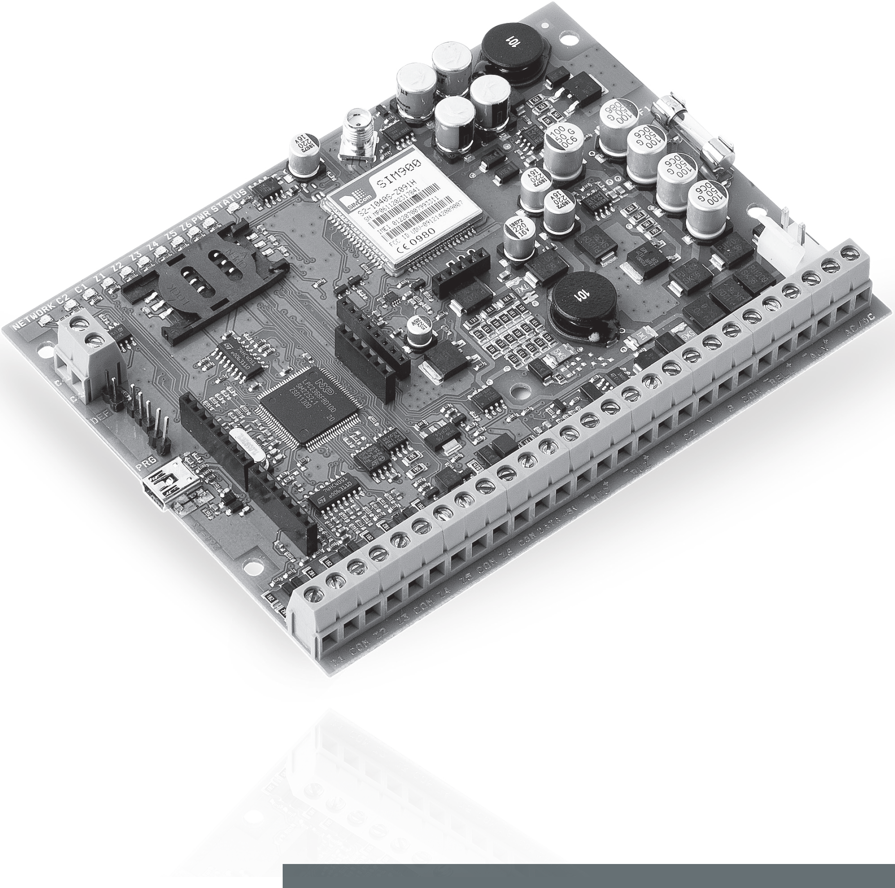


DISCOVERY telecom

ESIM264

GSM ALARM AND MANAGEMENT SYSTEM

INSTALLATION MANUAL

COMPLIES WITH EN 50131-1 GRADE 2, CLASS II REQUIREMENTS

Installation Manual v3.1
Valid for ESIM264 v7.15.00 and up

Safety instructions

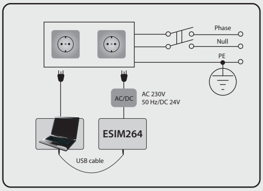
Please read and follow these safety guidelines in order to maintain safety of operators and people around:
- GSM alarm & management system ESIM264 (also referenced as alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- DO NOT use the system in hazardous environment.
- DO NOT expose the system to high humidity, chemical environment or mechanical impacts.
- DO NOT attempt to personally repair the system.
- System label is on the bottom side of the device.

GSM alarm system ESIM264 is a device mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel.

The system must be powered by main 16-24V 50 Hz ~1.5A max or 18-24V ⎓ 1,5A max DC power supply which must be approved by LST EN 60950-1 standard and be easily accessible nearby the device. When connecting the power supply to the system, switching the pole terminals places does not have any affect.

Any additional devices linked to the system ESIM264 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

Main power supply can be connected to AC mains only inside installation room with automatic 2-pole circuit breaker capable of disconnecting circuit in the event of short circuit or over-current condition. Open circuit breaker must have a gap between connections of more than 3mm and the disconnection current 5A.



Mains power and backup battery must be disconnected before any installation or tuning work starts. The system installation or maintenance must not be done during stormy conditions

Backup battery must be connected via the connection which in the case of breaking would result in disconnection of one of battery pole terminals. Special care must be taken when connecting positive and negative battery terminals. Switching the pole terminals places is NOT allowed.

In order to avoid fire or explosion hazards the system must be used only with approved backup battery.

The device is fully turned off by disconnecting 2-pole switch off device of the main power supply and disconnecting backup battery connector.

Fuse F1 type – Slow Blown 3A. Replacement fuses have to be exactly the same as indicated by the manufacturer.

If you use I security class computer for setting the parameters it must be connected to earth.

The WEEE (Waste Electrical and Electronic Equipment) marking on this product (see left) or its documentation indicates that the product must not be disposed of together with household waste. To prevent possible harm to human health and/or the environment, the product must be disposed on in an approved and environmentally safe recycling process. For further information on how to dispose of this product correctly, contact the system supplier, or the local authority responsible for waste disposal in your area.

Contents

Limited Liability

The buyer must agree that the system will reduce the risk of fire, theft, burglary or other dangers but does not guarantee against such events.

“ELDES UAB” will not take any responsibility regarding personal or property or revenue loss while using the system.

“ELDES UAB” liability according to local laws does not exceed value of the purchased system. “ELDES UAB” is not affiliated with any of the cellular providers therefore is not responsible for the quality of cellular service.

Manufacturer Warranty

The system carries a 24-month warranty by the manufacturer “ELDES UAB”. Warranty period starts from the day the system has been purchased by the end user. The warranty is valid only if the system has been used as intended, following all guidelines listed in the manual and within specified operating conditions. Receipt must be kept as a proof of purchase date.

The warranty is voided if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or other force majeure factors.

Package Content

1. ESIM264	qty. 1
2. Microphone	qty.1
3. SMA antenna	qty. 1
4. Buzzer	qty. 1
5. Back-up battery connection wire...	qty. 1
6. User manual	qty. 1
7. Resistors 5,6kΩ	qty. 6
8. Resistors 3,3kΩ	qty. 6
9. Plastic standoffs	qty. 4

About Installation Manual

This document describes detailed installation and operation process of alarm system ESIM264. It is very important to read the installation manual before starting to use the system.

1. GENERAL INFORMATION

1.1. Functionality

ESIM264 – micro-controller based alarm system for houses, cottages, country homes, garages and other buildings, also capable of managing electrical appliances via cellular GSM/GPRS network. It can also be used as Intercom system.

Examples of using the system:

- Property security.
- Alarm switch.
- Thermostat, heating and air-conditioner control, temperature monitoring.
- Lighting, garden watering, water pump and other electrical equipment control via SMS text messages.
- Remote listening to what is happening in the secured area.
- Main 230V power status with SMS text message.
- Two-way intercom device via GSM network.

1.2. Compatible Device Overview

Wired Devices		
Device	**Description**	**Max. Connectable Devices**
EKB2	LCD keypad	4*
EKB3	LED keypad	4*
EA1	Audio output module with 3,5mm jack	1**
EA2	Audio amplifier module 1W 8Ω	1**
EPGM1	16 zone and 2 PGM output expansion module	1
EPGM8	8 PGM output expansion module	1**

Wireless Devices		
Device	**Description**	**Max. Connectable Devices**
EW1	Wireless 2 zone and 2 PGM output expansion module	16***
EW1B	Battery-powered wireless 2 zone and 2 PGM output expansion module	16***
EWP1	Wireless motion detector	16***
EWD1	Wireless magnetic door contact	16***
EWD2	Wireless magnetic door contact/shock sensor/water sensor	16***
EWK1****	Wireless keyfob with 4 buttons	5***
EWK2****	Wireless keyfob with 4 buttons	5***
EWS1	Wireless indoor siren	16***
EWS2	Wireless outdoor siren	16***
EWS3	Wireless indoor siren	16***
EWF1	Wireless smoke detector	16***

* - A mixed combination of EKB2 and EKB3 keypads is supported. The combination can consist of up to 4 keypads in total.
** - Only 1 of these modules can be connected at a time if the module slots are implemented in ESIM264 unit.
*** - A mixed combination of wireless devices is supported. The combination can consist of up to 32 wireless devices in total.
**** - A mixed combination of EWK1 and EWK2 keyfobs is supported. The combination can consist of up to 5 keyfobs in total.

1.3. Default Parameters & Ways of Parameter Configuration

Main Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3**	**Configuration Tool**
SMS & EKB2 Menu Language	Depends on firmware version according to user's location	✓	✓	✓	✓
SMS Password	0000	✓	✓	✓	✓
User Password 1	1111		✓	✓	✓
User Password 2... 30	N/A		✓	✓	✓
Administrator Password	1470		✓	✓	✓
Duress Password	N/A		✓	✓	✓
SGS Password	N/A		✓	✓	✓
User 1... 5 Phone Number	N/A	✓	✓	✓	✓
Allow Control from Any Phone Number	Disabled	✓	✓	✓	✓
Date & Time	N/A	✓	✓	✓	✓
Exit Delay - Partition 1... 4	15 seconds	✓	✓	✓	✓
Info SMS Scheduler	Frequency (days) – 1; Time - 11	✓	✓	✓	✓

Zones

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Zone Name	Z1 - Zone 1; Z2 - Zone 2; Z3 - Zone 3; Z4 - Zone 4; Z5 - Zone 5; Z6 - Zone 6	✓			✓
Entry Delay	15 seconds	✓	✓	✓	✓
On-Board Zone Delay	800 milliseconds				✓
EPGM1 Zone Delay	800 milliseconds				✓
On-board Z1 Zone Type	Delay		✓	✓	✓
On-board Z2... Z12 Zone Type	Instant		✓	✓	✓
Keypad Zone Type	Instant		✓	✓	✓
EPGM1 Zone Type	Instant		✓	✓	✓
Wireless Zone Type	Depends on the connected wireless device		✓	✓	✓
Virtual Zone Type	Interior Follower			✓	✓
ATZ Mode	Disabled		✓	✓	✓
6-Zone Mode: Zone Connection Type	Type 1		✓	✓	✓
ATZ Mode: Zone Connection Type	Type 4		✓	✓	✓
On-board Zone Status	Enabled	✓	✓	✓	✓
Keypad Zone Status	Disabled	✓	✓	✓	✓
EPGM1 Zone Status	Enabled	✓	✓	✓	✓
Wireless Zone Status	Depends on the connected wireless device	✓	✓	✓	✓
Virtual Zone Status	Disabled			✓	✓
Stay attribute for individual zone	Disabled		✓	✓	✓
Arm-Disarm by Zone	N/A		✓	✓	✓
Force atrribute for individual zone	Disabled		✓	✓	✓
Tamper Name	Tamper 1, Tamper 2, Tamper 3, Tamper 4, Tamper 5, Tamper 6 etc.				✓
Chime	Enabled		✓	✓	✓

PGM Outputs

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
PGM Output Name	C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.	✓			✓
PGM Output Status	Disabled	✓	✓	✓	✓
EPGM8 PGM Output Status	Disabled	✓	✓	✓	✓
EPGM1 PGM Output Status	Disabled	✓		✓	✓
Wireless PGM Output Status	Enabled	✓	✓	✓	✓
Wireless PGM Output Type	Depends on the connected wireless device				✓
PGM Output Control by Event 1... 16	Disabled			✓	✓
PGM Output Control by Event Management					✓
Scheduler 1... 16	Disabled				✓
Turn ON/OFF PGM Output by Timer		✓			
Using Module EPGM8 Mode	Disabled		✓	✓	✓

Alarm Duration & Siren

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Alarm Duration	1 minute	✓	✓	✓	✓
EWS2 LED	Disabled		✓		✓
Bell Squawk	Disabled		✓	✓	✓
Activate Siren if Wireless Device is Lost	Disabled		✓	✓	✓

Alarm Notifications & Arm/Disarm Notifications

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Call in Case of Alarm	Enabled		✓	✓	✓
Send Alarm SMS to All Users Simultaneously	Disabled	✓	✓	✓	✓
Send Arm/Disarm SMS to User 1... 5	Enabled		✓	✓	✓
Send Arm/Disarm SMS to All Selected Users Simultaneously	Disabled	✓	✓	✓	✓

Main Power Status

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Main Power Loss Delay	30 seconds		✓	✓	✓
Main Power Restore Delay	120 seconds		✓	✓	✓

Peripheral Devices

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Temperature Sensor MIN	0 °C	✓	✓	✓	✓
Temperature Sensor MAX	0 °C	✓	✓	✓	✓
Allow adding New iButton Keys	Disabled	✓	✓	✓	✓

System Notifications

Parameter	Parameter	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
General Alarm	Enabled		✓	✓	✓
System Disarmed	Enabled		✓	✓	✓
System Armed	Enabled		✓	✓	✓
Main Power Loss Event Enabled	Enabled	✓	✓	✓	✓
Main Power Restore Event Enabled	Enabled	✓	✓	✓	✓
Low Battery	Enabled		✓	✓	✓
Periodical Info	Enabled		✓	✓	✓
Tamper Alarm Event	Enabled		✓	✓	✓
Battery Failed	Enabled		✓	✓	✓
System Started	Enabled		✓	✓	✓
Wireless Signal Loss	Enabled			✓	✓
Temperature Fallen	Enabled	✓	✓	✓	✓
Temperature Exceeded	Enabled	✓	✓	✓	✓
System Shutdown	Enabled		✓	✓	✓

Partitions

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Partition 0 Name	PART0		✓	✓	✓
Partition 1 Name	PART1		✓	✓	✓

Partitions

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Keypad 1... 4 Partition	PART0		✓	✓	✓
Keypad Partition Switch	Disabled		✓	✓	✓
User Password 1... 30 Partition	PART0		✓	✓	✓
User 1... 5 Phone Number Partition	PART0		✓	✓	✓
iButton 1... 5 Partition	PART0		✓	✓	✓
Zone Partition	PART0		✓	✓	✓

Monitoring Station

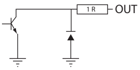
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
MS Mode	Disabled	✓	✓	✓	✓
Data Messages	All Enabled		✓	✓	✓
Account (Alarm System ID)	9999		✓	✓	✓
Monitoring Station Phone Number 1... 3 (Voice Calls/SMS)	N/A		✓	✓	✓
Attempts (Voice Calls/SMS)	3		✓	✓	✓
Monitoring Station Phone Number 1... 5 (CSD)	N/A		✓	✓	✓
Attempts (CSD)	3		✓	✓	✓
Server IP Address (GPRS)	0.0.0.0	✓	✓	✓	✓
DNS1 Server IP Address (GPRS)	N/A	✓	✓	✓	✓
DNS2 Server IP Address (GPRS)	N/A	✓	✓	✓	✓
Protocol (GPRS)	UDP	✓	✓	✓	✓
Server Port (GPRS)	20000	✓	✓	✓	✓
Local Port (GPRS)	N/A	✓	✓	✓	✓
APN (GPRS)	N/A	✓			✓
User (GPRS)	N/A	✓			✓
Password (GPRS)	N/A	✓			✓
Profile (GPRS)	Profile1	✓			✓
GPRS Attempts	3		✓	✓	✓
Delay Between Attempts (GPRS)	600 seconds		✓	✓	✓
Unit ID (GPRS)	0000		✓	✓	✓
Test Period (GPRS)	180 seconds		✓	✓	✓
Communication - Primary	N/A		✓	✓	✓
Communication - Backup 1... 4	N/A		✓	✓	✓
Protocol over GPRS	EGR100				✓

Additional Parameters					
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Event Log	Enabled		✓	✓	✓
Microphone Gain	12		✓		✓
Speaker Level	85		✓		✓
GSM Signal Loss Indication - Delay	180 seconds				✓
GSM Signal Loss Indication - Activate Output	N/A				✓
Show **ARMED** Status in Keypad (EKB2)	Disabled				✓

ELDES Smart Security					
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
ELDES Smart Security	Disabled				✓
Server Address	ss.eldes.lt				✓
Port	8082				✓
Ping Period	180 seconds				✓
Time Zone	0				✓

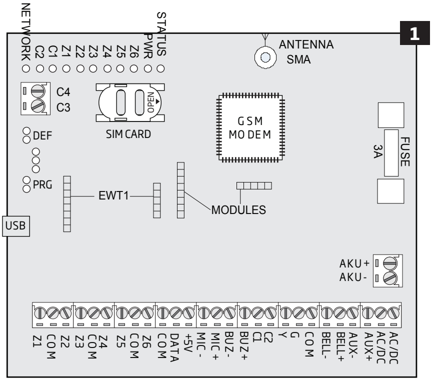
2. TECHNICAL SPECIFICATIONS

2.1. Electrical & Mechanical Characteristics

Electrical & Mechanical Characteristics	
Main power supply	16-24V 50 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current in standby without external sensors and keypad	Up to 80mA
Recommended backup battery voltage, capacity	12V; 1,3-7 Ah
Recommended backup battery type	Lead-Acid
Maximum battery charge current	900mA
Gsm modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
Number of zones on-board	6 (ATZ mode: 12)
Nominal zone resistance	5,6kΩ (ATZ Mode: 5,6kΩ and 3,3kΩ)
Number of PGM outputs on-board	4
On-board PGM output circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum commuting on-board PGM output values	4 x Voltage – 30V; current – 500mA.
BELL: Siren output when activated	Connected to COM
BELL: Maximum cable length for siren connection	Up to 100 meters
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
BELL+AUX: Maximum accumulative current of auxiliary equipment & siren	1 A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100 meters
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC
BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	1
DATA: Maximum cable length for 1-Wire communication	Up to 30 meters
DATA: Cable type for 1-Wire communication	Unshielded
Supported ibutton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	5
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100 meters
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2 meters
MIC: Cable type for microphone connection	Unshielded
Wireless transmitter-receiver frequency	868 Mhz
Wireless communication range	Up to 30m in premises; up to 150m in open areas
Maximum supported number of wireless devices	16
Event log size	500 events
Maximum supported number of zones	44
Maximum supported number of pgm outputs	44
Cable type for zone and pgm output connection	Unshielded
Communications	SMS, Voice calls, GPRS network, RS485, CSD
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS
Dimensions	140x100x18mm
Operating temperature range	-20...+55 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)

2.2. Main Unit, LED & Connector Functionality

Main Unit Functionality	
GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD	SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
ANTENNA	GSM/GPRS antenna SMA type connector
MODULES*	Slots for EA1, EA2 or EPGM8 module
EWT1	Slots for EWT1 wireless module



LED Functionality	
NETWORK	GSM network signal strength
C2, C1	PGM output C1, C2 status – on/off
Z1	Zone Z1 state – alarm/restore (ATZ mode: Z1 and Z7)
Z2	Zone Z2 state – alarm/restore (ATZ mode: Z2 and Z8)
Z3	Zone Z3 state – alarm/restore (ATZ mode: Z3 and Z9)
Z4	Zone Z4 state – alarm/restore (ATZ mode: Z4 and Z10)
Z5	Zone Z5 state – alarm/restore (ATZ mode: Z5 and Z11)
Z6	Zone Z6 state – alarm/restore (ATZ mode: Z6 and Z12)
PWR	Power supply status
STATUS	Micro-controller status

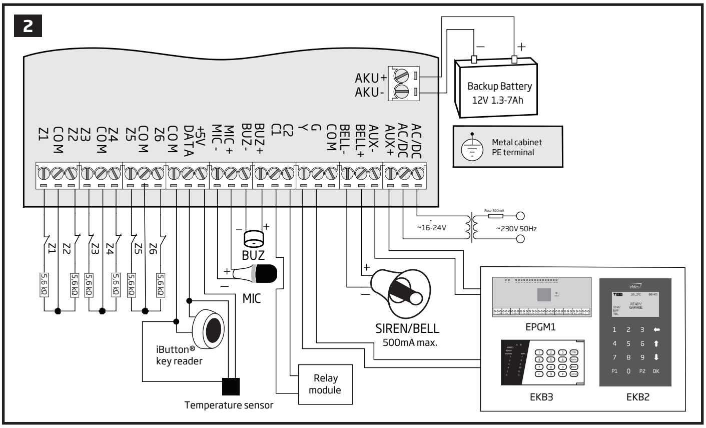
NETW indication	GSM signal strength
OFF	No GSM signal
Flashing every 3 sec.	Poor
Flashing every 1 sec.	Medium
Flashing several times per sec.	Good
Steady ON	Excellent

Connector Functionality	
Z1 - Z6	Security zones
COM	Common terminal for all zones
DATA	1-Wire® interface for iButton® key & temperature sensor connection
+5V	Temperature sensor power supply contact (+5V)
MIC-	Microphone negative terminal
MIC+	Microphone positive terminal
BUZ-	Mini buzzer negative terminal
BUZ+	Mini buzzer positive terminal
C1 - C4	PGM outputs
Y	RS485 interface CLOCK terminal (yellow wire)
G	RS485 interface DATA terminal (green wire)
COM	Common return terminal
BELL-	Siren negative terminal
BELL+	Siren positive terminal
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
AC/DC	Main power supply terminal
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

2.3. Wiring Diagrams

2.3.1. General Wiring

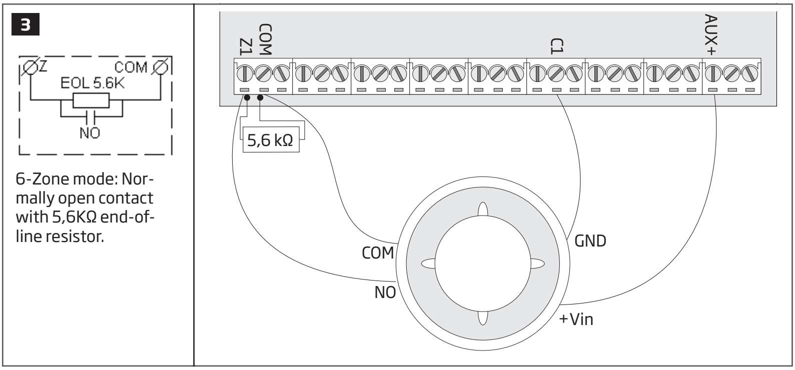
2



2.3.2. Zone Connection Types

Type 1 Example of 4-wire smoke detector wiring

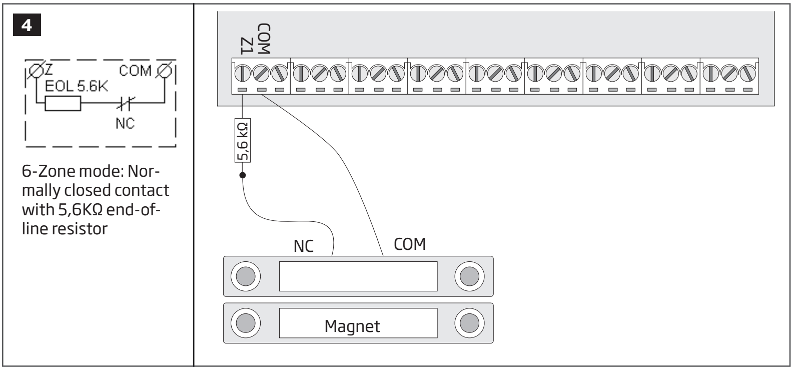
3



6-Zone mode: Normally open contact with 5,6KΩ end-of-line resistor.

Type 2 Example of magnetic door contact wiring

4



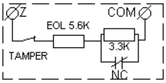
6-Zone mode: Normally closed contact with 5,6KΩ end-of-line resistor

NOTE: Based on the example given, in the event of an alarm, the smoke detector could be reset by turining OFF and ON the PGM output C1. For more details, please refer to **18.4. Turning PGM Outputs ON and OFF.**

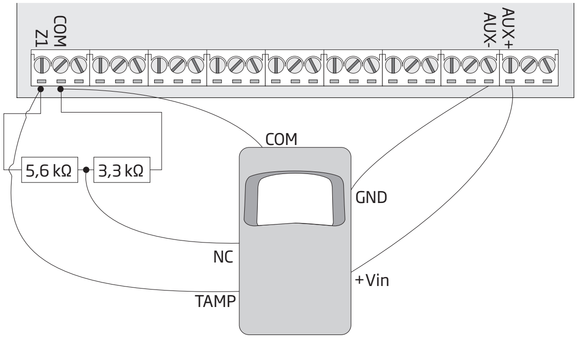
NOTE: The system does NOT support 2-wire smoke detectors.

Type 3 Example of motion detector wiring

5

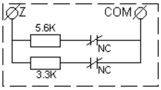


6-Zone mode: Tamper and 5,6KΩ end-of-line resistor and 3,3KΩ end-of-line resistor with normally closed contact.

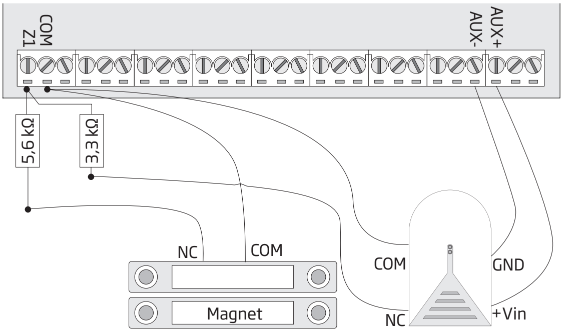


Type 4 Example of magnetic door contact (Z1) and glass break sensor (Z7) wiring

6

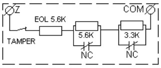


ATZ mode: 5,6KΩ end-of-line resistor and normally closed contact with 3,3KΩ end-of-line resistor and normally closed contact

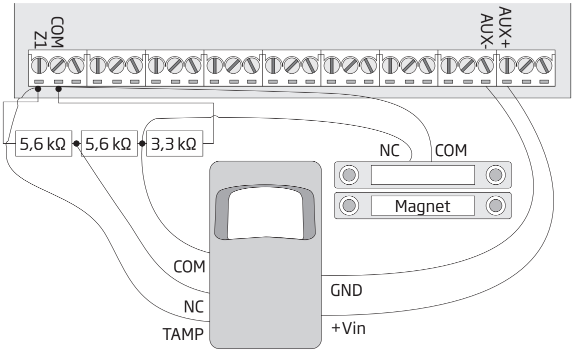


Type 5 Example of motion detector (Z1) and magnetic door contact (Z7) wiring

7

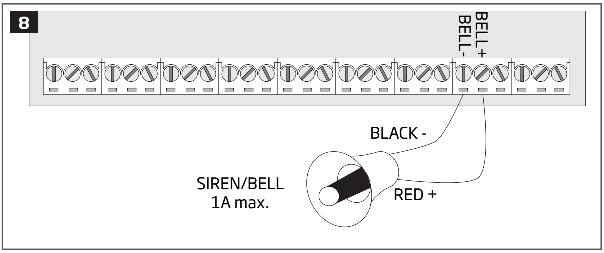


ATZ mode: Tamper, 5,6KΩ end-of-line resistor, 5,6KΩ end-of-line resistor with normally closed contact and 3,3KΩ end-of-line resistor with normally closed contact.



See also **14.3. 6-Zone Mode** and **14.4. ATZ (Advanced Technology Zone) Mode.**

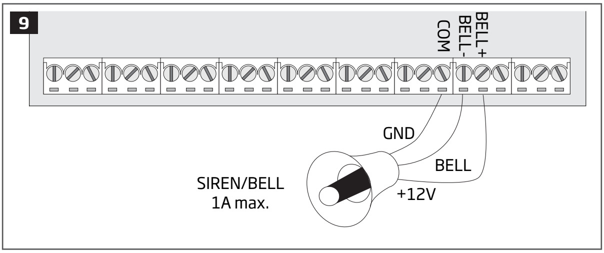
2.3.3. Siren



Piezo siren

1 Connect positive siren wire (red) to **BELL+** terminal.

2 Connect negative siren wire (black) to **BELL-** terminal.



Self-contained siren

1 Connect negative **GND** siren wire to **COM** terminal.

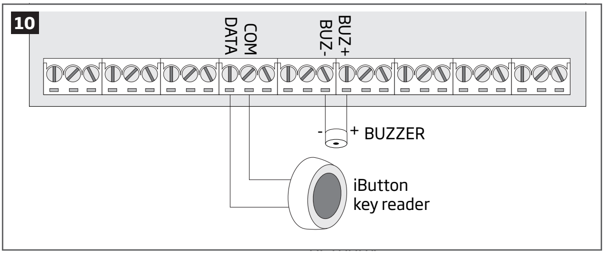
2 Controlling **BELL** siren wire must be connected to **BELL-** terminal.

3 Connect positive **+12V** siren wire to **BELL+** terminal.

See also **20. SIREN/BELL**.

NOTE: BELL- is the commuted terminal intended for siren control.

2.3.4. iButton Key Reader and Buzzer



Supported iButton key model: Maxim/Dallas DS1990A

The iButton key reader can be installed with buzzer or separately. The buzzer is intended for audio indication of exit/entry delay countdown providing short beeps.

1 Connect iButton key reader terminal wires to 1-Wire interface: **COM** and **DATA** terminals respectively.
2 Connect buzzer's negative terminal wire to **BUZ-** and positive terminal wire to **BUZ+.**
3 Additionally, a LED indicator for visual indication can be installed in parallel to buzzer or instead. Connect LED anode terminal to **BUZ-** and cathode to **BUZ+**.

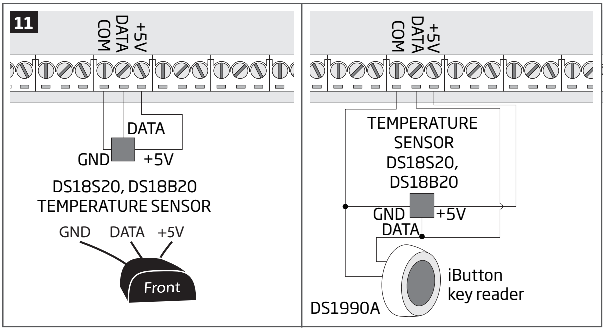
NOTE: The installation of buzzer is not necessary if EKB2/EKB3 keypad is used.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30 meters max.

2.3.5. Temperature Sensor and iButton Key Reader

Supported iButton key model: Maxim/Dallas DS1990A

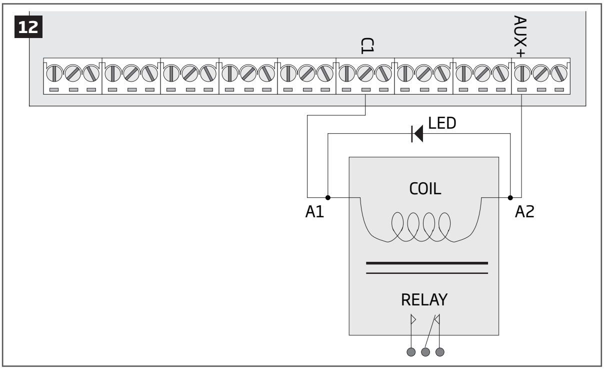
Supported temperature sensor model: Maxim/Dallas DS18S20, DS18B20



1 Connect temperature sensor **GND**, **DATA**, **+5V** terminals to 1-Wire interface: **COM**, **DATA** and **+5V** terminals respectively.
2 When connecting iButton key reader in parallel to temperature sensor, connect iButton key reader terminal wires to **COM** and **DATA** terminals respectively.

ATENTION: The cable length for connection to 1-Wire interface can be up to 30 meters max.

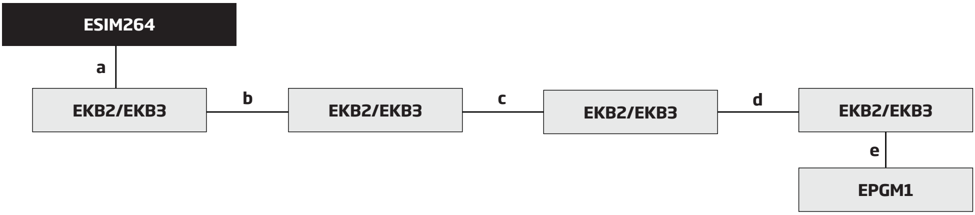
2.3.6. Relay Finder 40.61.9.12 with Terminal Socket 95.85.3 to PGM Output



1 Wire up relay **A1** terminal to **PGM** output **Cx** and **A2** terminal to **AUX+**.
2 In addition, connect LED indicator's anode terminal to relay **A2** terminal and cathode to **A1** terminal.

2.3.7. RS485

Serial Wiring Method



Max. cable length: a+b+c+d+e = up to 100 meters

NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

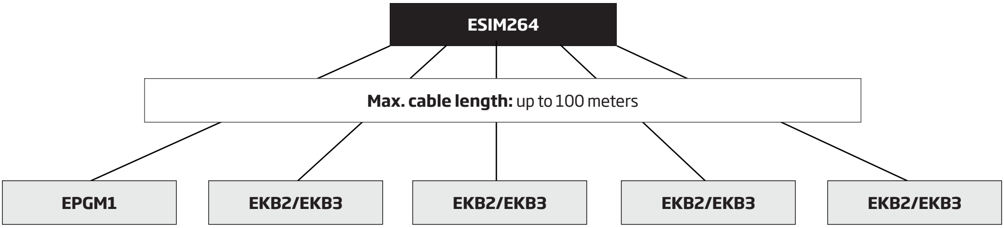
ATTENTION: The cable length must not exceed 100 meters in total.

ATTENTION: When wiring more than 1 keypad, please ensure that the set address of each keypad is different.

NOTE: You may connect only 1 EKB2/EKB3 keypad or a mixed combination of EKB2 and EKB3 keypads. The combination can consist of up to 4 keypads in total.

For more details on RS485 device installation, please refer to **32.1. RS485 Interface**

Parallel Wiring Method



NOTE: If necessary, the RS485 devices can be powered from an external 12-14V DC power supply instead of AUX+ and AUX- terminals

ATTENTION: The cable between ESIM264 and each RS485 device must be of the same length and can NOT exceed 100 meters.

ATTENTION: When wiring more than 1 keypad, please ensure that the set address of each keypad is different.

NOTE: You may connect only 1 EKB2/EKB3 keypad or a mixed combination of EKB2 and EKB3 keypads. The combination can consist of up to 4 keypads in total.

For more details on RS485 device installation, please refer to **32.1. RS485 Interface**

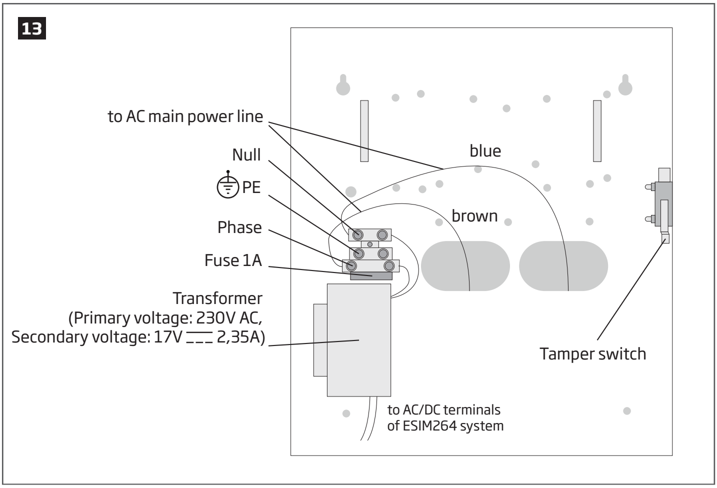
3. INSTALLATION

- The system can be installed in a metal or non-flammable cabinet only. For a convenient installation, ME1 metal cabinet is highly recommended. When using a different metal cabinet, it is necessary to ground it.
- For the connection of 230V transformer, use 3x0.75 mm^2 1 thread double isolated cable. 230V power supply cables must not be grouped with low voltage cable group.
- For the connection of auxiliary and BELL outputs, use 2x0.75 mm^2 1 thread unshielded cable of up to 100 meters length.
- For the connection of zone/PGM output connectors, use 0.50 mm^2 1 thread unshielded cable of up to 100 meters length.

System Installation in ME1 Metal Cabinet

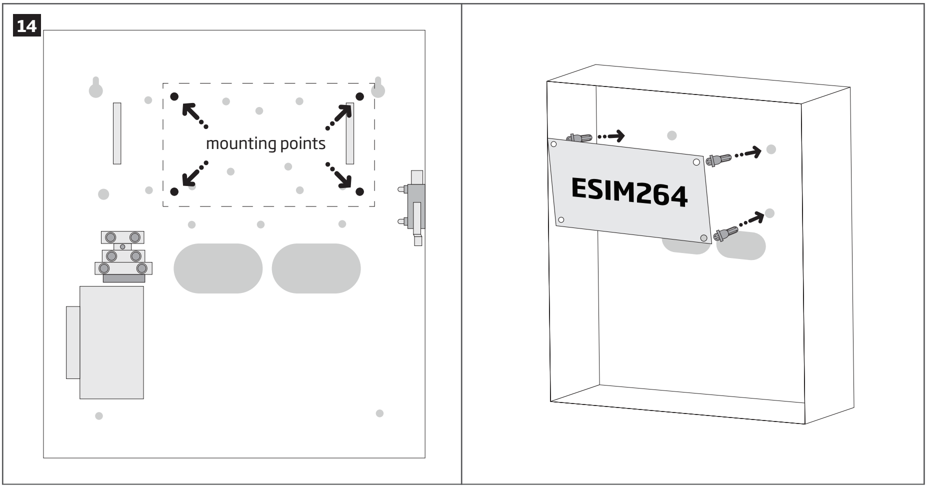
1. ME1 metal cabinet components

13

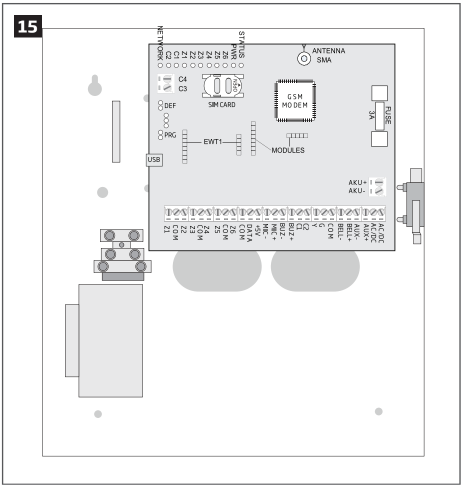


2. Insert the plastic standoffs into the appropriate mounting points and fix the board of ESIM264 on the holders as indicated below.

14

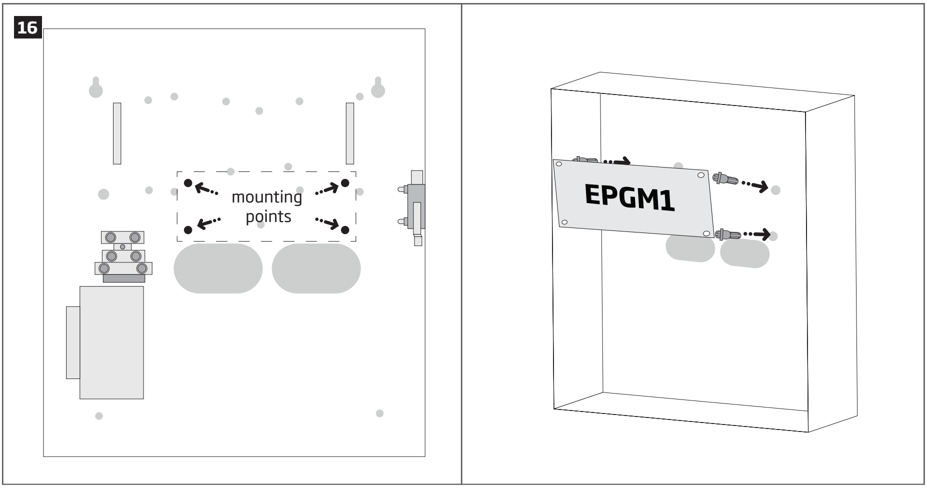


15

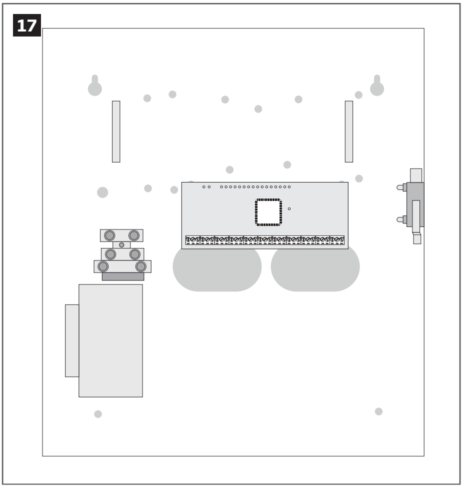


3. If EPGM1 module is to be installed, please install it in the first place and ESIM264 alarm system afterwards. EPGM1 must be mounted on the shorter plastic standoffs, while ESIM264 – on the longer ones. The mounting points of EPGM1 module are indicated below.

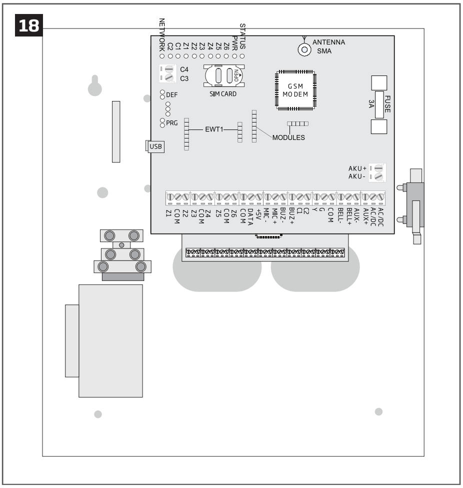
16



17



18

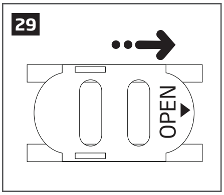


4. Wire up the system according to the wiring diagrams. Install the buzzer closer to iButton key reader in order to hear the exit delay countdown. A LED indicator can be used in parallel to the buzzer or instead. For a convenient installation, ED1 is highly recommended (see **2.3 Wiring Diagrams** for more details).

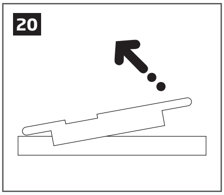
5. Disable the PIN code of the SIM card by inserting it into a mobile phone and following the proper menu steps. Ensure that the addition al services, such as **voice mail, call forwarding, report on missed/busy calls** are disabled on the SIM card. For more details on how to disable these services, please contact your GSM operator.

6. Once the PIN code is disabled, place the SIM card into the SIM CARD slot of the alarm system.

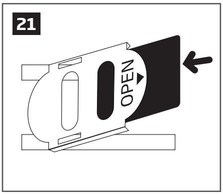
29

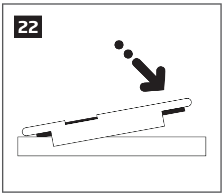


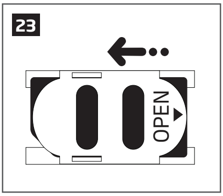
20



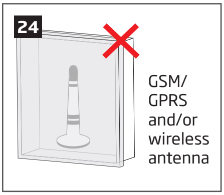
21





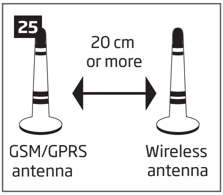


7. Connect the GSM/GPRS and wireless antennas and follow the recommendations for the installation:



Never install in the following locations:

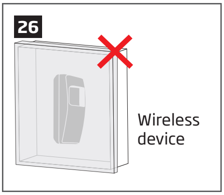
- inside the metal cabinet
- closer than 20 cm from the metal surface and/or power lines



Recommended installation:

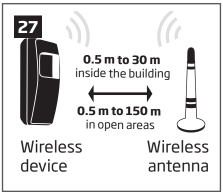
- keep the distance of at least 20 cm or more.

8. If one or more wireless devices are to be bound, follow the recommendations for the installation to achieve the strongest wireless signal:



Never install in the following locations:

- inside the metal cabinet
- closer than 20 cm from the metal surface and/or power lines



Recommended installation:

- face the front side of the wireless device towards the antenna
- keep the distance: 0.5 m to 30 m inside the building, 0.5 m to 150 m in open areas

9. Power up the system.

10. The system starts up in less than a minute. Indicator STATUS should be flashing indicating successful micro-controller operation.

11. The illuminated indicator NETWORK indicates that the system successfully registered to GSM network. To find the strongest GSM signal, place the GSM/GPRS antenna and follow the indications provided by NETWORK indicator (see **2.3. Main Unit, LED & Connector Functionality**).

12. Change the default SMS password (see **6. PASSWORDS** for more details).

13. Set the phone number for User 1 (see **8. USER PHONE NUMBERS** for more details).

14. Set system date and time (see **9. DATE AND TIME** for more details).

15. Once the system is fully configured, it is ready for use. However, if you fail to receive an SMS reply from the system, please check the SMSC (Short Message Service Center) phone number. For more details regarding the SMS centre phone number, please refer to **27.1. SMSC (Short Message Service Center) Phone Number.**

ATTENTION: The system is NOT compatible with pure 3G SIM cards. Only 2G/GSM SIM cards and 3G SIM cards with 2G/GSM profile enabled are supported. For more details, please contact your GSM operator.

NOTE: The installation of iButton key reader, EKB2/EKB3 keypad, EWK1 wireless keyfob is not mandatory. However, it is recommended to have those devices installed as an emergency switch in case your mobile phone is switched off or missing.

NOTE: For maximum system reliability we recommend you do NOT use a Pay As You Go SIM card. Otherwise, in the event of insufficient credit balance on the SIM card, the system would fail to make a phone call or send messages.

NOTE: We advise you to choose the same GSM SIM provider for your system as for your mobile phone. This will ensure the fastest, most reliable SMS text message delivery service and phone call connection.

NOTE: Even though alarm system ESIM264 installation process is not too complicated, we still recommend to perform it by a person with basic knowledge in electrical engineering and electronics to avoid any system damage.

4. GENERAL OPERATIONAL DESCRIPTION

When the system is being armed, it will initiate the exit delay countdown intended for the user to leave the secured area. During the countdown period the buzzer will emit short beeps and/or LED indicator will flash. By default, exit delay duration is 15 seconds. After the countdown is complete, the system will become armed and lock the configuration by keypad possibility. In case the user does not leave the secured area before the countdown is complete, the system will will arm in Stay mode if at least 1 zone has Stay attribute enabled. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the system until the violated zone or tamper is restored. In case it is required to arm the alarm system despite the violated zone presence, the violated zone can be bypassed or Force attribute enabled.

After the system is armed and if a zone (depending on type) or tamper is violated, the system will cause an alarm lasting for 1 minute (by default), During the alarm, the siren/bell will provide an alarm sound along with the buzzers of the keypads. By default, the system will also makes a phone call and send an SMS text message containing the violated zone or tamper number to a preset user and indicate the violated zone or tamper number on the keypad. If another zone or tamper is violated or the same one is restored and violated again during the alarm, the system will act as mentioned previously, but will not extend the alarm time.

After the user enters the secured area, the system will initiate the entry delay countdown intended for system disarming. During the countdown period, the buzzer will emit a steady beep and/or LED indicator will light ON. By default, entry delay duration is 15 seconds. After the user successfully performs the disarming process, the system will unlock the keypads. If the user does not disarm the system in time, the alarm system will cause an instant alarm.

NOTE: The alarm will be caused even if a tamper is violated while the system is disarmed.

For more details, please refer to **12. ARMING AND DISARMING**.

5. CONFIGURATION METHODS

!!! In this installation manual the underscore character ”_” represents one space character. Every underscore character must be replaced by a single space character. There must be no spaces or other unnecessary characters at the beginning and at the end of the SMS text message.

SMS

In order to configure and control the system by SMS text message, send the text command to the ESIM264 system phone number from one of the preset user phone numbers. The structure of SMS text message consists of 4-digit SMS password (the default SMS password is 0000 – four zeros), the parameter and value. For some parameters the value does not apply e. g. STATUS. The variables are indicated in lower-case letters, while a valid parameter value range is indicated in brackets.

EKB2

The system configuration and control by EKB2 keypad is carried out by navigating throughout the menu section list displayed on LCD screen. To navigate in the menu path, touch ↓, ↑ keys to select the desired menu section and touch OK key to open the selected section. To enter a required value, use 0... 9 keys and touch OK key for confirmation or cancel/go one menu section back by touching ← key. The value can be typed in directly by touching 0... 9 keys while highlighting the desired menu section. EKB2 menu type is “circle”, therefore when the last section in the menu list is selected, you will be brought back to the beginning of the list after touching the ↓ key. In this installation manual, the menu path is based on the EKB2 menu tree by starting at home screen view (see **31.1.1.6. EKB2 Menu Tree**). The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: Menu section CONFIGURATION is secured with administrator password. The default administrator password is **1470**.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the menu section CONFIGURATION is opened. The inactive EKB2 keypads will display 🛠 icon and **CONFIGURATION MODE** message.

NOTE: The keypad will automatically exit the menu section CONFIGURATION and return to home screen view if 1 minute after the last key-touch expires.

EKB3

The system configuration and control by EKB3 keypad is carried out by activating the Configuration mode using the administrator password (by default – administrator password is **1470**) and entering a valid configuration command using the number keys [0]... [9], [#] key for confirmation and [*] key to cancel the characters that are being entered. Alternatively, the user can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cancelled. When typing in the characters, the indication of each pressed key is provided by short beep of keypad buzzer and red indicators when the number keys [0]... [9] are being pressed. Some commands require [BYPS], [CODE] and [STAY] keys as well. The structure of a standard configuration command is a combination of digits. The commands, which do not require the Configuration mode being activated, are noted. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

NOTE: If you were not willing to activate Configuration mode, but accidentally typed in the * as the first character, please press [*] key again or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cancelled.

Activate/deactivate Configuration mode

EKB3

Enter administrator password:
* aaaa #
Value: *aaaa* – 4-digit administrator password.
Example: **1470#*

The following table provides a list of EKB3 indications, which are relevant during Configuration mode.

Indication	Description
Indicator ARMED flashing	Configuration mode activated successfully.
Indicator SYSTEM flashing	Valid parameter is entered and waiting for valid value to be enetered.
1 long beep	Non-existing command or invalid parameter value entered.
3 short beeps	Command entered successfully.

NOTE: The system can be configured using only one keypad at a time. Other connected keypads will be inactive while the Configuration mode is activated.

NOTE: Configuration mode will automatically deactivate if 1 minute after the last key-stroke expires.

Config Tool

Software *ELDES Configuration Tool* is intended for ESIM264 alarm system configuration via USB port locally or via GPRS connection remotely. This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use *ELDES Configuration Tool* software, please read the user guide provided in the software's HELP section.

Remote System Configuration via GPRS Connection

ATTENTION: The system will NOT send any data to monitoring station while configuring the system remotely via GPRS network. However, during the configuration session, the data messages are queued up and transmitted to the monitoring station after the configuration session is over.

ATTENTION: When the Configuration mode is activated by EKB3 keypad or menu section CONFIGURATION is opened by EKB2 keypad, remote system configuration will be disabled.

NOTE: The keypads will be inactive when the system is being configured remotely.

Before configuring ESIM264 remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM CARD1 slot of ESIM264 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to ESIM264.
- Default SMS password is changed to a new 4-digit password (see **6. PASSWORDS**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).
- APN, user name and password are set up (see **30.2.1. GPRS Network**).

Establishing Remote Connection Between ESIM264 System and Configuration Server

Initiate the connection to ELDES server

In order to activate a remote GPRS connection between ESIM264 system and ELDES configuration server please , send the following SMS text message from user phone number.

Upon the successful SMS text message delivery, the system establishes a connection session for 20 minutes. An SMS reply, containing device IMEI number and confirming a successful connection establishment, is sent shortly.

SMS

SMS text message content:
ssss_STCONFIG
Value: *ssss* – 4-digit new SMS password.
Example: *1111_STCONFIG*

Initiate the connection to third-party server

In case it is necessary to establish a connection between ESIM264 system and a third-party configuration server, send the following SMS text message.

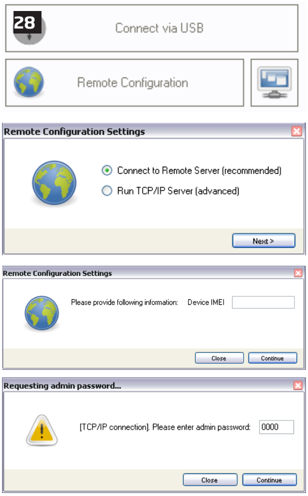
SMS

SMS text message content:
ssss_STCONFIG:add.add.add.add:Port or ssss_STCONFIG:host-name:pprrt
Value: *ssss* - 4-digit SMS password; *add.add.add.add* - public IP address of third-party configuration server; *pprrt* - port number of third-party configuration server, range - [1... 65535]; *host-name* - public host-name of third-party configuration server.
Example: *1111_STCONFIG:62.80.115.102:4522*

NOTE: Public IP address (host-name) and port number are necessary when connecting to a third-party-server for the first time only. When connecting to the server next time, *ssss_STCONFIG* is enough as the IP address (host-name) and port number are saved in the device memory after the first successful connection.

Connecting to ELDES Configuration Server using ELDES Configuration Tool Software

- Run *ELDES Configuration Tool* software.
- Press **Remote Configuration** button.
- In the next window, select **Connect to Remote Server (recommended)** and press **Next** button.
- Enter the received IMEI number in **Device IMEI** entry.
- Press **Continue** button.
- Upon the successfully established connection, the system prompts for an administrator password.
- By entering a valid administrator password, the system grants access to full configuration remotely.
- **Remote Configuration Management** window displays all performed configuration actions.



Remote Configuration Settings

● Connect to Remote Server (recommended)
○ Run TCP/IP Server (advanced)

Remote Configuration Settings

Please provide following information: Device IMEI

Requesting admin password...

[TCP/IP connection]. Please enter admin password: 0000

Ending the Configuration Process

Shut down the Connection with the Server

After the system configuration is complete, use one of the following methods to end the configuration process:

- Press **Disconnect** button and close *ELDES Configuration Tool* software;
- Wait for the system to reply with an SMS text message confirming the end of the session;
- Shut down the connection with the server at any time by sending an SMS text message.

SMS

SMS text message content:
ssss_ENDCONFIG
Value: *ssss* - 4-digit SMS password.
Example: *1111_ENDCONFIG*

6. PASSWORDS

For security reasons, the system uses the following types of passwords:

- **SMS password** – 4-digit password used for system arming/disarming and configuration by SMS text messages. By default, SMS password is 0000, which MUST be changed!
- **Administrator password** – 4-digit password used for Configuration mode activation by keypad and logging in to *ELDES Configuration Tool* software. By default, Administrator password is 1470, which is highly recommended to change.

Set SMS password

SMS

SMS text message content:
wwww_PSW_ssss
Value: *wwww* – 4-digit default SMS password; *ssss* – 4-digit new SMS password; range – [0001... 9999].
Example: *0000_PSW_1111*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → SMS PASSWORD → OK → ssss → OK
Value: *aaaa* – 4-digit administrator password; *ssss* – 4-digit new SMS password; range – [0001... 9999].

EKB3

Enter parameter 14 & new SMS password:
14 ssss #
Value: *ssss* – 4-digit new SMS password; range – [0001... 9999].
Example: *141111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set Administrator password

EKB2

Menu path:
OK → CONFIGURATION → OK → 1470 → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → ADMIN PASSWORD → OK → aaaa → OK
Value: *aaaa* – 4-digit new administrator password; range – [0000... 9999].

EKB3

Enter parameter 16 & new administrator password:
16 aaaa #
Value: *aaaa* – 4-digit new administrator password; range – [0000... 9999].
Example: *162538#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

7. SYSTEM LANGUAGE

The system comes equipped with 2 languages for communication with the user by SMS text messages and a single language for EKB2 keypad menu display. The default EKB2 menu language depends on ESIM264 firmware, which is based on the user's location, while one of languages for communication by SMS text messages is always English.

List of currently available system languages (firmwares):

- Czech
- English
- Estonian
- Finnish
- French
- Greek
- Hungarian
- Icelandic
- Italian
- Latvian
- Lithuanian
- Norwegian
- Portuguese
- Romanian
- Russian
- Slovak
- Spanish
- Swedish

To set a different SMS language, please refer to the following configuration methods.

Set SMS language

SMS

SMS text message content:
ll
Value: *ll* - SMS language, range - [CZ - Czech, EN - English, EE - Estonian, FI - Finnish, GR - Greek, HU - Hungarian, IC - Icelandic, IT - Italian, LV - Latvian, LT - Lithuanian, NO - Norwegian, PT - Portuguese, RO - Romanian, RU - Russian, SK - Slovak, SP - Spanish, SW - Swedish].
Example: *SK*

EKB2

Menu path:
OK → CONFIGURATION → OK → 1470 → OK → PRIMARY SETTINGS → OK → SMS LANGUAGE → OK → sms-lang → OK
Value: *aaaa* – 4-digit new administrator password; range – [0000... 9999]; *sms-lang* – SMS language.

NOTE: To obtain a firmware that features a different SMS and EKB2 menu language, please contact your local dealer.

NOTE: To change the language once the system has already been configured, you need to reset the device to the default configuration. For more details on how to do this, please refer to **35.2. Restoring Default Parameters.**

8. USER PHONE NUMBERS

The system supports up to 5 user phone numbers identified as User 1 through 5. When the phone number is set, the user will be able to arm/disarm the system by SMS text messages and free of charge phone calls (see **12.1. Free of Charge Phone Call** and **12.2. SMS Text Message**) as well as to configure the system by SMS text messages. User phone numbers are also used to receive alarm phone calls and SMS text messages from the system (see **17. ALARM INDICATIONS AND NOTIFICATIONS)**.

By default, the system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number (see **8.2. System Control from any Phone Number**).

To set User 1 phone number is mandatory, while the other 4 are optional. The supported phone number format is the following:

- **International (w/o plus) –** The phone numbers must be entered starting with an international country code in the following format: [international code][area code][local number], example for UK: 4417091111111.

Set user phone number

SMS

SMS text message content:
ssss_NRup:ttteeellnnuumm
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [1... 5]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1111_NR1:4417091111111*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → PHONE NUMBER → OK → ttteeellnnuumm → OK
Value: *aaaa* – 4-digit administrator password; *ttteeellnnuumm* – up to 15 digits user phone number.

EKB3

Enter parameter 17, user phone number slot & phone number:
17 up ttteeellnnuumm #
Value: *up* – user phone number slot, range – [01... 05]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *170144170911111111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View user phone number

SMS

SMS text message content:
ssss_HELPNR
Value: *ssss* – 4-digit SMS password.
Example: *1111_HELPNR*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → PHONE NUMBER → PHONE NUMBER
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user phone number

SMS

SMS text message content:
ssss_NRup:DEL
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [2... 5].
Example: *1111_NR2:DEL*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 2... 5 → OK → PHONE NUMBER → OK → OK
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: NEVER add a phone number of the device's SIM card as a user phone number!

ATTENTION: Once User 1 phone number is set, it will be restricted to modify it only.

NOTE: Multiple user phone numbers can be set by a single SMS text message, **Example**: *1111_NR1:4417091111111_ NR2:4417091111112_ NR5:4417091111113*

NOTE: Multiple user phone numbers can be deleted by a single SMS text message, **Example**: *1111_NR2:DEL_NR3:DEL*

8.1. System Control from any Phone Number

By default, the system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number. To allow/disallow system arming/disarming by phone call and SMS text messages that contain a valid SMS password from any phone number, please refer to the following configuration methods.

Enable system control from any phone number

SMS

SMS text message content:
ssss_STR:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_STR:ON*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 12 & parameter status value:
121#
Example: *121#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable system control from any phone number

SMS

SMS text message content:
ssss_STR:OFF
Value: *ssss* - 4-digit SMS password.
Example: *1111_STR:OFF*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CTRL FROM ANY NUM → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 12 & parameter status value:
12 0 #
Example: *120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

9. DATE AND TIME

The system comes equipped with internal real-time clock (RTC) that keeps track of the current date and time. Once the system is up and running, the user must set the correct date and time, otherwise the system will not operate properly. After shutting down and starting up the system, the date and time must be set again.

Set date and time

SMS

SMS text message content:
ssss_yyyy.mm.dd_hr:mn
Value: *ssss* – 4-digit SMS password; *yyyy* – year; *mm* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59].
Example: *1111_2013.03.16_14:33*

EKB2

Menu path:
a) OK → DATE/TIME SETTINGS → OK →yyyy-mm-dd hr:mn → OK
b) OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → DATE/TIME SETTINGS → OK → yyyy-mm-dd hr:mn → OK
Value: *aaaa* – 4-digit administrator password; *yyyy* – year; *mm* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59].

EKB3

Enter parameter 66, date & time:
66 yyyy mm dd hr mn#
Value: *yyyy* – year; *mm* – month, range – [01... 12]; *dd* – day, range – [01... 31]; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59].
Example: *66201305291235#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When the system is connected to the monitoring station via GPRS network connection (see **30. MONITORING STATION**) and/or when ELDES Smart Security feature is in use (see **35. ELDES Smart Security**), the date and time will be automatically synchronized with the monitoring station or ELDES Smart Security server upon the system startup.

10. USER PASSWORDS

The system supports up to 30 numeric user passwords, identified as User Password 1 through 30, allowing to carry out system arming/disarming by the keypad. By default, User Password 1 is preset as 1111 and assigned to Partition 1. For more details regarding user password partition, please refer to **23.4. User Password Partition**.

Set user password

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (1-16) → OK → USER PASSWORD 1... 16 → OK → PASSWORDS → OK → uuuu → OK

User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PASSWORDS → OK → uuuu → OK

Value: *aaaa* - 4-digit administrator password*; uuuu* - 4-digit user password, range - [0000... 9999].

EKB3

Enter parameter 15, user password slot & user password:
15 us uuuu #

Value: *us* - user password slot, range - [01... 30]; *uuuu* - 4-digit user password; range - [0000... 9999].
Example: *15021111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete user password

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → REMOVE PASSWORD → OK → uuuu → OK

Value: *aaaa* - 4-digit administrator password; *uuuu* - 4-digit user password.

EKB3

Enter parameter 65 & user password:
65 uuuu #

Value: *uuuu* - 4-digit user password.
Example: *651111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Replace user password

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (1-16) → OK → USER PASSWORD 1... 16 → OK → PASSWORD → OK → uuuu → OK

User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PASSWORD → OK → uuuu → OK

Value: *aaaa* - 4-digit administrator password; *uuuu* - 4-digit user password, range - [0000... 9999].

EKB3

Enter parameter 63, existing user password & new user password:
63 vvvv uuuu #

Value: *vvvv* - 4-digit existing user password; *uuuu* - 4-digit new user password, range - [0000... 9999].
Example: *6311113254#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system does not allow to set a duplicate password

One of the user passwords ranging from User Password 1 through 10 can be set as SGS (Security Guard Service) password, which is used for system arming/disarming by a security service employee. When used, the SGS password will be identified by a unique Contact ID code in the monitoring station.

Set SGS password

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → SGS PASSWORD → OK → N/A / us → OK

Value: *aaaa* – 4-digit administrator password; *N/A* – SGS password not in use; *us* – user password slot, range – [1... 10].

EKB3

Enter parameter 74 & user password slot:
74 us #

Value: *us* – user password slot, range – [01... 10].
Example: *7403#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The Duress password is used when system disarming is demanded by force. When used, the system will disarm as well as it will silently transmit an alert to the monitoring station. Only one of the user passwords ranging from User Password 1 through 10 can be set as Duress password.

Set Duress password

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → DURESS PASSWORD → OK → N/A / us → OK

Value: *aaaa* – 4-digit administrator password; *N/A* – Duress password not in use; *us* – user password slot, range – [1... 10].

EKB3

Enter parameter 73 & user password slot:
73 us #

Value: *us* – user password slot, range – [01... 10].
Example: *7309#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

11. iBUTTON KEYS

An iButton key is a unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. ESIM264 system supports up to 5 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.

11.1. Adding and Removing iButton Keys

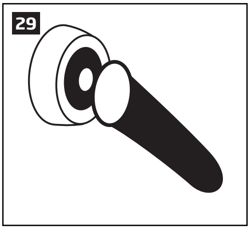
To add an iButton key to the system, do the following:

a) Disarm the system in all partitions (see **12. ARMING AND DISARMING**).

b) Enable Allow Adding New iButton Keys mode.

c) T ouch the key to the iButton key reader when the system is disarmed (see picture below).

29



d) The successfully added iButton key will be indicated by short beeps emitted by the system's buzzer.

e) Add as many iButton keys as necessary – touch one key after another to the reader – until the number of 5 keys is reached.

NOTE: iButton Key 1 can be added without Allow Adding New iButton Keys mode being enabled.

Enable Allow Adding New iButton Keys mode

SMS

SMS text message content:
ssss_IBPROG:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_IBPROG:ON*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 18 & parameter status value:
18 0 #
Example: *180#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When adding of iButton keys is complete, please disable Allow Adding New iButton Keys mode.

Disable Allow Adding New iButton Keys mode

SMS

SMS text message content:
ssss_IBPROG:OFF
Value: *ssss* - 4-digit SMS password.
Example: *1111_IBPROG:ON*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 18 & parameter status value:
18 1 #
Example: *181#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To view the ID of the added iButton keys, please refer to the following configuration methods.

View iButton key ID

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → IBUTTON 1... 5 → OK → ID
Value: *aaaa* - 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If the iButton key is lost or stolen, due to security reasons it is highly recommended to remove it from the system.

Remove individual iButton key from the system

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → IBUTTON 1... 5 → OK → REMOVE → OK
Value: *aaaa* - 4-digit administrator password..

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Remove all iButton keys from the system

SMS

SMS text message content:
ssss_RESETIB
Value: *ssss* - 4-digit SMS password.
Example: *1111_RESETIB*

12. ARMING AND DISARMING

The system features the following methods to carry out arming and disarming process:

- Free of charge phone call.
- SMS text message.
- EKB2/EKB3 keypad and user password.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm-Disarm by Zone.
- EGR100 middle-ware.

The system arms/disarms the partitions that the preset user phone number, EKB2/EKB3 keypad and user password, iButton key, EWK1 wireless keyfob or zone, set up for Arm-Disarm by Zone method, are assigned to. For example, if User 1 phone number is assigned to Partition 0, the user will be able to arm/disarm Partition 0 by a single phone call to the system (see **23. PARTITIONS**).

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message. For more details on SMS text message regarding system arming/disarming and how to manage it, please refer to **12.9. Disabling and Enabling Arm/Disarm Notifications**.

The system will allow to arm the system if the following system faults are present (see **29. INDICATION OF SYSTEM FAULTS**):

- Main power supply is lost.
- Low battery.
- Battery failed.
- Date/time not set.
- GSM connection failed.

When attempting to arm the system (by any method, except EKB2/EKB3 keypad and user password, EGR100 middle-ware) in case of violated zone/tamper presence, the system will reply with SMS text message containing violated zone/tamper number. Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system. For more details on how to arm the system despite the violated zone presence, please refer to **14.6. Zone Attributes** and **14.7. Bypassing and Activating Zones**

The system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number. For more details regarding arming/disarming the system from a non-preset phone number, please refer to **8.1. System Control from any Phone Number.**

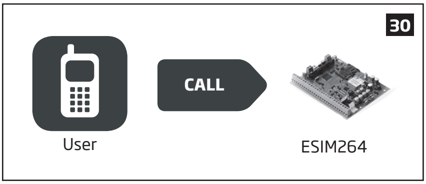
12.1. Free of Charge Phone Call

To arm and disarm the system, dial the system's phone number from any of 5 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). The phone call is free charge as the system rejects it and carries out arming/disarming procedure afterwards. When arming – the system rejects the phone call after 2 rings, when disarming – the system rejects the phone call immediately. If there is more than one preset user dialing to the system at the same time, the system will accept the incoming call from the user who was the first to dial while other user (-s) will be ignored.

When system's phone number is dialed for arming, the system will proceed as follows:

- Non-partitioned system:
    - If ready (no violated zone/tamper), the system will arm.
    - If unready (violated zone/tamper is present), the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.
- Partitioned system:
    - If all partitions are disarmed ready, the system will arm them.
    - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
    - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

The system will arm/disarm the partition corresponding to the one that the user phone number is assigned to. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition.**



12.2. SMS Text Message

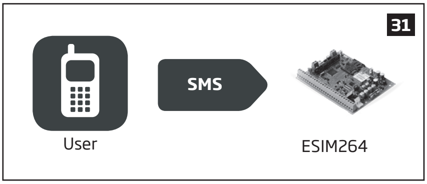
SMS

To arm the system by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). When the SMS text message for arming is sent to the system's phone number, the system will proceed as follows:

- Non-partitioned system:
  - If ready (no violated zone/tamper), the system will arm.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number.
- Partitioned system:
  - If all partitions are disarmed ready (no violated zone/tamper), the system will arm them.
  - If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). The system will then send an SMS text message, containing a list of violated zones/tampers, to user phone number that the system arming was initiated from.
  - If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones.

Arm the system

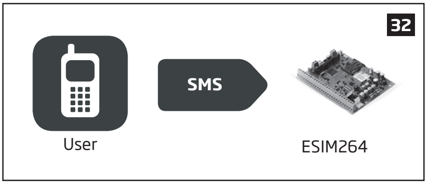
SMS text message content:
ssss_ARMp or ssss_ARMp,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1 – Partition 0, 2 – Partition 1].
Example: *1111_ARM1*



To disarm the system by SMS text message, send the following text to the system's phone number from any of 10 available user phone numbers:

Disarm the system

SMS text message content:
ssss_DISARMp or ssss_DISARMp,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, [1 – Partition 0, 2 – Partition 1].
Example: *1111_DISARM1,2*



Regardless of the partition a user phone number is assigned to, the user will be able arm/disarm by SMS text message method either Partition 0 , Partition 1 or both partitions simultaneously.

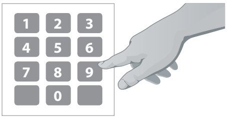
12.3. EKB2 Keypad and User Password

EKB2

READY message displayed in the home screen view by EKB2 keypad indicates that no violated zones and/or tampers are present, therefore the system can be armed. If the message is displayed as **NOT READY**, the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**). To arm the system by EKB2 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad (see **10. USER PASSWORDS** for user password management).

By default when a valid user password is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the keypad will display 🏃 icon next to the countdown timer. When the system is successfully armed, the keypad will display 🔒 icon for 5 seconds and switch to home screen view.

Arm the system



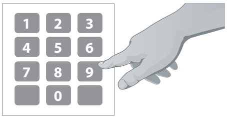
Enter user password:
uuuu → OK
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.
Example: *1111 → OK*

To cancel the system arming process, enter the user password again during exit delay countdown.

To disarm the system by EKB2 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad. By default, the system disarming process is as follows:

- To disarm the system by EKB2 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad. When a valid user password is entered, the keypad will display 🔓 icon for 3 seconds and switch to home screen view.

Disarm the system



Enter user password:
uuuu → OK
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.
Example: *1111 → OK*

The system will arm/disarm the partition corresponding to the one that user password and the keypad are assigned to. For example, if EKB2 keypad and user password is assigned to Partition 1, the user will be able to arm/ disarm only Partition 1. For more details on how to set user password and keypad partition, please refer to **23.4. User Password Partition** and **23.3. Keypad Partition and Keypad Partition Switch respectively.**

To arm/disarm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled) before arming/disarming process. For more details on keypad partition switch and how to enable it, please refer to **23.3. Keypad Partition and Keypad Partition Switch.**

Use keypad partition switch

Menu path:
P1 → [p] part-name → OK
Value: *part-name* – up to 15 characters partition name.

NOTE: If the user fails to enter a correct user password 10 times in a row, the system will block the keypad for 2 minutes and the keypad will display **KEYPAD BLOCKED** message. While the keypad is blocked, the system prevents from entering any user password. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

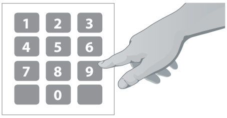
12.4. EKB3 Keypad and User Password

EKB3

Illuminated indicator READY on EKB3 keypad indicates that no violated zones and/or tampers are present, therefore the system can be armed. If the indicator is not illuminated, the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).

To arm the system by EKB3 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad (see **10. USER PASSWORDS** for user password management). By default, when a valid user password is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

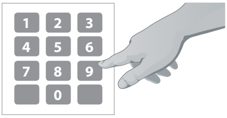


Enter user password:
uuuu
Value: *uuuu* – 4-digit user password.
Example: *1111*

To cancel the system arming process, enter the user password again during exit delay countdown.

To disarm the system by EKB3 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad. When a valid user password is entered, EKB3 keypad indicator ARMED will light OFF.

Disarm the system



Enter user password:
uuuu
Value: *uuuu* – 4-digit user password.
Example: *1111*

The system will arm/disarm the partition corresponding to the one that user password and the keypad are assigned to. For example, if EKB3 keypad and user password is assigned to Partition 0, the user will be able to arm/ disarm only Partition 0. For more details on how to set user password and keypad partition, please refer to **23.4. User Password Partition** and **23.3. Keypad Partition and Keypad Partition Switch respectively.**

To arm/disarm a different partition than the keypad is assigned to, use keypad partition switch feature (by default – disabled) to switch the keypad to a different partition before arming/disarming process. For more details on keypad partition switch and how to enable it, please refer to **23.3. Keypad Partition and Keypad Partition Switch.**

Use keypad partition switch

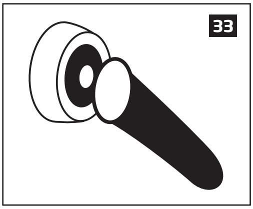
Hold the [*] key, release it after 3 short beeps & enter partition number:
* p
Value: p – partition number, range – [0... 1]
Example: **1*

NOTE: By default, User Password 1 is preset as **1111** and assigned to Partition 0.

12.5. iButton Key

To arm or disarm the system, touch the iButton key reader by any of 5 available iButton keys (see **11. iBUTTON KEYS** for iButton key management). When the iButton is touched to the iButton key reader for arming, the system will proceed as follows:

- If ready (no violated zone/tamper), the system will initiate exit delay and arm.
- If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones**) or a Force attribute enabled (see **14.6. Zone Attributes**).


33

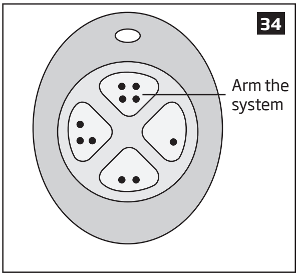
The system will arm/disarm the partition corresponding to the one that the iButton key is assigned to. For more details on how to set iButton key partition, please refer to **23.5. iButton Key Partition.**

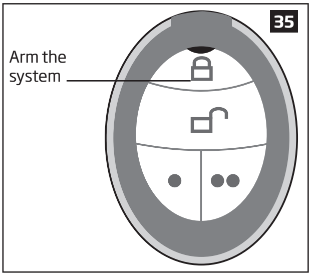
12.6. EWK1/EWK2 Wireless Keyfob

EWK1/ EWK2

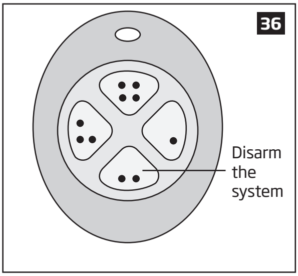
To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 – ∷ ;EWK 2 - 🔒). When EWK1/ EWK2 button is pressed for arming, the system will proceed as follows:

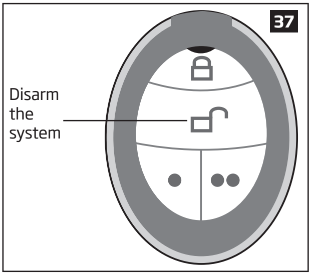
- If ready (no violated zone/tamper), the system will initiate exit delay and arm.
- If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **14.7. Bypassing and Activating Zones**), disabled (see **14.9. Disabling and Enabling Zones)** or a Force attribute enabled (see **14.6. Zone Attributes**).


34


35

To disarm the system, press 1 of 4 keyfob buttons set to disarm the system (by default, EWK1 - •• ; EWK2 - 🔓).


36


37

The system will arm/disarm the partition corresponding to the one that EWK1/EWK2 wireless keyfob is assigned to (see **23.6. EWK1/ EWK2 Wireless Keyfob Partition**). For example, if EWK1/EWK2 wireless keyfob is assigned to Partition 1, the user will be able to arm/ disarm only Partition 1. To arm a different partition than the EWK1/EWK2 wireless keyfob is assigned to, bind another EWK1/EWK2 keyfob to the system and assign it to a different partition.
For more details on how to manage EWK1/EWK2 keyfob buttons, please refer to *ELDES Configuration Tool* software's HELP section.

12.7. Arm-Disarm by Zone

ARM/ DISARM ZONE

The Arm-Disarm by Zone feature allows to use a zone for arming and disarming the alarm system when the zone is violated and restored. The process is performed by providing a low-level pulse for more than 3 seconds into the specified zone. It means that violating and restoring the zone leads to system arming and by repeating this action the system becomes disarmed. The system will arm/disarm the partition (-s) that the zone is assigned to. This method can be set up for one on-board zone only.

Set zone for Arm-Disarm by Zone method

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → ZONE 1... 12 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 34 & on-board zone number:
34 nn #
Value: *nn* – on-board zone number, range – [01... 12].
Example: *3403#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Arm-Disarm by Zone method

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ARM/DISARM BY ZONE → OK → N/A → OK
Value: aaaa – 4-digit administrator password.

EKB3

Enter parameter 34 & parameter status value
34 00 #
Example: *3400#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

12.8. Disabling and Enabling Arm/Disarm Notifications

By default, when the system is successfully armed or disarmed, it replies with confirmation by SMS text message to:

- user phone number, sharing the same partition as EKB2/EKB3 keypad and user password, iButton key, EWK1/EWK2 wireless keyfob or zone, set up for Arm/Disarm by Zone method.
- user phone number that the system arming/disarming by free of charge phone call was initiated from.
- user phone number that the system arming/disarming by SMS text message was initiated from.

The confirmation SMS text message is sent to the user phone number regarding each partition separately and contains system status and partition name.

To disable/enable this notification for individual user phone number, please refer to the following configuration methods.

Disable arm/disarm notification for individual user phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → SEND ARM/DARM SMS → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 75, user phone number slot & parameter status value:
75 us 0 #
Value: *us* – user phone number slot, range – [01... 05].
Example: *75030#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable arm/disarm notification for individual user phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → SEND ARM/DARM SMS → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 75, user phone number slot & parameter status value:
75 us 1 #
Value: *us* - user phone number slot, range - [01... 05].
Example: *75041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, the system sends SMS text message only to the first available user phone number when the system is successfully armed/disarmed. If the system did not receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number. To ignore the SMS delivery report and allow/disallow the system to send the SMS text message to every preset user phone number, please refer to the following configuration methods.

Enable arm/disarm notification for all preset user phone numbers

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → SEND ARM/DARM ALL → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 22 & parameter status value:
22 1 #
Example: *221#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable arm/disarm notification for all preset user phone numbers

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → SEND ARM/DARM ALL → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 22 & parameter status value:
22 0 #
Example: *220#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

13. EXIT AND ENTRY DELAY

When arming, the system initiates the exit delay countdown (by default – 15 seconds) intended for the user to leave the secured area. The exit delay is indicated by short beeps emitted by EKB2/EKB3 keypad buzzer and buzzer, connected to the alarm system. in addition, when arming by EKB2 keypad, 🏃 icon will be displayed next to the countdown timer on keypad screen during exit delay.

- a non-partitioned system, 🏃 icon will be displayed next to the countdown timer on EKB2 keypad screen during exit delay.
- a partitioned system, EKB2 keypad will display **ARMING part-name** message on the screen for 3 seconds and switch to partition selection menu during exit delay.

Exit delay is provided when arming the system by the following methods:

- EKB2/EKB3 keypad and user password.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm/Disarm by Zone.

To arm the system without exit delay, use one of the following system arming methods:

- Free of charge phone call.
- SMS text message.
- EGR100 middle-ware.

Set exit delay

SMS

SMS text message content:
ssss_EXITDELAY:ext
Value: *ssss* – 4-digit SMS password; *ext* – exit delay duration, range – [0... 600] seconds.
Example: *1111_EXITDELAY:20*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → EXIT DELAY → OK → ext → OK
Value: *aaaa* – 4-digit administrator password;, *ext* – exit delay duration, range – [0... 600] seconds.

EKB3

Enter parameter 72 & exit delay duration:
72 ext #
Value: *ext* – exit delay duration, range – [0... 600] seconds.
Example: *72259#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Alternatively, you can set exit delay value to 0 in order to arm the system without exit delay by any available method.

Once the exit delay has expired, the system initiates the entry delay countdown (by default – 15 seconds) if a Delay type zone is violated. The countdown is indicated by short beeps emitted by keypad buzzer and by steady beep emitted by system's buzzer. The indication is intended to advise the user that the system should be disarmed. Once the user presses/touches any key on the keypad during this delay, the buzzer of the keypad will be silenced. If the system is disarmed before the entry delay expires, no alarm will be caused.

Set entry delay for Delay zone

SMS

SMS text message content:
ssss_ENTRYDELAY:nn,eeeee or ssss_ENTRYDELAY:nn,eeeee;nn,eeeee;nn,eeeee;nn,eeeee

Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 44], *eeeee* – entry delay duration, range – [0... 65535] seconds.
Example: *1111_ENTRYDELAY:1,25;14,32;12,20*

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → ENTRY DELAY → OK → eeeee → OK

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → ENTRY DELAY → OK → eeeee → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → ENTRY DELAY → OK → eeeee → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → ENTRY DELAY → OK → eeeee → OK

Value: *aaaa* – 4-digit administrator password; *eeeee* – entry delay duration, range – [0... 65535] seconds.

EKB3

Enter parameter 54, partition number and entry delay duration:
54 nn eeeee #

Value: *nn* – zone number, range – [01... 44], *eeeee* – entry delay duration, range – [0... 65535] seconds
Example: *5403259#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on zone types, please refer to **14.5. Zone Type Definitions**.

14. ZONES

Detection devices such as motion detectors and door contacts are connected to the alarm system's zone terminals. Once connected, the associated zone's parameters must be configured.

ESIM264 comes equipped with 6 on-board zones allowing to connect up to 6 detection devices. For more details regarding zone expansion, please refer to **14.2. Zone Expansion**.

ESIM264 zones are classified by 5 categories:

Zone category	Description	Max. number of zones per device	Max. number of zones in total
On-board zones	Built-in wired zones of ESIM264 alarm system.	6/12*	6/12*
Keypad zones	Hardwired zones of EKB2/EKB3 keypad.	1	4
EPGM1 zones	Zones of EPGM1 - hardwired zone & PGM output expansion module.	16	16
Wireless zones	Non-physical zones automatically created by connected wireless devices.	2**	32***
Virtual zones	Non-physical zones intended for Panic button feature (alarm activaton upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using *ELDES Configuration Tool* software.	32****	32****

* - 6-Zone mode is enabled by default. ATZ mode doubles the on-board zone number and increases it to 12 in total.
** - Depends on the connected wireless device.
*** - Available only if no zones, EPGM1 zones and virtual zones are present.
**** - Available only if no zones, EPGM1 zones and wireless zones are present.

14.1. Zone Numbering

The zone numbers ranging from Z1 through Z12 are permanently reserved for on-board zones even when ATZ mode is disabled. The Z13-Z44 zone numbers are automatically assigned in the chronological order to the created virtual zones and the devices connected to the system: keypads, wireless devices, EPGM1 modules.

14.2. Zone Expansion

For additional detection device connection, the number of zones can be expanded by:

- enabling the ATZ (Advanced Technology zone) mode (see **14.4. ATZ (Advanced Technology Zone) Mode**).
- connecting EPGM1 hardwired zone and PGM output expansion module (see **31.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module).**
- connecting keypads (see **31.1.1. EKB2 - LCD Keypad** and **31.1.2. EKB3 - LED Keypad**).
- binding wireless devices (see **19. WIRELESS DEVICES**).
- creating virtual zones (see *ELDES Configuration Tool* software's Help section).

The maximum supported number of zones is 44.

14.3. 6-Zone Mode

By default, ESIM264 alarm system runs in the 6-Zone mode under zone connection Type 1 allowing to connect up to 6 detection devices of NO (normally-open) type to the on-board zone terminals as indicated in the wiring diagram of Type 1. Once a different zone connection type is set, the detection device wiring must be done according to the wiring diagram of the associated type. Available zone connection types for the 6-Zone mode:

- **Type 1** – Parallel wiring of NO (normally-open) detection device with 5,6kΩ EOL (end-of-line) resistor.
- **Type 2** – Serial wiring of NC (normally-closed) detection device with 5,6kΩ EOL resistor.
- **Type 3** – Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and NC (normally-closed) detection device with 3,3kΩ EOL resistor.

For zone wiring diagrams of the 6-Zone mode, please refer to **2.3.2. Zone Connection Types**.

Set zone connection type for 6-Zone mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ZONE TYPE:6-ZONE M → OK → TYPE 1... 3 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 39 & number of zone connection type:
391# - Type 1
392# - Type 2
393# - Type 3
Example: *392#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

14.4. ATZ (Advanced Technology Zone) Mode

The ATZ mode is a software-based feature that doubles the number of on-board zones and enables two detection devices to be installed per 1 zone terminal. Once this mode is enabled, the zone connection Type 4 is set automatically. The detection devices must be wired to the on-board zone terminals as indicated in the wiring diagram of the associated zone connection type. Available zone connection types for the ATZ mode:

- **Type 4** – Parallel wiring of 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL (end-of-line) resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.
- **Type 5** – Combination of serial and parallel wiring of tamper with 5,6kΩ EOL resistor and 2 NC (normally-closed) detection devices with 5,6kΩ and 3,3kΩ EOL resistors respectively. 5,6kΩ EOL resistor corresponds to zones ranging from Z1 through Z6, while 3,3kΩ EOL resistor corresponds to zones ranging from Z7 through Z12.

For zone wiring diagrams of the ATZ mode, please refer to **2.3.2. Zone Connection Types**.

Enable ATZ mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ATZ MODE → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 28 & parameter status value:
281#
Example: *281#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable ATZ mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ATZ MODE → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 28 & parameter status value:
280#
Example: *280#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set zone connection type for ATZ mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ZONE TYPE:ATZ MODE → OK → TYPE 4... 5 → OK

Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 38 & number of zone connection type:

381# - Type 4

382# - Type 5

Example: *381#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The ATZ mode applies to on-board zones only when enabled.

14.5. Zone Type Definitions

- **Interior Follower -** The zone can be violated during exit and entry delay without causing an alarm. If the zone is violated before the entry delay has begun, it will cause an instant alarm followed by single notification delivery even if the zone has been violated multiple times or another Interior Follower-type zone has been violated while alarm period (by default - 1 minute) is in progress. The zone is used where violating a zone during exit/entry delay is unavoidable. Typically, this zone is used for indoor protection devices, such as motion detectors, installed close to the exit/entry doors.
- **Instant** - The alarm is instantly caused if this zone is violated when the system is armed or during entry delay. This zone type is usually used for doors, windows or other zones, and shock detectors.
- **24-Hour** - When the system is either armed or disarmed, the zone will cause instant alarm if violated. Normally, this type of zone is used for securing the areas that require constant supervisory.
- **Delay -** This zone type can be violated during exit and entry delay without causing an alarm. If the zone is violated when the system is armed, it will initiate entry delay countdown intended for the user to disarm the system. If the zone is left violated after the exit delay expires, it will cause an instant alarm. If one more zone with Stay-enabled attribute exist and the Delay-type zone is not violated and restored during exit delay, the system will be armed in Stay mode (see **15. STAY MODE**). Typically, this zone type is used for door contacts installed at designated exit/entry doors.
- **Fire** - If this zone type is violated when the system is either armed or disarmed, the alarm will be instantly caused and the siren/bell will emit pulsating sound. Typically, this zone type is used for flame and smoke detectors.
- **Panic/Silent** - This zone operates the same as 24-Hour zone type, but the system will not activate the siren/bell and keypad buzzer if violated. Normally, this zone type used for panic alarm buttons.

Set zone type for individual zone

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WLESS ZONE 1... 16 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/SILENT → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → TYPE → OK → INTERIOR FOLLOWER | INSTANT | 24-HOUR | DELAY | FIRE | PANIC/ SILENT → OK

Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 53, zone number & zone type number:

53 nn 1 # - Interior Follower

53 nn 2 # - Instant

53 nn 3 # -24-Hour

53 nn 4 # - Delay

53 nn 5 # - Fire

53 nn 6 # - Panic/Silent

Value: *nn* - zone number, range - [01... 44]
Example: *53125#*

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: The system will NOT activate siren/bell and keypad buzzer only when Panic/Silent zone type is violated.

14.6. Zone Attributes

- **Stay** – If this attribute is enabled, the zone, regardless of type, will not cause an alarm if violated when the system is Stay armed. For more details on arming the system in the Stay mode, please refer to **15. STAY MODE**.
- **Force** – This attribute determines whether the system can be armed or not while a zone is violated. If a zone with the Force attribute enabled is left violated until the exit delay expires, it will be ignored. Once the system is armed and the zone is restored, the violation will not be ignored and the zone will operate according to the determined type. For more details on zone types, please refer to **14.5. Zone Type Definitions**.
- **Delay, ms** – This attribute determines the zone sensitivity level by delay time (By default – 800 milliseconds). If a zone is left triggered until the delay time expires, the zone is considered violated.
- **Delay becomes Instant in Stay mode** – This attribute determines whether or not any Delay type zone will operate as Instant type zone when the system is armed in the Stay mode. When the system is fully armed, the Delay type zone will operate normally. For more details on Delay and Instant zone types, please refer to **14.5. Zone Type Definitions**.
- **Chime** – This feature is used to emit 3 short beeps from the keypad buzzer and display 🚪 icon on EKB2 keypad screen whenever any Delay type zone is violated. Typically, the feature is used for designated exit/entry doors to indicate the opening of the doors.
- **Alarm count to bypass** – This attribute determines a number of times the zone can be violated until it is automatically bypassed. For more details on zone bypassing and how to activate a bypassed zone, please refer to **14.7. Bypassing and Activating Zones.**

Enable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → ENABLE → OK

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → STAY → OK → ENABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → STAY → OK → ENABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → STAY → OK → ENABLE → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 56, zone number & parameter status value:
56 nn 1 #

Value: *nn* – zone number, range – [01... 44].
Example: *56041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Stay attribute for individual zone

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STAY → OK → DISABLE → OK
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → STAY → OK → DISABLE → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → STAY → OK → DISABLE → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → STAY → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 56, zone number & parameter status value:
56 nn 0 #
Value: *nn* – zone number, range – [01... 44].
Example: *56190#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → ENABLE → OK
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → FORCE → OK → ENABLE → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → FORCE → OK → ENABLE → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → FORCE → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 82, zone number & parameter status value:
82 nn 1 #
Value: *nn* – zone number, range – [01... 44].
Example: *82061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Force attribute for individual zone

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → FORCE → OK → DISABLE → OK
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → FORCE → OK → DISABLE → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → FORCE → OK → DISABLE → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → STAY → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 82, zone number & parameter status value:
82 nn 0 #
Value: *nn* – zone number, range – [01... 44].
Example: *82110#*

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set Delay, ms atrribute

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable/disable Delay becomes Instant in Stay mode attribute

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Chime attribute

EKB2

Menu path:
OK → CONFIGURATION → OK →aaaa → OK → ZONES → OK → CHIME → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 32 & parameter status value:
32 0 #
Example: *320#*

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Chime attribute

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → CHIME → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 32 & parameter status value:
32 1 #
Example: *321#*

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set Alarm count to bypass attribute for individual zone

Config Tool | This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

14.7. Bypassing and Activating Zones

ATTENTION: Zone bypassing and activation must be carried out without Configuration mode being activated by the EKB3 keypad.

Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. When a zone is bypassed, EKB3 keypad indicator **BYPS** will light ON and EKB2 keypad will display **BYP** message in the home screen view.

Bypass individual violated zone

EKB2

Menu path:
OK → BYPASS → OK → BYPASS LIST 1... 3 → OK → Z1-zone-name... Z44-zone-name → OK → BYPASS → OK K
Value: *zone-name* - up to 24 characters zone name.

EKB3

Press the [BYPS] key, enter zone number & user password:
BYPS nn uuuu #
Value: *nn* – zone number, range – [01... 44]; *uuuu* – 4-digit user password.
Example: *BYPS091111#*

Bypass all violated zones

EKB2

Menu path:
OK → BYPASS → OK → BYP VIOLATED ZONES → OK

The zone will stay bypassed until the system is disarmed. Once the system is disarmed, the corresponding zone state will be indicated on the keypads (see **31.1.1. EKB2 - LCD Keypad** and **31.1.2. EKB3 - LED Keypad**) and Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS)**. Alternatively, the user can activate the bypassed zone by the following configuration methods.

Activate bypassed zone

EKB2

Menu path:
OK → BYPASS → OK → BYPASS LIST 1...3 → OK → Z1-zone-name... Z44-zone-name → OK → UNBYPASS → OK
Value: *zone-name* - up to 24 characters zone name.

EKB3

Press the [BYPS[key, enter zone number & user password:
BYPS nn uuuu #
Value: *nn* – zone number, range – [01... 44]; *uuuu* – 4-digit user password.
Example: *BYPS251111#*

NOTE: Zones can only be bypassed and activated when the system is not armed.

14.8. Zone Names

Each zone has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined zone terminal, for **Example:** Kitchen doors opened. The zone names are used in SMS text messages that are sent to the user during alarm. the By default, the zone names are: *Z1 – Zone1, Z2 – Zone2, Z3 – Zone3, Z4 – Zone4 etc.*

Set zone name

SMS

SMS text message content:
ssss_Znn:zone-name
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 44]; *zone-name* – up to 24 characters zone name.
Example: *1111_Z3:Door sensor triggered*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View zone names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS*

EKB2

EKB2:
Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → NAME

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → NAME

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → NAME

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → NAME

Value: *aaaa* - 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in zone names

NOTE: Multiple zone names can be set by a single SMS text message, **Example:** *1111_Z1:Kitchen doors opened;Z3:Movement in basement;Z4:Bedroom window opened*

14.9. Disabling and Enabling Zones

By default, all zones, except keypad and virtual zones, are enabled. To permanently disable/enable an individual zone, please refer to the following configuration methods.

Disable zone

SMS

SMS text message content:
ssss_Znn:OFF

Value: *ssss* - 4-digit SMS password; *nn* - zone number, range - [1... 44].
Example: *1111_Z13:OFF*

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → DISABLE → OK

Wireless zone: OK → CONFIGURATION → STATUS → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → STATUS → OK → DISABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → STATUS → DISABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → STATUS → DISABLE → OK

Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 52, zone number & parameter status value:
52 nn 0 #

Value: *nn* - zone number, range - [01... 44].
Example: *52360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable zone

SMS

SMS text message content:
ssss_Znn:ON
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 44].
Example: *1111_Z6:ON*

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → STATUS → OK → ENABLE → OK
Wireless zone: OK → CONFIGURATION → STATUS → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → STATUS → OK → DISABLE → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → STATUS → DISABLE → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → EPGM1 ZONE 1... 16 → OK → STATUS → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 52, zone number & parameter status value:
52 nn 1 #
Value: *nn* – zone number, range – [01... 44].
Example: *52151#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

15. STAY MODE

Stay mode allows the user to arm and disarm the alarm system without leaving the secured area. If the zones with Stay attribute enabled are violated when the system is Stay armed, no alarm will be caused. Typically, this feature is used when arming the system at home before going to bed.

The system can be Stay armed under the following conditions:

- If a zone with Stay attribute enabled is NOT violated during exit delay, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay. For more details on these methods, please refer to **13. EXIT AND ENTRY DELAY.**
- The system will instantly arm in Stay mode when using one of the following methods.

Arm the system in Stay mode

EKB2

Menu path:
P2 → uuuu → OK
Value: *uuuu* – 4-digit user password.

EKB3

Press the [STAY] key & enter user password:
STAY uuuu
Value: *uuuu* – 4-digit user password.
Example: *STAY1111*

When the system is successfully armed in Stay mode, EKB2 keypad will display **STAY** message in the home screen view.

ATTENTION: System arming in Stay mode by the keypad must be carried out without Configuration mode being activated.

NOTE: The system can be armed in Stay mode, only if there is at least one zone with Stay attribute enabled.

NOTE: Stay mode is not supported by virtual zones.

For more details on how to enable Stay attribute for zone, please refer to **14.6. Zone Attributes**.

16. TAMPERS

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren/bell and the keypad buzzer and send the SMS text message to the preset user phone number. The system will cause tamper alarm under the following conditions:

- If the enclosure of a detection device, siren/bell, metal cabinet or keypad is opened, the physical tamper switch will be triggered. By default, indicated as *Tamper x* in the SMS text message (x = tamper number).
- If the wireless signal is lost due to low signal level or low battery power on a certain wireless device and does not restore during 20 minute period. This event is identified as Wireless Signal Loss. By default, indicated as *Tamper x* * in the SMS text message (x = tamper number; * = wireless signal loss).

By default, tamper alarm notification by SMS text message is enabled. To disable/enable tamper alarm notification, please refer to the following configuration methods.

Disable tamper alarm notification

EKB2

Menu path:
Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → DISABLE → OK
Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → WLESS SIGN LOSS EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 08 0 # - Tamper alarm
25 11 0 # - Wireless signal loss
Example: *25110#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable tamper alarm notification

EKB2

Menu path:
Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → ENABLE → OK
Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → WLESS SIGN LOSS EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 08 1 # - Tamper alarm
25 11 1 # - Wireless signal loss
Example: *25081#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on how to view violated tamper, please refer to **17. ALARM INDICATIONS AND NOTIFICATIONS**

16.1. Tamper Names

Each tamper has a name that can be customized by the user. The tamper names are used in SMS text messages that are sent to the user during the tamper alarm. By default, the tamper names are: *Tamper 1, Tamper 2, Tamper 3, Tamper 4 etc*. To set a different tamper name, please refer to the following configuration methods.

Manage tamper name

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

17. ALARM INDICATIONS AND NOTIFICATIONS

When a zone, depending on zone type (see **14.5. Zone Type Definitions**), or tamper is violated, the system will cause an alarm. By default, the alarm duration is 1 minute (see **20. SIREN/BELL** regarding the alarm duration). During the alarm, the system will follow this pattern:

1. The system activates the siren/bell and the keypad buzzer.

a) The siren/bell will emit pulsating sound if the violated zone is of Fire type, otherwise the sound will be steady.

b) The keypad buzzer will emit short beeps.

c) Depending on violated zone type, EKB2 keypad will display **BURGLARY ALARM** message followed by one of the alarm messages in the home screen view:

- **ALARM.**
- **FIRE ALARM.**
- **24H ALARM.**

d) During the tamper alarm, EKB2 keypad will display **TAMPER ALARM** message in the home screen view.

e) If one or more zones are violated, EKB3 will light ON the corresponding violated zone indicator (-s) ranging from 1 through 12. Indicator SYSTEM will flash if one or more high-numbered zones are violated. If one or tampers are violated, indicator SYSTEM will light ON. For more details on viewing violated high-numbered zone and tamper numbers by EKB3 keypad, please refer to **29. INDICATION OF SYSTEM FAULTS.**

2. The system attempts to send an SMS text message, containing the violated zone/tamper name (see **14.8. Zone Names** on how to set a zone name), to the first preset user phone number, sharing the same partition as the violated zone/tamper. The system will send SMS text messages regarding each violated zone/tamper separately.

a) If the user phone number is unavailable and the system fails to receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

b) The system will continue sending the SMS text message to the next preset user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

3. If enabled, the system attempts to ring the first user phone number, sharing the same partition as the violated zone/tamper. The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the user will be able to listen on the mobile phone for approx. 30 seconds to what is happening in the area, surrounding the alarm system. This feature will be available only if a microphone is connected to the system (see **25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION**).

b) The system will dial the next preset user phone number, assigned to the same partition, if the previous user was unavailable due to the following reasons:

- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided "busy" signal.
- user did not answer the call after several rings, predetermined by the GSM operator.

c) The system will continue dialing the next preset user phone numbers in the priority order until one is available. The system dials only once and will not return to the first user phone number if the last one was unavailable.

d) The system will not dial the next preset user phone number if the previous one was available, but rejected the phone call.

To silent the siren/bell as well as to cease system phone calls and SMS text message sending to the user phone numbers, please disarm the system (see **12. ARMING AND DISARMING**).

View violated zones

SMS

SMS text message content:
ssss_INFO
Value: *ssss - 4-digit SMS password.*
Example: *1111_INFO*

EKB2

Menu path:
OK → VIOLATED ZONES → OK → ZONE 1... 44

EKB3

Please, refer to illuminated zone indicators ranging from 1 through 12 on the keypad. The flashing indicator SYSTEM stands for violated high-numbered zones (Z13-Z44). For more details on violated high-numbered zone indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View violated tampers

SMS

The systemwill automatically send an SMS text message, containing a violated tamper name, to user phone number.

EKB2

Menu path:
OK → VIOLATED TAMPERS → OK → TAMPER 1... 44

EKB3

The illuminated indicator SYSTEM stands for system fault presence including violated tamper. For more details on violated tamper indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

For more details details on how to disable/enable SMS text messages and phone calls to preset user phone number in case of alarm, please refer to **17.1. Enabling and Disabling Alarm Notifications**

ATTENTION: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. Monitoring Station**).

NOTE: If one or more zones/tampers are violated during the alarm, the system will attempt to send as many SMS text message and dial the user phone number as many times as the zone/tamper was violated.

NOTE: If the system sent the SMS text message and/or dialed the user phone number after disarming the system, it means that the SMS text message and/or phone call was queued up in the memory before the system was disarmed

17.1. Enabling and Disabling Alarm Notifications

By, default the system will ring the preset user phone numbers in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable call in case of alarm

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 30 & parameter status value:
30 1#
Example: *301#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable call in case of alarm

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → CALL IN CASE ALARM → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 30 & parameter status value:
30 0#
Example: *300#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By, default the system will send SMS text message to preset user phone numbers in case of alarm. To disable/enable this feature, please refer to the following configuration methods.

Disable SMS text message in case of alarm

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ALARM EVENT → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 0310 #
Example: *25010#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable SMS text message in case of alarm

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ALARM EVENT → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 01 1 #
Example: *25011#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, the system sends SMS text message to the first available user in case of alarm. If the system did not receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number. To ignore the SMS delivery report and allow/disallow the system to send the SMS text message to every preset user phone number, please refer to the following configuration methods.

Enable SMS text message to all preset user phone numbers in case of alarm

SMS

SMS text message content:
ssss_SMSALL:ON
Value: *ssss* - 4-digit SMS password
Example: *1111_SMSALL:ON*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → SEND ALARM SMS ALL → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 21 & parameter status value:
21 1 #
Example: *211#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable SMS text message to all preset user phone numbers in case of alarm	**SMS**	**SMS text message content:** ssss_SMSALL:OFF **Value:** *ssss* - 4-digit SMS password **Example:** *1111_SMSALL:OFF*
	EKB2	**Menu path:** OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → SEND ALARM SMS ALL → OK → DISABLE → OK **Value:** *aaaa* - 4-digit administrator password.
	EKB3	**Enter parameter 21 & parameter status value:** 21 0 # **Example:** *210#*
	Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, tamper alarm notification by SMS text message is enabled. For more details on how to disable/enable tamper alarm notification, please refer to **16. TAMPERS**.

ATTENTION: Regardles of the Call in Case of Alarm parameter status, the system will NOT ring the preset user phone number if the system is connected to the monitoring station (see **30. MONITORING STATION**) and/or when ELDES Smart Security feature is in use (see **35. ELDES Smart Security**).

18. PROGRAMMABLE (PGM) OUTPUTS

A PGM output is a programmable output that toggles to its set up state when a specific event has occurred in the system, the scheduled weekday and time has come or if the user has initiated the PGM output state change manually. Normally, PGM outputs can be used to open/close garage doors, activate lights, heating, watering and much more. When a PGM output turns ON, the system triggers any device or relay connected to it.

ESIM264 comes equipped with four open-collector PGM outputs allowing to connect up to four devices or relays. For more details on PGM output expanding, please refer to **18.2. PGM Output Expansion**.

ESIM264 PGM outputs are classified by 4 categories:

PGM output category	Description	Max. number of PGM outputs per device	Max. number of PGM outputs in total
On-board PGM Outputs	Built-in wired PGM outputs of ESIM264 alarm system.	4	4
EPGM8 PGM Outputs	PGM outputs of EPGM8 - hardwired PGM output expansion module.	8	8
EPGM1 PGM Outputs	PGM outputs of EPGM1 - hardwired zone & PGM output expansion module.	2	4
Wireless PGM Outputs	Non-physical PGM outputs automatically created by connected wireless devices.	2*	32**

* - Depends on the connected wireless device.
** - Available only if no EPGM1 PGM outputs are present.

For PGM output wiring diagram, please refer to **2.3.6. Relay Finder® 40.61.9.12 with Terminal Socket 95.85.3**.

18.1. PGM Output Numbering

The PGM output numbers ranging from C1 through C12 are permanently reserved for on-board PGM outputs even if EPGM8 module mode is disabled. The C13-C44 PGM output number are automatically assigned in the chronological order to the devices connected to the system: EPGM1 modules and wireless devices.

18.2. PGM Output Expansion

For additional electrical appliance connection, the number of PGM outputs can be expanded by:

- connecting EPGM8 hardwired PGM output expansion module. (see **18.2.1. EPGM8 Mode** and **31.3.1. EPGM8 - Hardwired PGM Output Expansion Module**)
- connecting EPGM1 hardwired zone and PGM output expansion module (see **31.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module**).
- binding the wireless devices (see **19. WIRELESS DEVICES**).

The maximum supported PGM output number is 76.

18.2.1. EPGM8 Mode

EPGM8 is an expansion module, which expands the system with 8 additional hardwired PGM outputs. For more details on EPGM8 module installation, please refer to **31.3.1. EPGM8 - Hardwired PGM Output Expansion Module.**

Once the EPGM8 module is installed, the EPGM8 mode must be enabled.

Enable EPGM8 mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 33 & parameter status value:
331#
Example: *331#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EPGM8 mode

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → USING EPGM8 → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 33 & parameter status value:
33 0 #
Example: *330#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

18.3. PGM Output Names

Each PGM output has a name that can be customized by the user. Typically, the name specifies a device type connected to a determined PGM output, for **Example:** Lights. The name can be used instead of PGM output number when controlling the PGM output by SMS text message. By default, the PGM output names are: *C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.*

Set PGM output name

SMS

SMS text message content:
ssss_Coo:out-name
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 44]; *out-name* – up to 16 characters PGM output name.
Example: *1111_C2:Lights*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View PGM output names

SMS

SMS text message content:
ssss_STATUS
Value: *ssss* – 4-digit SMS password.
Example: *1111_STATUS*

EKB2

Menu path:
On-board PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → NAME
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Space, colon, semi-colon characters, parameter names and/or values, such as PSW, STATUS, ON, OFF etc. are NOT allowed in PGM output names.

18.4. Turning PGM Outputs ON and OFF

By default, all PGM outputs are turned OFF. To instantly turn ON/OFF an individual PGM output and set its state to ON/OFF when the system starts-up, please refer to the following configuration methods.

Turn ON PGM output/ Set PGM output start-up state as ON

SMS

SMS text message content:
ssss_Coo:ON or ssss_out-name:ON
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_Lights:ON*

EKB2

Menu path:
On-board PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → ENABLED → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 61, PGM output number & parameter status value:
61 oo 1 #
Value: *oo* – PGM output number, range – [01... 76].
Example: *61031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Turn OFF PGM output/ Set PGM output start-up state as OFF

SMS

SMS text message content:
ssss_Coo:OFF or ssss_out-name:OFF
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name.
Example: *1111_C2:OFF*

EKB2

Menu path:
On-board PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → DISABLED → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 61, PGM output number & parameter status value:
61 oo 0 #
Value: *oo* – PGM output number, range – [01... 76].
Example: *61020#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To instantly turn ON an individual PGM output for a determined time period and automatically turn it OFF when the time period expires, please refer to the following configuration method.

Turn ON PGM output for time period

SMS

SMS text message content:
ssss_Coo:ON:hr.mm.sc or ssss_out-name:ON:hr.mn.sc
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *sc* – seconds, range – [00... 59].
Example: *1111_C4:ON:10.15.35*

To instantly turn OFF an individual PGM output for a determined time period and automatically turn it ON when the time period expires, please refer to the following configuration method.

Turn OFF PGM output for time period

SMS

SMS text message content:
ssss_Coo:OFF:00.00.sc or ssss_out-name:OFF:hr.mn.sc
Value: *ssss* – 4-digit SMS password;*oo* – PGM output number, range – [1... 76]; *out-name* – up to 16 characters PGM output name; *hr* – hours, range – [00... 23]; *mn* – minutes, range – [00... 59]; *sc* – seconds, range – [00... 59].
Example: *1111_Lights:OFF:00.00.23*

When the PGM output is turned ON or OFF, the system will send a confirmation by SMS text message to the user phone number that the SMS text message was sent from.

NOTE FOR EKB2/EKB3/CONFIG TOOL USERS: Only the startup state of the PGM output can be changed using these configuration methods.

NOTE: PGM output can be turned ON for a determined time period only when it is in OFF state

NOTE: PGM output can be turned OFF for a determined time period only when it is in ON state

NOTE: Multiple PGM outputs can be turned ON/OFF by a single SMS text message, **Example:** *1111_C1:ON C2:OFF Pump:ON C4:ON:00.20.25*

18.5. PGM Output Control by Event and Scheduler

The PGM outputs can automatically operate when a specific event occurs in the system and/or when the scheduled weekday and time comes.

PGM Output Actions

The automatic action of the determined PGM output can be set as follows:

- **Turn ON** – Determines whether the PGM output is to be turned ON.
- **Turn OFF** – Determines whether the PGM output is to be turned OFF.
- **Pulse** – Determines whether the PGM output is to be turned ON for a set period of time in seconds.

System Events

The aforementioned PGM output action can be automatically carried out under the following events that have occurred in the system:

- **System armed** – System is armed in a determined partition ranging from Partition 1 through 4 or any partition.
- **System disarmed** – System is disarmed in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm begins** – Alarm begins in a determined partition ranging from Partition 1 through 4 or any partition.
- **Alarm stops** – Alarm stops in a determined partition ranging from Partition 1 through 4 or any partition.
- **Temperature falls** – Temperature falls below the set MIN value of a determined temperature sensor 1-8.
- **Temperature rises** – Temperature rises above the set MAX value of a determined temperature sensor 1-8.
- **Zone violated** – A determined zone ranging from Z1 through Z76 is violated.
- **Zone restored** – A determined zone ranging from Z1 through Z76 is restored.
- **Scheduler starts** – Determines Start Time of a selected scheduler 1-16.
- **Scheduler ends** – Determines End Time of a selected scheduler 1-16.

The user can also set a custom text, which will be sent by SMS text message to user phone number when the automatic PGM output action is carried out.

Schedulers

The system supports up to 16 schedulers that allow the PGM outputs to operate according to the day of the week and time. When the scheduler, which includes the set weekday and time, is selected, the PGM output will operate according to it. Each scheduler includes the following parameters:

- **Always** – The scheduler is not in use.
- **At specified time** – Determines whether weekday and time settings are enabled:
  - **Start Time** – Determines the point in time when the PGM output action can begin.
  - **End Time** – Determines the point in time when the PGM output action can complete.
  - **On weekdays** – Determines days in week when the PGM output action is valid.

Additional Conditions

Additional condition narrows down the chances for a determined automatic PGM output operation to be carried out. If this feature is enabled, the PGM output will become dependent on one more system event that must be occurred prior or must occur after the aforementioned system event. The PGM output will not operate until the chain of system events meets the set values:

- **System armed** – System is armed in a determined partition ranging from 1 to 4 or any partition.
- **System disarmed** – System is disarmed in a determined partition ranging from 1 to 4 or any partition.
- **Zone violated** – A determined zone ranging from Z1 to 76 is violated.
- **Zone restored** – A determined zone ranging from Z1 to Z76 is restored.

Example: *PGM output C1 is set to be turned ON when zone Z6 is violated. The additional condition feature is enabled and set to allow this action to be carried out only if system's Partition 2 is disarmed. It means that the PGM output C1 will be turned ON when zone Z6 is violated, but only if system's Partition 2 is disarmed.*

Manage PGM output control by event & scheduler

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: When both - a system event is determined and a scheduler is selected, the PGM output will operate only if the determined event has occurred in the system during the scheduled time period.

ATTENTION: If the date and time are not set, the system will NOT be able to automatically control the PGM outputs. For more details on how to set date and time, please refer to **9. DATE AND TIME**.

18.6. Wireless PGM Output Type Definitions

- **Output** – Operates as normal PGM output that can be controlled by the user or automatically by event and scheduler. Normally, this type is used for any device or relay.
- **Siren** – Operates as siren output that automatically activates during alarm. Typically, this type is used for bell/siren connected to EW1 wireless device.

Set output type for individual wireless PGM output

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19. WIRELESS DEVICES

ESIM264 system can be equipped with a wireless transmitter-receiver module EWT1 (see **32.1. EWT1 - Wireless Transmitter-Receive**r) for system extension capabilities. The module allows the user to easily bind up to 16 ELDES-made wireless devices to the system. This includes the following:

- EWP1 – wireless PIR sensor (motion detector).
- EWD1 – wireless magnetic door contact.
- EWD2 - magnetic door contact/shock sensor/water sensor
- EWS1 and EWS3 – wireless indoor sirens.
- EWS2 – wireless outdoor sirens.
- EWK1 and EWK2 – wireless keyfobs.
- EW1 – wireless zone and PGM output expansion module.
- EW1B – wireless battery-powered zone and PGM output expansion module.
- EWF1 - wireless smoke detector.

The wireless devices can operate at a range of up to 30 meters from the alarm system unit while inside the building and at up to 150 meters range in open areas. The wireless connection is two-way and operates in one of four available channels at 868MHz non-licensed frequency range. The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period.

19.1. Binding, Removing and Replacing Wireless Devicess

When the wireless device is switched ON, it will initiate the data transmission to the system within its wireless connection range. In order to optimize battery power saving of the wireless device, the data transmission periods vary by itself while the device is switched ON, but still unbound. The data transmission period of the wireless devices when the alarm system is switched OFF or if the wireless device is unbound or removed is as follows:

- EKB3W, EW1, EW1B, EWP1, EWS1, EWS2, EWS3, EWF1:
  - First 360 attempts after the device startup (reset) - every 10 seconds.
  - The rest of attempts - every 1 minute.
- EWD1, EWD2:
  - First 360 attempts after the device startup (reset) - every 10 seconds.
  - The rest of attempts - every 2 minutes.

Once the wireless device is bound, it will attempt to exchange data with ESIM264 system. Due to battery saving reasons, all ELDES wireless devices operate in sleep mode. The data exchange will occur instantly if the wireless device is triggered (zone alarm or tamper alarm) or periodically when the wireless device wakes up to transmit the supervision signal, identified as Test Time, to the system as well as to accept the queued up command (if any) from the system. **Example:** *The alarm occurred at 09:15:25 and the system queued up the command for EWS2 siren to start sounding. By default, Test Time value of EWS2 siren is 7 seconds, therefore EWS2 siren will sound at 09:15:32.*

By default, the Test Time period is as follows:

- EWD1: every 60 seconds.
- EW1, EWD2, EWP1, EWF1: every 30 seconds.
- EW1B: every 20 seconds.
- EWS1, EWS2, EWS3: every 7 seconds.

To set a different Test Time value, please refer to the following configuration method.

Set Test Time

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Test Time affects the wireless device binding process due to the alarm system listening for the incoming data from the wireless device. The system binds the wireless device only when the first data packet is received.

An 8-digit wireless device ID code will be required in order to bind the device to the system or to remove it from the system. The wireless ID code is printed on a label, which can be located on the inner or outer side of the enclosure or on the printed circuit board (PCB) of the wireless device.

To bind a wireless device, please refer to the following configuration methods.

Bind wireless device to the system

SMS

SMS text message content:
ssss_SET:wless-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code.
Example: *1111_SET:535185D*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE FOR EWK1/EWK2 USERS: When binding EWK1/EWK2 wireless keyfob, it is necessary to press several times any button/key on the device.

Once a wireless device is bound, it occupies one of 32 available wireless device slots and the system adds one or two wireless zones and wireless PGM outputs depending on the wireless device model.

To remove a wireless device, please refer to the following configuration methods.

Remove wireless device from the system

SMS

SMS text message content:
ssss_DEL:wless-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code.
Example: *1111_DEL:535185D*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Once a wireless device is removed from the system, please restore its default parameters and remove the batteries from it.

To replace an existing wireless device with a new same model device, please refer to the following configuration methods

Replace wireless device

SMS

SMS text message content:
ssss_REP:wless-id<oldwl-id
Value: *ssss* – 4-digit SMS password; *wless-id* – 8-digit wireless device ID code of the old device; *oldwl-id* - *8*-digit wireless device ID code of the new device.
Example: *1111_REP:535185D<41286652*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When a wireless device is successfully replaced with a new one, the configuration of the old wireless device remains.

ATTENTION: In order to correctly remove the wireless device from the system, the user must remove the device using SMS text message or *ELDES Configuration Tool* software and restore the parameters of the wireless device to default afterwards. If only one of these actions is carried out, the wireless device and the system will attempt to exchange data to keep the wireless connection alive. This leads to fast battery power drain on the battery-powered wireless device.

19.2. Wireless Device Information and Signal Status Monitoring

Once a wireless device is bound, the user can view the following information of a determined wireless device:

- Battery level (expressed in percentage).
- Wireless signal strength (expressed in percentage).
- Error rate (number of failed data transmission attempts in 10-minute period).
- Firmware version.

To view the wireless device information, please refer to the following configuration methods.

View wireless device information

SMS

SMS text message content:
ssss_RFINFO:wless-id or ssss_RFINFO:Znn
Value: *wless-id* – 8-digit wireless device ID code; *nn* – wireless zone number, range – [13... 76].
Example: *1111_RFINFO:535185D*

EKB2

Menu path:
Battery level: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES → OK → wless-dev wless-id → OK → BATTERY

Wireless signal: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES → OK → wless-dev wless-id → OK → SIGNAL

Error rate: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES → OK → wless-dev wless-id → OK → ERROR RATE

Firmware version: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES → OK → wless-dev wless-id → OK → FW RELEASE

Value: *aaaa* – 4-digit administrator password; *wless-dev* – wireless device model; *wless-id* – 8-digit wireless device ID code.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The system supports up to 16 wireless devices. To view the number of unoccupied wireless device slots in the system, please refer to the following configuration methods

View unoccupied wireless device slots

SMS

SMS text message content:
ssss_STATUS_FREE
Example: *1111_STATUS_FREE*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

When the wireless signal between the system and a wireles device is lost and does not restore during 20 minute period, the system will send notification by SMS text message to preset user phone number. By default, the notification regarding the wireless signal status is enabled. To disable/enable this notification, please refer to **16. TAMPERS.**

19.3. Disabling and Enabling Siren if Wireless Signal is Lost

If a wireless device loses its wireless signal, the system will send notification by SMS text message to user phone number and activate the siren/bell. By default, the siren will not be activated when wireless signal is lost. To enable/disable this feature, please refer to the following configuration methods.

Enable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 76 & parameter status value:
76 1 #
Example: *761#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Siren if Wireless Signal is Lost

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS →OK → SRN IF WLESS LOSS → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 76 & parameter status value:
76 0 #
Example: *760#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20. SIREN/BELL

When the system is in alarm state, the siren/bell will sound until the set time (By default – 1 minute) expires or until the system is disarmed. To set the alarm duration, please refer to the following configuration methods.

Set alarm duration

SMS

SMS text message content:
ssss_SIREN:t
Value: *ssss* - 4-digit SMS password; *t* - alarm duration, range – [0... 5] minutes.
Example: *1111_SIREN:4*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION → OK → tt → OK
Value: *aaaa* - 4-digit administrator password; *tt* - alarm duration, range – [1... 10] minutes.

EKB3

Enter parameter 10 & alarm duration:
10 tt #
Value: *tt* - alarm duration, range – [00... 10] minutes.
Example: *1007#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View alarm duration

SMS

SMS text message content:
ssss_SIREN
Value: *ssss* - 4-digit SMS password
Example: *1111_SIREN*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → ALARM DURATION
Value: *aaaa* - 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For siren/bell wiring diagram, please refer to **2.3.3. Siren**.

NOTE: 0 value disables the siren/bell.

NOTE: Due to battery power saving reasons, the wireless siren will sound for 1 minute regardless of the set alarm duration time, unless it is set to 0.

20.1. Bell Squawk

If enabled, the siren/bell indicates the completed system arming and disarming process. After the system is successfully armed, the siren/bell will emit 2 short beeps and 1 long beep after the system is disarmed. To enable/disable the Bell Squawk feature, please refer to the following configuration methods.

Enable Bell Squawk

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 29 & parameter status value:
291 #
Example: *291#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Bell Squawk

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 29 & parameter statusvalue:
290 #
Example: *290#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.2. Indication by EWS2 Indicators

When enabled, the built-in LED indicators of EWS2 wireless outdoor siren will flash during the alarm. To enable/disable this feature, please refer to the following configuration methods.

Enable EWS2 LED indication

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 29 & parameter status value:
881 #
Example: *881#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable EWS2 LED indication

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 29 & parameter status value:
88 0 #
Example: *880#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

20.3. EWF1 Interconnection

The interconnection feature automatically links all wireless smoke detectors to each other that are connected to the same alarm system unit. When any EWF1 detects smoke, it sounds the alarm and sends the signal to the alarm system that causes an instant alarm along with the rest of EWF1 wireless smoke detectors. The device that detected smoke will auto-reset when the smoke clears, while the rest of EWF1 detectors will sound in accordance with the set time period (by default - 30 seconds).

By default, the interconnection feature is enabled and the siren alarm duration is 30 seconds. To manage these parameters, please refer to the following configuraiton methods.

Disable interconnection

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 29 & parameter status value:
50 0 #
Example: *500#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable interconnection

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 29 & parameter status value:
50 1 #
Example: *501#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set EWF1 siren alarm duration

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

For more details on EWF1 wireless smoke detector, please refer to **32.9. EWF1 - Wireless Smoke Detector**

21. BACKUP BATTERY, MAINS POWER SUPPLY STATUS MONITORING AND MEMORY

The system may come equipped with a backup battery maintaining power supply of the system when the mains power supply is temporally lost. The implemented feature allows the system to perform a self-test on the backup battery and notify User 1 by SMS text message as well as to indicate system fault by the keypad (see **29. INDICATION OF SYSTEM FAULTS**) if:

- battery has failed and requires replacement - battery resistance is 2Ω or higher; self-tested every 24 hours.
- battery power is running low - battery voltage is 10.5V or lower; constantly self-tested.

By default, all notifications regarding the backup battery status are enabled. To disable/enable a determined backup battery notification, please refer to the following configuration methods.

Disable Battery Failed notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → BATTERY FAIL EVENT → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 09 0 #
Example: *25090#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Battery Failed notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → BATTERY FAIL EVENT → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 09 1 #
Example: *25091#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable Low Battery notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → LOW BATTERY EVENT → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 06 0 #
Example: *25060#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Low Battery notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → LOW BATTERY EVENT → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 061 #
Example: *25061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If the household electricity is unstable in the system installation area, the system may temporally lose its power supply and continue operating on the backup battery power. The system supervises the mains power supply and notifiies User 1 by SMS text message as well as indicates system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**) when the mains power is lost. When the mains power restores, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, system notification by SMS text message regarding mains power supply status is enabled. To disable/enable this notification, please refer to the following configuration methods.

NOTE: In case of low back-up battery, the system will send the SMS text message to the user and transmit the data message to the monitoring station, but will NOT indicate a system fault on the keypad.

Disable mains power supply loss notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR LOSS EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 04 0 #
Example: *25040#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable mains power supply restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR LOSS EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 04 1 #
Example: *25041#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable mains power supply restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR REST EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 05 0 #
Example: *25050#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable mains power supply restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR REST EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, notification number & parameter status value:
25 05 1 #
Example: *25051#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, mains power supply loss and restore delay are 30 and 120 seconds respectively. To set a different mains power supply loss and restore delay duration, please refer to the following configuration methods.

Set mains power supply loss delay

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → MAIN POWER STATUS → OK → LOSS DELAY → OK → lllll → OK
Value: *aaaa* – 4-digit administrator password; *lllll* – mains power loss delay duration, range - [0... 65535] seconds.

EKB3

Enter parameter 70 & loss delay duration:
70 lllll #
Value: *lllll* – mains power loss delay duration, range - [0... 65535] seconds.
Example: *7043#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set mains power supply restore delay

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → MAIN POWER STATUS → OK → RESTORE DELAY → OK → rrrrr → OK
Value: *aaaa* – 4-digit administrator password; *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds.

EKB3

Enter parameter 71 & restore delay duration:
71 rrrrr #
Value: *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds.
Example: *71150#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

The configuration settings and event log records are stored in a built-in EEPROM memory, therefore even if the system is fully shut down, the configuration and event log remain. For more details regarding the event log, please refer to **28. EVENT LOG**

22. GSM CONNECTION STATUS MONITORING

The system constantly supervises the GSM connection. When the GSM signal is lost, the system indicator NETW will light OFF, the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) and the system will turn ON a determined PGM output if the GSM signal is lost for a longer time period than the set delay value (By default – 180 seconds). Once the GSM signal restores, the keypad will no longer indicate system fault and the determined PGM output will turn OFF.

By default, the PGM output for GSM signal loss indication is not set. To set the PGM output and delay duration for GSM signal loss indication, please refer to the following configuration method.

Manage GSM signal loss indication by PGM output

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23. PARTITIONS

ESIM264 system comes equipped with a partitioning feature that can divide the alarm system into two independently controlled areas identified as Partition 0 through 1, which are all supervised by one alarm system unit. Partitioning can be used in installations where shared alarm system is more practical, such as a house and a garage or within a single multi-storey building. When partitioned, each system element, like zone, user phone number, keypad, user password, iButton key and wireless keyfob can be assigned to one of the partitions. The user will then be able to arm/disarm the system partition that the zones and arm/disarm method are assigned to.

23.1. Zone Partition

Zone partition determines which system partition (-s) the zone will operate in.

Set zone partition

EKB2

Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → PARTITION → OK → PARTITION0... 1 → OK
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES → OK → WLESS ZONE 1... 16 → OK → PARTITION → OK → PARTITION0... 1 → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → KEYPAD 1... 4 ZONE → OK → PARTITION → OK → PARTITION0... 1 → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES → OK → EPGM1 ZONE 1... 16 → OK → PARTITION → OK → PARTITION0... 1 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 57, zone number & partition value:
57 nn p #
Value: *nn* – zone number, range – [01... 44]; *p* – partition number, range – [0... 1].
Example: *57031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.2. User Phone Number Partition

User phone number partition determines which system partition (-s) can be armed/disarmed from a certain user phone number by dialing system's phone number.

Set user phone number partition

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → PARTITION → OK→ PARTITION0... 1 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 59, user phone number slot & partition number:
59 us p #
Value: *nn* – zone number, range – [01... 44]; *p* – partition number, range – [0... 1].
Example: *59030#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.3. Keypad Partition and Keypad Partition Switch

Keypad partition determines which system partition the keypad will operate in. To identify which partition the keypad is operating in:

- EKB2 – Refer to partition name (by default – PART0) indicated in home screen view.
- EKB3 – Refer to the location of the illuminated indicator READY on the keypad. The indicator will be illuminated under section A or B, which represent Partition 0 and Partition 1 respectively.

The keypad must be assigned to the same partition as the user password (see **23.4. User Password Partition**) in order to arm/disarm the system by the keypad. For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User Password** and **12.4. EKB3 Keypad and User Password.**

Set keypad partition

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → KEYPAD 1... 4 → OK → PARTITION 0... 1 → OK
Value: *aaaa* – 4-digit administrator password;

EKB3

Enter parameter 51, keypad slot & partition number:
51 kk p #
Value: *kk* – keypad slot, range – [01... 04]; *p* – partition number, range – [0... 1];
Example: *51062#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Keypad partition switch allows to quickly change the keypad partition. When the keypad partition is changed and when 1 minute after the last key-stroke/key-touch expires, the system will return to the preset keypad partition. Typically, this feature is used for viewing arm/disarm status and alarms of a different partition or when arming/disarming a different system partition by EKB2/EKB3 keypad than the keypad is assigned to.

By default, keypad partition switch is disabled. To enable/disable this feature, please refer to the following configuration methods.

Enable keypad partition switch

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 77 & parameter status value:
77 1#
Example: *771#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable keypad partition switch

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → PARTITION SWITCH → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 77 & parameter status value:
77 0 #
Example: *770#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Keypad partition switch can only be used when the system is partitioned.

23.4. User Password Partition

User password partition determines which system partition can be armed/disarm using a certain user password. User password must be assigned to the same partition as the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) in order to arm/disarm the system by EKB2/EKB3 keypad . For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User Password** and **12.4. EKB3 Keypad and User Password.**

Set user password partition

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (1-16) → OK → USER PASSWORD 1... 16 → OK → PARTITION → OK → PARTITION0... 1 → OK
User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PARTITION → OK → PARTITION0... 1 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 87, user password & partition number:
87 uuuu p #
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [0... 1].
Example: *8711110#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.5. iButton Key Partition

iButton key partition determines which system partition can be armed/disarmed using a certain key. iButton key must be assigned to the partition (-s) that the user desires to arm. For more details on system arming/disarming by iButton key, please refer to **12.5. iButton Key.**

Set iButton key partition

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → IBUTTON 1... 5 → OK → PARTITION → OK → PARTITION0... 1 → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 60, iButton key slot & partition value:
60 ii p #
Value: *ii* – iButton key slot, range – [01... 05]; *p* – partition number, range – [0... 1].
Example: *60051#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

23.6. EWK1/EWK2 Wireless Keyfob Partition

EWK1/EWK2 wireless keyfob partition determines which system partition can be armed/disarmed using a certain EWK1/EWK2 wireless keyfob. For more details on system arming/disarming by EWK1/EWK2 wireless keyfob, please refer to **12.6. EWK1/EWK2 Wireless Keyfob.**

Set EWK1/EWK2 partition

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

24. TEMPERATURE SENSORS

The system may be equipped with a temperature sensor intended for temperature measurement in the surrounding area. This feature allows to monitor the temperature in real-time and receive a notification by SMS text message to User 1 phone number when the set temperature boundaries are exceeded.

24.1. Adding, Removing and Replacing Temperature Sensors

To add a temperature sensor to the system, do the following:

a) Shutdown the system.

b) Wire up the temperature sensor to the 1-Wire interface terminals (see **2.3.5. Temperature Sensor and iButton Key Reader for temperature sensor wiring diagram**).

c) Power up the system.

The real-time temperature value of the temperature sensor is included in the Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**) as well as it is indicated in the home screen view of EKB2 keypad.

To view the real-time temperature value measured by the temperature sensor, please refer to the following configuration methods.

View real-time temperature value

SMS

SMS text message content:
ssss_INFO
Value: *ssss* – 4-digit SMS password.
Example: *1111_INFO*

EKB2

Refer to home screen view on the keypad.

24.2. Setting Up MIN and MAX Temperature Boundaries. Temperature Info SMS

The system supports an SMS text message identified as the Temperature Info SMS, which is automatically delivered to User 1 phone number if the preset minimum (MIN) or maximum (MAX) temperature boundary of any temperature sensor is exceeded.

To set the MIN and MAX temperature boundaries for a certain temperature sensor, please refer to the configuration methods.

Set MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMP:mnn:mxx
Value: *ssss* – 4-digit SMS password; mnn – MIN boundary, range – [-55... 125] C; mxx - MAX boundary, range – [-55... 125] C.
Example: *1111_TEMP:-5:28*

EKB2

Menu path:
MIN: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMPERATURE SENSOR → OK → TEMP. MIN → OK → mnn → OK
MAX: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMPERATURE SENSOR → OK → TEMP. MAX → OK → mxx → OK
Value: *aaaa* – 4-digit administrator password; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C.
Keys P1 or P2 are used to enter minus character, e.g. -20.

EKB3

Enter parameter 19 & temperature boundary value:
19 mnn mxx #
Value: *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C. 00 value stands for minus character, e. g. 0020 = -20
Example: *19001532#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMP
Value: *ssss* – 4-digit SMS password.
Example: *1111_TEMP*

EKB2

Menu path:
MIN: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMPERATURE SENSOR → OK → TEMP. MIN
MAX: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMPERATURE SENSOR → OK → TEMP. MAX
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, Temperature Info SMS is enabled. To disable/enable it, please refer to the following configuration methods.

Disable Temperature Info SMS

SMS

SMS text message content:
ssss_TEMP:00:00
Value: *ssss* – 4-digit SMS password.
Example: *1111_TEMP:00:00*

EKB2

Menu path:
Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP LOW EVENT → OK → DISABLE → OK
Temperature exceeded: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP HIGH EVENT → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 24, event number & parameter status value:
25 14 0 # - Temperature fallen
25 15 0 # - Temperature exceeded
Example: *25140#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable Temperature Info SMS

EKB2

Menu path:
Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP LOW EVENT → OK → ENABLE → OK
Temperature exceeded: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP HIGH EVENT → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 24, event number & parameter status value:
25 14 1 # - Temperature fallen
25 15 1 # - Temperature exceeded
Example: *25151#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION

ESIM264 comes equipped with a microphone that allows the user to listen on his mobile phone to what is happening in the secured area. By installing one of the audio modules EA1 or EA2, the user will be able to have a 2-way voice communication (see **31.3.2. EA1 - Audio Output Module** and **31.3.3. EA2 - Audio Output Module with Amplifier**). Remote listening and 2-way voice communication can operate under the following conditions:

- The system makes a phone call to a preset user phone number in case of alarm and the user answers the call.
- The user initiates remote listening by sending the SMS text message, the system makes a phone call to the user phone number that the SMS text message was sent from and the user answers the call.

Initiate remote listening

SMS

SMS text message content:
ssss_MIC
Value: *ssss* – 4-digit administrator password
Example: *1111_MIC*

Set microphone gain

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *aaaa* – 4-digit administrator password; *mg* – microphone gain, range – [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set speaker level

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → SPEAKER LEVEL → OK → sl → OK
Value: *aaaa* – 4-digit administrator password; *sl* – speaker level, range – [0... 85].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode is enabled (see **30. MONITORING STATION).**

26. SYSTEM INFORMATION. INFO SMS

The system supports an informational SMS text message identified as the Info SMS, which can be delivered upon request. Once requested, the system will reply with Info SMS that provides the following:

- System date & time.
- System status: partition armed (ON)/disarmed (OFF).
- GSM signal strength.
- Mains power supply status.
- Temperature of the area surrounding the temperature sensor (if any).
- State of zones (OK/alarm).
- Name and status (ON/OFF) of PGM outputs.

Request for system information

SMS

SMS text message content:
ssss_INFO
Value: *ssss* - 4-digit SMS password.
Example: *1111_INFO*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

26.1. Periodic Info SMS

By default, the system sends Info SMS to User 1 phone number periodically once a day at 11:00 (frequency - 1 day; time - 11). The minimum period is every 1 hour (frequency - 0 days; time - 1). Typically, this feature is used to verify the power supply and online status of the system.

To set a different frequency and time or disable periodic Info SMS, please refer to the following configuration methods.

Set periodic Info SMS frequency and time

SMS

SMS text message content:
ssss_INFO:fff:it
Value: *ssss* - 4-digit SMS password; *fff* - frequency, range - [00... 99] days; *it* - time, range - [01... 23].
Example: *1111_INFO:3.15*

EKB2

Menu path:
Frequency: OK → CONFIGURATION → OK → aaaa → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → fff → OK
Time: OK → CONFIGURATION → OK → aaaa → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → TIME → it → OK
Value: *aaaa* - 4-digit administrator password; *fff* - frequency, range - [00... 125] days; *it* - time, range - [01... 23].

EKB3

Enter parameter 11, time & frequency:
11it fff #
Value: *it* - time, range - [01... 23]; *fff* - frequency, range - [00... 125] days.
Example: *110412#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable periodic Info SMS

SMS

SMS text message content:
ssss_INFO:00:00
Example: *1111_INFO:00.00*

EKB2

Menu path:
Frequency: OK → CONFIGURATION → OK → aaaa → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → FREQUENCY (DAYS) → 0 → OK
Time: OK → CONFIGURATION → OK → aaaa → PRIMARY SETTINGS → OK → INFO SMS SCHEDULER → OK → TIME → 0 → OK
Value: *aaaa* - 4-digit administrator password.

EKB3

Enter parameter 11, time & frequency:
11 00 00 #
Example: *110000#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: Unlike Info SMS upon request, periodic Info SMS text message does not included zone states, PGM output names and status.

27. SYSTEM NOTIFICATIONS

In case of a certain event, the system attempts to send an SMS text message to the first preset user phone number only. If the user phone number is unavailable and the system fails to receive the SMS delivery report during 20 seconds, it will attempt to send the SMS text message to the next preset user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

- mobile phone was switched off.
- was out of GSM signal coverage.

The system will continue sending the SMS text message to the next preset user phone numbers in the priority order until one is available. The system sends the SMS text message only once and will not return to the first user phone number if the last one was unavailable.

The following table provides the description of system notifications by SMS text message sent to the user phone number.

Seq. No.	**Event**	**Description**
1	General alarm	SMS text message sent to the user in case of system alarm occurrence.
2	System disarmed	SMS text message sent to the user about disarmed system.
3	System armed	SMS text message sent to the user regarding armed system.
4	Mains power loss S	SMS text message sent to the user in case the backup battery voltage is 10.5V or lower.
5	Mains power restore	SMS text message sent to the user in case the mains power supply is restored
6	Low battery	SMS text message sent to the user in case the backup battery voltage is 10.5V or lower
7	Periodical info	Info SMS text message sent to the user periodically by the set values.
8	Tamper alarm	SMS text message sent to the user in case of tamper violation. Indicated as Tamper x.
9	Battery failed	SMS text message sent to the user in case the backup battery resistance is 2Ω or higher (battery requires replacement).
10	System started	SMS text message sent to the user on system startup.
11	Wireless signal loss	SMS text message sent to the user in case the wireless signal is lost. Indicated as Tamper x *.
12	Temperature fallen	SMS text message sent to the user in case of temperature deviation by the set MIN value.
14	Temperature exceeded	SMS text message sent to the user in case of temperature deviation by the set MAX value.
15	System shutdown	When the system is running on backup battery power, it sends the SMS text message to the user before the backup battery power is fully depleted.

ATTENTION: The following methods provide the configuration of the master parameters, which override the notification parameters described in **12.9. Disabling and Enabling Arm/Disarm Notifications**.

To disable/enable a certain system notification, please refer to the following configuration methods.

Disable system notification

EKB2

Menu path:
General alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ALARM EVENT → OK → DISABLE → OKK
System armed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ARMED EVENT → OK → DISABLE → OK
System disarmed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → DISARMED EVENT → OK → DISABLE → OK
Mains power loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR LOSS EV → OK → DISABLE → OK
Mains power restore: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR REST EV → OK → DISABLE → OK
Low battery: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → LOW BATTERY EVENT → OK → DISABLE → OK
Battery failed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → BATTERY FAIL EVENT → OK → DISABLE → OK
Periodical info: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → PERIODIC SMS EV → OK → DISABLE → OK
Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → DISABLE → OK
System started: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → SYSTEM STARTED EV → OK → DISABLE → OK
Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → WLESS SIGN LOSS EV → OK → DISABLE → OK
System shutdown: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → SYSTEM SHUTDOWN EV → OK → DISABLE → OK
Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP LOW EVENT → OK → DISABLE → OK
Temperature exceeded: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP HIGH EVENT → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 01 0 # - General alarm
25 02 0 # - System armed
25 03 0 # - System disarmed
25 04 0 # - Mains power loss
25 05 0 # - Mains power restore
25 06 0 # - Low battery
25 07 0 # - Battery failed
25 08 0 # - Periodical info
25 10 0 # - Tamper alarm
25 11 0 # - System started
25 12 0 # - Wireless signal loss
25 13 0 # - System shutdown
25 14 0 # - Temperature fallen
25 15 0 # - Temperature exceeded
Example: *25040#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable system notification

EKB2

Menu path:
General alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ALARM EVENT → OK → ENABLE → OKK

System armed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → ARMED EVENT → OK → ENABLE → OK

System disarmed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → DISARMED EVENT → OK → ENABLE → OK

Mains power loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR LOSS EV → OK → ENABLE → OK

Mains power restore: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → MAIN PWR REST EV → OK → ENABLE → OK

Low battery: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → LOW BATTERY EVENT → OK → ENABLE → OK

Battery failed: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → BATTERY FAIL EVENT → OK → ENABLE → OK

Periodical info: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → PERIODIC SMS EV → OK → ENABLE → OK

Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → ENABLE → OK

System started: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → SYSTEM STARTED EV → OK → ENABLE → OK

Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → WLESS SIGN LOSS EV → OK → ENABLE → OK

System shutdown: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → SYSTEM SHUTDOWN EV → OK → ENABLE → OK

Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP LOW EVENT → OK → ENABLE → OK

Temperature exceeded: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TEMP HIGH EVENT → OK → ENABLE → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 25, event number & parameter status value:
25 01 1 # - General alarm
25 02 1 # - System armed
25 03 1 # - System disarmed
25 04 1 # - Mains power loss
25 05 1 # - Mains power restore
25 06 1 # - Low battery
25 07 1 # - Battery failed
25 08 1 # - Periodical info
25 10 1 # - Tamper alarm
25 11 1 # - System started
25 12 1 # - Wireless signal loss
25 13 1 # - System shutdown
25 14 1 # - Temperature fallen
25 15 1 # - Temperature exceeded

Example: *25061#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

27.1. SMSC (Short Message Service Center) Phone Number

An SMS center (SMSC) is a GSM network element, which routes SMS text messages to the destination user and stores the SMS text message if the recipient is unavailable. Typically, the phone number of the SMS center is already stored in the SIM card provided by the GSM operator. If the user fails to receive replies from the system, the SMS center phone number, provided by the GSM operator, must be set manually.

Set SMSC phone number

SMS

SMS text message content:
ssss_SMS_+ttteeellnnuumm

Value: *ssss* - 4-digit SMS password; *ttteeellnnuumm* - up to 15 digits SMSC phone number.
Example: *1111_SMS_+4417031111111*

ATTENTION: Before setting the SMSC phone number, please check the credit balance of the system's SIM card. The system will fail to reply if the credit balance is insufficient.

28. EVENT LOG

This feature allows to chronologically register up to 500 timestamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Wireless device management.
- Temperature deviation by MIN and MAX boundaries.
- System faults.

The event log is of LIFO (last in, first out) type that allows the system to automatically replace the oldest records with the the latest ones.

View event log

EKB2

Menu path:
OK → VIEW EVENT LOG → OK → uuuu → OK
Value: *uuuu* - 4-digit user password.

To export the event log to .log file or clear it, please refer to the following configuration method.

Export/clear event log

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, event log is enabled. To disable/enable this feature, please refer to the following configuration methods.

Disable event log

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → DISABLE → OK

EKB3

Enter parameter 36 and parameter status value:
36 0 #
Example: *360#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable event log

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → EVENT LOG → OK → ENABLE → OK

EKB3

Enter parameter 36 and parameter status value:
36 1 #
Example: *361#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

29. INDICATION OF SYSTEM FAULTS

The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault by the keypad as well as by SMS text message notification to the preset user phone number. By default the indication for all system faults is indicated on the keypad. To disable/enable the indication of a certain system fault, please refer to the following configuration method.

Disable/enable individual system fault indication on keypad

Config Tool This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: After enabling/disabling a certain system fault indication, it is necessary to restart the system by fully powering it down and powering it up again.

EKB2 Message **TBL** displayed in the home screen view indicates presence of system faults. In order to find out more on the particular system problem, please open menu section **TROUBLES**. The description on each system problem is indicated in the table below.

Menu path:

OK → TROUBLES

Name	Description
VIOLATED TAMPER	One or more tampers are violated
BATTERY FAILED	Backup battery requires replacement - backup battery resistance is 2Ω or higher
MAIN PWR FAILURE	Mains power supply is lost
DATE/TIME NOT SET	Date/time not set
GSM ERROR	GSM connection is lost

Yellow LED **SYSTEM** indicates system faults. **SYSTEM** LED indications are mentioned in the table below.

SYSTEM LED	Description
Steady ON	One or more tampers are violated; other system faults (see below)
Flashing	One or more high-numbered zones are violated

In order to find out more on the particular system fault, please enter command A provided below. After this procedure the system will activate red zone LEDs for 15 seconds. The description on each LED indication is mentioned in the table below.

Zone LED	Description
1	One or more tampers are violated
2	Backup battery requires replacement - backup battery resistance is 2Ω or higher
3	Mains power supply is lost
4	Date/time not set.
5	One or more high-numbered zones (Z13-Z44) are violated
6	GSM connection is lost

In order to find out which particular high-numbered zone is violated please , enter command B.

In order to find out which particular tamper is violated please , enter command C.

A. System fault indication - enter command:
[CODE#]

B. Violated high-numbered zone indication – enter command:
[CODE1]

C. Violated tamper indication – enter command:
[CODE2]

The number of violated high-numbered zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

Example: LED #3 from section A is flashing and LED #8 from section B is illuminated continuously. According to the table below LED #8 is equal to number 18, therefore 18 + 3 = 21.

Result: Violated high-numbered zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (steady ON)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	Zone LED 11 = 36
Zone LED 6 = 6	Zone LED 12 = 42

30. MONITORING STATION

The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the monitoring station when the MS (Monitoring Station) mode is enabled.

Enable MS mode

SMS

SMS text message content:
ssss_SCNSET:ON
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:ON*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → MS MODE → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password

EKB3

Enter parameter 23 & parameter status value:
23 1 #
Example: *231#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Disable MS mode

SMS

SMS text message content:
ssss_SCNSET:OFF
Value: *ssss* – 4-digit SMS password.
Example: *1111_SCNSET:OFF*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → MS MODE → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password

EKB3

Enter parameter 23 & parameter status value:
23 0 #
Example: *230#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Account is a 4-digit number (By default – 9999) required to identify the alarm system unit by the monitoring station.

Set account

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → ACCOUNT → OK → cccc → OK
Value: *aaaa* – 4-digit administrator password; cccc – 4-digit account number.

EKB3

Enter parameter 27 & account number:
27 cccc #
Value: *cccc* – 4-digit account number.
Example: *278853#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening/2-way voice communication is in progress. However, during the remote configuration session, firmware update process or remote listening/2-way voice communication process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening/2-way voice communication process is over.

ATTENTION: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode is enabled.

30.1. Data Messages - Events

The configuration of data messages is based on Ademco Contact ID protocol. The data messages can either be transmitted to the monitoring station alone or with duplication by SMS text message to preset user phone number. For more details on system notifications by SMS text message, please refer to **27. SYSTEM NOTIFICATIONS**.

Seq. No.	Contact ID® Code	Event	Description
1	1110	Fire alarm	Transmitted in case a zone of Fire type is violated.
2	3110	Fire restore	Transmitted in case a zone of Fire type is restored.
3	1121	Disarmed by user (Duress password)	Transmitted in case the system is disarmed by Duress password.
4	1130	Burglary alarm	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is violated.
5	3130	Burglary restore	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is restored.
6	1133	24-Hour zone alarm	Transmitted in case of zone of 24-Hour type is violated.
7	3133	24-Hour zone restore	Transmitted in case of zone of 24-Hour type is restored.
8	1144	Tamper alarm	Transmitted in case the tamper is violated.
9	3144	Tamper restore	Transmitted in case the tamper is restored.
10	1146	Panic/Silent zone alarm	Transmitted in case of zone of Panic/Silent type is violated.
11	3146	Panic/Silent zone restore	Transmitted in case of zone of Panic/Silent type is restored.
12	1158	Temperature risen	Transmitted in case of the temperature has increased above the MAX set value.
13	1159	Temperature fallen	Transmitted in case of temperature has decreased below the MIN set value.
14	1301	Mains power loss	Transmitted in case the main power supply is lost.
15	3301	Mains power restore	Transmitted in case the main power supply is restored.
16	1302	Low battery	Transmitted in case the backup battery voltage is 10.5V or lower / the wireless sensor battery level runs below 5%.
17	1308	System shutdown	When the system is running on backup battery power, it transmits the data message before the backup battery power is fully depleted.
18	1309	Battery failed	Transmitted in case the backup battery resistance is 2Ω or higher.
19	1358	GSM connection failed	Transmitted in case the GSM connection is lost.
20	1381	Wireless signal loss	Transmitted in case the connection with any wireless device is lost.
21	3381	Wireless signal restore	Transmitted in case the connection with any wireless device is restored.
22	1401	Disarmed by user	Transmitted in case the system is disarmed.
23	3401	Armed by user	Transmitted in case the system is armed.
24	1456	Disarmed in Stay mode	Transmitted in case the system is disarmed in Stay mode.
25	3456	Armed in Stay mode	Transmitted in case the system is armed in Stay mode.
26	1463	Disarmed by user (SGS password)	Transmitted in case the system is disarmed by SGS password.
27	3463	Armed by user (SGS password)	Transmitted in case the system is armed by SGS password.
28	1602	Test event/Kronos ping	Transmitted for system online status verification purposes.
29	3626	Date/time not set	Transmitted in case system date & time is not set.
30	1900	System started	Transmitted on system startup.

The following table refers to user codes included in arm/disarm data messages.

Type	Code
User Phone Number 1	0
User Phone Number 2	1
User Phone Number 3	2
User Phone Number 4	3
User Phone Number 5	4
iButton 1	5
iButton 2	6
iButton 3	7
iButton 4	8
iButton 5	9
User Password 1	10
User Password 2 or Arm/Disarm by Zone	11
User Password 3	12
User Password 4	13
User Password 5	14
User Password 6	15
User Password 7	16
User Password 8	17
User Password 9	18
User Password 10	19
User Password 11	20
User Password 12	21
User Password 13	22
User Password 14	23
User Password 15	24
User Password 16	25
User Password 17	26
User Password 18	27
User Password 19	28
User Password 20	29
User Password 21	30
User Password 22	31
User Password 23	32
User Password 24	33
User Password 25	34
User Password 26	35
User Password 27	36
User Password 28	37
User Password 29	38
User Password 30	39
Remote Code (EGR100)	40
KeyFob 1	85
KeyFob 2	86
KeyFob 3	87
KeyFob 4	88
KeyFob 5	89

Disable data message

EKB2

Menu path:

General alarm/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → ALARM/RESTORE EV → OK → DISABLE → OK

Mains power loss/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → MAIN POWER L/R EV → OK → DISABLE → OK

Armed by user: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → ARMED EVENT → OK → DISABLE → OK

Disarmed by user: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → DISARMED EVENT → OK → DISABLE → OK

Battery failed: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → BATTERY FAIL EVENT → OK → DISABLE → OK

Test event: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEST EVENT → OK → DISABLE → OK

System started: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → SYSTEM STARTED EV → OK → DISABLE → OK

Wireless signal loss/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → WLESS SIGN LOSS EV → OK → DISABLE → OK

Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEMP LOW EVENT → OK → DISABLE → OK

Temperature risen: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEMP HIGH EVENT → OK → DISABLE → OK

System shutdown: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES 2 → OK → SYSTEM SHUTDOWN EV → OK → DISABLE → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 24, event number & parameter status value:

24 01 0 # – General alarm/restore

24 02 0 # – Mains power loss/restore

24 03 0 # – Armed by user

24 04 0 # – Disarmed by user

24 05 0 # – Battery failed

24 06 0 # – Test event

24 07 0 # – System started

24 08 0 # – Wireless signal loss/restore

24 09 0 # – Temperature fallen

24 10 0 # – Temperature risen

24 13 0 # – System shutdown

Example: *24080#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Enable data message

EKB2

Menu path:

General alarm/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → ALARM/RESTORE EV → OK → ENABLE → OK

Mains power loss/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → MAIN POWER L/R EV → OK → ENABLE → OK

Armed by user: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → ARMED EVENT → OK → ENABLE → OK

Disarmed by user: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → DISARMED EVENT → OK → ENABLE → OK

Battery failed: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → BATTERY FAIL EVENT → OK → ENABLE → OK

Test event: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEST EVENT → OK → ENABLE → OK

System started: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → SYSTEM STARTED EV → OK → ENABLE → OK

Wireless signal loss/restore: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → WLESS SIGN LOSS EV → OK → ENABLE → OK

Temperature fallen: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEMP LOW EVENT → OK → ENABLE → OK

Temperature risen: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → TEMP HIGH EVENT → OK → ENABLE → OK

System shutdown: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DATA MESSAGES → OK → SYSTEM SHUTDOWN EV → OK → ENABLE → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 24, event number & parameter status value:

24 01 1 # – General alarm/restore

24 02 1 # – Mains power loss/restore

24 03 1 # – Armed by user

24 04 1 # – Disarmed by user

24 05 1 # – Battery failed

24 06 1 # – Test event

24 07 1 # – System started

24 08 1 # – Wireless signal loss/restore

24 09 1 # – Temperature fallen

24 10 1 # – Temperature risen

24 13 1 # – System shutdown

Example: *24031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2. Communication

The system supports the following communication methods and protocols:

- GPRS network – EGR100, Kronos protocol.
- Voice calls (GSM audio channel) – Ademco Contact ID protocol.
- RS485 data channel.
- CSD (Cricuit Switched Data).
- SMS – Cortex SMS format.

Any communication method can be set as primary or backup connection. The user can set up to 4 backup connections in any sequence order.

Initially, the system communicates via primary connection with the monitoring station. By default, if the initial attempt to transmit data is unsuccessful, the system will make additional attempts until the data is successfully delivered. If all attempts are unsuccessful, the system will follow this pattern:

a) The system switches to the backup connection that follows in the sequence (presumably - Backup 1).

b) The system then attempts to transmit data by the backup connection.

c) If the initial attempt is unsuccessful, the system will make additional attempts until the data is successfully delivered.

d) If the system ends up with all unsuccessful attempts, it will switch to the next backup connection in the sequence (presumably - Backup 2) and will continue to operate as described in the previous steps. The connection is considered unsuccessful under the following conditions:

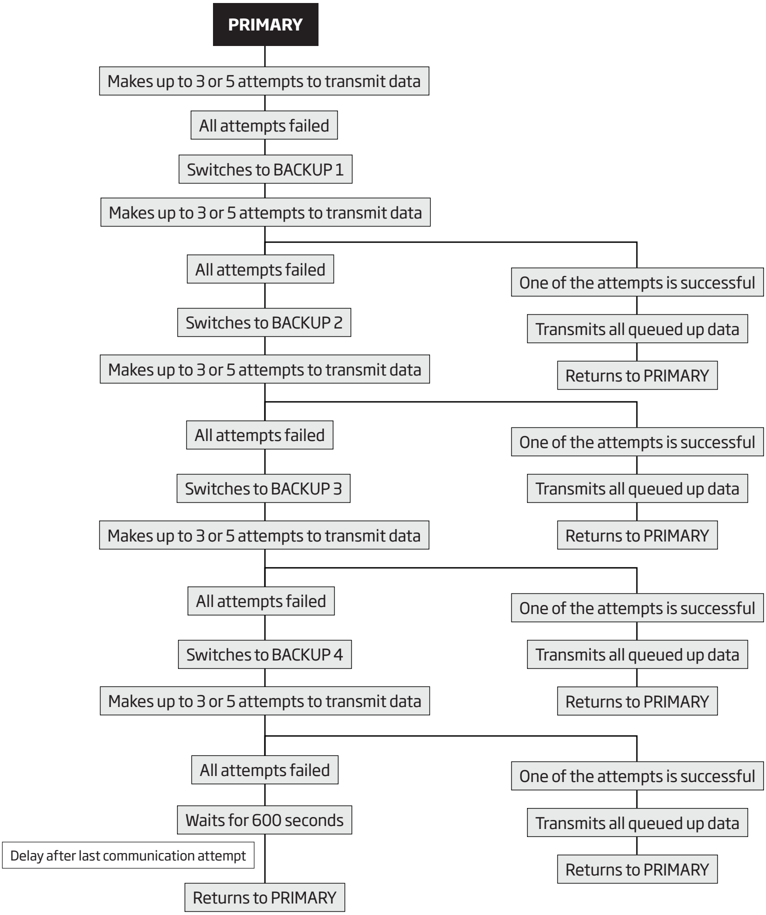
   - GPRS network – The system has not received the ACK data message from the monitoring station within 40 seconds.
   - Voice calls:
     - The system has not received the "handshake" signal from the monitoring station within 40 seconds.
     - The system has not received the "kissoff" signal from the monitoring station within 5 attempts each lasting 1 second.
   - CSD – The system has not received the ACK data message from the monitoring station within 35 seconds.
   - SMS – The system has not received the SMS delivery report from the SMSC (Short Message Service Center) within 45 seconds.

e) If one of the attempts is successful, the system will transmit all queued up data messages by this connection.

f) The system then returns to the primary connection and attempts to transmit the next data messages by primary connection.

g) If the system ends up with all unsuccessful attempts by all connections, it will wait until the *Delay after last communication attempt* time (By default – 600 seconds) expires and will return to the primary connection afterwards.

h) If a new data message, except Test Event (ping), is generated during *Delay* after last communication attempt time, the system will immediately attempt to transmit it to the monitoring station, regardless of *Delay* after last communication attempt being in progress.


PRIMARY
Makes up to 3 or 5 attempts to transmit data
All attempts failed
Switches to BACKUP 1
Makes up to 3 or 5 attempts to transmit data
All attempts failed
One of the attempts is successful
Switches to BACKUP 2
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Switches to BACKUP 3
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Switches to BACKUP 4
Transmits all queued up data
Makes up to 3 or 5 attempts to transmit data
Returns to PRIMARY
All attempts failed
One of the attempts is successful
Waits for 600 seconds
Transmits all queued up data
Delay after last communication attempt
Returns to PRIMARY
Returns to PRIMARY

NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method.

Set primary connection

EKB2

Menu path:
GPRS network: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → GPRS → OK

Voice calls: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → VOICE CALLS → OK

RS485: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → RS485 → OK

CSD: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → CSD → OK

SMS: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → SMS → OK

connection not in use: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → PRIMARY CONNECTION → OK → N/A → OK

Value: aaaa – 4-digit administrator password.

EKB3

Enter parameter 48 & communication method number:
48 0 # – GPRS network
48 1 # – Voice calls
48 2 # – RS485
48 3 # – CSD
48 4 # – SMS
Example: *484#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set backup connection 1... 4

EKB2

Menu path:
GPRS network: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → GPRS → OK

Voice calls: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → VOICE CALLS → OK

RS485: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → RS485 → OK

CSD: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → CSD → OK

SMS: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → SMS → OK

connection not in use: OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → BACKUP CONNECTION1... 4 → OK → N/A → OK

Value: *aaaa* – 4-digit administrator password.

EKB3

Enter parameter 83, backup connection slot number & communication method number:
83 bb 0 # – GPRS network
83 bb 1 # – Voice calls
83 bb 2 # – RS485
83 bb 3 # – CSD
83 bb 4 # – SMS
83 bb 5 # – connection not in use
Value: *bb* – backup connection slot number, range – [01... 05].
Example: *83031#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

If all attempts by all set connections are unsuccessful, the system will wait until the delay time (By default – 600 seconds) expires and will attempt to transmit data to the monitoring station again starting with the primary connection.

Set delay after last communication attempt

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → DELAY LAST ATTEMPT → OK → aaapp → OK
Value: *aaaa* – 4-digit administrator password; *aaapp* – duration of delay after last attempt, range – [0... 65535] seconds.

EKB3

Enter parameter 69 & duration of delay after last attempt:
69 aaapp #
Value: *aaapp* – duration of delay after last attempt, range – [0... 65535] seconds.
Example: *69200#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables delay after last communication attempt.

NOTE: The system is fully compatible with Kronos NET/Kronos LT monitoring station software for communication via GPRS network. When using a different monitoring station software, EGR100 middleware is required.

30.2.1. GPRS Network

The system supports data transmission to the monitoring station via IP-based networks by GPRS network. The supported data formats are the following:

- EGR100
- Kronos

To set up the system for data transmission via GPRS network, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set server IP address, which is a public IP address of the machine running EGR100 or, Kronos monitoring station software.
4. Set server port, which is a port of the machine running EGR100 or Kronos monitoring station software.
5. Select TCP or UDP protocol. UDP is highly recommended for EGR100 data format.
6. Select data format: EGR100 ir Kronos.
7. In case EGR100 is selected, set 4-digit Unit ID number. Unit ID number can be identical to Account number.
8. Set up APN, user name and password provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.

For detailed step-by-step instructions on how to establish the communication between ESIM264 alarm system and EGR100 middleware, please refer to the middleware's HELP file.

Set server IP address

SMS

SMS text message content:
ssss_SETGPRS:IP:add.add.add.add
Value: *ssss* – 4-digit SMS password; *add.add.add.add* – server IP address.
Example: *1111_SETGPRS:IP:65.82.119.5*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → GPRS SETTINGS → OK → SERVER IP → OK → add.add.add.add → OK
Value: *aaaa* – 4-digit administartor password; *add.add.add.add* – server IP address.

EKB3

Enter parameter 40 & server IP address:
40 add add add add #
Value: *add add add add* – server IP address.
Example: *40065082119005#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Kronos NET/Kronos LT software communicates via TCP protocol, while EGR100 middle-ware v1.2 and up supports both – TCP and UDP protocols. However, TCP protocol is NOT recommend to use with EGR100.

Set protocol

SMS

SMS text message content:
ssss_SETGPRS:PROTOCOL:ptc
Value: *ssss* – 4-digit SMS password; *ptc* – protocol, range – [TCP... UDP].
Example: *1111_SETGPRS:PROTOCOL:UDP*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → GPRS SETTINGS → OK → PROTOCOL → OK → TCP | UDP → OK
Value: *aaaa* – 4-digit administartor password.

EKB3

Enter parameter 43 & protocol number:
43 0 # - TCP
43 1 # - UDP

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS1 server IP address

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → GPRS SETTINGS → OK → DNS1 → OK → add.add.add. add → OK
Value: *aaaa* – 4-digit administartor password; *add.add.add.add* – DNS1 server IP address.

EKB3

Enter parameter 41 & DNS1 server IP address:
41 add add add add #
Value: *add add add add* – DNS1 server IP address.
Example: *41065082119001#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set DNS2 server IP address

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → GPRS SETTINGS → OK → DNS2 → OK → add.add.add. add → OK
Value: *aaaa* – 4-digit administartor password; *add.add.add.add* – DNS2 server IP address.

EKB3

Enter parameter 42 & DNS2 server IP address:
42 add add add add #
Value: *add add add add* – DNS2 server IP address.
Example: **42065082119002#**

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set data format as Kronos or EGR100

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set APN

SMS

SMS text message content:
ssss_SETGPRS:APN:acc-point-name
Value: *ssss* – 4-digit SMS password; *acc-point-name* – up to 31 character APN (Access Point Name) provided by the GSM operator.
Example: *1111_SETGPRS:APN:internet*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set user name

SMS

SMS text message content:
ssss_SETGPRS:USER:usr-name
Value: *ssss* – 4-digit SMS password; *usr-name* – up to 31 character user name provided by the GSM operator.
Example: *1111_USER:mobileusr*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Set password

SMS

SMS text message content:
ssss_SETGPRS:PSW:password
Value: *ssss* – 4-digit SMS password; *password* – up to 31 character password provided by the GSM operator.
Example: *1111_SETGPRS:PSW:mobilepsw*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station via GPRS network method is unsuccessful, the system will make up to 2 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → GPRS SETTINGS → OK → GPRS ATTEMPTS → OK → att → OK
Value: *aaaa* – 4-digit administrator password; *att* – number of attempts, range – [1... 255].

EKB3

Enter parameter 68 & number of attempts:
68 att #
Value: *att* – number of attempts, range – [01... 255].
Example: *6809#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

To report the online status, the system periodically transmits (By default – every 180 seconds) Test Event data message (ping) to the monitoring station via GPRS network.

Set test period

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → GPRS SETTINGS → OK → TEST PERIOD → OK → tteessttpp → OK
Value: *aaaa* – 4-digit administrator password; *tteessttpp* – test period, range – [0... 65535] seconds.

EKB3

Enter parameter 46 & number of attempts:
46 tteessttpp #
Value: *tteessttpp* – test period, range – [0... 65535] seconds.
Example: *46120#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: 0 value disables test period.

Unit ID is a 4-digit number (By default – 0000) required to identify the alarm system unit by EGR100 middle-ware. It is MANDATORY to change the default Unit ID before using EGR100.

Set unit ID

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → GPRS SETTINGS → OK → UNIT ID → OK → unid → OK
Value: *aaaa* – 4-digit administartor password; *unid* – 4-digit unit ID number.

EKB3

Enter parameter 47 & unit ID number:
47 unid #
Value: *unid* – 4-digit unit ID number.
Example: *472245#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

View GPRS network settings

SMS

SMS text message content:
ssss_SETGPRS?
Example: *1111_SETGPRS?*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

NOTE: Kronos NET/Kronos LT software communicates via TCP protocol, while EGR100 middle-ware v1.2 and up supports both – TCP and UDP protocols. However, TCP protocol is NOT recommend to use with EGR100.

ATTENTION: It is necessary to restart the system locally by powering down and powering up the system the system or remotely (see **33. REMOTE SYSTEM RESTART**) after changing the IP address or switching from TCP to UDP.

30.2.2. Voice Calls and SMS

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by Voice Calls or SMS communication method. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number format is the following:

- **International (w/o plus)** – The phone numbers must be entered starting with an international country code in the following format: [international code][area code][local number], example for UK: 4417091111111.

To set up the system for data transmission via Voice Calls or SMS, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).

2. Set 4-digit Account number (see **30. MONITORING STATION**).

3. Set Tel. Number 1... 3.

Set monitoring station phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → ttteeellnnuumm → OK
Value: *aaaa* – 4-digit administrator password; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.

EKB3

Enter parameter 26, phone number slot & phone number:
26 ps ttteeellnnuumm #
Value: *ps* – phone number slot, range – [01... 03]; *ttteeellnnuumm* – up to 15 digits monitoring station phone number.
Example: *2601441709111111 1#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → TEL. NUMBER 1... 3 → OK → OK
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via Voice Calls or SMS method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will continue to communicate with the monitoring station by switching to the next phone number that follows in the sequence and making up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → VOICE CALLS/SMS ST → OK → ATTEMPTS → OK → at → OK
Value: *aaaa* – 4-digit administrator password; at – number of attempts, range – [1... 10].

EKB3

Enter parameter 37 & number of attempts:
37 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *3706#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Due to the individual configuration of each monitoring station, the system may fail to deliver the data message via Voice Calls communication method. In such cases it is recommended to adjust the microphone gain until the optimal value, leading to successful data message delivery, is discovered.

Set microphone gain

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → GSM AUDIO → OK → MICROPHONE GAIN → OK → mg → OK
Value: *aaaa* – 4-digit administrator password; *mg* – microphone gain, range – [0... 15].

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

30.2.3. CSD

The system supports up to 5 monitoring station phone numbers for communication with the alarm system by CSD communication method. Tel. Number 1 is mandatory, the other four can be used as backup phone numbers and are not necessary. The supported phone number format is the following:

- **International (w/o plus) –** The phone numbers must be entered starting with an international country code in the following format: [international code][area code][local number], example for UK: 4417091111111.

To set up the system for data transmission via CSD, please follow the basic configuration steps:

1. Enable MS Mode parameter (see **30. MONITORING STATION**).
2. Set 4-digit Account number (see **30. MONITORING STATION**).
3. Set Tel. Number 1... 5.

Set monitoring station phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → tttееellnnuumm → OK
Value: *aaaa* – 4-digit administrator password; *tttееellnnuumm* – up to 15 digits monitoring station phone number.

EKB3

Enter parameter 85, number of entry & phone number:
85 ps tttееellnnuumm #
Value: *ps* – phone number slot, range – [01... 05]; *tttееellnnuumm* – up to 15 digits monitoring station phone number.
Example: *85014417091111111#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

Delete monitoring station phone number

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → OK
Value: *aaaa* – 4-digit administrator password.

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

By default, if the initial attempt to transmit data to the monitoring station's phone number via CSD method is unsuccessful, the system will make up to 4 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

Set attempts

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → MS SETTINGS → OK → CSD SETTINGS → OK → TEL. NUMBER 1... 5 → OK → OK
Value: *aaaa* – 4-digit administrator password; at – number of attempts, range – [1... 10].

EKB3

Enter parameter 84 & number of attempts:
84 at #
Value: *at* – number of attempts, range – [01... 10].
Example: *8403#*

Config Tool

This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

31. ELDES WIRED DEVICES

31.1. RS485 Interface

RS485 interface is used for the system to communicate with the following devices:

- EKB2 keypads (up to 4 units).
- EKB3 keypads (up to 4 units).
- EPGM1 modules (1 unit).

The terminals of RS485 interface are Y (yellow wire) and G (green wire), which are clock and data respectively. The devices, connected to RS485 interface, must be powered from the AUX+ and AUX- terminals.

For more details on RS485 device wiring, please refer to **3.2.7. RS485**.

31.1.1. EKB2 - LCD Keypad

EKB2 is an LCD keypad intended for using with ESIM264 alarm system.

Main EKB2 features:

- Alarm system arming and disarming (see **12.3. EKB2 Keypad and User Password**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- System information display (see **31.1.1.4. Visual and Audio Indications)**.
- Audio indication by built-in buzzer (see **31.1.1.4. Visual and Audio Indications**).
- Wireless device information display (see **19.2. Wireless Device Information and Signal Status Monitorin**g).
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).
- Temperature display (see **31.1.1.1.2 Keys Functionality**).
- Time display (see **31.1.1.1.2 Keys Functionality**).

The system configuration is performed by accessing EKB2 menu and entering the required values. ESIM264 system allows to connect up to 4 EKB2 keypads.

31.1.1.1. Technical Specifications

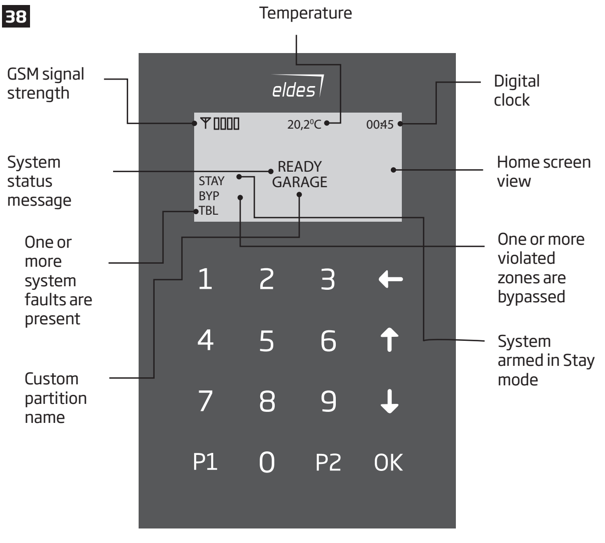
31.1.1.1.1 Electrical & Mechanical Characteristics

Power Supply	12-14V ⎓ 150mA max.
Maximum Keypad Connection Cable Length	100 m.
Dimensions	133 x 89 x 19 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of Operating Temperatures	0...+55°C

31.1.1.1.2 Keys Functionality

←	One menu level back / cancel
↑	Menu navigation – up
↓	Menu navigation – down
OK	Confirm (enter) value
0 ... 9	Value typing
P1	Keypad partition switch / minus symbol for entering negative temp. value
P2	Additional menu / minus symbol for entering negative temp. value

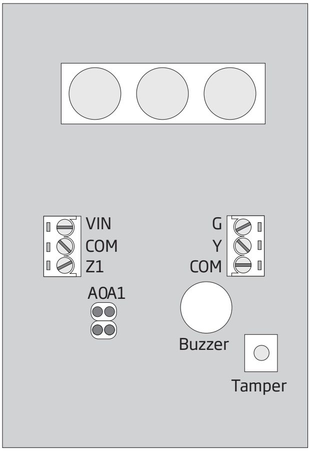
38



31.1.1.1.3 Connector and Main Unit Functionality

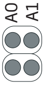
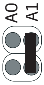
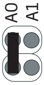
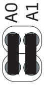
Vin	Positive power supply terminal
COM	Negative power supply terminal
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common terminal for Z1
Z1	Security zone terminal
A0	Keypad address pin
A1	Keypad address pin
Buzzer	Buzzer for audio indications
Tamper	Tamper-button for EKB2 enclosure status monitoring

39



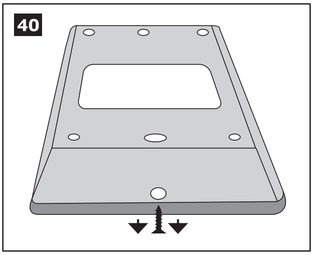
31.1.1.1.4 Keypad Address

A0 and **A1** pins located on the back side of the keypad are intended to set keypad address. The keypad address is set by putting the jumper (-s) on the pins. ESIM264 system allows to connect up to 4 EKB2 keypads - each set under different address. Jumper combinations for different keypad address configuration are indicated in the table below.

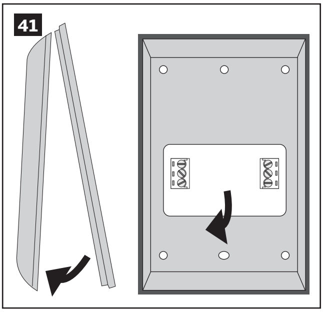
Jumper position	Address	Jumper position	Address
	Keypad 1		Keypad 3
	Keypad 2		Keypad 4

The address of each connected keypad is also indicated in *ELDES Configuration Tool* software.

31.1.1.2. Installation



40



41

1. Remove the screw located on the bottom side of the enclosure (see Fig. No. 40)
2. Detach keypad holder from EKB2 keypad by gently pulling the holder towards yourself (see Fig. No. 41).
3. Fix the keypad holder on the wall using the screws. (see Fig. No. 42)
4. Disconnect ESIM264 main power supply and backup battery.
5. Wire up keypad terminals to ESIM264 alarm system respectively – Vin to AUX+, **COM** to **AUX-**, **Y** to **Y**, **G** to **G** (see Fig. No. 43).
6. Connect a sensor and the resistor across **Z1** and **COM** terminalss in accordance with zone connection Type 1 or Type 2 (see **2.3.2. Zone Connection Types**). As keypad zone **Z1** is disabled by default, it can be enabled by SMS, ELDES Configuration Tool, EKB2 and EKB3 keypad. Keypad zone **Z1** must be enabled and resistor connected even if the tamper button alone is required (see Fig. No. 43).

   NOTE: Keypad zone connection type can differ from selected on-board zone connection type.

   NOTE: ATZ mode is NOT supported by keypad zones. ATZ mode is ineffective for keypad zones when enabled.

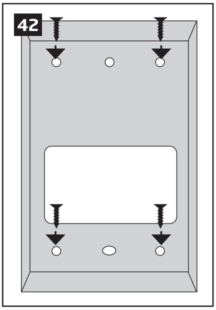
7. Set the keypad address by putting the jumper on A0 and A1 pins (see **32.1.1.1.4 Keypad Address**).
8. Fix the keypad into the holder.

   ATTENTION: Before fixing the keypad into the holder please , make sure that the tamper button is properly pressed (see Fig. No. 39).

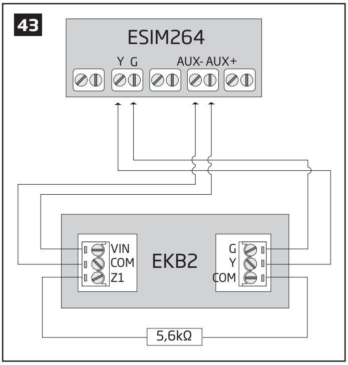
9. Screw in the bottom side of the enclosure. (see Fig. No. 40).
10. Power up ESIM264 alarm system.
11. EKB2 keypad is ready.

For more details on multiple keypad wiring, please refer to **3.2.7. RS485**

42



43



31.1.1.3. Visual and Audio Indications

EKB2 can be used even in dark premises as the LCD screen and keys are illuminated continuously. The illumination level lowers down if 3 minutes after the last key-touch expires while the system is disarmed. In case of alarm, the keypad illumination level is boosted and stays in this state until the system is disarmed.

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration, one long beep – for invalid configuration. In addition, the buzzer emits short beeps in case of alarm and exit/entry delay countdown.

31.1.1.4. EKB2 Zone and Tamper

Keypad EKB2 has one wired zone Z1 and one tamper button. By default, the keypad zone Z1 is disabled. The keypad zone can be enabled by SMS, EKB2 keypad, EKB3 keypad and *ELDES Configuration Tool* software (see **14.9. Disabling and Enabling Zones**). When Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM terminals must be connected with resistor of 5,6kΩ nominal.

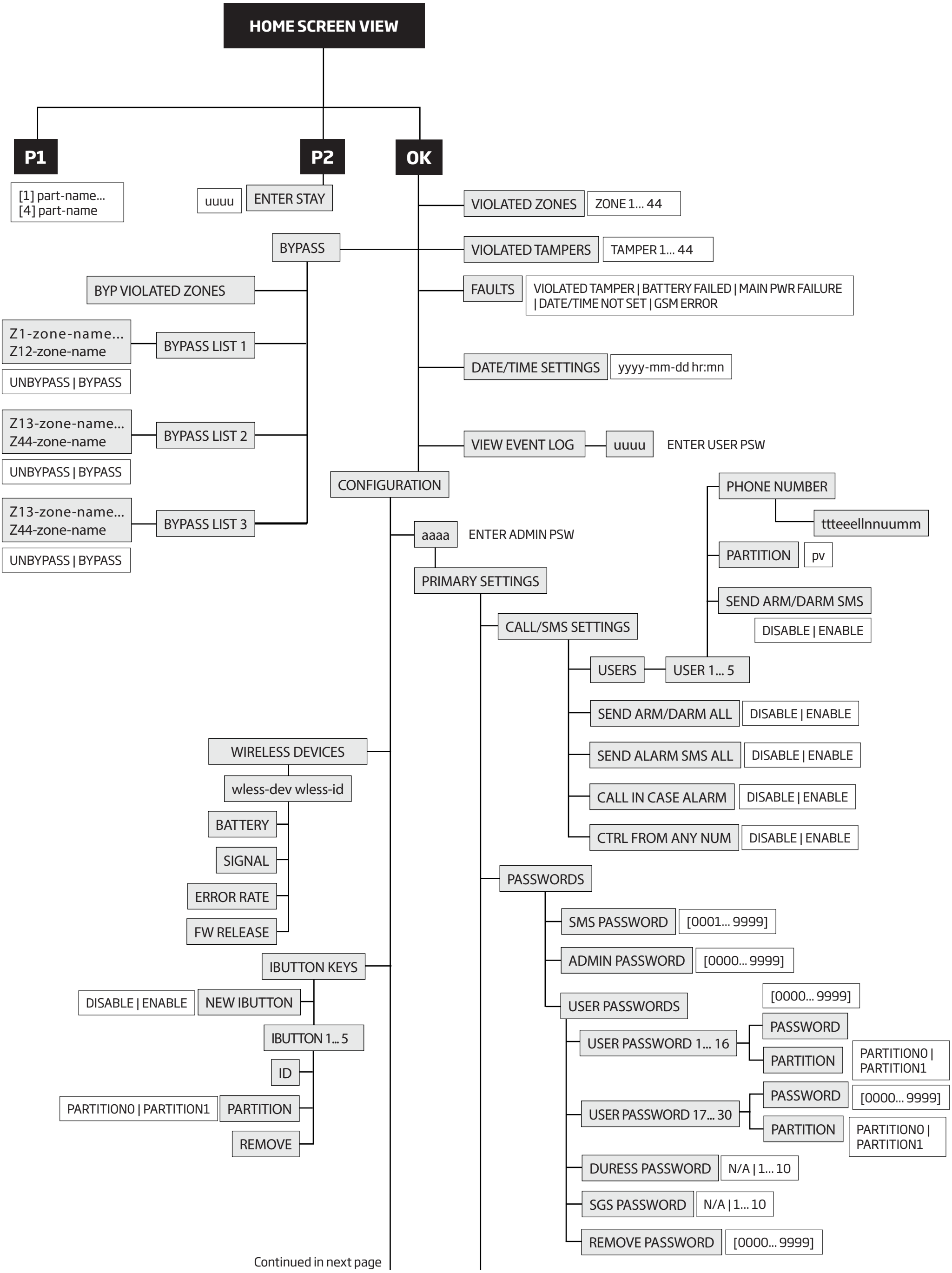
The tamper button is intended for monitoring the enclosure status of EKB2, therefore the system causes alarm if the enclosure is illegally opened. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

31.1.1.5. Icons and Messages

Icon / Message	Description
🚪	Chime - Delay zone violated when system is disarmed.
🏃	Exit delay countdown initiated.
🔒	System is armed and menu is locked.
🔓	System is disarmed and menu is unlocked
🛠 **+ CONFIGURATION MODE**	Configuration mode activated.
BURGLARY ALARM	Delay, Instant or Follow zone violated when system is armed.

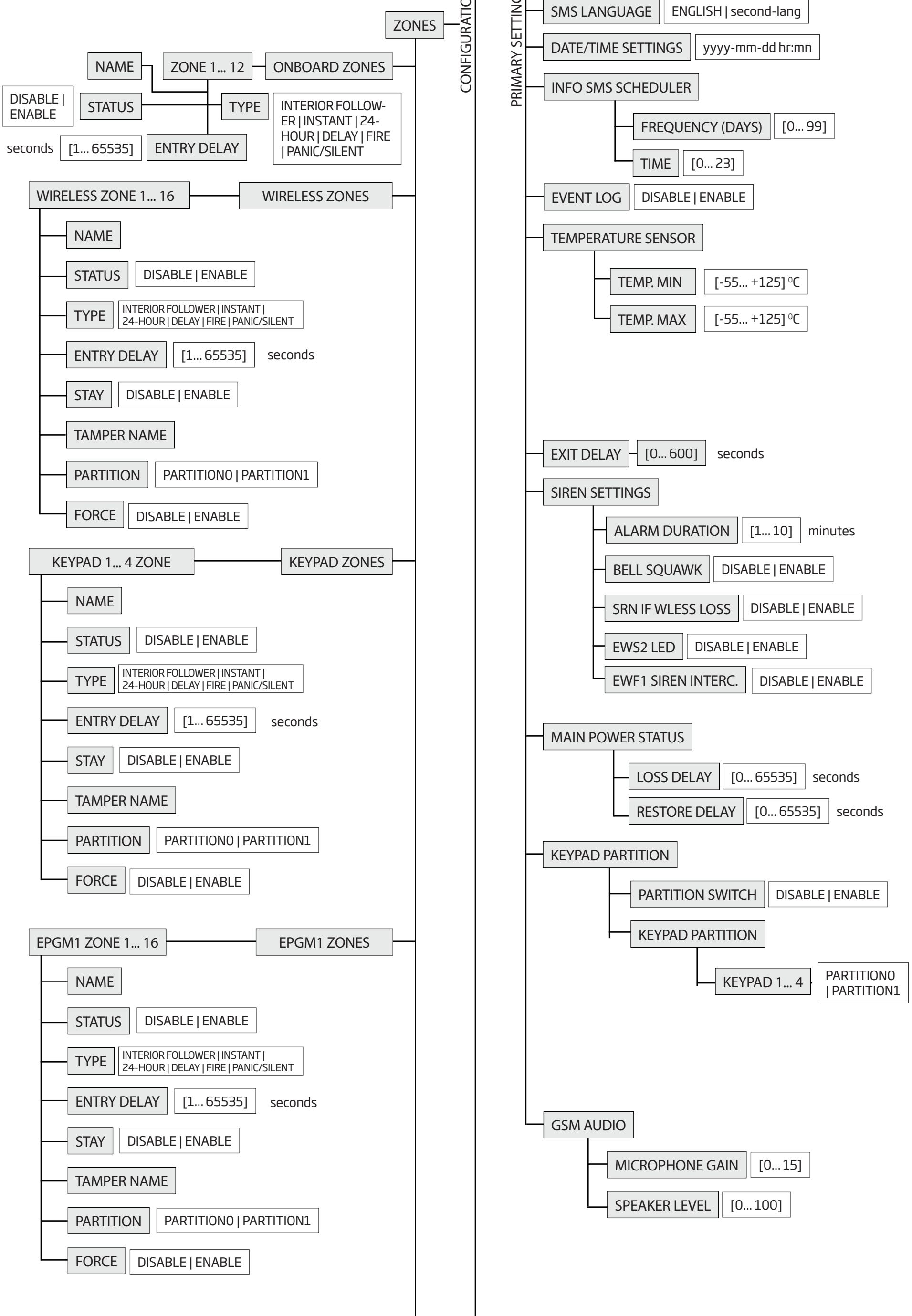
Icon / Message	Description
24 ALARM	24H zone violated.
FIRE ALARM	Fire zone violated.
TAMPER ALARM	Tamper violated
READY	System is ready to be armed.
NOT READY	System is not ready to be armed – one or more zones / tampers violated.
ARMED	System is armed (optional feature).
STAY	*Stay* mode activated
BYP	System armed in Stay mode
TBL	One or more system faults are present

31.1.1.6. Menu Tree



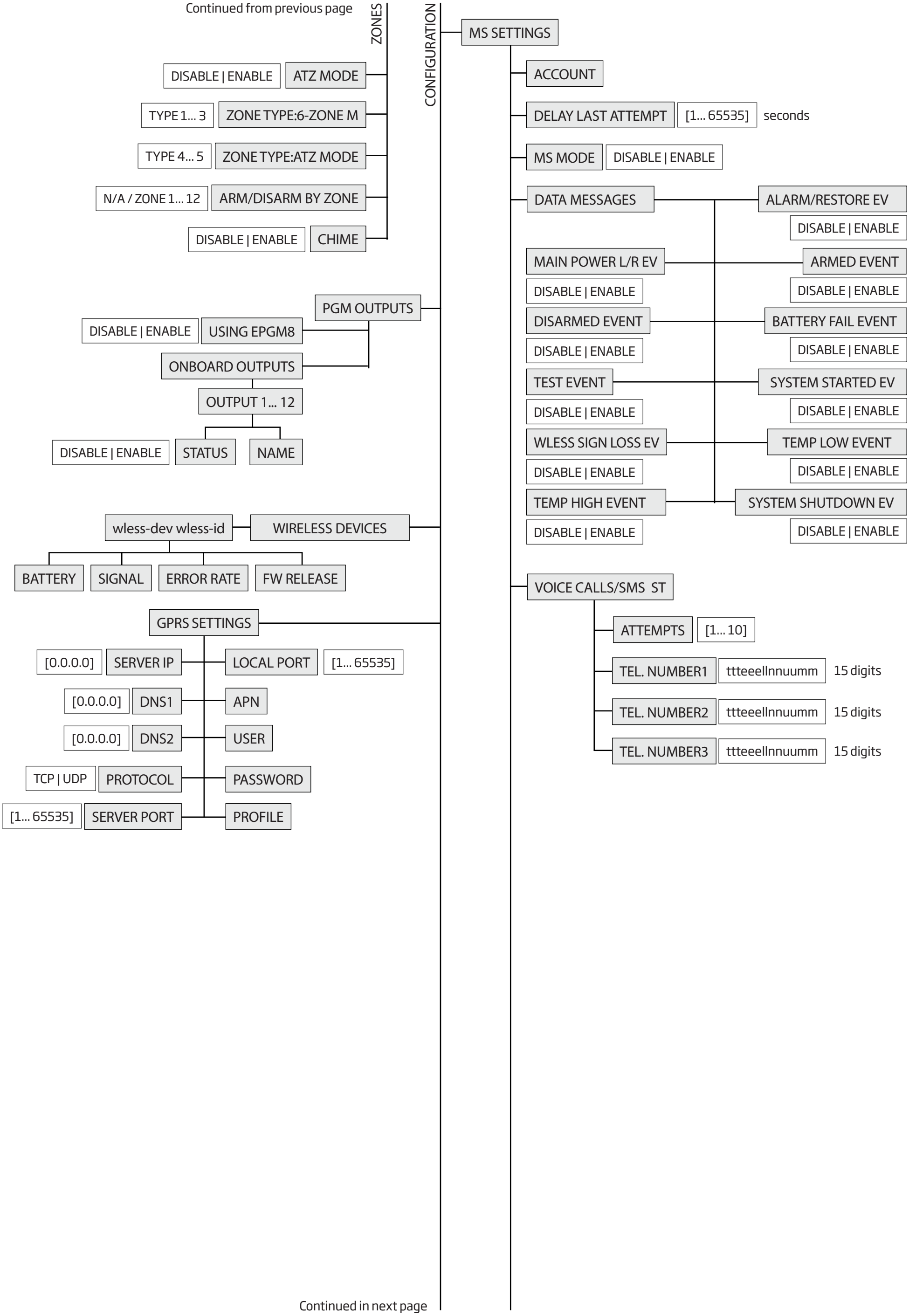
Continued in next page

Continued from previous page



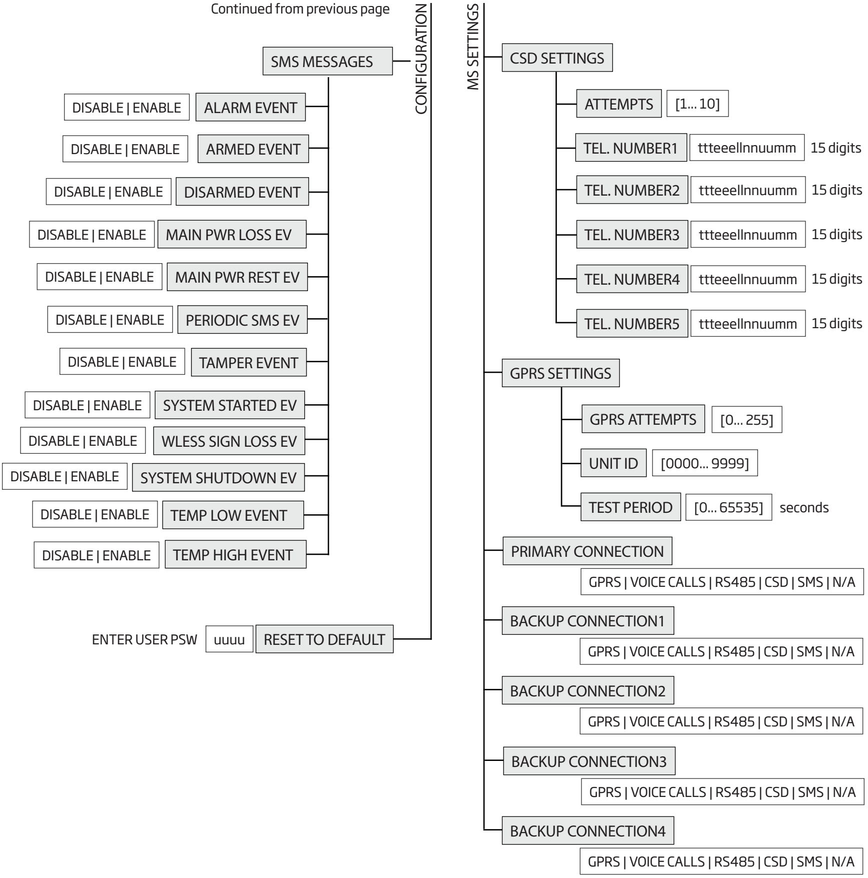
Continued in next page

Continued from previous page



Continued in next page

Continued from previous page



31.1.2. EKB3 - LED Keypad

EKB3 is a LED keypad intended for using with ESIM264 alarm system.

Main EKB3 features:

- Alarm system arming and disarming (see **12.4. EKB3 Keypad and User Password**).
- Arming and disarming in Stay mode (see **15. STAY MODE**).
- System parameter configuration (see **5. CONFIGURATION METHODS**).
- PGM output control (see **18.4. Turning PGM Outputs ON and OFF**).
- Visual indication by LED indicators (see **31.1.2.3. Visual and Audio Indications).**
- Audio indication by built-in buzzer (see **31.1.2.3. Visual and Audio Indications**).
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

The system configuration by EKB3 keypad is performed by activating the Configuration mode (see **5. CONFIGURATION METHODS**) and entering the required parameters & values. ESIM264 system allows to connect up to 4 EKB3 keypads.

31.1.2.1. Technical Specifications

31.1.2.1.1 Electrical & Mechanical Characteristics

Power Supply	12-14V ⎓ 150mA max
Maximum Keypad Connection Cable Length	100 m.
Dimensions	140x100x18mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of Operating Temperatures	-30...+55°C

31.1.2.1.2 LED Functionality

ARMED	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - system is ready – no violated zones and tampers
SYSTEM	Steady ON - system faults; flashing - violated high-numbered zone (Z13-Z44)
BYPS	Steady ON - zone bypass mode
1-12	Steady ON - violated zone Z1... Z12

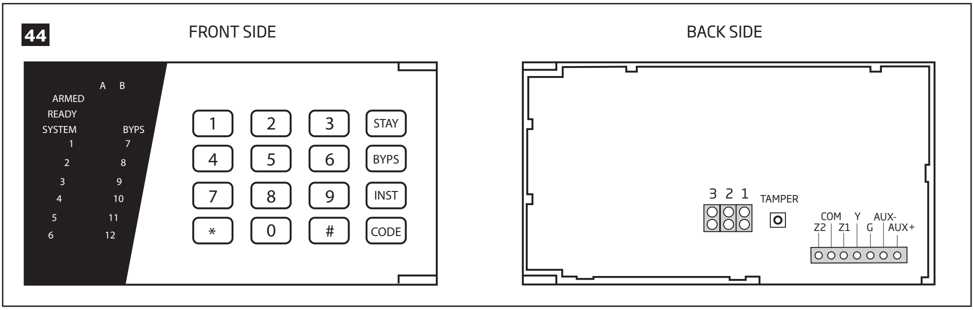
31.1.2.1.3 Keys Functionality

[BYPS]	Zone bypass mode
[CODE]	System fault list / violated high-numbered zone indication / violated tamper indication
[*]	1st character for Configuration mode activation/deactivation command / clear typed in characters / keypad partition switch (if enabled)
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[STAY]	Manual system arming in Stay mode
[INST]	N/A

31.1.2.1.4 Connector Functionality

AUX+	Positive power supply terminal
AUX-	Negative power supply terminal
G	RS485 interface for communication (green wire)
Y	RS485 interface for communication (yellow wire)
COM	Common terminal for Z1
Z1	Security zone terminal
Z2	N/A
3, 2	Keypad address pins
1	N/A

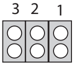
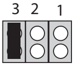
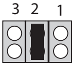
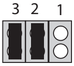
44



31.1.2.1.5 Keypad Address

Pins **3** and **2** located on the back side of the keypad are intended to set keypad address. The keypad address is set by putting the jumper (-s) on the pins. ESIM264 system allows to connect up to 4 EKB3 keypads - each set under different address. Jumper combinations for different keypad address configuration are indicated in the table below.

Address Configuration

Jumper position	Address
	Keypad 1
	Keypad 2
	Keypad 3
	Keypad 4

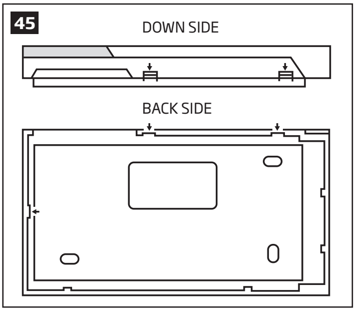
NOTE: Pins **1** are inactive.

The address of each connected keypad is also indicated in *ELDES Configuration Tool* software.

31.1.2.2. Installation

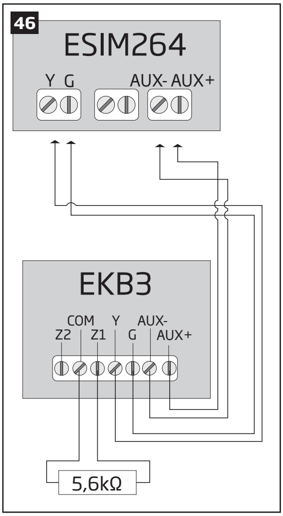
1. Detach keypad holder from EKB3 keypad . Keypad holder detach points are marked with arrows (see Fig. No. 45).

45



2. Disconnect alarm system ESIM264 power supply and backup battery before connecting the wires.

46



3. Wire up keypad terminals to ESIM264 alarm system respectively – **AUX+** to **AUX+**, **AUX-** to **AUX-**, **Y** to **Y**, **G** to **G**. (see Fig. No. 46).
4. Connect a sensor and the resistor across Z1 and COM terminalss in accordance with zone connection Type 1 or Type 2 (see **2.3.2. Zone Connection Types)**. As keypad zone Z1 is disabled by default, it can be enabled by SMS, ELDES Configuration Tool, EKB2 and EKB3 keypad. Z2 terminal is permanently inactive. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required (see Fig. No. 44).

NOTE: Keypad zone connection type can differ from selected on-board zone connection type.

NOTE: ATZ mode is NOT supported by keypad zones. ATZ mode is ineffective for keypad zones when enabled.

5. Set the keypad address by combining DIP switch positions (see **31.1.2.1.5 Keypad Address**).
6. Infix the keypad into the holder (see Fig. No. 45).

ATTENTION: Before fixing the keypad into the holder please , make sure that the tamper is properly pressed (see Fig. No. 44).

7. Power up ESIM264 alarm system.
8. EKB3 keypad is ready.

For more details on multiple keypad wiring, please refer to **3.2.7. RS485.**

31.1.2.3. Visual and Audio Indications

EKB3 keys have a LED back-light, therefore it is possible to use this keypad even in dark premises. The back-light lasts for 3 minutes after the last key-stroke while the system is disarmed. In case of alarm, the keypad back-light turns ON and lasts until the system is disarmed.

The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm and exit/entry delay countdown.

31.1.2.4. EKB3 Zone & Tamper

Keypad EKB3 has one wired zone Z1 and one tamper button. By default, the keypad zone Z1 is disabled. The keypad zone can be enabled by SMS, EKB2 keypad, EKB3 keypad, EKB3W keypad and *ELDES Configuration Tool* software (see **14.9. Disabling and Enabling Zones**). Zone Z1 is enabled, it operates like any other system zone, therefore a sensor can be connected to it. In addition, Z1 and COM terminals must be connected with resistor of 5,6kΩ nominal.

The tamper button is intended for monitoring the enclosure status of EKB3, therefore the system causes alarm if the enclosure is illegally opened. Keypad zone Z1 must be enabled and resistor connected even if the tamper button alone is required.

31.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module

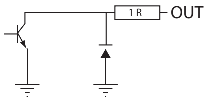
EPGM1 is a hardwired zone & PGM output expansion module intended for using with ELDES alarm systems.

Main EPGM1 features:

- hardwired zone expansion adding 16 additional zones
- 2 PGM output expansion for electrical appliance connection

31.1.3.1. Technical Specifications

31.1.3.1.1 Electrical & Mechanical Characteristics

Power Supply	10-24V ⎓ 100mA max without auxiliary equipment.
Number of Digital Inputs	16
Nominal Resistance	5,6kΩ
Number of PGM Outputs	2
Maximum PGM Output Current	250 mA
EPGM1 PGM Output Circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum Commuting PGM Output Values	Voltage – 30V; current 250mA
AUX: Auxiliary Equipment Power Supply	13,8V ⎓ 500 mA max
Dimensions	118 x 47 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of Operating Temperatures	-20...+55°C

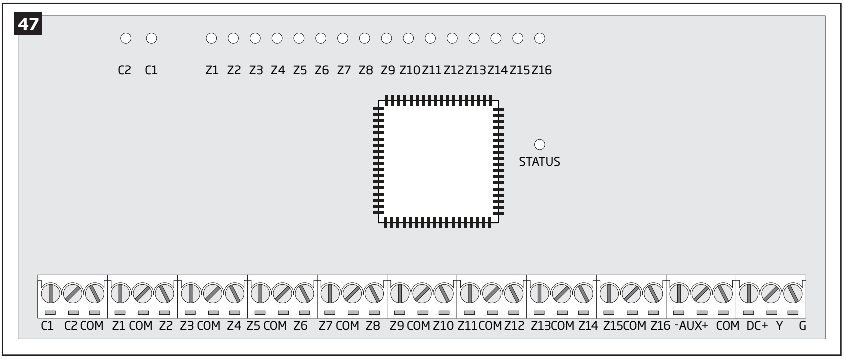
31.1.3.1.2 LED and Pin Functionality

C2, C1	PGM output C1, C2 status – on/off
Z1 - Z16	Zone Z1 - Z16 state – alarm/restore
STATUS	EPGM1 micro-controller status

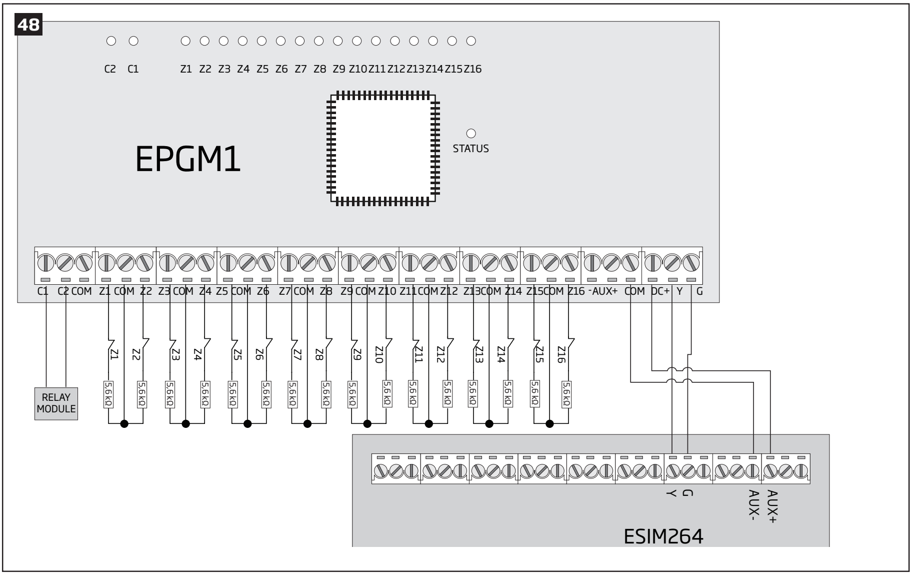
31.1.3.1.3 Connector Functionality

C1, C2	PGM output terminals
Z1 - Z16	Security zone terminals
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
Y	RS485 interface for communication (yellow wire)
G	RS485 interface for communication (green wire)
COM	Negative power supply terminal
DC+	Positive power supply terminal

47


C2 C1
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
STATUS
C1 C2 COM Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 Z7 COM Z8 Z9 COM Z10 Z11 COM Z12 Z13 COM Z14 Z15 COM Z16 -AUX+ COM DC+ Y G

48


C2 C1
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
EPGM1
STATUS
C1 C2 COM Z1 COM Z2 Z3 COM Z4 Z5 COM Z6 Z7 COM Z8 Z9 COM Z10 Z11 COM Z12 Z13 COM Z14 Z15 COM Z16 -AUX+ COM DC+ Y G
Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11 Z12 Z13 Z14 Z15 Z16
5,6 kΩ
RELAY MODULE
Y G
AUX- AUX+
ESIM264

31.1.3.2. Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Connect EPGM1 **DC+** terminal to ESIM264 **AUX+** terminal, EPGM1 **COM** terminal to ESIM264 **AUX-** terminal, EPGM1 **Y** and **G** terminals must be connected to ESIM264 **Y** and **G** terminals respectively (see Fig. No. 48).
3. Connect the resistors and sensors to EPGM1 module according to the selected zone connection **Type 1**, **Type 2** or **Type 3** (see **2.3.2 Zone Connection Types**). If ATZ mode is enabled, please connect the resistors and sensors according to zone connection Type 1 or Type 2.
4. Power up ESIM264 system.
5. Upon successful startup indicator **STATUS** should be blinking indicating successful EPGM1 operation.
6. EPGM1 is ready for use with ESIM264 alarm system.

NOTE: ATZ mode is not supported by EPGM1 zones.

NOTE: When ATZ mode is disabled, all EPGM1 zones must be wired in accordance with zone connection type set up in the system software-wise i.e. **Type 1**, **Type 2** or **Type 3**. If ATZ mode is enabled, EPGM1 zones can be wired in accordance with **Type 1** or **Type 2** only (mixed combination of these two zone connection types is permitted), regardless of the set up zone connection type in the system.

For more details on multiple EPGM1 module wiring, please refer to **3.2.7. RS485**

31.2. 1-Wire Interface

1-Wire interface is used for the system to communicate with an iButton key reader and up to 8 temperature sensors. 1-Wire interface COM and DATA terminals are ground and data respectively. When connecting single or multiple temperature sensors, the +5V terminal must be used along.

For more details on 1-Wire device wiring, please refer to **32.2.1 iButton Key Reader and Buzzer**

31.2.1. iButton Key Reader and Keys

The iButton key is a microchip enclosed in a stainless steel tab usually implemented in a small plastic holder. Each iButton key holds a unique 64-bit identity code (ID), which is used for alarm system ESIM264 arming and disarming procedure.

Main iButton features:

- Up to 5 iButton keys per alarm system unit ESIM264;
- Communication via 1-Wire interface.

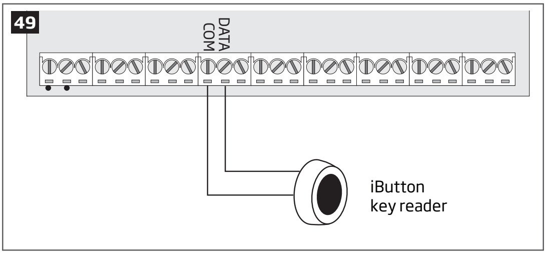
31.2.1.1. Technical Specifications

31.2.1.1.1 Electrical & Mechanical Characteristics

Supported iButton Key Model	Maxim/Dallas DS1990A
Communication Interface	1-Wire
Maximum Cable Length for 1-Wire Communication	up to 30 meters

31.2.1.1.2 Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Connect iButton key reader contact wires to 1-Wire interface on ESIM264 alarm system: **COM** and **DATA** terminals respectively.



3. Power up ESIM264 alarm system.
4 iButton key reader is ready for use with ESIM264 alarm system.

For more details on iButton key management, please refer to **11. iBUTTON KEYS**.

31.3. Modules Interface

31.3.1. EPGM8 - Hardwired PGM Output Expansion Module

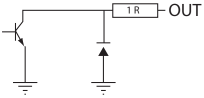
EPGM8 is a PGM output expansion module intended for using with alarm system ESIM264. This module allows to connect up to additional 8 electrical appliances.

Main EPGM8 features:

- PGM output expansion adding 8 additional PGM outputs;
- Compatible with ESIM264 alarm system

31.3.1.1. Technical Specifications

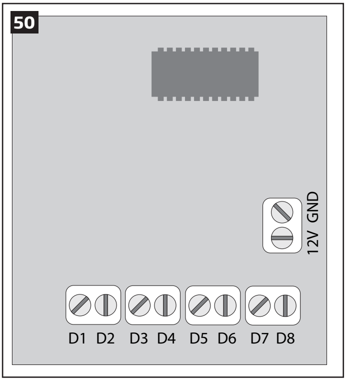
31.3.1.1.1 Electrical & Mechanical Characteristics

Power Supply	10-24V ⎓ 100mA max
Number of PGM Outputs	8
EPGM8 PGM Output Circuit	 Open collector output. Output is pulled to COM when turned on.
Maximum Commuting PGM Output Values	Voltage – 30V; current 500mA
Dimensions	40 x 55 x 15 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Range of Operating Temperatures	-20...+55°C

31.3.1.1.2 Connector Functionality

D1 - D8	PGM output terminals
12V	Positive power supply terminal
GND	Negative power supply terminal

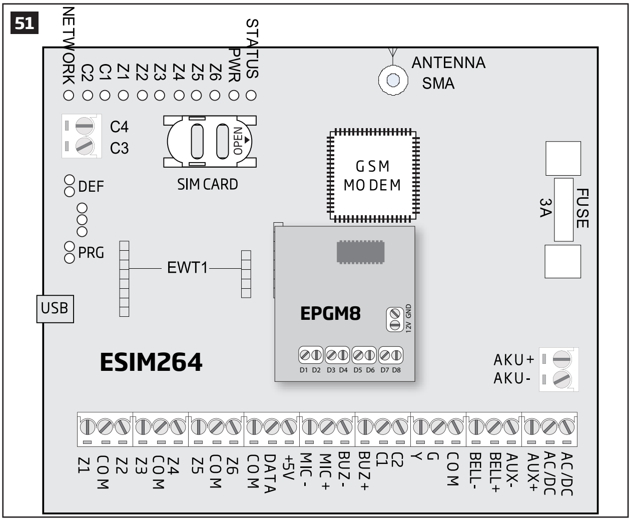
50



31.3.1.2. Installation

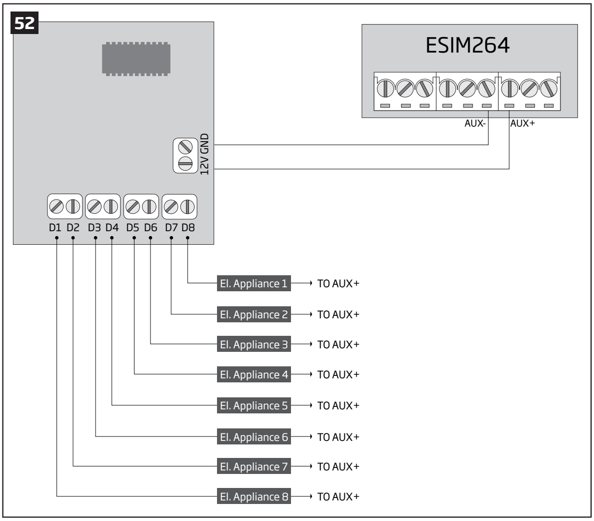
1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Insert EPGM8 pins into appropriate ESIM264 alarm system slots (see Fig. No. 51)

51



3. Connect EPGM8 **12V** positive power supply terminal with ESIM264 alarm system **AUX+** terminal and EPGM8 **GND** terminal with ESIM264 alarm system **AUX-** terminal. (see Fig. No. 52).
4. Connect the electrical appliances to **D1** – **D8** PGM outputs. (see Fig. No. 52).

52



5. Power up ESIM264 alarm system.
6. 6. Enable EPGM8 mode using EKB2/EKB3 keypad or ELDES Configuration Tool software. For more details, please refer to software's HELP section or **18.2.1. EPGM8 Mode.**
7. EPGM8 is ready for use with ESIM264 alarm system.

31.3.2. EA1 - Audio Output Module

EA1 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA1 features:

- Two-way voice conversation during a phone call;
- Possibility to connect headphones or desktop speakers.

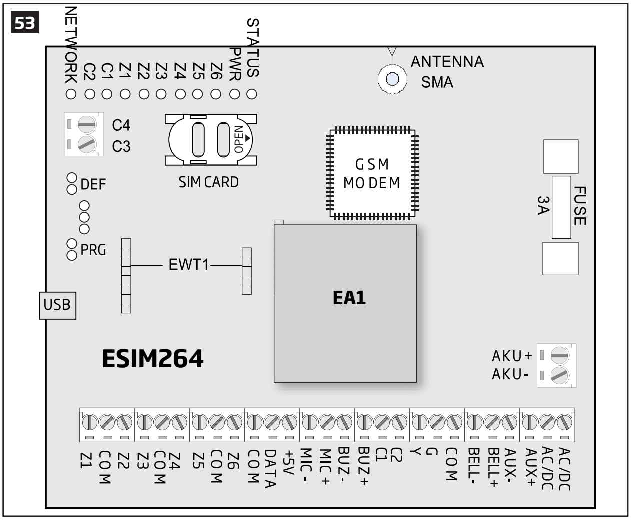
31.3.2.1. Technical Specifications

- 3,5 mm female jack
- Dimensions: 35 x 33 x 12 mm

31.3.2.2. Installation

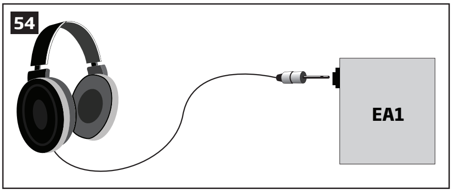
1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Insert EA1 pins into appropriate ESIM264 alarm system slots.

53



3. Connect headphones or desktop speakers to EA1 3,5 mm female jack.

54



4. Power up ESIM264 alarm system.
5. EA1 is ready for use with ESIM264 alarm system.

31.3.3. EA2 - Audio Output Module with Amplifier

EA2 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA2 features:

- Two-way voice conversation during a phone call;
- Possibility to connect a speaker.

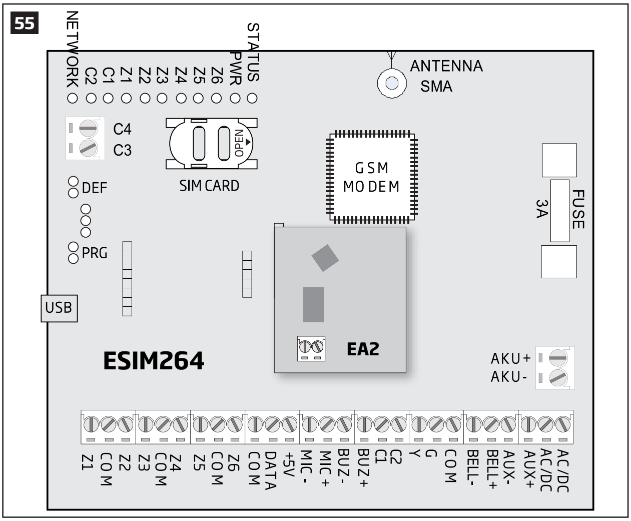
31.3.3.1. Technical Specifications

- 1W 8Ω audio amplifier
- Dimensions: 41 x 40 x 24 mm

31.3.3.2. Installation

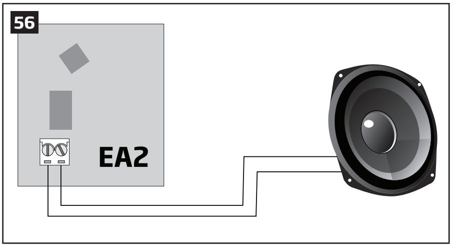
1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Insert EA2 pins into appropriate ESIM264 alarm system slots.

55



3. Connect a speaker to EA2 **Speaker** terminals.

56



4. Power up ESIM264 alarm system.
5. EA2 is ready for use with ESIM264 alarm system.

32. ELDES WIRELESS DEVICES

32.1. EWT1 - Wireless Transmitter-Receiver

Wireless transmitter-receiver EWT1 is an add-on module for ESIM264 system. It enables wireless transmission through alarm system ESIM264 and ELDES wireless devices, such as: wireless PIR movement sensors EWP1, wireless expansion modules EW1 and EW1B, wireless indoor sirens EWS1, wireless outdoor sirens EWS2, wireless magnetic door contacts EWD1, wireless magnetic door contacts/shock sensors EWD2, wireless smoke detectors EWF1 and wireless key-fobs EWK1 and EWK2.

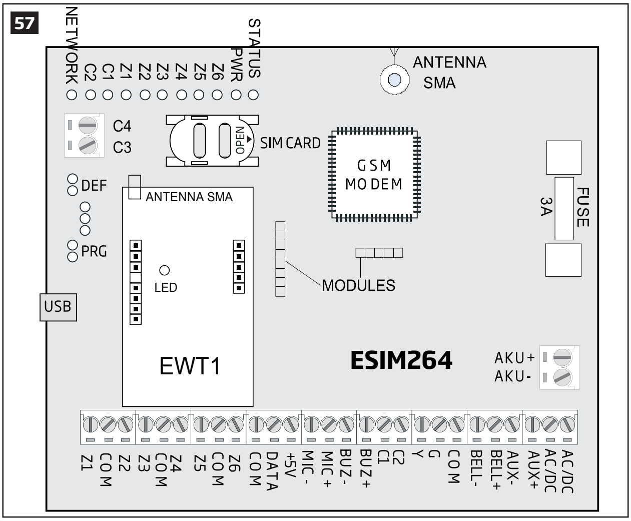
EWT1 enables ESIM264 alarm system to connect up to 16 wireless devices at a time. Maximum wireless connection range is 150 meters (in open areas).

32.1.1. Technical Specifications

32.1.1.1. Electrical & Mechanical Characteristics

Wireless Transmitter-Receiver Frequency	868 MHz
Dimensions	68x38x18mm
Operating Temperature Range	-20...+55°C
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Maximum Number of Wireless Devices	16

32.1.2. Installation



1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. 2. Insert EWT1 pins into appropriate ESIM264 slots as indicated in Fig. No. 57.
3. Mount the antenna to EWT1. It is not recommended to install the antenna inside the metal enclosure.
4. Power up ESIM264 system.
5. EWT1 is ready to use with ESIM264 system.

32.2. EW1 - Wireless Zone & PGM Output Expansion Module

Main EW1B features:

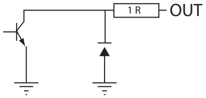
- 2 zones for wired sensor connection;
- 2 PGM outputs for electrical appliance connection;
- Powered by external power supply.

Wireless expansion module EW1 is a wireless device with 2 zones and 2 PGM outputs. This expansion module connects to ELDES wireless alarm systems and enables wireless access for to 2 wired devices such as movement PIR sensors, magnetic door contacts etc. In addition it allows to connect and control up to 2 appliances, i.e. lighting, heating etc. After the wiring process to EW1 it is necessary to bind EW1 to the alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool.*

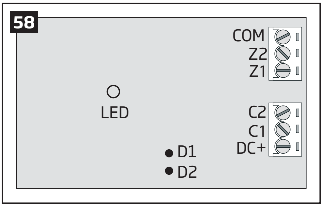
It is possible to connect up to 16 EW1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

32.2.1. Technical Specifications

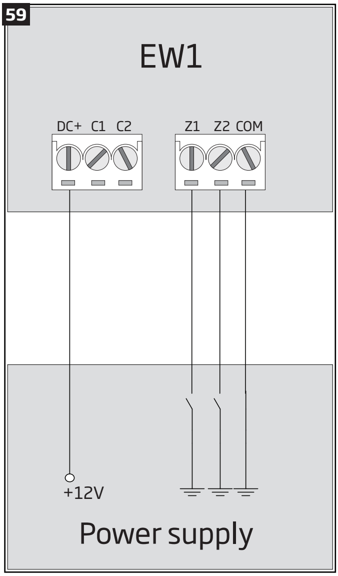
32.2.1.1. Electrical & Mechanical Characteristics

Power Supply	7-15V ⎓ 20mA max
Number of Zones	2
Zone Connection Type	Normally closed (NC)
Number of PGM Outputs	2
Maximum Commuting PGM Output Values	Voltage – 30V; current 500mA
EW1 PGM Output Circuit	 Open collector output. Output is pulled to COM when turned on.
Wireless Transmitter-Receiver Frequency	868 MHz
Range of Operating Temperatures	-20...+55°C
Dimensions	38x60x12mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

58



59



32.2.1.2. Connector & LED Functionality

COM	Common terminal for power supply, zones
Z2, Z1	Security zone terminals
C2, C1	PGM output terminals
DC+	Positive power supply terminal
D1, D2	Pins for restoring default parameters
LED	EW1 status

32.2.2. Installation

1. Disconnect ESIM264 alarm system main power supply and backup battery.
2. Wire up EW1 as indicated in Fig. No. 59.
3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
4. T he system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EW1 closer to ESIM264 alarm system device and bind it again.
5. EW1 module is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.2.4 Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.2.3. EW1 Zones, PGM Outputs & Tamper

Upon successful EW1 module binding process, the system adds 2 wireless Instant zones intended for wired sensor connection and 2 wireless PGM outputs intended for electrical appliance connection and control.

The wireless connection loss between EW1 and ESIM264 alarm system leads to system alarm regardless of system being armed or disarmed. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

32.2.4. Restoring Default Parameters

1. Disconnect EW1 power supply.
2. Short circuit (connect) pins D1 and D2.
3. Power up EW1 and wait until LED provides several short flashes.
4. Disconnect power supply.
5. Remove short-circuit from D1 and D2 pins.
6. Power up EW1.
7. Parameters restored to default.

32.3. EWP1 - Wireless Motion Detector

Main EWP1 features:

- Violated zone detection by built-in PIR movement sensor.

EWP1 is a wireless device with built-in PIR movement sensor and operates with ELDES wireless alarm systems. The user only needs to switch on the EWP1 sensor and bind it to ESIM264 alarm system by sending a corresponding command via SMS text message or using software ELDES Configuration Tool. User can also monitor temperature of the surrounding areas in real-time as EWP1 has a built-in temperature sensor. It is possible to connect up to 16 EWP1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

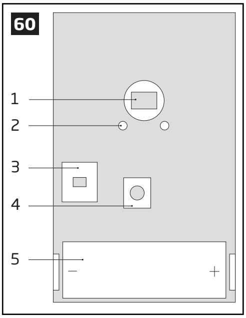
32.3.1. Technical Specifications

32.3.1.1. Electrical & Mechanical Characteristics

Battery Type	ER14505 AA Lithium Thionyl Chloride
Battery Voltage; Capacity	3,6 V; 2,4 Ah
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 MHz
Range of Operating Temperatures	-10 ... +55°C
Dimensions	104x60x33mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Detection Coverage Angle	90°
Maximum Detection Distance	10 meters
Compatible with Alarm Systems	ELDES Wireless
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas

* The operation time depends on different conditions and may vary.

60



1 Motion detector

2 LED indicators informing about status of PIR sensor EWP1

3 TAMPER button automatically identifies when the box of sensor EWP1 is open or closed

4 RESET button for reseting system parameters

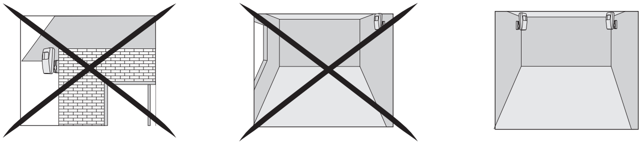
5 ER14505 3,6 V Lithium Thionyl Chloride battery

32.3.2. Installation

1. Choose the place where intrusion into the premises is the most probable and install the device. To avoid false triggers of the system do not install it in the following places:

- directing the lens to direct sunlight, for example, to the window of the premises;
- where there is a risk of sudden temperature alteration, for example, near a fireplace or heating system;
- where there is an enlarged possibility of dust or air flow;
- behind the curtain or some other cover blocking the detected zone.

61



2. Fix EWP1 sensors mounting holder with two screws to the wall and attach the sensor.

3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWP1 closer to alarm system device and bind it again.
5. EWP1 is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **32.3.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.3.3. EWP1 Zone & Tamper

Upon successful EWP1 sensor binding process, the system adds 1 wireless Instant zone intended for movement detection. By, default, the alarm is caused instantly if any movement is detected in coverage area of the sensor (when system is armed).

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWP1 sensor:

- **By tamper button.** EWP1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWP1 is illegally opened, the tamper button becomes unpressed. This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWP1 sensor and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

32.3.4. Battery Replacement

1. Open EWP1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWP1.
4. Insert the battery into the battery slot.
5. Batteries replaced.

For more details, please refer to **32.3.2. Installation.**

ATTENTION: Only ER14505 Lithium Thionyl Chlorid AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

32.3.5. Restoring Default Parameters

1. Remove any battery from EWP1.
2. Press and hold the RESET button.
3. Insert the battery back to EWP1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

32.4. EWD1 - Wireless Magnetic Door Contact

Main EWD1 features:

- Violated zone detection by magnetic contact;
- Panic button.

EWD1 is a wireless device with magnetic contact and panic button which is used to secure doors, windows or any other opening parts and it operates with ELDES wireless alarm systems. EWD1 is bind to ESIM264 alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Tool.* When EWD1 is connected to the system, two wireless zones are added. First wireless zone is used to monitor the magnetic contacts and the second wireless zone is for managing the panic button. By default panic button zone is configured as Silent zone and in case the panic button is pressed, the system causes silent alarm (no siren is activated).

It is possible to connect up to 16 EWD1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

32.4.1. Technical Specifications

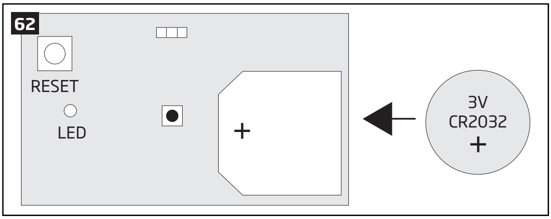
32.4.1.1. Electrical & Mechanical Characteristics

Battery Type	CR2032 3V Lithium
Number of Batteries	1
Battery Operation time	15 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55°C
Door Contact Dimensions	60x37x18mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Magnet Dimensions	60x17x16mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

* The operation time depends on different conditions and may vary.

32.4.2. Installation

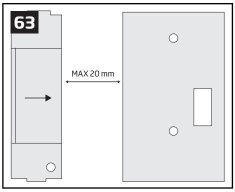
1. Open EWD1 enclosure and insert the battery (Fig. No. 62).



2. EWD1 consists of two parts: a magnet and a sensor. Sensor components are: a mounting part and the sensor. Magnet components are: a mounting part and the cover.

2.1 Fix the sensor mounting part with two screws on the door or window jamb.

2.2 Fix the magnet mounting part with two screws next to the sensor mounting part on door or window frame. The correct fixing position is indicated in Fig. No. 63.



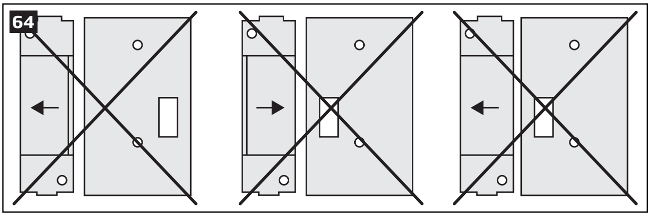
NOTE: The distance between magnet and sensor can be up to 20 mm only.

2.3 The sensor should be attached to the fixed sensors mounting part. When attaching sensor pay attention to the tamper (micro switch) - it must be pressed.

2.4 The magnet cover should be attached to the fixed magnet mounting part.

NOTE: It is not recommend to fix EWD1 in other ways than with screws, e.g. with duck tape. See Fig. No. 64 for the incorrect ways of fixing the magnetic door contact.

64



3. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
4. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWD1 closer to alarm system device and bind it again.
5. EWD1 magnetic door contact is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **32.4.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.4.3. EWD1 Zones & Tamper

Upon successful EWD1 magnetic door contact binding process,the system adds 1 wireless Instant zone and 1 wireless Panic/Silent zone. The wireless zones are applied to the following EWD1 components respectively:

- **Magnetic contact -** by default, causing alarm if doors/windows is opened when system is armed.
- **Panic button** - by default, causing silent alarm instantly when pressed.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWD1:

- **By tamper button.** EWD1 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWD1 is illegally opened, the tamper button becomes unpressed. This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWD1 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

32.4.4. Battery Replacement

1. Open EWD1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

For more details, please refer to **32.4.2. Installation.**

ATTENTION: Only ER14505 Lithium Thionyl Chlorid AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

32.4.5. Restoring Default Parameters

1. Remove the battery from EWD1.
2. Press and hold the RESET button.
3. Insert the battery back to EWD1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

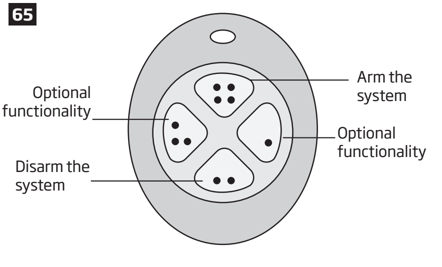
32.5. EWK1 - Wireless Keyfob

Main EWK1 features:

- Alarm system arming & disarming;
- Panic button;
- PGM output control;
- Sound indication by built-in mini buzzer.

Keyfob EWK1 – is a wireless device intended to arm and disarm ESIM264 alarm system, to open and close the gates or to control any other device connected to the alarm system. Wireless keyfob EWK1 is compatible with ELDES wireless alarm systems, therefore user can easily bind it to the alarm system using *ELDES Configuration Tool* software or sending a corresponding SMS command. EWK1 keyfob features four configurable buttons intended to operate according to individual needs. After the button is pressed, EWK1 internal buzzer's sound signal confirms a transferred command to ESIM264 alarm system via wireless connection. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button and holding it for 3 seconds. 3 short sound signals indicate a successfully carried out command while 1 long beep stands for failed command and feedback signal failure. By default one pair of buttons is already configured to arm and disarm the alarm system.

65



The virtual zones of ESIM264 system are intended for EWK1 button configuration. Please, refer to software's *ELDES Configuration Tool* HELP section for more details.

It is possible to connect up to 5 EWK1 devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

NOTE: Fig. No. 65 reflects the default EWK1 button configuration. All keyfob buttons are configurable according to individual needs.

32.5.1. Technical Specifications

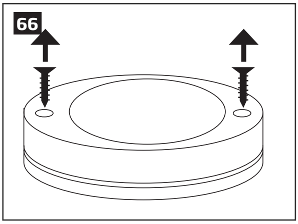
32.5.1.1. Electrical & Mechanical Characteristics

Battery Type	CR2032 Lithium
Battery Voltage; Capacity	3V; 240 mAh
Quantity of Batteries	1
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55°C
Wireless Keyfob Dimensions	54 x 42 x 13 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

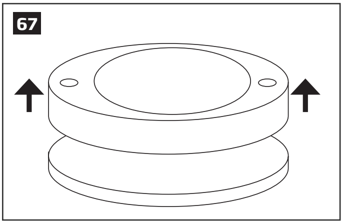
* The operation time depends on different conditions and may vary.

32.5.2. Installation

66

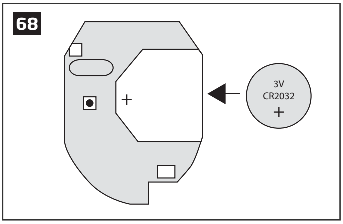


67



1. Unscrew the EWK1 keyfob housing.
2. Open EWK1 keyfob housing.
3. Insert CR2032 battery provided in the EWK1 package.
   Before inserting the battery, make sure that the battery's "+" sign is facing the outer side.

68



4. Close and screw up the keyfob housing.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. While binding the device to the alarm system, press any EWK1 button several times.
7. EWK1 is ready to use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **32.5.5. Restoring Default Parameters** for more details.

32.5.3. EWK1 Zones (Panic Button)

EWK1 keyfob supports a Panic Button feature allowing to cause alarm at any time when the specified button is pressed. This feature can be configured using *ELDES Configuration Tool* software by creating a virtual zone of Panic/Silent or 24-Hour type and assigning it to Virtual Alarm option. The Panic Button feature can be set up on any button of EWK1. For more details, please refer to software's HELP section.

32.5.4. Battery Replacement

1. Open EWD1 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

For more details, please refer to **32.5.2 Installation**.

ATTENTION: Only CR2032 3V batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

32.5.5. Restoring Default Parameters

1. Remove the battery from EWK1 keyfob.
2. Press and hold ∴ button.
3. Insert the battery back to EWK1.
4. Hold the button pressed until LED indicator provides several short flashes.
5. Release ∴ button.
6. Parameters restored to default.

32.6. EWS1 - Wireless Indoor Siren

Main EWS1 features:

- Audio alarm indication by built-in speaker.

EWS1 is a wireless device with built-in siren speaker and operates with ELDES wireless alarm systems. EWS1 has to be bind to the alarm system by sending a corresponding SMS text message or using software *ELDES Configuration Tool*. Upon successful EWS1 binding, the system adds one wireless zone and one wireless PGM output. The wireless zone is used to monitor the device (tamper - when the batteries are being removed) and the wireless PGM output is used to control the speaker. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS1 in order to save the battery power.

It is possible to connect up to 16 EWS1 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

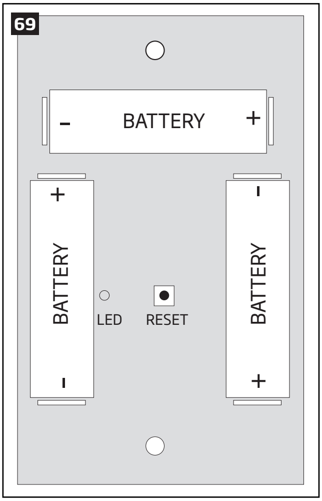
32.6.1. Technical Specifications

32.6.1.1. Electrical & Mechanical Characteristics

Battery Type	1,5V Alkaline AA type
Number of Batteries	3
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55°C
Dimensions	123x73x36mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Acoustic sound level	~97 dB measured at 1 m

* The operation time depends on different conditions and may vary.

69



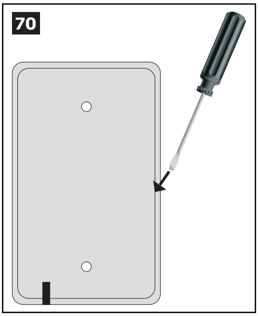
32.6.1.2. Main Unit & LED Functionality

RESET	Button for restoring default parameters
+ / -	Battery slots
LED	EWS1 status indication

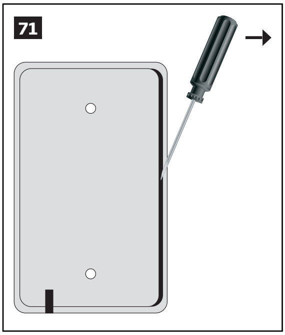
32.6.2. Installation

1. Open EWS1 enclosure.

70



71

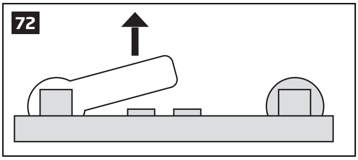


Insert a thin flat-shaped screwdriver or any tool alike into the gap located on the back of the enclosure (see Fig. No. 70).

Push the screwdriver down to the right carefully in order to detach the enclosure parts from each other (see Fig. No. 71).

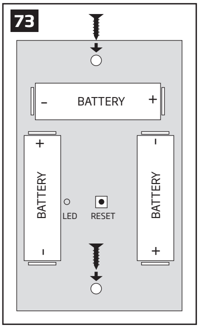
2. Once the enclosure is opened, remove the plastic tab inserted between one of the battery terminals and battery slot contact (see Fig. No. 72).

72



3. Fix the siren on the wall using the screws (see Fig. No. 73).

73



4. Close EWS1 enclosure. No tools are required for this action.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS1 closer to alarm system device and bind it again.
7. EWS1 siren is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **32.6.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.6.3. EWS1 Zone, PGM Output & Tamper

Upon successful EWS1 indoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS1 tamper control and the wireless PGM output is for siren control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. The wireless connection loss between EWS1 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

32.6.4. Battery Replacement

1. Open EWS1 enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS1
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **32.6.2 Installation**.

ATTENTION: Only CR2032 3V batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

32.6.5. Restoring Default Parameters

1. Remove any battery from EWS1.
2. Press and hold the RESET button.
3. Insert the battery back to EWS1.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

32.7. EWS2 – Wireless Outdoor Siren

Main EWS2 features:

- Audio alarm indication by built-in speaker;
- Visual alarm indication by built-in LED indicators;
- Range of operating temperature: -30...+55°C.

EWS2 is a wireless outdoor device with a built-in siren speaker, LED indicators and operates with ELDES wireless alarm systems. EWS2 has to be bind to the alarm system by sending a corresponding SMS text message or using software *ELDES Configuration Tool*. Upon successful EWS2 binding process, the system adds one wireless zone and one wireless PGM output. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS2 in order to save the battery power.

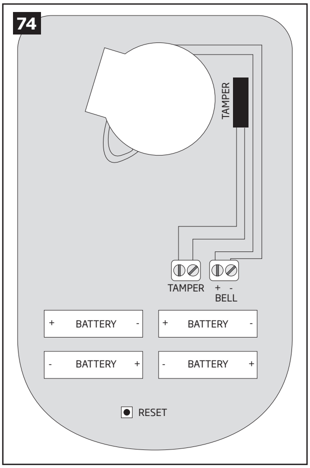
It is possible to connect up to 16 EWS2 devices to the alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

32.7.1. Technical Specifications

32.7.1.1. Electrical & Mechanical Characteristics

Battery Type	1,5V Alkaline AA type
Number of Batteries	4
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-30...+55°C
Dimensions	201 x 140 x 36 mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Acoustic sound level	~104 dB measured at 1 m

* The operation time depends on different conditions and may vary.

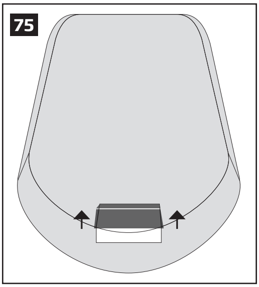

74

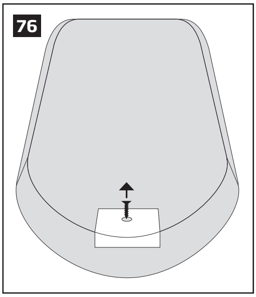
32.7.1.2. Main Unit, LED & Connector Functionality

RESET	Button for restoring default parameters
+ / -	Battery slots
LED indicators	Visual alarm indication
Tamper	Tamper button terminals
Bell+	Positive siren speaker terminal
Bell-	Negative siren speaker terminal

32.7.2. Installation

1. Open EWS2 enclosure.

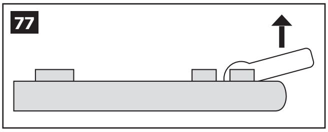

75


76

Remove the small blue lid located on the front side of the enclosure by pulling the lid up. (see Fig. No. 75).

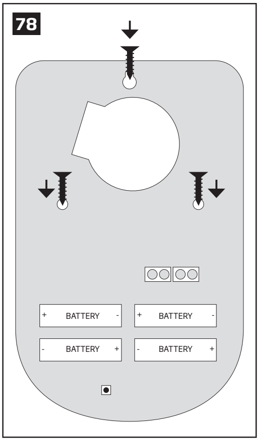
Unscrew the front side of the enclosure (see Fig. No. 76).

2. Once the enclosure is opened, remove the plastic tab inserted between one of the battery terminal and battery slot contact (see Fig. No. 77).


77

3. Fix the siren on the wall using the screws (see Fig. No. 78).

78



4. Close EWS2 enclosure (see Fig. No. 76, Fig. No. 75)
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS2 closer to alarm system device and bind it again.
7. EWS2 siren is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **32.7.6. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.7.3. EWS2 Zone, PGM Output & Tamper

Upon successful EWS2 outdoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS2 tamper control and the wireless PGM output is for siren control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWS2:

- **By tamper button.** EWS2 has a built-in tamper button intended for monitoring the enclosure status. Once the enclosure of EWS2 is illegally opened, the tamper button becomes unpressed. This action is followed by alarm which is sent by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWS2 and ESIM264 alarm system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

32.7.4. Battery Replacement

1. Open EWS2 enclosure.
2. Remove all 4 old batteries from the battery slots.
3. Postition the 4 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS2
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **32.7.2 Installation**.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using ELDES Configuration Tool software.

32.7.5. Restoring Default Parameters

1. Remove any battery from EWS2.
2. Press and hold the RESET button.
3. Insert the battery back to EWS2.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

32.8. EW1B - Battery-Powered Wireless Zone & PGM Output Expansion Module

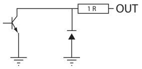
Main EW1B features:

- 2 zones for wired sensor connection;
- 2 PGM outputs for electrical appliance connection.

Wireless expansion module EW1B is a wireless device with 2 zones and 2 PGM outputs. This expansion module connects to ELDES wireless alarm systems and enables wireless access for to 2 wired devices such as movement PIR sensors, magnetic door contacts etc. In addition it allows to connect and control up to 2 appliances, i.e. lighting, heating etc. After the wiring process to EW1B it is necessary to bind EW1B to the alarm system by sending a corresponding command via SMS text message or using software *ELDES Configuration Too*l. t is possible to connect up to 16 EW1B devices to ESIM264 alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

32.8.1. Technical Specifications

32.8.1.1. Electrical & Mechanical Characteristics

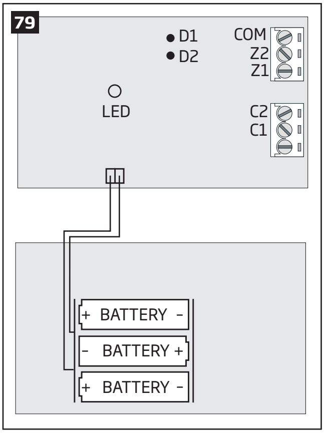
Battery Type	1,5V Alkaline AA type
Number of Batteries	3
Battery Operation Time	~18 months*
Number of Zones	2
Zone Connection Type	Normally closed (NC)
Number of PGM Outputs	2
EW1B PGM Output Circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum Commuting PGM Output Values	Voltage – 30V; current 500mA
Wireless Transmitter-Receiver Frequency	868 MHz
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Range of Operating Temperatures	-20...+55°C
EW1B PCB Dimensions	38x60x12mm
EW1B Enclosure Dimensions	90x110x40mm
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Enclosure rating	IP65

* The operation time depends on different conditions and may vary.

32.8.1.2. Connector & LED Functionality

COM	Common terminal for zones
Z2, Z1	Security zone terminals
C2, C1	PGM output terminals
D1, D2	Pins for restoring default parameters
LED	EW1B status

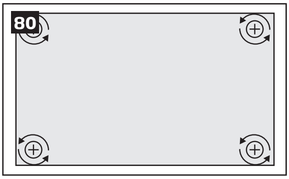
79



32.8.2. Installation

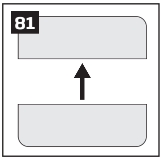
1. Push down the screwdriver and turn it counter-clockwise to unscrew EW1B enclosure (see Fig. No. 80)

80



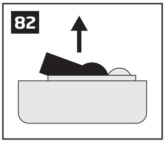
2. Detach the front side of the enclosure by pulling the front side up (see Fig. No. 81)

81



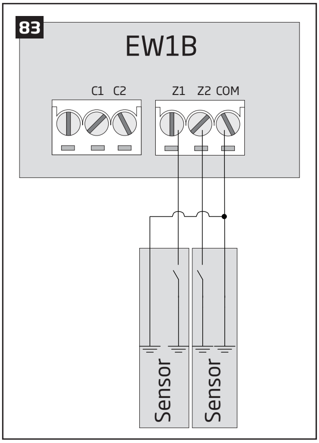
3. Remove the plastic tab inserted between one of the battery terminals and battery slot contacts (see Fig. No. 82).

82



4. Connect the ciruit as indicated in Fig. No. 83.

83



6. Close EW1B enclsoure (see Fig. No. 81, Fig. No. 80).
7. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
8. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EW1B closer to alarm system device and bind it again.
9. EW1B is ready for use.

NOTE: If you are unable to bind the wireless device please , restore the parameters of the wireless device to default and try again. See **33.8.5. Restoring Default Parameters** for more details.

ATTENTION: The minimum wireless connection range between the wireless device and wireless antenna of ESIM264 system can be 0,5 meters.

32.8.3. EW1B Zones, PGM Outputs & Tamper

Upon successful EW1B module binding process, the system adds 2 wireless Instant zones intended for wired sensor connection and 2 wireless PGM outputs intended for electrical appliance connection and control. The wireless connection loss between EW1B and ESIM264 alarm system leads to system alarm regardless of system being armed or disarmed. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

32.8.4. Battery Replacement

1. Open EW1B enclosure.
2. Remove all 3 old batteries from the battery slots.
3. Postition the 3 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals as indicated.
4. Insert the batteries into the battery slots.
5. Batteries replaced.

For more details, please refer to **32.8.2. Installation**.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using ELDES Configuration Tool software.

32.8.5. Restoring Default Parameters

1. Remove any battery from EW1B.
2. Short circuit (connect) pins D1 and D2.
3. Insert the battery back to EW1B.
4. Wait untill LED provides several short flashes.
5. Remove short-circuit from D1 and D2 pins.
6. Parameters restored to default.

32.9. EWF1 - Wireless Smoke Detector

Main EWF1 features:

- Photoelectric sensor for slow smouldering fires
- TEST button
- Non-radioactive technology for environmental friendly
- High and stable sensitivity
- Quick fix mounting plate for easy installation
- LED operation indicator
- Built-in speaker for audio alarm indication
- Auto-reset when smoke clears

EWF1 is a wireless photoelctric type smoke detector intended to use with ELDES wireless alarm systems. Photoelectric smoke detectors are generally more effective at detecting smouldering fires which smoulder for hours before bursting into flame. An optical method is used for the detection of visible smoke. When the concentration of smoke in the optical chamber exceeds a given threshold, EWF1 sounds the alarm and sends out a signal to the ESIM264 alarm system using the wireless connection and the system triggers the alarm. By default, when more than one EWF1 device is used, the system will automatically activate the interconnection feature (see **32.9.4. Interconnection**). ESIM264 system support up to 16 EWF1 devices, The maximum wireless connection range is 150 meters (in open areas).

32.9.1. Technical Specifications

32.9.1.1. Electrical & Mechanical Characteristics

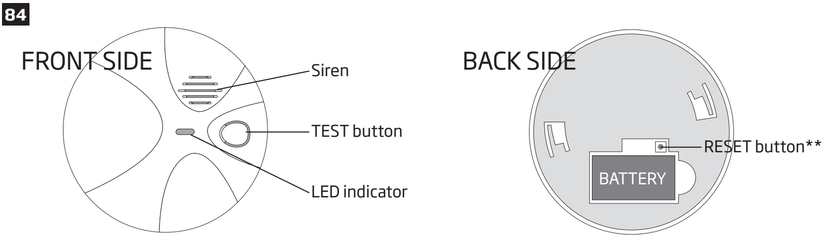
Detection Type	Photoelectric chamber
Alarm Sound Level	85 Decibels at 3 meters
Battery Voltage	9V
Battery Type	6F22 primary alkaline
Number of Batteries	1
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Range of Operating Temperatures	5oC to 45oC
Humidity	0-90% RH @ 0… +40 °C (non-condensing)
Sensitivity to Smoke	3.0-6.0 % Obs /m
Dimensions	110mm Ø
Compatible with Alarm Systems	ELDES Wireless
Acoustic sound level	~98 dB measured at 1 m

* The operation time depends on different conditions and may vary.

32.9.1.2. Main Unit & LED Functionality

TEST	Button for testing / button for testing and restoring default parameters (if RESET button not available)
LED	EWF1 status indication
SIREN	Built-in speaker for audio alarm indication
RESET**	Button for restoring default parameters

84



** Unavailaible on some EWF1 models

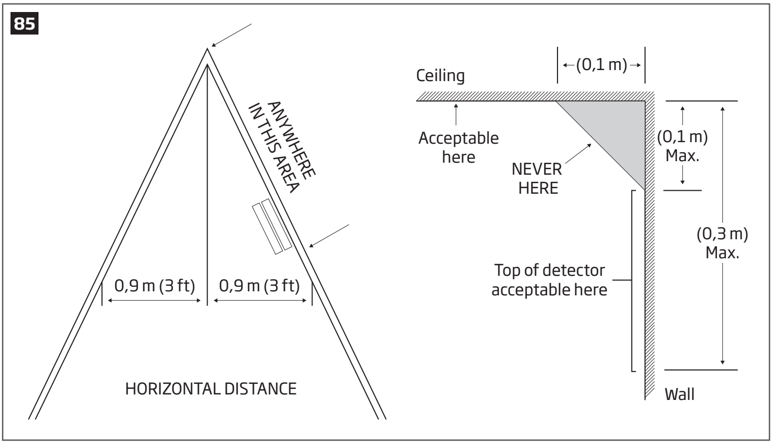
32.9.2. PLACEMENT

1. Install the wireless smoke detector as close to the center of the ceiling as possible. If this is not practical, mount no closer than 10 centimeters from a wall or corner. Also, if local codes allow, install wireless smoke detectors on walls, between 10 and 30 centimeters from ceiling/wall intersections.
2. Install a minimum of two wireless smoke detectors in every house, no matter how small the house is.
3. Install a wireless smoke detector in each room that is divided by a partial wall (either coming down from the ceiling at least 20 centimeters, or coming up from the floor).
4. Install a wireless smoke detector in lived-in attics or attics which ho use electrical equipment like furnaces, air conditioners, or heaters.

NOTE: For best protection we recommend that you install a wireless smoke detector in every room.

Recommended EWF1 placement locations

85



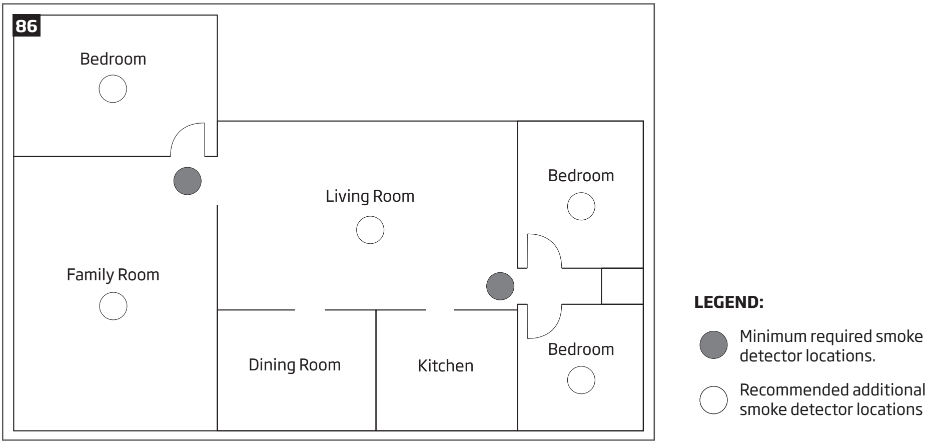
NOTE: Measurements shown are to the closest edge of the detector.

Typical Single-Story House

Install a wireless smoke detector on the ceiling or wall inside each bedroom and in the hallway outside each separate sleeping area. If a bedroom area hallway is more than 9 meters long, install a wireless smoke detector at each end.

If there is a basement: Install a wireless smoke detector on the basement ceiling at the bottom of the stairwell.

86


Bedroom
Living Room
Bedroom
Family Room
Dining Room
Kitchen
Bedroom
LEGEND:
● Minimum required smoke detector locations.
○ Recommended additional smoke detector locations

Typical Multi-Story or Split-Level House

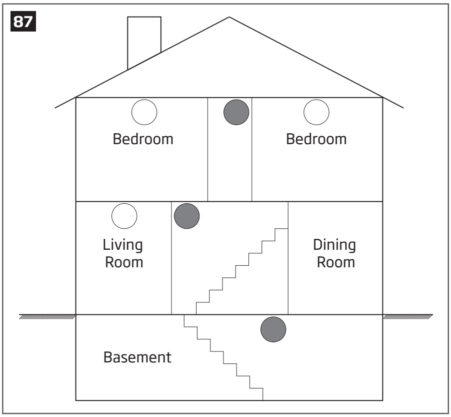
Install a wireless smoke detector on the ceiling or wall inside each bedroom and in the hallway outside each separate sleeping area. If a bedroom area hallway is more than 9 meter long, install a wireless smoke detector at each end. Please install a wireless smoke detector on the top of a first-to-second floor stairwell.

LEGEND:

● Minimum required smoke detector locations.

○ Recommended additional smoke detector locations

87



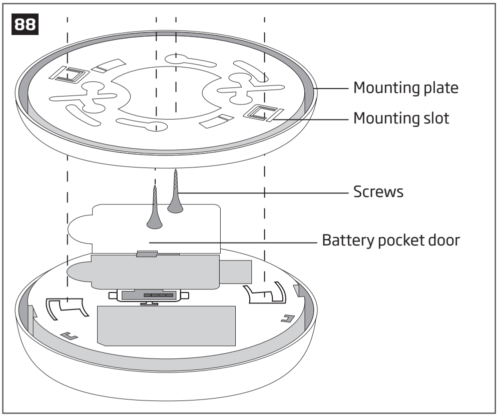
Incorrect EWF1 Placement

DO NOT place EWF1 in the following locations:

- Near appliances or areas where normal combustion regularly occurs (kitchens, near furnaces, hot water heaters). Use specialized wireless smoke detector with unwanted alarm control for this areas.
- In areas with high humidity, like bathrooms or areas near dishwashers or washing machines. Install at least 3 meters away from these areas.
- Near air returns or heating and cooling supply vents. Install at least 1 meter away from these areas. The air could blow smoke away from the detector, interrupting its alarm.
- In rooms where temperatures may fall below 5°C or rise above 45°C.
- In extremely dusty, dirty, or insect-infested areas where loose particles interfere with wireless smoke detector operation.

ATTENTION: Incorrect placement will result in a decrease of operational effectiveness.

32.9.3. Installation


88

1. Detach the mounting plate by turning it counter-clockwise from the back of EWF1 (see Fig. No. 88).
2. Secure the mounting plate to ceiling or wall with mounting screws.(see Fig. No. 88).
3. Lift to open the battery pocket door (see Fig. No. 88).
4. Insert the battery into the battery pocket considering the polarity terminals indicated on the enclosure of EWF1. Ensure the battery is securely connected. Red LED may flash briefly when the battery is being installed.
5. Close the battery pocket door by snapping it into place.
6. Position the smoke detector to the mounting plate by turning it clockwise to lock into place. Note that the device will not lock into the mounting plate without the battery being present in the battery pocket.
7. 7. Push the TEST button to verify if the wirless smoke detector is operational. See **32.9.5.1. Testing EWF1.**
8. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWF1 closer to alarm system device and bind it again.
10. EWF1 wireless smoke detector is ready for use.

NOTE: If you are unable to bind the wireless device, please restore the parameters of the wireless device to default and try again. See chapter **32.9.6. Restoring Default Parameters** for more details.

32.9.4. Interconnection

The interconnection feature automatically links all wireless smoke detectors resulting in causing an instant alarm in the system along with the rest of EWF1 wireless smoke detectors. For more details on interconnection feature and how to manage it, please refer to **20.4. EWF1 Interconnection.**

32.9.5. Maintenance

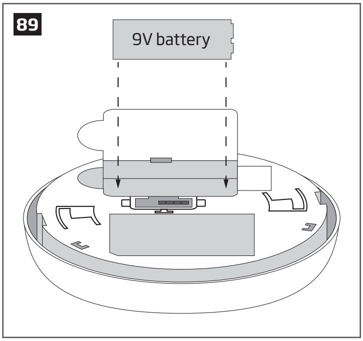
32.9.5.1. Testing EWF1

- The TEST button verifies if EWF1 is operational. Firmly push the TEST button and the wireless smoke detector will sound a loud beep. The alarm will stop sounding after releasing the TEST button. When testing EWF1 using *ELDES Configuration Tool* software, the detector will provide short beeps.
- Stand at arm's length from the wireless smoke detector when testing.
- Test wireless smoke detectors weekly and upon returning from vacation or when no one has been in the household for several days.
- Test each wireless smoke detector to be sure it is installed correctly and operating properly.
- DO NOT use an open flame to test this wireless smoke detector. You may ignite and damage the wireless smoke detector or your home.
- If the wireless smoke detector does not sound, please check the battery and signal level using *ELDES Configuration Tool* software.

ATTENTION: Test all wireless smoke detectors weekly to ensure proper operation.

32.9.5.2. Battery Replacement

89



1. Turn EWF1 counter-clockwise to detach it from the mounting plate.
2. Gently pull down the wireless smoke detector.
3. Remove the old battery from the battery pocket.
4. Postition the new 9V battery according to the appropriate battery slot positive/negative terminals indicated on the enclosure of EWF1. Ensure the plastic battery holder is fully depressed when the battery has been fitted.
5. Using the TEST button, test the wireless smoke detector to verify if it is operational. See **32.9.5.1. Testing EWF1.**
6. Re-attach the wireless smoke detector to the mounting plate by turning the wireless smoke detector clockwise until it snaps into place.

ATTENTION: Only 9V 6F22 primary alkaline type battery can be used. Install only new, high quality and unexpired batteries.

ATTENTION: The battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

NOTE: The system sends an SMS message to the preset user phone number as soon as the battery level runs below 5%.

32.9.6. Restoring Default Parameters

1. Remove the battery from EWF1.
2. Press and hold the RESET button.
3. Insert the battery back to EWF1.
4. Hold the RESET button until you hear a short beep.
5. Release the RESET button.

On some EWF1 models the RESET button is not available. On such EWF1 devices the reset process is as follows:

1. Remove the battery from EWF1.
2. Wait for 1 minute or more.
3. Press and hold the TEST button.
4. Insert the battery back to EWF1.
5. Hold the TEST button for 10 seconds or more.
6. Release the TEST button.

ATTENTION: EWF1 built-in speaker will sound while pressing and holding the TEST button. Please, ignore the sound.

32.9.7. Cleaning

Clean the wireless smoke detector at least once a month to remove dust, dirt, or debris. Using the soft brush or wand attachment of a vacuum cleaner, vacuum all sides and cover of wireless smoke detector. Be sure all the vents are free of debris.
If necessary, use a damp cloth to clean wireless smoke detector cover.

NOTE: Do not attempt to remove the cover to clean inside the wireless smoke detector. This will void your warranty.

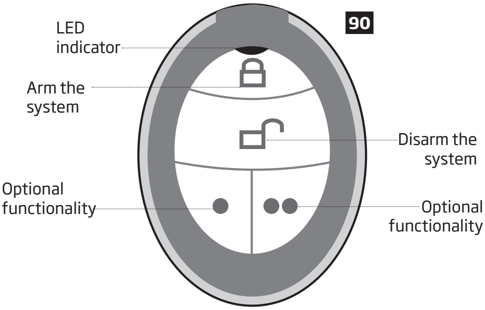
32.10. EWK2 - Wireless Keyfob

Main EWK2 features:

- Alarm system arming & disarming;
- Panic button;
- PGM output control;
- Sound indication by built-in mini buzzer;
- Visual indication by built-in LED indicator.

EWK2 is a wireless device intended to remotely arm and disarm ELDES alarm system, cause system alarm or to control any electric appliance connected to the alarm system's PGM output. In order to start using wireless keyfob EWK2, it has to be bound to ELDES wireless alarm system using *ELDES Configuration Tool* software or sending a corresponding SMS command. EWK2 keyfob features four configurable buttons intended to operate according to individual needs. After the button is pressed, EWK2 internal buzzer's sound signal and red LED indicator confirms a transferred command to ELDES alarm system via wireless connection. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button again and holding it for 3 seconds. 3 short sound signals and LED indicator flashes indicate a successfully carried out command, while 1 long beep and LED indicator flash stands for failed command and feedback signal failure. By default, one pair of buttons is already configured to arm and disarm the alarm system. It is possible to connect up to 5 EWK2 devices to ELDES alarm system at a time. The maximum wireless connection range is 150 meters (in open areas).

32.10.1. Technical Specifications



NOTE: Figure reflects the default EWK2 button configuration. All keyfob buttons are configurable according to individual needs.

32.10.1.1. Electrical & Mechanical Characteristics

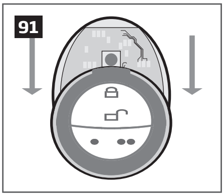
Battery Type	CR2032 Lithium
Battery Voltage; Capacity	3V; 240 mAh
Quantity of Batteries	1
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Range of Operating Temperatures	-20...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Dimensions	53 x 37 x 10 mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless

* The operation time depends on different conditions and may vary.

32.10.2. Installation

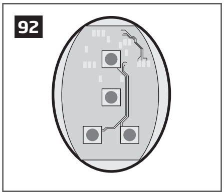
1. Open the EWK2 enclosure. Detach the front side of the enclosure by pulling the front side down

91

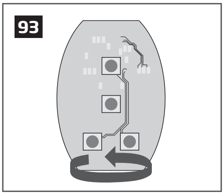


2. Once the enclosure is opened, remove the PCB from the EWK2 enclosure and flip the PCB so that the back side would be facing up.

92

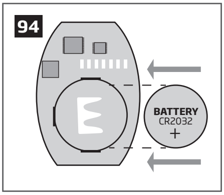


93



3. Insert the CR2032 type battery provided in the EWK2 package. Before inserting the battery, ensure that it is positioned plus-marked side up.

94



4. Insert the PCB back to the enclosure and close it.
5. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
6. While binding the device to the alarm system, press any EWK2 button several times.
7. EWK2 is ready for use.

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **32.10.5. Restoring Default Parameters** for more details.

32.10.3. EWK2 Zones (Panic Button)

EWK2 keyfob supports a Panic Button feature allowing to cause alarm at any time when the specified button is pressed. This feature can be configured using *ELDES Configuration Tool* by creating a virtual zone of Panic/Silent or 24-Hour type and assigning it to Virtual Alarm option. The Panic Button feature can be set up on any button of EWK2.

32.10.4. Battery Replacement

1. Open EWK2 enclosure.
2. Remove the old battery from the battery slot.
3. Postition the new battery according to the appropriate battery slot positive terminal indicated.
4. Insert the battery into the battery slot.
5. Battery replaced.

See **32.10.2. Installation** for more details.

ATTENTION: Only CR2032 3V battery can be used. Install only new, high quality and unexpired batteries.

ATTENTION: The battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset User 1 as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

32.10.5. Restoring Default Parameters

1. Press and hold ● and ●● buttons simultaneously.
2. Hold the buttons pressed until LED indicator and the buzzer provide several short flashes and beeps simultaneously.
3. Release the buttons.
4. Parameters restored to default.

32.11. EWD2 - Wireless Door Contact/Shock Sensor/Water Sensor

Main EWD2 features:

- Built-in shock sensor
- 2 wireless zones
- Available zone modes: magnetic door contact, shock sensor, water sensor, digital sensor
- 2 built-in tamper switches: on the front and on the back of the PCB

EWD2 is a wireless device intended to secure doors, windows or any other opening/clsoing mechanisms. In addition, the device comes equiped with a built-in shock sensor for vibration detection, an on-board zone terminal designed for external digital sensor or water sensor connection and 2 built-in tamper switches for EWD2 sabotage detection. In order to start using EWD2, it has to be bound to ELDES alarm system using *ELDES Configuration Tool* software or by sending a corresponding SMS text message to ELDES alarm system.

It is possible to connect up to 16 EWD2 devices to ESIM264 alarm system. The maximum wireless connection range is 150 meters (in open areas).

32.11.1. Technical Specifications

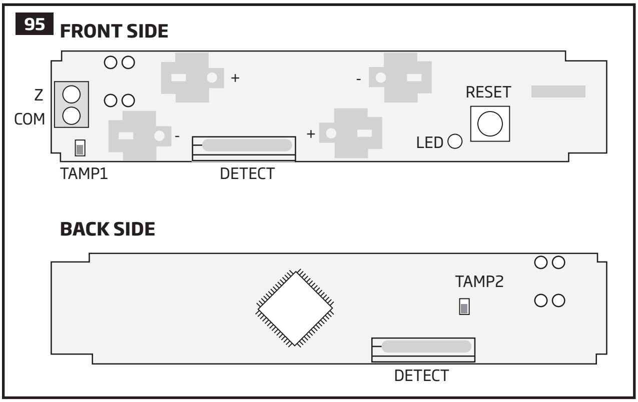
32.11.1.1. Electrical and Mechanical Characteristics

Batteries	1,5V Alkaline AAAA type, LR8 (IEC standard) / 25A (ANSI/NEDA standard)
Number of Batteries	2
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Range of Operating Temperatures	-20...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
EWD2 Dimensions	101 x 22 x 20 mm
Magnet Dimensions	47 x 17 x 10 mm
Compatible with Alarm Systems	ELDES Wireless

* The operation time depends on different conditions and may vary.

32.11.1.2. Main Unit and LED Functionality

95



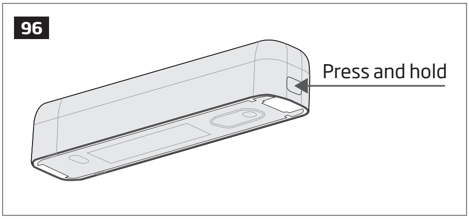
ATTENTION FOR EWD2 v1 AND EWD2 v2: If no sensor is to be connected to EWD2 on-board zone terminal, please make a short-circuit (connect) Z and COM terminals in order to avoid the unnecessary battery power usage.

Unit	Description
Z	Zone terminal
COM	Common terminal
TAMP1	Tamper switch
+ / -	Battery slots
DETECT	Magnet detector
LED	Light-emitting diode for indication of parameter restoring to default
RESET	Button for restoring default parameters
TAMP2	Tamper switch

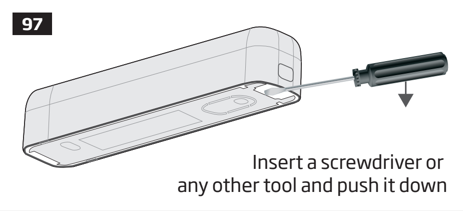
32.11.2. Installation

1. Remove the cover of EWD2 enclosure.

96

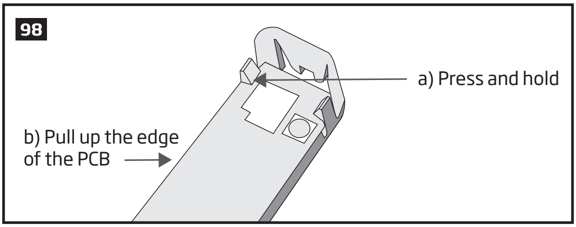


97



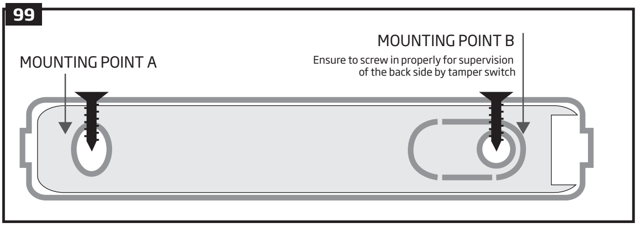
2. Remove the PCB (printed-circuit-board) from the enclosure.

98



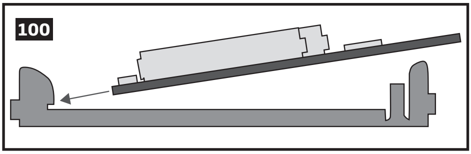
3. Screw in the enclsoure to the door or window jamb.

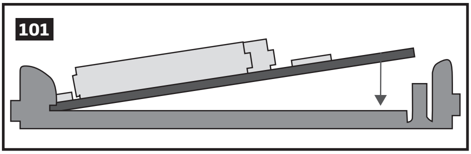
99

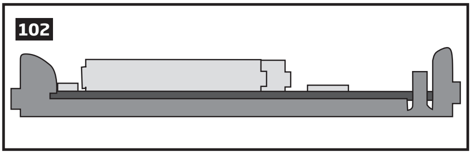

MOUNTING POINT A
MOUNTING POINT B
Ensure to screw in properly for supervision
of the back side by tamper switch

4. Wire up the external digital sensor (if any) or water sensor (if any) to Z and COM terminals, otherwise do not perform any wiring.

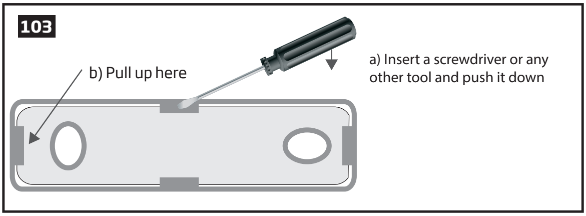
5. Insert the PCB back into the enclosure


100

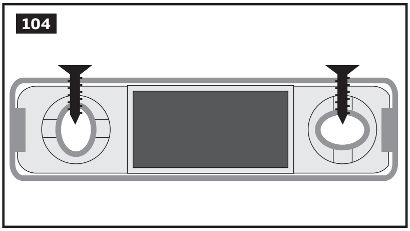

101

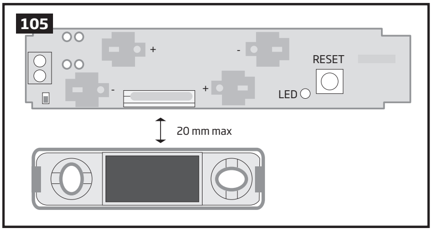

102

6. Remove the cover of the magnet enclosure.


103

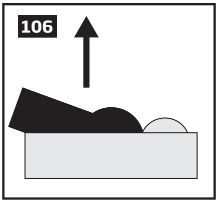
7. Screw in the magnet to the door or window frame and ensure that the magnet is fixed at the same height as the EWD2 magnet detector.


104


105

8. Cover the magnet. No tools are required for this action.

9. Remove the plastic tab inserted between one of the battery terminals and battery slots of EWD2.


106

10. Close EWD2 enclosure using the cover. No tools are required for this action.

11. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.

12. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWD2 closer to alarm system device and bind it again.

13. EWD2 is ready for use.

ATTENTION: Ensure that EWD2 device is properly fixed to the wall and the Mounting Point B portrayed in Fig. No. 99 is properly screwed in. Otherwise, the tamper switch will NOT supervise the back side of EWD2 enclosure (see also **32.11.3. EWD2 Zones and Tampers**).

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See **31.11.5. Restoring Default Parameters** for more details.

32.11.3. EWD2 Zones and Tampers

Upon successful EWD2 magnetic door contact binding process, the system adds 2 wireless Instant zones. The wireless zones can be set up to operate under one of the following modes each:

- **Zone 1:**
  - **Magnetic door contact** – Designed for causing an alarm (by default) if doors/windows are opened when the system is armed.
  - **External sensor** – Designed for causing an alarm (by default) if the wired digital sensor, connected to Z and COM terminals, is triggered when the system is armed. This mode does NOT operate with *Water sensor* mode on Zone 2 simultaneously.
- **Zone 2:**
  - **Shock sensor** – Designed for causing an alarm (by default) if the built-in shock sensor is triggered.

Possible zone mode combinations:

- **Zone 1:** Magnetic door contact + **Zone 2:** Shock sensor
- **Zone 1:** External Sensor + **Zone 2:** Shock sensor
- **Zone 1:** Magnetic door contact + **Zone2:** N/A
- **Zone 1:** External Sensor + **Zone2:** N/A
- **Zone 1:** N/A + **Zone 2:** Shock sensor

NOTE: *Water sensor* mode is not supported when EWD2 is used with ESIM264 alarm system.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWD2:

- **By tamper switch.** EWD2 comes equipped with 2 built-in tamper switches intended for enclosure supervision:
  - one located on the front side of the PCB supervising the front cover in case it is illegally opened (see Fig. No. 95).
  - the other one located on back of the PCB supervising the back side of the enclosure in case the EWD2 is illegally detached from the wall (see Fig. No. 95).

  Once the enclosure of EWD2 is tampered, the tamper switch will become triggered. This action will be followed by alarm, resulting in sending an SMS text message and/or phone call to the user. The SMS text message contains the violated tamper number.
- **By wireless connection loss.** The wireless connection loss between EWD2 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if both wireless zones are disabled.

For more details on EWD2 zone and tamper configuration, please refer to *ELDES Configuration Tool* software's HELP section.

32.11.4. Battery Replacement

1. Open EWD2 enclosure.
2. Remove both old batteries from the battery slots.
3. Insert the 2 new 1,5V Alkaline AAAA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB of EWD2.
4. Batteries replaced.

See **32.11.2. Installation** for more details.

ATTENTION: Only 1,5V Alkaline AAAA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

ATTENTION: The system sends an SMS message to a preset user phone number as soon as the battery level runs below 5%.

ATTENTION: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

32.11.5. Restoring Default Parameters

1. Remove any battery from EWD2.
2. Press and hold the RESET button.
3. Insert the battery back to EWD2.
4. Hold the RESET button until LED indicator provides several short flashes.
5. Release the RESET button.
6. Parameters restored to default.

32.12. EWS3 - Wireless Indoor Siren

Main features:

- Audio alarm indication by 2 built-in speakers.
- Visual alarm indication by built-in LED indicators: burglary/24-hour/tamper alarm and fire alarm indicated in different colours.
- 2 tamper switches: for enclosure opening and device detachment from the wall detection.

EWS3 is a wireless indoor device with built-in siren speakers and LED indicators operating with ELDES wireless alarm systems. The device is designed to notify the user by audio and visual signals in the event of alarm as well as in event of system arming/disarming (Bell Squawk feature must be enabled). In the event of burglary, 24-hour or tamper alarm, EWS3 will activate the speakers and flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator (both features require EWS3 Alarm LED and EWS3 Fire Alarm LED parameters to be enabled using *ELDES Configuration Tool* software or EKB2/EKB3 keypad)

To start using EWS3, it has to be bind to ELDES alarm system by sending a corresponding SMS message or using software *ELDES Configuration Tool*. Upon successful EWS3 binding process, the system adds one wireless zone and one wireless PGM output. In case of alarm, the siren provides a sound alarm for one minute. The configuration of this parameter is disabled for EWS3 in order to save the battery power.

It is possible to connect up to 16 EWS3 devices to ESIM264 alarm system. The maximum wireless connection range is 150 meters (in open areas).

32.12.1. Technical Specifications

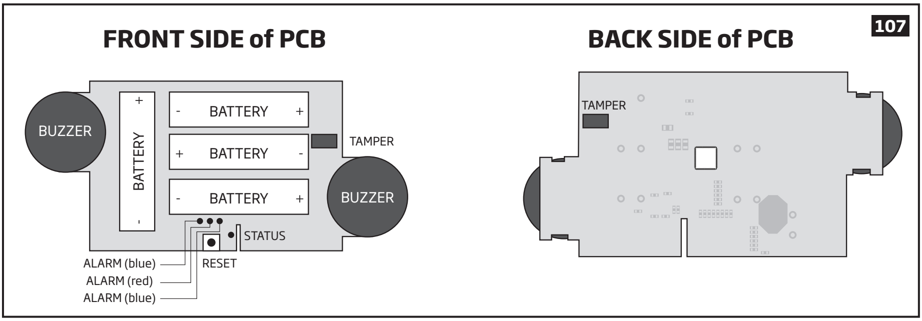
32.12.1.1. Electrical & Mechanical Characteristics

Battery Type	1,5V Alkaline AA type
Number of Batteries	4
Battery Operation Time	~18 months*
Wireless Transmitter-Receiver Frequency	868 Mhz
Rangeof Operating Temperatures	-25...+55°C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Dimensions	167 x 80 x 34 mm
Wireless Communication Range	Up to 30 meters in premises; up to 150 meters in open areas
Compatible with Alarm Systems	ELDES Wireless
Acoustic Sound Level	~90 dB measured at 1 m

* The operation time might vary in different conditions.

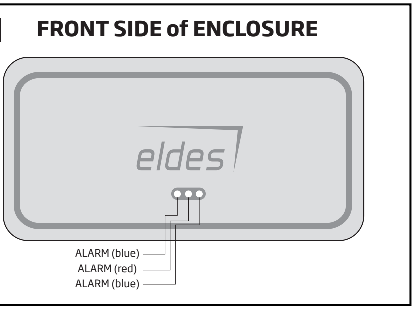
32.12.1.2. Main Unit, LED & Connector Functionality

107



RESET	Button for restoring default parameters
+ / -	Battery slots
STATUS	LED indicator for data transmission indication
ALARM (blue)	Blue LED indicators for visual alarm indication
ALARM (red)	Red LED indicator for visual alarm indication
BUZZER	Speakers for audio alarm indication
TAMPER	Tamper switches

108

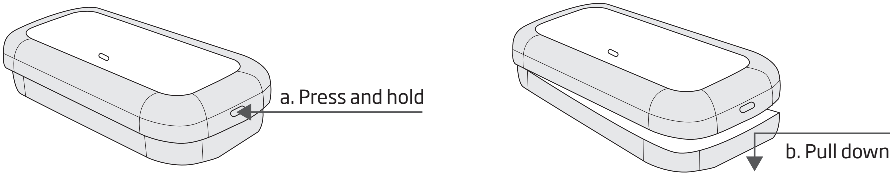


LED indication	Description
ALARM (blue) flashing	Burglary, 24-Hour or tamper alarm in progress
ALARM (red) flashing	Fire alarm in progress

32.12.2. Installation

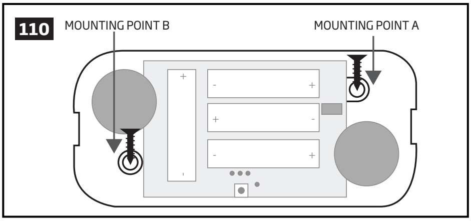
1. open EWS3 enclosure.

109

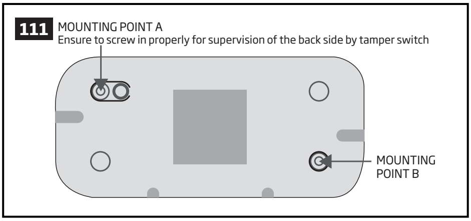


2. Once the enclosure is opened, fix the siren to the wall using the screws.

110



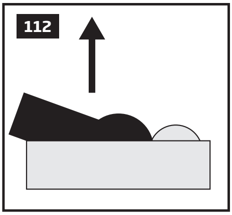
111


MOUNTING POINT A
Ensure to screw in properly for supervision of the back side by tamper switch
MOUNTING POINT B

3. Remove the plastic tab inserted between one of the battery terminals and battery slot contacts.

The wireless connection loss between EWS3 and ELDES alarm system leads to alarm. The system identifies this event as a tamper violation and sends an alarm by SMS text message and phone call to the user (-s) by default. The SMS
message contains the wireless device model, wireless ID code and tamper number.

112



4. STATUS indicator should start flashing indicating successful data transmission.
5. Close EWS3 enclosure by putting the cover back.
6. Bind the device to the alarm system by sending a corresponding command via SMS text message or using *ELDES Configuration Tool* software. Please, refer to the software's HELP section or refer to **19.1. Binding, Removing and Replacing Wireless Devices** for more details.
7. The system automatically informs about successful/unsuccessful binding process. If attempt to bind is unsuccessful, try to move EWS3 closer to alarm system device and bind it again.

ATTENTION: Ensure that EWS3 device is properly fixed to the wall and the Mounting Point A portrayed in Fig. No. 110 and Fig. No. 111 is properly screwed in. Otherwise, the tamper switch will NOT supervise the back side of EWS3 enclosure (see also **33.12.3. EWS3 Zone, PGM Output and Tamper**).

NOTE: If you are unable to bind the wireless device, please, restore the parameters of the wireless device to default and try again. See chapter **33.12.5. Restoring Default Parameters** for more details.

32.12.3. EWS3 Zone, PGM Output and Tamper

Upon successful EWS3 outdoor siren binding process,the system adds 1 wireless Instant zone and 1 wireless Siren PGM output. The wireless zone is intended for EWS3 tamper control and ability to assign a partition (-s), while the wireless PGM output is intended for siren speaker control.

In case of tamper violation, the alarm is caused regardless of system being armed or disarmed. There are 2 ways to detect tamper violation on EWS3:

- **By tamper switch.** EWS3 comes equipped with 2 built-in tamper switches intended for enclosure supervision:
  - one located on the front side of the PCB supervising the front cover in case it is illegally opened (see Fig. No. 107).
  - the other one located on back of the PCB supervising the back side of the enclosure in case the EWS3 is illegally detached from the wall (see Fig. No. 107).

Once the enclosure of EWS3 is tampered, the tamper switch will become triggered. This action will be followed by alarm, resulting in sending an SMS text message and/or phone call to the user. The SMS text message contains the violated tamper number.

- **By wireless connection loss.** The wireless connection loss between EWS3 and ESIM264 system leads to alarm. The system identifies this event as a tamper violation and sends alarm by SMS text message and phone call to the user (-s) by default. The SMS text message contains the violated tamper number and a star * character indicating wireless connection loss as a tamper alarm cause.

ATTENTION: The tamper will not operate if the wireless zone is disabled.

32.12.4. Battery replacement

1. open EWS3 enclosure.
2. Remove all 4 old batteries from the battery slots.
3. Postition the 4 new 1,5V alkaline AA type batteries according to the appropriate battery slot positive/negative terminals indicated on the PCB (printed-circuit-board) of EWS3
4. Insert the batteries into the battery slots.
5. Batteries replaced.

See chapter **33.12.2. Installation** for more details.

ATTENTION: Only 1,5V Alkaline AA type batteries can be used. Install only new, high quality and unexpired batteries. Do not mix the old batteries with the new ones.

ATTENTION: At least 1 battery must be removed if the device is not in use.

ATTENTION: In order to avoid fire or explosion hazards, the system must be used only with approved battery. Special care must be taken when connecting positive and negative battery terminals. Dispose old batteries only into special collection sites. Do not charge, disassemble, heat or incinerate old batteries.

NOTE: The system sends an SMS message to a preset user phone number as soon as the battery level runs below 5%.

NOTE: The battery status can be monitored in real-time using *ELDES Configuration Tool* software.

32.12.5. Restoring default parameters

1. Remove one battery from EWS3.
2. Press and hold the RESET button.
3. Insert the battery back to EWS3.
4. Hold the RESET button until LED indicator starts blinking.
5. Release the RESET button.
6. Parameters reset to default.

33. REMOTE SYSTEM RESTART

In some critical situations, a system restart may be required. To remotely carry out system restart, please refer to the following configuration method.

Restart the system

SMS

SMS text message content:
ssss_RESET
Value: *ssss* – 4-digit SMS password.
Example: *1111_RESET*

34. TECHNICAL SUPPORT

34.1. Troubleshooting

Indication	Possible reason
Indicator STAT is off	· No main power supply · Wiring done improperly · Blown fuse
Indicator NETW is off or flashing	· Missing SIM card · PIN code is enabled · SIM card is inactive · Disconnected antenna · GSM network signal too weak · Problems with GSM provider · Microcontroller is not started due to electrical mains noise or static discharge
System does not send any SMS text messages and/or does not ring	· SIM card credit balance depleted · Incorrect SMS centre phone number · No GSM network signal · User number is not added (or control from anu phone number is disabled) · SIM card changed before disconnecting main power supply or backup battery
Received SMS text message "Wrong syntax"	· Incorrect SMS text message structure · Extra space symbol could be left in SMS text message
Missing temperature indication in Info SMS text message/EKB2 keypad	· Temperature sensor not connected · Temperature sensor broken · Connection wires too long
24H and/or *Fire* zones do not work	· Specified zone must be enabled by SMS, ELDES Configuration Tool, EKB2 or EKB3 keypad.
No sound during remote listening	· Microphone not connected · Improper microphone connection

For product warranty repair service please , contact your local retail store where this product was purchased.
If your problem could not be fixed by the self-guide above, please contact your local distributor.

34.2. Restoring Default Parameters

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Power up the device for 7 seconds.
4. Power down the device.
5. Remove short circuit from DEF pins.
6. Parameters restored to default.

34.3. Updating the Firmware via USB Cable Locally

1. Disconnect the power supply and backup battery.
2. Short circuit (connect) DEF pins.
3. Connect the device via USB cable to the PC.
4. Power up the device.
5. The new window must pop-up where you will find the .bin file. Otherwise open *My Computer* and look for *Boot Disk* drive.
6. Delete the .bin file found in the drive.
7. Copy the new firmware .bin file to the very same window.
8. Power down the device.
9. Unplug USB cable.
10. Remove short circuit from DEF pins.
11. Power up the device.
12. Firmware updated.

NOTE: It is strongly recommended to restore default parameters after the firmware update.

34.4. Updating Firmware via GPRS Connection Remotely

ATTENTION: The system will NOT send any data to monitoring station while updating the firmware remotely via GPRS network. However, during the firmware update process, the data messages are queued up and transmitted to the monitoring station after the firmware upgrade process is over.

Before updating the firmware remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM CARD slot of Esim264 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to ESIM264.
- Default SMS password is changed to a new 4-digit password (see **6. PASSWORDS**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).
- APN, user name and password are set up (see **30.2.1. GPRS Network**).

Initiate FOTA

ESIM264 alarm system supports FOTA (firmware-over-the-air) feature. This allows to upgrade the firmware remotely via GPRS connection. Once the upgrade process is initiated, the system connects to the specified FTP server address where the firmware file is hosted and begins downloading and re-flashing the firmware. The firmware file must be located in a folder titled **Firmware**. In order to initiate the upgrade process please , send the following SMS message.

SMS

SMS text message content:
XXXX_FOTA:ftp-server-ip,port,firmware-file-name.bin,user-name,password

Value: *ssss* - 4-digit SMS password; *ftp-server-io* - public IP address of FTP server where EPIR firmware file is stored; *port* - port number of FTP server (usually - 21); *firmware-file-name.bin* - name of the firmware file, allowed max. length - up to 31 character; *user-name* - user name of FTP server login, allowed max. length - up to 31 character; *password* - password of FTP server login, allowed max. length - up to 31 character.
Example: *1111_FOTA:84.15.143.111,21,ESIM264fw bin,eldesuser,eldespassword*

ATTENTION: *Comma* character is NOT allowed to use in user name and firmware file name.

ATTENTION: "ELDES UAB" does not run a FTP server and does not host the firmware files online. Please, contact your local distributor to request the latest firmware file: support@eldes.lt

NOTE: It is strongly recommended to restore default parameters after the firmware update.

34.5. Frequently Asked Questions

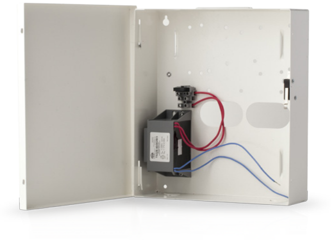
Question	Answer
1. Can ESIM264 operate as standalone device without SIM card inserted?	Yes, ESIM264 device can fully operate without any SIM card inserted. In this case you will not be able to configure and control the device by SMS and calls nor to receive any SMS reports and calls.
2. I am unable to arm the alarm system when one of the zones (some zones) is violated, although I was able to perform disarming. Is there a way to arm the alarm system while the zone is violated?	Due to security reasons it is recommended to restore the violated zone (-s) before arming the alarm system. However, you can enable a Force attribute or use the Bypass feature in order to arm the alarm system despite the violated zone (-s) being present. Please, refer to **14.5. Zone Type Definitions** and **14.7. Bypassing and Activating Zones**.
3. I have activated ATZ mode in *ELDES Configuration Tool* software, but I am unable to set the connection Type 5. Whenever I select Type 5 and press the "Write Settings" button it switches back to Type 4. What's wrong?	It appears that your *ELDES Configuration Tool* software is outdated. Please, download the latest *ELDES Configuration Tool* software version
4. When ESIM264 fully powers down my configuration becomes lost and I have to re-configure the device again. What's wrong?	This might have happened due to the jumper left on DEF pins or it is a hardware failure. Please, remove the jumper if it is present on DEF pins or contact your supplier for warranty service.
5. I have a smoke detector connected to ESIM264 system. How do I reset the smoke detector when the "Fire" zone is violated?	If the smoke detector is connected to one of the Esim264 PGM outputs you can reset it by turning the PGM output OFF and then back ON. This can be performed by SMS, EKB2 keypad, EKB3 keypad and *ELDES Configuration Tool* software. Please, refer to **18.4. Turning PGM Outputs ON and OFF.**
6. What happens if I switch backup battery pole terminals places?	Switching backup battery pole terminals places is forbidden. Otherwise this will lead to blown fuse and ESIM264 alarm system will have to be repaired.
7. How do I disable SMS reports and calls in case of tamper violation when alarm system is disarmed?	The SMS reports on tamper violation can be disabled by EKB2, EKB3 keypads or *ELDES Configuration Tool* software. For mor details, please refer to **16. TAMPERS** or to the software's HELP section. However, due to security reasons it is not recommended to disable this feature.
8. Is any additional configuration necessary when connecting EPGM1 module after wiring is done accroding to EPGM1 user manual?	No additional configuration is required in order to make EPGM1 module operational.
9. Does the number of EPGM1 zones duplicate when ATZ mode is activated in the system?	No, the number of EPGM1 zones does not duplicate in ATZ mode as EPGM1 module does not support ATZ mode. Only ESIM264 zones duplicate in ATZ mode.
10. I connect the wired siren to ESIM264 and I hear a silent sound alarm even when the alarm system is disarmed. In case of alarm system alarm the siren provides a loud sound alarm as it should. Why?	Please, connect the resistor of 3,3 kΩ nominal to the BELL- / BELL+ contacts This should solve the problem.
11. I am using Windows operating system. The windows of *ELDES Configuration Tool* are not fully displayed and some parts are like cut-off. What's wrong?	Please, update *ELDES Configuration Tool* software
12. The buzzer remains active when I disarm the alarm system using the keypad. Why?	The buzzer is intended for iButton indication only and it is not related to disarming process by keypad.
13. One of wireless devices connected to ESIM264 system sends a tamper alarm from time to time, although no tamper was violated. Why?	This happens due to wireless connection loss. There might be several reasons: 1. ELDES wireless device is installed too close or too far from ESIM264 system. 2. Interference of other electronic equipment. 3. Physical interference (building walls, floors etc.) 4. Metal material interference.
14. I have connected a wired magnetic door sensor, but I receive tamper alarm instead of zone alarm. What's wrong?	This happens due to incorrect resistor connection. Please, refer to corresponding connection circuit according to the selected zone connection type (Type 1 – 5). See **2.3.2 Zone Connection Types** for more details.
15. I disconnected the backup battery, but did not receive any SMS report on this event. How do I enable SMS report on backup battery disconnection?	By default, this notification is enabled. The system checks the backup battery resistance once a day and sends an SMS report to User 1 on backup battery replacement if more than 2Ω resistance is detected. For more details, please refer to **21. BACKUP BATTERY, MAINS POWER SUPPLY STATUS MONITORING AND MEMORY.**

Question	Answer
16. When I check system SIM card credit balance I see a lot of SMS delivery confirmation reports. How do I disable SMS delivery confirmation ESIM264 system?	Every time an SMS text message is sent to the user, the system must "know" that the message was successfully delivered. The only way to partly disable the SMS delivery report (for alarm notifications only) is to enable alarm SMS notifications to all users. This is useful when having only User1 phone number set up, as in case of alarm the system sends the alarm SMS text message to all preset users simultaneously, but does not require any SMS delivery report.
17. I have set zone names and/or PGM output names containing some Cyrillic and/or non-English characters. The zone names and PGM output names do not fully fit in the SMS message. What's wrong?	According to GSM standards 1 SMS text message may consist of up to 160 Latin alphabet/English characters maximum. If the message contains at least one non-latin/non-English character, the length of SMS message becomes at least half shorter, since those characters occupy more size of the SMS text message than the Latin ones. It is recommended not to use any non-Latin/ non-English characters in zone names and PGM output names.
18. The configuration of added wireless keyfob EWK1 to ESIM264 system is not visible in *ELDES Configuration Tool*. What's wrong?	*ELDES Configuration Tool* version is too old. Please, update it.
19. I am unable to run *ELDES Configuration Tool* - I receive error messages in Windows. Why?	Microsoft .NET Framework v3.5 is not installed in Windows system. Please, download this package from official Microsoft website free of charge and install it to your Windows system.
20. Info SMS report comes with wrong date and time. How do I correct it?	Please, set the correct system date and time using either *ELDES Configuration Tool*, EKB2, EKB3 keypad or SMS text message.
21. I receive an error message when attempting to configure the device or update the firmware remotely. Whats wrong?	It appears that the device is unable to establish a communication with configuration / FTP server. Please, check the GPRS settings in ESIM264 configuration (APN, user name, password), the location of the firmware ..bin file (must be located in the FTP server folder titled **Firmware**) and the mobile internet feature presence on the SIM card used with ESIM264. If this does not solve the problem, please contact your GSM operator (and ISP - for remote configuration problems) in order to request a list of blocked TCP ports.
22. I waited for at least 5 minutes, but did not receive any SMS message confirming that remote configuration via GPRS connection has stopped. What's wrong?	1. Send the *ssss_endconfig* SMS text message. 2. In *ELDES Configuration Tool* software press Disconnect button and repeat the steps from the beginning as described in **5.1. Remote System Configuration via GPRS Connection.**

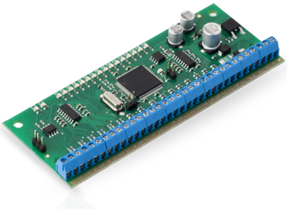
35. RELATED PRODUCTS

EKB2 - LCD keypad

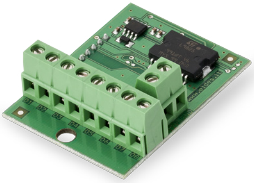
EKB3 - LED keypad



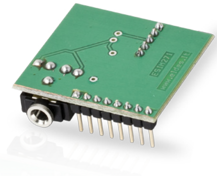
ME1 - metal cabinet



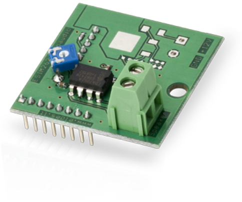
EPGM1 - hardwired zone and PGM output expansion module



EPGM8 - hardwired PGM output expansion module



EA1 - audio output module



EA2 - audio output module with amplifier

DS1990A-F5 - iButton key

DS18S20 - temperature sensor

ED1T - plastic enclosure with iButton key reader and temperature sensor

EWP1 - wireless PIR sensor (motion detector)

EWD1 - wireless magnetic door contact

EWS2 - wireless external siren

EWS1 - wireless internal siren

EWK1 - wireless keyfob

EWF1 – wireless smoke detector

EW1 - wireless zone and PGM output expansion module

EW1B - battery-powered wireless zone and PGM output expansion module

EWD2 - wireless door contact/shock sensor

EWK2 - wireless keyfob

EWS3 - wireless indoor siren