# AlarmView+

Wireless Intruder Alarm System
with Visual Verification

# Guardian+

Wireless Intruder Alarm System

# AVR+

Visual Verification Add-on


# Installation Guide

PIMA WIRELESS

## Table of contents

## Appendixes



## Figure index



## NOTICE AND DISCLAIMER

This guide will help installers and operators in the safe and efficient installation and use of the wireless systems described herein.

Before trying to install and use the systems, read this guide and become familiar with all safety requirements and operating procedures.

- The system must not be used for purposes other than those for which it was designed.
- The use of the software associated with the system is subject to the terms of the license provided as part of the purchase documents.
- PIMA Electronic Systems Ltd.'s exclusive warranty and liability is limited to the warranty and liability statement provided in this manual and the peripherals guide (P/N 4410399).
- This guide describes the maximum configuration of the systems with the maximum number of functions, including future options. Therefore, not all functions described in this guide may be available in a specific system.
- Warnings are given for situations and circumstances in which a possible hazard can arise.
- Cautions are given for situations or circumstances in which the system can possibly be damaged.
- Notes are given for situations that need special attention, or to improve the operating procedure.
- Wrong operation, or failure of the operator to effectively maintain the system, relieves the manufacturer (and seller) from all or any responsibility for consequent noncompliance, damage, or injury.
- The text and graphics contained in the guide are for the purpose of illustration and reference only. In no event shall manufacturer be liable for any special, direct, indirect, incidental, consequential, exemplary or punitive damages (including, without limitation, any and all damages from business interruption, loss of profits or revenue, cost of capital or loss of use of any property or capital or injury).

## Graphic signs in this guide

| Icon | | Description |
|---|---|---|
|  | **Caution** | Issues that may cause malfunctions |
|  | **Warning** | Issues that may cause damage and actual bodily harm |
|  | Note | Important note |

# 1 Introduction

This guide will help you to install PIMA's Wireless Intruder Alarm Systems: the AlarmView+, the Guardian+ and the AVR+. The three systems are easy to install, plug-n-play, and provide wireless intruder alarm capabilities, with or without Visual-Verification and optional remote Look-in.

Suitable for residential and small business applications, they present a comprehensive solution for security and personal safety.

Incorporating the PIMAlink cloud service and smartphone application by PIMA, users of the alarm system[1] can receive all alarm and other notifications via the app and can remotely perform the following operations:

- Arm/disarm
- Receive look-in images
- View zones and system status
- Bypass zones
- Stop the sirens
- Program the control panel

PIMA Wireless products include a range of various peripherals – detectors, sensors, cameras, etc.

The AlarmView+ and AVR+ offering incorporates the SmartView PIR/Camera that combines movement detection and image capturing, the OutView Wireless camera and a wide range of regular detectors.

With the Visual Verification, on an alarm event, the cameras transmit both the alarm event and the images to the control panel, which sends them over GPRS/GSM to the Monitoring Station, and optionally to the user's mobile phone or email.

Note that all three alarm systems have two versions: Single SIM, and Dual SIM. Single SIM systems cannot utilize any of the features of the dual SIM systems.

## 1.1 Version 2.10 new features

1. Support in PIMAlink cloud service
2. Support in PIMAlink smartphone application

[1] Starting system version 2.10

## 1.2 The AlarmView+


Figure 1. The AlarmView+ and PIMAlink diagram

### 1.2.1 Features

- Integrated PIMAlink (see section 1.5) cloud service and smartphone application
- Visual Verification images are sent to the system's contacts, by the PIMAlink app, or by MMS and E-mail messages.
- Remote Look-in images requests, by the PIMAlink app, or by text messages
- Remote Upload/Download initiation by the IP Receiver CMS software(without SMS)
- Wireless peripherals, including movement/smoke detectors, panic buttons, wireless keypad, key fobs, door contacts, etc.
- "SmartView" detector and camera with:
  - "Matched field-of view" between the detector and the camera, with no dead spots
  - Lowlight flash correction
  - High quality color images
- OutView outdoor camera
- Double and backup reporting
- Supports dual SIM
- End-user notifications by PIMAlink, SMS, MMS & E-mail
- Alarm reporting options:
  - ContactID and SIA, via GPRS with SMS back-up
  - Images via PIMAlink, MMS and E-mail

*MMS (Multimedia Messaging Service) costs money, including emails sent via this service.*

- Remote commands by PIMAlink or text messages
- PIMAlink notifications backup to contacts, by SMS and MMS
- Built-in Quad Band GSM/GPRS modem

- Advanced wireless visual link:
  - Two way supervised and secured radio network
  - 128-bit encryption key
  - Supervision report every 10 sec
  - 2.4 GHz FHSS (Frequency Hopping Spread Spectrum) & Diversity receiver (2 antennas)
- Supervised 868 MHz link for standard wireless peripherals
- Programmable trigger inputs (3)
- PGM output
- Graphical, menu-driven LCD display
- Easy battery replacement

## 1.3 The Guardian+

The Guardian+ is a full featured wireless alarm system, designed to answer the needs of most residential and small office installations. Based on the AlarmView+, it lacks the visual capabilities, including Visual Verification and look-in image options.

The Guardian+ peripherals are the same as those of the AlarmView+, except visual detectors and cameras.

The Guardian+ alarm system cannot be upgraded to include the complete enhanced visual features of the AlarmView+ system.

Figure 2. The Guardian+ alarm system

## 1.4 The AVR+ Visual Add-on

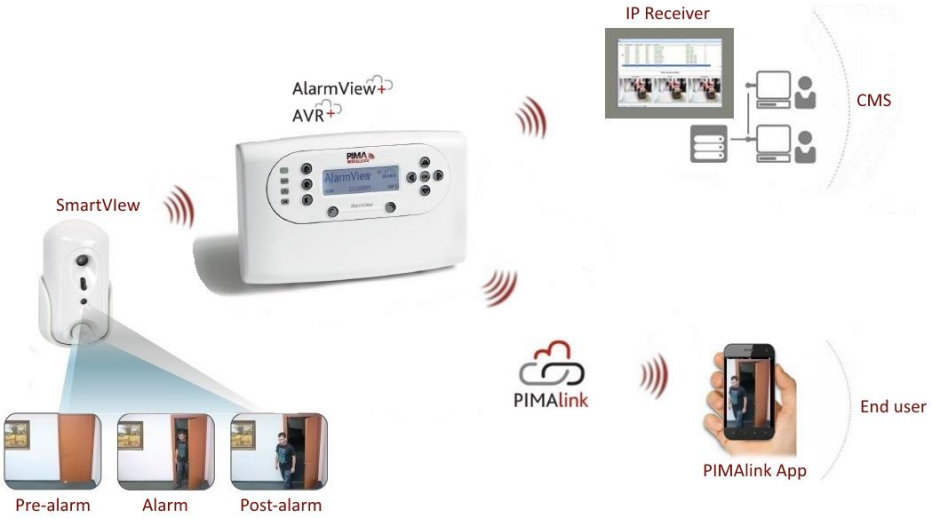



Figure 3. The AVR+ Visual Add-on

The AVR+ allows adding Visual Verification capacities to any intruder alarm system. Based on the AlarmView+ control panel, it is designed for sending Visual Verification and look-in images by up to 6 SmartView PIR/Cameras and OutView cameras.

By using trigger inputs and a PGM output, the AVR can do the following:

- Be Armed and Disarmed
- Trigger the external alarm system
- Serve as a GSM backup communication channel - when triggered by the external Alarm System (on alarm, for example), the AVR will report the CMS/end-user via GSM

### 1.4.1 Features

- Six SmartView PIR/Cameras or OutView cameras
- Trigger inputs: two for Arming and Disarming, one for communication Backup of the external alarm system
- One PGM output. It can be used for cellular backup of the master system alarm reporting
- Optional dual SIM
- Two way communication with the SmartView and OutView
- Alarm & image notifications to contacts via PIMAlink/MMS/SMS/E-mail
- Remote look-in images by contact requests (via PIMAlink/SMS)
- Remote Upload/Download initiation by the IP Receiver (without SMS)

## 1.5 PIMAlink

PIMAlink[2] is a PIMA cloud service and smartphone application, that allow receiving various push notifications and visual verification images from the alarm system, and remotely controlling it.

Every control panel that needs to be linked to the PIMAlink service, receives a special code that pairs it with the cloud service. This pairing code is also used for registering any smartphone with the PIMAlink app to the service.

### 1.5.1 Modes of operations

PIMAlink has 2 modes of operations, explained below:

1. CMS mode
2. Self-monitoring mode

#### CMS mode

In this mode, the control panel transmits the events to the IP Receiver at the CMS, which then relays it to the PIMAlink cloud and the end user. The IP Receiver does not delay, nor does it filter the transmissions, but the CMS can break the connection with PIMAlink, such in the case that the customer had canceled its subscription to the CMS.

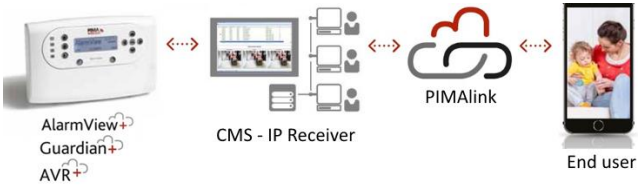



Figure 4. PIMAlink – CMS mode

[2] Starting ver. 2.10 of the AlarmView+/Guardian+/AVR+

### Self-monitoring mode

In this mode the end user receives notifications directly from the PIMAlink cloud to the app.


Figure 5. PIMAlink – self-monitoring mode

## 1.5.2 The PIMAlink app

The PIMAlink application allows its users to select on which events to receive notifications and on which not to. Up to 32 smartphones can be paired to a single alarm system.

Note that while the term "Users" is used both in the control panel and PIMAlink to refer to the same persons (who can arm and disarm the alarm system), the term "Contacts" may differ: normally, contacts of the alarm system will also be contacts of PIMAlink, but because there are only up to 6 contacts on the alarm system but up to 32 on PIMAlink, PIMAlink allows more persons to receive notifications.

The following and more operations are available using the PIMAlink application:

1. Receive push notifications on alarms, faults and other system events
2. Receive visual alarm verification images
3. Arm/disarm
4. Ask and receive look-in images
5. Bypass zones
6. Get the zone and system status
7. View the event log

## 1.6 Technical specifications[3]

| | |
|---|---|
| **General** | |
| Zones | Up to 30 of which 23 wireless, 1 hardwired, 6 visual |
| Wireless Peripherals | • Up to 6 key fob remotes, or keypads<br>• Up to 6 Panic buttons<br>• External siren |
| Arming modes | AWAY/HOME/PART |
| Alarm types | Silent, siren or sounder |
| Codes | 10 codes:<br>• Master user<br>• 6 users<br>• Duress<br>• Limited 24H<br>• Installer |
| Built-in siren | Piezoelectric, 85 dBA at 3 m |
| External siren | 1 siren, wireless (indoor/outdoor) |
| Event log | 256 events, non-volatile, with time and date stamp |
| Special functions | • Remote control by SMS from one (predefined) mobile phone, ensuring privacy and security.<br>• Remote Look-in via MMS Local USB connection for setup and firmware upgrade |
| I/O | 1 PGM output, 3 trigger inputs + trigger #1 can serve as zone #24 |
| Real-time clock | Time and date stamp |
| **Wireless** | |
| **Advanced wireless link for visual zones** | |
| Frequency Band | 2.4 GHz ISM band |
| TX Power | Up to 100 mW |
| Transmission method | • 2-way communication<br>• GFSK<br>• Frequency Hopping Spread Spectrum (FHSS) |
| Supervision | Up to 20 seconds |
| Secured wireless network | • 48-bit factory set ID code<br>• Built-in security using a link key (prevents unauthorized access)<br>• Data encryption (up to 48-bit) |
| Expected range[4] | Up to 100 m (outdoors) |
| **Wireless link for standard peripherals** | |
| Frequency | 868.6375 MHz |
| Supervision | Randomly, every 20-50 m + on every transmission |
| Transmission method | FM, narrow band |
| Expected Range | Up to 100 m outdoor. Can be extended indoors using the RP-15 Repeater |
| **Communication** | |
| **Modem** | |
| Interface | Quad-band GSM/GPRS |
| Report destinations | CMS Receivers, mobile phones, Email accounts |
| Reporting formats | SMS/MMS/E-mail (by SMTP)/GPRS-IP |

[3] The specifications of the detectors and accessories can be found in the peripherals guide (P/N 4410399)
[4] Range is impacted by building materials and interference

| | |
|---|---|
| End user contacts | Reporting options/formats:<br>• GSM/GPRS, SMS/MMS/Email (via mms) notifications<br>• 6 mobile phone numbers<br>• 6 E-mail accounts |
| CMS contacts | Reporting options/formats:<br>• GSM/GPRS, SMS/MMS/Email (via mms) notices<br>• 2 IP address<br>• 2 phone numbers<br>• 2 E-mail accounts |
| **Others** | |
| **Physical Characters** | |
| Casing | Plastic - PC/ABC 94/V0 |
| Weight:<br>With battery<br>Without battery | <br>687 gr<br>577 gr |
| Dimensions | 225 x 138 x 40 mm |
| **Environmental Data** | |
| Operating temperature | -10ºC - +49ºC |
| Storage temperature | -25ºC - +70ºC |
| Humidity | 85%, non-condensed |
| **Electrical Data** | |
| Power supply | +12VDC/1A |
| Current drain | 100 mA standby, 0.7A peak |
| Backup battery | +4.8 VDC,<br>4 x Ni-MH 2 Ah |

*The control panel reports on Low Battery condition 9-12 hours after AC loss. 1-4 hours later it will turn off. Overall, the control panel can stay more than 12 hours in standby mode.*

***We recommend using original AC adaptor and backup battery pack from PIMA Electronic Systems.***

# 2 Quick Reference Guide

## 2.1 System components

The alarm system consists of the control panel, and depending on the model, wireless zones (23), one hardwired zone, visual zones (6) and wireless peripherals (up to 36).

- The Control Panel: consists of the main circuitry, GPRS/GSM module, two wireless transceivers - standard and visual dedicated one.


Figure 6. The control panel

- Visual detectors:
  - SmartView: high quality, supervised, rapid-acquisition camera, with PIR detector.
  - OutView: high resistance outdoor camera, with trigger input from external sources, e.g., PIR detectors and magnets.
- Wireless detectors: the AlarmView system supports a wide range of wireless detectors, including door contacts, PIR and Pet-immune motion detectors, Smoke detectors, etc.
- Sirens: the control panel has a built-in siren. An external wireless siren (with a strobe) can also be installed.
- Keyfobs/keypads: accessories that are used to arm and disarm the AlarmView.
- Panic/Medical pendant and wrist watch: accessories that are used to send emergency and panic signals.

## 2.2 The Control Panel

The next figures show the control panel's buttons and parts. The three arming buttons are disabled in the AVR.

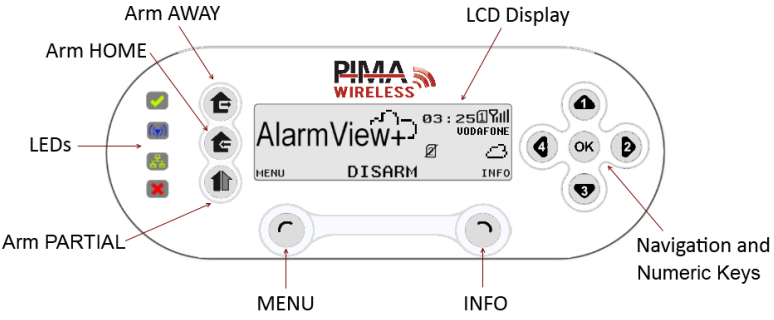



Figure 7. The control panel keys

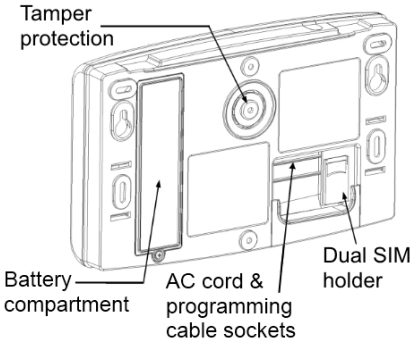



Figure 8. Control panel's back side

### 2.2.1 The buttons

The table below details the buttons of the control panel.

| Button | Function | Press to... |
|---|---|---|
| | AWAY | Arm AWAY (full) |
| | HOME | Arm HOME |
| | PART | Arm PARTIAL |
| | Left | Access the menus, Select , Insert |
| | Right | Display the system's status, Cancel, Delete |
| OK | OK | Confirm, Enter |
| 1 | Up | Scroll, type the characters A-Z, 0-9, #+_!@- space |
| 3 | Down | |
| 4 | Left | Scroll, Exit, Back, type numeral 4 |
| 2 | Right | Scroll, Enter, duplicate previous character, type numeral 2 |

## 2.2.2 The LCD display

The LCD screen displays the status, the current time, and the cellular provider and reception. See the following diagram for details.

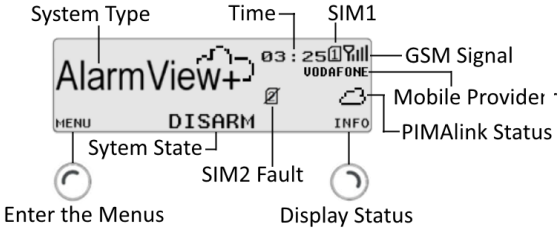



Figure 9. The LCD display and buttons

### The icons

The available icons are:

| | | | |
|---|---|---|---|
| | Transmission of SMS message | | Low backup battery |
| | GSM reception level | | Battery loss |
| | GSM network error | | SIM1 active, fault |
| | AC loss | | SIM2 fault[5] |
| | GPRS transmission | | SIM1+2 fault[5] |
| | PIMAlink connection OK | | PIMAlink unavailable |

## 2.2.3 Audible indications

The table below lists the sounds the Control Panel sounds.

| Tones | Sound | Sounded when... |
|---|---|---|
| ♪ | Single beep | key is pressed |
| ♪-♪ | Two beeps | menu timeout occurs – exit to main menu |
| ♪-♪-♪ | Three beeps | successful command or operation |
| ♪-♪-♪-♪... | Continuous beeps | at Entry/Exit delay |
| ♪--------♪ | Long beep | illegal command or entry refusal |
| 🔔🔔🔔 | Chime | the chime is activated |

[5] Displayed only in dual SIM systems

### 2.2.4 LED indications

The table below lists the color LEDs and their indications.

| LED | Color & Status | Description |
|---|---|---|
| | GREEN, ON | Power - OK |
| | BLUE, blinking | Wireless communication – OK |
| | GREEN, blinking | Cellular reception – OK |
| | OFF | No cellular reception |
| | ORANGE, 3 blinks | Event in process |
| | RED | System trouble; see display for info. |
| | WHITE, blinking | ALARM!<br>Enter the log or re-arm to stop blinking. |

### 2.2.5 The INFO screen

The INFO screen shows a grid of all active zones (up to #30, including visual zones, where available) in several status options. To display it, press the INFO button when the system is disarmed.

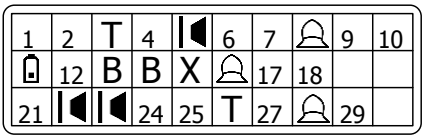



Figure 10. INFO screen example

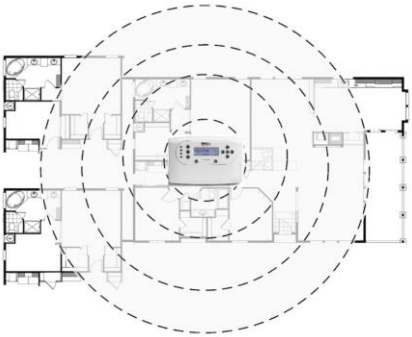
The next table explains the various zone indications. A zone with more than one status toggles between them, at one second interval.

| Status | Description | Zones in the above example |
|---|---|---|
| Empty cell | Undefined zone | 19, 20, 30 |
| 1-30 | Defined zone, Normal mode | 1, 2, 4, 6, 7, 9, 10, 12, 17, 18, 21, 24, 25, 27, 29 |
| | Open zone | 5, 22, 23 |
| T | Zone tamper open | 3, 26 |
| B | Bypassed zone | 13, 14 |
| | Low battery | 11 |
| X | Supervision loss | 15 |
| | Alarm | 8, 16, 28 |

# 3 System Installation

## 3.1 General guidelines

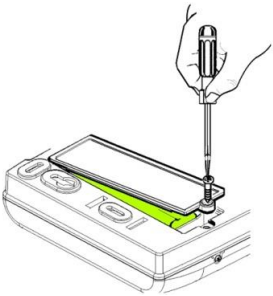
- The control panel should be installed at a location with optimum wireless reception from the detectors and peripherals.
- A convenient location for mains electricity supply and for user operation, near the main access point is preferable.
- For control panels which are operated using remote keypads, the panel can be concealed inside a cupboard or loft space in a convenient location for mains electricity supply.



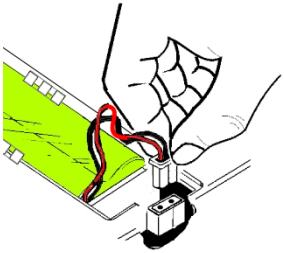
## 3.2 Quick installation

For quick installation, you can mount the control panel on any flat surface. To do that, do the following:

1. On the back side, release the crosshead ("Philips") screw of the battery compartment and remove the cover. The battery lies in the compartment, not connected.

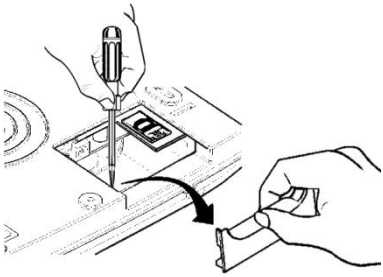


2. Connect the battery wires to the socket.



3. Close the compartment and fasten the screw.

4. Remove the plastic protector of the connectors' cavity, by applying pressure with a flathead screwdriver.



5. Insert the SIM card(s) to the SIM holder:
   a. In **single SIM** versions, insert the SIM card into the **upper slot** (labeled "SIM-1 Main").
   b. In **dual SIM** versions, first insert the backup SIM into the **lower slot** (labeled "SIM-2 Backup"), and then insert the main SIM into the **upper slot** (labeled "SIM-1 Main**"**). See the next figure.

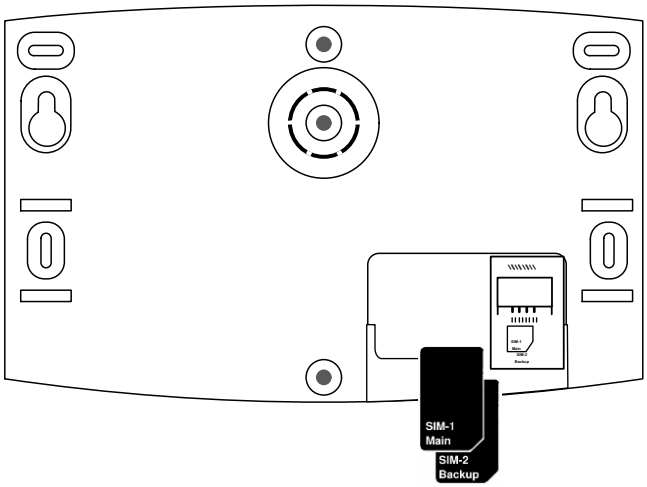
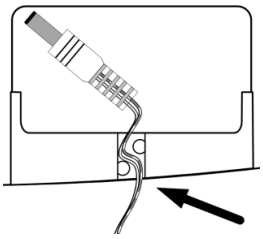


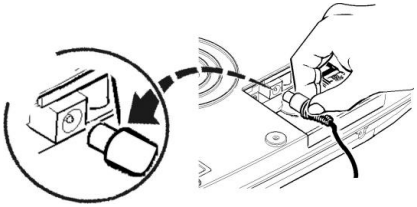

Figure 11. Inserting the SIM cards

- ***Do not use PIN Code SIM cards***
- ***Do not insert SIM cards under power (AC or DC)***

6. Attach the plastic protector back in place and pass the AC wires through the wires path.

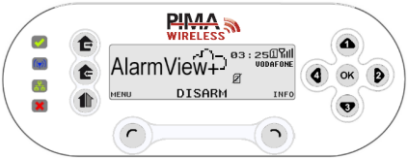


7. Plug the AC adapter into its socket, to the left of the SIM card holder



**Do not connect the AC adapter to power before connecting it to the control panel.**

8. Connect the AC adapter to power. Wait for the Power LED to light up and the LCD screen to show the normal display.
9. Ensure good reception of the wireless and GSM communications (see section 0, on page 30).




10. Secure the control panel to the designated surface: drill two holes, corresponding to the two keyhole hangers on the back plate and fasten the supplied screws, leaving a small space between the screw head and the surface.
11. Hang the control panel.

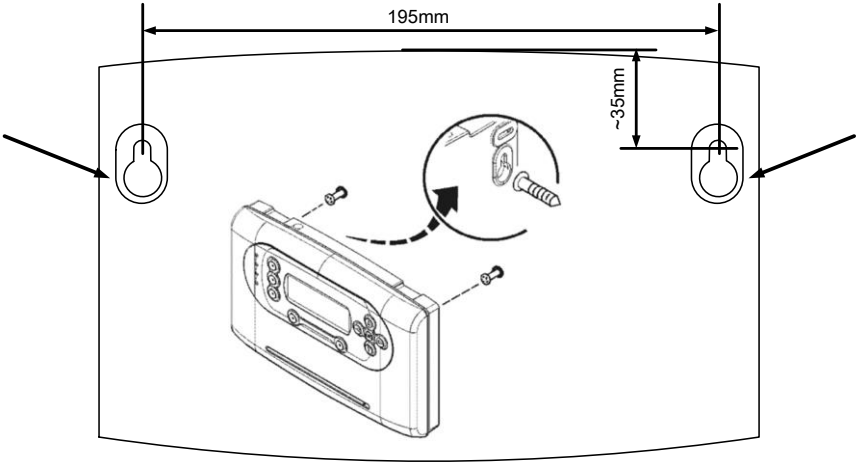
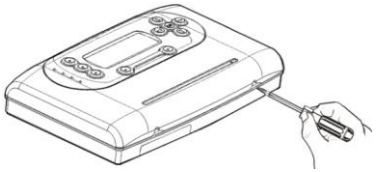



Figure 12. Quick installation diagram

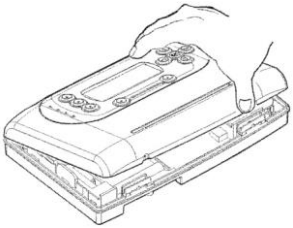
## 3.3 Professional mounting

If the control panel needs to be secured with a tamper protection, do the following steps:

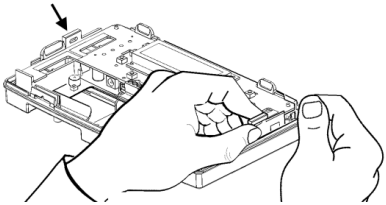
1. Open the front cover: insert a small flathead screwdriver into the two slots at the bottom of the control panel and apply pressure upwards.

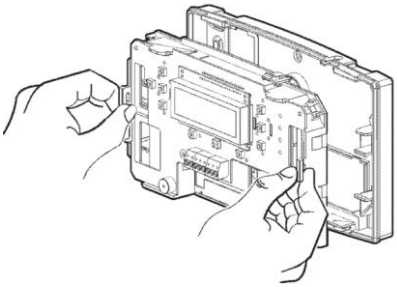


2. Lift and remove the front cover.

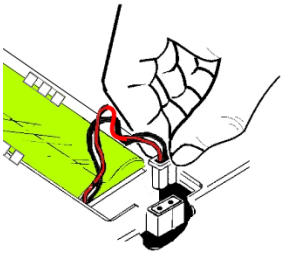


3. Pull out the plastic cradle of the circuit board, by pulling its two clips on both sides, and turn it over.





4. Connect the battery wires to the socket.



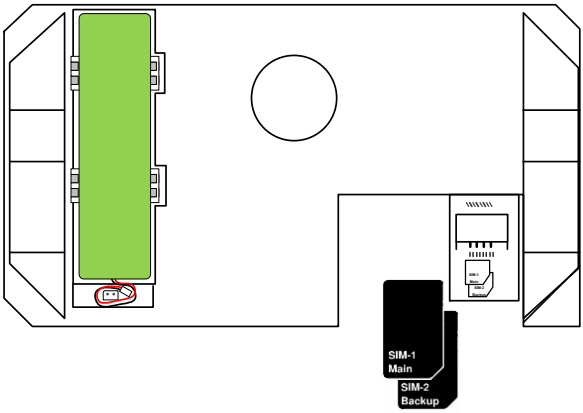



Figure 13. The back of the circuit's cradle

5. Insert the SIM card(s) to the SIM holder (see the previous figure):
   a. In **single SIM** versions, insert the SIM card into the **upper slot** (labeled "SIM-1 Main").
   b. In **dual SIM** versions, first insert the backup SIM into the **lower slot** (labeled "SIM-2 Backup"), and then insert the main SIM into the **upper slot** (labeled "SIM-1 Main**"**). See the previous figure.

- ***Do not use PIN Code SIM cards***
- ***Do not insert SIM cards under power (AC or DC)***

6. On the designated surface, drill holes, corresponding to those marked with arrows on the next figure and insert drywall plugs into them. Note, that the hole in the center of the back panel is designated for the tamper switch's knockout[6].

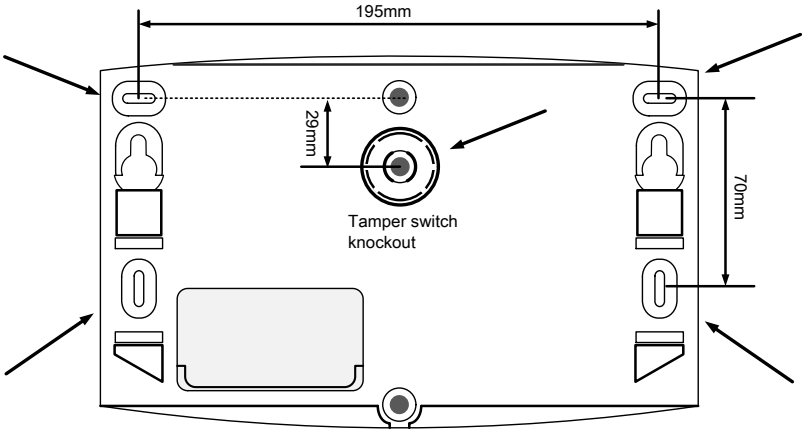
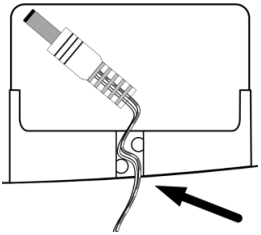



Figure 14. Wall mounting diagram

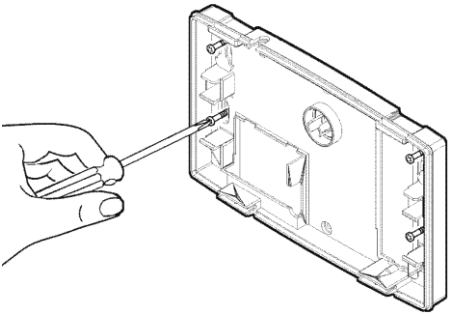
[6] When the control panel is forcibly removed from the wall, the knockout breaks and the tamper is activated.

***The tamper switch knockout must be secured with a dedicated screw, to comply with EN50131-1 regulation.***

7. Turn over the back panel and pass the AC adapter's plug and wires through the wires path.

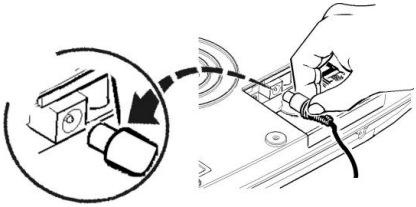


8. Turn over the back panel again and secure the it to the surface with screws.

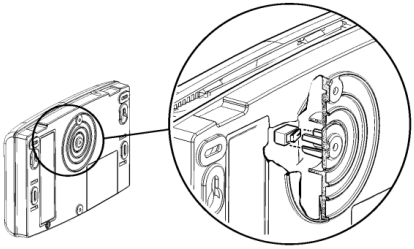


9. Plug the AC adapter into its socket, to the left of the SIM card holder.

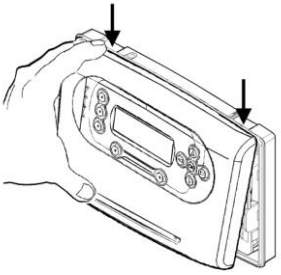
***Do not connect the AC adapter to power before connecting it to the control panel***

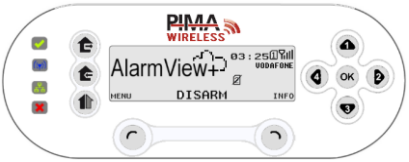


10. With the LCD screen facing you, insert the cradle into the mounted back plate - push it firmly, until the clasps are locked. Ensure the back tamper is pressed against the knockout.



11. Tilt the front cover towards the top side of the mounted back plate.
12. Insert the two jags on the front cover to the corresponding holes on the back plate, and push it down, until you hear an audible press.
13. Press the front cover against the back plate, until locked.
14. Secure the front cover with the two supplied Philips screws, at the bottom.
15. Connect the AC adapter to power. Wait for the Power LED to light up and the screen to show the normal display.






## 3.4 Other installation options

### 3.4.1 Standalone wired siren

Besides the control panel's built-in siren, you can also connect any self-powered external siren. To do so, you will need to connect it to an external power source.

***The wired siren's current consumption should not exceed 500 mA***

To connect the siren:

1. Run the siren's wires through the opening on the control panel's back plate.
2. Connect between the siren and the control panel's PGM terminals. See the scheme on the right.
3. Connect between the siren, the control panel and the external power source (-).
4. Connect between the siren and the external power source (+).

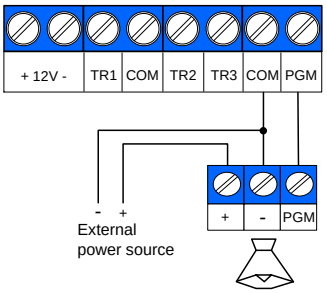



Figure 15. External siren wiring scheme

### 3.4.2 How to connect and use the trigger inputs[7]

The alarm system has three inputs on its terminal block, which can be used to arm and disarm it, by various triggers. See the next separated sub-section on the AVR.

When using the triggers to arm and disarm the control panel, the quick arm buttons are disabled. Also keyfobs, remote control by SMS and the smartphone app cannot be used.

[7] See section 10.5.4, on page 43 for the triggers' settings.

Connect the triggers according to the next diagram and table:

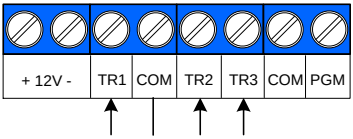



Figure 16. Trigger inputs

| Input | Default setting |
|---|---|
| TR1 | Arm AWAY |
| TR2 | Arm HOME |
| TR3 | Arm PART |

### 3.4.3 How to connect the AVR+ to external alarm system

The AVR+ adds Visual Verification capacities to any intruder alarm system. Based on the AlarmView+ control panel, it is designed for sending Visual Verification and look-in images by up to six SmartView PIR/Cameras and OutView cameras.

For the AVR+ to send indications to the master system, its PGM output must be connected to a 24H zone input on the master system - when the AVR+ will be in "Not Ready/Alarm" state, the external zone will be opened.

By combining trigger inputs and a PGM output, the AVR+ can do the following:

- Be Armed and Disarmed
- Indicate the external alarm system on "Not Ready" (open zone) and alarm situations
- Serve as a backup communication channel - when triggered by the external alarm system (on alarm, for example), the AVR will report the CMS/End-user over GSM/GPRS.

By default, the AVR+ will use the trigger inputs and PGM output as described in the following table and text:

| No. | AVR+ Default setting | Direction | External Alarm System |
|---|---|---|---|
| 1 | **TR1** - "Wired/External zone" (zone #24)[8] | ← | PGM output |
| 2 | **TR2** - "Arm AWAY" | ← | ON/OFF output |
| 3 | **PGM**[9] - "Not Ready/Alarm" | → | Zone input |

Mode of operation

1. Backup communication channel: the alarm is set off (or a fault occurs) on the external alarm system and triggers its PGM output → TR1 on the AVR+ is triggered and zone #24[10] is opened → the AVR reports the CMS/end-user
2. Arm AWAY: the external alarm system is armed and its ON/OFF output is triggered → TR2 on the AVR is triggered and the AVR is armed to AWAY mode
3. Not Ready/Alarm state: when trying to arm the external alarm system and the AVR+ is in "Not Ready/Alarm" state, the AVR+'s PGM output will trigger a zone input on the external alarm system. The system must be set so it cannot be armed with open zones.

[8] "Swinger Shutdown" is disabled by default
[9] See section 10.5.3, on page 43 for details on the PGM output options
[10] In the AVR: Zone #24 (the wired zone) is set as 24H zone by default

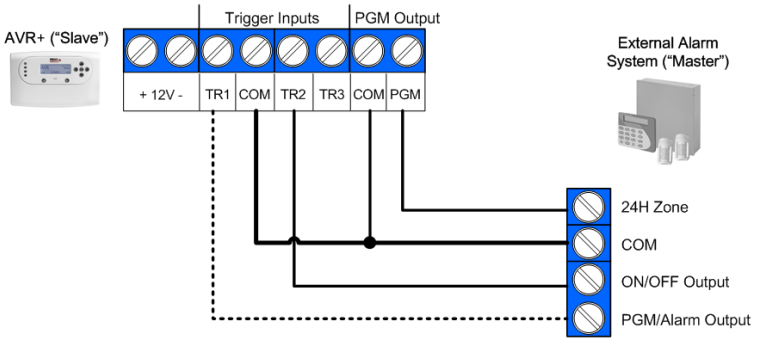
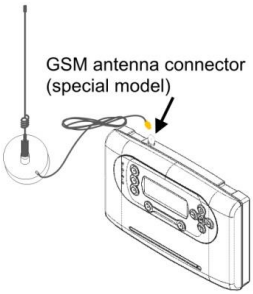



Figure 17. The AVR+ trigger inputs

### 3.4.4 External antenna (optional)

The control panel has a model with a connector for external GSM antenna (P/N 6110019), to improve GSM reception where necessary.

**This control panel model must be ordered separately!**




## 3.5 How to confirm system installation

To make sure all detectors are well identified by the control panel after installation, do the following:

1. Access the Installer menu and select **Service -> Tests -> Zone Tests**.
2. Press the **Test button** on each detector and check the reception level. See page 30 for details.

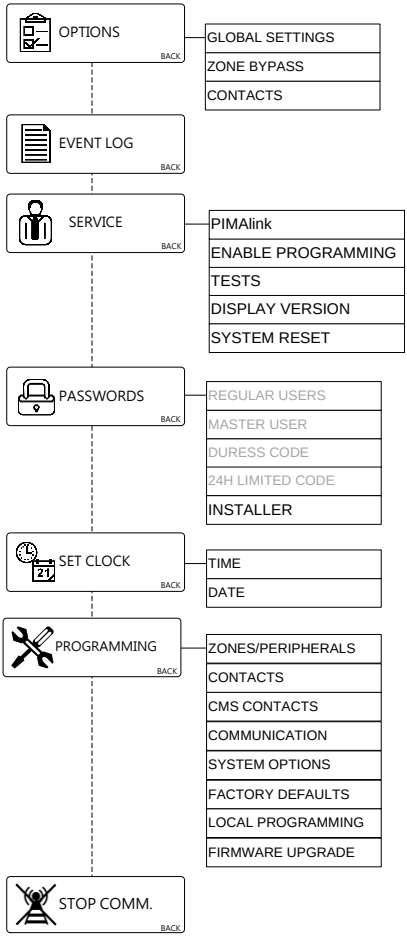
# 4 Setup and Programming

The alarm system has two menus and two related passwords: Installer and Master User. The two menus have the same sub-menus, except the Programming menu which is exclusive to the Installer.

Programming can also be done remotely, using PIMA's Programming Tool software[11].

*Some menus are feature depended and vary between models.*

## 4.1 The Installer's menu map

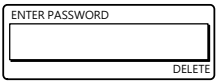



[11] Version 02.00.11.00 and higher

## 4.2 Accessing the menus

To access either of the menus:

1. Press the left key (under "MENU") - a password entry field will appear.




2. Use the numeric/navigation keys to enter a password. See section 2.2.1, on page 12, on how to enter characters.

## 4.3 The Master and Installer passwords

The next table lists the Master user and Installer passwords and their use.

| Password | Default | The password allows... |
|---|---|---|
| Master user | 1111 | Changing all passwords except the Installer's, viewing the event log, setting the time, and changing some system settings. |
| Installer | 1234 | Changing the Installer password, changing all settings the control panel and all detectors and peripherals. |

***You must change the default passwords during the installation of the system***

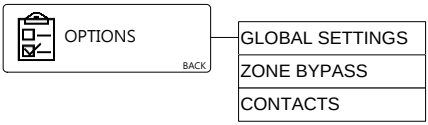
### 4.3.1 How to reset the passwords to factory defaults

To reset the passwords to their factory default:

1. Disconnect the control panel from both AC power and backup battery for 10 sec.
2. When you power up the control panel again, the Master User and Installer's default passwords (1111, 1234 respectively) can be used for 30 sec., to access the menus.

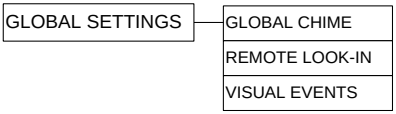
# 5 Options

This menu allows changing and controlling the general behavior of the Control Panel, as well as setting notifications for the contacts.

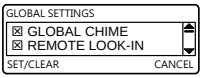



## 5.1 Global Settings

The Global Settings menu allows setting of three features, as explained below. The remote look-in and visual events features allows the end user to maximize the control of all privacy issues.




To change the **Global Settings**:



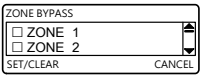

1. Access the Installer menu and select **Options → Global Settings**
2. **Set/Clear** (enable/disable) the options, which are:
   a. **Global Chime**: all chime zones
   b. **Remote Look-in**: sending requested look-in images to predefined mobile phones
   c. **Visual Events**: sending visual verification images to predefined mobile phones

## 5.2 Zone bypass

This menu allows bypassing zones until the next disarming of the alarm system

***Do not bypass zones unless necessary and only temporarily: bypassed zones do not sound the alarm when opened, nor are reported to the CMS.***

To bypass zones temporarily, do the following:



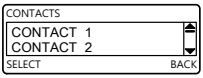

1. Access the Installer menu and select **Options → Zone Bypass**.
2. **Set** (enable) the zones to be bypassed. Press the Up/Down  keys to scroll between the zones.
3. **Clear** (disable) zones to un-bypass them.

## 5.3 Contacts

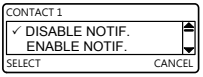
This menu allows setting which of the six available contacts will get notifications on alarms and other system events[12]. The events are set in the "Contact 1-6" menu. See section 10.2.2, on page 41.

To set a contact to receive notifications, do the following:

1. Access the Installer menu and select **Options → Contacts**.




2. Press **Contact X**. The options are:




   a. **Disable Notifications**: this contact will not receive any notification, including not via PIMAlink (if relevant).

   b. **Enable Notifications**: (default): this contact will receive all notifications, including SMS, MMS and Emails. If this contact is using the PIMAlink app, it will receive the notifications from both paths.

   c. **PIMAlink Backup**: this is a PIMAlink only menu - if the connection with PIMAlink is lost, this contact will receive all notifications via SMS/MMS/Email until the connection is restored.

[12] PIMAlink allows up to 32 contacts to receive notifications.

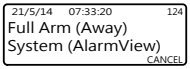
# 6 Event Log


This menu allows you to view the system log. The log keeps the last 256 events. While the alarm system is armed, it can log up to 10 events from the same zone.

Using the "Programming Tool" application, 500 events can be logged and viewed.

To view the Event Log:

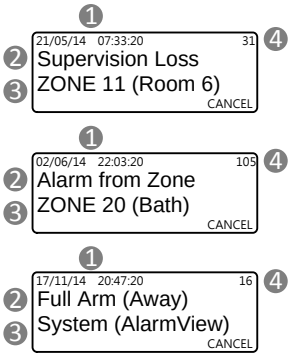
1. Access the Installer menu and select **Event Log**. The first event is the most recent one.




2. Use the Up/Down  keys to scroll between the events. See the next section for details.

3. Press  to exit the log

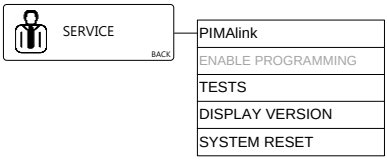
## 6.1 Log entry examples




The information of a log entry is displayed as follows:

1. Date and time the event was logged
2. Event description
3. Event source
4. Log entry serial number

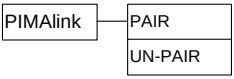
# 7 Service




The Service menu allows the Master user to connect to the control panel to PIMAlink, perform various tests to verify the installation and the proper operation of the system, and reset the alarm system.

The "Enable Programming" menu can be accessed only by the Master user - it enables it to allow the technician a 2 hour window to remotely access the alarm system[13].

## 7.1 PIMAlink




In this menu the Master User link the control panel to PIMAlink, by getting a pairing code. This unique code can be used to link up to 32 mobile phones with the PIMAlink app installed on it, to the PIMAlink server, and the control panel.

### 7.1.1 Pair

To get the pairing code, press **Pair** and wait for the PIMAlink server to create the code. After the code appears on the screen, there is a 10 minutes window to enter it in every mobile phone that needs to connect to PIMAlink. After 10 minutes the code expires; if another phone needs to connect to PIMAlink, the Master User must repeat the process and get a new code. The link between the already paired phones and PIMAlink is reserved in anyway.

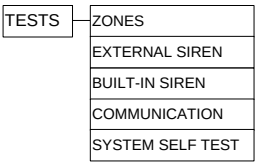
### 7.1.2 Un-pair

When pressing **Un-pair** two things happen:

1. The connection between the control panel and PIMAlink expires
2. The connection between every registered mobile phone and PIMAlink expires

Note that his action cannot be undone; should one need to re-connect to PIMAlink, the pairing process will have to be repeated.

## 7.2 Tests




The tests menu allows testing the zones and peripherals of the alarm system, the communication paths, and some more options.

[13] Provided that the default Access Code has been changed.

### 7.2.1 Zone

To test the zones:

1. Access the Installer menu and select **Service → Tests → Zone**.
2. The zone test screen is made of a grid that shows all active zones: zones 1-24 are displayed with their number, zones 25-30 are displayed with their RSSI[14] level. See the next two sub-sections for full details.
3. Trigger zones 1-24 - when a signal is received in the control panel, the zone number is replaced by the RSSI reception level.
4. Once the test is complete, press OK to exit.

#### Zone status options

There are three status options in the zone test display (see the next figure):

a. Number: this is the zone number. It appears in regular zones before testing, and in visual zones that are at fault

b. Signal strength indicators:

   1) Zones 1-24: the indicators appear as the zone is triggered

   2) Zones 25-30 (visual zones): the indicators interchange with the zone no.

c. Empty: the zone is disabled

#### RSSI reception level

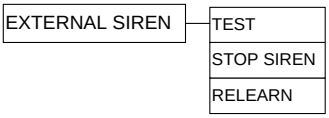
The signal strength indicators allow you to determine how good the communication, between the wireless devices and the control panel is. The number of the indicators is the quality of the reception, as explained in the table below. See also the previous figure

| Onscreen | Indicators | Reception/Indication |
|---|---|---|
| | 5 | **Excellent** |
| | 4 | **Strong** |
| | 3 | **Good** |
| | 2 | **Low**: see the warning below! |
| | 1 | **Poor**: see the warning below! |
| Numeral | - | 1. Zones 1-24: the zone was not triggered<br>2. Zones 25-30: the (visual) zone is at fault |

***"Poor" and "Low" reception levels are not acceptable. If you get a "poor" signal from any detector, re-locate it and re-test it, until the test result is between "Excellent" and "Good".***

[14] Received Signal strength Indication

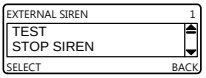
## 7.2.2 External Siren




See also "External Siren Indications", on page 57.

### Test

To test the external siren, do the following:




1. Access the Installer menu and select **Service → Tests → External Siren**.
2. Press **Test**.
3. Wait 5 sec. The siren will sound the alarm for 3 sec. and its LEDs will flash for few sec.
4. Press OK to exit.

### Stop siren

If the siren's tamper switch is tripped continuously, you can use this feature to stop (silent) the siren.

### Relearn

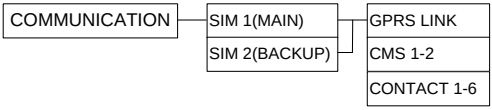
If the siren needs to be re-learned with the control panel, call PIMA support for instructions

## 7.2.3 Built-in siren

To test the built-in siren, do the following:

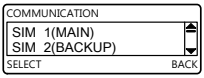
1. Access the Installer menu and select **Service → Tests → Built-In Siren**.
2. Press OK - the built-in siren will sound briefly.

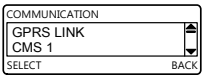
## 7.2.4 Communication




This menu allows testing the SIM card's communication setup, by trying to send and receive data. See the next table for complete details.

To test the SIM cards:




1. Access the Installer menu and select **Service → Tests → Communication**.
2. Select **SIM1** or **SIM2** (in dual SIM versions). If the selected SIM is currently idle, the alarm system will switch to it.
3. Select the test type and press OK.
4. Press OK at the end of the tests.

### Test types

The test types are described in the table below. All tests are replied by either "Passed" or "Failed" message.

| Test | Process |
|---|---|
| GPRS Link | Ping a website (www.google.com) |
| CMS 1-2 | Send a test event to the CMS:<br>a. In SIA/CID over SMS: to mobile phone<br>b. In Visual/CID over Email: to E-mail<br>c. In Visual/CID over GPRS: to PC, mobile phone |
| Contact 1-6 | Send "Periodic Test" by text message:<br>a. SMS Test: to mobile phone ("SMS Event Report" must be enabled. See page 41)<br>b. Email Test: to E-mail ("Email Event" must be enabled. See page 41) |

### 7.2.5 System self-test

The self-test checks the LCD display, the LEDs, the chime and the internal sounder.

To do the test:

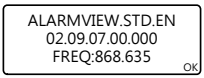
1. Access the Installer menu and select **Service → Tests → System Self Test**.
2. The LCD display will flicker for 8 sec. and the internal sounder will sound a series of beeps.

## 7.3 Display version

Use this feature to view the system's version and RF frequency

To view the system version and frequency:

1. Access the Installer menu and select **Service → Display Version**
   The system's software version and RF frequency will be displayed.




2. Press OK to exit.

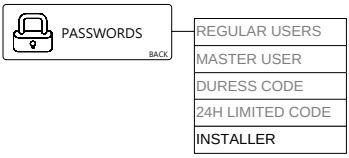
## 7.4 System reset

The system reset feature enables to reset the communication channels.

To do a system reset:

1. Access the Installer menu and select **Service → System Reset**.
2. Wait for the short process to end.

# 8 Passwords




The password menu allows you setting the Installer password. The other passwords on the menu can be set only by the Master User, in the User menu.

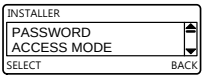
## 8.1 Installer

The Installer password can be 4-8 digits long and contain the numeric values of 1-4, for example 14412311. It cannot be deleted.

***You must change the default Installer password during installation***

To set the Installer password:

1. Access the Installer menu and select **Passwords → Installer**.
2. Select **Password** and type the desired password.




3. Press OK.

- *You cannot use the Installer password over the wireless keypad, only the control panel*
- *A minimum of 7 digit password is required to comply with EN requirements*

### 8.1.1 Access mode

There are two options for allowing the installer to access the alarm system remotely, via the Programming Tool application: User Initiated and Always, as explained below.

The alarm system keeps a record of any remote connection and reports it to the CMS.

a. **User Initiated**: in this mode the Installer cannot access the menu, unless the Master user permits it by opening a two hour access window (on the User menu: **Service → Enable Programming**).

b. **Always**: in this mode the Installer can access the system, without the need for the Master user approval.

***You must change the default Access Code, to be able to connect to the alarm system remotely in the "Always" mode: as a precaution, if the default code has not been changed, remote access without the Master user approval is disabled.***

To define the Installer's access mode, do the following:

1. Access the Installer menu and select **Passwords → Installer → Access Mode**.
2. Select **User Initiated** or **Always**.

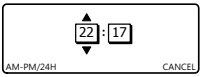
# 9 Set Clock


After a long power failure, or whenever the time is not accurate, the time and date need to be set

## 9.1 Time

To set the Time, do the following:

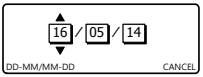
1. Access the Installer menu and select **Set Clock** → **Time**.
2. Press ↶ to change between 12H (AM/PM) and 24H time formats.
3. Press the up and down arrow keys 1 3 to set the hour and minute.
4. Press the right and left arrow keys 4 2 to move the cursor between the hours and the minutes.
5. Press OK to save.




## 9.2 Date

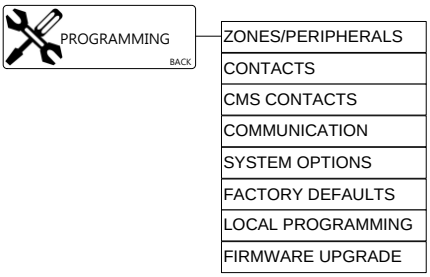
To set the Date, do the following:

1. Access the Installer menu and select **Set Clock** → **Date**.
2. Press ↶ to set the date format to either American (MM/DD) or European (DD/MM).
3. Press the up and down arrow keys 1 3 to set the date.
4. Press the right and left arrow keys 4 2 to move the cursor between the day, month and year.
5. Press OK to save.



# 10 Programming

The programming menu allows you to program the various functions of the alarm system.

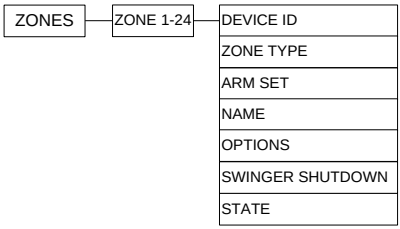



## 10.1 Zones/Peripherals

Enroll and define the wireless detectors and peripherals of the alarm system. Before enrolling, make sure all peripherals have the appropriate batteries.

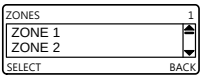
All three systems, the AlarmView, Guardian and AVR support up to 23 wireless zones and one hardwired. The AlarmView and AVR also support up to six Visual zones.

### 10.1.1 Zones

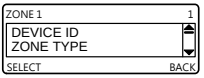



To enroll and define a wireless zone:

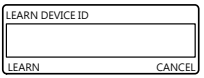
1. Access the Installer menu and select **Programming** → **Zones/ Peripherals** → **Zones**.



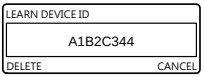

2. Select **Zone 1-24**[15].



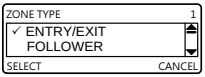

3. Select **Device ID** and press **Learn** to enroll a detector or a peripheral. If a number is displayed, the zone already has a device associated with. You can press "Delete", and enroll a new device.




4. Trigger a device or press its Test button. When the device is detected, press OK.

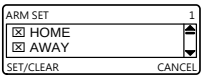



5. Select **Zone Type** and select the type. The available types are: **Normal**, **Entry/Exit**, **Follower**, **24H**, **Panic**, **Medical**, and **Fire**. See the "Glossary of terms", on page 59 for more on each type.

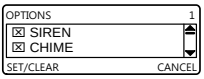



[15] Zone #1 is set as Entry/Exit zone by default; zone #24 is set as Normally Open

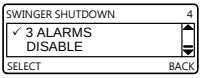
6. Select **Arm set** and set to which arming mode the zone will be armed. The available modes are: **Home**, **Away**, and **Part**. Multiple selection is allowed.




7. Select **Name** and give the zone a name. See section 2.2.1, on page 12 for details.
8. Select **Options** and set the zone options. Multiple selection is allowed. The available options are as follows:



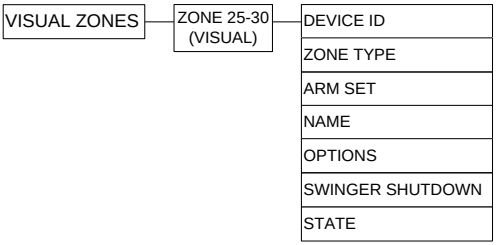

   - **Siren**: when the zone is violated, it will trigger the siren.
   - **Chime**: when the zone is opened while the control panel is disarmed, it will trigger the control panel's chime. This is normally used on doors and windows.
   - **Force Arm**: this zone can be armed when the "Force Arm" option is enabled. See section 10.5.2, on page 45 and the "Glossary of terms", on page 58 for more details.
9. Select **Swinger Shutdown** (see the "Glossary of terms", on page 58) and select between the available options: 1, 2 or 3 alarms, or Disable.




10. Select **State** and set if the zone is **Enabled** or **Disabled**.

*Zone #24 is a dedicated hardwired zone. As such, it does not have the "Device ID" option. To use this zone Trigger #1 must be set as "Wired/EXT zone". See section 10.5.4, on page 47*

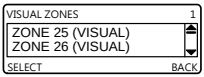
## 10.1.2 Visual zones (AlarmView and AVR only)



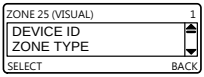

The alarm system supports up to six visual zones, namely SmartView PIR/cameras.

To enroll and define a visual zone:

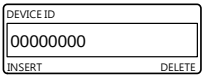
1. Access the Installer menu and select **Programming → Zones/ Peripherals → Visual Zones**.

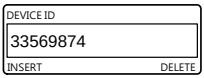



2. Select **Zone 25-30 (Visual)**.




3. Select **Device ID** and type the detector's serial number (8 digits)[16]. If a number is displayed, the zone already has a device associated with. You can press "Delete", and enroll a new device.

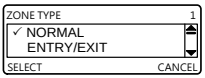


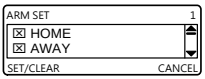

*Visual detectors cannot be enrolled automatically, to protect privacy and security*

[16] Or type it: the ID is printed on a label on the keyfobs and keypad

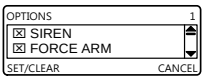
4. Select **Zone Type** and mark the type. See the previous "Zone" section for the available options.



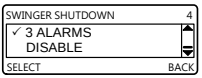

5. Select **Arm set** and set the arming mode in which the zone be armed. See the previous "Zone" section for the available options.




6. Select **Name** and give the zone a name. See section 2.2.1, on page 12 for details.
7. Select **Options** and set the zone options. Multiple selection is allowed. The available options are as follows:

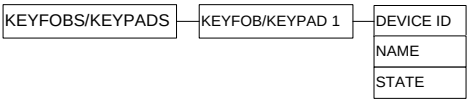



   - **Siren**: See the previous "Zone" section for the available options
   - **Force Arm**: See the previous "Zone" section for the available options
   - **Visual Verification**: send visual verification images to predefined contacts
   - **Remote Look-in**: allow predefined contacts to request look-in images by SMS
   - **Led Indication:** the SmartView's LED turns on at detection
8. Select **Swinger Shutdown** See the previous "Zone" section for the available options.




9. Select **State** and select if the zone is **Enabled** or **Disabled**.

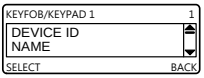
### 10.1.3 Keyfobs/keypads



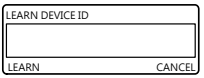

The alarm system supports the connection of up to six KF key fobs and RWK wireless keypads. See a separate Peripherals guide (P/N 4410399) for details on these devices.

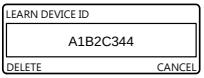
To enroll and define a key fob or a wireless keypad, do the following:

1. Access the Installer menu and select **Programming → Zones/ Peripherals → Key fobs/ Keypads → Key fob/Keypad 1-6**.




2. Select **Device ID** and press **Learn** to enroll the peripheral[16]. If a number is displayed[17], the zone already has a device associated with - you can press "Delete", and enroll a new device.

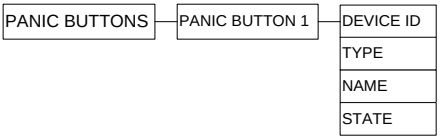



3. Press OK to save the ID.
4. Select **Name** and type a description for the keyfob/keypad. See section 2.2.1, on page 12 for details.
5. Select **State** and select **Enabled** or **Disabled**.

[17] Only the first seven digits are displayed (the eighth is always zero). The serial no. is printed on a label on the detector.

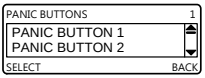
### 10.1.4 Panic button



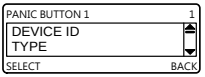

The alarm system supports the connection of up to six PCP buttons for Panic and Medical issues. See a separate Peripherals guide (P/N 4410399) for details on these devices.

To enroll and define a Panic/Medical button:

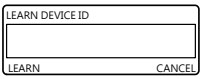
1. Access the Installer menu and select **Programming → Zones/ Peripherals → Panic Buttons**.

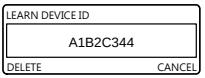



2. Select **Panic Button 1-6**.

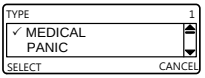



3. Select **Device ID** and press **Learn** . Press the panic button to enroll it[18]. If a number is displayed[17], the zone already has a button associated with. You can press "Delete", and enroll a new one. See a separate peripherals guide (P/N 4410399) for more details on the panic button.



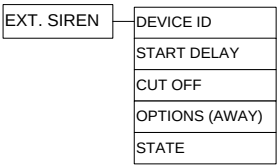




4. Select **Type** and select the button type: **Medical** or **Panic**. The type selected only determines the event reported.




5. Select **Name** and type a name/description for the panic button (see section 2.2.1, on page 12 for instructions).
6. Select **State** and select if the button is **Enabled** or **Disabled**.

### 10.1.5 External siren

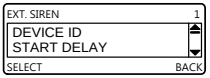



Set the parameters of the SIR External Wireless Siren. See also "External Siren Indications", on page 57.

See a separate Peripherals guide (P/N 4410399) for complete details on the siren.

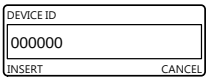
To enroll and define the siren:

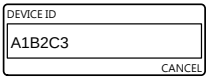
1. Access the Installer menu and select **Programming → Zones/ Peripherals → Ext. Siren**.



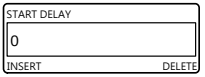

[18] Or just type it: the ID no. is printed on a label on the button.

2. Select **Device ID**, enter the siren's serial number and press **Insert** (see section 2.2.1, on page 12 for instructions). The number is printed on a label at the back of the siren (and also on the siren's package).

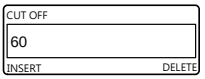


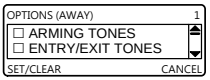

3. If required, select **Start Delay** and enter a delay in sec. before the siren will sound the alarm, between 0 (default) and 255.




4. Select **Cut Off** and enter the time, between 5 and 255 sec. (default - 60).




5. Select **Option (Away)** and set options, that are available only while the alarm system is armed to AWAY mode:




   a. **Arming tones**: the siren will beep once when arming the system, and twice when disarming.

   b. **Entry/Exit tones**: in addition to the control panel internal sounder, the siren will sound clock ticks during the exit and entry delays. See "External Siren Indications", on page 54 for details.

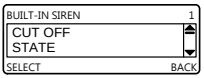
6. Select **State** and select if the siren is **Enabled** or **Disabled**.

### 10.1.6 Built-in siren

The system has an 85 dB internal siren, sufficient for indoor alarm.

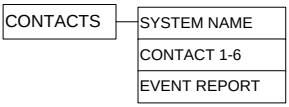
To define the built-in siren:

1. Access the Installer menu and select **Programming → Zones/ Peripherals → Built-In Siren**.




2. Select **Cut Off** and enter the time, between 5 and 255 sec. (default - 60).
3. Select **State** and select if the siren is **Enabled** or **Disabled**.

## 10.2 Contacts



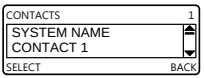

The system allows defining up to six contacts, for receiving event and fault notifications.

### 10.2.1 System name

The system name is used to personalize the alarm system in the messages the contacts receive.

To define the name:

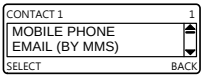
1. Access the Installer menu and select **Programming → Contacts**
2. Select **System Name**. Leave the default name or type a new one (see section 2.2.1, on page 12 for instructions).
3. Press OK.



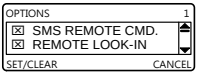
## 10.2.2 Contact 1-6

Define the various details of up to six contacts of the alarm system, as follows:

1. Access the Installer menu and select **programming → Contacts → Contact 1-6**.




2. Select **Mobile Phone** and enter a mobile phone number.
3. Select **Email (By MMS)** and enter an E-mail address. E-mails are sent via MMS (Multimedia Message Service) messages and cost money to the end user (by the service provider).
4. Select **Contact Name** and type a name (see section 2.2.1, on page 12 for instructions).
5. Select **Options** and set the contact's options, as described in the next table.




| Option | The contact will be... |
|---|---|
| **SMS Remote CMD.*** | allowed to arm, disarm and other operations by sending text messages. See section 12.2.1, on page 52 |
| **Remote Look-in*** | allowed to receive look-in images |
| **SMS Event Report*** | receiving notifications on alarms and other events by SMS |
| **MMS Visual** | receiving visual verification images by MMS |
| **Email Event** | receiving notifications on alarms and other events by E-mail |
| **Email Visual** | receiving visual verification images by E-mail (sent via MMS) |

** Must be enabled when using the Android app*

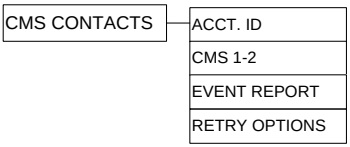
## 10.2.3 Event Report

1. Select **Event Report**.
2. Set the event types that will be reported to any of the contacts. The options are as follows:


| Option | The contact will be reported on... |
|---|---|
| **Alarm events** | any alarm occurrence |
| **Dis/Arm report** | arming to any mode, disarming |
| **Power report** | power loss, low battery |
| **Service report** | actions such as entering the menu |

See Appendix G, on page 61 for complete details on the reported events.

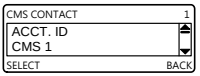
## 10.3 CMS contacts



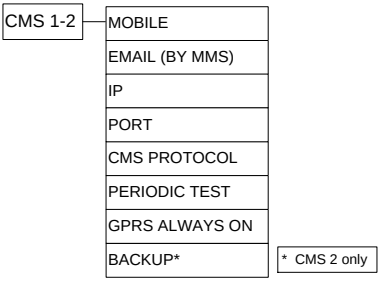

Here you can set two CMS contacts and their options.

To set the CMS contacts, do the following:

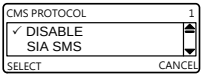
1. Access the Installer menu and select **Programming → CMS Contacts**.

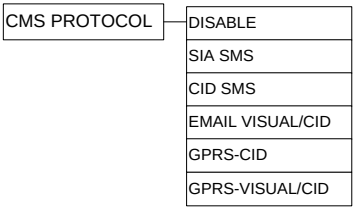



2. Select **Acct. ID** and type the account ID of this alarm system.
3. Select **CMS X** and set the following:




   a. Select **Mobile** and enter the CMS's phone number for receiving notifications by SMS.
   b. Select **Email (by MMS)** and enter the CMS's E-mail address. Note that E-mails are sent via MMS (Multimedia Message Service) messages and cost money to the end user (charged by the cellular provider). See section 2.2.1, on page 12 for instructions.
   c. Select **IP** and enter the IP address of the IP Receiver in the CMS. You can also enter a URL address for DDNS services.
   d. Select **Port** and enter the port number of the IP receiver.
   e. Select **CMS Protocol** and select the relevant option. The options are listed in the table below.

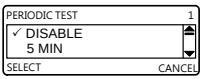


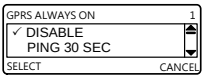

| | |
|---|---|
| **Disable**: | reporting to the CMS is disabled |
| **SIA SMS**: | events will be sent by SMS, in SIA |
| **CID SMS**: | events will be sent by SMS, in ContactID© |
| **E-mail Visual/ CID**: | visual and normal events will be sent by E-mail, in ContactID© |

| | |
|---|---|
| **GPRS-CID**: | events to the CMS will be sent as IP over GPRS, in ContactID© |
| **GPRS-Visual/ CID**: | visual and normal events will be sent to the CMS, as IP over GPRS, in ContactID© |

f. Select **Periodic Test** and select every how long a test event will be sent to the CMS for supervision. The options are: Disable (tests), 5/10/60 min, 24 hrs., one week, one month.

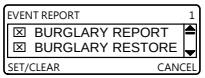



g. Select **GPRS Always ON** and select a ping interval in sec. The options are: 30, 45, 60 or 90. The alarm system will ping a web server to maintain an open session with the IP Receiver. See the "Glossary of terms", on page 58 for more details.

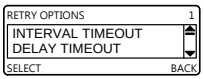



4. Press **BACK** .

5. Select **Event Report** and set which events will the alarm system report the CMS. The options are: Burglary Alarms, Burglary Restore, Fire alarms, Fire Restore, Arming and Disarming, Service events,
Service Restore, Power loss, Power Restore, Medical alarms, Medical Restore, and Visual alarms (verification images).



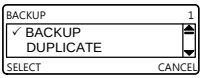

6. Select **Retry Options** and set the 2 available options, listed below:




- **Interval Timeout**: set the overall interval of the re-tries in min., between 6-30.
- **Delay Timeout**: set the delay between re-tries in sec., between 15-60.

  Example: if you set an interval of 10 min. and a delay of 15 sec., then for 10 min. the control panel will try to report the CMS, every 15 sec., which is 40 times (10x4)

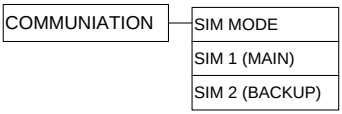
7. In **CMS 2** only, select **Backup** and set the two backup options, as follows:




- **Backup**: CMS 2 will serve as backup channel to CMS 1 in case of a communication loss with CMS 1
- **Duplicate**: all events will be reported both to CMS 1 and CMS 2 ("Double Report")

- *When CMS 2 is set as "Duplicate", "GPRS Always On" is automatically disabled*
- *Sending images may cause the IP Receiver to close the session*

## 10.4 Communication

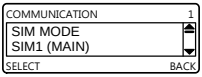



Set the mode of the SIM card(s) - single or dual[19] - and the cellular provider's details of each card. The alarm system comes with a list of your country's providers by default.

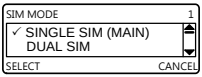
[19] See the "Glossary of terms", on page 49.

To set the SIM card(s) mode:

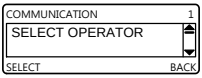
1. Access the Installer menu and select **Programming → Communication**.



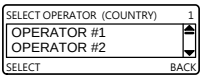

2. Select **SIM Mode** and select between the two following options:
   - **Single SIM (Main)**: one card in use
   - **Dual SIM**: two cards in use



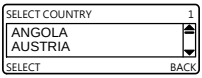

3. Back in the **Communication** screen, select **SIM1 (Main)** and press **Select** on **Select Operator**.



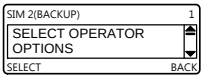

4. Use the up/down keys (1) (3) and scroll to the provider that matches the SIM card in use, and press **Select**.



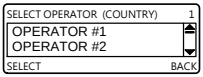

5. If you need to select a different country:
   a. Press **SIM 1** or **SIM 2** again.
   b. Press **BACK**.
   c. Scroll to the desired country, press **Select**, then repeat on steps 3-4.



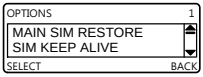

6. In dual SIM versions, in the **Communication** screen, select **SIM2 (Backup)**.




7. Press **Select Operator** and repeat on steps 4-5




8. Select **Options** and select between the options, as follows:
   a. **Main SIM Restore**: set how many hours after switching from SIM1 to SIM2 the control panel will try to switch back. The options are 1, 2 and 4 hours.
   b. **SIM Keep Alive**: cellular providers suspend the communication with SIM cards being idle for a long time. "Long time" varies between the different providers. To avoid this, the control panel will send a "Keep-alive" event in the interval set here. The options are once every 1-28 days.



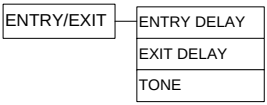

*Some SIM cards may have two options:*
- *PP – indicates a Prepaid/Pay As You Go card*
- *CN – indicates a Contract card*

## 10.5 System options

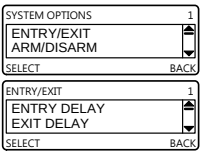
| SYSTEM OPTIONS | ENTRY/EXIT |
|---|---|
| | ARM/DISARM |
| | PGM OUTPUT |
| | TRIGGER INPUTS |
| | REMOTE ACCESS |

Set the system options.

## 10.5.1 Entry/Exit delay

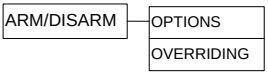



To set the entry and exit delays, do the following:




1. Access the Installer menu and select **Programming → System Options.**
2. Select **Entry/Exit**.
3. Select **Entry Delay** and type a value between 5 and 45 sec. (default - 30).
4. Press OK.
5. Select **Exit Delay** and type a value between 5 and 255 sec. (default - 5).
6. Press OK.
7. Select **Tone** and select between **High** or **Low**, for the delay countdown ticking sound.

## 10.5.2 Arm/Disarm

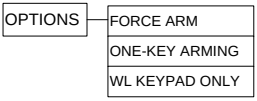



Define the arming and disarming options. For a detailed explanation of each, see the "Glossary of terms", on page 58.

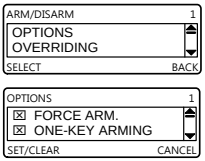
The alarm system cannot be armed in the following situations:

- The Fault LED is on
- A zone tamper is open
- An immediate zone is open
- "Force Arm" (see the "Glossary of terms", on page 58) is not enabled

### Options




To set the arming and disarming options, do the following:




1. Access the Installer menu and select **Programming → System Options → Arm/Disarm**.
2. Select **Option** and set the relevant options, listed in the next table.

| Option | Description |
|---|---|
| **Force Arm** | Allows arming with open zones. See "Arming modes", on the "Glossary of terms", on page 59. |
| **One-Key Arming** | Allows arming by only pressing the control panel's arming buttons (without the need to enter a user code). |

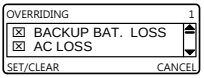
| Option | Description |
|---|---|
| **WL keypad only** | • If only the wireless keypad will be used for arming and disarming, user passwords can be up to four digits, and have the numerals of 0-9.<br>• To use both the wireless keypad and the control panel, passwords can be up to four digits, but have the numerals of 1-4 only. |

### Overriding

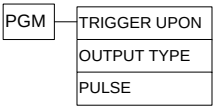
The alarm system can be armed by overriding 3 faults: Backup Battery Loss, AC Loss and Zone Supervision Loss. These faults are being reported and logged anyway, and must be resolved as soon as possible.

To set the overriding options, do the following:

1. Access the Installer menu and select **Programming → System Options → Arm/Disarm → Overriding**.
2. Set the faults to be overridden when arming.

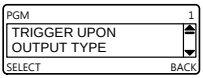



## 10.5.3 PGM output

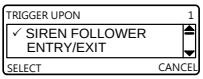



The alarm system allows one PGM connection. To set it, do the following:

1. Access the Installer menu and select **Programming → System Options → PGM Output**.

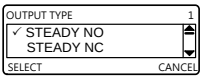



2. Select **Trigger Upon** and select what will trigger the output, as listed in the following table.




| Trigger | The PGM output is triggered when... |
|---|---|
| Siren Follower | The siren is activated |
| Entry/Exit | The Entry/Exit delay starts running |
| Not Ready/Alarm | A zone is open or alarming, a fault occurs |
| Arm Away, Home, or Part | The alarm system is armed |
| Power Fault | This fault occurs |
| Medical, Burglary, Fire | These alarms are set off |
| Remote SMS | SMS command is received |

3. Select **Output Type** and select the desired output type, as listed in the following table.




| Type | Mode |
|---|---|
| Steady N.O. | Normally Open |
| Steady N.C. | Normally Close |
| Pulse Low to High | - |
| Pulse High to Low | - |

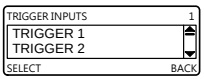
4. Select **Pulse** and type the pulse duration, between 1 and 255 sec.

## 10.5.4 Trigger inputs

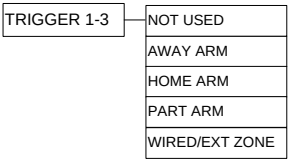
The alarm system allows three input connections, which can be utilized for arming the system by an external alarm system, and more. See section 3.4.1, on page 21 for more details.

To set the trigger inputs options, do the following:

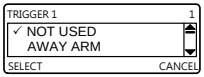
1. Access the Installer menu and select **Programming → System Options → Trigger Inputs**.




2. Select **Trigger 1-3**.

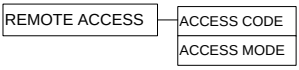



3. Select the triggering option. The available options are described in the next table.




| Trigger | The input is triggered upon/by… |
|---|---|
| Arm AWAY, Arm HOME, Arm PART | arming to one of these modes |
| Wired/Ext. Zone | signal via the hardwired zone (#24)[20] |

## 10.5.5 Remote access



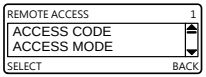

Set the parameters for remotely accessing the alarm system, using the "Programming Tool" PC application (via GPRS). When accessing remotely there are several limitations:

a. While the control panel is armed you cannot bypass zones, change the global options, change contacts, and change the system configuration.

b. After disarming the control panel the remote session is disconnected, to allow reporting the event.

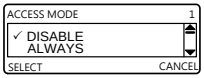
To set the remote access parameters, do the following:

1. Access the Installer menu and select **Programming → System Options → Remote Access**.




2. Select **Access Code** and type a new code to replace the default one (531902).

3. Select **Access Mode** and select when remote access is allowed. The available modes are listed in the next table. See section 8.1.1, on page 33 for more details.

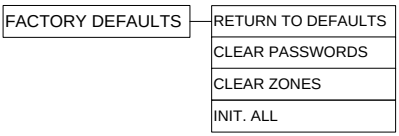



| Access Mode | Description |
|---|---|
| Disable | Remote access is disabled |
| Always | Remote access is enabled, without the need for the Master user's approval (only if the default Access Code was changed. If the code is the default one, the Master user will have to approve any remote access). |

[20] Only Trigger #1 can be set as and connected to a Wired/External zone

| Access Mode | Description |
|---|---|
| During Disarm | Remote access is enabled, only when the system is disarmed. |
| User Initiated (default) | Remote access is enabled, only after the Master allows a two hour window via the **Service → Enable Programming** menu. |

## 10.6 Factory defaults




Use this menu to reset the alarm system. The options on this menu are listed in the next table and the following sections.

| Option | What is defaulted? | What is not defaulted? |
|---|---|---|
| Return to Defaults | All the parameters, except those on the right | Passwords, Remote Access Code, zones and peripherals' IDs |
| Clear Passwords | All passwords, Remote Access Code | All other parameters |
| Clear Zones | All zones and peripherals' IDs | Zones and peripherals' parameters |
| Init All | Combines the three above options | - |

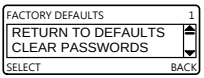
- *The log is not cleared in any of the above options*
- *Bypassed zones are not un-bypassed in any of the above options*

### 10.6.1 Return to defaults

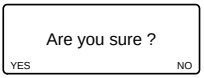
*The default settings may vary between various countries and regions*

To return to the factory defaults:

1. Access the Installer menu and select **Programming → Factory Defaults**.




2. Select **Return to Defaults** - a confirmation message will appear asking you to confirm the action.

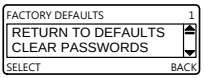



3. Press **YES** to confirm.

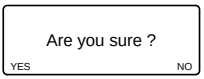
### 10.6.2 Clear Passwords

To clear (reset) all passwords:

1. Access the Installer menu and select **Programming → Factory Defaults**.




2. Select **Clear Passwords** - a confirmation message will appear asking you to confirm the action.



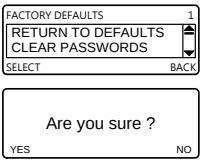

3. Press **YES** to confirm.

### 10.6.3 Clear zones

***After performing this action, you will be required to re-enroll all zones and peripherals.***

To clear all the zones:

1. Access the Installer menu and select **Programming → Factory Defaults**.
2. Select **Clear Zones** - a confirmation message will appear asking you to confirm the action.
3. Press **YES** to confirm.

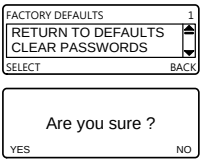



### 10.6.4 Initialize all

***This action resets all system parameters and zones***

To initialize the system:

1. Access the Installer menu and select **Programming → Factory Defaults**.
2. Select **Init All**. A confirmation message will appear asking you to confirm the action.
3. Press **YES** to confirm.

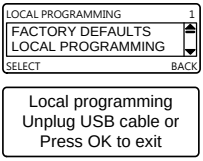



## 10.7 Local programming

The Local Programming mode is used for uploading and downloading data via the "Programming Tool" PC application11. See the Programming Tool guide (P/N 4410401) for complete details

To program the alarm system locally, do the following

1. Access the Installer menu and select **Programming → Local Programming**.
2. Run the "Programming Tool" and follow the instructions.
3. When you are finished, press OK.




***Make sure not to disconnect the USB or power cables during the session, as it may damage the integrity of the alarm system.***

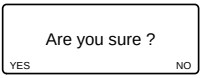
## 10.8 Firmware upgrade

Upgrading the Firmware requires the "Firmware Upgrade Tool". See the tool's guide (P/N 4410401) for more details

To perform a firmware upgrade:

1. Access the Installer menu and select **Programming** → **Firmware Upgrade** - a confirmation message will appear asking you to confirm the action.


2. Press **YES** to confirm.




3. Run the Firmware Upgrade Tool and follow the instructions.
4. When you finish, press OK.

- ***When performing Firmware Upgrade, you must follow the correct procedure, otherwise you can risk system failure, which will make its warranty void.***
- ***Disconnecting power or disconnecting the USB cable, at any stage during the upgrade process may result in system failure.***

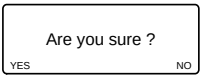
# 11 Stop Communication


The Stop Communication option allows you to temporarily stop all communication, cancel all pending messages and clear all communication buffers. This option may be used on the following situations:

a. During the installation process
b. During testing of the system
c. In the event of a false alarm

To stop communication and clear the buffers, do the following:

1. Access the Installer menu and select **Stop Comm**.
2. Press **Yes** to confirm - all messages in queue will be cleared and will not be sent.



# 12 Remote Operations

## 12.1 PIMAlink app

PIMAlink allows the Master user to control the alarm system, by a simple-to-use application. See our website at http://www.pima-alarms.com/?categoryId=91059, or the system's User Guide for complete details.

## 12.2 Text messages

Some operations of the alarm system - arming and disarming, requesting system status, activating and deactivating the PGM output, stopping the siren and requesting look-in images - are SMS operated.

These operations are processed, only if sent from a contact's phone, and only if the contact is allowed to perform them (see section 10.2.2, on page 41).

Every SMS message contains the event and the device or user name. For example: "Alarm from Kitchen AlarmView".

The alarm system sends a confirmation message (or fault report) on every text command.

Note, that SMS commands are not case sensitive.

### 12.2.1 Commands

Following are the available SMS commands:

| Action | Command |
|---|---|
| Arm AWAY | A/a |
| Arm HOME | H/h |
| Arm PARTI | P/p |
| Disarm | D/d |
| Open PGM output | 1O/o |
| Close PGM output | 1C/c |
| Stop siren | B/b |
| Request system status | S/s |
| Request command list | ? |
| Request look-in image | 25-30I/i<br>99I/i - all visual zones |

# Appendix A System Peripherals

| Peripheral | Description | P/N |
|---|---|---|
| SmartView | PIR/Camera (color) | 8812001 |
| OutView | Outdoor camera (color) | 8813001 |
| PCP | Panic Button/Pendant | 5432004 |
| PIR-S | Standard PIR Detector | 5431001 |
| PIR-P | Pet Immune PIR Detector | 5431002 |
| PIR-O | Outdoor PIR Detector | 5431003 |
| DCM | Door Contact/Magnet | 5432001 |
| SM | Smoke Detector | 5431004 |
| TD-5 | Temperature Detector +5ºC | 5436001 |
| WLD | Water Leakage Detector | 5436002 |
| REP | Range Extender/Repeater | 5435001 |
| DCO | $CO^2$ Detector with EU approval | 5431005 |
| SIR-B | Outdoor Siren – Blue | 5433001 |
| SIR-R | Outdoor Siren – Red | 5433002 |
| SIR-O | Outdoor Siren - Orange | 5433007 |
| SIR-I | Indoor Siren | 5433003 |
| RWK | Remote Wireless Keypad (bi-directional) | 5434001 |
| KF-1 | Hand-held 1-way Keyfob | 5432002 |
| KF-2 | Hand-held 2-way Keyfob (bi-directional) | 5432003 |

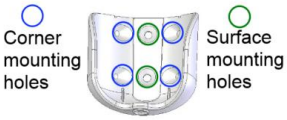
# Appendix B The SmartView Detector/ Camera

## B.1 How to mount the detector

Do the following steps to mount the detector:

1. Release the screw on the bottom of the bracket of the detector, and remove the bracket.

2. Drill holes for surface or corner mounting.
3. Insert the supplied wall plugs and fasten the bracket to the surface with the supplied screws.




4. Place the detector in the mounting bracket and fasten the screw.
5. If you need to adjust the direction of the detector, loosen the screw and rotate it.
6. Fasten the screw tightly.

## B.2 How to replace the battery

When the SmartView batteries are exhausted, do the following to replace them:

1. Release the screw of the bracket at the bottom and remove the detector.
2. Release the screw of the cover of the battery compartment at the back, and remove the cover.
3. Replace the two batteries with new alkaline batteries. See a sticker on the battery holder for correct polarity.
4. When you insert the batteries, the LED will light up in blue for 2-4 sec. to indicate correct installation.
5. Close the cover and fasten the screw.

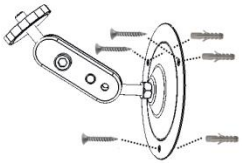
# Appendix C The OutView Camera

## C.1 How to mount the camera

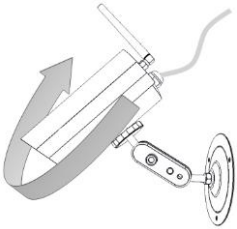
Before you mount the OutView camera, make sure it optimally covers the secured area.

Follow the next steps to mount the camera:

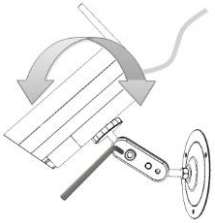
1. Use the template on page 11 and drill 3 matching holes on the mounting surface.
2. Insert the supplied wall plugs and mount the bracket, using the supplied screws.



3. Rotate the swiveling bracket's plastic knob clockwise, to its lower position.
4. Connect the camera to the bracket, by rotating it clockwise.
5. Tighten the plastic knob to secure the camera.



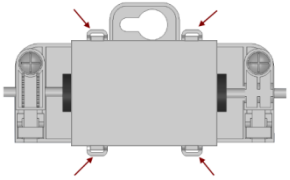
6. Connect the camera's cable to the terminal block and to power. See the next section for details.
7. Adjust the field of view of the camera.
8. Tighten the bracket's tilt screws with the supplied Allen wrench.



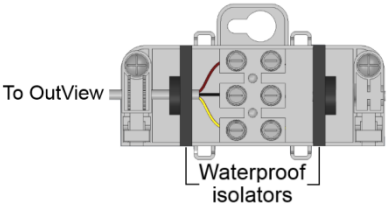
## C.2 How to connect the camera

The OutView is supplied connected with a 3-wire cable to a junction box. The box has a terminal block inside it. To connect the OutView, do the following:

1. Open the junction box: push the clasps outside and remove the lid.



2. Pull out the black waterproof isolator, on the side without the wires.



3. Puncture a hole in the center of the isolator, for the wires of the AC adapter and the trigger source.
4. Put the required wires through the isolator.
5. Connect the AC adapter wires to the Red (+) and Black (-) wires, on the terminal block. See the next section for a diagram.

*The positive wire of the AC adapter is marked with stripes*

6. Connect the wire from the trigger source to the Yellow wire of the OutView, on the terminal block. See the next diagram.

*Two-state triggers, like door contacts and beam detectors, cannot be used*

7. Release the screw on the junction box, on the side of the adapter and the trigger wires, and remove the plastic clip.
8. Put the isolator, now with the wires inserted into it, back in its place.
9. Replace the clip on the wires and fasten the screw.
10. Close the lid and make sure it is fastened by all four clasps.
11. Place the junction box in a weatherproof placement.
12. Plug the AC adapter to an indoor outlet.

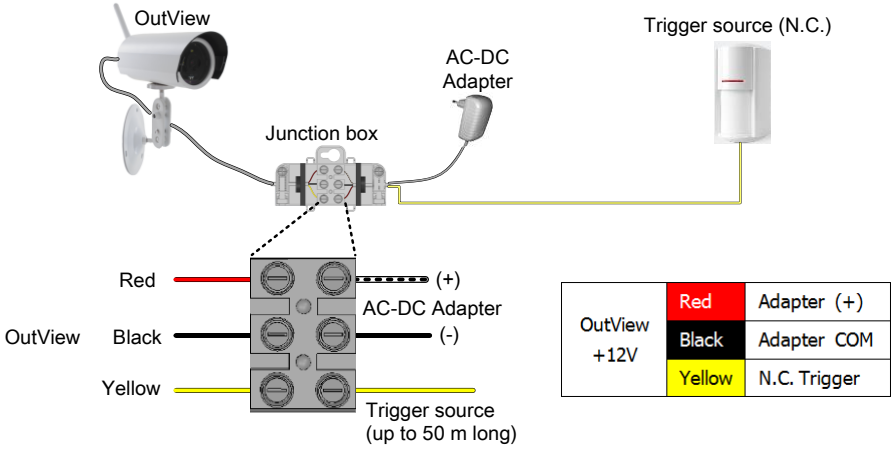



Figure 18. OutView connection diagram

- ***If the AC-DC adapter is also used to power the triggering detector, make sure it does not exceed its power output.***
- ***The OutView does not report a restore event.***

# Appendix D External Siren Indications

The SIR-B/R/O Wireless External Siren can indicate on various system activities.

If this is the first time the siren is set, before setting the available options, initialize the siren by selecting **Service -> Tests -> External Siren -> Test**.

The following table describes the activities and their indications:

| Action | Beeps | Strobe light/Trigger Inputs |
|---|---|---|
| Alarms: Burglary, 24H, Panic, Fire | Siren | Flashes |
| Arming AWAY | 1 | 3 flashes |
| Arming HOME/PART | 2 | 2 flashes |
| Arming with low battery | 5 | 3 flashes, 3 cycles |
| Arming with tamper condition | 5 | 3 flashes, 3 cycles |
| Disarming | 2 | Sequential flashes, 1 cycle |
| Disarming with low battery | 2 | Sequential flashes, 2 cycles |
| Disarming with tamper condition[21] | 2 | 3 sec. alarm, sequential flashes |

[21] Siren tone confirmation must be enabled in the control panel

# Appendix E Maintenance & Troubleshooting

## E.1 Cleaning the LCD screen

The LCD screen may occasionally get finger oil stains and accumulate dust. It should be cleaned only with a soft dry cloth or a special LCD screen cleanser. Avoid the use of abrasives of any kind.

***Do not use solvents such as kerosene, acetone or thinner. These will harm the external finish and damage the transparency of the window.***

## E.2 Replacing the Control Panel's battery

***Remove the transformer from the AC outlet or disconnect the power before replacing the backup battery.***

***For best performance and care, use suitable replacement batteries from Pima Electronic Systems.***

For instructions on how to replace the backup battery, see the "Quick installation" section, on page 15.

## E.3 SIM card icons and LED behavior

| | OK/ Active | Not detected/ At fault | Two SIMs at fault |
|---|---|---|---|
| **SIM-1 (Main)** |  |  |  |
| **SIM-2 (Backup)** |  |  | |
| **LED** | - |  |  |

# Appendix F Glossary of terms

**Alarm types** –

- **Burglary** – alarm caused by violation of intrusion zone
- **Fire** – alarm caused by violation of fire zone
- **Tamper** – alarm caused by opening tamper protection switch
- **Panic/Medical/Emergency** – alarm caused by activation of a panic/medical button

**Alarm Restore** – closing the alarm event and restoring the system to its previous state

- **Arming modes** and options–
  - **Away** – full arming of the system
  - **Home** – arming of perimeter detectors, as defined by the installer
  - **Partial** – arming of part of the premises, while leaving the other part unsecured
  - **One-Key Arming** – arming of the system pressing a single key, without any code
  - **Force Arm** – arming the system even if it is not ready, under the condition that all open zones will be closed by the end of the Exit delay. If the zone/s is open when the exit delay expires, an alarm is generated.
- **Bypassing Zones** – temporarily ignoring signals from a zone, to allow accessing to part of the protected area while the system is armed. Zone bypassing can also be used when a zone is at fault, but only until the fault is repaired. Bypassed zones are automatically un-bypassed (that is returning to normal mode) when disarming the alarm system.
- **Chime** – bell sound, typically assigned to entry points or back doors, to warn when a zone is opened while the system is disarmed.
- **CMS Contact** – Central Monitoring Station contact
- **Contact** – person that receive notifications on system events and faults, and can perform some actions remotely, by text messages.
- **Control panel** – is where the user can activate/deactivate the alarm system as well as change the various system configurations. This is the heart and brains of the system which also includes the system's communication module.
- **Detectors/Devices/Peripherals** –
  - **Device ID** – unique identifier of detectors and peripherals
  - **Types**:
    - **PIR (Passive Infrared) Detector** – heat emission detector of humans and animals
    - **Door Contact** – magnetically operated detector, usually used on doors and windows
    - **Keyfob** – small remote control for arming and disarming the system
    - **Smoke Detector** – sensing device which detects smoke particles of combustion
    - **Panic button** – button that triggers emergency alarm
- **Disarmed** – Normal, standby mode. All zones, except 24 hour zones (Panic, Fire, Tamper, etc.) are not active.
- **Dual SIM mode**[22] – The control panel checks the SIM card slots on power-up only, and sets the mode between Single of Dual. When two SIMs are detected, the SIM in the upper slot is defined as Main (SIM1), and the one in the lower as Backup (SIM2).

[22] For dual SIM versions only

- **Entry/Exit Delay** – predetermined time to allow entering and exiting the premises without triggering the alarm.
- **Event Group** – a group of events defined by type, for notifying the contacts
- **SIM Swap**[22] – The control panel automatically swaps from SIM1 to SIM2 (and vice versa), when one of the following occurs: low GSM reception, GSM/GPRS loss, Jamming, and CMS communication fault (including retries).
  The control panel will keep trying to send events via SIM 1 and when it does, it will swap from SIM2 back to SIM1. The control panel report on why the swap was performed. See section E.3, on page 58, for more information.
- **Swinger Shutdown** – this feature prevents a zone to repeatedly trigger the alarm, if it is opened and closed (this is a "swinger") again and again (or left open). With this feature ON, the zone will only trigger the alarm as many times as is designated - once, twice or three times.
- **System Ready** – all zones that are part of the defined arming mode are closed, and the system can be armed.
- **Users** –
  - **Regular** – can arm and disarm the system and view its status
  - **Master** – can change settings relating to the system behavior, change all passwords except the Installer's and do everything regular user can.
- **Zone** – protected area connected with detector
- **Zone Types** –
  - **Normal (Immediate)** – intrusion protected zone. Immediately activates the alarm if violated while the system is armed.
  - **Entry/Exit** – intrusion protected zone. Activates the alarm if violated while the system is armed, only after the entry/exit delay expires, to allow entering/exiting the protected area.
  - **Follower (Inhibited/Intermediate)** – intrusion protected zone that "follows" the entry/exit zones: if violated while any entry/exit zone has already been opened, it will not trigger the alarm. Typically used in zones adjoining the entry/exit route.
  - **24 hr.** – intrusion protected zone, that will immediately trigger the alarm if opened, regardless of the system state (armed or disarmed).
  - **Panic (Personal Attack) and Medical** – button operated zone, used in panic/distress or medical situations. Pressing the button will immediately trigger the alarm, regardless of the system state (armed or disarmed). Panic buttons and zones trigger silent alarm.
  - **Fire** – smoke and heat detectors, that will immediately trigger the alarm in fire/heat conditions, regardless of the system state (armed or disarmed).

# Appendix G Event Reporting

The contacts of the alarm system can be reported on various system events. The events are divided into several groups: alarms, arming and disarming, power loss and service events. See the table below for the full list of the events and their ContactID codes.

| Event | Text |
|---|---|
| **Alarms** | |
| Zone alarm | Alarm from Zone + *zone no. (zone name)* |
| Zone alarm restore | Zone Alarm Restore + *zone no. (zone name)* |
| Fire alarm | Fire Alarm + *zone no. (zone name)* |
| Fire alarm restore | Fire Alarm Restore + *zone no. (zone name)* |
| Gas alarm | Gas Alarm + *zone no. (zone name)* |
| Gas alarm restore | Gas Alarm Restore + *zone no. (zone name)* |
| Panic alarm | Panic Alert + *button name* |
| Panic alarm restore | Panic Alert Restore + *button name* |
| Tamper alarm | Tamper + *zone no. (zone name)* or *System (system name)* |
| Tamper alarm restore | Tamper Restore + *zone no. (zone name)* or *System (system name)* |
| Disarm with Duress code | Duress + *System (system name)* |
| Zone bypassed | Zone Bypassed + *zone no. (zone name)* |
| Zone un-bypassed | Zone Unbypassed + *zone no. (zone name)* |
| Bell cancel | Bell cancel + *user*[23] |
| **Arm and disarm** | |
| Arm to Away mode | Full Arm (Away) + *User no. (user name)/Peripheral no. (peripheral name)* |
| Arm to Home mode | Perimeter Arm (Home) + *User no. (user name)/ Peripheral no. (peripheral name)* |
| Arm to Part mode | Part Arm + *User no. (user name)/ peripheral no. (peripheral name)* |
| Disarm | Disarm +*User no. (user name)* |
| Disarm after alarm[24] | Disarm After Alarm +*User no. (user name)* |
| Disarm failed | Disarm Failed +*User no. (user name)* |
| Full/Perimeter/Part arm failed | Full/Perimeter/Part Arm Failed + *User no. (user name)/peripheral no. (peripheral name)* |
| **Service** | |
| AC loss | AC Loss + *System (system name)* |
| AC restore | AC Restore + *System (system name)* |
| Backup network error | Backup Network Error + *System (system name)* |
| Backup network restore | Backup network rest *System (system name)* |
| Backup SIM failure | Backup SIM failure + *System (system name)* |
| Backup SIM restored | Backup SIM Restored + *cause of switching event* |
| Communication loss | Communication Loss + *Source* |
| Communication restore | Comm. Restore + *Source* |
| Date was set | Set Date + MASTER CODE/INSTALLER |
| End remote programming | End Remote Prog + *System (system name)* |
| End system programming | End System Prog + *System (system name)* |
| Main SIM failure | Main SIM failure + *System (system name)* |

[23] Only to CMS contacts and only to the contact who cancelled the bell
[24] This action is not logged

| | |
|---|---|
| Main SIM restored | Main SIM Restored + *cause of switching*<br>The cause may be one of the following:<br>• SIM not inserted<br>• Pin code needed<br>• Low reception<br>• GSM loss<br>• GPRS loss<br>• Session open failure<br>• CMS1 Tx failure<br>• CMS2 Tx failure<br>• Keepalive failure |
| Periodic test | Periodic Test |
| Peripheral battery low | Accessory Battery + Zone |
| Peripheral battery restore | Accessory Batt. Rest + Zone |
| PGM close | PGM Close |
| PGM open | PGM Open |
| Remote look-in failed | Remote Look-In Failed |
| Remote look-in request | Remote Look-In Request |
| Remote programming | Remote Programming + *System (system name)* |
| RF interference | RF Interference |
| RF interference restore | RF Interference Rest |
| SIM Switched to Backup | SIM Switched to Back + *cause of event* |
| SIM switched to main | SIM Switched To Main + *cause of switching event* |
| Status report | Status Report |
| Supervision loss | Supervision Loss + *zone no. (zone name)* |
| Supervision restore | Supervision Restore + *zone no. (zone name)* |
| System battery loss | System Battery Loss + *System (system name)* |
| System battery low | System Battery + *System (system name)* |
| System battery low restore | System Battery Rest + *System (system name)* |
| System peripheral restore | Syst Periph Restore+ Zone |
| System peripheral trouble | Syst Periph Trouble + Zone |
| System programming | System Programming + *System (system name)* |
| Time was set | Set Time + MASTER CODE/INSTALLER |
| User code changed | User Code Changed +*User no. (user name)* |
| User code deleted[24] | User Code Deleted +*User no. (user name)* |
| Zone trouble | Zone Trouble + *zone no. (zone name)* |
| Zone trouble restore | Zone Trouble Restore + *zone no. (zone name)* |

# Appendix H SIA and ContactID Codes

## H.1 Events codes

### H.1.1 ContactID

| | |
|---|---|
| 101 | Emergency |
| 110 | Fire |
| 120 | Panic |
| 121 | Duress |
| 122 | Silent |
| 123 | Audible |
| 130 | Burglary |
| 131 | Perimeter |
| 132 | Interior |
| 134 | Entry/Exit |
| 137 | Tamper/CP |
| 301 | AC loss |
| 302 | Low system battery |
| 321 | Bell |
| 344 | RF receiver jam detect |
| 350 | Communication trouble |
| 351 | Telco fault |
| 381 | Loss of supervision RF |
| 383 | Sensor tamper |
| 384 | RF low battery |
| 401 | O/C by user |
| 406 | Cancel |
| 408 | Quick arm |
| 441 | Armed home |
| 456 | Partial arm |
| 459 | Recent close |
| 570 | Bypass |
| 602 | Periodic test report |
| 607 | Walk test mode |
| 641 | Senior watch trouble |

### H.1.2 SIA

| | |
|---|---|
| AR | AC Restore |
| AT | AC Trouble |
| BA | Burglary Alarm |
| BB | Burglary Bypass |
| BC | Burglary Cancel |
| BR | Burglary Restore |
| BT | Burglary Trouble / Jamming |
| BZ | Missing Supervision |
| CF | Forced Closing |
| CL | Closing Report |
| CR | Recent Close |
| FA | Fire Alarm |
| FR | Fire Restore |
| HA | Holdup Alarm (duress) |
| LR | Phone Line Restore |
| LT | Phone Line Trouble |
| OP | Opening Report |
| PA | Panic Alarm |
| QA | Emergency Alarm |
| RP | Automatic Test |
| RX | Manual Test |
| RY | Exit from Manual Test |
| TA | Tamper Alarm |
| TR | Tamper Restore |
| XR | Sensor Battery Restore |
| XT | Sensor Battery Trouble |
| YR | System Battery Restore |
| YT | System Battery Trouble |
| YX | Service Required |

## H.2 Device number

| | |
|---|---|
| Control Panel | 00 |
| Wireless Zones | 01-24 |
| Wireless Video Zones | 25-30 |
| Hardwires Zones | 51-53 |
| Remote Control Keyfobs/Panic | 31-50 |
| Wireless Keypads | 61-63 |
| Built-in Keyboard | 00 |
| External Wireless Siren | 70 |
| GSM/GPRS Modem | 80 |
| Local USB Access | 71 |

## H.3 User number

| | |
|---|---|
| Regular User | 01-25 |
| Master User | 26 |
| Duress code | 27 |
| 24H code | 28 |
| Installer code | 29 |

# Appendix I Confirmation Text Messages

Every SMS message received in the control panel (from a confirmed telephone number) is replied with a confirmation (or error) message. The next table lists the various messages.

| Message | Confirmation message | Error message |
|---|---|---|
| Arm Away/Home/ Part | *Armed Away/Home/Part* by *User Name* | *Arm Away/Home/Part failed* |
| Disarm | Disarmed by User Name | Disarm failed |
| xx25-30 (look-in image request) | *Picture from Zone No.* | *Operation failed* |
| Stop bell | *Bell canceled* by *User Name* | - |
| Status | • *Away/Home/Part/Disarm state*<br>• *PGM #1 Opened/Closed* | - |
| ? (command list) | • Away: A,a<br>• Home: H,h<br>• Part: P,p<br>• Disarm: D,d<br>• Image: xxI, xxi zone 25-30, all- 99<br>• PGM Open: 1O,1o<br>• PGM Close: 1C,1c<br>• Stop Bell: B,b<br>• Status: S,s<br>• Help: ? | - |

# Appendix J Limited Warranty

PIMA Electronic Systems Ltd. ("the Manufacturer") warrants its products hereinafter referred to as "the Product" or "Products" to be in conformance with its own plans and specifications and to be free of defects in materials and workmanships under normal use and service for a period of twelve (12) months from the date of shipment by the Manufacturer. The Manufacturer's obligations shall be limited within the warranty period and its option, to repair or replace the product or any part thereof. The Manufacturer shall not be responsible for dismantling and/or reinstallation charges. To exercise the warranty, the product must be returned to the Manufacturer freight prepared and insured.
The warranty does not apply in the following cases: improper installation, misuse, failure to follow installation and operating instructions, alteration, abuse, accident or tampering, and repair by anyone other than the Manufacturer.

The warranty is exclusive and expressly in lieu of all other warranties, obligations or liabilities, whether written, oral, express or implied, including any warranty of merchantability or fitness for a particular purpose, or otherwise. In no case shall the Manufacturer be liable to anyone for any consequential or incidental damages for breach of this warranty or any other warranties whatsoever, as aforesaid.

This warranty shall not be modified, varied or extended, and the Manufacturer does not authorize any person to act on its behalf in the modification, variation or extension of this warranty. This warranty shall apply to the Product only. All products, accessories or attachments of others used in conjunction with the Product, including batteries, shall be covered solely by their own warranty, if any. The Manufacturer shall not be liable for any damage or loss whatsoever, whether directly, indirectly, incidentally, consequentially or otherwise, caused by the malfunction of the Product due to products, accessories, or attachments of others, including batteries, used in conjunction with the Products. The Manufacturer does not represent that its Product may not be compromised and/or circumvented, or that the Product will prevent any death, personal and/or bodily injury and/or damage to property resulting from burglary, robbery, fire or otherwise, or that the Product will in all cases provide adequate warning or protection. User understands that a properly installed and maintained alarm may only reduce the risk of events such as burglary, robbery, and fire without warning, but it is not insurance of a guarantee that such will not occur or there will be no death, personal damage and/or damage to property as a result.

The Manufacturer shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function. However, if the Manufacturer is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regardless of cause of origin, the Manufacturer's maximum liability shall not in any case exceed the purchase price of the Product, which shall be fixed as liquidated damages and not as penalty, and shall be the complete and exclusive remedy against the Manufacturer.

Warning: The user should follow the installation and operation instructions and among other things test the product and the whole system at least once a week. For various reasons, including, but not limited to, changes in environmental conditions, electric or electronic disruptions and tampering, the Product may not perform as expected. The user is advised to take all necessary precautions for his/her safety and the protection of his/her property.

* Patent Pending Technology

# Appendix K Declaration of Conformity

FOR BETTER PROTECTION

## EC Declaration of Conformity

We, the undersigned,

**PIMA Electronic Systems Ltd.**
**Address:** 5 Hatzoref Street, Holon 5885633, Israel
**Phone:** +972.3.6506414
**Fax:** +972.3.5500442
**Website:** www.pima-alarms.com

Certify and declare under our sole responsibility that the following equipment:

| Brand | Model No/Cat. No | Product description |
|---|---|---|
| Burglar Alarm | AlarmView | Visual Verification Alarm Panel |
| | Guardian | Wireless Intruder Alarm Panel |
| | AVR | Add-on Visual Verification Module |

Was tested to and conforms with the requirements included in following standards:

| Standard | Directive |
|---|---|
| EN 60950-1:2001, A11, corrigendum 2004 | Low voltage Directive 2006/95/EC |
| EN 301 489-1 Ver 1.4.1: 2002-08<br>EN 301 489-3 V1.4.1 (2002-08)<br>EN 301 489-17 Ver 1.2.1: 2002-08<br>EN 50130-4:1995 , Amendment A1: 1998 | EMC Directive 2004/108/EC |
| EN 300 328 Ver 1.4.1 (2003)<br>EN 300 220-1 / V1.3.1 (2000-09)<br>EN 300 220-3 / V1.3.1 (2000-09)<br>EN 301 511-3 / V9.0.2 (2003-03) | Directive 1999/5/EC – RTTE |

And therefore complies with the requirements and provisions of the Council Directives of the European Parliament.

CE marking date 19/02/2007

Certification Manager: VP & CTO

Name: Haim Dembsky

Date: Holon, ISRAEL, Jul 29th, 2013

Signature:

PIMA ELECTRONIC SYSTEMS LTD. * PIMA FOR BETTER PROTECTION * 5 HAZOREF ST. HOLON 58858 ISRAEL

CE

Hereby,

Company: PIMA Electronic Systems Ltd.

Address: 5 Hatzoref Street, Holon 5885633

Country: Israel

Telephone number: +972.3.6506414

Fax number: +972.3.5500442

PIMA Electronic Systems Ltd. declares that the AlarmView system is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

**Federal Communications Commission (FCC) Part 15 Statement**

This equipment has been tested to FCC requirements and has been found acceptable for use. The FCC requires the following statement for your information.

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for a Class B computing device in accordance with the specifications in Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

If using an indoor antenna, have a quality outdoor antenna installed.

Reorient the receiving antenna until interference is reduced or eliminated.

Move the receiver away from the control/communicator.

Plug the control/communicator into a different outlet so that it and the receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions.

The user or installer may find the following booklet prepared by the Federal Communications Commission helpful: "Interference Handbook." This booklet is available from the U.S. Government Printing Office, Washington, DC 20402.

The user shall not make any changes or modifications to the equipment unless authorized by the Installation Instructions or User's Guide. Unauthorized changes or modifications could void the user's authority to operate the equipment.

**RoHS compliance - All our products are lead-free**

**PIMA Electronic Systems is ISO 9001 certified**

All data contained herein is subject to change without prior notice.
PIMA Electronic Systems Ltd.
* Patent Pending Technology

FOR BETTER PROTECTION

**Pima Electronic Systems Ltd.** **WWW.PIMA-ALARMS.COM**
5 Hatzoref Street, Holon 5885633
ISRAEL
Tel: +972.3.650.6414 Fax: +972.3.550.0442
E-mail: support@pima-alarms.com
sales@pima-alarms.com

Distributed and Supported by:

P/N: 4410375
Revision C, XX en (Mar 2016)
System version 2.10