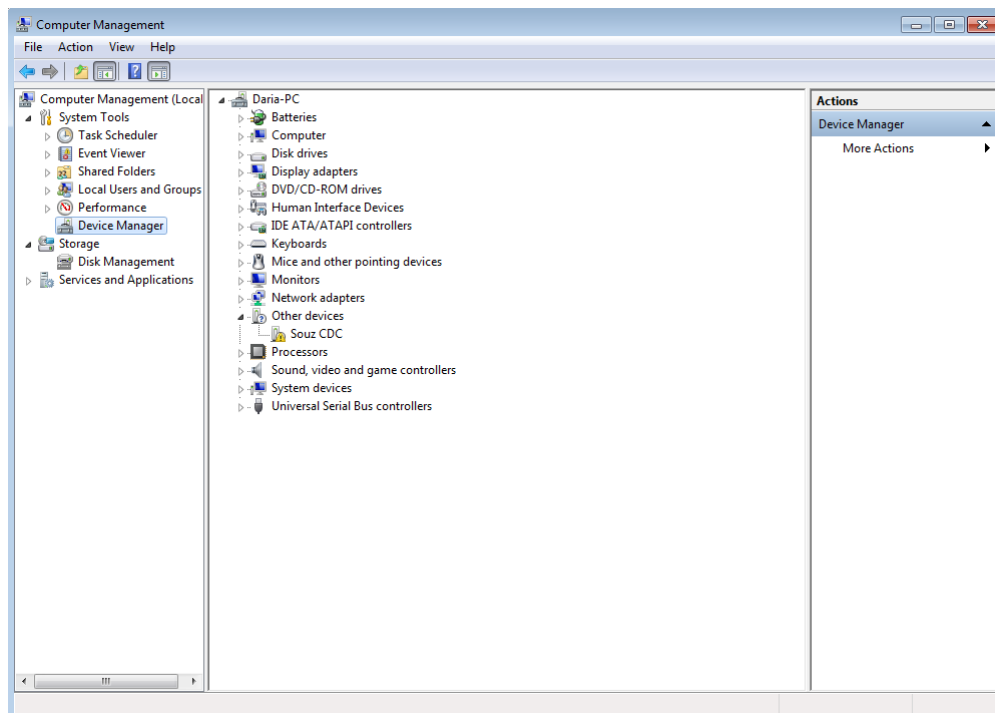


Figure 25

Right-click on the Soyuz CDC device and select the menu item "Update drivers".

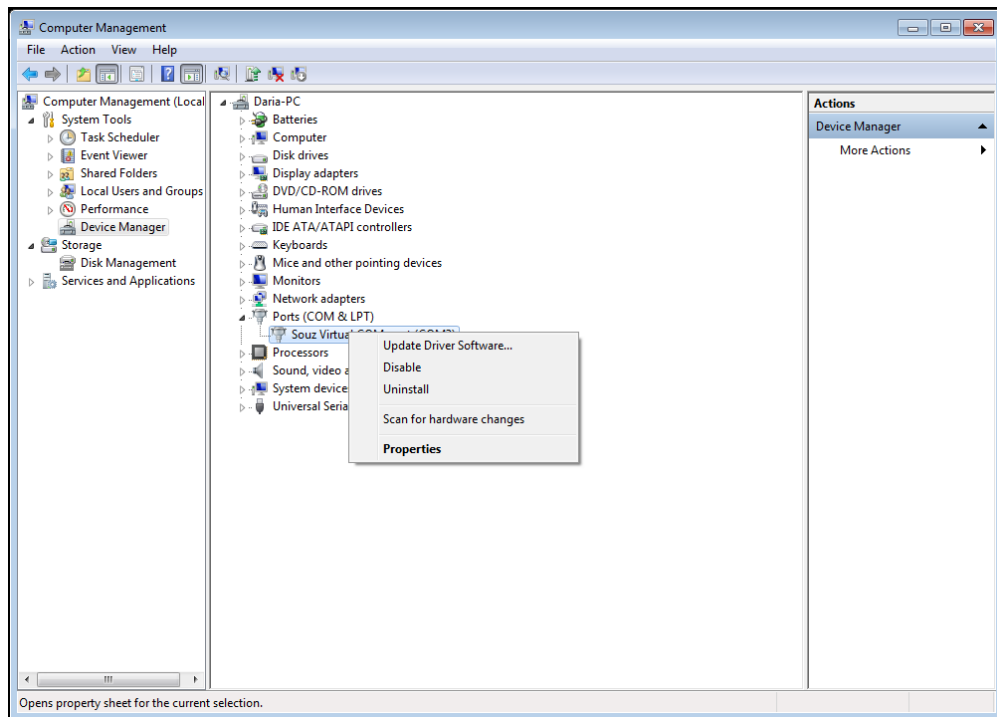


Figure 26

Reject the proposal to automatically find the driver for the new hardware, select the driver installation manually.

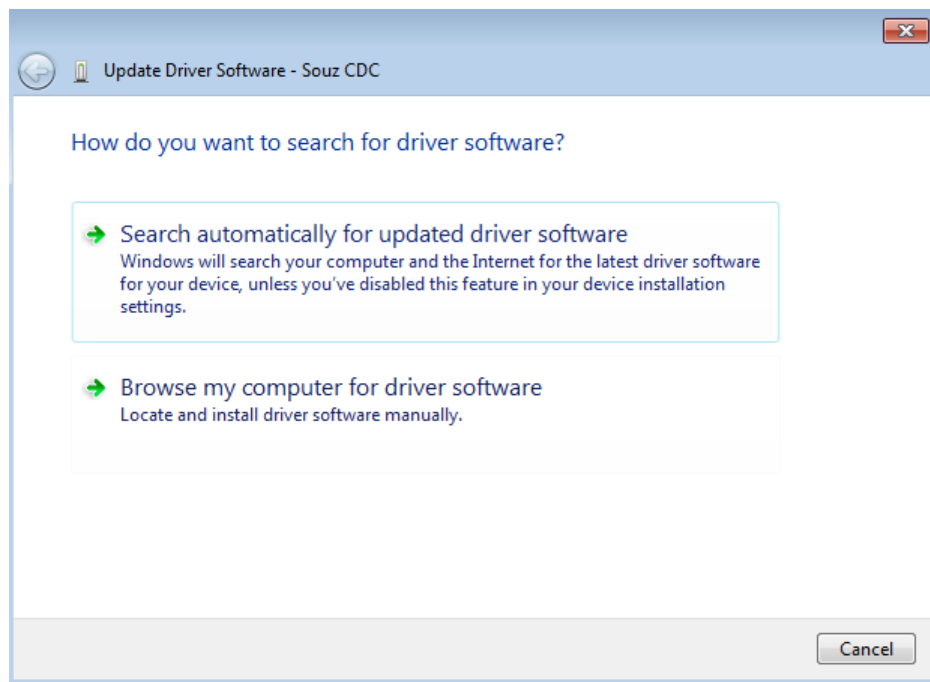
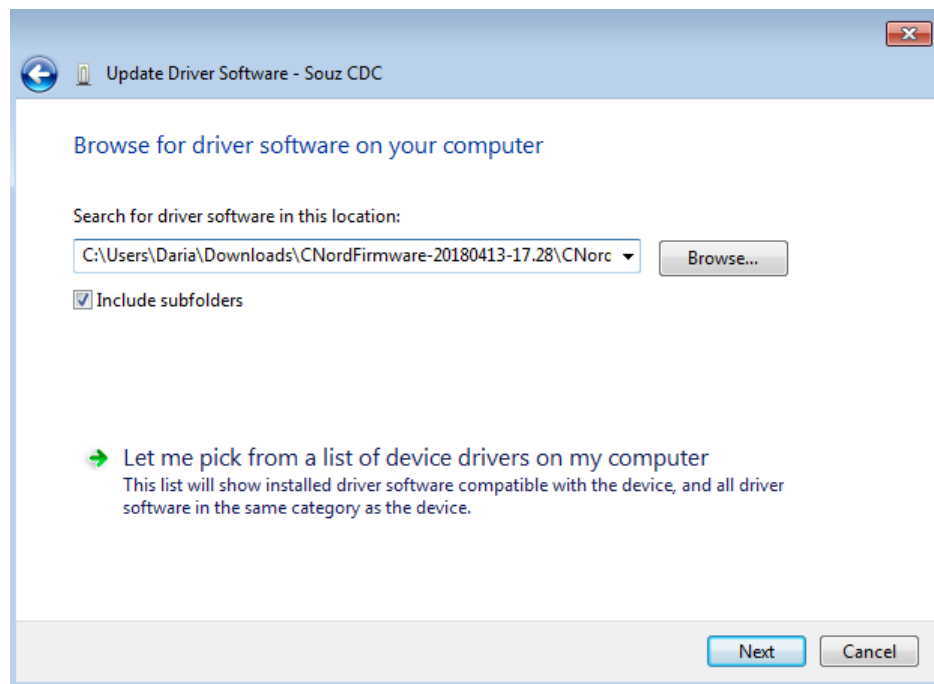


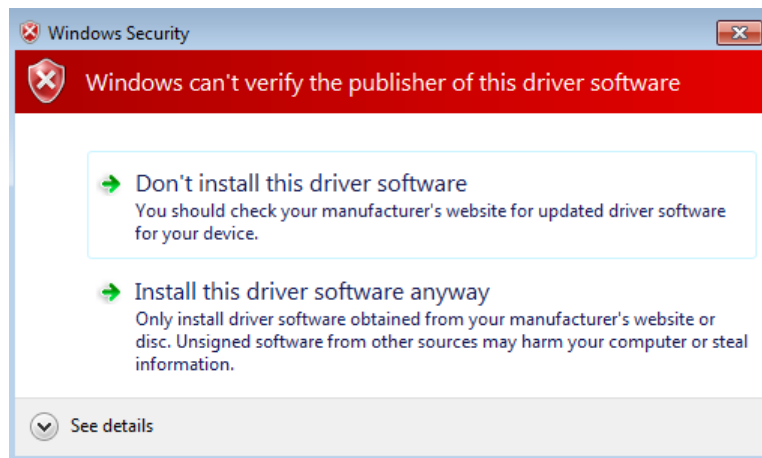
Figure 27: Selection of manual installation

Specify the path to the **Driver** folder and click Next.



*Figure 28: Selection of driver location*

The driver for the Nord GSM device does not have a digital signature. Therefore, you shall explicitly confirm to the operating system the need to install it.



*Figure 29: Confirming the driver installation without a digital signature*

After the driver installation is complete, click the “Close” button.

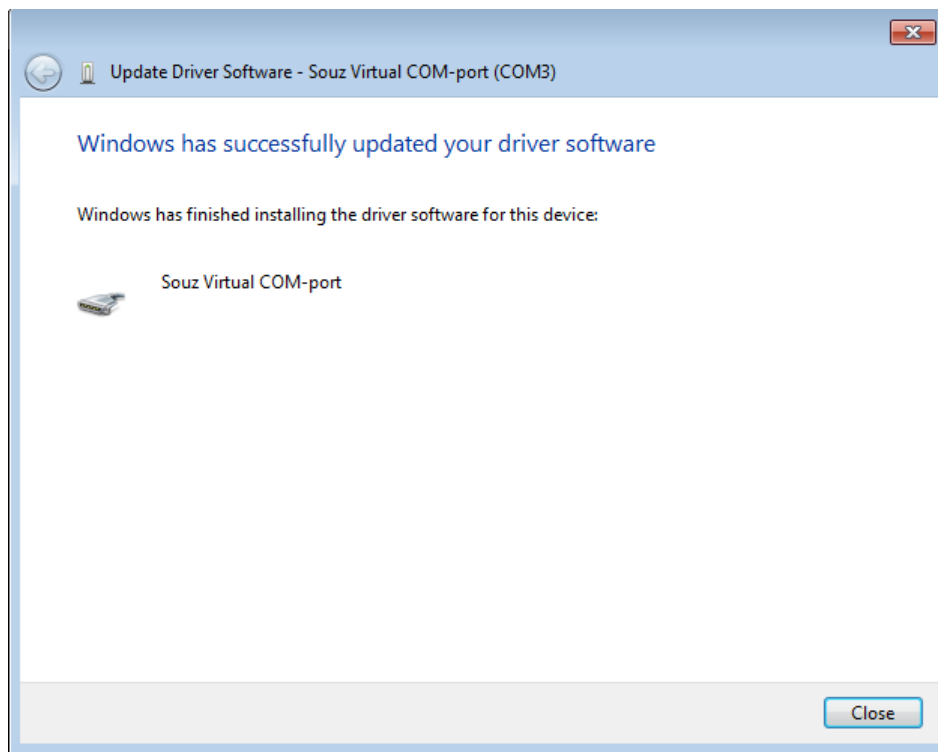


Figure 30: Completing the driver installation

To make sure that the driver for the device is installed, open the Windows Device Manager and find the virtual serial port that corresponds to the device connected to the computer.

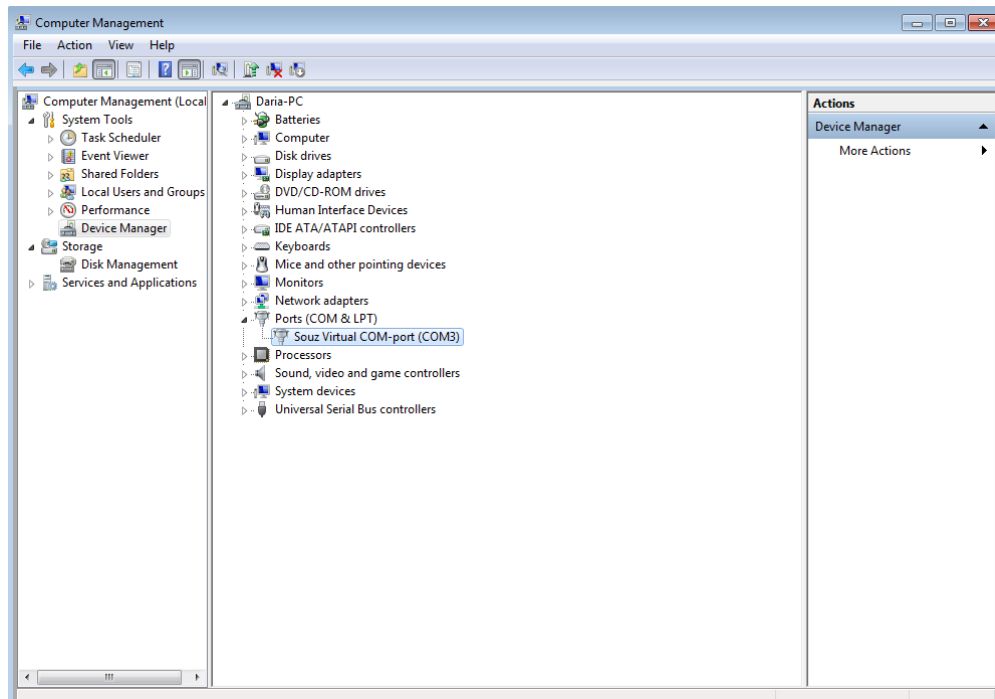


Figure 31: Device serial port of in the "Device Manager"

### 4.3 Driver Installation in Windows 8

Windows 8 operating system does not allow you to install drivers without a digital signature, as it was possible in previous versions. Therefore, before installing the driver for the device in this operating system, load it in a special mode - with the mandatory check of driver signature disabled.

To download the Windows 8 operating system with driver verification disabled, perform the following sequence of steps.

Press the key combination **Win + I**, then hold the button **Shift** and select the item “**Shutdown**” - “**Reboot**”:

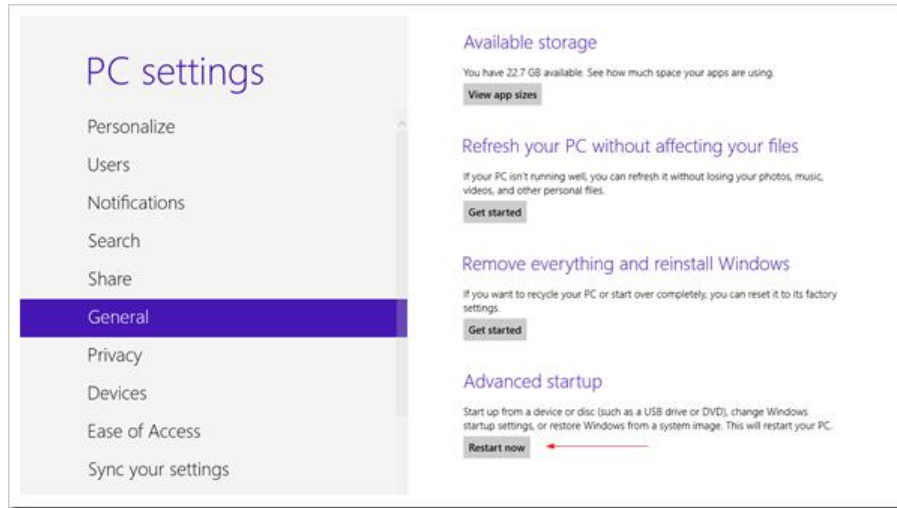


Figure 32: Reboot to change boot parameters

After the operating system restarts, the startup parameters window will appear. Select “**Diagnostics**”:

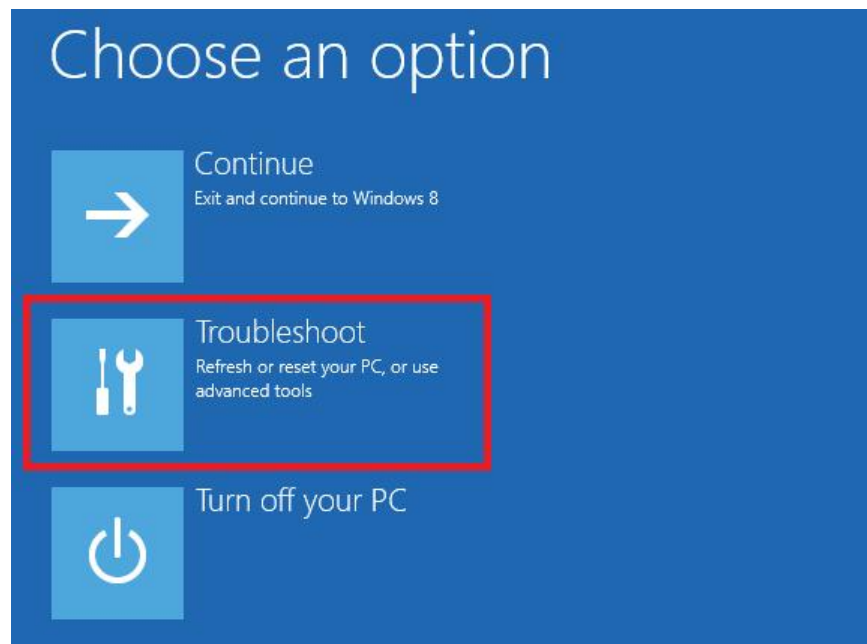


Figure 33: Entering the diagnostic mode

In the window “**Diagnostics**”, select the “**Additional parameters**”:

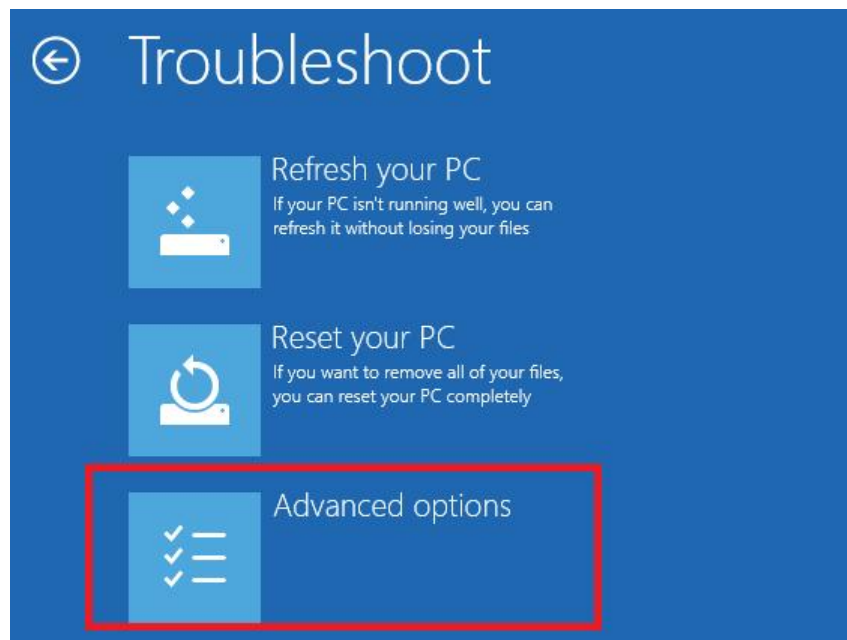


Figure 34: Advanced diagnostics parameters

In the “**Additional parameters**” window, select “**Boot parameters**”:

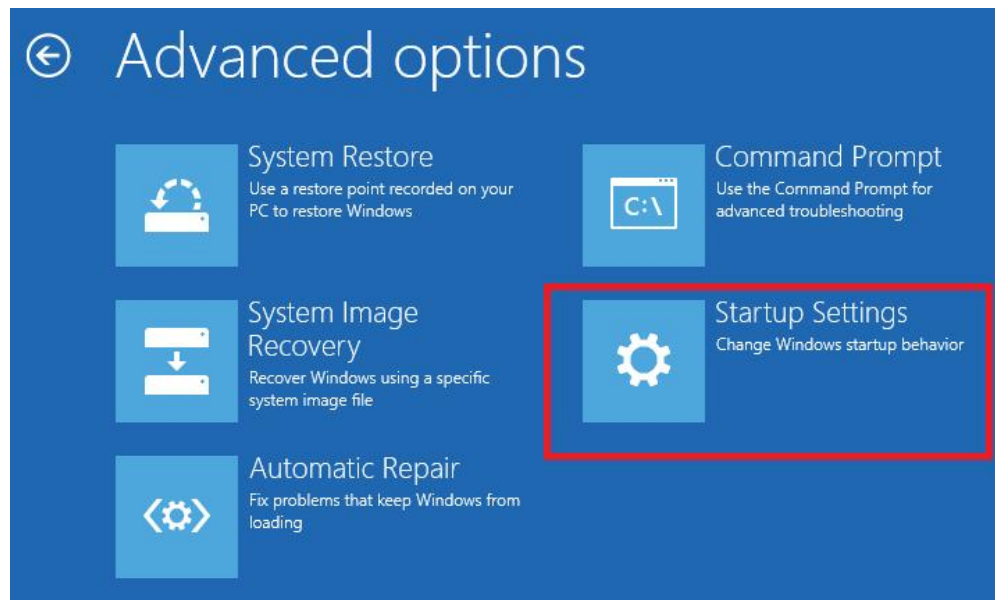
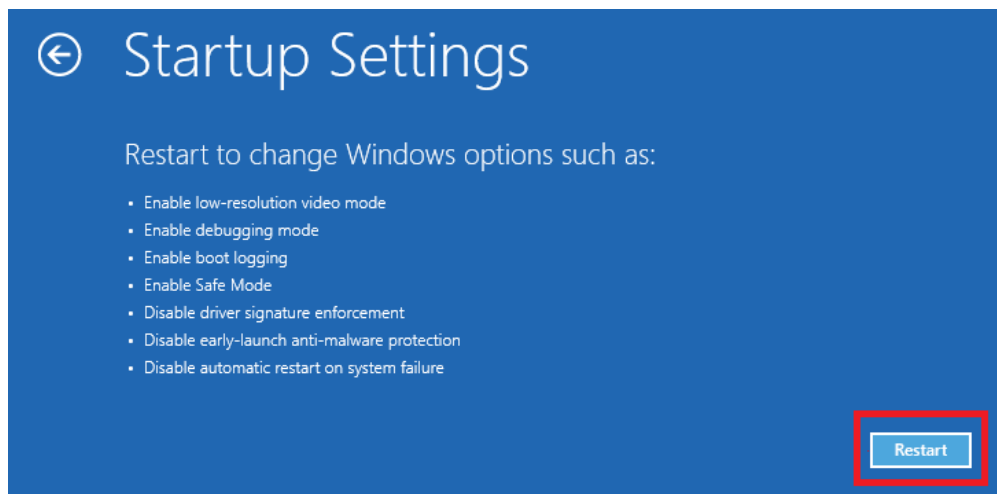


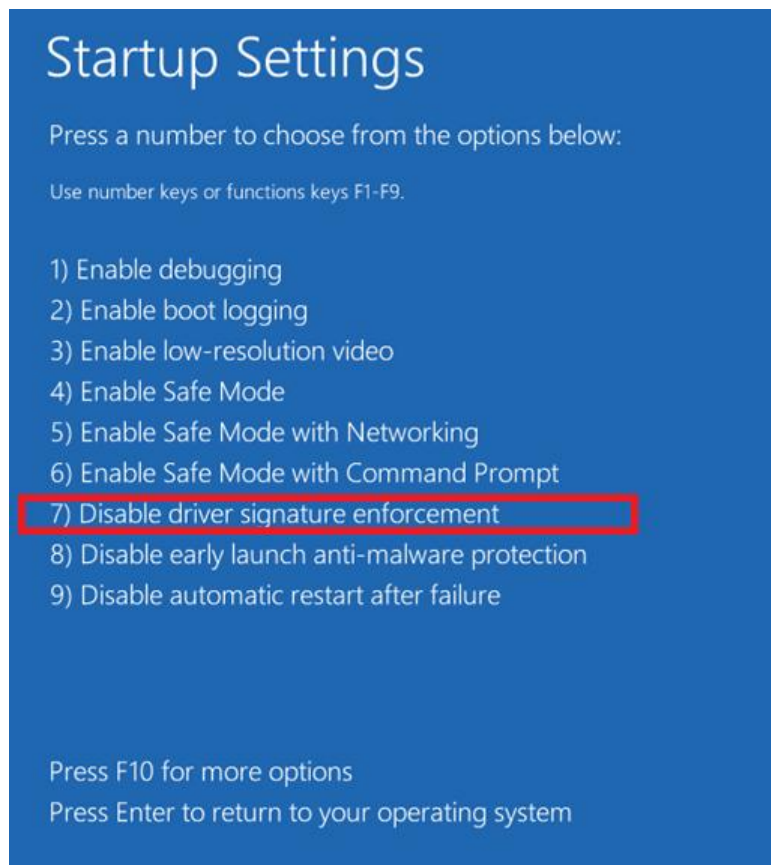
Figure 35: Operating system boot parameters

In the “**Boot parameters**” window, left-click the “**Reboot**” button:



*Figure 36: Reboot*

The operating system will reboot again, after which the “**Boot parameters**” window will appear. In this window, press the F7 button to continue loading the operating system with driver signature verification disabled:



*Figure 37: Disabling mandatory driver signature verification*

After the operating system starts, install the device driver in the same way as in the operating systems Windows XP/Windows 7. After installing the driver, restart your computer again to enable driver signature verification.



## 4.4 Utility to update software

The executable utility file is called **CnordFirmware.exe**, this file shall be run to update the software version of the device.

After the start, the utility searches for the device that is connected to the computer, determines its type, and displays the version of the software that is installed on it:

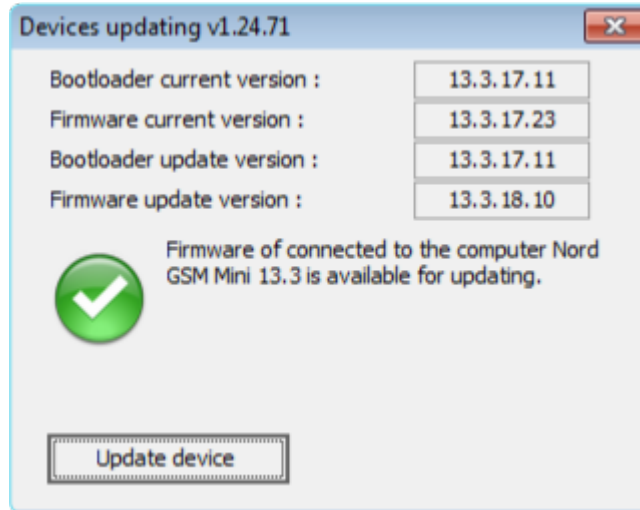


Figure 38: Display of software version on the device

If the software version on the device is smaller than the version of the update, it is necessary to update the firmware on the device. For this press the "Update device" button.

The device can be restarted several times during the update. After the firmware update is completed on the device, the corresponding message will appear in the utility window:

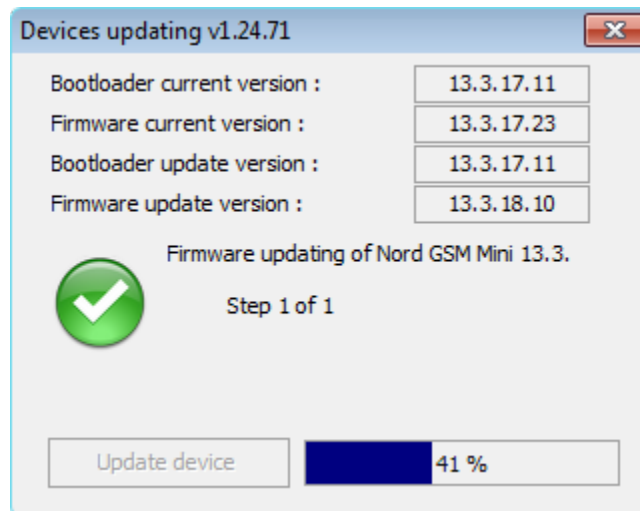
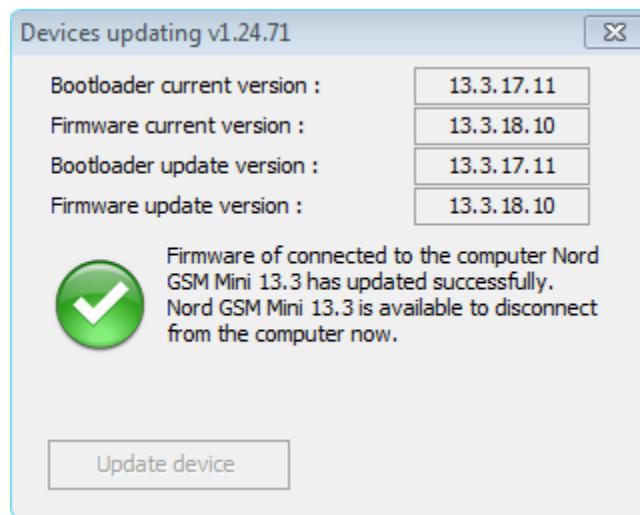


Figure 39: Software version update process



*Figure 40: Software version update is complete*

After that, the utility for updating the firmware via USB can be closed.

If an error message appears during the update process, it is recommended to disconnect the device from the computer, close the utility for updating the firmware, then reconnect the device to the computer and start the utility.

## 5 Device Configuration

A special configurator, called “Hubble”, is used to configure (change settings of) the device.

The current version of the configurator can be downloaded from the official support site of C.Nord company ([support.cnord.ru](http://support.cnord.ru)), from page «[Files for download](#)».

The configurator is supplied as a zip-archive with the name **hubble-X.XX.zip**, where **X.XX** is digits corresponding to the configurator version. Unpack the archive to the hard drive of the computer, preferably - to the root folder.

If you cannot unzip the archive to the root of the disk for some reason, unpack it to a folder in the name of which there are no Cyrillic symbols and spaces. If this condition is not met, then the device configurator will not work correctly.

The executable configurator file is called **hubble.exe**, this file shall be run to change the device settings.

The Hubble configurator is intended for changing the settings of the following devices: Nord GSM, Nord RF, Nord LAN, Soyuz GSM, Soyuz PCB GSM, TR-100 GSM IV and Serzhant GSM.

To start configuring the device, it is necessary to connect it to the computer via USB and run the configurator. In order for the configurator to be more convenient to run, it is recommended to place a shortcut for launching it on the desktop or in a folder of frequently used programs.

After the configurator is started, it automatically detects the device connected to the computer, checks the software version installed on the device, and loads the device settings.

If the version of the software installed on the device does not match the version required for the configurator, an error message will be displayed asking you to update the software on the device. In this case, it is necessary to shut down the configurator and update the software on the device as described in the “[Software Update](#)” section.

### 5.1 Control Panel and Tab Panel

### 5.2 Control Panel

The control panel is located at the top of the configurator main window:



*Figure 41: Control panel*

The following information is displayed on the left side of the control panel:

- device type;
- device software version;
- site number, specified in the device settings;
- device serial number.

The serial number of the device is assigned to it during production and is unique for the entire population of devices manufactured by the C.Nord company.

The “Read” button is designed to load the settings, that are currently stored in the device, into the configurator interface. It shall be remembered that if you make any changes in the device settings in the configurator, and then click on the “Read” button, all changes will be lost: the settings that were made in the configurator will be replaced with the settings loaded from the device.

The “Record” button is needed to save the configuration changes made in the configurator to the device.

The “Save...” button is designed to save the current settings to the file, which are displayed in the configurator. Use the “Open...” button to load the settings from the file.

To avoid errors related to setting up communication channels, it is recommended to save all settings related to connection to the Security Center and Cloud to the file on the disk, and begin to configure the device installed on the site with loading the file with these settings to the configurator.

### 5.2.1 Tab Panel

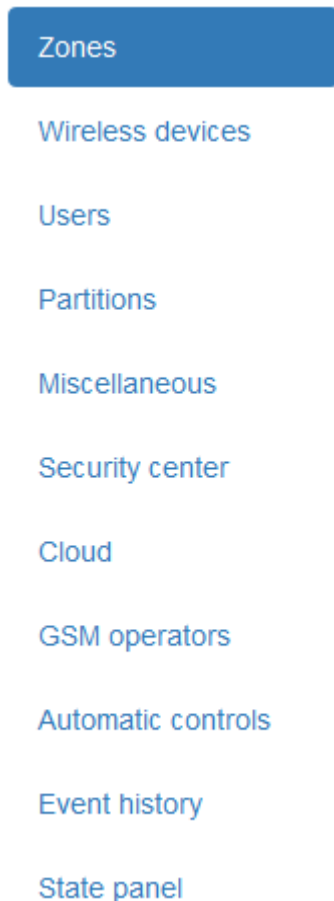


Figure 42: Tab panel

In the left part of the main window of the configurator there is a tab panel, with which it is possible to switch between groups of device settings.

On the “Zones” tab, the parameters of the wired zones connected to the device are configured.

The “Partitions” tab configures the partitions of the site. On this tab it is possible to specify in which partitions which wired zones are included, and in addition, specify which users can arm or disarm the partitions.

On the “Miscellaneous” tab, it is possible to set the intervals that are used when repeating the events sent to the Security Center, specify the type of backup power source connected to the device, turn on or off the sound and light indicator, etc.

Settings that the device shall use when transmitting events via GSM and Ethernet communication channels can be specified on the “Security Center” tab.

Parameters that determine the transmission of events over a radio channel are specified on the “Radio” tab.

The “Cloud” tab is intended to indicate to which Cloud the device shall be connected in order for the engineer to have a remote access to it. The parameter values on this tab shall only be changed if you are using Private Cloud, or it is necessary to specify the parameters for connecting to the Cloud manually.

On the “Ethernet” tab, it is possible to change the device connection settings to the local network. This tab is displayed in the configurator only if an optional Ethernet Adapter module is connected to the device.

The parameters of cellular operators, such as the access point name (APN), user name and password for access to packet data services, can be changed on the “GSM Operators” tab.

The “Automatic controls” tab is intended for programming the device behavior depending on various conditions. Any events formed by the device or time can act as the conditions. Arming or disarming and actions with open collectors are actions that the device can perform.

Events that are stored in the device non-volatile memory can be viewed on the “Event history” tab. Here it is possible to mark, as posted, the events that are waiting for delivery to the Security Center in the transmission queue.

The “State panel” tab displays the status of communication channels and wired zones in real time.

## 5.3 Zones

Use the “Zones” tab to configure the parameters of the wired zones connected to the device.

Number		Type	Norm	Enter delay	Exit delay
1	<button>Disable</button>	Arm	Opened	15 s	15 s
2	<button>Disable</button>	Panic button w/o fixation	Opened		

Figure 43: “Zones” tab

### 5.3.1 Zones Numbering

The numbers of zones displayed in the configurator correspond to the marking of the terminals on the printed circuit board: “Z1” - zone No. 1, “Z2” - zone No. 2.

### 5.3.2 Turning Zone On and Off

The on/off button of the zone is in the left column, just behind the zone number. The button color reflects the current status of the zone: if the button is green, the zone is on, if the button is red, then it is off. The inscription on the button corresponds to the operation that will be performed when the button is pressed: the green button says “Disable”, because when the button is pressed, the zone is turned off, and the red button says “Enable”, because when the red button is pressed, the zone is turned on.

In order for the device to start monitoring the zone condition, and also for the user to configure the zone, it shall be turned on. If the device has at least one *enabled* zone, which is of the type “Arm”, “Arm without siren” or “Bypass”, then such a zone shall be added to the part.

If the wired zone is *disabled*, its state, as well as the state changes, are ignored by the device. In addition, if the zone is disabled, it cannot be added to the part: it is not displayed in the list of zones available for adding to the part.

The zone disabling can be useful in case it is necessary to temporarily stop the zone monitoring, for example, due to its malfunction. It is possible to disable the zone either when connecting to the device locally (via USB) or when connecting remotely from the web-configurator.

### 5.3.3 Zone Type

Setting the type for the zone is a key moment for the zone configuration, since this parameter completely determines the device response to the change in the zone state. The following depends on the zone type:

- whether the device will react to the zone transition to the “Alarm” state always, or only at the time when the part, into which the zone is included, is armed;
- what event code will be sent to the receiver in case of alarm in the zone;
- whether the siren is activated in case of alarm in the zone;
- whether the power is turned off and on again at the “SMOKE” terminal after an alarm in the zone;
- whether the normal condition of the zone will be monitored while arming the part, into which the zone is included.

Differences between the types of wired zones are shown in the table below:

Zone type	Event codes	Arming/disarming	Siren	Note
Arm	E130 / R130	Yes	Yes	
Arm without siren	E146 / R146	Yes	No	
Bypass	E130 / R130	Yes	Yes	Zone alarm is specially handled during arming and disarming (see below).
Fire	E110 / R110	No	Yes	Zone alarm is accompanied by power reset of fire sensors (see below).
Panic button with fixation	E120 / R120	No	No	
Panic button without fixation	E120 / R120	No	No	Separate alarm repetition interval is used for the zone of this type (see below).
Sensor tamper	E144 / R144	No	Yes	
24-hour arm	E133 / R133	No	Yes	
24-hour	E150 / R150	No	Yes	
Water leak	E154 / R154	No	Yes	
Gas leak	E151 / R151	No	Yes	
Temperature sensor	E158 / R158	No	Yes	High temperature
Temperature sensor	E159 / R159	No	Yes	Low temperature

#### *Wired zone types*

If “Yes” is specified in the “Arming/disarming” column for the zone type, it means that this type of zone can be armed or disarmed together with any of the part, into which it is included. If “No” is specified in the “Arming/disarming” column for the zone type, it means that this type of zone is *always* armed.

If “Yes” is specified in the “Siren” column for the zone type, it means that in case of an alarm in a zone, the horn will be activated.

#### **”Bypass” Zone Type**

If the zone type is set to “Bypass”, then this zone is specially handled during arming and disarming.

When arming the bypass zone state is ignored: the device will be armed even if the zone configured as bypass is in alarm. In addition, the bypass zone state is ignored until the exit delay ends for all the zones of the part being armed. In this case, the exit delay for the zone itself cannot be set, it always has an exit delay equal to the largest exit delay of the other zones included in the part.

If the part, into which the bypass zone is included, is armed and the bypass zone becomes alarming, then first the check is made to see if the entry delay count for another part zone has started. If the entry delay count is in process, the alarm in the bypass zone is ignored. If there is no entry delay, the “Alarm” (**E130**) event will be generated for the bypass zone.

#### **”Fire” Zone Type**

When generating an alarm on zones with the “Fire” type, the device uses the “Warning”/“Fire” mechanism: it is based on the logic of the detector’s repeated operation after a power reset. The device switches to the generalized “Fire” state, which is accompanied by fire siren, as well as the repetition of fire alarms. This state is stored in the device memory, i.e. when the power or panel is reset, the generalized “Fire” state is saved.

#### **”Panic button without fixation” Zone Type**

If the zone type is “Panic button without fixation”, then such a zone has its own interval of alarm repeat.

The alarm repeat interval set for the device is not used for this type of zone. Instead, it is set to a value of 5 seconds. Thus, pressing the panic button again not earlier than after 5 seconds will result in the transition of another event to the panel.

### “Temperature Sensor” Zone Type

If a wired temperature sensor is connected to the device, and the 1-Wire line polling mode is enabled (enabled on the [Miscellaneous](#) tab), it will appear automatically in the “Zones” tab and will have a zone number in the range from 48 to 51. For temperature sensors, the upper and lower thresholds shall be specified, at which alarms will be generated. Range of permissible values for thresholds: from -55°C to 127°C. Read more [about connecting temperature sensors](#). A total of 4 temperature sensors can be connected to the device.

### 5.3.4 Zone Normal State

Using the value that is set in the “Norm” column, it is possible to define *normal* state for the alarm zone:

- if the normal state for the zone is defined as *closed*, then there shall be detectors in this zone. which also have *closed* contacts of their output relay in the normal state. In case of alarm, these detectors shall *open* the contacts of the output relay;
- if the normal state for the zone is defined as *open*, then there shall be detectors in this zone, which have *open* contacts of their output relay in the normal state. In case of alarm, these detectors shall *close* the contacts of the output relay;

It shall be noted that the vast majority of modern infrared and magnetic contact detectors have *normally closed* contacts of their output relay. Thus, for zones with these detectors, the normal state shall be defined as *closed*.

### 5.3.5 Terminating Resistors

This option is available only if devices allow to connect terminatig resistors to the zones.

Using the value, which is set in the “Resistors” column, it is possible to specify the number of terminating resistors installed in the zone.

If the terminating resistors are not used when connecting the zone, then for this zone the device can determine only one of two states: “Alarm” or “Norm”. This zone is very vulnerable: if the normal state for the zone is defined as *open*, then it is very simple to cut the zone cable in any accessible location, and the zone will remain in the normal state forever, there will never be any alarms on such a zone. The zone, which normal state is defined as *closed*, does not look any better: if one can short-circuit the signal cables of the zone, then there will never be any alarms on it. One terminating resistor, installed in the zone, allows to distinguish the failure in the zone from the alarm. What kind of fault can be detected - break or short circuit - depends on the normal state of the zone: for the zone *open* normal state, one terminating resistor allows to determine the zone break, and for the *closed* normal state – short circuit.

Two terminating resistors allow to determine both break and short circuit for a zone with any normal state.

For *minimal* counteraction against the alarm zone disabling, it is recommended to include one terminating resistor in the zones.

### 5.3.6 Entry Delay

The “Entry delay” parameter will allow delaying the generation of the “Alarm” signal for the time, which is indicated as the value for this parameter. Typically, this parameter is set for zones that the user *shall* violate to get to the alarm management device. As common examples of such zones, one can mention magnetic contact detectors that protect entrance doors to a guarded room.

How does the entry delay work? Suppose that we have a zone, it includes a magnetic contact detector, which is installed on the entrance door to the office. For this zone, an entry delay of 15 seconds is specified. The codebook, with which it is possible to disarm it, is inside the office, that is, it is necessary to open the front door to get to it. The user opens the entrance door, the magnetic contact detector is triggered, but the device does not generate an alarm, but starts counting the entry delay. If within 15 seconds the user enters the code with which the alarm will be disarmed, the alarm will not be generated, instead of it an event will be sent to the security panel to disarm the device. If the device is not disarmed within 15 seconds, an alarm will be generated.



The value of the “Entry delay” parameter can be specified only for zones of the type specified as “Arm” or “Arm without siren”. This is due to the fact that zones of all other types (with the exception of “Bypass”) cannot be armed or disarmed: they are always armed. As for the “Bypass” zone, the zones of this type are handled during arming or disarming in a special way, as described above, in the section “Zone Types”.

### “Probable Alarm” Event

If the zone with entry delay is violated, the device certainly generates the “Probable alarm” event (\*\* E138 \*\*). The number of the violated zone and the smallest number of the part, into which this zone is included, are transmitted as the event arguments. If several zones with entry delay are violated, an event “Probable alarm” will be generated for each zone.

On some sites, the control panel cannot be placed so that it is located in a separately guarded part of the room. Typically, these sites can include small rooms: shopping pavilions, garages, small offices and apartments. This means that during the entry delay countdown, the control panel can be disabled. The “Probable alarm” event allows the security panel to monitor the device operability after the entry delay countdown begins: if there is no event after the start of the entry delay, when the device is disarmed, it is an occasion to find out what is happening at the site.

To automatically monitor the reception of a disarming after a possible alarm in the Security Center, it is necessary to use the “Alarm entering” event handler or the “Event chain monitor” event handler.

### 5.3.7 Exit Delay

The purpose of the “Exit delay” parameter is very similar to that of the “Entry delay” parameter, but it is intended to allow the user to exit the guarded premises after he/she performed the arming. As a rule, the exit delay is set for zones that protect the entrance doors to the protected premises.

After the user arms the part (using the keyboard, wireless controller or TM reader), the device checks the status of all zones included in the part:

- if a faulty cable is detected, the device refuses to arm;
- if the alarm zone is detected, the device also refuses to arm;
- if there are no faulty or alarm zones, the device is armed and the exit delay counts, if any.

The arming event (**E401**) is generated immediately during arming, before the exit delay starts, if any. The number of the protected part and the number of the user, who performed the arming, are transmitted as arguments of the event.

After the exit delay countdown starts, the device ignores the status of all zones for which an exit delay is specified, as well as zones with a “Bypass” type. If the user has time to leave the premises and close the entrance door before the exit delay countdown has expired, then there will be no alarm after arming. If any of the zones are violated after the exit delay ends, an alarm will be generated.

For wireless devices, if the device allows to connect them, the state that was received during the last poll of the device is taken as current. Thus, the user of the wireless system may need to wait until the wireless detector sends a normal state to the device. In case you do not want to wait, it is possible to set the minimum possible delay for the wireless detectors.

It may happen that during the arming it is impossible to achieve the normal state of one or several zones, for example, if the detectors in the zones monitor the keyboard area. In this case, the zones shall be configured as *bypass*. The bypass zones are described in more detail above, in the section “Zone Types”.

An alarm in the zones with exit delay at the time of arming is ignored. This is done so that the user does not have to check and close the front door. But, if you want to be sure that all alarm zones are normal at the time of arming, it is possible to turn on alarm monitoring in zones with exit delay at the time of arming. To do this, check the parameter “Disable arming when triggering the alarm in zones with exit delay” in the “Miscellaneous” tab, in the “Arm and disarm” section.

## 5.4 Users

On the “Users” tab, the users of the site are created. It is possible to create up to 32 users in the device, and each user, in addition to personal code, can also have wireless keyfobs and TM-keys.

Number	Code	Keys	Keyfobs
1	<input type="button" value="Change"/>	<a href="#">Scan</a> <a href="#">Enter the number</a>	<input type="button" value="🗑"/>
2	<input type="button" value="Change"/>	<div>00000CBF1955 ✖</div> <div><a href="#">Scan</a> <a href="#">Enter the number</a></div>	<input type="button" value="🗑"/>
<input type="button" value="Add user..."/>			

Figure 44: “Users” tab

To create a new user, it is necessary to click the *Add user* button and enter the code in the new window, which the user will use when arming or disarming the site.

### New user

The code must contain 4 numbers, be unique, and differ from the alarm sound disable code (5422).

Figure 45: “Users” tab, code entry dialog


To add a Touch Memory key, click the **Scan** button in the “Keys” column, then attach the TM-key to the reader. If the reader is connected correctly, the key code will be displayed. It is possible to manually add a TM-key. To do this, press the button **Enter the number** and enter information from the key in the new window. Next, go to the [Partitions](#) tab and add the key to the partition it will control. One user can have several TM-keys, but a single TM-key can control the state of only one partition.

### Adding key for user No.2

Set the key to the reader unit

Figure 46: “Users” tab, adding TM-key

## Add TM key number



**Family code**  
TM key family code is 01

**Key number**  
12-digit device ID

**CRC**  
The amount calculated for the key number

Figure 47: “Users” tab, manually adding TM-key number

If the wireless keyfob is attached to the device, it is possible to add it to a specific user using the *Add keyfob* button. Connect the wireless keyfob to the device on the “Wireless devices” tab. After the keyfob is added, it is possible to go to the “Partitions” and match the keyfob with the partition it will control.

Number	Code	Keys	Keyfobs	
1	<input type="button" value="Change"/>	Scan <span>Enter the number</span>	<input type="button" value="Add keyfob"/>	<input type="button" value="Delete"/>
2	<input type="button" value="Change"/>	Scan <span>Enter the number</span>	<input type="button" value="Add keyfob"/>	<input type="button" value="Delete"/>
<input type="button" value="Add user..."/>				

Figure 48: “Users” tab, adding a keyfob

Use the recycle bin icon to delete previously created users.

## 5.5 Partitions

The “Partitions” tab configures the partitions of the site. It is possible to create up to 32 partitions in the device with the possibility of their independent arming and disarming.




Number	Zones	Arm and disarm	
1	<div>✕ №1, Arm</div> <div>✕ №2, Transient</div> <div>Add zone ▾</div>	<div>✕ User №1, code</div> <div>Add code ▾</div>	
2	<div>✕ №3, Arm</div> <div>✕ №8, Water leak</div> <div>Add zone ▾</div>	<div>✕ User №2, code</div> <div>Add code ▾</div>	
3	<div>✕ №19, Transient</div> <div>✕ №21, Arm</div> <div>Add zone ▾</div>	<div>✕ User №3, keyfob 1</div> <div>Add code ▾</div>	
<div>Add partition</div>			

Figure 49: “Partitions” tab

To create a partition, click the “Add partition” button. Each partition is assigned its own number, the numbers are given sequentially from 1 to 32. Each partition has the “Add zone” and “Add code” buttons located in the second and third column respectively.

Use the “Add zone” button in the drop-down menu to select the zones that will be added to this partition. The drop-down menu displays only *enabled* zones.

Use the recycle bin icon to delete previously created partitions.

### 5.5.1 Partition Management

In order for a user to use his or her personal code during the partition arming or disarming, the user shall be mapped to this partition. To do this, click the “Add code” button and select those users from the drop-down list who will be able to manage a particular partition.

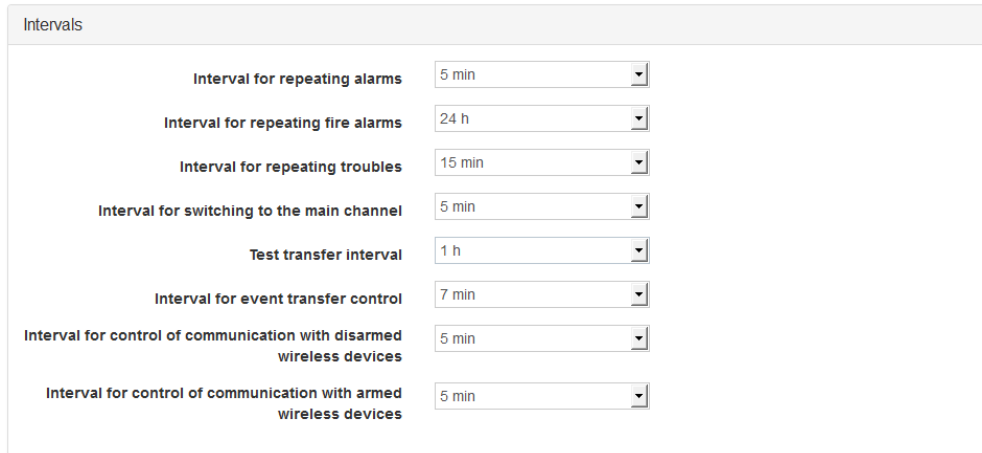
If a user has a TM-key and wants to manage partitions with it, they also shall be added to the selected partition. It is important to consider the following:

- If the TM-key or keyfob is not added to any partition, it will be automatically assigned to the first partition.
- One keyfob cannot manage several partitions, only one. The same situation is with a TM-key: only one partition can correspond to one key.
- One user can be assigned to several partitions. In this case, for arming or disarming, the user will have to specify the number of the partition that he/she is going to arm or disarm.
- The same zone can be added to several partitions, but remember that the zone is armed when all partitions into which it is included are armed.

## 5.6 Miscellaneous

On the “Miscellaneous” tab, it is possible to specify various parameters that determine the device operation.

### 5.6.1 Intervals



Intervals	
Interval for repeating alarms	5 min
Interval for repeating fire alarms	24 h
Interval for repeating troubles	15 min
Interval for switching to the main channel	5 min
Test transfer interval	1 h
Interval for event transfer control	7 min
Interval for control of communication with disarmed wireless devices	5 min
Interval for control of communication with armed wireless devices	5 min

Figure 50: “Miscellaneous” tab, “Intervals” section

#### Interval for repeating alarms

Use the “Interval for repeating alarms” parameter to specify the interval with which the device will generate *similar* alarms and transmit them to the receiver. The alarms are considered *similar* if they are originated in the same wired zone.

The value of the “Interval for repeating alarms” parameter is used for zones of all [types](#), with the exception of zones of the “Fire” and “Panic button without fixation” type. The alarm repetition interval for zones with the “Panic button without fixation” type is always 5 seconds, and the alarm repetition interval for zones of the “Fire” type is set by a separate parameter (see below).

Why is this parameter necessary? First of all, to reduce the number of events that will be transmitted to the repeater: one alarm event can be quite enough for the operator to start handling the site alarm. Repeated alarm on the same zone, as a rule, will not change anything. If the device detects an alarm in another zone, then such an alarm will be transmitted to the repeater and a countdown of its own alarm repetition interval will begin for this zone.

If the “Interval for repeating alarms” parameter is set to any numerical value, the device will generate events on a specific zone as follows:

- if an alarm is detected in the zone, an alarm event will be generated and the count of the specified interval will start;
- if an alarm reset is detected in the zone, a reset event will be generated, the count of the specified interval will be continued;
- in case of repeated alarm generation or reset in the zone, events will not be generated until the count of the specified interval is completed.

Numerical value means that only one alarm and one zone reset will be transmitted during the interval.

If the “Interval for repeating alarms” parameter is set to “Do not repeat” value, the device will generate events on a specific zone as follows:

- if an alarm is detected in the zone, an alarm event will be generated and the waiting of the zone alarm reset start;
- repeated events about the alarm in the zone *will not* be generated until an event about the alarm reset is generated on the zone;

- if an alarm reset is detected in the zone, a reset event will be generated, the alarm reset waiting in the zone will be terminated, the device will generate an alarm event in the zone again when it is detected.

The “Do not repeat” value means that a repeated zone alarm can only be transmitted after a reset of the previous alarm is transmitted on the zone.

The “Interval for repeating alarms” parameter does not relate to the alarms that are generated when the device tamper is triggered. Events about breaking or restoring a tamper are always generated after the tamper state changes.

### Interval for repeating fire alarms

The “Interval for repeating fire alarms” parameter specifies the interval with which the device will generate *similar* alarms on zones of the “Fire” type, and transmit them to the receiver. The alarms are considered *similar* if they are originated in the same wired zone.

The interval of fire alarm repetition is on the one hand designed to reduce the number of identical events that will be transmitted to the receiver, and on the other hand, to prevent a situation in which the personnel of the receiver will not pay attention to the fact that the device at the site is in the generalized “Fire” state: if [automatic reset of the generalized “Fire” state](#) is prohibited, then to reset it, it is necessary to type the code on the keypad.

The value of the “Interval for repeating fire alarms” parameter is applied as follows:

- if a fire alarm is detected, “Fire” event will be generated in the zone, the device will switch to the “Fire” state and the count of the specified interval will start;
- upon completion of the specified interval, the “Fire” event will be generated repeatedly on all zones along which it was generated during the interval counting. After that, the interval count will start again;
- if the generalized “Fire” state is reset, the interval count will be completed.

### Interval for repeating troubles

The “Interval for repeating troubles” parameter specifies the interval with which the device will generate *similar* troubles on zones, connected to the device. The alarms are considered *similar* if they are originated in the same wired zone. In this case, in contrast to the repetition intervals of repetition of security or fire alarms, the interval for repeating faults *stops*, if a recovery of the fault is detected and an event about it is generated.

For the wired zones, faults that are covered by the “Interval for repeating troubles” include the physical faults of the zone – a break and short circuit. These faults are only generated if one or two terminating resistors are connected to the zone.

If a type is specified for a wired zone, which implies arming, the event codes that are generated in case of faults/recoveries in such a zone will depend on the state (armed or disarmed) in which the zone was at the time of the fault detection:

- codes **E331** / **R331** will be generated if a break/recovery is detected for the zone, which is *disarmed*;
- codes **E141** / **R141** will be generated if a break/recovery is detected for the zone, which is *armed*;
- codes **E332** / **R332** will be generated if a short circuit/recovery is detected for the zone, which is *disarmed*;
- codes **E142** / **R142** will be generated if a short circuit/recovery is detected for the zone, which is *armed*;

Despite the fact that the codes **E141** and **E142** are considered alarms, the fault repetition intervals, rather than alarm repetition intervals, are used for the events with these codes.

The value of the “Interval for repeating troubles” parameter does not cover the following events about the faults that are generated by the device:

- discharge of the backup battery connected to the device. The event about the backup battery discharge (code **E302**) is formed once and repeated only when the device is turned on;
- malfunction of the backup battery connected to the device. The event about the backup battery failure (code **E309**) is formed every 12 hours, based on the results of each quality test of the backup battery;

### Interval for switching to the main channel

With the “Interval for switching to the main channel” parameter, it is possible to set the interval over which the device will attempt to initialize the connection to the repeater via the main IP channel. The main communication channel is the GPRS channel on SIM1.

For more details about the configuration of IP channels, as well as the rules for switching channels, see the description of the “[Security Center](#)” tab.

It shall be noted that it is possible to specify “Do not switch” as the value for the “Interval for switching to the main channel” parameter. In this case, the forced switching to the main communication channel will be disabled. This feature allows to use “equivalent” SIMs - if the device is connected via GPRS on SIM2, it will remain on this channel until the channel is operational.

### Test transfer interval

Use the “Test transfer interval” parameter to specify the interval with which the device will generate a test event and transfer it over the currently available communication channel. It is important to understand that this interval is always counted from the last event that was transmitted by the device. If there are no events for transfer at the expiration of the interval, a test event will be generated and transferred. If this parameter is set to “Do not transfer”, then the device will not generate test events (code **E602**).

### Interval for event transfer control

Use the “Interval for event transfer control” parameter to specify the interval during which the audit system is waiting for the event to be sent. The *audit system* is a program mechanism that controls the fact of the event transfer to the receiver.

If the “Interval for event transfer control” parameter is set to any numerical value, the device will work as follows:

- If the audit system registers the absence of the event transfer within the time interval specified by the parameter, then first the communication channel, which is currently used by the device, is switched;
- At the moment when the audit system has switched the communication channel, an event with the code **E754** is generated. The argument for the event with code E754 is the type of communication channel that stopped the event transfer (1 – GSM, 3 – radio). The argument value is transferred to the field assigned to the zone or user number.
- If the channel switching does not help, and events are still not transferred, then the audit system reboots the device after the expiry of the event transfer control interval.
- After the reboot, two events will be generated. The code of the first event is **R305**, this event registers the very fact of the device reboot. The second event code is **R754**, this event means that the reboot occurred by the audit system command.

The default value for this parameter is 7 minutes. If necessary, the value can be increased. If “Do not monitor” is specified for this parameter, the audit system will be disabled.

## 5.6.2 Siren

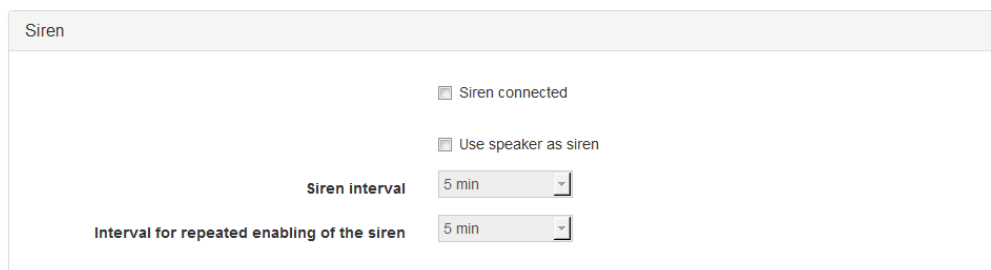


Figure 51: “Miscellaneous” tab, “Siren” section

**\*\* Siren connected\*\***

If the siren is connected to the same name output “Siren”, then it is necessary to check the appropriate box. This will turn on the monitoring of the communication line with the siren, which allows to detect break and short circuit of the line, both with the siren turned off and with the siren turned on. If any of these faults are detected, an event with the code **E321** - *Faulty siren* is generated, which is sent to the receiver.

In addition to the same name output, the siren can be connected to any of the seven open collectors, without the need to check the “Siren connected” box. It is important to note that the device does not monitor the line status if the siren is connected to an open collector.

The siren is connected to the open collector as follows:

- The “plus” cable of the siren can be connected to any plus output of the control panel, for example, to the output for powering keypad or zones.
- The “minus” siren cable shall be connected to one of seven open collectors: FIRE, DEFECT, LED\_G, LED\_Y, FIRE2, DEFECT2, DISABL.
- After connecting the siren, the output shall be configured using the automation rules. See more about the rules in the partition [Automatic controls section](#)

### Siren interval

The “Siren interval” parameter is responsible for duration of the siren sound, regardless of how it is connected. After the parameter interval expires, the siren will stop.

### Interval for repeated enabling of the sound

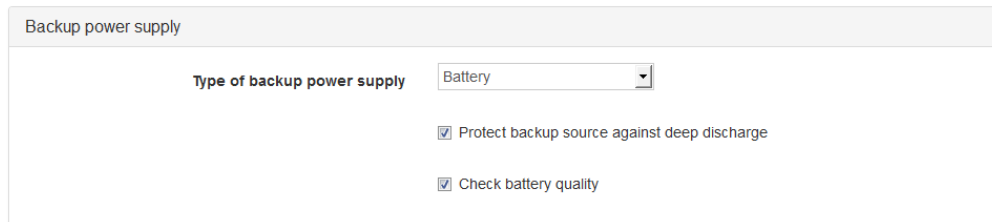
Use the “Interval for repeated enabling of the sound” parameter to specify the interval within which the siren will start to sound again, if the alarm reset has not occurred.

## 5.6.3 Backup Power Supply

### Type of backup power supply

Use the “Type of backup power supply” parameter to specify which backup source is connected to the device: Battery or UPS.

### If battery is connected



The screenshot shows a configuration window titled "Backup power supply". Inside, there is a label "Type of backup power supply" followed by a dropdown menu currently set to "Battery". Below this, there are two checked checkboxes: "Protect backup source against deep discharge" and "Check battery quality".

Figure 52: “Miscellaneous” tab, “Backup power supply” section

If the battery is selected as a backup power source, then it is possible to include two parameters:

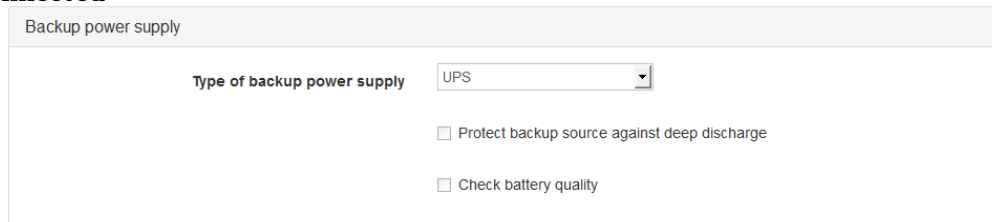
- *Protect backup source against deep discharge.*

If this parameter is selected, then when voltage reaches 8.5 V on the battery terminals, the device will turn off to prevent the battery from discharging to a critically low level at which its charge cannot be restored.

- *Check battery quality.*

To check the battery quality, the device periodically connects the load and monitors the voltage drop. If the voltage drop under the load exceeds 2 V, the event **E309 - Faulty battery** is generated.

### If UPS is connected



The screenshot shows the same "Backup power supply" configuration window, but the dropdown menu is now set to "UPS". The checkboxes for "Protect backup source against deep discharge" and "Check battery quality" are now unchecked.

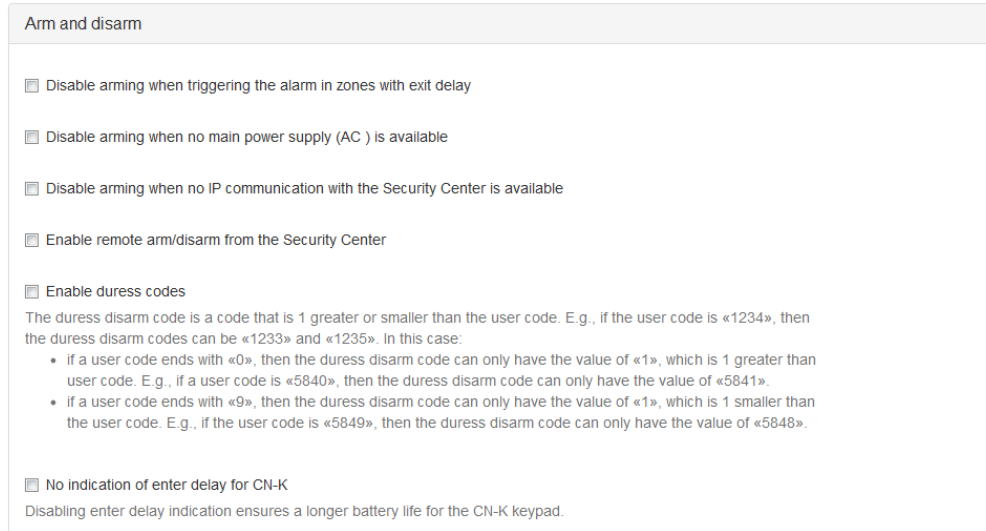
Figure 53: “Miscellaneous” tab, “Backup power supply” section, “UPS” is selected for “Type of backup power supply”

If the UPS is selected as a backup power source, enabling of the additional parameters (protection against deep discharge and battery quality control) is not available.



## 5.6.4 Arm and Disarm

In this section, it is possible to specify various parameters that will affect the process of arming or disarming.



The screenshot shows a configuration window titled "Arm and disarm". It contains several checkboxes and a text block. The checkboxes are: "Disable arming when triggering the alarm in zones with exit delay", "Disable arming when no main power supply (AC ) is available", "Disable arming when no IP communication with the Security Center is available", "Enable remote arm/disarm from the Security Center", "Enable duress codes", and "No indication of enter delay for CN-K". Below the "Enable duress codes" checkbox is a paragraph explaining that the duress disarm code is a code that is 1 greater or smaller than the user code, with examples. Below the "No indication of enter delay for CN-K" checkbox is a note that disabling this indication ensures a longer battery life for the CN-K keypad.

Arm and disarm

☐ Disable arming when triggering the alarm in zones with exit delay

☐ Disable arming when no main power supply (AC ) is available

☐ Disable arming when no IP communication with the Security Center is available

☐ Enable remote arm/disarm from the Security Center

☐ Enable duress codes

The duress disarm code is a code that is 1 greater or smaller than the user code. E.g., if the user code is «1234», then the duress disarm codes can be «1233» and «1235». In this case:

- If a user code ends with «0», then the duress disarm code can only have the value of «1», which is 1 greater than user code. E.g., if a user code is «5840», then the duress disarm code can only have the value of «5841».
- If a user code ends with «9», then the duress disarm code can only have the value of «1», which is 1 smaller than the user code. E.g., if the user code is «5849», then the duress disarm code can only have the value of «5848».

☐ No indication of enter delay for CN-K

Disabling enter delay indication ensures a longer battery life for the CN-K keypad.

Figure 54: “Miscellaneous” tab, “Arm and disarm” section

### Disable arming when triggering the alarm in zones with exit delay

By default, the alarm in zones with exit delay is ignored at the time of arming. This is done so that the user can arm the site and close the entrance door behind him/her without hurry. But, if you want to be sure that all alarm zones are normal at the time of arming, it is possible to enable alarm monitoring in zones with exit delay. To do this, check the *Disable arming when triggering the alarm in zones with exit delay* box.

### Disable arming when no main power supply (AC) is available

If this parameter is set, the device cannot be armed if it is running on a backup power supply and the main one is not available.

### Disable arming when no IP communication with the Security Center is available

If this parameter is set, the device cannot be armed if there is no GPRS communication.

### Enable remote arm/disarm from the Security Center

This parameter allows to remotely control the protection state from the mobile application and the repeater.

### Enable duress codes

The code of forced disarming is a code that differs from the user code by one unit plus or minus. For example, if the user code is “1234”, then the forced disarming codes will be “1233” and “1235”. At the same time:

- if the user code ends with “0”, then the forced disarming code will be only one – one more. For example, if the user code is “5840”, then the forced disarming code will be only “5841”.
- if the user code ends with “9”, then the forced disarming code will be only one – one less. For example, if the user code is “5849”, then the forced disarming code will be only “5848”.

## 5.6.5 Control and Indication

Management and indication

Light alarm is set on the Automatic Controls tab

☐ Rif-KTM (C.Nord) keypad connected

☐ User codes containing 6 numbers

Code to disable fire siren

☒ Enable using keypad as panic button  
The panic button is activated by the simultaneous long pressing of \* and #

☒ Enable continuous poll mode for the 1-Wire interface  
To connect wired temperature sensors or EW-12 extender, you must enable continuous poll mode for the 1-Wire interface.  
Continuous poll mode for the 1-Wire interface is not compatible with some proximity card-readers and Rif-KTM (C.Nord).

Figure 55: “Miscellaneous” tab, “Management and indication” section

### Light alarm is set up on the “Automatic controls” tab

In order for the user to visually monitor the alarm status on the site, a 12 V light alarm can be connected to the device. This alarm is set up on the [Automatic controls](#) tab.

### User codes containing 6 numbers

To use six-digit codes for arming and disarming, first it is necessary to set this parameter, and then create users. If the device already has users with a four-digit code, first it is necessary to delete them and set the parameter for using six-digit codes.

### Enable continuous poll mode for the 1-Wire interface

The continuous poll mode of 1-Wire shall be switched on if the wired temperature sensors is connected to the device. This mode is incompatible with some proximity card readers and the Rif-KTM (C.Nord) keypad.

## 5.6.6 Configuration Protection

This section is used to configure parameters to protect against unauthorized access and malicious modification of device settings.

Configuration protection

☒ Enable restore of factory defaults

Pause before reset

[Change panel access password...](#)

☐ Enable Theft protection function

Figure 56: “Miscellaneous” tab, “Configuration protection” section

### Password for access to the device

Mandatory password authentication during connection to the device via USB is another way to ensure security. By default, the password for connecting to the device via USB is **0000**. To increase security, it is necessary to change the default access password to a new one. The password length can be from 4 to 16 digits. It is recommended to set a password consisting of the maximum number of digits allowed.

Figure 57: “Miscellaneous” tab, “Configuration protection” section, dialog for changing password for accessing the device.

If the password is lost and the remote connection to the device is not possible, it is possible to restore access to the device only if all its parameters are reset to the factory ones. This will delete all device settings, including zones, users, partitions, etc., and the password for connecting to the device via USB will be default.

### Enable restore of factory defaults

The reset function can be enabled or disabled for a specific device. If you allow resetting the parameters, it is possible to set a **pause before reset**. By default, this parameter is set to 30 seconds, however, it is possible to select 5 minutes, 30 minutes, 12 hours or 24 hours. The configuration reset is possible only in case of USB connection.

If the reset function is enabled, the password entry window will contain the “Reset configuration” button.

Figure 58: “Miscellaneous” tab, “Configuration protection” section, dialog for resetting the device configuration.

When the “Reset configuration” button is clicked, the device generates an event with the code **E752** and starts counting the set pause.

It is recommended to set the maximum values of the *pause before reset* parameter, since such a delay provides additional protection. If the device is reset by an intruder, the private security company manages to react to unauthorized access to the device.

### Enable Theft protection function

If this function is enabled and the changes are stored in the device, then the values of the addresses for GPRS connection can no longer be changed for this device.

Before saving the configuration, the device issues a warning:

The screenshot shows a dialog box titled "Theft protection". Inside, it states: "The theft protection function is enabled in the configuration to be recorded on the panel." followed by "After the configuration is recorded, you won't be able to modify values for the following parameters:". A bulleted list follows: "• addresses for connection to the Security Center based onGPRS;" and "• station format for radio transfer." Below the list, it asks "Are you sure you want to record the configuration on the panel?". At the bottom right, there are two buttons: a green "Record" button and a white "Cancel" button with a grey border.

**Theft protection**

The theft protection function is enabled in the configuration to be recorded on the panel.

After the configuration is recorded, you won't be able to modify values for the following parameters:

- addresses for connection to the Security Center based onGPRS;
- station format for radio transfer.

Are you sure you want to record the configuration on the panel?

**Record** Cancel

*Figure 59: “Miscellaneous” tab, “Configuration protection” section, warning about enabling “Theft protection”*

The “Theft protection” function can be enabled both for USB connection and for remote programming. It is possible to disable the “Theft protection” function only by contacting the **company technical support** with an official request to “C.Nord”.

## 5.7 Security Center

Settings that the device Security Center use when transmitting events via GSM channels can be specified on the “Security Center” tab.

### 5.7.1 Device Identification

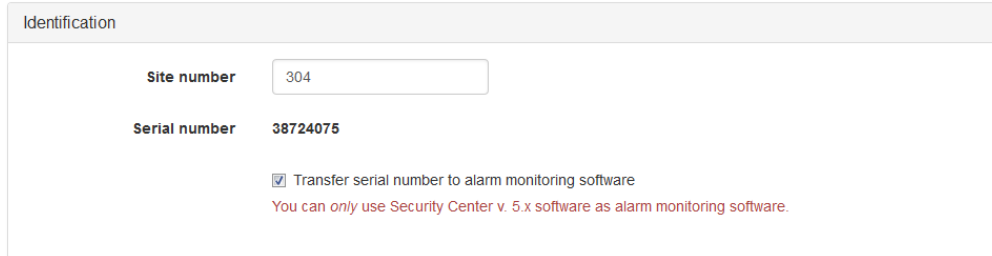


Figure 60: “Security Center” tab, “Identification” section

In the “Identification” section it is possible to specify the number of the site that will be used when transmitting events from the device.

Since the transmission of events from the device to the Security Center software is performed in a protocol that is the information equivalent of the Ademco ContactID protocol, each event, if possible, contains information about the number of the partition in which it occurred, as well as the zone number, which caused the formation of the event, or the number of the user who performed the partition arming or disarming. Thus, when transmitting over GSM, a single site number is sufficient to transmit any event from the device without loss of informativity.

In the “Identification” section, the “Device identifier” field displays the unique eight-digit serial number that the device receives at the production stage. This serial number can be transmitted to the receiver and serve as an alternative to the site number when identifying the device. The “Transmit device identifier to remote program” parameter is used to enable this feature. The possibility to use the serial number of the device instead of the site number is not implemented in the Security Center software: if the serial number is transmitted to the remote program, the serial number will simply be displayed in the site card on the “Equipment” tab.

If the Security Center version 4 is used as the remote software, then it is impossible to include the transmission of the serial number to the remote program: the device will not be able to connect to the Security Center.

To ensure that the events from the device are properly handled by the Security Center software, the following conditions shall be met:

- the site number specified when setting up the device shall match the site number created for the device in the Security Center software;
- in the “Site Manager” module, the value “C.Nord GSM (CML)” shall be specified on the “Equipment” tab for this site;
- before the first connection of the device to the Security Center software, make sure that the value in the “ID” field on the “Equipment” tab is not set.

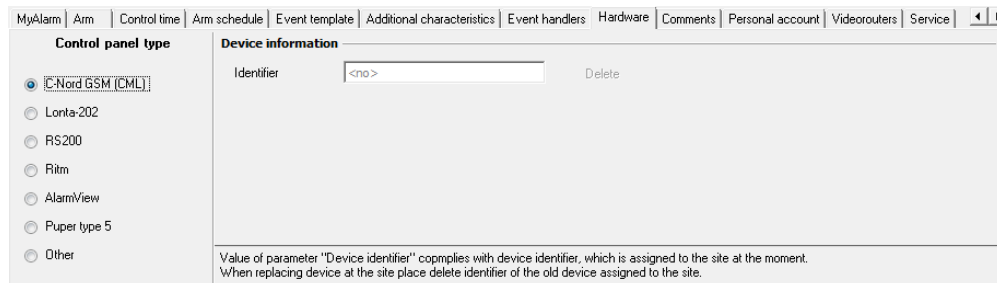
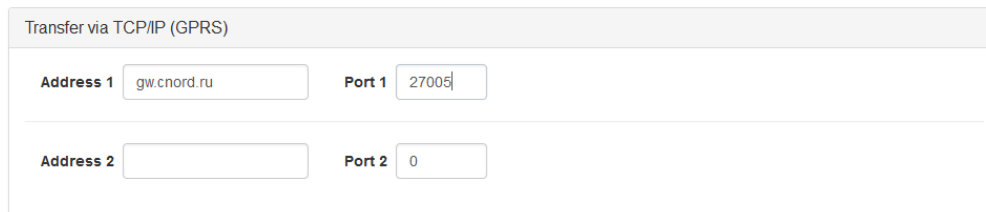


Figure 61: “Site Manager” module, “Equipment” tab

## 5.7.2 GPRS Transmission Parameters



Transfer via TCP/IP (GPRS)	
Address 1	gw.cnord.ru
Port 1	27005
Address 2	
Port 2	0

Figure 62: “Security Center” tab, “Transfer via TCP/IP (GPRS)” section

In the “Transfer via TCP/IP (GPRS)” section it is possible to specify up to two pairs of “address: port”, which will be used by the device when connecting to the receiver via GSM/GPRS.

It is possible to specify both the IP address and the DNS name for the “Address 1” and “Address 2” fields.

When initializing a GPRS connection, the device first tries to connect to the server with the parameters “Address 1:Port 1”. If the connection cannot be established, an attempt will be made to connect to the server with the parameters “Address 2:Port 2”. In this case, both pairs “address:port” are perceived by the device as equivalent: the differences between them are only in what pair will be used first to initialize the connection. If the device is connected to the receiver using the “Address 2:Port 2” pair, then this connection will not be considered a connection on the backup channel and will be closed only if communication with the receiver using this connection is lost. Both pairs “address:port” are valid for both SIMs installed in the device: irrespective of which SIM is currently active, the device will first attempt to connect to the receiver with the parameters “Address 1:Port 1”, and only if this attempt fails - it will try to connect with the parameters “Address 2:Port 2”. If there is only one TCP/IP address on the receiver, when configuring the device, the values for the parameters “Address 2:Port 2” shall be left blank.

The GSM/GPRS channel on SIM1 is considered the *main* for the device.

### Reception of Events in Security Center

To receive events from the device via TCP/IP (GSM/GPRS) in the Security Center software it is necessary to use the “C.Nord GSM (CML)” event source. This source of events can be added or it can be changed in the “Event manager” module.

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

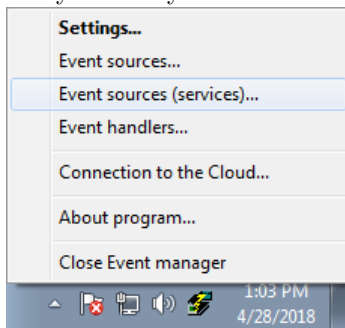


Figure 63: Context menu of “Event manager” module

To add the event source “C.Nord GSM (CML)” to the service of event sources, click the “Add” button and select the item corresponding to the source in the appeared menu.

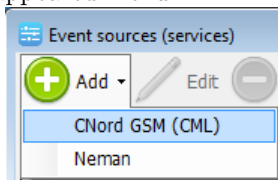


Figure 64: Menu of settings window of event source service

Figure 65: Event settings window of “C.Nord GSM (CML)”

See more information about the parameters of the source of events for “C.Nord GSM (CML)” in the documentation for the Security Center software.

### IP Address or DNS Name?

As the server address, it is recommended to specify a DNS name, not an IP address, and here’s the reason. As a rule, dedicated IP-address belongs to a specific carrier, which provides access to the Internet and cannot be transferred to a connection that is provided by *another* carrier. As for the DNS name, it belongs to the organization that registered it, for example - to a security company. Besides, the compliance of the DNS name and IP address is also specified by the security company.

What happens if, for some reason, it is necessary to cancel the contract with the carrier, which gives the security company access to the Internet? If you specify a DNS name for the connection to the receiver, it will be enough to change the entry that specifies the DNS name and IP address. If you specify an IP address, you will have to visit each site to change the address value.

Proceeding from the above, it is strongly *recommended* to use the DNS name, not the IP address.

### Reception of Events in Security Center

To receive events from the device via the CSD channel in the Security Center software it is necessary to use “GSM Events Source”. This source of events can be added or it can be changed in the “Event manager” module.

Any GSM modem, which command system is compatible with the Siemens MC35 modem can be used as an equipment for receiving events via the CSD channel.

### 5.7.3 Transmission Parameters via GSM voice channel

Figure 66: “Security Center” tab, “Transfer via GSM voice channel”

In the “Transfer via GSM voice channel” section, it is possible to specify the phone numbers that will be used for dialing to the receiver when transmitting events via the GSM voice channel. The transmission via the voice channel is performed with the help of analog DTMF signals, and Ademco Contact ID is used as an information protocol. Telephone numbers for voice channel transmission are set separately for each SIM, since a voice call within the

communication channel network can be cheaper.

When transmitting via the voice channel, the device first dials the first number specified for the currently active SIM, and if the transmission of the event fails, then it dials the second one. If there is only one number for voice dialing on the receiver, then the second phone number shall be left blank.

The GSM voice channel is considered active if at least one phone number is specified. If the device does not have to use the voice channel to transmit events, then both telephone numbers shall be empty.

### Reception of Events in Security Center

To receive events from the device via the GSM voice channel, it is necessary to use the dedicated receiver equipment. As an example of such equipment, we can mention the processor of the central station “Sentinel” manufactured by Pima Electronics or processors of the central station “SG System III”/“SG System IV” manufactured by DSC.

#### 5.7.4 SMS Transmission Parameters



The image shows a software interface titled "Transfer via SMS". Below the title, there are two input fields. The first field is labeled "Number for 1 SIM" and the second field is labeled "Number for 2 SIM". Both fields are empty text boxes.

Figure 67: “Security Center” tab, “Transfer via SMS” section

In the “Transfer via SMS” section it is possible to specify the phone numbers that will be used to send events to the receiver via the SMS channel.

When sending via SMS, the device uses a protocol that allows sending up to 5 events in one SMS message. This protocol is intended solely for transmitting information to the receiver *and cannot be used* to inform users of events on the site.

The phone number for SMS transmission is set separately for each SIM, since sending SMS within the carrier’s network can be cheaper.

SMS channel is considered active if a phone number is specified for it. If the device does not have to use the SMS channel to transmit events, the phone number shall be empty.

### Reception of Events in Security Center

To receive events from the device via the SMS channel in the Security Center software it is necessary to use “GSM Events Source”. This source of events can be added or it can be changed in the “Event manager” module.

Any GSM modem, which command system is compatible with the Siemens MC35 modem can be used as an equipment for receiving events via the SMS channel.

#### 5.7.5 Communication Channel Switching

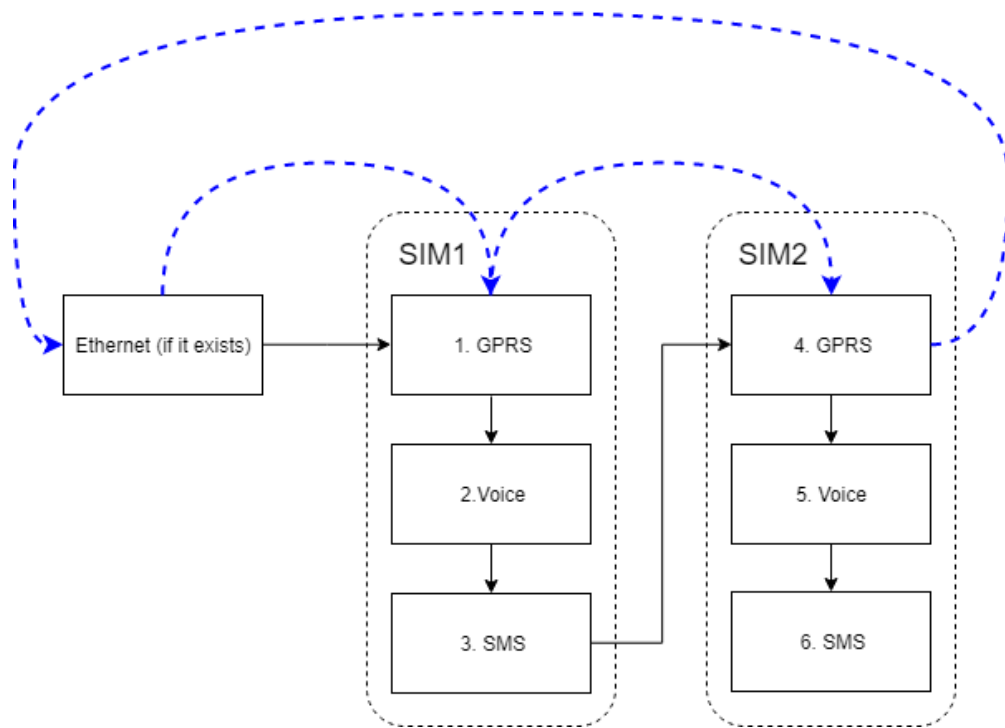
To determine the next communication channel, if the current IP channel does not work, the following rule applies:

- if there are no events for transmission, then switching to another IP channel is performed. For example, if GPRS does not work on SIM1, then the device switches to GPRS on SIM2 and vice versa;
- if there are events, then an attempt is made to transmit them via the backup channel on the SIM that is currently active. After the completion of sending events, attempts to connect via IP channels are renewed.

If the transmission via the backup channels to SIM1 failed, then the device will switch to SIM2 and will select channels there.

If there are no events to transmit, the device will search through the IP channels until the connection is made, or until the event for transmission appears. It is also important that the device can distinguish the situation “GPRS does not work” from the situation “no connection to Security Center”. In the first case, switching to another IP channel is performed, in the second case, attempts to connect to the console inside one GPRS session continue.





*Figure 68: Diagram of communication channel switching*

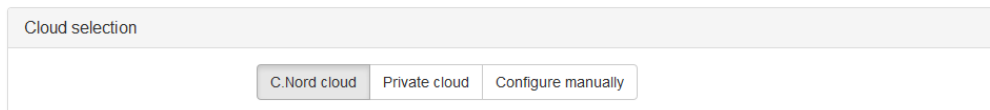
The order of switching IP channels in the absence of events is shown in the figure with blue dashed lines. Black solid lines show the scheme for switching all configured channels when there are events for transmission.

## 5.8 Cloud

Connecting the device to the “Cloud” provides the service functions of the device and allows to interact with it remotely with the help of the “MyAlarm” mobile application and the “Engineering panel” service. A detailed description of the technology can be found in [Remote Access to Device](#) section.

On the “Cloud” tab it is possible to choose to which “Cloud” the device shall be connected.

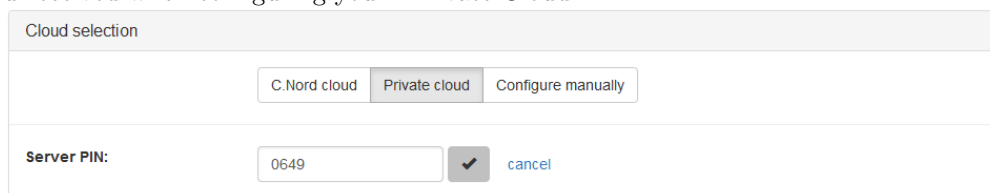
If you use the public “C.Nord Cloud” for work, then everything is simple - you need to click the button with the same name:



The screenshot shows a web interface titled "Cloud selection". At the bottom, there are three buttons: "C.Nord cloud", "Private cloud", and "Configure manually". The "C.Nord cloud" button is highlighted with a dark border, indicating it is the selected option.

*Figure 69: "Cloud" tab, public "Cloud" is selected.*

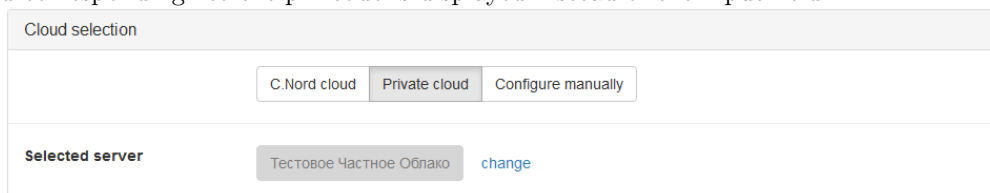
If the device shall work with the “Private Cloud”, then click the “Private Cloud” button, and then enter the pin code which you received when configuring your “Private Cloud”:



The screenshot shows the "Cloud selection" interface. The "Private cloud" button is now selected. Below the buttons, there is a section labeled "Server PIN:". It contains an input field with the value "0649", a checkmark icon, and a "cancel" link.

*Figure 70: "Cloud" tab, "Private Cloud" is selected.*

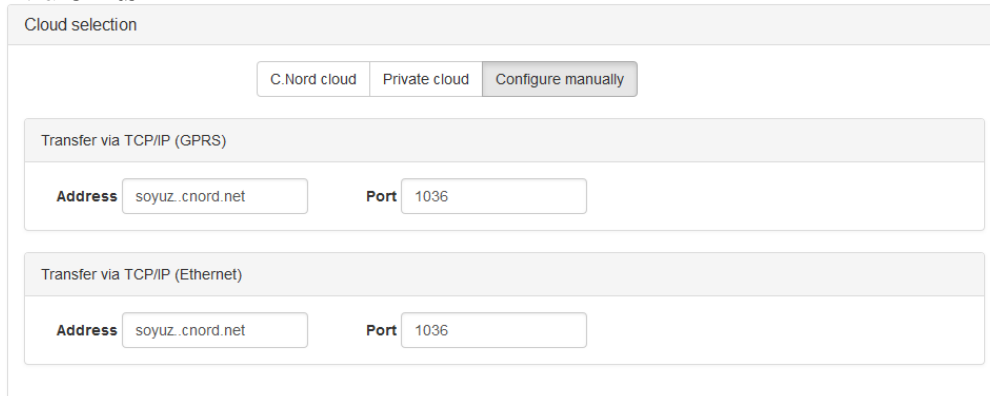
If the “Private Cloud” server pin is entered correctly, when you click the button with a “tick” the name of the “Private Cloud corresponding” to the pin code is displayed instead of the input field:



The screenshot shows the "Cloud selection" interface. The "Private cloud" button remains selected. Below it, the "Selected server" section now displays "Тестовое Частное Облако" instead of the input field. A "change" link is visible next to the server name.

*Figure 71: "Cloud" tab, name of the "Private Cloud" is displayed.*

If for some reason you need to configure the settings for connecting to the Private Cloud manually, then this option is also available: you need to click the “Configure manually” button and specify the addresses and ports to connect to the “Cloud” via GPRS:



The screenshot shows the "Cloud selection" interface. The "Configure manually" button is selected. Below the buttons, there are two sections for manual connection settings. The first section, "Transfer via TCP/IP (GPRS)", has an "Address" field with "soyuz.cnord.net" and a "Port" field with "1036". The second section, "Transfer via TCP/IP (Ethernet)", also has an "Address" field with "soyuz.cnord.net" and a "Port" field with "1036".

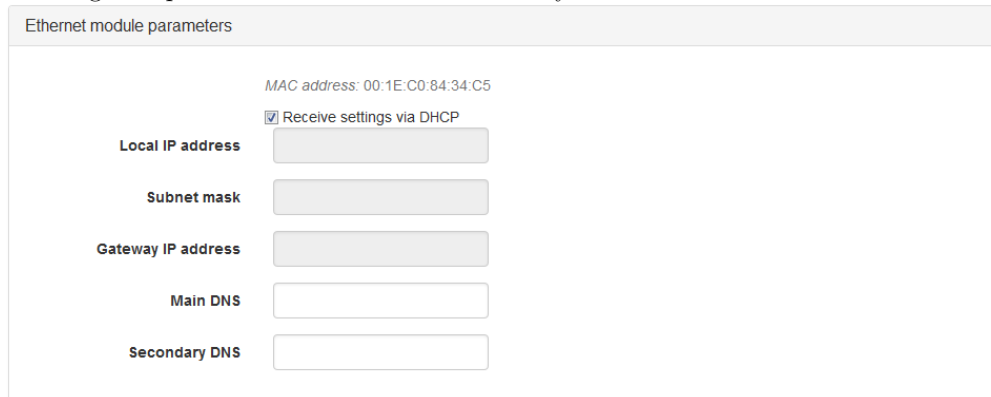
*Figure 72: "Cloud" tab, settings for manual connection.*

## 5.9 Ethernet

The tab is used to display and change the connection settings over the Ethernet network.

The “Ethernet” tab is displayed in the configurator only if the “Ethernet Adapter” is connected to the device.

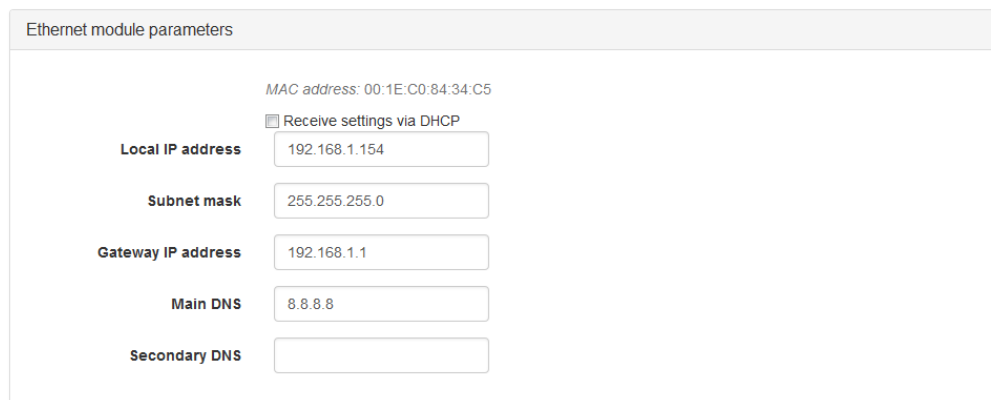
The tab displays the MAC address that is used by the Ethernet Adapter. This information can be useful if the settings for connecting to a public network are set individually for each device.



The screenshot shows the 'Ethernet module parameters' configuration window. At the top, the MAC address is displayed as '00:1E:C0:84:34:C5'. Below this, the checkbox 'Receive settings via DHCP' is checked. The fields for 'Local IP address', 'Subnet mask', and 'Gateway IP address' are empty. The 'Main DNS' and 'Secondary DNS' fields are also empty.

Figure 73: “Ethernet” tab, reception of settings from the DHCP server is enabled.

Besides, if the network to which the device is connected does not have a DHCP server that automatically configures the network connection settings, you can manually set these parameters by explicitly specifying the IP address that the device shall use, the subnet mask to which it belongs, IP address of the gateway to be used to access the public network, as well as the IP addresses of the DNS servers.



The screenshot shows the 'Ethernet module parameters' configuration window with manual settings. The MAC address remains '00:1E:C0:84:34:C5'. The 'Receive settings via DHCP' checkbox is now unchecked. The 'Local IP address' field contains '192.168.1.154', 'Subnet mask' contains '255.255.255.0', and 'Gateway IP address' contains '192.168.1.1'. The 'Main DNS' field contains '8.8.8.8', and the 'Secondary DNS' field is empty.

Figure 74: “Ethernet” tab, manual network setting.

## 5.10 GSM operators

Using the “GSM Operators” tab, the device records information necessary for correct operation of sim cards in the GSM network.

1 operator	2 operator
<b>Name</b> <input type="text" value="MEGAFON"/>	<b>Name</b> <input type="text" value="MTS"/>
<b>Network number (PLMN)</b> <input type="text" value="25002"/>	<b>Network number (PLMN)</b> <input type="text" value="25001"/>
<b>Access point</b> <input type="text" value="internet"/>	<b>Access point</b> <input type="text" value="internet.mts.ru"/>
<b>Username</b> <input type="text"/>	<b>Username</b> <input type="text" value="mts"/>
<b>Password</b> <input type="text"/>	<b>Password</b> <input type="text" value="mts"/>

3 operator	4 operator
<b>Name</b> <input type="text" value="TELE2"/>	<b>Name</b> <input type="text" value="BEELINE"/>
<b>Network number (PLMN)</b> <input type="text" value="25020"/>	<b>Network number (PLMN)</b> <input type="text" value="25099"/>
<b>Access point</b> <input type="text" value="internet.tele2.ru"/>	<b>Access point</b> <input type="text" value="internet.beeline.ru"/>
<b>Username</b> <input type="text"/>	<b>Username</b> <input type="text" value="beeline"/>
<b>Password</b> <input type="text"/>	<b>Password</b> <input type="text" value="beeline"/>

Figure 75: “GSM Operators” tab, operator settings.

By default, the configurator lists the most common carriers. Before starting the device via GSM it is important to make sure that the parameters of the SIM card used in the device are indicated. If there are no parameters for the selected carrier in the listed blocks, it is necessary to specify them manually, by filling in the fields *Name*, *PLMN*, *Access Point*, *Username*, *Password*. All these parameters can be requested by the device from the SIM card during registration in the network.

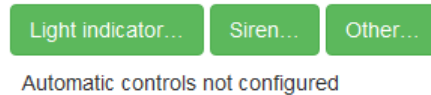
## 5.11 Automatic Controls

“Automatic controls” mechanism is designed to program the behavior of the device depending on certain conditions. Any events formed by the device or time can act as the conditions. Arming or disarming and actions with open collectors are actions that the device can perform.

Automation can be used to solve the following tasks on sites:

- scheduled arming and disarming;
- arming and disarming of several partitions at the same time;
- display of the partition status on the light indicator;
- activation of sound annunciators connected to the device open collectors;
- control of external devices connected to the device open collectors.

When switching to the “Automatic controls” tab, the buttons at the top of the window allow to configure the rules.



*Figure 76: Buttons for creating rules, "Automatic controls" tab*

The device already has the logic of working with light and sound annunciators. To set up open collectors to which the annunciators are connected, it is necessary to use the buttons “Light indicator...” or “Siren...”, depending on the type of the annunciator.

When creating rules, it is important to remember the following:

- If the collector is used to connect other devices (for example, fire indication device), it cannot be used anywhere else, including remote control, which will appear a little later.
- If the collector is already used for roles (Light indicator, Siren), then it cannot be used anywhere else.
- It is possible to create 8 rules with the role of “Light indicator” or “Siren”. And these rules do not depend on the number of standard rules of automation.

### 5.11.1 Light Indicator

#### Light indicator connection

Connect the light indicator to the device as follows:

- Connect the siren “plus” cable to any plus output of the control panel, for example, to the output for powering the keypad or zones.
- Connect the siren “minus” cable to one of seven open collectors: FIRE, DEFECT, LED\_G, LED\_Y, FIRE2, DEFECT2, DISABL.

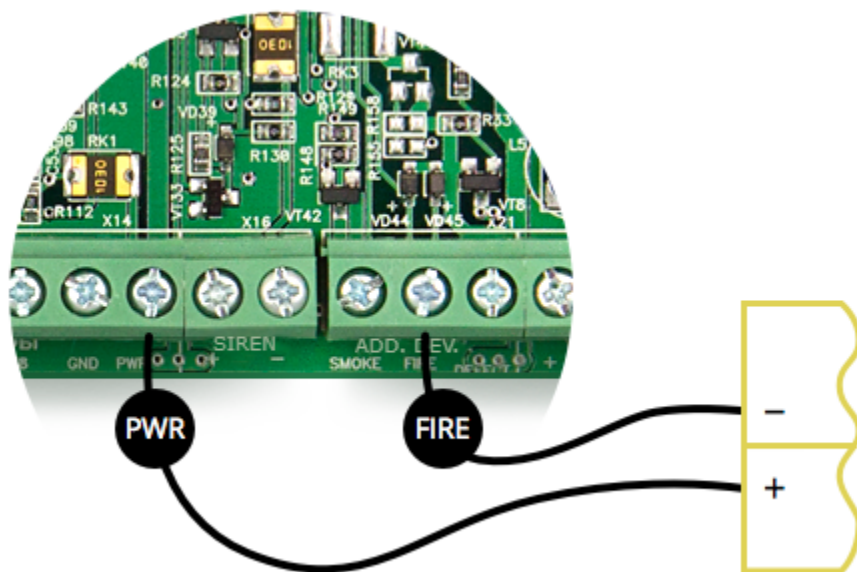


Figure 77: Light indicator connection to the device

Any light indicator with a voltage of 12 V can be connected to the devices. The maximum current shall not exceed 250 mA.

### Rule setting

For a light indicator that indicates the state of site or partition, it is necessary to set up a rule with the role of “Light indicator”. To create a rule in the “Automatic controls” tab, click the “Light indicator” button and select the output to which the annunciator is connected. In the event that several partitions are configured on the device, then when creating the rule, it is possible to specify the partition for which the light indicator will display the state.

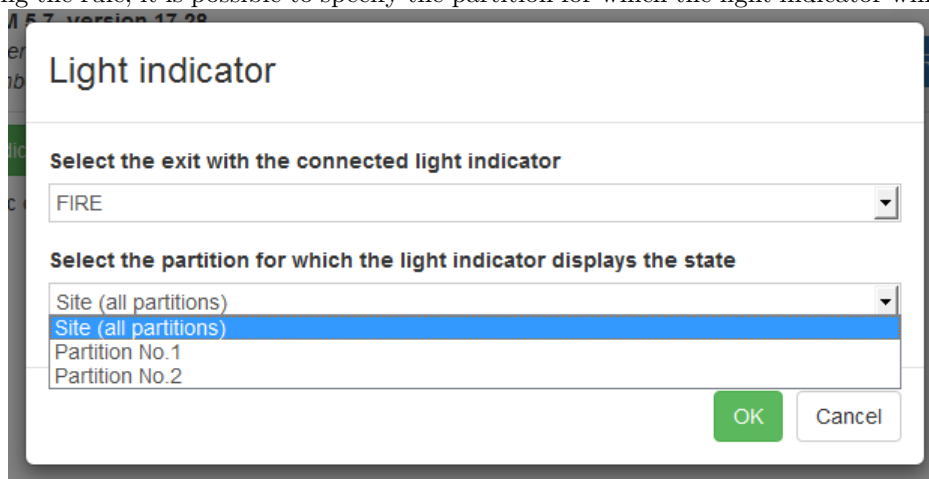


Figure 78: Creating “Light indicator” rule

### Annunciator operation description

If the “Light indicator” rule is configured to display the partition state:

- The light indicator is continuously lit when the partition is armed;
- The light indicator is not lit if the partition is disarmed;
- The light indicator flashes if the partition is in an alarm;
- The light indicator flashes with double flashes during the exit delay.

If the “Light indicator” rule is configured to display the site state:

- The light indicator is continuously lit if all partitions are armed;
- The light indicator does not light if at least one of the partitions is disarmed;
- The light indicator flashes if there is at least one partition in the alarm;
- The light indicator flashes with double flashes during the exit delay.

### 5.11.2 Siren

#### Siren connection

The siren is connected to the open collector as follows:

- The “plus” cable of the siren can be connected to any plus output of the control panel, for example, to the output for powering keypad or zones.
- Connect the siren “minus” cable to one of seven open collectors: FIRE, DEFECT, LED\_G, LED\_Y, FIRE2, DEFECT2, DISABL.

Any light indicator with a voltage of 12 V can be connected to the devices. The maximum current shall not exceed 250 mA.

#### Rule setting

For siren it is necessary to set up a rule with the role of “Siren”. To create a rule in the “Automatic controls” tab, click the “Siren” button and select the output to which the annunciator is connected.

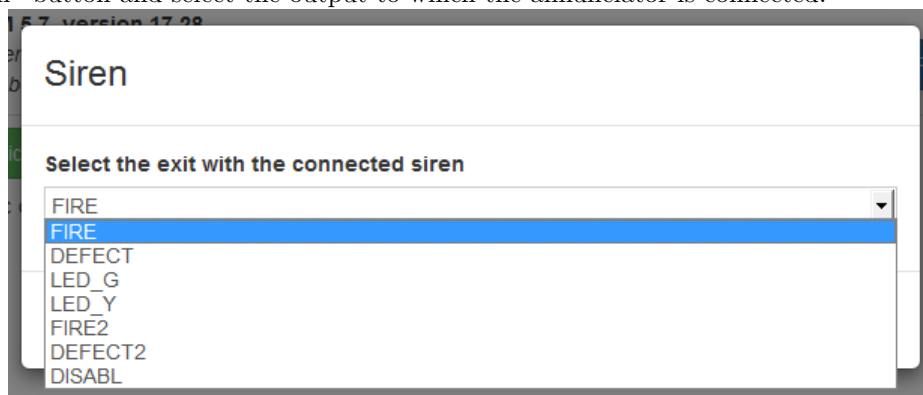


Figure 79: Creating “Siren” rule

The siren connected to the open collector differs from the siren connected to the same name “Siren” output: in the first case the device does not control the condition of this line. To configure the siren sound settings, go to the [Siren](#) section of the “Miscellaneous” tab.

### 5.11.3 Miscellaneous

In addition to the predefined rules, up to 16 other rules can be created in the device. When the conditions specified in the rule are met, the device can perform arming or disarming of one or all partitions, close or open the digital output, and also start the periodic closing and opening of the digital output at a predetermined interval.

**Add action**

Select action

Action: arm

Partition: any partition

Select condition

Condition: event

Event code: R401

Partition: any partition

Z/U:

Enter a value from 1 to 999, or leave blank if the zone or user number is irrelevant

OK Cancel

Figure 80: Window for creating rule

## Rule setting

Let's consider setting up rules for a specific example.

### Task

Configure arming of partition No. 1 on a schedule at 19.30 on Tuesdays and Wednesdays.

### Solution

To solve the task, it is necessary to create an action that arms the partition on a schedule.

1. On the "Automatic controls" tab, click the "Miscellaneous" button.
2. In the "Action" field, from the drop-down list, select the "Arming".
3. In the "Partition" field, select "1".
4. In the "Condition" field, select "on schedule".
5. Use the drop-down menus in the "Time" field to set the value to "19:30".
6. In the "Day" field, select "specify". In the days of the week that appear with this list, check "Tu" and "Wd" boxes. Uncheck other boxes.



Figure 81: Window for creating rule

- Click “OK” to save the rule. The rules will take effect after recording the settings in the device.

Light indicator...	Siren...	Other...		
<b>Arm partition 1</b> based on Tu, Wd, 07:30			Change...	
<b>The light indicator is connected to the FIRE exit</b> Displays the state for the entire site			Change...	
<b>Siren connected to LED_Y exit</b>			Change...	

Figure 82: All created rules

In this example, automatic arming is considered, but it is possible to specify the site disarming as an action. In this case, the site will be disarmed according on a specified schedule. It is also possible to configure the automatic closing and/or opening of the discrete outputs of the device.

It is possible to configure arming of all site partitions using the “All partitions” value of the “Partition” field. To configure the arming of several specific partitions, for each of them it is necessary to configure the arming separately. Arming can be set for certain days of the week, as in the example considered; for each day; only for weekdays (from Monday to Friday); and also for weekends only.

Automatic arming, like any other action, can be performed not only on a schedule, but also for an event. In this case, it is necessary to know the event code that will be used in the rule.

## 5.12 Event History

The tab is intended for displaying events that are stored in the device non-volatile memory.

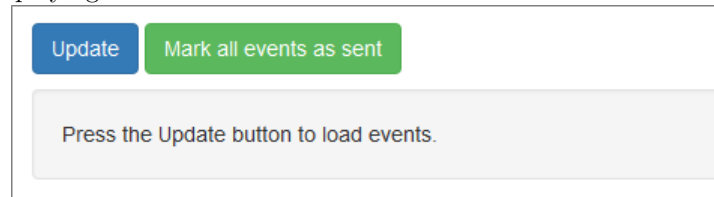


Figure 83: “Event history” tab

To load events from the device to the configurator, click the “Update” button.

The list of events that is displayed on the “Event history” tab is not automatically updated: to see what changes have occurred in the history of events over time, click the “Update” button again.

Update

Mark all events as sent

Save to file...

Time	Code	Description	Site	Partition	Z / U	Sent
04.05.2018 10:22:19	E627	Programming mode (USB) on	3	0	0	GPRS on SIM1 04.05.2018 14:34:10
04.05.2018 10:07:19	E137	Device case open	3	0	0	GPRS on SIM1 04.05.2018 14:34:09
04.05.2018 09:52:19	E301	Disable AC	3	0	0	GPRS on SIM1 04.05.2018 14:34:09

Figure 84: “Event history” tab, event list

The volume of device non-volatile memory allows to save at least 10,000 events. But on the “Event history” tab, no more than 200 recent events are displayed. Use the *Save to file..* button to download the full list of events to a file with the extension *.csv*.

The following information is displayed for each event history:

- time when the event was generated by the device and stored in non-volatile memory;
- code of the event, which is transmitted to the receiver;
- text description of the event;
- the number of the site for which the event was generated;
- partition number;
- zone or user number;
- information about the current state of the event (column “Sent”):
  - if the event is waiting for transmission, a “dash” is displayed;
  - if the event is sent to the receiver, information about the transmission channel is displayed, as well as the time when the confirmation of the event reception;
  - if event sending was canceled from the configurator, information about this event is displayed, as well as the time when the transmission was cancelled. To cancel the transmission of all waiting events to the receiver, click the “Mark all events as sent” button.

When an event is created, it receives a unique sequence number. The order of event numbering *does not depend* on the time that is set on the device: events created earlier have a smaller number, events created later have larger numbers. On the “Event history” tab, events are displayed in the reverse order: events created later are displayed above, and events created earlier are lower in the list.

## 5.13 State Panel

When performing work on the installation of a site, the engineer usually needs to check that the placement and connection of the sensors is correct and there are no malfunctions in their operation.

In the configurator, the “State panel” tab displays the current information on the status of wired zones and the status of communication channels.

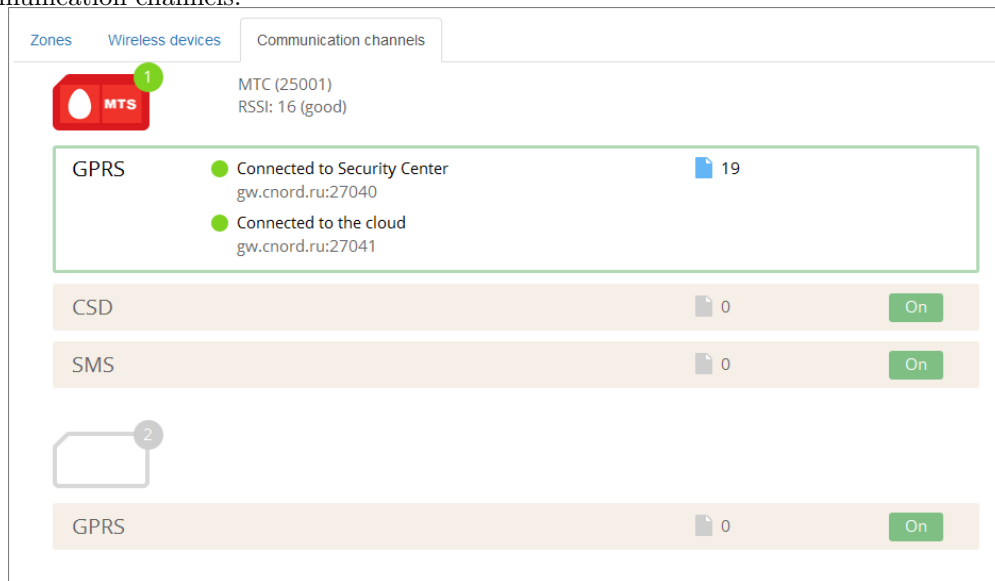


Figure 85: “State panel” tab, communication channels

### 5.13.1 Communication Channels

When installing and maintaining the device, it is important to know the current information about the status of communication channels. Use the “State panel” tab to see on which SIM-card and on what communication channel the device is currently operating.

For each communication channel available in the device settings, its current status is displayed: active/not active, whether there is connection to the Security Center and Cloud, what errors occurred when the channel was initialized, connected to the receiver or transmitted events.

Click the “On” button to force a transition to the communication channel that you want to check. In order for the engineer to make sure that the channel really works, pressing the “On” button generates a test event with the code **E602**, which will be transmitted over the channel if it is successfully initialized.

To the left of the “On” button, the number of events, that have been transferred to the receiver since the last time the channel was active, is displayed.

### 5.13.2 Wired Zones

For each wired zone that is enabled on the [Zones](#) tab, its physical state is displayed. For example, if the zone is currently disturbed (in alarm), then the icon with the number corresponding to the zone number will be red. If there is a fault on the zone, this will also be indicated in the state panel. If the zone is disabled in the device settings, then information on it will not be displayed.

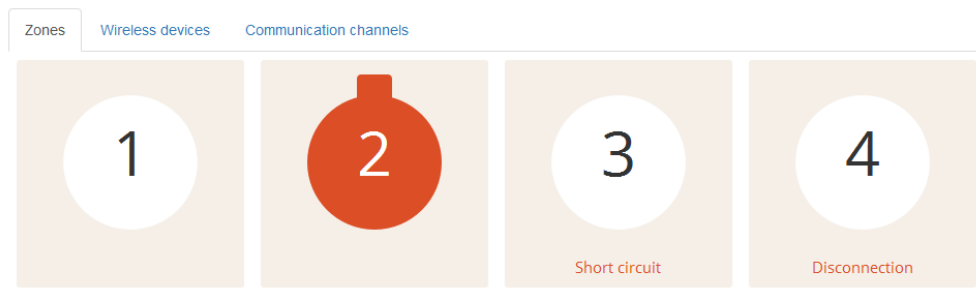


Figure 86: “State panel” tab, Zones in states: norm, alarm, short circuit, break

## 6 Remote Access to Device

### 6.1 Description of Remote Access Technology

Remote access to the device includes the following functions:

- Remote software update on site
- Remote configuration of the site
- Remote arming and disarming of the site by the user
- Remote arming and disarming of the site by the receiver operator
- Payment status management

All the above functions require a compatible remote software, for example, “Security Center”. In addition, to operate the functions of remote firmware update, configuration and arming/ disarming by the user, it is necessary to connect the device to the “Cloud” (C.Nord public cloud - [cloud.cnord.net](http://cloud.cnord.net) - or the private Cloud of the security organization).

The connection diagram is as follows:

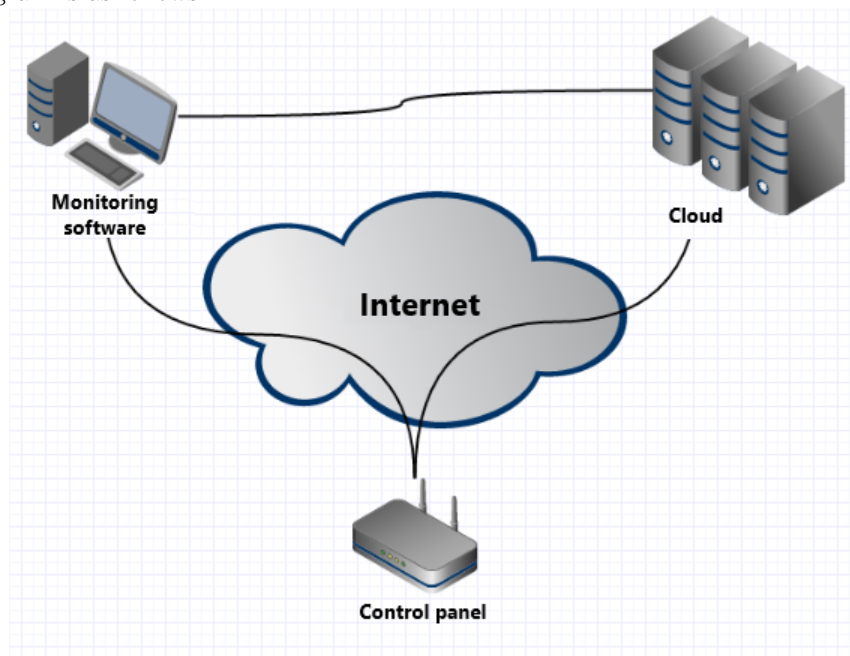


Figure 87

The device connects both to the alarm monitoring software and to the “Cloud” via CML protocol using streaming encryption (*CML protocol - C.Nord Markup Language - developed by C.Nord company*). The alarm monitoring software is also connected to the “Cloud” via the encrypted protocol.

#### 6.1.1 Communication Channel Device $\longleftrightarrow$ Receiver

This communication channel is used to operate the device security functions, such as:

- Transmission of events (alarm/arming/disarming/failure) to the receiver software
- Remote arming and disarming of the site by the receiver operator
- Payment status management

In the general case, the device connects to the receiver through a public network (Internet). However, some security companies use the allocated internal subnets of GSM carriers for communication ‘device  $\longleftrightarrow$  receiver’.

To transmit events to the receiver, various communication channels can be used: GPRS, Voice, SMS.

**Important:** remote arming/disarming and payment status management work only when the device is connected via IP communication channel GPRS.

### 6.1.2 Communication Channel Device $\longleftrightarrow$ “Cloud”

This communication channel is used for the device service functions, such as:

- Remote software update on site
- Remote configuration of the site
- Remote arming and disarming of the site by the user

In case of using the public “Cloud” the device connects to the “Cloud” via the Internet. If the Private Cloud is used, it is possible to connect through dedicated internal subnets of GSM carriers.

To operate all service functions, the device shall have IP connection with the “Cloud” via GPRS.

**Important:** Possible interruptions in connection of ‘device  $\longleftrightarrow$  “Cloud” ’ do not affect the security functions of the device in any way.

### 6.1.3 Communication Channel Receiver $\longleftrightarrow$ “Cloud”

This communication channel is used to ensure the operation of the device service functions.

**The alarm monitoring software transmits the following to the “Cloud”:**

- information about engineers and their permissions  
*for the engineering panel operation*
- information about administrators of the personal account and their sites  
*for operation of the personal account `my.cnord.net` and the `MyAlarm` mobile application*
- events by sites  
*for operation of the personal account and mobile applications*

**“Cloud” transmits the following to the alarm monitoring software:**

- events about engineer’s attempts to connect to a site  
*for the engineering panel operation*
- events about attempts to arm/disarm from the `MyAlarm` mobile application  
*for the mobile application operation*
- events about checking the panic button using the `Call-center`  
*for automatic check of the panic button*

In case of using the public “Cloud” the alarm monitoring software connects to the “Cloud” via the Internet.

**Important:** Possible interruptions in connection of ‘receiver  $\longleftrightarrow$  “Cloud” ’ do not affect the security functions of the device in any way.

## 6.2 Remote Access Setting

Remote access to the device is possible only if compatible software, for example, “Security Center” is installed on the receiver to which the device is connected. To use remote access to the device, it is necessary to do the following:

1. Create an engineer in the alarm monitoring software
2. To give the engineer the right to remote access to certain sites

### 6.2.1 Creating Engineer

To create an account for an engineer in the Security Center software, start the “Personnel manager” module and click the “New” button on the “Engineers” tab:

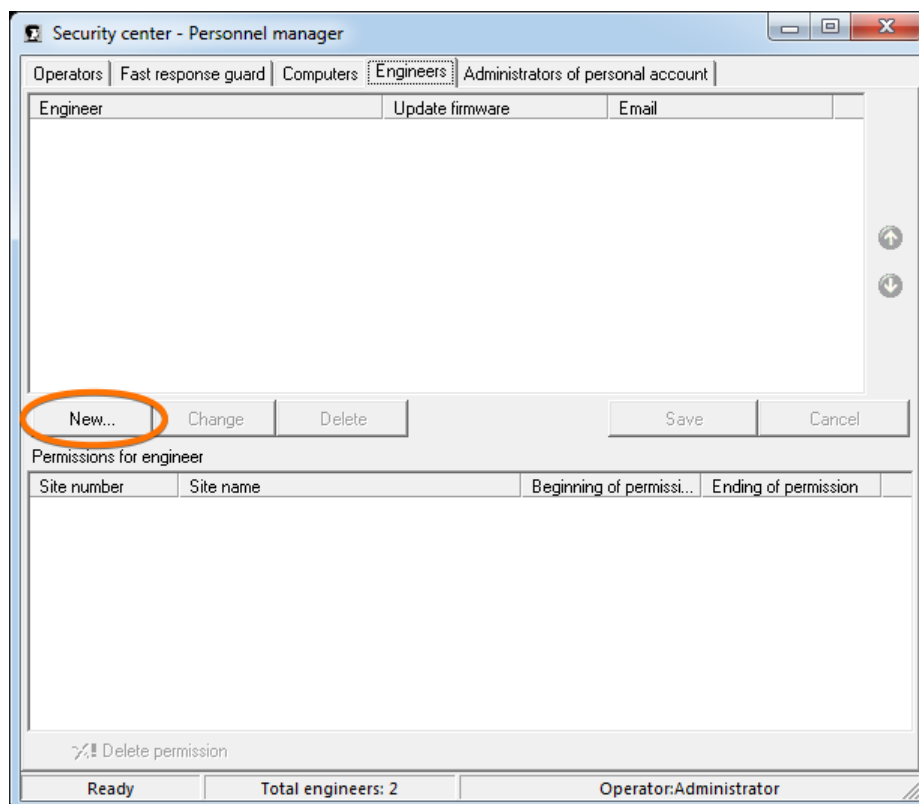


Figure 88

In the opened window fill in all fields with information about the engineer:

Figure 89

Pay particular attention to the “Email” field. It is to the e-mail address specified in this field that an email will be sent with a link where the engineer will need to go to complete the registration of the account in the “Cloud”. The engineer’s email serves to identify him in the “Cloud”. After the engineer is created, it is not possible to change the value of this field.

If the engineer for whom the account is created shall be able to remotely update the software on devices that are installed on the sites, check the box “Allow an engineer to remotely update software on site devices”. *This setting is available in the “Security Center” version 5 and above.*

**Important:** The engineer’s permission to update the software applies to all sites of the security company with the function of remote firmware upgrade.

In order for the changes to take effect, click the “Save” button on the “Engineers” tab. After this information about the engineers and their right to update the devices is synchronized with the “Cloud”.

## 6.2.2 Granting Permissions to Engineer

To give the engineer permission to remote access to equipment installed on the site in the Security Center software, the following actions shall be performed:

1. Run the “Site manager” module
2. Select the site to which you want to allow remote access
3. Go to the “Maintenance” tab
4. Click the “Add permission” button

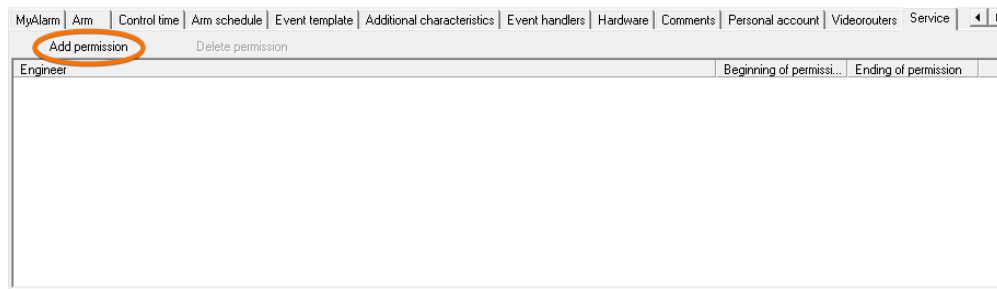


Figure 90

5. In the window that appears, select the engineer who needs remote access to the site

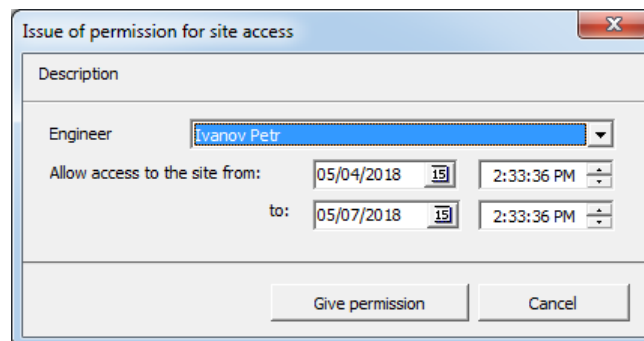


Figure 91

6. Specify the time interval during which the permission will be valid.
7. Click the “Give permission” button.

## 6.3 Device Remote Configuration

**Important:** Remote configuration is only available for devices that are configured to use IP communication channels – GPRS or Etehernet (if available).

**Important:** The functions described in this section work only if the device is connected to the Security Center software.

### 6.3.1 Selection of Site to Configure

To remotely change the settings in the devices, the tab “Remote access to sites” is located in the engineering panel:



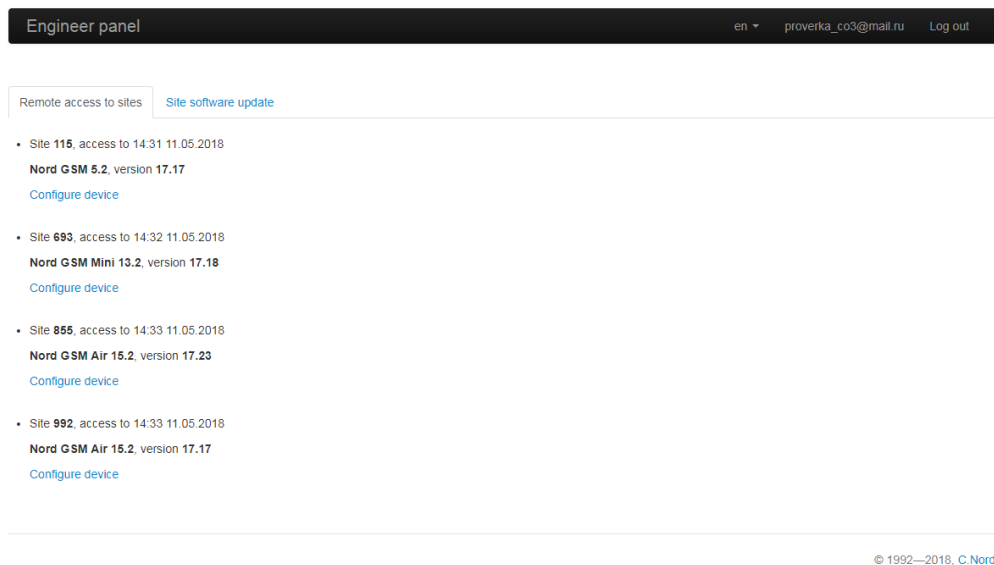


Figure 92

This tab displays a list of sites that are available to the engineer for configuration at the moment. The list and duration of the permissions are set in the Security Center software. To configure, click the corresponding site number.

### 6.3.2 Working with Configuration

The opened window for setting up the device is similar to the configurator intended for setting up the device connected to the computer, which is described in the “Configuration” section:

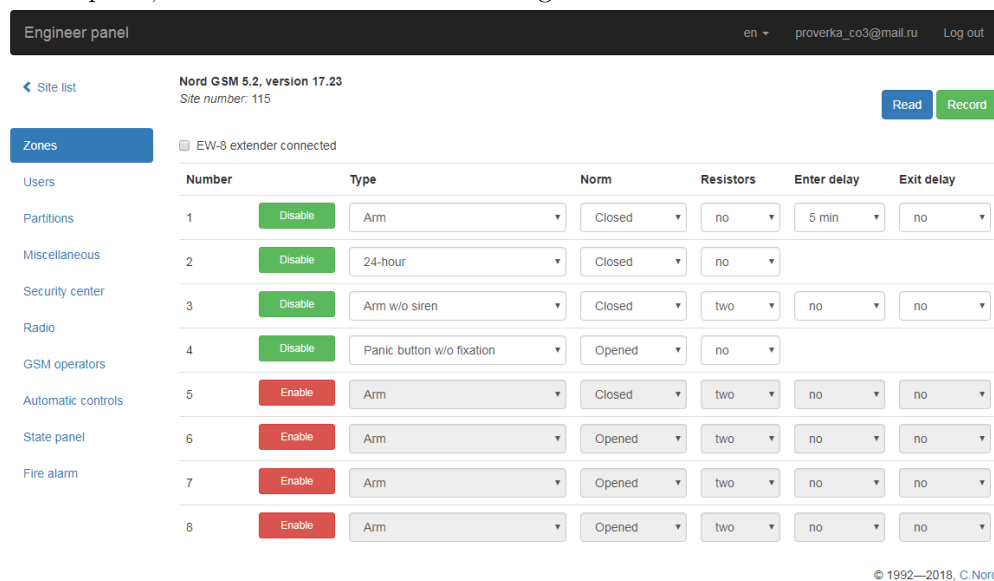


Figure 93

When you open the settings window from the device, its current configuration is read. Then it is possible to make the necessary changes and write them to the device with the corresponding button. After a successful download of the configuration, the message “Settings saved for writing to device” appears on the device.

**Important:** configuration reading and change are only available for devices that are currently connected to the “Cloud”. Otherwise an error message will be displayed: “Communicator installed on site is not currently connected to Cloud. Please try to connect to site later.”

Note that some configuration fields, for example, addresses to connect to the remote control, cannot be remotely changed. This excludes the possibility of remotely breaking the connection of the device with the receiver and

“Cloud”.

Actions that require local interaction with the device on the site are also not available, for example, connection of wireless sensors or addition of TM keys.

### 6.3.3 Work Features

#### Simultaneous Operation

Although the permissions for configuring one site can be simultaneously issued to several engineers, only one engineer can perform the direct configuration at a time. Access of the remaining engineers to the configuration panel is blocked and when they try to open the site for configuration, a warning is displayed: The site is currently being configured or updated.

#### Priority of Local Configuration

If during the remote configuration by one engineer, another engineer will change the device settings locally using the “desktop” configurator, it will be impossible to apply remote settings - the configuration download error message will be displayed.

## 6.4 Remote Software Update on Device

**Important:** Remote software update works only for devices that are configured to use IP communication channels – GPRS or Ethernet (if available).

**Important:** The functions described in this section work only if the device is connected to the Security Center software.

### 6.4.1 Information about Sites on Receiver

To remotely update the “firmware” in devices, the tab “Site software update” is located in the engineering panel:

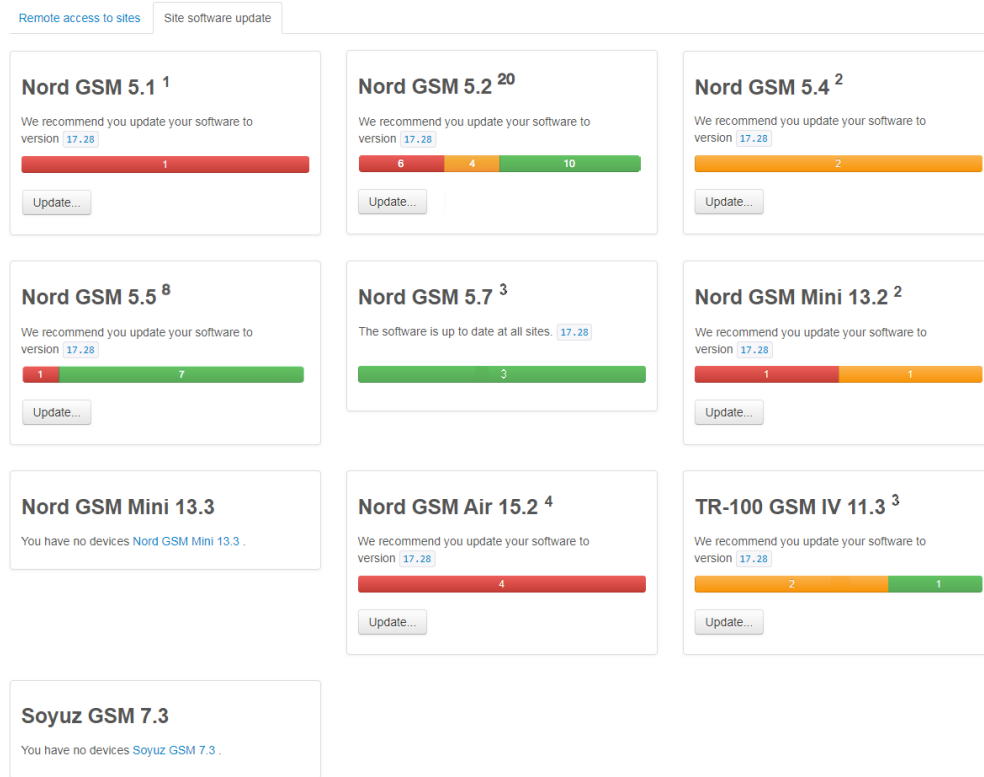


Figure 94

This tab displays statistics on software versions, grouped by device types. For example, for the “Nord GSM” device:



Figure 95

- 20 “Nord GSM” devices work for this receiver
- Current software version for “Nord GSM” - 5.40
- 10 devices are currently working on the old version, of which:
  - 6 - marked red - no plans to update
  - 4 - marked yellow - are in the process of updating
- 10 devices work on the current software version for this equipment

To open the software update page on devices of this type, click the “Update ...” button

## 6.4.2 Process of Remote Software Update on Device

The software update process on the device consists of several steps and is intended to work even on networks with a very unstable GPRS signal.

### Queuing for Upgrade

From the “Cloud” engineering panel, a command is given to set the device in the queue for updating.

If the device is connected to the “Cloud”, then a command will be sent to the device to reconnect and initiate the update process.

If the device is not connected to the Cloud, then the update process will not start until the device is connected.

### Downloading Current “Firmware”

Once the device has received the update command, it starts downloading the archive with the current software version. The total file size is from 200 to 500 Kb, depending on the type of device. “Firmware” is downloaded in parts to reduce the impact of communication interruptions.

Downloading duration heavily depends on the communication quality and can range from several minutes on the Ethernet channel to several hours on the GPRS channel.

### Archive Checking

After the “firmware” file is fully downloaded, the device checks its integrity and suitability for use on this type of device and on this hardware version of the board. If all checksums match and all compatibility checks are completed, the “firmware” is marked as “ready for installation”.

### Update

Next, the device waits for a state when at least one of the partitions is disarmed, and reboots to apply the update. Upgrade duration is no more than 10 seconds.

### Start

After updating the firmware, the device starts normally. All settings and protection status for partitions are saved in the same state as they were before updating.

### 6.4.3 Updating Software on Selected Site

If it is necessary to check the functions of the new software version on one or more sites before mass installation, it is possible to use the software update on the selected site.

To do this, click the “Update using site number...” button on the software update page:

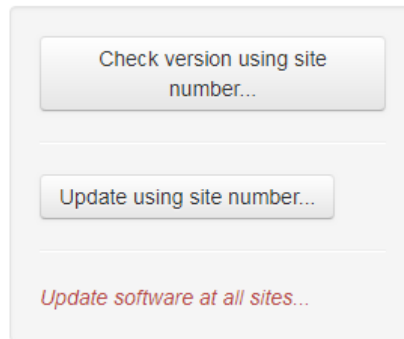


Figure 96

In the dialog that appears, enter the site number for the update:

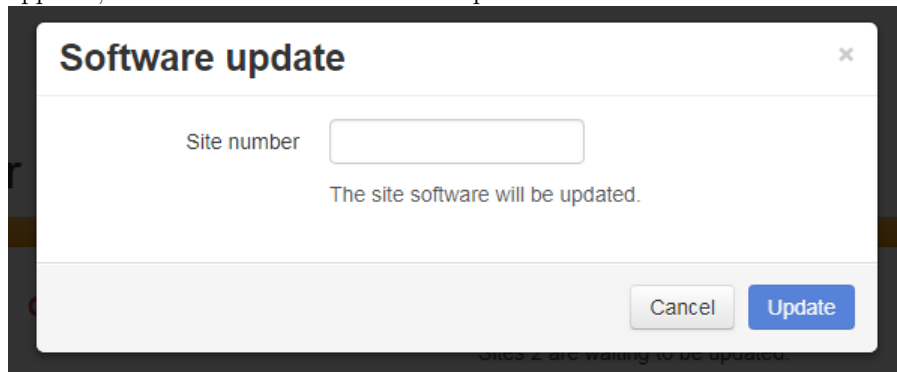


Figure 97

And click the “Update” button. After that, this site will be added to the queue for software update.

### 6.4.4 Updating Software on all Sites

After checking the software on several sites, it is possible to add all the remaining sites with the previous version of the software to the upgrade queue.

To do this, click the “Update software at all sites” button on the software update page:

In the dialog that appears:

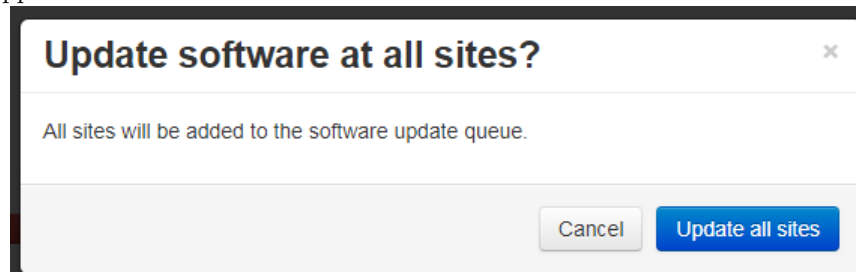


Figure 98

click the “Update all sites” button. After that, all sites of this type with the irrelevant version of the software will be added to the update queue.

### 6.4.5 Update Process Stopping

If for some reason there is a need to stop the update process, it can be interrupted until the device has completely downloaded the update file.

To do this, click “Cancel update...” and confirm the action.

## 7 Event codes

Contact ID	EPAF	Event	Note
E110	SY	Fire	Fire alarm
E118	SY	Warning	Fire danger
E120	SX	Alarm	Panic button
E121	RP	Alarm	Forced disarming
E130	AA..DR	Alarm	Armed zone
E133	AA..DR	Alarm	24-hour armed zone
E137	RS	Alarm	Open device case (tamper)
E138	SQ	Warning	Possible alarm
E141	AA..DR	Alarm	Break of armed zone
E142	AA..DR	Alarm	Short circuit of armed zone
E144	AA..DR	Alarm	Open sensor case (tamper)
E146	AA..DR	Alarm	Armed zone without alarm (silent alarm)
E150	AA..DR	Alarm	24-hour disarmed zone
E151	AA..DR	Alarm	Gas leak
E154	AA..DR	Alarm	Water leak
E301	RU	Fault	AC disconnection
E302	RW	Fault	Battery discharge
E306	–	System	Changed device settings
E309	RW	Fault	Faulty battery
E311	RW	Fault	Disconnected battery
E314	HK..LB	Fault	Fault of wireless device main battery or fire zone power supply, connected via EFW-2
E321	SC	Fault	Faulty siren
E331	HK..LB	Fault	Zone break
E332	HK..LB	Fault	Zone short circuit
E381	HK..LB	Fault	Communication with wireless device is lost
E384	HK..LB	Fault	Fault of backup battery of wireless device
E401	QT..23	Disarming	Disarming by user code
E403	QT..23	Disarming	Automatic disarming
E461	SL	Warning	Code breaking by user
E469	–	Disarming	Disarming of partition, which was armed, but was deleted from device settings during reconfiguration
E470	TA	Arming rejection	After this message arming rejection reason is transmitted (codes E471 – E476)
E471	–	Arming rejection	Security services are not paid
E472	RU	Arming rejection	No AC
E473	74	Arming rejection	No IP communication with receiver

E474	–	Arming rejection	Fault in
E475	–	Arming rejection	Alarm in zone which is included in partition to be armed
E476	RS	Arming rejection	Open device body
E499	QT..23	Disarming	Disarming from receiver
E521	–	System	Siren is disabled in settings
E601	SM	Test	Event is generated when channel is enabled in state panel
E602	SN	Test	Self-test
E627	–	System	Mode of programming via USB is enabled
E628	–	System	Mode of programming via USB is disabled
E750	–	System	Incorrect password when connecting via USB
E751	–	System	Discrete output is closed
E752	–	System	Reset to factory defaults is started
E754	–	System	Channel switching by audit system command
E756	56	Fault	Keypad fault
E757	57	Fault	Fault of communication with fire indication device “Fire”
E758	58	Fault	Fault of communication with CN-WRL
R110	DS..HJ	Reset	Fire alarm
R118	DS..HJ	Reset	Danger of fire
R120	DS..HJ	Reset	Panic button
R130	DS..HJ	Reset	Armed zone
R133	DS..HJ	Reset	24-hour armed zone
R137	RT	Reset	Closed device case (tamper)
R141	DS..HJ	Reset	Norm of zone after break (armed)
R142	DS..HJ	Reset	Norm of zone after short circuit (armed)
R144	DS..HJ	Reset	Closed sensor case (tamper)
R146	DS..HJ	Reset	Armed zone without siren (silent alarm)
R150	DS..HJ	Reset	24-hour disarmed zone
R151	DS..HJ	Reset	Gas leak
R154	DS..HJ	Reset	Water leak
R301	RV	Restoration	AC restored
R302	RX	Restoration	Battery charged
R305	RR	System	Device restart
R309	RX	Restoration	Operational battery
R311	RX	Restoration	Battery connected
R314	DS..HJ	Restoration	Main battery of wireless device is connected
R321	SD	Restoration	Operational siren
R331	DS..HJ	Restoration	Norm of zone after break
R332	DS..HJ	Restoration	Norm of zone after short circuit
R381	DS..HJ	Restoration	Restored communication with wireless device

R384	DS..HJ	Restoration	Wireless device backup battery is connected
R401	OV..WX	Arming	Arming by user code
R403	PR	Arming	Automatic arming
R499	OV..WX	Arming	Arming from receiver
R521	–	System	Siren enabled in device settings
R751	–	System	Open discrete output
R752	–	System	Reset of parameter values is cancelled
R753	–	System	Restart for an unknown reason
R754	–	System	Restart by audit system command
R755	–	System	Discrete output is opening-closing
R756	64	Restoration	Restoration of keypad fault
R757	65	Restoration	Restoration of communication with fire indication device “Fire”
R758	66	Restoration	Restoration of communication with CN-WRL
R903	–	System	Device firmware updated