

Agility™3

Picture Perfect Wireless Security

Quick Installation Guide

For detailed information please refer to the
Agility 3 Full Installer Manual, available on our website: www.riscogroup.com



RISCO
GROUP
Creating Security Solutions.
With Care.
riscogroup.com

Table of Contents

1.	INTRODUCTION	3
2.	INSTALLING THE MAIN PANEL	3
3.	LCD KEYPAD ALLOCATION AND LANGUAGE SELECTION	4
4.	WIRELESS DEVICE ALLOCATION	5
	QUICK DEVICE ALLOCATION AT THE MAIN PANEL.....	5
	TABLE OF DEVICE TRANSMISSIONS.....	6
5.	PROGRAMMING AGILITY 3 WITH THE LCD KEYPAD	7
6.	ACCESSING INSTALLER MENU	7
7.	SETTING THE SYSTEM CLOCK	7
8.	MEASURING AND DEFINING THE NOISE LEVEL THRESHOLD	8
9.	PROGRAMMING AND TESTING ZONES (DETECTORS)	9
10.	PROGRAMMING AND TESTING KEYFOBS	10
	1-WAY KEYFOB (4-BUTTON) PARAMETERS.....	10
	2-WAY KEYFOB (8-BUTTON) PARAMETERS.....	11
11.	PROGRAMMING KEYPADS.....	12
12.	PROGRAMMING AND TESTING SIRENS.....	13
13.	DEFINING COMMUNICATION CHANNELS	14
	CONNECTING WITH GPRS.....	14
	CONNECTING WITH IP.....	14
14.	DEFINING MONITORING STATION COMMUNICATION	14
15.	DEFINING FOLLOW-ME DESTINATIONS.....	15
16.	SETTING SYSTEM PARAMETERS (CONTROLS)	16
17.	CUSTOMIZING THE VOICE MENU.....	16
18.	DEFINING SYSTEM USERS (USER CODES).....	16
19.	CONNECTING TO THE CLOUD.....	17
	STEP 1: ENABLING CLOUD COMMUNICATION	17
	STEP 2: DEFINING GPRS OR IP COMMUNICATION	17
	STEP 3: DEFINING CLOUD PARAMETERS FOR IP OR GSM/GPRS.....	17
20.	PIR SETUP	18
21.	TESTING THE SYSTEM.....	18
22.	INSTALLER RESPONSIBILITIES FOR ASSISTING THE CUSTOMER.....	19

1. Introduction

This quick installation guide describes the main steps for installing the main panel and programming the Agility 3 using the 2-way wireless LCD keypad. For installation procedures of system devices (detectors and accessories), refer to the Full Installer Manual or the respective device's instructions.

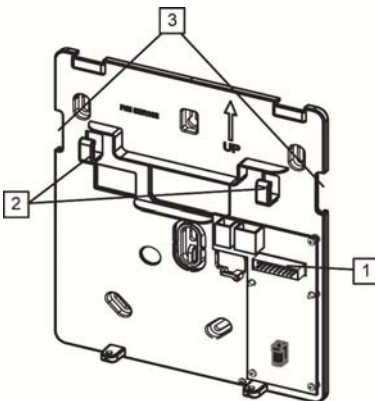
2. Installing the Main Panel

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  and  simultaneously for at least 2 seconds.
3. In the displayed language menu, select the system language (and customer default) settings and then press .

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
 4. *Table of Device 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 Slim Keypad	Press  and  simultaneously for at least 2 seconds.
PIR Detectors: <ul style="list-style-type: none"> • PIR • PIR camera • PIR-pet • PIR-pet camera NOTE: See <i>PIR Setup</i> , page 18.	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
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.
Gas Detector	Transmission is automatically sent 10 seconds after connecting to power supply, or after pressing the test button for 3 seconds (if pressed within 10 minutes of applying electrical power).
CO (carbon monoxide) Detector	Press back tamper switch for 3 seconds. Alternatively, transmission is automatically sent 10 seconds after installing battery.
2-Button Panic Keyfob	Press both buttons for at least 7 seconds
Wrist Band Panic Transmitter	Press the button for at least 7 seconds.







5. 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 3 with the LCD Keypad

This section describes system programming from the 2-way wireless LCD keypad. You can also program the Agility 3 system via the Configuration Software or PTM module. Refer to the CS documentation and the Full Installation Manual, respectively, for details.

The following controls on the LCD keypad are commonly used to program the system:

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)
	To exit the programming mode (followed by  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:**

- From the Installer menu, scroll to **5) Clock**, and then press .
- At the Time & Date option, press , 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.

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 > **; 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 the acceptable noise level threshold value (for example, if the resulting value is very high due to what you believe is a source of high background noise that is inherent to the main panel’s location), you may consider moving the main panel to a better location. If you believe the source of high background noise may only be temporary, you can measure the background noise again to check.

Another option you may consider is to re-define the noise level threshold value (for example, so the system will be more “forgiving” and generate less jamming events).

➤ 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 > **.
2. Enter the noise level threshold value you want between **00 –99**, and then press .
3. 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).

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:

- From the Installer menu select: **1)Programming > 2)Radio Device > 2)Modification > 1)Zones > 2)Parameters.**

2. Use   to select the required zone, and then press .



- 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 .

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.

➤ **To test zones by performing a Comm test:**





1. Use  to go back up to the root of the **Programming** menu. Press  to exit Programming menu, and then press  to confirm.
2. Using   select: **2)Testing > 2)Zone > 1)Comm Test**.
3. Use   to scroll to a zone to perform the Comm test, a number (percentage) appears representing the signal strength the panel received from each device.

NOTE: The signal strength for a device's Comm test should be higher than the resulting number that displays when measuring the background noise level (see *Measuring and Defining the Noise Level Threshold*, 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  to set its basic parameters.
3. Use the   keys to scroll between the options below followed by  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 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).
- **To test keyfobs by performing a Comm test:**
1. Use  to go back up to the root of the **Programming** menu. Press  to exit Programming and then press  to confirm.
 2. Using   select: **2)Testing > 3)Keyfobs > 1)Comm Test**.
 3. Use   to scroll to a zone to perform the Comm test, a number (percentage) appears representing the signal strength the panel received from each device.

NOTE: The signal strength for a device's Comm test should be higher than the resulting number that displays when measuring the background noise level (see *Measuring and Defining the Noise Level Threshold*, page 8).








11. Programming Keypads

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

➤ To program keypad (LCD or Slim) parameters:

1. From the installer menu select: **1)Programming > 2)Radio Devices > 2)Modification > 3)Keypads > 1)Parameters.**
2. Select a keypad, press  and set its basic parameters. Use   to scroll and  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:** For LCD keypad only. 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.

➤ To test keypads by performing a Comm test:




1. Use  to go back up to the root of the **Programming** menu. Press  to exit Programming and then press  to confirm.
2. Using   select: **2)Testing > 4)Keypad > 1)Comm Test.**
3. Use   to scroll to a zone to perform the Comm test, a number (percentage) appears representing the signal strength the panel received from each device.

NOTE: The signal strength for a device's Comm test should be higher than the resulting number that displays when measuring the background noise level (see *Measuring and Defining the Noise Level Threshold*, 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  and set its basic parameters. Use  to scroll and  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.

➤ To test sirens by performing a Comm test:

1. Use  to go back up to the root of the **Programming** menu. Press  to exit Programming, then press  to confirm.
2. Using , select **2)Testing > 5)Sirens > 1)Comm Test**.
3. Use  to scroll to a siren to perform the Comm test, a number (percentage) appears representing the signal strength the panel received from each device.

NOTE: The signal strength for a device's Comm test should be higher than the resulting number that displays when measuring the background noise level (see *Measuring and Defining the Noise Level Threshold*, 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 > **.

- 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.

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) > .**
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 3 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**) >  > 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  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 3 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 3 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 GPRS or IP Communication

- See *Defining Communication Channels*, page 14.

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 (**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 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 3 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 3 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 3 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 3 and the Cloud server (See *Connecting to the Cloud*, page 17).
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

Contacting RISCO Group

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

United Kingdom

Tel: +44-(0)-161-655-5500

E-mail: support-uk@riscogroup.com

Italy

Tel: +39-02-66590054

E-mail: support-it@riscogroup.com

Spain

Tel: +34-91-490-2133

E-mail: support-es@riscogroup.com

France

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

E-mail: support-fr@riscogroup.com

Brazil

Tel: +55-11-3661-8767

E-mail: support-br@riscogroup.com

China (Shanghai)

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

E-mail: support-cn@riscogroup.com

China (Shenzhen)

Tel: +86-755-82789285

E-mail: support-cn@riscogroup.com

Poland

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

E-mail: support-pl@riscogroup.com

Israel

Tel: +972-3-963-7777

E-mail support: support@riscogroup.com

Australia

Tel: + 1-800-991-542

E-mail: support-au@riscogroup.com

Belgium (Benelux)

Tel: +32-2522-7622

E-mail: support-be@riscogroup.com

USA

Tel: +1-631-719-4400

E-mail: support-usa@riscogroup.com

This RISCO product was purchased from:



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