Agility 4

Quick Installation Guide

Table of Contents

1. Introduction

This quick installation guide describes the main steps for installing the main panel and programming the Agility 4 using the 2-way wireless LCD or Panda keypad. The Agility 4 includes multi-socket communication modules (IPC2, GSM 2G or GSM 3G) that provide multiple, simultaneous communication channels for direct communication, and for communication via the Cloud.

For installation procedures of system devices (detectors and accessories), refer to the Full Installer Manual or the respective device's instructions.

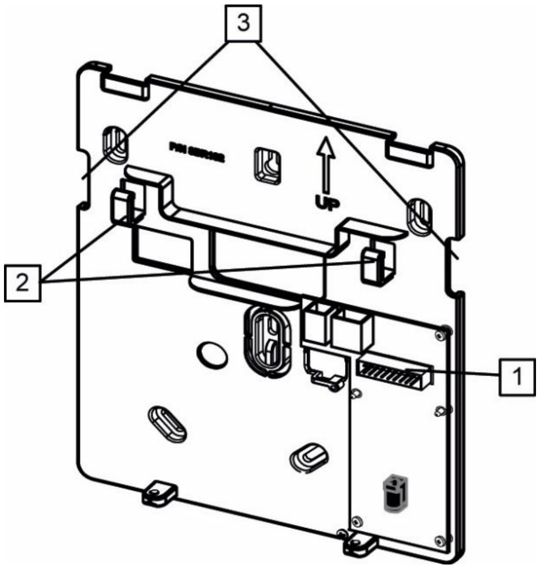
2. Installing the Main Panel

For optimal operation, the mounting location of the main panel should be:

- Centrally located among the wireless transmitting components
- In a location with good GSM reception
- Not visible from outside the protected premises, and not reachable by those for whom use is unintended (such as small children)
- Near an uninterrupted 230V AC electrical outlet, phone outlet, network cable outlet as needed
- In a place where the alarm can be heard during Home/Stay (Partial) Arming mode
- Away from sources of direct heat, electrical disturbance and large metal objects, which may hinder reception

➢ **To install the main panel:**

1. Disconnect the mounting bracket (back cover) from the main panel by releasing the two locking screws, and then carefully disconnecting the flat ribbon cable from the printed circuit board attached to the back bracket **[1]** while carefully leaving it connected to the main panel housing.



Mounting bracket (back cover)

2. Using the mounting bracket as a template, mark and then drill the mounting holes (plus another hole for the tamper switch), and install the anchors to the wall. Then secure the mounting bracket to the wall with the provided screws.
3. Connect the AC power cable only to the power supply terminals located on the backside of the mounting bracket. Then route the AC power cable via the dedicated hook **[2]** and opening **[3]** on the bracket. Ensure compliance with proper grounding requirements, according to applicable code and regulation (see Full Installation Manual), but **DO NOT yet connect the main panel to the electrical power supply (wall outlet or circuit breaker).**
4. Remove screw and open the battery compartment cover. **Observing the correct polarity**, connect the respective leads to the backup battery.

NOTE: The backup battery takes 24-hours to charge.

5. Adjust the tamper switch per customer requirements – for triggering a tamper alarm upon main panel (box) tampering, or both wall and box tampering.
6. On the respective terminal blocks, as required, connect all wiring such as phone and network (IP) cables.
7. Insert a SIM card into the SIM card holder as required.
8. Re-connect the flat ribbon cable, and re-connect the main panel to the bracket, fastening them with the 2 locking screws.
9. Now power-up the main panel by connecting the main panel to the electrical power supply (wall outlet or circuit breaker); "***Security system is on***" will be announced.

3. LCD Keypad Allocation and Language Selection

Newly installed systems require that the 2-way wireless LCD keypad be the first device to be allocated (enrolled) to the system, from which a default language is then defined.

➢ **To allocate the LCD keypad and define the system language:**

1. After powering-up, press the button on the main panel for 5 seconds; the unit beeps once as it enters “Learn” mode, and the LEDs light up, one-after-the-other.
2. Before performing other device allocations, first, allocate the LCD keypad to the system by pressing both 🔒🏠/ 🔒🏠 simultaneously for at least 2 seconds.
3. In the displayed language menu, select the system language (and customer default) settings and then press #?/ OK.

NOTE: If the keypad goes into “sleep mode” before finishing language selection, restore the system language selection on the keypad by simultaneously pressing * and **9**.

4. Wireless Device Allocation

All wireless devices (detectors and accessories) must also be allocated ("enrolled") to the system. This can be performed at:

- **Main panel:** Perform Quick Allocation of all devices by sending a RF signal transmission from each device to the main panel (see procedure below).
- **LCD keypad:** The following methods are available:

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

  For manually selecting a specific zone number to which a device is then allocated: You can perform this by the "Zone Allocation" method. Refer to the Full Installation Manual.
- **Configuration Software:** Refer to the Configuration Software documentation for details.

NOTE: For deletion of device allocations (for devices no longer used in the system), refer to the Full Installation Manual.

Quick Device Allocation at the Main Panel

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

NOTE: For quick allocation at the main panel, the system bit **Quick Learn** must be enabled.

➢ **To quickly allocate all wireless devices at the main panel:**

1. If the main panel is not already in Learn mode, press the button on the main panel for 5 seconds; the unit beeps once as it enters Learn mode (all the LEDs also light up, one after the other).
2. Make sure batteries are installed in each device before allocating them. For detectors, also make sure the covers are removed so the internal tamper switches are accessible.
3. Send a signal transmission from each device per instructions in the *Table of Devices* Transmissions, on page *6*. If a device is not listed in the table, refer to the device's specific instructions; the main panel beeps once to accept or beeps three times to reject. Once accepted, the system announces the device type and its zone (for example, "Detector, zone 1").

NOTE: For future use, it is recommended to write down for the customer the device description, zone number, and installation location of each allocated device.

Table of Device Transmissions

Wireless Device	Transmission procedure
2-Way LCD Keypad	Press 🔒 and 🏠 simultaneously for at least 2 seconds
2-Way Panda Keypad	Press 🔒 and 🏠 simultaneously for at least 2 seconds.
PIR Detectors: • **PIR** • **PIR camera** • **PIR-pet** • **PIR-pet camera** **NOTE:** See *PIR Setup*, page *16.*	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 Contacts 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
2-Way Panda Keyfob	Press 🔒 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.

5. Programming Agility 4 with the LCD/Panda Keypad

This section describes system programming from the 2-way wireless LCD keypad. You can also program the Agility 4 system via the Configuration Software or PTM module. Refer to the CS documentation and the Full Installation Manual, respectively, for details.

LCD keypad:

Button	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 between multiple options
🔒	To toggle between options (such as Y / N)
0	To exit the programming mode (followed by #? to confirm)

Panda keypad:

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

6. Accessing Installer Menu

- From an **allocated** LCD keypad, press * / ⚙↩, and then enter the installer code (default is **0132**).

7. Setting the System Clock

The system clock is set automatically after the main panel is configured with IP or GPRS communication.

➢ **To manually set the system clock:**

1. From the Installer menu, scroll to **5) Clock,** and then press #? / OK .
2. At the Time & Date option, press #? / OK , and then enter the time and date.

8. Measuring and Defining the Noise Level Threshold

You can measure (“calibrate”) the background noise that the main panel detects, and also define (“view/edit”) the acceptable threshold value, according to customer requirements.

Background noise (RF interference) is typically generated by other non-system devices operating in close proximity to the system, and a large amount of background noise may interfere with the system, causing “jamming.” Communication between your system’s wireless devices and the main panel must be stronger than any detected background noise at the panel, therefore perform a Communication test (see below) for each wireless device to check its signal strength.

Measuring the background 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 your system will tolerate before it generates jamming events. The lower you define the threshold value, the more “sensitive” the system will be (it will report jamming events more frequently), and the higher you define the threshold value, the “more tolerant” the system will be (it will report jamming events less frequently).

➢ **To measure the background noise detected by the system:**

1. From the Installer menu, go to: **2)Testing** > **1)Main unit** > **1)Noise Level** > **2)Calibrate >** #? **/** OK ; the detected level of background noise displays.

   NOTE: A lower resulting value means less background noise is detected by the system.

2. After measuring, if the resulting value is far from your defined noise level threshold value or if it is too high (See *Comm Test* below for an explanation) and you believe the source of background noise may inherent to the panel’s location , move the panel to a better location.

➢ **To define the system’s acceptable noise level threshold value:**

1. From the Installer menu, go to: **2)Testing > 1)Main unit > 1)Noise Level > 1)View/Edit >** #? **/** OK **.**
2. Enter the noise level threshold value you want between **00 –99,** and then press #? / OK .
   NOTE: 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).
3. See the following *Comm Test* procedure for an explanation of acceptable results..

Performing a Communication Test

The Comm. test displays results of the signal strength measured after the last device transmission (last detection or last supervision signal). Make sure to activate the detector prior to the test.

➢ **To perform a Communication Test:**

1. From the Installer menu, go to: **2)Testing > 2)Zone** [or instead] **3)Keyfob, 4)Keypad, or 5)Siren] > 1)Communication Test >** #? / OK **.**
2. Scroll with ◄ ► / ⇧ⓘ ⇩ to a zone to perform the test, a number (percentage) appears representing the signal strength the panel received from the device and which must be as follows:

RSSI>=CALIBRATION+8	√
RSSI<CALIBRATION⊥8	X

9. Programming and Testing Zones (Detectors)

The parameters available per zone (detector) may vary, according to the zone type. After programming the parameters, you can perform a Communications (Comm) test.

➢ **To program detector/zone parameters:**

1. From the Installer menu select: **1)Programming > 2)Radio Device > 2)Modification > 1)Zones > 1)Parameters**, and then press #? / OK .
2. Use ◄ ► / ▲ ▼ to select the required zone, and then press #? / OK .
3. Set the basic parameters for each zone as follows:

   1) Label: Provide a descriptive name. Use 🔒 🔒 / 🔒 🏠 to toggle between all the possible characters for each key, as shown in the chart:

Key	Respective characters available
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

   2) Partition: Use keys 1, 2, or 3 to set the partition assignment (default is 1).

   3) Type: Use ◄ ► / ▲ ▼ to select the desired zone type from the list, then press #? / OK .

   4) Sound: Use ◄ ► / ▲ ▼ to select the desired sound.

   5) Advanced: Depending on the detector type, includes chime, supervision, forced arm enabled, and additional parameters for 2-way detectors.

4. Perform a Comm. Test (see *Performing a Communication Test*, page *8*).

10. Programming and Testing Keyfobs

Each keyfob can be set up to perform different system operations and control different utility outputs. Up to eight keyfobs can be enrolled in the system. The programming options under the parameters menu vary according to the type of the remote control (1-way or 2-way). After programming the parameters, you can perform a Communication (Comm) test.

➢ **To program keyfob parameters at the LCD keypad:**

1. From the installer menu select: **1)Programming > 2)Radio Device > 2)Modification > 2)Keyfobs > 1)Parameters.**
2. Select a keyfob and then press #? / OK to set its basic parameters.
3. Use the ↲↱ / ⇧ⓘ ⇩ keys to scroll between the options below followed by #? / OK to select:

1-Way Keyfob (4-Button) Parameters

1) Label: Provide a meaningful name (see keypad's label table above for details).

2) Serial Number: Enter the device’s 11-digit unique code.

3) Partition: Assignment (in most cases this is left as 1).

4) Button 1: (the lock button): Full Arm.

5) Button 2: (the Unlock button): Disarm.

6) Button 3: (installer-defined).

7) Button 4: (installer-defined).

2-Way Panda Keyfob (4-Button) Parameters

1) Label: Provide a meaningful name (see keypad's label table above for details).

2) Serial Number: Enter the device’s 11-digit unique code.

3) Partition: Assignment (to all partitions).

4) Button 1: (the lock button): Full Arm.

5) Button 2: (the Unlock button): Disarm.

6) Button 3: (the House button): Partial Arm

7) Button 4: (the Star button): Get status

2-Way Keyfob (8-Button) Parameters

1) Label: Provide a meaningful name (see keypad's label table above for details).

2) Serial Number: Enter the device’s 11-digit unique code.

3) Partition: Use 🔒/🏠 to toggle between **Y/N** for the 3 partition possibilities (use ↲↱ / ⇧ⓘ ⇩ to scroll between partitions 1–3).

4) PIN code: If required, set a 4-digit PIN.

5) Panic Enable: Use 🔒/🏠 to toggle between **Y/N to** define whether or not sending a panic alarm from the remote control is permitted (disabled by default).

6), 7), 8): Installer-assigned buttons 1 through 3 (for respective utility outputs).

4. Press * / ⚙↩ to go back to the **Keyfobs** menu, and then select **2) Control**.
5. Use 🔒/🏠 to toggle between **Y/N** (and use ↲↱ / ⇧ⓘ ⇩ to scroll between the 3 options) as follows:

1) Instant Arm: Have Away (Full) arming without Exit Delay.

2) Instant Stay (Arm): Have Stay / Home (partial) arming without Exit Delay.

3) Disarm + Code: Relevant only if user code is defined using only digits 1–4 (corresponding to the numbered keyfob buttons 1–4).

6. Perform a Comm. Test (see *Performing a Communication Test*, page *8*).

11. Programming Keypads

Up to three keypads (LCD or Panda) can be allocated to the system. After programming the parameters for a keypad, you can then perform a Communication (Comm) test.

➢ **To program keypad (LCD or Panda) parameters:**

1. From the installer menu select: **1)Programming > 2)Radio Devices > 2)Modification > 3)Keypads > 1)Parameters.**
2. Select a keypad, press #? / OK and set its basic parameters. Use ◄►/▲ⓘ ▼ to scroll and #? / OK to select:

   1) Label: Provide a meaningful name (see keypad's label table above for details).

   2) Serial Number: Enter the device's 11-digit unique code.

   3) Emergency key: Defines whether the emergency keys will be activated (**Y**) or not (**N**).

   4) Function key: Define the operation of the ☎☎/✪✪ keys as either **Panic Alarm, MS Listen/Talk,** or **Disabled.**

   8) Supervision: Use 🔒/🏠 to toggle between **Y/N.**
3. Press * /⚙↩ to go back up to the **Keypads** menu, then select **2)Control** and scroll to:
   - **RF Wakeup**: Use 🔒/🏠 to toggle between **Y/N** to define whether the keypad LCD will light up automatically during the Entry Delay time.
4. Perform a Comm. Test (see *Performing a Communication Test*, page *8*).

12. Programming and Testing Sirens

Up to 3 internal or external sirens can be enrolled in the system. After programming the parameters, you can perform a Communication (Comm) test.

➢ **To program siren parameters:**

1. From the installer menu select **1)Programming** > **2)Radio Device** > **2)Modification** > **4)Sirens**
2. Select a siren, then press #? / OK and set its basic parameters. Use ◄►/▲ⓘ ▼ to scroll and #? / OK to select:

   1) Label: Provide a meaningful name.

   2) Supervision: Define if the siren is supervised.

   3) Volume: Set volume produced from the siren during alarm, squawk or exit/entry time.

   4) Strobe: Set the strobe operation of the external wireless siren.
3. Perform a Comm. Test (see *Performing a Communication Test*, page *8*).

13. Defining Communication Channels

The menus displayed reflect only the installed communication modules.

➢ **To define communication channels:**

1. From the installer menu select **1)Programming > 4)Communication > 1)Method.**
2. Select each method **(PSTN, IP and/or GSM)** and define its parameters as follows:

Connecting with GPRS

a) From the **Programming** menu select: **4)Communication > 1)Method > 2)GSM >** use ↲ ↱ / ⇖ ⓘ ⇘ to scroll to **2)GPRS >** #? / OK.

b) Use ↲ ↱ / ⇖ ⓘ ⇘ to scroll between **1)APN Code**, **2)APN User Name,** and **3) APN Password,** and then define the **APN code** and **user name & password** respectively. This information must correspond with that supplied by the SIM card service provider.

Connecting with IP

a) From Programming menu select: **4)Communication > 1)Method > 3)IP > 1)IP Config**

b) 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.

Connecting with Wi-Fi

a) From Programming menu select: **4)Communication > 1)Method > 3)IP > 1)IP Config > 8)Scan WiFi Net**

b) From the available networks list, scroll to your Router's Wi-Fi network, select the desired network and then press [enter].

14. Defining Monitoring Station Communication

You can define up to three monitoring station accounts and several associated parameters that define the nature of communication, event reporting and confirmation between the owner and the monitoring station.

➢ **To define monitoring station communication:**

1. Use * / ⚙↩ to go back up to **1)System** > **2)Controls** > **3)Communication > MSEnable >** use 🔒 / 🏠 to toggle between **Y / N** (select **Y** to enable) **>** #? / OK.

2. Use * / ⚙↩ to go back up to **1)Programming** > **4)Communication** > **2)MS** > scroll to select and define the options for the selected monitoring station **(1—3).**

15. Defining Follow-Me Destinations

Now that you have set up the methods for Agility 4 to communicate with the monitoring station and the customer, you can define the destinations to which Follow Me reports (event notifications) will be sent.

➢ **To define FM destinations:**

- Use (*)/⚙↩ to go back up to **4)Communication** > **4)Follow Me** > **1)Define FM >** FM destination index number (for example, **Follow Me 01) >** (#?)/ OK > then select and configure the following:

1) Report Type: Select channel: **SMS, Email, or Voice.** Reporting events by voice or email can be established through different communication channels, depending on the modules installed in the system.

2) Events: Select the event notifications that will be sent. Use 🔒/🏠 to toggle between **Y/N** for each option, and then press (#?)/ OK to confirm:

- **Alarms >** Intruder Alarm, Fire Alarm, Emergency Alarm, Panic Alarm, Tamper Alarm, Duress Alarm, No Movement
- **Arm/Disarm >** Arm, Disarm, Parent Control
- **Troubles >** False Code, Main Low Battery, WL Low Battery, Jamming, WL Lost, AC Off, PSTN Trouble, IP Network
- **GSM >** GSM Trouble, SIM Trouble, SIM Expire, SIM Credit
- **Environmental >** Gas Alert, Flood Alert, CO Alert, High Temp, Low Temp, Technical
- **Miscellaneous >** Zone Bypass, Periodic Test, Remote Prog., Comm Info

3) Restore Events: Select the "restored" events that will be sent (for same event types listed above – Alarms, Troubles, GSM, and Environmental).

4) Remote Ctrl: Define the following remote user operations (as either **Y** or **N**) which are performed via phone or SMS:

- **Remote Listen**
- **Remote Program**

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

NOTE: Additional Follow-Me e-mail notifications can be assigned in the RISCO Cloud

16. Setting System Parameters (Controls)

There are several system-wide parameters that define how the Agility 4 system works. They are collected under the System menu. All these parameters are set with default values that apply for most installations. If you wish to make a change, go through the menus to program any other system parameter.

17. Customizing the Voice Menu

Users can use the Voice menu to hear local messages on system status, troubles, and events, and to control the system through remote phone operation. You can utilize the system-provided messages, or customize your own.

➢ **To customize the Voice Menu:**

- Use ⊛/⚙↩ to go back up to the **1)Programming menu > 5)Audio >** then scroll to:

  1) Assign Messages: For zones and partitions create customized messages that will be used in place of the default messages. Refer to the Full Installation Manual for details.

  2) Local Messages: For the different alarm types, select **Y** (yes) or **N** (no) to define which messages will be announced locally (on main panel or external audio unit).

18. Defining System Users (User Codes)

The installer may initially set up system's users, however, the primary user / system responsible (Grand Master) should subsequently re-define all user codes for personalization and confidentiality.

User codes can be defined from the Web user application as well as from the LCD keypad.

➢ **To define system users from the LCD keypad:**

- Use ⊛/⚙↩ to go back up to the **1)Programming menu** > **3)Codes,** then scroll to the following options:

  1) User: For each user select a different **2-digit index number**, and then define the following:

  - **Label**: Enter a unique description to identify the user
  - **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**: Select an authority level (User, Cleaner, Arm Only, Duress, Door Bypass)

  2) Grand Master: Define the Grand Master code (default is 4 digits)

  3) Installer: Define the default installer code (default is 4 digits)

19. Connecting to the 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 #?/OK to confirm.

Step 2: Defining GPRS or IP/Wi-Fi Communication

- See *Defining Communication Channels,* page *12.*

Step 3: Defining Cloud Parameters for IP/Wi-Fi 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 (**riscoCloud.com** or 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 CP Password defined in the server under the Control Panel page definition.

4)Channel: Select the communication path for the Cloud (based on IP/Wi-Fi or GPRS communication) as appears in the available options.

NOTE: Before connecting to the Cloud, make sure the SIM card is installed.

5)Controls: The Agility 4 supports parallel channel reporting (via PSTN, IP/Wi-Fi, 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/Wi-Fi, GPRS, SMS, or voice), or only as a backup when the communication between the Agility 4 system and the Cloud is not functioning.

20. PIR Setup

PIR-based camera detectors perform detection with advanced still image capabilities. Up to eight PIR cameras can be used in the Agility 4 system. For the physical installation of PIR cameras, refer to the product instructions.

➢ **To set up PIR cameras:**

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 *Connecting to the Cloud,* page *15*).
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 **Video Events** tab.
   d) Click on the required picture.

   As necessary, adjust the PIR camera and repeat steps b—d.

21. Testing the System

Before leaving the site, it is important to fully test the system.

- **[For allocated devices]:** From the Installer menu, at **2)Testing** you can go through the communication test ("Comm test") and battery test.
- **[For the Main Panel]:** From the Installer menu, at **2)Testing** > **1)Main Panel** you can go through the tests for noise level, siren, speaker, battery, as well as confirm the main panel S/W version and serial number.
- **[For zones]:** From the Installer menu, at **2)Testing** > **2)Zone,** in addition to communication and battery tests, you can also perform a "Walk Test" – during which you arm the system, and then enter the protected area in order to trigger alarm events at each detector.
- You can also perform a test of the GSM signal strength (ranging from 0–5) from the Installer menu **> 2)Testing > 6)GSM > 1)Signal**
- You can perform a test to ensure Follow-Me is working

22. Installer Responsibilities for Assisting the Customer

1. Advise customer to change the default Grand Master code (and any other installer-defined user codes) after completing installation.
2. Instruct the user how to define user codes, proximity tags, and Follow-Me destinations.
3. For RISCO Cloud connected communication, instruct users with Smartphones to download the iRISCO App from the Apple App store or Android Play Store, and ensure that the connection between the app and the system is established.
4. When allocating the system devices, ensure that all zone information (type of device, zone number, location) is written down and provided to the customer for future use.
5. Instruct the user on the following operations, performed from keypads and/or keyfobs:
   - Away (Full) arming, Stay (Home) arming, and disarming
   - Sending a silent duress alarm to the monitoring station (perform a "duress disarm") in the event a user is forced to operate the system under duress
   - Activating a panic alarm
   - Checking the system status
   - Operating a utility output
   - Using voice menus for remote operation (when calling the system via PSTN or GSM)
   - Using SMS for remote operation

Standard Limited Product Warranty (“Limited Warranty”)

RISCO Ltd. (“**RISCO**") guarantee RISCO’s hardware products (“**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 delivery of the Product (the “**Warranty Period**”). This Limited Warranty covers the Product only within the country where the Product was originally purchased and only covers Products purchased as new.

Contact with customers only. This Limited Warranty is solely for the benefit of customers who purchased the Products directly from RISCO or from an authorized distributor of RISCO. RISCO does not warrant the Product to consumers and nothing in this Warranty obligates RISCO to accept Product returns directly from end users who 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 directly. RISCO’s authorized distributor or installer shall handle all interactions with its end users in connection with this Limited Warranty. RISCO’s authorized distributor or installer shall make no warranties, representations, guarantees or statements to its end users 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.

Remedies. In the event that a material defect in a Product is discovered and reported to RISCO during the Warranty Period, RISCO shall accept return of the defective Product in accordance with the below RMA procedure and, at its option, either (i) repair or have repaired the defective Product, or (ii) provide a replacement product to the customer.

Return Material Authorization. In the event that you need to return your Product for repair or replacement, RISCO will provide you with a Return Merchandise Authorization Number (RMA#) as well as return instructions. Do not return your Product without prior approval from RISCO. Any Product returned without a valid, unique RMA# will be refused and returned to the sender at the sender’s expense. 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 published in RISCO’s website at www.riscogroup.com 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 Product**”), 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 Product.

Entire Liability. The repair or replacement of Products in accordance with this Limited Warranty shall be RISCO’s entire liability and customer’s sole and exclusive remedy in case a material defect in a Product is discovered and reported as required herein. RISCO’s obligation and this Limited 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. This Limited 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, this Limited Warranty shall 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 failure or delay in the performance of the Product attributable to any means of communication 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 does not install or integrate the Product in the end user’s security system and is therefore not responsible for and cannot guarantee the performance of the end user’s security system which uses the Product or which the Product is a component of.

This Limited Warranty applies only to Products manufactured by or for RISCO. Further, this Limited Warranty does not apply to any software (including operating system) added to or provided with the Products or any third-party software, even if packaged or sold with the RISCO Product. Manufacturers, suppliers, or third parties other than RISCO may provide their own warranties, but RISCO, to the extent permitted by law and except as otherwise specifically set forth herein, provides its Products "AS IS". Software and applications distributed or made available by RISCO in conjunction with the Product (with or without the RISCO brand), including, but not limited to system software, as well as P2P services or any other service made available by RISCO in relation to the Product, are not covered under this Limited Warranty. Refer to the Terms of Service at: https://riscocloud.com/ELAS/WebUI/UserLogin/License for details of your rights and obligations with respect to the use of such applications, software or any service. RISCO does not represent that the Product may not be compromised or circumvented; that the Product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise, or that the Product will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce the risk of a burglary, robbery or fire without warning, but it is not insurance or a guarantee that such will not occur or will not cause or lead to personal injury or property loss. CONSEQUENTLY, RISCO SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON ANY CLAIM AT ALL INCLUDING A CLAIM THAT THE PRODUCT FAILED TO GIVE WARNING.

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 WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS, TO THE EXTENT PERMITTED BY LAW. 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 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.

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**

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 from:

FCC

5IN2699 D