riscogroup.com

WiComm Pro

Model: RW332M

EN

Quick Installation Guide

Visit our website: **www.riscogroup.com**

For more information about RISCO Group's branches, distributors and full product line, please visit **riscogroup.com**

Contents

1. Introduction

This quick installation guide describes the main steps for installing the main panel and programming the WiComm Pro using the Wireless Panda (2-Way LCD + Proximity) keypad.

The WiComm Pro utilizes Cloud-based Smartphone and Web user apps and with advanced wireless security and safety features. The WiComm Pro supports IP and 2G/3G plug-in multi-socket communication modules that provide multiple, simultaneous communication channels for direct communication, and for communication via the Cloud.

For installation procedures of system detectors and accessories, refer to the instructions packaged with each respective device.

2. Installing the System

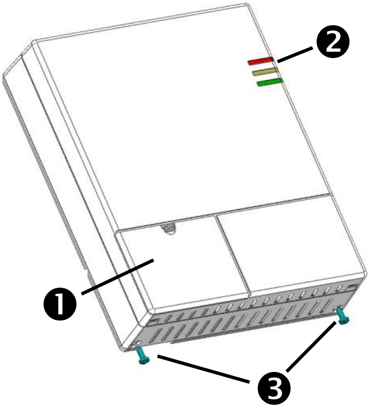
2.1 Mounting Main unit considerations

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

- Centrally located among the wireless devices
- 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
- Access to network (cable) connectivity, if utilizing IP communication
- In a place where the alarm can be heard during Stay (partial arming) mode
- Away from sources of direct heat, electrical disturbance and large metal objects which may hinder reception

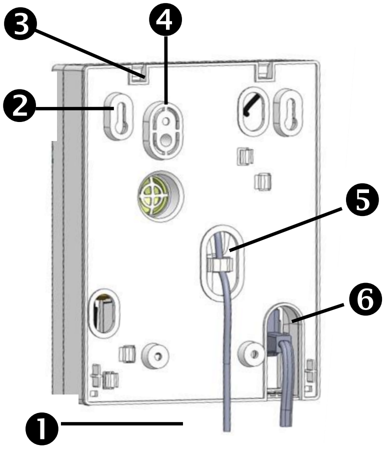
2.2 To Install the Main Panel

1. Disconnect the mounting bracket (back cover of main panel) by releasing the two locking screws at the base of the unit, and then lifting the unit upward to detach the two tabs from the respective grooves on the mounting bracket:

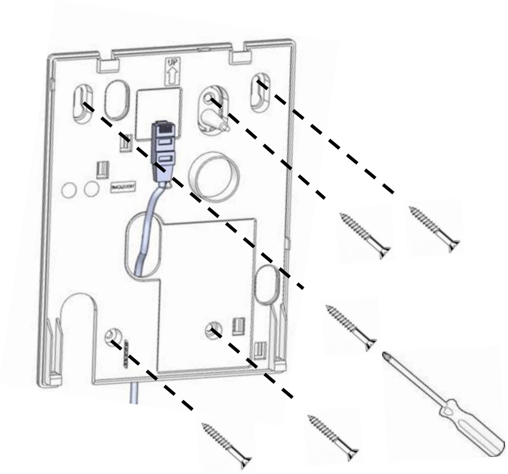


❶	Front access cover
❷	LED indicators
❸	Locking-screws (2)

2. Using the mounting bracket as a template, first mark and then drill all five holes on the wall (four mounting holes and one back tamper hole), then install the anchors. See page *5*.



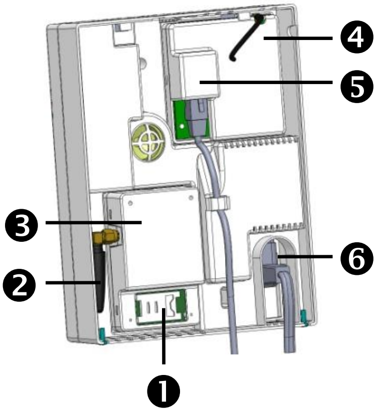
Mounting bracket – back side



Mounting bracket – front side

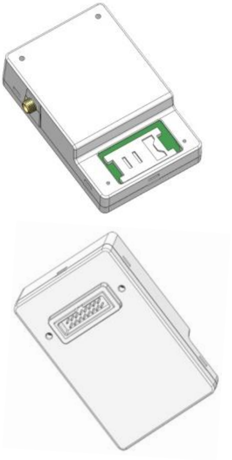
❶	Lower mounting screw locations (2)
❷	Upper mounting screw locations (2)

❸	Grooves for placing tabs from front cover (2)
❹	Back tamper screw location
❺	Wiring channel for network cable (shown with cable routed via hook)
❻	Opening for AC power cable (cable is installed onto the back of the panel only after the mounting bracket is secured to the wall)



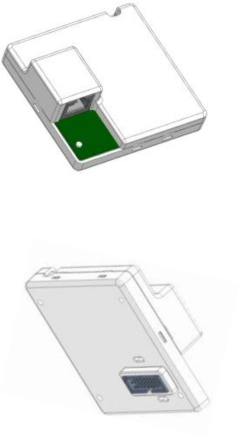
GSM Module

(front and back)



IP Module

(front and back)



❶	SIM holder on GSM module
❷	Antenna for GSM module (shown with internal antenna installed)
❸	GSM module
❹	IP module
❺	Network cable connector on IP module (shown with cable connected)
❻	AC power cable (shown installed from the back of the main panel)

3. Install the IP communication module in its cavity (back cover), with its connector fitting securely onto its respective socket.
4. Make sure the network cable is first routed through the wiring channel on the mounting bracket (and via the fastening hook). Then plug the network cable into its jack on the module (see illustration on page 5).

5. Insert the SIM card into its holder, as required
6. Screw the antenna onto its connector on the GSM module
7. Install the GSM module in its cavity, with its connector fitting securely onto its respective socket.

NOTE: Do not power-up the main panel yet.

8. Route the AC power cable through the opening in the housing (back cover), and secure its plug onto the socket (see illustration on page 5).

NOTE: The backup battery takes 24 hours to charge.

9. Affix the main panel onto the mounting bracket by positioning its two plastic tabs (located at the top of the panel) onto their respective grooves (located at the top of the mounting bracket), and then press to close the housing.
10. Install the two locking screws at the bottom of the main panel.
11. Connect the main panel to the AC power supply.

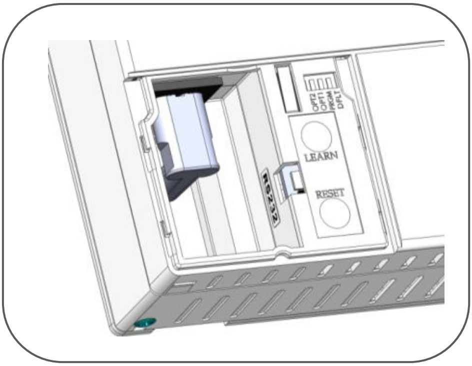
3. Wireless Device Allocation

3.1 Allocating the Keypad and Selecting a Language

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 quickly allocate a keypad and define the system language:**

1. After powering-up, press the **LEARN** button on the main panel for about 5 seconds; all three LEDs light up, one after the other, indicating the panel is in “Learn” (device allocation) mode.



2. Press 🏠 and 🔒 simultaneously for at least 2 seconds; the keypad will “beep” if allocated.
3. In the displayed language menu, select the system language (and customer default) settings, and then press OK to confirm.

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.

3.2 Wireless Device Allocation Options

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 an RF signal transmission from each device to the main panel (see procedure below).
- **LCD keypad:** The following methods are available:

  For having devices 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 device 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 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. Make sure batteries are installed in each device.
2. At the main panel press the **LEARN** button for 5 seconds; all three LEDs light up, one after the other, indicating the panel is in "Learn" (allocation) mode.
3. Send an RF signal transmission to the main panel from each device per the instructions in the *Table of Device Transmissions*, page *10*. If a device is not listed in the table, refer to the device's packaged instructions.

   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.

Wireless Device RF 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.
2-Way Slim Keypad	Press 🏠 and 🔒 simultaneously for at least 2 seconds.
PIR Detectors: • **PIR** • **PIR camera** • **PIR-pet** • **PIR-pet camera**	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
Wireless 2-Way Smoke Alarm & Heat Detector	Press the tamper switch for 3 seconds.
WL 2-Way Indoor Siren	Press the tamper switch for 3 seconds.
Siren	Press the reset switch on the siren. After a squawk sounds, within 10 seconds press tamper switch for at least 3 seconds.
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 allocated, short-press the **LEARN** button to exit Learn mode; the LEDs stop flashing.

4. Programming the System

4.1 Programming with LCD/Panda Keypad

This section describes system programming from the 2-way wireless LCD keypad. You can also program the WiComm Pro system via the Configuration Software (refer to the CS documentation and the Full Installation Manual).

The following buttons are commonly used for programming (the buttons shown are for the 2-Way Wireless Panda LCD & Proximity keypad):

Button	Description
⚙↩	To 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)

4.2 Accessing the Installer Menu

From an allocated keypad, press ⚙↩ if needed (to go back in a menu), and then enter the installer code (default is **0132**).

4.3 Manually Setting the Time & Date

The system clock is set automatically after the main panel is configured with IP or GSM communication. You can also configure it manually.

➢ **To manually set the time and date:**

1. From **Installer menu,** scroll to **5) Clock,** then press OK; Time & Date appears.
2. Press OK, enter the time and date, and then press OK.

4.4 Measuring and Defining the Noise Level Threshold

From the keypad 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.
2. After measuring, if the resulting value is far from your defined threshold value, or if the value is too high (See *4.5 Performing a Communication Test* below for an explanation of acceptable results) and you believe the source of background noise may be due to the main panel’s location, move the main 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,** 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). See *4.5 Performing a Communication Test* below for an explanation of acceptable results.

4.5 Performing a Communication Test

The Communication test displays the results of the signal strength measured at the panel after a wireless device's last transmission (last detection or last supervision signal).

➢ **To perform a Communication Test:**

1. Activate the wireless device.
2. From the Installer menu, go to: **2)Testing > 2)Zone [or instead 3)Keypad, 4)Keypad, or 5)Siren] > 1)Communication Test >** OK **.**
3. Scroll with ⇅ⓘ ⇅ to a zone to perform the test; the result (percentage) appears representing the signal strength the panel received from the device, which must be as follows:
   - The signal strength must be at least 30% (30 or more must display).
   - In addition, the Communication 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 background noise level measures 25%, the Communication test result must be 35% or more.

4.6 Programming Detectors and Accessories

Program the system either using the keypad, or via the *Configuration Software* (see the Configuration Software documentation).

For programming parameters of all zones and peripheral devices in the system (detectors and accessories), refer to the instructions packaged with each device.

IMPORTANT: After programming device parameters, it is recommended to perform a Communications test for each wireless device (see *4.5 Performing a Communication Test,* page 13).

4.7 Programming & Testing Zones (Detectors)

The parameters available per zone (detector) may vary, according to the zone type. Refer to the instructions packaged with each detector.

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

1. From the **Installer menu** select: **1)Programming > 2)Radio Device > 2)Modification > 1)Zones > 2)Parameters.**
2. Scroll with ⇧ⓘ ⇩ 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 ⌂ and 🔒 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, and then press OK.

   4) Sound: Use ⇧ⓘ ⇩ to select the desired sound.

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

4. Perform a Communications test (see *4.5 Performing a Communication Test*, page *13*).

4.8 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 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 *13*).

4.9 Programming Keypads

Up to three keypads 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,** 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 *4.5 Performing a Communication Test*, page *13*).

4.10 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 *4.5 Performing a Communication Test*, page *13*).

4.11 Defining Communication Channels

The menus displayed reflect only the installed communication modules.

➢ To define communication channels:

1. From the **Installer menu** go to: **1)Programming > 4)Communication > 1)Method**.

2. Select the method (for IP and/or GSM) and define the parameters as follows:

Connecting with GSM/GPRS

- **To connect with GSM:**

a. From the **Programming menu** go to: **4)Communication > 1)Method > 2)GSM >** use ⇧ⓘ ⇩ to scroll to **2)GSM >** OK .

b. Use ⇧ⓘ ⇩ to scroll between **1)APN Code**, **2)APN User Name,** and **3) APN Password.** By default, APN is set automatically, depending on the SIM card. If the SIM is not supported**,** define the **APN code** and **user name & password** respectively as defined by the SIM card service provider.

Connecting with IP

a. From the **Programming menu** go to: **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

- **To connect with Wi-Fi:**

Note: Your Router's Wi-Fi must be activated for the Control Panel to recognize and communicate with the Router.

a. To connect via Wi-Fi network, you must select your Router's Wi-Fi network.

b. Go to **Activities –> Wi-Fi screen**: available networks appear in a list.

c. Select the desired network and enter the password (if required).

4.12 Defining Monitoring Station Communication

Reporting to monitoring station can be directly from the panel to the monitoring station receiver or routed through the RISCO cloud. For direct communication from the panel to the monitoring station you can define up to 3 monitoring station accounts and several associated parameters that define the nature of communication, event reporting and confirmation between the system user 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).

4.13 Defining Follow-Me Destinations

The WiComm Pro can notify end users of various system events. Reporting can be done directly from the WiComm Pro to the end user by SMS (up to 16). Reporting can also be by Email or Push Notification from the main unit or using the RISCO Cloud. When using the Cloud, the number is unlimited.

➢ **To define Follow Me Report:**

- Use ⚙↩ to return 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, or Email.** (Reporting events by email can be established directly from the panel or from the RISCO Cloud).

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, 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 SMS remote user operation (as either **Y** or **N**) which is performed on the WiComm Pro:

- 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 destinations can be assigned in the RISCO Cloud.

4.14 Setting System Parameters

System- parameters define how the system works and are located under the System menu. All the parameters in the System menu are set with default values that apply for most installations. If you wish to change the parameter settings, scroll through the menus to program the required system parameters accordingly.

4.15 Defining System Users (User Codes)

The installer may initially set up system users via the keypad or Configuration Software. However, the Grand Master should define all the user codes (via the keypad or Web User application) for personalization and confidentiality.

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

- Use ⚙↩ to return 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 can operate (except for the Grand Master, who can operate all partitions). 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)

4.16 Connecting to the Cloud

The system 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 RISCO 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 GSM or IP Communication

See 4.11 Defining Communication Channels, page 17.

Step 3: Defining Cloud Parameters for IP or GSM

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

1)IP Address: The server IP address **(www.riscocloud.com)**

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 RISCO Cloud (based on IP or GSM communication) as appears in the available options.

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

5)Controls: The system supports parallel channel reporting (via IP, GSM, SMS) 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 RISCO Cloud (assuming there is an additional communication channel available – IP, GSM, or SMS), or only as a backup when the communication between the system and the Cloud is not functioning

4.17 Wireless PIR Camera Setup

PIR-based camera detectors perform detection with advanced still image capabilities. Up to eight PIR cameras can be used in the WiComm Pro 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 WiComm Pro and the RISCO Cloud server (See *4.16 Connecting to the* Cloud, page 22).
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.

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

5. 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 perform the Communication test and battery test.
- **[For the Main Panel]:** From the **Installer menu,** at **2)Testing** > **1)Main Panel** you can perform the tests for noise level, siren, speaker, battery, as well as confirm the main panel software 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 enter the protected area in order to trigger alarm events at each detector.
- **[For GSM signal]:** 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**
- **[For Follow-Me]:** You can perform a test to ensure Follow-Me is working

6. Assisting the Customer

The following are typical areas where it is recommended that the installer assist the customer.

- ✓ Advise customer to change the default Grand Master code after completing installation to one that is confidential.
- ✓ Instruct the user on how to define user codes and Follow-Me destinations.
- ✓ 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.
- ✓ 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.
- ✓ 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 (a "duress disarm") to the monitoring station in the event a user is forced to operate the system under duress
  - Activating a panic alarm
  - Using SMS for remote operation

7. Technical Specification

Configuration	
Communication modes (modules)	GPRS/GSM (2G), GSM (3G), IP,
Wireless zones	32
Wireless frequencies	868 MHz, 433 MHz
Camera frequency	869.525 MHz, 916 MHz, 430 MHz
System users (user codes)	32 (includes 1 installer, 1 sub-installer, and 1 Grand Master code)
Follow-Me destinations	16
Panel programming options	• Keypad (locally) • Configuration Software (locally, remotely)
Partitions	3
Monitoring station accounts	3
Event log	1000 entries
PIRs / PIR cameras	8
Sounders (internal/external)	3
Keypads	3
Keyfobs / remote controls	8
SMS for remote operation	yes
Main Panel (RW332M)	
Electrical power requirement	230VAC, 50/60 Hz 0.6A max.
AC power supply cord	• Diameter 14mm, conduit 16mm • Safety-approved, in compliance with IEC 60227
Current consumption (at main panel)	166mA standby
Backup battery (inside main panel)	• Li-Polymer rechargeable battery pack 2350 mAh. • Low voltage signal at 7.2 VDC
Humidity range	Average relative humidity of approximately 75%
Operating temperature	-10°c – 55°c (14°F to 131°F)
Dimensions (H x W x D)	197.5 mm x 152.5 mm x 52 mm 7.78 in x 6 in x 2.05 in
Weight	0.77 kg
Power Output	• Security 868.65 MHz, 10 mW • Camera 869.525 MHz, 100 mW
GSM G2, GSM G3 & GSM G4 Modules (RP512G2, RP512G3, RP512G4)	
Current consumption	Average: 30 mA Peak: 130 mA
IP Module (RP512IP)	
Current consumption	Average: 60 mA Peak: 115 mA

Wi-Fi Module (RP51200W)	
Current consumption	Average: 60 mA Peak: 115 mA
Wireless LCD Keypads: (RW332K/RW332KP)	
Current consumption	Average: 9µA Peak:150 mA

Compliance Statement

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

- EN50131-1
- EN50131-3 Grade 2, Environmental Class II
- EN50131-6 Type A
- EN50136-1
- EN50136-2
- EN50131-10 SPT Type Z
- EN50131-5-3
- Compatibility with serial interface with AS
- Compatibility with GPRS protocol
- Compatibility with TCP/IP protocol
- Control Panel method of operation: Pass-through
- Signaling security: Substitution security S2
- Information security I3

Alarm Transmission System Classification and Categories:

- GSM 2G/3G (SP5)
- IP (SP6)
- GSM primary and IP secondary (DP4),
- IP primary and GSM secondary (DP4)

EN50136 Compliance:

- RISCO has designed the WiComm Pro GSM and IP communication modules to be in compliance with the information security and substitution security requirements of EN50136.

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.

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:

Australia
Tel: +1800-991-542
support-au@riscogroup.com

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: