

# Agility™

Flexible Wireless Solution

## Installer Manual



Creating Security Solutions.  
*With Care.*

## **Important Notice**

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to RISCO Group. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the system.
- No part of its contents may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of RISCO Group.
- The information contained herein is for the purpose of illustration and reference only.
- Information in this document is subject to change without notice.
- Corporate and individual names and data used in examples herein belong to their respective owners.

## **Compliance Statement**

Hereby, RISCO Group declares that the Agility series of central units and accessories are designed to comply with:

- EN50131-1, EN50131-3 Grade 2
- EN50130-5 Environmental class II
- EN50131-6 Type A
- UK: DD243:2004, PD 6662:2004, ACPO (Police)
- USA: FCC: Part 15B, FCC part 68
- CANADA: CS-03, DC-01



All rights reserved.

© 2010 RISCO Group

March 2010

## Table of Contents

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1-1</b>
ARCHITECTURE .....	1-2
MAIN FEATURES.....	1-3
TECHNICAL SPECIFICATIONS.....	1-4
<b>CHAPTER 2 INSTALLING THE AGILITY.....</b>	<b>2-1</b>
AGILITY MAIN COMPONENTS.....	2-1
MOUNTING THE AGILITY .....	2-2
<i>Choosing the mounting location .....</i>	2-2
<i>Wall Mounting the Agility .....</i>	2-2
<i>Connecting the Backup Battery .....</i>	2-5
<i>Connecting the Agility to Power Supply - Configuration A .....</i>	2-6
<i>Ground Connection.....</i>	2-6
<i>Connecting the Agility to Power Supply - Configuration B.....</i>	2-7
<i>Completing Installation .....</i>	2-8
<i>DIP switch setting .....</i>	2-8
<i>Connecting a telephone line to the Agility .....</i>	2-9
<i>Connecting a network cable to the Agility .....</i>	2-10
<i>SIM Card Installation.....</i>	2-11
<i>External Audio Unit .....</i>	2-12
<b>CHAPTER 3 INSTALLER PROGRAMMING .....</b>	<b>3-1</b>
PROGRAMMING METHODS.....	3-1
<i>Configuration Software.....</i>	3-1
<i>Wireless Keypad .....</i>	3-1
<i>Installer Keypad .....</i>	3-2
<i>PTM: Data Storing Device .....</i>	3-2
WIRELESS DEVICE ALLOCATION .....	3-4
<i>Quick Allocation using the main unit button .....</i>	3-4
<i>Allocation using the keypad .....</i>	3-4
<i>Allocation using the Configuration Software .....</i>	3-5
<i>Transmitters Write Message Method .....</i>	3-7
DELETING WIRELESS ACCESSORIES.....	3-7
<b>CHAPTER 4 INSTALLER MENUS.....</b>	<b>4-1</b>
USING THE AGILITY KEYPAD KEYS .....	4-1
ACCESSING THE INSTALLER MENUS.....	4-2
PROGRAMMING MENU.....	4-2

<b>1. Programming: System Menu.....</b>	<b>4-2</b>
1.1 Timers .....	4-3
1.2 Controls .....	4-5
1.3 Labels .....	4-14
1.4 Sounds .....	4-15
1.5 System Settings.....	4-16
1.6 Service Information.....	4-16
1.7 Firmware Update .....	4-17
<b>2. Programming: Radio Devices Menu.....</b>	<b>4-18</b>
2.1 Allocation .....	4-18
2.2 Modification.....	4-18
2.3 Identification.....	4-40
<b>3. Programming: Codes Menu.....</b>	<b>4-41</b>
3.1 User .....	4-41
3.2 Grand Master .....	4-42
3.3 Installer .....	4-42
3.4 Sub-Installer .....	4-42
3.5 Code Length.....	4-43
3.6 DTMF Code.....	4-43
3.7 Parent Control.....	4-43
<b>4. Programming: Communication Menu.....</b>	<b>4-44</b>
4.1 Method.....	4-44
4.2 Monitoring Station .....	4-51
4.3 Configuration Software .....	4-57
4.4 Follow-Me .....	4-59
<b>5. Programming: Audio Messages Menu .....</b>	<b>4-65</b>
5.1 Assign Message .....	4-65
5.2 Local Message.....	4-65
<b>TESTING MENU .....</b>	<b>4-67</b>
1. Main Unit .....	4-67
2. Zone .....	4-68
3. Remote Control .....	4-68
4. Keypad.....	4-69
5. Siren.....	4-69
6. GSM.....	4-70
7. IP Unit .....	4-70
8. UO Unit.....	4-71
<b>ACTIVITIES MENU .....</b>	<b>4-71</b>
<b>FOLLOW ME MENU.....</b>	<b>4-72</b>
<b>CLOCK MENU .....</b>	<b>4-73</b>

EVENT LOG MENU .....	4-73
MACRO MENU .....	4-73
<i>Programming Macro Keys</i> .....	4-73
<i>Activating a Macro</i> .....	4-74
<b>APPENDIX A REPORT CODES.....</b>	<b>A-1</b>
<b>APPENDIX B INSTALLER EVENT LOG MESSAGES.....</b>	<b>B-1</b>
<b>APPENDIX C LIBRARY VOICE MESSAGES .....</b>	<b>C-1</b>
<b>APPENDIX D EN 50131 COMPLIANCE .....</b>	<b>D-1</b>
<b>APPENDIX E INSTALLER PROGRAMMING MAPS .....</b>	<b>E-1</b>
<b>APPENDIX F SIA CP-01 COMPLIANCE .....</b>	<b>F-1</b>

## Chapter 1 Introduction

The Agility is a Flexible Wireless Security Solution that incorporates state-of-the-art wireless and communication technology. Agility is ideal for installation in any home or office environment and supports RISCO Group's extensive range of one-way and two-way wireless security and safety devices, keypads, remote controls, keyfobs, panic buttons, fully wireless sirens and other accessories.

### Main Benefits:

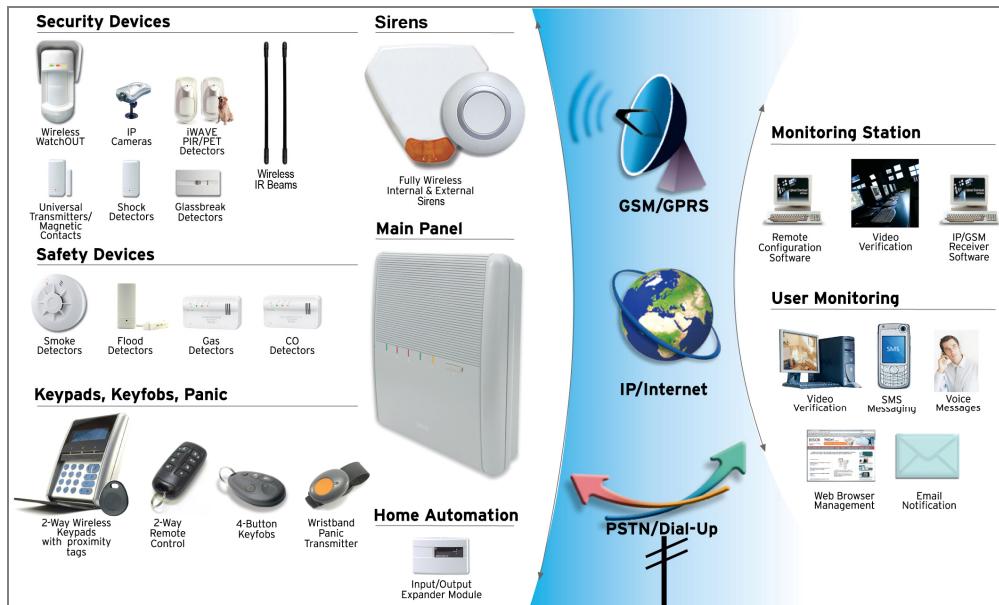
- ◉ Flexible Plug-in Communication
  - ❖ IP Module
  - ❖ GSM/GPRS Module
  - ❖ Fast PSTN Module
- ◉ Use any single module, any combination or all three modules for backup, or no communication for audible only installations
- ◉ 2-Way Wireless Keypad with full programming capability
- ◉ 2-Way 8 button Wireless Remote Control with code protection, key-lock and system status request and indication
- ◉ 2-way voice communication
- ◉ Easy enrolling of Wireless Devices without a keypad
- ◉ Remote enrolling according to Device ID
- ◉ Combine one-way or two-way transmitters in the same system
- ◉ Flash memory for easy firmware upgrade
- ◉ Simple physical installation with wall brackets
- ◉ Separate main panel, can be hidden for higher security
- ◉ Program Transfer Module (PTM) for program backup
- ◉ Simplified menu logic (only menus of installed devices are displayed, only menus according to the authorization code are displayed)

### Main Features:

- ◉ 32 wireless zones
- ◉ 3 partitions
- ◉ Up to 3 bi-directional wireless keypads
- ◉ Up to 8 Remote Control keyfobs (combination of 8 or 4 button) or one way
- ◉ Input/Output module:
  - ❖ 2-way wireless communication to the Agility
  - ❖ Local transformer with rechargeable backup batteries
  - ❖ 4 wired zones with selectable EOL resistance & 4 outputs (2x3A relay and 2x500mA)
  - ❖ Includes X-10 adaptor
- ◉ 32 user codes
- ◉ 250 event log
- ◉ Uses regular Sealed Lead Acid Battery 6V 3.2Ah

## Architecture

The following diagram provides an overview of the Agility's architecture and capabilities. Examine the figure before beginning with your Agility installation to obtain an overall picture of the full extent of the Agility system capabilities.



## Main Features

The following illustration describes the main features of the Agility:

<b>Detectors</b>	<b>Monitoring Station</b>	<b>Communication</b>	<b>Installer Programming</b>
<ul style="list-style-type: none"> <li>• 32 Wireless zones:</li> <li>• 4 Wired zones via optional Wireless I/O Expander</li> <li>• Total zones: 36</li> <li>• More than 25 zone types</li> <li>• Full zone supervision</li> <li>• 2-way and 1-way detectors combined on the same system</li> </ul>	<b>Monitoring Station</b> <ul style="list-style-type: none"> <li>• Remote programming, diagnostics and communication test.</li> <li>• Report to 3 MS.</li> <li>• Report thought PSTN, GSM, GPRS or IP.</li> <li>• MS polling through IP network.</li> <li>• Account number for each MS.</li> <li>• Flexible split reporting for backup.</li> <li>• Call Save mode for non-urgent reports.</li> <li>• Remote device enrollment.</li> </ul>	<b>Communication:</b> <ul style="list-style-type: none"> <li>• Flexible communication over GSM/GPRS, IP or PSTN.</li> <li>• Backup capability between the communication methods.</li> <li>• Supports major reporting formats.</li> <li>• Add on module for each communication type.</li> </ul>	<b>Installer Programming:</b> <ul style="list-style-type: none"> <li>• Local /Remote using configuration software</li> <li>• Program transfer module.</li> <li>• Full programming using bi-directional wireless keypad.</li> <li>• Flexible device enrollment by serial ID serial number or by RF allocation.</li> <li>• Keypad programming menu adjusted to existing hardware.</li> </ul>
<b>Sirens</b>			
<ul style="list-style-type: none"> <li>• Built-in siren</li> <li>• Fully wireless external and internal wireless sirens</li> <li>• Add up to 3 Sirens</li> </ul>			
<b>Bi-directional Keypad</b>			<b>User Operating Tools:</b>
<ul style="list-style-type: none"> <li>• Fully Wireless</li> <li>• LCD display</li> <li>• S.O.S / Two way communication emergency key</li> <li>• Double tamper protection (Box &amp; Wall)</li> </ul>			<ul style="list-style-type: none"> <li>• Bi-directional 8 button key fob</li> <li>• Bi-directional Keypad</li> <li>• 4 button keyfob</li> <li>• Remote phone operation</li> <li>• SMS</li> <li>• Configuration software</li> <li>• Web browser (will be available in future versions of Agility)</li> </ul>
<b>Codes:</b>			<b>Home Automation</b>
<ul style="list-style-type: none"> <li>• 1 installer code</li> <li>• 1 sub installer code</li> <li>• 1 grand master code</li> <li>• 32 user codes</li> <li>• 4 authority level</li> <li>• Optional 4 or 6 digits code definition</li> </ul>			<ul style="list-style-type: none"> <li>• 4 outputs via wireless I/O expander</li> <li>• 16 X-10 outputs via wireless I/O expander</li> <li>• Outputs can follow system, partition, zone or user events</li> <li>• Outputs can be scheduled, or activated automatically, or by user command (SMS, web browser or remote phone)</li> </ul>
<b>Follow Me:</b>	<b>Voice capabilities:</b>	<b>Wireless Features:</b>	<b>False Alarm Reduction:</b>
<ul style="list-style-type: none"> <li>• 16 follow me destinations</li> <li>• Follow me can be defined as voice message, SMS or Email</li> <li>• User control over the system</li> <li>• Security code protection</li> </ul>	<ul style="list-style-type: none"> <li>• 2-Way communication</li> <li>• Remote phone operation</li> <li>• Full voice menu guide</li> <li>• System event messaging</li> <li>• Local announcement messages</li> <li>• Voice description for zones, partitions, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Signal jamming indication</li> <li>• Receiver calibration</li> <li>• 868MHz/433 MHz radio frequencies</li> <li>• Programmable supervision time</li> <li>• Tamper detection in transmitters</li> <li>• Low battery detection in transmitters</li> </ul>	<ul style="list-style-type: none"> <li>• Swinger shutdown</li> <li>• Zone crossing</li> <li>• Report delay to MS</li> <li>• Abort alarm feature</li> <li>• Soak test</li> <li>• Final exit zone</li> </ul>



## Technical Specifications

The following technical specifications are applicable for the Agility:

### Electrical Characteristics

<b>Power</b>	230VAC (-15%+10%), 50Hz, 50mA
<b>Units consumptions</b>	Main board: Typical 130mA GSM: Stand by 35mA, Communication 300mA Modem: Stand by 20mA, Communication 60mA IP Card: 90mA (Max)
<b>Backup battery</b>	Sealed Lead Acid Battery 6V 3.2Ah
<b>Internal Siren intensity</b>	90 dBA @1m
<b>Operating temperature</b>	-10°C to 40°C (14°F to 131°F)
<b>Storage temperature</b>	-20°C to 60°C (-4°F to 140°F)

### Physical Characteristics

<b>Dimension</b>	268.5 mm x 219.5 mm x 64 cm (10.57 x 8.64 x 2.52 inch)
<b>Weight (no battery)</b>	1.31Kg (Full configuration) GSM module: 0.045 Kg

### Wireless Characteristics

<b>Radio Immunity</b>	According to EN 50130-4
<b>Frequency</b>	868.65 MHz/433.92 MHz

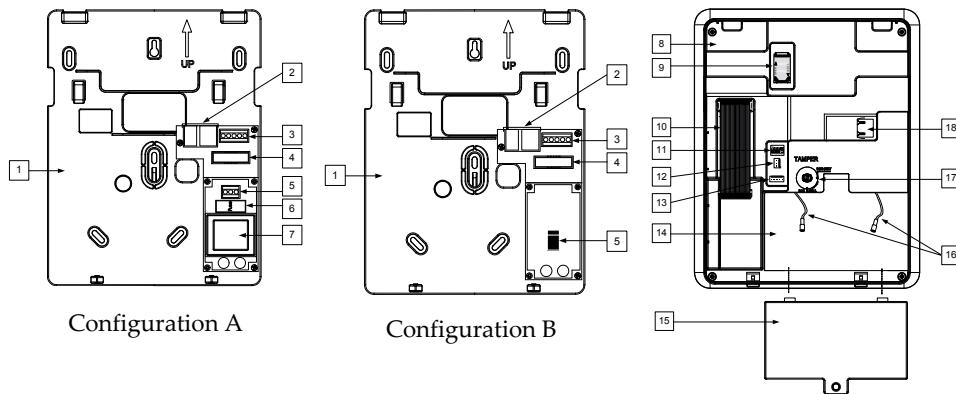
## Chapter 2 Installing the Agility

This chapter covers the installation procedures of the **Agility**, as follows:

- Agility Main Components, page 2-1
- Mounting the Agility, page 2-2
- Choosing the mounting location, page 2-2
- Wall Mounting the Agility page 2-2
- Connecting the Backup Battery, page 2-5
- Connecting the Agility to Power Supply, page 2-6
- Ground Connection, page 2-6
- DIP switch setting, page 2-8
- Connecting a telephone line to the Agility, page 2-9
- SIM Card Installation, page 2-9
- External Audio Unit, page 2-12

### Agility Main Components

The illustration below shows the internal components (when the Mounting Bracket is disassembled from the Back Panel).



*Figure 1: Agility Main Components*

- |                                      |                       |                                    |
|--------------------------------------|-----------------------|------------------------------------|
| 1. Installation Bracket              | 7. Transformer        | 13. RS 232 communication connector |
| 2. Telephone Jacks                   | 8. Back Panel         | 14. Battery compartment            |
| 3. Audio Unit terminals              | 9. SIM Card socket    | 15. Battery compartment cover      |
| 4. Ribbon flat cable jack            | 10. Ribbon flat cable | 16. Battery fusing leads           |
| 5. AC connection terminals/DC Socket | 11. DIP Switches      | 17. Tamper switch                  |
| 6. Fuse                              | 12. PTM connector     | 18. IP Card network connector      |

## Mounting the Agility

**IMPORTANT:** The Agility has no user replaceable parts (for instance: power cord, fuse, battery, etc.) only certified installers are allowed to replace faulty parts.

### Choosing the mounting location

Before you mount the **Agility**, study the premises carefully in order to choose the exact location of the unit for the best possible coverage and yet easily accessible to prospective users of the alarm system.

The mounting location of the **Agility** should be:

- ◎ Try to centrally locate the system between all the transmitters.
- ◎ Near an uninterrupted AC outlet.
- ◎ Near a telephone outlet.
- ◎ Far from sources of interference, such as:
  - ❖ Direct heat sources
  - ❖ Electrical noise such as computers, televisions etc.
  - ❖ Large metal objects, which may shield the antenna.
- ◎ In a place where the alarm can be heard during Part Arming mode.

### Wall Mounting the Agility

The **Agility** is comprised of two sub-assemblies:

- ◎ Mounting bracket,
- ◎ Main unit which in its turn is comprised from:
  - ❖ Front panel (not disassembled on a regular installation procedure)
  - ❖ Back panel

The mounting bracket is mounted on the wall, using the supplied proper hardware, as described below:

#### To mount the Agility on the Wall:

1. Separate the Mounting bracket as follows:
  - a. Release the Mounting bracket captive locking screws (1, Figure 2) located at the bottom of the unit by turning screws counterclockwise.

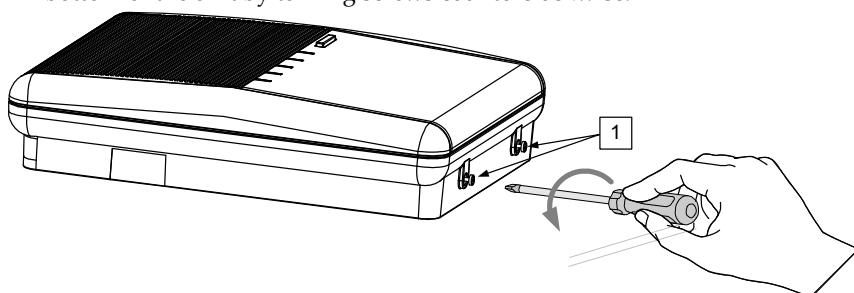
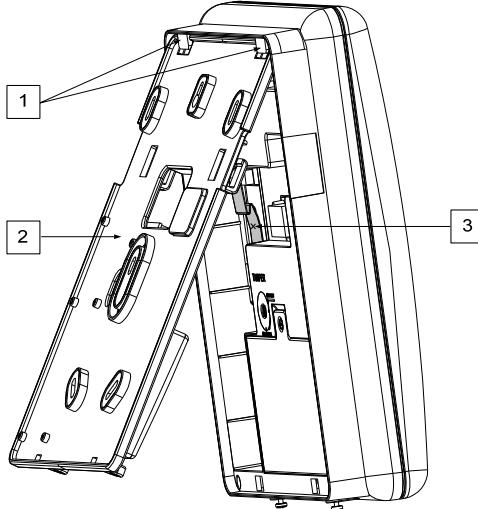


Figure 2: Mounting Bracket screws

- b. Gently, pull up the Mounting bracket to a 45° angle and slide it down to release the Mounting bracket (2, Figure 3) from the two locking tabs (1, Figure 3) at the top of the unit.

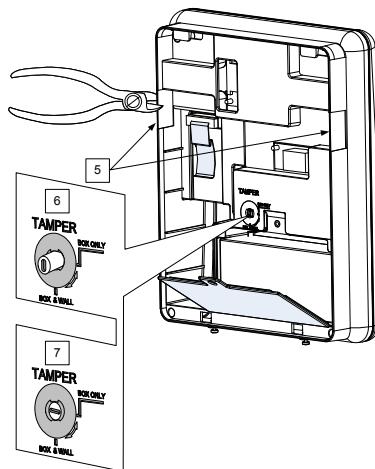
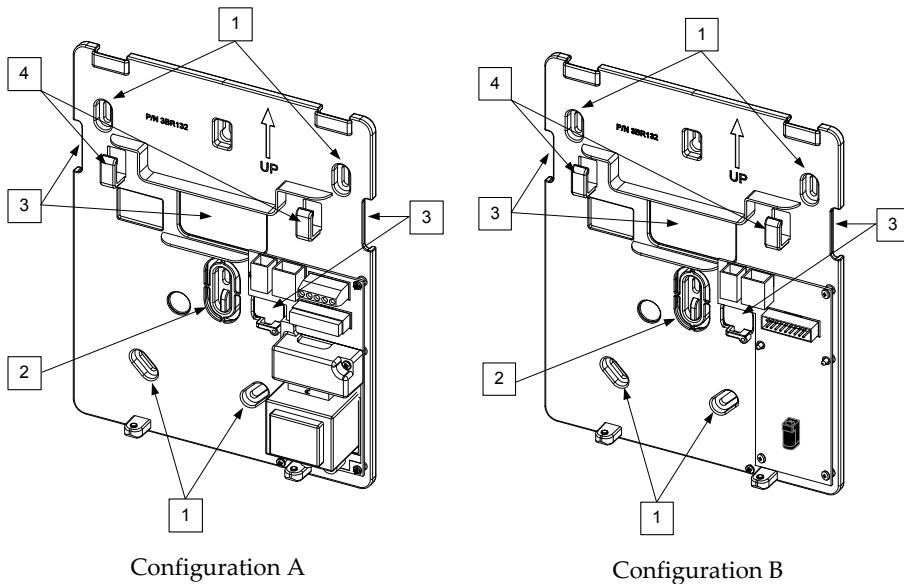
**Note:** Do not open the Mounting bracket to a larger angle in order not to break the two top tabs and not to tear up the ribbon flat cable connecting the power supply unit to the front panel (PCB).

- c. Disconnect the ribbon flat cable (3) from the power supply unit while leaving it connected to the Main panel.



*Figure 3: Mounting Bracket removal*

2. Hold the Mounting bracket against the wall as a template and mark the locations for the mounting holes (5 mounting holes item 1, and an additional hole for securing the tamper protection bracket item 2, are available, see Figure 4).
3. Drill the desired mounting holes and place the screw anchors. Use the supplied 5 Philips pan head screws to attach the Mounting bracket to the wall (ST4.2 mm x 32 mm DIN 7981).
4. According to the location of the wall cables, route and insert the wires and cables via the cable's openings (3) (including AC cable and telephone cable), see figure 3.
5. If required, remove cable knockouts (5) to allow wire passage.
6. Anchor cables with dedicated hooks (4).



7. Adjust the Tamper switch (using a flat screwdriver) according to your preferred configuration.
  - a. Box and Wall configuration (see Figure 4, detail 6) - Triggers the tamper when the box or the wall mounting are tampered.
  - b. Box only configuration (see Figure 4, detail 7) – Triggers the tamper when the box is tampered.

## Connecting the Backup Battery

The **Agility** has safety approved, sealed lead acid 6V, 3.2Ah rechargeable backup battery used in time of main power failure:

---

**Note:** The battery is supplied with the **Agility**.

---

### To insert the Backup battery:

Remove the battery compartment cover screw (see Figure 5,3) located at the top of the cover by turning screw counterclockwise and pull the **Agility** battery cover outward.

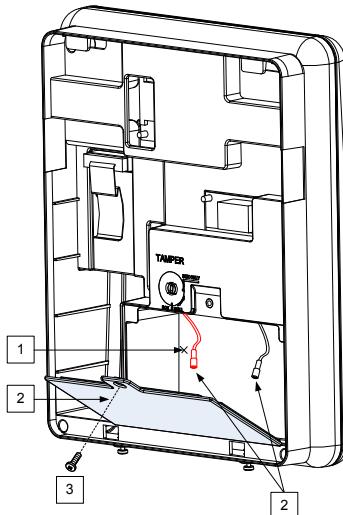


Figure 5: Battery Compartment

- a. Insert the battery into its place and connect the flying leads to the battery according to the correct polarity (Red +) (Black -).
- b. Return the battery compartment cover (after placing the battery in) and secure with locking screw.

---

**Note:** The **Agility** Rechargeable battery should be charged for at least 24 hours.

---

**Important:** When replacing the battery be sure to buy the same type. Failure to comply with this instruction may result in damage to personnel and/or equipment.

Dispose of used batteries according to the proper instructions.

## **Connecting the Agility to Power Supply - Configuration A**

---

**Note:** The Agility panel is permanently connected to the mains. The connection must be made according to your country's local regulations. As a general guideline, connect the Live Neutral and Ground using a safety approved 3-wire 18AWG power cable (14-mm minimum diameter flexible PVC cable which complies with IEC60227). The cable should be brought to the Agility panel in a protective plastic conduit (diameter - 16mm minimum).

A 2-pole 16A circuit breaker and earth leakage protector should be used to disconnect the live conductor, and should be provided as part of the building installation.

---

The Agility is powered by a safety approved 230VAC.

1. Remove the power supply unit cover (Figure 6, 1).
  2. Connect the power wire (Safety approved, SVT, 18AWG, 0.75mm<sup>2</sup>) to the power terminal located on the power supply unit (TB1) (2, Figure 6).
- 

**Note:** The power wire is not supplied with the **Agility**.

---

3. DO NOT connect the cable to the wall power supply at this point.

### **Ground Connection**

Grounding provides a degree of protection against lightning and induced transients for any piece of electronic equipment that may, due to lightning or static discharge, experience permanent or general malfunctions. The ideal ground is considered to be a unified earth ground in which an 8-foot copper-clad rod, located close to the existing power and telephone ground rods, is sunk several feet into the earth. Appropriate hardware and clamps are then used to electrically connect each of these rods together and then to the ground terminal of the device to be protected.

It may be possible to use an existing electrical ground on the premises if one is close enough to the Agility. When connecting the ground wire, use a solid 14-gauge wire [or larger (numerically *lower* size)]. Keep this wire as short as possible and do not run it in conduit, coil it, bend it sharply, or run it alongside other wiring. If you must bend it or change its direction, it should have a radius of at least 8 inches at the point from which it is bent. If in doubt, you may want to enlist the help of a licensed electrician in matters concerning such grounding.

#### **To connect to ground (Earth):**

Connect between the Agility's ground terminal and an acceptable electrical ground connection for the lightning transient protective devices in this product to be effective.

---

**Important:** Connecting to ground must be performed according to the local National Electrical Code.

---

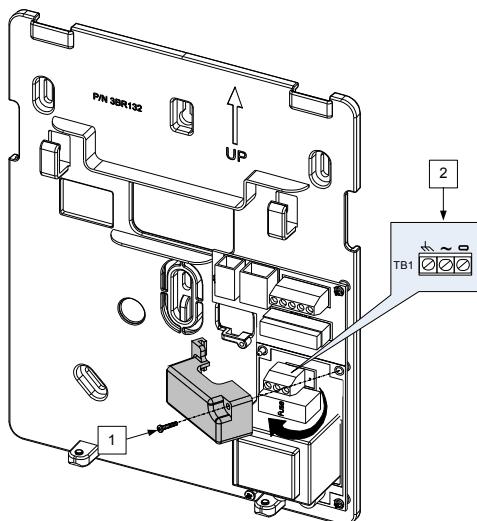


Figure 6: Connecting AC Power wires

**Connecting the Agility to Power Supply - Configuration B**

1. The Agility is powered by a 9VDC/1.0A Transformer.
2. Connect the transformer power jack to the power supply located on the power supply card (1, Figure 6A).
3. DO NOT connect the transformer inlet cable to the wall power supply at this point.

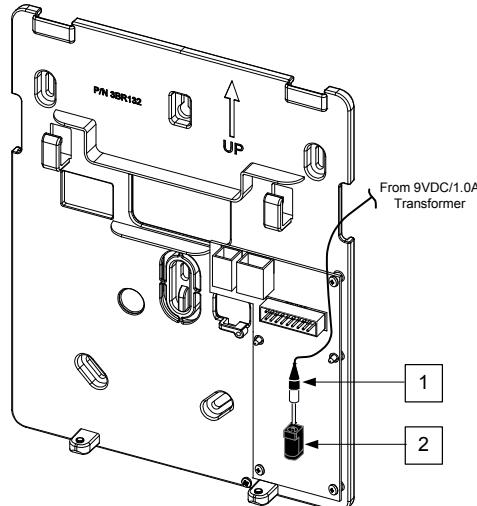


Figure 6A: Connecting DC Power Cable

## Completing Installation

1. Set the DIP Switches according to the DIP Switch Setting section (see page 2-8).
2. Connect the ribbon flat cable between the main panel and the mounting bracket (J1).
3. Mount the Main unit to the mounting bracket using captive locking screws.
4. Plug in the power cable to the wall power outlet.
5. Power up the Agility.

### DIP switch setting



**DIP Switch 1 (E-A): External Audio:** Used to define if the voice of the Agility will go from the main unit or from an External Audio Unit. When the external unit is connected to the Agility the voice will be heard only through the Audio voice unit.

**ON:** External Audio Unit is connected to the Agility

**OFF (Default):** External Audio unit not connected to the Agility.

**DIP Switch 2 (DFLT): Default jumper:** Used when performing the following 3 operations:

1. To return installer, sub-installer and grand master codes to their default factory values.

Set this DIP switch to **ON**, disconnect all power and then reconnect the power.

---

**Note:** Code Length does not change.

2. To manually erase wireless devices. Set this DIP switch to **ON** while power is connected. Execute a long press on the main unit button until a beep, indicating that all wireless devices have been erased, is heard.

3. To save or transfer data to or from the PTM device.

**ON:** To transfer data from the PTM to the panel.

**OFF:** To transfer data from the panel to the PTM. (Refer to *Chapter 3* for these procedures.)

**DIP Switch 3 (PRGM):** Enables loading local software updates to the Agility

**ON:** software updates to the Agility can be loaded

**OFF (Default):** software updates to the Agility can not be loaded

**DIP Switch 4 (BAT):** Defines the Battery Discharge Protection option settings

**ON:** Battery Discharge Protection is OFF: The battery may be totally discharged during continuous AC failure, thus battery replacement may be required (no deep discharge protection).

---

**Note:** In this position the Agility will start to operate from a battery power supply whether it is connected to the Mains or not.

**OFF (Default):** Battery deep Discharge Protection is ON: If an AC power outage occurs, the Agility automatically disconnects the battery when its backup battery voltage drops below 5.8 VDC, in order to prevent "deep discharge" that may damage the battery.

---

**Note:** In this position the Agility will not start to operate from a battery power supply, unless connected to the Mains first.

---

## Connecting a telephone line to the Agility

Connect the system to a telephone line if the system configuration includes an internal modem (identical for Configuration A and B).

1. Connect the incoming telephone line to the plug-in CONN2 jack RJ11 (pins 2, 3) or to plug-in CONN3 RJ31 (pins 4, 5) (see Figure 7: Telephone Line Jacks).
2. Connect any telephone on the premises to the plug-in CONN2 jack RJ11 (pins 1, 4) or to plug-in CONN3 RJ31 (pins 1, 8) (see Figure 7: Telephone Line Jacks).

---

**NOTE:** To ensure line seizure capability, and comply with FCC part 68 regulations, the equipment must be connected directly to the Phone company lines ('CO'). Whether connected via RJ11, RJ31, the line port must be connected to the CO lines without any other phones or other telecom equipment between them. Other telecom equipment can be connected only after (in series) the alarm panel.

---

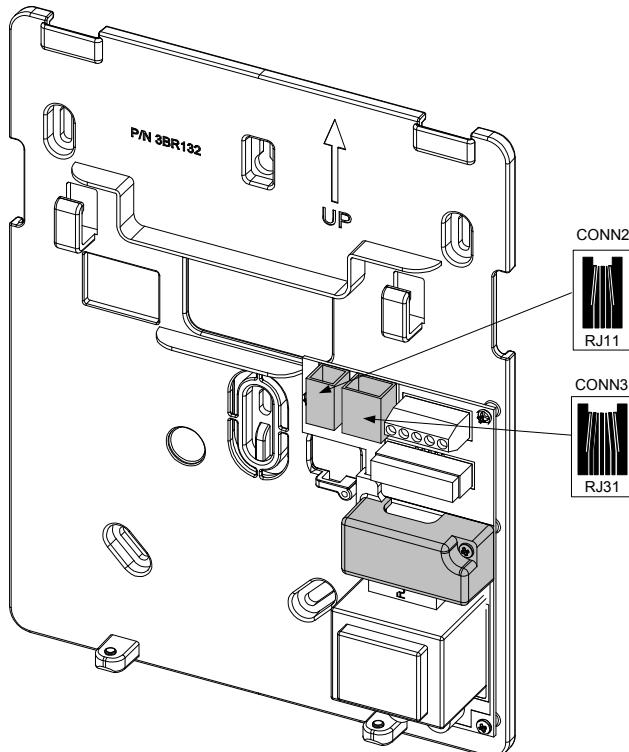
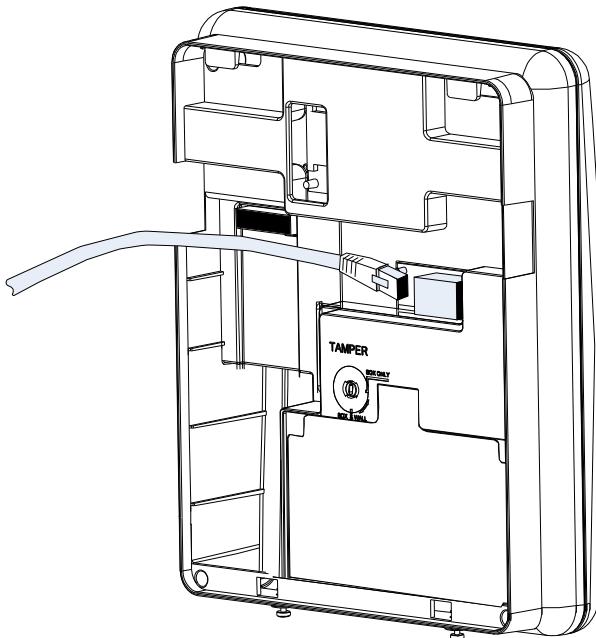


Figure 7: Telephone Line Jacks

## **Connecting a network cable to the Agility**

If your Agility is equipped with an IP Card, you should connect the incoming network cable in order to enable IP Communication.

1. Separate the Agility from the mounting bracket.
2. According to the location of the network cable, route and insert the cable via the cable's openings (see figure 3).
3. If required, remove cable knockouts (5, Figure 3) to allow cable passage.
4. Connect the incoming network cable to the plug-in.



## SIM Card Installation

If your Agility is equipped with a GSM/GPRS module, you should insert a SIM card in order to enable communication through the GSM/GPRS network.

1. Insert the SIM into the dedicated SIM card slot located on the rear side of the back panel (See Figure 1: Agility Main Components).

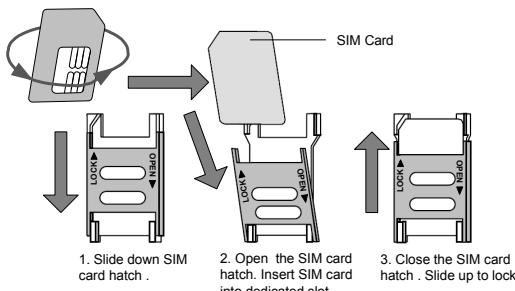


Figure 8: SIM Card Insertion

**Important:** Do not install SIM card while power is applied to the Agility.

Do not touch SIM Card connectors! If doing so, you may release an electrical discharge that could damage the SIM card.

2. If a PIN code is required for the SIM card, the Agility will indicate a PIN code trouble. To fix the trouble, and thus enable the SIM card to operate properly, enter the PIN code number, located in the Communication > GSM parameters menu.

**Note:** Ensure that you have the PIN code. Be aware that after three wrong attempts (recognized by the SIM card) to enter a PIN number, the SIM card will lock.

You will have to contact your local cellular provider to unlock the SIM card.

3. If you want to disable the SIM PIN code you should follow the steps:
  - a. Insert the SIM card into a standard GSM mobile phone.
  - b. Insert the PIN code.
  - c. Access the phone security menu and selecting PIN OFF. Once done, re-test by switching the phone OFF, then switching ON. The PIN code should not be requested again.
4. Once the SIM card is placed it is recommended to test the operation of the SIM by conducting a call and testing the GSM signal strength. For more information refer to the programming menus of the GSM menu.

**Note:** In some countries an SMS center phone number might be required in order to enable SMS messaging.

This phone number is provided by the provider. Programming the SMS center phone into the SIM can be done using a standard GSM mobile phone or from the Agility keypad or configuration software.

## External Audio Unit

The Agility enables to connect an external Audio Unit instead of the internal unit in order to listen to the system's audio messages in a distance from the main unit. In addition the unit enables you to talk into your premises.

To connect the Audio unit:

1. Wire the Audio unit to the Agility as displayed in the Wiring Diagram described in Figure 9. The terminals for wiring the Audio Unit to the Agility are located on mounting bracket the Agility.
2. Set DIP Switch 1 (E- A) (**External Audio**) to **On** position.

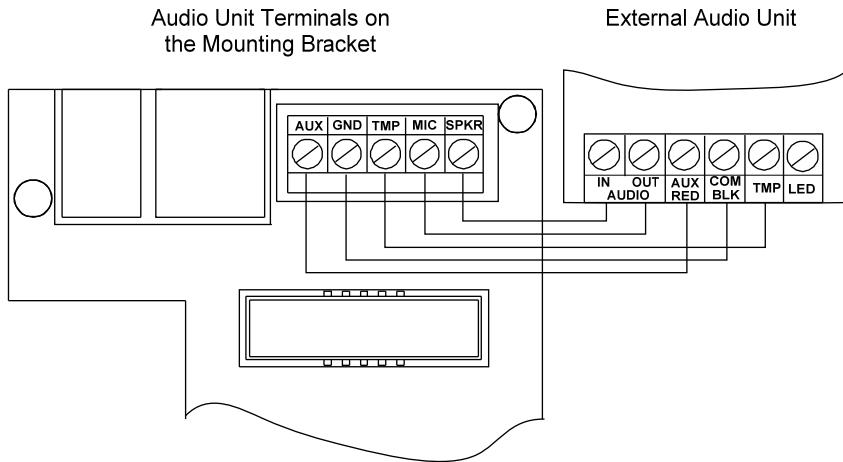


Figure 9: Wiring the External Audio Unit to Agility

## Chapter 3 Installer Programming

### Programming Methods

There are 4 available options for programming the Agility:

- Configuration Software
- Wireless Keypad
- Installer Keypad
- PTM

#### Configuration Software

A software application that enables you to program the Agility from a PC computer. It offers the following alternatives:

- Working locally, through a portable computer connected to the Agility via cable
- Working at a remote site, communicating with the Agility via a phone line, modem or IP address.

For further information on programming the Agility via the Configuration software, refer to the *Agility Configuration Software* manual.

#### Wireless Keypad

The Agility can be fully configured via the wireless keypad.

---

##### Notes:

1. The Agility can be programmed via any of the 2 way keypads in your system, but only using one keypad at a time for programming.
  2. During installer programming, the keypad will turn off after 4 minutes if no entry has been made to the keys. Press any button to restore the keypad. It will display the last parameter you were working on.
- 

#### To program the Agility via the Wireless Keypad, follow this procedure:

1. Perform system device allocation for the keypad (refer to page 3-4).
  2. Press  and enter the installer code (default code is 0132). The keypad will sound a confirmation sound.
- 

**Note:** If a Grand Master code is required to confirm the installer code, it should be entered at this stage after the installer code.

---

3. Go to the Programming menu and press . Once the panel is in programming mode, the Agility main unit LEDs will flash simultaneously and a confirmation sound will be heard.

---

**Note:** The installer can also program user activities by selecting the Activities menu instead of the Programming menu. Use the  buttons to navigate between the menus.

---

### **Installer Keypad**

For those systems that do not have keypads, RISCO Group offers the Agility installer a temporary keypad to be used as any Agility wireless keypad for configuring a system. An hour after exiting the programming mode the Installer Keypad will be erased from the Agility memory or when power is lost to the system.

#### **To program the Agility via the Installer Keypad, follow this procedure:**

1. To allocate the Installer Keypad into the system perform a short press on the main unit button.

2. Press the  buttons on the keypad simultaneously until the following message appears:

**Insert GM Code**

3. Enter the Grand Master code and press . The following confirmation message is heard: "Installer Keypad Allocated".

---

**Note:** When a wrong Grand Master code is entered, the keypad will be deleted. To continue this procedure, perform reallocation of the keypad.

---

4. Follow steps 2 and 3 of the wireless keypad (see page 3-1) to begin programming the system.

### **PTM: Data Storing Device**

The PTM is a tiny circuit board into which the Agility panel can transmit a copy of the system's configuration. The PTM stores this copy and can also transmit the configuration information back to the Agility panel.

#### **To transfer the system configuration from the panel to the PTM, follow this procedure:**

1. Disconnect the flat cable and remove the Agility main unit from its wall bracket.

---

**Note:** Make sure the battery is inserted into the main unit.

---

2. Make sure that Dipswitch 2 is set to OFF (default setting).

3. Place the PTM onto the 5-pin PTM located on the rear of the main unit PCB. The PTM LED will turn on.
4. Press the main unit button for 5 seconds. The PTM LED will flash quickly during the transmission of information to the PTM.
5. Once transmission is complete, the panel will sound a confirmation beep and the PTM LED will stop flashing and turn on steady.
6. Disconnect the PTM from the main unit.
7. Reconnect the flat cable to the main unit and replace the main unit in its wall bracket.

**To transfer the system configuration from the PTM to the Agility panel, follow this procedure:**

1. Disconnect the flat cable and remove the Agility main unit from its wall bracket.

---

**Note:** Make sure the battery is inserted into the main unit.

---

Make sure that the Default Enable system flag is on

2. Set Dipswitch 2 to ON.
3. Place the PTM onto the 5-pin PTM connector located on the main unit PCB.
4. All LEDs on the main unit will begin to flash simultaneously. The PTM LED will flash quickly during the transmission of information to the panel.
5. Once transmission is complete, the panel will sound a confirmation beep.

---

**Note:** If the procedure fails the panel will make 3 short error beeps, and you will need to do the procedure again

6. Disconnect the PTM from the main unit.
7. Reset Dipswitch 2 to OFF.
8. Reconnect the flat cable to the main unit and replace the main unit in its wall bracket.

## Wireless Device Allocation

Each wireless device must identify itself to the system receiver. The following section describes the different ways to allocate all of your devices to the system in order to later configure each device's parameters.

The learning procedure between the wireless devices and the main unit can be performed either from the main unit, a wireless keypad or via the Configuration Software.

### Quick Allocation using the main unit button

To perform quick allocation using the main unit button, follow this procedure:

---

**Note:** To enable Quick Allocation mode the System bit "Quick Learn" should be enabled.

---

1. Set the main unit to Learn mode with a long press on the main unit button. Each LED will light up one after another.

---

**Note:** The unit will sound each time you enter or exit the Learn mode.

---

2. Send a transmission from each device (refer to the *Transmitters write message method* table in section). The system will automatically identify each device according to different categories (for example: detectors, sirens, keypads, remote controls etc.) and enter each device and its default value into the unit's memory. Each device receives an index number from the system.
3. Exit the Learn mode with a short press on the main unit button.

### Allocation using the keypad

It is possible to perform allocation via the keypad in two different ways: RF Allocation or by entering the device's serial code.

To perform RF Allocation via the keypad, follow this procedure:

1. Go to the Installer menu and select Programming → Radio Device → Allocation → 1) RF Allocation. The system immediately goes into Learn mode.
2. Send a transmission from the device. (See table: *Transmitters write message method*)
3. The main unit will acknowledge the transmission with a sound. When the system recognizes the device the keypad LCD will display the device's serial number and category. The system also automatically allocates the device the next available index number.

To perform allocation via the keypad using a serial code, follow this procedure:

1. Go to the Installer menu and select Programming → Radio Device → Allocation → 2) By Code. Enter the device's 11 digit serial code number.

2. The system automatically recognizes the device and allocates it the next available index number. The system will sound the device type that has been allocated and the place it has been allocated to.

### To allocate zones to a predefined place via the keypad follow this procedure:

Compared to the RF and Code allocations mentioned before, where the wireless elements are allocated automatically by the system to the first available place, when it comes to zones allocation the Agility also enables the allocation of zones to a pre-defined location.

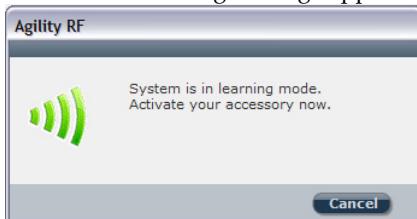
1. Go to the Installer menu and select Programming → Radio Device → Allocation → 3) Zone Allocation.
2. Select the zone number to which you want to assign the detector and press .
3. Using the arrow keys select the allocation method: RF or Code allocation.
  - RF allocation: Send a transmission from the device. (See table: *Transmitters write message method*)
  - Code allocation: Enter the device's 11 digit serial code number.
4. The system allocates the detector into the selected index number. The system will sound the device type that has been allocated and the place it has been allocated to.

### Allocation using the Configuration Software

It is possible to perform wireless device allocation via the configuration software in two different ways: RF Allocation or by entering the device's serial code.

#### To perform RF allocation from the configuration software

1. Establish Communication between the main unit and the Configuration software. (For more information refer to the *Configuration Software Manual*)
2. Open the Activities > Radio Device Allocation screen.
3. Click on the  button. This operation will set the main unit to Learn mode. The following message appears:



4. Send a transmission from the device. (See table below)

5. The main unit will acknowledge the transmission with a sound. When the system recognizes the device the **Radio Device Allocation** screen indicates that the status of allocation has been successful. The serial number, accessory type and the index number information will be displayed. The index number is automatically addressed by the system.

---

**Note:** If required you can change the index number of the wireless device by selecting the required index number and pressing the  button again.

---

6. To allocate an other wireless device click on the  button and then repeat stages 3-7.

#### To perform Code allocation from the configuration software

1. Establish Communication between the main unit and the Configuration software by selecting Communication>Connect from the main menu. (For more information refer to the *Configuration Software Manual*)
2. Open the **Radio Device Allocation** screen. In the *Allocation* area, enter the device's serial number.

---

**Note:** The serial number can be found on the device.

---

3. Select the wireless device index number. Automatic means that the index number is automatically addressed by the system,
4. Press the  button.
5. The main unit will acknowledge the transmission with a sound. When the system recognizes the device the **Radio Device Allocation** screen indicates that the status of allocation has been successful.

## Transmitters Write Message Method

<b>How to send a write message (transmission):</b>	
<b>Wireless Device</b>	<b>Sending Write Message</b>
<b>Detector/Contacts</b>	Press the tamper switch for 3 seconds
<b>2-Way Keypad</b>	Press both keys  and  simultaneously for at least 2 seconds
<b>1-Way Keypad</b>	Press the  key twice
<b>1-Way Key fob</b>	Press the  button for at least 2 seconds
<b>2-Way Remote Control</b>	Press both keys  and  simultaneously for at least 2 seconds
<b>Smoke Detector</b>	Insert battery. Write message is send automatically within 10 seconds.
<b>Siren</b>	Press the reset switch on the siren. After a squawk is sounded at the siren you have 10 seconds to press on the tamper switch for at least 3 seconds.
<b>Gas, CO detectors</b>	Press the test button for 3 seconds
<b>2 Panic Button Key fob</b>	Press both buttons for at least 7 seconds

## Deleting Wireless Accessories

Deleting all wireless devices can be done manually (from the main unit) or from the Configuration software.

### To manually delete all wireless accessories from the system:

1. Place Dip Switch 2 to **ON** position.
2. Press the main unit button until it sounds.
3. Replace Dip Switch 2 to **OFF** position.

### To delete a wireless accessory from the Wireless Keypad

1. Go to the Installer menus and select Programming → Radio Device → Modification
2. Select the device category
3. Go to Parameters option.
4. Select the device index number
5. Go to Serial number option and type in 000000000000.
6. Press . The device will be deleted

**To delete a wireless accessory from the system via the Configuration software:**

1. Establish Communication between the main unit and the Configuration software  
(For more information refer to the *Configuration Software Manual*)
2. In the **Radio Device Allocation** screen in the *Delete Accessories* area enter the device's serial code and click the **Delete** button.

**To delete all wireless accessories from the system via the Configuration software:**

1. Establish Communication between the main unit and the Configuration software by selecting Communication>Connect from the main menu. (For more information refer to the *Configuration Software Manual*)
2. In the **Radio Device Allocation** screen in the *Delete Accessories* area, click the **Delete All** button. When all accessories have been deleted the screen will indicate that deletion has been successful.

## Chapter 4 Installer Menus

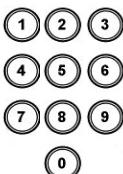
The following chapter describes the parameters and programming options of the system and radio devices. These parameters can be programmed via the Agility keypad or the configuration software by the installer.

**Note:** A note appears next to the parameters that can only be programmed via the configuration software.

For more information regarding the installation and use of the configuration software refer to the *Configuration Software* manual.

### Using the Agility keypad keys

The Agility two way keypad contains three LED indicators, an LCD display and a variety of keys. The following table describes the typical uses of the keys when in programming mode.

Keys	Description
	<p>The numerical keys on the keypad are used as quick keys, a numerical sequence used as a shortcut to program an option.</p> <p><b>To program the system using Quick keys:</b></p> <ol style="list-style-type: none"> <li>Access the installer menus (see below) and select the relevant main menu option.</li> <li>Press the quick keys in sequence to locate the parameter and press .</li> </ol> <p>Numerical keys are also used to input the numeric codes that may be required for arming, disarming, or used to activate specific functions.</p>
	Exits from the current menu and returns to Normal Operation mode
	Terminates commands and confirms data to be stored
	Used to browse through the menu: Scrolls up a list or moves the cursor
	Changes data

## Accessing the Installer Menus

To access the installer menus via the Agility keypad, follow this procedure:

- Press the  key to activate the keypad.  
Enter the installer code 0132 (default code).

---

**Note:** If the *Authorize Installer* system bit is defined as YES, a Grand Master code is required to authorize the installer to enter the programming mode. In this case the Grand Master code should be entered after the installer code via the *Grand Master menu* → *Activities* → *Authorize Installer*.

---

The following menu appears displaying a list of all the installer menus:

- 1) Programming
- 2) Testing
- 3) Activities
- 4) Follow Me
- 5) Clock
- 6) Event Log
- 7) Macro

Using the  keys to select the options.

## Programming Menu

All the system parameters are programmed by the installer via the programming menu. After accessing the installer menus, select the 1) *Programming* option. The following list appears:

1. System
2. Radio Devices
3. Codes
4. Communication
5. Audio
6. Exit

### 1. Programming: System Menu

The **System** menu provides access to parameters that are used for programming configuration settings applicable to the entire system. The **System** menu is divided into the following sub-menus:

1. Timers
2. Controls
3. Labels

- 4. Sounds**
- 5. Settings**
- 6. Service Information**
- 7. Firmware Update**

### **1.1 Timers**

The **Timers** menu contains parameters that specify the duration of an action.

#### **System: Timers**

Parameter	Default	Range
<b>Exit/Entry Delay 1</b>		
<b>Entry Delay 1</b>	30 sec	0-255 sec
Duration of entry delay 1 before the system is disarmed		
<b>Exit Delay 1</b>	45 sec	0-255 sec
Duration of exit delay 1 before the system is armed		
<b>Exit/Entry Delay 2</b>		
The amount of time before the system is armed/disarmed. Usually used to back door.		
<b>Entry Delay 2</b>	45 sec	0-255 sec
Duration of entry delay 2 before the system is disarmed		
<b>Exit Delay 2</b>	60 sec	0-255 sec
Duration of exit delay 2 before the system is armed		
<b>Bell Timeout</b>	04 min	01-90 min
Duration of the siren during alarm.		
<b>Bell Delay</b>	00 min	00-90 min
The time delay before a siren sound is produced after triggering an alarm.		
<b>AC Off Delay</b>	30 min	0-255 min
In the case of a loss of AC power, this parameter specifies the delay period before reporting the event or operating the Programmable Output. If the delay time is set to zero, there will be no delay period.		
<b>Jamming Time</b>	None	None, 10, 20 or 30 sec
Specifies the period of time that the system's receiver tolerates unwanted radio frequencies capable of blocking (jamming) signals produced by the system's transmitters. Once the specified time is reached, the system sends a report code to the monitoring station or activates a local siren, depending on the <i>Audible Jamming</i> system control.		
NONE: No jamming will be detected or reported.		

## System: Timers

Parameter	Default	Range
<b>RX Supervision</b>	3 hours	0-7 hours
Specifies how often the system expects to get a signal from the system's transmitters. If a signal from a zone is not received during the specified time the zone will be regarded as lost, the system will send a report code to the monitoring station, and the system status will be "Not Ready".		
<b>Notes:</b> 0 hours disables supervision It is recommended to set the supervision time to a minimum of 3 hours		
<b>TX Supervision</b>	058	0-255 min
Specifies how often a bi-directional wireless device generates a supervision request to the system.  If any of the accessories does not respond to the request, at least once, during the <b>RX Supervision</b> time, the system will regard the accessory as Lost.		
<b>Note:</b> The device will generate the supervision message according to the time defined.		
<b>Important:</b> The RX Supervision time should be higher than the Tx Supervision time in order to eliminate false lost event.		
<b>Redial Wait</b>	30 sec	0-255 sec
The number of seconds between attempts at redialing the same phone number.  Applies to both the <b>MS Retries</b> and <b>FM Retries</b> parameters.		
<b>Note:</b> Used for both PSTN and GSM.		
<b>More</b>		
<b>Swinger Limit Shutdown</b>	00	0-15 times
A swinger is a repeated violation of the same zone, often resulting in a nuisance alarm and usually due to a malfunction, an environmental problem, or the incorrect installation of a detector or sensor.  This parameter specifies the number of violations of the same zone reported during a single armed period, before the zone is automatically bypassed.		
<b>Note:</b> 00 to disables the swinger shutdown		
<b>No Activity</b>	00	0-99 hours
Determines the time limit for reception of signals from sensors used to monitor the activity of sick, elderly or disabled people. If no signal is received from a zone defined with the "No Activity" feature at least once within the defined time limit, a "no-activity" alert can be send to Follow Me destination, a local message can be heard and a report to Monitoring Station can be defined to be send.  Options: 0 =this parameter is inactive.		

**System: Timers**

Parameter	Default	Range
Last Exit Sound	00	0-255 seconds

Defines the last seconds of the Exit Time that the beep sound will change (main unit and keypads), indicating to the user that Exit Time is about to end.

**1.2 Controls**

The **Control** menu contains parameters that control specific system operations.

**System: Controls**

Parameter	Default
<b>Basic programming</b>	
<b>Quick Arm</b>	YES
<b>YES:</b> Eliminates the need for a user code when arming (Full or partial) the system by a keypad or 2-way remote control.	
<b>NO:</b> A valid user code is required for arming using a keypad or remote control.	
<b>Allow Bypass</b>	YES
<b>YES:</b> Permits zone bypassing by authorized system users after entering a valid user code.	
<b>NO:</b> Zone bypassing is NOT permitted.	
<b>Quick Status</b>	YES
<b>YES:</b> A user code is not required before pressing the status key/button on your wireless keypad or bi-directional remote control.	
<b>NO:</b> A user code is required to activate the status key.	
<b>False Code Trouble</b>	YES
<b>YES:</b> A false code report is sent to the monitoring station after five successive attempts at arming or disarming in which an incorrect user code is entered. No alarm sounds at the premises, but a trouble indication appears. The wireless keypad will be locked for 30 minutes.	
<b>NO:</b> A local alarm is sounded at the premises.	
<b>Siren Squawk</b>	YES
<b>YES:</b> Arming or disarming the system using a remote control, wireless keypad or a key-switch produces a brief "chirp" and activates the strobe as follows:	
<ul style="list-style-type: none"> <li>• One chirp indicates the system is armed (also when arming with a keypad).</li> <li>• Two chirps indicate the system is disarmed.</li> <li>• Four chirps indicate the system is disarmed after an alarm.</li> </ul>	
<b>NO:</b> No "chirp" is produced.	

## System: Controls

Parameter	Default
<b>Audible Panic</b>	NO
<b>YES:</b> The sirens operate when a "Police Alarm" is initiated at the keypad (if defined), the remote control or when a panic zone is activated.	
<b>NO:</b> No siren operation occurs during a "Panic Alarm," making the alarm truly "silent" (Silent Panic).	
<b>Note:</b> The system always transmits a panic report to the monitoring station.	
<b>Buzzer → Bell</b>	NO
<b>YES:</b> If an alarm occurs when the system is armed in the Stay Arm mode, a buzzer sounds for 15 seconds before the sirens operate.	
<b>NO:</b> An alarm in the Stay Arm mode causes sirens to operate simultaneously.	
<b>Audible Jamming</b>	NO
Relates to the <b>Jamming Time</b> parameter.	
<b>YES:</b> Once the specified time is reached, the system activates the siren and sends a report code to the monitoring station.	
<b>NO:</b> Once the specified time is reached the sirens do not operate.	
<b>Exit Beeps at Stay</b>	YES
Determines whether the system will sound beeps during exit time in Stay Arming.	
<b>YES:</b> Exit beeps will sound	
<b>NO:</b> Exit beeps will not sound	
<b>Forced Device Arming</b>	YES
<b>YES:</b> Arming a partition, using a remote control or key-switch can be performed with violated (not ready) zones in the system. Any violated (not ready) zone(s) in the partition will be bypassed automatically. The partition is then "force armed," and all intact zones are capable of producing an alarm.	
<b>NO:</b> The partition cannot be armed until all violated (not ready) zones are secured.	
<b>Arm Pre-warning</b>	YES
Related to auto Arm/Disarm operation.	
<b>YES:</b> For any partition(s) set up for Auto Arming, an audible Exit Delay (warning) countdown will commence 4.25 minutes prior to the automatic Arming. During this period, Exit Delay beeps will be heard.	
You can enter a valid User Code at any time during the countdown to delay the partition's automatic Arming by 45 minutes.	
When an "Auto-Arm" partition is disarmed, as described above, it can no longer be automatically armed during the current day.	
The extended 4.25 minutes warning does not apply to automatic Partial Arming.	

**System: Controls**

<b>Parameter</b>	<b>Default</b>
------------------	----------------

**NO:** Auto Arming for any programmed partition(s) takes place at the designated time. The programmed Exit Delay period and any audible signal occur as expected.

<b>Default Enable</b>	<b>YES</b>
-----------------------	------------

This option contains parameters that relate to what happens to the Installer, Sub-Installer and Grand Master codes if the Main Panel's DEFAULT Dip Switch 2 is in place when power to the Main Panel is switched off and then on. For more information regarding panel defaults refer to *Chapter 2, Dip Switch Setting*, see explanation of Dip Switch 2.

**YES:** The Installer, Sub-Installer and Grand Master codes will return to the original, factory default values.

**NO:** The Installer, Sub-Installer and Grand Master codes will **NOT** return to the original, factory default values by an unauthorized user.

<b>Main Button: Status-Y/Talk-N</b>	<b>YES</b>
-------------------------------------	------------

The Agility enables the MS to perform Listen-In and Talk functions in order to verify a cause of event or to guide someone in distress. The *Main Button: Status-Y/Talk-N* parameter determines the function of the button on the surface of the main unit to enable Listen-In and Talk.

**YES:** Status button – The system will relay the system status.

**NO:** Service call button – The system dials the Monitoring Station to establish 2-way communication.

<b>Quick Learn</b>	<b>YES</b>
--------------------	------------

Enables the button on the surface of the main unit to perform quick allocation of wireless devices. (See *Chapter 3 System Device Allocation: Manual Setup*)

**YES:** Quick learn mode is enabled. Long press on the main unit button will start Learn mode. The LEDs on the main unit will start flashing one after the other

**NO:** Quick learning mode is disabled. The main unit button is not in Learn mode.

**Advanced programming**

<b>Area</b>	<b>NO</b>
-------------	-----------

Changes the system operation to Area instead of Partition, which then changes only the operation of a common zone.

**YES:** When selected, the following points are relevant:

- A common zone will be armed after any partition is armed.
- A common zone will be disarmed only when all partitions are disarmed.

**NO:** When selected, the following points are relevant:

- A common zone will be armed only when all partitions are armed.
- A common zone will be disarmed when any partition is disarmed.

**System: Controls**

Parameter	Default
<b>Global Follower</b>	NO
<b>YES:</b> Specifies that all zones (that are programmed to follow an Exit/Entry Delay time) will follow the Exit/Entry Delay time of any armed partition.	
<b>NO:</b> Specifies that all zones (that are programmed to follow an Entry Delay time) will follow the Entry Delay time of only the partitions to which they are assigned.	
<b>Summer/Winter</b>	NO
<b>YES:</b> The system automatically sets its time of day clock one hour ahead in the spring (on the last Sunday in March) and one hour back in the Autumn (on the last Sunday in October).	
<b>NO:</b> No automatic time accommodation is made.	
<b>24 Hour Bypass</b>	NO
<b>YES:</b> It is possible for the user to bypass a 24-hour zone.	
<b>NO:</b> It is not possible for the user to bypass a 24-hour zone.	
<b>Technician Tamper</b>	NO
<b>YES:</b> It is necessary to enter the Installer Code to reset a Tamper alarm. Therefore, resetting a Tamper alarm requires the intervention of the alarm company. However, the system can still be set.	
<b>NO:</b> Correcting the problem resets a Tamper alarm, requiring no alarm company help.	
<b>Technician Reset</b>	NO
<b>YES:</b> It is necessary to enter the Installer Code to reset an alarmed partition after it has been disarmed. This requires the intervention of the alarm company.	
<b>Note:</b> Before the Ready LED can light all zones within the partition must be secured.	
<b>NO:</b> Once an alarmed partition is reset the Ready LED lights when all zones are secured.	
<b>Installer Tamper</b>	NO
<b>YES:</b> After a Tamper alarm, the system is not ready to arm. This requires the intervention of the alarm company.	
<b>NO:</b> After a Tamper alarm is restored the system is ready.	
<b>Low Battery Arm</b>	YES
<b>YES:</b> Allows arming of the system when a low battery condition is detected in the main unit.	
<b>NO:</b> Arming the system is disabled when a low battery condition is detected.	

**System: Controls**

Parameter	Default
<b>Siren Pre-Alarm</b>	NO
Specifies if the system will send a pre-alarm message to the siren while an entry delay starts.	
<b>YES:</b> The system sends a pre-alarm signal to the siren at the beginning of the entry delay. If the siren does not receive a cancellation signal from the system at the end of the entry time, the siren goes into alarm.	
<b>NO:</b> Pre-Alarm disabled	
<b>Bell 30/10</b>	NO
<b>YES:</b> The sirens cease to sound for 10 seconds after each 30 seconds of operation.	
<b>NO:</b> The sirens operate without interruption.	
<b>Fire Alarm Pattern</b>	NO
<b>YES:</b> During a fire alarm, the sirens produce a pattern of 3 short bursts followed by a brief pause.	
<b>NO:</b> During a fire alarm, the flow of sounds produced by the siren is a pattern of 2 seconds ON, then 2 seconds OFF.	
<b>IMQ</b>	NO
<b>YES:</b> Causes the following parameters to function as follows:	
<ul style="list-style-type: none"> <li>◆ <b>Auto Arm Bypass:</b> If there is an open zone during the Auto Arm process, the system will be armed, and a silent alarm will be activated (unless the open zone is closed).</li> <li>◆ A utility output defined as "Auto Arm Alarm" is activated.</li> <li>◆ A utility output defined as "Zone Loss Alarm" is activated</li> </ul>	
<b>NO:</b> Causes the following parameters to function as follows:	
<ul style="list-style-type: none"> <li>◆ <b>Auto Arm Bypass:</b> If the Auto Arm programming arms the system and there is an open zone during the auto arm, the system will bypass the open zones and arm the system.</li> <li>◆ A utility output defined as "Auto Arm Alarm" is deactivated.</li> <li>◆ A utility output defined as "Zone Loss Alarm" is deactivated.</li> </ul>	
<b>Disable Incoming Call</b>	NO
This parameter is used to disable all incoming calls trying to come in via the voice channel (PSTN or GSM).	
<b>YES:</b> Incoming calls from voice channel are disabled.	
<b>NO:</b> Incoming calls from voice channel are enabled.	
<b>Note:</b> Incoming data call via the GSM data channel is still enabled.	

## System: Controls

Parameter	Default
<b>Communication</b>	
<b>MS Enable</b>	YES
<b>YES:</b> Enables communication with the Central Station to report alarms, trouble, and supervisory events.	
<b>NO:</b> No communication with the Central Station is possible. Choose NO for installations that are NOT monitored by a Central Station.	
<b>Configuration Software Enable</b>	YES
<b>YES:</b> Enables communication between the alarm company and the system using the Configuration software. This enables modifying an installation's configuration, obtaining status information, and issuing Main Panel commands, all from a remote location.	
<b>NO:</b> Disables communication, as detailed above.	
<b>FM Enable</b>	YES
<b>YES:</b> Enables Follow-Me communication.	
If both the MS phones and the FM phones are defined, the system will first call the MS phones and then the FM phones.	
<b>NO:</b> Disables Follow-Me communication.	
<b>EN 50131 programming</b>	
<b>Authorize Installer</b>	NO
This option limits the Installer and Sub-installer authorization to access the programming menu.	
<b>YES:</b> A Grand Master code is required to authorize the installer to enter the programming mode for 1 hour.	
<b>NO:</b> The Installer does not need an authorization code.	
<b>Override Trouble</b>	YES
Specifies if the system/partition can be armed when there is a fault in the system.	
<b>YES:</b> The system will arm even if there is a fault in the system.	
<b>NO:</b> When the user starts the arming process and there is a system-fault, the user must confirm that he is aware of all faults before continuing with the Arming process.	
This is done via the User menu→Activities→Bypass Trouble.	
The system will not arm during forced arming if a fault occurred in the system	

**System: Controls**

Parameter	Default
<b>Restore Alarm</b>	NO
<b>YES:</b> The user must confirm that he is aware that alarm occurred in the system before rearming the system. The system will be in "Not Ready" status until he confirms the alarm. This is done via the User menu → Activities → Advanced → Restore Alarm.	
<b>NO:</b> The user does not need to confirm the alarm before rearming the system.	
<b>Mandatory Event Log</b>	NO
<b>YES:</b> Only mandatory events (specified in the EN standard) will be displayed in the Event Log.	
<b>NO:</b> All the events will be displayed in the Event Log.	
<b>Restore Troubles</b>	NO
<b>YES:</b> The user must manually confirm the restoral of each trouble to a normal condition. This is done via the User menu → Activities → Advanced → Restore Troubles.	
<b>NO:</b> The restoral report of each trouble is automatic .	
<b>Exit Alarm</b>	YES
<b>YES:</b> A violated zone outside the exit route will generate an alarm during the exit time. A report to the monitoring station for arming the system is sent at the beginning of the arming procedure.	
<b>NO:</b> A violated zone outside the exit route will cancel the arming process. A report to the monitoring station is send at the end of a successful arming procedure.	
<b>Entry Delayed Alarm</b>	NO
This feature is used to reduce false alarm reports to the MS.	
<b>YES:</b> The report to the MS and the siren alarm will be delayed for 30 seconds or until the end of the predefined entry delay (the shorter time of the two) following a violation of a zone outside the <b>entry</b> route.	
<b>NO:</b> A violated zone outside the <b>entry</b> route will generate an alarm during the entry time and a report will be sent to the MS.	
<b>20 Minutes Signal</b>	NO
<b>YES:</b> Prior to arming the system, the system will check for zones that did not send a signal for more than 20 minutes. These zones will be regarded as not ready. A partition assigned with a not ready zone cannot be armed.	
<b>NO:</b> Prior to arming, the system will not check whether a zone did not send a signal for more than 20 minutes.	

## System: Controls

Parameter	Default
<b>Attenuation</b>	NO
<b>YES:</b> The Agility receiver will be attenuated by 6 dB during the communication test.	
<b>NO:</b> The Agility receiver works in normal operation mode.	
<b>DD243 programming</b>	
<b>Bypass Exit/Entry</b>	YES
<b>YES:</b> It is possible for the user to bypass an Exit/Entry zone.	
<b>NO:</b> An Exit/Entry zone cannot be bypassed.	
<b>Entry Disable</b>	NO
<b>YES:</b> The alarm confirmation process will be disabled when the entry time starts.	
<b>NO:</b> The alarm confirmation process will start when the entry time starts.	
<b>Route Disable</b>	NO
<b>YES:</b> The panel disables the entry route zones (EX/EN, EX (OP)/EN, followers and Final Exit) from participating in the alarm confirmation process when the entry time starts.	
<b>Note:</b> Sequential confirmation can still be established from two confirmed zones, located off the entry route.	
<b>NO:</b> The entry route zones will participate in the alarm confirmation process when the entry time starts.	
<b>Installer Reset Confirmation</b>	NO
<b>YES:</b> An installer reset confirmation is required in order to reset the system after a confirmed alarm. The system cannot be armed until an Installer Reset Confirmation is performed. The reset can be done by entering the Anti code or entering the installation mode or by performing a "Installer reset" from the keypad.	
<b>NO:</b> Any means can be used to arm or disarm the system (keypad, remote phone operation etc.).	
<b>Key Switch Lock</b>	NO
<b>YES:</b> Only a Latched Key Switch zone can arm or disarm the system.	
<b>Note:</b> When the system has more than 1 zone defined as Latch Key Switch, the arm/disarm operation will occur only after all these zones are armed or disarmed.	
<b>NO:</b> Any means can be used to arm or disarm the system (keypad, remote phone operation etc.).	

**System: Controls**

Parameter	Default
<b>Entry Disarm</b>	NO
Determines if the system's disarming depends on the entry time.	
<b>YES:</b> Only a remote control can disarm the system during the entry time.	
<b>Note:</b> The system can not be disarmed with a remote control while the system is armed.	
<b>NO:</b> The system can be disarmed during any time using any disarming device.	
<b>CP-01 programming</b>	
<b>Exit Restart</b>	NO
This parameter is used to define if an exit time shall restart one additional time while an entry/exit zone is tripped twice during exit time.	
<b>YES:</b> Exit time will restart for one time only when an entry/exit zone is tripped during exit time.	
<b>NO:</b> Exit time will not be affected if an entry/exit zone is tripped during exit time.	
<b>Auto Stay</b>	NO
This parameter is used to define the system's arming mode when using a keypad and no exit/entry zone is tripped during exit mode.	
<b>YES:</b> If no exit/entry zone is tripped during exit time the system will be armed in STAY mode.	
<b>NO:</b> If no exit/entry zone is tripped during exit time the system will be armed in Away mode.	
<b>Exit Error</b>	NO
This parameter is used to define what will happen if an Exit/Entry zone is left open at the end of the exit time.	
<b>YES:</b>	
<ul style="list-style-type: none"> <li>◆ Local alarm will be activated at the end of the exit time.</li> <li>◆ Exit error report will be sent to the monitoring station together with an alarm report if the system has not been disarmed during the entry time that immediately started after the exit time expiration.</li> </ul>	
<b>NO:</b>	
<ul style="list-style-type: none"> <li>◆ No local alarm will be activated at the end of the exit time.</li> <li>◆ Only an alarm report will be sent to the monitoring station if the system has not been disarmed during the entry time that immediately started after the exit time expiration</li> </ul>	

## System: Controls

Parameter	Default
<b>3 Minute Bypass</b>	NO

**YES:** Bypasses all zones automatically for 3 minutes when power is restored to an "unpowered" system.  
**NO:** No bypassing occurs.

## 1.3 Labels

You can rename the labels that identify the system and partitions by changing the default labels (**Partition 1**, **Partition 2** and so on) to, for example, **The Jones's**, **Sales Dept**, or **Mastr Bedr** as appropriate.

Labels that can be renamed:

Parameter	Default	Range
<b>System</b>	<b>Security System</b>	Any 16 characters
Edits the global (system) label		
<b>Partition 1/2/3</b>	Partitions 1 through 3	Any 16 characters
Edits partition labels		

To rename labels using the keypad keys to produce characters see the table below:

Key	Data Sequence
1	1 . , ' ? ! " - ( ) @ / : _ + & * #
2	2 a b c A B C
3	3 d e f D E F
4	4 g h i G H I
5	5 j k l J K L
6	6 m n o M N O
7	7 p q r s P Q R S
8	8 t u v T U V
9	9 w x y z W X Y Z
0	0
 	Use these keys to toggle forwards and backwards through all the available characters.

## 1.4 Sounds

The **Sounds** menu contains parameters that enable you to set the sound(s) that will be produced by the system after the following system events:

### **System: Sounds**

Parameter	Default	Range
<b>Tamper Sound</b>	BELL/A Sil/D	1 to 6
Sets the sound(s) produced by a Tamper violation according to the following options:		
<ul style="list-style-type: none"> <li>♦ <b>Silent</b></li> <li>♦ <b>Bell</b> (External/Internal siren)</li> <li>♦ <b>Buzzer (main unit)</b></li> <li>♦ <b>Bell + Buzzer</b></li> <li>♦ <b>Bell/A Buzzer/D</b>: Bell when system armed, Buzzer when system disarmed</li> <li>♦ <b>Bell/A S/Disarm</b>: Bell when system armed, Silence when system disarmed</li> </ul>		
<b>Local Speaker Alarm Volume</b>	Level 5	0-5
Sets the main unit's internal speaker Alarm volume. The volume ranges between 0 (silent) to 5 (Max volume). After setting/changing the volume, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.		
<b>Local Speaker Squawk Volume</b>	Level 5	0-5
Sets the main unit's internal speaker Squawk volume. The volume ranges between 0 (silent) to 5 (Max volume). After setting/changing the volume, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.		
<b>Exit/Entry Beeps Volume</b>	Level 3	0-5
Determines the volume of the beeps sounded from the main unit during the Exit/Entry times.		
<b>Speaker Messages Volume</b>	Level 2	0-4
Determines the volume of the messages sounded from the main unit or the Listen-In and Talk unit.		

## 1.5 System Settings

This option allows to set the system settings as language, specific standardization and more.

### System: Settings

Parameter	Default	Range
<b>Default Panel</b>		
Restores programming options to factory defaults.		
The Panel Default option will be followed by questions regarding the defaults of the labels and erasing wireless devices. Use  to select your option.		
<b>Erase Wireless Device</b>		
Erase wireless devices without changing the system current programmed parameters .		
<b>Language</b>		
Sets the system language (Email, SMS and keypad language)		
<b>Standards</b>		
EN 50131	NO	
Sets the panel programming options in compliance with EN standards. (See Appendix D)		
DD243	NO	
Sets the panel programming options in compliance with DD243 standards.		
CP-01	NO	
Sets the panel programming options in compliance with CP-01 standards.		

## 1.6 Service Information

The **Service Information** menu enables you to insert information accessible to the system's users of the alarm company from whom the service is obtained.

### System: Service Information

Parameter	Default	Range
Name	Any 16 characters	
Enables you to insert and/or edit the name of the alarm company from whom service may be obtained. The information can be viewed by the user using the wireless keypad.		
Phone	Any 16 characters	
Enables you to insert and/or edit the service phone number. The information can be viewed by the user using the wireless keypad		

## 1.7 Firmware Update

The **Agility** enables you to remotely upgrade the main unit firmware versions via IP or GPRS channels. Under the **Firmware Update** menu you need to define the location of the upgrade file. The request to start the remote upgrade can be done from the Agility keypad or from the Agility Configuration Software. For detailed information refer to the *Remote Software Upgrade* instruction guide.

### System: Firmware Update

Parameter	Default	Range
<b>Server IP</b>	192.114.175.43	
Enter the IP address of the router/gateway where the upgrade file is located.		
<b>Server Port</b>	80	
Enter the port on the router/gateway where the upgrade file is located.		
<b>File Path</b>		
Enter the upgrade file name. For example: /Agility/0UK/cpcp.bin		
Please contact Customer Support services for the file name parameters.		

## 2. Programming: Radio Devices Menu

The **Radio Devices** menu provides access to sub-menus that are used for programming, defining and editing each of the system's wireless devices. The **Radio Devices** menu is divided into the following sub-menus:

1. Allocation
2. Modification
3. Identification

### 2.1 Allocation

Each wireless device must be identified to the system receiver before its parameters can be configured. See *Chapter 3* for further information on the allocation procedures.

### 2.2 Modification

The modification menu is used to change the values of the parameters configured by the system for each wireless device. The modification menu is divided into the following submenus:

1. Zones
2. Remote Controls (Keyfobs)
3. Keypads
4. Sirens
5. I/O Expanders

---

**Note:** This list varies according to the devices that have been allocated to the system. Only devices that have been allocated can be configured or modified by the installer.

---

#### 2.2.1 Zones

The **Zones** menu is divided into the following sub-menus:

- ◎ Parameters
- ◎ Alarm (Sequential) Confirmation
- ◎ Soak Test
- ◎ Zone Crossing

#### Parameters

---

**Note:** The parameters displayed, vary according to the type of zones connected to the system.

---

#### Zones: Parameters

Parameter	Default	Range
Label	Zone 01/02/03/ ...	Any characters

A label identifies the zone in the system. Up to 16 characters).

**Zones: Parameters**

Parameter	Default	Range
<b>Serial Number</b>		
The internal ID number of the zone. Each wireless device has its own unique ID number. Placing ID 0000000000 will delete the zone.		
<b>Partition</b>		
The partition (1 to 3) assignment for each zone.		
<b>Type</b>		
Each zone can be defined as one of the following types:		
<b>Not Used</b>		
Disables a zone. All unused zones should be given this designation.		
<b>Exit/Entry 1</b>		
Used for Exit/Entry doors. Violated Exit/Entry zones do not cause an intrusion alarm during the <b>Exit/Entry Delay</b> . If the zone is not secured by the end of the delay expires it will trigger an intrusion alarm.		
To start an arming process, this zone should be secured. When system is armed, this zone starts the entry delay time.		
<b>Exit/Entry 2</b>		
Same as above, except that the Exit/Entry 2 time period applies.		
<b>Exit(Op)/Entry 1</b>		
Used for an Exit/Entry door. This zone behaves as described in the <b>Exit/Entry 1</b> parameter, shown above, except that, if faulted, the arming process is <b>not</b> prevented. To avoid an intrusion alarm, it must be secured before the expiration of the <b>Exit Delay</b> period.		
<b>Exit(Op)/Entry 2</b>		
Same as above, except that the Exit (Op)/Entry 2 time period applies.		
<b>Entry Follower</b>		
Usually assigned to motion detectors and to interior doors protecting the area between the entry door and the system.		
This zone(s) causes an immediate intrusion alarm when violated unless an Exit/Entry zone was violated first. In this case, Entry Follower zone(s) will remain bypassed until the end of the Entry Delay period.		

## Zones: Parameters

Parameter	Default	Range
<b>Intruder (Instant)</b>		
	Usually intended for non-exit/entry doors, window protection, shock detection, and motion detectors.	
Causes an immediate intrusion alarm if violated after the system is armed or during the Exit Delay time period.		
	When Auto Arm and Pre-Warning are defined, the instant zone will be armed at the end of the Pre-Warning time period.	
<b>Interior + Exit/Entry 1</b>		
	Used for Exit/Entry doors, as follows:	
	<ul style="list-style-type: none"> <li>• If the system is armed in the Away (Full Arm) mode, the zone(s) provide a delay (specified by Exit/Entry 1) allowing entry into and exit from an armed premises.</li> <li>• If the system is armed in the Stay mode, the zone is bypassed.</li> </ul>	
<b>Interior + Exit/Entry 2</b>		
	Same as the <b>I + Exit/Entry 1</b> parameter, described above, but the Exit/Entry 2 time period is applicable.	
<b>Interior + Exit(Op)/Entry 1</b>		
	Used for an exit/entry door that, for convenience, may be kept open when the system is being armed, as follows:	
	<ul style="list-style-type: none"> <li>• In Away (Full Arm) mode behaves as an <b>Exit (Op)/Entry 1</b> zone.</li> <li>• In Stay mode, the zone will be bypassed.</li> </ul>	
<b>Interior + Exit(Op)/Entry 2</b>		
	Same as the <b>I + Exit (Op)/Entry 1</b> parameter, described above, but the Exit/Entry 2 time period is applicable.	
<b>Interior + Entry Follower</b>		
	Generally used for motion detectors and/or interior doors (for example, foyer), which would have to be violated after entry in order to disarm the system, as follows:	
	<ul style="list-style-type: none"> <li>• In Away (Full Arm) mode behaves as an Entry Follower zone.</li> <li>• In Stay mode, the zone will be bypassed.</li> </ul>	
<b>Interior + Intruder (Instant)</b>		
	Usually intended for non-exit/entry doors, window protection, shock detection and motion detectors.	
	<ul style="list-style-type: none"> <li>• In Away (Full Arm) mode behaves as an Intruder (instant) zone.</li> <li>• In Stay mode, the zone is bypassed.</li> </ul>	

**Zones: Parameters**

Parameter	Default	Range
<b>Entry Follower + Stay</b>		
Assigned to motion detectors and to interior doors protecting the area between the entry door and the keypad, as follows:		
• In Away (Full Arm) mode behaves like an Entry Follower Zone. • In Stay mode behaves like an Exit/Entry 1 zone.		
<b>24 Hours</b>		
Usually assigned to protect non-movable glass, fixed skylights, and cabinets (possibly) for shock detection systems.		
A violation of such a zone causes an instant intrusion alarm, regardless of the system's state.		
<b>Fire</b>		
For smoke or other types of fire detectors. This option can also be used for manually triggered panic buttons or pull stations (if permitted), as follows: If violated, it causes an immediate fire alarm, fire report to the monitoring station.		
<b>Panic</b>		
Used for external panic buttons and wireless panic transmitters. If violated, an immediate panic alarm is sounded (if the zone sound is not defined as silent or Audible Panic system control is enabled), regardless of the system's state and panic report is send to the monitoring station. An alarm display will not appear on the keypads.		
<b>Special</b>		
For external auxiliary emergency alert buttons and wireless auxiliary emergency transmitters. If violated, an immediate auxiliary emergency alarm is sounded, regardless of the system's state and report is sent to the monitoring station.		
<b>Tamper</b>		
For tamper detection. This zone operates the same as 24 hours zone, but it has a special reporting code.		
<b>Note:</b> For this zone type the zone sound is determined according to the Tamper Sound defined under System → Sound → Tamper		
<b>Water (Flood)</b>		
For flood or other types of water detectors. This zone operates the same as 24 hours zone, but it has a special flood report code. (See <i>Appendix A: Report Codes</i> )		

## Zones: Parameters

Parameter	Default	Range
<b>Gas</b>		
For Gas (natural gas) leak detector. This zone operates the same as 24 hours zone, but it has a special gas report code. (See <i>Appendix A: Report Codes</i> )		
<b>CO</b>		
For CO (Carbon Monoxide) gas detectors. This zone operates the same as 24 hours zone, but it has a special CO report code. (See <i>Appendix A: Report Codes</i> )		
<b>High Temperature</b>		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code. (See <i>Appendix A: Report Codes</i> )		
<b>Low Temperature</b>		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code. (See <i>Appendix A: Report Codes</i> )		
<b>Technical</b>		
This zone operates the same as 24 hours zone, its report code should be manually set according to the relevant detector connected to the zone.		
<b>Final Exit</b>		
Zones of this type must be the last detector to be activated on exit or the first detector to be activated on entry.  When arming the system, the related partition arms 10 seconds after this zone is closed, or opened and then closed. After it is triggered once, the zone acts as an exit (open)/entry 1 zone.		
<b>Exit Termination</b>		
This type of zone is used to avoid a false alarm by acting like an Exit (OP)/Entry zone.  When triggered (after arming the system and closing the door <b>or</b> opening the door, arming the system, and closing the door), the system's Exit Delay time period will be shortened to 3 seconds.  When you re-open the door, the entry time restarts.		
<b>UO Trigger</b>		
For a device or zone, which if violated at any time triggers a previously programmed Utility Output, capable of activating an external indicator, relay, appliance, and so on.		

**Zones: Parameters**

Parameter	Default	Range
<b>Day</b>		

Usually assigned to an infrequently used door, such as an emergency door or a movable skylight. Used to alert the system user if a violation occurs during the disarmed period (trouble by day; burglary at night), as follows:

- With the system armed (either Away or Stay), the zone acts as an instant zone. A violation of this zone after the system is armed or during the Exit Delay time period causes an immediate intrusion alarm.
- With the system disarmed, a violation of this zone attempts to alert the user by causing the  (Trouble) LED to flash rapidly. This directs the user to view the system's status.

Optionally, such a violation can be reported to the Monitoring Station as a Zone Trouble.

**Pulsed Key Switch**

Connect an external momentary action key switch to any zone given this designation. This zone will arm/disarm the partitions assigned to it.

**Pulsed Key Switch Delayed**

Used to apply the Exit/Entry Delay 1 parameter to the Pulsed Key Switch zone.

**Latched Key Switch**

Connect an external SPST latched (non-momentary) key switch follows:

- After arming one or more partitions using the key switch and then disarming using the keypad, the related partitions will be disarmed. In order to arm the partition using the key switch again, turn the key to the disarm position and then to the arm position.
- If a key switch latch is assigned to more than one partition and one of the partitions is armed by using the keypad (the key switch stays in the disarm position), then:
  - When changing the position of the key switch to the arm position, all the disarmed partitions, which belong to this key switch, will be armed.
  - When turning the key switch to the disarm position, all the partitions will be disarmed.

**Latched Key Switch Delay**

Used to apply the Exit/Entry Delay 1 parameter to the latched key switch zone.

## Zones: Parameters

Parameter	Default	Range
<b>Sound</b>	Bell+Buzzer	
Contains parameters that enable you to program the sound produced when a system zone triggers an alarm for the time defined under the Bell Time Out parameter.		
<b>Silent</b>		
Produces no sound		
<b>Bell</b>		
Activates the wireless sirens (internal or external) and alarm from the main unit assigned to the partitions of the zone.		
<b>Buzzer (main unit)</b>		
Activates the internal buzzer on the main unit.		
<b>Bell + Buzzer</b>		
Activates the wireless sirens and siren on the main unit simultaneously.		
<b>Bell/Arm Buzzer/Disarm</b>		
In a case of alarm, the following occurs:		
<ul style="list-style-type: none"> <li>• In Away mode (Full Arm) the wireless siren will operate.</li> <li>• In Disarm mode, only the buzzer on the main unit will operate.</li> </ul>		

## Advanced programming

<b>Chime</b>	None
--------------	------

The **Chime** parameter is used as an audible indication to a zone violation while the system is Disarmed. Define which sound occurs when violated:

Options:

- None
- Buzzer (Main unit)
- Chime Sound 1
- Chime Sound 2
- Chime Sound 3
- Zone message

## Controls

### Supervision

Choose which zone will be supervised by the system receiver according to the time defined under the timer RX Supervision. (See *page 4-4*)

**Zones: Parameters**

Parameter	Default	Range
<b>Forced Arming Y/N</b>		
	This option enables or disables the use of forced arming for each of the system's zones, as follows:	
	<ul style="list-style-type: none"> <li>♦ If forced arming is enabled for a particular zone, it allows the system to be armed even though this zone is faulty.</li> <li>♦ When a zone(s) enabled for forced arming is faulted, the ✓ LED blinks during the disarm period.</li> <li>♦ After arming, all zones enabled for forced arming are bypassed at the end of the <b>Exit Delay</b> time period.</li> <li>♦ If a faulted zone (one enabled for force arming) is secured during the armed period, it will no longer be bypassed and will be included among the system's armed zones.</li> </ul>	
<b>No Activity</b>		Y/N
	Determines whether the zone participates in the No Activity function. The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people. See Timer "No Activity" on page 4-4.	
<b>LED Enable Y/N</b> (Only for 2 Way PIR and 2 Way WatchOUT)		Y/N
	Defines the LED operation mode.	
YES: Detector's LED activated		
NO: Detector's LED deactivated		
<b>Abort Alarm</b>		Y/N
	This parameter defines whether a zone alarm report to the monitoring station will be immediate or delayed:	
YES: A report to the MS will be delayed according to the Abort Time Delay parameter (Communication→MS→MS Times→Abort Alarm).		
Note: If a valid User Code is entered to reset the alarm within the cancel delay time (Communication→MS→MS Times→Cancel Report), a cancel report alarm code will be sent to the Monitoring Station.		
NO: A report to the MS will be sent immediately.		
<b>Detection Mode</b> (Only for 2 Way Detectors)		Normal
<ul style="list-style-type: none"> <li>♦ Fast (Walk Test): When the detector is in disarm it will transmit after each detection</li> <li>♦ Normal (Default): When the detector is in disarm, there will be 2.5 minutes dead time between detection transmissions</li> </ul>		
<b>Note:</b> For both options, when the detector is armed it will transmit after each detection.		

## **Zones: Parameters**

Parameter	Default	Range
-----------	---------	-------

### **Sensitivity** (Only for 2 Way PIR and 2 Way WatchOUT)

Defines the PIR Sensitivity of the detector.

- ♦ Low
- ♦ Medium (2 Way WatchOUT)
- ♦ High
- ♦ Maximum (2 Way WatchOUT)

## **Alarm Confirmation**

The Alarm Confirmation menu enables to define protection against false alarms and will be used for alarm verification.

## **Zones: Alarm Confirmation**

Parameter	Default	Range
-----------	---------	-------

### **Confirm Partition**

Defines which partitions will be defined for alarm sequential confirmation.

Each confirmed partition has a separate timer, which is equivalent to the confirmation time defined in "Confirmation Time Window".

A confirmed intruder alarm will be reported if two separate alarm conditions are detected in the same confirmed partition, during the confirmation time.

### **Confirm Zones**

Define which zones will be defined for alarm sequential confirmation.

When the first zone goes into alarm the system transmits the first zone alarm. When the second zone goes into alarm, during the confirmation time, the panel transmits the zone alarm and the Police code.

#### **Notes:**

1. A confirmed zone will be part of the sequential confirmation only if the partition in which the alarm occurs is defined as confirmed partition as well.
2. Any Code can reset a confirmed alarm.
3. If the first zone is violated and not restored until the end of the confirmation time (no second zone alarm), than this zone will be excluded from the confirmation process until the next arming.

## **Soak Test**

The Soak Test feature is designed to allow false alarming for predefined detectors to be omitted from the system, while any alarms generated are displayed to the user for reporting to the MS. This is especially useful if Police response withdrawal is being threatened and a particular zone is causing unidentified problems.

Each zone can be placed on Soak Test. Any zone placed in the Soak Test list is omitted from the system for 14 days and is automatically reinstated after that time if NO alarms have been generated by it.

If a zone in the Soak Test list has an alarm during the 14-day period, the keypad indicates to the user that the test has failed. After the user looks at the View Fault option, the fault message will be erased. This will be indicated in the event log, but no alarm will be generated. The alarmed zone's 14-day Soak Test period is then reset and restarted.

### **Zone Crossing**

The **Zone Crossing** menu is used for additional protection from false alarms and contains parameters that enable you to link together two related zones. Both must be violated within a designated time period (between 1 and 9 minutes) before an alarm occurs.

This type of linking is used with motion detectors in *hostile* or *false-alarm prone* environments. **Default:** No cross zoning

---

#### **Zones: Zone Crossing**

---

##### **Parameter**

---

###### **1<sup>st</sup> Zone**

The 1<sup>st</sup> zone of a pair of zone defined for zone crossings.

###### **2<sup>nd</sup> Zone**

The 2<sup>nd</sup> zone of a pair of zone defined for zone crossings.

###### **Time**

The amount of time allowed between the triggering events for both zones to be considered a valid violation

---

##### **Correlation Type**

Determine how the Agility will process violations of the paired zones.

- ♦ Not correlate: Temporarily disables any associated zone pairings
- ♦ Ordered correlate: Effects an alarm so the first listed zone is tripped before the second
- ♦ Not ordered correlate: Affects an alarm in which either zone in the pair may be tripped first. If this case, the specified zone order (1st, 2nd) has no bearing on the alarm activation.

---

**Note:** Zones crossed within themselves are valid pairs. They need to register a violation twice to trigger the alarm. This process is known as Double Knock.

---

## 2.2.2 Remote Controls

The **Remote Controls** menu defines the operation of the remote controls. Up to 8 remote controls can be assigned to the system. The system supports 2 types of remote controls:

- One Way Remote Controls (4 button)
- Two Way (bidirectional) Remote Controls (8 button)

### Parameters

The programming options under the parameters menu vary according to the type of the remote control.

#### One Way Remote Control Parameters

Each one way remote control consists of 4 buttons, and each button can be programmed to a different mode of operation.

#### Remote Controls Parameters: One Way Remote Controls

##### Parameter

##### Label

A label identifying the user of the remote control.

##### Serial Code

The internal ID number of the remote control. Each wireless device has its own unique serial number. Placing ID 0000000000 will delete the remote control.

##### Partition

Assign the relevant partitions for the selected remote control.

##### Button 1 (✖)

Set the operation of button 1 of the remote control from the following options:

- ♦ None: Button disabled.
- ♦ Arm: The button is used for Away (Full) arming of the remote control's partitions.
- ♦ Stay: The button is used for Stay (Home) arming of the remote control's partitions.

##### Button 2 (✖)

Set the operation of button 2 of the remote control from the following options:

- ♦ None: Button disabled.
- ♦ Disarm: The button is used for disarming its assigned partitions.

##### Button 3

Set the operation of button 3 (Small blank button) of the remote control from the following options:

- ♦ None: Button disabled.
- ♦ Panic: The button is used to send a panic alarm.
- ♦ UO Control (1-20): The button is used to operate a single Utility Output.

**Remote Controls Parameters: One Way Remote Controls****Parameter****Button 4**

Set the operation of button 4 (Large blank button) of the remote control from the following options:

- ♦ None: Button disabled.
- ♦ Arm: The button is used for Away (Full) arming of the remote control's partitions.
- ♦ Stay: The button is used for Stay (Home) arming of the remote control's partitions.
- ♦ UO Control (1-20): The button is used to operate a Utility Output.

**Two Way Bi-directional Remote Controls**

The bi directional remote control is an 8 button rolling code wireless transmitter designed for remote system operation. Being bi-directional enables each command that is sent to the panel to receive a reply status indication back from the panel using its 3 color LEDs and internal buzzer siren. For higher security, commands can be defined to be activated with a 4 digit PIN code.

**Remote Controls Parameters: 2 Way Remote Control****Parameter****Label**

A label identifying the user of the remote control.

**Serial Code**

The internal ID number of the remote control. Each wireless device has its own unique serial number. Placing ID 0000000000 will delete the remote control.

**Partition**

Assign the relevant partitions for the selected remote control.

**PIN Code**

4 digit PIN code used for higher security when sending commands from the remote control. The code can be comprised from digits 1,2,3,4.

**Note:** The use of the PIN code depends on the control *Quick UO* or system control *Quick Arm*

**Panic Function**

Define whether sending panic alarm from the remote control is permitted. If permitted, pressing on keys  and  simultaneously for 2 seconds on the will send a panic alarm.

**UO Key 1/2/3**

Each remote control can activate up to 3 outputs. Assign to each of the keys 1-3 the relevant output.

## Controls

The Controls menu options are used for both types of remote controls.

### **Remote Controls: Controls**

#### Control

<b>Instant Arm</b>	NO
--------------------	----

**YES:** Away arming from any remote control will be instant.

**NO:** Away arming from any remote control will be delayed, following exit delay 1.

<b>Instant Stay</b>	NO
---------------------	----

**YES:** Stay arming from any remote control will be instant.

**NO:** Stay arming from any remote control will be delayed, following exit delay 1.

<b>Disarm + Code</b> (For 2 Way Remote Controls)	NO
--	----

Defines if a PIN code is required to perform the disarm operation while using any of the bidirectional remote controls.

#### Parent Control

The Parent Control option is used to monitor the activity of children. This option allows you to monitor when the children arrive home and disarm the system or when they arm the system in Away, using a remote control or the keypad. With each activation/deactivation of the system a message is sent to a specified Follow Me number.

After selecting this option, using the  key, define which of the remote controls are authorized with this feature and which are not.

### **2.2.3 Keypads**

The system can support up to 3 wireless keypads.

For detailed information regarding the operation of the keypads refer to the instructions supplied with the product.

#### Parameters

### **Keypads: Parameters**

Parameter	Default	Range
<b>Label</b>		
A label identifying the keypad		
<b>Serial Code</b>		
The internal ID number of the keypad. Each wireless device has its own unique serial number. Placing ID 000000000000 will delete the remote keypad.		

**Keypads: Parameters**

Parameter	Default	Range
<b>Emergency Keys</b>	YES	YES/NO

Defines whether the following keys will operate as emergency keys:

- ♦ Keys  and  and 

<b>Function Key</b>	Panic
---------------------	-------

Defines the operation of the   keys for each keypad.

- ♦ Disable: Keys disabled.
- ♦ Panic: Send a panic alarm to the monitoring station.
- ♦ MS Listen-In & Talk: The system dials the Monitoring Station to establish 2-way communication.

**UO Control**

Assign outputs that will be activated by a long press on keys    on the bidirectional keypad.

**Notes:**

Outputs can be assigned only if I/O is assigned to the system.

Each keypad can activate different outputs.

Only outputs defined as *Follow Code* can be activated by the keypad keys

**Controls**

The Controls menu defines programming options that are used for all keypads.

**Keypads: Controls**

Parameter	Default	Range
<b>RF Wake-up</b>	NO	

Determines whether the system can wake the keypad up during exit/entry times or when failing to set the system.

**YES:** The system wakes the keypad.

**NO:** The system cannot wake up a keypad. Use this option to save battery life. (Default)

**2.2.4 Sirens**

The **Sirens** menu enables to define all parameters of external and internal wireless sirens that can be connected to the system. Up to 3 sirens can be added to the system.

For detailed information regarding the operation of the sirens refer to the instructions supplied with the product.

## Wireless Device: Sirens

Parameter	Default	Range
<b>Label</b>		
A label identifying the siren.		
<b>Serial Code</b>		
The internal ID number of the sirens. Each wireless device has its own unique serial number. Placing ID 0000000000 will delete the siren.		
<b>Partition</b>		
Assign the partitions that will effect the sounder operation.		
<b>Supervision</b>	YES	
Choose if the siren will be supervised or not.		
<b>Volume</b>	9	0-9
Define the volume of the sounder for the following scenarios in the system.		
<b>Alarm Volume</b>	9	0-9
The sound volume produced during an alarm (0 indicates silence).		
<b>Squawk Volume</b>	9	0-9
The sound volume produced during squawk sounds (0 indicates silence).		
<b>Exit/Entry Volume</b>	9	0-9
The sound volume produced during exit/entry time. (0 indicates silence).		
<b>Strobe (External siren only)</b>		
Defines the parameters for the strobe of the external siren.		
<b>Strobe Control</b>		
Defines the Strobe operation mode:		
<ul style="list-style-type: none"> <li>♦ Always off: The strobe is deactivated</li> <li>♦ Follow Bell: The strobe is activated when the siren bell is triggered</li> <li>♦ Follow Alarm: The strobe is activated when an alarm event occurs in the system</li> </ul>		
<b>Strobe Blink</b>	40	
Defines the number of times that the strobe will blink in a minute:		
<ul style="list-style-type: none"> <li>♦ 20 times per minute</li> <li>♦ 30 times per minute</li> <li>♦ 40 times per minute</li> <li>♦ 50 times per minute</li> <li>♦ 60 times per minute</li> </ul>		
<b>Strobe Arm Blink</b>	05	00-20
Defines the time that the strobe will blink when the system is armed.		

## 2.2.5 I/O Wireless Expander

The **Wireless Input/Output Expander** is a self powered device enabling system control of additional 4 wired zones and has home automation capabilities. With the I/O Expander the system can control 4 outputs and 16 home automation units employing the X10 protocol.

### Wired Zones

The 4 inputs on the I/O Expander are regarded as zones 33-36 in the system.

#### I/O Expander: Wired Zones

Parameter	Default	Range
<b>Label</b>		
A label identifies the zone in the system. (up to 16 characters).		
<b>Partition</b>	1	
The partitions assignment for each zone.		
<b>Type</b>	Intruder	
Contains parameters that enable you to program the zone type for any zone. Refer to the list of options for the Zone Type on page 4-19.		
<b>Sound</b>	Bell	
Contains parameters that enable you to program the sound produced when a system zone triggers an alarm for the time defined under the Bell Time Out parameter. Refer to the list of options for the Zone Sound on page 4-24.		
<b>Advanced programming</b>		
<b>Chime</b>	None	
The Chime parameter is used as an audible indication to a zone violation while the system is Disarmed. When violated, the main unit can sound one of the 5 available chime options.		
<b>Controls</b>		
<b>Forced Arm</b>		
Define whether the zone can be force armed or not. For more information regarding the force arming feature refer to page 4-25.		
<b>No Activity</b>		
Determines whether the zone participates in the No Activity function. The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people. For more information regarding the force arming feature refer to page 4-25.		

## I/O Expander: Wired Zones

Parameter	Default	Range
-----------	---------	-------

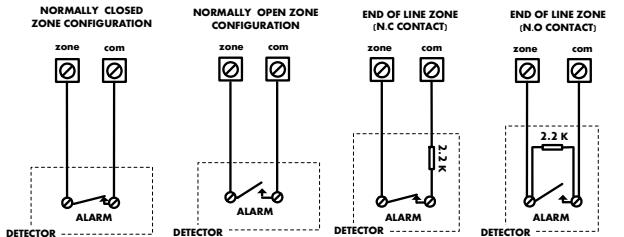
### Abort Alarm

This parameter defines whether a zone alarm report to the monitoring station will be immediate or delayed. For more information regarding the force arming feature refer to page 4-25.

### Termination

The Termination menu enables you to program the connection type used for the wired zones 33-36. The actual (physical) termination for each zone must comply with that selected in the zone termination menu.

- ♦ N/C: (Normally Closed) Uses normally-closed contacts and no terminating End-of-Line Resistor.
- ♦ N/O: (Normally Open) Uses normally-open contacts and no terminating End-of-Line Resistor
- ♦ EOL: (End of Line) Uses normally-closed (NC) and/or normally-open (NO) contacts in a zone terminated by a supplied  $2200\Omega$  End-of-Line Resistor



### Loop response

The Loop Response menu enables you to set the different times for which a wired zone violation must exist before the zone will trigger an alarm condition.

The following option are available:

Normal 400 ms	0.5 hours	2 hours	3.5 hours
Slow: 1 second	1 hour	2.5 hours	4 hours
Fast: 10 ms	1.5 hours	3 hours	

### Detection Mode

- ♦ Normal (Default): 2.5 minutes dead time between alarm detections transmissions.
- ♦ Fast (Walk Test): Alarm detection is immediately transmitted.

## Output Parameters

The I/O expander has 4 physical outputs on board. (2 relay 3Amp and 2 Transistor Outputs (500 mA)

### I/O Expander: Output Parameters

Parameter	Default	Range
<b>Label</b>		
A label identifies the output in the system.		
<b>Type</b>		
There are 4 types of outputs in the system as follows		
<ul style="list-style-type: none"> <li>♦ <b>Not Used</b></li> <li>♦ <b>Follow System:</b> The utility output will follow a System Event</li> <li>♦ <b>Follow Partition:</b> The utility output will follow a Partition Event.</li> <li>♦ <b>Follow Zone:</b> The utility output will follow a Zone Event. Each Utility Output can be activated by a group of up to five zones.</li> <li>♦ <b>Follow Code:</b> The utility output will be activated by a user defined as UO Control or from the user programming menu.</li> </ul>		
<b>Follow System Events:</b>		
<b>Bell</b>		
Activates when a bell is triggered. If a bell delay was defined, the utility output will be activated after the delay period.		
<b>No Telephone Line</b>		
Activates when a telephone line fault is detected. If a <b>PSTN Lost Delay</b> time period is defined, the utility output will be activated after the delay time		
<b>Monitoring Station Communication Fail</b>		
Activates when communication with the Central Station cannot be established. Deactivates after a successful call is established with the Central Station.		
<b>General Trouble</b>		
Activates when a system trouble condition is detected. Deactivates after the trouble has been corrected		
<b>Main unit Low battery</b>		
Activates when the Agility battery has insufficient reserve capacity and the voltage decreases to 6V.		
<b>AC Loss</b>		
Activates when the source of the Main Panel's AC power is interrupted. This activation will follow the delay time defined in the system control times and the <b>AC Off Delay Time</b> parameter.		

**I/O Expander: Output Parameters**

Parameter	Default	Range
<b>Bell burglary</b>		
Activates the Utility Output after any bell burglary alarm in any partition in the system.		
<b>Scheduler</b>		
The utility output will follow the predefined time programming that is defined in the scheduler of the weekly programs for utility output activation.		
<b>Tamper</b>		
Activates the utility output when a Tamper occurs in the system.		
<b>Duress</b>		
Activates the Utility Output when a duress alarm is initiated by any user defined as duress code.		
<b>GSM Trouble</b>		
Activates the utility output when there is trouble in the GSM module.		
<b>Follow Partition Events:</b>		
<b>Ready</b>		
Activates the utility output when all the selected partition(s) are in the Ready state.		
<b>Arm</b>		
Activates the utility output when the selected partition(s) is armed in Away (Full) mode. The utility output will be activated immediately, regardless of the Exit Delay time period.		
<b>Disarm</b>		
Activates the Utility Output when the selected partition(s) is disarmed.		
<b>Alarm</b>		
Activates the Utility Output when an alarm occurs in the selected partition(s).		
<b>Intruder alarm</b>		
Activates the utility output when an intrusion (Burglary) alarm occurs in the selected partition(s).		
<b>Fire</b>		
Activates the utility output when a fire alarm is triggered in the selected partition(s) from the keypads or a zone defined as Fire.		
<b>Panic</b>		
Activates the utility output when a panic alarm is triggered in the selected partition(s) from the keypads, remote controls or a zone defined as Panic.		

**I/O Expander: Output Parameters**

Parameter	Default	Range
<b>Special</b>		
Activates the utility output when a special alarm is triggered in the selected partition(s) from the keypads or a zone defined as Special .		
<b>Exit/Entry</b>		
Activates the Utility Output when the selected partition(s) initiates an Exit/Entry Delay period.		
<b>Zone Bypass</b>		
Activates the Utility Output when the relevant partitions are in ARM or STAY mode and any zone in the relevant partitions is bypassed.		
<b>Auto Arm Alarm</b>		
Activates the utility output when there is a not ready zone at the end of the pre-warning time during an auto-arm process. The output restore shall be on Bell-Timeout or at user Disarm.		
<b>Zone Lost</b>		
Activates the utility output when there is a lost wireless zone in the system. The output restore shall be on Bell-Timeout or at user Disarm.		
<b>Stay Follow</b>		
Activates the Utility Output when the selected partition(s) is armed in Stay mode.		
<b>Chime Follow</b>		
Activates the Utility Output following a chime sound in the selected partition(s)		
<b>Bell Stay Off</b>		
This parameter causes the utility output to function as follows:		
<ul style="list-style-type: none"> <li>• In Away arming mode, the utility output will follow the bell activation in the defined partitions.</li> <li>• In Stay arming mode, the utility output will not be activated.</li> </ul>		
<b>Bell</b>		
Activates the utility output when one of the defined partitions is in Alarm mode and the bell is triggered. This enables the connection of different sirens to different partitions.		
<b>Follow Zone Events:</b>		
<b>Zone</b>		
Activates the utility output when the selected zone is tripped. The tripped zone need not be armed to trigger the Utility Output.		

**I/O Expander: Output Parameters**

Parameter	Default	Range
<b>Alarm</b>		
Activates the utility output when the selected zone causes an alarm.		
<b>Arm</b>		
Activates the utility output when the selected zones are armed.		
<b>Disarm</b>		
Activates the utility output when the selected zones are disarmed.		

**Follow User Code:**

Defines the User Code(s) for triggering the selected UO. The activation of the UO is performed from the User Activities menu. Use the  key to toggle between [Y] YES or [N] NO for each user chosen to trip the designated Utility Output.

**Pattern**

For each output you need to define the pattern of operation. The available options are:

**Pulse N/O (Normally Open)**

The utility output is always Deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (pulled down) for the Pulse Duration specified, then deactivates automatically.

**Latched N/O (Normally Open)**

The Utility Output is always Deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (pulled down) and remains activated (latched) until the operation is restored.

**Pulse N/C (Normally Closed)**

The utility output is always Activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates for the Pulse Duration specified below and then reactivates automatically.

**Latched N/C (Normally Close)**

The Utility Output is always Activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates and remains deactivated (latched) until the operation is restored.

**I/O Expander: Output Parameters**

Parameter	Default	Range
<b>Activation / Deactivation</b>		

When the utility output is following more than one partition or zone, the installer can choose the logic of the Utility Output activation as follows:

- ♦ If the pattern operation of the output is defined as **Latch N/O** or **Latch N/C**, the **activation and deactivation** of the outputs can follow either after **all** the Partitions/Zones or after **any** of the Partitions/Zones.
- ♦ If the Pattern operation of the output is defined as **Pulse N/O** or **Pulse N/C**, the **activation** of the outputs can follow either after **all** the Partitions/Zones or after **any** of the Partitions/Zones. The **deactivation** operation follows the defined time period.

<b>Pulse Duration Length</b>	05 sec	01-90
------------------------------	--------	-------

The time that an output defined as Pulsed N.O or Pulsed N.C will be activated. At the end of the pulse duration the output reactivates automatically.

**X-10 Outputs**

The wireless I/O expander enables the system to control X – 10 devices. The I/O expander converts the information sent from the programmable utility output into the X – 10 protocol. Up to sixteen X-10 devices can be activated. These are recognized in the system as outputs 5-20.

**I/O Expander: X-10 Outputs**

Parameter	Default	Range
<b>Label</b>		
A label identifies the output in the system		
<b>Type</b>		
Refer to the explanation under the utility output section.		
<b>Pattern</b>		
Refer to the explanation under the utility output section.		
<b>Pulse Length</b>	05 sec	01-90
Refer to the explanation under the utility output section.		

**Parameters**

The following table describes the general parameters for the I/O module.

**I/O Expander: Parameters**

Parameter	Default	Range
<b>Serial Code</b>		

The internal ID number of the I/O Expander. Each wireless device has its own unique serial number.

**I/O Expander: Parameters**

Parameter	Default	Range
<b>Controls</b>		
<b>I/O Expander Supervision</b>		
Choose if the I/O Expander will be supervised or not.		
<b>Quick Output Operation</b>		
A user can activate a UO from the bidirectional remote control or keys  on the wireless keypad without the need to enter his user code.		
<b>X-10 House ID</b>		
Defines the house code, which matches the code defined by the X-10 modules.		
<b>UO DTMF Control</b>		
The Agility enables to activate 8 utility outputs from remote DTMF phone. To operate a UO via the telephone you must assign a specific UO to a digit on the phone.		

### 2.3 Identification

This option provides the ability to identify the serial number of a wireless device in the system from a keypad or from the configuration software.

When using a keypad follow this procedure:

Go to **Programming** → **Radio Devices Menu** → **Identification** and press . The following message appears on the keypad LCD:

Please start RF identification

Press on the device's Learn mode. The serial number of the relevant device appears on the keypad LCD.

### 3. Programming: Codes Menu

The **Codes** menu provides the ability do define parameters and codes for the system users.

#### 3.1 User

User rights can be defined by allocating each user a specific authority level and specific partitions. Up to 32 users can be defined in the system.

##### **Codes: User Codes**

Parameter	Default
<b>Labels</b>	
Used to define the user name. Up t o 32 characters can be used.	
<b>Partition</b>	
Enables you to assign the partition(s) in which all User Codes (except for the Grand Master) will operate.	
<b>Authority Level</b>	

Allocate an authority level to a user according to the following list:

- **User:** There are no restrictions in the number of User Codes (as long as they do not exceed the number of codes remaining in the system). The User has access to the following:
  - ◆ Arming and disarming
  - ◆ Bypassing zones
  - ◆ Viewing system status, trouble, and alarm memory
  - ◆ Activating designated Utility Outputs
  - ◆ Changing his/her own User Code
  - ◆ Setting keypad's settings
- **Cleaner:** The Cleaner Code is a temporary code, which is to be immediately deleted from the system as soon as it is used to arm. This code is typically used for maids, home attendants, and repairmen who must enter the premises before the owner(s) arrive. These codes are used as follows:
  - ◆ For one-time arming in one or more partitions
  - ◆ If first used to disarm the system, the code may be used once for subsequent arming
- **Arm Only:** There are no restrictions in the number of Arm Only Codes (as long as they don't exceed the number of codes remaining in the system). Arm Only Codes are useful for workers who arrive when the premises are already open, but because they are last to leave, they're given the responsibility to close the premises and arm the system. The users with Arm Only Codes have access for arming one or more partitions.

## Codes: User Codes

Parameter	Default
• <b>Duress:</b> When coerced into disarming the system, the user can comply with the intruder's wishes while sending a silent duress alarm to the Central Station. To do so, a special duress code must be used, which when used, will disarm the system in the regular manner, while simultaneously transmitting the duress alarm. In any other situation the Duress authority level behaves as the same as the User authority level.	

### 3.2 Grand Master

The Grand Master Code is used by the system's owner and is the highest Authority Level. The owner can set/change the Grand Master Code.

Default: 1234

**Note:** In the Configuration software the Grand Master is identified as Code 00.

### 3.3 Installer

The Installer Code provides access to the Installer Programming menu, allowing modification of all system parameters. The Installer Code is used by the **Agility** installation company technician to program the system.

The Installer can change the Installer Code.

Default: 0132

### 3.4 Sub-Installer

The Sub-Installer Code allows limited access to selected parameters from the Installer Programming menu. It is used by a technician sent by the **Agility** installation company to carry out restricted tasks defined at the time of system installation by the installation technician. The Sub-Installer can access with his code only those programming menus predefined for his access. Default: 0232

The Sub-Installer is prohibited to access the following parameters:

- Default Enable
- MS Enable
- Configuration Software Enable
- Code Length
- Installer Code

**Note:** In the Agility Configuration Software, the Configuration Software and Monitoring Station menus are unavailable to the sub-installer.

### 3.5 Code Length

The Code Length specifies the minimum number of digits requested. Default: 4 digits

---

#### Notes:

When you change the **Code Length** parameter, all User Codes are deleted and must be re-programmed or downloaded.

For a 6-digit Code Length system, 4-digit default codes like **1-2-3-4** (Grand Master), **0-1-3-2** (Installer), and **0-2-3-2** (Sub-Installer) become **1-2-3-4-0-0**, **0-1-3-2-0-0**, and **0-2-3-2-0-0**, respectively.

If you change the **Code Length** back to 4 digits, the system codes are restored to the default 4-digit codes.

---

#### EN50131-3 standard specifications:

- All code length are 4 digits: xxxx
  - For each digit 0-9 can be used
  - All codes from 0000 to 9999 are acceptable
  - Invalid codes cannot be created since after 4 digits are typed, the "Enter" is automatic.  
Codes are rejected when trying to create a code that does not exist.
- 

### 3.6 DTMF Code

This is a telephone remote access code made up of two digits that enables entry into the system when dialing in from a remote number.

Default code=00

### 3.7 Parent Control

The Parent Control option is used to monitor the activity of children. This option allows all users to monitor when the children arrive home and disarm the system or when they arm the system in Away mode. With each activation/deactivation of the system a message is sent to a specified Follow Me number.

Use the  key to toggle between [Y] YES or [N] NO for each user chosen to be assigned with the parent control feature.

## 4. Programming: Communication Menu

The **Communication** menu provides access to submenus and their related parameters that enable the system to establish communication with the Monitoring Station, Follow Me or Upload/Download.

The **Communication** menu is divided into the following sub-menus:

- 1. Method**
- 2. Monitoring Station**
- 2. Configuration Software**
- 3. Follow-Me**

### 4.1 Method

This option allows you to configure the parameters of the communication methods (channels) of the Agility. 3 optional communication types are available:

- 1. PSTN**
- 2. GSM**
- 3. IP**

#### 4.1.1 PSTN

The PSTN screen contains parameters for the communication of the Agility over the PSTN network

##### Communication Type: PSTN

Parameter	Default	Range
<b>Timers</b>		
Timers related to communication through the PSTN channel		
<b>PSTN Lost Delay</b>	04	00-20 minutes
The time after which the system will regard the PSTN line as lost. This time also specifies the delay before reporting the event into the event log or operating a utility output that follows this event. 00 indicates no supervision of the phone line.		
<b>Wait for Dial Tone</b>	3	0-255 seconds
The number of seconds the system waits to detect a dial tone.		
<b>Controls</b>		
<b>Alarm Line Cut</b>		
YES: Activates the external sirens if the land line, connected to the Agility panel is cut or the telephone service is interrupted for the time defined in the <b>PSTN Lost</b> time parameter. NO: No activation occurs.		

**Communication Type: PSTN**

Parameter	Default	Range
<b>Answering Machine Override</b>		
<b>YES:</b> The Answering Machine Override is enabled, as follows:		
<ul style="list-style-type: none"> <li>◆ The configuration software at the alarm company calls the account.</li> <li>◆ The software hangs up after one ring by the configuration operator.</li> <li>◆ Within one minute, the software calls again.</li> <li>◆ The system is programmed to pick up this second call on the first ring, thus bypassing any interaction with the answering machine.</li> </ul>		
<b>Note:</b> This feature is used to prevent interference from an answering machine with remote configuration operations.		
<b>NO:</b> The Answering Machine Override is disabled, and communication takes place in the standard manner.		

**Parameters**

<b>Rings to Answer</b>	12	01 to 15
The number of rings before the system answers an incoming call		

**Area code**

The system area telephone code. This code will be deleted from a telephone number while the system tries to dial the number through the GSM network.

**PBX Prefix**

A number dialed to access an outgoing line when the system is connected to a Private Branch Exchange (PBX) and not directly to a PSTN line. This number will be added automatically by the system while trying to call from a PSTN line.

**4.1.2 GSM**

The GSM screen contains parameters for the communication of the system over the GSM/GPRS network.

**Method: GSM**

Parameter	Default	Range
<b>Timers</b>		
Allows to program timers related to operation with the GSM module		
<b>GSM Lost</b>	10 min	001-255 min
The time after which the GSM module regards the GSM network as loss. Network loss is defined as RSSI level below the level defined GSM Network Sensitivity parameter.		

**Method: GSM**

Parameter	Default	Range
<b>SIM Expire</b>	00	00-36 months
A Pre-paid SIM card has a defined life length defined by the provider. After each charging of the SIM, the user will have to manually reset the expiration time of the SIM card. A notification will be displayed on the wireless keypad when asking for status indication.  Set the SIM expiring date (in months) using the numeric keys, according to the time given by the provider.		
<b>MS Keep Alive (Polling)</b>		
The time period that the system will establish automatic communication (polling) with the MS over GPRS, in order to check the connection.  3 polling times can be defined: Primary, Secondary and Backup. For each time period define the number of units between 1- 65535. Each unit represents a time frame of 10 seconds.	00000	0-65535 times
<p><b>Note:</b> When using the polling feature through GPRS the MS channel parameter must be defined as GPRS only.</p> <p>The report code for MS polling is 999 (Contact ID) or ZZ (SIA)</p>		
The use of these time periods depends on the reporting order to the MS defined by the Report Split MS Urgent parameter (See: [4]Communication > [2]MS > [7]Report Split)		
<ul style="list-style-type: none"> <li>◆ <b>Primary:</b> This time period is used when the MS channel is defined as <i>GPRS Only</i> and the Report Split parameter is <u>not</u> defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i>.</li> <li>◆ <b>Secondary:</b> This time period is used when the MS 2 channel is defined as <i>IP →GPRS Only</i> and the Report Split parameter is defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i>.</li> <li>◆ <b>Backup:</b> This time period will be assigned to the backup channel in the following case:           <ul style="list-style-type: none"> <li>▪ MS 2 channel is defined as <i>IP →GPRS Only</i></li> <li>▪ Report Split parameter is defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i></li> <li>▪ The communication with MS 1 is disconnected.</li> </ul> </li> </ul>		

**Method: GSM**

Parameter	Default	Range
<b>GPRS</b>		
Allows programming parameters that relate for the communication over the GPRS network.		

**Access Point Network (APN) Code**

To establish a connection to the GPRS network an APN (Access Point Name) code is required. The APN code differs from country to country and from one provider to another (the APN code is provided by your cellular provider). The system supports an APN code field of up to 30 alphanumeric characters and symbols (!, &, ? etc).

**APN User Name**

Enter APN user name (if required). The User name is provided by your provider. The system supports a user name field of up to 20 alphanumeric characters and symbols (!, &, ? etc).

**APN Password**

Enter the APN password (up to 20 alphanumeric characters and symbols.) as provided by your provider (if required).

**E-mail**

The following programming parameters are used to enable sending Follow Me event messages by e-mail through GPRS.

**Note:** To enable e-mail messaging, the GPRS parameters have to be defined.

**Mail Host**

The IP address or the host name of the SMTP mail server

**SMTP Port**

The port address of the SMTP mail server

**Email address**

The Email address that identifies the system to the mail recipient .

**SMTP User Name**

A name identifying the user to the SMTP mail server. The user name field can include up to 10 alphanumeric characters and symbols (!, &, ? etc). Provision for future functionality

**SMTP Password**

The password authenticating the user to the SMTP mail server. The password can include up to 10 alphanumeric characters and symbols (!, &, ? etc). Provision for future functionality

**Method: GSM**

Parameter	Default	Range
<b>Controls</b>		
Allows to control timers related to operation with the GSM module.		
<b>Caller ID</b>		
The Caller ID function enables to restrict SMS remote control operations to the predefined follow me phone numbers. If the incoming number is recognized as one of the Follow Me numbers, the operation will be executed.		
<b>Disable GSM</b>		
YES: The system will disable the GSM/GPRS module from any activity. NO: GSM/GPRS module is enabled in the system.		
<b>Parameters</b>		
Allows to program timers related to the operation with the GSM module.		
<b>SIM PIN Code</b>		
The PIN (Personal Identity Number) code is a 4 to 8 digit number giving you access to the GSM network provider.		
Note: You can cancel the PIN code request function by inserting the SIM card into a regular mobile phone and according to the phone settings, disable this function.		
<b>SMS Center Phone</b>		
A telephone number of the message delivery center. This number can be obtained from the network operator.		
<b>GSM Network Sensitivity (RSSI)</b>		
Set the minimum acceptable network signal level (RSSI level). Options: Disabled (No troubles for low signal reception) / Low signal / High signal		
<b>SIM Number</b>		
The SIM phone number. The system uses this parameter to receive the time from the GSM network in order to update the system time.		
<b>Prepaid SIM Card</b>		
Allows programming parameters that will be used when a prepaid SIM card is used in the system.		
<b>Get Credit by</b>		
Depending on the local network provider, the user can receive the credit level of the prepaid SIM card by sending a predefined SMS command to a defined number or by calling a predefined number through the voice channel. The activation of the credit request can be done by the Grand Master.		
♦ <b>SMS Credit Message:</b> Type in the message command as defined by the		

**Method: GSM**

Parameter	Default	Range
provider and the provider's phone number to which the credit level SMS message request will be sent.		
♦ <b>Voice Credit:</b> Type in the provider's phone number to which a call will be established		
♦ <b>Service Command:</b> Type in the service command message as defined by the provider		

**Phone to Get Credit Message**

The provider's phone number to which the credit level SMS message request will be sent to or a call will be established, depending on the selection in the **Get Credit by** parameter.

**Phone to Receive SMS Credit Message:**

The provider's telephone number from which an automatic SMS credit status message will be sent from.

**4.1.3 IP****Communication Type: IP**

Parameter	Default	Range
<b>IP Configuration</b>		
<b>Obtain Automatic IP</b>	YES	Y/N
Defines whether the IP address, which the Agility refers to, is static or dynamic.		
YES: The system refers to an IP address provided by the DHCP.		
NO: The system refers to a static IP Address.		
<b>Panel IP</b>		
The Agility IP address.		
<b>Subnet Mask</b>		
The subnet mask is used to determine where the network number in an IP address ends.		
<b>Gateway</b>		
The IP address of the local Gateway, which enables communication settings to other LAN segments. This address is the IP address of the router connected to the same LAN segment as the Agility.		
<b>DNS Primary</b>		
The IP address of the primary DNS server on the network.		
<b>DNS Secondary</b>		
The IP address of the secondary DNS server on the network		

**Communication Type: IP**

Parameter	Default	Range
<b>E-mail</b>		
Allows programming parameters that enable the Agility to send Email messages following Follow Me events		
<b>Mail Host</b>		
The IP address or the Host name of the mail server.		
<b>SMTP Port</b>		
The port address of the SMTP mail server. Default: 00025		
<b>E-mail address</b>		
Agility E-mail address. Default: YourCompany.com		
<b>SMTP User name</b>		
If required by the mail server, fill in the Authentication User name		
<b>SMTP User password</b>		
If required by the mail server, fill in the Authentication User password		
<b>Host Name</b>	(Up to 32 characters)	
IP address or a text name used to identify the Agility over the network.		
Default: Security System		
<b>MS Keep Alive (Polling)</b>	00000	0-65535
The time period that the system will establish automatic communication (polling) with the MS over the IP network, in order to check the connection. 3 polling times can be defined: Primary, Secondary and Backup. For each time period define the number of units between 1- 65535. Each unit represents a time frame of 10 seconds.		
<b>Note:</b> When using the polling feature through IP, the MS channel parameter must be defined as IP only.		
The use of these time periods depends on the reporting order to the MS defined by the Report Split MS Urgent parameter (See: [4]Communication > [2]MS > [7]Report Split)		
<ul style="list-style-type: none"> <li>◆ <b>Primary:</b> This time period is used when the MS channel is defined as <i>IP Only</i> and the Report Split parameter is <u>not</u> defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i>. Default: 00006 (60 seconds)</li> <li>◆ <b>Secondary:</b> This time period is used when the MS 2 channel is defined as <i>IP → IP Only</i> and the Report Split parameter is defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i>. Default: 360 (3600 seconds)</li> <li>◆ <b>Backup:</b> This time period will be assigned to the backup channel in the following case:           <ul style="list-style-type: none"> <li>▪ MS 2 channel is defined as <i>IP → IP Only</i></li> <li>▪ Report Split parameter is defined as <i>1<sup>st</sup> backup 2<sup>nd</sup></i></li> <li>▪ The communication with MS 1 is disconnected.</li> </ul>           Default: 00006 (60 seconds)         </li> </ul>		

## Controls

### Disable IP

YES: The system will disable the IP module from any activity.

NO: The IP module is enabled in the system.

## 4.2 Monitoring Station

The **Monitoring Station** menu contains parameters that enable the system to establish communication with the Monitoring Station and transmit data.

### Communication: Monitoring Station

Parameter	Default	Range
<b>Report Type</b>		
Type		

#### Type

Defines the communication type that the system will establish with each monitoring station. The system can report in 3 optional communication types:

- ♦ Voice
- ♦ SMS
- ♦ IP

#### Voice

Reports to the monitoring station will be done through the PSTN or GSM network. Reporting by Voice can be established through different channels. The optional channels depend on the hardware installed in your system. Select the required channel as follows:

- **PSTN/GSM:** The system checks for the availability of the PSTN line. During regular operation mode all calls and data transmission are carried out using the PSTN line. In the case of trouble in the PSTN line, the line is routed to the GSM line.
- **GSM/PSTN:** The panel checks for the availability of the GSM line. During regular operation mode all calls and data transmission are carried out using the GSM line. In the case of trouble in the GSM line, the line is routed to the PSTN line.
- **PSTN Only:** The outgoing calls are executed through the PSTN audio channel only. Use this option for installations where no GSM line is available.
- **GSM Only:** The outgoing calls are executed through the GSM audio channel only. Use this option for installations where no PSTN line is available.

Enter the monitoring station telephone number including area code and special letters (if required). If calling from PBX do not include the number for outgoing line.

**Communication: Monitoring Station**

Parameter	Default	Range
Function	Results	
Stop dialing and wait for a new dial tone	W	
Wait a fixed period before continuing	,	
Send the DTMF *	*	
Send the DTMF # character	#	
Delete numbers from the cursor position	[*] [0]	simultaneously

**SMS**

Events are sent to the monitoring station using encrypted SMS messages (128 BIT AES encryption). Each event message contains information including the account number, report code, communication format, time of event and more. The event messages are received by RISCO Group's IP/GSM Receiver Software located at the MS/ARC site. The IP/GSM Receiver translates the SMS messages to standard protocols used by the monitoring station applications (For example; Contact ID). This channel requires that RISCO Group's IP/GSM receiver has to be used at the MS side.

Enter the relevant phone numbers for the MS that will receive reports from the system. (See explanation in *Voice* type on page 4-51)

**IP**

Encrypted events are sent to the monitoring station over the IP or GPRS network using TCP/IP protocol. 128 BIT AES encryption is used. RISCO Group's IP/GSM Receiver Software located at the MS/ARC site receives the messages and translates them to standard protocols used by the monitoring station applications (For example; Contact ID).

**Note:** To enable GPRS communication the SIM card has to support GPRS channel

Reporting by IP can be established through different channels. The optional channels depend on the hardware installed in your system. Select the required channel via the Configuration Software as follows:

- **IP/GPRS:** The panel checks for the availability of the IP network. During regular operation mode all calls and data transmission are carried out using the IP network line. In the case of trouble in the IP network, the report is routed to the GPRS network.
- **GPRS/IP:** The panel checks for the availability of the GPRS network. During regular operation mode all calls and data transmission are carried out using the GPRS. In the case of trouble the report is routed to the IP network.

**Communication: Monitoring Station**

Parameter	Default	Range
<ul style="list-style-type: none"> <li><b>IP Only:</b> The report is executed through the IP network only.</li> <li><b>GPRS Only:</b> The report is executed through the GPRS network.</li> </ul> Enter the relevant IP and Port numbers for the MS that will receive reports from the system. (See <i>IP</i> and <i>Port</i> )		

**Accounts**
**Account Number**

The number that recognizes the customer at the monitoring station. You can define an account number for each monitoring station. These account numbers are the 6-digit numbers assigned by the central station.

**Notes for Account Number in Contact ID Communication Format:**

1. The account number will always be reported as 4 digits, for example: A number defined as 000012 will be reported as 0012
2. If more than 4 digits were defined, the system always sends the last 4 digits of the account number, for example: Account number that was defined as 123456 will be sent as 3456.
3. In Contact ID you can place digits and letters A-F. The A character is always sent as 0 for example: Account number that was defined as 00C2AB will be sent as C20B.

**Notes for Account Number in SIA Communication Format:**

1. Account number for SIA should be defined as a decimal number (Only digits 0..9)
2. Account number can be reported as 1 to 6 digits. To send an account number with less than 6 digits use the "0" digit, for example: For account number 1234 enter 001234. In this case the system will not send the "0" digit to the monitoring station.
3. In order to send the "0" digit in SIA format, located at the left side of the number, use the "A" digit instead of the "0" digit. For example, for account number 0407 enter 00A407, for a 6 digit account number such as 001207 enter AA1207.

**Communications Format**

Enables the system to contact the Monitoring Station in order to obtain details of the communication protocol used by the digital receiver for each account.

The codes are automatically uploaded when the communication format has been selected:

- ◆ **Contact ID:** The system allocates Report Codes supporting ADEMCO Contact (Point) ID
- ◆ **SIA:** The system allocates Report Codes supporting the SIA (Security Industry Association) format

**Note:** See Appendix A for the report codes list.

## Communication: Monitoring Station

Parameter	Default	Range
<b>Controls</b>		
Allows to program control related to operation with the Monitoring Station.		
<b>Handshake</b>	NO	
<b>YES:</b> All LEDs on the Agility main unit light for one second when the handshake signal is received from the Central Station's receiver.		
<b>NO:</b> No indication for establishing communication with the Central Station's receiver.		
<b>Kiss-Off Y/N</b>	NO	
<b>YES:</b> All LEDs on the Agility main unit light for one second and an audible sound is emitted when the kissoff signal is received from the Central Station's receiver.		
<b>NO:</b> No indication for establishing communication with the Central Station's receiver.		
<b>Parameters</b>		
Allows to program parameters related to operation with the Monitoring Station.		
<b>MS Retries</b>	08	01-15
The number of times the system redials the Monitoring Station after failing to establish communication.		
<b>Alarm Restore</b>	BTO	
Specifies under what conditions an Alarm Restoral is reported. This option informs the MS of a change in the specified condition(s) during an alarm restore. These reports need a valid Report Code.		
<ul style="list-style-type: none"> <li>♦ <b>On Bell Time Out (BTO)</b> - Reports the restoral after the audible alarm times out.</li> <li>♦ <b>Follow Zone</b> - Reports the restoral when the zone in which the alarm occurs returns to its non-violated (secured) state.</li> <li>♦ <b>At Disarm</b> - Reports the restoral when the system (or the partition in which the alarm occurs) is disarmed, even if the siren has already timed out.</li> </ul>		

## MS Timers

Allows to program timers related to operation with the Monitoring Station.

### Periodic Test

The Periodic Test enables you to set the time period that the system will automatically establish communication to the Monitoring Station in order to check the connection. The periodic test involves sending the account number and a valid test report code (Contact ID 602, SIA TX). Set the test time and daily interval for Periodic Test Reporting.

**Communication: Monitoring Station**

Parameter	Default	Range
<b>Abort Alarm</b>	15 sec	0-255 sec
Defines the time delay before reporting an alarm to the MS. If the alarm system is disarmed within the Abort Window, no alarm transmission shall be sent to the MS.		
<hr/>		
<b>Cancel Delay</b>	5 min	0-255 min
If an alarm is sent in error, it is possible for the MS to receive a Cancel Alarm Code, sent subsequently to the initial Alarm Code. This happens if a valid User Code is entered to reset the alarm in the Cancel Delay time window that starts after the defined Abort Alarm time is over.		
<hr/>		
<b>Note:</b> Cancel Alarm report code should be defined.		
<hr/>		
<b>Listen In</b>	120	1-240 seconds
The time duration for the monitoring station to Listen in and perform voice alarm verification. After this period the system hangs up the line.		
The monitoring station can expand the listen in time during the conversation by pressing the digit "1" on the telephone. In this case, the Listen In time will reset and start over again.		
<hr/>		
<b>Confirmation</b>		
The confirmation times relate to the Zone Sequential Confirmation.		
<hr/>		
<b>Confirm Start</b> (Confirm delay time)	0	0-120 min
Specifies that the system cannot start a sequential confirmation process until the timer has expired. This time starts when the system has set and will prevent confirmed alarms being generated in situations when a person has been accidentally locked in the building.		
<hr/>		
<b>Confirm Time Window</b>	030	30-60 min
Specifies a time period that starts when an alarm is triggered for the first time. If a second alarm is triggered before the end of the confirmation time window, the system will send a confirmed alarm to the monitoring station.		
<hr/>		
<b>No Arm</b>	0	0-12 weeks
A No Arm code will be sent to the MS if no arming or disarming has been established during the time defined (1-12 weeks).		
(0=not activated)		

## Communication: Monitoring Station

Parameter	Default	Range
<b>Report Split</b>		

The Report Split menu contains parameters that enable the routing of specified events to up to three MS Receivers. (See *Appendix A Reports Codes*)

### MS Arm/Disarm

Reports Arming/Disarming (meaning Closings/Openings) events to the MS

- ♦ Do not call (no report)
- ♦ Send 1st: Reports Openings and Closings to MS 1
- ♦ Send 2nd: Reports Openings and Closings to MS 2
- ♦ Send 3rd: Reports Openings and Closings to MS 3
- ♦ Send all: Reports Openings and Closings to the all defined MS.
- ♦ 1st Backup 2nd: Reports Openings and Closings to MS 1. If communication is not established, calls MS 2.

### MS Urgent

Reports urgent (alarm) events to the Central Monitoring Station

- ♦ Do not call (no report)
- ♦ Call 1st: Reports urgent events to MS 1
- ♦ Call 2nd: Reports urgent events to MS 2
- ♦ Call 3rd: Reports urgent events to MS 3
- ♦ Call all: Reports urgent events to the all defined MS.
- ♦ 1st Backup 2nd: Reports urgent events to MS 1. If communication is not established, calls MS 2

### MS Non Urgent

Reports non-urgent events (troubles and test reports) to the MS

- ♦ Do not call (no report)
- ♦ Call 1st: Reports non-urgent events to MS 1
- ♦ Call 2nd: Reports non-urgent events to MS 2
- ♦ Call 3rd: Reports non-urgent events to MS 3
- ♦ Call all: Reports non-urgent events to the all defined MS.
- ♦ 1st Backup 2nd: Reports non-urgent events to MS 1. If communication is not established, calls MS 2

**Communication: Monitoring Station**

Parameter	Default	Range
<b>Report Codes</b>		

Enables you to view or program the codes transmitted by the system to report events (for example, alarms, troubles, restores, supervisory tests, and so on) to the monitoring station. The codes specified for each type of event transmission are a function of the Central Station's own policies. Before programming any codes, it is important to check the Central Station protocols. Reporting codes are assigned by default, according to the selected communication format SIA or Contact ID

Assigns a specified report code for each event, based on the reporting format to the monitoring station. An event that is not assigned with a report code will not be reported to the monitoring station. For list of report events refer to *Appendix A*.

**4.3 Configuration Software**

The **Configuration Software** menu contains parameters that enable the configuration software to establish connection with the system.

**Communication: Configuration software**

Parameter	Default	Range
<b>Security</b>		
Enables you to set parameters for remote communication between the technician and the system using the Configuration software		
<b>Access Code</b>	5678	
Enables you to define an Access Code that is stored in the system. RISCO Group recommends using a different 4-digit Access Code for each installation. In order to enable communication between the alarm company and the system the same Access Code must subsequently be entered into the corresponding account profile created for the installation in the configuration software For successful communication, the Access Code along with the ID code must match between the configuration software and the system.		
<b>Remote ID</b>	0001	
Defines an ID Code that serves as an extension of the Access Code. In order to enable communication between the alarm company and the Installation, the same Remote ID code must be entered into the account profile in the configuration software. For successful communication, the ID Code along with the Access Code must match between the Upload/Download software and the Main Panel. Dealers often use the customer's Monitoring Station Account Number for the ID Code, but you can use any 4-digit code unique to the installation		

## Communication: Configuration software

Parameter	Default	Range
<b>MS Lock</b>	000000	

MS Lock is a security function used in conjunction with the configuration software. It provides greater proprietary security when viewing Monitoring Station parameters.

The same 6-digit code, which will be stored in the panel, must be entered into the corresponding account profile created for the installation in the Configuration software.

If there is no match between the MS Lock Code defined in the Main Panel and the MS Lock Code defined in the Configuration software, the Installer will not have permission to change the following Monitoring Station parameters from the Configuration software:

MS Lock, Installer Code, MS IP Port, MS IP Address, MS Phone, Default Enable, MS Account, MS Format, MS Channel, MS Backup, MS Enable, Remote ID, Access Code.

## Call Back

<b>Call Back</b>	YES
------------------	-----

The call back feature requires the system to call back to a pre-programmed telephone number to which the alarm company's configuration software computer is installed. This provides more security for remote operations using the configuration software.

**YES:** Call back is enabled

**NO:** Call back is disabled

## Call Back Phones

Define 3 numbers that the panel can call to perform Configuration Software communication. If no numbers have been defined, a call back can be performed to any phone. The installer will enter a phone number when establishing communication to the panel. If at least one number has been defined, it will be the only number that the call back can be established too.

When the Configuration Software establishes communication to the panel, it sends the panel its calling phone number. (This number needs to be defined as *My Number* under the GSM and PSTN Communication menu in the Configuration Software.)

If the panel identifies one of the numbers as one of the numbers predefined in the panel, the call will hang up and the panel will call back to that same number.

**Communication: Configuration software**

Parameter	Default	Range
<b>Configuration Software Port (IP Gateway)</b>	00000	

The IP and port address of the configuration's software PC. If you have a router connected to the PC of the configuration software then you should enter the IP of the router.

This definition will be used when there is a request to create a remote connection from the panel to the configuration software. The connection can be done over IP or GPRS.

**Note:** In the configuration software, under Communication → Configuration → GPRS you should enter the IP address of the PC that the software is installed in.

**4.4 Follow-Me**

In addition to reporting to the monitoring station, the Agility has a Follow-Me feature which enables reporting a system events to a predefined follow me destinations using a voice message, SMS message or Email. Up to 16 Follow Me destinations can be defined in the system.

**Parameters****Communication: Follow-Me**

Parameter	Default	Range
<b>Label (via the Configuration Software)</b>		

A label identifying the follow me destination

**Type**

Defines the type of reporting events to a follow me destination:

- **Voice:** Report to follow me will be done by voice message thorough the PSTN or GSM network. (See *Channel → For Voice Messaging* below). Type in the telephone number including area code or special letters for Follow Me defined as SMS or Voice.
- **SMS:** Report to follow me will be done by SMS. Each event message contains information including the system label. Event type and time. Type in the telephone number including area code or special letters for Follow Me defined as SMS or Voice.
- **E-mail:** Report to follow me will be done by e-mail thorough IP or GPRS. Each e-mail contains information including the system label. Event type and time. (See *Channel → For E-mail report* below) Type in the e-mail address for follow me destination defined as e-mail type.

## Communication: Follow-Me

Parameter	Default	Range
<b>Channel</b>		

Reporting events by Voice or Email can be established through different channels. The optional channels depend on the hardware installed in the system. Select the required channel as follows:

### For Voice Messaging:

- **PSTN/GSM:** The system checks for the availability of the PSTN line. During regular operation mode voice messaging is carried out using the PSTN line. In the case of trouble in the PSTN line, the line is routed to the GSM line.
- **GSM/PSTN:** The panel checks for the availability of the GSM line. During regular operation mode voice messaging is carried out using the GSM line. In the case of trouble in the GSM line, the line is routed to the PSTN line.
- **PSTN Only:** The outgoing calls are executed through the PSTN audio channel only. Use this option for installations where no GSM line is available.
- **GSM Only:** The outgoing calls are executed through the GSM audio channel only. Use this option for installations where no PSTN line is available.

### For E-mail report:

- **IP/GPRS:** The system checks for the availability of the IP network. During regular operation emails will be sent using the IP network line. In the case of trouble in the IP network, the email is routed to the GPRS network.
- **GPRS/IP:** The system checks for the availability of the GPRS network. During regular operation mode emails will be sent using the GPRS. In the case of trouble the email is routed to the IP network.
- **IP Only:** The report is executed through the IP network only.
- **GPRS Only:** The report is executed through the GPRS network

## Events

Each Follow Me destination can be assigned with its own set of events. Choose the events that will be reported to each Follow Me

Event	Description	Default
<b>Alarms</b>		
Intruder	Intruder alarm in the system	Yes
Fire	Fire alarm in the system	Yes
Emergency	Emergency alarm in the system	Yes
Panic (S.O.S)	A panic alarm in the system	Yes
Tamper	Any tamper alarm in the system	No
Duress Alarm	Duress alarm in the system from user xx	Yes
No Movement	No movement report indication	No

**Communication: Follow-Me**

Parameter	Default	Range
<b>Arm/Disarm</b>		
Arm	Arming operation has been performed in the system	No
Disarm	Disarming operation has been performed in the system	No
Parent Control	System armed/disarmed by user/remote control defined with the Parent control feature	No
<b>Troubles</b>		
False Code	After 5 unsuccessful attempts of entering an incorrect code.	No
Main Low Battery	Low battery indication from the Agility main panel (below 6V)	No
Wireless Low Battery	Low battery indication from any wireless device in the system	No
WL Jamming	Jamming indication in the system	No
WL Lost	Wireless device lost. When no supervision signal is received from a wireless device	No
AC Off	Interruption in the source of the main AC power. This activation will follow the delay time predefined in the AC Loss Delay timer	No
PSTN Trouble	PSTN lost event. If PSTN Loss Delay time period is defined, the message will be sent after the delay time	No
IP Network	Communication trouble with the IP network.	No
<b>GSM</b>		
GSM Trouble	General GSM trouble (SIM card fault, Network availability, Network Quality, PIN code error, Module communication, GPRS password, GPRS IP fault, GPRS Connection, PUK code fault)	No
SIM Trouble	Any trouble with the SIM card	No
SIM Expire	Report to Follow Me will be established 30 days before the SIM Expiration Time defined for a prepaid SIM card.	No
SIM Credit	An automatic SMS credit message (or any other message) received from the provider's number predefined in <i>SMS Receive Phone</i> will be transferred to the Follow Me number	No

### Communication: Follow-Me

Parameter		Default	Range
<b>Environmental</b>			
Gas Alert	Gas (natural gas) alert from a zone defined a Gas detector		No
Flood Alert	Flood alert from a zone defined as flood type		No
CO Alert	CO (Carbon Monoxide) alert from a zone defined a CO detector		No
High Temperature	High Temperature alert from a zone defined a Temperature detector		No
Low Temperature	Low Temperature alert from a zone defined a Temperature detector		No
Technical	Alert from the zone defined as Technical		No
<b>Miscellaneous</b>			
Zone Bypass	Zone has been bypassed		No
Periodic test	Follow Me test message will be established following the time defined in the Periodic Test parameter under the MS parameters		No
Remote programming	System is in remote installation mode		No
<b>Restore Events:</b>			
<b>Alarms</b>			
Intruder Alarm	Intruder alarm in the system restored		Yes
Tamper	Tamper alarm in the system restored		No
<b>Troubles</b>			
Main Low Battery	Low battery indication from the Agility main panel restored		No
WL Low Battery	Low battery indication from any wireless device in the system restored		No
Jamming	Jamming indication in the system restored		No
WL Lost	Wireless device lost restored		No
AC Off	Interruption in the source of the main AC power restored		No
PSTN Trouble	PSTN lost event restored		No
IP Network	Communication trouble in the IP restored		No
GSM Trouble	General GSM trouble restored		No

**Communication: Follow-Me**

Parameter	Default	Range
<b>Environmental</b>		
Gas Alert	Gas Alert restored	No
Flood Alert	Flood Alert restored	No
CO Alert	CO Alert restored	No
High Temperature	High Temperature Alert restored	No
Low Temperature	Low Temperature Alert restored	No
Technical	Technical Alert restored	No
<b>Remote Control</b>		
<b>Remote Listen</b>	No	
Enables the user of the follow me phone to perform remote listen and talk operation with the premises.		
<b>Remote program</b>	No	
Enables the user of the follow me phone to enter the Remote Operation menu and perform all available programming options. For more details see the User manual.		
<b>Partition</b>		
Assign the partitions from which events will be reported to the follow me number.		
<b>Controls</b>		
Allows to program control related to operation with the Follow Me		
<b>Disarm Stop Follow Me</b>	No	
YES: The Follow-Me calls will stop when the partitions are disarmed by a user code		
NO: The Follow-Me calls will continue to be made when the partitions are disarmed by a user code		
<b>Parameters</b>		
Allows to program parameters related to operation with the Follow Me		
<b>Follow Me Retries</b>	03	01-15
The number of times the Follow Me phone number is redialed		
<b>Voice Message Recurrence</b>	01	01-05
This number of times a voice message repeats itself when establishing a call to a Follow Me number.		

**Communication: Follow-Me**

Parameter	Default	Range
<b>Follow Me Periodic Test</b>		

The Periodic Test enables you to set the time period that the system will automatically establish communication to a Follow Me destination defined with the Periodic Test event.

## 5. Programming: Audio Messages Menu

This menu is used to define voice message parameters. The Audio Messages menu is divided into the following sub menus:

### 1. Assign Message

### 2. Local Message

#### 5.1 Assign Message

The installer can assign a voice message to a **zone**, **partition**, **output** or **macro**. When an event occurs this voice message will be heard accordingly.

Each message can be comprised of up to 4 words. Each word has been pre-recorded and assigned a number. When comprising a message the installer will enter the number of each word into the message sequence. The system recognizes the numbers and sounds the words assigned to those numbers. For example: For the system to sound “Top Floor Guest Bedroom”, the installer must enter the following sequence: 119 050 061 019.

The table in *Appendix C: Library Voice Messages* displays the directory of the pre-recorded programming descriptors, each is identified by a 3 digit number.

**Note:** The first five descriptors allow for customized words specific for the client's needs. The customized words can be recorded via the telephone. Each recording is 2 seconds long.

#### To assign a message follow this procedure:

1. Go to Programming → Audio Messages → Assign Message.
2. Select the relevant device and go to **Define**.
3. Enter the relevant descriptor numbers (see *Appendix 3: Library Voice Messages*) and press  .
4. Go to **Play** to hear the message.

#### 5.2 Local Message

Upon event occurrence, the system can announce the security situation to occupants of the premises by sounding a local announcement message. This announcement message can be enabled or disabled, per event. Enable or disable each message announcement according to your customer request.

#### Audio Messages: Local Messages

Parameter	Description	Default
Intruder alarm	Intruder alarm	Yes
Fire alarm	Fire alarm	Yes
Emergency	Emergency (medical) alarm	Yes
Panic alarm	Panic alarm	Yes

**Audio Messages: Local Messages**

Parameter	Description	Default
Tamper alarm	Tamper alarm	Yes
Environmental alert	Flood, Gas, CO or Temperature alert	Yes
Away arm	System/Partition armed in Away(Full arm)	Yes
Stay arm	System/Partition armed in Stay(Part set arm)	Yes
Disarm	System/Partition disarmed	Yes
Audible Status	Status heard when pressing the status button on the keypad/remote control	Yes
Exit / Entry	System in exit or entry delay	Yes
Auto arm	System in auto arm process	Yes
Output On/Off	Output activated or deactivated (Outputs defined as Follow Code)	No
Walk test	Walk test. The Agility will sound the zone number and description	Yes
No Movement	No movement message	Yes
Miscellaneous	Chime status and Macro messages	Yes

## Testing menu

The following menu is used to perform tests on the system. Note that each test refers to the last time the device was activated. Tests can be performed on the following elements:

1. Main Unit
2. Zone
3. Remote Control
4. Keypad
5. Siren
6. GSM
7. IP Unit
8. UO Unit

### 1. Main Unit

---

#### Main Unit

---

##### Parameter

---

##### Noise Level

---

This feature establishes the threshold noise level of the main unit receiver. The threshold noise level can be established automatically or manually (when using a keypad).

##### To establish the main unit receiver's noise level:

**Automatic:** For automatic calibration select [2] Calibration. After the calibration process is accomplished, the new noise threshold level is displayed.

**Manual:** For manual calibration select [1] View/Edit. The value displayed is the last measured value. Set a new threshold level and press  to confirm.

#### Siren

---

Activates the main unit siren.

#### Speaker

---

Sounds the local test message: "Test message". Select *Start* to activate the feature. Select *Stop* to end the test.

#### Battery

---

Displays the battery voltage of the main unit.

#### Version

---

Displays the main unit's software version.

#### Serial Number

---

Displays the main unit's serial number.

## 2. Zone

### Zone

#### Parameter

##### Comm Test

Displays the results of the last measurement performed after the last transmission (last detection or last supervision signal). To receive an updated signal strength, activate the detector prior to performing the communication test.

For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main unit.

##### Battery Test

Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.

##### Walk Test

Used to easily test and evaluate the operation of selected zones in your system. It is recommended to perform walk test after installing all wireless devices and also prior to performing Testing operation.

The keypad LCD displays the following information:

Zone xx:  
TRIP TMP TRBL

Zone number; TRIP: Successful detection; TMP: Tamper detection and Trbl: Low battery

### Version

This menu displays software version of the selected 2-way detector.

## 3. Remote Control

### Remote Control

#### Parameter

#### Default      Range

##### Comm Test

Displays the results of the last measurement performed after the last transmission. To receive an updated signal strength, activate the remote control prior to performing the communication test.

For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main unit.

##### Battery Test

Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.

##### Version

This menu displays information regarding the 2-way remote control's version.

## 4. Keypad

### Keypad

#### Parameter

**Default****Range**

#### Comm Test

Displays the results of the last measurement performed after the last transmission. To receive updated signal strength, activate the keypad prior to performing the communication test.

For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main unit

#### Battery Test

Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.

#### Version

This menu displays information regarding the keypad's version.

## 5. Siren

### Siren

#### Parameter

#### Comm Test

The siren communication test performs a communication test between the Agility and the selected siren. The value displayed indicates the siren's signal strength as received by the Agility.

For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main unit.

#### Battery Test

Speaker batteries voltage: Tests the selected siren's speaker batteries voltage.

Radio (Transceiver) batteries voltage: Tests the selected siren's radio's batteries voltage.

#### Sound Test

Activates squawk sound in the selected siren.

**Siren**
**Parameter**
**Noise Level**

This feature establishes the threshold noise level of the wireless siren receiver. The threshold noise level can be established automatically or manually (when using a keypad).

**To establish a siren receiver's noise level:**

1. Select the siren for which you want to calibrate its receiver.
2. For automatic calibration select [2] **Calibration**. After the calibration process is accomplished, the new noise threshold level is displayed.
3. For manual calibration select [1] **View/Edit**. The value displayed is the last measured value. Set a new threshold level and press  to confirm.

**Version**

This menu displays information regarding the siren's version.

**6. GSM**
**GSM**
**Parameter**
**Default      Range**
**Signal (RSSI)**

Displays the signal level measured by the GSM module. (0=No signal, 5= Very high signal)

**Version**

Displays information regarding the GSM card version.

**IMEI**

View the IMEI number of the GSM module. This number is used for identification of the Agility at the RISCO IP receiver when using GSM or GPRS communication.

**7. IP Unit**
**IP Unit**
**Parameter**
**Default      Range**
**IP Address**

View the IP address of the Agility

**Version**

View the version on the IP card

**IP Unit**

Parameter	Default	Range
<b>MAC Address</b>		

View the MAC address of the IP card. This number is used for identification of the Agility at the RISCO IP receiver when using IP communication.

**8. UO Unit****UO Unit**

Parameter	Default	Range
<b>Comm Test</b>		
Displays the results of the last measurement performed after the last transmission. To receive an updated signal strength, activate the UO unit prior to performing the communication test.		
For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main unit.		
<b>Battery Test</b>		
Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.		
<b>Version</b>		
This menu displays information regarding the UO unit's version.		

**Activities Menu**

The installer can perform special activities on the system via the Activities menu. Some of these activities can also be performed by the user.

**Activities**

Parameter	Default	Range
<b>Main Buzzer On/Off</b>		
Used to activate/deactivate the main unit buzzer.		
<b>KP Sleep Time</b>	10 seconds	00-60 seconds
Used to set the keypad's Sleep mode time. (The LCD display is turned off.)		
<b>Siren TMP Mute</b>		
Used to silence an alarm initiated by a tamper from a siren for 20 minutes. Use this option for example, when replacing the siren battery.		

## Activities

Parameter	Default	Range
<b>Avoid Report Programming</b>		

Some protocols have a report code to the monitoring station for entering and exiting the installer programming. To avoid the entering report and save time, this function postpones the report for two minutes during which the engineer can enter the programming menu and no report will be made.

### Bypass Box Tamper

Provides ability to bypass box tamper condition. When activated and tamper condition occurs, there will be no alarm, no indication to the MS and no record in the event log.

**Note:** To enable Bypass Box Tamper, both the **Allow Bypass** and **24 Hour Bypass** parameters must be set to **YES** (refer to page 4-6 and page 4-8 for more information).

### Installer Reset

Use this option to reset an alarm.

### Configuration Software Connect

Enables to establish remote communication with the configuration software at a predefined location through IP or GPRS.

**Note:** The location of the configuration software should be predefined under Communication→Configuration Software→IP Gateway

### Firmware Update

This option activates a firmware update process. The update can be established through IP or GPRS. The location of the new firmware should be predefined under Installer Programming→System→Firmware Update.

Once the communication method is selected (IP or GPRS) a special manufacturer password should be entered. Please refer to your local RISCO branch for this password.

## Follow Me Menu

### Follow Me

#### Parameter

#### Define

Used to define Follow Me destinations phone number or E-mail address according to its type: Voice message, SMS or E-mail

#### Test FM

Used to test Follow Me reporting.

## Clock Menu

Clock				
Parameter	Default	Range		
<b>Time + Date</b>				
Allows the setting of the system time and date. This definition is required for setting the scheduler programming in the system.				
<b>Scheduler</b>	On/Off			
Enables you to activate or deactivate preprogrammed schedules that were defined by your installer. Up to 8 weekly programs can be defined in the system during which the system automatically arms / disarms or activates utility outputs.				
<b>Note:</b> The definition of the scheduling programs is done from the configuration software.				
<b>Automatic Clock</b>				
Used to get an automatic time update (NTP or Daytime) through the IP network or GPRS.				
<b>Server</b>	Select the Internet time protocol NTP or Daytime			
<b>Host</b>	The IP address or server name.			
<b>Port</b>	The server port.			
<b>Time Zone (GMT/ UTC)</b>				
Use the  key to add an hour to the GMT/UTC time. Use the  key to subtract an hour from the GMT/UTC time.				

## Event Log Menu

Allows the viewing of significant system events including date and time. Scroll the list using the arrow keys to view the events in the system.

## Macro Menu

### Programming Macro Keys

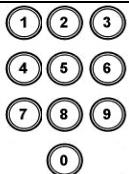
Agility enables the installer or Grand Master to record a series of commands and assign them to a macro. When the macro is pressed, the recorded commands are executed from beginning to end. Up to 3 macros can be programmed to a system using the Agility keypad or the Agility Configuration Software.

Before programming a macro, it is recommended to perform your required series of commands, making a note of every key you press while doing so.

**Note:** Macros cannot be programmed to perform disarming commands.

### To program a macro:

1. In the Macro menu select a macro (A, B or C) and press .
2. Enter the sequence of characters according to the following table:

Key	Represents
	Used to enter numerical characters
	Used to move the cursor to the left
	Used to move the cursor to the right
Press 1 twice	Represents the  character
Press 3 twice	Represents the  character
Press 4 twice	Represents the  key
Press 6 twice	Represents the  key
Press 7 twice	Represents the * character
Press 9 twice	Represents the # character
	Deletes your entry from the cursor position forward
	Use to toggle between  /  /  /  /#/* and all of the numeric characters
	Used to end the sequence and save it to memory

3. Press  to save your entry.

The series of characters is saved and assigned to the selected macro.

*For example:*

To arm partition 1 with the code 1234, enter the following sequence:

1  1 2 3 4

### Activating a Macro

Press 7/8/9 on the keypad for 2 seconds to activate the macro A/B/C respectively. A confirmation message will be heard: "[Macro X] activated".

## Appendix A Report Codes

<b>Report Codes</b>			
<b>Parameter</b>	<b>Contact ID</b>	<b>SIA</b>	<b>Report Category</b>
<b>Alarms</b>			
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Fire alarm	115	FA	Urgent
Fire alarm restore	115	FH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
Duress alarm	121	HA	Urgent
Duress alarm restore	121	HH	Urgent
Box tamper	137	TA	Urgent
Box tamper restore	137	TR	Urgent
Confirmed alarm	139	BV	Urgent
Confirmed alarm restore	139		Urgent
Recent Close	459		Non- urgent
<b>Main Troubles</b>			
Low battery	302	YT	Non- urgent
Low battery restore	302	YR	Non- urgent
AC loss	301	AT	Non- urgent
AC restore	301	AR	Non- urgent
Clock not set	626		Non- urgent
Clock set	625		Non- urgent
False code	421	JA	Non- urgent
False code restore	421		Non- urgent
Main phone trouble	351	LT	Non- urgent
Main phone trouble restore	351	LR	Non- urgent
RF Jamming	344	XQ	Non- urgent
RF Jamming restore	344	XH	Non- urgent
GSM trouble	330	IA	Non- urgent
GSM trouble restore	330	IR	Non- urgent

**Report Codes**

Parameter	Contact ID	SIA	Report Category
GSM Pre-Alarm			Non- urgent
IP Network trouble			Non- urgent
IP Network trouble restore			Non- urgent
<b>Arm/Disarm</b>			
User Arm	401	CL	Arm/Disarm
User Disarm	401	OP	Arm/Disarm
Stay arm	441	CG	Arm/Disarm
Disarm after alarm	458	OR	Arm/Disarm
Keyswitch Arm	409	CS	Arm/Disarm
Keyswitch Disarm	409	OS	Arm/Disarm
Auto Arm	403	CA	Arm/Disarm
Auto Disarm	403	OA	Arm/Disarm
Remote Arm	407	CL	Arm/Disarm
Remote Disarm	407	OP	Arm/Disarm
Forced Arm	574	CF	Arm/Disarm
Quick Arm	408	CL	Arm/Disarm
No Arm	654	CD	Arm/Disarm
Auto Arm fail	455	CI	Arm/Disarm
<b>Detectors(Zones)</b>			
Burglary alarm	130	BA	Urgent
Burglary alarm restore	130	BH	Urgent
Fire alarm	110	FA	Urgent
Fire alarm restore	110	FH	Urgent
Foil alarm	155	BA	Urgent
Foil alarm restore	155	BH	Urgent
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
24 Hour alarm	133	BA	Urgent
24 Hour alarm restore	133	BH	Urgent

**Report Codes**

Parameter	Contact ID	SIA	Report Category
Entry/Exit	134	BA	Urgent
Entry/Exit restore	134	BH	Urgent
Water (Flood) alarm	154	WA	Urgent
Water (Flood) alarm restore	154	WH	Urgent
Gas alarm	151	GA	Urgent
Gas alarm restore	151	GH	Urgent
Carbon Monoxide alarm	162	GA	Urgent
Carbon Monoxide alarm restore	162	GH	Urgent
Environmental alarm	150	UA	Urgent
Environmental alarm restore	150	UH	Urgent
Low Temperature (Freeze alarm)	159	ZA	Urgent
Low Temperature restore	159	ZH	Urgent
High Temperature	158	KA	Urgent
High Temperature restore	158	KH	Urgent
Zone trouble	380	UT	Urgent
Zone trouble restore	380	UJ	Urgent
Burglary trouble	380	BT	Urgent
Burglary trouble restore	380	BJ	Urgent
Zone bypass	570	UB	Urgent
Zone bypass restore	570	UU	Urgent
Burglary bypass	573	BB	Urgent
Burglary bypass restore	573	BU	Urgent
Zone supervision loss	381	UT	Urgent
Zone supervision restore	381	UJ	Urgent
Tamper	144	TA	Urgent
Tamper restore	144	TR	Urgent
Zone lost	381	UT	Urgent
Zone lost restore	381	UJ	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Soak fail	380	UT	Urgent

**Report Codes**

Parameter	Contact ID	SIA	Report Category
Soak fail restore	380	UJ	Urgent
Zone Alarm	134	BA	Urgent
Zone Alarm restore	134	BH	Urgent
Zone confirm alarm	139	BV	Urgent
Zone confirm alarm restore	139		Urgent
No activity	393	NC	Urgent
No activity restore	393	NS	Urgent

**Wireless Keypad**

Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Keypad lost	355	BZ	Urgent
Keypad lost restore	355		Urgent

**Wireless Keyfob**

Arm	409	CS	Arm/Disarm
Disarm	409	OS	Arm/Disarm
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent

**Wireless Siren**

Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Siren lost	355	BZ	Urgent
Siren lost restore	355		Urgent

**Wireless I/O Expander**

Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
I/O Expander lost	355	BZ	Urgent
I/O Expander lost restore	355		Urgent

**Report Codes**

Parameter	Contact ID	SIA	Report Category
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
AC trouble	301	AT	Non- urgent
AC trouble restore	301	AR	Non- urgent
RF Jamming	380	XQ	Urgent
RF Jamming restore	380	XH	Urgent
<b>Miscellaneous</b>			
Enter programming (local)	627	LB	Arm/Disarm
Exit programming (Local)	628	LS (LX )	Arm/Disarm
Enter programming (Remote)	627	RB	Arm/Disarm
Exit programming (Remote)	628	RS	Arm/Disarm
MS periodic test	602	RP	Non- urgent
MS keep alive (polling)	999	ZZ	Urgent
Call back	411	RB	Non- urgent
System reset	305	RR	Urgent
Listen in begin	606	LF	Urgent
Cancel Report	406	OC	Urgent
Walk Test	607	BC	Non- urgent
Walk Test restore	607		Non- urgent
Exit Error	374		Non- urgent

## Appendix B Installer Event Log Messages

Event Message	Description
Activate UO=xx	UO XX activation
Actv UO=xx KF=zz	UO XX is activated from remote control ZZ
Alarm abort P=y	Alarm aborted on partition Y
Alarm Zone=xx	Alarm in zone no. XX
Anti-code reset	Remote reset
Auto Add GSM	GSM Module added to the main unit
Auto Add IP card	IP Module added to the main unit
Auto Add MODEM	Modem added to the main unit
Auto Del GSM	GSM Module was removed from the main unit
Auto Del IP card	IP Module removed from the main unit
Auto Del MODEM	Modem removed from the main unit
Auto test fail	Failure of zone self-test
Auto test OK	Automatic zone self-test OK
Away fail P=y	Partition Y failed to arm
Away:P=y C=zz	Partition Y armed by user no. ZZ
Away:P=y KF=zz	Partition Y armed by remote control ZZ
Bell tamper	Bell tamper alarm
Bell tamper rst	Bell tamper alarm restore
Box tamper	Box tamper alarm from main unit
Box tamper rst	Box tamper alarm restore
Bypass Box+Bell	Box + Bell tamper is bypassed
Bypass Trbl C=xx	System troubles were bypassed by user XX
Bypass Zone=xx	Zone no. XX is bypassed
Cancel Alarm P=x	Cancel alarm event has occurred from partition X. A valid user function is entered to reset the alarm after the defined Abort alarm time
Change code=xx	Changing user code XX
Change FM=yy	Changing Follow-Me number YY
Change tag=xx	Changing keypad tag for user XX
Clock not set	Time is not set
Clock set C=xx	Time defined by user no. XX
CO Alarm Zn=xx	CO alert from zone XX defined as a CO detector
CO Rst. Zn=xx	CO alert restored from zone XX defined as a CO detector
Com ok IP card	Communication OK between the Agility and IP card
Comm OK Siren=y	Communication OK between the Agility and Siren Y
Comm. OK GSM	Communication OK between the Agility and GSM
Comm.OK I/O Mdl.	Communication OK between the Agility and I/O module
Conf. alarm P=y	Confirmed alarm occurred in partition Y

Event Message	Description
Confirm rs Z=xx	Restore zone confirmed alarm
Confirm Zone=xx	Confirmed alarm occurred from zone XX
CP reset	The control panel has reset
Date set C=xx	Date defined by user no. XX
Day Away:P=y	Daily arm on partition Y
Day disarm:P=y	Daily disarm on partition Y
Day stay: P=y	Daily STAY arming in partition Y
Disarm:P=y C=zz	Partition Y disarmed by user ZZ
Disarm: P=y KF=zz	Partition Y disarmed by remote control ZZ
Duress C=xx	Duress alarm from user no. XX
Enter program	Entering installer programming from keypad or configuration software
Exit Error Zn=xx	Exit error event from zone XX The zone was left open at the end of the exit time
Exit program	Exiting installer programming from keypad or configuration software
False code	False code alarm
False restore	False code alarm restore
Fire Keypad=y	Fire alarm from wireless keypad Y
Fire ok Zone=xx	Trouble restore in fire zone no. XX
Fire trbl Zn=xx	Trouble in fire zone no. XX
Fire Zone=xx	Fire alarm in zone no. XX
Foil ok Z=xx	Restore in foil (Day) zone no. XX
Foil Zone=xx	Trouble in foil (Day) zone no. XX
Forced P=y	Partition Y is force armed
Found Zone=xx	Wireless zone found, zone no. XX
Gas Alarm Zn=xx	Gas (natural gas) alert from zone XX defined as a gas detector
Gas Rst. Zn=xx	Gas (natural gas) alert restored from zone XX defined as a gas detector
GSM:IP OK	IP connection OK
GSM:IP Trouble	IP address is incorrect
GSM:Mdl comm.OK	Communication between the GSM/GPRS Module and the Agility is OK
GSM: Module comm.	Internal GSM/GPRS BUS module trouble
GSM:NET avail.	GSM network is not available
GSM:NET avail.OK	GSM Network is available
GSM:NET qual.OK	GSM Network quality is acceptable
GSM:NET quality	The GSM RSSI level is low
GSM:PIN code err	PIN code entered is incorrect
GSM:PIN code OK	PIN code is correct

Event Message	Description
GSM:PUK Code err	PUK code required
GSM:PUK Code OK	PUK Code entered is correct
GSM:SIM OK	SIM Card in place
GSM:SIM trouble	SIM card missing or not properly sited
H.Temp rst Zn=xx	High temperature alert restored from zone XX defined as a temperature detector
High Temp. Zn=xx	High temperature alert from zone XX defined as a temperature detector
I/O:AC Rstr	AC power restore on I/O module
I/O:AC Trouble	AC power trouble on I/O module
I/O: Battery Rstr	I/O module battery trouble restored
I/O: Battery Trbl	I/O module battery trouble alert
I/O: Jamming	I/O module jamming alert
I/O: Jamming Rstr	I/O module jamming alert restored
I/O: Lost	I/O module is regarded as lost following supervision test
I/O: Tamper	I/O module tamper alert
I/O: Tamper Rstr	I/O module tamper alert restored
IO: Lost Restore	The Agility received a signal from I/O module after it has been regarded as lost
IPC:DHCP error	Failed to acquire an IP address from the DHCP server
IPC:DHCP ok	Succeeded to acquire an IP address from the DHCP server
IPC: Network err	Failed to connect to IP network
IPC: Network ok	Successful connection to IP network
IPC:NTP error	Failed to acquire time data from the time server
IPC:NTP ok	Succeeded to acquire time data from the time server
Jamming OK Zn=xx	Zone XX jamming OK
Jamming restore	Wireless receiver jamming restore
Jamming Z=xx	Zone XX jamming trouble
KP=y Low Bat.Rst	Low battery trouble restored from keypad Y
KP=y Low Battery	Low battery trouble from keypad Y
Ksw away:P=y	Partition Y is armed by key switch
Ksw disarm:P=y	Partition Y is disarmed by key switch
L.bat rstr KF=yy	Low battery trouble restore from wireless remote control YY
L.Temp rst Zn=xx	Low temperature alert restored from zone XX defined as a temperature detector
Lost Zone=xx	Wireless zone lost, zone no. XX
Low Bat rs Z=xx	Low battery trouble restored from wireless zone no. XX
Low bat. Zn=xx	Low battery trouble from wireless zone no. XX
Low bat.KF=yy	Low battery trouble from wireless remote control XX

Event Message	Description
Low Temp. Zn=xx	Low temperature alert from zone XX defined as a temperature detector
Main:AC restore	AC power restore on main panel
Main: Battery rst	Low battery trouble restore from the main panel
Main: Low AC	Loss of AC power from the main panel
Main: Low battery	Low battery trouble from the main panel
MS=y call error	Communication fail trouble to MS phone no. Y
MS=y restore	Communication fail trouble restore to MS phone no. Y
Msg Box Tamper	Tamper alarm from the Listen In message box unit
Msg Box Tmp Rst.	Tamper alarm restore from the Listen In message box unit
No Com IP card	Communication failure between the Agility and IP card
No comm I/O Mdl.	Communication failure between the Agility and I/O module
No comm Siren=y	Communication failure between the Agility and siren Y
No comm. GSM	No communication between the GSM/GPRS Module and the Agility
Phone fail	If the phone line is cut or the DC level is under 1V
Phone restore	Phone line trouble restore
Police Keypad=y	Police (panic) alarm from wireless keypad Y
Police KF=yy	Police (panic) alarm from remote control YY
PTM: Send Data	Load new parameters into the Agility from PTM accessory
Radio l.bat S=y	Radio low battery trouble from siren Y
Radio l.bat rS=y	Radio low battery restore from siren Y
Remote away:P=y	The system has been armed from the configuration software
Remote program	The system has been programmed from the configuration software
Remote stay:P=y	The system has been armed in STAY mode from the configuration software
Restore Zone=xx	Alarm restore in zone no. XX
RF Jamming	Wireless receiver jamming
Rmt disarm:P=y	Partition Y disarmed from the configuration software
Siren=y Lost	Siren Y is regarded as lost following supervision test
Siren=y Lost Rst	The Agility received a signal from siren Y after it has been regarded as lost
Soak fail Z=xx	Zone XX has failed in the soak test
Special KP=y	Special alarm from the from wireless keypad Y
Spkr l.bat rsS=y	Speaker low battery restore from siren Y
Spkr low bat S=y	Speaker low battery trouble from siren Y
Start exit P=y	Exit time started in partition Y
Stay:P=y C=zz	Partition Y stay armed by user ZZ
Stay: P=y KF=zz	Partition Y stay armed by remote control ZZ
Tamper I/O Mdl.	Tamper alarm from I/O module
Tamper I/O Mdl.	Tamper alarm restored from I/O module

Event Message	Description
Tamper Keypad=y	Tamper alarm from keypad ID=Y
Tamper rs Zn=xx	Tamper alarm restore on zone no. XX
Tamper rst KP=y	Keypad Y tamper restore
Tamper Siren=y	Tamper alarm from wireless siren Y
Tamper Zone=xx	Tamper alarm from zone no. XX
Tech alarm Zn=xx	Alarm from zone XX defined as Technical
Tech rstr Zn=xx	Alarm restored from zone XX defined as Technical
Tmp rstr Siren=y	Tamper alarm restore from wireless siren Y
Unbyp Box+Bell	Box + Bell reinstated from bypass
Unbypass Zone=xx	Zone no. XX is reinstated from bypass
Unknown event	Unknown event alert
User login C=xx	User XX has entered into programming mode. User 99 represents remote programming from the configuration software
Water Alrm Zn=xx	Flood alarm from zone no. XX
Water rstr Zn=xx	Flood alarm restore on zone no. XX
Z=xx auto bad	Zone self-test failed, zone no. XX
Z=xx auto ok	Zone self-test OK, zone no. XX
Zn=xx Trouble	Zone trouble event from zone XX
Zn=xx Trouble OK	Zone trouble event restore from zone XX

## Appendix C Library Voice Messages

001	(Custom)	E	046	East	M	087	Macro	130	Store
002	(Custom)		047	Elevator		088	Magnet	131	Student room
003	(Custom)		048	Emergency		089	Main	132	Study
004	(Custom)		049	Entrance		090	Master	T	Technical
005	(Custom)		050	Entry		091	Middle	133	Temperature
A			051	Executive		092	Motion	134	Third
006	A	F	053	External	N	093	Near	135	To
007	Above		054	Family		094	New	136	Top
008	Air conditioner		055	Fence		095	North	137	TV
009	An		056	Fire	O	096	Nursery	138	
010	And		057	First		097	Of	139	Under
011	Apartment		058	Flood		098	Office	140	Up
012	Area	G	059	Floor		099	On	141	Upstairs
013	At		060	For	P	100	Outdoor	V	Video camera
014	Attic		061	Foyer		101	Output	W	
B			062	Front		102	Outside	143	Wall
015	Baby's room		063	Game		103	Panic	144	Warehouse
016	Back	H	064	Garage		104	Partition	145	Washroom
017	Balcony		065	Garden		105	Passage	146	West
018	Basement		066	Gas		106	Patio	147	Window
019	Bathroom	I	067	Gate		107	Perimeter	Y	
020	Bedroom		068	Girl's room	R	108	Pool	148	Yard
021	Before		069	Glass		109	Rear	Z	
022	Behind		070	Guest		110	Reception	149	Zone
023	Bottom		071	Hallway		111	Refrigerator	Numbers	
024	Boy's room		072	High		112	Relay	150	0
025	By		073	In		113	Right	151	1
C			074	Indoor		114	Roof	152	2
026	Camera	K	075	Inside		115	Room	153	3
027	Ceiling		076	Internal	S	116	Safe	154	4
028	Cellar		077	Is		117	Safety	155	5
029	Central	L	078	Keyfob		118	Second	156	6
030	Children		079	Kitchen		119	Sensor	157	7
031	Cleaner		080	Landing		120	Shock	158	8
032	CO		081	Left		121	Shop	159	9
033	Computer room		082	Library		122	Shutter		
034	Contact		083	Light		123	Side		
035	Control		084	Living		124	Siren		
036	Corner		085	Lobby		125	Site		
037	Curtain		086	Low		126	Smoke		
D						127	South		
038	Desk					128	Sprinkler		
039	Detector					129	Stairs		
040	Device								
041	Dining								
042	Door								
043	Down								
044	Downstairs								
045	Dressing								

## Appendix D EN 50131 Compliance

### Compliance Statement

Hereby, RISCO Group declares that the Agility series of central units and accessories are designed to comply with:

- EN50131-1, EN50131-3 Grade 2
- EN50130-5 Environmental class II
- EN50131-6 Type A
- UK: DD243:2004, PD 6662:2004, ACPO (Police)
- USA: FCC: Part 15B, FCC part 68
- CANADA: CS-03, DC-01

### Possible logical keys calculations:

- Logical codes are codes punched in the wireless keypad to allow Level 2 (users) and Level 3 (installer) access.
- All codes - 4 digits structure: xxxx
- 0-9 can be used for each digit.
- There are no disallowed codes - codes from 0001 to 9999 are acceptable.
- Invalid codes cannot be created due to the fact that after the code 4<sup>th</sup> digit has been punched, "Enter" is automatically applied. Code is rejected when trying to create a non existing code.

### Possible physical keys calculations:

- Physical keys are implemented in the Wireless Keyfobs.
- It is assumed that only a user possesses a Keyfobs, therefore a physical key is considered as access Level 2
- Each Keyfob has 24 bit identification code comprising  $2^{24}$  options.
- A Keyfob has to be recognized and registered by the Agility, therefore, a "write" process must be performed.
- A valid Keyfob is one "Learned" by the panel and allowing Arm/Disarm
- A non valid Keyfob is one not "Learned" by the panel and not allowing Arm/Disarm.

### System Monitoring

- The main unit is monitored for AC trouble, battery fault, low battery and more.
- The I/O Wireless Expander is monitored for AC trouble, battery fault, low battery and more.
- All other wireless elements are monitored for low voltage battery.

## Setting the Agility to comply with EN 50131 requirements

1. Access the Installer programming mode.
2. From the [1] System menu select [5] to access the Settings menu.
3. From the Settings menu select [4] to access the Standard option.
4. Select EN 50131. Once selected, the following changes will occur in the Agility software:

### Report Codes

Feature	EN 50131 Compliance
<b>Timers</b>	
Phone Line cut delay	Immediate (0 minutes)
Entry Delay	45 seconds (maximum allowed)
AC Delay	Immediate (0 minutes)
Jamming Time	0 minutes
RX Supervision	2 hours
<b>System Controls</b>	
Quick Arm	Set to NO
False Code Trouble	Set to Yes
Forced Arming	Set to NO
Authorize installer	Set to YES
Override Trouble	Set to NO
Restore Alarm	Set to YES
Mandatory Event Log	Set to YES
Restore Trouble	Set to YES
Exit Alarm	Set to NO
20 Minutes Signal	Set to YES
Entry Alarm	Set to NO
Attenuation	Set to YES

## Appendix E Installer Programming Maps

<b>1) Programming</b>	See programming menu on page E-2.		
<b>2) Testing</b>			
<b>1) Main Unit</b>			
	1) Noise Level	4) Battery	
	2) Siren	5) Version	
	3) Speaker	6) Serial Number	
<b>2) Zone</b>			
	1) Communication Test	3) Walk Test	
	2) Battery Test	4) Version	
<b>3) Remote Control</b>			
	1) Communication Test	3) Version	
	2) Battery Test		
<b>4) Keypad</b>			
	1) Communication Test	3) Version	
	2) Battery Test		
<b>5) Siren</b>			
	1) Communication Test	4) Noise Level	
	2) Battery Test	5) Version	
	3) Sound Test		
<b>6) GSM</b>			
	1) Signal	3) IMEI	
	2) Version		
<b>7) IP Unit</b>			
	1) IP Address	3) MAC Address	
	2) Version		
<b>8) I/O Module</b>			
	1) Communication Test	3) Version	
	2) Battery Test		
<b>3) Activities</b>			
	1) Main Buzzer		
	2) KP Sleep Time		
	3) Siren TMP Mute		
	4) Avoid Report Prog		
	5) Bypass Box Tamp		
	6) Installer Reset		
	7) CS Connect		
	8) Firmware Update		
<b>4) Follow Me</b>			
	1) Define		
	2) Test Follow Me		
<b>5) Clock</b>			
	1)Time and Date		
	2) Scheduler Enable		
	3) Auto. Clock		
	1) Server	3) Port	
	2) Host	4) Time Zone	
<b>6) Event Log</b>			
<b>7) Macro</b>			

### Installer Programming menu:

**1) System**

**1) Timers**

- 1) Ex/En Delay 1
- 2) Ex/En Delay 2
- 3) Bell Timeout
- 4) Bell Delay
- 5) AC Off Delay
- 6) Jamming Time
- 7) RX Supervision
- 8) TX Supervision
- 9) Redial Wait
- 0) More

1) Swinger Shutdown

2) No Activity

3) Last Exit Sound

**2) Controls**

**1) Basic**

- Quick Arm
- Allow Bypass
- Quick Status
- False Code Trouble
- Siren Squawk
- Audible Panic
- Buzzer → Bell
- Audible Jamming
- Exit Beeps At Stay
- Forced Arming
- Arm Pre-Warning
- Default Enable
- Main But: Status/Talk
- Quick Learn

**2) Advanced**

- Area
- Global Follower
- Summer/Winter
- 24 Hour Bypass
- Technician Tamper
- Technician Reset
- Installer Tamper
- Low Battery Arm
- Siren Pre-alarm
- Bell 30/10
- Fire Alarm Pattern
- IMQ
- Disable Incoming Call

**3) Communication**

- MS Enable
- Configuration Software Enable
- FM Enable

## 4) EN 50131

- Authorize Installer
- Override Trouble
- Restore Alarm
- Mandatory Events
- Restore Troubles
- Exit Alarm
- Entry Alarm
- 20 Minutes Signal
- Attenuation

## 5) DD243 Prog

- Bypass Exit/Entry
- Entry Disable
- Route Disable
- Installer Confirmation
- Keypad Lock
- Entry Disarm

## 6) CP-01

- Exit Restart
- Auto Stay
- Exit Error
- 3 Min. Bypass

## 3) Labels

- 1) System
- 2) Partition 1
- 3) Partition 2
- 4) Partition 3

## 4) Sounds

### 1) Tamper Sound

- Silent
- Bell
- Buzzer (main)
- Bell + Buzzer
- Bell/A + Buzzer/D
- Bell/A + S/Disarm

- 2) Local Alarm
- 3) Local Squawk
- 4) Ex/En Beeps
- 5) Speaker Volume

## 5) Settings

- 1) Default Panel
- 2) Erase WL Device
- 3) Language
- 4) Standards

EN 50131  
DD243  
CP-01

## 6) Service Info

- 1) Service Name
- 2) Phone

<b>7) Firmware Update</b>	1) Server IP 2) Server Port 3) File Path
<b>2) Radio Devices</b>	
<b>1) Allocation</b>	1) RF Allocation 2) By Serial code 3) Zone Allocation
<b>2) Modification</b>	
	1) Zones
	1) Parameters
	1) Label 2) Serial No. 3) Partition 4) Type 5) Sound 6) Advanced
	1) Chime 2) Controls
	Supervision Forced Arming No Activity LED Enable Abort Alarm
	3) Detection Mode 4) Sensitivity
	2) Alarm Confirmation
	1) Confirm Partition 2) Confirm Zones
	3) Soak Test 4) Cross Zones
<b>2) Keyfobs</b>	
	1) Parameters
	<b>1-Way Keyfob</b> <b>2-Way Keyfob</b>
	1) Label      1) Label 2) Serial No.      2) Serial No. 3) Partition      3) Partition 4) Button 1      4) PIN Code 5) Button 2      5) Panic Enable 6) Button 3      6) UO Button 1 7) Button 4      7) UO Button 2 8) UO Button 3
	2) Controls
	Instant Arm Instant Stay Code Disarm
	3) Parent Control

## 3) Keypads

### 1) Parameters

- 1) Label
- 2) Serial No.
- 3) Emergency Keys
- 4) Function Key
- 5) UO Control

### 2) Controls

RF Wake-up

## 4) Sirens

- 1) Label
- 2) Serial Number
- 3) Partition
- 4) Supervision
- 5) Volume

- 1) Alarm
- 2) Squawk
- 3) Exit Entry

## 5) Strobe (Ext.l)

- 1) Strobe Ctrl
- 2) Strobe Blink
- 3) Strobe Arm Blink

## 5) I/O Modules

### 1) Wired Zones

- 1) Label
- 2) Partition
- 3) Type
- 4) Sound
- 5) Advanced

- 1) Chime
- 2) Control
- 3) Termination
- 4) Loop Response
- 5) Detection Mode

### 2) Outputs

- 1) Label
- 2) Type
- 3) Pattern
- 4) Pulse Length

### 3) X-10 Outputs

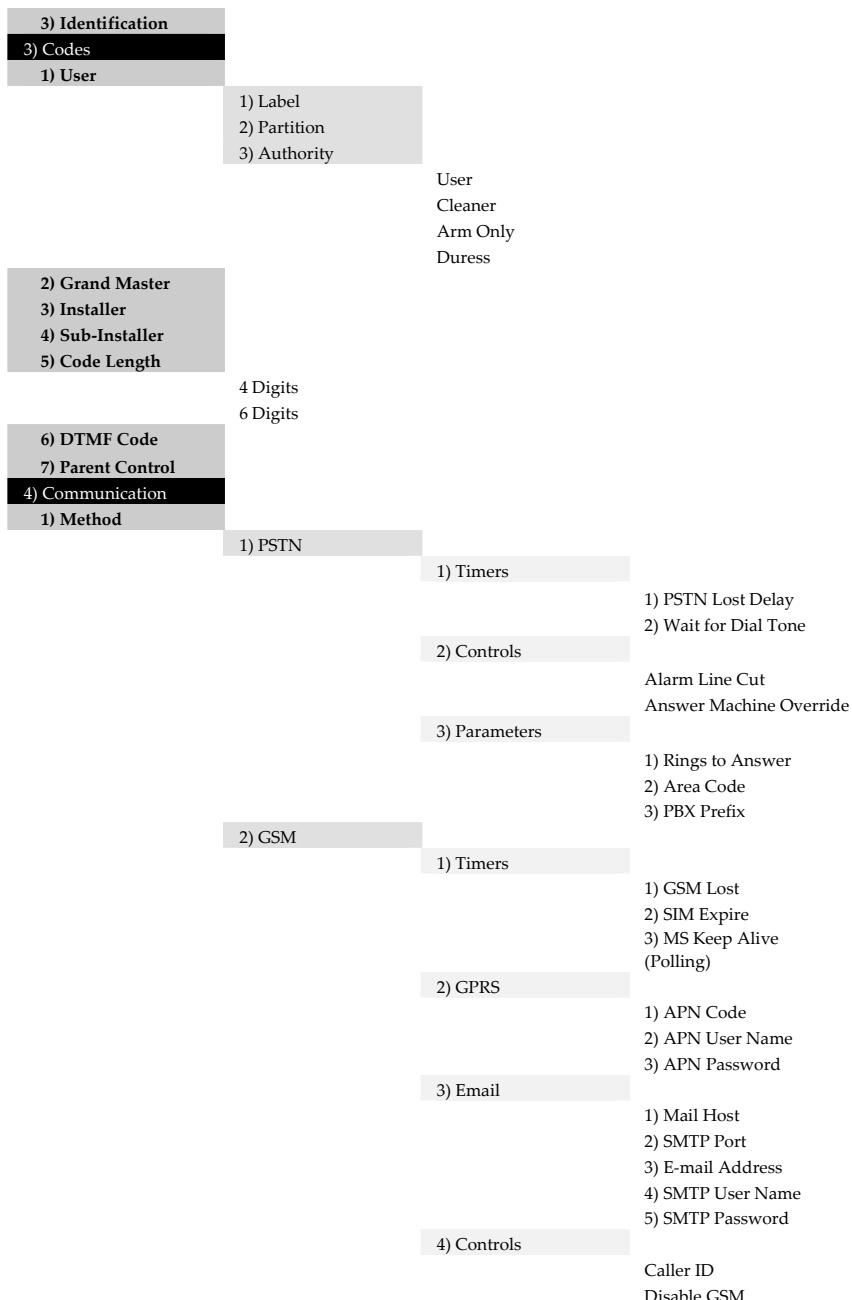
- 1) Label
- 2) Type
- 3) Pattern
- 4) Pulse Length

### 4) Parameters

- 1) Serial No.
- 2) Control

- 1) Supervision
- 2) Quick UO/X10

- 3) X10 House ID
- 4) UO DTMF Control



## 5) Parameters

- 1) SIM PIN Code
- 2) SMS Center Phone
- 3) GSM RSSI
- 4) SIM Number

## 6) Pre-Paid SIM

- 1) Get Credit by
- 2) SMS Receive Phone

## 3) IP

### 1) IP Configuration

- 1) Obtain Auto IP
- 2) Panel IP
- 3) Subnet Mask
- 4) Gateway
- 5) DNS Primary
- 6) DNS Second

### 2) E-mail

- 1) Mail Host
- 2) SMTP Port
- 3) E-mail Address
- 4) SMTP Name
- 5) SMTP Password

### 3) Host Name

- 4) MS Keep Alive
- (Polling)
- 5) Controls

Disable IP

## 2) Monitoring Station

### 1) Report Type

Voice  
SMS  
IP

### 2) Accounts

### 3) Comm Format

Contact ID  
SIA

### 4) Controls

Handshake  
Kissoff

### 5) Parameters

- 1) MS Retries
- 2) Alarm Restore

### 6) MS Timers

- 1) Periodic Test
- 2) Abort Alarm
- 3) Cancel Delay
- 4) Listen In
- 5) Confirmation
- 6) No Arm

- 7) Report Split
  - 1) MS Arm/Disarm
  - 2) MS Urgent
  - 3) MS Non Urgent
- 8) Report Codes
  - 1) Edit Codes
  - 2) Delete All
- 3) Configuration s/w**
  - 1) Security
    - 1) Access code
    - 2) Remote ID
    - 3) MS Lock
  - 2) Call Back
  - 3) IP Gateway
- 4) Follow-Me**
  - 1) Define
    - 1) Report type
      - Voice
      - SMS
      - Email
    - 2) Events
    - 3) Restore events
    - 4) Remote control
  - 5) Partition
  - 2) Controls
    - Disarm stop FM
  - 3) Parameters
    - 1) FM Retries
    - 2) Voice Mesg Rec
    - 3) Periodic test
- 5) Audio**
  - 1) Assign Message**
    - 1) Zone
    - 2) Partition
    - 3) Output
    - 4) X10 output
    - 5) Macro
  - 2) Local Message**
    - 0) Exit

## Appendix F SIA CP-01 Compliance

### Compliance Statement

Hereby, RISCO Group declares that the Agility series of central units and accessories are designed to comply with SIA CP 01.

The minimum requirement system for SIA-FAR Installations to comply with CP-01 standards:

- A minimum of 1 keypad (Agility KP) must be installed
- 1 CP-01 Control Panel (Agility Main)
- All system keypads must be audible (mute disabled).

### Setting the Agility to comply with SIA CP 01 requirement

1. Access the Installer programming mode.
2. From the [1] System menu select [5] to access the Settings menu.
3. From the Settings menu select [4] to access the Standard option.
4. Select CP 01, once selected, the following changes will occur in the Agility software:

#### Report Codes

Feature	CP 01 Compliance
<b>Timers</b>	
Phone Line cut delay	Immediate (0 minutes)
Entry Delay	45 seconds (maximum allowed)
AC Delay	Immediate (0 minutes)
Jamming Time	0 minutes
RX Supervision	2 hours
<b>System Controls</b>	
Quick Arm	Set to NO
False Code Trouble	Set to Yes
Forced Arming	Set to NO
Authorize installer	Set to YES
Override Trouble	Set to NO
Restore Alarm	Set to YES
Mandatory Event Log	Set to YES
Restore Trouble	Set to YES
Exit Alarm	Set to NO

**Report Codes**

<b>Feature</b>	<b>CP 01 Compliance</b>
20 Minutes Signal	Set to YES
Entry Alarm	Set to NO
Attenuation	Set to YES

<b>Feature</b>	<b>Range</b>	<b>Shipping default</b>	<b>Quick Key / Remark</b>
Exit Delay time	45 sec - 255 sec	45 seconds	[1][1][1][2] / [1][1][2][2]
Progress annunciation	Not programmable	Enabled	
Exit Restore	For re-entry during exit delay	Enabled	[1][2][41]
Auto Stay arm on un-vacated premises	If there is no exit after full arm	Enabled	[1][2][42]
Entry Delay(s)	30 sec - 240 sec**	30 seconds	[1][1][1][1] / [1][1][2][1]
Abort Window - for non-fire zones	May be disabled by zone	Enabled	[2][0][4]
Abort window- for non-fire zones	15 sec - 45 sec**	30 seconds	[5][6][0][1]
Abort annunciation	Announce that no alarm was transmitted	Enabled	LCD Display message
Communication Cancel window	5-255 minutes	005 minutes	[5][6][0][2]
Duress feature	Not a duplicate of other user codes	Disabled	[4][1] Can define dedicated user with authority level
Cross zoning	(XX) sec 1-9 minutes	Disabled	[2][7]
Swinger shutdown	For all non-fire zones, shutdown at 1 or 2 trips	One trip	[5][6][8]

Feature	Range	Shipping default	Quick Key / Remark
Fire alarm verification	Depends on sensors	Enabled	[1][2][10]
Call waiting cancel	Depends on user phone line	Disabled (Empty string)	[5][6][0][3] String required for activation
System test (test report + walk test mode + siren)	Test periodically	Disabled	[6][8][0][5] / [6][8][0][6] Report to MS enabled when report code is entered
AC Power Loss indication		Enabled	LCD message display during AC power loss

## **FCC Compliance (Valid for 433MHz versions)**

### **FCC Part 15 Note (Radio):**

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

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

FCC ID: JE4AGILITY

IC: 6564A-AGILITY

### **FCC Warning:**

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

## FCC Part 68 Note (Telecom):

- 1 This equipment complies with Part 68 of the FCC Rules and the requirements adopted by the ACTA. On the bottom panel of this equipment is a label, that contains among other information, a product identifier in the format US:RISAL10BMD2400. If requested, this number must be provided to the telephone company.
- 2 This equipment is designed to be connected to the telephone network using a terminal block, RJ31X or RJ 11. See Installation Instructions for details.
- 3 A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.
- 4 The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. The REN of this alarm system is part of the product identifier that has the format US:RISAL10BMD2400.
- 5 If this equipment US:RISAL10BMD2400 causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
- 6 The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
- 7 If trouble is experienced with this equipment US:RISAL10BMD2400, for repair or warranty information please contact Rokonet Industries USA Inc 2822 NW 79th Ave. Miami, Florida 33122 USA, phone number 305 592 3820, URL: [sales@rokonetusa.com](mailto:sales@rokonetusa.com).  
If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

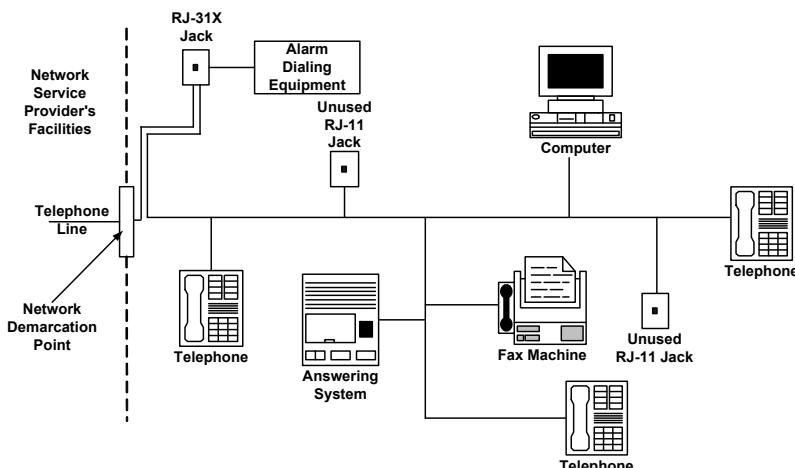
- 8** The user or installer is not to make any repairs to the product or the telephone interface, in case of problems please contact RISCO's customer service.
- 9** Connection to party line service is subjected to state tariffs. Contact the state public utility commission, public service commission or corporation for information.
- 10** If your home has additional alarm dialing equipment other then the AGILITY system which is connected to the telephone line , ensure the installation of this equipment US:RISAL10BMD2400 does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or qualified installer.

**Caution:**

To ensure proper operation, this equipment must be installed according to the enclosed installation instructions. To verify that the equipment is operating properly and can successfully report an alarm, this equipment must be tested immediately after installation, and periodically thereafter, according to the enclosed test.

Equipment must be installed according to the manufacturer instructions in order for the alarm dialing equipment to work properly when other equipment connected to the same line is in use, see drawing below for info.

Verification of the Line Seize capability should be made immediately after installation, and periodically thereafter, in order to ensure that this equipment can initiate a call even when other equipment (telephone, answering machine, computer modem, etc.) connected to the same line in use.



**Customer Premises Equipment and Wiring**

## FCC Part 68 Self Declaration (Telecom):



Date: December 18, 2008

Ref: sDOC\_2400BPS\_modem\_ACTA

## Supplier Declaration of Conformity (SdC)

December 4, 2008

Risco Ltd., Located at 14 Hachoma street, Rishon Lezion 75655, Israel,  
Hereby declare that the 2400 BPS modem ,  
p/n RP128MD2400A, RW132MD2400A , bearing labeling identification number  
US:RISAL10BMD2400 complies with the Federal Communications commission's  
("FCC") rules and regulations 47 CFR part 68, and the Administrative Council on  
Terminal Attachments ("ACTA") adopted technical criteria: TIA-968-A, TIA-968-A-  
1, TIA-968-A-2 and TIA-968-A-3, TIA-968-A-4, TIA-968-A-5 , TIA-1096 and  
TIA-1096-A , Telecommunications – Telephone Terminal Equipment – Technical  
Requirements for Connection of Terminal Equipment To the Telephone Network.

Signed,

Efi Goren  
Certification Manager  
Risco Ltd.



## RISCO Group Safety Warnings:

- Only authorized service personnel are allowed to install the systems.
- For products powered by high voltage\* (not including products powered by an external adapter):  
Installation should be done by a qualified electrician and according to the country's national electrical codes.
- Installation or usage of the product not according to the intended use as defined by RISCO Group and as described in the manuals can result in severe injury or even death.
- For products powered by high voltage:  
The product should be connected to an easily accessible wall outlet, so that power can be disconnected immediately in case of any malfunction or hazard. If the product is permanently connected to AC mains (120/230V), then the connection should include an easily accessible disconnection device (i.e. circuit breaker).
- For products powered by high voltage and/or connected to telephone lines:  
Disconnect the AC power and the telephone line before conducting any maintenance activities.
- If you need to clean the product, use only a soft cloth or sponge moistened lightly with water, and then wipe it dry. The use of abrasive materials of any kind is strictly forbidden.
- For products that contain batteries:  
**CAUTION:** Risk of explosion if battery is replaced by an incorrect type.  
Dispose of used batteries according to battery manufacturer instructions
- Product maintenance should be performed at least once a year by trained and certified personnel.

\* High Voltage: 60 VDC and/or 42.4 VAC

## Notes

## Notes

## **RISCO Group Limited Warranty**

RISCO Group and its subsidiaries and affiliates ("Seller") warrants its products to be free from defects in materials and workmanship under normal use for 24 months from the date of production. Because Seller does not install or connect the product and because the product may be used in conjunction with products not manufactured by the Seller, Seller cannot guarantee the performance of the security system which uses this product. Seller's obligation and liability under this warranty is expressly limited to repairing and replacing, at Seller's option, within a reasonable time after the date of delivery, any product not meeting the specifications. Seller makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose.

In no case shall seller be liable for any consequential or incidental damages for breach of this or any other warranty, expressed or implied, or upon any other basis of liability whatsoever.

Seller's obligation under this warranty shall not include any transportation charges or costs of installation or any liability for direct, indirect, or consequential damages or delay.

Seller does not represent that its product may not be compromised or circumvented; that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection.

Seller, in no event shall be liable for any direct or indirect damages or any other losses occurred due to any type of tampering, whether intentional or unintentional such as masking, painting or spraying on the lenses, mirrors or any other part of the detector.

Buyer understands that a properly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not insurance or a guaranty that such event will not occur or that there will be no personal injury or property loss as a result thereof.

Consequently seller shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning. However, if seller is held liable, whether directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, regardless of cause or origin, seller's maximum liability shall not exceed the purchase price of the product, which shall be complete and exclusive remedy against seller. No employee or representative of Seller is authorized to change this warranty in any way or grant any other warranty.

**WARNING:** This product should be tested at least once a week.

## Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website [www.riscogroup.com](http://www.riscogroup.com) or as follows:

### **United Kingdom**

Tel: +44-161-655-5500

[technical@riscogroup.co.uk](mailto:technical@riscogroup.co.uk)

### **Italy**

Tel: +39-02-66590054

[support@riscogroup.it](mailto:support@riscogroup.it)

### **Spain**

Tel: +34-91-490-2133

[support-es@riscogroup.com](mailto:support-es@riscogroup.com)

### **France**

Tel: +33-164-73-28-50

[support-fr@riscogroup.com](mailto:support-fr@riscogroup.com)

### **Belgium**

Tel: +32-2522-7622

[support-be@riscogroup.com](mailto:support-be@riscogroup.com)

### **USA**

Tel: +1-631-719-4400

[support-usa@riscogroup.com](mailto:support-usa@riscogroup.com)

### **Brazil**

Tel: +55-11-3661-8767

[support-br@riscogroup.com](mailto:support-br@riscogroup.com)

### **China**

Tel: +86-21-52-39-0066

[support-cn@riscogroup.com](mailto:support-cn@riscogroup.com)

### **Poland**

Tel: +48-22-500-28-40

[support-pl@riscogroup.com](mailto:support-pl@riscogroup.com)

### **Israel**

Tel: +972-3-963-7777

[support@riscogroup.com](mailto:support@riscogroup.com)

All rights reserved.

No part of this document may be reproduced in any form without prior written permission from the publisher.