



# Programming Guide for the FORCE and VISION Alarm Systems

Control panel ver. 1.6 and up

## TABLE OF CONTENTS

<b>1</b>	<b>How to Connect LCD Keypad .....</b>	<b>3</b>
1.1	FORCE .....	3
1.2	VISION .....	3
<b>2</b>	<b>Menus and codes.....</b>	<b>4</b>
2.1.1	Code setting guidelines .....	4
2.1.2	Activation codes .....	4
2.2	Changing the default Master and Technician codes .....	4
2.3	The technician menu .....	4
2.3.1	System Configuration.....	5
2.3.2	Tests & Diagnostics.....	5
<b>3</b>	<b>Peripherals.....</b>	<b>6</b>
3.1	Zone expanders .....	6
3.2	Tampers and EOLs.....	6
3.3	Keypad Settings <sup>2</sup> .....	7
3.4	Wireless peripherals.....	7
<b>4</b>	<b>Zones .....</b>	<b>11</b>
4.1	Zone Settings .....	11
4.2	Zone Types Settings .....	13
4.2.1	Attributes.....	13
4.3	Copy Zones .....	14
4.3.1	Single to Multiple.....	14
4.3.2	Multiple to Multiple .....	14
4.4	Partitions Names .....	14
<b>5</b>	<b>Outputs.....</b>	<b>15</b>
5.1	Onboard.....	15
5.2	Zone Expanders .....	16
5.3	Outputs Expander.....	16
5.4	Wireless Sirens .....	16
<b>6</b>	<b>CMS &amp; Communications .....</b>	<b>17</b>
6.1	Monitoring Stations.....	17
6.1.1	CMS 1-3.....	17
6.1.2	Radio.....	19
6.1.3	Custom Zones Reports .....	20
6.2	PIMA Cloud.....	20
6.3	General Settings.....	21
6.4	Telephone Settings .....	21

6.5	Network Settings.....	21
6.6	Cellular Settings.....	22
<b>7</b>	<b>Faults.....</b>	<b>23</b>
7.1	AC Fault.....	23
7.2	Low Battery, Phone Line, Network, Cellular Module.....	23
7.3	Invalid Code.....	23
7.4	CMS Comm., Tamper Open, Invalid Code, Other Faults.....	23
<b>8</b>	<b>Timers and Counters.....</b>	<b>24</b>
8.1	Programmable Output Types.....	25
<b>9</b>	<b>General Settings.....</b>	<b>26</b>
9.1	Arming Prevention.....	27
<b>10</b>	<b>Reset to Defaults.....</b>	<b>28</b>
10.1	Resetting to factory defaults.....	28
<b>11</b>	<b>Tests &amp; Diagnostics.....</b>	<b>29</b>
11.1	Event Memory.....	29
11.2	Zone Test.....	29
11.3	Output Test.....	30
11.4	Power Diagnostics.....	30
11.5	Communication Tests.....	30
11.6	Communication Monitor.....	30
11.7	Wireless Peripherals.....	31
<b>12</b>	<b>Service and Remote Upgrading.....</b>	<b>32</b>

## APPENDIXES

<b>Appendix A.</b>	<b>Implementing Partitions.....</b>	<b>33</b>
<b>Appendix B.</b>	<b>Remote Up/Download.....</b>	<b>34</b>
<b>Appendix C.</b>	<b>Programmable Output Types.....</b>	<b>35</b>
<b>Appendix D.</b>	<b>Technician and CMS Codes.....</b>	<b>36</b>
<b>Appendix E.</b>	<b>Text and Characters.....</b>	<b>37</b>
<b>Appendix F.</b>	<b>Zone and System Status.....</b>	<b>38</b>
<b>Appendix G.</b>	<b>CMS Event Reporting.....</b>	<b>39</b>

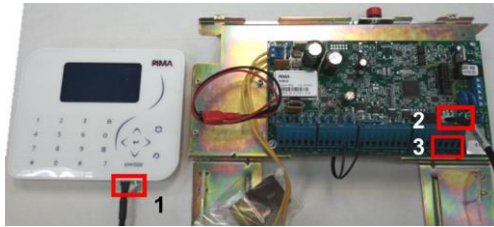
# 1 How to Connect LCD Keypad

Connect an LCD keypad (KLT/KLR500) to program the alarm system; see how below.

## 1.1 FORCE

Connect the keypad to the control panel in one of the following two options:

1. Connect a Molex cable (P/N 3411119) between the keypad's socket at the bottom (no. 1 in the image below), and the technician keypad's connector (no. 2 in the image).
2. Connect four wires (not supplied) between the FORCE BUS terminals in the control panel (no. 3 in the image) and the keypad's terminal block (open the keypad's back cover).



## 1.2 VISION

Connect a Molex cable (P/N 3411119) between the keypad's socket (no. 1 in the image below) and one of the technician keypad's connectors (marked with two red rectangles in the image).



## 2 Menus and codes



Some of the menus are *FORCE* only; see relevant footnotes.

The alarm system has two programming menus: User, and Technician; each menu is accessed using its Master code. In addition, a Central Monitoring Station (CMS) menu can be accessed using a separate CMS Lock code:

- **Master User code:** allows accessing all the user menus.
- **Master Technician code:** allows accessing all the technician menus, except locked CMS menu.
- **CMS Lock code:** an optional code for preventing access to the CMS settings by using the Master technician code. This code only allows the technician/CMS to set and access the CMS' communication definitions, including the account ID and the paths.

### 2.1.1 Code setting guidelines

Note the following when setting codes in the *FORCE* security system:

- All codes are made of four to six digits, except the *Quick Arm* (two digits)
- A code cannot start with the *Quick Arm's* two digits or the four digits of any code.
- A code cannot be viewed, nor retrieved.

### 2.1.2 Activation codes

Eight codes to be used for activating devices (via relay outputs) by the system users - whether it is an electric gate or a floodlight, users can turn them on and off using these codes. Triggering the outputs is done using the *Activation Codes 1-8* programmed output types (see Appendix C, on page 35).

Activation codes are subject to keypad and user partitioning.

## 2.2 Changing the default Master and Technician codes

To enter the menus for the first time, the default codes must be changed. Follow the next steps to change the codes.

1. Connect the alarm system to power and wait for the main screen to be displayed.
2. Press 5555; the codes' menu is displayed.
3. Press ← - the cursor moves to the right of the *Master Code*.
4. Enter a new 4-6 digit code. Write down the code and advise the system owner to keep it in a safe place.
5. Press ← to save the code.
6. Press the down arrow to the *Tech. Code* and press ←.
7. Enter a new 4-6 digit technician code.
8. Press ← to save the code.
9. Press ⏪ to exit.

```
User Menu
Master Code:--
Tech. Code:--

Press 0 to Exit.
```

### 2.3 The technician menu

The *Technician* menu has two sub-menus: *System Configuration* and *Tests & Diagnostics*.

### 2.3.1 System Configuration<sup>1</sup>

The *System Configuration* menu includes the sub-menus listed in the next table:

Menu	Parameters
<b>Peripherals</b>	Zone and output expanders, keypads, tamper switches, and EOL resistors.
<b>Zones</b>	Zone and zone type definitions, copy zones.
<b>Outputs</b>	Control panel and expanders' relay outputs.
<b>CMS &amp; Communications</b>	CMS 1-2 definitions, PIMA cloud, and radio report codes.
<b>Faults</b>	System responses to faults and entering false code.
<b>Timers &amp; Counters</b>	Programmable output types and other timers
<b>General Settings</b>	System name, service provider, Master technician code, and other parameters.
<b>Reset to Defaults</b>	Partial or full system reset

### 2.3.2 Tests & Diagnostics

See chapter 11, on page 29.

<sup>1</sup> Some menus are *FORCE* only.

# 3 Peripherals

The *Peripherals* menu includes the following sub-menus:

- 1) Zone Expanders; see below.
- 2) Tamper and EOLs; see below.
- 3) Keypads (addressable):
  - **FORCE**: ID=1-16; **FORCE Lite/32**: ID=1-8. Keypad with ID=0 is not supervised, nor can use partitions.
  - **VISION**: ID=0
- 4) Keypad Settings; see section 3.3, on page 7.
- 5) Outputs Expanders; enter the number of the installed expanders.
- 6) Wireless Peripherals; see section 3.3, on page 7.

## 3.1 Zone expanders<sup>2</sup>

System Configuration ► Peripherals ► Zone Expanders

The *Zone Expanders* menu includes the following sub-menus:

- 1) Remote Zone Exp.: set the number of the ZEX508 and ZEX516 zone expanders.



*Each 16-zone expander is programmed as two eight-zone expanders, and occupies two consecutive ID numbers. For example, if expander #3 is a 16-zone one, it takes ID #3 and #4, so expander #4, the next one will take ID #5 (and not #4).*

- 2) Local Zone Expander: select if the ZEL508 local zone expander is installed.
- 3) Zone Doubling: select if in use.

## 3.2 Tamper and EOLs<sup>3</sup>

System Configuration ► Peripherals ► Tamper and EOLs

Parameter	Description
Tamper 1	TMPR1 input is active.
Tamper 1+EOL	TMPR1 input is EOL supervised, for detecting short (single EOL).
Tamper 2	TMPR2 input is active. <b>FORCE Lite/32</b> : unavailable
Tamper 2+EOL	TMPR2 input is EOL supervised, for detecting short (single EOL).
External Siren+EOL	The SIREN Ext/Int output is EOL supervised, for detecting cut and short.
Internal Siren+EOL	
Double EOL	Two EOL resistors are used on all EOL supervised loops.
Resistor 1-2	Enter the resistors values in Ohm. The value entered is multiplied by 100. For example, when using a 2.2kΩ resistor, set the value to 220.

<sup>2</sup> **FORCE** only

<sup>3</sup> EOL: **FORCE** only

## 3.3 Keypad Settings<sup>2</sup>

System Configuration ► Peripherals ► Keypad Settings

Press \* or # to select a keypad. Note that the *Keypad Settings* menu applies only for addressable keypads, and it includes the following sub-menus:

- 1) Name: user text, up to 16 characters.
- 2) Options

Parameter	Description
Illum. During Alarm	The keypad will illuminate during the alarm time
Illum. During Delay	The keypad will illuminate during the exit/entry delay times

- 3) Partitions: select the keypad's partitions by pressing the desired numbers; the selected partition/s will stay on.

## 3.4 Wireless peripherals

Note: The *FORCE* system supports 2-way wireless peripherals by control panel with firmware ver. 1.6 and up.

System Configuration ► Peripherals ► Wireless Peripherals

- 1) Global Settings

Parameter	Description	Default	Range
Expanders	The no. of wireless receivers. Note, that <i>FORCE</i> automatically allocates wireless zones with numbers higher than any hardwired zone. If a hardwired zone expander is installed when wireless zones are already defined, <i>FORCE</i> will reallocate the wireless zones. One 2-way receiver can be installed or two 1-way. The 2-way receiver must be the first one (number 1).	0	0-2
Supervision	An interval during which, if the control panel receives no wireless event, it transmits a <i>Supervision Loss</i> report.	12h	1-24h
Jamming Alert	Alarm and report when the receiver is jammed	-	-
Enrollment-Any Event	<ul style="list-style-type: none"> <li>• <u>Selected</u>: any event (detection, tamper) can be used for enrollment.</li> <li>• <u>Cleared</u>: only "Enrollment" event can be used for enrollment.</li> </ul>		
Cancel	<ul style="list-style-type: none"> <li>• <u>Selected</u>: do not send 'Start Delayed Siren' at the beginning of entry delay. If not selected, the siren will be activated if disarming is not received by the siren at the end of the entry delay.</li> </ul>		

- 2) Enroll and delete

After the receiver installation and before peripherals enrollment, please enter the following menu:

Installer Menu ► Diagnostic ► Wireless Peripherals ► Receiver

Record the displayed *Noise Level*



If the value is greater than 15 – relocate the receiver or track the noise origin.

While enrolling, make sure that the received signal strength of each peripheral exceeds the recorded noise level.

- Detectors

Parameter	Description
Enroll	<p>The selected zone is the next available one. Press * or # to scroll.</p> <p>1) Manual:</p> <ul style="list-style-type: none"> <li>Serial no.: the peripheral's serial number (printed on the product's label). To enter letters (A-F), press the asterisk key repeatedly.</li> <li>Additional zone: the second zone number for the door contact (DCM)<sup>4</sup> and the Smoke/Heat detector (DSH). Note: applied to 1-way peripherals only.</li> </ul> <p>For 2-way detector DCM743 you should enroll twice if you want to use the external (auxiliary) input. See DCM743 manual.</p> <p>In smoke &amp; heat detector DSH743 there is no distinction between smoke zone and heat zone; in addition, there is a possibility to set the detection type – see Wireless Zone Characteristics.</p> <ul style="list-style-type: none"> <li>Enroll: press to enroll the detector.</li> </ul> <p>2) Auto: activate the detector; see <i>Enrollment-Any Event</i> above.</p> <ul style="list-style-type: none"> <li><u>Status</u>: the system is waiting for a signal or displays the received detector.</li> <li><u>Enroll</u>: press to enroll the detector, or if multiple detectors are received, scroll between them using the left-right arrow keys and then press <i>Enroll</i>.</li> </ul>
Delete	<p>1) Delete: press * or # to select a zone.</p> <ul style="list-style-type: none"> <li>Delete the selected zone.</li> </ul> <p>2) Delete All: delete all the defined zones.</p>

- Keyfobs and Panic Buttons

Parameter	Description
Enroll	<p>The selected User is the next available one. Press * or # to scroll.</p> <p>1) Manual:</p> <ul style="list-style-type: none"> <li>Serial no.: the device's serial number (printed on the product's label). To enter a letter (A-F), press the asterisk key repeatedly.</li> <li>Enroll: press to enroll a keyfob to the selected user.</li> </ul> <p>2) Auto: press any keyfob button. For RMC743 model, press  and  simultaneously for 2 seconds min.</p> <p>Status: the system is waiting for a signal, or displays the received keyfob.</p> <ul style="list-style-type: none"> <li>Enroll: press to enroll the keyfob, or if multiple keyfobs are received, scroll between them using the left-right arrow keys and press <i>Enroll</i>.</li> </ul> <p>3) For receiver WRF743 (2-way), up to 16 keyfobs can be enrolled.</p>
Delete	<p>1) Delete: press * or # to select a user (printed on the product's label). To enter a letter (A-F), press the asterisk key repeatedly.</p> <ul style="list-style-type: none"> <li>Delete the selected keyfob.</li> </ul> <p>2) Delete All: delete all the defined keyfobs.</p>

<sup>4</sup> When using the additional zone of the door contact, the first zone must be enrolled, even if it is not going to be used. After enrolling the two zones, the first zone can be deleted and re-used.





- Sirens

Parameter	Description
Enroll	<ol style="list-style-type: none"> <li>1) Manual: <ul style="list-style-type: none"> <li>▪ Serial no.: the siren's serial number.</li> <li>▪ Enroll: press to enroll the selected siren.</li> </ul> </li> <li>2) Auto: for 1-way (SRO143) press the siren's enrollment button. For 2-way (SRO743) press the tamper switch for at least 3 seconds. See the SRO743 for detailed description. <ul style="list-style-type: none"> <li>▪ Status: the system is waiting for a signal, or displays the received siren.</li> <li>▪ Enroll: press to enroll the selected siren.</li> </ul> </li> </ol>
Delete	<ol style="list-style-type: none"> <li>1) Delete: press * or # to select a user. <ul style="list-style-type: none"> <li>▪ Delete the selected siren.</li> </ul> </li> <li>2) Delete All: delete all the defined sirens.</li> </ol>

- Repeaters

Parameter	Description
Enroll	<ol style="list-style-type: none"> <li>1) Manual: <ul style="list-style-type: none"> <li>▪ Serial no.: the repeater's serial number.</li> <li>▪ Enroll: press to enroll the repeater.</li> </ul> </li> <li>2) Auto: the selected repeater is the next available one. Press * or # to scroll, and press the enrollment button on the repeater. <ul style="list-style-type: none"> <li>▪ Status: the system is waiting for a signal, or displays the received repeater/s.</li> <li>▪ Enroll: press to enroll the repeater, or, if multiple repeaters are received, scroll between them using the left-right arrow keys and press <i>Enroll</i>.</li> </ul> </li> </ol>
Delete	<ol style="list-style-type: none"> <li>1) Delete: press * or # to select a repeater. <ul style="list-style-type: none"> <li>▪ Delete the selected repeater.</li> </ul> </li> <li>2) Delete All: delete all the defined repeaters.</li> </ol>

- Arming Stations

Parameter	Description
Enroll	<ol style="list-style-type: none"> <li>Manual: <ul style="list-style-type: none"> <li>Serial no.: the device's serial number.</li> <li>Enroll: press to enroll the arming station.</li> </ul> </li> <li>Auto: the selected arming station is the next available one. Press * or # to scroll. For 1-way (KAS143) – press the enrollment button on the device.   For 2-way (KAS743) – press on  . Note: refer also to the specific manual of KAS743 <ul style="list-style-type: none"> <li>Status: the system is waiting for a signal, or displays the received arming station/s.</li> <li>Enroll: press to enroll the arming station, or, if multiple devices are received, scroll between them using the left-right arrow keys and press <i>Enroll</i>.</li> </ul> </li> </ol>
Delete	<ol style="list-style-type: none"> <li>Delete: press * or # to select a device. <ul style="list-style-type: none"> <li>Delete the selected arming station.</li> </ul> </li> <li>Delete All: delete all the defined arming stations.</li> </ol>
Settings	<ol style="list-style-type: none"> <li>Partitions: for each arming station, select its allocated partitions.</li> <li>Name: user text, up to 28 characters.</li> </ol>
Notes for KAS743	<ol style="list-style-type: none"> <li>You can use only 4-digits codes</li> <li>Up to 4 unit can be installed in the system.</li> <li>See the KAS743 manual for full details.</li> </ol>

## 4 Zones

The *Zones* menu includes the following sub-menus:

- 1) Zone Settings; see below.
- 2) Zone Type Settings; see section 6), on page 11.
- 3) Copy Zones; see section 4.3, on page 14.
- 4) Partitions Names; see section 4.3.2, on page 14.

### 4.1 Zone Settings

System Configuration ► Zones ► Zone Settings

Press \* or # to select a zone.

- 1) Type: select the zone type from the list; see the list below.
- 2) Name: user text, up to 28 characters.
- 3) Delay/24H: select from the following options.

Parameter	Description
Instant	Instant alarm zone
Entry Delay 1-2	Entry delayed zones
Delay Follower	Delay following zone
24-Hour	24-hour alarm zone

- 4) Attributes: select from the following list.

Parameter	Description
Disabled	The zone is permanently inactive
Normally Open	<ul style="list-style-type: none"> <li>• <b>Selected:</b> Normally Open</li> <li>• <b>Cleared:</b> Normally Close</li> </ul>
Allocated to Home 1-4	Allocate the zone to a <i>Home</i> mode
EOL Supervision <sup>5</sup>	Cut and/or short <sup>6</sup> zone supervision
Chime Zone	The keypad buzzer will sound when the zone is opened
Roller Blinds	The zone's sensitivity is adjusted to roller blinds

- 5) False Alarms: select from the list that follows (*Inactive* is also an option).

Parameter	Description
Double Knock	The zone will trigger the alarm, only if two pulses are detected during the <i>Double Knock</i> time (see section 8, on page 24).
Cross Zoning	The zone will trigger the alarm, only if another cross zone is opened too, during the <i>Cross Zoning</i> time (see 8, on page 24).

- 6) Partition Allocation: allocate the zone to partition/s; the selected number/s will stay on.
- 7) Wireless Zones

This menu refers to wireless zones parameters only. Each parameter is relevant to specific detector type or types. See the following table:

<sup>5</sup> **FORCE** only

<sup>6</sup> Depending on the defined number of resistors. See section 9, on page 42.



## 2-way detector parameters

Parameter	Options	PIR Standard DPS743	PIR PET DPP743	PIR+MW outdoor DPD743	Curtain detector DPC743	Outdoor curtain detector DCD	Dorr contact DCM743	Smoke & Heat detector DSH743	Flood detector DFL743
PIR sensitivity	High/Low	⊙	⊙	⊙	⊙	⊙			
MW Sensitivity/range	Minimum/0.25/0.5 0.65/0.85/Maximum			⊙		⊙			
Smoke & Heat mode	Smoke/Heat/both							⊙	
Enable Anti-Mask	Enable/Disable			⊙		⊙			
Enable LED operation	Enable/Disable	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙
EOL	Enable/Disable						⊙		
10 mSec sensitivity	Enable/Disable Disble – sensitivity is 200mSec						⊙		
Enable disposition detection	Enable/Disable			⊙					
Enable magnet detection	Enable/Disable						⊙		
Enable magnet bypassing	Enable/Disable						⊙		
Blind roller	Enable/Disable						⊙		
Blind roller pulses	0-15						⊙		

8) Soak Test Mode: select to put the zone in test mode for up to one week; see section 8, on page 24 for details.

## 4.2 Zone Types Settings

System Configuration ► Zones ► Zone Types Settings



Some settings are built-in and cannot be changed. If a different setting is required, use the Custom Zone types.

Zone Type <sup>7</sup>	Settings
Burglary, Panic, Silent Panic, Fire, Duress, Medical, Anti-Mask, Shock Sensor, Key Switch Modes, Custom Zone Types	<ol style="list-style-type: none"> <li>1) Sensitivity: the zone sensitivity in milliseconds. Range: 1-3000, default: 400. Closing the relay for one second re-sets the detector.</li> <li>2) Attributes: see next.</li> <li>3) Audible Notification: <ul style="list-style-type: none"> <li>▪ Alarm tone: when calling the contacts, hi-lo alarm will be</li> <li>▪ Message 1 – Recorded message #1 will be activated.</li> <li>▪ Message 2 – Recorded message #2 will be activated.</li> <li>▪ Notes: <ul style="list-style-type: none"> <li>○ Message 1 &amp; 2 use Voice Module VOX502 (purchased separately).</li> <li>○ Configure Output Type (see paragraph 5) of the VOX502 outputs accordingly – Message 1 or 2.</li> </ul> </li> </ul> </li> </ol>
Key Switch Modes	Key Switch in Away/Home 1-4: select the key type and set its sensitivity (see above).
Custom Zone Types	<ol style="list-style-type: none"> <li>1) Custom Zone Type 1-5: see the other zone types above, and in addition: <ul style="list-style-type: none"> <li>• Report &amp; Trigger: select a standard zone type (Burglary, Panic, etc.) to be used for reporting the CMS and triggering outputs or select a <i>Custom Type</i>. A <i>Custom Type</i> can be used to trigger outputs to activate/deactivate special devices such as pumps and heaters).</li> <li>• Name: user text, up to 16 characters.</li> </ul> </li> </ol>


### 4.2.1 Attributes

System Configuration ► Zones ► Zone Types Settings ► Zone Type ► Attributes

The zone type attributes are listed in the table below:

Attribute	Description
Trigger Sirens	The sirens will activate in alarm (via the <i>External</i> and <i>Internal Siren</i> programmed output types; see section 5.1, on page 15 for a warning).
Ext. Siren at Disarm	The external siren will activate in alarm (via the <i>External Siren</i> programmed output type) while at disarm.
Reports at Disarm	Reports to the CMS will be transmitted while at disarm

<sup>7</sup> Some are **FORCE** only

Attribute	Description
Auto-Bypass	The zone is automatically bypassed after triggering the alarm three consecutive times. It will be reinstated when the system/partition is disarmed, or the <i>Auto-bypass Limit</i> time elapses; see 8, on page 24.
Different Siren Tone	A different tone will be sounded when the zone triggers the alarm
Alarm Re-triggering	The zone will re-trigger the alarm as long as it is open.   <i>This attribute can only be used, if the Trigger Sirens attribute is also selected.</i>
Activate Buzzer	The keypad's buzzer will sound beeps throughout the alarm time
User Bypass	Users can temporarily bypass the zone

## 4.3 Copy Zones

[System Configuration](#) ► [Zones](#) ► [Copy Zones](#)

Select between copying a single zone's attributes, type, partitions, and name to other zones, and copying succeeding zones to a different location.

- 1) Single to Multiple
- 2) Multiple to Multiple

### 4.3.1 Single to Multiple

- 1) Copy Zone to Zones: select the zone to be copied and to which zone/s.
- 2) Copy Options:

Attribute	What will be copied
Zone Attributes	The parameters from the zone attribute screen
Zone Type	The zone type
Zone Partitions	The partitions that the zone is allocated to
Zone Name	The zone name

### 4.3.2 Multiple to Multiple

- 1) Define a group of consecutive zones to be copied.
- 2) Select a zone from which the zones will be copied to; for example, if you select to copy zones 21-34 (14 zones) and select zone 47, the 14 zones will be copied to zones 47-60.
- 3) Copy Options: see above.

## 4.4 Partitions Names

[System Configuration](#) ► [Zones](#) ► [Partitions Names](#)

Partitions can have unique names that will appear in the contacts reports and the event memory. Use # or \* to scroll and select the partition.

- Name: user text, up to 16 characters.

# 5 Outputs<sup>8</sup>

The *Outputs* menu includes the following sub-menus:

- 1) Onboard: see below.
- 2) Zone Expanders: see section 5.2.
- 3) Outputs Expander: see section 5.3.
- 4) Wireless Sirens: see section 5.4.

## 5.1 Onboard

*System Configuration* ► *Outputs* ► *Onboard*

The *Onboard* menu includes the following sub-menus (outputs):

- 1) External Siren
- 2) Internal Siren
- 3) Relay
- 4) On/Off
- 5) Alarm

### 5.1.1 Ext/Int siren outputs


The external and internal siren outputs have the following features:

- Supplying high current
- Can only trigger DC sirens
- Can be triggered separately



**Warning: the sirens outputs will be triggered only if you do not change the sirens' default programmed output types.**

Every output has the following parameters:

Parameter	Description												
Output Type	<p>The output type (event) that triggers the selected physical output. The triggering timer is set in the <i>Timers and Counters</i> menu; see Appendix C for the complete list of the output types.</p> <p>The next types are followers only.</p> <table border="1"> <thead> <tr> <th>Programmable output type</th> <th>Triggered when...</th> </tr> </thead> <tbody> <tr> <td>Zone open</td> <td>a zone is opened</td> </tr> <tr> <td>Arm Away</td> <td>the system (or all partitions) is armed Away</td> </tr> <tr> <td>Arm Home</td> <td>the system (or all partitions) is armed in Home 1-4</td> </tr> <tr> <td>Technician on-site</td> <td>Technician code is entered</td> </tr> <tr> <td>Walk test</td> <td><i>Walk test</i> started</td> </tr> </tbody> </table>	Programmable output type	Triggered when...	Zone open	a zone is opened	Arm Away	the system (or all partitions) is armed Away	Arm Home	the system (or all partitions) is armed in Home 1-4	Technician on-site	Technician code is entered	Walk test	<i>Walk test</i> started
Programmable output type	Triggered when...												
Zone open	a zone is opened												
Arm Away	the system (or all partitions) is armed Away												
Arm Home	the system (or all partitions) is armed in Home 1-4												
Technician on-site	Technician code is entered												
Walk test	<i>Walk test</i> started												
	<p> <b>Note</b> <i>The default programmable output types do not need to be changed in most installations.</i></p>												

<sup>8</sup> *FORCE* only, except *Wireless Sirens*.

Parameter	Description
Positive Polarity	<p><u>ON/OFF, Alarm (Open Collector)</u></p> <ul style="list-style-type: none"> <li>▪ <u>Checked</u>: the output is normally switched to ground, and disconnected when activated.</li> <li>▪ <u>Cleared</u>: the output is normally disconnected, and supplies ground when activated.</li> </ul> <p><u>Relay</u></p> <ul style="list-style-type: none"> <li>▪ <u>Checked</u>: the C and NC terminals are normally shorted. When activated, the C and NO terminals are shorted.</li> <li>▪ <u>Cleared</u>: the C and NO terminals are normally shorted; C and NC terminals are shorted when activated.</li> </ul>
Partitions	The physical output's partition allocation. Press # or * to scroll between partitions. The selected partitions stay on.
Name	User text, up to 16 characters.

## 5.2 Zone Expanders

*System Configuration ► Outputs ► Zone Expanders*

The outputs' parameters of the ZEX508/516 zone expanders are the same as those of the onboard outputs, above. The expanders' relay outputs are:

- The ZEX508, 8-zone expander has one relay. The expander's ID number and the relay number are the same.
- The ZEX516, 16-zone expander has two relays - 1 & 2. The expander takes 2 consecutive ID numbers, and so are its relays. For example, if the expander no. is 4, set relays #4 and #5.

Press # or \* to scroll between expanders.

## 5.3 Outputs Expander

*System Configuration ► Outputs ► Output Expander*

The OEX508 outputs expander's parameters are the same as those of the onboard outputs, above. Press # or \* to scroll between expanders.

Relay 1-8: press the desired relay and set its parameters.

## 5.4 Wireless Sirens

*System Configuration ► Outputs ► Wireless Sirens*

Press # or \* to scroll between sirens, and set its programmable output type, partitions, and name.



## 6 CMS & Communications

The *CMS & Communications* menu includes the following sub-menus:

- 1) Monitoring Stations: see below.
- 2) PIMA Cloud; see section 6.2, on page 20.
- 3) General Settings; see section 6.1.3, on page 20.
- 4) Telephone Settings; see section 6.4, on page 21.
- 5) Network Settings; see section 6.5, on page 21.
- 6) Cellular Settings; see section 6.6, on page 22.

### 6.1 Monitoring Stations

*System Configuration* ► *CMS & Communications* ► *Monitoring Stations*

The *Monitoring Stations* menu includes the following sub-menus:

- 1) CMS 1-3; see below.
- 2) Radio; see section 6.1.2, on page 19.
- 3) Custom Zones Reports; see section 6.1.3, on page 20.

#### 6.1.1 CMS 1-3

*System Configuration* ► *CMS & Communications* ► *Monitoring Stations* ► *CMS 1-3*

You can configure up to 3<sup>9</sup> different CMS (monitoring station) independently. Each one can be configured to communication paths, account IDs, telephone numbers and more. Force will report the events to all the CMS's. Backup paths are defined within each CMS.

The *CMS 1-3* menu includes the following sub-menus:

- 1) Comm. Paths; see below.
- 2) Event Reporting: see page 18.
- 3) CMS Name: user text, up to 16 characters.
- 4) CMS Lock Code: set a lock code to the definitions of this CMS.

#### Communication Paths

*System Configuration* ► *CMS & Communications* ► *Monitoring Stations* ► *CMS 1-2* ► *Comm. Paths*

The *Communication Paths* menu includes the following sub-menus:

- 1) Telephone (PSTN).

Parameter	Description	Default	Range
Account ID	The partitions' ID number. If you only set partition 1's ID, it will serve for all other partitions.	-	1-999999
Telephones	Set up to four telephone numbers of the CMS (up to 16 digits per number).	-	1-4
Protocol	Select the PSTN protocol between ContactID, SIA <sup>10</sup> , and NPAF.	ContactID	-

<sup>9</sup> 3 CMS is supported from Force firmware version 1.4.13 and up

<sup>10</sup> Consult with PIMA support.

Parameter	Description	Default	Range
System ID	A parameter required by the NPAF protocol only. Consult the CMS.	0	-
ACKs	Handshake Wait: how long the control panel will wait for a Handshake message, before disconnecting the call and redialing.	20 sec.	20-250 sec.
	Kissoff Wait: how long the control panel will wait for a Kissoff message, before resending it. Change the default only if necessary, for example if there are communication delays.	0 mS.	1-5000 mS.
	ACK Frequency: select between Lo-Hi, 1400, 2300, and SIA.	Lo-Hi	-
Periodic Test	A daily test report to the CMS; press # to reset and disable reporting.	-	-
Test Interval	An interval (in hours) for a test report to the CMS. If longer than 24 hours, the interval will start over every time it overlaps the Periodic test.	-	-
Number of Dials	The number of dials and redials that if fail (no ACK is received), a communication fault is reported.	-	-
Primary Path	Select if the telephone is the primary path for reporting the CMS.	-	-

- 2) Cellular-Voice: see the Telephone (PSTN) menu above.
- 3) Network (Ethernet): in addition to the above Telephone (PSTN) parameters, the network has the following parameters:

Parameter	Description	Default	Range
Network Addresses	<u>IP/URL 1-2</u> : the CMS's IP/URL address. Address #2 only serves as a backup. <u>Port 1-2</u> : enter the port no.		
Supervision	Supervision (test) report interval. The report is designated to the IP receiver at the CMS.	5 min	0 (disabled) - 59:59 mm:ss
Retries	Set the number of retries if no ACK is received.	10	2-250
Disable Encryption	Data will be not encrypted. Verify that CMS IP receiver is adjusted for non-encrypted reports.  <b>Caution</b> Non-encrypted reporting causes the system and the CMS to be more vulnerable to cyber attacks!		
16 digits Acc. ID	The account ID field in the report frame will always be 16 digits, with leading '0'. Use this feature only by special request from the CMS.		

- 4) Cellular Data: see Network (Ethernet) above.

## Event Reporting

*System Configuration ► CMS & Communications ► Monitoring Stations ► CMS 1-3 ► Event Reporting*

Select the events to report to the CMS. The optional events are:

- Alarms: Burglary, Panic, Fire, Duress, Medical, Tamper, Custom Zone 1-5.

- Faults
- Invalid Code, Arming/Disarming, Technician On-site, Remote test, Periodic test, Zone Bypass, Zone Restore, Pre-alarm (Entry Delay), Power-up, Zone/Output Toggle.
- Zone/output Toggle – each change in zoned and output will be reported. This may cause load on the communication traffic. Use this feature only upon special request such as connection to special CMS software that requires it.

## 6.1.2 Radio<sup>11</sup>

[System Configuration](#) ► [CMS & Communications](#) ► [Monitoring Stations](#) ► [Radio](#)

See section 6.1.1 above for details on the parameters, except those on the next table:

Parameter	Description	Default	Range
Format	The radio format; obtain it from the CMS.	-	
Reporting Codes	See below.	-	
Transmissions No.	The number of transmissions and re-transmissions per report	5	1-16
Frames Per Transmission	The number of frames per single transmission	10	1-16

### Reporting Codes

[System Configuration](#) ► [CMS & Communications](#) ► [Monitoring Stations](#) ► [Radio](#) ► [Reporting Codes](#)

The radio reporting and restore codes for alarms and other events. Note the following:

1. The codes apply only for some radio protocols. Consult the CMS before setting them.
2. A zone is reinstated in the following conditions:
  - a. The alarm system/partition is disarmed (or the first partition, if the zone is allocated to more than one).
  - b. A user un-bypasses a zone
  - c. *Bypass Limit* time elapses
3. Following are several points regarding the *zone restore* reporting:
  - A *zone restore* report is generated, when an alarmed zone is closed and rearms itself. When siren time elapses, the zone status is checked and if it has already been closed, the report is generated.
  - If the zone is not set to trigger the sirens, the report is sent as soon as the zone is closed.
  - If a zone had triggered the alarm and was meanwhile closed, the report will be generated as the alarm system is disarmed.
  - In partitioned system, a *zone restore* report is generated, only when the partition it's allocated to, is disarmed.

The *Reporting Codes* menu includes the following sub-menus:

Parameter	Description
Zones	For each zone, set codes for the following events: <i>Alarm+Restore</i> , <i>Fault+Restore</i> , <i>Bypass+Restore</i> . Press # or * to scroll between zones.
Arm/Disarm-User	For each user, set event codes for <i>Arming</i> and <i>Disarming</i> . Press # or * to scroll between users.

<sup>11</sup> **FORCE** only

Parameter	Description
Arm/Disarm-Other	Set codes for <i>Arming</i> and <i>Disarming</i> events, in any way other than by users.
Faults	Set event and restore codes for the following events: 1) Power: <i>AC Fault, Low Battery, Power Loss, Detector's Voltage Failure, Fuse, Peripheral's Power Fault.</i> 2) Communication: <i>Communication Fault, Telephone Line Fault, Cellular Fault, Network Fault.</i> 3) Sirens: <i>External Siren Fault, Internal Siren Fault.</i>
Alarms and Others	Set event and restore codes for the following events: 1) <i>Panic and Fire alarms, Technician On-site, Invalid Code, Test.</i> 2) <i>Tampers: Tamper 1-2 and Peripherals' Alarm and Restore codes.</i>

### 6.1.3 Custom Zones Reports

System Configuration ► CMS & Communications ► Monitoring Stations ► Custom Zones Reports

Set the codes (ContactID, SIA alarm and restore) for the custom zones. Custom zones are based on modified zone types, but allow reporting with unique ContactID and SIA codes.

Below is a list of more frequently used events, which can be used with the custom zones.

Event	ContactID	SIA	Event	ContactID	SIA
Gas detected	151	GT	Low temp	159	ZA
Refrigeration	152	ZA	High Humidity	168	-
Loss of heat	153	ZA	Low Humidity	169	-
Water Leakage	154	WA	Low water pressure	201	WT
Low bottled gas level	157	GA	Low water level	204	WT
High temp	158	KA			

## 6.2 PIMA Cloud

System Configuration ► CMS & Communications ► PIMA Cloud

Parameter	Description
Network (Ethernet)	1. Select the communication path to the cloud.
Cellular Data	2. The cloud's URL (force.pimalink.com) and IP address (13000) 3. Set the Port to zero for the other path.
Main Path	Select if the cloud will be the main communication path. When cleared, this path will back up the main path.



- **Do not change the default URL or IP. Consult PIMA when required.**
- **Do not select more than one main path!**

## 6.3 General Settings

System Configuration ► CMS & Communications ► General Settings

Parameter	Description
Remote Up/Download	<ul style="list-style-type: none"> <li>• <b>Checked:</b> remote upload/download without the need for user permission is enabled. Note that this is valid only after downloading one time at least.</li> <li>• <b>Cleared:</b> remote upload/download is enabled only with user permission (see the User guide [P/N 4410460] for how to details)</li> </ul>
Remote Disarm	Enable remote system disarm via the <b>PIMAlink 3.0</b> app.

## 6.4 Telephone Settings<sup>12</sup>

System Configuration ► CMS & Communications ► Telephone Settings

Parameter	Description
Connected to Line	The control panel is connected to a PSTN line
External Line Access	Access number (up to 7 digits) for private PBX
Prefix	Set digit/s to be dialed before any of the PSTN telephone numbers.
Check Dial Tone	<ul style="list-style-type: none"> <li>• <b>Selected:</b> dial tone is checked before dialing</li> <li>• <b>Cleared:</b> dial tone is not checked before dialing</li> </ul>
VoIP	The telephone line uses Voice over IP technology
Telephone Line Test-Armed	When the alarm system (or all the partitions) is armed Away, dial tone will be checked every one minute.
Telephone Line Test-Disarmed	When the alarm system is disarmed, dial tone will be checked every one minute.

## 6.5 Network Settings

System Configuration ► CMS & Communications ► Network Settings

Parameter	Description
Connected to Network	The control panel is connected to Ethernet network.
DHCP	<ul style="list-style-type: none"> <li>• <b>Selected:</b> IP address is automatically assigned by the router (exit the Technician menu to implement).</li> <li>• <b>Cleared:</b> use static IP (next)</li> </ul>
Static IP	Enter the control panel's IP address. Make sure DHCP (previous) is cleared (exit the Technician menu to apply).
Netmask, DNS, Default Gateway	Set when using <i>Static IP</i> .
Callback Address, Port	Set an IP address and port number for the FORCE Manager upload/download software. These parameters are in the user menu, under <i>Remote Service/Over Network</i> .

<sup>12</sup> **FORCE Lite:** unavailable

## 6.6 Cellular Settings

System Configuration ► CMS & Communications ► Cellular Data Settings

Parameter	Description
Cellular Modem	Select <i>Installed</i> , if a modem is installed.
Virtual Provider	The SIM card's provider is virtual
Callback Address, Port	See <i>Network Settings</i> above.
Double SIM	The cellular transmitter includes 2 SIMs. SIM #1 is the main SIM i.e. the system will use it as long as it is not faulted. SIM #2 is the backup, activated when a fault is detected in the link of SIM #1. See next paragraph for options. See also Timers 8, page 24).
SIM 1 not exist	An option to use SIM2 as single SIM. Use when there is a mechanical problem in the SIM tray.
Use SIM 2	Temporary parameter for tests. After the tests system will return to use SIM 1.
Firmware upgrade	Please consult PIMA support for using this option.
APN-1/2 Settings	<ol style="list-style-type: none"><li>1) Name. The options are:<ol style="list-style-type: none"><li>a. Enter the APN's name (up to 16 characters).</li><li>b. Enter '1' if the service provider sets the name<sup>13</sup>.</li><li>c. Leave blank if APN is not in use.</li></ol></li><li>2) User, Password: obtain from the service provider.</li></ol>

<sup>13</sup> **FORCE** version 1.2 and higher.

## 7 Faults

The *Faults* menu includes the following sub-menus: *AC Fault*, *Low Battery*, *Phone Line Fault*, *Network Fault*, *Cellular Modem Fault*, *CMS Comm. Fault*, *Tamper Open*, *Invalid Code*, and *Other Faults*; see below.

### 7.1 AC Fault

System Configuration ► Faults ► AC Fault

Parameter	Description
Attributes	See section 4.2.1, on page 13, and in addition: <u>Burglary Output Activation</u> : activate any physical output that is triggered by the Burglary Alarm programmable output type.
Report Delay	Range: 0-250 minutes. If the fault is fixed before the delay elapses, it will not be reported, but only recorded. The delay also applies to activating outputs and the keypad buzzer.
Report Time Span	A time span (in minutes) during which the AC fault will be reported at a random time. This feature is useful when many control panels try to report the CMS at the same time, for example, when a wide-scale power outage occurs.
Audible Notification	Select <i>Alarm Tone</i> when notifying the contacts by phone.

### 7.2 Low Battery, Phone Line, Network, Cellular Module

- 1) Attributes: see section 4.2.1, on page 13.
- 2) Report Delay: see *AC Fault* above.
- 3) Audible Notification: see *AC Fault* above.

### 7.3 Invalid Code

This alarm is generated when a user exceeds the *Code Keystrokes* counter; see *Timers and Counters* on the next page. To reset the counter before an alarm is triggered, wait 30 seconds.

In partitioned systems, the *Invalid Code* programmed output type is activated only if the code is entered in a keypad that shares at least one partition with the output. The report will be under the lowest partition number.

### 7.4 CMS Comm., Tamper Open, Invalid Code, Other Faults

- 1) Attributes: see section 4.2.1, on page 13.
- 2) Audible Notification: see *AC Fault* above.

## 8 Timers and Counters

The *Timers and Counters* menu includes the following parameters.

Parameter	Description	Default	Range	
Programmable Output Types	See next section.			
Entry Delay 1-2	A period that allows entering the premises through delayed and follower zones, and disarming (system/partition) without triggering an alarm.	30/60 sec.	0-250	
Exit Delay	A period that allows exiting the premises through delayed and follower zones, after arming (system/partition) without triggering an alarm.	30 sec.		
Double Knock	A period during which only if a detector activates twice, it triggers an alarm.			
Cross Zoning	A period during which only if two cross-zones activate, an alarm is triggered.			
Soak Test	A number of days during which the zone is in test mode: if it activates it will not trigger an alarm (but the event will be recorded). The zone is automatically reinstated.	3 days	1-7	
Bypass Limit	A time limit before arming the alarm system (or a partition) during which a zone can be bypassed by a user. The zone is un-bypassed when the timer elapses or the alarm system/partition is disarmed, whichever comes first.	0 hr.	0-250	
Auto-Bypass Limit	A period during which a zone that was automatically bypassed after triggering the alarm three times during one arming session is reinstated.			
Inactivity	A period (days) during which if the alarm system has not been armed, ContactID event no. 654 is reported.	7 days	0-99	
Code Keystrokes	The number of allowed keystrokes, when entering codes. Any more keystrokes will trigger an alarm and lock the keypad; see next. To reset the counter, wait 30 seconds.	24	10-250	
Keypad Lockout	A period during which the keypad is locked, due to illegal number of keystrokes (see above).	180 sec.	0-250	
Siren beep	The arming/disarming indication beep length	300 mSec	0-1000	
Report Delay				
<ul style="list-style-type: none"> <li>▪ AC Fault</li> <li>▪ Telephone fault</li> <li>▪ Cellular Modem Fault</li> <li>▪ Network Fault</li> </ul>	The time between the occurrence of the fault and reporting the event. If the fault is fixed before the delay expires, no event is reported.		120 min	0-250



Parameter	Description	Default	Range
▪ Phone Line Fault			0 min
Back to SIM 1	When SIM 1 is at fault, the control panel switches to SIM 2. Set here after how long the control panel will switch back to SIM 1.		24 hr. 6-72
SIM 2 Test	The interval for the control panel to switch to SIM 2 for testing it (for several minutes), before switching back to SIM 1.		7 days 0-60

## 8.1 Programmable Output Types

System Configuration ► Timers and Counters ► Programmable Output Types

See *Programmable Output Types*, on page 35, for details on all the programmable output types.



*The default alarms and sirens programmable-output-types match the default zone types, and should not be changed in most installations.*

Each Programmable-output-type's timer has three options, described below.

Time (sec)	Description	Use example
0	The output type will activate the physical output until the alarm system is disarmed.	Burglary alarm: turn on a floodlight
1-9998	The output type will activate for the set time.	Fire Alarm: open an escape door
9999	The output type will activate for as long as the source event exist.	AC Fault: flashlight blinking



Programmable output type	Default
<b>Alarms</b>	
Burglary, Panic, Silent Panic, Fire, Medical, Duress, Anti-mask.	240 sec.
Custom Zone Types 1-5 <sup>14</sup>	
<b>Faults</b>	
Any Fault, AC Fault, Low Battery, Phone line/Net, Cellular Modem, Comm. Fault.	9999
Tamper	240 sec.

Programmable output type	Default
External/Internal Siren	240 sec.
Zone Bypass	9999
Smoke Detector Reset	60 sec.
Chime Activation	3 sec.
Output-Key fob	5 sec.
Energy Saving (a timer that is added to the 'Zone Open' output type)	15 min
Invalid Code	24 keystrokes
Operation Codes 1-8	5 sec.

<sup>14</sup> See *Custom Zones Reports*, on page 72.

## 9 General Settings

Following are the parameters of the *General Settings* menu:

Parameter	Description
System Name	User text, up to 16 characters.
Service Provider	User text, up to 24 characters. To display the text, press and hold the zero key.
Contract Expiration	Date to display appropriate message onscreen
Technician Code	Change code, 4-6 digits.
One Key Arming	Use the Arm Away, Home1 (   ) , and number keys to arm, without a password.
Alarms at Arm	Alarm messages will be displayed when the control panel is armed.
Final Door Arming	Closing any delayed zone during the exit delay terminates the delay.
Home Modes-Instant	No exit delay when arming in Home 1-4 modes
Additional CMSs	<ul style="list-style-type: none"> <li>• <u>Selected</u>: setting CMS 2 parameters + code is enabled</li> <li>• <u>Cleared</u>: setting CMS 2 parameters + code is enabled only by using the Master technician code.</li> </ul>
Zone Bypass-Auto Arm	Open zones are automatically bypassed when auto-arming
Momentary Key	<ul style="list-style-type: none"> <li>• <u>Selected</u>: momentary key switch</li> <li>• <u>Cleared</u>: toggle key switch</li> </ul>
Keyfob-Force Arming	Allows arming with a keyfob with open zones and faults
Beep on Arming	<ul style="list-style-type: none"> <li>• No beep</li> <li>• Always: the siren will sound a beep, whenever the alarm system is armed.</li> <li>• With Key switch/Key fob: the siren will sound a beep, when the alarm system is armed with a key switch or key fob.</li> </ul>
Beep on Disarming	<ul style="list-style-type: none"> <li>• No beep</li> <li>• Always: the siren will sound 2 beeps, whenever the alarm system is disarmed.</li> <li>• With Key switch/Key fob: the siren will sound two beeps, when the alarm system is armed with a key switch or key fob.</li> <li>• Always+Alarm in Memory: the siren will sound three beeps, whenever the alarm system is disarmed, if the alarm was triggered when the system was armed.</li> <li>• With Key Switch/Key fob+Alarm in Memory: the siren will sound three beeps, whenever the alarm system is disarmed with a key fob or key switch, if the alarm was triggered when the system was armed.</li> </ul>
Arming Prevention	See below.

## 9.1 Arming Prevention

[System Configuration](#) ► [General Settings](#) ► [Arming Prevention](#)

For some faults, you can allow the users to arm the alarm system only after they override them<sup>15</sup>. The faults are *AC Fault*, *Low Battery*, *Expander/Tamper*, *Telephone Line*, *Cellular modem*, and *Network*.

Select any fault to allow the user to override it.

<sup>15</sup> In the user's *System Options/Faults Override* menu (user permission required).

# 10 Reset to Defaults

The *Reset to Defaults* menu includes the following sub-menus:

- 1) Select Parameters: select what parameters to reset from the following list:
  - Communication (including the CMSs)
  - Zones (and partitions)
  - Outputs (onboard and expanders)
  - User (all except the Master)
  - Full System Reset - includes all the above.
- 2) Reset to Defaults: press to reset the selected parameters.



***Warning: this action cannot be undone!***

## 10.1 Resetting to factory defaults

If the Master technician code is unavailable, **FORCE** can nevertheless be reset to factory defaults.

To reset to the factory defaults, do the following:

1. Disconnect **FORCE** from AC and battery power for five seconds.
2. Reconnect AC power.
3. Within 30 seconds from when the main screen is displayed, press 000000 (six zeros). The system reset screen is displayed.
4. Press on *Press and Wait*.
5. When the reset process is over, set new Master codes; see section 2.2, on page 4 for details.
6. Reconnect the battery.

# 11 Tests & Diagnostics

In the main screen, press *Tests & Diagnostics*. This menu includes the sub-menus that follows.

- 1) Event Memory; see below.
- 2) Zone Test; see below.
- 3) Output Test; see below.
- 4) Power Diagnostics; see next page.
- 5) Communication Tests; see next page.
- 6) Communication Monitor; see next page.
- 7) Wireless Peripherals; see next page.

## 11.1 Event Memory

### *Tests & Diagnostics* ► *Event Memory*

The *Event Memory* stores up to 1,000 events. Each event is made of a time stamp, the event description, and the event source. Scroll through the events using the up/down arrow keys.

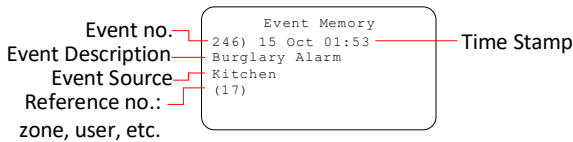


Figure 1. Event memory log

## 11.2 Zone Test

### *Tests & Diagnostics* ► *Zone Test*

The *Zone Test* menu includes the following sub-menus:

- 1) Single Zone: enter the desired zone number, trigger the detector and check the *Successfully Tested* field.
- 2) All Zones: walk through the entire premises, trigger the detectors and check the display:
  - Tested: the number of tested zone, out of the overall defined zones.
  - Last Tested (zone)
  - Failed/Not Tested: a list of the zones that failed the test, or were not tested.
- 3) Audible Indication: select from the following list:

Parameter	Description
⊙ Keypad Buzzer	The keypad's buzzer will emit beeps on every detection
⊙ Beep-External Siren	The <i>External Siren</i> will emit a beep on every detection
⊙ Beep-Internal Siren	The <i>Internal Siren</i> will emit a beep on every detection

## 11.3 Output Test

### Tests & Diagnostics ► Output Test

The *Output Test* menu includes the following sub-menus, for testing the physical outputs. If an output is not functioning properly, it helps defining whether it is a hardware or configuration based problem. In addition, the test triggers the buzzer on the tested expander, for locating it easily.

- 1) Onboard: select any of the control panel's outputs and *Activate/Deactivate* it. The available outputs are *External/Internal Siren, Relay, On/Off, Alarm*.
- 2) Zone Expanders: select an expander (press # or \*) and *Activate/Deactivate* the expander's relay output/s. To easily locate the expander, press *Activate Buzzer* and *Activate/Deactivate* the expander's buzzer.
- 3) Output Expanders: select an expander (press # or \*) and an output, and *Activate/Deactivate* it. To easily locate the expander, press *Activate Buzzer* and *Activate/Deactivate* the expander's buzzer.
- 4) Keypad Buzzer: *Activate/Deactivate* the buzzer.

## 11.4 Power Diagnostics

### Tests & Diagnostics ► Power Diagnostics

The *Power Diagnostics* menu includes the following sub-menus, for viewing the control panel and peripherals' voltage and the current status.

- 1) Zone Expanders: select *Local* or *Remote Expanders* and view the card's voltage and current.
- 2) Keypads: select a keypad (press # or \*) and see its current voltage and current.
- 3) Output Expanders: select an expander (press # or \*) and see its voltage and current.
- 4) Battery Voltage: the backup battery's voltage status.
- 5) Panel Current: the control panel and the peripherals' current consumption. Note that *PS* on the display indicates that the peripheral is powered by a local power supply and so its current is not pulled from the control panel.

## 11.5 Communication Tests

### Tests & Diagnostics ► Communication Tests

- 1) CMS: test the CMS's telephones, IP/URL's etc., by generating a Test report. During the test the communication transactions are displayed onscreen.
- 2) PIMA cloud: test the cloud's IP/URL.
- 3) Cellular signal: the signal strength in percent.
- 4) Internet test: Test the internet connection.

## 11.6 Communication Monitor

### Tests & Diagnostics ► Communications Monitor

Select a path and view the **FORCE**'s online communication transactions. The transactions are displayed for several minutes and you can trigger events and follow the keyboard screen.

## 11.7 Wireless Peripherals

### Tests & Diagnostics ► Wireless Peripherals

Select any wireless peripheral to display its serial number, battery level and signal strength.

When testing wireless zone in *Single Zone* option, the \* sign may be displayed. This sign, attached to the signal strength, indicates that the detector is 2-way. For example:

\* Good

If the sign \* is not displayed for 2-way peripheral, there is incompatibility issue with this peripheral, and it should be replaced.

Note: The 'N/A' indication in the signal strength field means that the peripheral has not been received by the receiver yet. Check the reason for this, e.g., the peripheral location.

# 12 Service and Remote Upgrading

User Menu ► Communication Tests ► Remote Service

This menu enables various maintenance operation remotely. This menu can also be accessed by holding down key '6'.

Parameter	Description
Enable access now	Pressing this option enables the technician to connect to the system remotely and executing operations like configuration
Network	<p>The connection will be via the Ethernet port of the alarm system. Enter the remote server IP address and port. See also paragraph 5) for pre-defined address.</p> <p>Connect: make connection now. The server may be Force Manager software.</p>
Cellular	<p>The connection will be via the cellular channel of the alarm system. This requires cellular modem installed (for example - CLM412). Enter the remote server IP address and port. See also paragraph 5) for pre-defined address.</p> <p>Connect: make connection now. The server may be Force Manager software</p>
Upgrade/Update	<p>Enable remote firmware upgrading or changing some parameters from internet server, as follows:</p> <ol style="list-style-type: none"><li>1. Firmware: choose last version for firmware upgrading.</li><li>2. Language: Use this to change the menu language of the alarm system. Note: the zone and user names must be updated manually.</li><li>3. Logo No.: download specific logo to be displayed on the LCD keypad. Consult PIMA support for this option.</li><li>4. Over network: the upgrading will be executed via the Ethernet port of the alarm system.</li><li>5. Over cellular: the upgrading will be executed via the cellular link of the alarm system. This requires cellular modem installed (for example - CLM412).</li></ol> <p>Note: if the existing firmware version does not include the Upgrade option (old versions), you can upgrade using the following: Select Network or Cellular as described above for Remote Service, and enter the following address: 1ADGJ:10020 Press 'Connect'.</p>





## Appendix A. Implementing Partitions

You can define up to 16 true partitions. Each partition is consisted of several zones, and is normally a defined area, such as a building floor, a store, or a compartment. Every partition can have its own subscriber ID no., user codes, keypads, peripherals, etc.

Partitions' event reporting is subject to the following:

Event	The reported ID no.
Zone alarm	All the partitions IDs to which the zone is allocated
Arming/Disarming	<ul style="list-style-type: none"><li>• If the zone is allocated to more than one partition, a separate report will be sent on each partition.</li><li>• If only partition #1 ID is defined, any event will carry that number.</li></ul>
Keypad alarm	All the partitions IDs to which the keypad is allocated
Non-zone Fault	Partition #1

Zone, keypads, users, and contacts can be allocated to more than one partition. In such a case, the following will apply:

1. Arming a zone is subject to all the partitions that the zone is allocated to: it will only be armed when all its partitions are armed.
2. An armed zone becomes disarmed, as soon as one of the partitions it is allocated to is disarmed.
3. Arming and disarming via a keypad is subject to both the keypad and the user's partitioning. For example, if a user that is allocated to partitions 1, 3 & 5, enters its code in a keypad that is allocated to partitions 4, 5 & 7, only partition 5 will either be armed or disarmed.
4. A keypad can only display and control the partition/s to which it is allocated. The *Armed* LED stays on only when ALL the keypad's partitions are armed, and flashes when only some partitions are armed.

# Appendix B. Remote Up/Download

## 1. User authorization

The parameter *Remote Up/Download* under *CMS & Communication/General Settings* sets if connecting remotely to **FORCE** for upload/download is enabled and if it requires a user approval. See the user guide on how the user approves the connection<sup>16</sup>.

Uploading and downloading is done using the Force Manager PC software (see a separate guide). Connection between the PC and **FORCE** is made possible only with the Up/download code or the technician code.



**Using the CMS lock code to connect to FORCE requires user permit.**


## 2. Upload/download code

The 6-digit upload/download code allows connecting and programming the **FORCE** system (except CMS locked menus) remotely. You should set the code the first time you connect the Force Manager software to **FORCE** (it cannot be done locally).

## 3. Connection options

Below are the options on the User menu *System Options/Communication/Remote Service*<sup>17</sup>:

Option	Description
Allow Access Now	<p>The user must always use this option when you need to remotely connect to the alarm system, in the conditions that follow:</p> <ul style="list-style-type: none"><li>• When you use the Master Technician code, and not the <i>Up/Download code</i> to connect with the Force Manager software to <b>FORCE</b>.</li><li>• When you use the upload code but the <i>Remote Up/Download</i> parameter (under <i>CMS &amp; Communication/General Settings</i>) is not enabled.</li><li>• When you use a code that is other than the Master technician or up/download codes.</li><li>• When you use the default Technician code (1234)</li></ul> <p>Change the default <i>Up/Download code</i> on the first connection to <b>FORCE</b>. If you do not have the Technician code, you can define a new CMS (if available) and set its parameters. Upon the first connection of <b>FORCE Manager</b> to force the up/download code set in the <b>FORCE Manager</b> becomes the <b>FORCE</b>'s code for future connections.</p>
Over Network/ Cellular Data	<p>To connect over network or cellular set the IP address in the <i>Communication/Monitoring Stations/Network, Cellular Settings</i> menus, in <i>Callback No./Callback Address</i> parameters.</p> <p>The user can manually enter the address in the User menu.</p>

<sup>16</sup> Up to 5 minutes from approving the connection, the control panel picks up a call immediately, regardless of parameter, such as number of rings. The user can press the  button for 2 seconds to cancel the approval.

<sup>17</sup> The user can press and hold key '6' to enter this menu (ver. 1.2 and higher)

# Appendix C. Programmable Output Types

Output Type	Activation	Deactivation <sup>18</sup>	Timer			Partitioning	Default
			1-9998 (sec)	9999 (Follower)	0 (Latch) <sup>19</sup>		
<b>Alarms:</b> Burglary, Panic, Silent panic, Fire, Medical, Duress, Anti-mask, Custom zone type 1-5	Alarm triggering	Activation time elapses, or disarming.	✓	⊘	✓	✓	240 sec
<b>Faults:</b> Any fault, AC, Low battery, Phone line/Network, Cellular modem, Communication, Tamper	Fault occurrence		✓	✓	✓	⊘	9999
External siren	Siren triggered		✓	⊘	✓	✓	240 sec
Internal siren			✓	⊘	✓	✓	
Zone bypass <sup>20</sup>	Bypassing a zone		✓	✓	✓	✓	9999
Smoke Reset	Fire zone, or keypad alarm.	Activation time elapses, or key is pressed and held.	✓	⊘	⊘	✓	60 sec
Chime Activation	Chime triggered	Activation time elapses	✓	⊘	⊘	✓	3 sec
Output-Key fob: output activation by a keyfob	<ul style="list-style-type: none"> <li>PIMA key fob: press the</li> <li>Visonic key fob: press the asterisk (*) key</li> </ul>	Activation time elapses, or key pressed again.	✓	⊘	⊘	✓	5 sec
Energy saving	All zones are closed	Activation time elapses	✓	⊘	⊘	✓	15 min
Code keystrokes	<i>Code Keystrokes</i> counter exceeds limit	Activation time elapses	✓	⊘	✓	✓ <sup>21</sup>	24 key-strokes
Operation code 1-8	Entering a code	Activation time elapses	✓	⊘	✓ <sup>22</sup>	✓	5 sec
CMS ACK	Receiving Ack from PSTN/cellular CMS for the reporting	Activation time elapses	⊘	⊘	⊘	⊘	5 sec

<sup>18</sup> For non-follower timers

<sup>19</sup> Latched, until system/partition disarming.

<sup>20</sup> See more below the table.

<sup>21</sup> Subject to the keypad's partitioning

<sup>22</sup> Toggle mode

# Appendix D. Technician and CMS Codes

There are two technician codes in the **FORCE** security system: Master and CMS lock code, which allows limiting the access to the CMS menus by a password.

## 1. Master technician code

By default, and as long as no CMS lock code (see next) has been set, the Master technician code enables to access all the technician menus, including all the CMSs’.

To enter the technician menu for the first time, follow the next steps:

1. On versions 1.3 and higher, enter the default Master code (5555), set new 4-6 digit Master User and Technician codes, and press **↵**.
2. On previous versions, do the following steps:
  - a) Enter the default Master code (5555) and set a new code.
  - b) Enter the new code to enter the User menu, scroll to *Other Options*, and press **↵**.
  - c) Scroll to *Technician Permit*, and press **↵**.
  - d) Immediately enter the default Master technician code *1234*.
  - e) Enter a new 4-6 digit Master technician code, and press **↵**.

## 2. CMS lock code

The CMS lock code ensures the CMS definitions from unauthorized access. Setting such a code prevents the Master technician code from accessing the locked CMS menus.



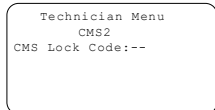
Note

*The CMS lock code is to be used, only when a technician needs to set the CMS definitions and doesn't have the Master technician code in hand.*

*If access to the CMS menus has been limited by the Master Technician, the technician code must be obtained and the Other CMS parameter under General Settings should be disabled.*

If you need to set the CMS definitions and you don't have the Master technician code, follow the next steps:

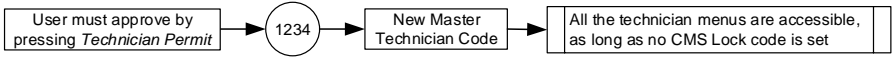
1. The user must grant you access via the *Technician Permit* menu (*User menu/Other Options*).
2. Immediately enter the default Master technician code, *1234*- the next undefined CMS lock code screen is displayed<sup>23</sup>.
3. Enter a new 4-6 digit lock code.
4. Press the **↻** button.



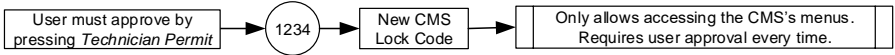
From now on, these CMS definitions are only accessed using the new lock code. Whenever there will be a need to change or view these CMS's definitions, the user will have to approve it, after pressing the *Technician Permit* menu. A technician that has the Master technician code, will not be able to view or change these definitions.

<sup>23</sup> Providing there is an available CMS menu

Changing default Master Technician code



Setting CMS Lock code



## Appendix E. Text and Characters

Text is entered like in a telephone set: each key is allocated with several characters; each keystroke presents a different character. For example, press 8 twice to type U.

The keystrokes and character table are described in the table and image that follow:

Key	Set 1	Set 2	Set 3
1	1.,?!()/*:~+#@'	1.,?!()/*:~+#@'	1.: :
2	ABC2	abc2	2
3	DEF3	def3	3
4	GHI4	ghi4	4
5	JKL5	jkl5	5
6	MNO6	mno6	6
7	PQRS7	pqrs7	7
8	TUV8	tuv8	8
9	WXYZ9	wxyz9	9
0	Space, 0		
#	Delete, return to default		
*	Uppercase/lowercase/digits		

1.,'()/*:~+#'	ABC2	DEF3
1	2	3
GHI4	JKL5	MNO6
4	5	6
PQRS7	TUV8	WXYZ9
7	8	9
Letter Case	Space, 0	
*	0	#

# Appendix F. Zone and System Status

## 1. Zone status

Letter	Indication
A	Zone alarm
B	Zone bypass
C	Chime zone
F	Fault (tamper/disconnection/short)
L	Low battery (wireless peripheral)
M	Anti-mask alarm (wireless peripheral)
O	Armed partition
T	Zone test
V	Supervision loss (wireless peripheral)

## 2. System status (main screen)

Letter	Indication
G	Cellular data communication
N	Network in use (including with PIMA cloud)
P	Phone line in use
R	Relay (device) activation
S	Siren activation

# Appendix G. CMS Event Reporting

Below is a table with a list of the events that are reported to the CMS and private users.

Source	Reporting
Zone: Burglary, Shock sensor, Panic, Silent Panic, Fire, Duress, Medical, Tamper, Anti-mask, Custom + keypad alarms	Alarm/Restore/Fault. Tamper: including External and Internal Siren and EOL supervised loops.
Fault: AC Power <sup>24</sup> , Low Battery (including in peripherals), Phone Line, Cellular add-on/Cellular Modem+ SIM, Fuse current, CMS communication	Fault/Restore
Invalid code (after programmed keystrokes)/Arming/Disarming/ Technician On-site/Remote Test/Periodic Test/Zone Bypass (only zones that are set to report on alarm)/Pre-alarm/Power-up	Matching event
Zone/Output Toggle	Open/close activation/deactivation

## 1. Custom zones reporting codes

A custom zone allows flexibility when you want to report on events that are not the zone type's default events. These events can be water or gas leak, for example (see the Glossary, next).

Below are common events with their ContactID and SIA codes.

Event	ContactID
Gas leak	151
Freeze	152
Low heat	153
Water leak	154
Low gas pressure	157
High temperature	158
Low temperature	159
Low water pressure	201
Low water level	204

Event	SIA
Gas leak	GA
Restore	GH
High temperature	KA
Restore	KH
Water leak	WA
Restore	WH
Freeze	ZA
Restore	ZH

<sup>24</sup> When the report is delayed, if the fault does not exist by the time the delay elapses, no report is sent.

Copyright © 2020 by PIMA Electronic Systems Ltd. All rights reserved. E&OE



Manufactured by:

PIMA Electronic Systems Ltd.

[www.pima-alarms.com](http://www.pima-alarms.com)

5 Hatzoref Street, Holon 5885633, ISRAEL

Tel: +972.3.6506411

Email: [support@pima-alarms.com](mailto:support@pima-alarms.com)

P/N: 4410526

Revision: D2, XX en, Feb 2023

Changes:

D1: added Internet test option in Test and Diagnostic - > Communication tests

Added CMS ACK output in Appendix C

D2: corrected keyfob enrollment buttons