

eldes®

ESIM264

GSM ALARM AND MANAGEMENT SYSTEM

INSTALLATION MANUAL

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

Installation Manual v3.3

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 and 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.



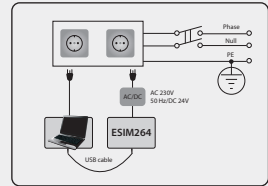
The system must be powered by main 16-24V 50 Hz ~1.5A max or 18-24V --- 1,5A max DC power supply which must be approved by LST EN 60950-1 standard and be easily accessible nearby the device. When connecting the power supply to the system, switching the pole terminals places does not have any affect.



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



The 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 (0.12in) 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 mains power 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.

Contents

1. GENERAL INFORMATION	6
1.1. Functionality	6
1.2. Compatible Device Overview	6
1.3. Default Parameters and Ways of Parameter Configuration	6
2. Technical Specifications	10
2.1. Electrical and Mechanical Characteristics	10
2.2. Main Unit, LED and Connector Functionality	11
2.3. Wiring Diagrams	12
3. INSTALLATION	18
4. GENERAL OPERATIONAL DESCRIPTION	22
5. CONFIGURATION METHODS	23
5.1. SMS Text Messages	23
5.2. EKB2 LCD Keypad	23
5.3. EKB3 LED Keypad	23
5.4. ELDES Configuration Tool Software	24
6. PASSWORDS	25
7. SYSTEM LANGUAGE	26
8. USER PHONE NUMBERS	27
8.1. System Control from any Phone Number	28
9. DATE AND TIME	29
10. USER CODES	30
11. iBUTTON KEYS	32
11.1. Adding and Removing iButton Keys	32
12. ARMING AND DISARMING	34
12.1. Free of Charge Phone Call	34
12.2. SMS Text Message	35
12.3. EKB2 Keypad and User Code	35
12.4. EKB3 Keypad and User Code	36
12.5. iButton Key	37
12.6. EWK1/EWK2 Wireless Keyfob	37
12.7. Arm-Disarm by Zone	38
12.8. Disabling and Enabling Arm/Disarm Notifications	39
13. EXIT AND ENTRY DELAY	41
14. ZONES	43
14.1. Zone Numbering	43
14.2. Zone Expansion	43
14.3. 6-Zone Mode	43
14.4. ATZ (Advanced Technology Zone) Mode	44
14.5. Zone Type Definitions	45
14.6. Zone Attributes	46
14.7. Bypassing and Activating Zones	48
14.8. Zone Names	49
14.9. Disabling and Enabling Zones	50
15. STAY MODE	51
16. TAMPERS	52
16.1. Tamper Names	52
17. ALARM INDICATIONS AND NOTIFICATIONS FOR USER	53
17.1. Enabling and Disabling Alarm Notifications	54
18. PROGRAMMABLE (PGM) OUTPUTS	57
18.1. PGM Output Numbering	57
18.2. PGM Output Expansion	57
18.3. PGM Output Names	58
18.4. Turning PGM Outputs ON and OFF	58
18.5. PGM Output Control by Event and Scheduler	60
18.6. Wireless PGM Output Type Definitions	61

Contents

19. WIRELESS DEVICES	62
19.1. Pairing, Removing and Replacing Wireless Device	62
19.2. Wireless Device Information	63
19.3. Wireless Signal Status Monitoring	64
19.4. Disabling and Enabling Siren if Wireless Signal is Lost	64
19.5. EWT1 - Wireless Transmitter-Receiver	65
19.6. EWF1 - Wireless Smoke Detector	66
20. WIRED SIREN/BELL	68
20.1. Bell Squawk	69
20.2. Indication by EWS2 - Wireless Outdoor Siren Indicators	69
20.3. Indication by EWS3 - Wireless Indoor Siren Indicators	70
21. BACKUP BATTERY, MAINS POWER STATUS MONITORING AND MEMORY	71
21.1. Backup Battery Status Monitoring	71
21.2. Mains Power Status Monitoring	72
21.3. Memory	73
22. GSM CONNECTION STATUS MONITORING	74
23. PARTITIONS	74
23.1. Zone Partition	74
23.2. User Phone Number Partition	74
23.3. Keypad Partition and Keypad Partition Switch	75
23.4. User Code Partition	76
23.5. iButton Key Partition	76
23.6. EWK1/EWK2 Wireless Keyfob Partition	76
24. TEMPERATURE SENSOR	77
24.1. Adding, Removing and Replacing Temperature Sensors	77
24.2. Setting Up MIN and MAX Temperature Boundaries. Temperature Info SMS	77
25. REMOTE LISTENING AND 2-WAY VOICE COMMUNICATION	79
26. SYSTEM INFORMATION. INFO SMS	80
26.1. Periodic Info SMS	80
27. SYSTEM NOTIFICATIONS	82
27.1. SMSC (Short Message Service Center) Phone Number	84
28. EVENT LOG	85
29. INDICATION OF SYSTEM FAULTS	86
30. MONITORING STATION	87
30.1. Data Messages - Events	88
30.2. Communication	92
31. WIRED DEVICES	102
31.1. RS485 Interface	102
31.2. 1-Wire Interface	108
31.3. Modules Interface	108
32. REMOTE SYSTEM RESTART	111
33. TECHNICAL SUPPORT	112
33.1. Troubleshooting	112
33.2. Restoring Default Parameters	112
33.3. Updating the Firmware via USB Cable Locally	112
33.4. Updating Firmware via GPRS Connection Remotely	113
33.5. Frequently Asked Questions	113
34. RELATED PRODUCTS	115

TERMS OF USE

The following terms and conditions govern use of the ESIM264 device and contains important information on limitations regarding the product's use and function, as well as information on the limitations of the manufacturer's liability. Please carefully read these terms and conditions. For more information on your product, please visit eldesalarms.com

TECHNICAL SUPPORT

In order to ensure continuous and proper operation of the ESIM264 device and uninterrupted service, it is the responsibility of the User to make sure that: (i) the product is properly installed, and (ii) there is constant internet or GSM connection and electrical supply (low battery must be replaced in time).

If you experience difficulty during the installation or subsequent use of the system, you may contact ELDES, UAB distributor or dealer in your country/region. For more information see eldesalarms.com

WARRANTY PROCEDURES

Warranty and out of warranty service should be obtained by contacting the system integrator/dealer/retailer/e-tailer or distributor where the customer purchased the product. When requesting for service, the proof of purchase and the product serial number must be provided. The return of the defective product should be strictly through the original route of purchase, and the customers shall pack the product appropriately to prevent the returned product from suffering in the transportation.

MANUFACTURER WARRANTY

ELDES provides a limited warranty for its products only to the person or entity that originally purchased the product from ELDES or its authorized distributor or retailer and only in case of defective workmanship and materials under normal use of the system for a period of twenty four (24) months from the date of shipment by the ELDES, UAB (Warranty Period). Warranty obligations do not cover expandable materials (power elements and/or batteries), holders and enclosures. The warranty remains valid only if the system is used as intended, following all guidelines outlined in this manual and in accordance with the operating conditions specified. The warranty is void if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or force majeure factors.

If a hardware defect arises and a valid claim is received within the Warranty Period, at its own discretion, ELDES, UAB will either (a) repair a hardware defect at no charge, using new or refurbished replacement parts, or (b) exchange the product with a product that is new or which has been manufactured from new or serviceable used parts and is at least functionally equivalent to the original product, or (c) refund the purchase price of the product.

LIMITED LIABILITY

The buyer must agree that the system will reduce the risk theft, burglary or other dangers but does not provide guarantee against such events. ELDES, UAB will not assume any responsibility regarding personal or property, or revenue loss while using the system. ELDES, UAB is not affiliated with any of the internet providers, therefore, it shall not be responsible for the quality of internet service.

ELDES, UAB shall also assume no liability due to direct or indirect damage or loss, as well as unrecieved income when using the system, including cases, when the damages arise due to the above mentioned risks, when due to breakdown or malfunction the user is not informed in a timely manner about a risk which has arisen. In any case, the liability of ELDES, UAB, as much as it is allowed by the laws in force, shall not exceed the price of acquisition of the product.

CONSUMER PROTECTION LAWS

FOR CONSUMERS WHO ARE COVERED BY CONSUMER PROTECTION LAWS OR REGULATIONS IN THEIR COUNTRY OF PURCHASE OR, IF DIFFERENT, THEIR COUNTRY OF RESIDENCE, **THE BENEFITS CONFERRED BY THIS WARRANTY ARE IN ADDITION TO ALL RIGHTS AND REMEDIES CONVEYED BY SUCH CONSUMER PROTECTION LAWS AND REGULATIONS.** This warranty grants upon you specific legal rights, and you may also have other rights that vary by country, state or province.

DISPOSAL AND RECYCLING INFORMATION



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 of 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.

Content of Pack

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

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.

Copyright © "ELDES UAB", 2016. All rights reserved

It is strictly forbidden to copy and distribute the information contained in this document or to pass thereof to a third party without an a priori written authorization obtained from ELDES, UAB. ELDES, UAB reserves the right to update or modify this document and/or related products without an a priori warning. ELDES, UAB hereby declares that GSM alarm and management system ESIM264 is in compliance with the essential requirements and other relevant provisions of the Directive 1999/5/EC. The declaration of conformity is available at eldesalarms.com.

CE 1383

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. Connectible 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. Connectible Devices
EWD2	Wireless magnetic door contact/shock sensor/flood sensor	16***
EWK1****	Wireless keyfob with 4 buttons	5****
EWK2****	Wireless keyfob with 4 buttons	5****
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 16 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 and Ways of Parameter Configuration

Main Settings					
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
SMS and EKB2 Menu Language	Depends on firmware version according to user's location	✓	✓	✓	✓
SMS Password	0000	✓	✓	✓	✓
User Code 1	1111		✓	✓	✓
User Code 2... 30	N/A		✓	✓	✓
Administrator Password	1470		✓	✓	✓
Duress Password	N/A		✓	N/A	✓
SGS Password	N/A		✓	✓	✓
User 1... 5 Phone Number	N/A	✓	✓	✓	✓
Allow Control from Any Phone Number	Disabled	✓	✓	✓	✓
Date and Time	N/A	✓	✓	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	✓			✓

Zones

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
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		✓	✓	✓
Alarm Count to Bypass	0				✓
Arm-Disarm by Zone	N/A		✓	✓	✓
Force attribute 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 and 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 and 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	✓	✓	✓	✓

Mains power Status

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
Mains power Loss Delay	30 seconds		✓	✓	✓
Mains 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		✓	✓	✓
Mains Power Loss Event Enabled	Enabled	✓	✓	✓	✓
Mains 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		✓	✓	✓
Keypad 1... 4 Partition	PART0		✓	✓	✓
Keypad Partition Switch	Disabled		✓	✓	✓
User Code 1... 30 Partition	PART0		✓	✓	✓
User 1... 5 Phone Number Partition	PART0		✓	✓	✓
iButton 1... 5 Partition	PART0		✓	✓	✓
Zone Partition	PART0		✓	✓	✓

Monitoring Station

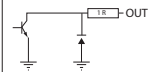
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3	Configuration Tool
MS Mode	Disabled	✓	✓	✓	✓
Data Messages	All Enabled		✓	✓	✓
Account (Alarm System ID)	9999		✓	✓	✓
Monitoring Station Phone Number 1... 3 (Voice Calls/SMS)	N/A		✓	✓	✓
Attempts (Voice Calls/SMS)	3		✓	✓	✓
Monitoring Station Phone 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				✓

2. TECHNICAL SPECIFICATIONS

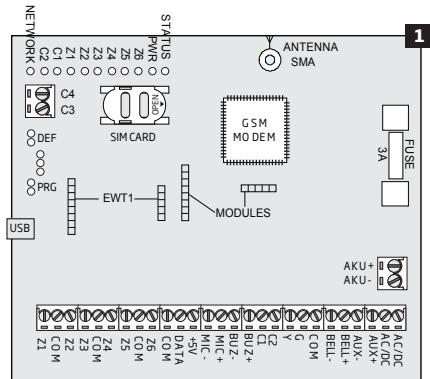
2.1. Electrical and Mechanical Characteristics

Electrical and Mechanical Characteristics	
Mains power	16-24V 50 Hz ~1.5A max / 18-24V $\overline{\text{---}}$ 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
Backup battery charge current	Up to 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	5,6k Ω (ATZ Mode: 5,6k Ω and 3,3k Ω)
Number of PGM outputs on-board	4
On-board PGM output circuit	 <p>Open Collector Output. Output is pulled to COM when turned ON.</p>
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 100m (328.08ft)
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
BELL + AUX: Maximum accumulative current of auxiliary equipment and siren	1 A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100m (328.08ft)
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 30m (98.43ft)
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 100m (328.08ft)
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2m (6.56ft)
MIC: Cable type for microphone connection	Unshielded
Wireless band	ISM868 /ISM 915
Wireless communication range	Up to 30m (98.43ft) in premises; up to 150m (492.13ft) 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 (5.51x3.94x0.71in)
Operating temperature range	-20...+55°C (-4... 131°F)
Humidity	0-90% RH @ 0... +40°C (0-90% RH @ 32... 104°F) (non-condensing)

2.2. Main Unit, LED and 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 EPGMB module
EWT1	Slots for EWT1 wireless module



LED Functionality

NETWORK	GSM network signal strength and status
C2, C1	PGM output C1 and C2 status. Steady ON = turned ON; OFF = turned OFF
Z1	Zone Z1 state (ATZ mode: Z1 and Z7). Steady ON = violated; OFF = restored.
Z2	Zone Z2 state (ATZ mode: Z2 and Z8). Steady ON = violated; OFF = restored.
Z3	Zone Z3 state (ATZ mode: Z3 and Z9). Steady ON = violated; OFF = restored.
Z4	Zone Z4 state (ATZ mode: Z4 and Z10). Steady ON = violated; OFF = restored.
Z5	Zone Z5 state (ATZ mode: Z5 and Z11). Steady ON = violated; OFF = restored.
Z6	Zone Z6 state (ATZ mode: Z6 and Z12). Steady ON = violated; OFF = restored.
PWR	Power supply status. Steady ON = power supply OK; OFF = no power.
STATUS	Micro-controller status. Flashing = micro-controller OK; OFF = micro-controller fault.

NETWORK indication

Description

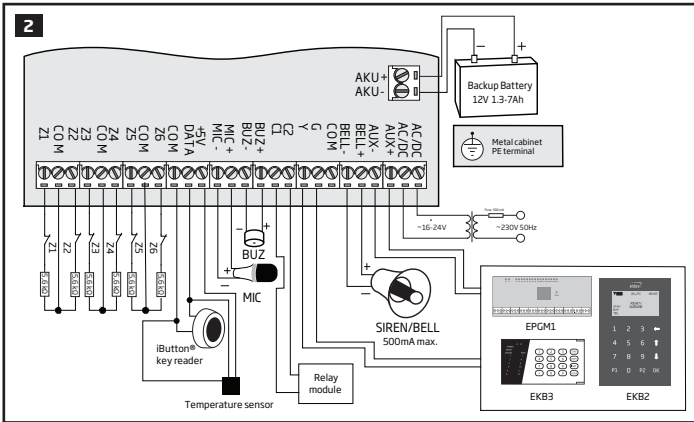
OFF	No GSM signal - SIM card missing; PIN code enabled on SIM card; GSM antenna disconnected or faulty; GSM operator's fault; GSM signal unavailable in the are
Flashing every 3 sec.	Poor GSM signal strength
Flashing every 1 sec.	Medium GSM signal strength
Flashing several times per sec.	Good GSM signal strength
Steady ON	Excellent GSM signal strength

Connector Functionality

Z1 - Z6	Security zones
COM	Common terminal for all zones
DATA	1-Wire® interface for iButton® key and 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	Mains power terminal
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

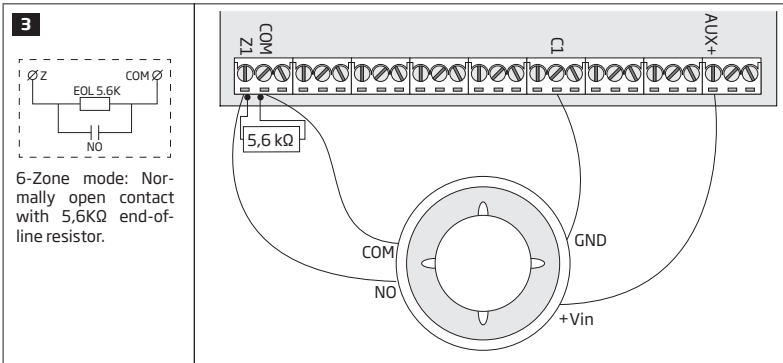
2.3. Wiring Diagrams

2.3.1. General Wiring

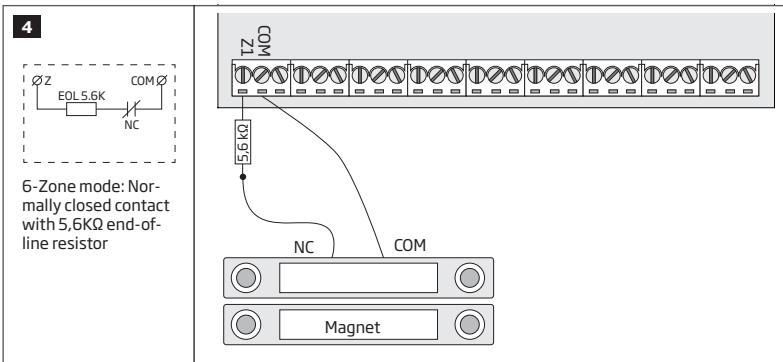


2.3.2. Zone Connection Types

Type 1 Example of 4-wire smoke detector wiring



Type 2 Example of magnetic door contact wiring

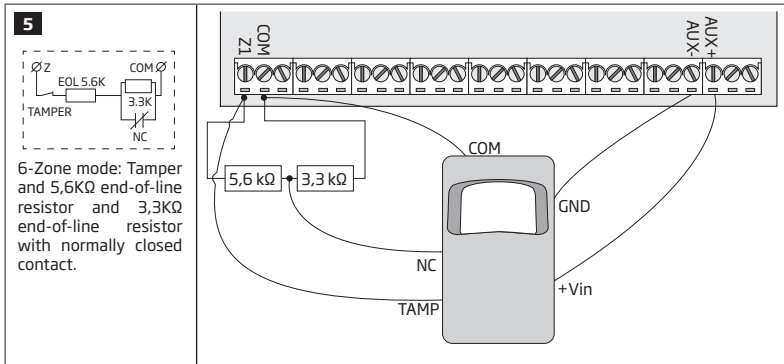


NOTE: Based on the example given, in the event of an alarm, the smoke detector could be reset by turning OFF and ON the PGM output C1. For more details, please refer to **18.4. Turning PGM Outputs ON and OFF.**

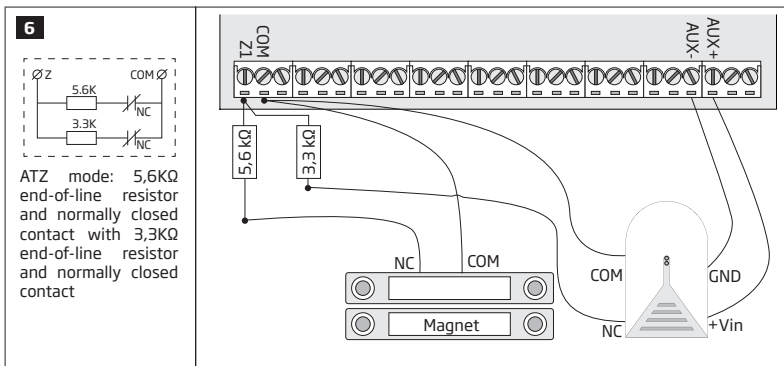
NOTE: The system does NOT support 2-wire smoke detectors.

Type 3

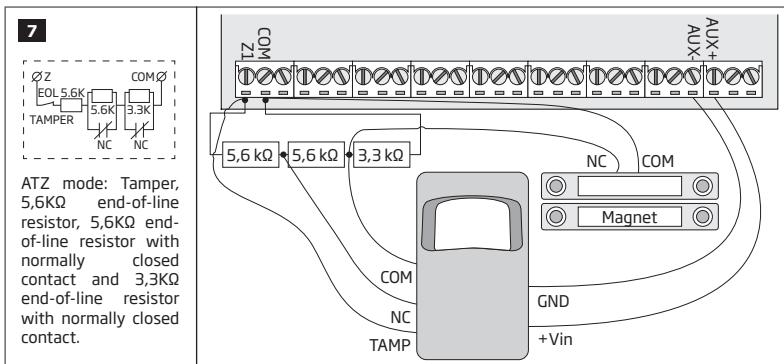
Example of motion detector wiring

**Type 4**

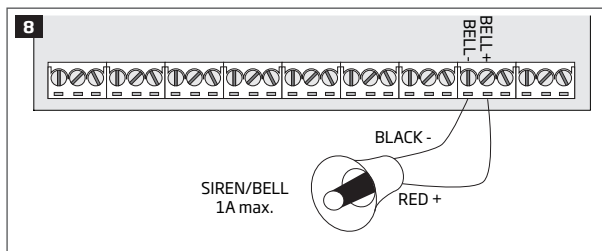
Example of magnetic door contact (Z1) and glass break sensor (Z7) wiring

**Type 5**

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

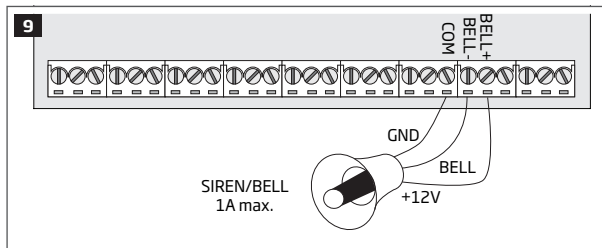
See also **14.3. 6-Zone Mode** and **14.4. ATZ (Advanced Technology Zone) Mode**.

2.3.3. Siren



Piezo siren

- 1 Connect positive siren wire (red) to **BELL+** terminal.
- 2 Connect negative siren wire (black) to **BELL-** terminal.



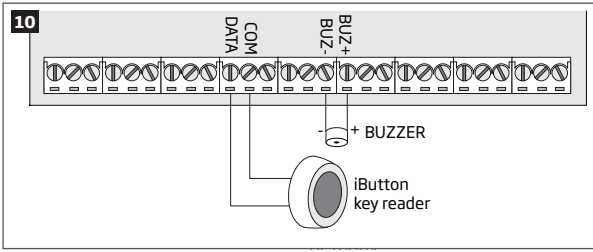
Self-contained siren

- 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. WIRED 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+**.

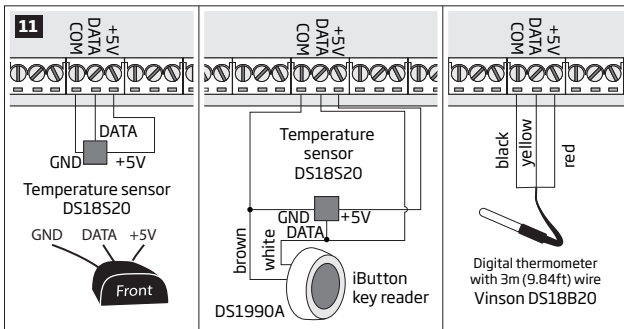
NOTE: The installation of buzzer is not necessary if EKB2/EKB3 keypad is used.

ATTENTION: The cable length for connection to 1-Wire interface can be up to 30m (98.43ft) 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

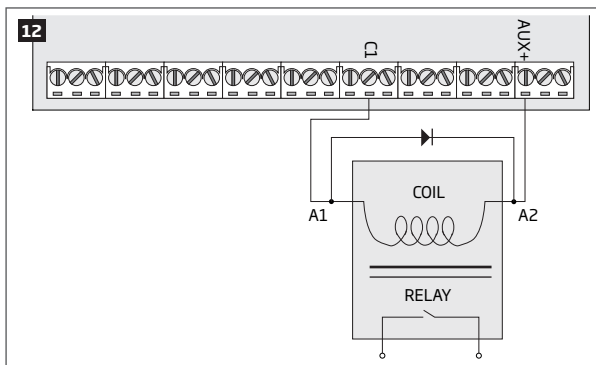


- 1 Depending on the model, connect temperature sensor **GND**/black wire, **DATA**/yellow wire, **+5V**/red wire terminals to 1-Wire interface: **COM**, **DATA** and **+5V** terminals respectively.
- 2 When connecting iButton key reader in parallel to temperature sensor, connect iButton key reader terminal wires to **COM** and **DATA** terminals respectively.

ATTENTION: The cable length for connection to 1-Wire interface can be up to 30m (98.43ft) max.

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

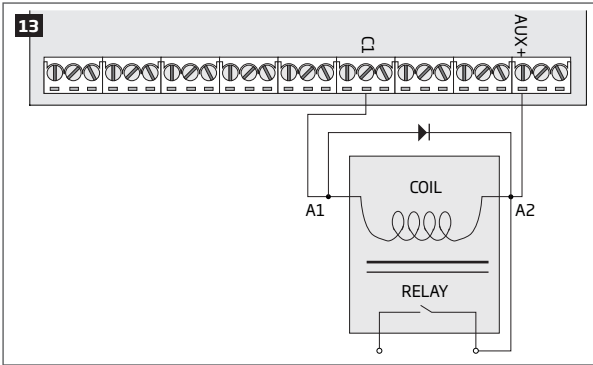
Example of relay wiring for negative PGM output control



- 1 Wire up relay **A1** terminal to PGM output **Cx** and **A2** terminal to **AUX+**.
- 2 In addition, connect the switching diode to relay's **A2** and **A1** terminals.

NOTE: We highly recommend using switching diode model 1N4148 or similar.

Example of relay wiring for positive PGM output control

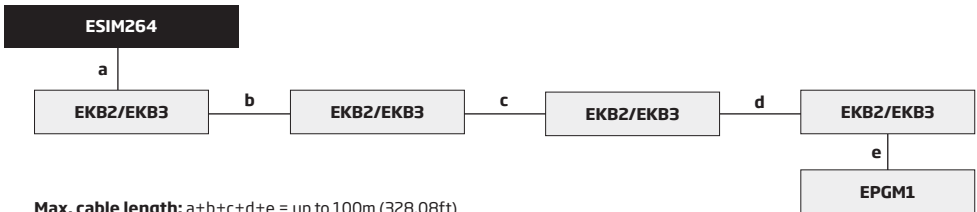


- 1 Wire up relay **A1** terminal to PGM output's **Cx** terminal and **A2** terminal to **AUX+** and one of the relay's switch contacts: NC or NO.
- 2 In addition, connect the switching diode to relay's **A2** and **A1** terminals.

NOTE: We highly recommend using switching diode model 1N4148 or similar.

2.3.7. RS485

Serial Wiring Method



Max. cable length: $a+b+c+d+e =$ up to 100m (328.08ft)

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

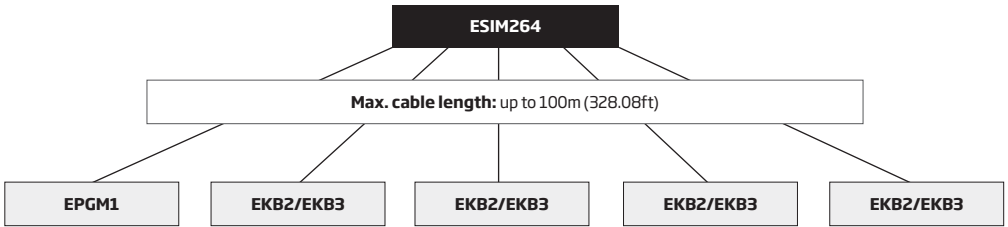
ATTENTION: The cable length must not exceed 100m (328.08ft) in total.

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 100m (328.08ft).

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.

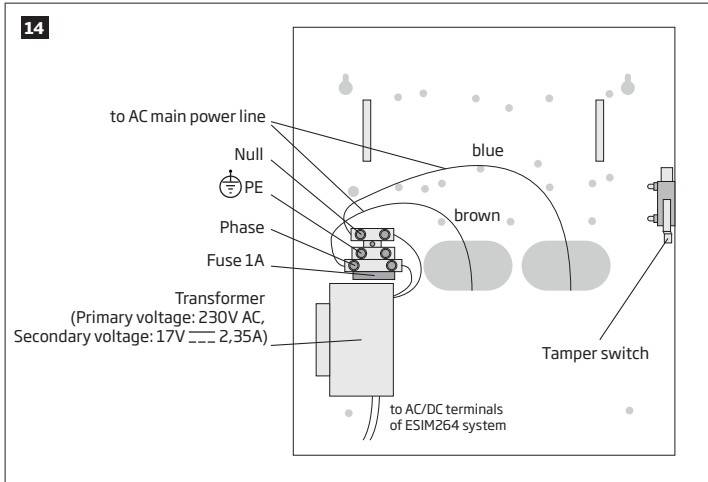
For more details on RS485 device installation, please refer to **32.1. RS485 Interface**

3. INSTALLATION

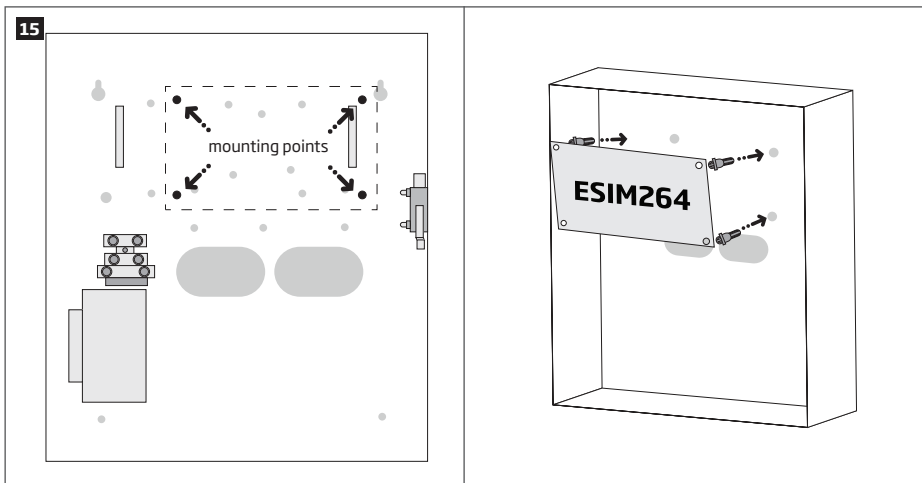
- The system can be installed in a metal or non-flammable cabinet only. For a convenient installation, ME1 metal cabinet is highly recommended. The metal cabinet must always be grounded as well as ESIM264 system's PCB by connecting one of the COM terminals to the PE contact of the metal cabinet.
- For the connection of 230V transformer, use $3 \times 0.75 \text{ mm}^2$ ($3 \times 0.03 \text{ in}^2$) 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 $2 \times 0.75 \text{ mm}^2$ ($2 \times 0.03 \text{ in}^2$) 1 thread unshielded cable of up to 100m (328.08ft) length.
- For the connection of zone/PGM output connectors, use 0.50 mm^2 (0.02 in^2) 1 thread unshielded cable of up to 100m (328.08ft) length.

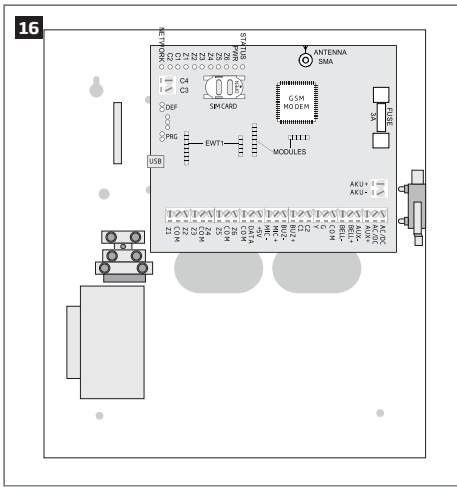
System Installation in ME1 Metal Cabinet

1. ME1 metal cabinet components

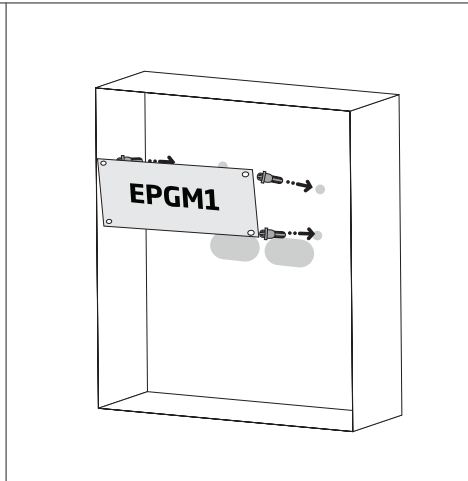
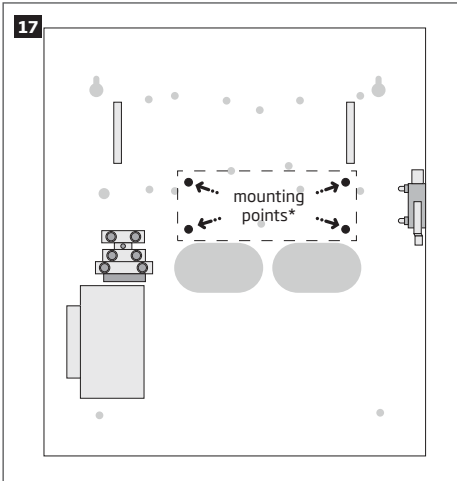


2. Insert the plastic standoffs into the appropriate mounting points and fix the board of ESIM264 on the holders as indicated below.

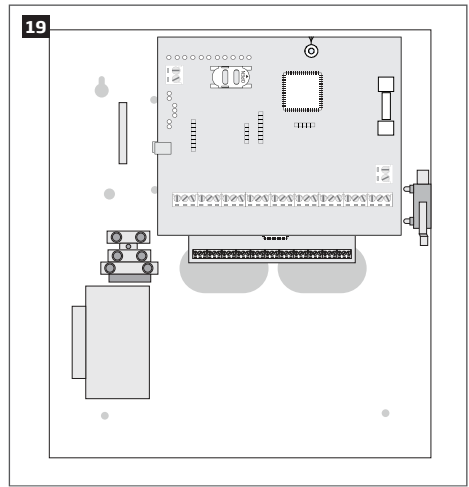
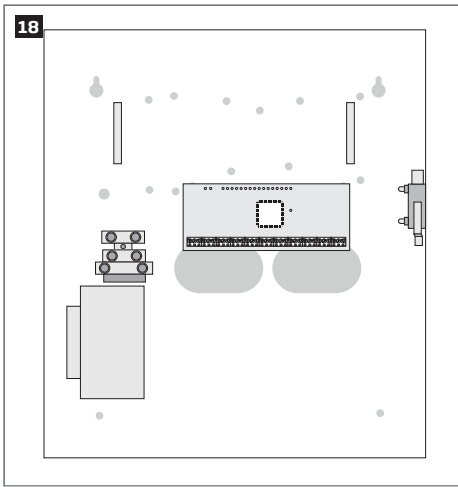




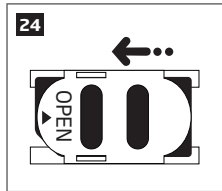
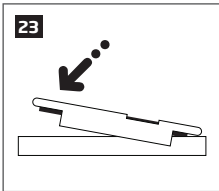
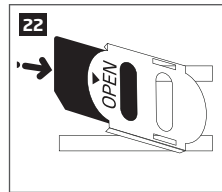
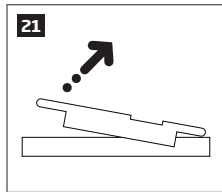
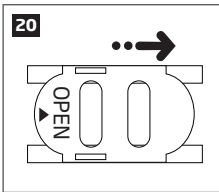
3. If EPGM1 module is to be installed, please install it in the first place and ESIM264 alarm system afterwards. EPGM1 must be mounted on the shorter plastic standoffs, while ESIM264 - on the longer ones. The mounting points of EPGM1 module are indicated below.



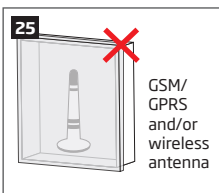
* The standard ME1 metal cabinet does NOT contain the mounting points intended for EPGM1 module mounting, therefore it will be necessary to drill out the mounting points by yourself.



4. Wire up the accessories, such as keypads, zone and PGM output expansion modules, temperature sensor according to the wiring diagrams. Install the buzzer closer to iButton key reader in order to hear the exit delay countdown (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 additional 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.



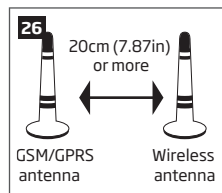
7. Connect the GSM/GPRS and wireless antennas and follow the recommendations for the installation:



GSM/
GPRS
and/or
wireless
antenna

Never install in the following locations:

- inside the metal cabinet
- keep the distance of at least 20cm (7.87in) or more.



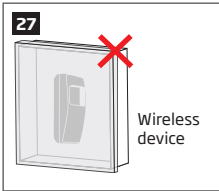
GSM/GPRS
antenna

Wireless
antenna

Recommended installation:

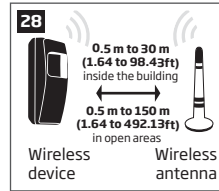
- keep the distance of at least 20cm (0.66ft) or more.

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



Never install in the following locations:

- inside the metal cabinet
- keep the distance of at least 20cm (7.87in) or more.



Recommended installation:

- face the front side of the wireless device towards the antenna
- keep the distance: 0,5 to 30m (1.64 to 98.43ft) inside the building, 0,5 to 150m (1.64 to 492.13ft) in open areas

For more details on how to install the wireless devices, please refer to **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION manual** located at eldesalarms.com

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 and 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/EWK2 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 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 make a phone call and send an SMS text message containing the violated zone or tamper number to a listed 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.

5.1. SMS Text Messages



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 listed 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

5.2. EKB2 LCD Keypad



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 **3.1.1.1.6. 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.

5.3. EKB3 LED Keypad



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 (⏏), (⏏) and (⋮) 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 ☑ flashing	Configuration mode activated successfully.
Indicator ⚠ flashing	Valid parameter entered and awaiting for valid value to be entered.
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.

5.4. ELDES Configuration Tool Software

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.

ELDES Configuration Tool is freeware and can be downloaded from at: eldesalarms.com

5.4.1. Remote 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.

ELDES Configuration Tool software provides remote system configuration ability via Internet using one of the following methods:

- ELDES proxy server (recommended). The connection can be established on the system via GPRS network.
- Running TCP/IP server on *ELDES Configuration Tool* (advanced). The connection can be established on the system via GPRS network.

In order to start using the remote configuration feature, please run the step-by-step wizard and follow the steps provided in the start page of *ELDES Configuration Tool* software. Please, note that it will be necessary to send an SMS text message to the system's phone number in order to initiate the remote connection. By following the steps you will be instructed on what text must be sent to the system's phone number in such case.

5.4.2. Ending the Remote Connection Session

Terminate the connection with server

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

- Click **Disconnect** or Stop button and close *ELDES Configuration Tool* software.
- The session will automatically expire in 20 minutes. Before the last 5 minutes, the software will offer the user to extend the session for another 20 minutes.
- Alternatively, the connection with the server can be terminated 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`

Once the session is expired or terminated, the system will reply with an SMS text message confirming the end of the session.

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:

wwwwww_PSW_ssss

Value: *wwwwww* - 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 and 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 and 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:



Value: // - 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: 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 FOR USER**).

By default, the system accepts incoming calls and SMS text messages from any phone number. Once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number (see **8.1. 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:ttteeellnnumm

Value: ssss - 4-digit SMS password; up - user phone number slot, range - [1... 5]; ttteeellnnumm - up to 15 digits user phone number.

Example: 1111_NR1:44170911XXXX1

EKB2

Menu path:

OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 5 → OK → PHONE NUMBER → OK → ttteeellnnumm → OK

Value: aaaa - 4-digit administrator password; ttteeellnnumm - up to 15 digits user phone number.

EKB3

Enter parameter 17, user phone number slot and phone number:

17 up ttteeellnnumm #

Value: up - user phone number slot, range - [01... 05]; ttteeellnnumm - up to 15 digits user phone number.

Example: 170144170911XXXX1#

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_NR1:44170911XXXX1_NR2:44170911XXXX2_NR5:44170911XXXX3`

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, once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number. To permit/deny system arming/disarming by phone call and SMS text message that contain a valid SMS password, configuration by SMS text message 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 and parameter status value:

`12 1 #`

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 and 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_2015.03.16_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 and 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: `66201505291235#`

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, the date and time will be automatically synchronized with the monitoring station upon the system startup.

10. USER CODES

The system supports up to 30 numeric user codes, identified as User Code 1 through 30, allowing to carry out system arming/disarming by the keypad. By default, User Code 1 is listed as 1111 and assigned to Partition 0. For more details regarding user code partition, please refer to **23.4. User Code Partition**.

Set user code

EKB2

Menu path:

User code 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 code 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 code, range - [0000... 9999].

EKB3

Enter parameter 15, user code slot and user code:

15 us uuuu #

Value: us - user code slot, range - [01... 30]; uuuu - 4-digit user code; range - [0000... 9999].

Example: 15021111#

Config Tool

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

Delete user code

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 code.

EKB3

Enter parameter 65 and user code:

65 uuuu #

Value: uuuu - 4-digit user code.

Example: 651111#

Config Tool

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

Replace user code

EKB2

Menu path:

User code 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 code 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 code, range - [0000... 9999].

EKB3

Enter parameter 63, existing user code and new user code:

63 vvvv uuuu #

Value: vvvv - 4-digit existing user code; uuuu - 4-digit new user code, 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 codes ranging from User Code 1 through 10 can be set as SGS (Security Guard Service) code, which is used as a checkpoint by a security service guard upon his/her visit in the secured location. When used, a data message, containing a certain event code, will be delivered to the monitoring station. However, NO system arming or disarming will be carried out after entering the SGS password.

Set SGS code

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 code not in use; us - user code slot, range - [1... 10].

EKB3

Enter parameter 74 and user code slot:

74 us #

Value: us - user code 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 code is used when system arming or disarming is demanded by force. When used, the system will arm/disarm as well as it will silently transmit an alert to the monitoring station. Only one of the user code ranging from User Code 1 through 10 can be set as Duress code.

Set Duress code

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 code slot, range - [1... 10].

EKB3

Enter parameter 73 and user code slot:

73 us #

Value: us - user code 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

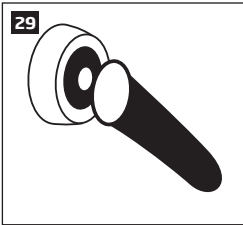
An iButton key is a unique 64-bit ID code containing chip enclosed in a stainless steel tab usually implemented in a small plastic holder. ESIM264 system supports up to 5 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.

11.1. Adding and Removing iButton Keys

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

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

- Disarm the system in all partitions (see **12. ARMING AND DISARMING**).
- Enable Allow Adding New iButton Keys mode.
- Touch the key to the iButton key reader when the system is disarmed (see picture below).



- The successfully added iButton key will be indicated by short beeps emitted by the system's buzzer.
- Add as many iButton keys as necessary - touch one key after another to the reader - until the number of 5 keys is reached.

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 and 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 and 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 code.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm-Disarm by Zone.
- EGR100 middle-ware.

The system arms/disarms the partitions that the listed user phone number, EKB2/EKB3 keypad and user code, iButton key, EWK1/EWK2 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**):

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

In case of violated zone/tamper presence when attempting to arm the system by free of charge phone call, SMS text message, iButton key and Arm-Disarm by Zone method, 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 regardless of the violated zone presence, please refer to **14.6. Zone Attributes** and **14.7. Bypassing and Activating Zones**.

Once a user phone number is listed, the system ignores any incoming calls and SMS text messages from a non-listed phone number as well as it rejects the SMS text messages containing wrong SMS password even from a listed user phone number. For more details regarding arming/disarming the system from a non-listed 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 listed user dialling 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.

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.

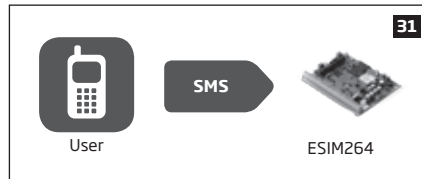
Arm the system

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:

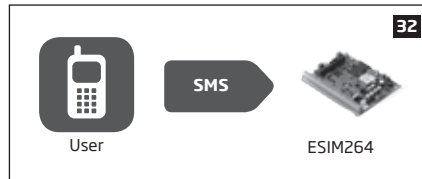
Disarm the system

SMS text message content:

`ssss_DISARMp` or `ssss_DISARMp,p`

Value: ssss - 4-digit SMS password; p - partition number, range - [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.

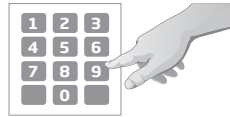
12.3. EKB2 Keypad and User Code

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 codes using the number keys on the keypad (see **10. USER CODES** for user code management).

By default when a valid user code 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 code:

UUUU → OK

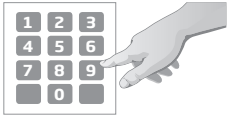
Value: UUUU - 4-digit user code.

Example: 1111 → OK

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

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

Disarm the system



Enter user code:

UUUU → OK

Value: UUUU - 4-digit user code.

Example: 1111 → OK

The system will arm/disarm the partition corresponding to the one that user code and the keypad are assigned to. For example, if EKB2 keypad and user code is assigned to Partition 1, the user will be able to arm/ disarm only Partition 1. For more details on how to set user code and keypad partition, please refer to **23.4. User Code 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 code 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 code. The keypad will automatically unblock once the 2-minute time has expired and display **KEYPAD UNBLOCKED** message.

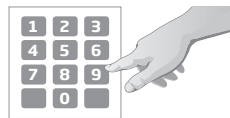
12.4. EKB3 Keypad and User Code

EKB3

Illuminated indicator  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 codes using the number keys on the keypad (see **10. USER CODES** for user code management). By default, when a valid user code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator  will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system




Enter user code:

UUUU

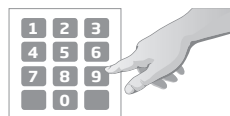
Value: UUUU - 4-digit user code.

Example: 1111

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

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

Disarm the system



Enter user code:

UUUU

Value: UUUU - 4-digit user code.

Example: 1111

The system will arm/disarm the partition corresponding to the one that user code and the keypad are assigned to. For example, if EKB3 keypad and user code is assigned to Partition 0, the user will be able to arm/ disarm only Partition 0. For more details on how to set user

code and keypad partition, please refer to **23.4. User Code 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 and enter partition number:
 *P
Value: p - partition number, range - [0... 1]
Example: *1

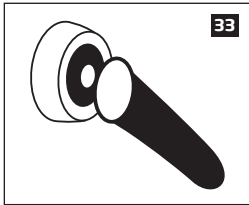
NOTE: By default, User Code 1 is listed as **1111** and assigned to Partition 0.

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**).



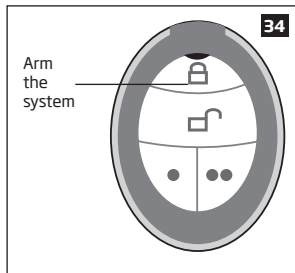
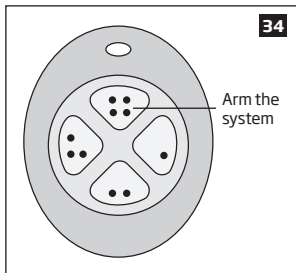
The system will arm/disarm the partition corresponding to the one that the iButton key is assigned to. For more details on how to set iButton key partition, please refer to **23.5. iButton Key Partition**.

12.6. EWK1/EWK2 Wireless Keyfob

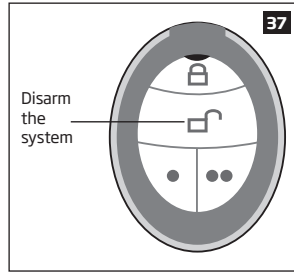
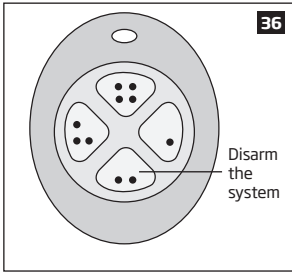


To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 - ; EWK2 -). When EWK1/EWK2 button is pressed for arming, the system will proceed as follows:

- If ready (no violated zone/tamper), the system will initiate exit delay and arm.
- If unready, the system will not arm. 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**).



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



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, pair another EWK1/EWK2 keyfob with 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 and 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 and 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 code, 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 and parameter status value:

75 up 0 #

Value: up - 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 and parameter status value:

75 up 1 #

Value: up - 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 45 seconds, it will attempt to send the SMS text message to the next listed user phone number. To ignore the SMS delivery report and allow/disallow the system to send the SMS text message to every listed user phone number, please refer to the following configuration methods.

Enable arm/disarm notification for all listed 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 and 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 listed 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 and parameter status value:


220 #


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.

- in a non-partitioned system,  icon will be displayed next to the countdown timer on EKB2 keypad screen during exit delay.
- in 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 code.
- 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 and 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.

SMS

SMS text message content:

`ssss_ENTRYDELAY:nn,eeee` or `ssss_ENTRYDELAY:nn,eeee;nn,eeee;nn,eeee;nn,eeee`

Value: `ssss` - 4-digit SMS password; `nn` - zone number, range - [1... 44], `eeee` - 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` → `eeee` → `OK`

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

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

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

Value: `aaaa` - 4-digit administrator password; `eeee` - 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], `eeee` - 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 and PGM output expansion module.	16	16
Wireless zones	Non-physical zones automatically created by connected wireless devices.	4**	32***
Virtual zones	Non-physical zones intended for Panic button feature (alarm activation upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using <i>ELDES Configuration Tool</i> 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 keypad zones, EPGM1 zones and virtual zones are present.

**** - Available only if no keypad 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 (for more details on technical specifications and installation, please refer to the latest user manual of the device located at eldesalarms.com).
- connecting keypads (see **31.1.1. EKB2 - LCD Keypad** and **31.1.2. EKB3 - LED Keypad**).
- pairing 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 → TYPE1...3 → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 39 and number of zone connection type:

39 1 # - Type 1

39 2 # - Type 2

39 3 # - Type 3

Example: 392#

Config Tool

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

NOTE: The system supports a mixed combination of Type 1 and Type 2 zone connection types simultaneously regardless of the type (Type 1 or Type 2) selected in the system's configuration. This applies to on-board zones, keypad zones and EPGM1 zones. **Example:** On-board zone Z1 and keypad zone is wired based on Type 1, while on-board zone Z3 and EPGM1 zone is wired based on Type 2.

NOTE: Type 3 is NOT supported by keypad zones.

NOTE: ATZ mode is NOT supported by keypad zones and EPGM1 zones. If ATZ mode is enabled, EPGM1 zones must be wired in accordance with the last selected 6-Zone mode zone connection type before the ATZ mode has been enabled. The ATZ mode setting does NOT affect the zone connection type of the keypad zones.

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 and parameter status value:

28 1 #

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 and parameter status value:

28 0 #

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 3B and number of zone connection type:

3B 1 # - Type 4

3B 2 # - Type 5

Example: 3B1#

Config Tool

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

NOTE: Once enabled, the ATZ mode DOES NOT affect EPGM1 zones, nor keypad zones and applies to on-board zones only.

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. 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, shock sensors or other zones.
- **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. 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. Once the alarm is caused by violating a Fire-type zone followed by turning OFF the alarm using any available disarm method, the system will ignore the violations of any Fire-type zone (including the repeated violations of the said zone) caused within a 1-minute time frame. 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 and 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 and 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 and 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 and 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 → FORCE → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 82, zone number and 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 attribute

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 and parameter status value:

B20 #

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 and parameter status value:

B21 #

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


NOTE for EKB3: The Configuration mode must remain deactivated before bypassing a violated zone or activating a bypassed zone.

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  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 


Value: zone-name - up to 24 characters zone name.

EKB3

Press the  key, enter zone number and user code:

 nn uuuu #

Value: nn - zone number, range - [01... 44]; uuuu - 4-digit user code.

Example:  091111#

Bypass all violated zones

EKB2

Menu path:

OK → BYPASS → OK → BYP VIOLATED ZONES → OK

The zone will remain 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 $\$$ key, enter zone number and user code:

$\$$ nn uuuu #

Value: nn - zone number, range - [01... 44]; uuuu - 4-digit user code.

Example: $\$$ 251111#

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

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 and 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 → OK → EPGM1 ZONE 1... 16 → OK → STATUS → DISABLE → OK`

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 52, zone number and 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 Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exists, 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 code.

EKB3

Press the  key and enter user code:

 uuuu

Value: uuuu - 4-digit user code.

Example:  1111

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 listed 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 (see **19.3. Wireless Signal Status Monitoring**).

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:

OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 25, event number and parameter status value:

25 08 0 #

Example: 25080#

Config Tool

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

Enable tamper alarm notification

EKB2

Menu path:

OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES → OK → TAMPER EVENT → OK → ENABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 25, event number and parameter status value:

25 08 1 #

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 FOR USER**

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 FOR USER

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.**
 - **Z4H 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 Δ will flash if one or more high-numbered zones are violated. If one or tampers are violated, indicator Δ 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 listed 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 45 seconds, it will attempt to send the SMS text message to the next listed 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 listed 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. By default, 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 listed 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 dialling the next listed 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 listed 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 Δ represents 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 system will 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  represents system fault presence including violated tamper. For more details on violated tamper indication, please refer to **29. INDICATION OF SYSTEM FAULTS**.

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

ATTENTION: Phone calls to the listed 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. The capacity of the queue is 24 events maximum.

NOTE: If the system sent the SMS text message and/or dialled 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 listed 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 and parameter status value:

301#

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 and parameter status value:

300#

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 the listed 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 and parameter status value:

25 03 0 #

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 and 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 45 seconds, it will attempt to send the SMS text message to the next listed user phone number. To ignore the SMS delivery report and allow/disallow the system to send the SMS text message to every listed user phone number, please refer to the following configuration methods

Enable SMS text message to all listed 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 and 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 listed 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 Z1 and parameter status value:

`Z10 #`

Example: Z10#

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: Regardless of the Call in Case of Alarm parameter status, the system will NOT ring the listed user phone number if the system is connected to the monitoring station (see **30. MONITORING STATION**).

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 and 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 and PGM Output Expansion Module**).
- pairing 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 and parameter status value:

33 1 #

Example: 331#

Config Tool

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

Disable EPGMB mode

EKB2

Menu path:

OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → USING EPGMB → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 33 and 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, e.g. 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... 44]; 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 and parameter status value:****61 oo 1 #****Value:** oo - PGM output number, range - [01... 44].**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 and parameter status value:****61 oo 0 #****Value:** oo - PGM output number, range - [01... 44].**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.mm.sc****Value:** ssss - 4-digit SMS password; oo - PGM output number, range - [1... 44]; 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.mm.sc****Value:** ssss - 4-digit SMS password; oo - PGM output number, range - [1... 44]; 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** - Operates based on Start Time of a selected scheduler 1-16.
- **Scheduler ends** - Operates based on 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 Z76 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 and scheduler

Config Tool

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

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**.

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.

NOTE: When PGM output action is selected as pulse, the PGM output will turn ON or turn ON for a set period of time based on the PGM output state set up (ON or OFF) for system startup.

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-Receiver**) for system extension capabilities. The module allows the user to easily pair up to 16 ELDES-made wireless devices to the system. This includes the following:

- EWD2 - wireless magnetic door contact/shock sensor/flood sensor.
- EWS3 - wireless indoor siren.
- EWS2 - wireless outdoor siren.
- EWK1 and EWK2 - wireless keyfob.
- EWF1 - wireless smoke detector.

RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION manual and the latest user manual of the wireless device located at eldesalarms.com

The wireless devices can operate at a range of up to 30m (98.43ft) from the alarm system unit while inside the building and up to 150m (492.13ft) range in open areas. The wireless connection is two-way and operates in one of four available channels in ISM868 (EU version) / ISM915 (US version) non-licensed band.

The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period, known as Test Time. When the wireless device is switched ON, it will initiate the Test Time transmission to the system within its wireless connection range. In order to optimize battery power saving of the wireless device, the Test Time periods vary by itself while the device is switched ON, but still unpaired. When the alarm system is switched OFF or if the wireless device is unpaired or removed the Test Time period of the wireless device is as follows (non-customizable):

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

Once the wireless device is paired, 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, based on Test Time value, to the system as well as to accept the queued up command (if any) from the system. By increasing the Test Time period, EWS2/EWS3 siren response time will decrease. Example: *The alarm occurred at 09:15:25 and the system queued up the command for EWS3 siren to start sounding. By default, Test Time value of EWS3 siren is 7 seconds, therefore EWS3 siren will sound at 09:15:32.*

By default, the Test Time period is as follows (customizable):

- EWF1 EWD2: every 30 seconds.
- 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.

19.1. Pairing, Removing and Replacing Wireless Device

Wireless device management can be easily and conveniently carried out using the graphical interface of *ELDES Configuration Tool* software. If you intend to manage the wireless devices by SMS text message, an 8-character wireless device ID code will be required in order to pair the device with 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 pair a wireless device, please refer to the following configuration methods.

Pair wireless device with the system

SMS

SMS text message content:

`ssss_SET:wless-id`

Value: *ssss* - 4-digit SMS password; *wless-id* - 8-character 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: When binding EWK1/EWK2 wireless keyfob, it is necessary to press several times any button on the device.

Once a wireless device is paired, it occupies one of 16 available wireless device slots and the system adds single or multiple 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-character 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-character wireless device ID code of the new device; *oldwl-id* - 8-character wireless device ID code of the old device.

Example: `1111_REP:535185D < 41286652`

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.

NOTE: If you are unable to pair a wireless device, please restore the wireless device's parameters to default and try again. For more details on how to restore the default parameters, please refer to the user manual provided along with the wireless device or visit eldesalarms.com to download the latest user manual.

19.2. Wireless Device Information

Once a wireless device is paired, 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) - indicated only in EKB2 keypad menu.
- Firmware version.
- Test Time period (expressed in milliseconds) of a wireless device - indicated only in SMS text message reply.

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-character wireless device ID code; *nn* - wireless zone number, range - [13.. 44].

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-character 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.**19.3. Wireless Signal Status Monitoring**

If the wireless signal is lost due to poor signal strength or low battery power on a certain wireless device and does not restore within 1-hour period (EN 50131-1 Grade 2 requirement), the system will cause an alarm. 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). The user will also be notified by SMS text message as soon as the wireless signal is restored.

ELDES Configuration Tool software indicates a timer of the last Test Time signal delivered by a paired and unpaired wireless device. The software will also warn you if the delivery of the Test Time signal is delayed for a time period 3 times longer than the Test Time period of a paired wireless device. In case the Test Time signal delivery of an unpaired wireless device is delayed for more than 1,5 minute, a warning will follow and the icon of such wireless device will be removed from the software's interface in 10 seconds.

19.4. Disabling and Enabling Siren if Wireless Signal is Lost

If a wireless device loses its wireless signal for 1 hour or longer, 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 and 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 and parameter status value:****76 0 #****Example: 760#****Config
Tool**This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

19.5. EWT1 - Wireless Transmitter-Receiver

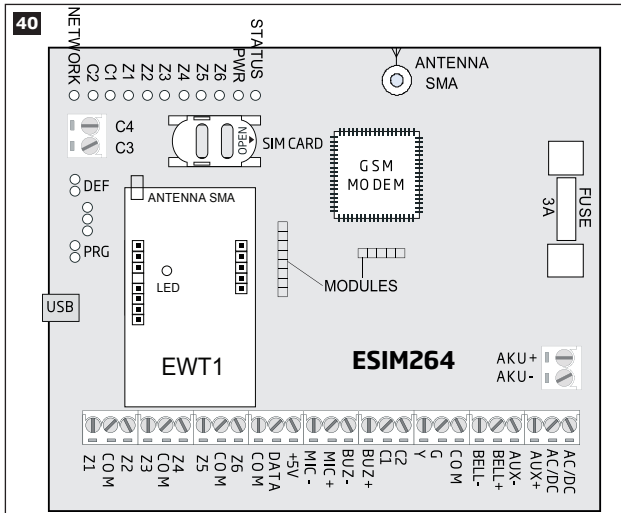
Wireless transmitter-receiver EWT1 is an add-on module for ESIM264 system. It enables wireless transmission through alarm system ESIM264 and ELDES wireless devices, such as: wireless magnetic door contacts/shock sensors, wireless zone and PGM output expansion modules, wireless indoor sirens, wireless outdoor sirens,, wireless smoke detectors and wireless keyfobs.

EWT1 enables ESIM264 alarm system to connect up to 16 wireless devices at a time. Maximum wireless connection range is 150m (492.13ft) (in open areas).

19.5.1. Electrical and Mechanical Characteristics

Wireless band	ISM868/ISM915
Dimensions	68x38x18mm (2.72x1.50x0.71in)
Operating temperature range	-20...+55°C (-4...131°F)
Wireless communication range	Up to 30m (98.43ft) in premises; up to 150m (492.13ft) in open areas
Maximum number of wireless devices	16

19.5.2. Installation



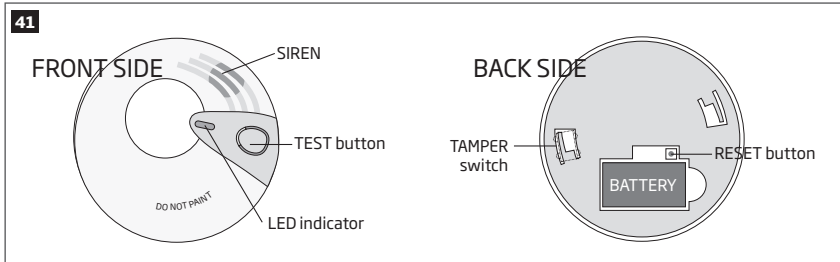
1. Disconnect ESIM264 alarm system mains power and backup battery.
2. Insert EWT1 pins into appropriate ESIM264 slots.
3. Mount the antenna to EWT1. It is not recommended to install the antenna inside the metal enclosure.
4. Power up ESIM264 system.
5. EWT1 is ready to use with ESIM264 system.

19.6. EWF1 - Wireless Smoke Detector

Main 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

For more details on EWF1 wireless smoke detector, please refer to the user manual of the device.



19.6.1. Interconnection

The interconnection feature automatically links all wireless smoke detectors that are paired with the alarm system. When any EWF1 detects smoke, it will sound the built-in siren and send the signal to the alarm system resulting in an instant alarm followed by built-in siren sound caused by the rest of EWF1 wireless smoke detectors. EWF1 device that detected smoke will auto-reset when the smoke clears, while the rest of EWF1 smoke detectors will continue to 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 configuration methods.

Disable interconnection

EKB2

Menu path:

OK → **iiii** → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → DISABLE → OK

Value: *iiii* - 4-digit installer code.

EKB3

Enter parameter 50 and 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 → **iiii** → OK → PRIMARY SETT INGS → OK → SIREN SETTINGS → OK → EWF1 SIREN INTERC. → OK → ENABLE → OK

Value: *iiii* - 4-digit installer code.

EKB3

Enter parameter 29 and 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.

NOTE: The maximum supported EWF1 siren alarm duration is 255 seconds (4 mins. 15 secs.) even if the system's alarm duration value is longer.

NOTE: System's alarm duration has a higher priority against the EWF1 siren alarm duration, therefore EWF1 will sound as long as the system's alarm duration set up, unless the set up value for EWF1 siren alarm duration is shorter.

For more details on EWF1 wireless smoke detector, please refer to the user manual of the device.

20. WIRED 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 SETTINGS → 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 and 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 SETTINGS → 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 may sound for up 6 minutes max. regardless of the set system alarm duration time, even if it is set longer than 6 minutes.

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 and parameter status value:

29 1 #

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 and parameter status value:

29 0 #

Example: 290#

Config Tool

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

20.2. Indication by EWS2 - Wireless Outdoor Siren 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 88 and parameter status value:

88 1 #

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 SETTINGS → OK → SIREN SETTINGS
→ OK → EWS2 LED → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 88 and 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. Indication by EWS3 - Wireless Indoor Siren Indicators

When enabled, the built-in LED indicators of EWS3 wireless indoor siren will flash during the alarm. In the event of burglary, 24-hour or tamper alarm, EWS3 will flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator. To enable/disable these features, please refer to the following configuration methods.

Enable EWS3 LED indication

EKB2

Menu path:

Burglary/24-hour/tamper alarm LED: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 ALARM → OK → ENABLE → OK

Fire alarm: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → ENABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 94/93 and parameter status value:

Burglary/24-hour/tamper alarm LED: 94 1 #

Fire alarm LED: 93 1 #

Example: 931 #

Config Tool

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

Disable EWS3 LED indication

EWS3

Menu path:

Burglary/24-hour/tamper alarm LED: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 ALARM → OK → DISABLE → OK

Fire alarm LED: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → SIREN SETTINGS → OK → EWS3 FIRE LED → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 94/93 and parameter status value:

Burglary/24-hour/tamper alarm LED: 94 0 #

Fire alarm LED: 93 0 #

Example: 940 #

Config Tool

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

21. BACKUP BATTERY, MAINS POWER STATUS MONITORING AND MEMORY

21.1. Backup Battery Status Monitoring

The system may come equipped with a backup battery maintaining power supply of the system when the mains power supply is temporarily lost. The implemented feature allows the system to perform a self-test on the backup battery and notify the listed user phone number 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 and 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 and 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 and 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 and parameter status value:**

25 061 #

Example: 25061#**Config Tool**This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

21.2. Mains Power Status Monitoring

If the household electricity is unstable in the system installation area, the system may temporarily lose its power supply and continue operating on the backup battery power. The system supervises the mains power supply and notifies the listed user phone number 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 the listed user phone number 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 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 and 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 loss 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 and 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 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 and 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 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 and 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 loss and restore delay are 30 and 120 seconds respectively. To set a different mains power loss and restore delay duration, please refer to the following configuration methods.

Set mains power loss delay

EKB2

Menu path:

OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → MAINS POWER STATUS → OK → LOSS DELAY → OK → llll → OK

Value: aaaa - 4-digit administrator password; llll - mains power loss delay duration, range - [0... 65535] seconds.

EKB3

Enter parameter 70 and loss delay duration:

70 llll #

Value: llll - 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 restore delay

EKB2

Menu path:

OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → MAINS 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 and 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.

21.3. Memory

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 supervises the GSM connection every 10 minutes. When the GSM connection loss is detected, the system indicator NETWORK will light OFF and the system will attempt to restore the GSM connection. In case the system fails to restore the GSM connection within a 3-minute period (by default), the keypad will indicate the system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) and the system will continue the attempt to restore the GSM connection. In addition, the system may turn ON a determined PGM output to indicate the GSM connection loss fault (by default - disabled).

Once the GSM connection is restore, the keypad will no longer indicate the system fault condition, while the specified 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 code, 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 and partition number:

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 and 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 ✓ 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 code (see **23.4. User Code 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 Code** and **12.4. EKB3 Keypad and User Code**.

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 and partition number:**

51 kk p #

Value: kk - keypad slot, range - [01... 04]; p - partition number, range - [0... 1];

Example: 51041#

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 assigned 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 and 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 and 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 Code Partition

User code partition determines which system partition can be armed/disarming using a certain user code. User code 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 Code** and **12.4. EKB3 Keypad and User Code**.

Set user code partition

EKB2

Menu path:

User code 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 code 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 code and partition number:

87 uuuu p #

Value: uuuu - 4-digit user code; 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 and partition value:

60 i p #

Value: i - 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 SENSOR

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 the listed user 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:

- Shutdown the system.
- 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**).
- 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 the listed user phone number if the specified minimum (MIN) or maximum (MAX) temperature boundary is exceeded.

To set the MIN and MAX temperature boundaries, please refer to the configuration methods.

Set MIN and MAX temperature boundaries

SMS

SMS text message content:

`ssss_TEMP:mnn:mx`

Value: ssss - 4-digit SMS password; *mnn* - MIN boundary, range - [-55...125] C; *mx* - MAX boundary, range - [-55...125] C.

Example: 1111_TEMP:-5;2B

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 → mx → OK

Value: aaaa - 4-digit administrator password; *mnn* - MIN boundary, range - [-55...125] C; *mx* - MAX boundary, range - [-55...125] C.

Keys P1 or P2 are used to enter minus character, e.g. -20.

EKB3

Enter parameter 19 and temperature boundary value:

`19 mnn mx #`

Value: *mnn* - MIN boundary, range - [-55...125] C; *mx* - 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 25, event number and 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 25, event number and 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 module EA2, the user will be able to have a 2-way voice communication (see **31.3.2. 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 listed 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 SETTINGS → 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 SETTINGS → 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 listed 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 and 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 the listed user 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 and 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 and frequency:

110000#

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 listed user phone number only. If the user phone number is unavailable and the system fails to receive the SMS delivery report during 45 seconds, it will attempt to send the SMS text message to the next listed 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 listed 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	SMS text message sent to the user in case the mains power is lost.
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 <i>Tamper x</i> .
9	Battery failed	SMS text message sent to the user in case the backup battery resistance is $\geq 2\Omega$ 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 <i>Tamper x *</i> .
12	Temperature fallen	SMS text message sent to the user in case of temperature deviation by the set MIN value.
13	Temperature exceeded	SMS text message sent to the user in case of temperature deviation by the set MAX value.
14	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 → OK

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 and 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 → OK

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 and 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_+ttteeellnnumm**Value:** ssss - 4-digit SMS password; ttteeellnnumm - 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 code.

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.

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

EKB3

1. Steady ON or flashing indicator Δ represents certain system faults. For more details, please refer to the following table below.

Indication	Description
Steady ON	One or more tampers are violated; other system faults (see below)
Flashing	One or more high-numbered zones (Z13-Z76) are violated (see below)

2. In order to find out more on a certain system fault, please enter the following command.

View system faults

Enter command:

... #

After this procedure the keypad will illuminate red indicators for 15 seconds. The description of each indication is provided in the table below.

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 (see step #3)
6	GSM connection is lost

3. In order to find out the violated high-numbered zone, please enter the following command and refer to the table below.

View violated high-numbered zones

Enter command:

... 1

4. In order to find out which particular tamper is violated, please enter the following command. In case there is a combination of flashing and illuminated red indicators on the keypad, please refer to the table below in order to find out the violated high-numbered tamper (Tamper 13 - 44).

View violated tampers

Enter command:

... 2

The following table provides the combinations of red indicators belonging to a certain indicator section (A or B) on the keypad. The combination of the flashing red indicator in section A and illuminated (steady ON) red indicator in section B represents the respective number of a violated high-numbered zone or tamper.

B (steady ON)	LED #7	LED #8	LED #9	LED #10	LED #11	LED #12
A (flashing)						
LED #1	Z13	Z19	Z25	Z31	Z37	Z43
LED #2	Z14	Z20	Z26	Z32	Z38	Z44
LED #3	Z15	Z21	Z27	Z33	Z39	
LED #4	Z16	Z22	Z28	Z34	Z40	
LED #5	Z17	Z23	Z29	Z35	Z41	
LED #6	Z18	Z24	Z30	Z36	Z42	

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.

When using the MS mode, the data messages transmitted to the monitoring station (see **30.1. Data Messages - Events**) will gain the highest priority for the delivery, therefore based on the communication method (see **30.2. Communication**), a constant and stable connection with the monitoring station must be ensured. In case of connection failure, the system will attempt to restore the connection and if the monitoring is unavailable for a lengthy period of time, the system might consume a large amount of voice calls/data resulting in additional charges applied by the GSM operator according to the cell phone service plan.

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 and 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 and 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 and 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 connection, remote firmware update or remote listening/2-way voice communication is in progress. However, during the remote connection session or remote listening/2-way voice communication process, the data messages will be queued up and transmitted to the monitoring station after the remote connection session or remote listening/2-way voice communication process is over, while during the remote firmware update process NO data will be queued up and all data messages will be lost.

ATTENTION: Phone calls to the listed user phone number in case of alarm are disabled by force when MS mode is enabled.

NOTE: Additional charges may apply for voice calls/data traffic based on your cell phone service plan when using the MS mode.

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 listed 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	3121	Armed by user (Duress code)	Transmitted in case the system is armed by Duress code.
4	1121	Disarmed by user (Duress code)	Transmitted in case the system is disarmed by Duress code.
5	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.
6	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.
7	1133	24-Hour zone alarm	Transmitted in case of zone of 24-Hour type is violated.
8	3133	24-Hour zone restore	Transmitted in case of zone of 24-Hour type is restored.
9	1144	Tamper alarm	Transmitted in case the tamper is violated.
10	3144	Tamper restore	Transmitted in case the tamper is restored.
11	1146	Panic/Silent zone alarm	Transmitted in case of zone of Panic/Silent type is violated.
12	3146	Panic/Silent zone restore	Transmitted in case of zone of Panic/Silent type is restored.
13	1158	Temperature risen	Transmitted in case of the temperature has increased above the MAX set value.
14	1159	Temperature fallen	Transmitted in case of temperature has decreased below the MIN set value.
15	1301	Mains power loss	Transmitted in case the mains power is lost.
16	3301	Mains power restore	Transmitted in case the mains power is restored.
17	1302	Low battery	Transmitted in case the backup battery voltage is 10.5V or lower / the wireless sensor battery level runs below 5%.
18	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.
19	1309	Battery failed	Transmitted in case the backup battery resistance is 2Ω or higher.
20	1358	GSM connection failed	Transmitted in case the GSM connection is lost.
21	1381	Wireless signal loss	Transmitted in case the connection with any wireless device is lost.
22	3381	Wireless signal restore	Transmitted in case the connection with any wireless device is restored.
23	1401	Disarmed by user	Transmitted in case the system is disarmed.
24	3401	Armed by user	Transmitted in case the system is armed.
25	1456	Disarmed in Stay mode	Transmitted in case the system is disarmed in Stay mode.
26	3456	Armed in Stay mode	Transmitted in case the system is armed in Stay mode.
27	3463	SGS code entered	Transmitted in case the SGS code is entered.
28	3602	Test event/Kronos ping	Transmitted for system online status verification purposes.
29	3626	Date/time not set	Transmitted in case system date and 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	ID
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 Code 1	10
User Code 2 or Arm/Disarm by Zone	11
User Code 3	12
User Code 4	13
User Code 5	14
User Code 6	15
User Code 7	16
User Code 8	17
User Code 9	18
User Code 10	19
User Code 11	20
User Code 12	21
User Code 13	22
User Code 14	23
User Code 15	24
User Code 16	25
User Code 17	26
User Code 18	27
User Code 19	28
User Code 20	29
User Code 21	30
User Code 22	31
User Code 23	32
User Code 24	33
User Code 25	34
User Code 26	35
User Code 27	36
User Code 28	37
User Code 29	38
User Code 30	39
Remote Code (EGR100)	40
KeyFob 1	85
KeyFob 2	86
KeyFob 3	87
KeyFob 4	88
KeyFob 5	89

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 → MAINS 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 → OK → SYSTEM SHUTDOWN EV → OK → DISABLE → OK

Value: aaaa - 4-digit administrator password.

EKB3

Enter parameter 24, event number and 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.

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 → MAINS 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 and 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

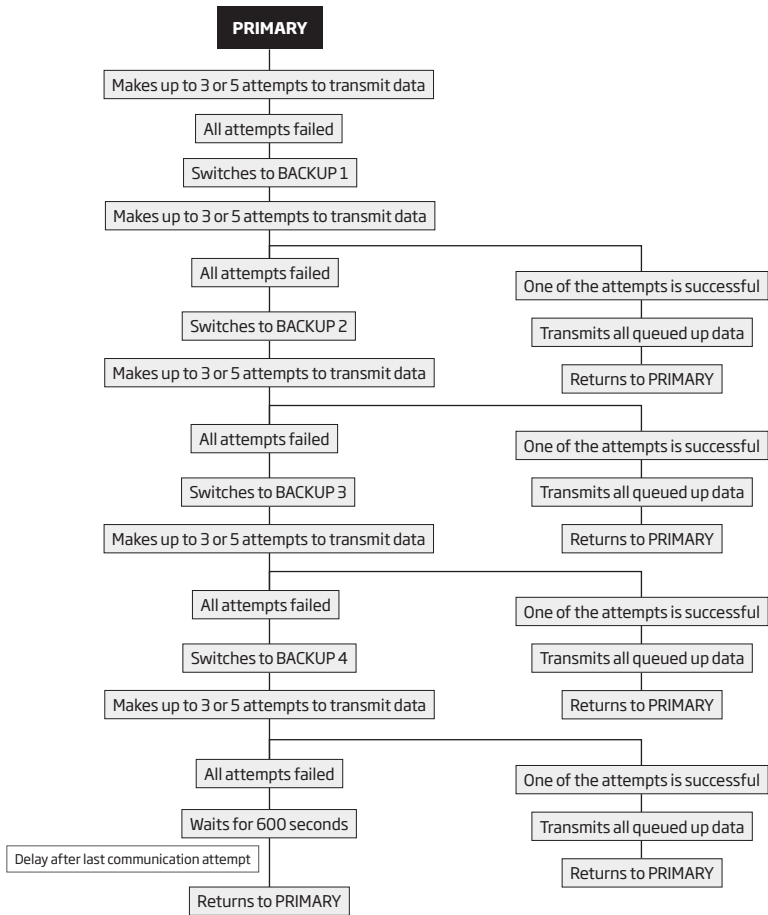
The system supports the following communication methods and protocols:

- GPRS network - EGR100, Kronos protocol.
- Voice calls (GSM audio channel) - Ademco Contact ID protocol.
- RS485 data channel.
- CSD (Circuit 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.



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 and 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 and 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... 04].

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 and 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. EGR100 is freeware and can be downloaded at eldesalarms.com/en/download. Alternatively, you can use ESR100 digital receiver. For more details, please refer to eldesalarms.com

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 ESR100 digital receiver or the machine running EGR100 or Kronos monitoring station software.
4. Set public server port, which is a port of ESR100 digital receiver or 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 or 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 middle-ware'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 administrator password; add.add.add.add - server IP address.

EKB3

Enter parameter 40 and 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.

Set server port

SMS

SMS text message content:

`ssss_SETGPRS:PORT:pprrt`

Value: *ssss* - 4-digit SMS password; *pprrt* - server port number, range - [1... 65535].

Example: `1111_SETGPRS:PORT:5521`

EKB2

Menu path:

`OK → CONFIGURATION → OK → aaaa → OK → GPRS SETTINGS → OK → SERVER PORT → OK → pprrt → OK`

Value: *aaaa* - 4-digit administrator password; *pprrt* - server port number, range - [1... 65535].

EKB3

Enter parameter 44 and server port number:

`44 pprrt #`

Value: *pprrt* - server port number, range - [1... 65535].

Example: `443365#`

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 administrator password; *add.add.add.add* - DNS1 server IP address.

EKB3

Enter parameter 41 and 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 administrator password; *add.add.add.add* - DNS2 server IP address.

EKB3

Enter parameter 42 and DNS2 server IP address:

`42 add add add add #`

Value: *add add add add* - DNS2 server IP address.

Example: `41065082119002#`

Config Tool

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

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 administrator password.

EKB3

Enter parameter 43 and protocol number:

`43 0 #` - TCP

`43 1 #` - UDP

Example: `431#`

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 administrator password.

EKB3

Enter parameter 43 and 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 administrator password; `add.add.add.add` - DNS1 server IP address.

EKB3

Enter parameter 41 and 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 administrator password; `add.add.add.add` - DNS2 server IP address.

EKB3

Enter parameter 42 and 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 and 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 → tteesstpp → OK`

Value: *aaaa* - 4-digit administrator password; *tteesstpp* - test period, range - [0... 65535] seconds.

EKB3

Enter parameter 46 and number of attempts:

`46 tteesstpp #`

Value: *tteesstpp* - 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 ESR100 digital receiver or EGR100 middle-ware. It is MANDATORY to change the default Unit ID before using ESR100 or 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 administrator password; unid - 4-digit unit ID number.

EKB3

Enter parameter 47 and 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 **32. 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: 44170911XXXX1.

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 → ttteeellnnumm → OK

Value: aaaa - 4-digit administrator password; ttteeellnnumm - up to 15 digits monitoring station phone number.

EKB3

Enter parameter 26, phone number slot and phone number:

26 ps ttteeellnnumm #

Value: ps - phone number slot, range - [01... 03]; ttteeellnnumm - up to 15 digits monitoring station phone number.

Example: 260144170911XXXX1#

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 and 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 SETTINGS → 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: 44170911XXXX1.

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 → tteeeellnnumm → OK

Value: aaaa - 4-digit administrator password; tteeeellnnumm - up to 15 digits monitoring station phone number.

EKB3**Enter parameter 85, number of entry and phone number:****85 ps tttteellnnumm #****Value:** ps - phone number slot, range - [01... 05]; tttteellnnumm - 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 and 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. WIRED DEVICES

31.1. RS485 Interface

The system comes equipped with RS485 interface used for the communication with the following devices:

- EKB2 - LCD keypad. Up to 4 units supported.
- EKB3 - LED keypad. Up to 4 units supported.
- EPGM1 - hardwired zone and PGM output expansion module. 1 unit supported.

The terminals of RS485 interface are Y (yellow wire) and G (green wire) terminals, which are data bus. The devices, connected to RS485 interface, must be powered from the AUX+ and AUX- terminals or by an external power supply.

For more details on RS485 device wiring, please refer to **3.2.7. RS485**.

For more details on technical specifications and installation, please refer to the latest user manual of the device located at eldesalarms.com

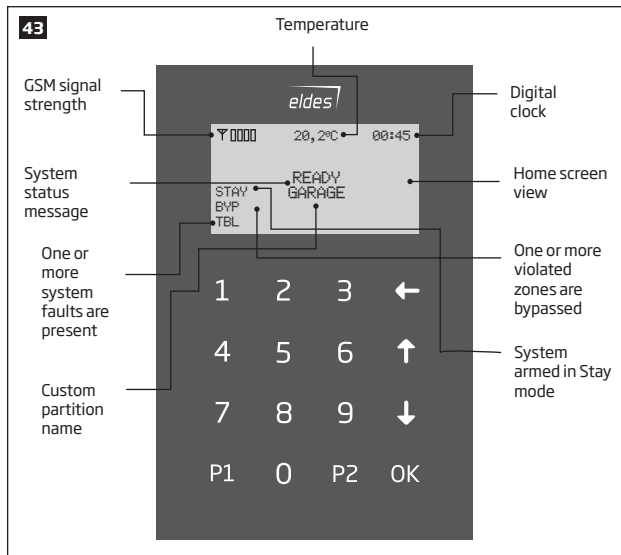
31.1.1. EKB2 - LCD Keypad

Main features:

- Alarm system arming and disarming (see **12.3. EKB2 Keypad and User Code**).
- 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 **31.1.1.1. Icons and Messages**).
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).
- Audio indication by built-in buzzer.
- Wireless device information display (see **19.2. Wireless Device Information**).
- Temperature display (see **31.1.1.1. Icons and Messages**).
- Time display (see **31.1.1.1. Icons and Messages**).

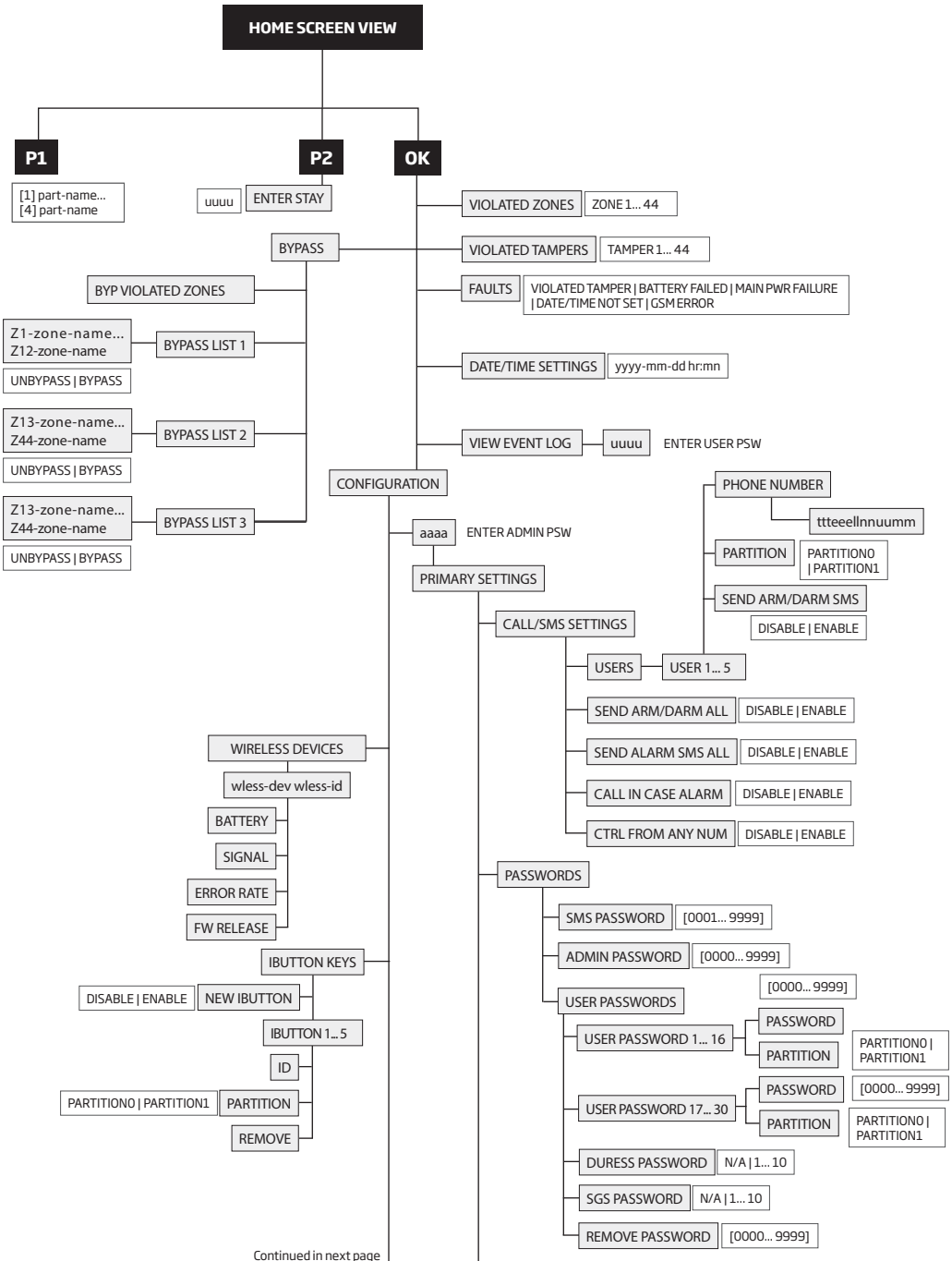
For more details on technical specifications and installation, please refer to the latest user manual of the device located at eldesalarms.com

31.1.1.1. Icons and Messages

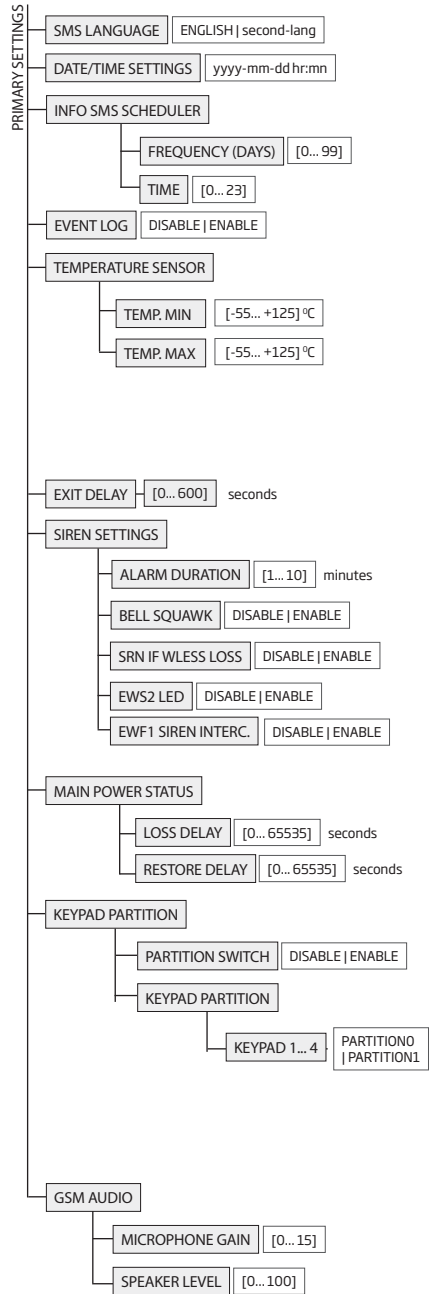
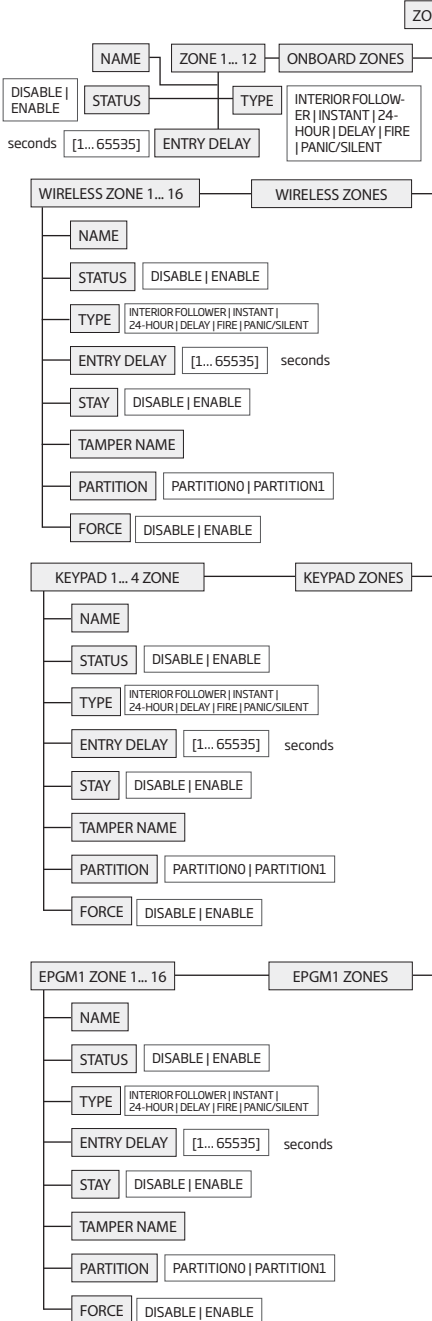


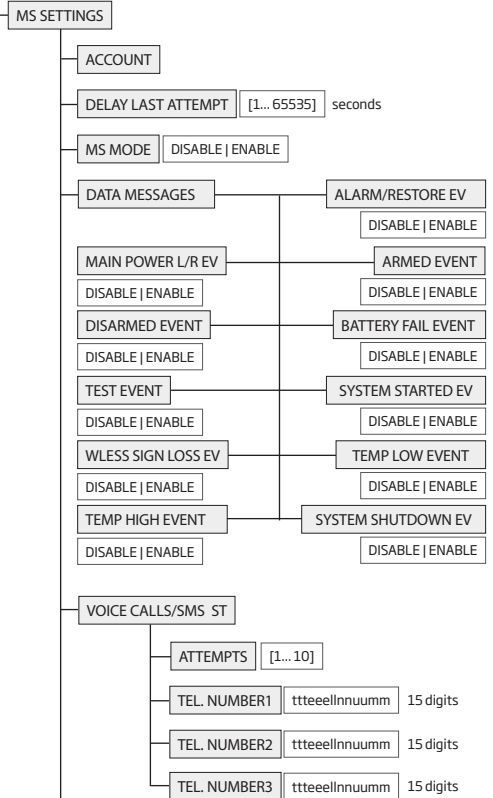
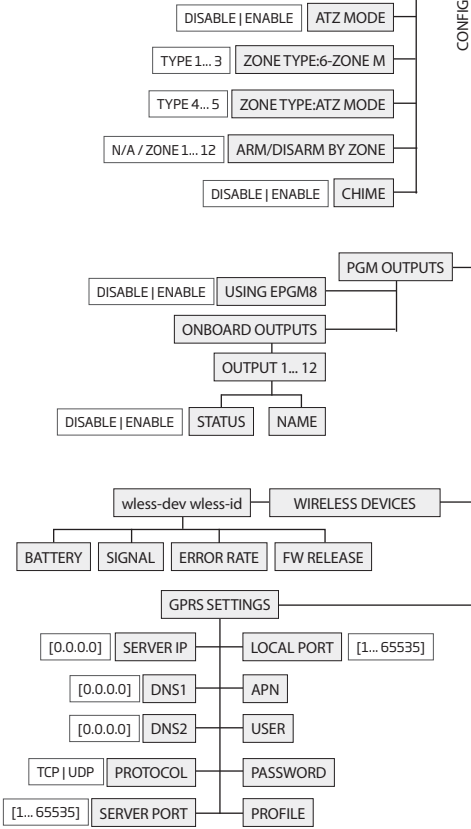
Icon / Message	Description
	Chime - Delay zone violated when system is disarmed.
	Exit delay countdown initiated.
	System is armed and menu is locked.
	System is disarmed and menu is unlocked
	Configuration mode activated.
+ CONFIGURATION MODE	
BURGLARY ALARM	Delay, Instant or Follow zone violated when system is armed.

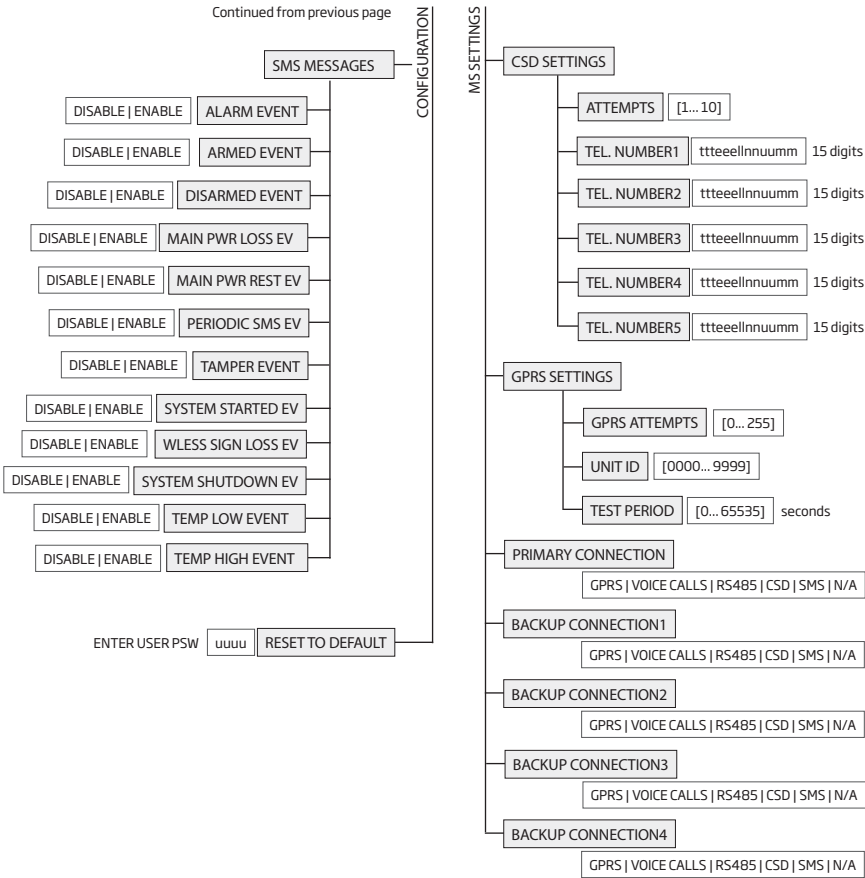
Icon / Message	Description
Z4 ALARM	24H zone violated.
FIRE ALARM	Fire zone violated.
TAMPER ALARM	Tamper violated
READY	System is ready to be armed.
NOT READY	System is not ready to be armed - one or more zones / tampers violated.
ARMED	System is armed (optional feature).
STAY	Stay mode activated
BYP	System armed in Stay mode
TBL	One or more system faults are present



Continued in next page







31.1.2. EK33 - LED Keypad

Main features:

- Alarm system arming and disarming (see **12.4. EK33 Keypad and User Code**).
- 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 **31.1.2.1. LED Functionality**).
- Audio indication by built-in buzzer.
- Keypad partition switch (see **23.3. Keypad Partition and Keypad Partition Switch**).

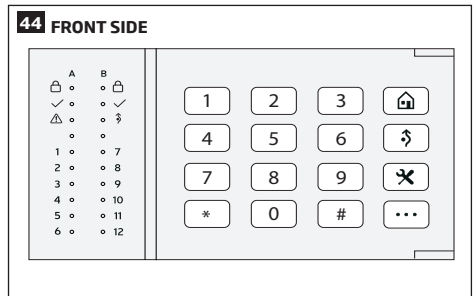
For more details on technical specifications and installation, please refer to the latest user manual of the device located at eldesalarms.com

31.1.2.1. LED Functionality

	INDICATION	DESCRIPTION
🔒 (red)	Steady ON	System armed / exit delay in progress
	Flashing	Configuration mode activated
✓ (green)	Steady ON	System is ready - no violated zones and/or violated tampers exist
⚠️ (orange)	Steady ON	System faults exist
	Flashing	Violated high-numbered zone
🔓 (orange)	Steady ON	Violated zone bypassed
1-12 (red)	Steady ON	Zone violated / configuration command being typed in

31.1.2.2. Keys Functionality

	DESCRIPTION
🏠	1st character for STAY-arming
🔓	1st character for violated zone bypass and bypassed zone activation
✘	N/A
⋮	1st character for system fault list indication / 1st character for violated high-numbered zone indication / 1st character for violated tamper indication
0 - 9	Command typing
*	1st character for Configuration mode activation or deactivation / clear typed in characters / 1st character for keypad partition switch (if enabled)
#	Typed in command confirmation



31.2. 1-Wire Interface

1-Wire interface is used for the system to communicate with an iButton key reader and a temperature sensor. 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 **2.3.4. iButton Key Reader and Buzzer** and **2.3.5. Temperature Sensor and iButton Key Reader**.

Main iButton features:

- Up to 5 iButton keys per alarm system unit ESIM264;
- Communication via 1-Wire interface.

31.3. Modules Interface

The system might be equipped with modules interface slots thus enabling to use one of the following devices at a time:

- EPGM8 - hardwired PGM output expansion module (for more details on technical specifications and installation, please refer to the latest user manual of the device located at eldesalarms.com)
- EA1 - audio output module (see **31.2.1. EA1 - Audio Output Module**)
- EA2 - audio output module with amplifier (see **31.2.2. EA2 - Audio Output Module with Amplifier**)

31.3.1. EA1 - Audio Output Module

EA1 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA1 features:

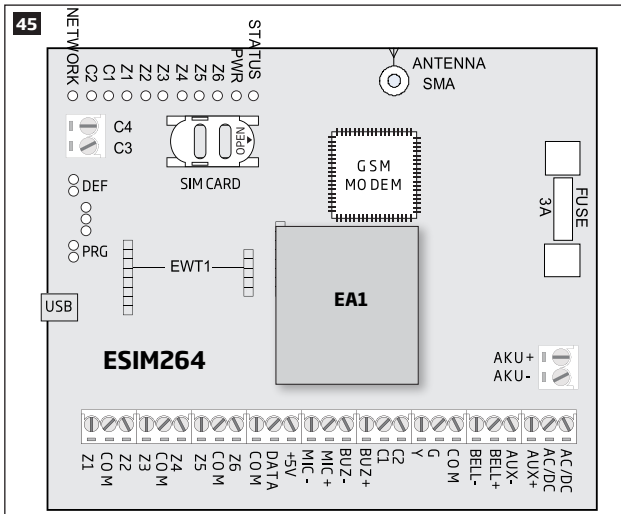
- Two-way voice conversation during a phone call;
- Possibility to connect headphones or desktop speakers.

31.3.1.1. Technical Specifications

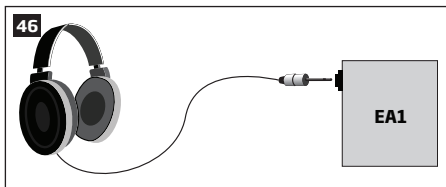
- 3,5 mm female jack
- Dimensions: 41x40x24mm (1.61x1.57x0.95in)

31.3.1.2. Installation

1. Disconnect ESIM264 alarm system mains power and backup battery.
2. Insert EA1 pins into appropriate ESIM264 alarm system slots.



3. Connect headphones or desktop speakers to EA1 3,5 mm female jack.



4. Power up ESIM264 alarm system.
5. EA1 is ready for use with ESIM264 alarm system.

31.3.2. EA2 - Audio Output Module with Amplifier

EA2 audio output module enables a duplex audio connection for ESIM264 alarm system.

Main EA2 features:

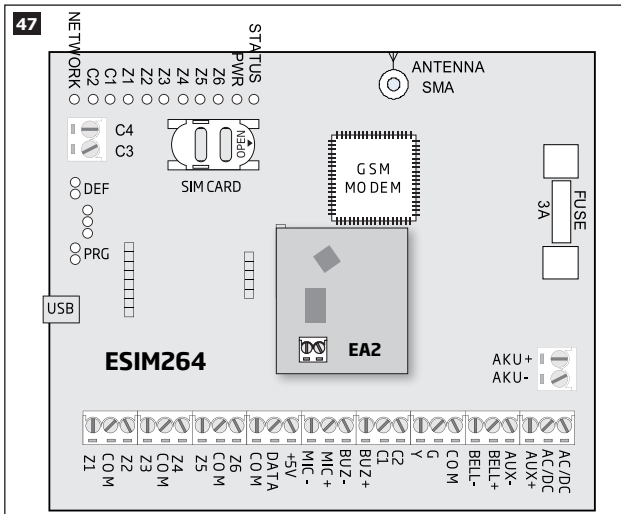
- Two-way voice conversation during a phone call;
- Possibility to connect a speaker.

31.3.2.1. Technical Specifications

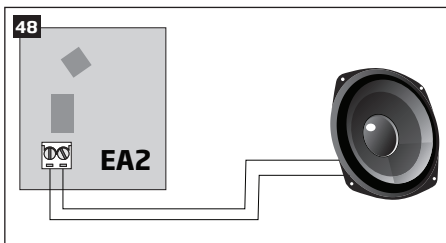
- 1W 8Ω audio amplifier
- Dimensions: 35x33x12mm (1.38x1.30x0.47in)

31.3.2.2. Installation

1. Disconnect ESIM264 alarm system mains power and backup battery.
2. Insert EA2 pins into appropriate ESIM264 alarm system slots.



3. Connect a speaker to EA2 **Speaker** terminals.



4. Power up ESIM264 alarm system.
5. EA2 is ready for use with ESIM264 alarm system.

32. 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`

33. TECHNICAL SUPPORT

33.1. Troubleshooting

Indication	Possible reason
Indicator STATUS is OFF	<ul style="list-style-type: none">· No mains power· Blown fuse· Micro-controller is unable to initiate due to electrical mains noise or static discharge
Indicator PWR is OFF	<ul style="list-style-type: none">· No mains power· Wiring done improperly· Blown fuse
Indicator NETWORK is OFF	<ul style="list-style-type: none">· Missing SIM card· PIN code is enabled· SIM card is inactive· Disconnected antenna· GSM operator's fault· GSM signal unavailable in the area
System is unable to send any SMS text messages and/or does not ring	<ul style="list-style-type: none">· Insufficient SIM card credit balance· Incorrect SMS centre phone number· No GSM network signal· User phone number is not added (or control from any phone number is disabled)· SIM card changed before disconnecting mains power or backup battery
Received SMS text message "Wrong syntax"	<ul style="list-style-type: none">· 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	<ul style="list-style-type: none">· Temperature sensor not connected· Temperature sensor fault· Cable length of the 1-Wire interface is exceeded (30 m 98.43ft) max.)
24H and/or Fire zones do not work	<ul style="list-style-type: none">· Specified zone must be enabled by SMS, <i>ELDES Configuration Tool</i>, EKB2 or EKB3 keypad.
No sound during remote listening	<ul style="list-style-type: none">· 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. More up to date information about your device and other products can be found at the manufacturer's website eldesalarms.com

33.2. 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.

33.3. 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.

33.4. Updating Firmware via GPRS Connection Remotely

ATTENTION: The system will NOT transmit any data to monitoring station while updating the firmware remotely via GPRS network. All data messages will be lost and will NOT be 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 and 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:

`ssss_FOTA:ftp-server-ip,port,firmware-file-name.bin,user-name,password`

Value: *ssss* - 4-digit SMS password; *ftp-server-ip* - public IP address of FTP server where ESIM264 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: Firmware filename MUST be renamed in lowercase format before using it.

ATTENTION: Comma and underscore character is NOT allowed to use in user name, password 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.

NOTE: It is strongly recommended to restore default parameters after the firmware update.

33.5. 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 <i>ELDES Configuration Tool</i> 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 <i>ELDES Configuration Tool</i> software is outdated. Please, download the latest <i>ELDES Configuration Tool</i> software version by visiting eldesalarms.com/en/download .
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 <i>ELDES Configuration Tool</i> 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 <i>ELDES Configuration Tool</i> software. For more 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.

Question	Answer
8. Is any additional configuration necessary when connecting EPGM1 module after wiring is done according 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 <i>ELDES Configuration Tool</i> are not fully displayed and some parts are like cut-off. What's wrong?	Please, update <i>ELDES Configuration Tool</i> software by visiting eldesalarms.com/en/download and downloading the latest version.
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: <ol style="list-style-type: none"> 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 .
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 listed 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 <i>ELDES Configuration Tool</i> . What's wrong?	<i>ELDES Configuration Tool</i> version is too old. Please, update it.
19. I am unable to run <i>ELDES Configuration Tool</i> - 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 <i>ELDES Configuration Tool</i> , EKB2, EKB3 keypad or SMS text message.
21. I receive an error message when attempting to configure the device or update the firmware remotely. What's 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?	<ol style="list-style-type: none"> 1. Send the <i>ssss_ENCONFIG</i> SMS text message. 2. In <i>ELDES Configuration Tool</i> software press Disconnect button and repeat the steps from the beginning as described in 5.4.1. Remote Connection.

34. RELATED PRODUCTS



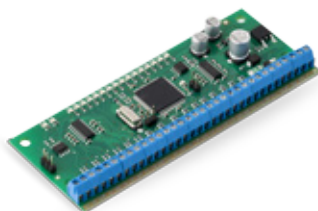
EKB2 - LCD keypad



EKB3 - LED keypad



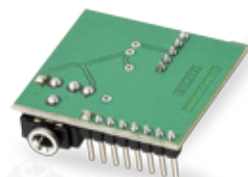
ME1 - metal cabinet



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



EWS2 - wireless external siren



EWF1 - wireless smoke detector



EWK1 - wireless keyfob



ESR100 - digital receiver



EWD2 - wireless door contact/shock sensor



EWK2 - wireless keyfob



EWS3 - wireless indoor siren



Vinson DS18B20 - digital thermometer with 3m (9.84ft) wire

Made in the European Union
eldesalarms.com