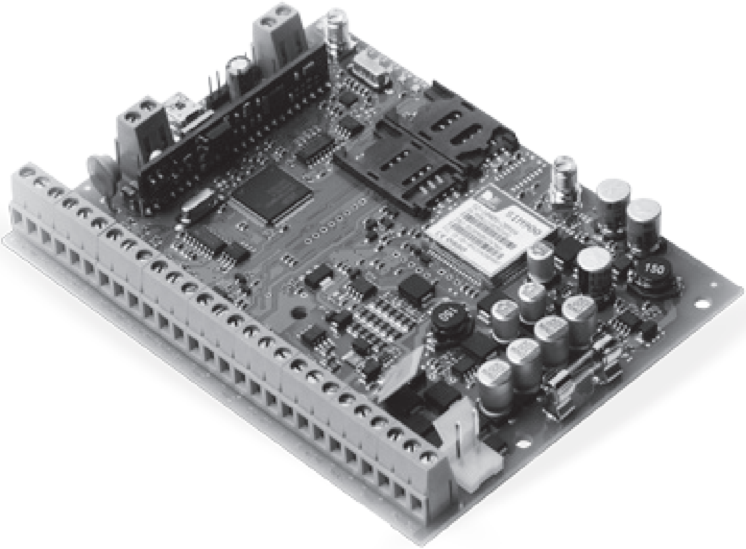


eldes

ESIM364

GSM ALARM AND MANAGEMENT SYSTEM

INSTALLATION MANUAL

Installation Manual v1.5
Valid for ESIM364 v02.06.12 and up

Safety instructions

Please read and follow these safety guidelines in order to maintain safety of operators and people around:

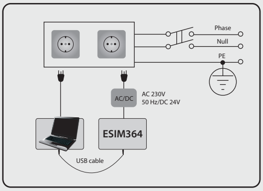
- GSM alarm & management system ESIM364 (also referenced as alarm system, system or device) has radio transceiver operating in GSM 850/900/1800/1900 bands.
- DO NOT use the system where it can be interfere with other devices and cause any potential danger.
- DO NOT use the system with medical devices.
- 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 ESIM364 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 ESIM364 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

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



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

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

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

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

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

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

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

Contents

Limited Liability

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

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

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

Manufacturer Warranty

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

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

Package Content

1. ESIM364	qty. 1
2. Microphone	qty.1
3. SMA antenna	qty. 2
4. Buzzer	qty. 1
5. Back-up battery connection wire...	qty. 1
6. User manual	qty. 1
7. Resistors 5,6kΩ	qty. 12
8. Resistors 3,3kΩ	qty. 6
9. Plastic standoffs	qty. 4

About Installation Manual

This document describes detailed installation and operation process of alarm system ESIM364. It is very important to read the installation manual before starting to use the system.

Hereby, “ELDES UAB” declares that this GSM alarm and management system ESIM364 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at www.eldes.lt

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

15.105 statement (for digital devices)

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be located or operating in conjunction with any other antenna or transmitter..

1. GENERAL INFORMATION

1.1. Functionality

ESIM364 – 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.
- Mains power status notification by SMS text message.
- Two-way intercom device via GSM network.

1.2. Compatible Device Overview

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

Wireless Devices		
Device	**Description**	**Max. Connectable Devices**
EW1	Wireless 2 zone and 2 PGM output expansion module	32***
EW1B	Battery-powered wireless 2 zone and 2 PGM output expansion module	32***
EWP1	Wireless motion detector	32***
EWD1	Wireless magnetic door contact	32***
EWD2	Wireless magnetic door contact/shock sensor	32***
EWK1****	Wireless keyfob with 4 buttons	5***
EWK2****	Wireless keyfob with 4 buttons	5***
EWS1	Wireless indoor siren	32***
EWS2	Wireless outdoor siren	32***
EKB3W	Wireless LED keypad	4***
EWF1	Wireless Smoke Detector	32***

* - 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 ESIM364 unit.
*** - A mixed combination of wireless devices is supported. The combination can consist of up to 32 wireless devices in total.
**** - A mixed combination of EWK1 and EWK2 keyfobs is supported. The combination can consist of up to 5 keyfobs in total.

1.3. Default Parameters & Ways of Parameter Configuration

Main Settings					
Parameter	**Default Value**	**Configurable by:**			
		SMS	**EKB2**	**EKB3/ EKB3W**	**Configuration Tool**
SMS & EKB2 Menu Language	Depends on firmware version according to user's location	✓	✓	✓	✓
SMS Password	0000	✓	✓	✓	✓
User Password 1	1111		✓	✓	✓
User Password 2... 30	N/A		✓	✓	✓
User Password Name	N/A				✓
Administrator Password	1470		✓	✓	✓
Duress Password	N/A		✓	✓	✓
SGS Password	N/A		✓	✓	✓
User 1... 10 Phone Number	N/A	✓	✓	✓	✓
User 1... 10 Name	N/A				✓
Allow Control from Any Phone Number	Disabled	✓	✓	✓	✓
Date & Time	N/A	✓	✓	✓	✓
Exit Delay - Partition 1... 4	15 seconds	✓	✓	✓	✓
Info SMS Scheduler	Frequency (days) – 1; Time - 11	✓	✓	✓	✓

Zones

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Zone Name	Z1 - Zone 1; Z2 - Zone 2; Z3 - Zone 3; Z4 - Zone 4; Z5 - Zone 5; Z6 - Zone 6	✓			✓
Entry Delay	15 seconds	✓	✓	✓	✓
On-Board Zone Delay	800 milliseconds				✓
EPGM1 Zone Delay	800 milliseconds				✓
On-board Z1 Zone Type	Delay		✓	✓	✓
On-board Z2... Z12 Zone Type	Instant		✓	✓	✓
Keypad Zone Type	Instant		✓	✓	✓
EPGM1 Zone Type	Instant		✓	✓	✓
Wireless Zone Type	Depends on the connected wireless device		✓	✓	✓
Virtual Zone Type	Interior Follower			✓	✓
ATZ Mode	Disabled		✓	✓	✓
6-Zone Mode: Zone Connection Type	Type 1		✓	✓	✓
ATZ Mode: Zone Connection Type	Type 4		✓	✓	✓
On-board Zone Status	Enabled	✓	✓	✓	✓
Keypad Zone Status	Disabled	✓	✓	✓	✓
EPGM1 Zone Status	Enabled	✓	✓	✓	✓
Wireless Zone Status	Depends on the connected wireless device	✓	✓	✓	✓
Virtual Zone Status	Disabled			✓	✓
Stay attribute for individual zone	Disabled		✓	✓	✓
Arm-Disarm by Zone	N/A		✓	✓	✓
Force atrribute for individual zone	Disabled		✓	✓	✓
Shared 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/ EKB3W	Configuration Tool
PGM Output Name	C1 – Controll1, C2 – Controll2, C3 – Controll3, C4 – Controll4 etc.	✓			✓
PGM Output Status	Disabled	✓	✓	✓	✓
EPGM8 PGM Output Status	Disabled	✓	✓	✓	✓
EPGM1 PGM Output Status	Disabled	✓		✓	✓
Wireless PGM Output Status	Enabled	✓	✓	✓	✓
Wireless PGM Output Type	Depends on the connected wireless device				✓
PGM Output Control by Event 1... 16	Disabled			✓	✓
PGM Output Control by Event Management					✓
Scheduler 1... 16	Disabled				✓
Turn ON/OFF PGM Output by Timer		✓			
Using Module EPGM8 Mode	Disabled		✓	✓	✓

Alarm Duration & Siren

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Alarm Duration	1 minute	✓	✓	✓	✓
EWS2 LED	Disabled		✓		✓
Bell Squawk	Disabled		✓	✓	✓
Activate Siren if Wireless Device is Lost	Disabled		✓	✓	✓

Alarm Notifications & Arm/Disarm Notifications

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Call in Case of Alarm	Disabled		✓	✓	✓
Send Alarm SMS to All Users Simultaneously	Disabled	✓	✓	✓	✓
Send Arm/Disarm SMS to User 1... 10	Enabled		✓	✓	✓
Send Arm/Disarm SMS to All Selected Users Simultaneously	Disabled	✓	✓	✓	✓

Main Power Status

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Main Power Loss Delay	30 seconds		✓	✓	✓
Main Power Restore Delay	120 seconds		✓	✓	✓

Peripheral Devices

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Temperature Sensor 1... 8 Name	N/A	✓			✓
Primary Temeprature Sensor	No. 1	✓	✓	✓	✓
Secondary Temperature Sensor	No. 2	✓	✓	✓	✓
Temperature Sensor 1... 8 MIN	0 °C	✓	✓	✓	✓
Temperature Sensor 1... 8 MAX	0 °C	✓	✓	✓	✓
Allow adding New iButton Keys	Disabled	✓	✓	✓	✓
iButton 1... 16 Name	N/A				✓

System Notifications

Parameter	Parameter	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
System Armed	Enabled		✓	✓	✓
System Disarmed	Enabled		✓	✓	✓
General Alarm	Enabled		✓	✓	✓
Mains Power Loss/Restore	Enabled	✓	✓	✓	✓
Battery Failed	Enabled		✓	✓	✓
Battery Dead or Missing	Enabled		✓	✓	✓
Low Battery	Enabled		✓	✓	✓
Siren Fail/Restore	Enabled		✓	✓	✓
Date/Time Not Set	Enabled		✓	✓	✓
GSM Connection Failed	Disabled		✓	✓	✓
GSM/GPRS Antenna Fail/Restore	Disabled		✓	✓	✓
Tamper Alarm	Disabled		✓	✓	✓
Keypad Failed	Enabled		✓	✓	✓
Temperature Info	Enabled	✓	✓	✓	✓
System Started	Enabled		✓	✓	✓
Periodical Info	Enabled		✓	✓	✓
Wireless Signal Loss	Enabled		✓	✓	

Partitions

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Partition 1 Name	PART1		✓	✓	✓
Partition 2 Name	PART2		✓	✓	✓
Partition 3 Name	PART3		✓	✓	✓
Partition 4 Name	PART4		✓	✓	✓
Keypad 1... 4 Partition	PART1		✓	✓	✓
Keypad Partition Switch	Disabled		✓	✓	✓
User Password 1... 30 Partition	PART1		✓	✓	✓
User 1... 10 Phone Number Partition	PART1		✓	✓	✓
iButton 1.. 16 Partition	PART1		✓	✓	✓
Zone Partition	PART1		✓	✓	✓

Monitoring Station

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	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... 3 (PSTN)	N/A		✓	✓	✓
Attempts (PSTN)	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	✓	✓	✓	✓
SIM1 APN (GPRS)	N/A	✓			✓
SIM1 User (GPRS)	N/A	✓			✓
SIM1 Password (GPRS)	N/A	✓			✓
SIM2 APN (GPRS)	N/A				✓
SIM2 User (GPRS)	N/A				✓
SIM2 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... 5	N/A		✓	✓	✓
Protocol over GPRS	EGR100				✓

Additional Parameters

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	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				✓

Dual-SIM Management

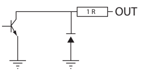
Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
SIM Card Switch	Disabled				✓
Return to Primary SIM	Enabled				✓
Send SMS / Call via	Currently in Use SIM				✓
Try to Find Operator for a Maximum of	3 times				✓

Smart Security

Parameter	Default Value	Configurable by:			
		SMS	EKB2	EKB3/ EKB3W	Configuration Tool
Smart Security	Disabled				✓
Server Address	ss.eldes.lt				✓
Port	8082				✓
Ping Period	180 seconds				✓
Time Zone	0				✓

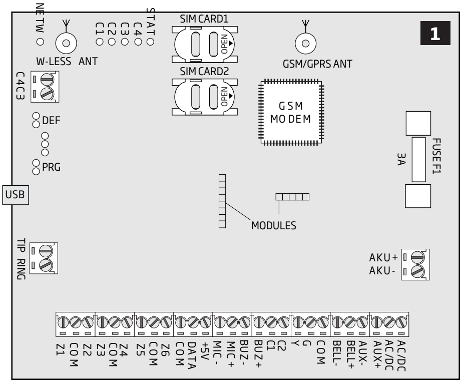
2. TECHNICAL SPECIFICATIONS

2.1. Electrical & Mechanical Characteristics

Electrical & Mechanical Characteristics	
Main power supply	16-24V 50 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current in standby without external sensors and keypad	Up to 80mA
Recommended backup battery voltage, capacity	12V; 1,3-7 Ah
Recommended backup battery type	Lead-Acid
Maximum battery charge current	900mA
Gsm modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
Number of zones on-board	6 (ATZ mode: 12)
Nominal zone resistance	5,6kΩ (ATZ Mode: 5,6kΩ and 3,3kΩ)
Number of PGM outputs on-board	4
On-board PGM output circuit	 Open Collector Output. Output is pulled to COM when turned ON.
Maximum commuting on-board PGM output values	4 x Voltage – 30V; current – 500mA.
BELL: Siren output when activated	Connected to COM
BELL: Maximum siren output current	1A
BELL: Maximum cable length for siren connection	Up to 100 meters
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
AUX: Maximum accumulative current of auxiliary equipment	1,1A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100 meters
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC
BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	8
DATA: Maximum cable length for 1-Wire communication	Up to 30 meters
DATA: Cable type for 1-Wire communication	Unshielded
Supported ibutton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	16
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100 meters
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2 meters
MIC: Cable type for microphone connection	Unshielded
Wireless transmitter-receiver frequency	868 Mhz (EU version) / 915 Mhz (US version)
Wireless communication range	Up to 30m in premises; up to 150m in open areas
Maximum supported number of wireless devices	32
Event log size	500 events
Maximum supported number of zones	76
Maximum supported number of pgm outputs	76
Cable type for zone and pgm output connection	Unshielded
Communications	SMS, Voice calls, GPRS network, RS485, CSD, PSTN
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS
Dimensions	140x100x18mm
Operating temperature range	-20...+55 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)

2.2. Main Unit, LED & Connector Functionality

Main Unit Functionality	
GSM MODEM	GSM network 850/900/1800/1900MHz modem
SIM CARD1	Primary SIM card slot / holder
SIM CARD2	Secondary SIM card slot / holder
DEF	Pins for restoring default settings
USB	Mini USB port
FUSE F1	3A fuse
W-LESS ANT	Wireless antenna SMA type connector
GSM/GPRS ANT	GSM/GPRS antenna SMA type connector
MODULES*	Slots for EA1, EA2 or EPGM8 module



LED Functionality	
NETW	GSM network signal strength
C1	PGM output C1 status - ON/OFF
C2	PGM output C2 status - ON/OFF
C3	PGM output C3 status - ON/OFF
C4	PGM output C4 status - ON/OFF
STAT	Micro-controller status

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

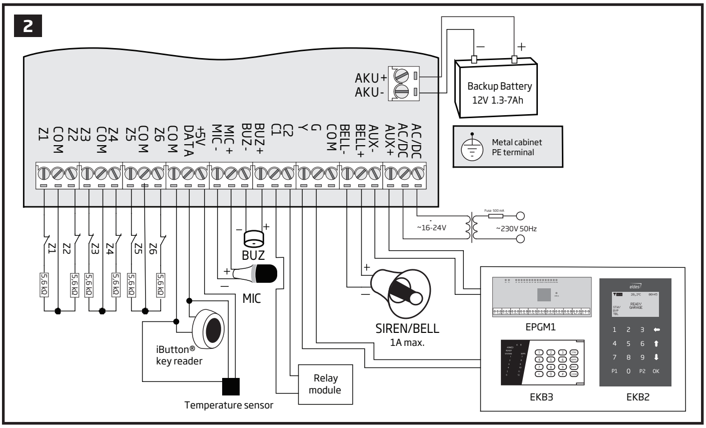
Connector Functionality	
TIP*	PSTN (landline) terminal
RING*	PSTN (landline) terminal
DATA	1-Wire interface for iButton key & temperature sensor connection
+5V	Temperature sensor power supply terminal (+5V)
MIC-	Microphone negative terminal
MIC+	Microphone positive terminal
BUZ-	Buzzer negative terminal
BUZ+	Buzzer positive terminal
C1 - C4	PGM output terminals
Z1 - Z6	Security zone terminals
Y	RS485 interface CLOCK terminal (yellow wire)
G	RS485 interface DATA terminal (green wire)
COM	Common return terminal
BELL-	Siren negative terminal
BELL+	Siren positive terminal
AUX-	Negative power supply terminal for auxiliary equipment
AUX+	Positive power supply terminal for auxiliary equipment
AC/DC	Main power supply terminals
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

* - Optional, implementable on request in advance

2.3. Wiring Diagrams

2.3.1.General Wiring

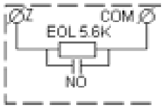
2



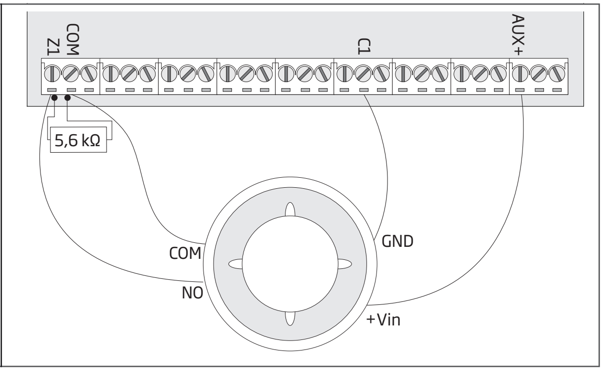
2.3.2. Zone Connection Types

Type 1 Example of 4-wire smoke detector wiring

3

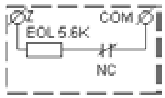


6-Zone mode: Normally open contact with 5,6KΩ end-of-line resistor.

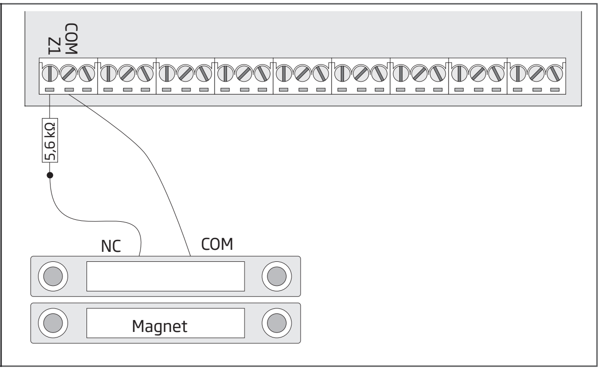


Type 2 Example of magnetic door contact wiring

4



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

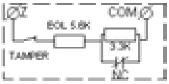


NOTE: Based on the example given, in the event of an alarm, the smoke detector could be reset by turining OFF and ON the PGM output C1. For more details, please refer to **18.4. Turning PGM Outputs ON and OFF.**

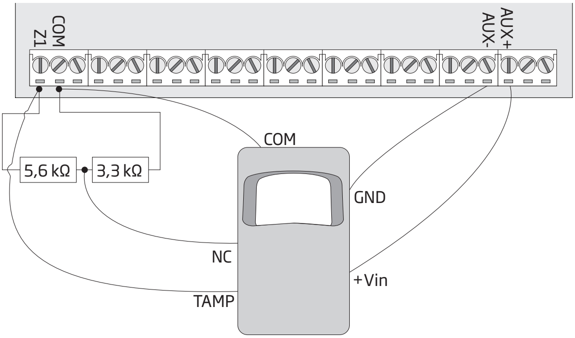
NOTE: The system does NOT support 2-wire smoke detectors.

Type 3 Example of motion detector wiring

5

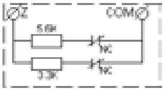


6-Zone mode: Tamper and 5,6KΩ end-of-line resistor and 3,3KΩ end-of-line resistor with normally closed contact.

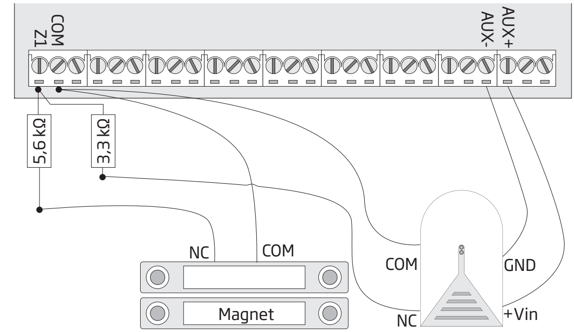


Type 4 Example of magnetic door contact (Z1) and glass break sensor (Z7) wiring

6

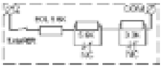


ATZ mode: 5,6KΩ end-of-line resistor and normally closed contact with 3,3KΩ end-of-line resistor and normally closed contact

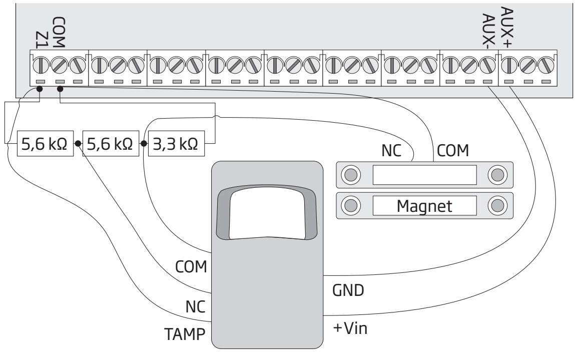


Type 5 Example of motion detector (Z1) and magnetic door contact (Z7) wiring

7



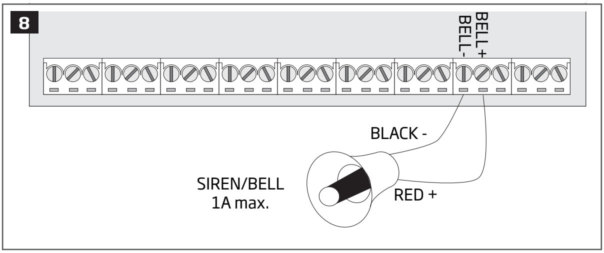
ATZ mode: Tamper, 5,6KΩ end-of-line resistor, 5,6KΩ end-of-line resistor with normally closed contact and 3,3KΩ end-of-line resistor with normally closed contact.



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

2.3.3. Siren

8

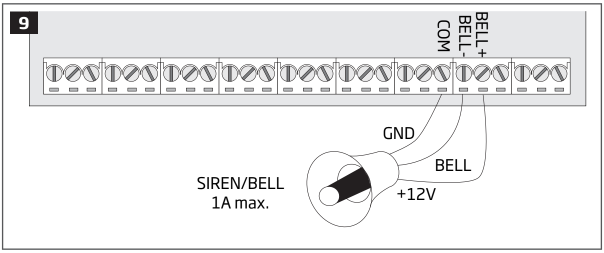


Piezo siren

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

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

9



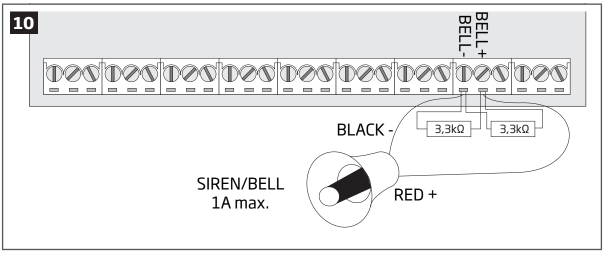
Self-contained siren

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.

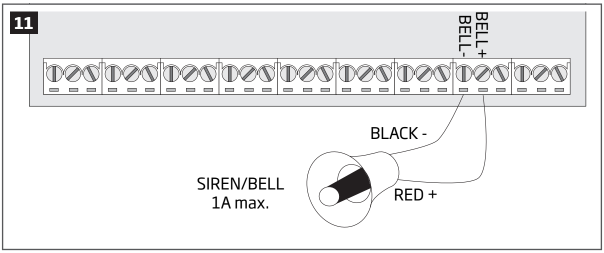
10



Siren status monitoring

By default, the system monitors siren status and indicates system fault on the keypad if the siren is broken/disconnected. However, this feature requires a pair of parallelly connected resistors of 3,3kΩ nominal across **BELL+** and **BELL-** terminals.

11



No siren status monitoring

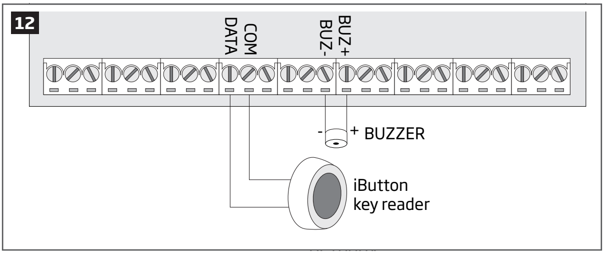
If the siren status monitoring feature is not required, do not connect any resistor in parallel and disable siren fault indication on the keypad (see **29. INDICATION OF SYSTEM FAULTS**).

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

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

NOTE: Siren status monitoring feature supervises the resistance across **BELL+** and **BELL-** terminals. The resistance must be ranging from 1kΩ through 3,3kΩ, otherwise the system will indicate system fault.

2.3.4. iButton Key Reader and Buzzer



Supported iButton key model: Maxim/Dallas DS1990A

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

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

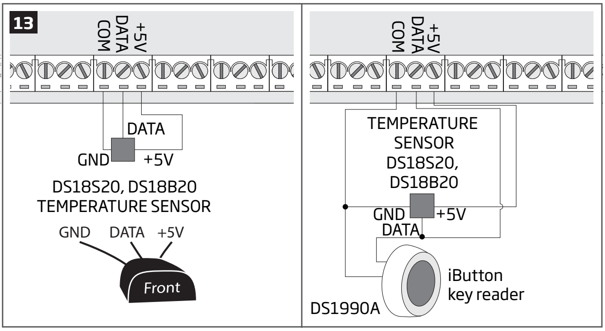
NOTE: The installation of buzzer is not necessary if EKB2/EKB3 keypad is used.

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

2.3.5. Temperature Sensor and iButton Key Reader

Supported iButton key model: Maxim/Dallas DS1990A

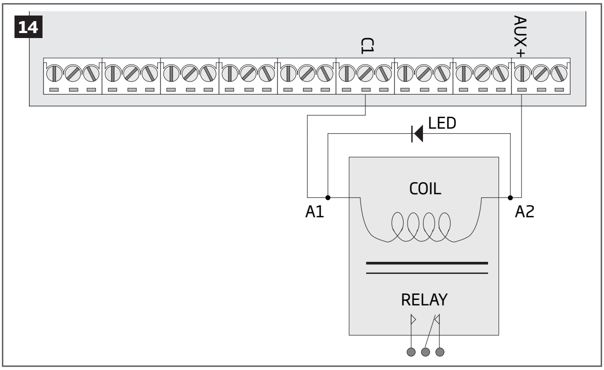
Supported temperature sensor model: Maxim/Dallas DS18S20, DS18B20



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

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

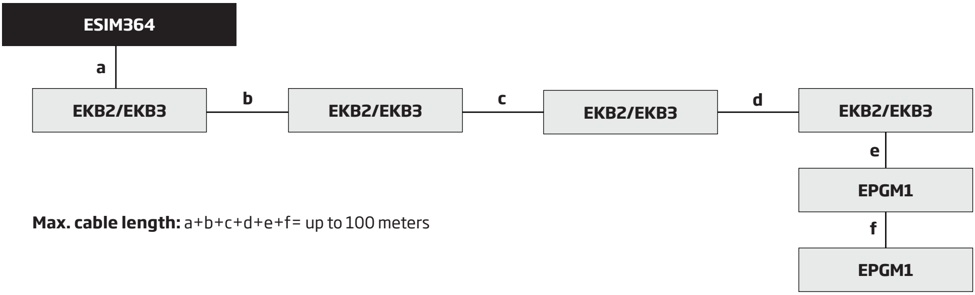
2.3.6. Relay Finder 40.61.9.12 with Terminal Socket 95.85.3 to PGM Output



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

2.3.7. RS485

Serial Wiring Method



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

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

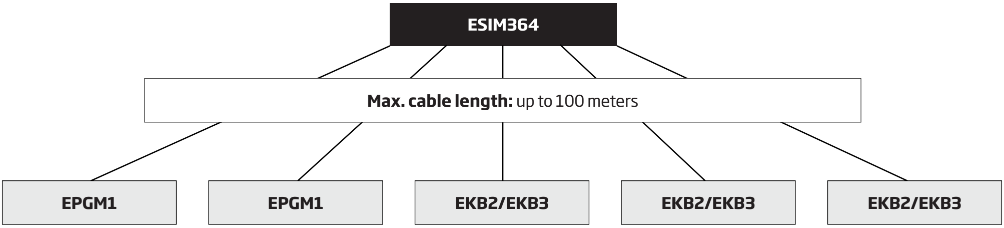
ATTENTION: The cable length must not exceed 100 meters in total.

ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module 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

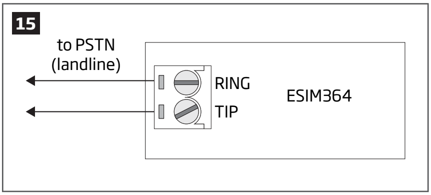
ATTENTION: The cable between ESIM364 and each RS485 device must be of the same length and can NOT exceed 100 meters.

ATTENTION: When wiring more than 1 keypad and/or EPGM1 module, please ensure that the set address of each keypad and/or EPGM1 module 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**

2.3.8. RING/TIP



ATTENTION: The **TIP/RING** connectors and PSTN module are NOT included in a standard ESIM364 alarm system unit. These components are optional and can be implemented on request in advance.

3. INSTALLATION

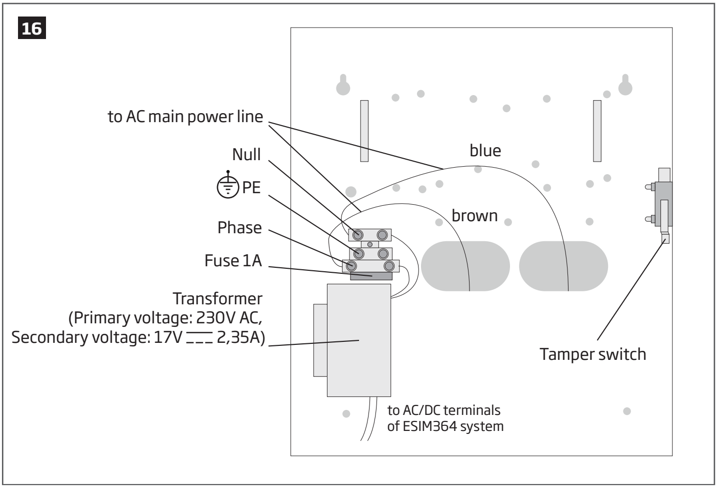
When professional installation, OEM integration or assembly by a third-party is expected, the installation instructions and assembly requirements approved for equipment approval must be provided to the integrators to clearly identify the specific requirements necessary to maintain RF exposure compliance. The grantee of a transmitter, typically the manufacturer, is responsible for ensuring installers and integrators have a clear understanding of the compliance requirements by including the required instructions and documentation with the product and, if necessary, to provide further support to fulfill grantee responsibilities for ensuring compliance. The integrators must be fully informed of their obligations and verify the resolution of any issues and concerns with each transmitter manufacturer or grantee.

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

System Installation in ME1 Metal Cabinet

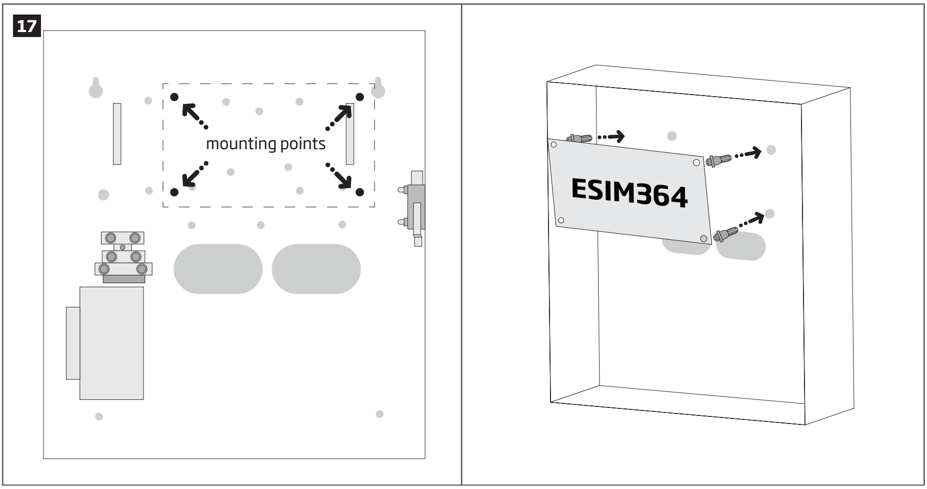
1. ME1 metal cabinet components

16

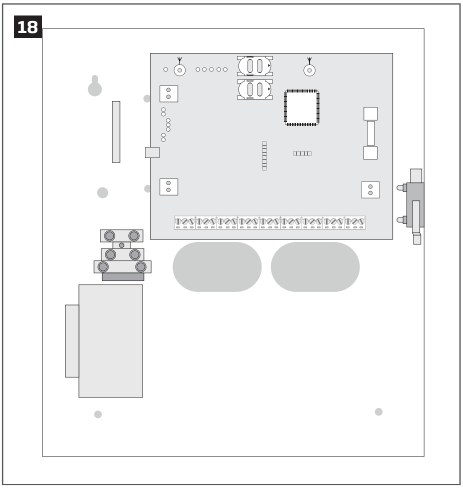


2. Insert the plastic standoffs into the appropriate mounting points and fix the board of ESIM364 on the holders as indicated below.

17

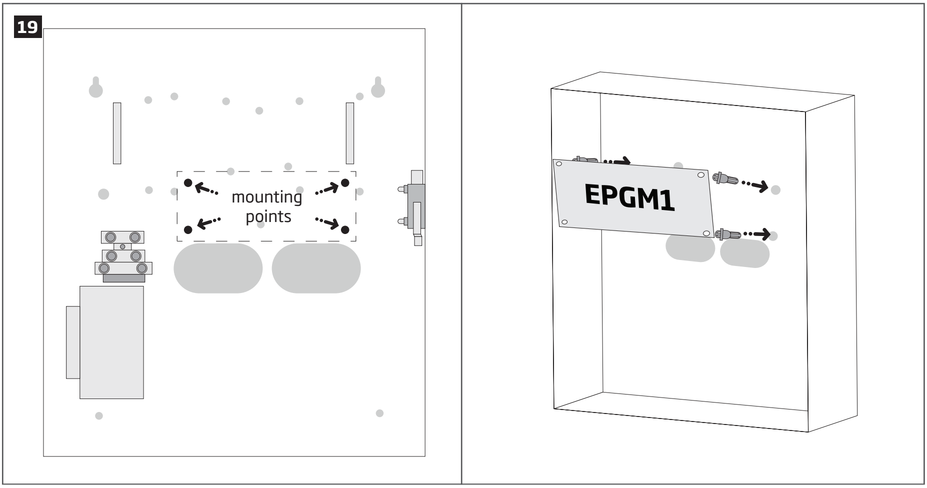


18

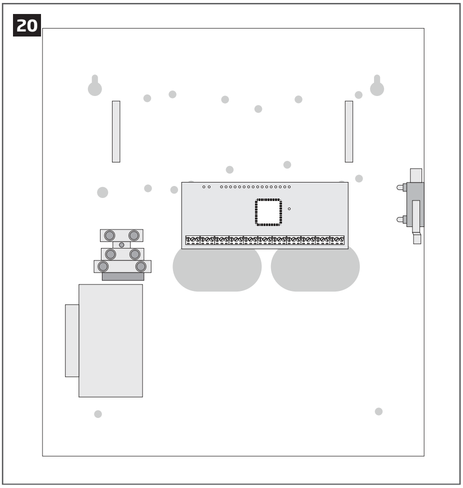


3. If EPGM1 module is to be installed, please install it in the first place and ESIM364 alarm system afterwards. EPGM1 must be mounted on the shorter plastic standoffs, while ESIM364 – on the longer ones. The mounting points of EPGM1 module are indicated below.

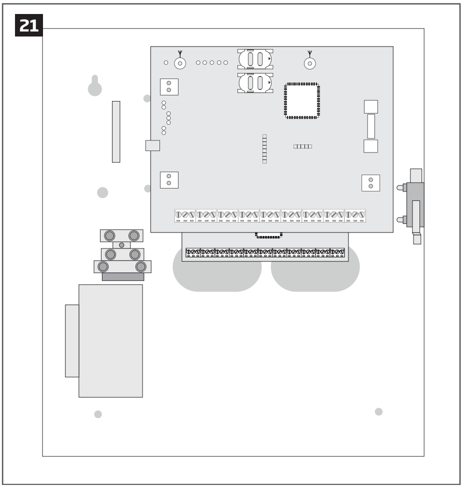
19



20



21

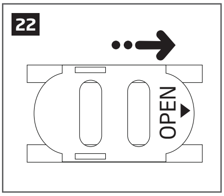


4. Wire up the system according to the wiring diagrams. Install the buzzer closer to iButton key reader in order to hear the exit delay countdown. A LED indicator can be used in parallel to the buzzer or instead. For a convenient installation, ED1 is highly recommended (see **2.3 Wiring Diagrams** for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

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

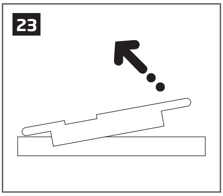
6. Once the PIN code is disabled, place the SIM card into the SIM CARD1 slot of the alarm system. If Dual-SIM feature is to be used, insert another SIM card into the SIM CARD2 slot. For more details, please refer to **31. DUAL-SIM MANAGEMENT.**

22

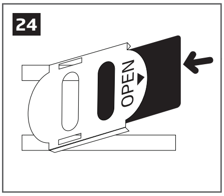


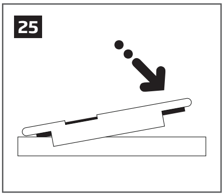
Inserting a SIM card into SIM CARD1 slot is mandatory as it is the main SIM card slot, while using a SIM card in SIM CARD2 slot is optional.

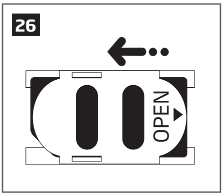
23



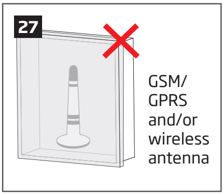
24





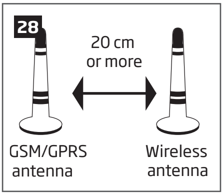


7. Connect the GSM/GPRS and wireless antennas and follow the recommendations for the installation:



Never install in the following locations:

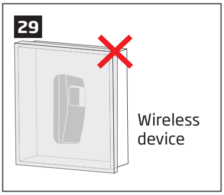
- inside the metal cabinet
- closer than 20 cm from the metal surface and/or power lines



Recommended installation:

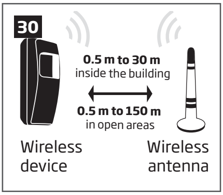
- keep the distance of at least 20 cm or more.

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



Never install in the following locations:

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



Recommended installation:

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

For more details on how to install the wireless devices, please refer to **33. ELDES WIRELESS DEVICES** and **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual located at www.eldes.lt/download

9. Power up the system and wait until indicator STAT lights up.
10. The system starts up in less than a minute. Indicator STAT should be flashing indicating successful micro-controller operation.
11. The illuminated indicator NETW 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 NETW indicator (see **2.3. Main Unit, LED & Connector Functionality**).
12. Change the default SMS password (see **6. PASSWORDS** for more details).
13. Set the phone number for User 1 (see **8. USER PHONE NUMBERS** for more details).
14. Set system date and time (see **9. DATE AND TIME** for more details).
15. Once the system is fully configured, it is ready for use. However, if you fail to receive an SMS reply from the system, please check the SMSC (Short Message Service Center) phone number. For more details regarding the SMS centre phone number, please refer to **27.1. SMSC (Short Message Service Center) Phone Number.**

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

NOTE: The installation of iButton key reader, EKB2/EKB3/EKB3W keypad, EWK1 wireless keyfob is not mandatory. However, it is recommended to have those devices installed as an emergency switch in case your mobile phone is switched off or missing.

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

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

NOTE: Even though alarm system ESIM364 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. By default, exit delay duration is 15 seconds. After the countdown is complete, the system will become armed and lock the configuration by keypad possibility. In case the user does not leave the secured area before the countdown is complete, the system will will arm in Stay mode if at least 1 zone has Stay attribute enabled. By default, if there is at least 1 violated zone or tamper, the user will not be able to arm the system until the violated zone or tamper is restored. In case it is required to arm the alarm system despite the violated zone presence, the violated zone can be bypassed or Force attribute enabled.

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

After the user enters the secured area, the system will initiate the entry delay countdown intended for system disarming. During the countdown period, the buzzer will emit a steady beep. 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.

EN50131-1
GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All passwords must consist of 6 digits.
- The system must prompt for SMS and administrator passwords (see **6. PASSWORDS**) when configuring the system using *ELDES Configuration Tool* software.
- The system must prompt for user (see **10. USER PASSWORDS**) and administrator (see **6. PASSWORDS**) passwords when configuring the system by EKB2, EKB3, EKB3W keypad.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

SMS

In order to configure and control the system by SMS text message, send the text command to the ESIM364 system phone number from one of the preset user phone numbers. The structure of SMS text message consists of 4-digit SMS password (the default SMS password is 0000 – four zeros), the parameter and value. For some parameters the value does not apply e. g. STATUS. The variables are indicated in lower-case letters, while a valid parameter value range is indicated in brackets.

EKB2

The system configuration and control by EKB2 keypad is carried out by navigating throughout the menu section list displayed on LCD screen. To navigate in the menu path, touch ↓, ↑ keys to select the desired menu section and touch OK key to open the selected section. To enter a required value, use 0... 9 keys and touch OK key for confirmation or cancel/go one menu section back by touching ← key. The value can be typed in directly by touching 0... 9 keys while highlighting the desired menu section. EKB2 menu type is "circle", therefore when the last section in the menu list is selected, you will be brought back to the beginning of the list after touching the ↓ key. In this installation manual, the menu path is based on the EKB2 menu tree by starting at home screen view (see **32.1.1.6. EKB2 Menu Tree**). The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

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

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

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

EKB3/
EKB3W

The system configuration and control by EKB3/EKB3W keypad is carried out by activating the Configuration mode using the administrator password (by default – administrator password is **1470**) and entering a valid configuration command using the number keys [0]... [9], [#] key for confirmation and [*] key to cancel the characters that are being entered. Alternatively, the user can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cancelled. When typing in the characters, the indication of each pressed key is provided by short beep of keypad buzzer and red indicators when the number keys [0]... [9] are being pressed. Some commands require [BYPS], [CODE] and [STAY] keys as well. The structure of a standard configuration command is a combination of digits. The commands, which do not require the Configuration mode being activated, are noted. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

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

NOTE FOR EKB3W USERS: Even if Back-light Timeout has expired, the character will be considered as type in once the appropriate EKB3W key is pressed. For more details, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout .**

Activate/deactivate Configuration mode

EKB3/
EKB3W

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

EN50131-1
GRADE 3

Activate/deactivate Configuration mode

EKB3/
EKB3W

Enter administrator and SMS passwords:
* aaaaaa uuuuuu #
Value: *aaaaaa* – 6-digit administrator password; *uuuuuu* – 6-digit user password.
Example: **147000111111#*

The following table provides a list of EKB3/EKB3W indications, which are relevant during Configuration mode.

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

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

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

Config Tool

Software *ELDES Configuration Tool* is intended for ESIM364 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: www.eldes.lt

Remote System Configuration via GPRS Connection

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

ATTENTION: When the Configuration mode is activated by EKB3/EKB3W keypad or menu section CONFIGURATION is opened by EKB2 keypad, remote system configuration will be disabled.

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

Before configuring ESIM364 remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM CARD1 slot of ESIM364 device (see **2.2. Main Unit, LED & Connector Functionality**).
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to ESIM364.
- Default SMS password is changed to a new 4-digit password (see **6. PASSWORDS**).
- At least User 1 phone number is set up (see **8. USER PHONE NUMBERS**).
- APN, user name and password are set up (see **30.2.1. GPRS Network**).

Establishing Remote Connection Between ESIM364 System and Configuration Server

Initiate the connection to ELDES server

In order to activate a remote GPRS connection between ESIM364 system and ELDES configuration server please , send the following SMS text message from user phone number.

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

SMS

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

Initiate the connection to third-party server

In case it is necessary to establish a connection between ESIM364 system and a third-party configuration server, send the following SMS text message.

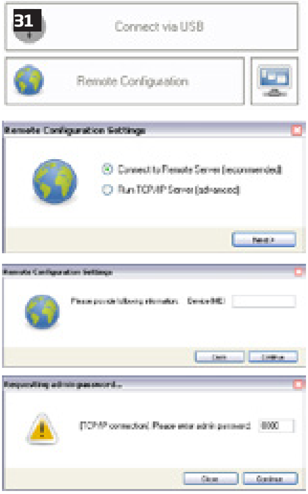
SMS

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

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

Connecting to ELDES Configuration Server using ELDES Configuration Tool Software

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


31
Connect via USB
Remote Configuration
Remote Configuration Settings
○ Connect to Remote Server (recommended)
○ Run TCP/IP Server (advanced)
Next >
Remote Configuration Settings
Back
Continue
Requesting admin password...
Close
Continue

Please provide following information: Device IMEI

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

Ending the Configuration Process

Shut down the Connection with the Server

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

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

SMS

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

6. PASSWORDS

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

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

Set SMS password

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Set Administrator password

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

EN50131-1 GRADE 3

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All passwords must consist of 6 digits.
- The system must prompt for SMS and administrator passwords when configuring the system using *ELDES Configuration Tool* software.
- The system must prompt for user (see **10. USER PASSWORDS**) and administrator passwords when configuring the system by EKB2, EKB3, EKB3W keypad.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

7. SYSTEM LANGUAGE

The system comes equipped with a single language for communication with the user by SMS text messages and EKB2 keypad menu display. The system language depends on ESIM364 firmware, which is based on the user's location.

List of currently available system languages (firmwares):

- Czech
- English
- Estonian
- Finnish
- French
- Greek
- Hungarian
- Italian
- Latvian
- Lithuanian
- Portuguese
- Russian
- Slovak
- Spanish

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

8. USER PHONE NUMBERS

The system supports up to 10 user phone numbers identified as User 1 through 10. 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 1**2.2. SMS Text Message**) as well as to configure the system by SMS text messages. User phone numbers are also used to receive alarm phone calls and SMS text messages from the system (see **17. ALARM INDICATIONS AND NOTIFICATIONS**).

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

To set User 1 phone number is mandatory, while the other 9 are optional. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for UK: +4417091111111. This format can be used when setting up the phone number by SMS text message and *ELDES Configuration Tool* software.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: 004417091111111. This format can be used when setting up the phone number by SMS text message, EKB2/EKB3/EKB3W keypad and *ELDES Configuration Tool* software.
- **Local –** The phone numbers must be entered starting with an area code in the following format: [area code][local number], example for UK:017091111111. This format can be used when setting up the phone number by SMS text message, EKB2/ EKB3/EKB3W keypad and *ELDES Configuration Tool* software.

Set user phone number

SMS

SMS text message content:
ssss_NRup:ttteeellnnuumm
Value: *ssss* – 4-digit SMS password; *up* – user phone number slot, range – [1... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1111_NR1:+4417091111111*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 10 → OK → PHONE NUMBER → OK → ttteeellnnuumm → OK
Value: *aaaa* – 4-digit administrator password; *ttteeellnnuumm* – up to 15 digits user phone number.

EKB3/ EKB3W

Enter parameter 17, user phone number slot & phone number:
17 up ttteeellnnuumm #
Value: *up* – user phone number slot, range – [01... 10]; *ttteeellnnuumm* – up to 15 digits user phone number.
Example: *1701004417091111111#*

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... 10 → OK → 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... 10].
Example: *1111_NR2:DEL*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 2... 10 → OK → PHONE NUMBER → OK → OK
Value: *aaaa* – 4-digit administrator password.

Config Tool

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

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

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

NOTE: Multiple user phone numbers can be set by a single SMS text message, **Example:** *1111_NR1:+4417091111111_NR2:+4417091111112_NR6:017091111113_NR10:+4417091111114*

NOTE: Multiple user phone numbers can be deleted by a single SMS text message, **Example:** *1111_NR2:DEL_NR3:DEL_NR6:DEL_NR9:DEL_NR:10:DEL*

8.1. User Phone Number Names

When the system is armed or disarmed by free of charge phone call or SMS text message, the system sends a confirmation by SMS text message to user phone number that the system arming/disarming was initiated from. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user phone number.

Manage user phone number name

Config Tool

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

8.2. System Control from any Phone Number

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

Enable system control from any phone number

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Disable system control from any phone number

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

9. DATE AND TIME

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

Set date and time

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

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

10. USER PASSWORDS

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

Set user password

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (1-16) → OK → USER PASSWORD 1... 16 → OK → PASSWORDS → OK → uuuu → OK
User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PASSWORDS → OK → uuuu → OK
Value: *aaaa* – 4-digit administrator password*; uuuu* – 4-digit user password, range – [0000... 9999].

EKB3/ EKB3W

Enter parameter 15, user password slot & user password:
15 us uuuu #
Value: *us* – user password slot, range – [01... 30]; *uuuu* – 4-digit user password; range – [0000... 9999].
Example: *15021111#*

Config Tool

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

Delete user password

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → REMOVE PASSWORD → OK → uuuu → OK
Value: *aaaa* – 4-digit administrator password; *uuuu* – 4-digit user password.

EKB3/ EKB3W

Enter parameter 65 & user password:
65 uuuu #
Value: *uuuu* – 4-digit user password.
Example: *651111#*

Config Tool

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

Replace user password

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (1-16)→ OK → USER PASSWORD 1... 16 → OK → PASSWORD → OK → uuuu → OK
User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK → USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PASSWORD → OK → uuuu → OK
Value: *aaaa* – 4-digit administrator password; *uuuu* – 4-digit user password, range – [0000... 9999].

EKB3/ EKB3W

Enter parameter 63, existing user password & new user password:
63 vvvv uuuu #
Value: *vvvv* – 4-digit existing user password; *uuuu* – 4-digit new user password, range – [0000... 9999].
Example: *6311113254#*

Config Tool

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

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

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

Set SGS password

EKB2

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

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

EKB3/ EKB3W

Enter parameter 74 & user password slot:
74 us #

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

Config Tool

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

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

Set Duress password

EKB2

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

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

EKB3/ EKB3W

Enter parameter 73 & user password slot:
73 us #

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

Config Tool

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

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following features:

- All passwords must consist of 6 digits.
- The system must prompt for user and administrator (see **6. PASSWORDS**) passwords when configuring the system by EKB2, EKB3, EKB3W keypad.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

10.1. User Password Names

When the system is armed or disarmed by entering a user password using a keypad, the system sends a confirmation by SMS text message to user phone number, sharing the same partition (-s) as the keypad and user password. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the user password.

Manage user password name

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. ESIM364 system supports up to 16 iButton keys each holding a unique identity code (ID), which is used for system arming and disarming.

11.1. Adding and Removing iButton Keys

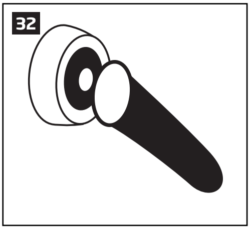
To add an iButton key to the system, do the following:

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

b) Enable Allow Adding New iButton Keys mode.

c) T ouch the key to the iButton key reader when the system is disarmed (see Fig. No. 32).

32



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

e) Add as many iButton keys as necessary – touch one key after another to the reader – until the number of 16 keys is reached.

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

Enable Allow Adding New iButton Keys mode

SMS	**SMS text message content:** ssss_IBPROG:ON **Value:** *ssss* – 4-digit SMS password. **Example:** *1111_IBPROG:ON*
EKB2	**Menu path:** OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → NEW IBUTTON → OK → ENABLE → OK **Value:** *aaaa* – 4-digit administrator password.
EKB3/ EKB3W	**Enter parameter 18 & parameter status value:** 18 0 # **Example:** *180#*
Config Tool	This operation may be carried out from the PC using the *ELDES Configuration Tool* software.

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

Disable Allow Adding New iButton Keys mode

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

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

View iButton key ID

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → IBUTTON KEYS → OK → IBUTTON 1... 16 → 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... 16 → 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*

11.2. iButton Key Names

When the system is armed or disarmed by iButton key, the system sends a confirmation by SMS text message to preset user phone number, sharing the same partition (-s) as the key. The SMS text message is sent regarding each partition separately and contains system status and partition name as well as it may contain a user name, set to the iButton key.

Manage iButton key name

Config Tool

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

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/EKB3W keypad and user password.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm-Disarm by Zone.
- EGR100 middle-ware.

The system arms/disarms the partitions that the preset user phone number, EKB2/EKB3/EKB3W keypad and user password, 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 1, 2 and 4, the user will be able to arm/disarm Partition 1, 2 and 4 by a single phone call to the system (see **23. PARTITIONS**).

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

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

- Main power supply is lost.
- Low battery.
- Battery dead or missing.
- Battery failed.
- Siren failed.
- Date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Wireless antenna failed.

When attempting to arm the system (by any method, except EKB2/EKB3/EKB3W keypad and user password, EGR100 middle-ware) in case of violated zone/tamper presence, the system will reply with SMS text message containing violated zone/tamper number. Due to security reasons it is highly recommended to restore the violated zone/tamper before arming the system. For more details on how to arm the system despite the violated zone presence, please refer to **14.6. Zone Attributes** and **14.7. Bypassing and Activating Zones.**

The system ignores any incoming calls and SMS text messages from a non-preset phone number as well as it rejects the SMS text messages containing wrong SMS password even from a preset user phone number. For more details regarding arming/disarming the system from a non-preset phone number, please refer to **8.2. System Control from any Phone Number**.

EN50131-1 **GRADE 3**

To comply with EN50131-1 Grade 3 standard requirements, the system must be equipped with the following feature:

- System arming is blocked if any system fault exists. The user wil not be able to arm the system until all existing system faults are solved.

For complete list of EN50131-1 Grade 3 standard requirements and how to enable/disable the associated features, please refer to **35. EN 50131-1 GRADE 3.**

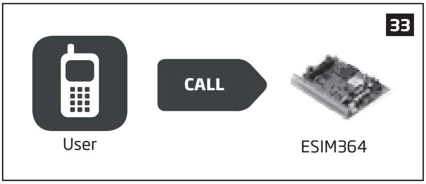
12.1. Free of Charge Phone Call

To arm and disarm the system, dial the system's phone number from any of 10 available user phone numbers (see **8. USER PHONE NUMBERS** for user phone number management). The phone call is free charge as the system rejects it and carries out arming/disarming procedure afterwards. When arming – the system rejects the phone call after 2 rings, when disarming – the system rejects the phone call immediately. If there is more than one preset user dialing to the system at the same time, the system will accept the incoming call from the user who was the first to dial while other user (-s) will be ignored.

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

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

When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by dialing the system's phone number. For example, if User 1 is assigned to Partition 1, 2 and 3, the user will be able to arm/disarm Partition 1, 2 and 3 by a single phone call to the system from User 1 phone number. 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

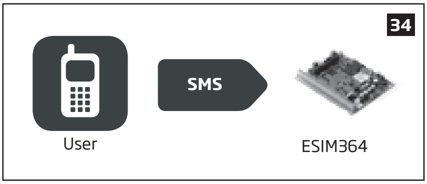
SMS

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

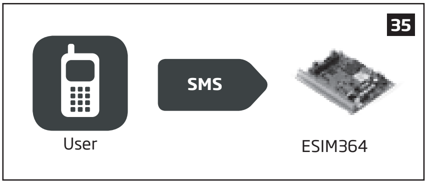
SMS text message content:
ssss_ARMp or ssss_ARMp,p,p,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4].
Example: *1111_ARM1*



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,p,p
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4].
Example: *1111_DISARM1,2,4*



When a user phone number is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by sending the SMS text message to the system's phone number. For example, if User 3 is assigned to Partition 2 and 3, the user will be able to arm/disarm Partition 2 and/or 3 by sending an SMS text message from User 3 phone number. For more details on how to set user phone number partition, please refer to **23.2. User Phone Number Partition**.

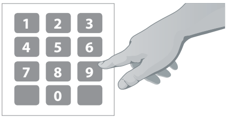
12.3. EKB2 Keypad and User Password

EKB2

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

- **Non-partitioned system** – When a valid user password is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the keypad will display 🏃 icon next to the countdown timer. When the system is successfully armed, the keypad will display 🔒 icon for 5 seconds and switch to home screen view.
- **Partitioned system; arming the same partition as the keypad is assigned to** – When a valid user password is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. If ← key is touched during exit delay, the keypad will display 🏃 icon next to the countdown timer. When successfully armed, the keypad will display 🔒 icon for 3 seconds and switch to home screen view.
- **Partitioned system; arming a different partition than the keypad is assigned to** – When a valid user password is entered, the keypad will display the partition selection menu. Once a partition that is to be armed is selected, the system will initiate exit delay, but will not indicate it on EKB2 keypad due to the difference between keypad partition and the one being armed. Then the keypad will display **ARMING part-name** message for 3 seconds followed by partition selection menu. When the keypad back-light timeout expires, the home screen view will follow.

Arm the system



Enter user password/menu path:
Non-partitioned system: uuuu → OK
Partitioned system: uuuu → OK → [p] part-name → OK
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.
Example: *1111 → OK → [2] PART2 → OK*

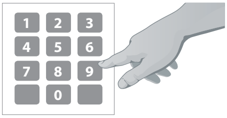
To cancel the system arming process:

- **Non-partitioned system** – Enter the user password again during exit delay countdown.
- **Partitioned system** – Select the partition again, that is currently being armed, from the partition selection menu during exit delay countdown. The keypad will display **part-name ARMING TERMINATED** message followed by the partiton selection menu. When the keypad back-light timeout expires, the home screen view will follow.

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

- **Non-partitioned system** – When a valid user password is entered, the keypad will display 🔓 icon for 3 seconds and switch to home screen view.
- **Partitioned system** – When a valid user password is entered, the keypad will display the partition selection menu. Once a partition that is to be disarmed is selected, the keypad will display **part-name DISARMED** message for 3 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires.

Disarm the system



Enter user password/menu path:
Non-partitioned system: uuuu → OK
Partitioned system: uuuu → OK → [p] part-name → OK
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.
Example: *1111 → OK → [3] GARAGE → OK*

When a user password is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by EKB2 keypad using partition selection menu if one of the user password partitions correspond to the keypad partition. For example, if User Password 3 is assigned to Partition 1, 2 and 4, while EKB2 keypad is assigned to Partition 2, the user will be able to arm/disarm Partition 1, 2 and 4 by entering User Password 3 and selecting the partitions from the partition selection menu. For more details on how to set keypad partition and user password partition, please refer to **23.3. Keypad Partition and Keypad Partition Switch** and **23.4. User Password Partition**.

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

Use keypad partition switch

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

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

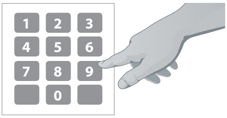
12.4. EKB3 Keypad and User Password

EKB3

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

To arm the system by EKB3 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad (see **10. USER PASSWORDS** for user password management). By default, when a valid user password is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED and the number [1]... [4] key, indicating the partition that is to be armed, will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

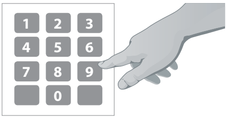


Enter user password:
uuuu
Value: *uuuu* – 4-digit user password.
Example: *1111*

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

To disarm the system by EKB3 keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad. By default, when a valid user password is entered, EKB3 keypad indicator ARMED and the number [1]... [4] key, indicating the partition that has been disarmed, will light OFF.

Disarm the system



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

The system will arm/disarm the partition corresponding to the one that user password (see **23.4. User Password Partition**) and the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) are assigned to. For example, if User Password 4 is assigned to Partition 2, 3 and 4, while EKB3 keypad is assigned to Partition 2, the user will be able to arm/disarm only Partition 2 by entering User Password 4.

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

Hold the [1]... [4] key and release it after 3 short beeps:
Value: [1]... [4] key – parition number 1... 4.

If 4 partitions exist in the system, user can arm/disarm all the partitions simultaneously. When this feature is used, the system will proceed as follows:

- **If all partitions are disarmed ready (no violated zone/tamper):**
  - The system will initiate exit delay.
  - The keypad indicator ARMED along with number [1]... [4] keys will light ON.
  - The partitions will arm.
- **If one or more partitions are disarmed unready (keypad number [1]... [4] key flashing, indicating the partition that contains violated zone/tamper):**
  - The system will initiate exit delay.
  - Keypad indicator ARMED (if the keypad is switched to a non-violated partition) along with number [1]... [4] keys will light ON.
  - The ready partition (-s) will arm and the unready one (-s) will be skipped. 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**).
- **If a combination of armed and disarmed ready partitions is present:**
  - The system will initiate exit delay
  - The keypad indicator ARMED (if the keypad is switched to a disarmed partition) along with number [1]... [4] key (-s), indicating the partition (-s) that is to be armed, will light ON.
  - The disarmed ready partitions will be armed and the armed ones will be skipped.

Arm/disarm all 4 partitions simultaneously

Hold the [0] key, release it after 3 short beeps and enter user password:
0 uuuu
Value: *uuuu* – 4-digit user password.
Example: *0 1111*

NOTE: To arm/disarm all partitions simultaneously, the user password must be assigned to all 4 partitions and the keypad partition switch feature enabled (see **23.3. Keypad Partition and Keypad Partition Switch**).

NOTE: The system will deny disarming all partitions simultaneously if at least one partition contains violated zone/tamper.

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

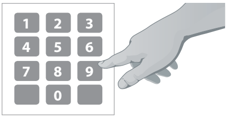
12.5. EKB3W Keypad and User Password

EKB3W

Illuminated indicator READY on EKB3W 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 EKB3W keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad (see **10. USER PASSWORDS** for user password management). By default, when a valid user password is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator ARMED will light ON on EKB3W keypad. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system

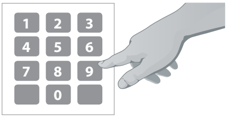


Enter user password:
uuuu
Value: *uuuu* – 4-digit user password.
Example: *1111*

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

To disarm the system by EKB3W keypad, enter any out of 30 available 4-digit user passwords using the number keys on the keypad. By default, when a valid user password is entered, EKB3W keypad indicator ARMED will light OFF.

Disarm the system



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

The system will arm/disarm the partition corresponding to the one that user password (see **23.4. User Password Partition**) and the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) are assigned to. For example, if User Password 4 is assigned to Partition 2, 3 and 4, while EKB3W keypad is assigned to Partition 2, the user will be able to arm/disarm only Partition 2 by entering User Password 4.

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

Hold the [*] key, release it after 3 short beeps & enter partition number:
* p
Value: *p* – partition number, range – [1... 2]
Example: **2*

NOTE: Only Partition 1 and Partition 2 can be armed/disarmed using EKB3W keypad.

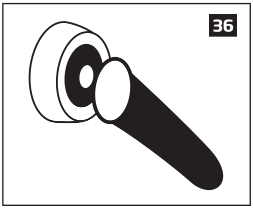
NOTE: By default, User Password 1 is preset as **1111** and assigned to Partition 1

12.6. iButton Key

To arm or disarm the system, touch the iButton key reader by any of 16 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:

- **Non-partitioned system:**
  - 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**).

- **Partitioned system:**
  - If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and 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, sharing the same partition (-s) as the iButton key. 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**).
  - If a combination of armed and disarmed ready partitions is present, the system will initiate exit delay, arm the disarmed ready partitions and skip the armed ones.


36

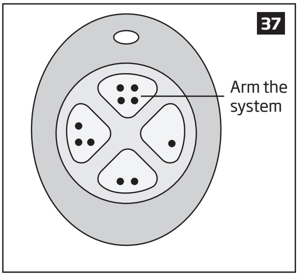
When an iButton key is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by touching the iButton key to the reader. For example, if iButton 5 is assigned to Partition 1 and 4, the user will be able to arm/disarm Partition 1 and 4 by touching iButton 5 to the reader. For more details on how to set iButton key partition, please refer to **23.5. iButton Key Partition**.

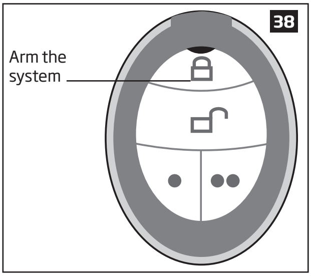
12.7. EWK1/EWK2 Wireless Keyfob

EWK1/ EWK2

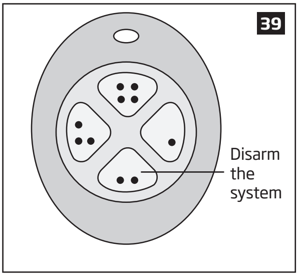
To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 – ⁘ ;EWK 2 - 🔒). When EWK1/ EWK2 button is pressed for arming, the system will proceed as follows:

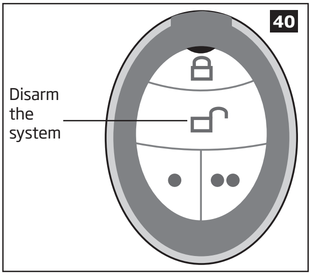
- **Non-partitioned/partitioned system:**
  - If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and arm them.
  - If unready, the system will not arm and provide a list of violated zones/tampers by SMS text message to user phone number. In such case the 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 Zone**s), disabled (see **14.9. Disabling and Enabling Zone**s) 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 3, the user will be able to arm/ disarm only Partition 3. To arm a different partition than the EWK1/EWK2 wireless keyfob is assigned to, bind another EWK1/EWK2 keyfob to the system and assign it to a different partition.
For more details on how to manage EWK1/EWK2 keyfob buttons, please refer to *ELDES Configuration Tool* software's HELP section.

12.8. 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/ EKB3W

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

Config Tool

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

Disable Arm-Disarm by Zone method

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

12.9. 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/EKB3W keypad and user password, iButton key, EWK1 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 as well as it may contain a user name assigned to user phone number, user password or iButton key. For more details on names, please refer to **8.1. User Phone Number Names**, **10.1. User Password Names** and **11.2. iButton Key Names**.

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... 10 → OK → SEND ARM/DARM SMS → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 75, user phone number slot & parameter status value:
75 us 0 #
Value: *us* – user phone number slot, range – [01... 10].
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... 10 → OK → SEND ARM/DARM SMS → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 75, user phone number slot & parameter status value:
75 us 1 #
Value: *us* - user phone number slot, range - [01... 10].
Example: *75091#*

Config Tool

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

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

Enable arm/disarm notification for all preset user phone numbers

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Disable arm/disarm notification for all preset user phone numbers

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

13. EXIT AND ENTRY DELAY

When arming, the system initiates the exit delay countdown (by default – 15 seconds) intended for the user to leave the secured area. The exit delay is indicated by short beeps emitted by EKB2/EKB3/EKB3W keypad buzzer and buzzer, connected to the alarm system. When arming:

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

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

- EKB2/EKB3/EKB3W keypad and user password.
- iButton key.
- EWK1/EWK2 wireless keyfob.
- Arm/Disarm by Zone.

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

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

Set exit delay

SMS

SMS text message content:
ssss_EXITDELAY:p,ext or ssss_EXITDELAY:p,ext;p,ext;p,ext;p,ext
Value: *ssss* – 4-digit SMS password; *p* – partition number, range – [1... 4], *ext* – exit delay duration, range – [0... 600] seconds.
Example: *1111_EXITDELAY:1,20;3,43*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → EXIT DELAY → OK → PARTITION 1... 4 → OK → ext → OK
Value: *aaaa* – 4-digit administrator password;, *ext* – exit delay duration, range – [0... 600] seconds.

EKB3/ EKB3W

Enter parameter 72, partition number & exit delay duration:
72 pp ext #
Value: *pp* – partition number, range – [01... 04], *ext* – exit delay duration, range – [0... 600] seconds.
Example: *7203259#*

Config Tool

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

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

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

Set entry delay for Delay zone

SMS

SMS text message content:
ssss_ENTRYDELAY:nn,eeeee or ssss_ENTRYDELAY:nn,eeeee;nn,eeeee;nn,eeeee;nn,eeeee
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76], *eeeee* – entry delay duration, range – [0... 65535] seconds.
Example: *1111_ENTRYDELAY:1,25;54,14;12,20*

EKB2

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

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → ENTRY DELAY → OK → eeeee → OK

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

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17... 32 → OK → EPGM1 ZONE 1... 32 → OK → ENTRY DELAY → OK → eeeee → OK

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

EKB3/ EKB3W

Enter parameter 54, partition number and entry delay duration:
54 nn eeeee #
Value: *nn* – zone number, range – [01... 76], *eeeee* – entry delay duration, range – [0... 65535] seconds
Example: *5403259#*

Config Tool

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

NOTE: Due to battery power saving reasons, EKB3W keypad buzzer will not sound during exit and entry delay if the violated Delay type zone is not of the associated EKB3W keypad.

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.

ESIM364 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**.

ESIM364 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 ESIM364 alarm system.	6/12*	6/12*
Keypad zones	Hardwired zones of EKB2/EKB3 keypad.	1	4
EPGM1 zones	Zones of EPGM1 - hardwired zone & PGM output expansion module.	16	32
Wireless zones	Non-physical zones automatically created by connected wireless devices.	2**	64***
Virtual zones	Non-physical zones intended for Panic button feature (alarm activaton upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using *ELDES Configuration Tool* software.	64****	64****

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

14.1. Zone Numbering

The zone numbers ranging from Z1 through Z12 are permanently reserved for on-board zones even when ATZ mode is disabled. The Z13-Z76 zone numbers are automatically assigned in the chronological order to the created virtual zones and the devices connected to the system: keypads, wireless devices, EPGM1 modules.

14.2. Zone Expansion

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

- enabling the ATZ (Advanced Technology zone) mode (see **14.4. ATZ (Advanced Technology Zone) Mode**).
- connecting EPGM1 hardwired zone and PGM output expansion module (see **32.1.3. EPGM1 – Hardwired Zone & PGM Output Expansion Module**).
- connecting keypads (see **32.1.1. EKB2 – LCD Keypad**, **32.1.2. EKB3 – LED Keypad** and **33.1. EKB3W – Wireless LED Keypad**).
- binding wireless devices (see **19. WIRELESS DEVICES**).
- creating virtual zones (see *ELDES Configuration Tool* software's Help section).

The maximum supported number of zones is 76.

14.3. 6-Zone Mode

By default, ESIM364 alarm system runs in the 6-Zone mode under zone connection Type 1 allowing to connect up to 6 detection devices of NO (normally-open) type to the on-board zone terminals as indicated in the wiring diagram of Type 1. Once a different zone connection type is set, the detection device wiring must be done according to the wiring diagram of the associated type. Available zone connection types for the 6-Zone mode:

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

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

Set zone connection type for 6-Zone mode

EKB2

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

EKB3/ EKB3W

Enter parameter 39 & 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.

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/ EKB3W

Enter parameter 28 & 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/ EKB3W

Enter parameter 28 & 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/ EKB3W

Enter parameter 38 & number of zone connection type:

381# – Type 4

382# – Type 5

Example: *381#*

Config Tool

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

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

14.5. Zone Type Definitions

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

Set zone type for individual zone

EKB2

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

Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → 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 → 1ST... 4TH KEYPAD 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 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → ENABLE → OK

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

EKB3/ EKB3W

Enter parameter 53, zone number & zone type number:

53nn1# – Interior Follower

53nn2# – Instant

53nn3# –24-Hour

53nn4# – Delay

53nn5# – Fire

53nn6# – Panic/Silent

Value: *nn* – zone number, range – [01... 76]

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**.
- **Shared** – This attribute determines whether a zone, assigned to multiple partitions, will cause an alarm or not in the associated armed partition if violated. If a zone with the Shared attribute enabled is violated when at least one of the associated partitions is disarmed, the alarm will not be caused. Once the system is armed in all of the associated partitions, the zone with Shared attribute enabled will operate according to the determined type. Typically, this attribute is used for shared areas, such as corridors.
- **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.

NOTE: Due to battery power saving reasons, EKB3W wireless keypad buzzer will not sound if the Bell attribute is not enabled and the violated Delay type zone is not of the associated EKB3W wireless keypad. For more details on EKB3W wireless keypad, please refer to **33.2.1. EKB3W - Wireless LED Keypad.**

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 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → ENABLE → OK

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

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → ENABLE → OK

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

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 1 #
Value: *nn* – zone number, range – [01... 76].
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 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STAY → OK → DISABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STAY → OK → DISABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → DISABLE → OK

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

EKB3/ EKB3W

Enter parameter 56, zone number & parameter status value:
56 nn 0 #

Value: *nn* – zone number, range – [01... 76].
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 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → ENABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → ENABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → FORCE → OK → ENABLE → OK

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

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 1 #

Value: *nn* – zone number, range – [01... 76].
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 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → FORCE → OK → DISABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → FORCE → OK → DISABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STAY → OK → DISABLE → OK

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

EKB3/ EKB3W

Enter parameter 82, zone number & parameter status value:
82 nn 0 #

Value: *nn* – zone number, range – [01... 76].
Example: *82110#*

Config Tool

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

Enable/disable Shared attribute for individual zone

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

Set Delay, ms atrribute

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

Enable/disable Delay becomes Instant in Stay mode attribute

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

Disable Chime attribute

EKB2

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

EKB3/ EKB3W

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

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

Enable Chime attribute

EKB2

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

EKB3/ EKB3W

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

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

14.7. Bypassing and Activating Zones

ATTENTION: Zone bypassing and activation must be carried out without Configuration mode being activated by the EKB3/EKB3W keypad.

Zone bypassing allows the user to deactivate a violated zone and arm the system without restoring the zone. If a bypassed zone is violated or restored during exit/entry delay, or when then system is armed, it will be ignored. When a zone is bypassed, EKB3/EKB3W keypad indicator **BYPS** will light ON and EKB2 keypad will display **BYP** message in the home screen view.

Bypass individual violated zone

EKB2

Menu path:
OK → BYPASS → OK → BYPASS LIST 1... 5 → OK → Z1-zone-name... Z76-zone-name → OK → BYPASS → OK
Value: *zone-name* - up to 24 characters zone name.

EKB3/ EKB3W

Press the [BYPS] key, enter zone number & user password:
BYPS nn uuuu #
Value: *nn* - zone number, range - [01... 76]; *uuuu* - 4-digit user password.
Example: *BYPS091111#*

Bypass all violated zones

EKB2

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

The zone will stay bypassed until the system is disarmed. Once the system is disarmed, the corresponding zone state will be indicated on the keypads (see **32.1.1. EKB2 - LCD Keypad**, **32.1.2. EKB3 - LED Keypad** and **33.1. EKB3W - Wireless 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... 5 → OK → Z1-zone-name... Z76-zone-name → OK → UNBYPASS → OK
Value: *zone-name* - up to 24 characters zone name.

EKB3/ EKB3W

Press the [BYPS[key, enter zone number & user password:
BYPS nn uuuu #
Value: *nn* – zone number, range – [01... 76]; *uuuu* – 4-digit user password.
Example: *BYPS251111#*

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

14.8. Zone Names

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

Set zone name

SMS

SMS text message content:
ssss_Znn:zone-name
Value: *ssss* – 4-digit SMS password; *nn* – zone number, range – [1... 76]; *zone-name* – up to 24 characters zone name.
Example: *1111_Z3:Door sensor triggered*

Config Tool

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

View zone names

SMS

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

EKB2

EKB2:
Menu path:
On-board zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → ONBOARD ZONES → OK → ZONE 1... 12 → OK → NAME
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → NAME
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → NAME
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → 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... 76].
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 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → DISABLE → OK

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

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → DISABLE → OK

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

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 0 #
Value: *nn* – zone number, range – [01... 76].
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... 76].
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 → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → STATUS → OK → ENABLE → OK

Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → STATUS → ENABLE → OK

EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → STATUS → ENABLE → OK

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

EKB3/ EKB3W

Enter parameter 52, zone number & parameter status value:
52 nn 1 #
Value: *nn* – zone number, range – [01... 76].
Example: *52151#*

Config Tool

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

15. STAY MODE

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

The system can be Stay armed under the following conditions:

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

Arm the system in Stay mode

EKB2

Menu path:
Non-partitioned system: P2 → uuuu → OK
Partitioned system: P2 → uuuu → OK → [p] part-name → OK
Value: *uuuu* – 4-digit user password; *p* – partition number, range – [1... 4]; *part-name* – up to 15 characters partition name.

EKB3/ EKB3W

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

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

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

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

NOTE: Stay mode is not supported by virtual zones.

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

16. TAMPERS

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

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

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

Disable tamper alarm notification

EKB2

Menu path:
Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → DISABLE → OK
Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, event number & parameter status value:
25 13 0 # - Tamper alarm
25 18 0 # - Wireless signal loss
Example: *25180#*

Config Tool

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

Enable tamper alarm notification

EKB2

Menu path:
Tamper alarm: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → TAMPER ALARM → OK → ENABLE → OK
Wireless signal loss: OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → WLESS SIGN LOSS EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, event number & parameter status value:
25 13 1 # - Tamper alarm
25 18 1 # - Wireless signal loss
Example: *25131#*

Config Tool

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

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

16.1. Tamper Names

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

Manage tamper name

Config Tool

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

17. ALARM INDICATIONS AND NOTIFICATIONS

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

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

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

b) The keypad buzzer will emit short beeps.

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

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

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

e) If one or more zones are violated, EKB3/EKB3W will light ON the corresponding violated zone indicator (-s) ranging from 1 through 12. Indicator SYSTEM will flash if one or more high-numbered zones are violated. If one or tampers are violated, indicator SYSTEM will light ON. For more details on viewing violated high-numbered zone and tamper numbers by EKB3/EKB3W keypad, please refer to **29. INDICATION OF SYSTEM FAULTS**.
For more details on how EKB3W keypad operates and indicates the alarms, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout**

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

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

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

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

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

a) When the call is answered, the system will shut down the siren/bell and play the audio file that can be listened to on the user's mobile phone. This feature will be available only if an audio file is recorded and assigned to the violated zone (see **17.2. Audio Files**).

b) When the audio record has played, 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**).

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

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

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

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

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

View violated zones

SMS

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

EKB2

Menu path:
OK → VIOLATED ZONES → OK → ZONE 1... 76

EKB3/ EKB3W

Please, refer to illuminated zone indicators ranging from 1 through 12 on the keypad. The flashing indicator SYSTEM stands for violated high-numbered zones (Z13-Z76). For more details on violated high-numbered zone indication, please refer to **29. INDICATION OF SYSTEM FAULTS.**

Config Tool

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

View violated tampers

SMS

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

EKB2

Menu path:
OK → VIOLATED TAMPERS → OK → TAMPER 1... 76

EKB3/ EKB3W

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

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

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

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

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

17.1. Enabling and Disabling Alarm Notifications

By, default the system will not ring the preset user phone numbers in case of alarm. To enable/disable this feature, please refer to the following configuration methods.

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/ EKB3W

Enter parameter 30 & parameter status value:
30 0 #

Example: *300#*

Config Tool

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

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/ EKB3W

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

Config Tool

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

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

Disable SMS text message in case of alarm

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → GENERAL ALARM → OK → DISABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, event number & parameter status value:
25 03 0 #
Example: *25030#*

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 1 → OK → GENERAL ALARM → OK → ENABLE → OK
Value: *aaaa* - 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, event number & parameter status value:
25 03 1 #
Example: *25031#*

Config Tool

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

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

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

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

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

SMS

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

EKB2

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

EKB3/ EKB3W

Enter parameter 21 & parameter status value:
21 0 #
Example: *210#*

Config Tool

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

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

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

17.2. Audio Files

The system comes equipped with a feature allowing to record up to 16 audio files of up to 6 seconds length using the microphone of the PC. The recorded file can be assigned to any system zone, except virtual zone, and be played when the alarm is caused by zone with an audio file assigned. This feature will be available only if the system is able to dial user phone number in the event of an alarm and the user answers the call. The supported audio file format is as follows:

- Max. number of audio files: up to 16
- Max. audio length: up to 6 seconds
- File format: .wav
- Specifications: 8,000 kHz; 8 Bit; Mono

Record and manage audio files

Config Tool

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

Assign audio file to individual zone

Config Tool

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

NOTE: Single audio file can be assigned to multiple zones.

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.

ESIM364 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**.

ESIM364 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 ESIM364 alarm system.	4	4
EPGM8 PGM Outputs	PGM outputs of EPGM8 - hardwired PGM output expansion module.	8	8
EPGM1 PGM Outputs	PGM outputs of EPGM1 - hardwired zone & PGM output expansion module.	2	4
Wireless PGM Outputs	Non-physical PGM outputs automatically created by connected wireless devices.	2*	64**

* - 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-C76 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 32.3.1. EPGM8 - Hardwired PGM Output Expansion Module**)
- connecting EPGM1 hardwired zone and PGM output expansion module (see **32.1.3. EPGM1 - Hardwired Zone & PGM Output Expansion Module**).
- binding the wireless devices (see **19. WIRELESS DEVICES**).

The maximum supported PGM output number is 76.

18.2.1. EPGM8 Mode

EPGM8 is an expansion module, which expands the system with 8 additional hardwired PGM outputs. For more details on EPGM8 module installation, please refer to **32.3.1. 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/ EKB3W

Enter parameter 33 & 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 EPGM8 mode

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

18.3. PGM Output Names

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

Set PGM output name

SMS

SMS text message content:
ssss_Coo:out-name
Value: *ssss* – 4-digit SMS password; *oo* – PGM output number, range – [1... 76]; *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
Wireless PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → NAME
Value: *aaaa* – 4-digit administrator password.

Config Tool

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

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

18.4. Turning PGM Outputs ON and OFF

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

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

SMS

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

EKB2

Menu path:
On-board PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → ENABLED → OK
Wireless PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → STATUS → OK → ENABLED → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

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

SMS

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

EKB2

Menu path:
On-board PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → ONBOARD OUTPUTS → OK → OUTPUT 1... 12 → OK → STATUS → OK → DISABLED → OK
Wireless PGM output: OK → CONFIGURATION → OK → aaaa → OK → PGM OUTPUTS → OK → WIRELESS OUTPUTS 1... 4 → OK → OUTPUT 13... 76 → OK → STATUS → OK → DISABLED → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

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

Turn ON PGM output for time period

SMS

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

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

Turn OFF PGM output for time period

SMS

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

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

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

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

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

18.5. PGM Output Control by Event and Scheduler

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

PGM Output Actions

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

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

System Events

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

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

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

Schedulers

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

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

Additional Conditions

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

- **System armed** – System is armed in a determined partition ranging from 1 to 4 or any partition.

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

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

Manage PGM output control by event & scheduler

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

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

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

18.6. Wireless PGM Output Type Definitions

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

Set output type for individual wireless PGM output

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

19. WIRELESS DEVICES

ESIM364 system has a built-in wireless module for system extension capabilities. The wireless module easily allows the user to bind up to 32 ELDES-made wireless devices to the system. This includes the following:

- EWP1 – wireless PIR sensor (motion detector).
- EWD1 – wireless magnetic door contact.
- EWD2 - magnetic door contact/shock sensor
- EWS1 and EWS2 – wireless indoor and outdoor sirens.
- EWK1 and EWK2 – wireless keyfobs.
- EKB3W – wireless keypad.
- EW1 – wireless zone and PGM output expansion module.
- EW1B – wireless battery-powered zone and PGM output expansion module.
- EWF1 - wireless smoke detector.

The wireless devices can operate at a range of up to 30 meters from the alarm system unit while inside the building and at up to 150 meters range in open areas. The wireless connection is two-way and operates in one of four available channels at 868 Mhz (EU version) / 915 Mhz (US version) non-licensed frequency range. The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period, identified as Test Time.

For more details on how to install the wireless devices, please refer to **33. ELDES WIRELESS DEVICES** and **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual located at www.eldes.lt/download

19.1. Binding, Removing and Replacing Wireless Devicess

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

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

Once the wireless device is bound, it will attempt to exchange data with ESIM364 system. Due to battery saving reasons, all ELDES wireless devices operate in sleep mode. The data exchange will occur instantly if the wireless device is triggered (zone alarm or tamper alarm) or periodically when the wireless device wakes up to transmit the supervision signal, identified as Test Time, to the system as well as to accept the queued up command (if any) from the system. **Example:** *The alarm occurred at 09:15:25 and the system queued up the command for EWS2 siren to start sounding. By default, Test Time value of EWS2 siren is 7 seconds, therefore EWS2 siren will sound at 09:15:32.*

By default, the Test Time period is as follows:

- EKB3W, EWD1: every 60 seconds.
- EW1, EWP1, EWF1, EWD2: every 30 seconds.
- EW1B: every 20 seconds.
- EWS1, EWS2: 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.

NOTE FOR EKB3W USERS: In comparison with other ELDES wireless devices, EKB3W keypad features some exceptions regarding the wireless communication. For more details on EKB3W keypad wireless communication and back-light timeout, please refer to **33.1.7. Wireless Communication, Sleep Mode and Back-light Timeout.**

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

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

Bind wireless device to the system

SMS

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

Config Tool

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

NOTE FOR EWK1/EWK2/EKB3W USERS: When binding EWK1/EWK2 wireless keyfob or EKB3W wireless keypad, it is necessary to press several times any button/key on the device.

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

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

Remove wireless device from the system

SMS

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

Config Tool

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

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

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

Replace wireless device

SMS

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

Config Tool

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

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

NOTE: If you are unable to bind 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 www.eldes.lt/en/download to download the latest user manual

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

19.2. Wireless Device Information and Signal Status Monitoring

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

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

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

View wireless device information

SMS

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

EKB2

Menu path:
Battery level: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → BATTERY
Wireless signal: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → SIGNAL
Error rate: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → ERROR RATE
Firmware version: OK → CONFIGURATION → OK → aaaa → OK → WIRELESS DEVICES 1... 2→ OK → wless-dev wless-id → OK → FW RELEASE
Value: *aaaa* – 4-digit administrator password; *wless-dev* – wireless device model; *wless-id* – 8-digit wireless device ID code.

Config Tool

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

The system supports up to 32 wireless devices. To view the number of unoccupied wireless device slots in the system, please refer to the following configuration methods

View unoccupied wireless device slots

SMS

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

Config Tool

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

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

19.3. Disabling and Enabling Siren if Wireless Signal is Lost

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

Enable Siren if Wireless Signal is Lost

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Disable Siren if Wireless Signal is Lost

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

20. SIREN/BELL

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

Set alarm duration

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

View alarm duration

SMS

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

EKB2

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

Config Tool

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

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

NOTE: 0 value disables the siren/bell.

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

20.1. BELL Output Status Monitoring

The system constantly supervises the BELL output. If the siren/bell is disconnected/cut-off, the system will instantly send the notification by SMS text message to User 1 and indicate system fault condition on the keypad (see **29. INDICATION OF SYSTEM FAULTS**). Once the bell/siren is connected/fixed, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, the notification by SMS text message regarding the BELL output status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable Siren Fail/ Restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & 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.

Disable Siren Fail/ Restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → SIREN FAIL/REST EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & 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.

20.2. 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 SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 29 & 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 SETT INGS → OK → SIREN SETTINGS → OK → BELL SQUAWK → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 29 & parameter statusvalue:
29 0 #
Example: *290#*

Config Tool

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

20.3. Indication by EWS2 Indicators

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

Enable EWS2 LED indication

EKB2

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

EKB3/ EKB3W

Enter parameter 29 & 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 SETT INGS → OK → SIREN SETTINGS → OK → EWS2 LED → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

20.4. EWF1 Interconnection

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

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

Disable interconnection

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Enable interconnection

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Set EWF1 siren alarm duration

Config Tool

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

For more details on EWF1 wireless smoke detector, please refer to **33.9. EWF1 - Wireless Smoke Detector**

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

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

- battery has failed and requires replacement – battery resistance is 2Ω or higher; self-tested every 24 hours.
- battery is dead or missing – battery is not present or battery voltage is below 5V; self-tested every 1 minute.
- 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 1 → OK → BATTERY FAILED → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

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 1 → OK → BATTERY FAILED → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

Disable Battery Dead or Missing notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

Enable Battery Dead or Missing notification

EKB2

OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → BATTERY DEAD/MISS → OK → ENABLE → OK
Value: aaaa – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 06 1 #
Example: *25061#*

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 1 → OK → LOW BATTERY EVENT → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 07 0 #
Example: *25070#*

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 1 → OK → LOW BATTERY EVENT → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 07 1 #
Example: *25071#*

Config Tool

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

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

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

Disable mains power supply loss/restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

Enable mains power supply loss/restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 1 → OK → MAIN POWER L/R EV → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

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

Config Tool

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

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

Set mains power supply loss delay

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Set mains power supply restore delay

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETT INGS → OK → MAIN POWER STATUS → OK → RESTORE DELAY → OK → rrrrr → OK

Value: *aaaa* – 4-digit administrator password; *rrrrr* – mains power restore delay duration, range - [0... 65535] seconds.

EKB3/ EKB3W

Enter parameter 71 & restore delay duration:
71 rrrrr #

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

Config Tool

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

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

22. GSM CONNECTION AND ANTENNA STATUS MONITORING

The system constantly supervises the GSM connection. When the GSM signal is lost, the system indicator NETW will light OFF, the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) and the system will turn ON a determined PGM output if the GSM signal is lost for a longer time period than the set delay value (By default – 180 seconds). Once the GSM signal restores, the system will notify User 1 by SMS text message, the keypad will no longer indicate system fault and the determined PGM output will turn OFF.

By default, the notifications by SMS text message regarding GSM signal loss is disabled. To enable/disable thus notification, please refer to the following configuration methods.

Enable GSM Connection Failed notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 11 1 #
Example: *25111#*

Config Tool

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

Disable GSM Connection Failed notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → GSM CONNECT FAILED → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 11 0 #
Example: *25110#*

Config Tool

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

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.

The system constantly monitors the GSM/GPRS antenna status. If the GSM/GPRS antenna is disconnected/cut-off, the system will send notification by SMS text message to User 1 and the keypad will indicate system fault condition (see **29. INDICATION OF SYSTEM FAULTS**) . Once the antenna is connected/fixed, the system will notify User 1 by SMS text message and the keypad will no longer indicate system fault.

By default, the notification by SMS text message regarding the GSM/GPRS antenna status is disabled. To enable/disable this notification, please refer to the following configuration methods.

Enable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → ENABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 12 1 #
Example: *25121#*

Config Tool

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

Disable GSM/GPRS Antenna Fail/Restore notification

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → SMS MESSAGES 2 → OK → GSM ANT FAIL/REST → OK → DISABLE → OK
Value: *aaaa* – 4-digit administrator password.

EKB3/ EKB3W

Enter parameter 25, notification number & parameter status value:
25 12 0 #
Example: *25120#*

Config Tool

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

23. PARTITIONS

ESIM364 system comes equipped with a partitioning feature that can divide the alarm system into four independently controlled areas identified as Partition 1 through 4, which are all supervised by one alarm system unit. Partitioning can be used in installations where shared alarm system is more practical, such as a house and a garage or within a single multi-storey building. When partitioned, each system element, like zone, user phone number, keypad, user password, iButton key and wireless keyfob can be assigned to single or multiple partitions. The user will then be able to arm/disarm the system partition (-s) that the zones and arm/disarm method, except EKB2 keypad, are assigned to.

The following table reflects the values used for system element assignment to partitions by EKB2/EKB3/EKB3W keypad. A sum of values is used to assign the element to multiple partitions.

Partition	Value
Partition 1	1
Partition 2	2
Partition 3	4
Partition 4	8

Example1: The user wants to assign a certain iButton key to Partition 4 only. According to the table value 8 reflects Partition 4. He would then have to enter value 8.

Example2: The user wants to assign a certain user password to Partition 2 and 3. According to the table value 2 reflects Partition 2, while value 4 reflects Partition 3, therefore 2 + 4 = 6. He would then have to enter value 6.

Example3: The user wants to assign a certain zone to Partition 1, 3 and 4. According to the table value 1 reflects Partition 1, while values 4 and 8 reflect Partitions 3 and 4 respectively, therefore 1 + 4 + 8 = 13. He would then have to enter value 13.

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 → pv → OK
Wireless zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → WIRELESS ZONES 1... 4 → OK → WIRELESS ZONE 13... 76 → OK → PARTITION → OK → pv → OK
Keypad zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → KEYPAD ZONES → OK → 1ST... 4TH KEYPAD ZONE → OK → PARTITION → OK → pv → OK
EPGM1 zone: OK → CONFIGURATION → OK → aaaa → OK → ZONES → OK → EPGM1 ZONES 1-16... EPGM1 ZONES 17-32 → OK → EPGM1 ZONE 1... 32 → OK → PARTITION → OK → pv → OK
Value: *aaaa* – 4-digit administrator password; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 57, zone number & partition value:
57 nn pv #
Value: *nn* – zone number, range – [01... 76]; *pv* – partition value (see **23. PARTITIONS**).
Example: *57032#*

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 or sending an SMS text message.

Set user phone number partition

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → CALL/SMS SETTINGS → OK → USERS → OK → USER 1... 10 → OK → PARTITION → pv → OK
Value: *aaaa* – 4-digit administrator password; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 59, user phone number slot & partition value:
59 us pv #
Value: *us* – user phone number slot, range – [01... 10]; *pv* – partition value (see **23. PARTITIONS**).
Example: *591013#*

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 – PART1) indicated in home screen view.
- EKB3W – Refer to the location of the illuminated indicator READY on the keypad. The indicator will be illuminated under section A or B, which represent Partition 1 and Partition 2 respectively.

The keypad must be assigned to the same partition as the user password (see **23.4. User Password Partition**) in order to arm/disarm the system by the keypad. For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User Password, 12.4. EKB3 Keypad and User Password** and **12.5. EKB3W Keypad and User Password.**

Set keypad partition

EKB2

Menu path:
EKB2 partition: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → [k] EKB2 → OK → PARTITION 1... 4 → OK
EKB3 partition: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → KEYPAD PARTITION → OK → [k] EKB3→ OK → PARTITION 1... 4 → OK
EKB3W partition: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → KEYPAD PARTITION → OK → EKB3W PARTITION → OK → EKB3W wless-id → OK → PARTITION 1... 2 → OK
Value: *aaaa* – 4-digit administrator password; *k* – keypad slot, range – [1... 4]; *wless-id* – 8-digit wireless device ID code.

EKB3/ EKB3W

Enter parameter 51, keypad slot & partition number:
EKB2/EKB3 partition: 51 kk p #
EKB3W partition: 51 kw r #
Value: *kk* – EKB2/EKB3 keypad slot, range – [01... 04]; *kw* – EB3W keypad slot, range – [05... 08]; *p* – EKB2/EKB3 partition number, range – [1... 4]; *r* – EKB3W partition number, range – [1... 2].
Example: *51062#*

Config Tool

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

NOTE: The keypad can only be assigned to one partition.

NOTE: EKB3W keypad assignment is restricted to Partition 1 and Partition 2.

NOTE: The slots for EKB3W keypads are automatically assigned to the bound keypad in the chronological order, hence the earliest bound keypad would acquire slot 5, while the latest bound keypad would acquire slot 8.

Keypad partition switch allows to quickly change the keypad partition. When the keypad partition is changed and when 1 minute after the last key-stroke/key-touch expires, the system will return to the preset keypad partition. Typically, this feature is used for viewing arm/disarm status and alarms of a different partition or when arming/disarming a different system partition by EKB3/EKB3W 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/ EKB3W

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

Config Tool

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

Disable keypad partition switch

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

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

23.4. User Password Partition

User password partition determines which system partition (-s) can be armed/disarm using a certain user password. User password must be assigned to the same partition as the keypad (see **23.3. Keypad Partition and Keypad Partition Switch**) in order to arm/disarm the system by EKB2/EKB3/EKB3W keypad . For more details on system arming/disarming by the keypad, please refer to **12.3. EKB2 Keypad and User Password, 12.4. EKB3 Keypad and User Password** and **12.5. EKB3W Keypad and User Password.**

Set user password partition

EKB2

Menu path:
User password 1... 16: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK→ USER PSW (1-16) → OK → USER PASSWORD 1... 16 → OK → PARTITION → OK → pv → OK
User password 17... 30: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → PASSWORDS → OK → USER PASSWORDS → OK→ USER PSW (17-30) → OK → USER PASSWORD 17... 30 → OK → PARTITION → OK → pv → OK
Value: *aaaa* – 4-digit administrator password; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 87, user password & partition value:
87 uuuu pv #
Value: *uuuu* – 4-digit user password; *pv* – partition value (see **23. PARTITIONS**).
Example: *8711118#*

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 (-s) 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... 16 → OK → PARTITION → OK → pv → OK
Value: *aaaa* – 4-digit administrator password; *pv* – partition value (see **23. PARTITIONS**).

EKB3/ EKB3W

Enter parameter 60, iButton key slot & partition value:
60 ii pv #
Value: *ii* – iButton key slot, range – [01... 16]; *pv* – partition value (see **23. PARTITIONS**).
Example: *600511#*

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.

NOTE: EWK1/EWK2 wireless keyfob can only be assigned to one partition.

24. TEMPERATURE SENSORS

The system may be equipped with up to 8 temperature sensors intended for temperature measurement in the surrounding areas. This feature allows to monitor the temperature of up to 8 different areas in real-time and receive a notification by SMS text message to User 1 phone number when the set temperature boundaries are exceeded.

24.1. Adding, Removing and Replacing Temperature Sensors

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

a) Shutdown the system.

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

c) If more than one temperature sensor is required, wire another sensor in parallel to the previous one.

d) By default, the first added temperature sensor will be identified as primary and the second one – as secondary temperature sensor (see **24.2. Primary and Secondary Temperature Sensors**).

e) Add as many temperature sensors as necessary – wire up one after another in parallel – until the number of 8 sensors is reached.

f) Power up the system.

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

View real-time temperature values of individual temperature sensor

SMS

SMS text message content:
ssss_ITEMP:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_ITEMP:4*

EKB2

Menu path:
OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *tm.p* – real-time temperature value.

Config Tool

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

View real-time temperature values of all temperature sensors

SMS

SMS text message content:
ssss_ITEMP:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_ITEMP:?*

EKB2

Menu path:
OK → TEMP SENSORS INFO → OK → 1. tm.p C (PRIM) | (SEC)... 8. tm.p C
Value: *tm.p* – real-time temperature value.

Config Tool

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

If a temperature sensor is faulty, it is recommended to remove it or replace it by a functional sensor.

Remove/replace individual temperature sensor

Config Tool

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

NOTE: When multiple temperature sensors are connected, please touch and hold the sensor with your fingers and watch the temperature value change to identify the number of the temperature sensor slot.

24.2. Primary and Secondary Temperature Sensors

By default, the first added temperature sensor is automatically set as primary, while the second one is set as secondary temperature sensor. The real-time temperature values of the primary and secondary temperature sensors are included in the Info SMS text message (see **26. SYSTEM INFORMATION. INFO SMS**) as well as the temperature measured by the primary temperature sensor is indicated in the home screen view of EKB2 keypad.

To set a different temperature sensor as primary or secondary, please refer to the following configuration methods.

Set primary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:PRIM:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:PRIM:4*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → PRIMARY TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *aaaa* – 4-digit administrator password

EKB3/EKB3W

Enter parameter 89 & temperature sensor slot:
89 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *8903#*

Config Tool

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

Set secondary temperature sensor

SMS

SMS text message content:
ssss_TEMPI:SEC:ts
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range - [1... 8].
Example: *1111_TEMPI:SEC:3*

EKB2

Menu path:
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → SECOND. TEMP SENS → OK → 1... 8 CONNECTED → OK
Value: *aaaa* – 4-digit administrator password

EKB3/EKB3W

Enter parameter 90 & temperature sensor slot:
90 ts #
Value: *ts* – temperature sensor slot, range - [01... 08].
Example: *9005#*

Config Tool

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

To view the slot number of primary and secondary temperature sensors, please refer to the following configuration methods.

View primary and secondary temperature sensor slot number

SMS

SMS text message content:
ssss_TEMPI:?
Value: *ssss* – 4-digit SMS password.
Example: *1111_TEMPI:?*

EKB2

Menu path:
Primary: OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: *tm.p* – real-time temperature value.

Config Tool

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

View primary and secondary temperature sensor real-time temperature values

SMS

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

EKB2

Menu path:
Primary: OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (PRIM)
Secondary: OK → TEMP SENSORS INFO → OK → 1... 8 tm.p C (SEC)
Value: *tm.p* – real-time temperature value.

Config Tool

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

NOTE: Primary and secondary temperature sensors can be set by a single SMS text message, **Example:** *1111_TEMPI:PRIM:4,SEC:3*

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

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

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

Set MIN and MAX temperature boundaries

SMS

SMS text message content:
ssss_TEMPts:MIN:mnn,MAX:mxx
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C.
Example: *1111_TEMP2:MIN:-5,MAX:28*

EKB2

Menu path:
MIN: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN → OK → mnn → OK
MAX: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MAX → OK → mxx → OK
Value: *aaaa* – 4-digit administrator password; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C.
Keys P1 or P2 are used to enter minus character, e.g. -20.

EKB3/ EKB3W

Enter parameter 19 & temperature Value:
19 ts mnn mxx #
Value: *ts* - temperature sensor slot, range – [1... 8]; *mnn* – MIN boundary, range – [-55... 125] C; *mxx* - MAX boundary, range – [-55... 125] C. 00 value stands for minus character, e. g. 0020 = -20
Example: *1906001530#*

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_TEMPts
Value: *ssss* – 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP4*

EKB2

Menu path:
MIN: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → OK → TEMP. MIN
MAX: OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → 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.

NOTE: MIN and MAX boundaries can also be set separately by multiple SMS text messages, **Example:** *1111_TEMP1:MIN:6 and 1111_TEMP1:MAX:40*

24.4. Temperature Sensor Names

The temperature sensor name is included in the Temperature Info SMS when delivered to the User 1 phone number. This feature allows easier identification of the temperature sensor and normally it is used when monitoring temperature changes in different areas.

Set temperature sensor name

SMS — **SMS text message content:**
ssss_TEMPts:NAME:temp-sens-name
Value: *ssss* – 4-digit SMS password; *ts* – temperature sensor slot, range – [1... 8]; *temp-sens-name* – 4 to 24 characters temperature sensor name.
Example: *1111_TEMP3:NAME:Warehouse*

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

View temperature sensor name

SMS — **SMS text message content:**
ssss_TEMPts
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP3*

EKB2 — **Menu path:**
OK → CONFIGURATION → OK → aaaa → OK → PRIMARY SETTINGS → OK → TEMP SENSORS → OK → TEMPERATURE SENS 1... 8 → 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.

Delete temperature sensor name

SMS — **SMS text message content:**
ssss_TEMPts:NAME:
Value: *ssss* - 4-digit SMS password; *ts* - temperature sensor slot, range – [1... 8].
Example: *1111_TEMP2:NAME:*

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

ESIM364 comes equipped with a microphone that allows the user to listen on his mobile phone to what is happening in the secured area. By installing one of the audio modules EA1 or EA2, the user will be able to have a 2-way voice communication (see **32.3.2. EA1 - Audio Output Module** and **32.3.3. EA2 - Audio Output Module with Amplifier**). Remote listening and 2-way voice communication can operate under the following conditions:

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

Initiate remote listening

SMS

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

Set microphone gain

EKB2

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

Config Tool

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

Set speaker level

EKB2

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

Config Tool

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

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

26. SYSTEM INFORMATION. INFO SMS

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

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

Request for system information

SMS

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

Config Tool

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

26.1. Periodic Info SMS

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

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

Set periodic Info SMS frequency and time

SMS

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

EKB2

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

EKB3/ EKB3W

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

Config Tool

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

Disable periodic Info SMS

SMS

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

EKB2

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