

eldes

EPIR3

GSM Alarm System

Contents

Technical Specifications **4**

Components of the EPIR3 security system **5**

1. 7-STEP START GUIDE **6**
OVERVIEW 6

2. QUICK START GUIDE **9**
2.1. How and where to fix the holder to the wall 9
2.2. Prepare the SIM card 12
2.3. How to insert the SIM card 13
2.4. Plug the power supply connector into the device 15
2.5. Place the device into the holder 15
2.6. Slide the device down to fix it 15
2.7. Insert the plug into the mains socket 15
2.8. How to check the detector is working 15
2.9. About the back-up battery and how to replace it 16
2.10. How to program EPIR3 system 17
2.11. How to arm and disarm the system 24
2.12. A 15 second delay allows you to leave the premises 25
2.13. Receiving an alarm call 25
2.14. In case of mains power failure 26
2.15. Receiving an SMS text message when temperature exceeds the set values 26
2.16. Additional capabilities 26

3. HOW TO MANAGE THE WIRELESS DEVICES **27**
3.1. How to bind a wireless device to the system 28
3.2. How to remove a wireless device from the system 32
3.3. EKB3W wireless keypad overview 34
3.4. EWK1 and EWK2 wireless keyfob overview 42

Contents

4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE 44

5. HOW TO PROGRAM THE SYSTEM USING EKB3W WIRELESS KEYPAD 57

6. TROUBLESHOOTING 82

7. ADDITIONAL INFORMATION FOR ADVANCED USERS 83

7.1. How to connect a wired siren or a LED indicator to the wired output 83
7.2. How to connect a sensor to the wired zone 87
7.3. Automatic system arming/disarming 92
7.4. Zones 92
7.5. Tampers 94
7.6. Programmable (PGM) outputs 95
7.7. Siren 96
7.8. Alarm indications and notifications 98
7.9. System notifications 99
7.10. Back-up battery, mains power supply status monitoring and memory 102
7.11. Monitoring staton 103
7.12. System configuration using ELDES Configuration Tool software 112
7.13. How to reset the system to default settings 117
7.14. How to upgrade the firmware locally via USB connection 117
7.15. How to upgrade the firmware remotely via GPRS connection 118
7.16. Smart Security 120

8. Related products 122

Copyright © "ELDES UAB", 2014. All rights reserved.

It is forbidden to copy and distribute information in this document without advance written authorisation from ELDES UAB. We reserve the right to update or modify this document and/or related products without warning. The EPIR3 GSM Alarm System complies with the essential requirements and relevant provisions of Directive 1999/5/EC. The declaration of conformity may be viewed at www.eldes.lt

Protecting your home and property with the EPIR3 alarm system

Where and how to use the alarm system

The EPIR3 is a convenient, easy to use, remote control security system for houses, cottages, country homes, garages and other buildings.

It uses an internal SIM card (not supplied by ELDES) and an infra red sensor, and communicates with your mobile phone so you can:

- Protect your property while you are away from home
- Listen to what is happening in your property following a security alert
- Switch the system on or off from anywhere in the world at no cost
- Receive SMS text messages updating you on the system status
- Include up to ten users to receive system status messages and/or security alerts
- Receive SMS text messages updating you on the temperature of the surrounding area

In addition, the EPIR3 system has a built-in wireless module for system extension capabilities.The wireless module easily allows you to bind ELDES-made wireless devices to the system. For more details, please, refer to section **3. HOW TO MANAGE THE WIRELESS DEVICES.**

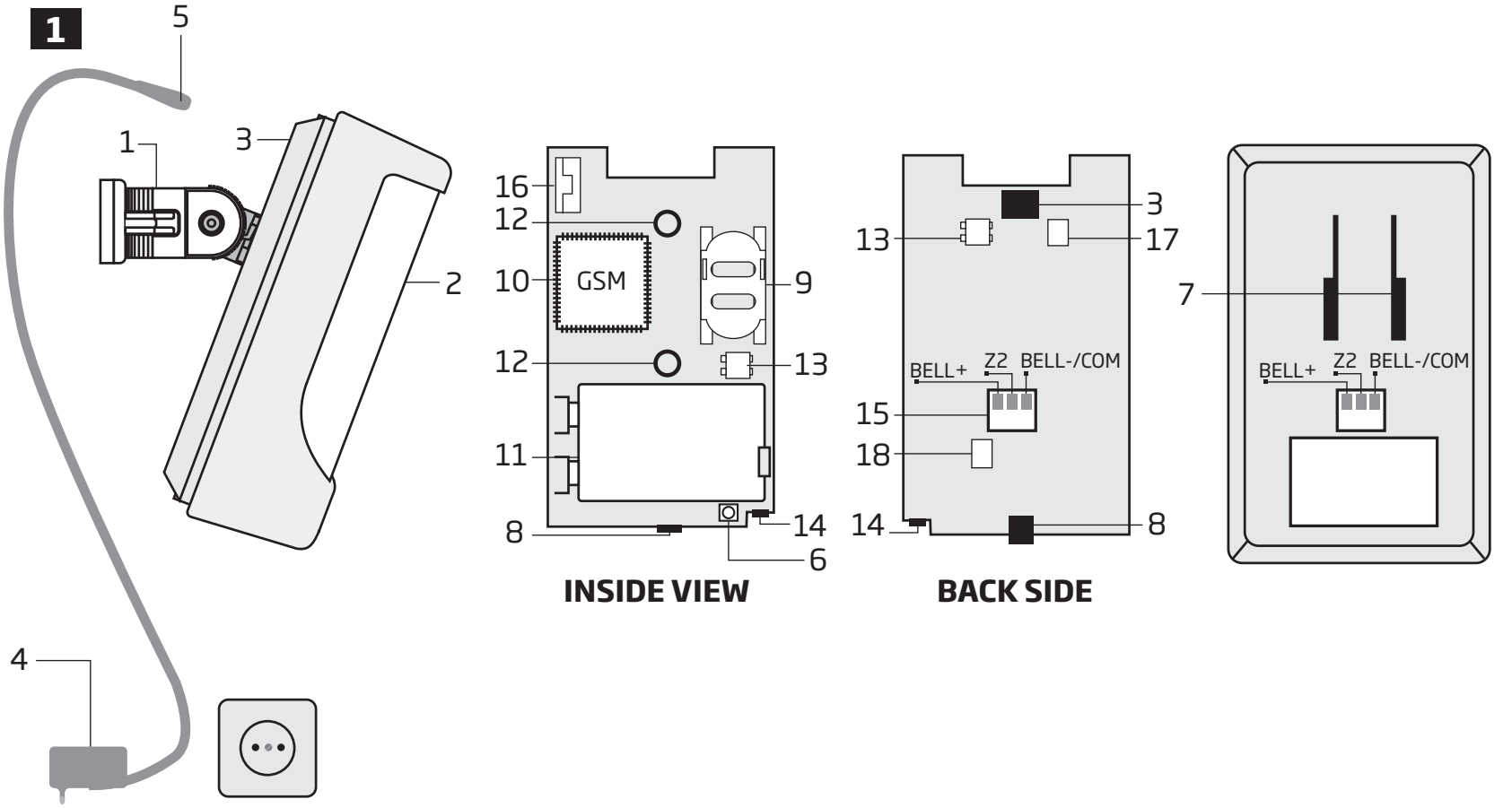
IMPORTANT Please read the user manual before operating the system. The user manual will show you how to install and operate the EPIR3 alarm security system safely and easily. You'll find a quick start guide in section 1 and 2. To learn how to take advantage of additional functions, see sections 3, 4, 5 and 7.

Technical Specifications

Supply voltage	11-15V ⎓ 500mA max
Current used in idle state	up to 50mA
Back-up battery voltage, capacity	8.4V; 250mAh
Back-up battery type	Ni-Mh
GSM modem frequency	850/900/1800/1900 Mhz
Dimensions	124x67x58mm
Operating temperature range	-10...+40 °C
Humidity	0-90% RH @ 0... +40 °C (non-condensing)
Back-up battery operating time	up to 24 hours*
Detection angle	90°
Maximum motion detection range	10 metres
Wireless transmitter-receiver frequency	868 Mhz
Wireless communication range	up to 30m in premises; up to 150m in open areas
Maximum number of wireless devices	16
Communications	SMS, Voice Calls, GPRS Network
Supported protocols	Ademco Contact ID, EGR100, Kronos, Cortex SMS
BELL+: siren output commuted values	Current - 150mA max.; voltage - 15V (EPIR3 on external power supply) / 7V (EPIR3 on back-up battery)

* - with Smart Security disabled; with wireless transmitter-receiver module disabled

Components of the EPIR3 security system



1. EPIR3 holder for fixing on the wall
2. Lens for movement detector and LED
3. Power supply socket to connect to mains electricity
4. Power supply transformer
5. Power supply connection lead
6. Reset button to restore default parameters
7. Holder to fix the unit in place
8. Mini-USB connector to allow programming via your PC
9. Holder for SIM card
10. GSM module
11. Back-up battery in case of mains power supply failure
12. Motion detector to sense possible intruders
13. TAMPER button to alert you if anyone interferes with the unit
14. Microphone to allow you to listen in to an incident using your mobile phone
15. Wired zone for wired sensor & output for siren or indicator connection
16. Built-in GSM antenna
17. Fuse F1 model - MINISMDC050F 0.5A
18. Fuse F2 model - MINISMDC020F 0.2A

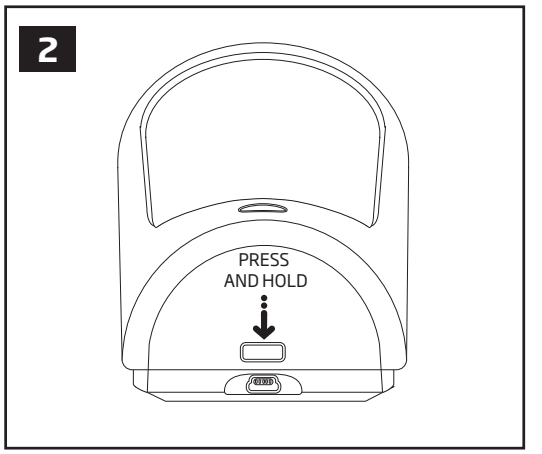
Connector	Description
BELL- / COM	Siren output negative terminal / output terminal / common return terminal
Z2	Security zone terminal
BELL+	Siren output positive terminal

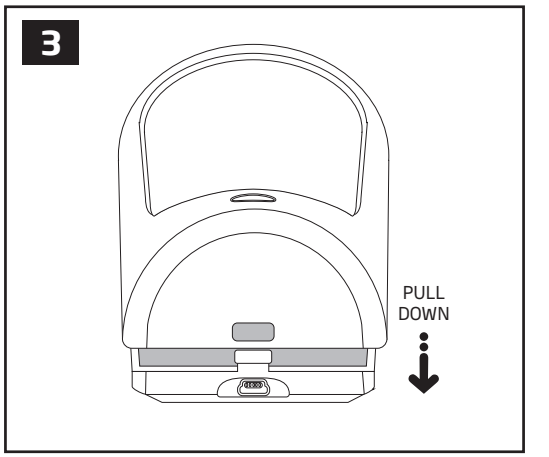
1. 7-STEP START GUIDE

OVERVIEW

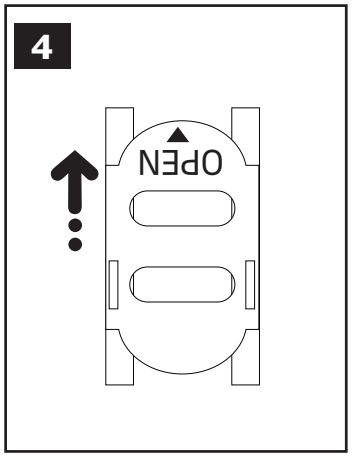
This section tells you how to install the EPIR3 system quickly by following the very basic instructions consisting of only 7 steps. For step-by-step device programing using software, please refer to section **2. QUICK START GUIDE**.

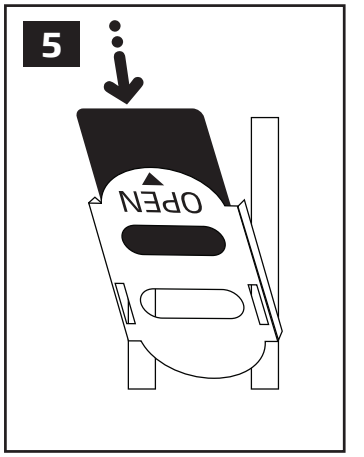
1. Remove the front cover of the device.

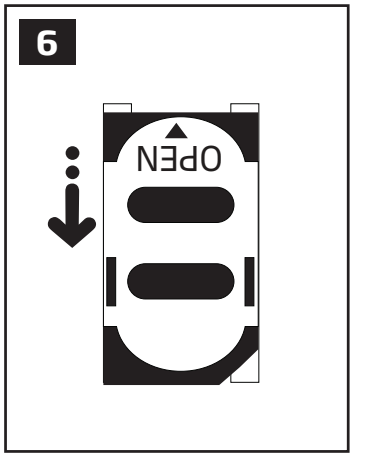




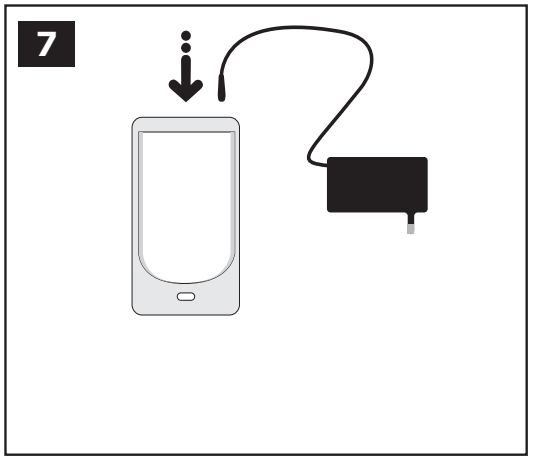
2. Open the SIM card holder by first sliding the the cover to the right then hinging it upwards. Then insert the SIM card with disabled PIN code request into the holder. Ensure that gold contacts are face down when SIM card cover is flipped back down and slide the SIM card cover back to lock SIM card in place.

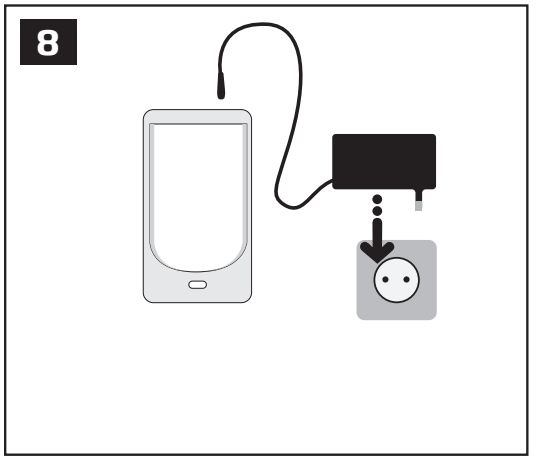






3. Plug the power supply connector into the device and insert the plug into the mains socket





4. Wait for 1 minute for the device to start up. Then using your mobile phone dial the phone number of the SIM card inserted in the device and wait until the phone call is automatically rejected by the device. The device will reply you with SMS text message confirming that your phone number has been successfully stored in the device memory



5. Using your mobile phone type an SMS text message containing the following text: 0000 PSW XXXX (replace **XXXX** with any 4-digit combination).. The result should look something like this: 0000 PSW 2583. Now send this SMS text message to your device's phone number and wait for a reply confirming that the SMS password has been successfully changed.

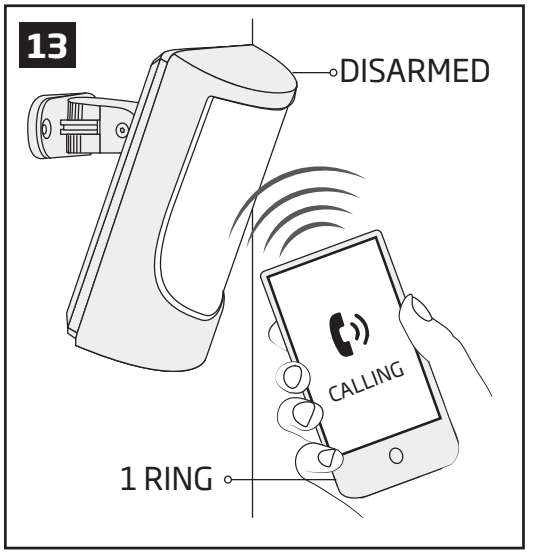


6. Your system is now ready to be armed and disarmed. Before arming the system, ensure that you are not standing in front of the device.



7. To arm your system dial the device SIM card's phone number and wait until it rings three times and then drops the call. This means the system is now successfully armed. To disarm the system, dial the SIM card and wait until it rings once and then drops the call. The system is now successfully disarmed. In both cases be sure to wait until the system automatically drops your call. Again in both cases the user will receive a short SMS text message each time the system is successfully armed or disarmed.





2. QUICK START GUIDE

OVERVIEW

This section tells you how to install the EPIR3 system quickly and easily and covers all the procedures required for full system operation. The alarm system functions via the GSM network, so you will first need to purchase a SIM card so you can 'talk' to and program your device via your mobile phone. Due to the dual element technology of a built-in PIR sensor, the device features the pet immunity against the animals of up to 40 kg weight in order to prevent them from causing false alarms while moving within the secured premises.

How to expand your system with additional wireless devices

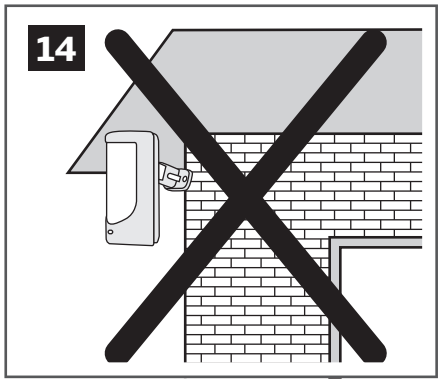
Your EPIR3 system has a built-in wireless module providing expansion capabilities to your system by binding additional ELDES wireless devices to it. However, the EPIR3 system can operate fully without any wireless devices bound to it.

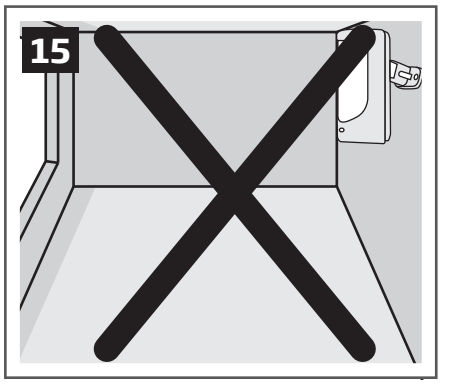
This section does not cover the procedures for adding wireless devices to the system. If you intend to use the wireless devices with your EPIR3 system, follow the instructions for setting up the EPIR3 in this section then refer to section **3: HOW TO MANAGE THE WIRELESS DEVICES.**

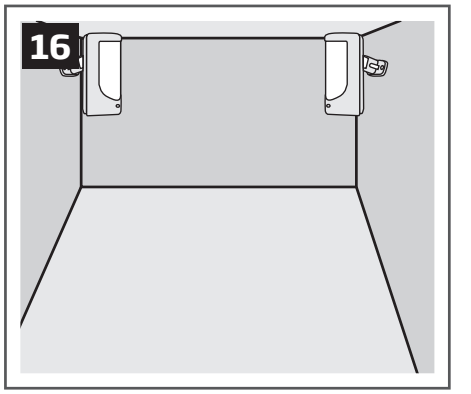
Step-by-step system installation

2.1. How and where to fix the holder to the wall

The system should be installed indoors, **in stationary environment ONLY.** Choose a location where unauthorised entry is most likely.

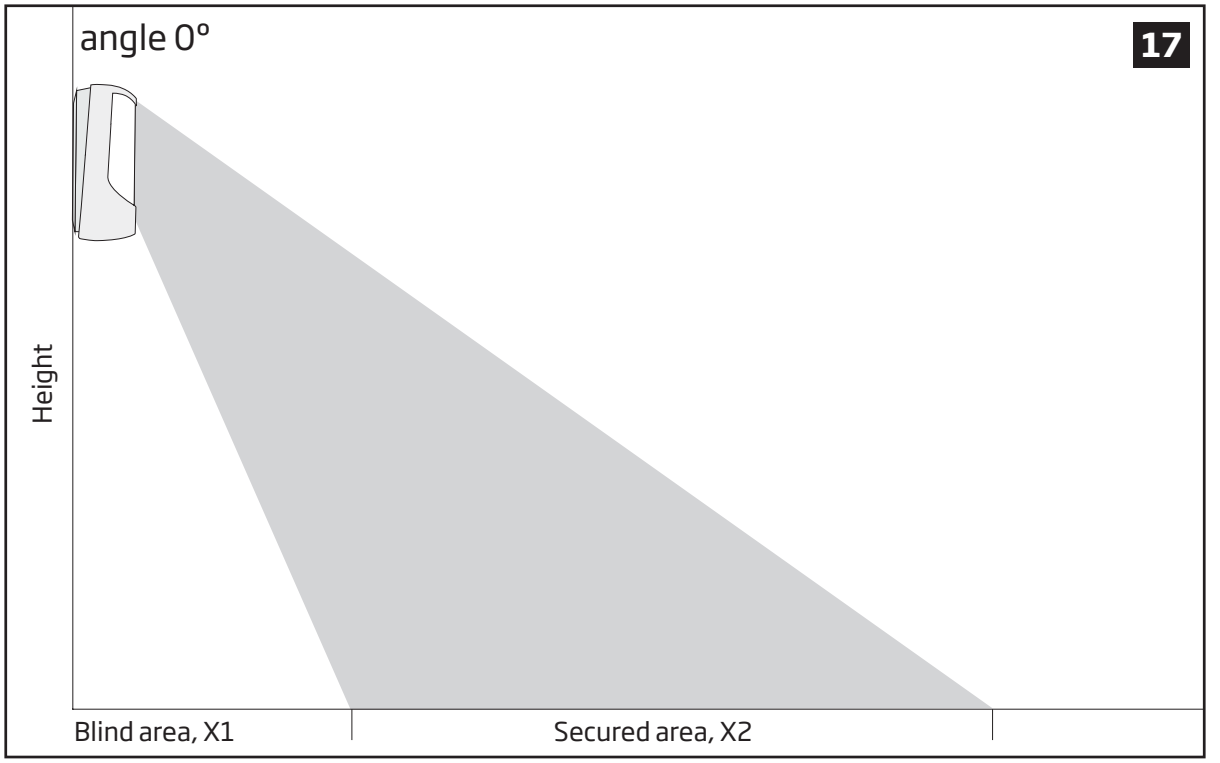




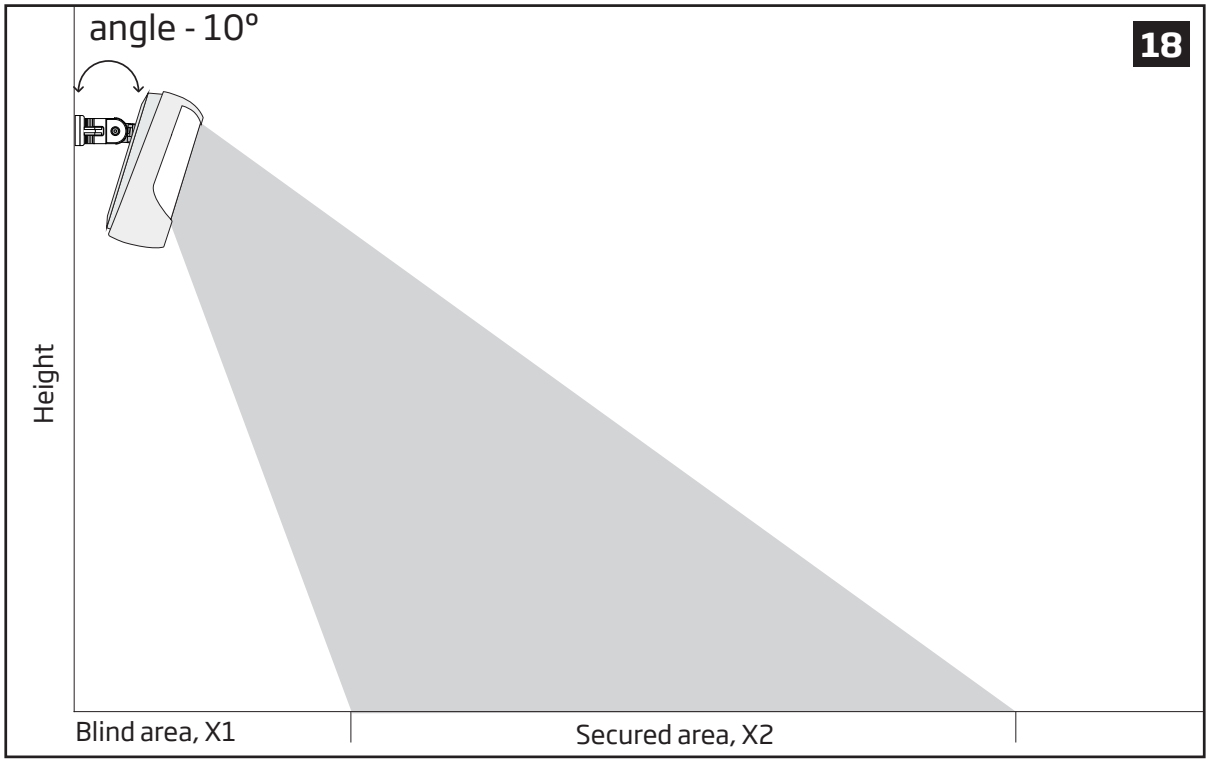


To prevent false alarms, avoid installing the unit in the following locations:

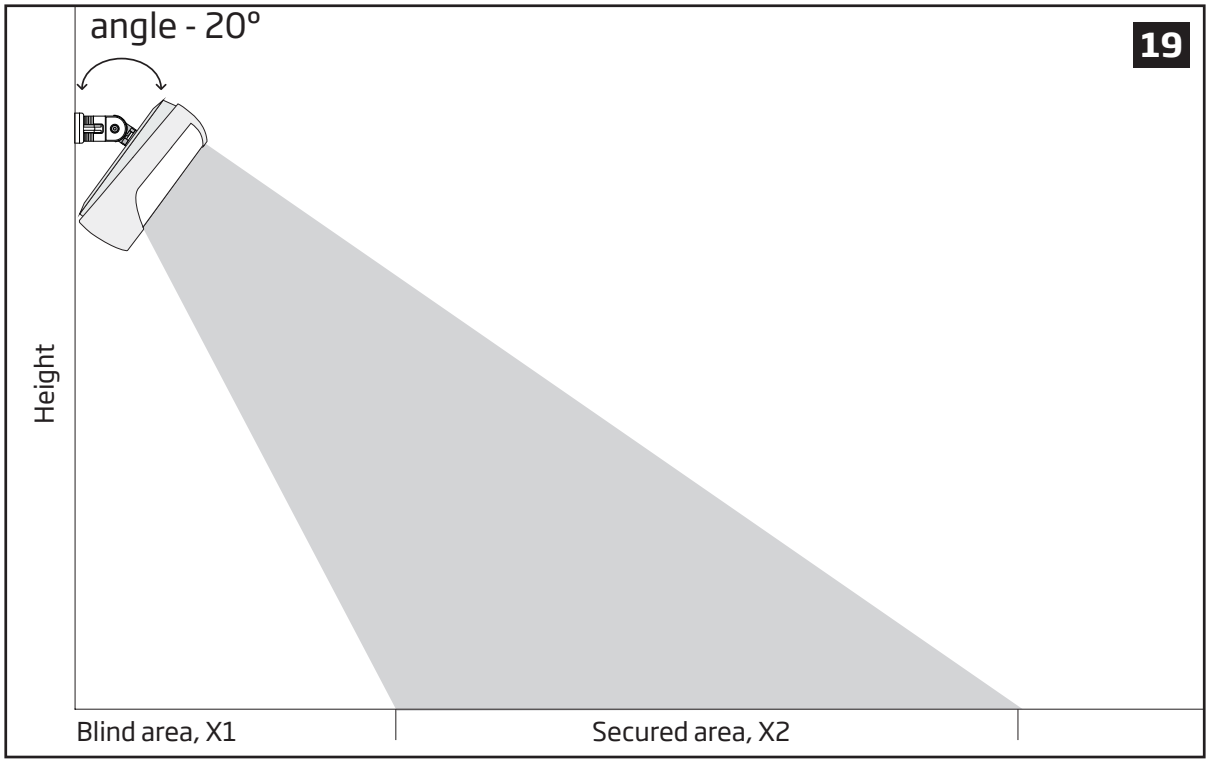
- With the lens facing direct sunshine, for instance in front of windows
- Places with high temperature fluctuations, such as near fireplaces, boilers, ovens etc
- Anywhere with high dust or air flow
- In an area surrounded by metal or thick walls where the GSM connection may be lost



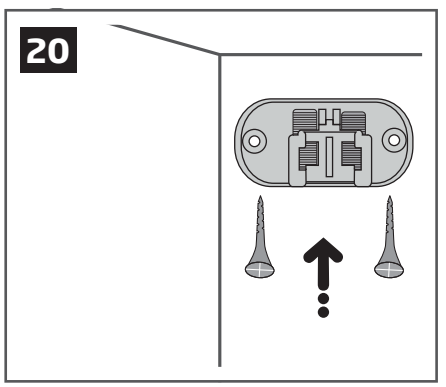
height	X1	X2
2,5 meters	3,5 m	7,5 m
2,3 meters	3 m	8m
2,1 meters	1,5 m	9,5 m
1,5 meters	0 m	11 m



height	X1	X2
2,5 meters	2 m	3 m
2,3 meters	1,5 m	3 m
2,1 meters	1 m	3,5 m
1,5 meters	0 m	3 m

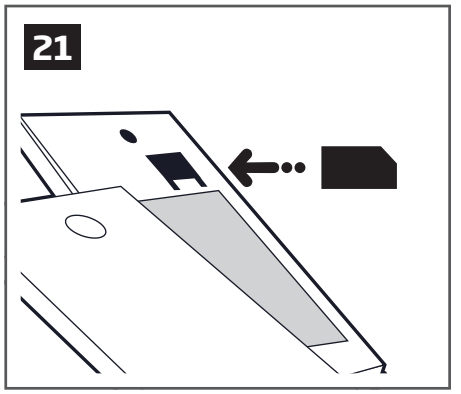


height	X1	X2
2,5 meters	2,5 m	7,5 m
2,3 meters	2,5 m	5,5 m
2,1 meters	1,5 m	6,5 m
1,5 meters	0 m	4,5 m



After a suitable location for your EPIR3 is chosen, fix the holder to the wall using the screws supplied.

2.2. Prepare the SIM card



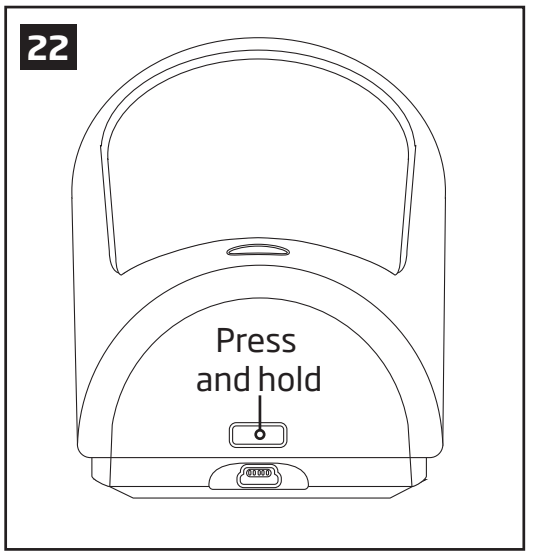
Place the SIM card in your mobile phone and disable the PIN code by following the appropriate menus on your mobile phone. This will help ensure that when you install the SIM card in the EPIR3 it will operate correctly.

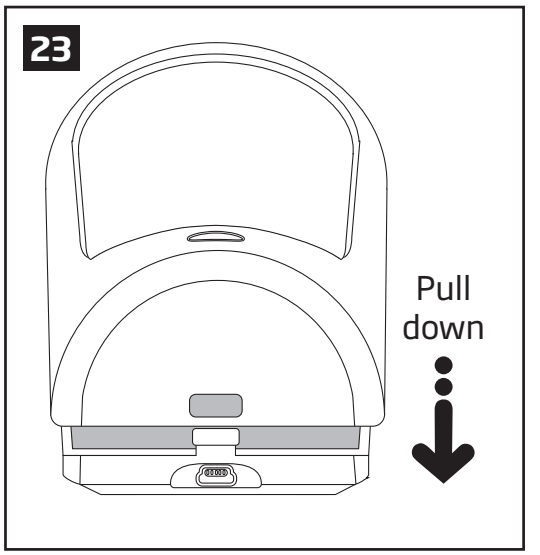
IMPORTANT RECOMMENDATIONS

- We advise you to choose the same GSM SIM provider for your system as for your mobile phone. This will ensure the fastest, most reliable SMS text message delivery service and phone call connection.
- For maximum system reliability we recommend you do NOT use a Pay As You Go SIM card. Otherwise, in the event of insufficient credit balance on the SIM card, the system would fail to make a phone call or send messages.
- We also recommend you to disable **call forwarding, voice mail/text message reports on missed/ busy calls**. Please contact your GSM provider for more details on these services and how to disable them.

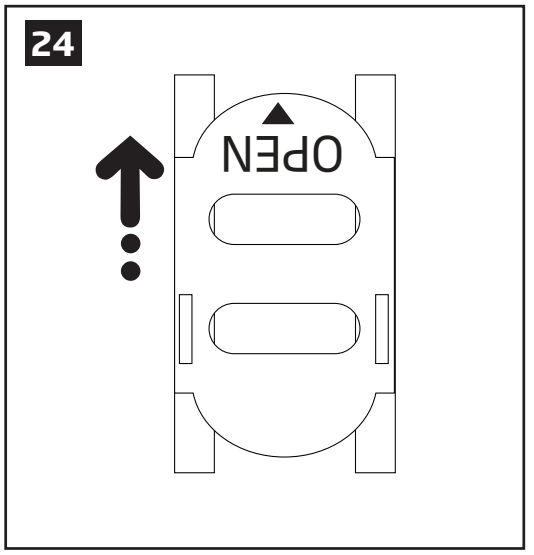
2.3. How to insert the SIM card

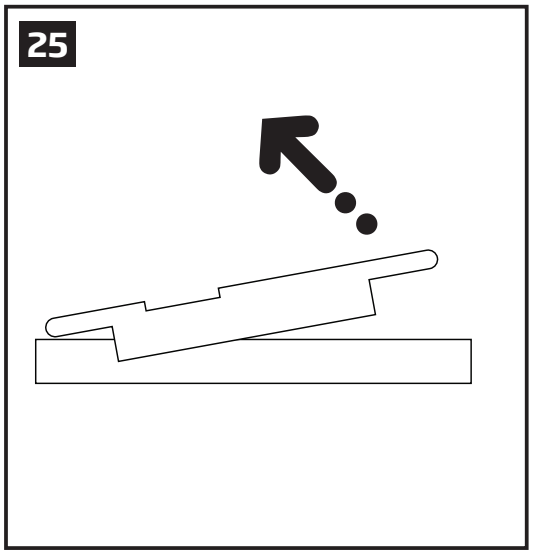
The SIM card must be prepared as described in section **2.2. Prepare the SIM card** before being inserted into the device.



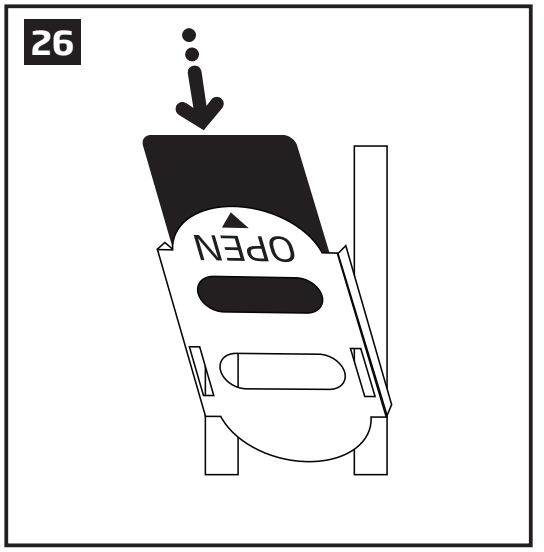


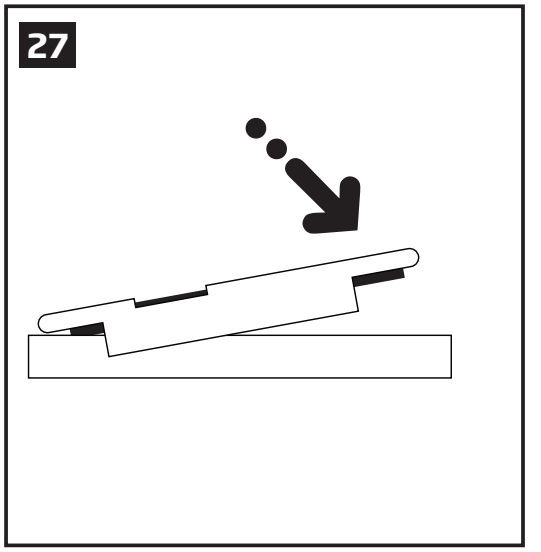
To insert the SIM card, first remove the front cover of the device (containing the detector lens)



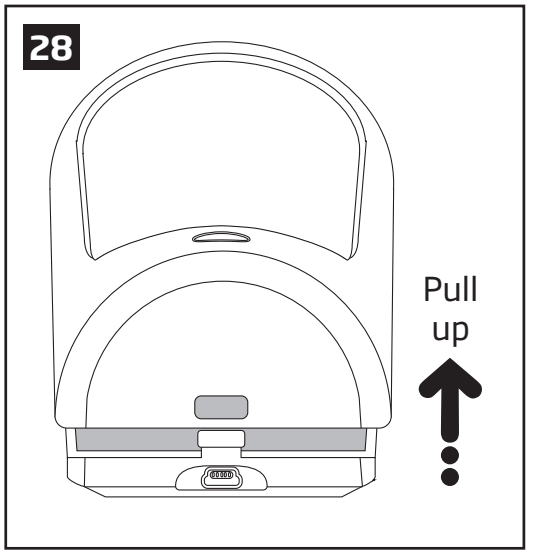


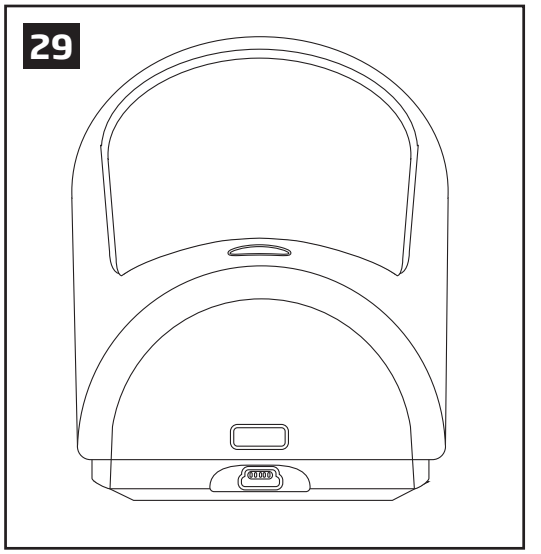
Open the SIM card holder by first sliding the the cover to the right then hinging it upwards.





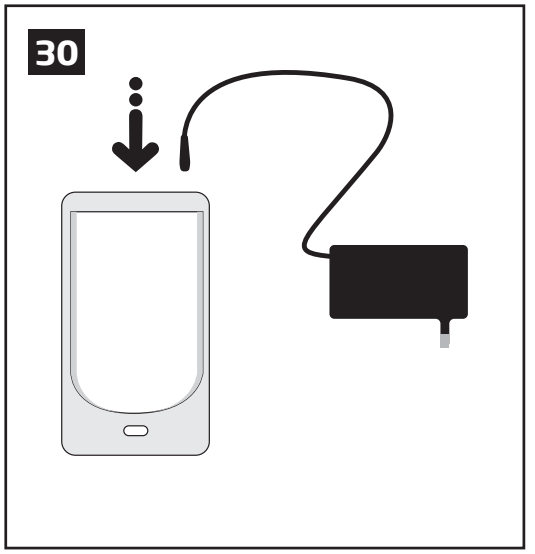
Then insert the SIM card into the holder. Insert SIM card so that gold contacts are face down when SIM card cover is flipped back down.



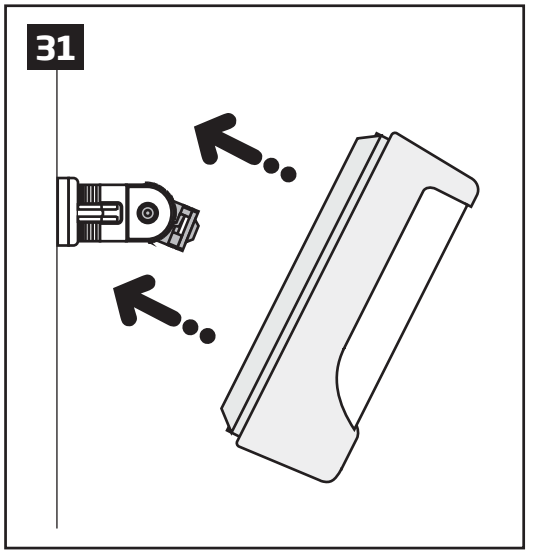


Fit the front cover

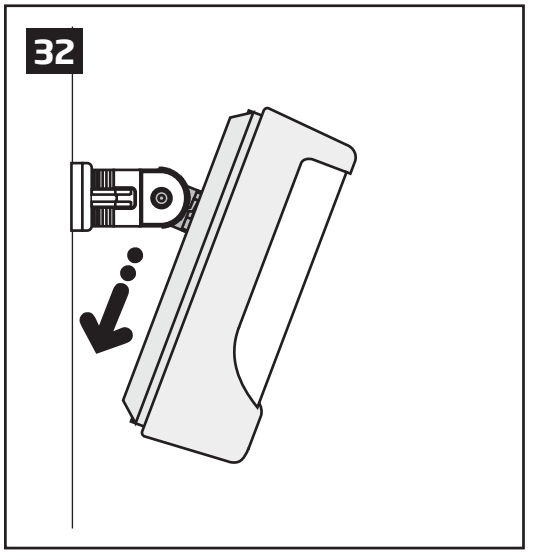
For more information see the diagram of the EPIR3 and the description of components on page <5>.



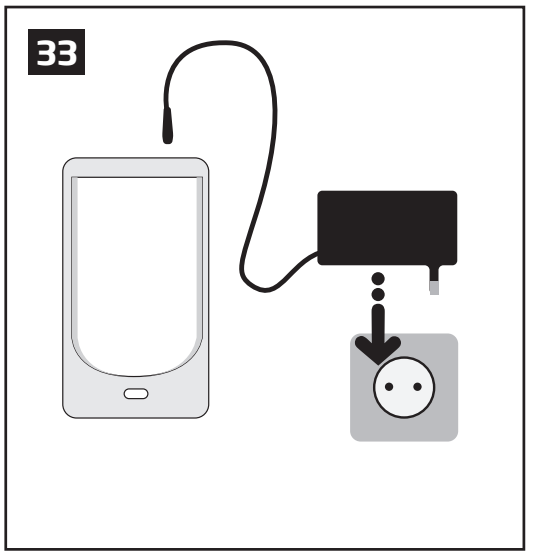
2.4. Plug the power supply connector into the device



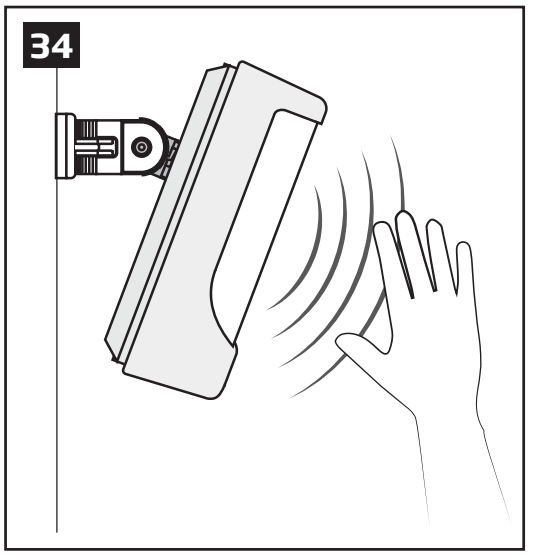
2.5. Place the device into the holder



2.6. Slide the device down to fix it



2.7. Insert the plug into the mains socket



2.8. How to check the detector is working

The system will start in 1 - 2 minutes. To test that the system is working, when the red LED is switched off move your hand in front of the EPIR3 lens. The system will detect the motion and the LED will light up for a few seconds.

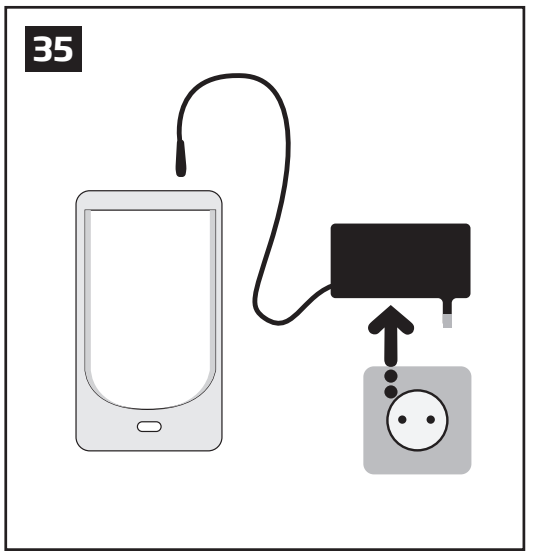
NOTE: Ensure that the device is properly fixed into the holder, otherwise it will prevent from using the back tamper switch for supervision of the enclosure's back side. **For more information** see the diagram of the EPIR3 and the description of components on page <5>.

If the LED indicator blinks fast (a few times a second), the SIM card may not be inserted properly or the PIN code may not have been disabled.

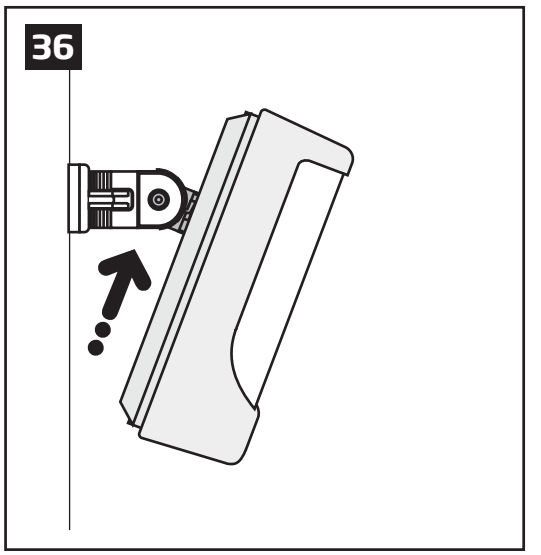
2.9. About the back-up battery and how to replace it

The back-up battery should last for at least two years. Its lifespan will largely depend on the surrounding temperature and the frequency of disruptions to the mains power. During mains failure the battery should power the system for up to twenty-four hours.

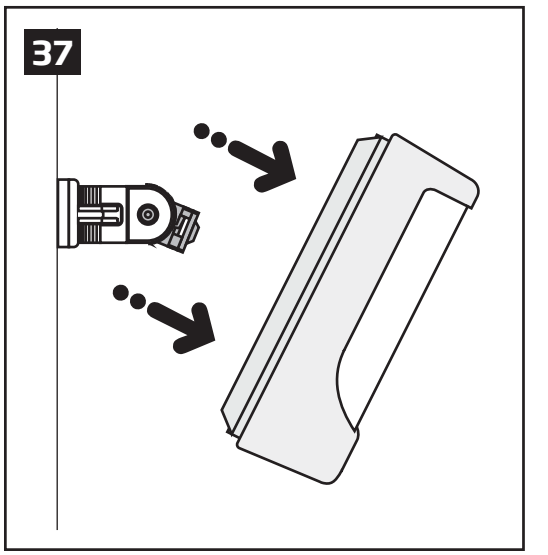
How to replace the battery:



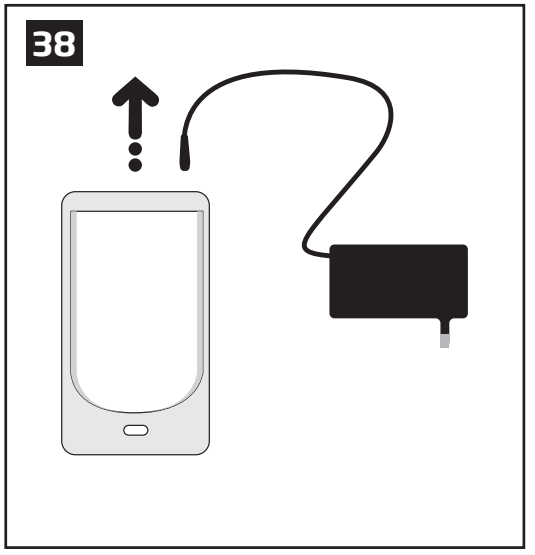
1. Unplug the power supply from the mains electricity socket.



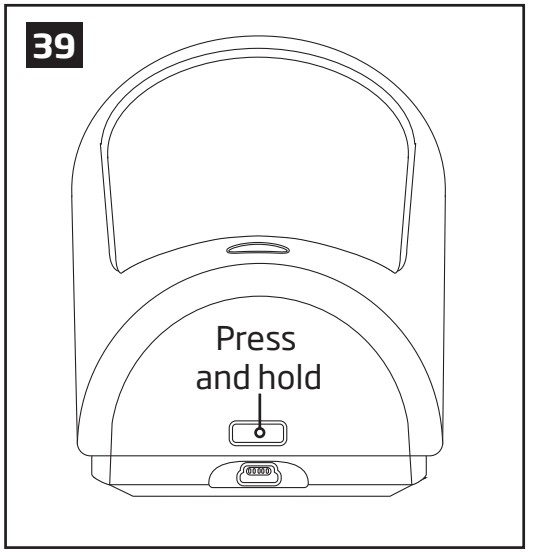
2. Slide the EPIR3 up.

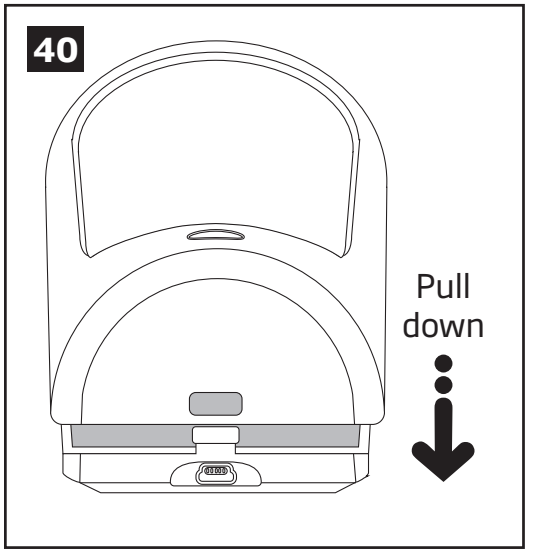


3. Remove the EPIR3 from its holder.

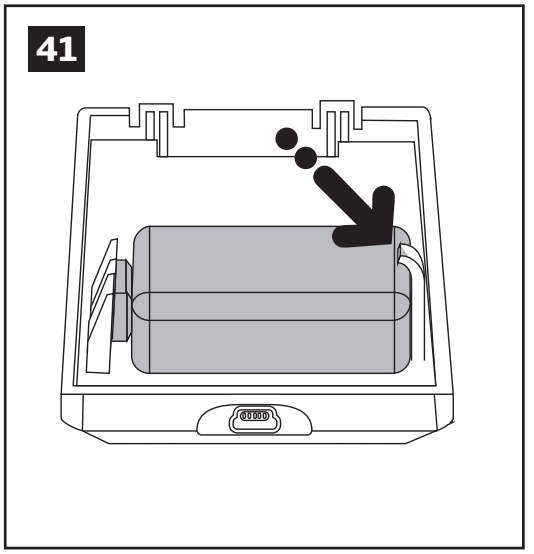


3. Unplug the power supply connector.

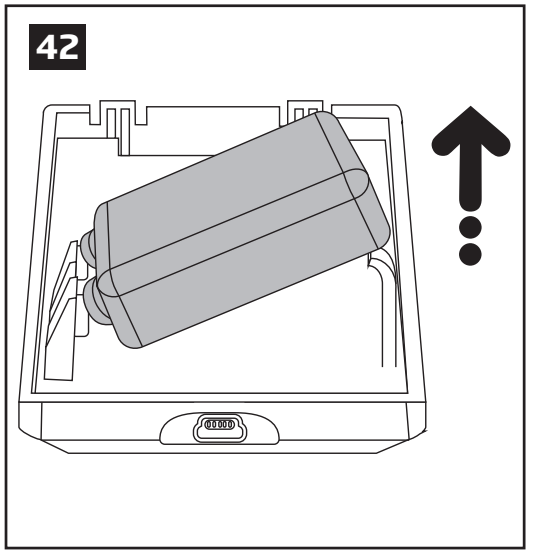




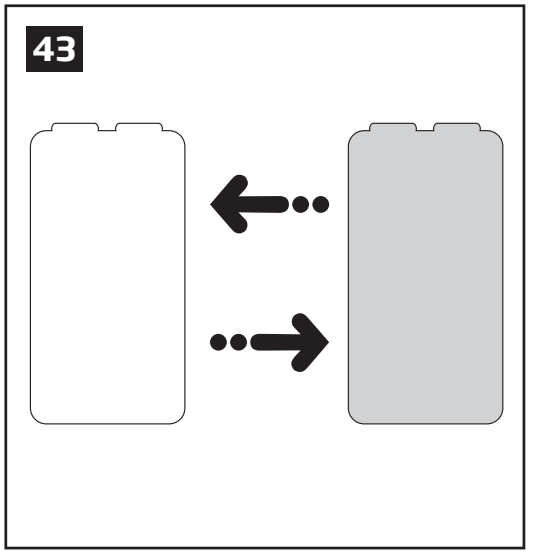
4. Remove the front cover of the device (containing the detector lens)



4. Gently push the plastic battery holder to the right side and hold



5. Pull up the battery



8. Replace the battery with the type specified in the technical specifications.

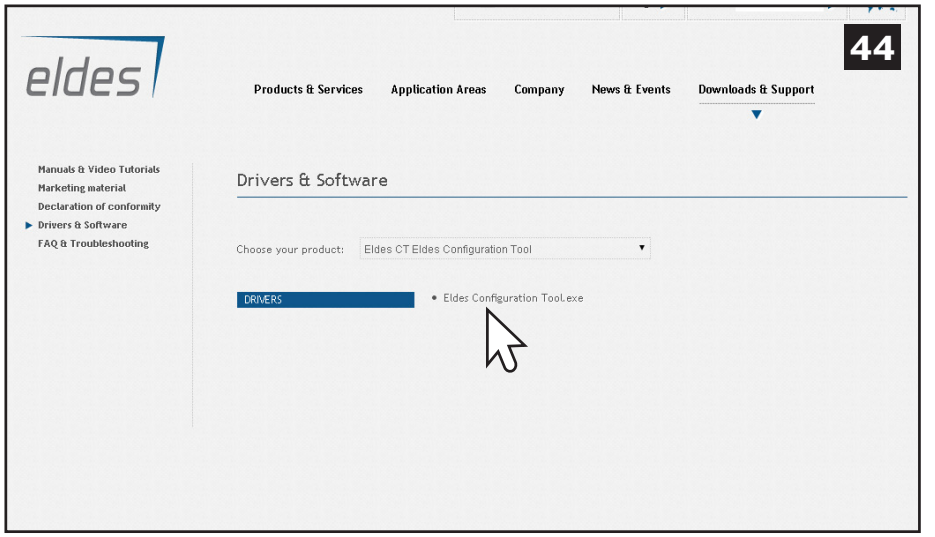
2.10. How to program EPIR3 system

Before you continue, you need to program your EPIR3 system. We recommend that you program the EPIR3 system using your PC and *ELDES Configuration Tool* software as it's the quickest, easiest way and offers more options for your system, such as flexible SMS text message management.

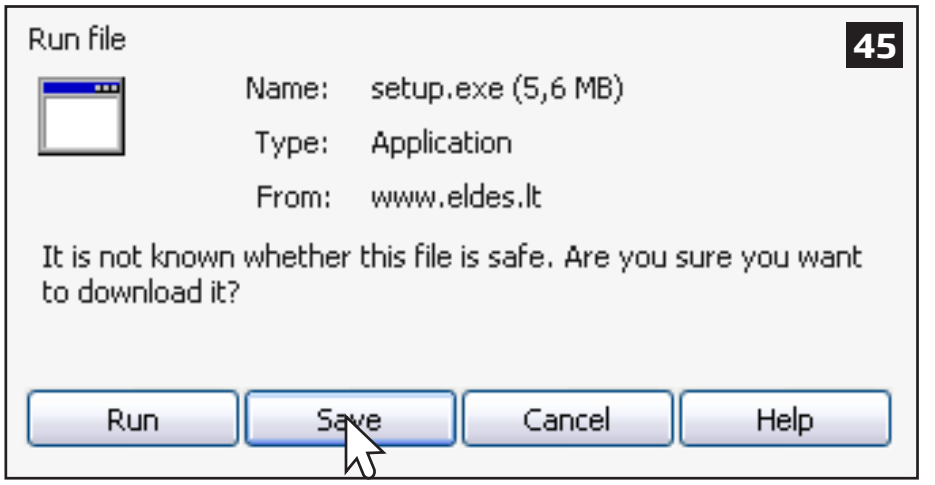
NOTE
If you wish to program the EPIR3 system by SMS text message, please refer to section **4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE**. If not, please proceed to section **2.10.1** ***Download ELDES Configuration Tool software***.

2.10.1. Download *ELDES Configuration Tool* software.

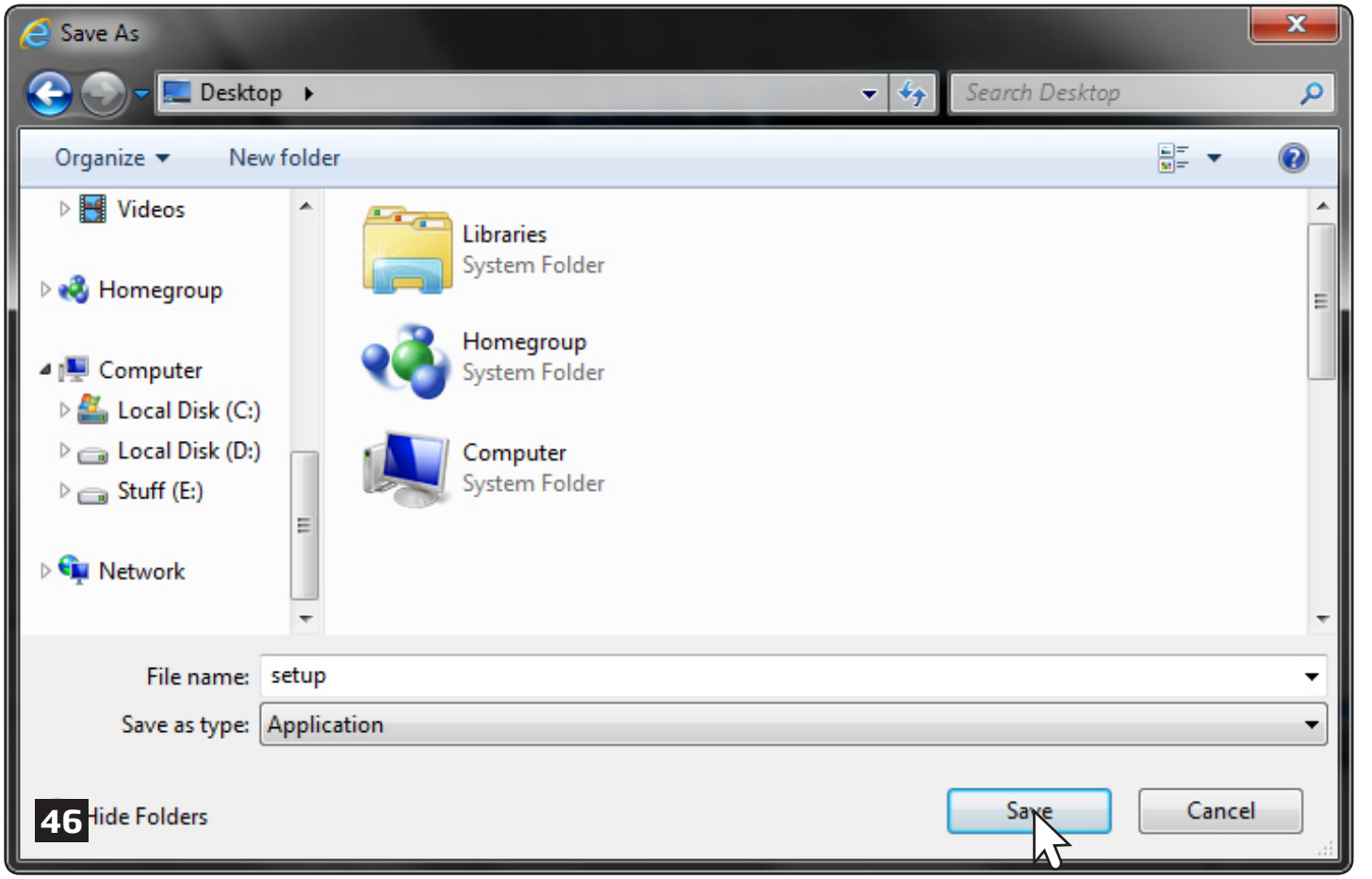
Visit **www.eldes.lt** , you will find a link to the *Configuration Tool* under the menu option **Downloads & Support → Drivers & Software → Eldes CT Eldes Configuration Tool**



Once you are at *Configuration Tool* section, left-click on the *ELDES Configuration Tool v3.x.xx (setup.exe)*.



In the newly popped-up window left-click on the Save button.

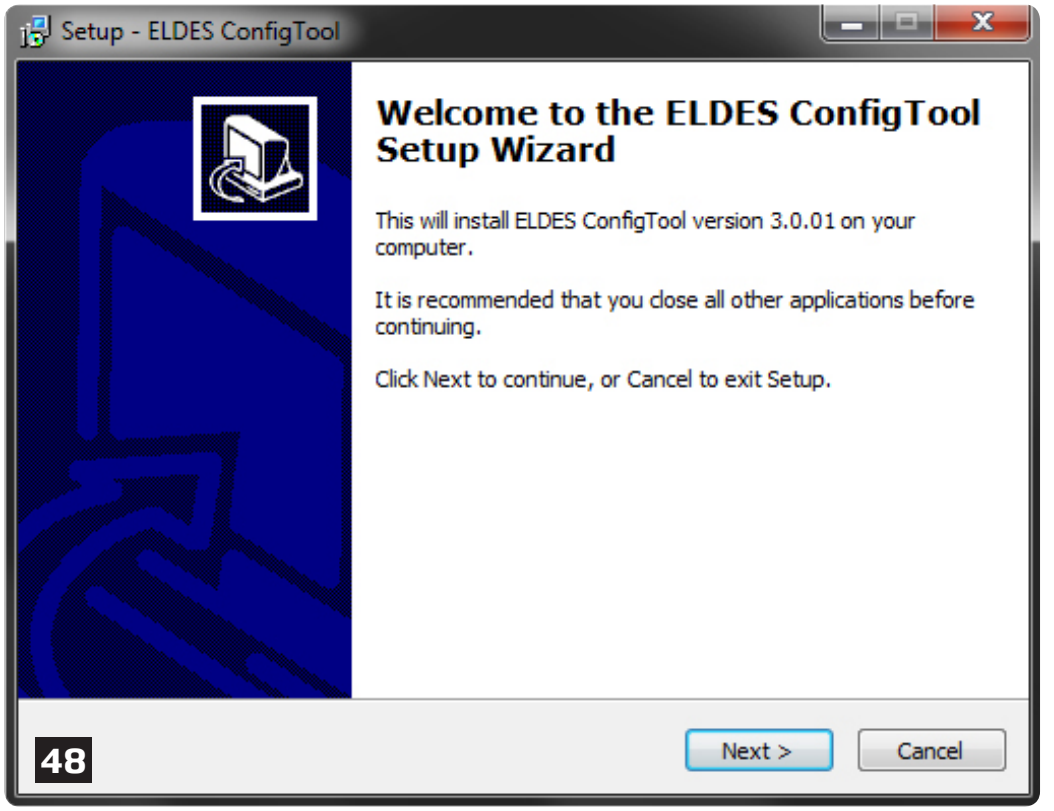


Specify a location for *setup* file and left-click on the *Save* button.
We recommend placing the file on your desktop.

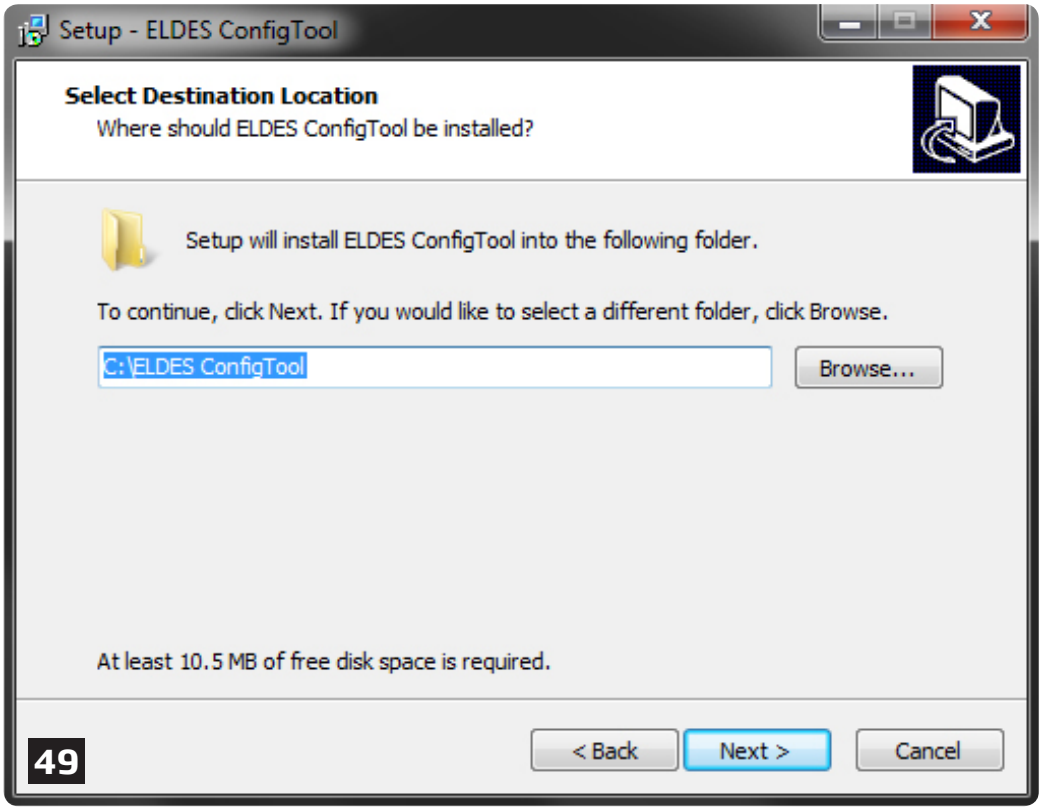
2.10.2. install ELDES Configuration Tool software.



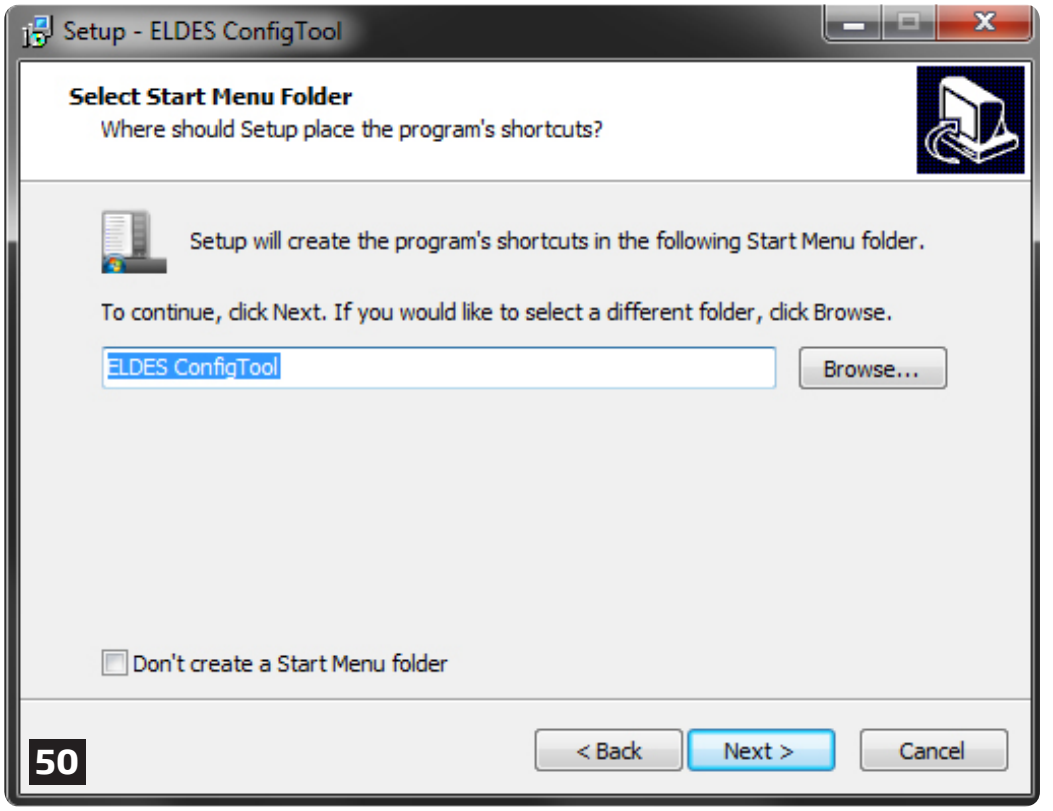
Double left-click on the downloaded setup file to run it.



In the newly popped-up window left-click on the *Next* button to continue.

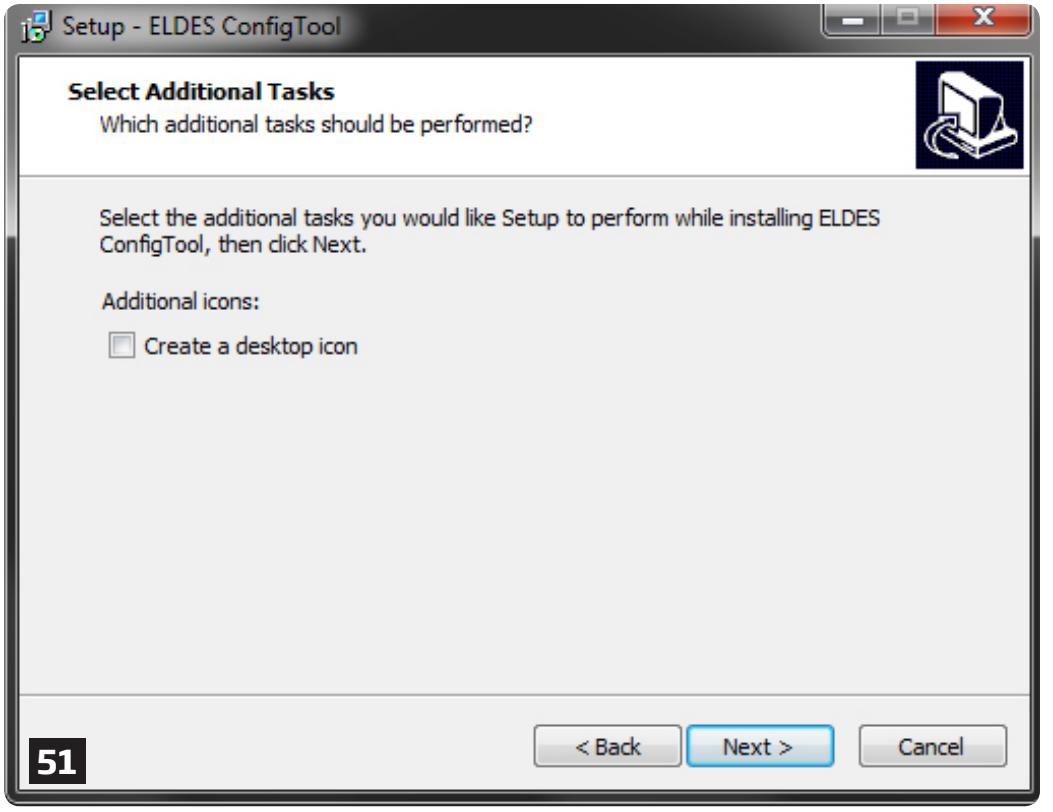


In the next window left-click on the *Next* button to continue.



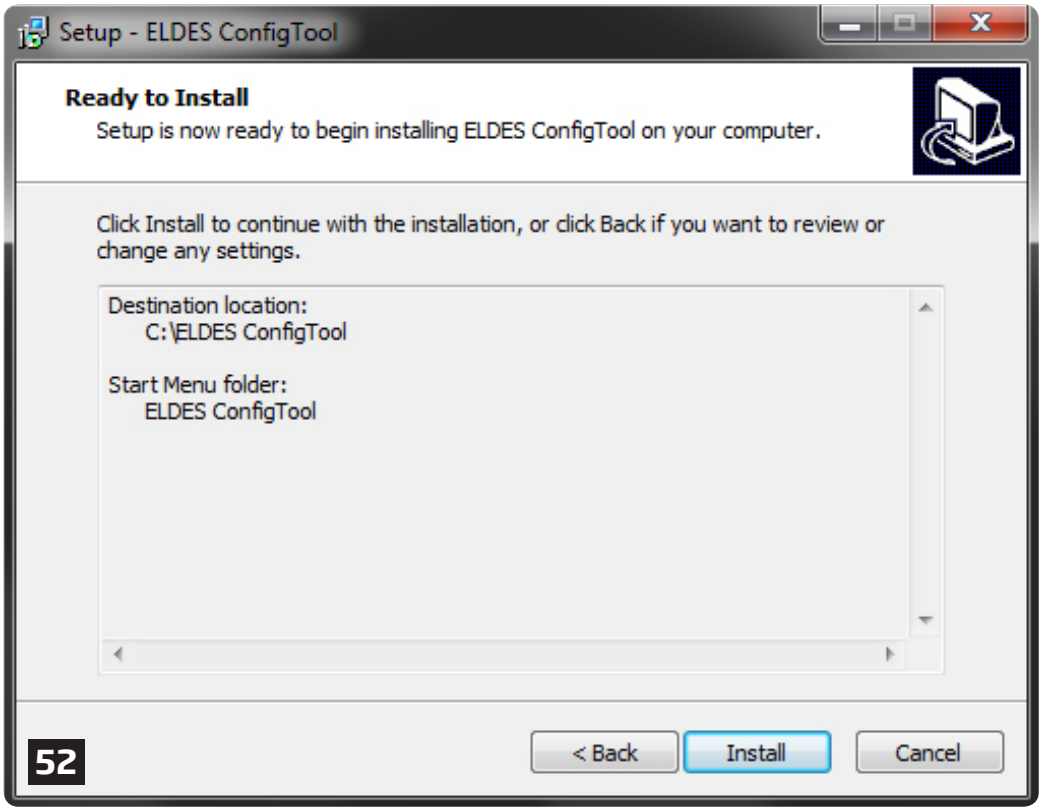
50

In the following window left-click on the *Next* button to continue.

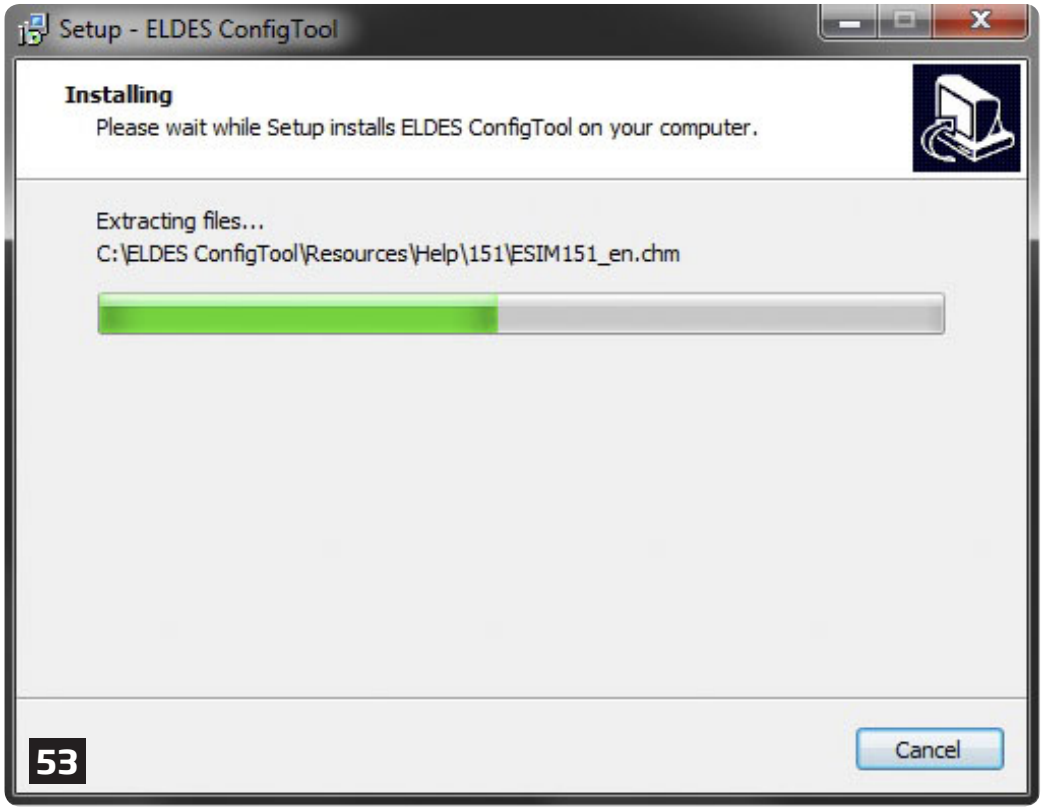


51

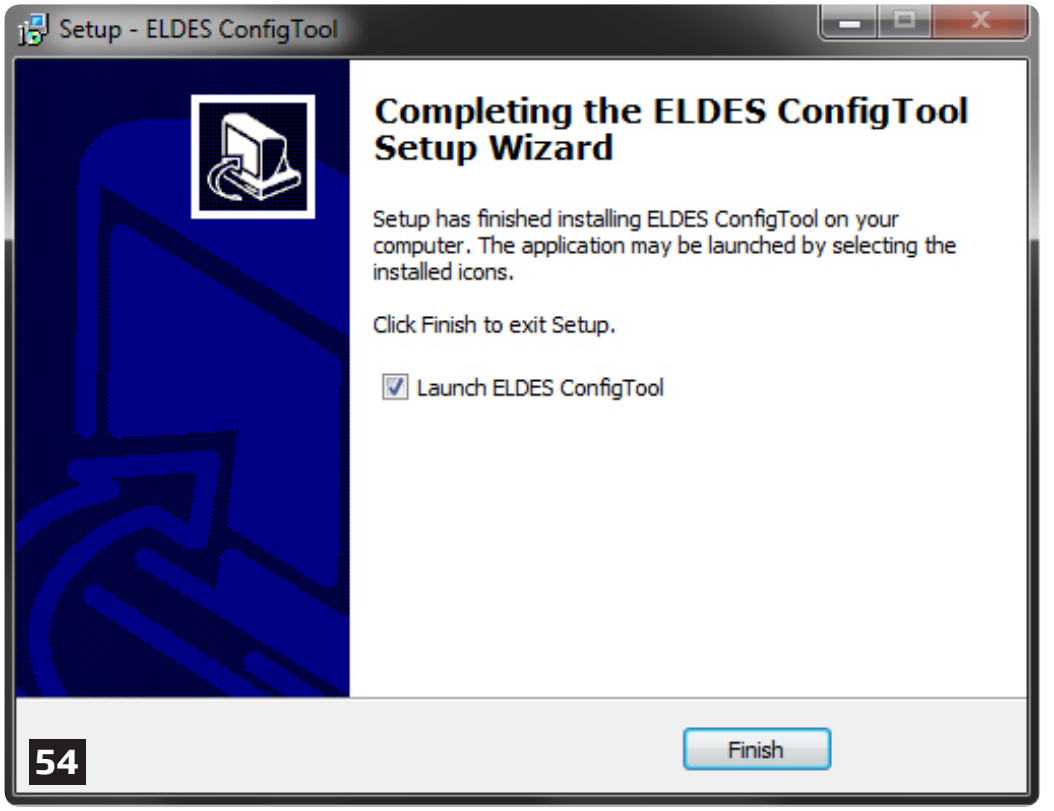
In the next window left-click on the *Next* button to continue.



In the following window left-click on the *Install* button to begin the installation process.



Wait for the installation progress to complete and do not click on any button.

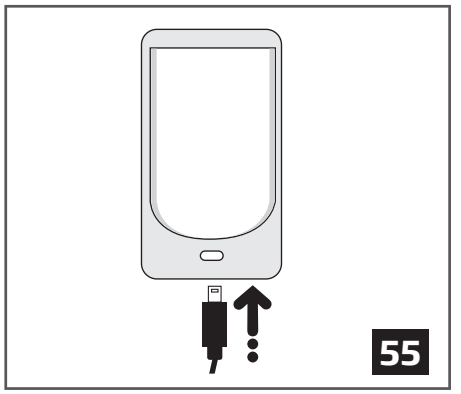


After the successful installation, the following window will pop-up. Left-click on the *Finish* button in order to end the installation and launch *ELDES Configuration Tool* software after-wards.

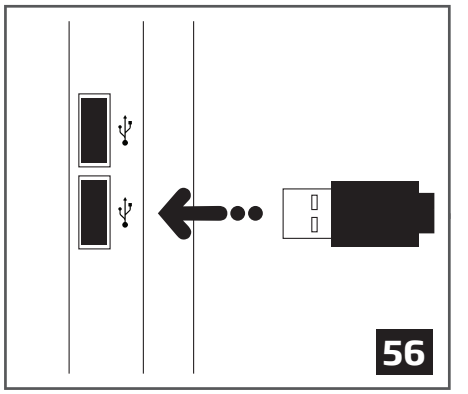
NOTE: You do not have to repeat the installation process the next time when you want to run ELDES Configuration Tool software again.

2.10.3. Connect EPIR3 to your PC via the USB cable

IMPORTANT: Before connecting EPIR3 to your PC via the USB cable, first ensure the EPIR3 is powered up.



Plug the miniUSB connector into EPIR3.



Plug the USB connector into your PC.

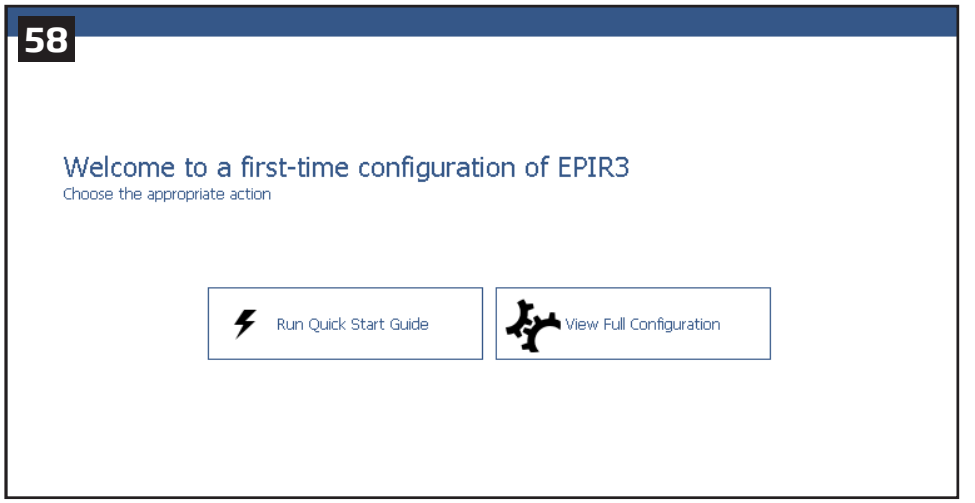
2.10.4. Run *ELDES Configuration Tool* software.

57



Run the software anytime you want by double left-clicking on the *ELDES ConfigTool* shortcut located on the desktop.

58



On successful first-time connection, a *Welcome to first-time configuration of EPIR3* window will show up. Left-click on the *Run Quick Start Guide* button and follow the step-by-step instructions to program the EPIR3 system. After completing all steps, your system will be ready for use.

2.11. How to arm and disarm the system

To arm your system dial the SIM card and wait until it rings three times and then drops the call. This means the system is now successfully armed.

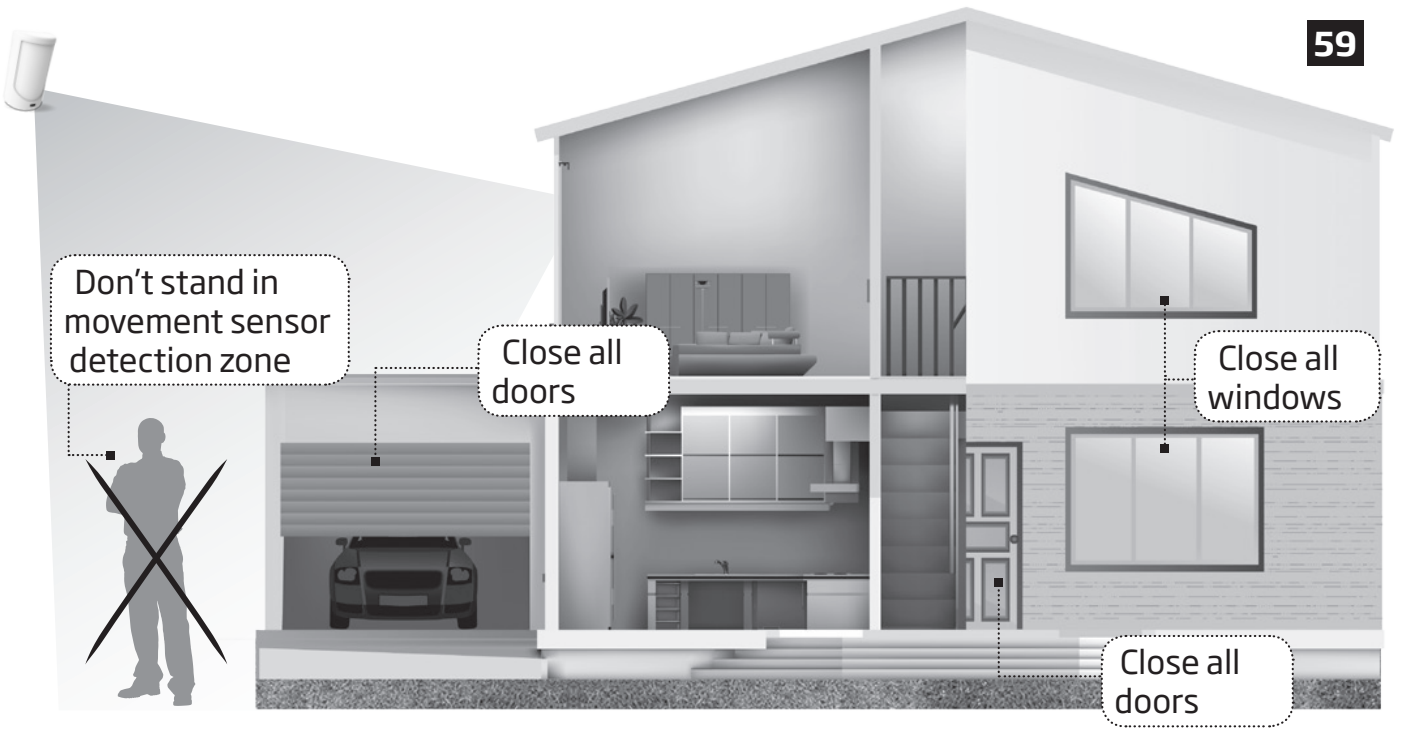
To disarm the system, dial the SIM card and wait until it rings once and then drops the call. The system is now successfully disarmed.

In both cases be sure to wait until the system automatically drops your call. Again in both cases the user will receive a short SMS text message each time the system is successfully armed or disarmed.

IMPORTANT: Dialing the SIM card is free of charge as the system drops your call in both cases.

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

Alternatively, you can arm/disarm your EPIR3 system by sending an SMS text message (see section **4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE**) as well as using a wireless keypad EKB3W (see section **3.3.3. How to arm the system by EKB3W** and **3.3.4. How to disarm & turn off alarm by EKB3W**) or a wireless keyfob EWK1/EWK2 (see section **3.4.1. How to arm the system by EWK1 or EWK2** and **3.4.2 How to disarm & turn off alarm by EWK1 or EWK2**).



2.12. A 15 second delay allows you to leave the premises

When you arm the system via your phone, a keyfob or a keypad, the system will give you a 15 second delay before it activates, giving you time to leaving the premises. You can change the time delay at any time (see *ELDES Configuration Tool* software's *Help* section).

The red LED on the detector lens will start to blink, indicating the time delay is in operation and you must leave room. The red light will go off after 15 seconds when the system will be armed.

2.13. Receiving an alarm call

When the detector is armed and motion is detected in the room, the system will send a SMS text message to *User 1* and then ring the user until the call is answered. If the call is not answered after several rings (predetermined by your mobile phone operator) the system will hang up. If the call is not picked up by *User 1*, the system will ring all the pre-programmed numbers in order of priority starting with *User 2* until a user picks up or the call expires. If the first user is "busy" or "out of radio coverage", the system will also ring the next pre-programmed number. When a call is answered, the system will activate the remote microphone so you can listen to what is happening

in the building.

You can also program the system to send an SMS text message to all users (see *ELDES Configuration Tool* software's *Help* section).

NOTE: Due to the dual element technology of a built-in PIR sensor, the device features the pet immunity against the animals of up to 40 kg weight in order to prevent them from causing false alarms while moving within the secured premises.

2.14. In case of mains power failure

The system will automatically switch to the back-up battery supply in case of mains power failure. At this time you will receive an SMS text message warning message after 2 minutes. When the mains power has been restored you will also receive an SMS text message after 2 minutes. Likewise the system will warn you by when the back-up battery is getting low, just before the system is switched off.

2.15. Receiving an SMS text message when temperature exceeds the set values

The system comes equipped with a feature intended for temperature measurement in the surrounding area. This feature allows to monitor the temperature and receive a notification by SMS text message, identified as the Temperature Info SMS, to user phone number when the set temperature MIN or MAX boundaries are exceeded. For this purpose you may use the system's built-in temperature sensor or one of the temperature sensors incorporated in the wireless device (if any). The following wireless devices contain a built-in temperature sensor:

ATTENTION: The supported temperature range is -10... +40 °C.

- EWP1 & EWP2 - wireless PIR sensors (motion detectors);
- EWS1 & EWS3 - internal sirens;
- EWS2 - external sirens;
- EWF1 – wireless smoke detectors;
- EW2 - wireless zone and PGM output expansion module;
- EWD2 - magnetic door contacts/shock sensors/flood sensors

By default, temperature measurement feature is disabled. To enable it, please refer to *ELDES Configuration Tool* software. To set the MIN and MAX temperature boundaries, please refer to section **4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE** or *ELDES Configuration Tool* software.

2.16. Additional capabilities

You can also use your mobile to request information about the system, the power supply and the network quality. Plus you can listen in to what's happening in the secured location through a remote microphone. See section 3 for more details.

EPIR3 system comes equipped with built-in wireless module allowing to enhance your security system with the addition ELDES wireless PIRs (Passive Infrared Sensors), sirens, magnetic door and window sensors or expansion modules. See section **3. HOW TO MANAGE THE WIRELESS DEVICES** for more details.

3. HOW TO MANAGE THE WIRELESS DEVICES

IMPORTANT: Before you continue, first follow the entire section **2. QUICK START GUIDE** and prepare the system for use as described.

OVERVIEW

Your EPIR3 has a built-in wireless module. This section tells you how to bind and remove a wireless device using your PC and *ELDES Configuration Tool* as well as briefly describing every available wireless device which can operate together with your EPIR3 system.

It is possible to connect up to 16 wireless devices to the EPIR3 system. This includes the following:

- EWP1 & EWP2 - wireless PIR sensors (motion detectors);
- EWD1 - magnetic door contacts;
- EWD2 - magnetic door contacts/shock sensors/flood sensors
- EWS1 & EWS3 - internal sirens;
- EWS2 - external sirens;
- EWK1 & EWK2 - wireless keyfobs to arm and disarm the system without using a mobile phone;
- EKB3W – wireless keypads to arm,disarm and configure the system without using a mobilephone;
- EWF1 – wireless smoke detectors;
- EW2 - wireless zone and PGM output expansion module;
- EWR2 - wireless signal repeater

You can also attach more devices which are not part of the ELDES wireless range by using expansion module EW1 with 2 inputs and 2 programmable outputs

Main features of built-in wireless module:

- Up to 16 ELDES wireless devices per one EPIR3 unit;
- Two-way wireless communication;
- Supervised communication link with configurable self-test period;
- Maximum wireless connection range is 150 meters in open areas, within a building wireless range will be up to 30m, depending on building construction.

The wireless devices can operate at a range of up to 30 meters from the alarm system unit while inside the building and at up to 150 meters range in open areas. The wireless connection is two-way and operates in one of four available channels at 868 Mhz non-licensed frequency range. The communication link between the wireless device and the alarm system is constantly supervised by a configurable self-test period, identified as Test Time. For more details on how to install the wireless devices, please refer to **RADIO SYSTEM INSTALLATION AND SIGNAL PENETRATION** manual located at www.eldes.lt/download

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

EKB3W, EW2, EWP1, EWP2, EWS1, EWS2, EWS3, EWF1:

- First 36 attempts after the device startup (reset) - every 10 seconds.
- The rest of attempts - every 1 minute.

EWD1, EWD2:

- First 360 attempts after the device startup (reset) - every 10 seconds.
- The rest of attempts - every 2 minutes.

Once the wireless device is bound, it will attempt to exchange data with EPIR3 system. Due to battery saving reasons, all ELDES wireless devices operate in sleep mode. The data exchange will occur instantly if the wireless device is triggered (zone alarm or tamper alarm) or periodically when the wireless device wakes up to transmit the supervision signal, identified as Test Time, to the system as well as to accept the queued up command (if any) from the system. **Example:** *The alarm occurred at 09:15:25 and the system queued up the command for EWS2 siren to start sounding. By default, Test Time value of EWS2 siren is 7 seconds, therefore EWS2 siren will sound at 09:15:32.*

By default, the Test Time period is as follows:

- EKB3W, EWD1: every 60 seconds.
- EW2, EWP1, EWP2, EWF1, EWD2: every 30 seconds.
- EWS1, EWS2, EWS3: every 7 seconds.

To set a different Test Time value, please refer to *ELDES Configuration Tool* software.

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

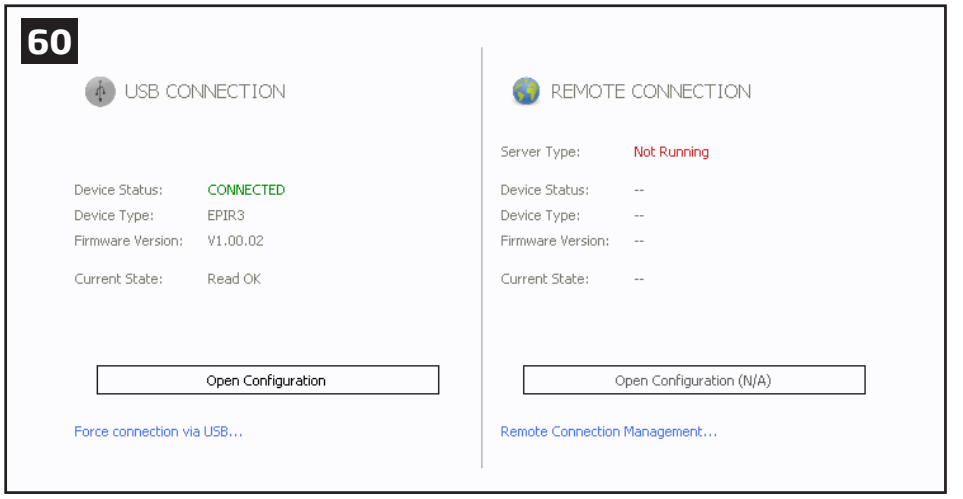
NOTE FOR EKB3W: In comparison with other ELDES wireless devices, EKB3W keypad features some exceptions regarding the wireless communication. For more details on EKB3W keypad wireless communication and back-light timeout, please refer to section **3.3.1. Sleep mode, how to wake up EKB3W and view system alarms or faults**.

3.1. How to bind a wireless device to the system

IMPORTANT: Before you continue, first ensure the EPIR3 is powered up and connected to your PC via the USB cable.

1. Turn on the wireless device by following the instructions provided in the user manual of the wireless device.

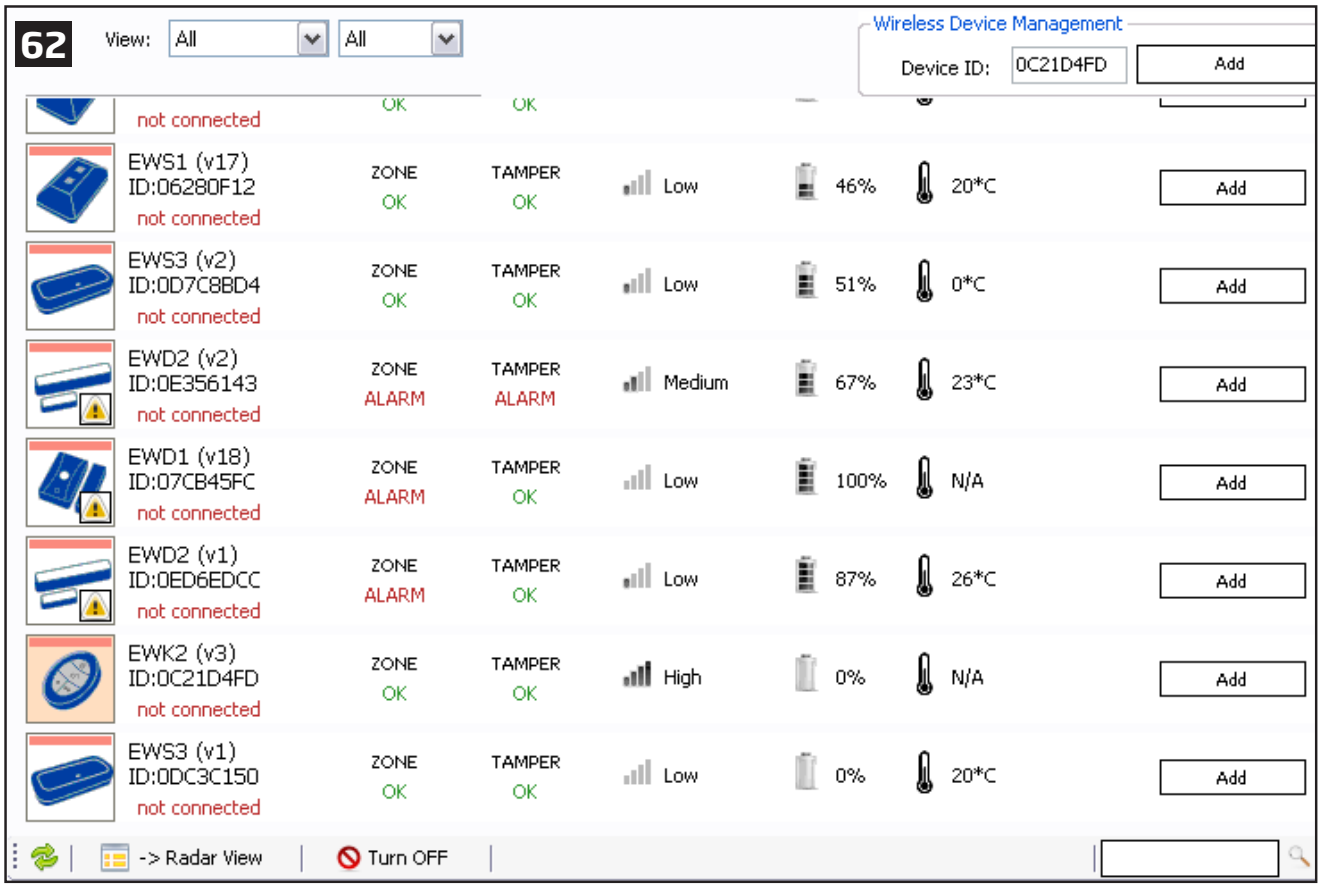
2. Run *ELDES Configuration Tool* software and left-click on the *USB CONNECTION / Open Configuration button*.



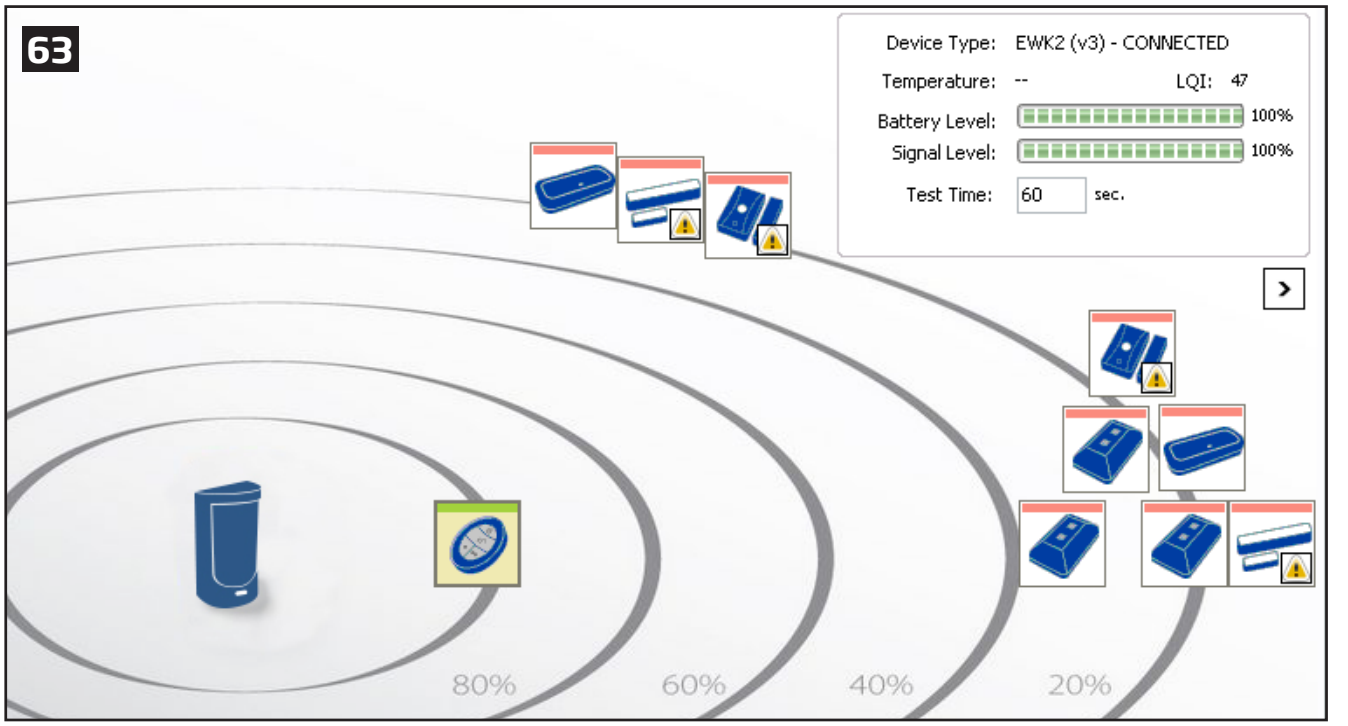
3. Open *Wireless Device Management* section and click on the **Turn ON** button in order to activate the system's wireless transmitter-receiver.



By default, this section uses a list view to show ELDES wireless devices visible to EPIR3 within its wireless signal range



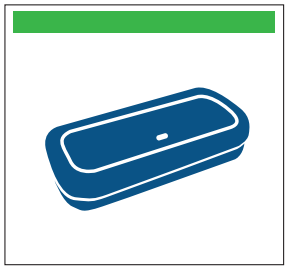
Alternatively, you can switch to radar view by clicking on the *Radar View* button.



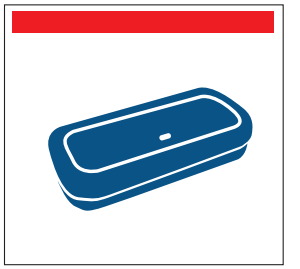
4. **List view:** Left-click on the *Add* button located next to the unbound wireless device icon (red stripe above the icon).



Unbound devices are indicated by a device icon with a red stripe above the icon. Once the device is bound, the stripe turns to green:



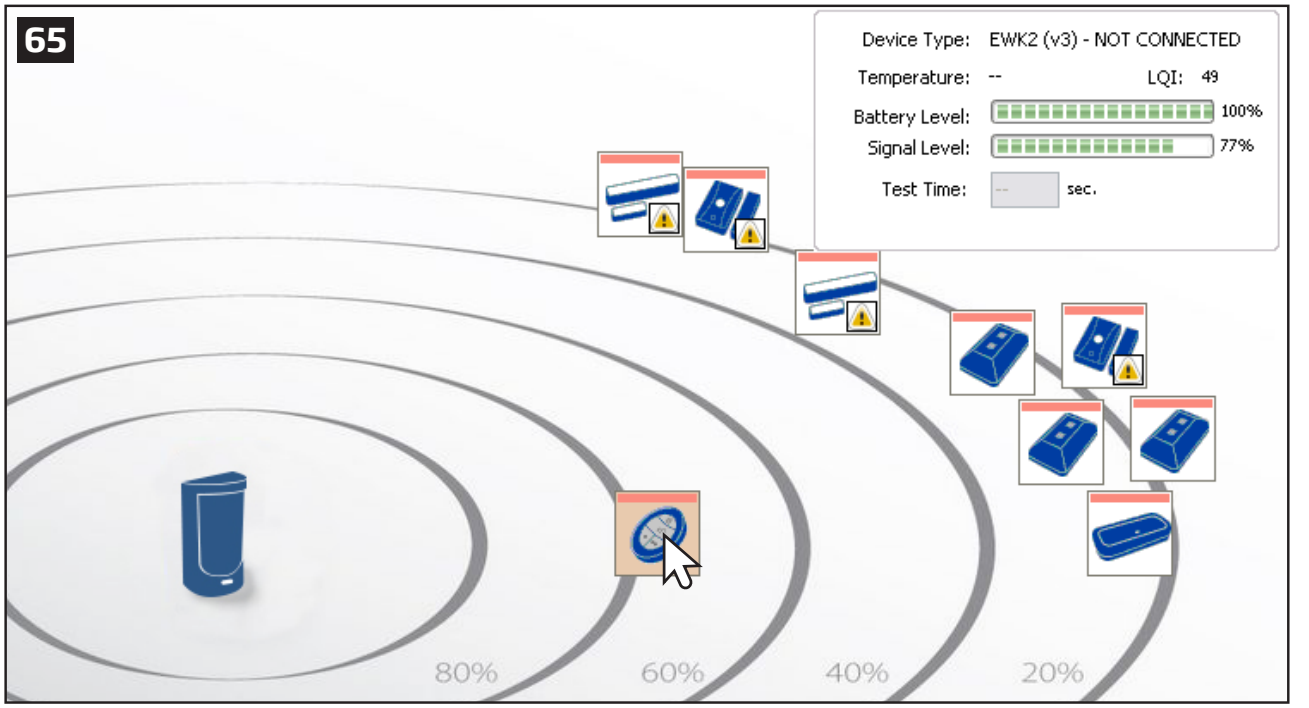
Wireless device bound to alarm system (green stripe above the icon).



Wireless device not bound to alarm system (red stripe above the icon).

The wireless devices are automatically arranged according to the strength of their wireless signal, expressed in percentage terms.

Radar view: Left-click (highlight) on the unbound wireless device icon (red stripe above the icon) to select it and click on the *Add* button afterwards.



IMPORTANT FOR EWK1/EWK2: After left-clicking on the *Add* button it is necessary to press **any** button on the EWK1/EWK2 keyfob several times.

7. After the successful wireless device binding process, the stripe above the wireless device icon will turn green. In addition, the following information related to the bound wireless device will appear:

Device Type – Wireless device model and connection with alarm system status:
- **CONNECTED** – Wireless device is bound to alarm system;
- **NOT CONNECTED** – Wireless device is not bound to alarm system.

Temperature – Temperature of the area surrounding the wireless device. The temperature is measured by built-in temperature sensor (if any).

Battery Level – Battery status of the wireless device:
- 0% - Battery is empty;
- 100% - Battery is full.

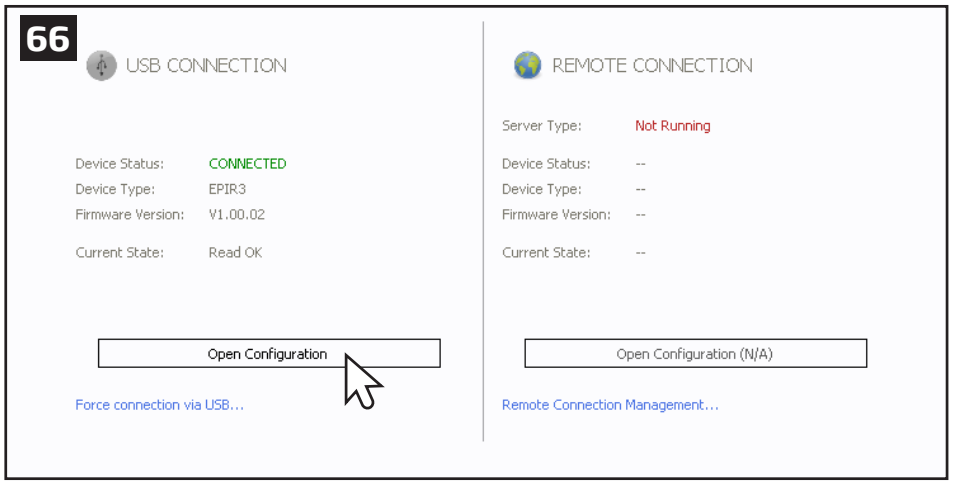
Signal Level – Wireless connection signal strength:
- 0% - No wireless signal;
- 100% - Wireless signal is perfect.

Test Time - The time period intended to test the wireless device battery status, signal strength and temperature of the area surrounding the wireless device. For more details regarding Test Time, please refer to section **3. HOW TO MANAGE THE WIRELESS DEVICES.**

3.2. How to remove a wireless device from the system

IMPORTANT: Before you continue, first ensure the EPIR3 is powered up and connected to your PC via the USB cable.

1. Run *ELDES Configuration Tool* software and left-click on the *USB CONNECTION / Open Configuration button*.

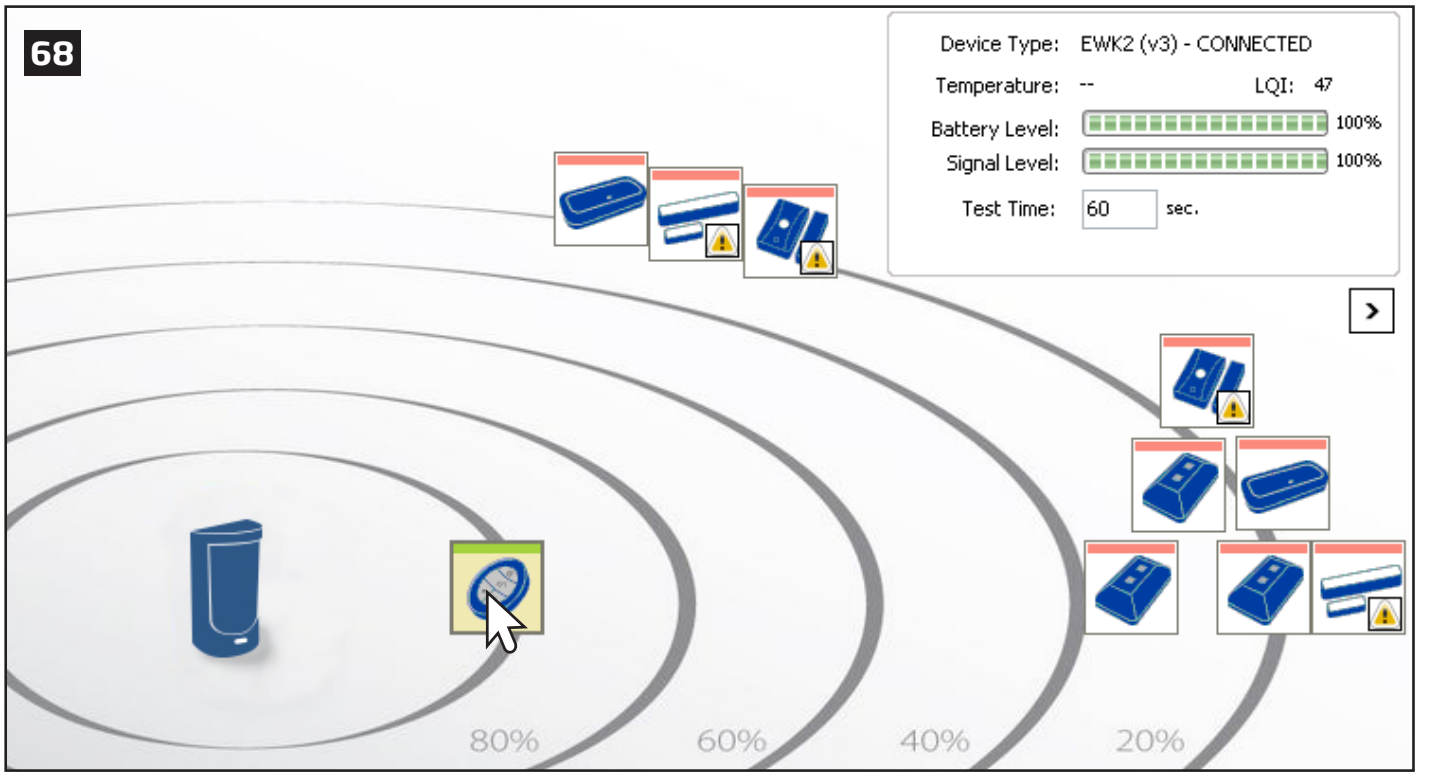


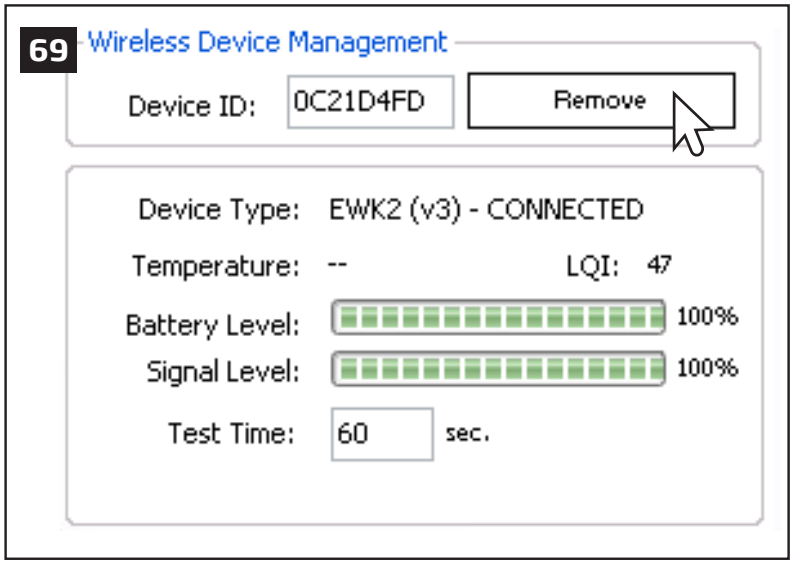
2. Open *Wireless Device Management* section.

3. **List view:** Left-click on the *Remove* button located next to the bound wireless device icon (green stripe above the icon).



Radar view: Left-click (highlight) on the bound wireless device icon (green stripe above the icon) to select it and click on the *Remove* button afterwards.





4. After the successful wireless device removal process, the stripe above the wireless device icon will turn red.

ATTENTION: In order to correctly remove the wireless device from the system, the user must restore the parameters of the wireless device to default afterwards. If this action is not carried out, the wireless device and the system will attempt to exchange data to keep the wireless connection alive. This leads to fast battery power drain on the battery-powered wireless device.

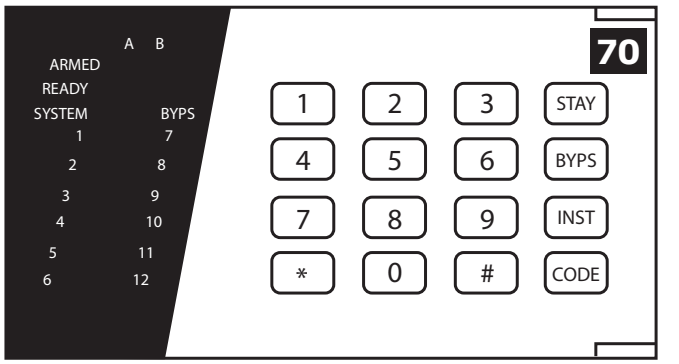
3.3. EKB3W wireless keypad overview

ATTENTION: The EKB3W commands provided in this user manual are intended for basic control of the EPIR3 system. For complete configuration and control using EKB3W, please refer to section **4.HOW TO PROGRAM THE SYSTEM USING EKB3W WIRELESS KEYPAD**.

EKB3W is a wireless LED keypad intended for using with EPIR3 alarm system.

LED Functionality

ARMED	Steady ON - Alarm system is armed / exit delay in progress; flashing - Configuration mode activated
READY	Steady ON - System is ready – no violated zones and tampers
SYSTEM	Steady ON - System faults; flashing - violated high-numbered zones
BYPS	Steady ON - Zone bypass mode
1-12	Steady ON - Violated zone / flashing - violated tamper



Keys Functionality

[BYPS]	Zone bypass mode
[CODE]	System fault list / violated high-numbered zone indication / violated high-numbered tamper indication
[*]	Clear typed in characters
[#]	Confirm (enter) command
[0] ... [9]	Command typing
[STAY]	Manual system arming in Stay mode
[INST]	1st character for Configuration mode activation/deactivation command

The green LED **READY** indicates that no zones or tampers are violated and the system is ready for arming. LED **SYSTEM** lights up or flashes in case of zone violation or if system faults are present. The alarm system cannot be armed until the fault is corrected or violated zone (-s) is restored, bypassed or set up to operate under *Force* mode. The system can still be armed even when the following faults are present:

- backup battery problem;
- main power supply failure;
- date & time not set;
- GSM connection problem.

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 will continuously provide short beeps for 10 seconds (by default) in case of alarm when the violated zone or tamper is of the associated EKB3W keypad.

Visual Indication

EKB3W keys have a back-light and in case of alarm the keypad back-light turns on and lasts for 10 seconds (by default) if the violated zone or tamper is of the associated EKB3W keypad. For battery power saving reasons the back-light and LED light lasts for 10 seconds after the last key-stroke. However, this duration is configurable.

3.3.1.Sleep mode, how to wake up EKB3W and view system alarms or faults

Once EKB3W is bound, it will attempt to exchange data with the system. The communication process follows this pattern:

Sleep mode. Due to battery power saving reasons, most of the time EKB3W keypad operates in sleep mode and periodically (by default – every 60 seconds) transmits the supervision signal, identified as Test Time, to the EPIR3 system. When the keypad operates in the sleep mode, only the transmitter remains operational, while the receiver as well as the the LED indicators and the back-light are switched OFF. However, when the keypad transmits the supervision signal to the system, it will NOT activate its buzzer and/or the LED indicators.

How to wake up EKB3W and view system alarms, faults. When any EKB3W key is pressed, the keypad LED

indicators and the back-light will activate for a set up period of time (by default - 10 seconds), identified as Back-light Timeout. During the Back-light Timeout, the Test Time will automatically switch to 2 seconds period allowing to indicate system alarms, faults and arm/disarm process on the EKB3W keypad. The Back-light timeout will expire after 10 seconds (by default) of EKB3W idling resulting in return to sleep mode. Meanwhile:

a) if a zone or tamper, which is of the associated EKB3W keypad, is violated, EKB3W will instantly wake up and initiate the Back-light Timeout. Meanwhile the keypad buzzer will emit short beeps and the LED indicators will light ON indicating the violated zone or tamper number.
b) if a zone or tamper, which is not of the associated EKB3W keypad, is violated, EKB3W keypad will NOT wake up and will NOT initiate the Back-light Timeout as well as the buzzer will NOT emit short beeps and the LED indicators will NOT light ON.

To configure Back-light Timeout and Test Time parameters, please refer to *ELDES Configuration Tool* software.

NOTE: Even when Back-light Timeout has expired, the character will be considered as typed in once the appropriate EKB3W key is pressed, therefore we recommend using the [*] key to wake up the keypad. However, if another character is typed in and you wish to cancel it, please press the [*] key or wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the typed in characters have been cancelled.

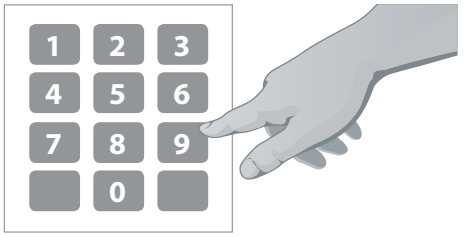
NOTE: To have exit and entry delay indication on the keypad, we highly recommend installing EKB3W near the designated entrance/exit door and using EKB3W zone for wired magnetic door contact connection.

3.3.2. How to configure and control the system by EKB3W

The system configuration and control by EKB3W keypad is carried out by entering a valid configuration command using the number keys [0]... [9], [#] key for confirmation and [*] key to clear the characters that have been 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 cleared. 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 [BYPS], [CODE] and [STAY] 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.

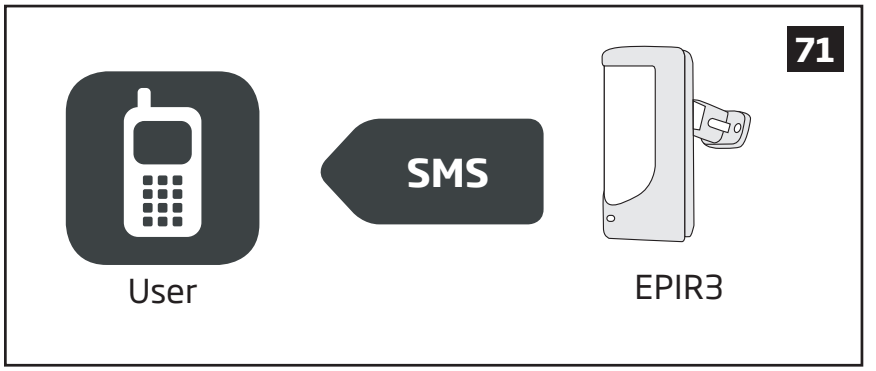
3.3.3. How to arm the system by EKB3W

1. To arm the system, enter any out of 10 available 4-digit user codes using the number keys:



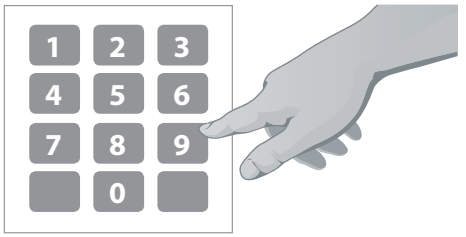
Enter user code:
uuuu
Value: *uuuu* – 4-digit user code
Example: 1111

2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area. The countdown is indicated by short beeps provided by the mini- buzzer built in to the keypad (if fitted).
3. After the system is successfully armed, the keypad's LED indicator **ARMED** will light up and the system will reply with confirmation by SMS text message to User 1 phone number (by default).



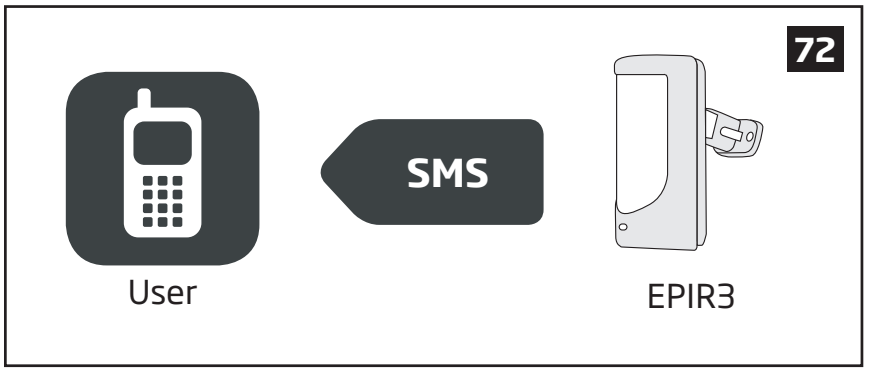
3.3.4. How to disarm & turn off alarm by EKB3W

1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. 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 or turn off the alarm, enter any out of 10 available 4-digit user codes using the number keys:



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

3. After the system is successfully disarmed, LED indicator **ARMED** will light off and the system will reply with confirmation by SMS text message to User 1 phone number (by default).



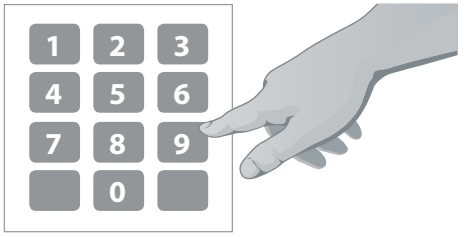
3.3.5. About STAY mode and how to activate it by EKB3W

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:

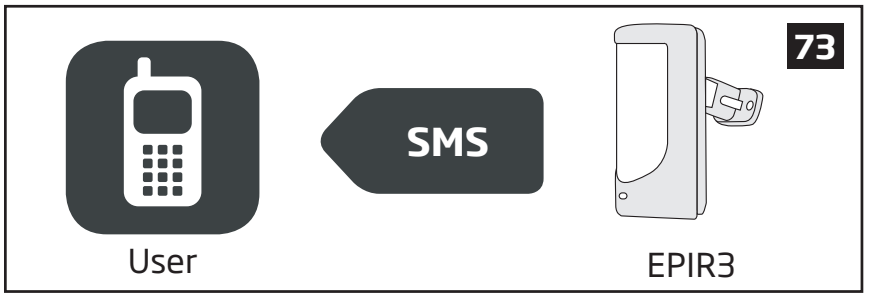
- **Automatic** - If a Delay-type zone is NOT violated during exit delay and a zone (-s) with Stay attribute enabled exist, the system will arm in Stay mode. The system can be Stay-armed using EKB3W - wireless keypad only.
- **Manual** - The system will skip exit delay countdown and instantly arm in Stay mode when using EKB3W keypad and ELDES Smart Security cloud - based server.

1. Arm the system in Stay mode manually by entering the following combination using [STAY] and number keys:



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

2. After the system is successfully Stay-armed, the keypad's LED indicator **ARMED** will light up and the system will reply with confirmation by SMS text message to User 1 phone number (by default).



For more details on how to disarm & turn off the alarm by EKB3W keypad, please refer to section **3.3.4. How to disarm & turn off alarm by EKB3W**.

3.3.6. Alarm indications & how to view violated zones / tampers by EKB3W

EKB3W 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.

The violated zone number is indicated by illuminated zone indicator or flashing indicator **SYSTEM** (if the violated zone number is above 12). The violated tamper number is indicated by flashing zone indicator or illuminated indicator **SYSTEM** (if the violated tamper number is above 12). In both cases. the mini-buzzer can be silenced by disarming the system using any method.

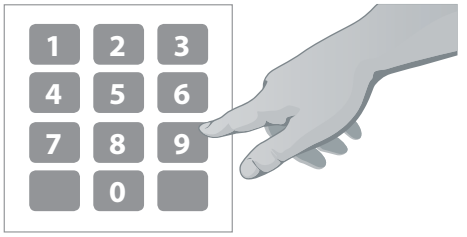
For more details on EKB3W violated high-number zone & tamper number indication, please refer to section **3.3.8. Fault messages**.

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. The buzzer emits short beeps during exit delay. Due to battery saving reasons the buzzer will beep during entry delay and in case of alarm only if the violated zone is of the associated EKB3W keypad.

3.3.7. How to bypass a violated zone & activate a bypassed zone by EKB3W

Arming the system is disabled while there's at least 1 violated zone. Bypassing the zone allows to temporally disable a particular violated zone and arm the alarm system afterwards.

Bypass a violated zone by entering the following combination using [BYPS], number and [#] keys:



Press the [BYPS] key, enter zone number & user code:
BYPS nn uuuu#
Value: *nn* – zone number, range – [01... 34]; *uuuu* – 4-digit user code
Example: BYPS051111#

To activate a bypassed zone, enter the same combination again.

NOTE: The alternative way to activate all bypassed zones at once is to disarm the system.

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

3.3.8. Fault messages

Yellow LED **SYSTEM** indicates a system fault. **SYSTEM** LED indications are mentioned in the table below.

SYSTEM LED	Description
Illuminated continously	One ore more high-numbered tampers (Z13 - Z34) are violated; other system fault
Flashing	One or more high-numbered zones (Z13 - Z34) are violated

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

Zone LED	Description
1	One or more high-numbered tampers (tamper 13 - tamper 34) are violated.
2	Backup battery problem.
3	Main power supply problem.
4	Date/time not set.
5	One or more high-numbered zones are violated.
6	GSM connection problem.

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

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

A. System fault indication - enter command:
[CODE#]

B. Violated high-number zone indication – enter command:
[CODE1]

C. Violated high-number tamper indication – enter command:
[CODE2]

EKB3W indicates up to 12 zones on the keypad, in this section you can learn how to identify higher- numbered zones (Z13-Z34). The number of the violated high-numbered zone or tamper can be calculated using the table below according to the formula: number from zone LED section B + number from zone LED section A.

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

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

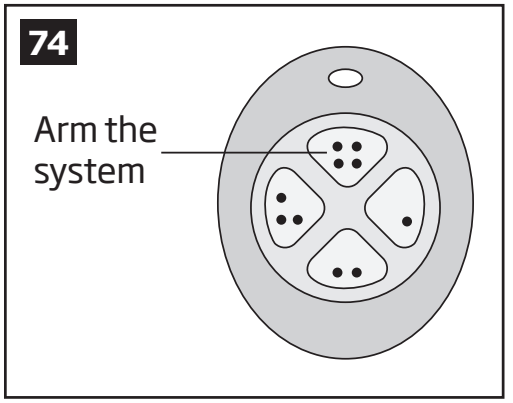
Zone LED section - A (flashing)	Zone LED section - B (illuminated continously)
Zone LED 1 = 1	Zone LED 7 = 12
Zone LED 2 = 2	Zone LED 8 = 18
Zone LED 3 = 3	Zone LED 9 = 24
Zone LED 4 = 4	Zone LED 10 = 30
Zone LED 5 = 5	
Zone LED 6 = 6	

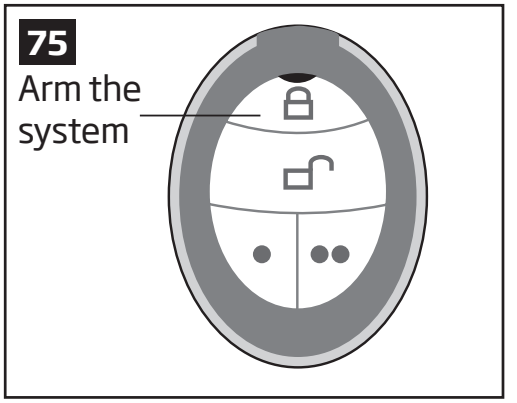
3.4. EWK1 and EWK2 wireless keyfob overview

EWK1/EWK2 is a wireless keyfob intended for using with EPIR3 alarm system. EWK1/EWK2 keyfob features four configurable buttons intended to operate according to individual needs. After the button is pressed, EWK1/EWK2 internal buzzer's sound signal (and red indicator; on EWK2 only) confirms a successfully carried out command. The status of the sent command can be checked by attempting to receive the feedback signal from the alarm system. This can be performed by pressing down the same button and holding it for 3 seconds. 3 short sound signals indicate a successfully carried out command while 1 long beep stands for failed command and feedback signal failure. By default one pair of buttons is already configured to arm and disarm the alarm system.

3.4.1. How to arm the system by EWK1 or EWK2

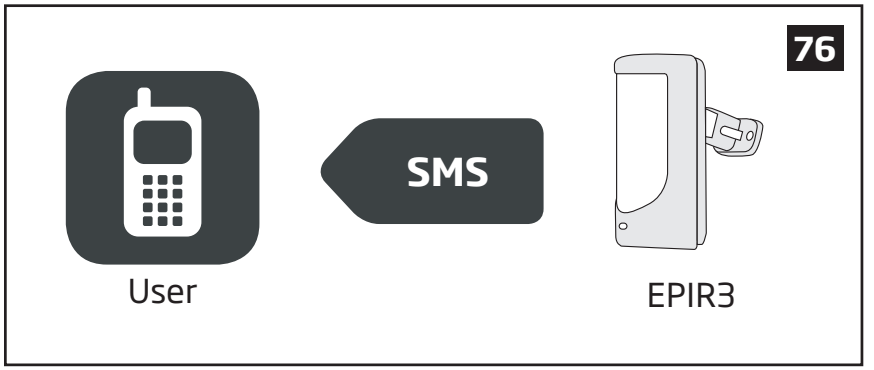
1. To arm the system, press 1 of 4 keyfob buttons set to arm the system (by default, EWK1 – ;EWK 2 - ).





2. The system will initiate the exit delay countdown (by default – 15 seconds) intended for user to leave the secured area.

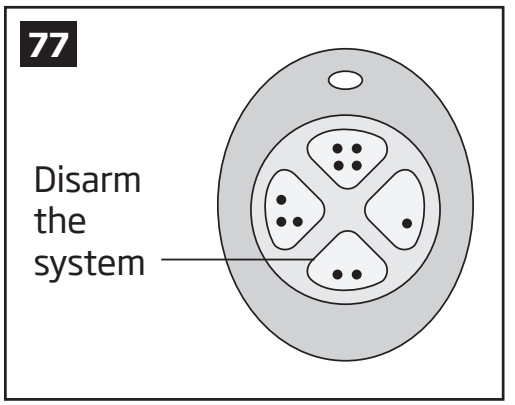
3. After the system is successfully armed, it will reply with confirmation by SMS message to User 1 phone number (by default).

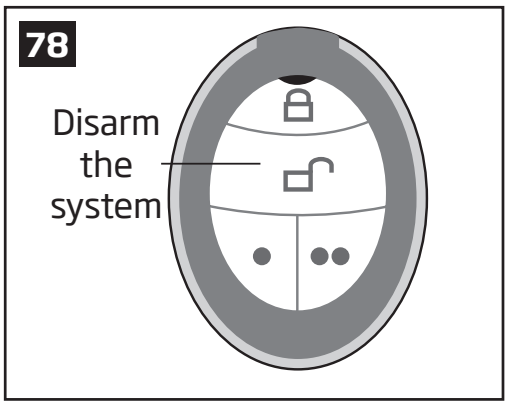


3.4.2. How to disarm & turn off alarm by EWK1 or EWK2

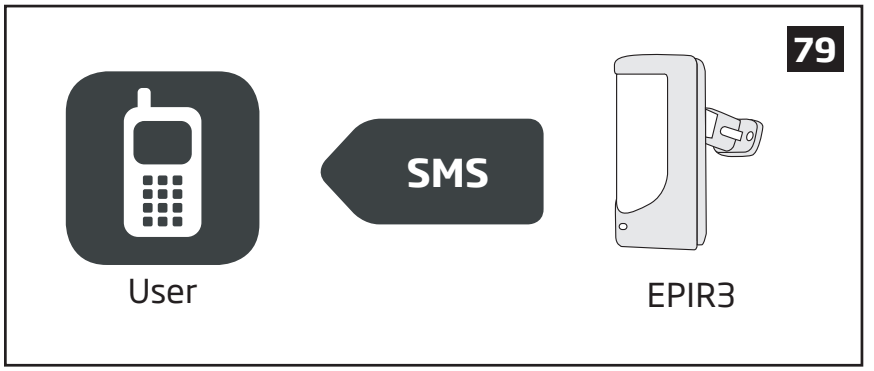
1. The system will initiate the entry delay countdown (by default – 15 seconds) after the user has entered the secured area. Entry delay countdown is intended for user to disarm the system before the alarm is caused.

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





3. After the system is successfully disarmed, it will reply with confirmation by SMS message to User 1 phone number (by default).



4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE

NOTE: The system supports a flexible SMS text message management replies.

In order to configure and control the EPIR3 system using SMS text message, send the text command to the phone number of EPIR3 from one of the pre-programmed user numbers.

ESSENTIAL INFORMATION FOR PROGRAMING VIA YOUR MOBILE PHONE

- The underscore symbol '_' in these instructions represents a space. So when following instructions and typing an SMS text message, replace the underscore symbol with a single space.
- Similarly, 'XXXX' means password.
- Make sure you don't leave any spaces at the beginning or end of the message.
- If you receive the message "wrong syntax" please check your message and try again.

Main Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Change the SMS password	0000_PSW_XXXX	XXXX = [0001... 9999] All SMS text message commands start with a password, so be sure to change the default password to a memorable number. It must be a four digit number – anything except four zeros. Non-numerical characters such as dots, colons and spaces are not allowed.	0000_PSW_1111
Add or change a single user phone number	XXXX_NRn: +441700XXXX111 or XXXX_NRn: 00441700XXXX111 or XXXX_ NRn:01700XXXX111	NRn = [NR1... NR10] The EPIR3 alarm system allows you to enter up to ten different mobile numbers to gain access to and control the system. User 1 number is mandatory - all the others can be skipped. All numbers must be entered in one of the following formats: • **International (with plus)** – The phone numbers starting with plus and an international country code in the following format: +[international code][area	1111_ NR1:+44321XXXX4

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Main Settings			
Function	**Command**	**Value Range / Comment**	**Example**
		code] [local number], example for UK: +441709XXXX111. • **International (with 00)** – The phone numbers starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for UK: 00441709XXXX111. • **Local** – The phone numbers starting with an area code in the following format: [area code][local number], example for UK: 01700XXXX111.	
Add or change multiple user phone numbers	XXXX_ NR1:441700XXXX111_ NR2:00441700XXXX112_ NR3:0111XXXX3_ NR4:0111XXXX4_ NR5:0044111XXXX5_ NR10:XXXX_ +44111XXXX0	Enter numbers based on priority, because in case of alert, the system will attempt to contact the first number entered before the second and so on.	1111_ NR1:+4432XXXX341_ NR4: 0321XXXX52
Verify added user phone numbers	XXXX_HELPNR	The system will send you a text by return, with all pre-programmed numbers.	1111_HELPNR
Delete a single user phone number	XXXX_NRn:DEL	NRn = [NR1... NR10]	1111_NR2:DEL
Delete multiple user phone numbers	XXXX_NR2:DEL_ NR3:DEL_NR4:DEL_ NR5:DEL NR10:DEL		1111_NR3:DEL_ NR4:DEL_NR5:DEL
Set date & time	XXXX_MMMM.mn.dd_ hh:mi	MMMM = year; mn = month, [01... 12]; dd = day, [01... 31]; hh = hour, [00... 23]; mi = minutes, [00... 59]	1111_2012.05.25_ 14:15

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Main Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Arm the system	XXXX_ARM	The system will send you a text confirmation by return.	1111_ARM
Disarm the system	XXXX_DISARM	The system will send you a text confirmation by return.	1111_DISARM
Change the exit delay timer	XXXX_ EXITDELAY:YY	YY = [0... 600] value is in seconds When you exit your protected building, having just armed the system, you have to leave within a specified time to avoid activating the alarm. (The manufacturer pre-set default is 15 seconds.) During this time the detector will ignore any motion. This period is called the exit delay. By default, while the time-out is running, the LED will blink once a second.	1111_EXITDELAY:20
Disable the exit delay timer	XXXX_ EXITDELAY:0		1111_EXITDELAY:0

NOTE: A combination of different phone number formats is allowed to use.

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Zone Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Edit zone alarm text	XXXX_Zn: NewTextHere	Zn = [Z1... Z34]	1111_Z1: Motion_detected
Disable a zone	XXXX_Zn:OFF	Zn = [Z1... Z34]	1111_Z5:OFF
Enable a zone	XXXX_Zn:ON	Zn = [Z1... Z34]	1111_Z7:ON
Change the entry delay timer	XXXX_ ENTRYDELAY:n,YY	n = [Z1... Z34], YY = [0... 65535] value is in seconds When you enter your protected building, you have to disarm the system within a specified time to avoid activating the alarm (manufacturer pre-set default is 15 seconds). During this time the detector will ignore any motion. This period is called entry delay. By default, while the time-out is running, the LED will bling once a second.	1111_ ENTRYDE-LAY:1,25
Disable the entry delay timer	XXXX_ ENTRYDELAY:Zn,0	Zn = [Z1... Z34]	1111_ ENTRYDELAY:Z5,0
Check your system and zone status	XXXX_STATUS	The system will reply to the user who sent the SMS text message, with the following up-to-date information: • system status (armed/disarmed); • status of zones & PGM outputs (ON/OFF); • zone alarm texts; • PGM output names.	1111_STATUS

PGM Output Settings**			
Function	**Command**	**Value Range / Comment**	**Example**
Rename PGM output	XXXX_Cn: NewNameHere	Cn = [C1... C32]	1111_C2:Pump
Turn ON PGM output / set PGM output startup status to ON	XXXX_Cn: ON or XXXX_OutputName:ON	Cn = [C1... C32]	1111_Pump:ON

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

PGM Output Settings**			
Turn OFF PGM output / set PGM output startup status to OFF	XXXX_Cn: OFF or XXXX_OutputName:OFF	Cn = [C1... C32]	1111_C3:OFF
Turn ON PGM output for a specified time period	XXXX_Cn:ON: HH.MM.SS or XXXX_ OutputName:ON:HH.MM.SS	Cn = [C1... C32]; HH = hour, [00... 23]; MM = minutes, [00... 59]; SS = seconds, [00... 59]	1111_C3:ON: 13.23.48
Turn OFF PGM output for a specified time period	XXXX_Cn: OFF:HH.MM.SS or XXXX_OutputName: OFF:HH.MM.SS	Cn = [C1... C32]; HH = hour, [00... 23]; MM = minutes, [00... 59]; SS = seconds, [00... 59]	1111_Pump:OFF: 15.20.01

- The EPIR3 system supports wireless PGM outputs allowing connection and control of various electrical appliances: water pumps, heating, lighting, blinds etc. The maximum number of PGM wireless outputs which can be connected to the EPIR3 system is 32.

Alarm Duration Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Change system alarm duration	XXXX_SIREN:T	T = [0... 5] vale is in minutes	1111_SIREN:4
Check system alarm duration	XXXX_SIREN	The system will reply to the user who sent the SMS text message, with the current alarm duration set	1111_SIREN

System Status Information			
Function	**Command**	**Value Range / Comment**	**Example**
Check the status of your system	XXXX_INFO	The system will reply to the user who sent the SMS text message, with the following up-to-date information: • system date & time; • system status (armed/disarmed); • GSM signal strength level; • main power supply status; • state of zones (OK/alarm).	1111_INFO

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

System Status Information			
Function	**Command**	**Value Range / Comment**	**Example**
Set the periodic system status SMS text message	XXXX_IN-FO:FF.TT	FF = frequency in days, [01... 10]; TT = time, [01... 23] By default, this status SMS text message will be sent daily at 11:00am.	1111_INFO:02.10 This status SMS text message will be sent every 2nd day at 10:00am.
Disable periodic system status SMS text message	XXXX_ INFO:00.00		1111_INFO:00.00

Alarm Notification Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Disable ring from the system in case of alarm	XXXX_ CALLS:OFF	By default the system makes a phone call to the User 1 number in the event of an alarm. You may wish to configure the system so that a phone call is NOT made when an alarm occurs (you may prefer to receive only SMS notifications).	1111_CALLS:OFF
Enable ring from the system in case of alarm	XXXX_ CALLS:ON		1111_CALLS:ON
Disable SMS text message from the system in case of alarm	XXXX_ SMS:OFF	The system sends an SMS text message to the User 1 number in the event of an alarm. You may wish to configure the system to cease sending these messages when alarm occurs.	1111_SMS:OFF
Enable SMS text message from the system in case of alarm	XXXX_ SMS:ON		1111_SMS:ON

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Alarm Notification Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Enable SMS to all users simultaneously in case of alarm	XXXX_ SMSALL:ON	By default, in case of alarm the system sends an SMS message to User 1. If the system does not receive a successful SMS message delivery confirmation in 20 seconds from the recipient, the SMS message is sent to User 2, and if there is still no delivery confirmation received, to Users 3, 4 and 5, but the sequence will stop as soon as a delivery confirmation is received. You may wish to configure the system to send these messages to all pre-programmed user numbers simultaneously when alarm occurs.	1111_SMSALL:ON
Disable SMS text message to all users simultaneously in case of alarm	XXXX_ SMSALL:OFF		1111_SMSALL:OFF

External Power Supply & Backup Battery Status Notification Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Disable SMS text message regarding the external power supply	XXXX_M:OFF	The EPIR3 will let you know when the mains 230V power supply fails or recovers. In some remote places where the mains power supply is unreliable, you may wish to configure the system to ignore these changes. This command applies to User 1 only.	1111_M:OFF
Enable SMS text message regarding the external power supply	XXXX_M:ON		1111_M:ON
Disable SMS text message regarding the battery replacement	XXXX_BATREPORT: OFF	The system checks the backup battery resistance every 10 days. If the backup battery is disconnected or needs to be replaced (if more than 2,5Ω resistance is detected), the system sends an SMS message to User 1. You may wish to configure the system to ignore these changes.	1111_ BATREPORT:OFF
Enable SMS text message regarding the battery replacement	XXXX_BATREPORT: ON		1111_ BATREPORT:ON

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Temperature Notification Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Set temperature MIN and MAX values	XXXX_TEMP: MIN:MAX	MIN = minimum temperature boundary, [-10... 40] C; MAX = maximum temperature boundary, [-10... 40] C.	1111_TEMP:-10:30
Check the temperature XXXX_TEMP		The system will reply to the user who sent the SMS text message, with the temperature value measured by the pre-selected (using ELDES Configuration Tool software) temperature sensor.	1111_TEMP

System Control from Any Phone Number Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Unblock unknown incoming numbers	XXXX_STR:ON	By default, the EPIR3 alarm system can only be accessed from each of up to ten mobile phones that you program into it.. To allow access from any phone number you need to enable the current feature, which will allow all password holders to access the system.	1111_STR:ON
Block unknown incoming numbers	XXXX_STR:OFF		1111_STR:OFF

Remote Listening			
Function	**Command**	**Value Range / Comment**	**Example**
Hear what is happening in your property	XXXX_MIC	You can listen in to what is happening at your protected property whenever you want by sending this SMS text message. The system will make a phone call to you and enable the microphone in EPIR3. You must answer the call within 20 seconds to listen in to what is happening in your property. If you do not pick up, the system will stop trying and will return to its previous state. NOTE: If there is an alarm the system will automatically make a call so that you can listen to what is happening in the property. In this case, the system will try the pre-programmed numbers in order until its call is answered. The phone call in the event of alarm will be made UNLESS „Disable ring from the system in case of alarm" has been selected, see „alarm notification settings" above.	1111_MIC

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Detector Sensitivity Level Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Change the sensitivity level of the detector	XXXX_LEVEL:YY	YY = [20... 99] The greater the value, the lower the sensitivity level of the detector. The EPIR3 device is pre-set by the manufacturer at the optimal detector sensitivity level. However, in some cases, for instance where the system is installed in windy premises, the air flow can cause false alarms. In this case you can reduce the sensitivity level.	1111_LEVEL:35
Check the sensitivity level of the detector	XXXX_LEVEL		1111_LEVEL

Wireless Device Management			
Function	**Command**	**Value Range / Comment**	**Example**
Disable wireless module	XXXX_RF:OFF	The system disables the built-in wireless module	1111_RF:OFF
Enable wireless module	XXXX_RF:ON		1111_RF:ON
Bind a wireless device to the system	XXXX_SET:YYYYYYYY	YYYYYYYY = 8-character wireless device ID code	1111_ SET:5261841A
Remove a wireless device from the system	XXXX_DEL:YYYYYYYY	YYYYYYYY = 8-character wireless device ID code	1111_ DEL:5261841A
Replace a wireless device by another wireless device of the same model	1111_REP:YYYYYY <ZZZZZZZZ	YYYYYYYY = old 8-character wireless device ID code; ZZZZZZZZ = new 8-character wireless device ID code	1111_ REP:5261841A <41286652
Verify free wireless channels	XXXX_STATUS_FREE	The system will send you a text by return, with the number of available free wireless channels.	1111_STATUS_FREE

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Wireless Device Management			
Function	**Command**	**Value Range / Comment**	**Example**
Get wireless device information	XXXX_RFINFO:Zn or XXXX_RFINFO: YYYYYYYY	Zn = [Z3... Z34] The system will send you a text by return, with the following information: • wireless device battery level; • wireless signal level; • Test Time value • firmware version.	1111_ RFINFO:5261841A
Verify wireless device operation status	XXXX_TEST:Zn	Zn = [Z3... Z34] The system will send you a text by return indicating if a wireless device is operational.	1111_TEST:Z6
Get wireless device temperature	XXXX_TEMP:Zn	Zn = [Z3... Z34] The system will send you a text by return indicating temperature value measured by a built-in temperature sensor (if any) of a specified wireless device.	1111_TEMP:Z9

SMS Central Number Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Verify SMS text message central number	XXXX_ SMS_+4411111111	The SMS central number is normally already saved in the SIM by your mobile phone network provider. However if you fail to receive SMS text messages from the EPIR3, you will have to enter it yourself having first got it from your mobile phone provider. If you continue to have problems communicating with the SIM card you installed into EPIR3, try using a SIM card from a different mobile telephone operator.	1111_SMS_ +44255XXXX1

Smart Security			
Function	**Command**	**Value Range / Comment**	**Example**
Get Smart Security ID code	XXXX_SMART_ID	The system will send you a text by return, with the multi-character code required by Smart Security feature.	1111_SMART_ID

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Remote System Restart			
Function	**Command**	**Value Range / Comment**	**Example**
Restart system remotely	XXXX_RESET	In some critical situations it might be necessary to restart the system, for instance after changing the GPRS settings.	1111_RESET

Monitoring Station Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Enable MS Mode	XXXX_SCNSET:ON	The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the monitoring station when the MS (Monitoring Station) mode is enabled.	1111_SCNSET:ON
Disable MS Mode	XXXX_SCNSET:OFF		1111_SCNSET:OFF
Set server IP address	XXXX_ SETGPRS:IP:add.add. add.add	ADD.ADD.ADD.ADD = server IP address. Public IP address of the machine running EGR100 or Kronos monitoring station software.	1111_ SETGPRS:IP:65.82.110.15
Set server port number	XXXX_ SETGPRS:PORT:port	port = port number, 1... 65535]. Forwarded port of the machine running EGR100 or Kronos monitoring station software.	1111_SETGPRS:PORT:5521

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

Monitoring Station Settings			
Function	**Command**	**Value Range / Comment**	**Example**
Select protocol	XXXX_SETGPRS:PRO-TOCOL:PPP	PPP = protocol, [TCP... UDP] TCP or UDP protocol. UDP is highly recommended for EGR100 data format.	1111_ SETGPRS:PROTOCOL:UDP
Set APN	XXXX_ SETGPRS:APN:ACCPN	ACCPN = access-point-name. Access-point-name of GPRS parameters provided by the GSM operator.	1111_SETGPRS:APN:internet
Set user name	XXXX_ SETGPRS:USER:USR	USR = user name. User name of GPRS parameters provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.	1111_SETGPRS:USER:int-user
Set password	XXXX_ SETGPRS:PSW:PASS	PASS = password Password of GPRS parameters provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.	1111_SETGPRS:PSW:int-pass
View server IP address, port, protocol and GPRS parameters	XXXX_SETGPRS?	The system will reply you with server IP address, port, protocol and GPRS parameter values.	1111_SETGPRS?

NOTE: The underscore symbol '_' in these instructions represents a space. So when typing an SMS text message, replace the underscore symbol with a single space.

5. HOW TO PROGRAM THE SYSTEM USING EKB3W WIRELESS KEYPAD

In order to configure and control the EPIR3 system using EKB3W wireless keypad, please refer to the following information first.

ESSENTIAL INFORMATION FOR PROGRAMING VIA EKB3W WIRELESS KEYPAD

- Before configuring the system using EKB3W wireless keypad, the Configuration mode must be activated by entering ***[INST]adminpassword#*** command. By default the command is ***[INST]1470#***.
- To deactivate Configuration mode, enter the aforementioned command again.
- If you entered unnecessary characters by mistake, press [*] key to clear the characters that have been entered. Alternatively, you can wait for 10 seconds until the keypad buzzer will provide a long beep indicating that the entered characters have been cleared.

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

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

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

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

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
		Main Settings	
Change SMS password	14xxxx#	xxxx	0001 - 9999
Set user code	15yyxxxx#	yy	01 - 10
		xxxx	0000 - 9999
Replace user code	63yyyyxxxx#	yyyy	0000 - 9999
		xxxx	0000 - 9999
Delete user code	65xxxx#	xxxx	0000 - 9999
Change administrator password	16aaaa#	aaaa	0000 - 9999
Set user phone number	17xxyyyyyyyyyyyyyyy#	xx	01 -10
		yyyyyyyyyyyyyyy	
Set security guard phone number	55yyyyyyyyyyyyyyy#	yyyyyyyyyyyyyyy	
Set system date and time	66YYYYMMDDhrmn#	YYYYM	
		MM	01 - 12
		DD	01 -31
		hr	min
		mn	00- 59

Comment	Example
4-digit administrator password	**INST1470#**
Main Settings	
new 4-digit SMS password default password = 0000 must be changed!	142258#
user code slot	15025562#
new 4-digit user code default User Code 1 = 1111 recommended to change	
existing 4-digit user code	6355623281#
new 4-digit user code	
existing 4-digit user code	653281#
new 4-digit administrator password	161508#
default password = 1470 recommended to change	
user phone number slot	17004417091111111#
user phone number, 15 digits max.; supported format: • International (with 00) – Example for UK: 00441709111XXXX. • Local – Example for UK: 01709111XXXX.	
security guard phone number, 15 digits max.; supported format: • International (with 00) – Example for UK: 00441709111XXXX. • Local – Example for UK: 01709111XXXX.	55017091111111#
year	66201408231625#
month	
day	
hours	
minutes	

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Disable control from any phone number	120#		
Enable control from any phone number	121#		

Zone Settings			
Set entry delay	54xxyyyyy#	xx	01 - 34
		yyyyy	0 - 65535
Set exit delay	72xxx#	xxx	0 - 600
Disable zone	52xx0#	xx	01 - 34
Enable zone	52xx1#	xx	01 - 34
Bypass violated zone (must be entered without activating Configuration mode in advance)	BYPSxxyyyy#	xx	01 - 34
		yyyy	0000 - 9999
Activate byppased zone (must be entered without activating Configuration mode in advance)	BYPSxxyyyy#	xx	01 - 34
		yyyy	0000 - 9999

Comment	Example
4-digit administrator password	**INST1470#**
system arming/disarming and configuration by a non-preset phone number is denied	120#
system arming/disarming and configuration by a non-preset phone number providing a valid SMS password is permited	121#

Zone Settings	
zone number	540245#
entry delay in seconds	
exit delay in seconds	7258#
zone number	52380#
zone number	52121#
zone number	BYPS093281#
4-digit user code	
zone number	BYPS093281#
4-digit user code	

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Set zone type	53xx1#		
	53xx2#		
	53xx3#		
	53xx4#		
	53xx5#		
	53xx6#		
		xx	01 - 34
STAY Mode Settings			
Enable STAY attribute for individual zone	56xx1#	xx	01 - 34
Disable STAY attribute for individual zone	56xx0#	xx	01 - 34
Manual system arming in STAY mode (must be entered without activating Configuration mode in advance)	STAYxxxx	xxxx	
PGM Output Settings			
Turn ON PGM output/set PGM output startup state as ON	61xx1#	xx	01 - 32

Comment	Example
4-digit administrator password	**INST1470#**
Interior Follower	53053#
Instant	
24-Hour	
Delay	
Fire	
Panic/Silent	
zone number	
STAY Mode Settings	
zone number	56031#
zone number	56270#
4-digit user code	STAY3281#
PGM Output Settings	
PGM output number	61201#

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Turn OFF PGM output/set PGM output startup state as OFF	61xx0#	xx	01 - 32
Siren/Alarm Settings			
Set alarm duration	10xx#	xx	00 - 10
Disable Bell Squawk	290#		
Enable Bell Squawk	291#		
Disable siren activation in case of wireless signal loss with wireless device	760#		
Enable siren activation in case of wireless signal loss with wireless device	761#		
Notification Settings			
Disable periodic INFO SMS	110000#		
Set periodic INFO SMS	11xxyy#	xx	01 - 23
		yy	00 - 99
Disable call in case of alarm	300#		

Comment	Example
4-digit administrator password	**INST1470#**
PGM output number	61250#
Siren/Alarm Settings	
alarm duration in minutes	1005#
disable system arm/disarm indication by siren sound	290#
enable 2 short siren beeps when the system is armed; 1 long siren beep when the system is disarmed	291#
system will not activate siren if it loses wireless signal with a wireless device	760#
system will activate siren if it loses wireless signal with a wireless device	761#
Notification Settings	
disable INFO SMS	
set time (hours = xx) for periodic INFO SMS delivery or period in hours (if the period = yy in days is set to 0)	110315#
system will not call any preset user phone number in case of alarm	300#

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Enable call in case of alarm	301#		
Disable SMS in case of alarm	310#		
Enable SMS in case of alarm	311#		
Disable call in case of alarm for individual user phone number	28xx0#	xx	1 - 10
Enable call in case of alarm for individual user phone number	28xx1#	xx	1 - 10
Disable simultaneous SMS delivery in case of alarm	210#		
Enable simultaneous SMS delivery in case of alarm	211#		
Disable SMS in case of alarm to Security Guard	390#		

Comment	Example
4-digit administrator password	**INST1470#**
system will call all the preset user phone numbers in case of alarm starting with User 1. if the call is not answered or user is unavailable, the system will move to the next preset user phone number until the call is answered or rejected	301#
system will not send SMS text message to any preset user phone number in case of zone/tamper alarm	310#
system will send SMS text message to all preset user phone numbers in case of zone/tamper alarm starting with User 1. if the SMS text message is not delivered (SMS delivery report not received) within 20 seconds, the system will move to the next preset user phone number until the SMS text message is delivered	311#
user phone number slot	28030#
user phone number slot	28041#
system will not send SMS text messages to all preset user phone numbers simultaneously in case of zone/tamper alarm	210#
system will send SMS text messages to all preset user phone numbers simultaneously in case of zone/tamper alarm regardless of SMS text message delivery status	211#
system will not send SMS text message to preset Security Guard phone number in case of zone/tamper	390#

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Enable SMS in case of alarm to Security Guard	391#		
Disable arm/ disarm SMS for individual user phone number	75xx0#	xx	1 - 10
Enable arm/ disarm SMS for individual user phone number	75xx1#	xx	1 - 10
Disable simultaneous SMS delivery regarding arm/disarm	220#		
Enable simultaneous SMS delivery regarding arm/disarm	221#		
Disable SMS regarding arm/ disarm to Security Guard	500#		
Enable SMS in case of alarm to Security Guard	501#		
Disable SMS regarding mains power supply loss/restore	130#		

Comment	Example
4-digit administrator password	**INST1470#**
system will send SMS text message to preset Security Guard phone number in case of zone/tamper	391#
user phone number slot	75060#
user phone number slot	75101#
system will not send SMS text message to all preset user phone numbers simultaneously regarding system arm/disarm	220#
system will send SMS text message to all preset user phone numbers simultaneously regarding system arm/disarm regardless of SMS text message delivery status	221#
system will not send SMS text message to preset Security Guard phone number regarding system arm/disarm	500#
system will send SMS text message to preset Security Guard phone number regarding system arm/disarm	501#
system will not send SMS text message to any preset user phone number regarding mains power supply loss/restore	130#

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Enable SMS regarding mains power supply loss/restore	131#		
Disable SMS in case of back-up battery fault	190#		
Enable SMS in case of back-up battery fault	191#		
Disable SMS delivery report for all system notifications	380#		
Enable SMS delivery report for all system notifications	381#		
Detector Sensitivity Level Settings			
Set PIR detector sensitivity level	79xx#	xx	20 - 99
GSM Audio Settings			
Set microphone gain for remote listening	64xx#	xx	00 - 15
Set speaker level	67xxx#	xx	00 - 100

Comment	Example
4-digit administrator password	**INST1470#**
system will send SMS text message to all preset user phone numbers regarding mains power supply loss/restore starting with User 1. if the SMS text message is not delivered (SMS delivery report not received) within 20 seconds, the system will move to the next preset user phone number until the SMS text message is delivered	131#
system will not send SMS text message to any preset user phone number in case of back-up battery fault	190#
system will send SMS text message to all preset user phone numbers in case of back-up battery fault starting with User 1. if the SMS text message is not delivered (SMS delivery report not received) within 20 seconds, the system will move to the next preset user phone number until the SMS text message is delivered	191#
disable SMS delivery report to verify the SMS delivery to user phone number status	380#
the system waits for the GSM provider to confirm the successful SMS text message delivery. in case of no SMS delivery report within 20 seconds, the system sends an SMS text message to the next preset user phone number	381#
Detector Sensitivity Level Settings	
higher value = lower sensitivity level	7960#
GSM Audio Settings	
adjust built-in microphone sensitivity level	6410#
speaker level	6725#

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Monitoring Station Settings			
Enable MS mode	231#		
Disable MS mode	230#		
Set Account number	27cccc#	cccc	0000 - 9999
Disable data message	24010#		
	24020#		
	24030#		
	24040#		
	24050#		
	24060#		
	24070#		
	24080#		
	24090#		
	24100#		
	24110#		
	24120#		
	24130#		
	24140#		
	24150#		
	24160#		
	24170#		

Comment	Example
4-digit administrator password	**INST1470#**
Monitoring Station Settings	
allow data message delivery to the monitoring station	231#
disallow data message delivery to the monitoring station	230#
4-digit number required to identify the alarm system unit by the monitoring station.	275614#
burglary alarm/restore	24070#
mains power supply loss/restore	
armed/disarmed by user	
test event	
battery fault	
tamper alarm/restore	
silent alarm/restore	
system started	
24-hour alarm/restore	
fire alarm/restore	
low battery	
temperature risen	
temperature fallen	
wireless signal loss/restore	
armed/disarmed in STAY mode	
system shut down	
armed/disarmed automatically	

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Enable data message	24011#		
	24021#		
	24031#		
	24041#		
	24051#		
	24061#		
	24071#		
	24081#		
	24091#		
	24101#		
	24111#		
	24121#		
	24131#		
	24141#		
	24151#		
	24161#		
	24171#		
Set primary connnection	480#		
	481#		
	482#		

Comment	Example
4-digit administrator password	**INST1470#**
armed/disarmed by user	24051#
test event	
battery fault	
tamper alarm/restore	
silent alarm/restore	
system started	
24-hour alarm/restore	
fire alarm/restore	
low battery	
temperature risen	
temperature fallen	
wireless signal loss/restore	
armed/disarmed in STAY mode	
system shut down	
armed/disarmed automatically	
armed/disarmed by user	
test event	
GPRS network	481#
Voice calls	
SMS	

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Set backup connections	83bb0#		
	83bb1#		
	83bb2#		
	83bb3#		
		bb	01 - 02
Set delay after last communication attempt	69xxxxx#	xxxxx	0 - 65535
Set server IP address	40xxxxxxxxxxx#	xxxxxxxxxxx	
Set server port number	44xxxxx#	xxxxx	0 - 65535
Set DNS1	41xxxxxxxxxxx#	xxxxxxxxxxx	
Set DNS2	42xxxxxxxxxxx#	xxxxxxxxxxx	
Select protocol	430#		
	431#		
Set number of GPRS attempts	68xxx#	xxx	01 - 255
Set test period	46xxxxx#	xxxxx	0 - 65535
Set Unit ID	47xxxx#	xxxx	0000 - 9999
Set monitoring station phone number	26 xx yyyyyyyyyyyyyyy#	xx yyyyyyyyyyyyyyy	01 - 03

Comment	Example
4-digit administrator password	**INST1470#**
GPRS network	83020#
Voice calls	
SMS	
not in use	
backup connecton slot	
period in seconds	69100#
server IP address excluding dots	40085222120085#
sever port number	44250#
DNS1 IP address	40085222120081#
DNS2 IP address	40085222120082#
TCP	431#
UDP	
number of data transmission attempts via GPRS network in case the intitial attempt was unsuccessful	6825#
ping period via GPRS network in seconds	46260#
4-digit number required to identify the alarm system unit by EGR100 middle-ware (communication via GPRS network)	475563#
monitoring station phone number slot for communicaiton via Voice Calls	26020044170911XXXX1#
monitoring station phone number, 15 digits max.; supported format: • International (with 00) – Example for UK: 0044170911XXXX1. • Local – Example for UK: 0170911XXXX1.	

Function	EKB3W command	Value	Range
Activate/deactivate Configuration mode	**INSTaaaa#**		
Set number of Voice Calls attempts	37xx#	xxx	01 - 10

Comment	Example
4-digit administrator password	**INST1470#**
number of data transmission attempts via Voice Calls in case the intitial attempt was unsuccessful	3706#

6. TROUBLESHOOTING

Fault	Possible reason
Lens indicator OFF	• No mains 230V power • Power supply connector is unplugged • Signal too weak or out of coverage
Indicator is blinking once a second	• SIM card is missing • PIN code hasn't been disabled • SIM card is not active
System does not send any SMS text messages and/or does not ring	• SIM card account is depleted • Incorrect SIM central number • No network signal • User number is not programmed in (or call was made from an unprogrammed number and access from such numbers has been disabled)
SMS text message received: "Incorrect Format"	• Wrong syntax • Space is in wrong place in text/SMS message • Manufacturer default password has not been changed • The NR1 user has not been programmed in
Your existing EPIR3 does not recognise an ELDES wireless device	**EITHER** • Wireless mode is disabled. Please refer to *ELDES Configuration Tool* software to enable it. **OR** • Wireless device battery is out of energy or the device is not switched ON.
Some users are not getting arm-disarm and/or alarm notifications.	• If you normally configure your EPIR3 by SMS text message, you should be aware that there are some user options which can be set when using the Configuration Tool but not when using configuration by SMS. Review system settings using the Configuration Tool and you will see a fuller picture of settings for individual users.

If you cannot find the answer to your problem above, please contact your local distributor.

More up to date information about your device and other ELDES products can be found at www.eldes.lt

7. ADDITIONAL INFORMATION FOR ADVANCED USERS

OVERVIEW

This section contains the wired zone and output wiring diagrams and other system features, such as zone, tamper, PGM output, siren operation, monitoring station operational description and settings, remote configuration via GPRS network connection and firmware upgrade procedure.

In this section you will meet the following icons indicating configuration and control of a certain feature supported by the EPIR3 system:



Please, refer to section **4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE.**



Please, refer to section **5. HOW TO PROGRAM THE SYSTEM USING EKB3W WIRELESS KEYPAD.**



Please, refer to *ELDES Configuration Tool* software and its HELP section.



The function can be operated by EWK1 - wireless keyfob



The function can be operated by EWK2 - wireless keyfob

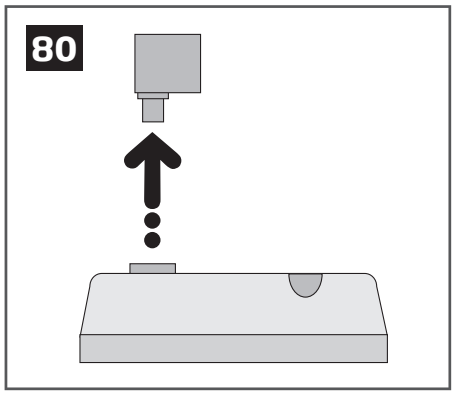
7.1. How to connect a wired siren or a LED indicator to the wired output

The output can be set to operate either as a siren output leading the connected wired siren activation in case of alarm or for showing the following system conditions by a connected LED indicator:

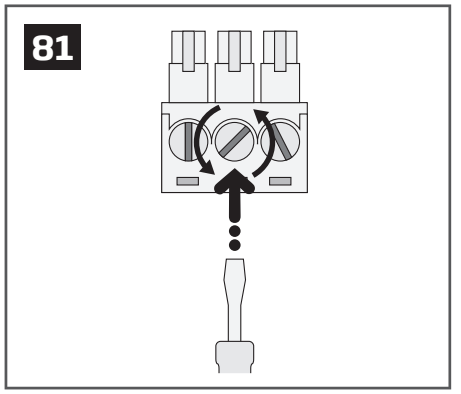
- **NO SIM Inserted -** SIM card not present. The LED indicator will flash if the SIM card is not present in the EPIR3.
- **SIM PIN Enabled -** PIN code left enabled. The LED indicator will flash with pauses if the PIN code is not disabled on the SIM card that is inserted in the EPIR3.
- **GSM Operator Error -** GSM connection error. The LED indicator will flash with pauses in case of this error.
- **Exit/Entry Delay -** Exit and entry delay time-out. The LED indicator will flash during countdown of exit and entry delay time-out.
- **Zone Z1 Violated -** Zone Z1 violation. When PIR detector's zone Z1 is violated, the LED indicator will illuminate and turn OFF when the detector's zone Z1 is restored.
- **Alarm -** System alarm. The LED indicator will turn ON in case of alarm and turn OFF when the alarm ends.
- **System Armed -** System armed or disarmed. LED indicator will be illuminated once the system is armed and turned OFF once the system is disarmed.

Wired siren/bell

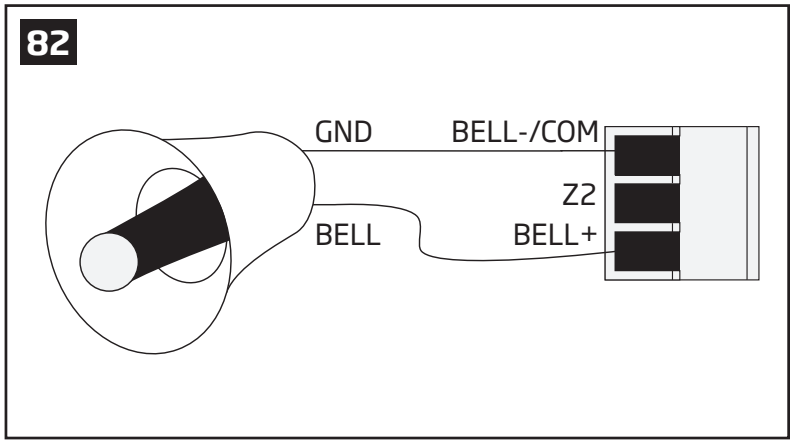
1. Remove the terminal block from the slot.



2. Loosen the screws of the terminals using a flathead screwdriver.

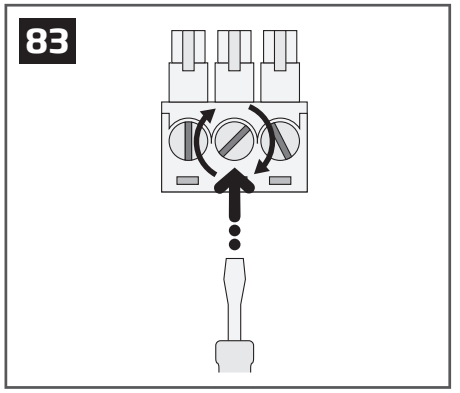


3. Connect **BELL** wire (usually – red) of the wired bell/siren to **BELL+** terminal, while the **GND** (usually - black) wire to **BELL - / COM** terminal.

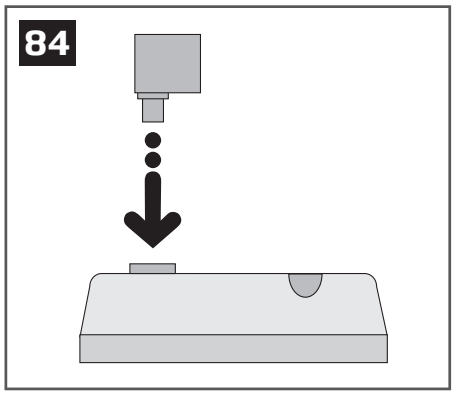


The wired siren/bell, connected to the wired output, must be piezo type and powered from +7... +11V. The current consumption must not exceed 150 mA.

4. Screw in the terminals.



5. Insert back the terminal block.



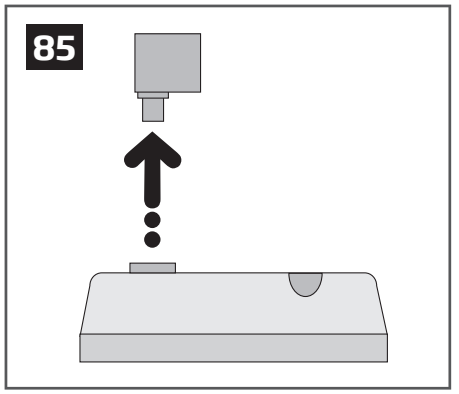
6. Set the **Output Mode** as **Siren** under *Management* section in the *ELDES Configuration Tool* software.

NOTE: No additional power supply is required for the siren/bell.

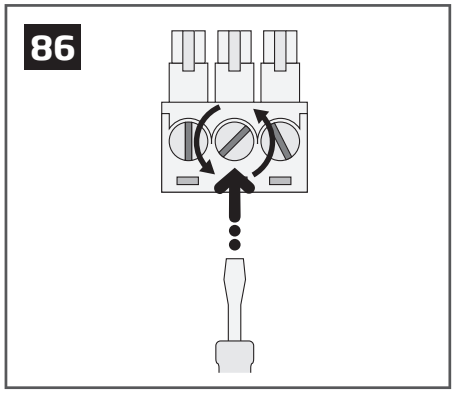
NOTE: For a more convenient installation, we recommend using EWS1, EWS2 and EWS3 wireless sirens.

System condition indication by LED indicator

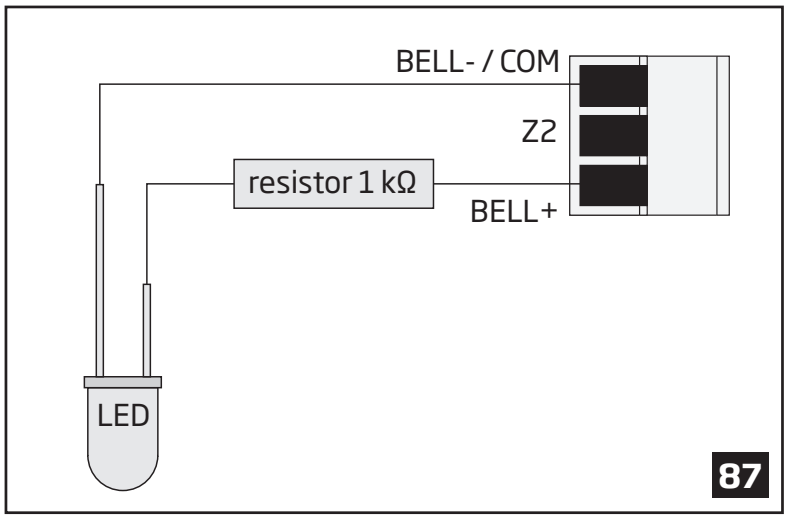
1. Remove the terminal block from the slot.



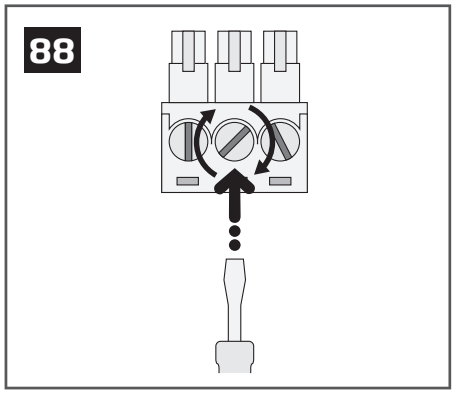
2. Loosen the screws of the terminals using a flathead screwdriver.



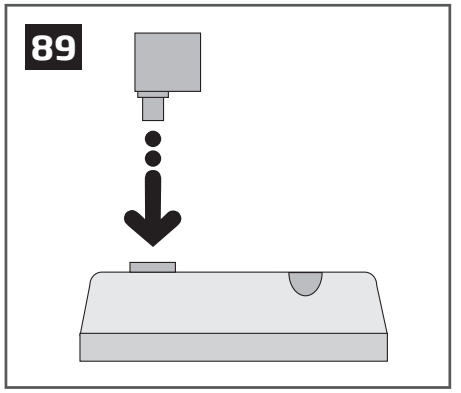
3. Connect LED indicator's **anode** lead (longer) to any of 1 kΩ nominal resistor lead and to the **BELL+** terminal, while the **cathode** lead (shorter) to **BELL - / COM** terminal.



4. Screw in the terminals.



5. Insert back the terminal block.



5. Under *Management → Settings* section in *ELDES Configuration Tool* software, set the **Output Mode** as **Indicator** and under the **Output Indication** column, enable the check-box (-es) corresponding to the desired system conditions, e. g. **System Armed** check-box.

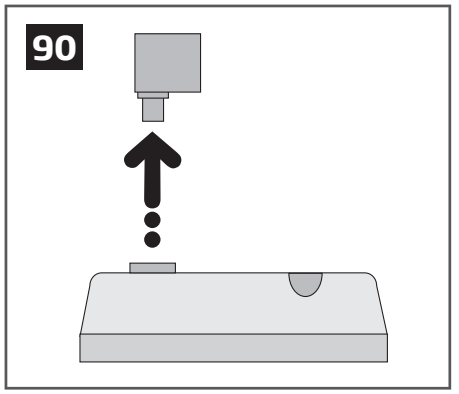
NOTE: The resistor and the LED indicator are NOT supplied with the EPIR3 system and are NOT mandatory to use. Please, obtain these components from your local store if desired.

7.2. How to connect a sensor to the wired zone

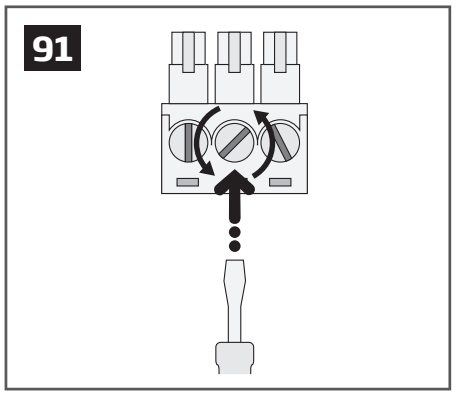
EPIR3 system comes equipped with the wired zone, therefore you may wish to connect a wired sensor to your system.

7.2.1. Connecting a wired sensor of NO (normally open) type

1. Remove the terminal block from the slot.

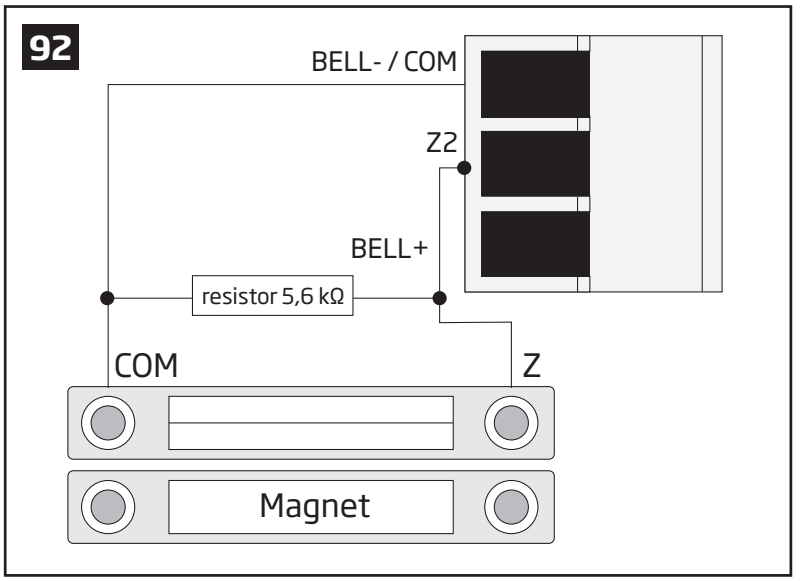


2. Loosen the screws of the terminals using a flathead screwdriver.

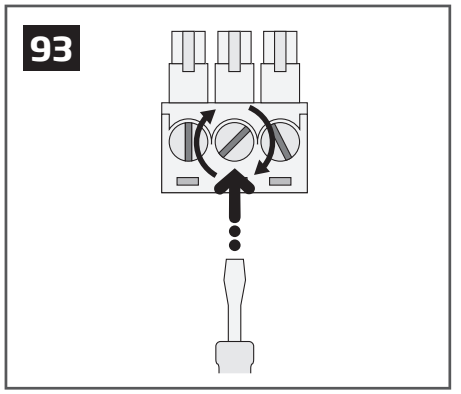


3. Connect the 5.6 kΩ nominal resistor, supplied with your EPIR3 system, across **BELL- / COM** and **Z2** terminal in parallel to the connected wires of the detection device.

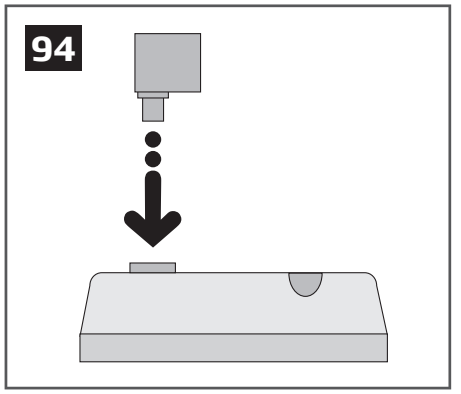
4. Connect the **Z** wire (usually – yellow) of the wired detection device to **Z2** terminal, while the **COM** (usually - green) wire to **BELL - / COM** terminal.



5. Screw in the terminals.



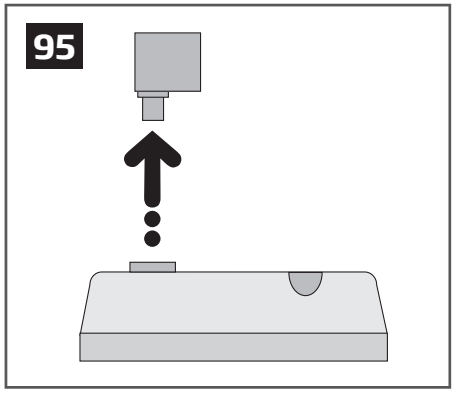
6. Insert back the terminal block.



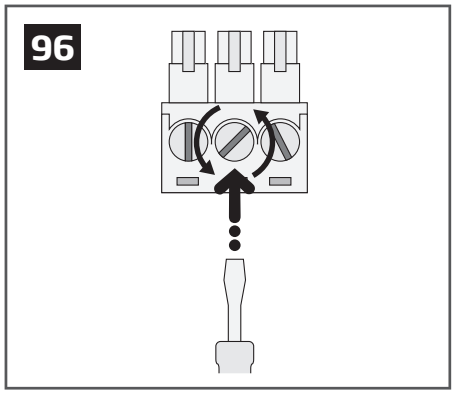
7. Set **Zone Status** of **Z2** to **Enabled** under *Zones/On Board* section in *ELDES Configuration Tool* software.

7.2.2. Connecting a wired sensor of NC (normally closed) type

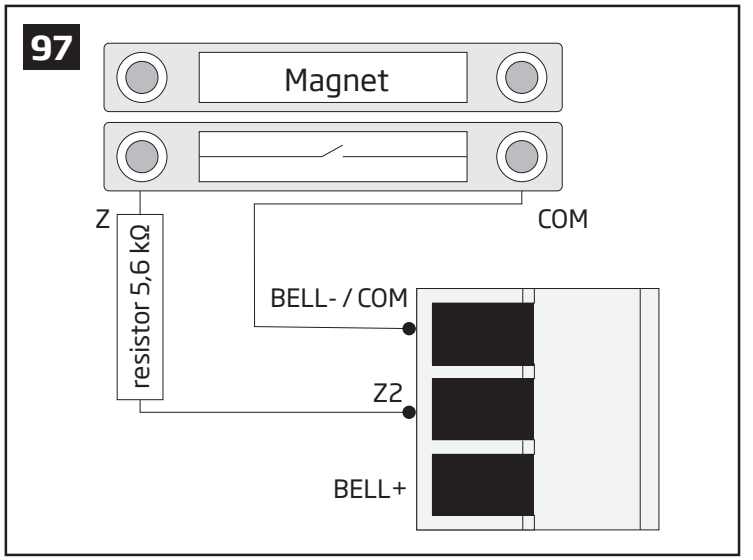
1. Remove the terminal block from the slot.



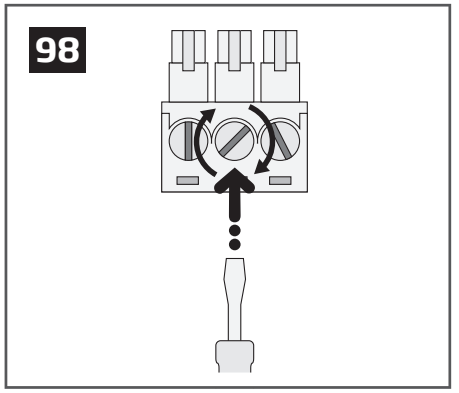
2. Loosen the screws of the terminals using a flathead screwdriver.



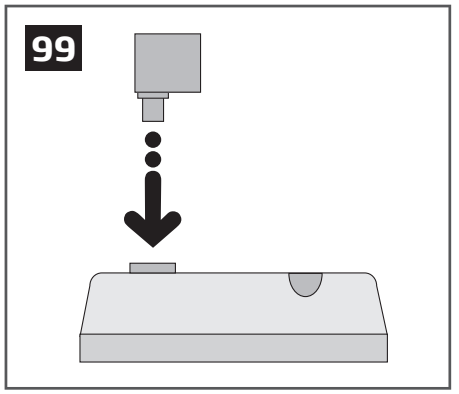
3. Connect the **COM** (usually - green) wire to **BELL - / COM** terminal.
4. Connect the **Z** wire (usually – yellow) of the wired detection device to any terminal of the 5.6 kΩ nominal resistor (supplied with your EPIR3 system), while the other resistor terminal - to **Z2** terminal.



5. Screw in the terminals.



6. Insert back the terminal block.



7. Set **Zone Status** of **Z2** to **Enabled** under *Zones/On Board* section in *ELDES Configuration Tool* software.

7.3. Automatic system arming/disarming



The system comes equipped with automatic arm/disarm based on the assigned scheduler (-s). When one or more schedulers are assigned, the system will automatically arm/disarm on the specified weekdays and time set up in the scheduler. The system allows to assign up to 8 different schedulers. Each scheduler includes the following parameters:

- **Action:**
  - **Arm system**
  - **Disarm system**
- **Sch. No** – Determines scheduler number assigned to a certain action.
- **Status** – Determines scheduler status (enabled/disabled).
- **Hour** – Determines the point in time when the scheduler is to take effect in hours.
- **Minutes** – Determines the point in time when the scheduler is to cease to take effect in minutes.
- **Mo/Tu/We/Th/Fr/Sa/Su** – Determines day (-s) in the week when the scheduler is to be valid.

7.4. Zones

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

EPIR3 comes equipped with 1 wireless zone and 1 on-board zone. For more details regarding zone expansion, please refer to section **7.4.2. Zone expansion**.

EPIR3 zones are classified by 3 categories:

Zone category	Description	Max. number of zones per device	Max. number of zones in total
On-board zones	Built-in wired zones of EPIR3 alarm system.	2	2*
Wireless zones	Non-physical zones automatically created by connected wireless devices.	2*	32**
Virtual zones	Non-physical zones intended for Panic button feature (alarm activation upon pressing the button) on EWK1/EWK2 wireless keyfob. Virtual zones can be manually created using *ELDES Configuration Tool* software.	32***	32***

* - Depends on the connected wireless device.
** - Available only if no virtual zones are present.
*** - Available only if no wireless zones are present.

7.4.1. Zone numbering

The zone numbers ranging from Z1 through Z2 are permanently reserved for on-board zones. The Z3-Z34 zone numbers are automatically assigned to the created virtual zones and the wireless devices connected to the system in the chronological order.

7.4.2. Zone expansion

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

- binding wireless devices (see section **3. HOW TO MANAGE THE WIRELESS DEVICES**).
- creating virtual zones (see *ELDES Configuration Tool* software's Help section).

The maximum supported number of zones is 34.

7.4.3. Zone type definitions



- **Interior Follower** – If the zone is violated it will cause an instant alarm followed by single notification delivery even if the zone has been violated multiple times or another Interior Follower-type zone has been violated while alarm period (by default - 1 minute) is in progress. Typically, this zone is used for indoor protection devices, such as motion detectors, installed close to the exit/entry doors.
- **Instant** – The alarm is instantly caused if this zone is violated. After each alarm notification will be sent to user. This zone type is usually used for windows or other zones, and shock detectors.
- **24-Hour** – When the system is either armed or disarmed, the zone will cause instant alarm if violated. Normally, this type of zone is used for securing the areas that require constant supervisory.
- **Delay** – This zone type can be violated during exit and entry delay without causing an alarm. If the zone is violated when the system is armed, it will initiate entry delay countdown intended for the user to disarm the system. If the zone is left violated after the exit delay expires, it will cause an instant alarm.

NOTE: If one more zone with Stay-enabled attribute exist and the Delay-type zone is not violated and restored during exit delay, the system will be armed in Stay mode (see section **3.3.5. About STAY mode and how to activate it by EKB3W**). Typically, this zone type is used for door contacts installed at designated exit/entry doors.

- **Fire** – If this zone type is violated when the system is either armed or disarmed, the alarm will be instantly caused and the siren will emit pulsating sound. Typically, this zone type is used for flame and smoke detectors.
- **Panic/Silent** – This zone operates the same as 24-Hour zone type, but the system will not activate the siren and keypad buzzer if violated. Normally, this zone type used for panic alarm buttons.

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

7.4.4. Zone attributes

- **Stay** – If this attribute is enabled, the zone, regardless of type, will not cause an alarm if violated when the system is Stay armed. For more details on arming the system in the Stay mode, please refer to section **3.3.5. About STAY mode and how to activate it by EKB3W**.

- **Force** – This attribute determines whether the system can be armed or not while a zone is violated. If a zone with the Force attribute enabled is left violated until the exit delay expires, it will be ignored. Once the system is armed and the zone is restored, the violation will not be ignored and the zone will operate according to the determined type. For more details on zone types, please refer to section **7.4.3. Zone type definitions**.

7.4.5. Zone names



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

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

7.5. Tampers

The tamper circuit is a single closed loop such that a break in the loop at any point will cause a tamper alarm regardless of the system status – armed or disarmed. During the tamper alarm, the system will activate the siren and the EKB3W wireless keypad buzzer (if violated tamper is the keypad's tamper on board) and send the SMS text message to the preset user phone number. The system will cause tamper alarm under the following conditions:

- If the enclosure of the EPIR3 system or wireless device is opened, the physical tamper switch will be triggered. By default, indicated as *Tamper x* in the SMS text message (x = tamper number).
- If the wireless signal is lost due to low signal level or low battery power on a certain wireless device and does not restore within 60 minute period. This event is identified as Wireless Signal Loss. By default, indicated as No wireless signal in the SMS text message [wless-dev] [wless-id] [Tamper x] (*wless-dev* = wireless device model; *wless-id* = 8-digit wireless device ID code; x = tamper number).

By default, tamper alarm notification by SMS text message is enabled

7.5.1. Tamper names



Each tamper has a name that can be customized by the user. The tamper names are used in SMS text messages that are sent to the user during the tamper alarm. By default, the tamper names are: *Box Tamper, Tamper 2, Tamper 3, Tamper 4 etc.*

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

7.6. Programmable (PGM) outputs

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

EPIR3 comes equipped with EW2,EW2B wireless zone and PGM output expansion module support allowing to connect up to two devices or relays per module. For more details on how to bind the wireless devices, please refer to section **3. HOW TO MANAGE THE WIRELESS DEVICES**.

7.6.1. PGM output numbering

The PGM output numbers ranging from C1 through C32 are automatically assigned to the wireless devices connected to the system in the chronological order.

7.6.2. PGM output names



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

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

7.6.3. Turning PGM outputs ON and OFF

By default, all PGM outputs are turned OFF and the PGM output state is set to OFF when the system starts-up.

The PGM output can be turned ON for a determined time period and automatically turned OFF when the time period expires. As well as it can be turned OFF for a determined time period and automatically turned ON when the time period expires

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

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

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

7.6.4. PGM output type definitions

- **Output** - Operates as normal PGM output that can be controlled by the user. Normally, this type is used for any device or relay.
- **Siren** - Operates as siren output that automatically activates during alarm. Typically, this type is used for bell/siren connected to EW2,EW2B wireless device.

7.7. Siren

When the system is in alarm state, the siren will sound until the set time (By default - 1 minute) expires or until the system is disarmed.

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

7.7.1. Bell Squawk

If enabled, the siren indicates the completed system arming and disarming process. After the system is successfully armed, the siren/ bell will emit 2 short beeps and 1 long beep after the system is disarmed.

7.7.2. Indication by EWS2 Indicators

When enabled, the built-in LED indicators of EWS2 wireless outdoor siren will flash during the alarm.

7.7.3. Indication by EWS3 Indicators

When enabled, the built-in LED indicators of EWS3 wireless indoor siren will flash during the alarm. In the event of burglary, 24-hour or tamper alarm, EWS3 will flash the blue LED indicators, while in case of a fire alarm, the device can flash the red LED indicator.

7.7.4. EWF1 Interconnection

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

By default, the interconnection feature is enabled and the siren alarm duration is 30 seconds.

7.7.5. Disabling and enabling siren if wireless signal is lost

If a wireless device loses its wireless signal for 60 minutes or longer, the system will send notification by SMS text message to user phone number and activate the siren. By default, the siren will be activated when wireless signal is lost.

7.8. Alarm indications and notifications

When a zone, depending on zone type (see section **7.4.3. Zone type definitions**), or tamper is violated, the system will cause an alarm. By default, the alarm duration is 1 minute (see section **7.7. Siren** regarding the alarm duration). During the alarm, the system will follow this pattern:

1. The system activates the siren.

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

b) The EKB3W wireless keypad buzzer will emit short beeps.

NOTE: Alarm must be caused only on EKB3W zone.

e) If one or more zones are violated and keypad are manually waked up, EKB3W will light ON the corresponding violated zone indicator (-s) ranging from 1 through 12. Indicator SYSTEM will flash if one or more high-numbered zones are violated. If one or more tampers are violated, indicator SYSTEM will light ON. For more details on viewing violated high-numbered zone and tamper numbers by EKB3W keypad, please refer to section. **3.3.8. Fault messages.**
For more details on how EKB3W keypad operates and indicates the alarms, please refer to section **3.3.1. Sleep mode, how to wake up EKB3W and view system alarms or faults.**

2. The system attempts to send an SMS text message, containing the violated zone/tamper name (see section **7.4.5. Zone names** and **7.5.1. Tamper names** on how to set a zone or tamper name respectively), to the first preset user phone number. The system will send SMS text messages regarding each violated zone/tamper separately.

a) If the user phone number is unavailable and the system fails to receive the SMS delivery report during 45 seconds, it will attempt to send the SMS text message to the next preset user phone number. The user phone number may be unavailable due to the following reasons:

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

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

3. By default, the system attempts to ring the first user phone number The system will dial regarding each violated zone/tamper separately.

a) When the call is answered, the system will shut down the siren and the user will be able to listen on the mobile phone for approx. 30 seconds to what is happening in the area, surrounding the alarm system.

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

- mobile phone was switched off.
- mobile phone was out of GSM signal coverage.
- provided “busy” signal.

- user did not answer the call after several rings, predetermined by the GSM operator.

c) The system will continue dialing the next preset user phone numbers in the priority order until one is available. The system will dial the user phone number 5 times if the first user phone number was out of GSM signal coverage/switched OFF, otherwise the system will dial only once. If the system ends up with all unsuccessful to contact any preset user phone number, will stop dialing and will not return to the first user phone number.

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

To silent the siren as well as to cease system phone calls and SMS text message sending to the user phone numbers, please disarm the system using a free of charge phone call, SMS text message, EKB3W wireless keypad or EWK1/EWK2 wireless keyfob.

For more details details on how to disable/enable SMS text messages and phone calls to preset user phone number in case of alarm, please refer to section **7.9. System notifications.**

NOTE: Phone calls to the preset user phone number in case of alarm are disabled by force when MS mode and/or Smart Security feature is enabled (see section **7.11. Monitoring station**).

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

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

7.9. System notifications

By default in case of a certain event, the system attempts to send an SMS text message to the first preset user phone number only. If the user phone number is unavailable and the system fails to receive the SMS delivery report during 45 seconds, it will attempt to send the SMS text message to the next preset user phone number, assigned to the same partition as the previous one. The user phone number may be unavailable due to the following reasons:

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

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

To change the SMS text message delivery algorithm, user can enable/disable the following parameters for certain events:

- **Send SMS text message to all users simultaneously** - This parameter determines whether to ignore

the SMS delivery report or not. Once enabled, the system will attempt to send the SMS text message to every preset user phone number that is enabled to receive a certain event from the system by SMS text message. In addition, this parameter overrides the SMS delivery report parameter regardless of the SMS delivery report parameter's status (enabled/disabled).

- **SMS delivery report** - This parameter determines whether to request for SMS delivery report or not. Once disabled, the system will not verify the status of the SMS text message delivery and will attempt to deliver the SMS text message only to the first preset user phone number regardless if the next preset user phone number (-s) is enabled to receive a certain event by SMS text message or not.

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

Seq. No.	Event	Description	
1	Tamper alarm		SMS text message sent to the user in case of tamper violation. Indicated as *Tamper x*.
2	Zone alarm		SMS text message sent to the user in case of zone alarm occurrence.
3	Mains power loss		SMS text message sent to the user in case the mains power supply is lost.
4	Mains power restore		SMS text message sent to the user in case the mains power supply is restored.
5	Periodical info		Info SMS text message sent to the user periodically by the set values.
6	System armed		SMS text message sent to the user regarding armed system.
7	System disarmed		SMS text message sent to the user about disarmed system.
8	System started		SMS text message sent to the user on system startup.
9	Low battery		SMS text message sent to the user in case the back-up battery runs below 8V.

Seq. No.	Event	Description	
10	System shutdown		When the system is running on backup battery power, it transmits the SMS text message before the back-up battery power is fully depleted.
11	Failed to arm		SMS text message sent to the user in case the system denies arming due to existing violated zone (-s)/tamper (-s).*
12	Wireless device low battery		SMS text message sent to the user in case the battery level of a wireless device reaches 5%.

***ATTENTION:** If this feature is disabled for the user who wishes to arm the system, notification regarding the failed arming will not be delivered.

13	Battery failed		SMS text message sent to the user in case the backup battery resistance is 2,5Ω or higher (battery is disconnected or requires replacement). Self-tested every 10 days.
14	Temperature exceeded		SMS text message sent to the user in case the temperature has increased above the MAX set value.
15	Temperature fallen		SMS text message sent to the user in case the temperature has decreased below the MIN set value.
16	Temperature sensor fault		SMS text message sent to the user in case the temperature sensor is faulty.

7.10. Back-up battery, mains power supply status monitoring and memory







The system comes equipped with a back-up battery maintaining power supply of the system when the mains power supply is temporally lost. The implemented feature allows the system to perform a self-test on the back-up battery and notify preset user phone number by SMS text message if:

- battery has failed and requires replacement – battery resistance is 2,5Ω or higher; self-tested every 10 days.
- battery power is running low – battery voltage is below 8V; constantly self-tested.

If the household electricity is unstable in the system installation area, the system may temporally lose its power supply and continue operating on the backup battery power. The system supervises the mains power supply and notifies preset user phone number by SMS text message as well as indicates system fault condition on the keypad (see section **3.3.8. Fault messages**) after 60 seconds after the mains power loss. When the mains power restores, after 120 seconds the system will notify the user by SMS text message and the keypad will no longer indicate system fault.

The configuration settings are stored in a built-in EEPROM memory, therefore even if the system is fully shut down, the configuration remains.

For more details on how to manage back-up battery and power supply notifications, please refer to section **7.9. System notifications.**

7.11. Monitoring staton

The system can be configured to report events to the monitoring station by transmitting data messages to the monitoring station. The system connects to the monitoring station when the MS (Monitoring Station) mode is enabled.

4-digit Account number (by default - 9999) must be set up on the system in order to identify the alarm system unit by the monitoring station.

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening is in progress. However, during the remote configuration session, firmware update process or remote listening process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening process is over.

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

7.11.1. Data Messages - Events

The configuration of data messages is based on Ademco Contact ID protocol. The data messages can either be transmitted to the monitoring station alone or with duplication by SMS text message to preset user phone number. For more details on system notifications by SMS text message, please refer to **7.9. System notifications.**

Seq. No.	Contact ID® Code	Event	Description
1	1110	Fire alarm	Transmitted in case a zone of Fire type is violated.
2	3110	Fire restore	Transmitted in case a zone of Fire type is restored.
3	1130	Burglary alarm	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is violated.

Seq. No.	Contact ID® Code	Event	Description
4	3130	Burglary restore	Transmitted in case a zone of Delay (if not disarmed before entry delay countdown is completed), Interior Follower or Instant type is restored.
5	1133	24-Hour zone alarm	Transmitted in case of zone of 24-Hour type is violated.
6	3133	24-Hour zone restore	Transmitted in case of zone of 24-Hour type is restored.
7	1144	Tamper alarm	Transmitted in case the tamper is violated.
8	3144	Tamper restore	Transmitted in case the tamper is restored.
9	1146	Panic/Silent zone alarm	Transmitted in case of zone of Panic/Silent type is violated.
10	3146	Panic/Silent zone restore	Transmitted in case of zone of Panic/Silent type is restored.
11	1158	Temperature risen	Transmitted in case of the temperature has increased above the MAX set value.
12	1159	Temperature fallen	Transmitted in case of temperature has decreased below the MIN set value.
13	1301	Mains power loss	Transmitted in case the main power supply is lost.
14	3301	Mains power restore	Transmitted in case the main power supply is restored.
15	1302	Low battery	Transmitted in case the backup battery voltage runs below 8V.
16	1308	System shutdown	When the system is running on backup battery power, it transmits the data message before the backup battery power is fully depleted.
17	1311	Battery failed	Transmitted in case the backup battery resistance is 2Ω or higher (battery requires replacement). The battery is self-tested every 10 days.
18	1381	Wireless signal loss	Transmitted in case the connection with any wireless device is lost.
19	3381	Wireless signal restore	Transmitted in case the connection with any wireless device is restored.

Seq. No.	Contact ID® Code	Event	Description
20	1401	Disarmed by user	Transmitted in case the system is disarmed.
21	3401	Armed by user	Transmitted in case the system is armed.
22	1403	Disarmed automatically	Transmitted in case the system is disarmed based on scheduled time.
23	3403	Armed automatically	Transmitted in case the system is armed based on scheduled time.
24	1456	Disarmed in Stay mode	Transmitted in case the system is disarmed in Stay mode.
25	3456	Armed in Stay mode	Transmitted in case the system is armed in Stay mode.
26	1570	Zone bypassed	Transmitted in case a violated zone is bypassed.
27	3570	Bypassed zone activated	Transmitted in case a bypassed zone is activated.
28	1602	Test event/Kronos ping	Transmitted for system online status verification purposes.
29	3626	Date/time not set	Transmitted in case system date & time is not set.
30	1900	System started	Transmitted on system start-up.

The following table refers to user codes included in arm/disarm data messages.

Type	Code
User Phone Number 1	0
User Phone Number 2	1
User Phone Number 3	2
User Phone Number 4	3
User Phone Number 5	4
User Phone Number 6	5
User Phone Number 7	6
User Phone Number 8	7
User Phone Number 9	8
User Phone Number 10	9
User Code 1	10

Type	Code
User Code 2	11
User Code 3	12
User Code 4	13
User Code 5	14
User Code 6	15
User Code 7	16
User Code 8	17
User Code 9	18
User Code 10	19
KeyFob 1	54
KeyFob 2	55
KeyFob 3	56
KeyFob 4	57
KeyFob 5	58
Scheduler	70
Remote Code (EGR100)	71

7.11.2. Communication





The system supports the following communication methods and protocols:

- GPRS network – EGR100, Kronos protocol.
- Voice calls (GSM audio channel) – Ademco Contact ID protocol.
- CSD (Cricuit Switched Data).
- SMS – Cortex SMS format.

Any communication method can be set as primary or backup connection. The user can set up to 3 backup connections in any sequence order.

Initially, the system communicates via primary connection with the monitoring station. By default, if the initial attempt to transmit data is unsuccessful, the system will make additional attempts until the data is successfully delivered. If all attempts are unsuccessful, the system will follow this pattern:

a) The system switches to the backup connection that follows in the sequence (presumably - Backup 1).

b) The system then attempts to transmit data by the backup connection.

c) If the initial attempt is unsuccessful, the system will make additional attempts until the data is successfully delivered.

d) If the system ends up with all unsuccessful attempts, it will switch to the next backup connection in the sequence (presumably - Backup 2) and will continue to operate as described in the previous steps. The connection is considered unsuccessful under the following conditions:

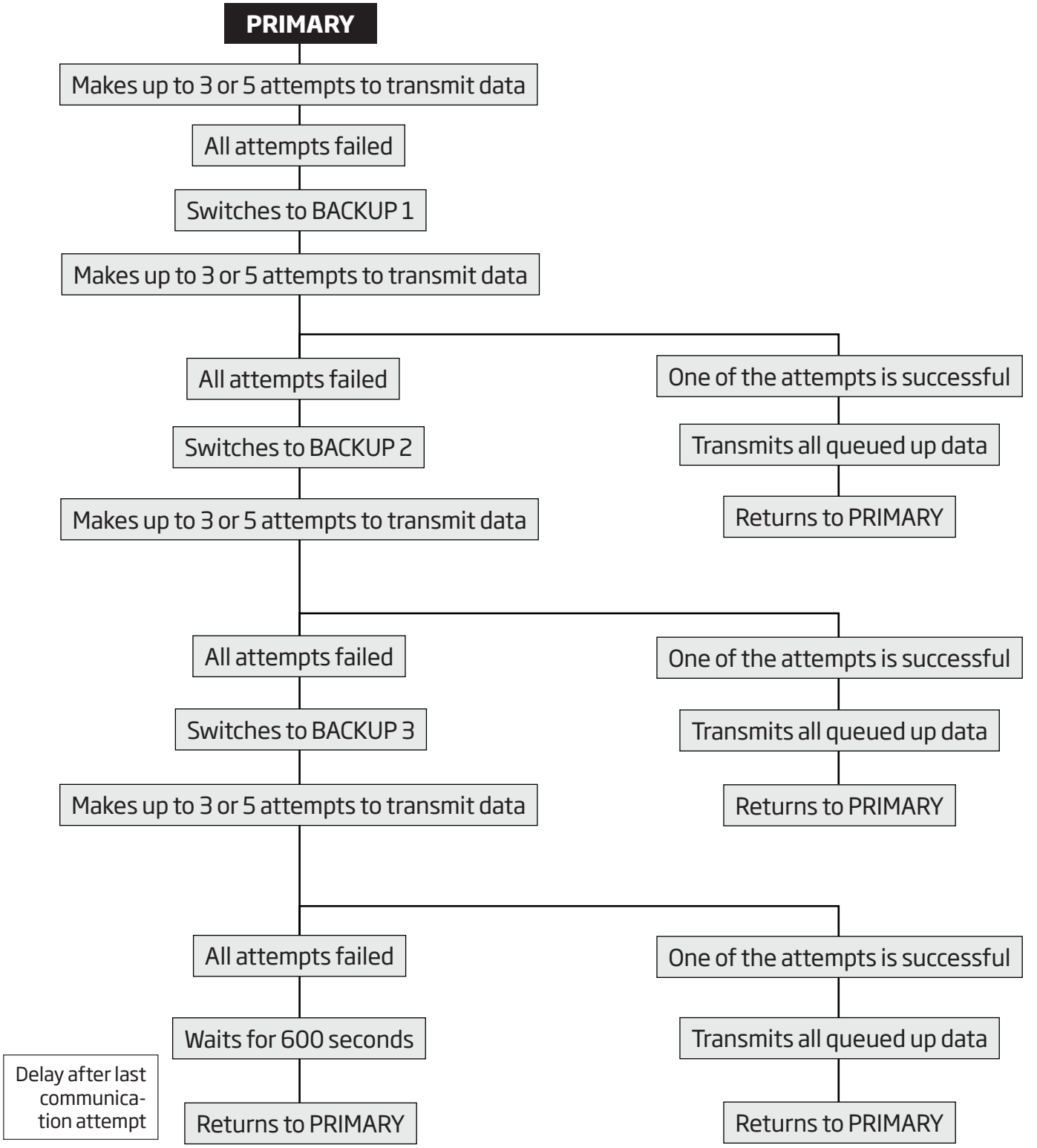
- **GPRS network** – The system has not received the ACK data message from the monitoring station within 40 seconds.
- **Voice calls:**
  - The system has not received the "handshake" signal from the monitoring station within 40 seconds.
  - The system has not received the "kissoff" signal from the monitoring station within 5 attempts each lasting 1 second.
- **CSD** – The system has not received the ACK data message from the monitoring station within 35 seconds.
- **SMS** – The system has not received the SMS delivery report from the SMSC (Short Message Service Center) within 45 seconds.

e) If one of the attempts is successful, the system will transmit all queued up data messages by this connection.

f) The system then returns to the primary connection and attempts to transmit the next data messages by primary connection.

g) If the system ends up with all unsuccessful attempts by all connections, it will wait until the *Delay after last communication attempt* time (By default – 600 seconds) expires and will return to the primary connection afterwards.

h) If a new data message, except Test Event (ping), is generated during *Delay* after last communication attempt time, the system will immediately attempt to transmit it to the monitoring station, regardless of *Delay* after last communication attempt being in progress.



NOTE: The number of attempts, indicated in the diagram, are default and depends on the determined communication method.

7.11.2.1. GPRS Network

The system supports data transmission to the monitoring station via IP-based networks by GPRS network. The supported data formats are the following:

- EGR100
- Kronos

To set up the system for data transmission via GPRS network, please follow the basic configuration steps:



1. Enable MS Mode parameter (see **7.11. Monitoring Station**).



2. Set 4-digit Account number (see **7.11. Monitoring Station**).



3. Set server IP address, which is a public IP address of the machine running EGR100 or Kronos monitoring station software.



4. Set server port, which is a port of the machine running EGR100 or Kronos monitoring station software.



5. Select TCP or UDP protocol. UDP is highly recommended for EGR100 data format.



6. Select data format: EGR100 or Kronos



7. In case EGR100 is selected, set 4-digit Unit ID number. Unit ID number can be identical to Account number.



8. Set up APN, user name and password provided by the GSM operator. Depending on the GSM operator, only APN might be required to set up.



By default, if the initial attempt to transmit data to the monitoring station via GPRS network method is unsuccessful, the system will make up to 2 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.



To report the online status, the system periodically transmits (By default – every 180 seconds) Test Event data message (ping) to the monitoring station via GPRS network

For detailed step-by-step instructions on how to establish the communication between EPIR3 alarm system and EGR100 middleware, please refer to the middleware's HELP file.

NOTE: The system is fully compatible with Kronos NET/Kronos LT monitoring station software for communication via GPRS network. When using a different monitoring station software, EGR100 middleware is required. EGR100 is freeware and can be downloaded at www.eldes.lt/ en/download

NOTE: Kronos NET/Kronos LT software communicates via TCP protocol, while EGR100 middle-ware v1.2 and up supports both – TCP and UDP protocols. However, TCP protocol is NOT recommend to use with EGR100.

ATTENTION: It is necessary to restart the system locally by powering down and powering up the system the system or remotely (see section **4. HOW TO PROGRAM THE SYSTEM USING YOUR MOBILE PHONE**) after changing the IP address or switching from TCP to UDP.

7.11.2.2. Voice Calls and SMS

The system supports up to 3 monitoring station phone numbers for communication with the alarm system by Voice Calls or SMS communication method using Ademco Contact ID or Cortex SMS data format respectively. Tel. Number 1 is mandatory, the other two can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone numbers must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for *UK: +441709111XXXX* . This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone numbers must be entered starting with 00 and an international country code in the following format: 00[international code][area code][local number], example for *UK: 00441709111XXXX*. This format can be used when setting up the phone number by EKB3W keypad.
- **Local** – The phone numbers must be entered starting with an area code in the following format: [area code] [local number], example for *UK: 01709111XXXX*. This format can be used when setting up the phone number by EKB3W keypad and *ELDES Configuration Tool* software.

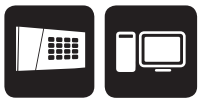
To set up the system for data transmission via Voice Calls or SMS, please follow the basic configuration steps:



1. Enable MS Mode parameter (see **7.11. Monitoring Station**).



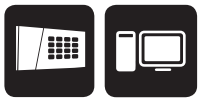
2. Set 4-digit Account number (see **7.11. Monitoring Station**).



3. Set Tel. Number 1... 3.



By default, if the initial attempt to transmit data to the monitoring station's Tel Number 1 via Voice Calls or SMS method is unsuccessful, the system will make up to 4 additional attempts. After all unsuccessful attempts, the system will continue to communicate with the monitoring station by switching to the next phone number that follows in the sequence and making up to 4 additional attempts if the initial attempt is unsuccessful. If all attempts to all phone numbers are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.



Due to the individual configuration of each monitoring station, the system may fail to deliver the data message via Voice Calls communication method. In such cases it is recommended to adjust the microphone gain until the optimal value, leading to successful data message delivery, is discovered.

7.11.2.3. CSD

The system supports up to 5 monitoring station phone numbers for communication with the alarm system by CSD communication method. Tel. Number 1 is mandatory, the other four can be used as backup phone numbers and are not necessary. The supported phone number formats are the following:

- **International (with plus)** – The phone number must be entered starting with plus and an international country code in the following format: +[international code][area code][local number], example for *UK: +441709111XXXX*. This format can be used when setting up the phone number by *ELDES Configuration Tool* software.
- **International (with 00)** – The phone number must be entered starting with 00 and an international country code in the following ž format: 00[international code][area code][local number], example for *UK: 00441709111XXXX*. This format can be used when setting up the phone number by EKB3W keypad.

To set up the system for data transmission via CSD, please follow the basic configuration steps:



1. Enable MS Mode parameter (see **7.11. Monitoring Station**).



2. Set 4-digit Account number (see **7.11. Monitoring Station**).



3. Set Tel. Number 1... 5.



By default, if the initial attempt to transmit data to the monitoring station's phone number via CSD method is unsuccessful, the system will make up to 4 additional attempts. If all attempts are unsuccessful, the system will switch to next backup connection that follows in the sequence and will attempt to transmit data until it is successfully delivered to the monitoring station.

7.12. System configuration using ELDES Configuration Tool software

Software *ELDES Configuration Tool* is intended for EPIR3 system configuration locally via USB port or remotely via GPRS network connection. This software simplifies system configuration process by allowing to use a personal computer in the process. Before starting to use *ELDES Configuration Tool* software, please read the user guide provided in the software's HELP section.
ELDES Configuration Tool is freeware and can be downloaded from at: www.eldes.lt

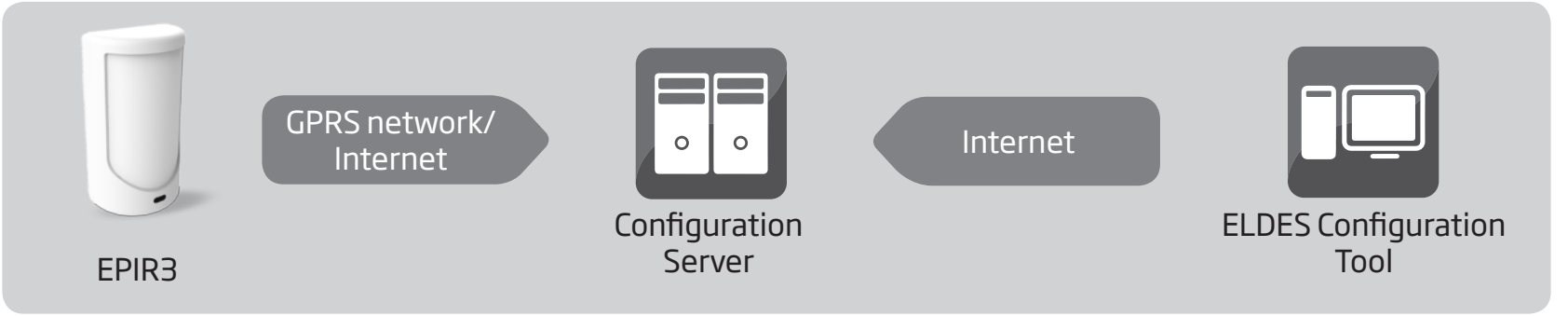
NOTE: *ELDES Configuration Tool* software is secured with administrator password. The default administrator password is 1470.

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening is in progress. However, during the remote configuration session, firmware update process or remote listening process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening process is over.

7.12.1. Remote system configuration via configuration server

Before configuring EPIR3 system remotely via GPRS network connection, please ensure that:

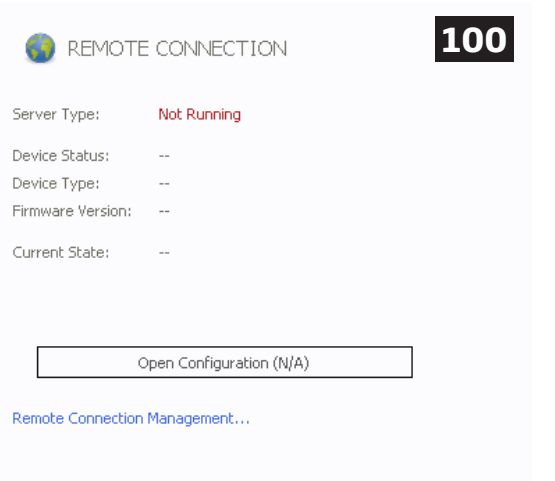
- SIM card is inserted into SIM card slot of EPIR3 device.
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to EPIR3 device.
- Default SMS password is changed to a new 4-digit password.
- At least User 1 phone number is set up.
- APN, user name and password are set up - please, contact your GSM operator to find out these parameters.



a) In order to activate a remote connection between EPIR3 system and ELDES configuration server, please send the following SMS text message from preset user phone number. Upon the successful SMS text message delivery, the system establishes a connection session for 20 minutes.

Initiate connection with ELDES server

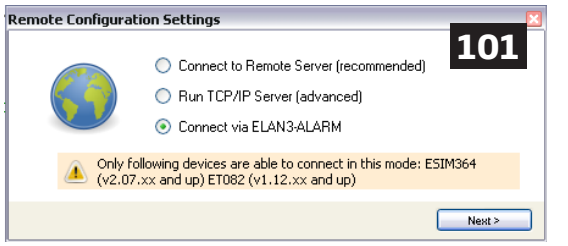
SMS text message content:
ssss_STCONFIG
Value: *ssss* – 4-digit SMS password.
Example:
1111_STCONFIG



b) Once the SMS text message containing device IMEI number and confirming a successful con-nection establishment is received, please run *ELDES Configuration Tool* software.

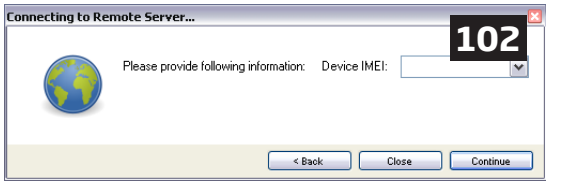
c) Click **Remote Connection Management...**

d) In the next window, select **Connect to Remote Server (recommended)** and click **Next** button.



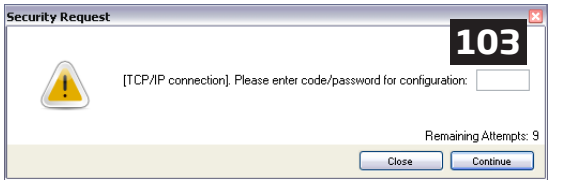
e) In **Device IMEI** entry, enter the IMEI number previously received by SMS text message.

f) Click **Continue** button.

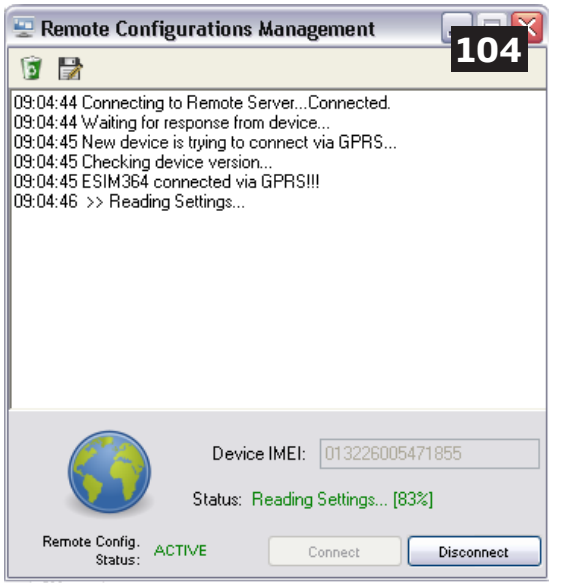


g) By default, upon the successfully established connection, the system will prompt for an administrator password..

h) By entering a valid administrator password, the system grants access to full configuration remotely.



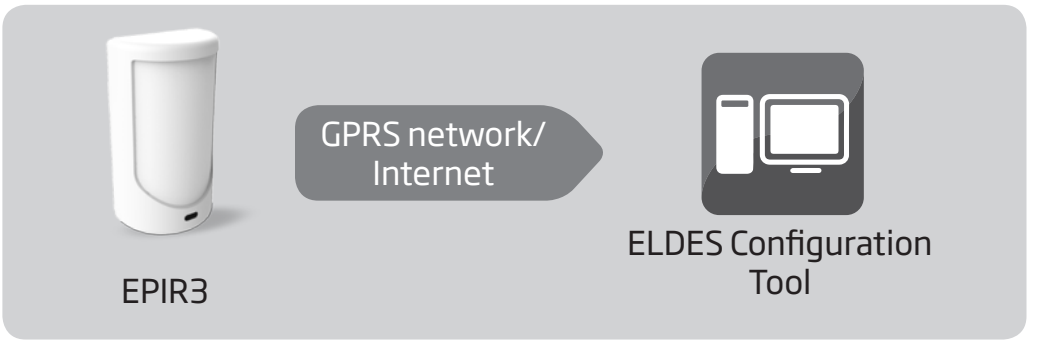
i) **Remote Configuration Management** window displays all performed configuration ac-tions and connectivity information.



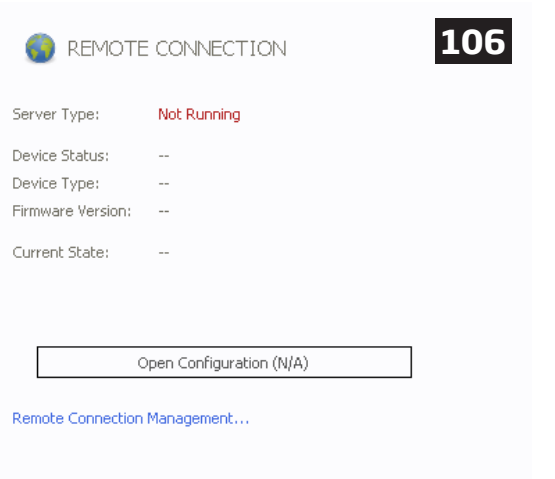
7.12.1. Remote system configuration via direct connection

Before configuring EPIR3 system remotely via GPRS network connection, please ensure that:

- SIM card is inserted into SIM card slot of EPIR3 device.
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to EPIR3 device.
- Default SMS password is changed to a new 4-digit password.
- At least User 1 phone number is set up.
- APN, user name and password are set up - please, contact your GSM operator to find out these parameters.
- Machine running *ELDES Configuration Tool* software provides access via public IP address.
- TCP port 5000 is forwarded for the IP address of the machine running ELDES Configuration Tool software.

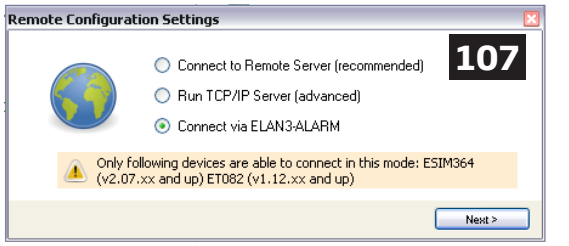


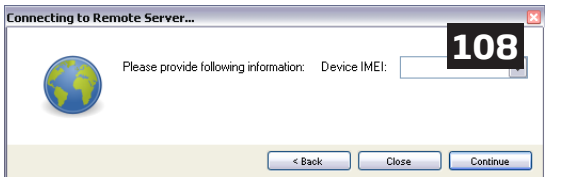
a) Run *ELDES Configuration Tool* software.
b) Click **Remote Connection Management...**
c) In the next window, select Run **TCP/IP Server (advanced)** and click Next button.
d) Set a TCP port for listening for incoming connections or leave the default TCP port 5000.
e) Click **Continue** button.
f) In order to activate a remote connection between EPIR3 system and *ELDES Configuration Tool* software running as remote configuration server, please send the following SMS text message from preset user phone number. Upon the successful SMS text message delivery, the system establishes a connection session for 20 minutes.

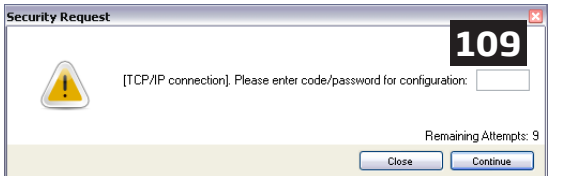


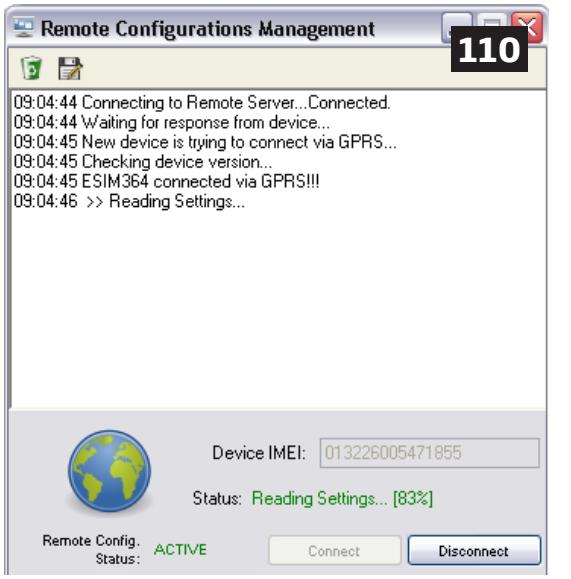
Initiate connection with ELDES Configuration Tool

SMS text message content:
ssss_STCONFIG:add.add.add.add:pprrt or
ssss_STCONFIG:host-name:pprrt
Value: *ssss* – 4-digit SMS password; add.add.add.add. – public IP address of the machine running ELDES Configuration Tool software; *pprrt* – TCP port number, range – [1... 65535]; *host-name* – public host-name of the machine running *ELDES Configuration Tool* software.
Example:
1111_STCONFIG:62.80.115.102:4522









g) By default, upon the successfully established connection, the system will prompt for an administrator password.
h) By entering a valid administrator password, the system grants access to full configuration remotely.
i) **Remote Configuration Management** window displays all performed configuration actions and connectivity information.

7.12.2. Ending the configuration process

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

- Click **Disconnect** or **Stop** button and close *ELDES Configuration Tool* software;
- The session will automatically expire in 20 minutes. Before the last 5 minutes, the software will offer the user to extend the session for another 20 minutes.
- Alternatively, the connection with the server can be terminated at any time by sending an SMS text message.

Terminate the connection

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

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

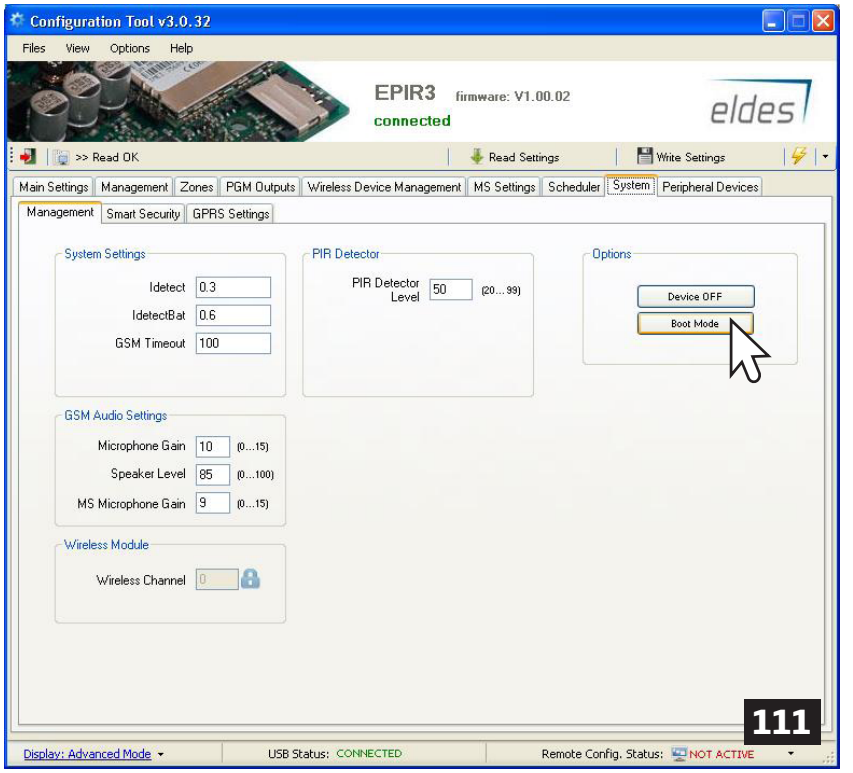
7.13. How to reset the system to default settings

1. Unplug USB cable (if any)
2. Open EPIR3 enclosure.
3. Press and hold the RESET button.
4. Wait for the LED to flash quickly several times.
5. Power down EPIR3.
6. Power up EPIR3.
7. Configuration has been restored to default.

7.14. How to upgrade the firmware locally via USB connection

1. Disconnect the power supply and backup battery..
2. Open EPIR3 enclosure.
3. Connect EPIR3 to the PC via USB cable.
4. Press and hold the RESET button.
5. Connect the power supply.
6. Release the RESET button after the new window pops-up containing a .bin file. Otherwise open My Computer and look for Boot Disk drive.
7. Delete the .bin file located in this drive.
8. Copy and paste in the very same window.
9. After the copying is done, power down EPIR3.
10. Unplug USB cable.
11. Power up EPIR3.
12. Firmware upgraded.

NOTE: Alternatively, boot mode for EPIR3 firmware upgrade can be activated using ELDES Configuration Tool software.



7.15. How to upgrade the firmware remotely via GPRS connection

ATTENTION: The system will NOT send any data to the monitoring station while remote configuration, remote firmware update or remote listening is in progress. However, during the remote configuration session, firmware update process or remote listening process, the data messages will be queued up and transmitted to the monitoring station after the remote configuration session, firmware update or remote listening process is over.

Before updating the firmware remotely via GPRS connection, make sure that:

- SIM card is inserted into SIM card slot of EPIR3 device.
- Mobile internet service (GPRS) is enabled on the SIM card.
- Power supply is connected to EPIR3 device.
- Default SMS password is changed to a new 4-digit password.
- At least User 1 phone number is set up.
- APN, user name and password are set up - please, contact your GSM operator to find out these parameters.

FOTA

EPIR3 alarm system supports FOTA (firmware-over-the-air) feature. This allows to upgrade the firmware remotely via GPRS connection. Once the upgrade process is initiated, the system connects to the specified FTP server address where the firmware file is hosted and begins downloading and re-flashing the firmware. The firmware file must be located in a folder titled **Firmware**. In order to initiate the upgrade process, please, send the following SMS message.

SMS text message content:

XXXX_FOTA:ftp-server-IP,port, firmware-file-name.bin,user-name,password

Value: *ftp-server-IP* - IP address of FTP server where EPIR3 firmware file is stored; *port* - port number of FTP server (usually - 21); *firmware-file-name.bin* - name of the firmware file, allowed max. length - up to 31 character; *user-name* - user name of FTP server login, allowed max. length - up to 31 character; *password* - password of FTP server login, allowed max. length - up to 31 character.

Example:

1111_FOTA:84.15.143.111,21,EPIR3fw. bin,eldesuser,eldespassword

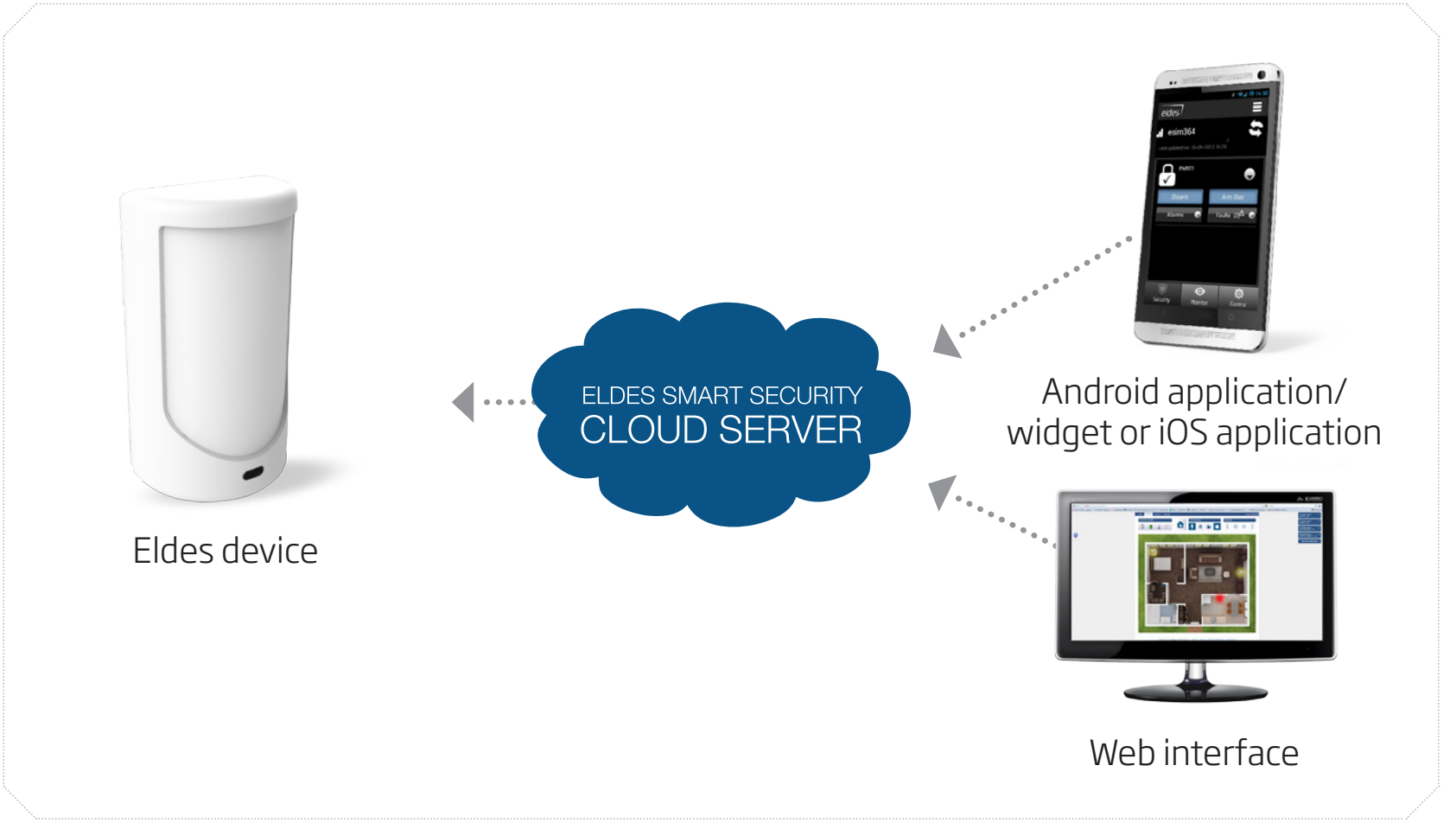
ATTENTION: Comma character is NOT allowed to use in user name and firmware file name.

ATTENTION: "ELDES UAB" does not run a FTP server and does not host the firmware files online. Please, contact your local dealer to request the latest firmware file.

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

7.16. Smart Security

ELDES Smart Security is a cloud-based platform providing a user-friendly graphical interface intended for system status monitoring and control. The solution consists of:



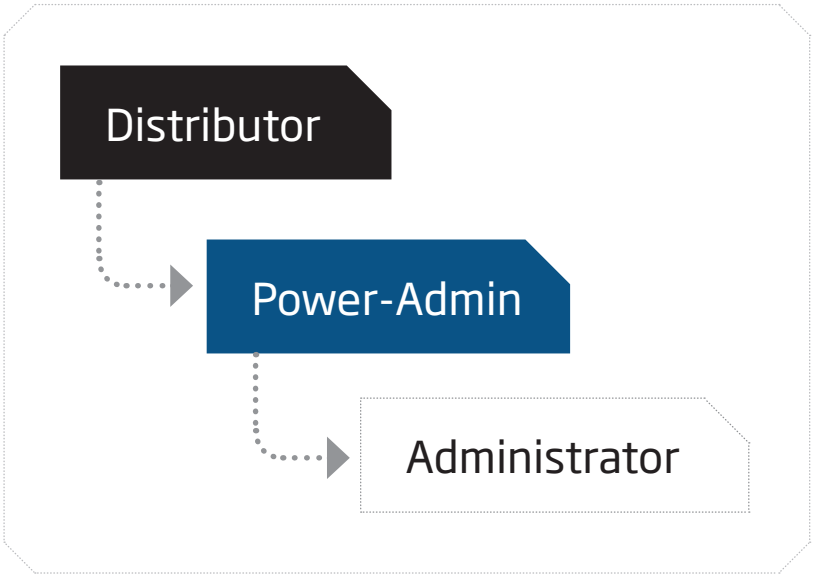
- **ELDES device** – The following ELDES devices come or can be equipped with ELDES Smart Security:
  - ESIM364
  - EPIR2
  - EPIR3
  - ESIM120
  - any other ELDES device on request
- **Android application/widget and iOS application** – The graphical interface can be accessed via a smart-phone application developed for Android and iOS-based (iPhone, iPad) devices.
- **Web interface** – ELDES Smart Security grants access to the device configuration (ESIM120) and user administration options as well as all features mentioned above when accessed via a web-browser.
- **ELDES Smart Security cloud server –** The server links all ELDES Smart Security components to each other.

ELDES Smart Security solution allows to perform the following*:

- Arm/disarm the system
- Control any electric appliance connected to the output of the ELDES device
- View system faults and alerts
- Monitor GSM signal strength, back-up battery level and temperature

* - depends on the ELDES device in use. For more details on the available features, please refer to ELDES device user manual.

User hierarchy



For more details on Smart Security solution, please refer Smart Security manual located at www.eldes.lt/download

8. Related products



EWP1 - wireless PIR sensor (motion detector)



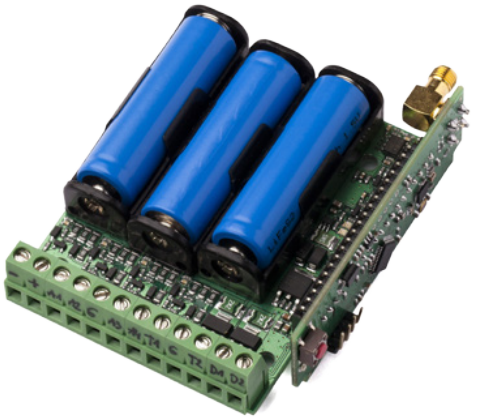
EWD1 - wireless magnetic door contact



EWS2 - wireless external siren



EWF1 – wireless smoke detector



EW2 - wireless zone and PGM output expansion module



EKB3W – wireless LED keypad



EWK2 - wireless keyfob



EWD2 - wireless magnetic door contact/ shock sensor/flood sensor



EWS3 - wireless internal siren



EWP2 - wireless PIR sensor (motion detector)



EWR2 - wireless signal repeater

Contents of pack:

Item	Quantity
EPIR3 alarm system	1
Power supply	1
User manual	1
MiniUSB cable	1
Back-up battery	1
Screws	1
5,6kΩ resistor	1

Not included: You will need to supply your own SIM card – we recommend you get a contract SIM, not Pay As You Go.

Limited Liability

The buyer agrees that the system will reduce the risk of fire, theft, burglary or other danger but that it does not guarantee against the occurrence of such events.

ELDES UAB will not take any responsibility for the loss of personal effects, property or revenue whilst using the system. The liability of ELDES UAB is limited to the value of the system purchased.

ELDES UAB is not affiliated with any mobile/wireless/cellular provider and is therefore not responsible for the quality of such services.

Manufacturer's Warranty

The system carries a 24-month manufacturer warranty from ELDES UAB.

The warranty begins the day the system is purchased by the user and the receipt must be retained as proof of purchase date. 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.

Dear Customer,

Thank you for choosing to purchase the EPIR3 alarm system to protect your property. Your thoughtful decision will ensure reliable protection for many years as all ELDES products are manufactured to meet the highest standards.

We are confident that you will be completely satisfied with your product. However, in the unlikely event that you do experience a problem, please contact the dealer from whom you made your purchase.

UAB ELDES
www.eldes.lt

User Manual v1.2

Valid for EPIR3 v01.02.00 and up
(later referred to as 'the EPIR3', 'the system', 'the device' 'the unit' or 'the detector')

Please read and follow these safety guidelines to safeguard yourself and others:

- DO NOT use the system where it can interfere with other devices - such as medical devices
- The alarm system radio transceiver operates in the GSM850, GSM900, GSM1800 and GSM1900 bands
- DO NOT use the system in hazardous environments
- DO NOT expose the system to high humidity, chemical environments or mechanical impact
- DO NOT attempt to repair the system yourself - any repairs must be carried out by fully qualified personnel only

The EPIR3 comes with its own power supply unit so you can plug it in straight away. The unit is not meant for outdoor use, i.e. you should use it inside a building and the power supply must be plugged into a standard Euro 2-pin socket or UK 3-pin socket (depending on the version you have bought). The main circuit should be protected by short circuit or over-current protection.

Please use the power supply unit which comes with your EPIR3, as it meets the EN 60950-1 standard. Any additional device you connect to the system, such as a computer, must also be powered by an EN 60950-1 approved supply.

Disconnect the mains power before installing. Never install or carry out maintenance during stormy weather. The electric socket that powers the system must be easily accessible. In case of power cut, the system is powered by a back-up battery.

WARNING: Only use the approved back-up battery with the system to avoid fire or explosion. Take care when connecting positive and negative battery terminals.

To switch the system off, unplug the external electric power supply and disconnect the battery by first removing the front cover of the device. A blown fuse cannot be replaced by the user. The replacement fuse has to be of the kind indicated by the manufacturer (fuse F1 model – MINISMDC050F 0.5A; fuse F2 model - MINISMDC020F 0.2A).

If you use a computer to select your ideal settings, it must be earthed.



The WEEE (Waste Electrical and Electronic Equipment) symbol on this product (see left) means it must not be disposed of in household waste. To prevent possible harm to human health and/or the environment, you must dispose of this product in an approved and environmentally safe recycling facility. For further information contact your system supplier, or your local waste authority.

Made in the European Union
www.eldes.lt