ESIM384

GSM ALARM AND MANAGEMENT SYSTEM

USER MANUAL

EN

User Manual v1.1

Safety instructions

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

- GSM alarm and management system ESIM384 (also referenced as "alarm system", "system" or "device") has radio transceiver operating in GSM EU band 900/1800MHz or GSM quad band 850/900/1800/1900MHz.
- 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.

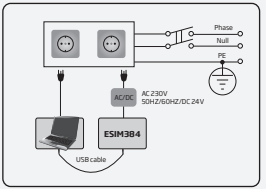
GSM alarm system ESIM384 is a device mounted in limited access areas. Any system repairs must be done only by qualified, safety aware personnel.

The system must be powered by main 16-24V 50/60 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 ESIM384 (computer, sensors, relays etc.) must be approved by LST EN 60950-1 standard.

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.

External power supply can be connected to AC mains only inside installation room with automatic 2-pole circuit breaker capable of disconnecting circuit in the event of short circuit or over-current condition. Open circuit breaker must have a gap between connections of more than 3mm (0.12in) and the disconnection current 5A.



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

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

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

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

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

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

Terms of use

The following terms and conditions govern use of the ESIM384 device and contains important information on limitations regarding the product's use and function, as well as information on the limitations of the manufacturer's liability. Please carefully read these terms and conditions. For more information on your product, please visit www.eldesalarms.com

Technical support

In order to ensure continuous and proper operation of the ESIM384 device and uninterrupted service, it is the responsibility of the User to make sure that: (I) the product is properly installed, and (II) there is constant electrical supply. If you experience difficulty during the installation or subsequent use of the system, you may contact "ELDES, UAB" distributor or dealer in your country/region. For more information see www.eldesalarms.com

Warranty procedures

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

Manufacturer Warranty

"ELDES, UAB" provides a limited warranty for its products only to the person or entity that originally purchased the product from "ELDES, UAB" or its authorized distributor or retailer and materials under normal use of the system for a period of twenty four (24) months from the date of shipment by the "ELDES, UAB" (Warranty Period). Warranty obligations do not cover expandable materials (power elements and/or batteries), holders and enclosures. The warranty remains valid only if the system is used as intended, following all guidelines outlined in this manual and in accordance with the operating conditions specified. The warranty is void if the system has been exposed to mechanical impact, chemicals, high humidity, fluids, corrosive and hazardous environments or force majeure factors. If a hardware defect arises and a valid claim is received within the Warranty Period, at its own discretion, "ELDES, UAB" will either (a) repair a hardware defect at no charge, using new or refurbished replacement parts, or (b) exchange the product with a product that is new or which has been manufactured from new or serviceable used parts and is at least functionally equivalent to the original product, or (c) refund the purchase price of the product.

Limited Liability

The buyer must agree that the system will reduce the risk theft, burglary or other dangers but does not provide guarantee against such events. "ELDES, UAB" will not assume any responsibility regarding personal or property, or revenue loss while using the system. "ELDES, UAB" shall also assume no liability due to direct or indirect damage or loss, as well as unreceived income when using the system, including cases, when the damages arise due to the above mentioned risks, when due to breakdown or malfunction the user is not informed in a timely manner about a risk which has arisen. In any case, the liability of "ELDES, UAB", as much as it is allowed by the laws in force, shall not exceed the price of acquisition of the product.

CONSUMER PROTECTION LAWS

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

About User Manual

This document describes basic configuration and usage of alarm system ESIM384. It is very important to read the user manual before starting to use the system.

Contents of Pack

Item	Quantity	Item	Quantity
1. ESIM384	1	5. Resistors 5,6kΩ	16
2. SMA antenna	2	6. Resistors 3,3kΩ	8
3. Back-up battery connection wire	1	7. Plastic standoffs	4
3. User manual	1		

* These following components are optional (sold separately) and are not included in device's contents of pack:
Buzzer;
Microphone.

! For complete system configuration and control, please refer to installation manual at www.eldesalarms.com

Contents

1. GENERAL INFORMATION

ESIM384 is an alarm system for private houses, cottages, village houses, garages, warehouses and other buildings, also capable of turning on/off the electrical appliances by SMS text message and alarm system keypads/touchpad. This alarm system provides a simple thus effective way of use.

The system may consist of:

- ESIM384 alarm system device.
- Up to 4 EKB2/EKB3 wired keypads.
- Up to 4 EKB3W/EWKB4 wireless keypads.
- Up to 4 EWKB5 wireless touchpads.
- Wired and/or wireless detection devices: movement sensors, magnetic door contacts, smoke sensors etc.
- Other devices: indoor/outdoor sirens, zone/PGM output expansion modules, heating, lighting, gates etc.

1.1. Short Description of Main Definitions

The following table provides the explanation of main definitions which are met in this user manual.

Definition	Description
System; alarm system	ESIM384 device
SMS	Short Message Service text
Keypad	Device with a set keys allowing to configure and control the system, view violated zones/tampers and system faults
EKB2	Model of wired LCD keypad
EKB3	Model of wired LED keypad
EKB3W	Model of wireless LED keypad
EWKB4	Model of wireless LED keypad
EWKB5	Wireless touchpad
EWM1	Wireless power socket
EWK2	Model of wireless keyfob
User phone number; User 1... 10	Phone number of the user allowed to arm/disarm the system control the electrical appliance by SMS text message as well as to receive notifications by SMS text messages from the system
System phone number	Phone number of the SIM card inserted in ESIM384 device

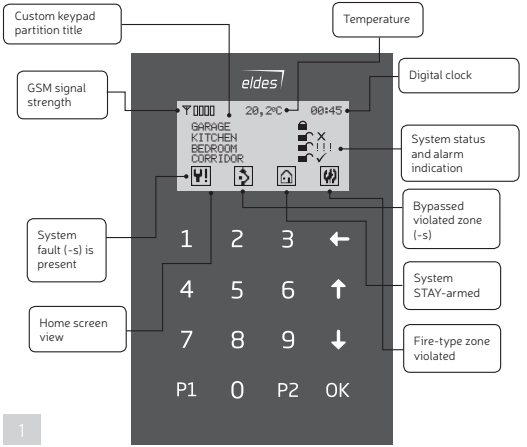
iButton key	Microchip containing a unique 64-bit ID code intended for system arming/disarming.
User code	Multi-digit combination intended for system arming/disarming and viewing system status temperature and other information using a keypad. The system supports up to 29 user codes.
Master code	Multi-digit combination intended for arming/disarming, viewing system status, temperature and other information; for electrical appliance control and minor system configuration using a keypad
Zone	Alarm system input for wired and wireless sensor connection
PGM output	Alarm system output for connection of electrical appliances (heating, lighting, gates etc.)
Partition	Section dividing one alarm system into two or more independent parts software-wise

1.2. Partitions

Your alarm system may be partitioned into up to 4 partitions, known as Partition 1 through Partition 4 . Each system partition operates independently from each other, therefore partitioning the system allows to use 1 alarm system unit to secure up to 4 different areas, for example: office and warehouse, house and garage etc. By default, the system is NOT partitioned and all user phone numbers, user codes (except for master code, which is assigned to all 4 system partitions by default), keypads, iButton keys, zones are assigned to Partition 1.

1.3. EKB2 Keypad Overview

EKB2 is an LCD keypad intended for using with ESIM384 alarm system.



1

Keys Functionality

←	One menu level back / cancel
↑	Menu navigation – up
↓	Menu navigation – down
OK	Confirm (enter) value
0 ... 9	Value typing
P1	Minus character to enter negative temp. value
P2	Additional menu / minus character to enter negative temp. value

Main Messages & Icons

Icon	Description
(by default - disabled)	Partition is armed and menu is locked
(by default - disabled)	Partition is disarmed and menu is unlocked
	Configuration mode activated
! ! !	Zone or tamper alarm in partition
✓	Partition is ready to be armed.
X	Partition is not ready to be armed – one or more zones / tampers violated.
	One or more system faults present
	One or more violated zones bypassed
	One or more partitions STAY-armed
	One or more Fire-type zones violated
	Alarms in alarm log present

EKB2 LCD screen is intended for displaying alarm system status messages and alerts. Icon ✓ is displayed on the screen that no zones and/or tampers are violated and the partition is prepared for arming. Icon ✗ shows up in case of zone violation or icon [!] if system faults are present. The partition cannot be armed until the violated zone (-s) is restored, disabled, bypassed or set up to operate under Force mode or violated tamper (-s) is restored. By default, the following faults allow partition arming if present:

- mains power is lost.
- low battery.
- battery dead or missing.
- battery failed.
- siren failed.
- date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.
- Keypad lost.

Audio Indication

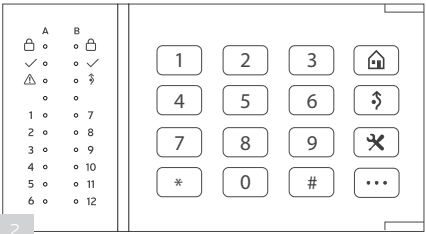
The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm.

Visual Indication

EKB2 can be used even in dark premises as the LCD screen and keys are illuminated continuously. The illumination level lowers down if 3 minutes after the last key-touch expires while the system is disarmed. In case of alarm, the keypad illumination level is boosted and stays in this state until the system is disarmed.

1.4. EKB3/EKB3W/EWKB4 Keypad Overview

EKB3/EKB3W/EWKB4 is a LED keypad intended for using with ESIM384 alarm system.



LED Functionality

	Steady ON - alarm system is armed / exit delay in progress; flashing - Configuration mode activated
	Steady ON - system is ready – no violated zones and tampers
	Steady ON - system faults; flashing - violated high-numbered zones
	Steady ON - zone bypass mode
1-12	Steady ON - violated zone

Keys Functionality

	Bypass violated zone
	System fault list / violated high-numbered zone indication / violated tamper indication
*	Clear typed in characters
#	Confirm (enter) command
0 - 9	Command typing
1 - 4	Keypad partition switch (only on EKB3) / steady ON - armed partition indication (only on EKB3) / flashing - violated partition indication (only on EKB3)
1 - 2	Keypad partition switch (only on **EKB3W and EWKB4**)
0	Simultaneous 4-partition arming (only on EKB3)
	Manual system arming in *Stay* mode
	1st character for Configuration mode activation/deactivation command

The green indicator ✓ indicates that no zones and/or tampers are violated and the system is prepared for arming. Yellow indicator ⚠ lights up or flashes in case of zone violation or if system faults are present. The partition cannot be armed until the violated zone (-s) is restored, disabled, bypassed or set up to operate under Force mode or violated tamper (-s) is restored. By default, the following faults allow partition arming if present:

- mains power is lost.
- low battery.
- battery dead or missing.
- battery failed.
- siren failed.
- date/time not set.
- GSM connection failed.
- GSM/GPRS antenna failed.

Audio Indication
The built-in buzzer uses two types of sound signals – three short beeps and one long beep. Three short beeps stand for successfully carried out configuration command, one long beep – for invalid configuration command. In addition, the buzzer emits short beeps in case of alarm.

Visual Indication
EKB3 keys have a LED back-light, therefore it is possible to use this keypad even in dark premises. The back-light lasts for 60 seconds after the last key-stroke while the system is disarmed. In case of alarm, the keypad back-light turns ON and lasts until the system is disarmed.

EKB3W and EWKB4 keys have a LED back-light, which will be activated once any key is pressed. Due to battery power saving reasons, the back-light and LED light last for 10 seconds after the last key-stroke.

1.5. EWKB5 wireless touchpad overview

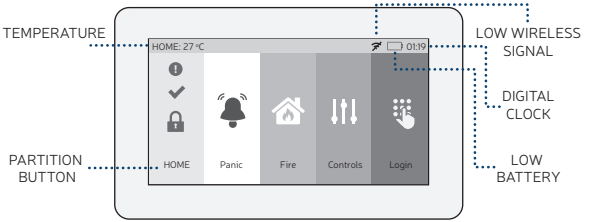
EWKB5 is a wireless accessory equipped with a 4.3" true-colour touch screen and compatible with ESIM384 alarm system.

Device features:
- Arming and disarming
- Violated zone bypass and bypassed zone activation
- PGM output control
- Customizable user-friendly graphical menu
- Navigation through the menu using the touch screen
- Multilingual voice-guided audio instructions
- Adjustable brightness and volume level
- Battery or externally-powered

EWKB5 has 1 built-in zone terminal, which is by default designed for passive wired digital sensor connection, such as magnetic door contact, and 2 tamper switches for enclosure state supervision in case it is illegally opened or detached from the wall. Regardless if the tamper switch alone is to be used, the zone must be enabled and the resistor of 5,6kΩ nominal must be connected across Z1 and COM connectors. It is possible to connect up to 4 EWKB5 devices to alarm systems. The maximum wireless connection range is 300m (~984ft) (in open areas).

Main menu features:
- Partition button – arms/disarms the system once a valid master/user code is entered; indicates partition status (armed/disarmed), presence of system faults.
- Quick arm button – arms the system by touching and holding this button; master/user code not required (customizable, hidden by default; not shown in picture).
- Fire – instantly causes fire alarm by pressing and holding this button (customizable, hidden by default).
- Panic – instantly causes silent alarm by pressing and holding this button (customizable, hidden by default).
- Controls – opens PGM output menu, thus letting you turn a certain PGM output ON or OFF (customizable, hidden by default).
- Login – grants access to settings menu once a valid master code is entered.

Dashboard features:
Low wireless signal – appears when the wireless signal strength drops below 30%.
Low battery – appears when the battery power drops below 5%.
Temperature – measured by a wired Dallas temperature sensor or a wireless device paired with the system (customizable, disabled and hidden by default)
Digital clock – displays system's current time.



For more details on how to configure and pair the device with the system, please visit www.eldesalarms.com to get the latest alarm system's installation/user manual.

2. BASIC CONFIGURATION AND USE

System configuration described in this document is based on the default system parameter values. Your alarm system installer may have changed those values. For more details, please contact your alarm system installer.

This chapter provides a description of basic configuration and use of ESIM384 alarm system by the following methods:

- SMS text message
- EKB2 LCD keypad
- EKB3 LED keypad
- EKB3W wireless keypad
- EWKB4 wireless keypad
- EWKB5 wireless touchpad
- By ELDES Configuration software

SMS

In order to configure and control the system using SMS text message, send the text command to the ESIM384 system phone number from one of the listed user phone numbers. In this user manual the underscore symbol "_" represents one space character. Every underscore symbol 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 message. ssss – 4-digit SMS password set by your alarm system installer.

EKB2

The system configuration and control by EKB2 keypad is performed 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 value 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 user manual, the menu path is provided under "tree" view by starting at home screen view. In this user manual valid parameter range is indicated in brackets.

EKB3/ EKB3W/ EWKB4

The system configuration and control by EKB3/EKB3W/EWKB4 keypad is carried out by 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. Additionally, the red indicators light up when the number keys [0] [9] are being pressed. Some commands require [ ], [ ] and [ ] keys as well. The structure of a standard configuration command is a combination of digits. The variables are provided in lower-case letters, while a valid parameter value range is provided in brackets.

!

If you have accidentally typed in an unnecessary character, please press [*] key or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cleared.

!

NOTE for EKB3W/EWKB4: Even if Back-light Timeout has expired, the character will be considered as type in once the appropriate EKB3W/EWKB4 key is pressed.

ELDES Configuration software

ELDES Configuration software is intended for ESIM384 alarm system configuration locally via USB port or remotely via GPRS network or Ethernet connection (ELAN3-ALARM device required). This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use ELDES Configuration software, please read the user guide provided in the software's documentation. Also, the system could be configured without connecting external power supply. When connecting to the PC with installed ELDES Configuration software via USB cable the system will be powered from PC USB power source. However, the device However, the device will NOT fully function when USB-powered. The user will be able to carry out some major part of system's configuration, with the exception of those functions, which are strictly related to GSM modem (disabled during the selected configuration period) or associated with the Wireless connectivity (also disabled).

3. MASTER AND USER CODES

The system supports up to 30 numeric codes, identified as Master code and User code 2 through 30, allowing to carry out system arming/disarming as well as minor system configuration and control by the keypad.

Master code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View event log.
- View and clear alarm log.
- Set/delete user codes.
- Turn ON/OFF electrical appliance.
- Set an existing user code as Duress code.
- Set an existing user code as SGS code.

User code is authorized to carry out the following:

- Arm/disarm partition.
- Bypass violated zones.
- View violated zones and tampers.
- View system faults.
- Set system date and time.
- View temperature sensor information.
- View and clear alarm log.

3.1. Managing User and Master Codes

By default, only master code is listed as 1111 and assigned to Partition 1, 2, 3 and 4. For more details regarding user and master code partition management, please refer to **3.3. Assigning User and Master Code Partition**.

1. To set a new master code:

EKB2

Enter an existing master code, navigate through the following path using OK and arrow keys and enter a new master code:
OK → vvvv → OK → CODES→ OK → MASTER CODE → OK → CODE → OK → mmmm → OK
Value: *vvvv* – 4-digit existing master code, range – [0000... 9999]; *mmmm* – 4-digit new master code, range – [0000... 9999].

EKB3/ EKB3W/ EWKB4

Press [···], [0], enter and existing master code and a new master code:
[···] [0] vvvv [0] [1] mmmm [#]
Value: *vvvv* – 4-digit existing master code; *mmmm* - 4-digit new master code; range - [0000... 9999].
Example: [···] [0] [1] [1] [1] [1] [0] [1] [2] [2] [2] [2] [#]

2. To add a user code:

EKB2

Enter the master code, navigate through the following path using OK and arrow keys and enter a user code:
User code 2... 16: OK → mmmm → OK → CODES → OK → USER CODE (2-16) → OK → USER CODE 2... 16 → OK → CODE → OK → uuuu → OK
User code 17... 30: OK → mmmm → OK → CODES → OK → USER CODE (17-30) → OK → USER CODE 17... 30 → OK → CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code, range – [0000... 9999].

EKB3/ EKB3W/ EWKB4

Press [···], [0], enter the master code, user code slot and a user code:
[···] [0] mmmm us uuuuu [#]
Value: *mmmm* - 4-digit master code; us - user code slot, range - [02... 30]; *uuuu* - 4-digit user code, range - [0000... 9999].
Example: [···] [0] [1] [1] [1] [1] [0] [9] [2] [5] [5] [6] [#]

3. To delete an existing user code:

EKB2

Enter the master code, navigate through the following path using OK and arrow keys and enter the user code you wish to delete:
OK → mmmm → OK → CODES → OK → REMOVE CODE → OK → uuuu → OK
Value: *mmmm* – 4-digit master code; *uuuu* – 4-digit user code.

EKB3/ EKB3W/ EWKB4

Press [···], [0], enter the master code and the user code slot you wish to delete:
[···] [0] mmmm us [#]
Value: *mmmm* - 4-digit master code; *us* - user code slot, range - [02... 30].
Example: [···] [0] [1] [1] [1] [1] [0] [9] [#]

3.2. Setting Duress and SGS Codes

- **Duress code** - The Duress code is used when system arming or disarming is demanded by force. When used, the system will arm/disarm as well as it will silently transmit an alert to the monitoring station. Only one of the user codes ranging from User code 2 through 10 can be set as Duress code. .
- **SGS code** – The user codes ranging from User code 2 through 10 can be set as SGS (Security Guard Service) code, which is used as a checkpoint by a security service guard upon his/her visit in the secured location. When used, a data message, containing a certain event code, will be delivered to the monitoring station. However, NO system arming or disarming will be carried out after entering the SGS code.

1. To set an existing user code as Duress code:

EKB2

Enter the master code, navigate through the following path using OK and arrow keys and select the user code you wish to set as Duress code:
OK → mmmm → OK → CODES → OK → DURESS CODE → OK → N/A | USER CODE 2... 10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – Duress code not in use.

EKB3/ EKB3W/ EWKB4

Press [···], [3], enter the user code slot you wish to set as Duress code and enter the master code:
[···] [3] us mmmm [#]
Value: *us* - user code slot, range - [02... 10]; *mmmm* - 4-digit master code.
Example: [···] [3] [0] [8] [2] [2] [2] [2] [#]

2. To set an existing user code as SGS code:

EKB2

Enter the master code, navigate through the following path using OK and arrow keys and select the user code you wish to set as SGS code:
OK → mmmm → OK → CODES → OK → SGS CODE → OK → N/A | USER CODE 2... 10 → OK
Value: *mmmm* – 4-digit master code; *N/A* – SGS code not in use.

EKB3/ EKB3W/ EWKB4

Press [···], [4], enter the user code slot you wish to set as SGS code and enter the master code:
[···] [4] us mmmm [#]
Value: *us* - user code slot, range - [02... 10]; *mmmm* - 4-digit master code.
Example: [···] [4] [0] [4] [2] [2] [2] [2] [#]

3.3. Assigning User and Master Code Partition

User/master code partition determines which system partition (-s) can be armed/disarm using the master code or a certain user code. For more details on how to arm/disarm the system, please refer to **5. ARMING, DISARMING AND TURNING OFF THE ALARM**.

The following table reflects the values used for system element assignment to partitions by EKB2/EKB3/EKB3W/EWKB4 keypad. A sum of values is used to assign the element to multiple partitions.

Partition	Partition value (pv)
Partition 1	1
Partition 2	2
Partition 3	4
Partition 4	8

Example #2: *The user wants to assign a certain user code 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.*

Example #3: *The user wants to assign the master code 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.*

To assign the master code or a certain user code to a certain partition (-s):

EKB2

Enter the master code, navigate through the following path using OK and arrow keys, select the master code or a certain user code and enter the partition value you wish the code to assign to.
Master code: OK → mmmm → OK → CODES → OK → MASTER CODE → OK → PARTITION → OK → pv → OK
User code 2... 17: ... → CODES → OK → USER CODE (2-17) → OK → USER CODE 2... 17 → OK → PARTITION → OK → pv → OK
User code 18... 30: ... → CODES → OK → USER CODE (18-30) → OK → USER CODE 18... 30 → OK → PARTITION → OK → pv → OK
Value: *mmmm* – 4-digit master code; *pv* – partition value (see table on page 18).

EKB3/ EKB3W/ EWKB4

Press [···], [5], enter 01 or user code slot, partition value you wish the code to assign to and the master code:
Master code: [···] [5] 01 pv mmmm [#]
User code: [···] [5] us pv mmmm [#]
Value: *us* - user code slot, range - [02... 30]; *pv* – partition value (see table on page 18); *mmmm* - 4-digit master code.
Example: [···] [5] [0] [5] [0] [4] [2] [2] [2] [2] [#]

4. SETTING UP DATE AND TIME

! When the alarm system is connected to a monitoring station the date and time are set automatically. The system retrieves this data from the monitoring station by itself.

SMS

1. Send the following SMS text message to the phone number of ESIM384 alarm system:

   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_2011.12.15_13:45*

2. The system will reply with confirmation by SMS text message to user phone number who sent the SMS text message after the date and time is set successfully.

EKB2

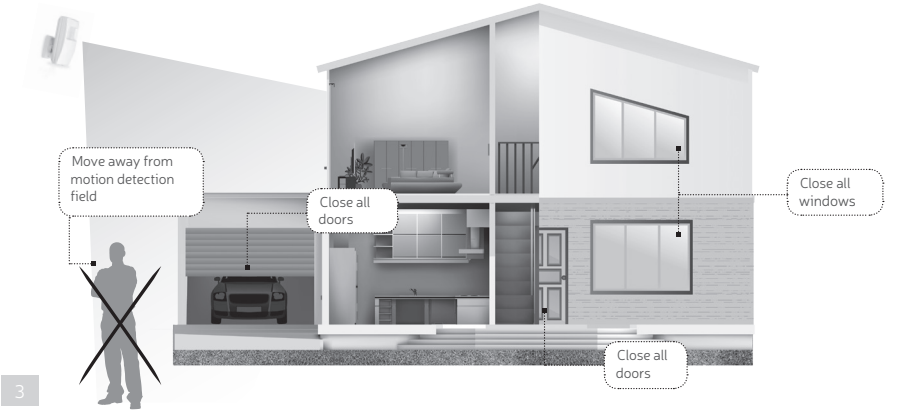
Navigate through the following menu path using *OK* and arrow keys and enter the date and time values using the number keys:

Menu path:
OK → DATE/TIME SET → OK → yyyy-mm-dd_hr:mn → OK

Value: *yyyy* – year; *mm* – month, range – [01... 12]; *dd* – day, range - [01... 31]; *hr* – hours, range – [00... 23], *mn* – minutes, range – [00... 59].
Example: *2015-12-15 13:45*

5. ARMING, DISARMING AND TURNING OFF THE ALARM

Before arming the system it is necessary to close all doors and windows in the secured area and move yourself away from the motion detection field.



3

Your alarm system installer may have enabled a Force attribute for certain zone (-s), thus allowing to arm the system, while the zone with Force attribute enabled is violated. This event is identified as Partial Arm.

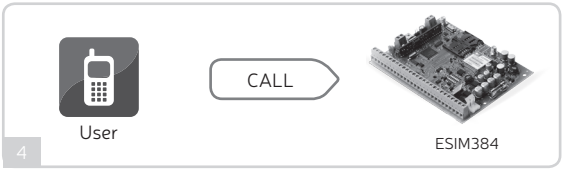
5.1. Free of Charge Phone Call

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

When system's phone number is dialled 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. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (resulting in partial arm; please contact your alarm system installer to set up this parameter), while the tampers can be disabled (please contact your alarm system installer to set up this parameter).
- **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 dialling 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 contact your alarm system installer.



4

! Your alarm system installer may have disabled system arming and/or disarming by free of charge phone call and SMS text message for a certain user.

By default, all listed user phone numbers are granted with permission to arm and disarm the system by free of charge phone call and SMS text message. To disable/enable arming or disarming for certain listed user phone numbers, please refer to the following configuration method.

Manage arming and disarming for listed user phone numbers

ELDES Configuration software

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

5.2. 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.

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*

5

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 followed by SMS text message delivery to the user.
  - 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 **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter), while the tampers can be disabled (please contact your alarm system installer to set up this parameter).

- **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.

To disarm the system and turn OFF the alarm 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 and turn OFF the alarm

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*

! Your alarm system installer may have disabled system arming and/or disarming by free of charge phone call and SMS text message for a certain user.

5.3. EKB2 Keypad and User/Master Code

✓ icon displayed next to the partition name in the home screen view of EKB2 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If ✗ icon is displayed instead, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please, contact your alarm system installer to set up this feature) or a Force attribute enabled (please, contact your alarm system installer to set up this parameter), while the tampers can be disabled (please, contact your alarm system installer to set up this feature). icon appears in the home screen view if system fault (-s) exist (see **13. INDICATION OF SYSTEM FAULTS**).

When a user/master code is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by EKB2 keypad using partition selection menu. However, if a user/master code 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, but the keypad will only display Partition 2 name and the related information in home screen view. For more details on how to set the keypad partition and user/master code partition, please refer to **3.3. Assigning User and Master Code Partition** and contact your alarm system installer.

5.3.1. Arming the System

To arm the system by EKB2 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **3. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

- **Non-partitioned system** - When a valid user code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps, the keypad will switch to home screen view and display the countdown timer.

Arm the system	Enter user/master code: uumm → OK Value: uumm – 4-digit user/master code.

- **Partitioned system - arming a single partition** – When a valid user or master code 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. When the keypad back-light timeout expires, the home screen view will follow. If ← key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timer next to the partition name that is being armed.

Arm the system

Enter user/master code and select partition:

uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK

Value: *uumm* – 4-digit user or master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name

- **Partitioned system - arming multiple partitions simultaneously** – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **ARM ALL** menu item is selected the system will proceed as follows:
  - if all partitions are disarmed-ready (no violated zone/tamper), the system will initiate exit delay. During the exit delay, the keypad's buzzer will emit short beeps and the keypad will display multiple **ARMING part-name** messages for 3 seconds reflecting each partition the user/master code is assigned to, followed by partition selection menu.
  - if one or more partitions are disarmed-unready (contains violated zone/tamper), 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 (-s) reflecting ready partition (-s), while the unready partition (-s) will be skipped indicated by **part-name NOT READY** message (-s) followed by partition selection menu. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.
  - if a combination of armed and disarmed-ready partitions exists, 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 (-s) seconds reflecting ready partition (-s), while the pre-armed partition (-s) will be skipped. Each message will be displayed for 2 seconds and corresponds to the partition (-s) the user/master code is assigned to.

When the keypad back-light timeout expires, the home screen view will follow. If ← key is touched twice during exit delay, the keypad will return to home screen view and display the countdown timers next to the partition names the keypad is assigned to.

Arm all partitions simultaneously

Enter user/master code:

uumm → OK → ARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → ARM ALL → OK

Value: *uumm* – 4-digit user/master code

When successfully armed:

- the countdown timers will disappear.
- user will be notified by SMS text message
- in addition, the keypad may display 🔒 icon next to the partition name that has been armed (by default – disabled).

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

5.3.2. Cancelling System Arming

To cancel the arming process:

- **Non-partitioned system** – Enter the user/master code 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 for 2 seconds followed by partition selection menu.

5.3.3. Disarming the System and Turning OFF the Alarm

To disarm and turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

- **Non-partitioned system** – When a valid user or master code is entered, the keypad will switch to home screen view.

Disarm the system and turn OFF the alarm	**Enter user/master code:** uumm → OK **Value:** *uumm* – 4-digit user/master code.

- **Partitioned system - disarming a single partition** – When a valid user or master code 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 2 seconds and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ← key may be touched in order to instantly return to home screen view.

Disarm the system and turn OFF the alarm	**Enter user/master code and select partition:** uumm → OK → [p] part-name → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → [p] part-name → OK **Value:** *uumm* – 4-digit user or master code; *p* – partition number, range – [1... 4], *part-name* – up to 15 characters partition name.

- **Partitioned system - disarming multiple partitions simultaneously** – When a valid user or master code is entered, the keypad will display the partition selection menu. Once **DISARM ALL** menu item is selected, the keypad will display multiple **part-name DISARMED**

messages for 2 seconds reflecting each partition the user/master code is assigned to and return to partition selection menu followed by home screen view after the keypad back-light timeout expires. Alternatively, the ← key may be touched in order to instantly return to home screen view.

Disarm all partitions and turn OFF the alarm simultaneously	**Enter user/master code:** uumm → OK → DISARM ALL → OK or OK → uumm → OK → ARM/DIS PARTITION → OK → DISARM ALL → OK **Value:** *uumm* – 4-digit user/ master code

When successfully disarmed, the keypad may display 🔓 icon next to the partition name that has been disarmed (by default - disabled) and notify the user by SMS text message.

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

5.4. EKB3,EKB3W and EWKB4 Keypads and User/Master Code

EKB3 keypad can operate either in 2-partition or in 4-partition mode. The description of the following procedure is based on 4-partition mode operation on EKB3 keypad. The arming/disarming procedure in 2-partition mode using EKB3 keypad would be carried out identically to EKB3W/EWKB4 wireless keypads. The user will be able arm/disarm only the first two system partitions using EKB3W/ EWKB4 keypad. Partition 3 and Partition 4 are NOT supported by EKB3W/EWKB4 keypad. For more details on 2-partition mode, please contact your alarm system installer.

Illuminated indicator ✓ on EKB3 keypad indicates that no violated zones and/or tampers are present, therefore the partition is ready for arming. If the indicator ✓ is not illuminated, the partition is unready for arming, therefore the user must restore all violated zones and/or tampers before arming the partition. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter), while the tampers can be disabled (please contact your alarm system installer to set up this parameter). Indicator ⚠ will illuminate or flash if system fault (-s) exist (see **13. INDICATION OF SYSTEM FAULTS**).

The system will arm/disarm the partition corresponding to the one that user/master code and the keypad are assigned to. For example, if User code 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 code 4. For more details on how to set the keypad partition and user/master code partition, please refer to **3.3. Assigning User** and Master Code Partition and contact your alarm system installer.

5.4.1. Arming the System by keypads

To arm the system by EKB3 keypad, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad (see **3. MASTER AND USER CODES** for user/master code management). By default, the arming process is as follows:

- **EKB3 -** When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator 🔒 along with 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.
- EKB3W/EWKB4 - **Non-partitioned system** – When a valid user/master code is entered, the system will initiate exit delay, the keypad's buzzer will emit short beeps and the indicator 🔒 will light ON. When the system is successfully armed, the keypad's buzzer will silent down.

Arm the system	**Enter user/master code:** uumm **Value:** *uumm* – 4-digit user or master code. **Example:** [2] [2] [2] [2]

! If the user fails to enter a correct user/master code 10 times in a row, the system will block the keypad for 2 minutes. While the keypad is blocked, the system prevents from entering any user/master code. The keypad will automatically unblock once the 2-minute time has expired.

5.4.2. Cancelling System Arming

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

5.4.3. Disarming the System and Turning OFF the Alarm by keypads

To disarm and turn OFF the alarm, enter any out of 29 available 4-digit user codes or master code using the number keys on the keypad. By default, the system disarming process is as follows:

- **EKB3** – When a valid user/ master code is entered, indicator 🔒 and the number [1] key will light OFF and the user will be notified by SMS text message.
- **EKB3W/EWKB4** – When a valid user/ master code is entered, indicator 🔒 will light OFF and the user will be notified by SMS text message.

5.5. Arming the system by EWKB5 touchpad

1. To arm the system, touch the Partition button and enter a valid 4-digit user/master code using the on-screen numpad. Alternatively, the user can touch and hold the Quick Arm button in order to arm the system without entering the user code. However, both methods require

the user/master code in order to disarm the system.
2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured premises. The countdown initiation will be indicated by voice-guided instructions followed by short beeps emitted by the touchpad.
3. Once the system is successfully armed, the touchpad will display icon on the Partition button followed by SMS text message confirmation delivered to the listed user phone number (by default).

5.5.1. Disarming the system and turning off the alarm by EWKB5 touchpad
1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured premises. Entry delay countdown is intended for user to enter a valid user code and disarm the system before the alarm is caused.
2. To disarm the system and/or turn off the alarm, enter a valid 4-digit user/master code using the on-screen numpad.
3. Once the system is successfully disarmed, the icon displayed on the Partition button will turn to spyna-atrakinta followed by SMS text message confirmation delivered to the listed phone number (by default).

For more details on how to configure and pair the device with the system, please visit www.eldesalarms.com to get the latest alarm system's installation/user manual.

5.6. iButton Key

To arm or disarm the system and turn OFF the alarm, touch the iButton key reader by any of 16 available iButton keys. 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 initiate exit delay and arm followed by SMS text message delivery to the user.
- 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 **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter), while the tampers can be disabled (please contact your alarm system installer to set up this parameter).

Partitioned system:

- If all partitions are disarmed ready (no violated zone/tamper), the system will initiate exit delay and arm them followed by SMS text message delivery to the user.
- 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). In order to arm the unready partition, the user must restore all violated zones and tampers assigned to the unready partition before arming the system. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter).
- 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 followed by SMS text message delivery to the user.

7

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 contact your alarm system installer.

5.7. EWK2 Wireless Keyfob

EWK2

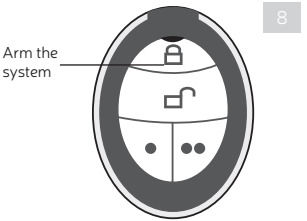
To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK 2 - 🔒). When EWK2 button is pressed for arming, the system will proceed as follows:

Non-partitioned system/partitioned system - arming a single partition:

- If ready (no violated zone/tamper), the system will arm followed by SMS text message delivery to the user.
- If unready, the system will not arm. In such case the user must restore all violated zones and tampers before arming the system. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter).

Partitioned system - arming multiple partitions simultaneously:

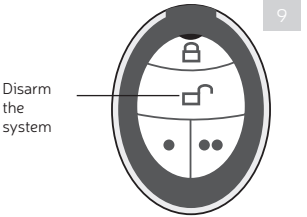
- If all partitions are disarmed ready (no violated zone/tamper), the system will arm them followed by SMS text message delivery to the user.
- If one or more partitions are disarmed unready (violated zone/tamper is present), the system will arm the ready partition (-s) and skip the unready one (-s). In order to arm the unready partition, the user must restore all violated zones and tampers assigned to the unready partition before arming the system. Alternatively, the violated zones can be bypassed (see **8. BYPASSING AND ACTIVATING ZONES**), disabled (please contact your alarm system installer to set up this parameter) or a Force attribute enabled (please contact your alarm system installer to set up this parameter).
- If a combination of armed and disarmed ready partitions is present, the system will arm the disarmed ready partitions and skip the armed ones followed by SMS text message delivery to the user.



EWK2

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

9



To verify if the system has been successfully armed, do not release the *Arm the system* keyfob button and wait for the 3 short keyfob buzzer's beeps/indicator's flashes indicating the successfully carried out command. The long beep/flash indicates the unsuccessful command.

When EWK2 keyfob is assigned to multiple partitions, the user will be able arm/disarm the corresponding system partitions by pressing the corresponding button. For example, if EWK2 is assigned to Partition 1 and 4, the user will be able to arm/disarm Partition 1 and 4 by pressing the corresponding button. For more details on how to set EWK2 keyfob partition, please contact your alarm system installer.

6. ARMING IN STAY MODE

EKB2

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

The system can be Stay armed under the following conditions:

- If a Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exists, the system will arm in Stay mode. When arming the system in Stay mode under this condition, one of the available arming methods must be used that provide exit delay i.e. EKB2/EKB3/EKB3W/EWKB4 keypad and iButton key. In addition, the user will be able to arm the system in Stay mode using EWK2 keyfob if the alarm system installer has pre-assigned the Stay-arm function to one of the keyfob buttons.
- The system will instantly arm in Stay mode when using one of the following methods.

EBK3/ EKB3W/ EWKB4

EWK2

EKB2

Menu path:

Non-partitioned system: P2 → uumm → OK

Partitioned system: P2 → uumm → OK → [p] part-name → OK

Value: *uumm* – 4-digit user/master code; *p* – partition number, range – [1... 4]; *part-name* – up to 15 characters partition name.

EBK3/ EKB3W/ EWKB4

Press the [⌂] key and enter user/master:

[⌂] uumm

Value: *uumm* – 4-digit user/master code.

Example: [⌂] [1] [1] [1] [1]

EWK2/ EWK2A

This operation may be carried out from the wireless keyfob if pre-assigned using the PC running *ELDES Configuration* software.

When one or more system partitions are successfully armed in Stay mode, EKB2 keypad will display [⌂] icon in the home screen view.

!

The system can also be instantly Stay-armed using ELDES Cloud Services.

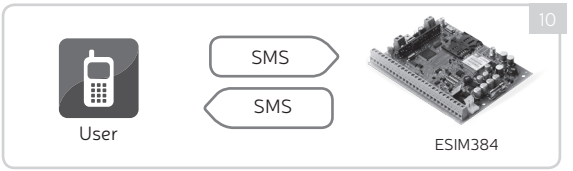
Stay mode is not supported by virtual zones.

To disarm the system, please use one of the methods described in **5. ARMING, DISARMING AND TURNING OFF THE ALARM**.

The system can be armed in Stay mode, only if at least one zone with Stay attribute enabled exists. Please contact your alarm system installer to set up this parameter.

7. ALARM INDICATIONS AND NOTIFICATIONS FOR USER. VIEWING VIOLATED ZONES AND TAMPERS

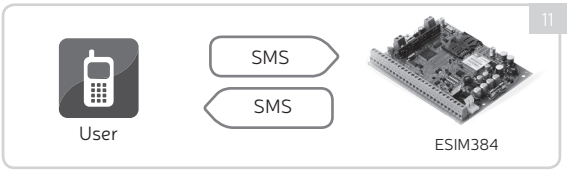
By default configuration, the system makes a phone call to User 1 in case of alarm. By answering the call, the user is able to listen on his/her mobile phone to what is happening in the area surrounding ESIM384 unit. This feature is provided by a microphone (if any) connected to ESIM384. The system will attempt to dial the first user phone number (presumably User 1) assigned to the partition that has been violated. The system will move to the next listed user (presumably to User 2) in the priority order in case the previous user was unavailable (out of GSM coverage, busy or did not answer the call). This routine will be continued until one of the listed users is a available, but will not return to the first user if none of the users were available. In addition, the system will not make a phone call to the next listed user in a row if the previous user was available, but rejected the phone call. The phone calls will cease to be made to the user as soon as the system is disarmed.



Your alarm system installer may have configured the system to ring the next available user even if the previous one was unavailable.

SMS

By, default configuration the system sends an SMS text message containing violated zone or tamper number in case of alarm. The SMS text message can also contain a text regarding wireless signal loss from a certain wireless device (if any) in case the tamper violation is caused due to wireless connection loss between ESIM384 and a wireless device. The system will attempt to deliver the SMS text message in the priority order starting with the first user (presumably User 1) assigned to the partition that has been violated. In case of failure to deliver the SMS text message, the system will attempt to send it to the next listed user (presumably User 2) in the priority order if the previous one was unavailable (the system did not receive a successful SMS text message delivery confirmation within 45 seconds from the recipient). This routine will be continued until one of the listed users is available, but will not return to the first user if none of the users were available. The SMS text messages will cease to be sent to the user phone number as soon as the system is disarmed.



See also **9. VIEWING SYSTEM INFORMATION**.

!

Your alarm system installer may have configured the system to send the SMS text message to the next available user even if the previous one has received it.

EKB2

The built-in EKB2 buzzer and ESIM384 buzzer (if any) provide short beeps continuously in case of alarm. In addition, the LCD screen back-light level will be boosted and the **!!!** icon will be displayed in the home screen view of EKB2 keypad next to the violated partition name. The buzzer can be silenced by disarming the system using any method. Navigate through the following menu path using OK and arrow keys to view the violated zone or tamper number:

Menu path:

View violated zone: OK → uumm → OK → VIOLATED ZONES → OK → ZONE 1... 80
View violated tamper: OK → uumm → OK → VIOLATED TAMPERS → OK → TAMPER 1... 80

Value: *uumm* – 4-digit user or master code.

EKB3/ EKB3W/ EWKB4

The built-in EKB3/EKB3W/EWKB4 buzzer emits short beeps continuously and ESIM384 buzzer (if any) emits a steady beep in case of alarm. In addition, the violated zone number is indicated by illuminated zone LED or flashing indicator ⚠ (if the violated zone number is above 12). The violated tamper number is indicated by illuminated indicator ⚠. The buzzer can be silenced by disarming the system using any method. When EKB3 keypad is operating in 4-partition mode, in case of violated zone/tamper [1]...[4] key will flash corresponding the alarmed partition number. For more details on EKB3/EKB3W/EWKB4 violated high-numbered zone and tamper number indication, please refer to **13. INDICATION OF SYSTEM FAULTS.**

By default configuration, the siren/bell (if any) provides continuous alarm sound for 1 minute in case of alarm. The fire alarm is indicated by pulsating siren/bell alarm sound. The alarm sound can be silenced by disarming the system using any method.

8. BYPASSING AND ACTIVATING ZONES

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, EKB2 keypad will display ⛔ icon in the home screen view.

EKB2

Enter valid user/master code and navigate through the following path using OK and arrow keys to bypass a violated zone (-s):

Menu path:

Bypass a zone: OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 3 → OK → ZONE 1... 80 → OK → BYPASS → OK

Bypass all certain partition zones: OK → uumm → OK → BYPASS → OK → BYP VIOLATED ZONES → OK→ [p] part-name → OK

Value: *uumm* – 4-digit user or master code.

Enter valid user/master code, navigate through the following path using OK and arrow keys to activate a bypassed zone:

Menu path:

Activate a bypassed zone: OK → uumm → OK → BYPASS → OK → BYPASS LIST 1... 3 → OK → ZONE 1... 80 → OK → UNBYPASS → OK

Value: *uumm* – 4-digit user or master code.

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

EKB3

When a zone is bypassed, EKB3/EKB3W/EWKB4 keypad indicator will light ON. Bypass a violated zone by entering a valid user/master code and entering the following combination using [*], number and [#] keys:

Press the [*] key, enter zone number and user/master code:

[*] nn uumm #

Value: *nn* – zone number, range – [01... 80]; *uumm* – 4-digit user or master code.

Example: [*] [5] [0] [1] [1] [1] [1] [#]

! Bypassing a violated tamper is NOT allowed. Please, restore the tamper (for example: close sensor's enclosure) before arming the system.

! The zone will remain bypassed until the system is disarmed. Once the system is disarmed, the zone's current state will be indicated on the keypads.

! Your alarm system installer may have set a certain limit of zone violations resulting in automatic bypass of the zone once the limit is exceeded.

9. VIEWING SYSTEM INFORMATION

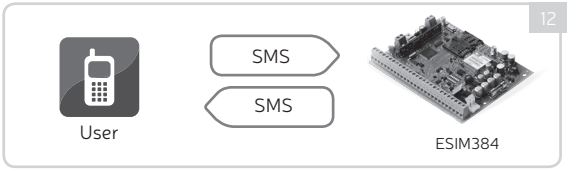
SMS

1. In order to find out the system's current information, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

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

2. The system will reply to the user phone number that sent the SMS text message with the following up-to-date information:

   - System date and time.
   - System status: partition armed (ON)/disarmed (OFF).
   - GSM signal strength level.
   - Mains power status.
   - Temperature of the area surrounding ESIM384 primary and secondary temperature sensors (if any).
   - State of zones (OK/alarm).
   - Name and status (ON/OFF) of PGM outputs.

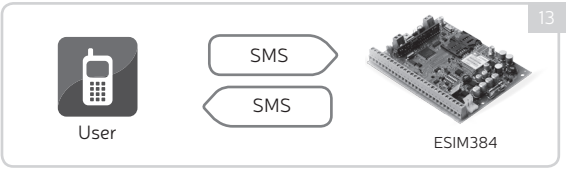


See also **12. MANAGING AND VIEWING TEMPERATURE INFORMATION**.

9.1. Managing Periodical System Information

SMS

1. By default configuration, the SMS text message mentioned in chapter **9. VIEWING SYSTEM INFORMATION** is sent periodically to User 1 phone number at 11:00 daily.



2. In order to set a different SMS sending frequency (in days) and time, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_INFO:fff,it
   Value: *ssss* - 4-digit SMS password; *fff* – frequency in days, range – [0... 99]; *it* – time, range – [0... 23]
   Example: *1111_INFO:2.15 (every 2nd day at 15:00)*

3. In order to disable periodic SMS text message, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_INFO:00.00
   Value: *ssss* - 4-digit SMS password.
   Example: *1111_INFO:00.00*

4. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.

! Unlike system information SMS text message upon request, periodical system information SMS text message does not included zone states, PGM output names and status.

10. VIEWING ZONE AND PGM OUTPUT INFORMATION

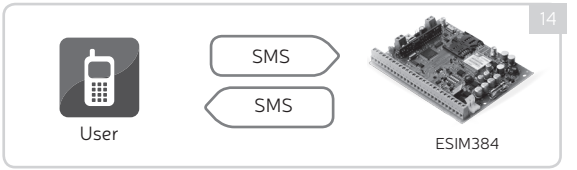
SMS

1. In order to find out the current zone and PGM output information, send the following SMS text message to the system' s phone number from any out of 10 listed user phone numbers:

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

2. The system will reply to the user phone number that sent the SMS text message with the following up-to-date information:

   - System status: partition armed (ON)/disarmed (OFF).
   - Status of zones and PGM outputs (ON/OFF).
   - Zone alarm texts.
   - PGM output names.



11. SMS TEXT MESSAGE DELIVERY RESTRICTIONS

By default, the system is restricted to send out up to 25 SMS text messages daily and up to 400 SMS text messages monthly. To change the limits or disable SMS text message delivery restrictions, please refer to the following configuration method.

Manage SMS text message delivery limits	**ELDES Configuration software**	This operation may be carried out from the PC using the *ELDES Configuration* software.

When the daily or monthly SMS text message delivery limit is exceeded, the system will notify the administrator by SMS text message. The limit counter will automatically reset once the date and time synchronization period takes effect (by default - every 30 days). Alternatively, you can reset the limits by referring to the following configuration method.

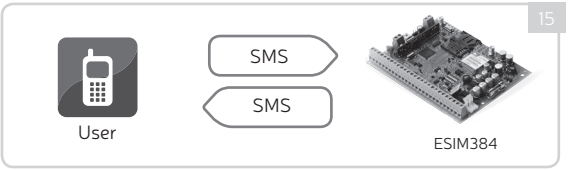
Reset SMS text message delivery limit counter	**SMS**	**SMS text message content:** ssss_REMOVEBAN **Value:** *ssss* – 4-digit SMS password. **Example:** *1111_REMOVEBAN*

! 0 value disables daily/monthly SMS text message delivery restrictions.

12. MANAGING AND VIEWING TEMPERATURE INFORMATION

SMS

1. The system supports up to 8 temperature sensors. If at least 1 or 2 (primary and/or secondary) temperature sensors are installed in your system, it can send an SMS text message containing temperature value in case the set lowest or highest temperature limit value is exceeded. This SMS text message is sent to User 1 only. By default, configuration by this SMS text message is disabled.



2. In order enable or set a different lowest, highest temperature limit value or specify a name for a determined primary or secondary temperature sensor, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_TEMPn:MIN:tm,MAX:tmx,NAME:temp-sens-name
   Value: *ssss* - 4-digit SMS password; *n* - primary or secondary temperature sensor number, range - [1... 8]; *tm* - lowest temperature limit boundary in °C, range - [-55... 125]; *tmx* - highest temperature limit boundary in °C, range - [-55... 125]; *temp-sens-name* - temperature sensor name, length - 4... 24 characters.
   Example: *1111_TEMP2:MIN:-15,MAX:30,NAME:Garage*

3. In order to disable this SMS text message, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_TEMPn:MIN:0,MAX:0
   Value: *ssss* - 4-digit SMS password; *n* - primary or secondary temperature sensor number, range - [1... 8].
   Example: *1111_TEMP1:MIN:0,MAX:0*

SMS

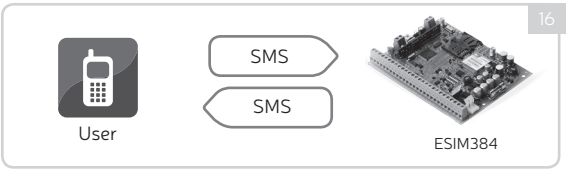
4. In order to find out, which temperature sensors are set as primary and secondary, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

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

5. In order to find out the current temperature of all temperature sensors, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

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

6. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.



See also **9. VIEWING SYSTEM INFORMATION**.

EKB2

Enter valid user/master code and navigate through the following path using OK and arrow keys to view real-time temperature sensor values:

Menu path:

OK → uumm → OK → TEMP SENSORS INFO → OK → 1... 8

Value: *uuuu* – 4-digit user or master code.

Also, you may use the on-board temperature sensors or the built-in temperature sensor of the following wireless devices:

- EWP2 – wireless motion detector.
- EWP3 – wireless motion detector.
- EWD2 - wireless magnetic door contact/shock sensor/flood sensor.
- EWD3 - wireless magnetic door contact/shock sensor/flood sensor.
- EWS3 – wireless indoor siren.
- EWS2 – wireless outdoor siren.
- EWF1 - wireless smoke detector.
- EWF1CO - wireless smoke and CO detector.
- EW2 - wireless zone and PGM output expansion module (an external temperature sensor (-s) must be connected to EW2 for this purpose).
- EWM1 - wireless power socket.

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

View real-time temperature value of the 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

Fore more about temperature information please refer to ESIM384 installation manual, located at www.eldesalarms.com.

13. INDICATION OF SYSTEM FAULTS

The system comes equipped with self-diagnostic feature allowing to indicate the presence of any system fault by the keypad as well as by SMS text message notification to the listed user phone number.

EKB2

icon displayed in home screen view indicates presence of system faults. In order to view the currently present system faults, please enter a valid user/master code to access menu section **FAULTS**. The description on each system fault is provided in the table below. Enter valid user/master code and navigate through the following path using OK and arrow keys to view system faults that are currently present.

Menu path:

OK → uumm → OK → FAULTS → OK

Value: *uumm* – 4-digit user/master code.

Name	Description
MAIN POWER LOSS	Mains power is lost
LOW BATTERY	Low backup battery power - backup battery voltage is 10.5V or lower
BATTERY DEAD/MISS	Backup battery is not present or the battery voltage runs below 5V
BATTERY FAILED	Backup battery requires replacement - backup battery resistance is 2Ω or higher
SIREN FAILED	Wired siren is disconnected/broken
VIOLATED TAMPER	One or more tampers are violated
DATE/TIME NOT SET	Date/time not set
GSM CONNECT FAILED	GSM connection is lost
GSM ANTENNA FAILED	GSM/GPRS antenna is disconnected/broken
WLESS ANTENNA FAIL	Wireless antenna is disconnected/broken
COM BUS FAILED	RS485 device, such as keypad, ELAN3-ALARM or EPGM1 is disconnected/broken
CO LEVEL CRITICAL	Critical level 4 of carbon monoxide (CO) concentration detected by EWF1CO is reached
EWM1 FAULTS	One or more EWM1 device faults exist - enter this menu item to view the existing EWM1 device faults (see **15. POWER CONSUMPTION MONITORING**)
WLESS BATT LOW	Low wireless device battery power - battery level is running below 5%
RF JAMMER DETECTED	Wireless signal is blocked by jammer

Alternatively, existing EWM1 device faults can be viewed by accessing menu section **FAULTS** of the PGM output associated with a certain EWM1 device (see **15. POWER CONSUMPTION MONITORING**).

EKB3/ EKB3W/ EWKB4

Yellow LED ⚠ indicates system faults. ⚠ LED indications are mentioned in the table below.

⚠ LED	Description
Steady ON	One or more tampers are violated; other system faults (see below)
Flashing	One or more high-numbered zones (Z13-Z80) are violated

In order to find out more on the particular system fault, please enter command A provided below. After this procedure the system will activate red zone LEDs for 15 seconds. The description on each LED indication is mentioned in the table below.

Zone LED	Description
1	Mains power is lost
2	Low backup battery power - backup battery voltage is 10.5V or lower
3	Backup battery is not present or the battery voltage runs below 5V
4	Backup battery requires replacement - backup battery resistance is 2Ω or higher
5	Siren is disconnected/broken
7	One or more tampers are violated
8	Date/time not set
9	One or more high-numbered zones (Z13-Z80) are violated
10	GSM connection is lost
11	GSM/GPRS antenna is disconnected/broken
12	Wireless antenna is disconnected/broken

In order to find out which particular high-numbered zone is violated, please enter command B.
In order to find out which particular tamper is violated, please enter command C.

A. System fault indication - enter command:

[•••] [#]

B. Violated high-numbered zone indication – enter command:

[•••] [1]

EKB3/ EKB3W/ EWKB4

C. Violated tamper indication – enter command:

[···] [2]

The number of violated high-numbered zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

Example: LED #3 from section A is flashing and LED #8 from section B is steady ON. According to the table below LED #8 is equal to number 18, therefore 18 + 3 = 21.

Result: Violated high-numbered zone or tamper number is 21.

Zone LED section - A (flashing)	Zone LED section - B (steady ON)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	Zone LED 11 = 36
Zone LED 6 = 6	Zone LED 12 = 42

14. CONTROLLING ELECTRICAL APPLIANCES

Your system features 4 or more PGM outputs intended for connection and control of various electrical appliances. This provides a possibility to control garage gates, turn on and off your house heating, lighting, cooling system, reset smoke sensors to restored state etc. The PGM outputs must be configured by your installer before using them.

14.1. Turning ON/OFF the Electrical Appliances Instantly

SMS

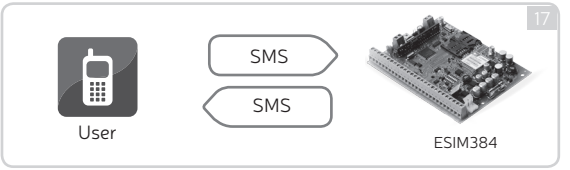
1. In order to turn ON a specified PGM output, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_Coo:ON or ssss_out-name:ON
   Value: *ssss* - 4-digit SMS password; *oo* – PGM output number, range – [1... 48]; *out-name* – PGM output name.
   Example: *1111_Pump:ON*

2. In order to turn OFF a specified PGM output, send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_Coo:OFF or ssss_out-name:OFF
   Value: *ssss* - 4-digit SMS password; *oo* – PGM output number, range – [1... 48]; *out-name* – PGM output name.
   Example: *1111_C2:OFF*

3. The system will reply with confirmation by SMS text message to the user phone number that sent the SMS text message.



EKB2

1. In order to turn ON a specified PGM output, enter the master code and navigate through the following menu path using OK and arrow keys.

Menu path:
On-board PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → out-name → ON → OK
Wireless PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → out-name → ON → OK
Value: *mmmm* – 4-digit master code; *out-name* – up to 16 characters PGM output name.

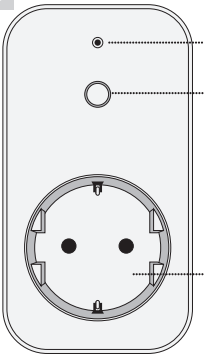
2. In order to turn OFF a specified PGM output, enter the master code and navigate through the following menu path using OK and arrow keys.

Menu path:
On-board PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → out-name → ON → OK
Wireless PGM output: OK → mmmm → OK → PGM OUTPUTS → OK → out-name → ON → OK
Value: *mmmm* – 4-digit master code; *out-name* – up to 16 characters PGM output name.

! For more information about PGM output control, please read the ESIM384 installation manual at www.eldesalarms.com

15. POWER CONSUMPTION MONITORING

EWM1 is a wireless device intended to provide a wireless connection access to any electrical appliance, such as lights, air-conditioner, watering equipment etc. By pairing EWM1 wireless power socket to the system and plugging the appliance into the electrical outlet of EWM1, the user will be able to control the appliance via wireless keyfob, keypad, SMS text message or according to the scheduled time as well as to monitor real-time power consumption value and view today's or monthly power consumption reports. In case of EWM1 failure, you can view the existing device faults using EKB2 LCD keypad.



LED indication	Description
Flashing (green)	EWM1 is unpaired or wireless connection with ELDES alarm system is lost
Steady ON (red)	Fault is present
OFF	Relay is turned OFF
Steady ON (green)	Relay is turned ON
Flashing (red)	EWM1 is resetting to default

SMS

1. In order to request today's and monthly power consumption reports, please send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

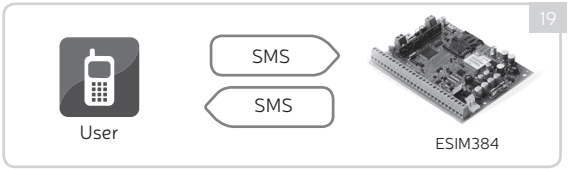
   SMS text message content:
   ssss_EWM1INFO
   Value: *ssss* - 4-digit SMS password.
   Example: *1111_EWM1INFO*

2. In order to reset the power consumption counter of a certain EWM1 device paired with the system, please send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_EWM1RESET:out-name
   Value: *ssss* - 4-digit SMS password; *out-name* - PGM output name associated with a certain EWM1 device.
   Example: *1111_EWM1RESET:Controll13*

3. In order to reset the power consumption counter of all EWM1 devices paired with the system, please send the following SMS text message to the system's phone number from any out of 10 listed user phone numbers:

   SMS text message content:
   ssss_EWM1RESET:ALL
   Value: *ssss* - 4-digit SMS password.
   Example: *1111_EWM1RESET:ALL*



EKB2

1. Enter master code and navigate through the following menu path using OK and arrow keys to monitor and view the power consumption:

Menu path:

Real-time power consumption: OK → mmmm → OK → PGM OUTPUTS → OK → out-name → OK → REAL TIME ENERGY
Today's power consumption: ... → out-name → OK → TODAY ENERGY
Monthly power consumption: ... → out-name → OK → MONTHLY ENERGY
Value: *mmmm* - 4-digit master code; *out-name* - PGM output name associated with a certain EWM1 device

2. Enter master code, navigate through the following menu path using OK and arrow keys and select **YES** to reset the power consumption counter of the selected EWM1 device:

Menu path:

OK → mmmm → OK → PGM OUTPUTS → OK → out-name → OK → RESET COUNTER → OK → YES | NO → OK
Value: *mmmm* - 4-digit master code; *out-name* - PGM output name associated with a certain EWM1 device

3. [!] icon displayed in home screen view indicates presence of system and EWM1 device faults. Enter master code and navigate through the following menu path using OK and arrow keys to view EWM1 device faults:

Menu path:

OK → mmmm → OK → PGM OUTPUTS → OK → out-name → OK → FAULTS → OK
Value: *mmmm* - 4-digit master code; *out-name* - PGM output name associated with a certain EWM1 device

Name	Description
OVERVOLTAGE	Voltage has increased above 260VAC.
UNDERVOLTAGE	Voltage has dropped below 190VAC.
OVERCURRENT	Current has increased above 12,5A
RELAY FAULT	Unable to power up the appliance due to faulty relay
TEMP. FAULT	Environmental temperature has dropped below -35°C (-31°F) or increased above +90°C (+194°F)

In order to clear the existing faults, please press the ↻ button on EWM1, turn OFF the electrical appliance or turn OFF the wireless PGM output associated with EWM1.

16. VIEWING EVENT AND ALARM LOGS

16.1. Event Log

The event log allows to chronologically register up to 500 timestamped records regarding the following system events:

- System start.
- System arming/disarming.
- Zone violated/restored.
- Tamper violated/restored.
- Zone bypassing.
- Wireless device management.
- Temperature deviation by MIN and MAX boundaries.
- System faults.
- Configuration via USB.
- User phone number that initiated the remote configuration.

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

EKB2

Enter master code and navigate through the following menu path using OK and arrow keys to view the event log:

Menu path:

OK → mmmm → OK → VIEW EVENT LOG → OK

Value: *mmmm* - 4-digit master code.

16.2. Alarm Log

The alarm log provides a list of last 16 alarm events generated after last arming period. The alarm log can be viewed via EKB2 and includes only the alarms of the partition that the user/master code is assigned to. Each alarm record includes alarm type, partition number and zone number.

When highlighted, the date and time of the alarm occurrence can be viewed at the bottom of EKB2 screen. In case of alarm,  icon will appear in home screen view of EKB2. The alarm log auto-clears when the next system arming follows or after viewing it via the keypad.

EKB2

Enter user/master code, navigate through the following menu path using OK and arrow keys to view/clear the alarm log:

Menu path:

OK → uumm → OK → ALARM LOG → OK

Value: *uumm* - 4-digit user or master code.

Syntax of alarm log record: *[alarm-type P:p Z:nn]*

Value: *alarm-type* - BURGLARY/FIRE/24H/SILENT/TAMPER/WS LOST, *p* - partition number, range - [1... 4], *nn* - zone/tamper number, range - [1... 80].

#1 example of alarm log record: *BURGLARY P:1 Z:1*

Value: *BURGLARY* - Instant, Int. Follower or Delay-type zone alarm; *P:1* - Partition 1; *Z:1* - zone Z1.

#2 example of alarm log record: *TAMPER P:2 Z:13*

Value: *TAMPER* - tamper alarm; *P:2* - Partition 2; *Z:13* - tamper 13.

#3 example of alarm log record: *FIRE P:4 Z:9*

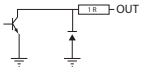
Value: *FIRE* - Fire-type zone alarm; *P:4* - Partition 4; *Z:9* - zone Z9.

#4 example of alarm log record: *WS LOST P:2 Z:14*

Value: *WS LOST* - wireless signal loss alarm; *P:2* - Partition 2; *Z:14* - tamper 14.

17. TECHNICAL SPECIFICATIONS

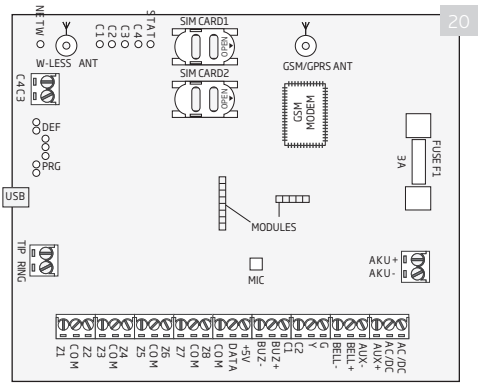
17.1. Electrical and Mechanical Characteristics

Electrical and Mechanical Characteristics	
Power supply	16-24V 50/60 Hz ~1.5A max / 18-24V ⎓ 1,5A max
Current consumption in idle state w/o external devices connected	Up to 80mA
Recommended backup battery voltage, capacity	12V; 1,3-7Ah
Recommended backup battery type	Lead-Acid
Backup battery charge current	Up to 500mA
Backup battery charge duration	Up to 30 hours for 7Ah battery
Gsm modem frequency	850/900/1800/1900MHz
Cable type for GSM/GPRS antenna connection	Shielded
Number of zones on-board	8 (ATZ mode: 16)
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 30V; 500mA
BELL: Siren output when activated	Connected to COM
BELL: Maximum siren output current	1A
BELL: Maximum cable length for siren connection	Up to 100m (328.08ft)
BELL: Cable type for siren connection	Unshielded
AUX: Auxiliary equipment power supply voltage	13,8V DC
AUX: Maximum accumulative current of auxiliary equipment	1,1A
AUX: Maximum cable length for auxiliary equipment connection	Up to 100m (328.08ft)
AUX: Cable type for auxiliary equipment connection	Unshielded
BUZ: Maximum current of mini buzzer	150mA
BUZ: Power supply voltage of buzzer	5V DC

BUZ: Cable type for mini buzzer connection	Unshielded
Supported temperature sensor model	Maxim®/Dallas® DS18S20, DS18B20
Maximum supported number of temperature sensors	8
DATA: Maximum cable length for 1-Wire communication	Up to 30m (98.43ft)
DATA: Cable type for 1-Wire communication	Unshielded
Supported iButton key model	Maxim®/Dallas® DS1990A
Maximum supported number of iButton keys	16
Maximum supported number of keypads	4 x EKB2 / EKB3
Y/G: Maximum cable length for RS485 communication	Up to 100m (328.08ft)
Y/G: Cable type for RS485 communication	Unshielded
MIC: Maximum cable length for microphone connection	Up to 2m (6.56ft)
MIC: Cable type for microphone connection	Unshielded
Wireless band	ISM868 /ISM 915
Wireless communication range	Up to 30m (98.43ft) in premises; up to 150m (492.13ft) in open areas
Maximum supported number of wireless devices	32
Event log size	500 events
Maximum supported number of zones	80
Maximum supported number of PGM outputs	48
Cable type for zone and PGM output connection	Unshielded
Generated PSTN line values	Voltage: 48V; current: 25mA; impedance: 270Ω
Communications	SMS, Voice calls, GPRS network, CSD, PSTN, Ethernet via ELAN3-ALARM
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS, SIA IP
Dimensions	140x100x18mm (5.51x3.94x0.71in)
Operating temperature range	-20...+55°C (-4... +131°F)
Humidity	0-90% RH @ 0... +40°C (0-90% RH @ +32... +104°F) (non-condensing)

17.2. Main Unit, LED and 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

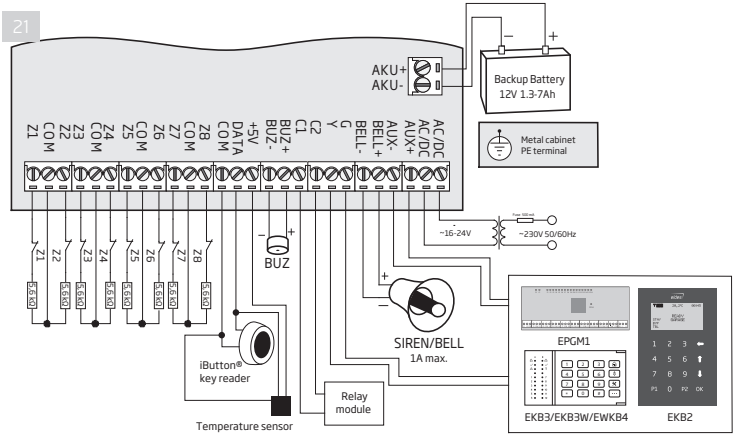
NETW indication	GSM signal strength
OFF	No GSM signal
Flashing every 3 sec.	Poor
Flashing every 1 sec.	Medium
Flashing several times per sec.	Good
Steady ON	Excellent

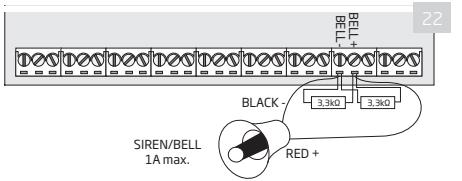
Connector	Functionality
TIP*	PSTN (landline) terminal
RING*	PSTN (landline) terminal
DATA	1-Wire interface for iButton key and temperature sensor connection
+5V	Temperature sensor power supply terminal (+5V)
BUZ-	Buzzer negative terminal
BUZ+	Buzzer positive terminal
C1 - C4	PGM output terminals
Z1 - Z8	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	Mains power terminals
AKU-	Backup battery negative terminal
AKU+	Backup battery positive terminal

* - Optional, implementable on request in advance

17.3. Wiring Diagrams

17.3.1. General Wiring





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 3,3kΩ nominal resistors connected in parallel across **BELL+** and **BELL-** terminals.

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 **13. INDICATION OF SYSTEM FAULTS**).

Made in the European Union

www.eldesalarms.com