

WICOMM Smart Hub Reference Manual



Models: RW232M, RW232M8B, RW232M8C, RW232M87

Table of Contents

1. INTRODUCTION	5
EXPANDING YOUR SYSTEM	5
SELF-INSTALLATION	5
2. SYSTEM COMPONENTS	6
KIT AND OPTIONAL DEVICES.....	6
SERIAL NUMBERS.....	8
3. GUIDELINES FOR USING THE RISCO EXPRESS INSTALLATION WIZARD	10
SELF-INSTALLATION	10
WELCOME SCREEN.....	10
CONNECT TO NETWORK	10
<i>Connecting a network cable to the WiComm Smart Hub</i>	10
<i>SIM Card Installation</i>	10
<i>Connecting the WiComm Smart Hub to the Power Supply</i>	11
PERSONAL INFO.....	11
SYSTEM INFO	12
SET-UP DEVICES	12
USER & CODES	12
INSTALL DEVICES.....	13
DONE	13
4. SMART HUB INDICATIONS AND CONNECTIONS	14
SMART HUB FRONT VIEW	14
SMART HUB REAR VIEW	14
LEDs INDICATION	15
5. DEVICE MOUNTING CONSIDERATIONS	16
MOUNTING CONSIDERATIONS FOR SMART HUB.....	16
WIRELESS SIGNAL LOSS THROUGH CERTAIN BUILDING MATERIALS	17
PLACING THE SMART HUB	18
MOUNTING CONSIDERATIONS FOR DETECTORS	19

MOUNTING CONSIDERATIONS FOR PIR DETECTORS	20
ACTIVATING THE BATTERY OF DOOR / WINDOW DETECTOR	21
<i>Activating the battery</i>	21
HOW TO MOUNT THE DOOR / WINDOW DETECTOR	21
<i>Mounting with Adhesive Tape</i>	21
<i>Mounting with Screws</i>	22
ACTIVATING THE BATTERIES OF THE PIR DETECTOR.....	24
HOW TO MOUNT THE PIR DETECTOR	24
<i>Mounting with Adhesive Tape</i>	24
<i>Mounting with Screws</i>	25
6. WIRELESS DEVICE ALLOCATION	28
TABLE OF ADDITIONAL DEVICES ALLOCATION PROCEDURE	29
7. LOGGING INTO THE USER WEB & APP	30
SETTING THE TIME ZONE	30
CHANGING USER CODES	31
CHANGE ZONE LABELS	35
SMART HUB SETUP	36
<i>General</i>	36
<i>Setup Timers</i>	37
<i>Setup Sounds</i>	38
<i>Setup Voice Messages</i>	39
<i>Setup Devices</i>	40
<i>Stay Mode</i>	42
<i>System Testing</i>	43
<i>Service Mode</i>	44
8. USER OPERATIONS	45
USER OPERATIONAL DEVICES	45
FULL SETTING.....	46
STAY / PARTIAL SETTING	47
AREA SETTING	48
UNSETTING.....	49
9. REPLACING BATTERIES.....	50
SERVICE MODE	50
BATTERY REPLACEMENT OF DOOR / WINDOW DETECTOR	50
BATTERY REPLACEMENT OF PIR DETECTOR	52

10. TECHNICAL SPECIFICATIONS	53
11. STANDARD COMPLIANCE	54
RED COMPLIANCE STATEMENT: (MODELS: RW232M8B, RW232M8C, RW232M87) ...	55
IC WARNING (MODEL: RW232M).....	55
FCC NOTE (MODEL: RW232M).....	56

1. Introduction

This easy to install, “out-of-the-box”, system utilizes cutting-edge technologies to protect your home or small business against intrusion and safety hazards.

Easy to operate and robust, your security system is designed to provide you with peace of mind. Even during a power outage, it keeps fully working, monitoring, and providing alarm notifications.

System configuration is performed by the RISCO Express Wizard. Control is performed on-site or remotely using a wireless slim keypad or remote keyfob, a mobile device (smartphone or Tablet PC) running the Android or iOS operating system, or a computer / laptop running a browser-based Web application. When using a PIR Camera motion detector with Smartphone and Web application, users can also remotely view real-time images of the secured premises upon alarm activation, or at any given time. This “visual verification” feature can help you determine whether an alarm is false or real. In addition, 24/7 monitoring of your system can be available through security-monitoring services.

Expanding your System

This kit contains all the necessary components required to operate your security system, however you can enhance and customize your system by adding additional detectors and accessories.

Note: It is recommended to add additional devices before starting the self-installation process.

Self-Installation

For basic and simple installation it is necessary to use the RISCO Express Wizard that explains step-by-step on how to program and install the system (*see* 3. GUIDELINES FOR USING THE RISCO EXPRESS WIZARD).

From a computer or tablet with an internet connection and a web browser, follow the instructions from URL: <http://riscocloud.com/express>.

2. System Components

Kit and Optional Devices

The following list includes the full range of components and devices available for the Smart Hub. Some of these components and devices are included inside the kit you purchased and others can be purchased separately.

Note: The type and quantity of components and devices inside the kit may vary from kit to kit.

Smart Hub



Electrical power adapter, Ethernet cable, screws and anchors



LCD Keypads including proximity reader for using proximity tags



Wireless Slim Keypad including proximity reader for using proximity tags



4 Button Remote Keyfob



Magnetic Door/Window Contact
(includes detector and magnet)



A “pet-friendly” PIR Motion Detector



A “pet-friendly” PIR Motion Detector
with Camera



Wireless Smoke and Heat Detector



Indoor Wireless Sounder



Wireless acoustic Glassbreak Detector



Wireless Flood Detector



Note: For device Technical Specifications, see RISCO's website at <https://www.riscogroup.com>.

Serial Numbers

Serial numbers are used to identify the components of your security system as used in the RISCO Express Wizard. Each serial number consists of 11 digits.

It is recommended to keep a record of component serial numbers and locations that correspond to the devices serial numbers, as shown in these illustrations.



Magnetic door/window contact



PIR Motion detector



4 Button
Remote Keyfob

3. Guidelines for using the RISCO Express Installation Wizard

Self-Installation

It is necessary to use the RISCO Express Wizard to successfully and professionally install your WiComm Smart Hub System.

The RISCO Express Wizard walks you through the programming and installation of the system and connecting to the Cloud and Monitoring Station.

From a computer or tablet with an internet connection and a web browser, follow the stages of the RISCO Express Wizard instructions from URL:

<http://riscocloud.com/express>

Welcome Screen

Enter the Kit Number without the “W” (see Serial Numbers) and 4-digit Code as printed on the Smart Hub.

Connect to Network

Connecting a network cable to the WiComm Smart Hub

Your WiComm Smart Hub communicates via cellular and/or internet. For cellular you need to install a SIM card with data communication enabled (check with your SIM card provider). For internet communication, connect the incoming network cable to the plug-in.

SIM Card Installation

Insert the SIM into the dedicated SIM spring-loaded card slot located on the rear side of the Smart Hub. The card clicks into place.

To enable 3G communication please ensure you move the locking switch to the right to secure the SIM and enable it to operate.




Locking Switch



Important: Do not install the SIM card while power is applied to the WiComm Smart Hub. If power was applied before inserting the SIM card and the battery remains connected, hold down the reset button for 2 minutes and then release to reset the Smart Hub and enable the SIM card.

Connecting the WiComm Smart Hub to the Power Supply

1. Plug in the power adapter to your security system. Verify the following:

- The Power Led  is shortly lit in **GREEN** and then lit in **AMBER**.
- The Status light  is lit in **GREEN**.

- The communication LED  flashes **AMBER**.
2. After power up, the system will automatically establish communication with the cloud. Please note that it may take a few minutes until communication with the cloud is established, before continuing with the RISCO Express Installation Wizard setup.
 3. Continue with the remainder of the installation wizard and test the system until all the devices are successfully installed, as indicated in the wizard.

When the installation wizard is complete, the Power Led  and the communication LED  will turn **GREEN**.

Personal Info

Enter the following registration details (Name, Email and Password [the Password must be at least 6 characters and contain at least one capital letter, one letter and one digit number]) into the provided fields. If you are already registered, enter your email and password on the right side of the window.

Select the "I have read and agree to the Terms & Conditions and Privacy Policy" box. Next, enter the 4-digit verification code sent to your inbox and used for creating your account.

If the email is not received, please check your junk mail.

System Info

Enter a name for your system, for example, 10 Birchford Street.

The system can be divided into “Areas”, for example, Garage, Home Office and House. Enter a name that is easily recognizable for each of the areas.

Set-up Devices

This step enables the system to identify the detectors and accessories supplied in the basic kit. Additional detectors and accessories supplied and not shown in the list can be entered one at a time by entering the 11-digit Serial Number of each device.

Click the Configure button to the right of a device name. A screen will open with instructions on how to set-up the device. Repeat the procedure for the rest of the devices.

User & Codes

Assign new User Codes and a Master User Code.

Note: During system setup, it is recommended to change the Master User Code. The default Master User Code is 1234.

In addition, you can assign a Proximity Tag that is a personal electronic disc that when presented close to the Proximity-supported keypad functions the same as entering a personal user code.


It is recommended to add a user code for every user operating the system, as this user code will provide historical data of all functions performed by a specific user.

Install Devices

Select the preferable network connection: Local Network (via router) or Mobile Connection (via SIM card). It is also possible to select both. Next, physically install the devices after considering the best location and then test the devices detection strength.

Note: It may take up to 5 minutes for the panel to connect to the network : During

installation of the devices, the communication LED  flashes **AMBER**. Once

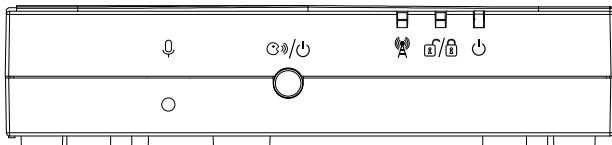
installation is complete, the **GREEN**  LED flashes.

Done

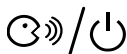
You have successfully completed the registration of your security system which is now ready for use. Refer to Chapter 7 for instructions on how to: log onto your WiComm Smart Hub; change the time zone; and operate your system.

4. Smart Hub Indications and Connections

Smart Hub Front View



Microphone



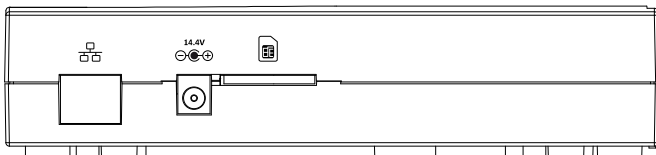
Status Button

Press 1 second: The system will play local status messages

Press 3 seconds: Quick learn mode

Press 2 minutes: Resets the Smart Hub

Smart Hub Rear View



Ethernet connection




14.4V

Power Adaptor connector



SIM Card slot.

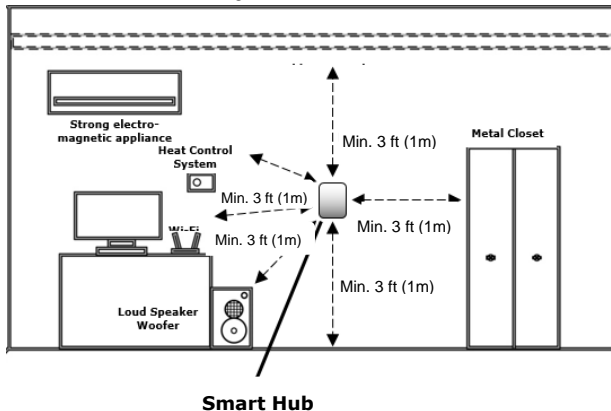
LEDs Indication

LED displays	Color	State	Status
 Power LED	Green	ON	Power OK
	Red	ON	AC trouble
	Orange	ON	Battery trouble.
 Status LED	Red	ON	System set (Full Set or Part Set)
		rapid flash	Alarm
		slow flash	System is in entry/exit delay before unsetting / setting the system
	Green	ON	System ready
		slow flash	System in Exit delay with front door open
	Orange	ON	System Trouble
	OFF		System not ready for setting
 Communication LED	Green	ON	GSM/IP connected
		slow flash	Cloud connected
	Orange	slow flash	GSM/IP Trouble
All LEDs	Orange	Slow flash	Battery Replacement mode (service mode)
	Green	Sequence flash	Wireless Learn mode

5. Device Mounting Considerations

Mounting Considerations for Smart Hub

For optimum installation of the Smart Hub and detectors, make sure to follow the recommendations for the mounting location, as illustrated below.

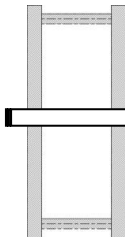


Note: The above illustrative diagram is intended to provide best results.

Wireless Signal Loss through certain building materials

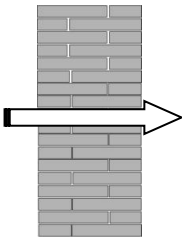
It is helpful to identify certain building materials that may be the cause of loss of signal strength and to make sure that the area around the Smart Hub is free of such materials, as much as possible. If signal interference is experienced, you may want to consider moving the Smart Hub.

0% - 10% loss of signal



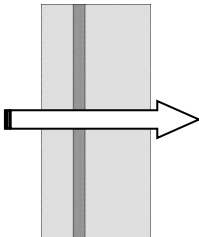
Wallboard and Wood

5% - 35% loss of signal



Light Concrete or Brick

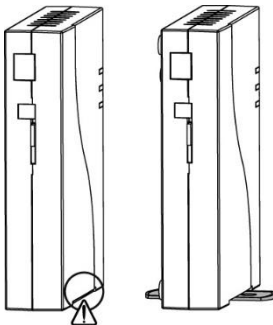
70% - 90% loss of signal



Heavy Concrete and Steel Reinforcement

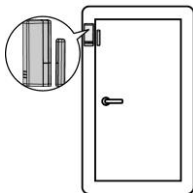
Placing the Smart Hub

For upright independent placement:
Stand the Smart Hub on a surface (e.g. table), adjust the swivel base of the Smart Hub so that it is in a stable upright position.

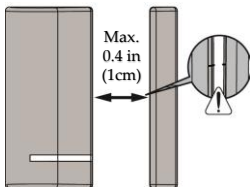


Mounting considerations for Detectors

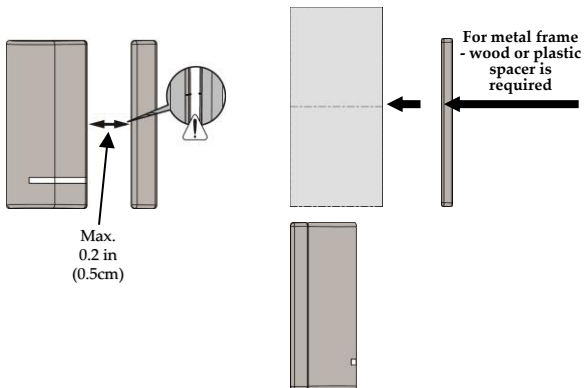
Wood & Metal Frame



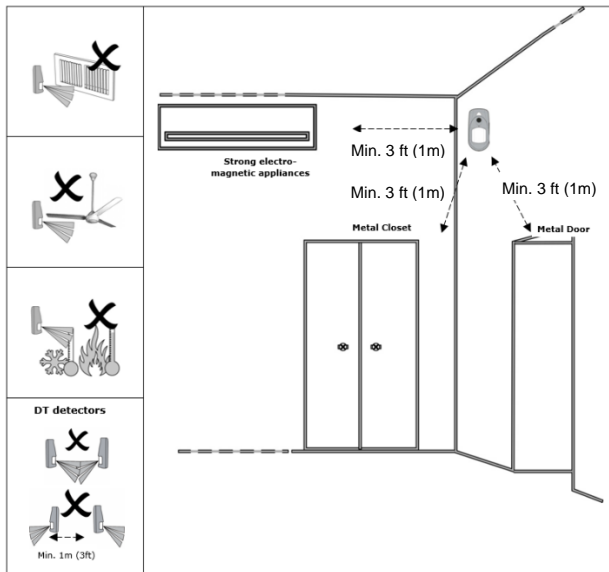
Wood Frame



Metal Frame (possible 30% signal loss)



Mounting considerations for PIR detectors



Note: Place the detector just a foot (30 cm) or so lower than the ceiling. To provide maximum coverage, the detector should be placed in a corner facing away from any windows and ideally towards the entrance of the room, or, follow the height specified in their Installation Instructions.

Activating the Battery of Door / Window Detector

Activating the battery

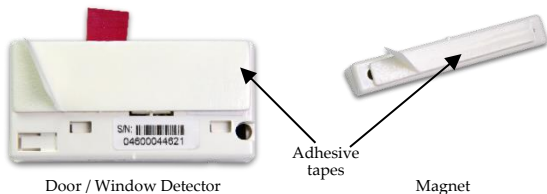


Remove the red battery isolation strip to activate the battery.

How to Mount the Door / Window Detector

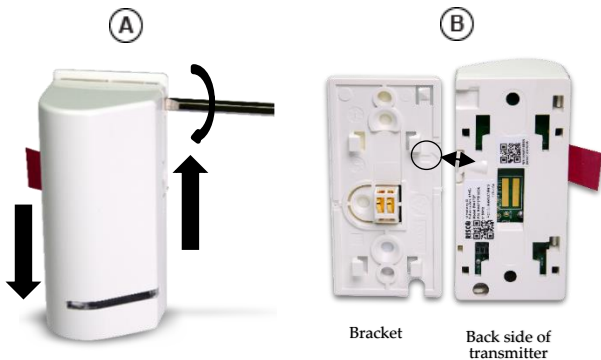
Mounting with Adhesive Tape

Peel the two-sided adhesive tapes from the detector and magnet and attach the detector and magnet to the mounting location.



Mounting with Screws

1. Insert a flathead screwdriver and rotate to detach the back of the transmitter from the back bracket (A). At the mounting location, note the alignment marks for both components (B), and then install accordingly using 2 mounting screws (C).
2. Detach magnet casing (D) and install with mounting screws (E).



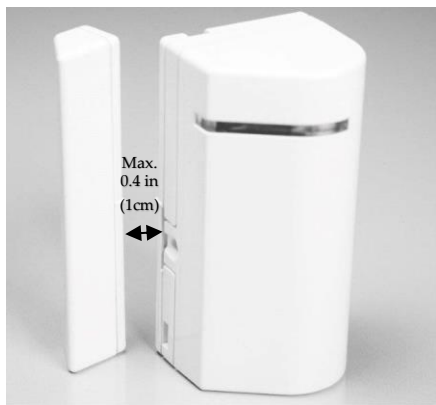
Ⓒ



Ⓓ



Ⓔ



The mark on the magnet's case must be aligned with the mark on the transmitter's case.

Activating the Batteries of the PIR Detector

Red battery isolation strips

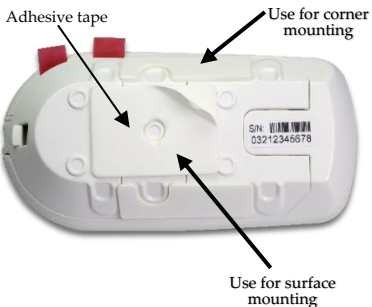


Remove the red battery isolation strips to activate the batteries.

How to Mount the PIR Detector

Mounting with Adhesive Tape

Peel the two-sided adhesive tapes from the detector and attach the detector to the mounting location.



Mounting with Screws



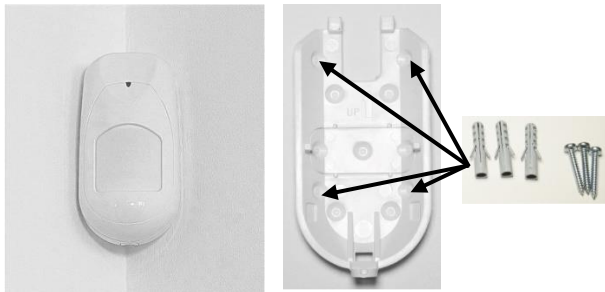
1. Release screw using a Phillips screwdriver.



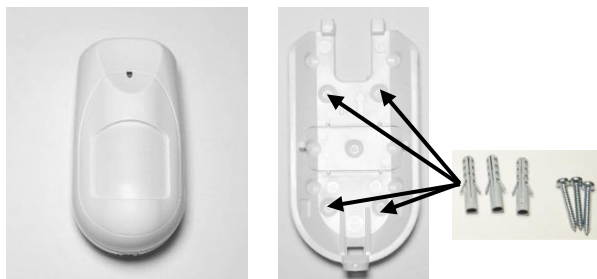
2. Insert a flathead screwdriver into the slot and push to remove cover.

3. Open the knockout holes of the mounting bracket, and use them as a template for mounting.

Corner Mounting



Surface Mounting





4. Slide the PIR detector downward onto the mounting bracket.



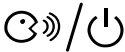
5. Insert and fasten the screw into the hole located at the bottom of the detector to lock the detector to the mounting bracket.

6. Wireless Device Allocation

The initial installation of the system must be performed using the RISCO Express Wizard. If additional accessories are purchased at a later stage, they must be allocated (“enrolled”) to the system using the method described below, and not using the RISCO Express Wizard.

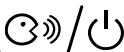
You can quickly allocate all system devices (including keypads) at the control panel. In case of future enrollment of additional devices, refer to the device Installation Instructions.

1. To enter the Smart Hub into Quick learn mode press the








button for 3 seconds – all LEDs will sequentially flash.

2. When the Smart Hub is in the Quick learn mode, perform the transmission procedure listed in the table below.



3. When complete, press the button once to exit this mode. The Smart Hub will announce when the device is allocated. The zone name may be edited using the user website at <https://www.riscocloud.com>.

Table of Additional Devices Allocation Procedure

Wireless Device	Transmission procedure
PIR Detectors: Motion Detector-PIR camera Motion Detector Pet camera	Press the tamper switch for 3 seconds.
Door/Window Detector	Press the tamper switch for 3 seconds.
Remote Keyfob	Press  for at least 2 seconds
LCD Keypad	Press  and  simultaneously for at least 2 seconds
Slim Keypad	Press  and  simultaneously for at least 2 seconds.
Smoke/Heat Detector	After inserting battery, transmission is sent automatically within 10 seconds.
Internal Sounder	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.
Glassbreak Detector	Press the tamper switch for 3 seconds.

7. Logging into the User Web & App

Log into the iRISCO website at <https://www.riscocloud.com>.

RISCO
GROUP
Creating Security Solutions.
With Care.

Username/Email Address

Password

System PIN Code

Log In

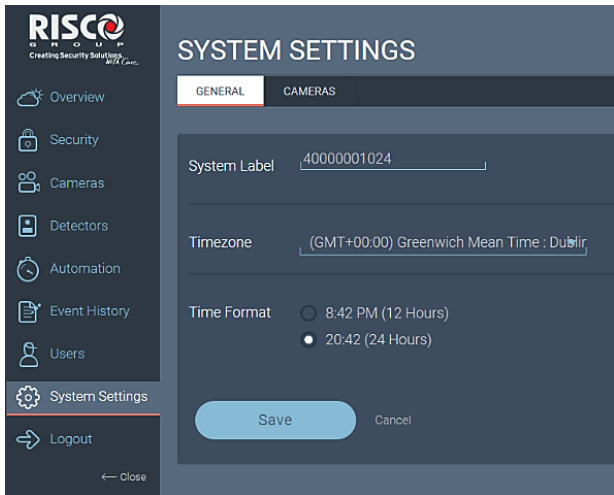
English (United Kingdom) [Register](#) [Lost password?](#)

© 2016 All rights reserved to RISCO Group LTD www.riscogroup.com

1. Enter your email address and password selected at the start of registration.
2. For the required “PIN Code” enter your assigned 4-digit Master User code selected during the “User & Codes” stage of the RISCO Express Wizard.

Setting the Time Zone

1. Click the **System Settings** link in the left-hand column of the screen.
2. Click the **Date and Time** button; the SYSTEM SETTINGS page displays the current time zone and time format.
3. Make the required changes.
4. Click **Save**.



Note: The date and time, Time Zone descriptions and users cannot be set by the smartphone application and must be set through the website using the Master User / PIN code only.

Changing User Codes

1. Click the **Users** link in the left-hand column of the screen.
2. To edit a user, select an existing user to edit.
3. To add a new user, select "+Add New User" to add a user that can control the system via the Web/APP and on a keypad, if installed.

RISCO
Creating Security Solutions
since 1988


Overview
Security
Cameras
Detectors
Automation
Event History
Users
System Settings
Logout

← Close


USERS

USERS & PERMISSIONS FOLLOWERS

+ Add New User + Add New CP User

 Douglas Luscombe (Grand Master)
📞
@ sample63@gmail.com

Michelle (User)

 Michelle (User)
📞
@ sample67@gmail.com

4. Select “+Add New CP User” to add a user that can control the system only via a keypad, if installed.

RISCO GROUP
Creating Security Solutions™

USERS

USERS & PERMISSIONS FOLLOWERS

< Michelle

Personal Details:

Name* Michelle

Email Address* sample67@gmail.com @

Phone Number

Language English (United Kingdom)

Web Password

Change Photo

Security System Access:

Authority Level User

Partitions* Choose partitions...

User Code*

Notifications Edit

Save Cancel Delete

5. Click the arrow to the right of “Authority Level” and select one of the following:
 - **User** – used to set/unset the system.
 - **Set Only** – used only to set the system.
 - **Cleaner** – used only for one-time setting and unsetting.
 - **Duress** – used to unset the system when forced to, in which case it will send out a Duress notification.

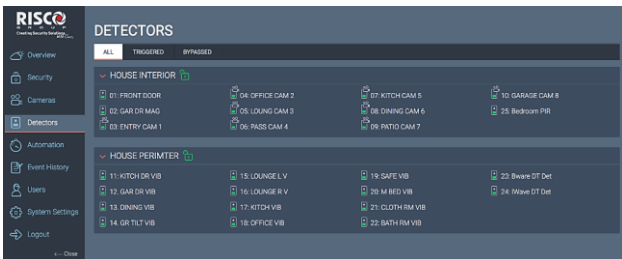
The screenshot shows the RISCO Group web interface. On the left is a dark sidebar with the RISCO Group logo and navigation menu items: Overview, Security, Cameras, Detectors, Automation, Event History, Users (highlighted), System Settings, and Logout. The main content area is titled 'USERS' and has two tabs: 'USERS & PERMISSIONS' (active) and 'FOLLOWERS'. Below the tabs is a back arrow and the text 'New CP User'. The form contains the following fields:

- Personal Details:**
 - Name* (text input field)
- Security System Access:**
 - Authority Level (dropdown menu with 'User' selected and a list of options: User, Arm Only, Cleaner, Duress)
 - Partitions* (text input field)
 - User Code* (text input field)

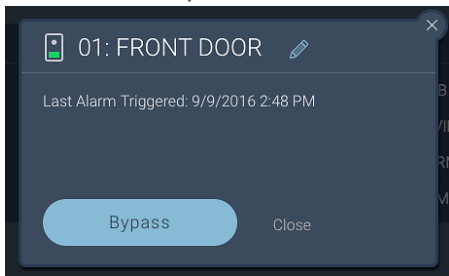
At the bottom of the form are two buttons: 'Save' (blue) and 'Close' (white). A '← Close' link is also present at the bottom left of the sidebar.

Change Zone Labels

1. Click the **Detectors** link in the left-hand column of the screen.



2. Select the detector you wish to edit.



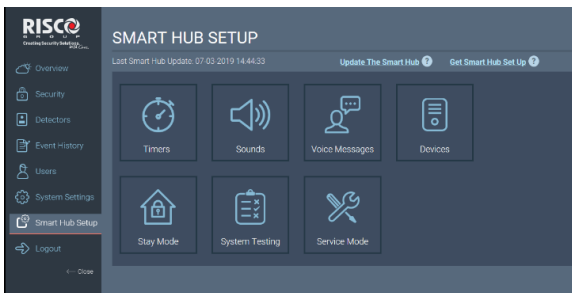
3. Select the pencil icon next to the zone label.
4. Edit the zone label.
5. Click **Close**.

Smart Hub Setup

Smart Hub Setup allows you to configure the parameters of your control panel.

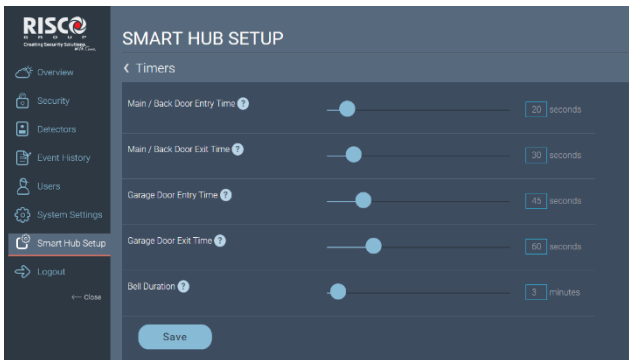
General

1. Click the **Smart Hub Setup** link in the left-hand column of the screen.
2. Before configuring the parameters, click the **Get Smart Hub Setup** link (in the top right of the main Smart Hub Setup screen below) to obtain the current panel parameters.
3. Select from one of the following buttons (options):
 - Timers
 - Sounds
 - Voice Messages
 - Devices
 - Stay Mode
 - System Testing
 - Service Mode



Setup Timers

1. Click the **Timers** button.



2. Define the following:

Main / Back Door Entry Time

The amount of time before the system is set/unset. Usually used on front entrance door: Duration of entry delay 1 before the system is unset.

Main / Back Door Exit Time

Duration of exit delay 1 before the system is set.

Garage Door Entry Time

The amount of time before the system is set/unset. Usually used on back door: Duration of entry delay 2 before the system is unset.

Garage Door Exit Time

Duration of exit delay 2 before the system is set.

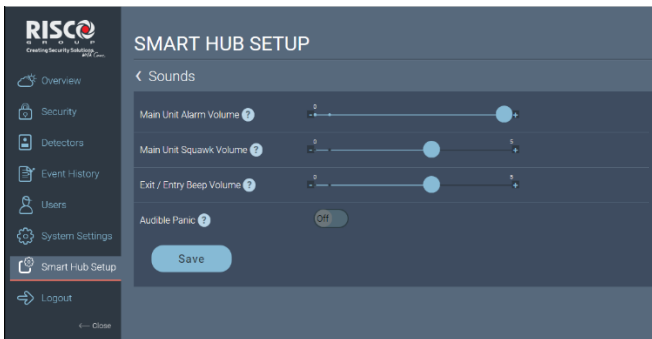
Bell Duration

Specific period of time for the alarm to sound.

3. Click **Save** to save the configuration for this page.

Setup Sounds

1. Click the **Sounds** button.



2. Define the following:

Main Unit Alarm Volume

Sets the main unit's internal speaker Alarm volume. The volume ranges between 0 (silent) to 5 (Max volume).

Main Unit Squawk Volume

Sets the main unit's internal speaker Squawk volume. The volume ranges between 0 (silent) to 5 (Max volume).

Exit / Entry Beep Volume

Determines the volume of the beeps sounded from the main unit during the Exit/Entry times.

Audible Panic

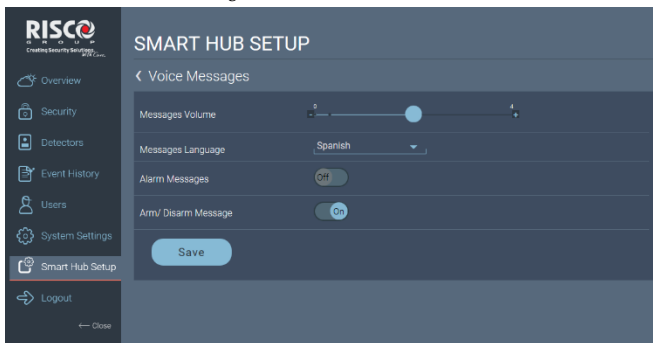
YES: The sirens operate when a panic zone is activated.

NO: No siren operation occurs during a "Panic Alarm," making the alarm truly "silent" (Silent Panic).

3. Click **Save** to save the configuration for this page.

Setup Voice Messages

1. Click the **Voice Messages** button.



2. Define the following:

Messages Volume

Determines the volume of the messages sounded from the main unit.

Messages Language

Sets the system language of the messages.

Alarm Messages

Select between On to sound a message when an alarm is sounded, or Off to not sound a message when an alarm is sounded.

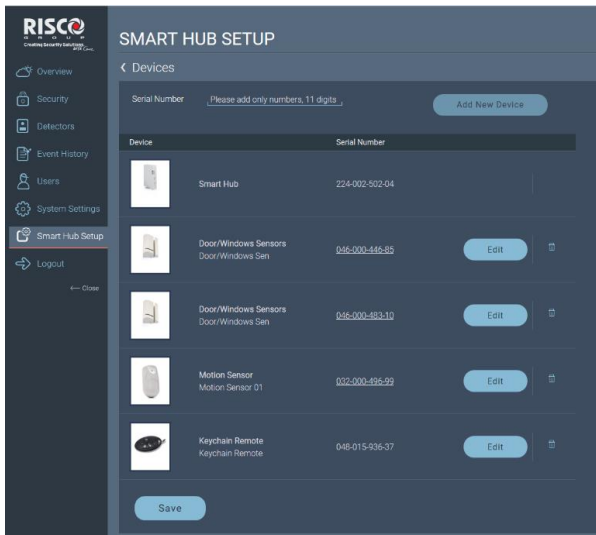
Arm/Disarm Message

Select between On to sound a message when the system is set, or Off to not sound a message when the system is set.

3. Click **Save** to save the configuration for this page.

Setup Devices

1. Click the **Devices** button.



2. To edit device parameters, click the **Edit** button to the right of the device name.
3. To add a new device, under Serial Number (at the top of the screen) enter the device's 11-digit Serial Number and then click the **Add New Device** button (at the top right of the screen). A new screen will open with instructions on how to set-up the device (an example is shown below).



Notes:

1. Additional sensors and accessories supplied and not shown in the list can be entered one at a time by entering the 11-digit Serial Number of each device on the top of the SETUP KIT screen.

2. To remove the device from the system, click the recycle bin icon.

Motion Sensor With Camera 045-000-000-00

- 1 Make sure the serial number printed on the detector is this: **0450000000**
- 2 If batteries supplied separately, then insert batteries as show on the video clip, otherwise, just remove the red divider
- 3 Place the sticker with the number on the back of the detector
- 4 Choose a name for the detector.
For example: Main entrance or Second Floor North
 This field is required
- 5 Select at least one area this detector will be assigned to:
 R1
 R2
 R3
Please select at least one option
- 6 Check this option if you want this detector to be activated after a short delay, allowing you to enter the premises without triggering an alarm
 Enable delayed activation



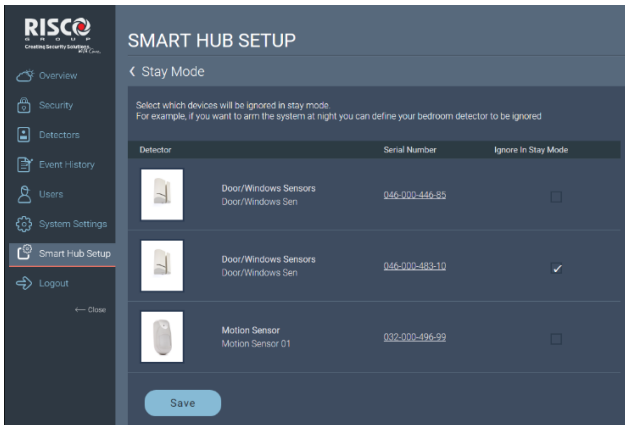
4. After completing all the instructions, click the **Done** button; you will return to the previous screen.
5. Repeat the procedure for the remainder of the devices.

Note: If Setup is not performed, the device will operate with default parameters.




6. After completing the procedure, click **Done**.

Stay Mode

1. Click the **Stay Mode** button.



The screenshot shows the RISCO SMART HUB SETUP interface. On the left is a navigation menu with options: Overview, Security, Detectors, Event History, Users, System Settings, Smart Hub Setup (highlighted), and Logout. The main content area is titled 'SMART HUB SETUP' and 'Stay Mode'. It includes instructions: 'Select which devices will be ignored in stay mode. For example, if you want to arm the system at night you can define your bedroom detector to be ignored'. Below this is a table with three rows of detector information.

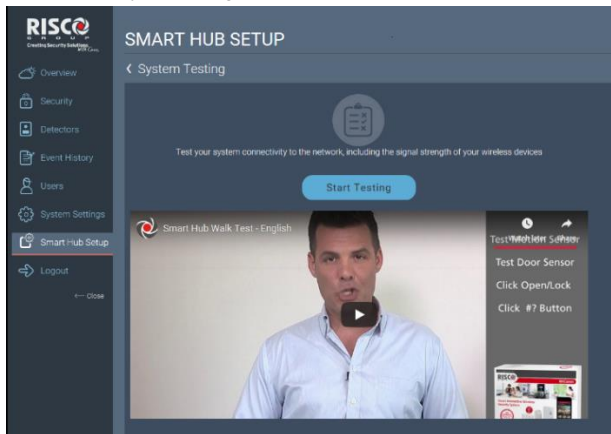
Detector	Serial Number	Ignore In Stay Mode
 Door/Windows Sensors Door/Windows Sen	046-000-446-85	<input type="checkbox"/>
 Door/Windows Sensors Door/Windows Sen	046-000-483-10	<input checked="" type="checkbox"/>
 Motion Sensor Motion Sensor 01	032-000-496-99	<input type="checkbox"/>

At the bottom of the table is a blue 'Save' button.

2. Select the checkboxes of the detectors that will be ignored when set in Stay Mode.
3. Click **Save** to save the configuration for this page.

System Testing

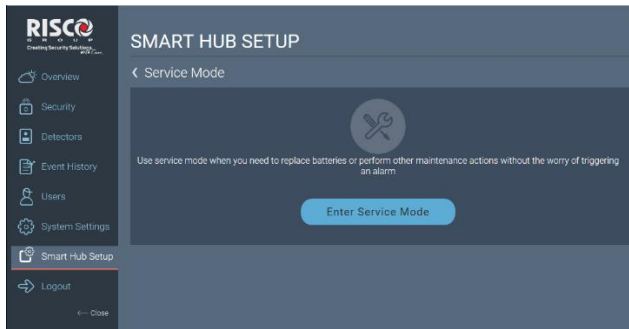
1. Click the **System Testing** button.



2. In the screen that opens, click the **Start Testing** button; all devices in the system will be successively tested for system connectivity.

Service Mode

1. Click the **Service Mode** button.



2. In the screen that opens, click the **Enter Service Mode** button and then replace the battery of the device within the pre-defined by installer time period.

After completing Smart Hub configuration modification, click the **Update the Smart Hub** link (in the top right of the main Smart Hub Setup screen) to update the panel with the configured parameters.

8. User Operations

This chapter describes the user-operational procedures for the WiComm.

User Operational Devices

WiComm can use several operating devices. The most typical ones are listed below.



4 Button Remote Keyfob

Using the 4-button remote control you can set/unset and receive system status messages.



Smartphone App

For Android and iOS, use the iRISCO Smartphone app for system operation and control. Using the App, you can set/unset, visually verify alarms by still images from the PIR cameras, view system status and more.



Slim/LCD Keypad

Using the 2-way keypad with proximity reader (additional purchase, not included in the kit) you can set/unset, operate separate Areas, send a panic alarm, receive system status messages and more.



Web User App

The Web user app (www.riscocloud.com) enables remote monitoring, control and configuration of the system from any location with Internet connectivity. It includes all the capabilities of the iRISCO Smartphone application.

FULL SETTING


FULL SETTING is used when the protected premises is vacated, and all system detectors are therefore activated. After setting, you must exit via the designated exit door within the designated "exit delay" (60 seconds)



Press 



From the Security screen of the App press the


RED  icon on the top of the screen.



Press  / 



From the Security tab click on the RED square

under the FULL SET () column

STAY / PARTIAL Setting


STAY/PARTIAL Setting sets only part of the premises while enabling people to remain on another unset part of the premises.



Press 




From the Security screen of the App press the

YELLOW  icon on the top of the screen.



Press  / 



From the Security tab, click the **YELLOW**
square under the PARTIAL OR STAY ()
column

AREA Setting


In some cases, you may want to divide your property into Areas that can be set and unset separately. For example, if you have a Home Office. There can be up to 3 areas. Each area can be managed as a separate security system that can be set and unset individually, regardless of the condition of the other. The areas can be set at FULL SET or PART SET, one at a time or all at once. Each user can only control the Areas that he has been assigned with.



From the Security screen of the App slide the relevant button of a selected AREA. Each AREA is set individually.

Slide to the right for setting an Area in FULL SET or slide to the left for setting an Area in STAY / PARTIAL.



Press Area number (1-3) followed by  for

FULL SETTING or  for STAY / PART SETTING.

From the Security tab click on the relevant square of each Area. Note that each AREA is set individually. **RED** square is for FULL SETTING and **YELLOW** square is for STAY / PART SETTING. Once selected you will be required to enter in your PIN code.


Note: To set an AREA from the Remote Keyfob please contact your dealer.

Unsetting


Unsetting your system causes the detectors not to trigger an alarm when violated. When entering a set site, a 30 seconds entry delay countdown begins, during which time you must unset the system in order not to activate alarms.

The following table describes how to unset your system when set or when silencing an alarm.



Press  for full system unsetting.



For full unset press, the **GREEN**  icon on the top of the screen.


For Area unsetting slide the relevant button of a selected Area.



Press  /  followed by code or proximity tag attached to the numbers 0 and 9.



From the Security tab:

Full unset: Click on the **GREEN** square under the Unset () column.

Area unset: click on the relevant **GREEN** square for each area and enter your PIN code.

9. Replacing Batteries

Service Mode

Since the wireless devices of your system are battery powered, battery replacement of these devices will be required periodically. Your Smart Hub provides you with a low battery indication for each device that is assigned to the system.

When battery replacement is required, place your Smart Hub into Service mode. This mode is used to silence the tamper alarm initiated by any tamper for a period of 20 minutes. During this time, you can replace batteries without causing a tamper alarm when opening the various devices. There are 2 options for activating the Service mode

a. LCD keypad:

1. From the Grand Master menu, go to **Activities > Advanced > Service Mode**. Once selected, a confirmation message will appear on the LCD screen.
2. Replace the batteries in the relevant detectors. Follow the instructions of each device (refer to the section *Replacing the Battery*).

Note: The Service mode will automatically timeout after 20 minutes. You can also deactivate it by again going to **Activities > Advanced > Service Mode**.

b. Web User Interface:

1. Log into the website at <https://www.riscocloud.com>
2. Click the **Smart Hub Setup** link in the left-hand column of the screen.
3. Click the **Service Mode** button.
4. To start the procedure, click the **Enter Service Mode** button.
5. Replace the batteries in the relevant detectors. Follow the instructions of each device (refer to the section *Replacing the Battery*).

Note: A timer on the screen indicates the time remaining before the system automatically exits the Service mode. If required to exit beforehand, press the **Exit Service Mode** button at the bottom of the screen.

Battery Replacement of Door / Window Detector

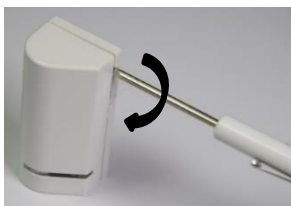
Enter Service Mode and then follow the following procedure.

1. Release screw using a Phillips screwdriver (A) and then insert a flathead screwdriver into the slot and twist to open cover (B).

(A)



(B)



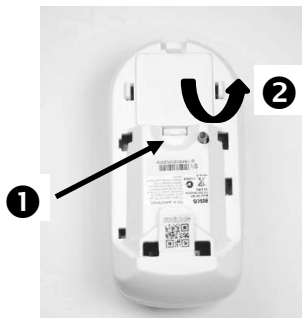
2. Insert the battery while observing + - polarity.



3. Put back cover firmly into place and secure with screw.



Battery Replacement of PIR Detector



1. Press in the tab and lift to open the battery compartment cover.



2. Insert the batteries while observing + - polarity.



3. Slide back cover into place and secure with screw.

For battery replacement of other devices, refer to the specific device installation instructions.

10. Technical Specifications

Electrical	
Electrical power requirement	100-240V, 50/60 Hz 0.9A
Power consumption (at main panel)	Typical 14.4VDC 0.15A – 2.5A
Backup battery	7.2V,NiMH,1.8Ah
Environmental	
Operating Temperature	-10°C – 55°C (14°F to 131°F)
Physical	
Dimension	182mm X 135mm X 40mm
Wireless	
Frequency	433.92 MHz, 868.65MHz, 869.525MHz, 915MHz, 916MHz
Power Output	Security 868.65MHz: 10mW Camera 869.525MHz: 100mW

11. Standard Compliance

Model	Description
RW232M	FCC-ID: JE4RW232M915 Contains FCC ID:QIPEHS6 IC: 6564A-RW232M Contains IC :7830A-EHS6 Frequency:915Mhz ,916Mhz
WL 132KF1	FCC ID: JE4WL132KF1915 IC: 6564A-WL132KF1 Frequency: 915 MHz
RWX73F	FCC ID: JE4RWX73F915 IC: 6564A-RWX73F Frequency: 915 MHz
RWX95P	FCC ID: JE4RWX95915 IC: 6564A-RWX95 Frequency: 915 MHz
RW132KL1P RW132KL2P	FCC ID: JE4RW132KLXP1356 Contains FCC ID: JE4STAMP915 IC: 6564A-RW132KL2P Frequency: 915 MHz, 13.56 MHz
RW132KPPW3	FCC ID: JE4RW132KPP1356 Contains FCC ID: JE4STAMP915 IC: 6564A-RW132KPPW3 Frequency: 915 MHz, 13.56 MHz
RWX34S	Contains FCC ID: JE4STAMP915 Frequency: 915 MHz
RWX35S	FCC ID: JE4RWX35S915 Frequency: 915 MHz
WL S42	Contains FCC ID: JE4STAMP915 IC: 6564A-WLS42 Frequency: 915 MHz

Model	Description
RWT6G	FCC ID: JE4RWT6G915 IC: 6564A-RWT6G915 Frequency: 915 MHz
RWT6F	FCC ID: JE4RWT6F915 IC: 6564A-RWT6F Frequency: 915 MHz

RED Compliance Statement: (Models: RW232M8B, RW232M8C, RW232M87)

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.

IC Warning (Model: RW232M)

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) This device must accept any interference, including interference that may cause undesired operation of the device. The distance between user and product should be no less than 40cm.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement la distance entre l'utilisateur et les produit devraient être au moins 40 cm.

FCC Note (Model: RW232M)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a different circuit from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
- The distance between user and device should be no less than 20cm

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

- (1) This device may not cause harmful interference, and
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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 privity with, any recipient of a product.

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

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

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

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

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

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

RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT

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

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

RISCO does not guarantee that the product will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product will in all cases provide adequate warning or protection.

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

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

Contacting RISCO Group

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

Belgium (Benelux)

Tel: +32-2522-7622

support-be@riscogroup.com

Israel

Tel: +972-3-963-7777

support@riscogroup.com

United Kingdom

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

support-uk@riscogroup.com

China (Shanghai)

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

support-cn@riscogroup.com

Italy

Tel: +39-02-66590054

support-it@riscogroup.com

USA

Tel: +1-631-719-4400

support-usa@riscogroup.com

France

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

support-fr@riscogroup.com

Spain

Tel: +34-91-490-2133

support-es@riscogroup.com



© RISCO Group 01/2021. All rights reserved.

5IN2541 D