riscogroup.com

Agility 4

Installer Manual

Model: RW132V

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 4 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
- EN50136-1 EN50136-2 and EN50131-10:
  PSTN (SP2); GSM 2G/3G (SP4); IP (SP4); GSM primary and IP secondary (DP3)
  IP primary and GSM secondary (DP3)
  Signaling Security: Substitution security S2
  Information security I3
  For more information, refer to Appendix F
- UK: PD 6662:2017
- USA: FCC: Part 15B, Part 15C, FCC Part 68

Table of Contents

Chapter 1 Introduction

RISCO Group's Agility 4 elegantly combines state-of-the-art video verification utilized from Cloud-based Smartphone / Web apps with advanced wireless security and safety features. Monitoring stations and/or designated system users can now identify false alarms, as video verification helps enable immediate confirmation of an intrusion-in-progress, thereby prioritizing response, increasing efficiency, and giving you on-the-go control and monitoring of your protected site.

Connecting the system to the RISCO Cloud server also enables Smartphone and Web interface users to control and manage their systems remotely, including the ability to arm and disarm the system and perform other operational, programming, and maintenance functions.

The Agility 4 also offers one or more multi-socket communication modules (IP, GSM 2G or GSM 3G) that provide multiple, simultaneous communication channels for direct communication, and for communication via the Cloud.

Featuring a simple installation, and a comprehensive range of peripherals, Agility 4 is the ideal wireless solution for residences and small businesses.

Installing and Servicing the Agility 4 System

The Agility 4 system is intended to be installed and serviced only by an alarm system installer (or similar professional, such as electrician). The system is not intended to be installed or serviced by the user / customer.

Key Benefits

- Flexible plug-in primary / backup communication modules:
  - IP module
  - GSM/GPRS module
  - Fast PSTN module
- 2-way wireless LCD/Panda 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-serial number
- Can combine 1–way or 2-way transmitting devices 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

- Simplified menu logic (only menus of installed devices are displayed, only menus according to the authorization code are displayed)
- Full voice-guided menu for remote system operation

Key Features

- 32 wireless zones
- 3 partitions
- Up to 3 bi-directional wireless keypads
- Up to 8 rolling code keyfobs
- Input/output module:
  - 2-way wireless communication to the Agility 4
  - Local transformer with rechargeable backup batteries
  - 4 wired zones with selectable EOL resistance & 4 outputs (2 x 3A-and 2 x 500 mA relays)
  - Includes X-10 adaptor
- 32 user codes + Grand Master code
- 1000 event log
- Uses regular sealed lead acid battery 6V 3.7 Ah
- 16 Follow Me destinations
- 2-way listen-in and talk with VOX
- Supports 2-way wireless curtain detectors
- Supports magnetic door/contact detectors with shutter
- Supports video verification with IP cameras
- Supports Snapshot Follow Event

Main Features

Detectors
- 32 Wireless zones:
- 4 Wired zones via optional Wireless I/O Expander
- Total zones: 36
- More than 25 zone types
- Full zone supervision
- 2-way and 1-way detectors combined on the same system
- Image capture and transmission via camera
- Snapshot Follow Event

Monitoring Station
- Remote programming, diagnostics and communication test.
- Report to 3 MS.
- Report through PSTN, GSM/GPRS or IP.
- MS polling through IP network.
- Account number for each MS.
- Flexible split reporting for backup.
- Call Save mode for non-urgent reports.
- Remote device enrollment

Communication
- Flexible multi-socket communication over GSM/GPRS, IP or PSTN.
- Backup capability via the Cloud by IP & GPRS/GSM
- Supports major reporting formats.
- Add on module for each communication type.
- Cloud Support

Installer Programming
- Local /Remote using Configuration Software
- Program transfer module.
- Full programming using bi-directional wireless keypad.
- Flexible device enrollment by serial ID serial number or by RF allocation.
- Keypad programming menu adjusted to existing hardware

2-way LCD Keypad
- Fully Wireless
- LCD display
- S.O.S / Two way communication emergency key
- Double tamper protection (Box & Wall)
- 2-Way Wireless Slim Keypad Reader

2-way Panda Keypad
- Fully Wireless
- S.O.S / Two way communication emergency key
- Double tamper protection (Box & Wall)
- Proximity Tag operation
- Battery economy mode

User Operating Tools
- 2-way 8 button key fob
- Bi-directional Keypad
- 4 button keyfob
- Remote phone operation
- SMS
- Configuration software
- Web browser
- Smartphone App for self-monitoring

Follow Me:
- 16 follow me destinations
- Follow me can be defined as voice message, SMS, Email or to smartphones
- User control over the system
- Security code protection
- Unlimited email destinations from the Cloud server

Wireless Features
- Signal jamming indication
- Receiver calibration
- 868MHz/433 MHz radio frequencies
- Programmable supervision time
- Tamper detection in transmitters
- Low battery detection in transmitters

Voice capabilities
- 2-Way communication
- Remote phone operation
- Full voice menu guide
- System event messaging
- Local announcement messages
- Voice description for zones, partitions, etc.

Home Automation
- 4 outputs via wireless I/O expander
- 16 X-10 outputs via wireless I/O expander
- Outputs can follow system, partition, zone or user events
- Outputs can be scheduled, or activated automatically, or by user command (SMS, Web browser or remote phone)

Codes
- 1 installer code
- 1 sub installer code
- 1 grand master code
- 32 user codes
- 4 authority levels
- Optional 4 or 6 digits code definition

Video Verification
- **One or more IP Cameras (inside and outside)**
- Up to 8 eyeWave™ PIR cameras
- Smartphone/Web access
- False alarm reduction

Sirens
- Built-in siren
- Fully wireless external and internal wireless sirens
- Up to 3 Sirens

False Alarm Reduction
- Swinger shutdown
- Zone crossing
- Report delay to MS
- Abort alarm feature
- Soak test
- Final exit zone

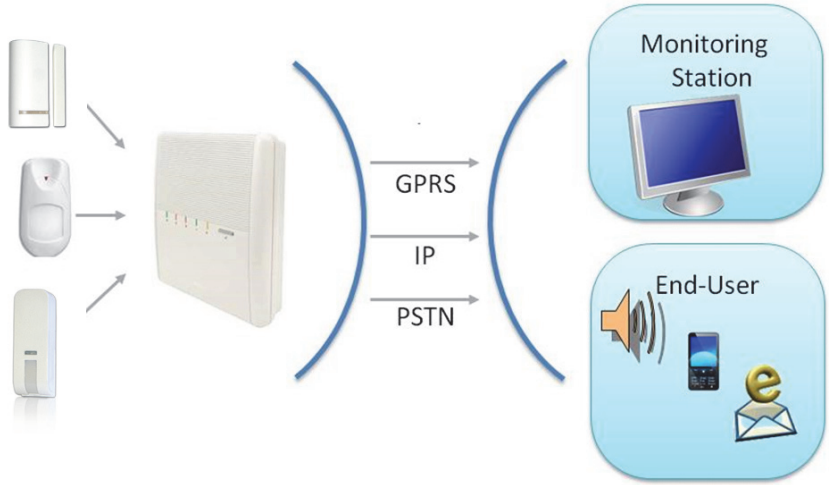
Agility 4 Architecture

Traditional

Agility 4 can communicate information to monitoring stations (and Follow Me destinations) through various communication channels, depending on the physical communication modules installed inside the main panel. Communication can be established through PSTN, IP, or GSM/GPRS.

All methods can be used for:

- Reporting events to monitoring stations
- Sending automatic notifications to the owner
- Remote system programming and maintenance
- Owner remote control



Multiple Reporting Destinations

- System Users: System users can use the Cloud-based iRISCO smartphone and Web User interface for receiving event notifications. Also, multiple Follow-Me recipients are notified of events via voice (voice mail), SMS, or e-mail.
- Monitoring Station: Events are reported to monitoring station(s) directly or via the RISCO Cloud, in any of the supported channels. Agility 4 supports all major monitoring station reporting formats and protocols - including direct connection to the monitoring station or via the Cloud using SIA IP.
- Installer: According to how the system is programmed, installers can also receive Follow-Me reporting, just like system users.

Cloud Communication

Agility 4 can be constantly connected to a dedicated application server (the "RISCO Cloud") via IP or GPRS.

The RISCO Cloud handles all communication between the Agility 4 system, monitoring stations and Smartphone/Web users, enabling remote monitoring and control, as well as a RISCO's VUpoint video verification solution that utilizes IP cameras:

Cloud communication can be defined as either parallel or back-up.

Parallel Communication

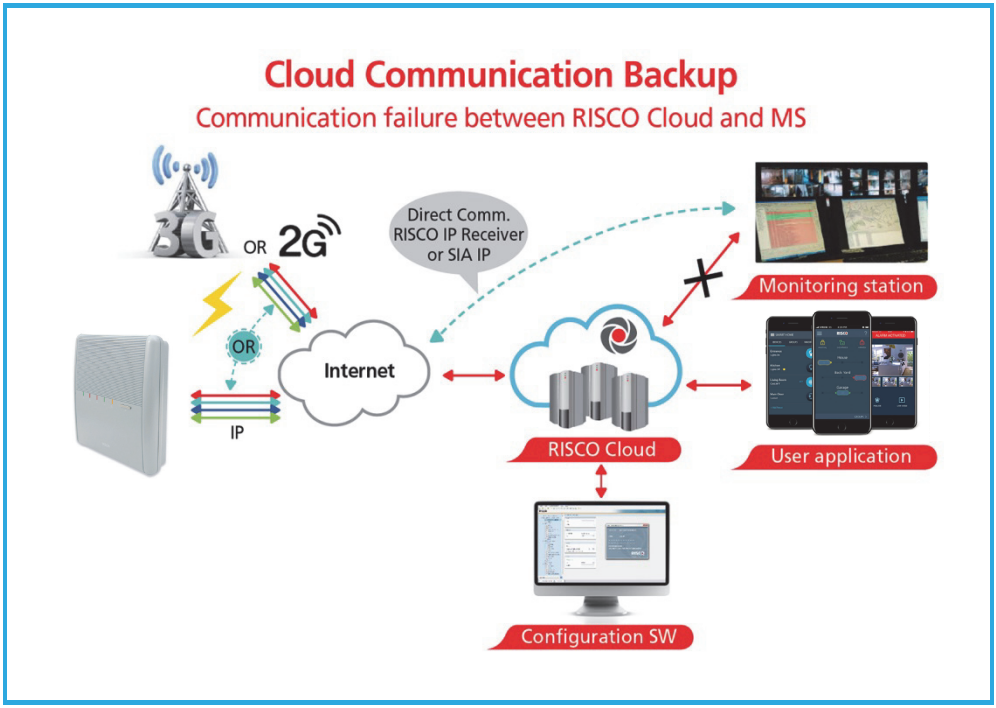
Parallel communication can be accomplished as follows:

- **If using single-socket communication modules** (IP and GPRS/GSM), one of the modules is connected to the Cloud, while the other module is connected directly (for example, for reporting to the monitoring station). Each single-socket module supplies a single communication channel, thus providing the "parallel" communication capabilities by utilizing the two modules.
- **If using multi-socket modules** (IP, GSM 2G, GSM 3G) a single multi-socket module provides multiple communication channels simultaneously ("in parallel") – for example, for user reporting via the Cloud while simultaneously reporting to the monitoring station directly. If two multi-channel modules (IP and GSM) are installed, each module provides its own parallel communication capabilities

Back-up Communication

Backup communication can be accomplished as follows:

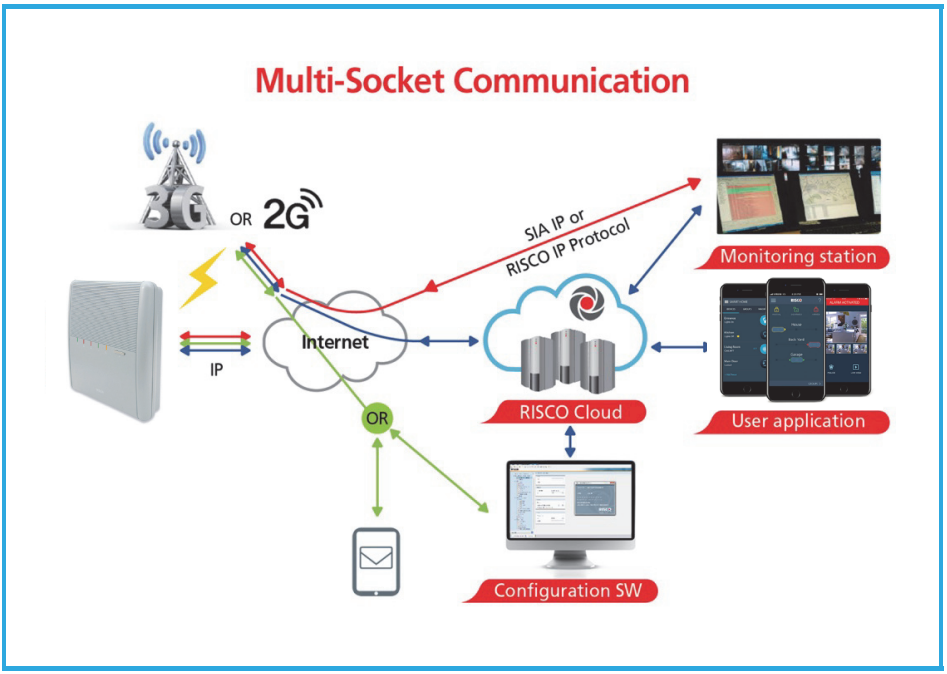
- **If using single-socket communication modules** (IP and GPRS/GSM), a total of two communication channels are available – one channel per module, which can utilize a variety of reporting frameworks – directly, and through the RISCO Cloud (for example, one channel reporting to the user via the Cloud, while the other channel simultaneously reporting directly to the monitoring station). Each of these modules can be used for the primary communication. **NOTE:** PSTN can also be used as a backup or primary channel to the monitoring station.
- **If using multi-socket modules** (IP, GSM 2G, GSM 3G), any individual multi-socket module installed can provide multiple, simultaneous communication channels with a variety of reporting frameworks, both directly and through the RISCO Cloud – for example, one channel reporting to the user via the Cloud, while the other channel simultaneously reporting directly to the monitoring station. If both IP and GSM multi-socket modules are installed, when utilizing direct communication either of the modules can take over and connect as a communication failure backup if the other fails. **NOTE:** PSTN can also be used as a backup or primary channel to the monitoring station.



Enhanced Capabilities of Multi-Socket Communication Modules

Multi-socket communication modules each provide multiple, simultaneous communication channels for services and reporting (for example to the user and monitoring station) – directly, or via the Cloud. Multi-socket module services and reporting abilities include:

- iRISCO Smartphone app & Web user interface: Connected via RISCO Cloud
- Monitoring Station: Direct connection using SIA-IP, or with the RISCO IP Receiver installed at the monitoring station
- Configuration Software: Connection with panel via RISCO Cloud or directly using various channels, including GSM & IP networks – see CS documentation
- Follow-Me: Events are sent to FM destinations by E-mail, SMS, or voice
- SynopSYS: Connection via IP / GPRS



Video Verification with IP Camera

Agility 4 supports RISCOs revolutionary, live **VUpoint** video verification solution which seamlessly integrates an unlimited number of IP cameras to provide an unprecedented level of security and live video monitoring capabilities to monitoring stations and end-users alike. Powered by the RISCO Cloud, VUpoint enables the initiation of live video streaming on demand from any IP camera which can be viewed directly using the iRISCO smartphone or Web applications. VUpoint can be configured so that any detector or event, whether intrusion, safety or panic, can trigger the IP camera. For verification purposes, users can monitor intrusion events using snapshot images and live video, and monitoring stations can identify costly false alarms for higher efficiency.

Snapshot Follow Event

Agility 4 also supports advanced PIR camera functionality to "follow" (capture and send snapshots) of event activations – other than those of the PIR camera itself – which occur within the PIR's partitions. This, together with video verification, enables comprehensive visual verification capabilities for your system.

Technical Specifications

The following technical specifications are applicable for the Agility 4:

Electrical Characteristics	
Power	230 VAC (-15%+10%), 50 Hz, 50 mA
Units consumptions	Main board: Typically 130 mA GSM: Standby 35 mA, Communication 300 mA Modem: Standby 20 mA, Communication 60 mA IP Card: 115 mA (max)
Backup battery	Sealed lead acid battery 6V 3.7 Ah
Voice Configuration	External, in parallel with internal or additional external Audio Unit
Internal Siren intensity	100 dBA @1 m
Operating temperature	-10°C to 55°C (14°F to 131°F)
Storage temperature	-20°C to 60°C (-4°F to 140°F)
Physical Characteristics	
Dimension	268.5 mm x 219.5 mm x 64 mm (10.57 x 8.64 x 2.52 in)
Weight (no battery)	1.31 kg (2.9 lbs) –full configuration GSM module: 45 gr. (.1 lbs) IP module: 34 gr. (.07 lbs)
Wireless Characteristics	
Radio Immunity	According to EN 50130-4
Power Output	868.65 MHz: 10mW Max. 869.525 MHz: 100mW Max.
Frequency	868.65 MHz or 433.92 MHz
Camera Frequency	869.525 MHz, 916 MHz, 430 MHz

Important Safety Precautions

WARNING: Installation or usage of this product that is not in accordance with the intended use as defined by the supplier and as described in the instructional materials can result in damage, injury or death.

WARNING: Make sure this product is not accessible by children and those for whom operation of the system is not intended.

WARNING: Customer should never attempt to repair the wireless security alarm system or component, nor try to open the main panel casing, as doing so could result in damage, injury or death – customer should always contact your installer / supplier agent for service.

WARNING: This main panel should be connected to an easily-accessible wall outlet, so that power can be disconnected immediately in case of malfunction or hazard. If the unit is permanently connected to an electrical power supply, then the connection should include an easily-accessible disconnection device, such as a circuit breaker.

WARNING: Coming into contact with 230 VAC can result in death. If the main panel is opened while it is connected to the electrical power supply, be extremely careful not to handle the power supply module or other hardware that is connected to the 230 VAC.

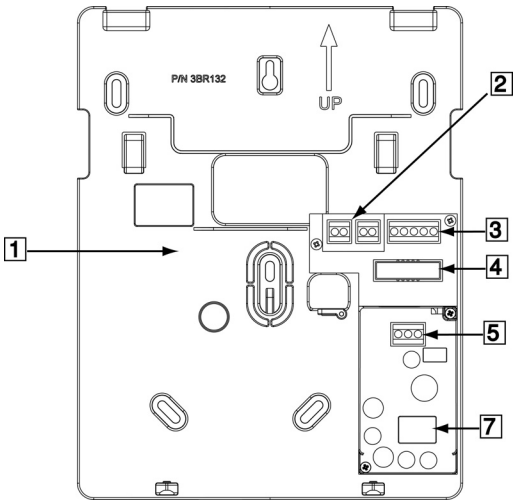
WARNING: Risk of explosion exists if a battery is replaced by an incorrect type.

CAUTION: Dispose of used system component batteries according to applicable law and regulations.

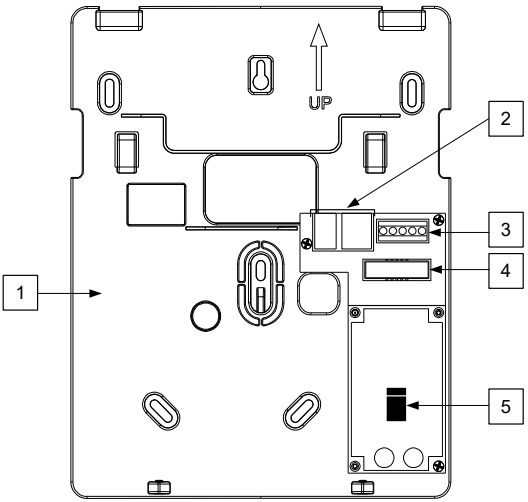
Chapter 2 Installing the Agility 4

Agility 4 Main Components

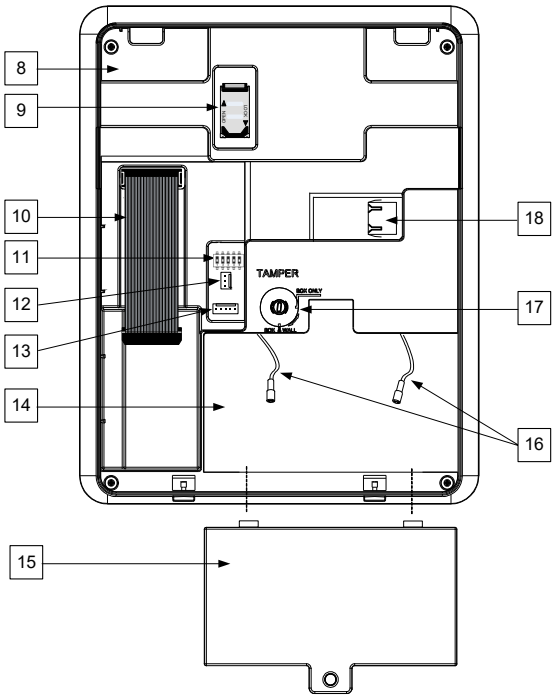
The illustration below shows the internal components when the main panel's mounting bracket (back cover) is detached from the main panel housing.



Main Panel Bracket – Configuration A:	
1	Main panel mounting bracket
2	Telephony terminals
3	Terminal block (peripherals, ground)
4	Ribbon cable jack
5	AC connection terminals (or DC socket)
7	Transformer



Main Panel Bracket – Configuration B	
1	Main panel mounting bracket
2	Telephony terminals
3	Terminal block (peripherals, ground)
4	Ribbon cable-connector
5	AC connection terminals (or DC socket)



Main Panel Housing	
8.	Main panel
9.	SIM card holder
10.	Ribbon cable
11.	DIP switches
12	RS 232 connector
13	PTM connector
14.	Battery compartment (shown with battery removed)
15.	Battery compartment cover
16.	Battery connectors
17.	Tamper switch
18.	IP card network connector

Describing the Communication Modules

PSTN

The Agility 4's PSTN modem is an easy-to-add plug-in module that enables a typically inexpensive PSTN connection, for use as either the primary communication channel or as a failure back-up channel to Cloud-communication via-GSM/GPRS or IP. The modem enables the panel to communicate with a monitoring station using common format protocols (SIA, Contact ID).

GSM/GPRS

The easily-installed Agility 4's GSM/GPRS plug-in module enables system communication over 2G/3G networks for both users and monitoring stations, for event reporting, system control, and programming. GSM/GPRS can be used as the primary communication channel, or as a failure back-up for IP or PSTN communication channels.

GPRS connectivity enables the system to be constantly connected to the RISCO Cloud, which in turn enables visual verification to end users and monitoring stations alike, and provides end users with system control via the Smartphone and Web applications. Cloud-connected users can receive real-time push notification messages to Smartphones, or e-mail notifications.

Without Cloud connectivity, users can additionally control the system using DTMF or SMS, and can also be configured to receive event notifications via SMS, voice messages, and e-mail (in parallel to the Cloud-based notifications), depending on system configuration. Reporting events to monitoring stations is via GPRS, voice, or SMS (using the RISCO IP Receiver). Events can be reported in SIA, SIA IP, and Contact ID monitoring protocols. The GSM/GPRS module also supports two-way voice communication between users and the monitoring station, which can be beneficial for elderly care, especially in times of emergency.

IP

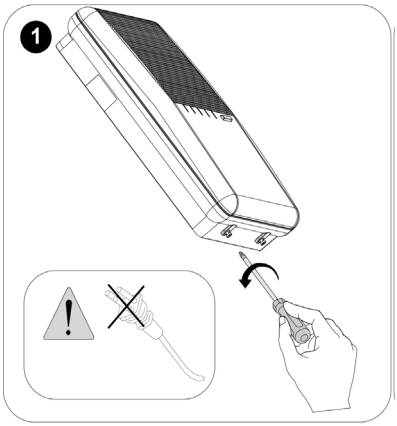
The easily-installed Agility 4's IP plug-in module enables system communication over a TCP/IP network. It can be used as the primary communication channel or as a failure back-up for GSM/GPRS or PSTN communication channels.

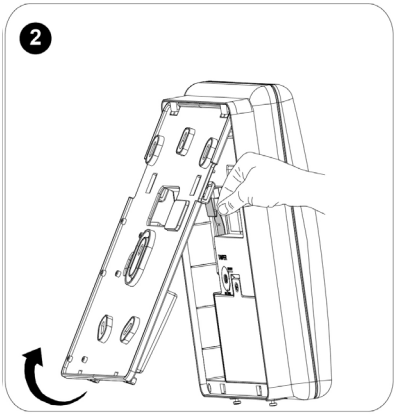
Using IP connectivity, the system can be constantly connected to the RISCO Cloud server, which enables visual verification to end users and monitoring stations alike, and provides end users with real-time event reporting and system control via the Smartphone and Web applications. The IP module also enables users to receive e-mail alerts and system status information.

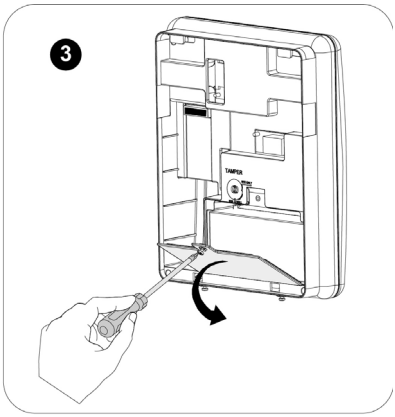
The IP module supports common format protocols (SIA, Contact ID) to send alerts to monitoring stations using the RISCO IP Receiver.

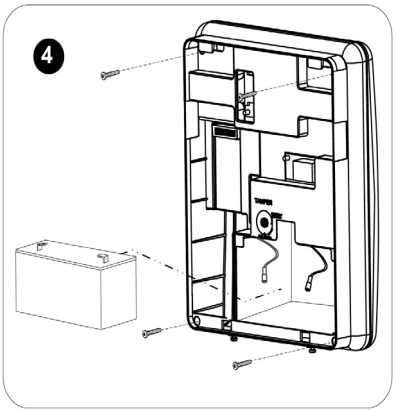
The IP module also enables remote programming of the system main panel using the Configuration Software over an IP line.

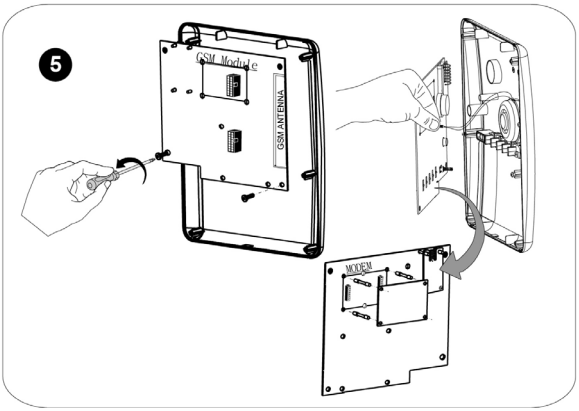
Installing the PSTN Module



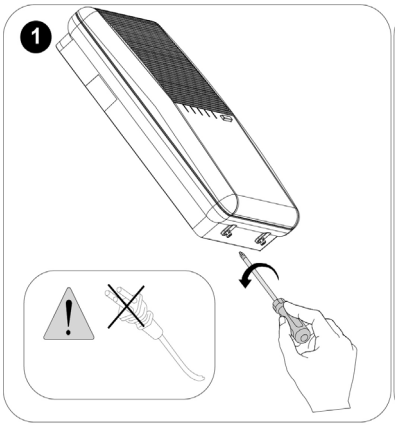


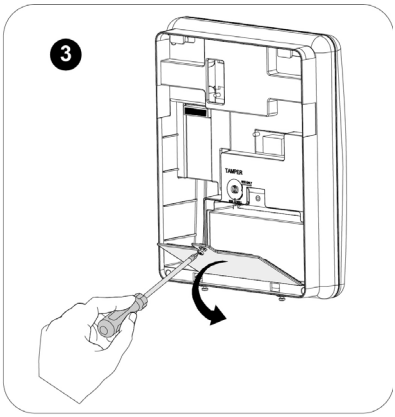


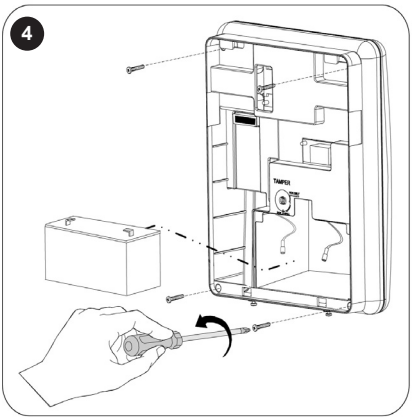


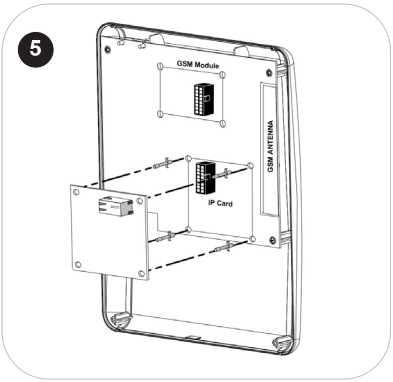


Installing the IP Module

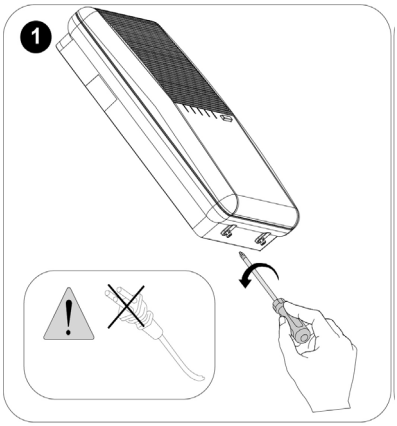


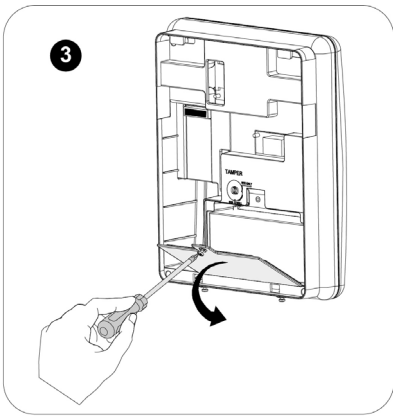


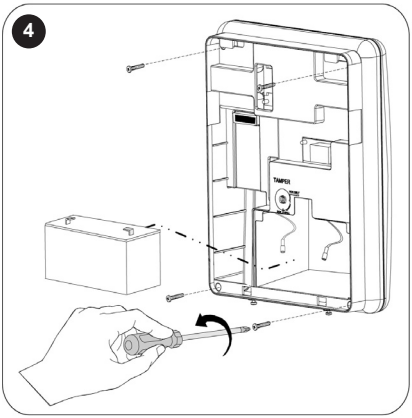


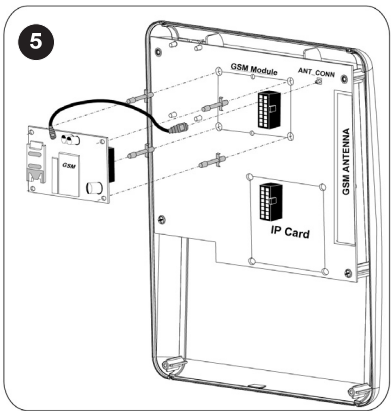


Installing the GSM/GPRS Module









NOTE: For the 3G module, attach the GSM antenna using the double-sided adhesive.

Installing the Main Panel

IMPORTANT: Only alarm system installers or similar professionals (such as electricians) should install and service the Agility 4 system.

Choosing the Mounting Location

Before you mount the main panel, study the premises carefully in order to choose the best exact location. The mounting location should be:

- Centrally located among the wireless system transmitters
- In a protected area, that is not visible from outside of the protected premises
- Mounted a minimum of 1.2 to 1.5 meters from the floor, in order to achieve optimal supervision communication with the peripheral devices
- Not reachable by small children
- Near an uninterrupted 230V AC electrical outlet
- Near a telephone outlet or IP network cable outlet if either is used
- In an area with a good GSM reception level
- In a place where the alarm can be heard during Partial Arming mode
- Far from:
  - Direct heat
  - Sources of electrical disturbance
  - Large metal objects, which may hinder the antenna reception.

Wall Mounting the Main Panel

The main panel is comprised of two sub-assemblies:

- Mounting bracket
- Main panel which in its turn is comprised of:
  - 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 main panel on the wall:

1. Separate the mounting bracket as follows:
2. Release the mounting bracket captive locking screws (Figure 1, detail 1) located at the bottom of the unit, by turning screws counter-clockwise.

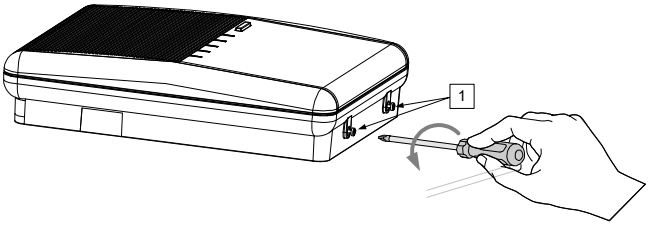


Figure 1: Mounting Bracket screws

3. Gently, pull up the mounting bracket to a 45° angle and slide it down to release the mounting bracket (Figure 2, detail 2) from the two locking tabs (Figure 2, detail 1) 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-cable connecting the power supply module (PCB) to the front panel module.

4. Disconnect the ribbon cable (see Figure 2, detail 3) from the power supply module while leaving it connected to the main panel.

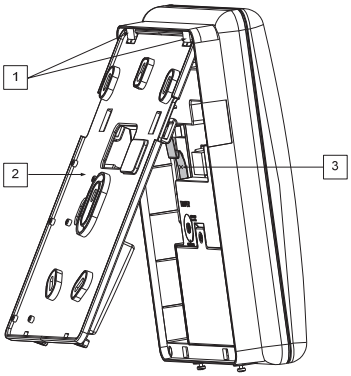


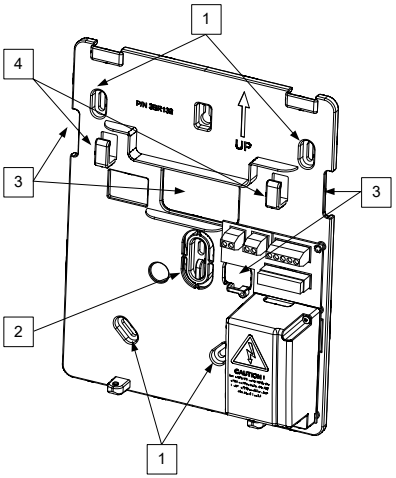
Figure 2: Mounting Bracket removal

5. Hold the mounting bracket against the wall as a template and mark the locations for the 5 mounting holes and an additional hole for securing the tamper protection bracket item (see Figure 3, detail 2), are available,).

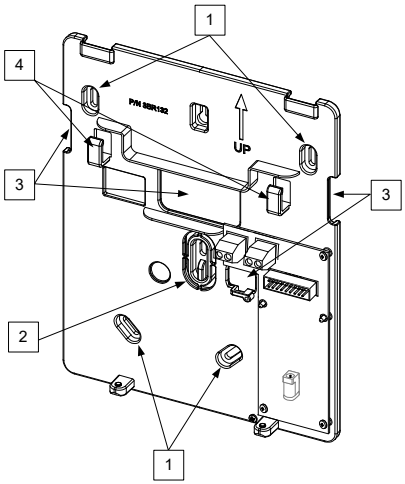
6. Drill the desired mounting holes and install the anchors to the wall. Use the supplied 5 Philips pan head screws to attach the mounting bracket to the wall (ST4.2 mm x 32 mm DIN 7981).

7. According to the location of the wall cables, route and insert the wires and cables via the cable's openings (see Figure 3, detail 3) including AC cable and telephone cable. See the following sections on wiring/connection tasks.

8. Anchor cables with dedicated hooks (see Figure 3, detail 4).



Configuration A



Configuration B

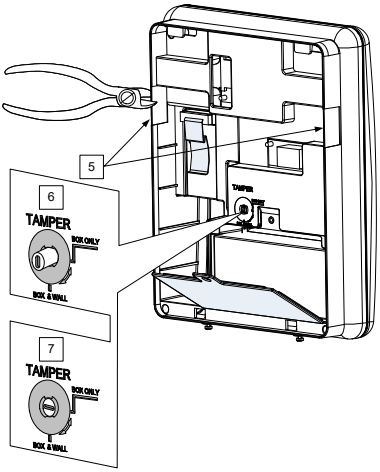


Figure 3: Wall Installation

9. Adjust the tamper switch (using a small flathead screwdriver) according to your preferred configuration:
   a. Box and Wall configuration (see Figure 3, detail 6) - Triggers the tamper when the box (main panel) or the wall mounting are tampered with.
   b. Box only configuration (see Figure 3, detail 7) – Triggers the tamper when the box (main panel) is tampered with.

Installing the Backup Battery

Agility 4 has a safety approved, sealed lead acid 6V, 3.7 Ah rechargeable backup battery for use in case of a power failure:

WARNING: Risk of explosion exists if battery is replaced by an incorrect type.

CAUTION: Install with correct polarity.

CAUTION: Dispose of used batteries according to applicable law and regulations.

To install the backup battery:

1. Remove the battery-cover screw (see Figure 4, detail 3) and pull the cover outward.

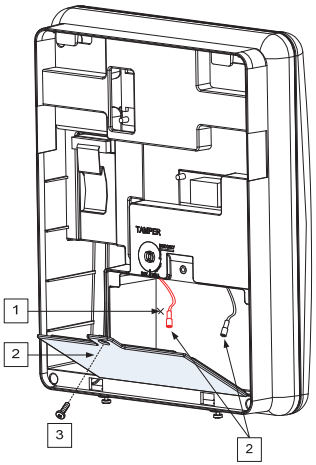


Figure 4: Battery Compartment

2. Insert the battery into its place and attach the connectors with the correct polarity.
3. Reinstall the battery-cover and secure it with the locking screw.

NOTE: The rechargeable battery should be charged for at least 24 hours.

Connecting to the Power Supply - Configuration A

For this configuration, the Agility 4 main panel is permanently connected to the mains via wall power supply or circuit breaker. The connection must be made in compliance with applicable electrical code and regulations. The Agility 4 is powered by a safety-approved 230 VAC.

Guidelines for Configuration A

- Connect the Live, Neutral and Ground using a safety-approved 3-wire, 18 AWG power cable (14-mm minimum diameter, flexible PVC cable that complies with IEC60227). The cable should be brought to the main panel in a protective plastic conduit, with a 16mm minimum diameter.
- 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.

To connect the power supply cable to the panel:

NOTE: The power cable is not supplied with Agility 4 system

1. Remove the power supply unit cover
2. Connect the power cable (safety approved, SVT, 18AWG, 0.75mm^2) the power supply terminals located on the power supply PCB.

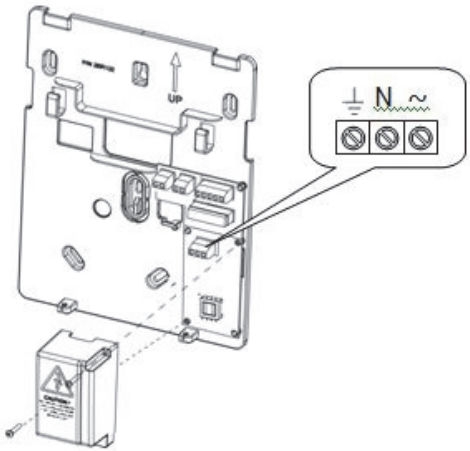


Figure 5A: Connecting AC power cable wires

3. **DO NOT connect the power cable to the electrical power supply at this point.**
4. Ensure proper grounding (see *Grounding Guidelines*, page *21*).

Grounding Guidelines

WARNING: The system must be connected to a protective grounding terminal in the building installation. Use a min 18 AWG yellow/green conductor for this 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 4. When connecting the ground wire, use a solid 14-gauge wire [or larger (numerically *lowe*r) 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 ground the Agility 4 system:

- Connect the Agility 4 ground terminal to an adequate electrical grounding connection for the lightning transient protective devices in this product to be effective.

WARNING: The Agility 4 connection to a grounding terminal must be performed according to applicable electrical code and regulations.

Connecting to the Power Supply – Configuration B

In this configuration, the Agility 4 main panel is powered via a 9 VDC / 1.0 A transformer.

1. Connect the transformer plug into the DC socket-located on the bracket module (PCB).
2. Route the cable through the hook and opening on the bracket.
3. **DO NOT connect the transformer's power cable to the wall power supply at this point.**

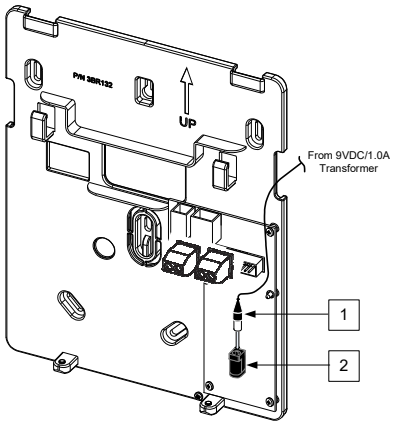
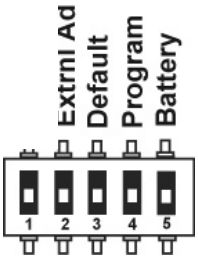


Figure 5B: Connecting DC Power Cable

DIP Switch Settings

IMPORTANT: As of Agility 4, DIP switches 1–4 in previous versions have been shifted to 2–5, respectively. DIP switch 1 is for future use.



DIP Switch 1: (future use)

DIP Switch 2 (E-A): External Audio: Used to define if the audio from the system will be heard from the control panel or from an external audio unit. If an external unit is connected to the Agility 4 system, the audio will be heard only through the external audio unit.

- **ON**: External audio unit is connected to the Agility 4 system
- **OFF** (Default): External audio unit is not connected to the Agility 4 system

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

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 the code length does not change.

WARNING: When performing this procedure, the main panel is open, so be extremely careful not to handle the power supply module, or any other components connected to 230 VAC. Coming into contact with 230 VAC can result in death.

2.

DIP Switch 4 (PRGM): Enables loading local software updates to the Agility 4

- **ON**: software updates to the Agility 4 can be loaded
- **OFF** (Default): software updates to the Agility 4 cannot be loaded

DIP Switch 5 (BAT): Defines the Battery Discharge Protection option settings

- **ON**: Battery Discharge Protection is **OFF**: The battery may therefore become totally discharged during a continuous AC power outage, thus battery replacement may be required (no “deep discharge” protection).

NOTE: In this position the system will start to operate from the backup battery

whether or not it is connected to the AC power supply (wall outlet / circuit breaker).

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

NOTE: In this position the system will not start to operate from the backup battery, unless first connected to the AC power supply (wall outlet / circuit breaker).

NOTE: If the battery voltage drops below 5.8 V or it is not connected, its keypad menu reading is "0.0".

Connecting to a Telephone Line

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 LINE terminal.
2. Connect a telephone on the premises to the SET terminal.

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.

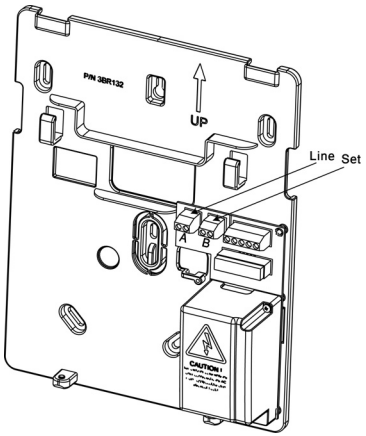


Figure 6: Telephone Line Wiring

Connecting a Network Cable

If your Agility 4 system is equipped with an IP card, connect the incoming network cable to enable IP communication.

1. Separate the main panel from its mounting bracket.
2. According to the location of the network cable, route and insert the cable via the opening on the main panel (see Figure 3, page 18).
3. Connect the incoming network cable to the Ethernet connector.

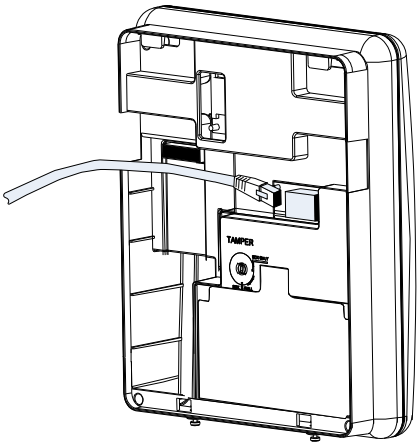


Figure 7: Network Cable Wiring

Installing the SIM Card

If your Agility 4 system is equipped with a GSM/GPRS module, insert a SIM card in order to enable GSM/GPRS communication.

CAUTION: Do not install SIM card while the main panel is powered up.
CAUTION: Do not touch SIM Card circuitry /connectors, as it could damage the SIM card.

1. Insert the SIM into the dedicated SIM card slot located on the rear side of the back panel.

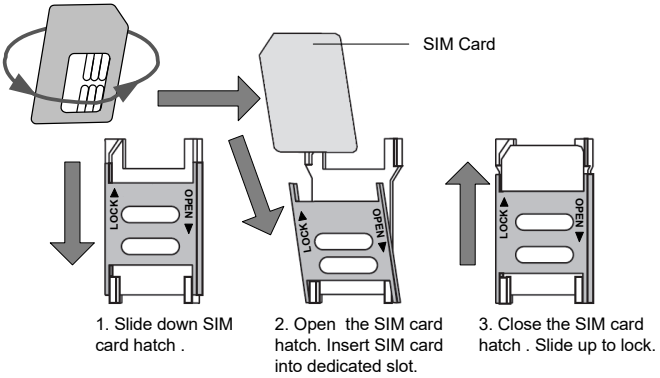


Figure 8: Installing the SIM Card

2. If a PIN code is required for the SIM card, a trouble code will appear. To remedy, enter the PIN code at the following location: **Communication > GSM parameters menu**.

NOTE: Ensure that you enter the correct PIN code. After three wrong attempts, the SIM card may lock and you may have to contact your provider to unlock it.

Disabling a SIM PIN

1. Insert the SIM card into a standard GSM mobile phone.
2. Insert the PIN code.
3. Access the phone security menu and select **PIN OFF**. Once done, re-test by switching the phone off, then switching it on. The PIN code should not be requested again.
4. Once the SIM card is inserted it is recommended to test the operation 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 wireless LCD/Panda keypad or Configuration Software.

GSM Module LED Indications

LED	Function
1	LD2: On=power on, off= no power **NOTE:** After powering up the GSM module with the SIM card installed, the module performs an automatic test of the GSM signal (RSSI) level. For the first 30 seconds after powerup, the red LD2 repeatedly flashes from 0–5 times (with a 5-second delay between each flashing cycle) to indicate the RSSI level: **5 flashes: very high** **4 flashes: high** **3 flashes: medium** **2 flashes: low** **1 flash: very low** **0 flashes: no network connection** If the signal level is not satisfactory or poor, consider installing the GSM in a location with better signal reception.
2	LD4: After power-up, LD4 blue LED starts to blink slowly ON and OFF in equal intervals after the modem is woken up. When the modem is ready and initialization has started, the ON/OFF intervals change – short interval ON and long interval OFF When initialization is finished successfully and the module has received parameters from the panel, LD2 red LED is constantly ON and LD4 blue LED continues to blink in short intervals ON and long intervals OFF.
3	LD3: The green LED is ON while module is in some activity – voice, internet etc.
4	LD1: Yellow LED indicates that the module is stuck

NOTES:

1. During burning software, all LEDs blink at different speed.
2. If after power-up there is no SIM card or the module cannot register to a network or the panel does not send parameters, it remains in the state of blue LED blinking slowly in equal ON/OFF intervals.

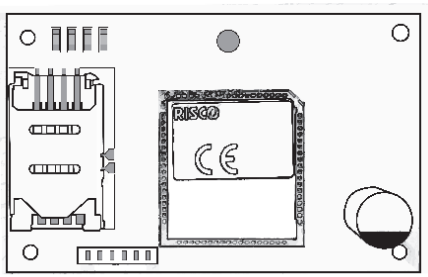


Figure 9: GSM Module LEDs

External Audio Unit Installation

The system can be connected to a remote external audio unit to be used instead of the main panel's internal speaker for listening to the system's audio messages. In addition, the external audio unit enables you to talk to your protected premises.

To connect the external audio unit:

1. Wire the external audio unit to the terminal block, located on the bracket's power module (PCB), as per the following figure.
2. Set DIP switch 2 (E- A) to the **On** position **(s**ee *DIP Switch Setting*, page *23*).

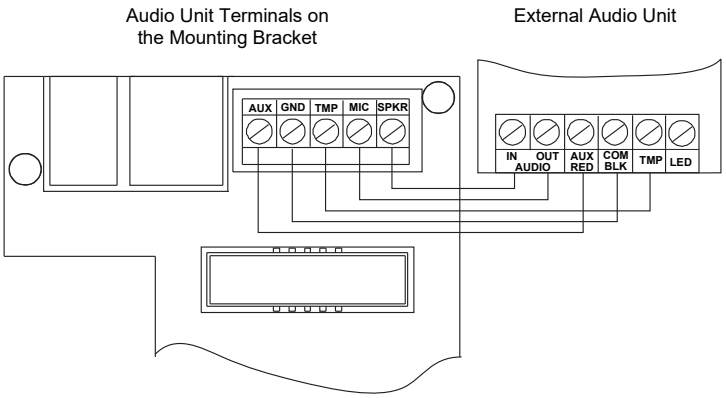


Figure 10: Wiring the External Audio Unit

Completing the Main Panel Installation

1. Re-connect the ribbon cable connecting the main panel and the mounting bracket.
2. Mount the main panel onto the mounting bracket using captive locking screws.

Powering Up the System

After completing all the tasks for module installation, backup battery installation, electrical power supply and terminal board wiring, grounding, DIP switch setting, closing up the main panel and mounting it, you can now power-up the system.

- Power up the system by applying electrical power at the wall outlet or circuit breaker.

Chapter 3 Installer Programming

Programming Methods

The following options are available for the installer to program the Agility 4 system:

NOTE: The Agility 4 can be programmed only using one keypad at a time.

- **Temporary " Installer" LCD/Panda Keypad** (typically used for example, if customer's kit doesn't include an LCD keypad)
- **Customer's Wireless LCD/Panda Keypad**
- **Configuration Software**

Allocating the Installer's LCD/Panda Keypad & Defining the System Language

Although an installer can use a customer's wireless LCD/Panda keypad, RISCO Group offers the Agility 4 installer a temporary "installer" wireless LCD/Panda keypad to be used for fully configuring the system. This LCD/Panda keypad will be allocated temporarily, and not as a permanent part of the system. After temporarily allocating the LCD/Panda keypad, the other system devices can then be allocated with it, and the system further configured.
When the temporary installer LCD/Panda keypad is allocated, it prompts the installer to define a default system language.

NOTE: An hour after exiting the programming mode, the installer LCD/Panda keypad will be erased from the system's memory (also when power is lost to the system).

To (temporarily) allocate the installer keypad and define the system language:

1. After the main panel is connected to the power supply, short press the main panel button; the status is announced at the panel.

Note: If the keypad lapses into sleep-mode before you have chosen the language, restore the choose-system-language display through simultaneously pressing [*] and [9])

2. With battery installed, press the keypad's  /  buttons simultaneously during the status announcement until the following message appears: **Grand Master Code:**

3. Enter the Grand Master code (default is 1234) and then press  /  ; you are

now in the User Menu.

NOTE: When a **wrong** Grand Master code is entered, the keypad will not be allocated. To continue this procedure, start the keypad allocation procedure again.

4. Press  /  twice to exit the User Menu, and enter the system again using the installer code (default is 0132).
5. Now that you have temporarily allocated this "installer" LCD/Panda Keypad to the system, you can now allocate other system devices. See *Wireless Device* Allocation, page *31.*

Allocating the Customer's LCD/Panda Keypad & Setting the Default Language

Agility 4 can be fully configured via the customer's wireless LCD/Panda keypad.
New systems require that the LCD/Panda keypad be the first device to be allocated to the system, from which it then prompts the installer to define a default language. After the LCD/Panda keypad allocation, the other system devices can then be allocated with it, and the system further configured:

To allocate the LCD/Panda keypad and define the system language:

1. After the main panel is connected to the power supply, press the button on the main panel for 5 seconds. The unit beeps once and enters "Learn" mode. The LEDs light up one after the other.
2. With battery installed, press the keypad's  /  buttons on the keypad simultaneously for at least 2 seconds until a generic device allocation message is broadcast and also displayed on the keypad.
3. In the displayed language menu, select the default system language, and then press  / 

NOTE: If the keypad lapses into sleep-mode before you have chosen the language, restore the -system-language display by simultaneously pressing * and **9**.

4. Now that you have allocated this LCD/Panda Keypad to the system, you can now allocate other system devices with the LCD/Panda keypad. See *Wireless Device* Allocation, page *31.*

Configuration Software

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

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

For further information on programming the Agility 4 system via the Configuration software, refer to the Configuration Software manual.

Wireless Device Allocation

All wireless devices (detectors and accessories) must also be allocated (registered) to the system. Allocations can be performed via:

- **Main panel:** Quick allocation of all devices is performed by sending a RF signal transmission from each device. Zones are automatically (and sequentially) assigned.
- **LCD/Panda keypad** (the following methods are available):

  For having zones assigned automatically (and sequentially): You can either perform by the "RF Allocation" method, or by entering each device's unique 11-digit code (serial number) into the system.

  For manually selecting a specific zone number to which a device is then allocated: You can perform this by the "Zone Allocation" method.

- **Configuration Software**

NOTE: Regardless of the allocation method used, make sure to first install the batteries in all devices before performing the allocation procedure.

Quick Allocation of all Devices at the Main Panel

You can quickly allocate all system devices (including keypads) at the main panel.

To perform quick device allocation at the main panel:

NOTE: To enable Quick Allocation mode the System bit "*Quick Learn*" should be enabled (default).

1. Long-press the main panel button; each LED on the main panel will light up, one after another, indicating the system is in "Learn mode."

   NOTE: The panel will sound each time you enter or exit the Learn mode.

2. Make sure batteries are installed in each device before allocating. For detectors, also

make sure the covers are removed so the tamper switches are accessible.

3. Send a signal transmission from each device per the chart below (if a device is not listed on the chart, refer to the device's specific instructions); the main panel beeps once to accept or three times to reject. Once accepted the system announces the device type and its assignment (for example, "Detector, zone 1"). Each device receives an index number from the system, and zones are assigned automatically (and sequentially, in the order allocated).

NOTE: For future use, it is recommended to write down the device assignment / zone and installation location of each allocated device.

Table of Device Transmissions

Wireless device	Transmission procedure
2-Way Panda Keypad	Press  and  simultaneously for at least 2 seconds
2-Way LCD Keypad	Press  and  simultaneously for at least 2 seconds
2-Way Slim Keypad	Press  and  simultaneously for at least 2 seconds.
PIR Detectors: • **PIR** • **PIR camera** • **PIR-pet** • **PIR-pet camera** **NOTE**: See *PIR Camera Setup*, page *38*.	Press the tamper switch for 3 seconds.
Curtain detector	After inserting battery, close the bracket and wait 3 seconds.
1-Way Magnetic Contact Detectors	Press the tamper switch for 3 seconds.
2-Way Magnetic Contact Detectors	Press the tamper switch for 3 seconds. **NOTE:** After programming parameters for this device and exiting Programming mode, press the Tamper switch for 3 seconds, and then wait 1 minute for the main panel to download the parameters from the detector
2-Way Remote Control	Press  and  simultaneously for at least 2 seconds
1-Way Keyfob	Click  for at least 2 seconds
Smoke Detector	After inserting battery, transmission is send automatically within 10 seconds.
Siren	Press the reset switch on the siren. After a squawk sounds, you have 10

	seconds to press on the tamper switch for at least 3 seconds.
I/O Module	1. Set the Agility 4 system to Learn mode. 2. Send a WRITE message within 15 seconds after I/O module power up, by pressing the Wall and Cover tampers switches simultaneously for at least 3 seconds (when the PCB IS installed ONLY the cover tamper has to be pressed).
2-Button Panic Keyfob	Press both buttons for at least 7 seconds
Wrist Band Panic Transmitter	Press the button for at least 7 seconds.

4. When all the devices have been enrolled, short-press the main panel button to exit Learn mode; the unit beeps once and the LEDs stop flashing.

Device Allocation using the Wireless LCD/Panda Keypad

RF Allocation Method

Using the RF Allocation method, zones are assigned automatically and sequentially.

To perform device allocation by RF Allocation:

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 of Device Transmissions*, page *32*).
3. The main-panel will acknowledge the transmission with a beep and LCD/Panda keypad displays the device's automatically-assigned zone and index numbers, the device's
   11-digit serial number, and the device's description.
4. When finished allocating the system device(s), press (*) / repeatedly until you arrive back to **Radio Device**, then press (0) to Exit, and (#?) / OK to confirm.

Serial Number Method

When performing allocation by entering the device's serial number ("code"), zones are assigned automatically and sequentially.

To perform device allocation by serial number:

1. Go to the Installer menu and select **Programming → Radio Device → Allocation → 2) By Code**.

2. Enter the device's 11 digit serial number ("code"), and then press  /  .

3. The main panel will acknowledge the transmission with a beep and the LCD/Panda keypad displays the device's automatically-assigned zone and index numbers, the device's 11-digit serial number, and the device's description.

4. When finished allocating the system device(s), press  /  repeatedly until you arrive back to **Radio Device**, then press  to Exit, and  /  to confirm.

Zone Allocation Method

When performing allocation by the Zone Allocation method, you manually select a specific zone / index number to which the device is then allocated.

To allocate devices with zones manually-specified:

1. From the Installer menus select: **Programming** > **Radio Device** > **Allocation** > **3) Zone Allocation**.

2. Using  to scroll between the 2 digits of the zone number, enter the zone number of your choice (from 01 –32), and then press  /  .

3. Now use  to select the allocation method (**RF** Allocation or Serial Number method) and then perform the respective zone allocation procedure (per RF Allocation or Serial Number procedures listed above); the main panel will acknowledge the transmission with a beep and the LCD/Panda keypad displays your manually-assigned zone and index numbers, the device's 11-digit serial number, and the device's description.

Allocating Devices using the Configuration Software

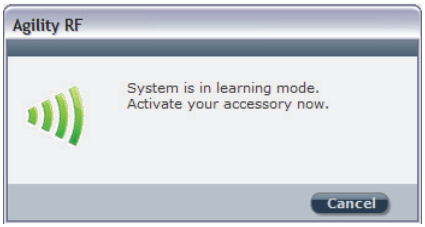
Perform wireless device allocation via the Configuration Software in two different ways: RF Allocation or by entering the device's code (serial number).

To perform RF device allocation from the Configuration Software

1. Establish Communication between the main panel and the Configuration software. (For more information, refer to the *Configuration Software Manual*)

2. Open the **Activities > Radio Device Allocation** screen.

3. Click Allocate... . This operation will set the main panel to Learn mode. The following message appears:



4. Send a transmission from the device (see *Table of Device Transmissions*, page 32).

5. The main panel 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 assigned by the system.

NOTE: If required you can change the index number of the wireless device by selecting the required index number and clicking Allocate... again.

---

6. To allocate another wireless device click Clear and then repeat from step 2.

To perform device allocation by serial number from the Configuration Software

1. Establish Communication between the main panel 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. Click the Allocate... button.

5. The main panel 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.

Deleting Devices

Deleting wireless device allocations can be done from the LCD/Panda keypad or from the Configuration Software. Deleting can be done for all devices simultaneously, or for a single device.

Deleting all Devices Simultaneously from the LCD/Panda Keypad

To delete all devices simultaneously from the wireless LCD/Panda keypad:

1. Go to the Installer menus and select **Programming → 1)System → 5) Settings → 2)Erase WL →**  /  .
2. Press  /  to confirm the deletion.

Deleting a Single Device from the LCD/Panda Keypad

To delete a single device allocation from the wireless LCD/Panda keypad:

1. Go to Installer menus and select **Programming → Radio Device → 4) Delete →**  /  .
2. Use  /  to scroll to the device category, and press  /  .
3. Enter (or scroll to) the device to delete, and then press  /  .
4. Press  /  again to confirm the deletion.
5. Press  /  to go back and delete additional devices (and repeat this procedure) as needed.

NOTE: If you enter all zeros (00000000000) in place of the device's 11-digit serial number (for example at **Programming →Radio Device → Modification→Parameters**) this will also delete the device allocation.

Deleting all Devices Simultaneously from the Configuration Software

To delete all device allocations from the Configuration Software:

1. Establish Communication between the main panel 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.

Deleting a Single Device from the Configuration Software

To delete a single device 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. In the **Radio Device Allocation** screen in the *Delete Accessories* area enter the device's serial code and click the **Delete** button.

Establishing Communication to the RISCO Cloud

Agility 4 can be configured to be constantly connected to the RISCO Cloud, an application server that handles all communication between the system, service providers and Smartphone/Web users. The Cloud enables remote monitoring and control of the system, sending event notifications, and viewing real-time video clips via VUpoint IP cameras – for both monitoring stations and system users.

Step 1: Enabling Cloud Communication

- From the Programming menu select: **1) System > 2) Controls > 3) Communication > Cloud Enable** > toggle to **[Y]** using / , and then press / to confirm.

Step 2: Defining the (GPRS or IP) Communication Channel

Connecting with GPRS

1. From Programming menu select : **4)Communication > 1)Method > 2)GSM > 2)GPRS**
2. Use / to scroll between **1)APN Code** and **2)APN User Name** and then define the APN code and user name respectively. This information must correspond with that supplied by the SIM card service provider.

Connecting with IP

3. From Programming menu select: **4)Communication > 1)Method > 3)IP > 1)IP Config**
4. Now define whether the system's IP address is Static or Dynamic. If Dynamic select **[Y]** (the system refers to an IP address provided by the DHCP). If Static select **[N]** and define all other parameters in the menu.

Step 3: Defining Cloud Parameters for IP or GSM/GPRS

From the Installer menu Programming select: **4) Communication > 5) Cloud,** and then define the following parameters:

1. **IP Address:** The server IP address (**www.riscocloud.com**, or that of your organization's Cloud server)
2. **IP Port:** The server port is set to **33000.**
3. **Password**: The password for server access as provided by your provider (if required). This password should be identical to the main panel password as defined in the server under the Main Panel page definition (AAAAAA by default).
4. **Channel:** Select the communication path for the Cloud (based on IP or GPRS communication) as appears in the available options.

NOTE: The SIM card must be installed (see *Installing the SIM Card*, page *26).*

5. **Controls:** The Agility 4 supports parallel channel reporting (via PSTN, IP, GPRS SMS, or voice) to both the monitoring station and Follow Me users. Use this setting to decide if the panel reports events to the monitoring station or Follow Me in parallel to the report to the Cloud (assuming there is an additional communication channel available – PSTN, IP, GPRS SMS, or voice), or only as a backup when the communication between the Agility 4 and the Cloud is not functioning.

Step 4: Registering the Agility 4 to the RISCO Cloud

Registering with the RISCO Cloud enables the user to monitor, control and configure the Agility 4 system from any location.

The Agility 4 panel must be connected to the Internet via the network cable or via wireless connection. The panel will then automatically register itself to the RISCO Cloud. The Installer can then associate the panel with a company or assign a site to a company in the RISCO Cloud. (For further details and instructions, refer to the *RISCO Cloud Installer Quick Guide*).

iRISCO Smartphone App

The iRISCO Smartphone app provides smart and easy control of the Agility 4 system, enabling on-the-go users to receive event notifications, view the system status and event history, arm/disarm the system, activate home automation devices, bypass zones, and utilize IP cameras for visual verification and self-monitoring.

iRISCO is available for iOS and Android

PIR Camera Setup

PIR-based camera detectors perform detection with advanced still image and video recording capabilities. Up to eight PIR detectors / cameras can be used in the Agility 4 system.

For the physical installation of the PIRs, refer to the product instructions.

To set up PIR camera detectors:

1. Allocate the PIR camera as any other detector (see prior allocation procedures)
2. Set the PIR camera parameters as they appear under the Advanced Zone parameters per product instructions.
3. Set communication between the Agility 4 and the Cloud server (See *Establishing Communication to the RISCO Cloud,* page *37*).
4. Log in to the Web User Application (www.riscocloud.com), then go to the main display and select the Video option.
5. Adjust the PIR camera view as follows:
   a. Select camera.
   b. Perform a snapshot from the server.
   c. Go to the **History** tab.
   d. Click on the required picture.
6. As necessary, adjust the PIR camera and repeat steps b—d.

Chapter 4 Installer Menus

The following chapter describes the parameters and programming options of the system that are installer-programmed via a wireless LCD/Panda keypad or Configuration Software.

Describing the Wireless LCD/Panda Keypad

The wireless LCD/Panda keypad contains three LED indicators, LCD/Panda display and numerical buttons.

Button (LCD Keypad)	Button (Panda Keypad)	Primary function
		To "wake-up" the keypad, go back one level, exit menus (similar to the Esc key)
		To select, confirm, "OK" (similar to the Enter key)
		To scroll
		To toggle between options (such as Y / N)
		To exit the programming mode (followed by  /  to confirm)

NOTE: 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.

Accessing the Installer Menus

To access the installer menus via the wireless LCD keypad:

1. Click  /  to activate the LCD/Panda keypad.
1. Enter the installer code (0132 is the default).

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***.

2. Use  to scroll through all the main installer menus:
   1) **Programming**
   2) **Testing**
   3) **Activities**
   4) **Follow Me**
   5) **Clock**
   6) **Event Log**
   7) **Macro**
3. Press  to select a main installer menu.
4. Use  to scroll through the list of all sub-menus.

Programming Menu

After selecting the Programming Menu, you can scroll between the following list of its sub-menus:

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

1. System Sub-Menu

The System sub-menu has the following items:

1. Timers
2. Controls
3. Labels
4. Sounds
5. Settings
6. Service Information

7. Firmware Update

8. Picture Server

1.1 Timers

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

System: Timers		
Parameter	**Default**	**Range**
Exit/Entry Delay 1		
The amount of time before the system is armed/disarmed. Usually used at front entrance door.		
Entry Delay 1	30 sec	0-255 sec
Duration of entry delay 1 before the system is disarmed		
Exit Delay 1	45 sec	0-255 sec
Duration of exit delay 1 before the system is armed		
Exit/Entry Delay 2		
The amount of time before the system is armed/disarmed. Usually used at the back door.		
Entry Delay 2	45 sec	0-255 sec
Duration of entry delay 2 before the system is disarmed		
Exit Delay 2	60 sec	0-255 sec
Duration of exit delay 2 before the system is armed		
Bell Timeout	04 min	01-90 min
Duration of the siren during alarm.		
Bell Delay	00 min	00-90 min
The time delay before a siren sound is produced after triggering an alarm.		
AC Off Delay	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.		
Jamming Time	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 *Audible Jamming* system control. NONE: No jamming will be detected or reported.		

System: Timers

Parameter	Default	Range
RX Supervision	0 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".

Notes: 0 hours disables supervision
It is recommended to set the supervision time to a minimum of 3 hours

TX Supervision	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 **RX Supervision** time, the system will regard the accessory as Lost.

Note: The device will generate the supervision message according to the time defined.

Important: The RX Supervision time should be higher than the Tx Supervision time in order to eliminate false lost event.

Redial Wait	30 sec	0-255 sec

The number of seconds between attempts at redialing the same phone number.

Applies to both the **MS Retries** and **FM Retries** parameters.

Note: Used for both PSTN and GSM.

More

Swinger Limit Shutdown	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.

Note: 00 to disables the swinger shutdown

No activity	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.		
Entry Bypass	30 seconds	(15–240)
When the 2-Way Wireless Slim Keypad Reader is defined as Bypass mode, this timer defines the period during which an Open Delay zone type (typically door) can be opened without triggering an alarm event.		
Service Time	20 minutes	1-240 minutes
The time period that all tampers (main unit and accessories) can be opened for purposes of battery replacement without triggering a tamper alarm (see *Service Mode*, page *132*).		

1.2 Controls

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

System: Controls	
Parameter	**Default**
Basic programming	
Quick Arm	YES
YES: Eliminates the need for a user code when arming (Full or partial) the system by a keypad or 2-way remote control. **NO**: A valid user code is required for arming using a keypad or remote control.	
Allow Bypass	YES
YES: Permits zone bypassing by authorized system users after entering a valid user code. **NO**: Zone bypassing is NOT permitted.	
Quick Status	YES
YES: A user code is not required before pressing the status key/button on your wireless keypad or bi-directional remote control. **NO**: A user code is required to activate the status key.	
False Code Trouble	YES
YES: 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. **NO:** A local alarm is sounded at the premises.	

System: Controls	
Parameter	**Default**
Siren Squawk	YES

YES: 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:

- One chirp indicates the system is armed (also when arming with a keypad).
- Two chirps indicate the system is disarmed.
- Four chirps indicate the system is disarmed after an alarm.

NO: No "chirp" is produced.

Audible Panic	NO

YES: The sirens operate when a "Police Alarm" is initiated at the keypad (if defined), the remote control or when a panic zone is activated.

NO: No siren operation occurs during a Panic Alarm, making the alarm silent at the protected site.

Note: The system always transmits a panic report to the monitoring station.

Buzzer → Bell	NO

YES: If an alarm occurs when the system is armed in the Stay Arm mode, a buzzer sounds for 15 seconds before the sirens operate.

NO: An alarm in the Stay Arm mode causes sirens to operate simultaneously.

Audible Jamming	NO

Relates to the **Jamming Time** parameter.

YES: Once the specified time is reached, the system activates the siren and sends a report code to the monitoring station.

NO: Once the specified time is reached the sirens do not operate.

Exit Stay Beeps	YES

Determines whether the system will sound beeps during exit time in Stay Arming.

YES: Exit beeps will sound

NO: Exit beeps will not sound

Forced Arming	YES

YES: Arming a partition, using a Slim keypad (from ver. 3.84L), 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.

NO: The partition cannot be armed until all violated (not ready) zones are secured.

System: Controls	
Parameter	**Default**
Arm Pre-warning	YES

Related to auto Arm/Disarm operation.

YES: 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.

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.

Default Enable	YES

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 3 is in place when power to the main panel is switched off and then on. For more information regarding main panel defaults refer to *DIP Switch Setting*, page *23*.

Note: The Default Enable parameter's state is not reset upon performing system default.

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.

Main Button: Status-Y/Talk-N	YES

The Agility 4 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.

Quick Learn	YES

Enables the button on the surface of the main unit to perform quick allocation of wireless devices. (See *Quick Allocation of all Devices at the* , page *31*).

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.

System: Controls	
Parameter	**Default**
Advanced programming	
Area	NO

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.

Global Follower	NO

YES: 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.

NO: 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.

Summer/Winter	NO

YES: 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).

NO: No automatic time accommodation is made.

24 Hour Bypass	NO

YES: It is possible for the user to bypass a 24-hour zone.

Note: When set, this parameter also applies to the zone's associated tamper settings. Thus, bypassing a zone, also bypasses its tamper.

NO: It is not possible for the user to bypass a 24-hour zone.

Technician Tamper	NO

YES: 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.

NO: Correcting the problem resets a tamper alarm, requiring no alarm company help.

System: Controls	
Parameter	**Default**
Technician Reset	NO
YES: 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.	
Note: Before the Ready LED can light all zones within the partition must be secured.	
NO: Once an alarmed partition is reset the Ready LED lights when all zones are secured.	
Installer Tamper	NO
YES: After a tamper alarm, the system is not ready to arm. This requires the intervention of the alarm company. **NO:** After a tamper alarm is restored the system is ready.	
Low Battery Arm	YES
YES: Allows arming of the system when a low battery condition is detected in the main unit. **NO:** Arming the system is disabled when a low battery condition is detected.	
Siren Pre-Alarm	NO
Specifies if the system will send a pre-alarm message to the siren while an entry delay starts. **YES**: 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. **NO**: Pre-Alarm disabled	
Bell 30/10	NO
YES: The sirens cease to sound for 10 seconds after each 30 seconds of operation. **NO**: The sirens operate without interruption.	
Fire Pattern	NO
YES: During a fire alarm, the sirens produce a pattern of 3 short bursts followed by a brief pause. **NO**: During a fire alarm, the flow of sounds produced by the siren is a pattern of 2 seconds ON, then 2 seconds OFF.	

System: Controls	
Parameter	**Default**
IMQ	NO

YES: Causes the following parameters to function as follows:

- **Auto Arm Bypass:** 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).
- A utility output defined as "Auto Arm Alarm" is activated.
- A utility output defined as "Zone Loss Alarm" is activated

NO: Causes the following parameters to function as follows:

- **Auto Arm Bypass:** 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.
- A utility output defined as "Auto Arm Alarm" is deactivated.
- A utility output defined as "Zone Loss Alarm" is deactivated.

Disable Incoming Call	NO

Used to disable all incoming calls trying to come in via the voice channel (PSTN or GSM).

YES: Incoming calls from voice channel are disabled.

NO: Incoming calls from voice channel are enabled.

Note: Incoming data call via the GSM data channel is still enabled.

Bypass Unique Code	YES	YES/NO

YES: Unique code for the purpose of the door bypass feature. The codes used for the door bypass feature are defined with door bypass authority level

NO: The regular user code can be used as a bypass code (Not including ***Arm only*** authority level). The same user codes will be used from a bypass keypad and from a regular keypad

Silent Remote Install	NO

YES: During Configuration Software programming and during remote software update all panel sounds are suppressed.

NO: The panel generates sounds during programming by Configuration Software.

AntiMask=Tamper	NO

Used to determine the operation of anti-masking detection in a bus zone.

YES: Anti mask violation will activate tamper alarm.

NO: Anti mask violation will be regarded as trouble event.

Power Management	NO

YES: In case of a power failure, the system will disable the IP Module to save battery life.

NO: Does not extend battery life in case of a power failure.

Note: This option functions only with Multi-Socket IP.

System: Controls	
Parameter	**Default**
Communication Controls	
MS Enable	YES
Use  /  to toggle between Y (yes) and N (no) to define whether there will be communication to the monitoring station. **YES:** Enables communication with the monitoring station to report alarms, trouble, and supervisory events. **NO:** No communication with the monitoring station is possible. Choose **NO** for installations that are NOT monitored by a monitoring station.	
Configuration Software Enable	YES
YES: 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. **NO:** Disables communication, as detailed above.	
FM Enable	YES
YES: 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. **NO:** Disables Follow-Me communication.	
Cloud Enable	NO
Yes: Enables communication between the Agility 4 system and the RISCO Cloud server. **NO:** Does not enable communication, as detailed above.	
EN 50131 programming	
Authorize Installer	NO
This option limits the Installer and Sub-installer authorization to access the programming menu. **YES:** A Grand Master code is required to authorize the installer to enter the programming mode for 1 hour. **NO:** The Installer does not need an authorization code.	
Override Trouble	YES
Specifies if the system/partition can be armed when there is a fault in the system. **YES**: The system will arm even if there is a fault in the system. **NO:** 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**
Restore Alarm	NO
YES: 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.** **NO**: The user does not need to confirm the alarm before rearming the system.	
Mandatory Event Log	NO
YES: Only mandatory events (specified in the EN standard) will be displayed in the Event Log. **NO**: All the events will be displayed in the Event Log.	
Restore Troubles	NO
YES: 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.** **NO**: The restoral report of each trouble is automatic .	
Exit Alarm	YES
YES: 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. **NO:** 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.	
Entry Alarm	NO
This feature is used to reduce false alarm reports to the MS. **YES**: 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 **entry** route. **NO**: A violated zone outside the **entry** route will generate an alarm during the entry time and a report will be sent to the MS.	
20 Minutes Signal	NO
YES: 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. **NO:** 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**
Attenuation	NO
YES: The Agility 4 receiver will be attenuated by 6 dB during the communication test. **NO**: The Agility 4 receiver works in normal operation mode.	
PD6662 programming	
Bypass Exit/Entry	YES
YES: It is possible for the user to bypass an Exit/Entry zone. **NO:** An Exit/Entry zone cannot be bypassed.	
Entry Disable	NO
YES: The alarm confirmation process will be disabled when the entry time starts. **NO:** The alarm confirmation process will start when the entry time starts.	
Route Disable	NO
YES: 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.	
Note: Sequential confirmation can still be established from two confirmed zones, located off the entry route.	
NO: The entry route zones will participate in the alarm confirmation process when the entry time starts.	
Installer Confirmation	NO
YES: 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 an "installer reset" from the keypad. **NO:** Any means can be used to arm or disarm (keypad, remote phone operation etc.).	
Key Switch Lock	NO
YES: Only a latched key switch zone can arm or disarm the system.	
Note: 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.	
NO: Any means can be used to arm or disarm (keypad, remote phone operation etc.).	
Entry Disarm	NO
Determines if the system's disarming depends on the entry time. **YES:** A remote control or keypad proximity tag can disarm the system during the entry time.	
Note: The system cannot be disarmed with a remote control while the system is armed. This parameter setting is relevant only for the Away Arm state and not for Stay Arm.	
NO: The system can be disarmed during any time using any disarming device.	

System: Controls	
Parameter	**Default**
CP-01 programming	
Exit Restart	NO
Used to define if an exit time shall restart one additional time while an entry/exit zone is tripped twice during exit time. **YES**: Exit time will restart for one time only when an entry/exit zone is tripped during exit time. **NO**: Exit time will not be affected if an entry/exit zone is tripped during exit time.	
Auto Stay	NO
Used to define the system's arming mode when using a keypad and no exit/entry zone is tripped during exit mode. **YES**: If no exit/entry zone is tripped during exit time the system will be armed in STAY mode. **NO**: If no exit/entry zone is tripped during exit time the system will be armed in Away mode.	
Exit Error	NO
Used to define what will happen if an Exit/Entry zone is left open at the end of the exit time. **YES:** o Local alarm will be activated at the end of the exit time. o 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. **NO:** o No local alarm will be activated at the end of the exit time. o 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	
3 Minute Bypass	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:

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

To rename labels using the keypad keys to produce characters:

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**
Tamper Sound	Bell+Buzzer	1 to 6
Sets the sound(s) produced by a Tamper violation according to the following options: ○ **Silent** ○ **Bell (**External/Internal siren**)** ○ **Buzzer (main unit)** ○ **Bell + Buzzer** ○ **Bell/A Buzzer/D:** Bell when system armed, Buzzer when system disarmed ○ **Bell/A S/Disarm:** Bell when system armed, Silence when system disarmed		
Local Alarm	Level 1	0-5, OFF
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.		
Local Squawk	Level 1	0-5, OFF
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.		
Exit/Entry Beeps Volume	Level 1	0-5, OFF
Determines the volume of the beeps sounded from the main unit during the Exit/Entry times.		
Speaker Volume	Level 1	0-4
Determines the volume of the messages sounded from the main unit or the Listen-In and Talk unit.		

1.5 System Settings

System: Settings		
Parameter	**Default**	**Range**
Default Panel		
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 toggle your Y/N option.		
Erase Wireless Device		
Erase wireless devices without changing the system current programmed parameters.		
Language		
Sets the system language (Email, SMS and keypad language)		
Standards		
EN 50131	NO	
Sets the panel programming options in compliance with EN standards. (See *Appendix* F:*).*		
PD6662	NO	
Sets the panel programming options in compliance with PD6662 standards.		
CP-01	NO	
Sets the panel programming options in compliance with CP-01 standards.		
Customer		
Modify here the 3-character system Customer ID as per label format (See *Labels,* page *54*). Changing the Customer ID results in changing the system language and default settings according to the predefined factory Customer ID settings. Use this setting to alter the Customer ID specified upon first-time start-up for the Agility 4. Consult with your RISCO representative to acquire the appropriate Customer ID.		

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 4 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 wireless LCD keypad or from the Agility 4 Configuration Software. For detailed information refer to the *Remote Software Upgrade* instruction guide.

System: Firmware Update		
Parameter	**Default**	**Range**
Server IP	firmware.riscogroup.com	
Enter the IP address/URL of the router/gateway where the upgrade file is located.		
Server port	00080	
Enter the port on the router/gateway where the upgrade file is located.		
File Path	/WirelessPanels/OEN/FAT.txt	
Enter the upgrade file name. For example: /AgilityV4/0EN/cpcp.bin		
Please contact Customer Support services for the file name parameters.		

1.8 Picture Server

The Agility 4 enables you to define a server on which to store and access images captured by system-related cameras. Use this feature for the http solution

System: Picture Server		
Parameter	**Default**	**Range**
Server IP		
Enter the IP address of the router/gateway of the server where the pictures are to be located.		
Server port	**00000**	
Enter the port on the router/gateway of the server where the pictures are to be located.		
File Path	**Agility**	
Enter the upgrade file name.		
Please contact Customer Support services for the file name parameters.		
Username		
Enter user name (if required). The user name is provided the server administrator. The system supports a user name field of up to 32 alphanumeric characters and symbols (!, &, ? etc).		

System: Picture Server		
Parameter	Default	Range

Password

Enter the password (up to 24 alphanumeric characters and symbols.) as provided the server administrator (if required).

Image Channel

Choose here the image transmitting channel for the HTTP server, subject to the system's installed networks.

Note: This feature requires that the monitoring station receiver supports the SIA IP protocol.

The four options are:

- **IP/GPRS**: The panel checks for the availability of the IP network. During regular operation mode images are transmitted using the IP network line. In the case of trouble in the IP network, the images are routed through the GPRS network.
- **GPRS/IP**: The panel checks for the availability of the GPRS network. During regular operation mode all image transmission are carried out using the GPRS. In the case of trouble the images are routed through the IP network.
- **IP Only**: The images are transmitted through the IP network only.
- **GPRS Only**: The images are transmitted through the GPRS network only.

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

4. Delete

2.1 Allocation

Each wireless device must be identified to the system receiver before its parameters can be configured. See *Wireless Device* Allocation, page *31* 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. Keyfobs (Remote Controls)
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
- Cross Zones

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). Use  to toggle between all the possible characters for each key:

Serial Number

The serial number of the zone. Each wireless device has its own unique serial number. Entering 00000000000 will delete the zone's allocation.

Partition

The partition (1 to 3) assignment for each zone.

Type

Each zone can be defined as one of the following types:

Not Used

Zones: Parameters		
Parameter	**Default**	**Range**
Disables a zone. All unused zones should be given this designation.		
Exit/Entry 1		
Used for Exit/Entry doors. Violated Exit/Entry zones do not cause an intrusion alarm during the **Exit/Entry Delay.** If the zone is not secured by the end 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.		
Exit/Entry 2		
Same as above, except that the Exit/Entry 2 time period applies.		
Exit(Op)/Entry 1		
Used for an Exit/Entry door. This zone behaves as described in the **Exit/Entry 1** parameter, shown above, except that, if faulted, the arming process is **not** prevented. To avoid an intrusion alarm, it must be secured before the expiration of the **Exit Delay** period.		
Exit(Op)/Entry 2		
Same as above, except that the Exit (Op)/Entry 2 time period applies.		
Entry Follower		
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.		
Intruder (Instant)		
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.		
Interior + Exit/Entry 1		
Used for Exit/Entry doors, as follows: • 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. • If the system is armed in the Stay mode, the zone is bypassed.		

Parameter	Default	Range
Interior + Exit/Entry 2		
Same as the **I + Exit/Entry 1** parameter, described above, but the Exit/Entry 2 time period is applicable.		
Interior + Exit(Op)/Entry 1		
Used for an exit/entry door that, for convenience, may be kept open when the system is being armed, as follows: ♦ In Away (Full Arm) mode behaves as an **Exit (Op)/Entry 1** zone. ♦ In Stay mode, the zone will be bypassed.		
Interior + Exit(Op)/Entry 2		
Same as the **I + Exit (Op)/Entry 1** parameter, described above, but the Exit/Entry 2 time period is applicable.		
Interior + Entry Follower		
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: ♦ In Away (Full Arm) mode behaves as an Entry Follower zone. ♦ In Stay mode, the zone will be bypassed.		
Interior + Intruder (Instant)		
Usually intended for non-exit/entry doors, window protection, shock detection and motion detectors. ♦ In Away (Full Arm) mode behaves as an Intruder (instant) zone. ♦ In Stay mode, the zone is bypassed.		
Entry Follower + Stay		
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.		
24 Hours		
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.		

Zones: Parameters		
Parameter	**Default**	**Range**
Fire		
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.		
Panic		
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.		
Special		
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.		
Tamper		
For tamper detection. This zone operates the same as 24 hours zone, but it has a special reporting code.		
Note: For this zone type the zone sound is determined according to the Tamper Sound defined under **System → Sound → Tamper**		
Water (Flood)		
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 Appendix A:)* .		
Gas		
For the gas (natural gas) leak detector. This zone operates the same as 24 hours zone, but it has a special gas report code. *(See Appendix A)*		
CO		
For CO (Carbon Monoxide) gas detectors. This zone operates the same as 24 hours zone, but it has a special CO report code *(see Appendix A:)* .		
High Temperature		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code *(see Appendix A:)* .		

Zones: Parameters		
Parameter	Default	Range
Low Temperature		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code *(see Appendix A:)* .		
Technical		
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.		
Final Exit		
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.		
Exit Termination		
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 **or** opening the door, arming the system, and closing the door), the system's Exit Delay time period will be shortened to 10 seconds. When you re-open the door, the entry time restarts. **Note:** Exit Termination requires allocation of at least one Exit/Entry zone type in the partition.		
UO Trigger		
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**
Day		
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.		
Latch Key Switch Delay		
Used to apply the Exit/Entry Delay 1 parameter to the latched key switch zone.		

Zones: Parameters		
Parameter	**Default**	**Range**
Key Box		
(Designed for the Danish market) A keybox is defined as a physical container in which to place the house keys. The Agility 4 keybox zone behaves as follows: ♦ Opening a key box zone (regardless of system arming status) sends a message to the monitoring station and recorded in the event log. ♦ There will be no indication on the screen that this zone is open. ♦ Tampering a keybox causes a tamper alarm. ♦ If this zone is open, then the system can be armed.		
Open Delay		
Use this zone for a door when used with slim keypads defined as bypass mode. This zone behaves as follows: ♦ If the system is armed and the zone is opened without bypass code approval the zone acts as an instant zone. ♦ If the system is armed and the zone is opened during the *Bypass Entry Timer* it acts as an exit/entry zone (see *Entry Bypass,* page *44).* ♦ When the system is disarmed, this zone activates as an Exit (open) /Entry zone.		
Sound	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.		
Silent		
Produces no sound		
Bell		
Activates the wireless sirens (internal or external) and alarm from the main unit assigned to the partitions of the zone.		
Buzzer (main unit)		
Activates the internal buzzer on the main unit.		
Bell + Buzzer		
Activates the wireless sirens and siren on the main unit simultaneously.		
Bell/Arm Buzzer/Disarm		
In a case of alarm, the following occurs: ♦ In Away mode (Full Arm) the wireless siren will operate. ♦ In Disarm mode, only the buzzer on the main unit will operate.		

Zones: Parameters		
Parameter	**Default**	**Range**
Advanced programming		
Chime	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	YES	YES/NO

Choose which zone will be supervised by the system receiver according to the time defined under the timer RX Supervision *(see RX Supervision, page 43).*

Forced Arming	NO	YES/NO

This option enables or disables the use of forced arming for each of the system's zones, as follows:

- If forced arming is enabled for a particular zone, it allows the system to be armed even though this zone is faulty.
- When a zone(s) enabled for forced arming is faulted, the ✓ LED blinks during the disarm period.
- After arming, all zones enabled for forced arming are bypassed at the end of the **Exit Delay** time period.
- 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.

No Activity	NO	YES/NO

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 *No activity*, page *43*).

LED Enable Y/N (Only for 2 Way PIR and 2 Way WatchOUT) YES		YES/NO

Defines the LED operation mode.

YES: Detector's LED activated

NO: Detector's LED deactivated

Zones: Parameters		
Parameter	**Default**	**Range**
Abort Alarm	YES	YES/NO
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.		
Sensitivity (Only for 2-way PIR, 2-way WatchOUT, and 2-way Curtain detectors)		
Defines the sensitivity of the detector. o Low (2 -way PIR, 2 -way WatchOUT, and 2-way Curtain) o Medium (2-way WatchOUT) o High (2 -way PIR, 2 -way WatchOUT, and 2-way Curtain) o Maximum (2-way WatchOUT)		
RWX106 Detector Parameters (for 2 way WL Indoor Curtain detectors)		
LED Enable	Yes	Yes/No
Defines the LED operation mode. YES: Detector's LED activated NO: Detector's LED deactivated		
Detection Mode	Normal	Fast/Normal (2.5 min)
Use this parameter to define the minimum period between alarm transmissions. **Normal:** Only one alarm message is transmitted in any 2.5-minute time-period **Fast:** Alarm detection is immediately transmitted.		
Sensitivity	LOW	HIGH/LOW
Specifies the level of PIR channel sensitivity.		
RWX107DT Detector Parameters (for 2 way WL Outdoor DT Curtain detectors)		
LED Enable	Yes	Yes/No
Defines the LED operation mode. YES: Detector's LED activated NO: Detector's LED deactivated		
Anti-Mask	NO	YES/NO
Defines whether to activate the operation of anti-masking detection.		

Zones: Parameters			
Parameter		Default	Range
	Detection Mode	Normal	Fast/Normal (2.5 min)
	Use this parameter to define the minimum period between alarm transmissions. **Normal:** Only one alarm message is transmitted in any 2.5-minute time-period **Fast:** Alarm detection is immediately transmitted.		
	Sensitivity	LOW	HIGH/LOW
	Specifies the level of PIR channel sensitivity.		
	MW Sensitivity	65%	Min., 25%, 50%, 65%, 85%, Max.
	Specifies the level of MW channel sensitivity.		
RWX350D Detector Parameters (for 2 way Beyond WL DT Detectors)			
	Sensitivity	LOW	HIGH/LOW
	Specifies the level of PIR channel sensitivity.		
	MW Senstivity	65%	Min., 25%, 50%, 65%, 85%, Max.
	Specifies the level of MW channel sensitivity.		
	Anti-Mask	NO	YES/NO
	Defines whether to activate the operation of anti-masking detection.		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Detection Mode	Normal	Fast/Normal (2.5 min)
	Use this parameter to define the minimum period between alarm transmissions. **Normal:** Only one alarm message is transmitted in any 2.5-minute time-period **Fast:** Alarm detection is immediately transmitted.		
	Position Sensor Enabled	No	Yes/No
	Specifies whether to send an alarm following change in the position of the detector.		
Camera Parameters (for 2 -way eyeWAVE PIR cameras – RWX95CMP and Beyond WL DT Cameras – RWX350DC)			
	Images at Alarm	3	(1–7)
	Specifies the number of images to be captured when an alarm event occurs.		
	Image Interval	1.0	0.5, 1.0, and 2 seconds
	Specifies the time in between image captures.		

Zones: Parameters		
Parameter	**Default**	**Range**
Image Pre- Alarm	YES	YES/NO
Specifies if an image capture is to be performed upon each System Away arming. The picture is sent only in the event of an alarm occurrence, together with the alarm images.		
Image Resolution	QVGA	QVGA (320X240) VGA (640X480)
Specifies image quality, as defined by pixel resolution. A QVGA image file is approximately 7 Kb and VGA image file is 18 Kb		
Image Quality	High	High/Low
Specifies the extent of jpeg image lossy compression (Low=more compression, smaller file size; High=less compression, larger file size)		

Parameter	Default	Range
Colored Image	YES	YES/NO

Specifies whether the captured and transmitted photographic image is to be color or black and white.

Camera Trigger

Enables a PIR camera to "follow" (capture and send snapshots) of event activations (other than those of the PIR camera itself) which occur within the PIR's partitions. The snapshots are sent to the Follow Me user and/or monitoring station to help verify if an alarm event is real. At the keypad, PIRs can be configured as "**Y**" to "follow" any of the selections listed below.
NOTE: All selections have defaults as "**N**" except for Intruder:

- **Follow System:**
  - Duress Y/N **N**
- **Follow Partition** (can only follow the same partitions configured for the PIR's detection):
  - Panic Y/N **N**
  - Fire Y/N **N**
  - Emergency/Medical Y/N **N**
  - Intruder Y/N **Y**
  - Tamper Y/N **N**
  - No Activity Y/N **N**
  - Confirmed Alarm Y/N **N**
- **Follow Zone** (camera is activated following a zone alarm or tamper):
  - Zone 01 Y/N **N**
  - Zone 02 Y/N **N**
  - Etc.

Zones: Parameters		
Parameter	**Default**	**Range**
X73 Parameters		
This section refers to the programming options of the two-way magnetic contact RWX73M and RWX73F. **NOTE:** After programming X73 parameters and exiting Programming mode, press the Tamper switch for 3 seconds, and then wait 1 minute for the main panel to download the parameters to the detector.		
RWX73 M Parameters		
The RWX73M is a 2-way supervised transmitter that combines Magnetic/Door contact against opening doors and windows with additional universal input. The RWX73M operates with RISCO Group 2-way wireless systems		
Magnet	Enable	Enable/Disable
Enable or disable the transmitter's magnet.		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period **OFF:** Alarm detection is immediately transmitted		
Input Termination (IN 1):	NO	NO/NC/DEOL/Shutter
Use this parameter to program the connection type used for each of the system's zones. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions. **Shutter**: Specifies that the Input will count the number of open and close pulses received. If the zone exceeds the predefined number of pulses, the zone will be tripped and act according to its type definition. After a 25-second timeout, the pulse counter is restarted. The pulse length is the currently defined Loop Response time period.		
Input Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
Shutter Pulse	02	01-16
Define here the number of pulses for the input.		

Zones: Parameters		
Parameter	**Default**	**Range**
RWX73 F Parameters (Universal/Shutter Mode)		
The RWX73F is a 2-way multi-function supervised transmitter with two separate channels that combines Magnetic/Door contact against opening doors/windows with an additional universal input or shutter. The RWX73F has two reed switches for protection against opening doors and windows, and against any attempt to tamper the detector using large magnets. The RWX73F operates with RISCO Group 2-way wireless systems		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period **OFF**: Alarm detection is immediately transmitted		
Input 2 Termination (External Zone):	NO	NO/NC/DEOL/Shutter
Use this parameter to program the connection type used for Input 2. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions. **Shutter**: Specifies that the Input 2 will count the number of open and close pulses received. If the zone exceeds the predefined number of pulses, the zone will be tripped and act according to its type definition. After a 25-second timeout, the pulse counter is restarted. The pulse length is the currently defined Loop Response time period.		
Input 2 Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
Shutter Pulse		01-16
Define here the number of pulses for the input.		
RWX73 F Parameters (Universal Mode)		
The RWX73F is a 2-way multi-function supervised transmitter with two separate channels that combines Magnetic/Door contact against opening doors/windows with an additional universal input. The RWX73F has two reed switches for protection against opening doors and windows, and against any attempt to tamper the detector using large magnets. The RWX73F operates with RISCO Group 2-way wireless systems		
Magnet	Enable	Enable/Disable

Zones: Parameters		
Parameter	**Default**	**Range**
Enable or disable the transmitter's magnet.		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period OFF: Alarm detection is immediately transmitted		
Input 1 Termination (External Zone):	NO	NO/NC/DEOL
Use this parameter to program the connection type used for Input 1. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions.		
Input 1 Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
Anti-Sabotage	Disable	Enable/Disable
Enable or disable the transmitter's anti-sabotage magnet.		
Two-way Smoke Detector Parameters		
Operation Mode		Smoke/Heat/ Smoke + Heat
Set operation mode of the two-way smoke detector (model RWX34S): Smoke Only: Smoke alarm only Heat Only: Heat alarm only Smoke + Heat: Smoke or heat alarm		
RWX78M Parameters (2 way Slim Contact detectors)		
LED	On	On/Off
Defines the LED operation mode. On: Detector's LED activated Off: Detector's LED deactivated		
Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
RWX78S Detector Parameters (for 2 way Slim Shock detectors)		
LED Enabled	Yes	Yes/No

Zones: Parameters			
Parameter		Default	Range
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Shock Sensitivity	TBD	0-100%
	Defines the detector’s level of sensitivity.		
RWX78SM Detector Parameters (for 2 way Slim Shock and Contact detectors)			
Magnet			
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Hold On	On	On/Off
	Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Shock			
	Shock	Enabled	Enabled/Disabled
	Defines whether to enable or disable shock detection		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Shock Sensitivity	TBD	0-100%
	Defines the detector’s level of sensitivity. RWX78SM Detector Parameters (for 2 way Slim Shock and Contact detectors)		
RWX78MU Detector Parameters (for 2 way Magnetic Contact and Universal detectors)			
Magnet			
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Hold On	On	On/Off

Zones: Parameters		
Parameter	**Default**	**Range**
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Universal		
Universal	Enable	Enable/Disable
Defines whether to enable or disable the universal zone input.		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
External Zone		NO/NC/DEOL/Shutter
Defines the termination of the external zone input.		
Response Time		10/500 ms
Define the response time of the external zone input (applicable for NO and NC terminations only).		
Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination). **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Pulses number	On	2/4/6/8/10/12/14/16
Defines the pulse number threshold for shutter input.		
Input Protection	On	On/Off
Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).		
RWX78SMU Detector Parameters (for 2 way Magnetic Contact, Shock and Universal detectors)		
Magnet		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
Hold On	On	On/Off

Zones: Parameters			
Parameter		**Default**	**Range**
	Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Shock			
	Shock	Enabled	Enabled/Disabled
	Defines whether to enable or disable shock detection		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Shock Sensitivity	TBD	0-100%
	Defines the detector’s level of sensitivity.		
Universal			
	Universal	Enable	Enable/Disable
	Defines whether to enable or disable the universal zone input.		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	External Zone		NO/NC/DEOL/Shutter
	Defines the termination of the external zone input.		
	Response Time		10/500 ms
	Define the response time of the external zone input (applicable for NO and NC terminations only).		
	Hold On	On	On/Off
	Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination). **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
	Pulses number	On	2/4/6/8/10/12/14/16
	Defines the pulse number threshold for shutter input.		
	Input Protection	On	On/Off
	Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).		

Zones: Parameters		
Parameter	**Default**	**Range**
RWX78SU Detector Parameters (for 2 way Shock and Universal detectors)		
Shock		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
Shock Sensitivity	TBD	0-100%
Defines the detector’s level of sensitivity.		
RWX78SM Detector Parameters (for 2 way Slim Shock and Contact detectors)		
Universal		
Universal	Enable	Enable/Disable
Defines whether to enable or disable the universal zone input.		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
External Zone		NO/NC/DEOL/Shutter
Defines the termination of the external zone input.		
Response Time		10/500 ms
Define the response time of the external zone input (applicable for NO and NC terminations only).		
Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination). **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Pulses number	On	2/4/6/8/10/12/14/16
Defines the pulse number threshold for shutter input.		
Input Protection	On	On/Off
Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).		

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), then 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.

Cross Zones

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 Zone crossing

Zones: Zone Crossing
Parameter
1st Zone
The 1st zone of a pair of zones defined for zone crossings.
2nd Zone
The 2nd zone of a pair of zones defined for zone crossings.
Time
The amount of time allowed between the triggering of events for both zones to be considered a valid violation
Correlation Type
Determines how the Agility 4 will process violations of the paired zones. Please note that in either of the following cases, both of the (paired) zones need to be tripped in order to have alarm activation. ♦ Not correlate: Temporarily disables any associated zone pairings ♦ Ordered correlate: Triggers an alarm only if the 1st zone is tripped before the 2nd. ♦ Not ordered correlate: Triggers an alarm regardless of which of the two zones is tripped first.

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 Number
The serial number of the remote control. Each wireless device has its own unique serial number. Placing ID 00000000000 will delete the remote control's allocation.
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: o None: Button disabled. o Arm: The button is used for Away (Full) arming of the remote control's partitions. o 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: o None: Button disabled. o 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: o None: Button disabled. o Panic: The button is used to send a panic alarm. o Status: Main unit broadcast of system status o 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: o None: Button disabled. o Arm: The button is used for Away (Full) arming of the remote control's partitions. o Stay: The button is used for Stay (Home) arming of the remote control's partitions. o UO Control (1-20): The button is used to operate a utility output.

Two Way Bi-directional Remote Controls

The bidirectional remote control is a 4 or 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 (8-button remote control).

Remote Controls Parameters: 2 Way Remote Control
Parameter
Label
A label identifying the user of the remote control.
Serial Number
The serial number of the remote control. Each wireless device has its own unique serial number. Placing ID 00000000000 will delete the remote control's allocation.
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 using 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	N

Use  to toggle between Y (yes) and N (no) to define whether or not sending a panic alarm from the remote control is permitted. If permitted, pressing on keys  and  simultaneously for 2 seconds 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	
Instant Arm	YES
YES: Away arming from any remote control will be instant. **NO**: Away arming from any remote control will be delayed, following exit delay 1.	
Instant Stay	YES
YES: Stay arming from any remote control will be instant. **NO**: Stay arming from any remote control will be delayed, following exit delay 1.	
Disarm + Code (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, of two kinds: LCD/Panda keypads, or Outdoor/Indoor Slim keypads.

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

Parameters

Keypads: Parameters		
Parameter	**Default**	**Range**
Label		
A label identifying the keypad		
Serial Number		
The unique serial number of the keypad. Each wireless device has its own unique serial number. Placing ID 00000000000 will delete the keypad's allocation.		

Keypads: Parameters		
Parameter	**Default**	**Range**
Emergency Keys	YES	YES/NO

Defines whether the following keys will be activated or not (Y / N) to operate as emergency keys

LCD Keypad:

- Press Keys 4 and 5 simultaneously to send a fire alarm.
- Press Keys 7 and 8 simultaneously to send an emergency alarm.

Panda Keypad:

- Press Keys 4 and 6 simultaneously to send a fire alarm.
- Press Keys 7 and 9 simultaneously to send an emergency alarm.

Slim Keypad:

- Press buttons 1 + 2 simultaneously for two seconds to send a panic alarm
- Press buttons 3 + 4 simultaneously for 2 seconds to send a fire alarm
- Press buttons 5 + 6 simultaneously for 2 seconds to send an emergency / medical alarm

Function Key (Only LCD keypad)	Panic

Defines the operation of the (*) (#) keys for each keypad.

- Disabled: Keys disabled.
- Panic Alarm: Send a panic alarm to the monitoring station.
- MS Listen /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 1 2 3 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

Mode (only for slim keypad)

Use this parameter to define the slim keypad operation mode.

1. Arm/Disarm: the slim keypad is to have full user control of the system.
2. Bypass: designed for the Danish market; the slim keypad is to operate in bypass mode.

Note: For further information, see the keypad documentation.

Door Bell Sound (only for slim keypad)

Use this parameter to define the chime sound (broadcast by the main unit) when the slim keypad door chime button () is pressed as follows:

- None
- Chime sound 1/2/3

Supervision

Choose if the keypad (Slim, LCD or Panda) will be supervised or not.

Auto Status

The panel provides relevant data on the keypad icons, following keypad wake up by the user. For example, connection status and arm/disarm state.

Controls

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

Keypads: Controls

Parameter	Default	Range
RF Wake-up	NO	YES/NO

Use  to toggle between Y (yes) and N (no) to define 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
Label		
A label identifying the siren.		
Serial Code		

Wireless Device: Sirens		
Parameter	**Default**	**Range**
The unique serial number of the sirens. Each wireless device has its own unique serial number. Placing ID 00000000000 will delete the siren's allocation.		
Partition		
Assign the partitions that will affect the sounder operation.		
Supervision	YES	
Choose if the siren will be supervised or not.		
Volume	9	0-9
Define the volume of the sounder for the following scenarios in the system.		
Alarm Volume	9	0-9
The sound volume produced during an alarm (0 indicates silence).		
Squawk Volume	5	0-9
The sound volume produced during squawk sounds (0 indicates silence).		
Exit/Entry Volume	OFF	0-9
The sound volume produced during exit/entry time. (0 indicates silence).		
Strobe (External siren only)		
Defines the parameters for the strobe of the external siren.		
Strobe Control		
Defines the Strobe operation mode: o Always off: The strobe is deactivated o Follow Bell: The strobe is activated once when the siren bell is triggered o Follow Alarm: The strobe is activated when an alarm event occurs in the system		
Strobe Blink	40	
Defines the number of times that the strobe will blink in a minute: o 20 times per minute o 30 times per minute o 40 times per minute o 50 times per minute o 60 times per minute		
Strobe Arm Blink	05	00-20
Defines the time that the strobe will blink when the system is armed.		

2.2.5 Wireless I/O 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
Label		
A label identifies the zone in the system. (up to 16 characters).		
Partition	1	
The partitions assignment for each zone.		
Type	Intruder	
Contains parameters that enable you to program the zone type for any zone. Refer to page 59 for a list of Zone Type options.		
Sound	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 65.		
Advanced programming		
Chime	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.		
Control		
Forced Arming	N	
Define whether the zone can be force armed or not. For more information regarding the force arming feature refer to page 66.		
No Activity	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. For more information regarding the force arming feature refer to page 66.		
Abort Alarm	Y	
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 66.		

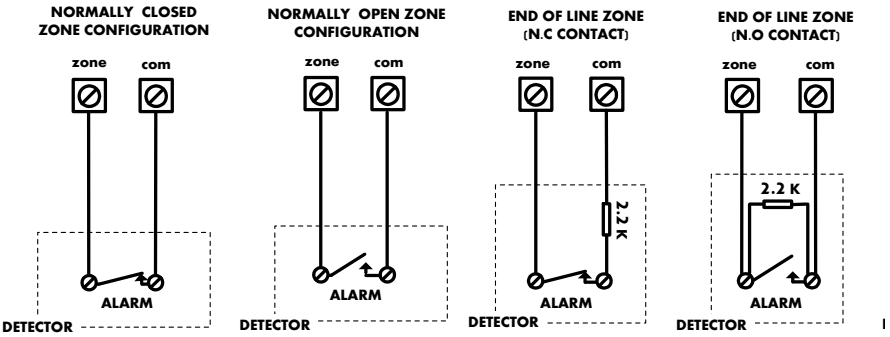
I/O Expander: Wired Zones

Parameter	Default	Range

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 2200Ω 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**
Label		
A label identifies the output in the system.		
Type		
There are 4 types of outputs in the system as follows o **Not Used** o **Follow System**: The utility output will follow a System Event o **Follow Partition**: The utility output will follow a Partition Event. o **Follow Zone**: The utility output will follow a Zone Event. Each Utility Output can be activated by a group of up to five zones. o **Follow Code:** The utility output will be activated by a user defined as UO Control or from the user programming menu.		
Follow System Events:		
Bell		
Activates when a bell is triggered. If a bell delay was defined, the utility output will be activated after the delay period.		
No Telephone Line		
Activates when a telephone line fault is detected. If a PSTN Lost Delay time period is defined, the utility output will be activated after the delay time		
Monitoring Station Communication Fail		
Activates when communication with the Central Station cannot be established. Deactivates after a successful call is established with the Central Station.		
General Trouble		
Activates when a system trouble condition is detected. Deactivates after the trouble has been corrected		
Main unit Low battery		
Activates when the Agility 4 battery has insufficient reserve capacity and the voltage decreases to 6V.		
AC Loss		
Activates when the source of the main panel's AC power supply is interrupted. This activation will follow the delay time defined in the system control times and the **AC Off Delay Time** parameter.		

I/O Expander: Output Parameters		
Parameter	Default	Range
Bell burglary		
Activates the Utility Output after any bell burglary alarm in any partition in the system.		
Scheduler		
The utility output will follow the predefined time programming that is defined in the scheduler of the weekly programs for utility output activation.		
Tamper		
Activates the utility output when a Tamper occurs in the system.		
Duress		
Activates the Utility Output when a duress alarm is initiated by any user defined as duress code.		
GSM Trouble		
Activates the utility output when there is trouble in the GSM module.		
Follow Open Delay		
This output is activated once an Entry Bypass timer starts (see *Entry Bypass,* page *44*). The output is designed to be part of the bypass keypad solution for the Danish market. The output behavior depends on the output pattern as follows: **Pulsed**: Use this option to activate an electronic lock. The time duration is as defined by the installer under Pulse Duration Length (see *Pulse Duration Length,* page *92).* **Latched**: While the system is disarmed, entering a bypass *code* will activate the output like an access control reader. Output operation using the bypass code during disarm mode will not be registered in the event log. During Away mode, opening an Open Delay zone (during the Bypass Entry Time) will shorten the output time to 3 seconds.		
Door Bell		
Activates the Utility Output when a door button is pressed on a slim keypad. This output operates only as a pulse output (as defined by Pulse Duration Length (see *Pulse Duration Length,* page *92).*		
Follow Partition Events:		
Ready		
Activates the utility output when all the selected partition(s) are in the Ready state.		

I/O Expander: Output Parameters		
Parameter	Default	Range
Arm		
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.		
Disarm		
Activates the Utility Output when the selected partition(s) is disarmed.		
Alarm		
Activates the Utility Output when an alarm occurs in the selected partition(s).		
Intruder alarm		
Activates the utility output when an intrusion (Burglary) alarm occurs in the selected partition(s).		
Fire		
Activates the utility output when a fire alarm is triggered in the selected partition(s) from the keypads or a zone defined as Fire.		
Panic		
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.		
Special		
Activates the utility output when a special alarm is triggered in the selected partition(s) from the keypads or a zone defined as Special .		
Exit/Entry		
Activates the Utility Output when the selected partition(s) initiates an Exit/Entry Delay period.		
Zone Bypass		
Activates the Utility Output when the relevant partitions are in ARM or STAY mode and any zone in the relevant partitions is bypassed.		
Auto Arm Alarm		
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.		
Zone Lost		
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.		

I/O Expander: Output Parameters		
Parameter	**Default**	**Range**
Stay Follow		
Activates the Utility Output when the selected partition(s) is armed in Stay mode.		
Chime Follow		
Activates the Utility Output following a chime sound in the selected partition(s)		
Bell Stay Off		
This parameter causes the utility output to function as follows: ♦ In Away arming mode, the utility output will follow the bell activation in the defined partitions. ♦ In Stay arming mode, the utility output will not be activated.		
Bell		
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.		
No Activity		
Activates the utility output when an event of NO ACTIVITY occurs in the system. . The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people		
Confirmed alarm		
Activates the utility output when a confirmed alarm occurs in the system.		
Follow Zone Events:		
Zone		
Activates the utility output when the selected zone is tripped. The tripped zone need not be armed to trigger the Utility Output.		
Alarm		
Activates the utility output when the selected zone causes an alarm.		
Arm		
Activates the utility output when the selected zones are armed.		
Disarm		
Activates the utility output when the selected zones are disarmed.		

I/O Expander: Output Parameters		
Parameter	**Default**	**Range**
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  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.		
Activation / Deactivation		
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: o 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. o 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.		
Pulse Duration Length	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
Label		
A label identifies the output in the system		
Type		
Refer to the explanation under the utility output section.		
Pattern		
Refer to the explanation under the utility output section.		
Pulse Length	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
Serial Number		
The internal ID number of the I/O Expander. Each wireless device has its own unique serial number.		
Controls		
I/O Expander Supervision		
Choose if the I/O Expander will be supervised or not.		
Quick Output Operation		
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.		
X-10 House ID		
Defines the house code, which matches the code defined by the X-10 modules.		
UO DTMF Control		
The Agility 4 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/display:

```
Please start RF
identification
```

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

2.4 Delete

For deletion of single devices, see *Deleting a Single Device from the LCD/Panda* Keypad, page *36*.

3. Programming: Codes Menu

The **Codes** menu provides the ability to 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
Labels	
Used to describe the user. Up to 32 characters can be used.	
Partition	
Enables you to assign the partition/s (1—3) in which each user (except for the Grand Master, whom can operate all 3) can-operate. Use  /  to scroll to the partitions, and then press  /  to toggle between enabling [**Y**] or disabling.	
Authority Level	
Allocate an authority level to a user according to the following list: **NOTE:** The installer does not assign the actual codes. Assigning the codes is done by the Grand Master / system users. **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 open, but typically are	

last to leave, thus they typically close the premises and arm the system. The users with Arm Only Codes have access for arming one or more partitions.

- **Duress**: When forced into disarming the system, by entering a specific code, a system user can comply with the intruder's demands while simultaneously sendir a silent duress alarm to the monitoring station. In any other situation the duress authority level behaves as the same as the user authority level (see prior page).
  NOTE: Under no circumstances should the duress code be used haphazardly or without reason. Monitoring stations, along with police departments, treat duress codes very seriously and take immediate action.
- **Door Bypass:** Use this authority level when the slim keypad reader is defined in Bypass mode. The authorization code defined here initiates the Entry Bypass Timer (see *Entry Bypass*, page *44*). This authority is recognized only on a slim (not LCD/Panda) keypad.

3.2 Grand Master

The Grand Master Code (default = **1234**) is typically used by the system's owner and is the highest Authority Level. This person can set/change the Grand Master Code.

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 4 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 4 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: 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

NOTE: When you change the Code Length parameter, all user codes are deleted and must be re-programmed or downloaded.

NOTE: 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.

NOTE: 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. Cloud

4.1 Method Sub-Menu

The Method sub-menu allows you to configure the parameters of the available communication channels for the system:

1. PSTN

2. GSM

3. IP

4.1.1 PSTN

The PSTN screen contains parameters for the system communication over the PSTN network

Method: PSTN			
Parameter		**Default**	**Range**
Timers			
Timers related to communication through the PSTN channel			
	PSTN Lost	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.		
	Wait for Dial Tone	3	0-255 seconds
	The number of seconds the system waits to detect a dial tone.		
Control			
	Alarm Line Cut	No	
	YES: Activates the external sirens if the land line, connected to the Agility 4 panel is cut or the telephone service is interrupted for the time defined in the **PSTN Lost** time parameter. **NO**: No activation occurs.		

Method: PSTN		
Parameter	**Default**	**Range**
Answering Machine Override	Yes	

YES: The Answering Machine Override is enabled, as follows:

- The Configuration Software at the alarm company calls the account.
- The software hangs up after one ring by the configuration operator.
- Within one minute, the software calls again.
- The system is programmed to pick up this second call on the first ring, thus bypassing any interaction with the answering machine.

Note: This feature is used to prevent interference from an answering machine with remote configuration operations.

NO: The Answering Machine Override is disabled, and communication takes place in the standard manner.

CS via PSTN	Yes	

YES: The system allows access to Configuration Software through a PSTN connection

NO: The system does not allow access to Configuration Software through a PSTN connection

Parameters		
Rings to Answer	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 PSTN 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 system communication over the GSM/GPRS network.

Method: GSM		
Parameter	**Default**	**Range**
Timers		
Allows to program timers related to operation with the GSM module		
GSM Lost	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.		
SIM Expire	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.		

Method: GSM		
Parameter	**Default**	**Range**
MS Keep Alive (Polling)	00000	0-65535 times

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.

Note: When using the polling feature through GPRS the MS channel parameter must be defined as GPRS only.
The report code for MS polling is 999 (Contact ID) or ZZ (SIA)

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)

- **Primary**: This time period is used when the MS channel is defined as *GPRS Only* and the Report Split parameter is not defined as *1st backup 2nd*.
- **Secondary**: This time period is used when the MS 2 channel is defined as *IP →GPRS Only* and the Report Split parameter is defined as *1st backup 2nd*.
- **Backup**: This time period will be assigned to the backup channel in the following case:
  - MS 2 channel is defined as *IP →GPRS Only*
  - Report Split parameter is defined as *1st backup 2nd*
  - The communication with MS 1 is disconnected.

GPRS

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).

Method: GSM			
Parameter		**Default**	**Range**
	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		
Controls			
Allows to control timers related to operation with the GSM module.			
	Caller ID	NO	NO/YES
	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.		
	Disable GSM	NO	NO/YES
	YES: The system will disable the GSM/GPRS module from any activity. NO: GSM/GPRS module is enabled in the system.		

Method: GSM		
Parameter	**Default**	**Range**
CS via GPRS (out)	YES	NO/YES
YES: Enables to connect the panel to remote Configuration Software via the GPRS channel. The connection can be established either from the LCD/Panda keypad (**Installer Menu > Activities > 7)CS Connect > 2)Via GPRS)** or via SMS request command from the Configuration Software. **NO:** Communication between the Configuration Software and the panel via GPRS is disabled		
CS via GPRS (Listener mode)	NO	NO/YES
YES: The installed GSM/GPRS communication module enters into listener mode. Configuration Software can then initiate connection to it. **Note**: When using the polling feature through GPRS the MS channel parameter must be defined as GPRS only. The report code for MS polling is 999 (Contact ID) or ZZ (SIA) The listening mode feature in the GSM/GPRS module can occur only if there is a static IP address for the SIM card (Please consult the local telecommunication provider). **NO**: The installed GSM/GPRS communication module will not enter into listener mode and therefore Configuration Software cannot initiate connection to it.		
CS via CSD	YES	NO/YES
YES: Configuration Software can attempt to contact the panel through the GSM CSD channel. **NO**: Configuration Software cannot attempt to contact the panel through the GSM CSD channel.		
Parameters		
Allows to program timers related to the operation with the GSM module.		
SIM PIN Code		
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.		
SMS Center Phone		
A telephone number of the message delivery center. This number can be obtained from the network operator.		
GSM Network Sensitivity (RSSI)		
Set the minimum acceptable network signal level (RSSI level). Options: Disabled (No troubles for low signal reception) / Low signal / High		

Method: GSM		
Parameter	**Default**	**Range**
signal		
SIM Number		
The SIM phone number. The system uses this parameter to receive the time from the GSM network in order to update the system time.		
Prepaid SIM Card		
Allows programming parameters that will be used when a prepaid SIM card is used in the system.		
Get Credit by		
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. • **SMS Credit Message**: Type in the message command as defined by the provider and the provider's phone number to which the credit level SMS message request will be sent. • **Voice Credit**: Type in the provider's phone number to which a call will be established • **Service Command**: 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

Method: IP		
Parameter	**Default**	**Range**
IP Configuration		
Obtain Automatic IP	YES	Y/N
Defines whether the IP address, which the Agility 4 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.		
Panel IP		
The Agility 4's IP address.		

Method: IP			
Parameter		**Default**	**Range**
	Subnet Mask		
	The subnet mask is used to determine where the network number in an IP address ends.		
	Gateway		
	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 4.		
	DNS Primary		
	The IP address of the primary DNS server on the network.		
	DNS Secondary		
	The IP address of the secondary DNS server on the network		
E-mail			
Allows programming parameters that enable the Agility 4 to send e-mail messages following Follow Me events			
	Mail Host		
	The IP address or the Host name of the mail server.		
	SMTP Port		
	The port address of the SMTP mail server. Default: 00025		
	E-mail address		
	Agility 4's e-mail address. Default: YourCompany.com		
	SMTP User name		
	If required by the mail server, fill in the Authentication User name		
	SMTP User password		
	If required by the mail server, fill in the Authentication User password		
Host Name		Security_System	(Up to 32 characters)
IP address or a text name used to identify the Agility 4 over the network. Default: Security System			
MS Keep Alive (Polling)		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.			

Note: 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)

- **Primary**: This time period is used when the MS channel is defined as *IP Only* and the Report Split parameter is not defined as *1st backup 2nd*. Default: 00003 (30 seconds)
- **Secondary**: This time period is used when the MS 2 channel is defined as *IP→IP Only* and the Report Split parameter is defined as *1st backup 2nd*. Default: 360 (3600 seconds)
- **Backup**: This time period will be assigned to the backup channel in the following case:
  - MS 2 channel is defined as *IP→IP Only*
  - Report Split parameter is defined as *1st backup 2nd*
  - The communication with MS 1 is disconnected.

  Default: 00003 (30 seconds)

Controls		
Disable IP	NO	YES/NO
YES: The system will disable the IP module from any activity. NO: The IP module is enabled in the system.		
CS via IP	YES	YES/NO
YES: The system allows access to Configuration Software through an IP connection NO: The system does not allow access to Configuration Software through an IP connection		

4.2 Monitoring Station

The Monitoring Station sub-menu contains parameters that enable the system to establish communication with the (up-to-three) monitoring stations and transmit data.

Communication: Monitoring Station

Parameter	Default	Range
Report Type		
Type		
Defines the communication type that the system will establish with each monitoring station. The system can report in 4 optional communication types: • **Voice** • **SMS** • **IP** • **SIA 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.

Function	Results
Stop dialing and wait for a new dial tone	**W**
Wait a fixed period before continuing	**,**
Send the DTMF ∗ character	**∗**
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 Receiver Software located at the monitoring station site. The IP 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 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 the Voice type on page 106).

Note: An appropriate GSM/SMS transceiver must be connected to the same PC as an IP Receiver.

Communication: Monitoring Station			
Parameter		Default	Range
	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 Receiver Software located at the monitoring station 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. • **IP Only**: The report is executed through the IP network only. • **GPRS Only**: The report is executed through the GPRS network. Enter the relevant IP and Port numbers for the MS that will receive reports from the system		

Communication: Monitoring Station		
Parameter	**Default**	**Range**
SIA IP		
Reports to the monitoring station can be transmitted using the SIA IP protocol to standard SIA IP receivers. Using SIA IP enables transmission of visual imagery from PIR cameras. Reporting by SIA IP can be established through the hardware channels installed in your system. Reporting of the SIA IP is 128 BIT AES encrypted. SIA IP reports also support labels reporting. Usage of SIA IP requires setting: • Encryption Key (see page 111) • SIA IP Receiver Number • SIA IP Receiver Line Number		
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.

Communication: Monitoring Station		
Parameter	**Default**	**Range**

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* on page *136* for the report codes list.

Controls

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

Handshake	NO	YES/NO

YES: All LEDs on the Agility 4 main panel light for one second when the handshake signal is received from the monitoring station's receiver.

NO: No indication for establishing communication with the monitoring station's receiver.

Kiss-Off Y/N	NO	YES/NO

YES: All LEDs on the Agility 4 main panel light for one second and an audible sound is emitted when the kissoff signal is received from the monitoring station's receiver.

NO: No indication for establishing communication with the monitoring station's receiver.

SIA Text	No

YES: SIA formatted report to the monitoring station will support text transmission over the voice channel.

Note: The monitoring station receiver should support the SIA Text protocol.

NO: The SIA formatted report will not support text.

SIA IP + SN	N

Select whether or not to add the panel's serial number (for sending events with images to the monitoring station software) via SIA IP protocol

SIA with Partition

Indicates the partition when reporting to the monitoring station in SIA over the voice channel (PSTN or GSM).

Parameter	Default	Range
Random MS Test		
YES: At First power up the system will set a random hour which then becomes the fixed hour for the panel to report periodic testing to the Monitoring Station. This time can be viewed under the Periodic test timer fields. **NO**: The periodic test will be according to the time defined by the installer defined under the MS periodic timer		
Parameters		
Allows to program parameters related to operation with the Monitoring Station.		
MS Retries	08	01-15
The number of times the system redials the Monitoring Station after failing to establish communication.		
Alarm Restore	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. ♦ **On Bell Time Out (BTO) -** Reports the restoral after the audible alarm times out. ♦ **Follow Zone -** Reports the restoral when the zone in which the alarm occurs returns to its non-violated (secured) state. ♦ **At Disarm** - Reports the restoral when the system (or the partition in which the alarm occurs) is disarmed, even if the siren has already timed out.		
Encryption Key		
A 32-digit digital signature and authentication for purposes of safeguarding data transmission to and from the monitoring station. The key must be defined for both the panel and monitoring station. For use when SIA IP report type is in effect. A unique key can be defined for each of up to three monitoring stations.		
Receiver Number		
A 4 digit number which states the SIA IP receiver number as supplied from the monitoring station. A unique key can be defined for each of up to three monitoring stations.		
Line Number		
A 4 digit number which states the SIA IP receiver line number as supplied from the monitoring station. A unique key can be defined for each of up to three monitoring stations.		
MS Timers		
Allows to program timers related to operation with the monitoring station.		

Communication: Monitoring Station		
Parameter	**Default**	**Range**
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.		
Abort Alarm	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.		
Cancel Delay	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.		
Note: Cancel Alarm report code should be defined.		
Listen In	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.		
Confirmation		
The confirmation times relate to the Zone Sequential Confirmation.		
Confirm Start (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.		
Confirm Time Window	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.		

Parameter	Default	Range
No Arm	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)

Report Split

The Report Split menu contains parameters that enable the routing of specified events to up to three MS Receivers. See Appendix A on page *136*.

MS Arm/Disarm

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

- Do not call (no report)
- Call 1st: Reports Openings and Closings to MS 1
- Call 2nd: Reports Openings and Closings to MS 2
- Call 3rd: Reports Openings and Closings to MS 3
- Call 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**
Report Codes		
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 see *Appendix A* on page *136*.		

4.3 Configuration Software

The Configuration Software sub-menu contains parameters that enable the Configuration Software to establish connection with the system.

Communication: Configuration software		
Parameter	**Default**	**Range**
Security		
Enables you to set parameters for remote communication between the technician and the system using the Configuration Software		
Access Code 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.	5678	

Communication: Configuration software		
Parameter	**Default**	**Range**
Remote ID	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		
MS Lock	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		
Call Back Enabled	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		

Communication: Configuration software		
Parameter	**Default**	**Range**
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.		
Configuration Software IP Gateway		

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 4 has a Follow-Me feature which enables reporting a system events to predefined destinations using a voice message, SMS message or e-mail. Up to 16 Follow Me destinations can be defined in the system.

NOTE: The actual destinations (telephone numbers, email addresses) are defined outside of the Installer Programming menu, or can be done from the User menus by the Grand Master**.**

NOTE: Additional Follow-Me (known as "Follower") e-mail notifications can be assigned in the RISCO Cloud.

Define FM

Communication: Follow-Me		
Parameter	**Default**	**Range**
Label (via the Configuration Software)		
A label identifying the follow me destination		
Report 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). Enter the e-mail address for Follow Me destination defined as e-mail type.		
Channel		
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.		

Communication: Follow-Me		
Parameter	**Default**	**Range**

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-receive its own set of event notifications. Choose the events that will be reported to each Follow Me destination.

Event	Description	Default
Alarms		
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
Arm/Disarm		
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
Troubles		
False Code	After 5 unsuccessful attempts of entering an incorrect code.	No
Main Low Battery	Low battery indication from the Agility 4 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

Communication: Follow-Me		
Parameter		**Default Range**
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
GSM		
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 *SMS Receive Phone* will be transferred to the Follow Me number	No
Environmental		
Gas Alert	Gas (natural gas) alert from a zone defined a Gas detector	Yes
Flood Alert	Flood alert from a zone defined as flood type	Yes
CO Alert	CO (Carbon Monoxide) alert from a zone defined a CO detector	Yes
High Temperature	High Temperature alert from a zone defined a Temperature detector	Yes
Low Temperature	Low Temperature alert from a zone defined a Temperature detector	Yes
Technical	Alert from the zone defined as Technical	No

Communication: Follow-Me		
Parameter		**Default Range**
Miscellaneous		
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
Communication Info	The following information is sent by e-mail on power up and acquiring the GPRS and Ethernet communication parameters (Assumption is that SMTP is predefined): • Panel UID • Panel version • Ethernet IP parameters • GPRS IP parameters	No
Restore Events:		
Alarms		
Intruder Alarm	Intruder alarm in the system restored	Yes
Tamper	Tamper alarm in the system restored	No
Troubles		
Main Low Battery	Low battery indication from the Agility 4 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
Environmental		
Gas Alert	Gas Alert restored	No
Flood Alert	Flood Alert restored	No
CO Alert	CO Alert restored	No

Communication: Follow-Me				
Parameter		**Default**	**Range**	
High Temperature	High Temperature Alert restored			No
Low Temperature	Low Temperature Alert restored			No
Technical	Technical alert restored			No

Remote Control

Remote Listen — No

Enables the user of the follow me phone to perform remote listen and talk operation with the premises.

Remote program — No

Enables the user of the follow me phone to enter the Remote Operation menu and perform all available programming options.

Partition

Assign the partitions from which events will be reported to the follow me number.

Controls

Allows to program control related to operation with the Follow Me

Disarm Stop Follow Me — Yes — Yes/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

Parameters

Allows to program parameters related to operation with the Follow Me

Follow Me Retries — 08 — 01-15

The number of times the Follow Me phone number is redialed

Voice Message Recurrence — 01 — 01-05

This number of times a voice message repeats itself when establishing a call to a Follow Me number.

Follow Me Periodic Test

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.

4.5 Cloud

You can define the server settings for Cloud communication with the Agility 4 system.

Communication: Cloud

Parameter	Default	Range
IP Address		
The IP address or server name. If the Agility 4 system is connected to the RISCO Cloud for self-monitoring, then use: www.riscocloud.com. Otherwise enter the IP address or name where the Cloud server is located.		
IP Port	33000	
The server port address.		
Password	AAAAAA	Up to 6 characters (case sensitive)
Specify the password for server access. This password should be identical to the **CP Password** defined in the server under the Main Panel page definition.		
Channel		

Communication with the Cloud can be established through an IP or GPRS channel, depending on your system installed hardware.

- **IP Only**— Communication to the Cloud through the IP network only
- **GPRS Only**— Communication to the Cloud through the GPRS network only
- **IP/GPRS**— The panel checks for the availability of the IP network. By default the primary communication channel to the Cloud is via IP network. In the case of trouble in the IP network, the communication is routed through the GPRS network as a backup. Later on, it will check every 10 minutes when the primary communication channel is available
- **GPRS/IP**— The panel checks for the availability of the IP network. By default the primary communication channel to the Cloud is via GPRS network. In the case of trouble in the IP network, the communication is routed through the IP network as a backup. Later on, it will check every 10 minutes when the primary communication channel is available.

Communication: Cloud		
Parameter	**Default**	**Range**
Controls		
The Agility 4 supports parallel channel reporting (via PSTN, IP, GPRS SMS, or voice) to both the monitoring station and FM when connected in Cloud mode. Use this setting to decide if the panel reports events to the monitoring station or follow-me in parallel to the report to the Cloud or only as a backup when the communication between the Agility and the Cloud is not functioning. Note: When the backup mode is functioning, the MS specifications are as defined under MS menu (see *Monitoring Station*, page *106)*, MS report type, and Follow-Me menu (see *Follow-Me*, page *116*).		
MS Call All	**N**	
Yes: Parallel reporting to the monitoring station can be established via both the Cloud and non-Cloud channels. **No:** Communication to the monitoring station via the non-Cloud channels can be established only in backup mode (when the Cloud connection is down)		
FM Call All	**N**	
Yes: Parallel reporting to the Follow Me destination can be established via both the Cloud and non-Cloud channels. **No:** Communication to the Follow Me destination via the non-Cloud channels can be established only in backup mode (when Agility 4– Cloud connection is down)		
App Arm	**Y**	
Enables controlling the App arm functionality (for full arm or partial arm) from the Smartphone or Web interface applications. **Yes:** Full arm and partial arm are enabled **No:** Full arm and partial arm are disabled		
App Disarm	**Y**	
Enables controlling the App disarm functionality (for full disarm) from the Smartphone or Web interface applications. **Yes:** Full disarm is enabled **No:** Full disarm is disabled		
App Exit Delay	**Y**	
Enables controlling the App Exit Delay functionality from the Smartphone or Web interface applications. **Yes:** Exit Delay is enabled **No:** Exit Delay is disabled		

5. Programming: Audio Messages Menu

The Audio Messages menu is used to define voice message parameters. This 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:

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 C: 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
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 clicking the status button on the keypad/remote control	Yes
Entry / Exit	System in entry or exit 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 4 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. Keyfob
4. Keypad
5. Siren
6. GSM
7. IP Unit
8. UO Unit

1. Main Unit

Main Unit
Parameter
Noise Level

From an LCD/Panda keypad, you can measure ("calibrate") the background noise level (RF interference) that the main panel detects, and also define ("view/edit") the acceptable threshold value, according to customer requirements. Measuring the noise level provides an indication whether the main panel is mounted at a good location, and defining the threshold value enables you to determine how much background noise the system will tolerate before it generates jamming events.

To measure the background noise level detected at the main panel:

- Select **Calibrate**; the detected background noise level displays. If the resulting value is far from your defined threshold value, or if the value is too high and you believe the source of background noise may inherent to the main panel's location, you should move the main panel to a better location. See *Comm Test*, on the following page for an explanation of acceptable results.

To define the system's acceptable noise level threshold value:

- Select **View/Edit,** enter the threshold value (between **00 –99),** and then press  /  . The higher the number you set for the threshold value, the more "sensitive" the system will be in generating jamming events (more frequently). The lower the number set for the threshold value, the "more tolerant" the system will be in generating jamming events (less frequently). See *Comm Test*, on the following page for an explanation of acceptable results.

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
The Communication test displays the results of the signal strength measured at the panel after the last device transmission (last detection or last supervision signal). Make sure to activate the detector prior to the test. For successful communication: 1) The signal strength (the Comm. test result) should be at least 30% (30 or more must display). 2) In addition, the Comm. test result must be at least 10% higher than the result obtained when performing the procedure to measure ("calibrate") the background noise level that the panel detects. For example, if the noise level measures 25%, the Comm. test result must be 35% or more.
Battery Test
For the selected zone or device, displays the results of the last battery test performed after the last transmission. An OK-message is displayed for a successful test. For an updated battery test result, activate the device before testing.
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 and allocating all wireless devices and also prior to performing system operation.
The keypad LCD/Panda displays the following information for example:
 	
`Zone xx:`
`TRIP TMP TRBL`
 	
Zone number; TRIP: (Successful detection); TMP: (Tamper detection) and Trb (Low battery)

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

3. Keyfob

Keyfob		
Parameter	**Default**	**Range**
Comm Test		
The Communication test displays the results of the signal strength measured at the panel after the last device transmission (last detection or last supervision signal). For successful communication: 1) The signal strength (the Comm. test result) should be at least 30% (30 or more must display). 2) In addition, the Comm. test result must be at least 10% higher than the result obtained when performing the procedure to measure (“calibrate”) the background noise level that the panel detects. For example, if the noise level measures 25%, the Comm. test result must be 35% or more.		
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		
The Communication test displays the results of the signal strength measured at the panel after the last device transmission (last detection or last supervision signal). Make sure to activate the device prior to the test. For successful communication: 1) The signal strength (the Comm. test result) should be at least 30% (30 or more must display). 2) In addition, the Comm. test result must be at least 10% higher than the result obtained when performing the procedure to measure (“calibrate”) the background noise level that the panel detects. For example, if the noise level measures 25%, the Comm. test result must be 35% or more.		
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		

Keypad		
Parameter	**Default**	**Range**
This menu displays information regarding the keypad's version.		

5. Siren

Siren		
Parameter		
Comm Test		
The Communication test displays the results of the signal strength measured at the panel after the last device transmission (last detection or last supervision signal). Make sure to activate the device prior to the test. For successful communication: 1) The signal strength (the Comm. test result) should be at least 30% (must display at least 30 or more). 2) In addition, the Comm. test result must be at least 10% higher than the result obtained when performing the procedure to measure ("calibrate") the background noise level that the panel detects. For example, if the noise level measures 25%, the Comm. test result must be 35% or more.		
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 enables measuring ("calibrating") and displaying the background (RF) noise as measured at the siren, and also enables setting the noise level threshold – so that the panel won't cause jamming events as frequently if, for example, the siren is located where there is an unusually high amount of background noise.

To calibrate (measure) the background noise at the siren:

1. At **4)Noise Level,** press  /  , then scroll to the siren to measure and press  /  .
2. Scroll to **Calibrate** and then press  /  ; the result displays.

To define the noise level threshold value:

1. At **4)Noise Level,** press  /  , then scroll to the siren to measure and press  /  .
2. Scroll to **View/Edit** and then press  /  .
3. Enter a new threshold level value (between 00—99), and press  /  . Keep in mind the lower the number you set, the more "sensitive" the system will be (generating jamming events more frequently), and the higher the number you set, the more "tolerant" the system will be (generating jamming events less frequently).

Version
This menu displays information regarding the siren's version.

6. GSM

GSM		
Parameter	**Default**	**Range**
Signal (RSSI)d		(0–5)

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

GSM		
Parameter	**Default**	**Range**
View the IMEI number of the GSM module. This number is used for identification of the Agility 4 at the RISCO IP receiver when using GSM communication.		
IP Address		
The IP address given to the GSM when used in the Listener mode.		
IMSI		
International Mobile Subscriber Identity (IMSI) is a number that uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network.		
ICCID		
Integrated Circuit Card Identifier is a SIM card that contains its unique serial number (ICCID). ICCIDs are stored in the SIM cards and are also printed on the SIM card during a personalization process.		

7. IP Unit

IP Unit		
Parameter	**Default**	**Range**
IP Address		
View the IP address of the Agility 4		
Version		
View the version on the IP card		
MAC Address		
View the MAC address of the IP card. This number is used for identification of the Agility 4 at the RISCO IP Receiver when using IP communication.		

8. UO Unit

UO Unit		
Parameter	**Default**	**Range**
Comm Test		

UO Unit		
Parameter	**Default**	**Range**
The Communication test displays the results of the last signal strength measurement performed after the last device transmission (last detection or last supervision signal). When performing a Comm. test, make sure to activate the device prior. For successful communication: 1) The signal strength (the Comm. test result) should be at least 30% (must display at least 30 or more). 2) In addition, the Comm. test result must be at least 10% higher than the result obtained when performing the procedure to measure ("calibrate") the background noise level that the panel detects.		
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 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**
Main Buzzer On/Off	Off	
Used to activate/deactivate the main unit buzzer.		
KP Sleep Time	10 seconds	10-60 seconds
Used to set the keypad's Sleep mode time. (The LCD/Panda display is turned off.)		
Service Mode		
Grand masters and Installers can silence any tamper (and suppress a report to the monitoring station) in the system from the main unit or any accessory for a period specified in Service Time (see *Service Time*, page 44). Use this option, when system accessories require battery replacement.		
Avoid Report Programming		
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		

Activities		
Parameter	**Default**	**Range**
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 pages 44 and 47 respectively 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 CS location 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.

System Restart

Enables to restart the main panel via the keypad

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**
Time + Date		
Allows the setting of the system time and date. This definition is required for setting the scheduler programming in the system.		

Clock		
Parameter	**Default**	**Range**
Scheduler		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.		
Note: The definition of the scheduling programs is done from the Configuration Software.		
Automatic Clock		
Used to get an automatic time update (NTP or Daytime protocols) through the IP network or GPRS.		
Server		
Select the Internet time protocol as **NTP** or **Daytime**		
Host		
The IP address or server name.		
Port		
The server port.		
Time Zone (GMT/ UTC)		
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

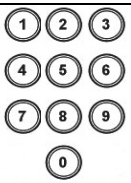
Agility 4 enables the installer or Grand Master to record a series of commands and assign them to a macro. When the macro is pressed, the recorded commands are executed from beginning to end. Up to 3 macros can be programmed to a system using the wireless LCD/Panda keypad or the Agility 4 Configuration 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.
NOTE: Macros cannot be activated from the Slim keypad.

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	Description
	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
 and 0 simultaneously /  and 0 simultaneously	Deletes your entry from the cursor position forward
 (LCD Keypad) /  (Panda Keypad)	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

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
Alarms			
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Fire alarm	115	FA	Urgent
Fire alarm restore	115		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
Confirmed HU alarm (PD6662)	129	HV	Urgent
Main Troubles			
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 restore	330	IR	Non- urgent
GSM Pre-Alarm			Non- urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
IP Network trouble			Non- urgent
IP Network trouble restore			Non- urgent
Arm/Disarm			
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
Detectors(Zones)			
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
Entry/Exit	134	BA	Urgent
Entry/Exit restore	134	BH	Urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
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
Soak fail restore	380	UJ	Urgent
Zone Alarm	134	BA	Urgent
Zone Alarm restore	134	BH	Urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
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
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
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

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
Miscellaneous			
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
Call back	411	RB	Non- urgent
System reset	305	RR	Urgent
Abort Alarm	406	BC	Urgent
Listen in begin	606	LF	Urgent
MS keep alive (polling)	999	ZZ	Urgent
Cancel Report	406	OC	Urgent
Walk Test	607	BC	Non- urgent
Walk Test restore	607		Non- urgent
Exit Error	374		Non- urgent
Enter Quick Learn	627	LB	Urgent
Exit Quick Learn	628	LS	Urgent
Enter Service Mode	393	LB	Non- urgent
Exit Service Mode	393	LX	Non- urgent
Finished Uploading Pictures			Urgent
MS Trigger		ZY	Non- urgent
MS Trouble			Non- urgent
Fail Cloud Communication			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
AL.Reinstate P=y	Alarm reinstatement on partition Y
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 code=xx	Bypass code XX has been used
* 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 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
Cloud Connected " ,	Cloud communication channel is functioning
Cloud Disconnect" , //	Cloud communication channel is not functioning
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 4 and IP card
Comm OK Siren=y	Communication OK between the Agility 4 and Siren Y
Comm. OK GSM	Communication OK between the Agility 4 and GSM

Event Message	Description
Comm.OK I/O Mdl.	Communication OK between the Agility 4 and I/O module
Conf. alarm P=y	Confirmed alarm occurred in partition Y
Conf. Hold-Up P=y	Confirmed Hold-Up Alarm in partition Y
Confirm rs Z=xx	Restore zone confirmed alarm
* Confirm Zone=xx	Confirmed alarm occurred from zone XX
CP reset	The main 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
Device Tmpr Byp	Device Tamper Bypass
* 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 main KP	Fire alarm from
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 and the Agility 4 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

Event Message	Description
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
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
HU.Reinstate P =Y	Hold-Up Reinstatement in partition y
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 4 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
KeyBox Open Z=xx	Zone XX defined as KeyBox type is open
KeyBox Rst Z=xx	Zone XX defined as KeyBox type is closed
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

Event Message	Description
* 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
* 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 4 and IP card
* No comm I/O Mdl.	Communication failure between the Agility 4 and I/O module
* No comm Siren=y	Communication failure between the Agility 4 and siren Y
* No comm. GSM	No communication between GSM/GPRS module and the Agility 4
* 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
* Radio l.bat 5S=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 4 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

Event Message	Description
Tamper I/O Rst.	Tamper alarm restored from I/O module
* 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

* Specifies which events will be written in the event log once the mandatory *Event* control bit is selected (see page *51*).

Appendix C: Library Voice Messages

001	(Customized 1)
002	(Customized 2)
003	(Customized 3)
004	(Customized 4)
005	(Customized 5)

A

006	A
007	Above
008	Air conditioner
009	An
010	And
011	Apartment
012	Area
013	At
014	Attic

B

015	Baby's room
016	Back
017	Balcony
018	Basement
019	Bathroom
020	Bedroom
021	Before
022	Behind
023	Bottom
024	Boy's room
025	By

C

026	Camera
027	Ceiling
028	Cellar
029	Central
030	Children
031	Cleaner
032	CO
033	Computer room
034	Contact
035	Control
036	Corner
037	Curtain

D

038	Desk
039	Detector
040	Device
041	Dining
042	Door
043	Down
044	Downstairs
045	Dressing

E

046	East
047	Elevator
048	Emergency
049	Entrance
050	Entry
051	Executive
052	Exit
053	External

F

054	Family
055	Fence
056	Fire
057	First
058	Flood
059	Floor
060	For
061	Foyer
062	Front

G

063	Game
064	Garage
065	Garden
066	Gas
067	Gate
068	Girl's room
069	Glass
070	Guest

H

071	Hallway
072	High

I

073	In
074	Indoor
075	Inside
076	Internal
077	Is

K

078	Keyfob
079	Kitchen

L

080	Landing
081	Left
082	Library
083	Light
084	Living
085	Lobby
086	Low

M

087	Macro
088	Magnet
089	Main
090	Master
091	Middle
092	Motion

N

093	Near
094	New
095	North
096	Nursery

O

097	Of
098	Office
099	On
100	Outdoor
101	Output
102	Outside

P

103	Panic
104	Partition
105	Passage
106	Patio
107	Perimeter
108	Pool

R

109	Rear
110	Reception
111	Refrigerator
112	Relay
113	Right
114	Roof
115	Room

S

116	Safe
117	Safety
118	Second
119	Sensor
120	Shock
121	Shop
122	Shutter
123	Side
124	Siren
125	Site
126	Smoke
127	South
128	Sprinkler
129	Stairs
130	Store
131	Student room
132	Study

T

133	Technical
134	Temperature
135	Third
136	To
137	Top
138	TV

U

139	Under
140	Up
141	Upstairs

V

142	Video camera

W

143	Wall
144	Warehouse
145	Washroom
146	West
147	Window

Y

148	Yard

Z

149	Zone

Numbers

150	0
151	1
152	2
153	3
154	4
155	5
156	6
157	7
158	8
159	9

Appendix D: Remote Firmware Upgrade

This appendix explains how to perform remote upgrade of your Agility 4 main panel software using the Configuration Software. Remote software upgrade is performed via IP or GPRS.

Prerequisites

- Agility 4 Configuration Software
- Agility 4 control panel version 4.76 and later
- Agility 4 system equipped with a GSM/GPRS or IP module

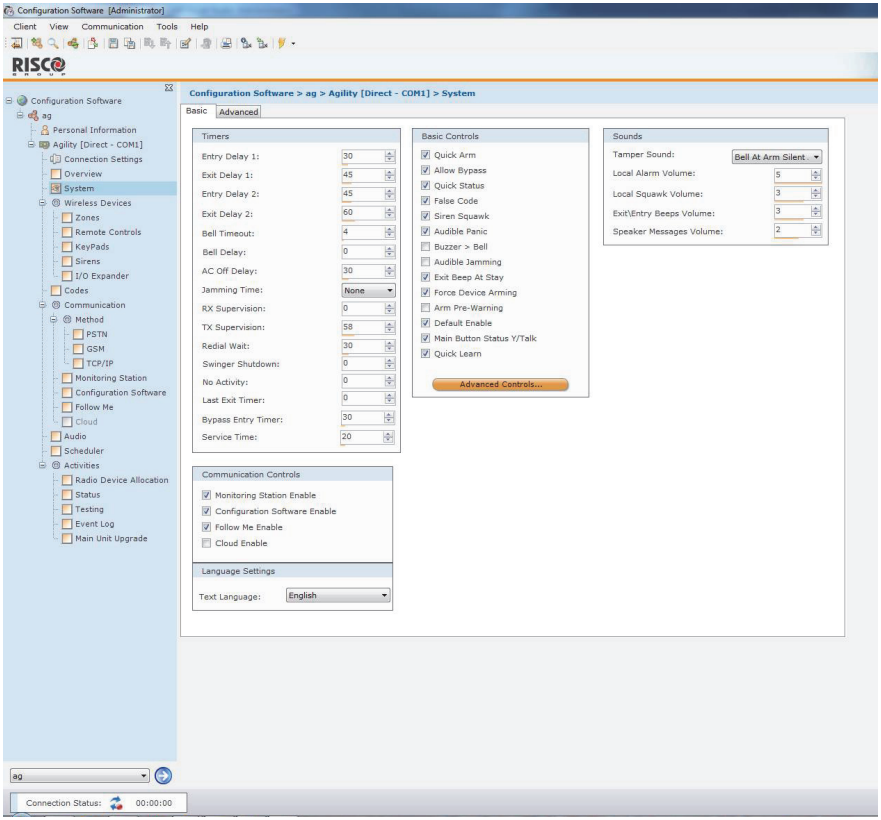
NOTE: Back up panel parameters into the Configuration Software before performing software upgrade. With established connection to the Agility main panel: **Communication > Receive > All**

Step 1: Verify the current version of your Agility 4 main panel

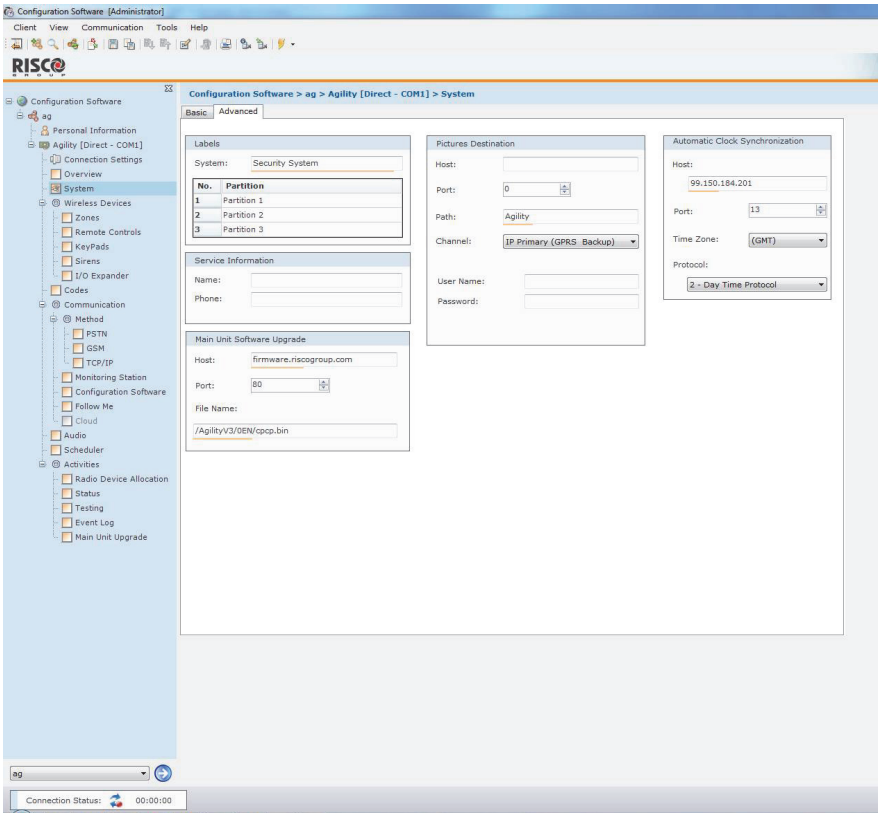
In order to later confirm that the upgrade procedure has been successful (step 4), take note of the current version of your Agility 4 main panel software.

1. Login to the Agility 4 Configuration Software program.
2. Select a client.
3. Click **Connect**  to establish connection to the Agility 4 main panel.
4. Go to the **Activities → Testing** screen.
5. In the *Main Unit* tab, click on the **Test** button. The current version of the main panel appears in the *Panel version* textbox.

Step 2: Enter the location of the upgrade file



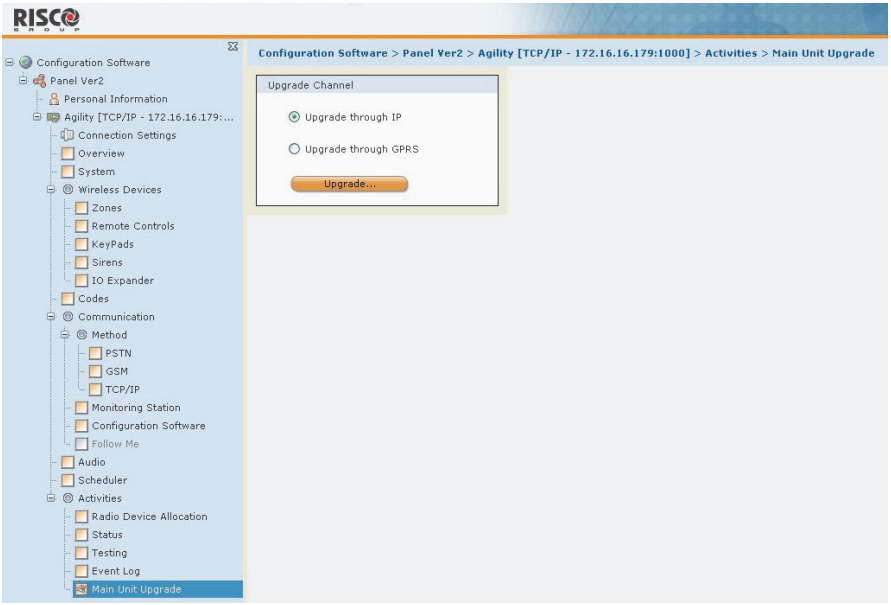
System Screen (Basic Tab)



System Screen (Advanced tab)

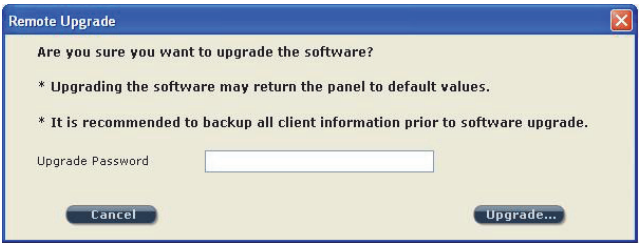
1. In the **System** screen, in the *Main Unit Software Upgrade* section, enter the relevant information regarding the location of the upgrade file:
   - **Host**: Enter the IP address of the router/gateway where the upgrade file is located. Default: **firmware.riscogroup.com**
   - **Port**: Enter the port on the router/gateway where the upgrade file is located. Default: **80**
   - **File Name**: Enter the upgrade file name. For example: /WirelessPanels/OEN/FAT.txt
     Please contact Customer Support services for the file name parameters.
2. Click **Send** .

Step 3: Perform upgrade



NOTE: Make sure you are online and connected to the Agility 4 control panel (if not, click Connect).

1. In the **Activities → Main Unit Upgrade** screen select the Upgrade Channel from two options:
   - **Upgrade through IP**
   - **Upgrade through GPRS**
2. Click on the **Upgrade…** button. The following dialog box appears:



3. The message that appears informs you that remote software upgrade may result in returning the main panel to its default values, therefore it is recommended to backup all client information before performing the upgrade.
4. Enter the Upgrade Security password and click **Upgrade…**.
   Please contact Customer Support services at your local RISCO Group branch for the password.

NOTE: For users with Agility 4 Configuration Software, for some versions the following message will appear: "The upgrade process will commence after disconnecting this session."

5. Click **OK**.
6. Disconnect from the current session (Click **Disconnect** ) to begin the upgrade procedure. The LEDs on the Agility 4 main panel will begin to flash during the upgrade procedure as follows: The Power  LED will light up and the other LEDs will flash rapidly.

NOTE: If upgrade fails, the previous Agility 4 main panel software version is automatically recovered.

Step 4: Restoration of panel-to-system communication

In the event that the firmware upgrade involved a database change, the panel resets all parameters (except those for communication, as per the list below*). In this case, to re-enable Agility 4-to- panel communication, reconnect to the panel from Configuration Software and “Send All” parameters as follows:

Communication > Send > All

Consult RISCO technical support for further details.

* Saved communication parameters list:

a. **System Parameters:**
   i. CS Enable
   ii. FM Enable.
   iii. MS Enable
   iv. Cloud Enable
   v. Disable incoming call
   vi. Random periodic test
   vii. SIA with text
   viii. CS Call back

b. **MS Parameters:**
   i. MS LOCK

c. Configuration Software Parameters:

i. Access code
ii. Remote ID
iii. All the CS enable flags (PSTN, IP, GSM in, out, SCD).
    1. CS via GPRS (out)
    2. CS via GPRS (List)
    3. CS via CSD
    4. CS via IP
    5. CS via Modem

d. Codes:

i. Installer code
ii. Sub installer code
iii. GM Code

e. GSM Parameters:

i. GSM APN code
ii. GSM APN user
iii. GSM APN password
iv. GSM PIN Code

f. IP Module Parameters:

i. IP Dynamic/Static
ii. IP Address
iii. IP Subnet
iv. IP Gateway
v. IP NetBIOS name
vi. IP DNS1
vii. IP DNS2

g. Cloud Parameters:

i. Cloud CHANNEL
ii. Cloud PASSWORDELAS PORT.
iii. Cloud IP

Appendix E: Installer Programming Maps

Installer menu:

Note: Programming menu is on page 154.

1) Programming
2) Testing

- 1) Main Unit
  - 1) Noise Level
  - 2) Siren
  - 3) Speaker
  - 4) Battery
  - 5) Version
  - 6) Serial Number
- 2) Zone
  - 1) Communication Test
  - 2) Battery Test
  - 3) Walk Test
  - 4) Version
- 3) Remote Control
  - 1) Communication Test
  - 2) Battery Test
  - 3) Version
- 4) Keypad
  - 1) Communication Test
  - 2) Battery Test
  - 3) Version
- 5) Siren
  - 1) Communication Test
  - 2) Battery Test
  - 3) Sound Test
  - 4) Noise Level
  - 5) Version
- 6) GSM
  - 1) Signal
  - 2) Version
  - 5) IMSI
  - 3) IMEI
  - 4) IP Address
  - 6) ICCID
- 7) IP Unit
  - 1) IP Address
  - 2) Version
  - 3) MAC Address
- 8) I/O Module
  - 1) Communication Test
  - 2) Battery Test
  - 3) Version

3) Activities

- 1) Main Buzzer
- 2) KP Sleep Time
- 3) Service Mode
- 4) Avoid Report Prog
- 5) Bypass Box Tamp
- 6) Installer Reset
- 7) CS Connect
- 8) Firmware Update
- 9) System Restart

4) Follow Me

- 1) Define
- 2) Test Follow Me

5) Clock

- 1)Time and Date
- 2) Scheduler Enable
- 3) Auto. Clock
  - 1) Server
  - 2) Host
  - 3) Port
  - 4) Time Zone

6) Event Log
7) Macro

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
      - 4) Entry Bypass
      - 5) Service Time
  - **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
      - Bypass Unique Code

		Silent Remote Install
		AntiMask
		Power Management
	3) Communication	
		MS Enable
		Configuration Software Enable
		FM Enable
		Cloud Enable
	4) EN 50131	
		Authorize Installer
		Override Trouble
		Restore Alarm
		Mandatory Events
		Restore Troubles
		Exit Alarm
		Entry Alarm
		20 Minutes Signal
		Attenuation
	5) PD6662 Prog	
		Bypass Exit/Entry
		Entry Disable
		Route Disable
		Installer Confirmation
		Keyswitch 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
  - PD6662
  - CP-01
- 5) Customer

6) Service Info

- 1) Service Name
- 2) Phone

7) Firmware Update

- 1) Server IP
- 2) Server Port
- 3) File Path

8) Picture Server

- 1) Server IP
- 2) Server Port
- 3) File Path
- 4) Username
- 5)Password
- 6) Image Channel

2) Radio Devices

1) Allocation

- 1) RF Allocation
- 2) By Serial code
- 3) Zone Allocation

2) Modification

- 1) Zones
  - 1) Parameters
    - 1) Label
    - 2) Serial No.
    - 3) Partition
    - 4) Type
    - 5) Sound
    - 6) Advanced
      - 1) Chime
      - 2) Control
        - Supervision
        - Forced Arming
        - No Activity
        - LED Enable
        - Abort Alarm
      - 3) Detection Mode
      - 4) Sensitivity
      - 5) Camera Parms
        - Images at Alarm
        - Image Interval
        - Image Pre-Alarm
        - Image Resolution
        - Image Quality
        - Colored Image
      - 6) PIR Camera Triggers
      - 6) X73/X78 Contact

- Magnet
- Alarm Hold On
- Input Termination
- Input Response Time
- Shutter Pulse

7) Two-way Detector
- Operation Mode

2) Alarm Confirmation
- 1) Confirm Partition
- 2) Confirm Zones

3) Soak Test

4) Cross Zones

2) Keyfobs

1) Parameters

1-Way Keyfob	***2-Way Keyfob***
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 (LCD/Panda Only)
- 5) UO Control
- 6) Mode (Slim only)
- 7) Door Bell Sound (Slim only)
- 8) Supervision
- 9) Auto Status

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) Activation / Deactivation
- 5) Pulse Length

4) Parameters

- 1) Serial No.
- 2) Control
  - 1) Supervision
  - 2) Quick UO/X10
- 3) X10 House ID
- 4) UO DTMF Control

3) Identification
4) Delete

3) Codes

1) User

1) Label
2) Partition
3) Authority

User
Cleaner
Arm Only
Duress
Door Bypass

2) Grand Master
3) Installer
4) Sub-Installer
5) Code Length

4 Digits
6 Digits

- **6) DTMF Code**
- **7) Parent Control**
- 4) Communication
  - **1) Method**
    - 1) PSTN
      - 1) Timers
        - 1) PSTN Lost Delay
        - 2) Wait for Dial Tone
      - 2) Controls
        - Alarm Line Cut
        - Answer Machine Override
        - CS via PSTN
      - 3) Parameters
        - 1) Rings to Answer
        - 2) Area Code
        - 3) PBX Prefix
    - 2) GSM
      - 1) Timers
        - 1) GSM Lost
        - 2) SIM Expire
        - 3) MS Keep Alive (Polling)
      - 2) GPRS
        - 1) APN Code
        - 2) APN User Name
        - 3) APN Password
      - 3) Email
        - 1) Mail Host
        - 2) SMTP Port
        - 3) E-mail Address
        - 4) SMTP User Name
        - 5) SMTP Password
      - 4) Controls
        - Caller ID
        - Disable GSM
        - CS via GPRS (out)
        - CS via GPRS (Listener mode)
        - CS via CSD
      - 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	
		SIA IP	
	2) Accounts		
	3) Comm Format		
		Contact ID	
		SIA	
	4) Controls		
		Handshake	
		Kissoff	
		SIA Text	
		SIA IP +SN	
		SIA with Partition	
		Random MS Test	
	5) Parameters		
		1) MS Retries	
		2) Alarm Restore	
		3) Encryption Key	
		4) Receive Number	
		5) Line Number	
	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
  - Call Back Enabled
  - Call Back Phones
- 3) CS / IP Gateway

4) Follow-Me

- 1) Define
  - 1) Report type
    - Voice
    - SMS
    - Email
  - 2) Events
  - 3) Restore events
  - 4) Remote control
    - Remote listen
    - Remote program
  - 5) Partition
- 2) Controls
  - Disarm stop FM
- 3) Parameters
  - 1) FM Retries
  - 2) Voice Mesg Rec
  - 3) Periodic test

5) Cloud

- 1) IP Address
- 2) IP Port
- 3) Password
- 4) Channel
  - IP Only
  - GPRS Only
  - IP/GPRS
  - GPRS/IP
- 5) Controls
  - MS Call All
  - FM Call All
  - App Arm
  - App Disarm
  - App Exit Delay

5) Audio

1) Assign Message

- 1) Zone
- 2) Partition
- 3) Output
- 4) X10 output
- 5) Macro

2) Local Message

- Intruder Alarm
- Fire Alarm

Emergency
Panic Alarm
Tamper Alarm
Environment Alarm
Away Arm
Stay Arm
Disarm
Audible Status
Entry / Exit
Auto Arm
Output On/Off
Walk Test
No Movement
Miscellaneous

0) Exit

Appendix F: EN 50131 and EN 50136 Compliance

Compliance Statement

Hereby, RISCO Group declares that the Agility 4 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: PD 6662:2017
- USA: FCC: Part 15B, Part 15C, FCC Part 68

EN50136 Compliance

- EN50136-1 EN50136-2 and EN50131-10: PSTN (SP2); GSM 2G/3G (SP4); IP (SP4); GSM primary and IP secondary (DP3); IP primary and GSM secondary (DP3)
- PSTN module can be connected to monitoring station via any EN50136 compliant receiver, which shall meet all requirements of securing messages.
- When IP and/or GSM modules are in use, IP Receiver software is also in use. The IP Receiver should be connected to automation software, which serves as the EN50136 annunciator. If connection between the IP Receiver and the automation software is lost, an error message will appear on the IP Receiver queue.
- In order to have an indication of ACK received from the monitoring station transceiver, the parameter Kiss-Off Y/N should be set to Y

Possible logical code 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 4th digit has been punched, "Enter" is automatically applied. Code is rejected when trying to create a non existing code.

Possible physical key 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 4, 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 4 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 4 software:

Report Codes Feature	EN 50131 Compliance
Timers	
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
System Controls	
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 Feature	EN 50131 Compliance
20 Minutes Signal	Set to YES
Entry Alarm	Set to NO
Attenuation	Set to YES

Appendix G: SIA CP-01 Compliance

Compliance Statement

Hereby, RISCO Group declares that the Agility 4 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 Main panel (Agility Main)
- All system keypads must be audible (mute disabled).

Setting the Agility 4 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 4 software:

Report Codes

Feature	CP 01 Compliance
Timers	
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
System Controls	
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

Feature	Range	Shipping default	Quick Key / Remark
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	Annunciate 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]
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

Appendix H: Agility 4 Accessories

868MHz part numbers	433MHz part numbers	Description
Keypads		
RW132KPPW30B	RW132KPPW30I	2-Way LCD keypad
RW332KPP800A	RW332KPP400A	WL Panda KP+Prox,868
RW332KP0800A	RW332KP0400A	WL Panda KP,868
RW132KL2P00A	RW132KL2P00H	2-Way white internal Slim keypad + Proximity
RP200KT0000A	RP200KT0000A	RISCO 10 Proximity tags, black, 13.56 MHz
Keyfobs		
RW132KF1800A		4 button, black, remote control
RP128T4RC00B	RP296T4RC00B	4 button, gray, remote control
RWX132KF800A		2-Way WL remote control
RWT51P80000A	RWT51P40000A	Wristband panic transmitter
RWT52P86800A	RWT52P43300A	2-button panic keyfob
RWT54086800A		4-button zone keyfob
RWT50P86800B		Wireless pendant transmitter
RWX332KF800A	RWX332KF400A	Panda 2Way KeyFob
Wireless Sirens		
RWS42086800B	RWS42043300B	Wireless Indoor round sounder
RWS33200800A	RWS33200400A	WL 2W Internal Sounder
RWS52A86800B	None	Wireless oval external sounder, amber
RWS50x86800B	RWS50x43300B	Wireless triangle external sounder (x: A=amber, R=red, B=blue)
RWS20A86800B	None	Wireless ProSound external sounder
RWS401x8000B	RWS401B4000B	Wireless Lumin8 external sounder 868 (x: A=amber, R=red, B=blue) 433 (blue)
Communication		
RW132MD2400A		Agility PSTN module
RW132G30000A		GSM/3G MSoc + Ant. Plastic box
RW132G20000A		GSM/2G Agility Plug-in Module
RW132IP0000A		Plug-in TCP/IP module
RP51200W000A		Wi-Fi Plug-in + metal box ant.
RP512IP0000A		IP Multi-Socket Plug-in Module
RCGSMANT100A		Agility GSM antenna, 3m
Safety		
RWT6FW86800B	RWT6FW43300B	Wireless flood detector
RWX34S86800B	RWX34S43300B	Wireless smoke detector and heat
RWX35S00800C	RWX35S00400C	WL Smoke & Heat
Perimeter		
	RWX312PR400C	2-Way wireless WatchOUT PIR
RWT312PR800C	RWT312PR400C	Wireless WatchOUT PIR
RWT6G086800C	RWT6G043300C	Wireless Glassbreak detector
RWT6SW86800D		Wireless Shock detector
RWT62W86800B	RWT62W43300B	Wireless Shock + Contact
RWX10680000A	RWX10640000A	1 & 2-Way WL Curtain PIR
PIR Cameras		

868MHz part numbers	433MHz part numbers	Description
RWX95CM8000C	RWX95CM4000C	2-Way wireless eyeWAVE PIR Cam
RWX95CMP800C	RWX95CMP400C	2-Way Wireless eyeWAVE Pet Cam
RWX350DC800A	RWX350DC400A	WL Beyond DT Cam
PIR Detectors		
RWX95086800C	RWX95043300B	2-Way Wireless iWAVE PIR
RWX95P86800C	RWX95P43300B	2-Way Wireless iWAVE Pet
RWT92086800E	RWT92043300E	iWISE Wireless PIR detector
RWT92P86800E		iWISE WL PIR PET detector
RWX96086800A	RWX96043300A	1&2 Way WL Piccolo PIR
RWX96P86800A	RWX96P43300A	1&2 Way WL Piccolo Pet
RWX515PR080A	RWX515PR040A	2 Way WL BWare PIR
RWX515PT080A		2 Way WL BWare Pet
Shock&Magnetic Contact Detectors		
RWT7808680MA	None	1-Way Slim Contact
RWT72M86800E	RWT72M43300E	Wireless Door/Window Contact
	RWT72C43300E	Wireless Universal transmitter
RWT72P86800E	None	Wireless Pulse Count transmitter
RWT72X86800E	None	Wireless Dual Channel transmitter
RWT72I86800E	None	Wireless door/window contact
RWX73M86800B		2-Way door/window contacts
RWX73F86800A	RWX73F43300A	2-Way multi-function contacts
RWX73F8BL00A		2-Way Multi Contact, Black
RWX73F8BR00A		2-Way Multi Contact, Brown
RWX7808680MA	RWX7804330MA	2-way Slim Contact
RWX780868SMA	RWX780433SMA	2-way Slim Shock&Contact
RWX780868S0A		2-way Slim Shock Detector
RWX75M86800A		2-Way WP Door/Window Contacts
DT Detectors		
RWX350D0800A	RWX350D0400A	WL Beyond DT
RWX95DT0800B		2 Way WL iWave DT,
RWX95DTP800B		2 Way WL iWave DT Pet
RWX515DT080A		2 Way WL BWare DT
RWX515DTP80A		2 Way WL BWare DT Pet
RWX107DT800A	RWX107DT400A	WL Outdoor DT Curtain
Input / Output Expander		
RW132I04000B		Wireless Input/Output Expander

Miscellaneous – part numbers	Description
RVCM11W0000B	VUpoint 1.3MP WiFi Cube Camera
RVCM52W0100B	VUpoint 1.3MP WiFi Bullet Camera
RVCM32W0200A	VUpoint 1.3MP WiFi Dome Camera
RVCM11P0900A	Cube 1.3MP PoE SD Slot
RVCM32P1000A	Dome 2MP PoE SD Slot
RVCM52P1100A	Bullet 2MP PoE SD Slot
RVCM52P1300A	Bullet Varifocal 2MP PoE SD Slot
RVCM72P1200B	Eyeball 2MP PoE SD Card
RVCM61H0300A	IP Cam: PT, 1.3MP, WiFi, SD Slot
RVCM52E0400A	IP Cam: Bullet 4MP 2.7-12mm WDR
RVCM32E0500A	IP Cam: Dome, 4MP, 2.7-12mm, WDR
RVCM72E0700A	IP Cam: Eyeball 4MP WDR H.265
RVCM82E0800A	IP Cam: IR PTZ, 2MP, Starlight, H.265
RW132CB0000A	RS232 PC-to-panel cable
RW132EUSB00A	Agility-to-USB adaptor
RAX73MS0000A	X73 Magnet spacers x 10, white
RAX73MSB000A	X73 Magnet spacers x 10, brown
RAX73MSBL00A	X73 Magnet spacers x 10, black
RAX73XS0000A	X73 Transmitter spacers x 10, white
RAX73XSB000A	X73 Transmitter spacers x 10, brown
RAX73XSBL00A	X73 Transmitter spacers x 10, black
RA78UNI0000A	X78 External/Shutter TB Bracket
RA350SSLR00A	WL Beyond 180° Solar Swivel Kit

RED Compliance Statement

Hereby, RISCO Group declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU . For the CE Declaration of Conformity please refer to our website: **www.riscogroup.com.**

FCC Note

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:

a) Reorient or relocate the receiving antenna.

b) Increase the separation between the equipment and receiver.

c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

d) Consult the dealer or an experienced radio/TV technician.

FCC Warning

This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications to this equipment which are not expressly approved by the party responsible for compliance (RISCO Group's) could void the user's authority to operate the equipment.

FCC ID: JE4STAMP433, JE4STAMP433-916 Valid for P/N RW132x4t0zza

Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates ("**RISCO**") guarantee RISCO's hardware products to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by RISCO, for a period of (i) 24 months from the date of connection to the RISCO Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the "**Product Warranty Period**" respectively).

Contact with customers only. This Product Warranty is solely for the benefit of the customer who purchased the product directly from RISCO, or from any authorized distributor of RISCO. Nothing in this Warranty obligates RISCO to accept product returns directly from end users that purchased the products for their own use from RISCO's customer or from any installer of RISCO, or otherwise provide warranty or other services to any such end user. RISCO customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. RISCO's customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that RISCO has any warranty or service obligation to, or any contractual privy with, any recipient of a product.

Return Material Authorization. In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, RISCO shall, at its option, and at customer's expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization ("**RMA**") number from RISCO prior to returning any Product to RISCO. The returned product must be accompanied with a detailed description of the defect discovered ("**Defect Description**") and must otherwise follow RISCO's then-current RMA procedure in connection with any such return. If RISCO determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty ("**Non-Defective Products**"), RISCO will notify the customer of such determination and will return the applicable Product to customer at customer's expense. In addition, RISCO may propose and assess customer a charge for testing and examination of Non-Defective Products.

Entire Liability. The repair or replacement of products in accordance with this warranty shall be RISCO's entire liability and customer's sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. RISCO's obligation and the Warranty are contingent upon the full payment by customer for such Product and upon a proven weekly testing and examination of the product functionality.

Limitations. The Product Warranty is the only warranty made by RISCO with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, the Product Warranty does not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the product and a proven weekly testing and examination of the product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow RISCO's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without RISCO's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond RISCO's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any delay or other failure in performance of the product

attributable to any means of communications, provided by any third party service provider (including, but not limited to) GSM interruptions, lack of or internet outage and/or telephony failure.

BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY.

RISCO makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:

DISCLAIMER. EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND LOSS OF DATA. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT BY CUSTOMER OR END USER SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT

IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

RISCO does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.

RISCO does not guarantee 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.

Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof. Consequently RISCO shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.

No employee or representative of RISCO is authorized to change this warranty in any way or grant any other warranty.

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website **www.riscogroup.com** or via the following:

Belgium (Benelux)
Tel: +32-2522-7622
support-be@riscogroup.com

China (Shanghai)
Tel: +86-21-52-39-0066
support-cn@riscogroup.com

France
Tel: +33-164-73-28-50
support-fr@riscogroup.com

Israel
Tel: +972-3-963-7777
support@riscogroup.com

Italy
Tel: +39-02-66590054
support-it@riscogroup.com

Spain
Tel: +34-91-490-2133
support-es@riscogroup.com

United Kingdom
Tel: +44-(0)-161-655-5500
support-uk@riscogroup.com

USA
Tel: +1-631-719-4400
support-usa@riscogroup.com

This RISCO product was purchased at:

FCC

CE

5IN2861