RISCO
A LIFETIME OF SECURITY

LightSYS Air

Quick Installer Guide

See the *LightSYS Air Installation and Programming Manual* at **www.riscogroup.com** for additional, detailed information.

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

Contents

INTRODUCTION 4

GETTING STARTED 4

Main Steps for Initial System Setup 4

IMPORTANT SAFETY PRECAUTIONS 5

INSTALLATION 6

Step 1: Creating a Plan for Mounting the System 6

Main Panel Mounting Guidelines 6

To Install the Main Panel 6

Step 2: Wiring, Settings, and Module Installations at the Main Panel 10

Installing Plug-In Communication Module 10

Installing a GSM Module 10

Installing a SIM Card 10

Connecting to IP 10

Connecting to Wi-Fi 10

SYSTEM INITIALIZATION, DEVICE ALLOCATION, GENERAL SYSTEM CONFIGURATION 11

Step 1: Working with the Keypad and Installer Menus 11

Describing Dynamic Keypad Menus 11

Table of Menu Navigational Keys 11

Designating Labels 12

Entering the Installer Programming Menu at Initial System Setup 12

Step 2: Powering-Up and Initializing the System 12

Initial System Power-Up and Language Selection 13

Defining Partitions after Initialization 14

Configuring Communication Modules 14

Entering or Deleting a SIM Card PIN 14

Defining APN Automatically and Manually 15

IP/Wi-Fi 15

Setting Dynamic IP / Static IP 15

Step 3: Allocating Wireless Devices 16

Quick Allocation of all Devices 16

Access Point Mode 18

Allocation of Wireless Devices via RF Transmission 28

Step 4: Advanced Zone Configuration for Wireless Zones 29

Measuring Background Noise Level and Defining its Threshold Limit 29

Performing a Wireless Comm. Test for Measuring Signal Strength 30

Step 5: Configuring System Communication 31

Defining Primary Communication Channels & Parameters 31

Defining Communication with the Monitoring Station 32

Enabling Monitoring Station Communication 32

Defining Monitoring Station Account Parameters 32

Step 6: Configuring Cloud Connectivity 33

Enabling / Disabling Cloud Communication 33

Defining RISCO Cloud Connectivity 33

Step 7: Configuring Common System Parameters 34

Defining System Users 34

Defining User Codes 34

Changing the Default Installer Code 34

Changing the Default Grand Master Code 35

Defining Follow Me Destinations 35

Enabling Follow Me 35

Defining Follow Me Parameters 35

Defining System Timers 35

INSTALLER PROGRAMMING 36

Step 1: Defining Additional Parameters in the Installer Programming Menu 36

Step 2: Exiting Installer Programming Menu after Initial System Configuration 36

Step 3: Defining Parameters in other Installer Menus 36

Step 4: Main Panel Initial Settings 37

TESTING THE SYSTEM 38

INSTALLER RESPONSIBILITIES FOR ASSISTING CLIENTS 38

TECHNICAL SPECIFICATION 39

Introduction

The LightSYS Air supports IP or 4G plug-in multi-socket communication modules that provide multiple, simultaneous communication channels for direct communication, and for communication via the Cloud.

Getting Started

This guide covers the main tasks required to install and set up the LightSYS Air system. Installation and setup should be performed by a professional alarm system installer. For additional comprehensive details, refer to the *LightSYS Air Installation and Programming Manual.* For installation procedures of system detectors and accessories, refer to the instructions packaged with each respective device.

Main Steps for Initial System Setup

INSTALLATION

Step 1: Creating a Plan for Mounting the System
Step 2: Wiring, Settings, and Module Installations at the Main Panel

SYSTEM INITIALIZATION, DEVICE ALLOCATIONS & GENERAL SYSTEM CONFIGURATION

Step 1: Working with the Keypad and Installer Menus
Step 2: Powering-Up and Initializing the System
Step 3: Allocating Wireless Devices
Step 4: Advanced Zone Configuration for Wireless Zones
Step 5: Configuring System Communication
Step 6: Configuring Cloud Connectivity
Step 7: Configuring Common System Parameters

INSTALLER PROGRAMMING

Step 1: Defining Additional Parameters in the Installer Programming Menu
Step 2: Exiting Installer Programming Menu after Initial System Configuration
Step 3: Defining Parameters in other Installer Menus

TESTING THE SYSTEM

INSTALLER RESPONSIBILITIES FOR ASSISTING THE CLIENT

Important Safety Precautions

⚠ **WARNING:** Installation or usage of this product that is not in accordance with the intended use and manufacturer instructions can result in damage, injury or death. The system is NOT meant to be installed or serviced by those other than professional security alarm system installers.

⚠ **WARNING:** Make sure this product is not accessible by those for whom operation of the system is not intended, such as children.

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

⚠ **WARNING:** Coming into contact with 230 VAC can result in death. If the main panel is open while it is connected to the electrical power supply, do not touch any AC electrical wiring.

⚠ **WARNING:** Replace only detector and accessory batteries as needed, and with the correct type to avoid the risk of explosion. Do not replace the main panel backup battery – call a professional alarm system installer.

⚠ **CAUTION:** Dispose of batteries according to applicable law and regulation.

Installation

Step 1: Creating a Plan for Mounting the System

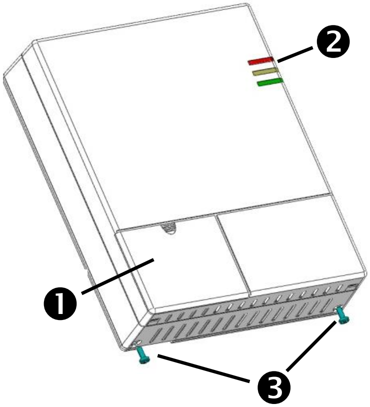
Main Panel Mounting Guidelines

Before you mount the main panel and peripheral components, make a plan for obtaining the most optimal location for the panel, which (depending on configuration-specific requirements) should typically be:

- In a location with good GSM reception
- In a secure location that is hidden and not reachable by those for whom use is unintended (such as small children)
- Near an uninterrupted 230 VAC electrical outlet, an easily accessible disconnection device such as a circuit breaker (if permanently connected to the electrical power supply), grounding connection, and network cable outlet, as needed
- In a dry place, away from sources of electrical and RF disturbance, and not near large metal objects which may hinder reception

To Install the Main Panel

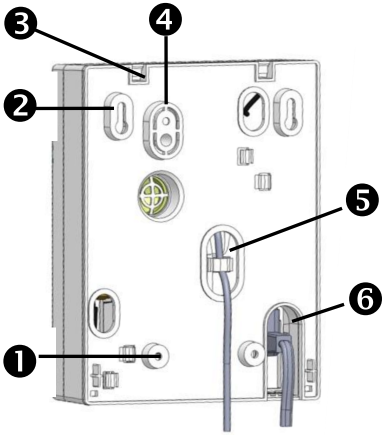
1. Disconnect the mounting bracket (back cover of main panel) by releasing the two locking screws at the base of the unit, and then lifting the unit upward to detach the two tabs from the respective grooves on the mounting bracket:



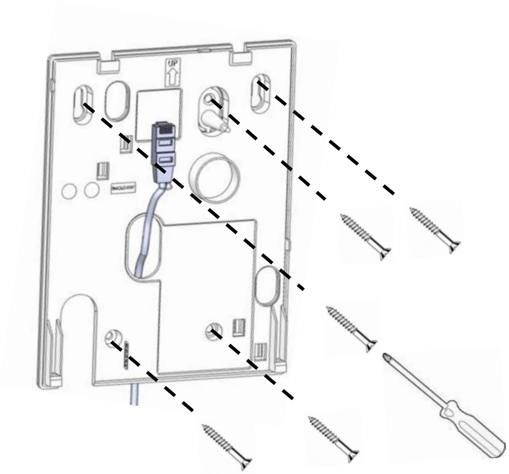
❶	Front access cover
❷	LED indicators
❸	Locking-screws (2)

Main Panel Indication LEDs			
	Color	**State**	**Status**
Power LED	Green	ON	Power OK
	Red	ON	AC trouble
	Orange	ON	Battery trouble.
Status LED	Red	ON	System armed (Away or Stay)
		Rapid flash	Alarm
		Slow flash	System is in exit delay
	Green	ON	System ready
		Slow flash	System in Exit/Entry delay with front door open
		Off	System not ready for arming
	Orange	ON	System Trouble
Communication LED	Green	ON	Cloud connected
		Slow flash	GSM/IP OK
	Orange	Slow flash	GSM/IP Trouble
All LEDs	Green	Sequence flash	Wireless Learn mode
All LEDs	Orange	Slow flash	Battery Replacement mode (service mode)
All LEDs	Green	Slow flash	System in installation Mode/System in upgrade mode
All LEDs	Green → Red	Slow flash	Access Point Mode
All LEDs	Green	Rapid flash	Accessories Upgrade Mode

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 *8*.

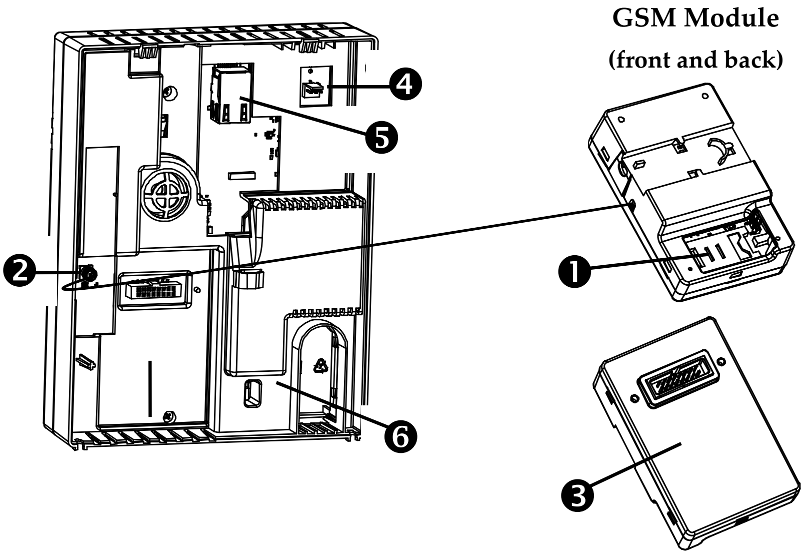


Mounting bracket – back side



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 power cable (cable is installed onto the back of the panel only after the mounting bracket is secured to the wall)



❶	SIM holder on GSM module
❷	Connect the wire from the GSM Module to the GSM antenna connector located on the main unit
❸	GSM module
❹	Not used
❺	Network cable connector on IP (shown with cable connected)
❻	Power cable (shown installed from the back of the main panel)

3. 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.
4. Insert the SIM card into its holder, as required.
5. Attach the antenna onto its connector on the GSM module.
6. 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.

7. Route the power cable through the opening in the housing (back cover), and secure its plug onto the socket.

NOTE: The backup battery takes 24 hours to charge.

8. 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.
9. Install the two locking screws at the bottom of the main panel.
10. Connect the main panel to the AC power supply.

Step 2: Wiring, Settings, and Module Installations at the Main Panel

Installing Plug-In Communication Module

⚠ **CAUTION:** Before installing any communication or audio module, in order to prevent damage to system components, make sure the main panel is NOT powered up, and that the panel's backup battery is DISCONNECTED.

NOTE: See the installation instructions included with each module for module connection locations on the PCB. Also see the *LightSYS Air Installation and Programming* manual for further details.

Installing a GSM Module

GSM modules provide data communication over a cellular network. The G2 and G4 GSM modules provide generation 4 GSM communication.

- Install according to the instructions packaged with the module.

Installing a SIM Card

- For GSM communication, install a SIM card in its holder on the GSM module. Later during installer programming, you can enter /disable the PIN and define the APN.

Connecting to IP

IP provide data communication over TCP/IP.

Connect the incoming LAN cable to its jack on the IP onboard. Make sure that the cable is connected to the network.

Connecting to Wi-Fi

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

1. To connect via Wi-Fi network, you must select your Router's Wi-Fi network.
2. Go to Activities –> Wi-Fi screen: available networks appear in a list.
3. Select the desired network and enter the password (if required).

System Initialization, Device Allocation, General System Configuration

For installer programming using the Configuration Software, see its documentation.

Step 1: Working with the Keypad and Installer Menus

Describing Dynamic Keypad Menus

The LightSYS Air installer menus and user menus are dynamic, in that they display menu items according to the devices connected in the system.

Table of Menu Navigational Keys

The following describes the typical WL Panda keypad keys used for programming:
NOTE: Other keypad buttons may differ – see their packaged instructions.

Key	**Description**
1—0	For entering codes, using quick keys (to quickly access a menu option, labels, and for entering other numeric values).
⚙↩	To go back a step in the menu, to exit a menu or return to the beginning of a menu.
⇅ⓘ	Long-press to get system status
OK	Confirm (after entering) / OK / Save
⇅ⓘ ⇅	For scrolling through menus and menu options, and for toggling, such as between "ON" and "OFF" options.
🔒 🏠	To toggle between options
A, B, C, D	Used to select a group

Designating Labels

The following table describes all the available characters at the WL Panda keypad.

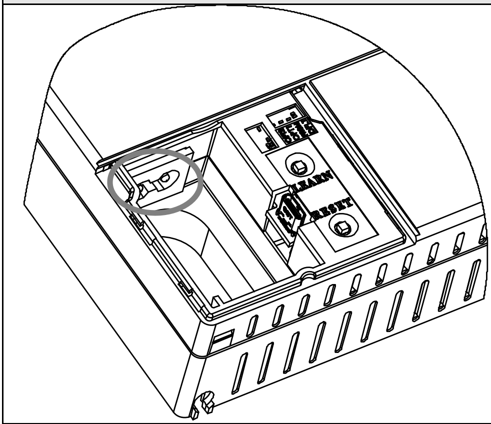
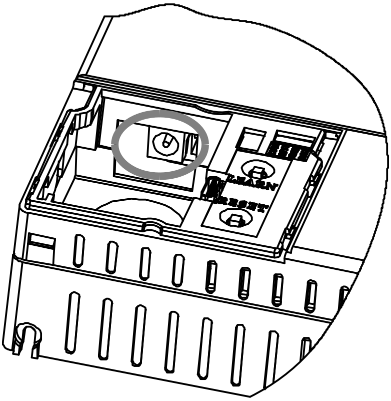
Key	Character Options	Key	Character Options
1	1 . , ‘ ? ! \ “ — < > @ / : _ + * #	7	7 P Q R S
2	2 A B C	**8**	8 T U V
3	3 D E F	**9**	9 W X Y Z
4	4 G H I	**0**	0 (also use for blank space)
5	5 J K L	**A**	To toggle between lower case and capital letter
6	6 M N O	🏠 🔒	To scroll through all possible characters, to toggle through options (Yes/No)

Entering the Installer Programming Menu at Initial System Setup

After initial system power-up, language, time and date setting, viewing enabled zones and defining system partitions, you’ll be in the Installer Programming menu, at Auto Settings.

IMPORTANT: After you finish initial system setup programming tasks from the Installer Programming menu, in order to exit you must perform the procedure for *Step 2: Exiting Installer Programming Menu after Initial System Configuration*, page *36.*

Step 2: Powering-Up and Initializing the System

Configuration A: **AC Connection**	**Configuration B:** **DC Connection**
	

You must initially allocate the Panda Keypad or Panda Keyfob to the main panel.

To enter local programming mode:

1. Open the AC/DC connection cover and press the LEARN button for 3 seconds. The unit beeps once and enters “Learn” mode; the LEDs light up in Green one after the other.
2. Send a Write message by pressing both keys, 🔒 🏠 (Panda Keypad) / 🔒 🏠 (Panda Keyfob), simultaneously for at least 2 seconds. the keypad will sound a confirmation beep and the system will beep to acknowledge.
3. To exit "Learn" mode, short-press the LEARN button; the unit beeps once and the LEDs stop flashing.

When a new system is powered-up the first time, here are the initialization steps:

1. Initial power-up & language selection. The system automatically connects to the Cloud.
2. View enabled zones, define the maximum number of system partitions, and set the time & date.

Initial System Power-Up and Language Selection

NOTE: During regular system operation (after initial system setup) the language can be subsequently changed by pressing ⚙↩ + **9** simultaneously.

➢ **To initially power-up and select a language:**

1. Power-up the main panel; the keypad panel takes a few seconds to initialize (there may be an automatic 3-minute upgrade that runs automatically, during which the upgrade and power icons may display on the keypad **– make sure you do not disconnect**).
2. Press ⚙↩ when prompted.
3. Scroll to select a language, and then press OK.

Defining Partitions after Initialization

- **To define the partition quantity after system initialization:**

1. Go to: **1 > 5 > 7 (System > Settings > Partition Qty,** and then press OK; MAXIMUM PARTITIONS? 08 (08—32) displays.
2. Enter the maximum number of partitions to enable in the system – the default is 08 (meaning up to 8), but up to 32 can be selected. If you want more than 8 partitions, enter the number. Now press OK.

NOTE: You can opt to define the maximum partitions at a later stage – from the keypad (during installer programming), or from the Configuration Software.

Configuring Communication Modules

Entering or Deleting a SIM Card PIN

If your SIM card requires a PIN (personal ID number) you will need to enter it. If not, you will need to disable it.

- **To enter or delete a SIM card PIN:**

1. From the **Installer Programming menu** select **5 > 1 > 2 > 5 > 1,** enter the PIN, and then press OK.

   -OR-

   If a PIN is not needed, you can choose to disable it by inserting the SIM card in a cell phone and disabling the code.
2. You can manually define APN definitions if you don't have them configured automatically (the default). See *Defining APN Automatically and Manually,* page *15.*

   NOTE: It is recommended to test the operation of a SIM card by conducting a call and testing the GSM signal strength. See *Testing the System,* page *38.*

Defining APN Automatically and Manually

NOTE: When using a RISCO SIM card, LightSYS Air version 3.4.1 and above supports connection by Auto APN to: “risco.tele2.com” / “iot.tele2.com" or to “m2m.tele2.com”.

After the SIM card is installed and upon establishing GSM/GPRS communication, the system’s auto-APN feature will automatically configure the APN definitions. However, there may be cases where you will need to manually define the APN by entering the APN (Access Point Name) code supplied from the cellular provider, user name, and password.

NOTE: If any of the APN definition fields are populated manually, the auto-APN feature will not operate.

➢ **To manually set the APN definitions:**

1. From the installer Programming menu, select: **5 > 1 > 2 > 2 > 1** **(Communication > Method > GSM > GPRS > APN code),** then press OK.
2. Enter the **APN code,** and then press OK.
3. Scroll to **2) APN User Name**, press OK, enter the **user name,** and press OK.
4. Scroll to **3) APN Password,** press OK, enter the **password,** and press OK.

IP/Wi-Fi

Setting Dynamic IP / Static IP

Go to: **5 > 1 > 3 > 1 > 1,** scroll to either **1) Dynamic IP** or **2) Static IP,** then press OK**.**

Step 3: Allocating Wireless Devices

Quick Allocation of all Devices

Quick Allocation of all Devices at the Main Panel using LEARN Button

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

Function	Description
LEARN Button	Used for local allocation of wireless devices. To enter local programming mode, press the button for 3 seconds. The unit beeps once and enters “Learn” mode. The LEDs light up in Green one after the other. To exit "Learn" mode short-press the LEARN button; the unit beeps once and the LEDs stop flashing.
Panel RESET	Press and hold the RESET button for 20 seconds.
Panel Power Off	Remove the AC Power and press and hold the RESET button fora 20 seconds.
Front Tamper Switch	Used to indicate tamper alarm when opening the front cover.
USB Type-C Connctor	Use this connector for local programming using the configuration software.

Quick allocation is possible only in Disarm Mode. Attempting to enter during Arm will respond with error beeps.

To perform quick device allocation at the main panel:

1. Press 3 sec the LEARN button; each Green LED on the main panel will light up one after another, indicating the system is in “Learn mode.”

   NOTES:

   - The panel will sound each time you enter or exit the Learn mode.
   - During Learn mode the status shown on the keypad is “System in RF Allocation Mode”.
   - There is no Alarm during Learn mode.

2. Make sure batteries are installed in each device before allocating. For detectors, also make sure the covers are removed so the tamper switches are accessible.
3. Send a signal transmission from each device per the table below (if a device is not listed on the chart, refer to the device’s specific instructions); the main panel beeps once to accept or three times to reject. Once accepted the system announces the device type and its assignment (for example, “Detector, zone 1”). Each device receives an index number from the system, and zones are assigned automatically (and sequentially, in the order allocated).

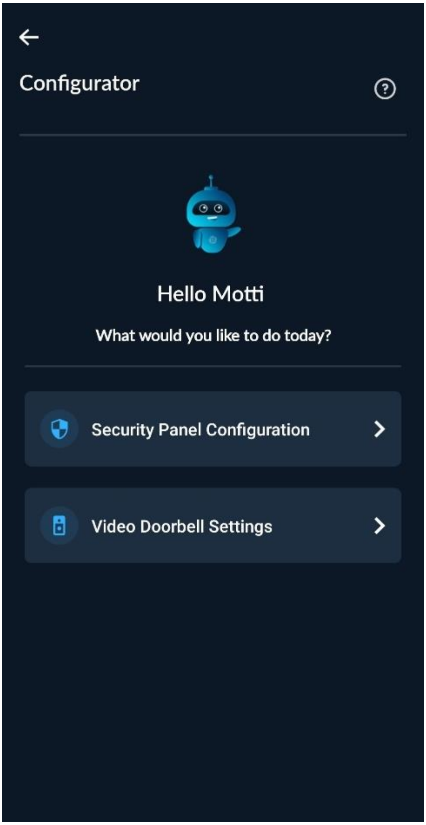
   NOTE: For future use, it is recommended to write down the device assignment / zone and installation location of each allocated device.

Access Point Mode

This feature enables the setup of the WiFi connection of the LightSYS Air panel that is configured without a keypad to the local network using the Handy App application.

Connecting the Control Panel to the Local Network

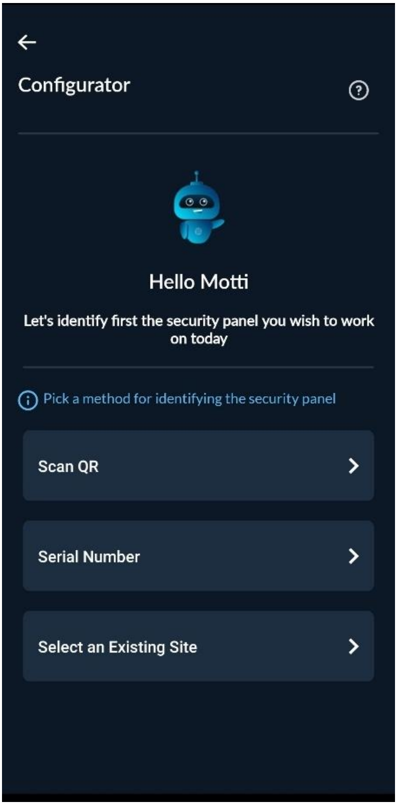
1. Open the Handy App Application.
2. From the menu, select "Configurator".
3. Select "Security Panel Configuration".



Hello Motti

What would you like to do today?

4. Select "Scan QR" and scan the Panel's QR Code or select "Serial Number" and enter the Panel's Serial Number.



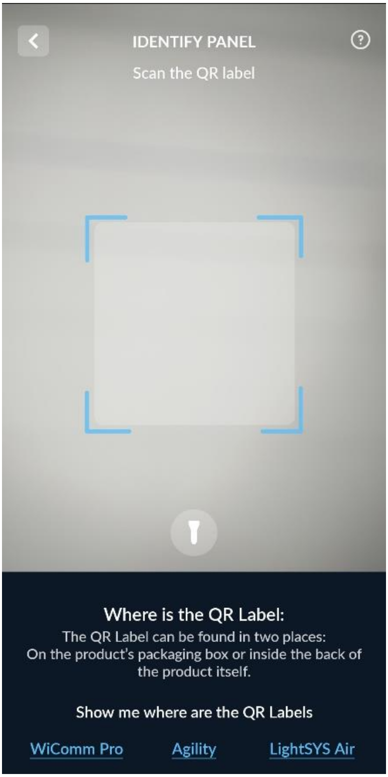
Configurator

Hello Motti

Let's identify first the security panel you wish to work on today

Pick a method for identifying the security panel

If the Scan QR option is selected, the following screen is displayed.



IDENTIFY PANEL

Scan the QR label

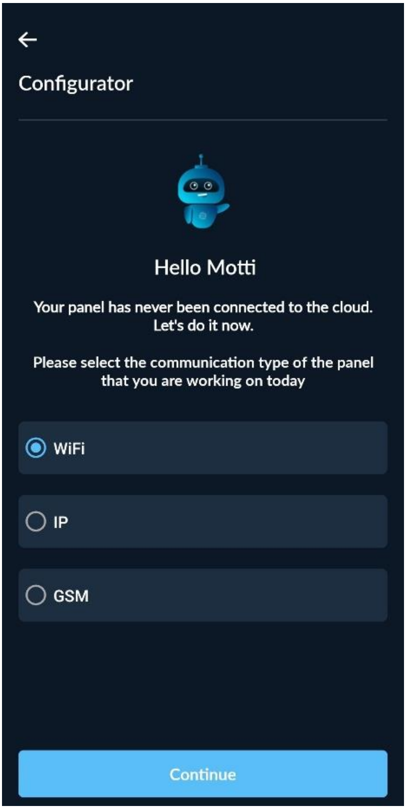
Where is the QR Label:

The QR Label can be found in two places:
On the product's packaging box or inside the back of the product itself.

Show me where are the QR Labels

Note: *To locate the QR Code, under "Show me where are the QR Labels" click "LightSYS Air".*

5. Click the "Next" button and then select the "WiFi" option.



Configurator

Hello Motti

Your panel has never been connected to the cloud. Let's do it now.

Please select the communication type of the panel that you are working on today

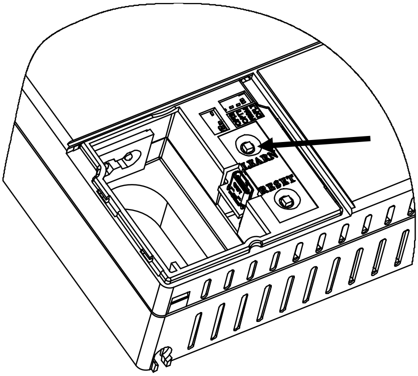
● WiFi

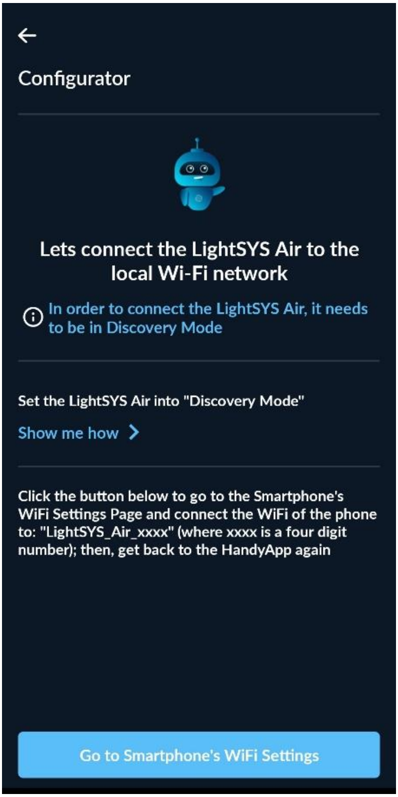
○ IP

○ GSM

Continue

6. Click the “Continue” button.
7. Allocate system devices remotely through the Access Point. Press the LEARN button for 10-15 sec; the panel will beep once. Wait until a second beep is heard indicating the system is in “Access Point mode”; all three LEDs flash green and then red.





Configurator

Lets connect the LightSYS Air to the local Wi-Fi network

In order to connect the LightSYS Air, it needs to be in Discovery Mode

Set the LightSYS Air into "Discovery Mode"

Show me how

Click the button below to go to the Smartphone's WiFi Settings Page and connect the WiFi of the phone to: "LightSYS_Air_xxxx" (where xxxx is a four digit number); then, get back to the HandyApp again

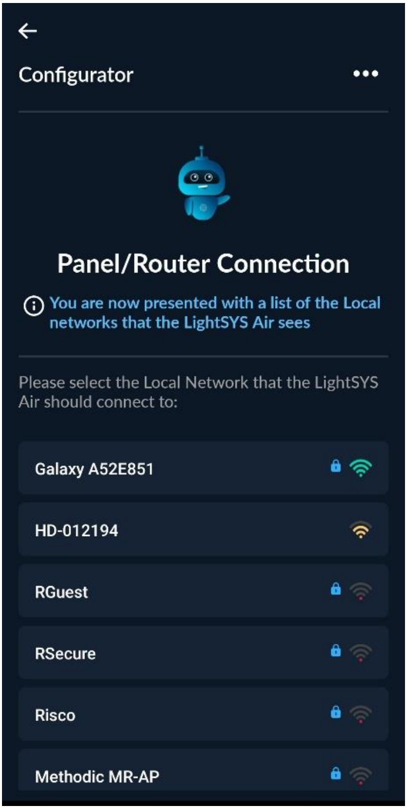
8. Click the "Go to Smartphone's WiFi Settings" button and connect the Wi-Fi to "LightSYS_Air_xxxx".where "xxxx" is the last four digits of the panel's ID No. A list of local networks will open that the LightSYS Air "sees".

9. Select the "LightSYS_Air_xxxx" network; the password is "Riscoyyyy" where "yyyy" is the Grand Master Code. For example, in the default panel the password is "Risco1234".

10. Return to the HandyApp Configurator.

Connecting to a Panel Network

1. When prompted by the App, connect the panel to a local network by selecting the network that was scanned via the panel.



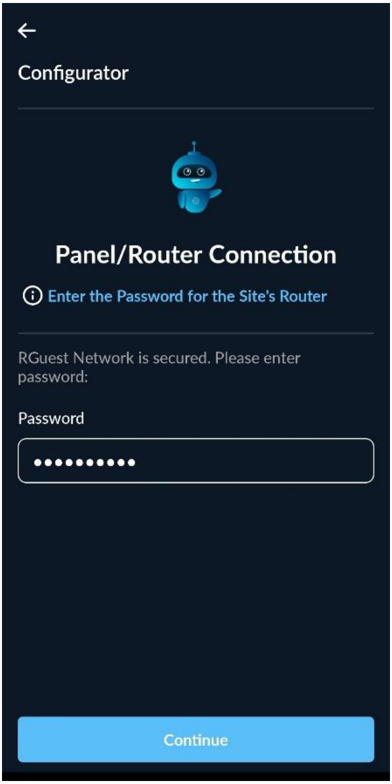
Panel/Router Connection

ⓘ You are now presented with a list of the Local networks that the LightSYS Air sees

Please select the Local Network that the LightSYS Air should connect to:

- Galaxy A52E851
- HD-012194
- RGuest
- RSecure
- Risco
- Methodic MR-AP

2. Enter the password of the local network.
3. Click the "Continue" button.



Configurator

Panel/Router Connection

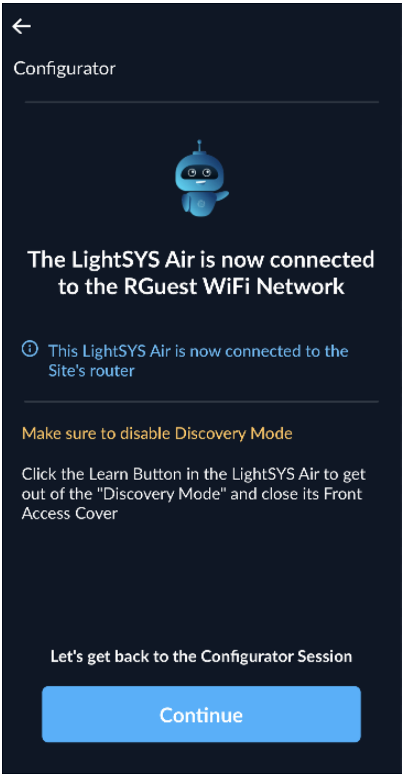
Enter the Password for the Site's Router

RGuest Network is secured. Please enter password:

Password

●●●●●●●●●●●

When connected successfully, the following screen is displayed.



The LightSYS Air is now connected to the RGuest WiFi Network

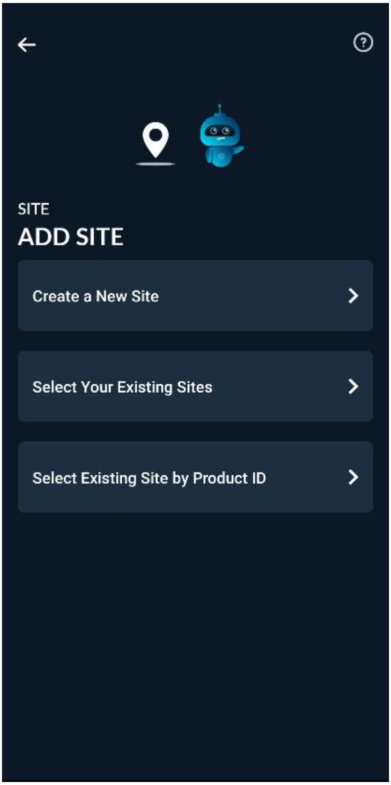
ⓘ This LightSYS Air is now connected to the Site's router

Make sure to disable Discovery Mode

Click the Learn Button in the LightSYS Air to get out of the "Discovery Mode" and close its Front Access Cover

Let's get back to the Configurator Session

4. Click the “Continue” button.



SITE

ADD SITE

Create a New Site
Select Your Existing Sites
Select Existing Site by Product ID

5. Select one of the following options:
    - Create a New Site
    - Select existing sites
    - Select an existing site by entering a Product ID of a RISCO product.

NOTE: The above screen will not appear when the panel that is connected to the cloud is an existing panel that is already in a site. In such a case, the details of the site are displayed.

Table of Device Transmissions

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

6. 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.

   Timeout - In case of no activity (no allocation) more than time defined by "Service Time" timer, the system exits Automatically from Learn Mode.

Each wireless transmitting device must be allocated (via keypad or Configuration Software) by either sending an RF transmission (see below), or by entering the device's 11-digit code (see the *LightSYS Air Installation and Programming Manual*).

Allocation of Wireless Devices via RF Transmission

- **To allocate wireless devices via RF transmission (from the WL Panda keypad):**

1. From the **installer Programming menu,** go to **7> 2> 2> 1 > 1 (Install > WL Device > Allocation >By RF > Zone).**
2. Each zone appears in one of the following formats: "**Select (—:——:————)"** which indicates the zone is available for allocating, or "**Select (B1:WME01 SN:XXXX)"** which, in this example, indicates the zone has already been allocated.

   NOTE: If you try to allocate the same wireless zone number twice, the second allocation will re-write (cancel) the prior allocation.
3. Scroll to the zone number you want to allocate (or enter the zone number using 3 digits – for example enter 022 for zone 22), and then press OK; the wireless expander is now in "learn" mode for the next 180 seconds.
4. Per the Table of Device Transmissions above, within the remaining time, send an RF transmission from a wireless device that you want to sync with the selected wireless expander. If *"write message not found"* displays, it means the transmission was not received and the device was not allocated.
5. Repeat from step 3 for each additional wireless transmitting device to be allocated for this wireless expander.
6. After you have allocated the devices for this specific wireless expander, repeat the procedure from step 2 for all additional wireless expanders (and then their respective transmitting devices).
7. Now define the basic parameters for the wireless zones, such as labels, partitions, etc.
8. After, it may be beneficial to perform advanced programming such as measuring and setting the background noise threshold level, followed by performing a wireless communication test (see *Performing a Wireless Comm. Test for Measuring Signal Strength,* page *30).*

Step 4: Advanced Zone Configuration for Wireless Zones

- **Configuring advanced parameters for wireless zones:**

1. At the **installer Programming menu,** go to: **2>1>2>7>5 (Zones > Parameters > By Category > Advanced > WL Parameters),** and then press OK.
2. Enter the wireless zone number to program, and then press OK.
3. Scroll through and configure the relevant parameters for the zone, pressing OK after each to confirm.

Measuring Background Noise Level and Defining its Threshold Limit

If the system uses wireless devices, you can measure ("calibrate") the background noise that the main panel detects, and also define the acceptable threshold value. Background noise (RF interference) is typically generated by other non-system devices operating in close proximity to the system, and high amounts may interfere with the system, causing "jamming." Communication between your system's wireless devices (via wireless expander module/s) and the main panel must be stronger than any detected background noise at the main panel, therefore regardless if the current level of background noise the panel detects seems insignificant, it is recommended to additionally perform a Wireless Communication Test, to check a wireless device's signal (see *Performing a Wireless Comm. Test for Measuring Signal Strength*, page *30*).

Measuring the background noise level provides an indication whether the main panel is mounted at a good location, and defining the threshold limit 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 less sensitive the system will be (it will report jamming events less frequently).

- **To calibrate (measure) the background noise:**

1. From the **installer Programming menu,** select **7 > 2 > 1 (Install >WL Device > RX Calibration)**; select receiver.
2. To re-calibrate (re-measure) the background noise, press ⌂ to toggle to **Y** (yes), and then press OK; the new result ("NEW THOLD") displays.
3. Press OK to confirm. If the resulting value is not acceptable, for example if it is high due to what you believe is a source of high background noise that's

inherent to the main panel's location, then you may want to move the main panel to a better location. Another option you may consider is to re-define the noise level threshold value (see below) – for example, so the system will be more "forgiving" and generate fewer jamming events.

➢ **To define the noise level threshold value:**

1. From the **Installer Programming menu**, select **7 > 2 > 1 (Install >WL Device > RX Calibration);** CHOOSE RECEIVER (wireless expander) displays.
2. Scroll to select the wireless expander module, and then press OK; the most recently measured result ("THOLD") for that Wireless Expander module displays.
3. Press 🏠 to toggle to **N** (no), and then press OK; the most recently measured result displays again, over which you can now enter a new threshold value (between **01—99**), and then press OK.

Performing a Wireless Comm. Test for Measuring Signal Strength

A Wireless Communication test result (the signal strength between the wireless device and the main panel) must be higher than the background noise measured at the main panel. If the background noise level is higher, you will most likely need to move the wireless device to a better location.

➢ **To perform a Wireless Communication test:**

1. Exit the Installer Programming menu (see *Step 2: Exiting Installer Programming Menu after Initial System Configuration*, page *36*).
2. Ensure all wireless devices are activated.
3. Enter the installer code (default is **1111**), and then press OK.
4. Scroll to **Maintenance**, then press OK; you are in Installer Maintenance menu.
5. Scroll to **Wireless Test**, then press OK; Zones displays.
6. At Zones, press OK; Comm. Test displays.
7. At Comm. Test, press OK.
8. Scroll through all wireless zones to view each of their results. The test results range from **01** (lowest) to **99** (highest), and display as per this example:

```
001 RWX107D  2-W
RSSI:99%
```

EXPLANATION:
001=zone: zone description: 99 = result (signal strength)

Step 5: Configuring System Communication

Defining Primary Communication Channels & Parameters

➢ **To define the primary communication channel:**

1. From **installer Programming menu** go to: **5) Communication menu > 1) Method**
2. Scroll to the primary comm. channel **(GSM** or **IP/Wi-Fi)** then press OK.
3. Scroll through the respective parameters (see table below), and define the relevant ones, pressing OK after each parameter that is set.

NOTES:

- For setting the backup communication channel to the monitoring station, see *Defining Monitoring Station Account Parameters*, page *32.*
- LightSYS Air menus reflect only the communication modules that are installed.
- To establish GPRS communication, a SIM card must be installed.
- For IP communication, you can set it to Dynamic IP or Static IP (see **IP/Wi-Fi**
- Setting Dynamic IP / Static IP, page *15).*

Primary Channel	Parameters
GSM	**1) Timers > 1)GSM Lost, 2)GSM Net Loss, 3)SIM Expire, 4)MS Polling** [Primary, Secondary, Backup] **2) GPRS > 1)APN Code, 2)APN User Name, 3) APN Password** **3) Email > 1)Mail Host, 2)SMPT Port, 3)Email Address, 4)SMPT UserName, 5)SMPT Password** **4) Controls > 1)Caller ID (Y/N), 2)LED Enable (Y/N)** **5) Parameters > 1)PIN Code, 2)SIM Number, 3)SMS Centre PH, 4) GSM RSSI** [Disable, Low signal, High signal] **6) Prepay SIM > 1)Get Credit By** [Credit SMS, Credit Voice, Service Cmnd], **2)PN To Send, 3)PN to Receive, 4)SMS Message**
IP	**1) IP Config > 1)Obtain IP** [Dynamic IP, Static IP], **2)Panel Port**, **3)Panel IP**, **4)Subnet Mask**, **5)Gateway**, **6)DNS Primary**, **7)DNS Secondary**, **8)Wi-Fi Scan**, **9)Add Wi-Fi Net**, **10)WPS Button** **2) E-mail** [Mail Host, SMTP Port, Email Address, SMTP Name, SMTP Password,] **3) Host Name** [Security_System] **4) MS Polling** [Primary, Secondary, Backup]

Defining Communication with the Monitoring Station

You enable and define communication settings for monitoring station account(s), along with the backup communication channel and other associated parameters that define the nature of communication, event reporting and confirmation between the system and the monitoring station. Monitoring station link-up options are via TCP/IP, and GSM/GPRS.

Enabling Monitoring Station Communication

➢ **To enable monitoring station communication:**

1. From **installer Programming menu** go to: **1)System > 2)Controls > 3)Communication > 1)MS Enable.**
2. Press 🏠 to scroll to **Y**, and then press OK.

Defining Monitoring Station Account Parameters

➢ **To define parameters for a monitoring station account:**

1. From **installer Programming menu** go to: **5)Communication >2) MS > 1)Report Type;** MS1 (MS account 1) displays.
2. Scroll to the MS account number you want to define, and then press OK.
3. Scroll to select the reporting type **(IP, SMS, SIA IP)**, and then press OK; the available primary/backup communication channel options appear (according to the primary communication channel already selected).
4. Scroll to select from the primary/backup communication channel options, and then press OK.
   NOTE: If "GSM Only," or "IP Only" is selected, it will not have a backup communication channel.
5. Enter IP Address and IP Port as needed, and then press OK.
6. Go to: **5)Communication** > **2)MS > 2)Accounts,** scroll to select an account number to define, enter its account number, and then press OK.
7. Go to: **5)Communication** > **2)MS > 3)Comm Format**, and then press OK**.** Scroll to select a transmission format **(Contact ID** or **SIA),** and then press OK**.**
8. Go to: **5)Communication** > **2)MS >** scroll to and define other options as needed: **4)Controls, 5)Parameters, 6)MS Times, 7)Report Split, 8)Report Codes**.
9. Repeat the procedure for all other monitoring station accounts used.

Step 6: Configuring Cloud Connectivity

The RISCO Cloud is RISCO's application server that handles all communication between the system, monitoring station, as well as system users (for Smartphone, Web app, and Follow-Me). Cloud communication enables remote monitoring and control of the system, sending event notifications, zone licensing and viewing real time video verification via RISCO's VUpoint IP cameras.

Enabling / Disabling Cloud Communication

The system is Cloud-enabled by default.

➢ **To enable or disable Cloud communication:**

1. From the **installer Programming menu** go to: **1)System > 2)Controls > 3)Communication > 4)Cloud Enable [N/Y].**
2. Press 🏠 to toggle between **Y** and **N** to enable/disable Cloud communication, and then press OK.

Defining RISCO Cloud Connectivity

If using IP and/or GSM modules, you need to define the network connectivity to the RISCO Cloud server.

➢ **To define network connectivity to the RISCO Cloud:**

1. With Cloud communication enabled, from **Installer Programming menu** go to: **5)Communication menu > 5)Cloud**
2. Scroll to, and define parameters for the following as needed (note that customer-specific parameters may differ):
   - **1) IP Address:** (default is **riscocloud.com**)
   - **2) IP Port:** (default is **33000**)
   - **3) Password:** Password for server access (default is **AAAAAA**).
   - **4) Channel:** Select **IP Only, GSM Only, IP/GSM or GSM/IP,** depending on the installed communication modules in the panel.
   - **5) Controls:** Press 🏠 to toggle between **Y** and **N** to enable/disable MS Call All, FM Call All, App Arm, App Disarm, App Exit Delay and Encryption.

Step 7: Configuring Common System Parameters

Defining System Users

The installer or Grand Master must set up permissions for all the system users – the partitions each user is allowed to operate, and the authority level for each user. The installer can designate the code length (see the *LightSYS Air Installation and Programming Manual*). However, the Grand Master will set the actual numerical codes for each user. The installer can also change default installer, sub-installer and Grand Master codes.

Defining User Codes

➢ **To define user codes:**

1. From **installer Programming menu** go to: **4)Codes > 1)User,** then press OK.
2. Scroll to a user's index number (1—128 users possible), then press OK; the user number and "1) Partition" display.
3. Press OK. To assign the partition(s) this user will be allowed to operate, do the following:
   a. While scrolling through each block of 10 partitions, select partition(s) to allow operation by this user by entering a partition number to select it (it will display), or by entering the number again to clear it (it will not display).
   a. When finished selecting all partition numbers press OK.
4. To assign an authority level for this user, do the following:
   a. After assigning partitions (step 3), scroll to **2)Authority,** then press OK.
   b. Press 🏠 to go to the authority level for this user **(User, Arm Only, Maid, Unbypass, Guard, Duress, UO/Door Control, Master)**, then press OK.

Changing the Default Installer Code

The default installer code is **1111.** You can either use this code during system programming, or you can change it.

➢ **To change the installer code:**

1. From the **installer Programming menu** select **4)Codes > 3)Installer,** and then press OK; CODE: 1111 displays.
2. Scroll to each digit and enter a new code, then press OK.
3. Re-enter the new code, and then press OK.

Changing the Default Grand Master Code

The default Grand Master code is **1234,** which can be changed by the installer. Be sure to advise the customer that that after system installation, the primary system user ("Grand Master") should change the Grand Master code to be unique and confidential (refer to the LightSYS Air User Manual).

➢ **To change the default Grand Master code:**

1. From the **Installer Programming menu** select **4)Codes > 2)Grand Master**, and then press OK; **** displays
2. Scroll through the asterisks and enter a new code, and then press OK.

Defining Follow Me Destinations

You can enable and define multiple Follow-Me destinations.
NOTE: The actual telephone numbers and email addresses for FM destinations are defined by the Grand Master in the User menu.

Enabling Follow Me

➢ **To enable using Follow Me destinations:**

- From the **Installer Programming menu** go to: **1)System > 2)Controls > 3)Communication > 2)FM Enable**, use 🏠 to toggle to **Y** to enable (or to **N** to disable), and then press OK.

Defining Follow Me Parameters

➢ **To define parameters for a Follow Me destination:**

1. From the **Installer Programming menu** go to: **5)Communication menu > 4)Follow Me > 1)Define FM);** Follow Me 01 displays (1st FM destination).
2. Scroll to a FM number to define, and then press OK.
3. Scroll through the following options and define them as needed: **Report Type, Partition, Events, Restore Events, Remote Control.**

Defining System Timers

You can change the system defaults for the various system timers, as needed.
See the *LightSYS Air Installation and Programming Manual* for details.

➢ **To define system timers:**

1. From the **Installer Programming menu,** select **1)System > 1)Timers**
2. Scroll to select from the options and modify their parameters as needed.

INSTALLER PROGRAMMING

Step 1: Defining Additional Parameters in the Installer Programming Menu

For additional system parameters (from the Installer Programming menu), program them as needed. See the *LightSYS Air Installation and Programming Manual.*

Step 2: Exiting Installer Programming Menu after Initial System Configuration

IMPORTANT: After programming at initial system setup from the Installer Programming menu, you must exit it. You can then program additional parameters as needed from the other installer menus.

➢ **To exit Installer Programming menu after initial system programming:**

⚠ **WARNING: In the main panel box/enclosure do not touch any AC electrical wiring to/from the mains fuse terminals nor the mains fuse terminals, as 230 VAC can result in electric shock and death.**

1. Close the main panel box/enclosure in order to prevent a front tamper alarm.
2. Press ⚙↩ on keypad repeatedly to go to the beginning of the current menu.
3. Press **0** to exit, toggle with 🏠 to **Y** to save all your programming settings, and then press OK; TAMPER TESTING displays as the system checks for tamper trouble conditions.

NOTE: The Tamper Test does not include all 2-Way devices.

4. If an alarm sounds and you want to quit with a current tamper trouble condition, press ⚙↩, press 🏠 to toggle to **Y** (yes), and then press OK.
   If you select N (no), you will not be able to exit Programming mode until the tamper trouble condition has been restored to normal.

Step 3: Defining Parameters in other Installer Menus

After performing the Exiting Installer Programming Menu procedure, you can access other installer menus to define parameters, as needed (see the *LightSYS Air Installation and Programming Manual*).

Step 4: Main Panel Initial Settings

Settings	Operation	Status
2: Default	1. Using the HandyApp, scan the control panel's ID and note the unique 8-digit reset key that will display. 2. Reset the control panel. 3. From the keypad, press ⚙↩ + 8 simultaneously: <Enter reset key:> will display. 4. Enter the reset key and press OK. **NOTE:** The reset key should be entered within 5 minutes of panel reset.	Intended for Installer programming at initial system setup (from the Installer Programming menu), this setting allows the installer to set the installer, sub-installer and Grand Master codes.
8: Box tamper bypass	From the Installer Programming menu, go to: 1 > 5 > 8 > 2 (System > Settings > Bypass Tamper > Box tamper), and then press OK (✓).	**YES**: Box tamper protection is bypassed (not active) **NO**: Box tamper protection is not bypassed (active)

Testing the System

It is important to fully test the system. Here are typical, recommended system tests. See the *LightSYS Air Installation and Programming Manual* for more test information.

- ✓ Background noise-level threshold & calibration for wireless devices. See page 29.
- ✓ Wireless Communication Test for wireless devices. See page *30.*
- ✓ Walk Test (for zones) – enables to easily test and evaluate the protected areas in your system. Go to: **Installer Maintenance menu > Walk test**
- ✓ Monitoring Station (MS) Test (see the *LightSYS Air Installation Manual*)
- ✓ GSM signal strength – go to **Installer Maintenance menu > Diagnostics > GSM > Signal** – and view the signal strength result (0—5).
- ✓ Additional tests at **Installer Maintenance menu** for keypads, sirens, strobes, wireless, and diagnostics
- ✓ Follow-Me Test: After programming FM destination(s), go to: **User Menu > Follow Me > Test FM**. Trigger a Follow-Me Test activation, and see if the FM notification is received at the FM destination.

Installer Responsibilities for Assisting Clients

Here are some typical, recommended areas for you to assist the client:

- ✓ Advise client to change the Grand Master code to one that is confidential
- ✓ For RISCO Cloud-enabled communication, instruct users with Smartphones to download the iRISCO App from the Apple App store or Android Play Store, and ensure that a connection between the app and the system is established.
- ✓ Instruct how to define user codes, proximity tags, and Follow-Me contacts.
- ✓ Instruct how to do the following from keypads and keyfobs:
  - Full arm, partial arm, and disarm
  - Send a duress disarm (silent alarm) to the monitoring station
  - Activate a panic alarm
  - Check system status
  - Use SMS for remote operation

Technical Specification

Configuration	
Communication modes (modules)	GPRS, GSM (4G), IP/WI-FI (built-in)
Wireless zones	128
Wireless frequencies	868.65 MHz, 433.92 MHz
Camera frequency	869.525 MHz, 916 MHz
System users (user codes)	128 (includes 1 installer, 1 sub-installer, and 1 Grand Master code)
Follow-Me destinations	64
Panel programming options	• Keypad (locally) • Configuration Software (locally, remotely)
Partitions	32
Monitoring station accounts	3
Event log	2000 entries
PIR cameras	32
Sounders (internal/external)	3
Keypads	8
Keyfobs / remote controls	128
SMS for remote operation	yes
WL Repeater	4
Programmable utility outputs (UO)	Supports up to 4 programmable utility outputs (UOs)
Main Panel (RW432MV, RW432MVBL, RW432M, RW432MBL)	
Electrical power requirement	AC Connection: 100-240 VAC, 50/60Hz,0.1A Max. DC Connection: Via AC/DC Adapter, 14.4V DC/2.5A
AC power supply cord	• Diameter 14mm, conduit 16mm • Safety-approved, in compliance with IEC 60227
Current consumption (at main panel)	210mA standby
Backup battery (inside main panel)	Li-Polymer rechargeable battery 3.7V,5Ah
Low battery voltage signal	3.3VDC
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 G4 Modules (RP512G4, RP512G4T, RP512G4L)	
Current consumption	30 mA standby, 300 mA communicating
NOTE: The RP512G4L GSM module does not support 3G networks or e-mail reporting.	
WL Panda Keypad for LightSYS Air/LightSYS Plus:(RW432KPP2/ RW432KPP2BL)	
Current consumption	30µA standby current, 150 mA maximum

Compliance Statement

Hereby, RISCO Group declares that the LightSYS Air is 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
- PD6662:2017
- 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 4G (SP5)
- IP/Wi-Fi (SP6)
- GSM primary and IP/ Wi-Fi secondary (DP4),
- IP/ Wi-Fi primary and GSM secondary (DP4)

EN50136 Compliance:

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

Standard Limited Product Warranty (“Limited Warranty”)

RISCO Ltd. (“**RISCO**") guarantee RISCO’s hardware products (“**Products**”) to be free from defects in materials and workmanship when used and stored under normal conditions and in accordance with the instructions for use supplied by RISCO, for a period of (i) 24 months from the date of delivery of the Product (the “**Warranty Period**”). This Limited Warranty covers the Product only within the country where the Product was originally purchased and only covers Products purchased as new.

Contact with customers only. This Limited Warranty is solely for the benefit of customers who purchased the Products directly from RISCO or from an authorized distributor of RISCO. RISCO does not warrant the Product to consumers and nothing in this Warranty obligates RISCO to accept Product returns directly from end users who purchased the Products for their own use from RISCO’s customer or from any installer of RISCO, or otherwise provide warranty or other services to any such end user directly. RISCO’s authorized distributor or installer shall handle all interactions with its end users in connection with this Limited Warranty. RISCO’s authorized distributor or installer shall make no warranties, representations, guarantees or statements to its end users or other third parties that suggest that RISCO has any warranty or service obligation to, or any contractual privy with, any recipient of a Product.

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

Return Material Authorization. In the event that you need to return your Product for repair or replacement, RISCO will provide you with a Return Merchandise Authorization Number (RMA#) as well as return instructions. Do not return your Product without prior approval from RISCO. Any Product returned without a valid, unique RMA# will be refused and returned to the sender at the sender’s expense. The returned Product must be accompanied with a detailed description of the defect discovered (“**Defect Description**”) and must otherwise follow RISCO’s then-current RMA procedure published in RISCO’s website at www.riscogroup.com in connection with any such return. If RISCO determines in its reasonable discretion that any Product returned by customer conforms to the applicable warranty (“**Non-Defective Product**”), RISCO will notify the customer of such determination and will return the applicable Product to customer at customer’s expense. In addition, RISCO may propose and assess customer a charge for testing and examination of Non-Defective Product.

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

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

EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY. RISCO does not install or integrate the Product in the end user's security system and is therefore not responsible for and cannot guarantee the performance of the end user's security system which uses the Product or which the Product is a component of.

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

EXCEPT FOR THE WARRANTIES SET FORTH HEREIN, RISCO AND ITS LICENSORS HEREBY DISCLAIM ALL EXPRESS, IMPLIED OR STATUTORY, REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS WITH REGARD TO THE PRODUCTS, INCLUDING BUT NOT LIMITED TO ANY REPRESENTATIONS, WARRANTIES, GUARANTEES, AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS, TO THE EXTENT PERMITTED BY LAW. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, RISCO AND ITS LICENSORS DO NOT REPRESENT OR WARRANT THAT: (I) THE OPERATION OR USE OF THE PRODUCT WILL BE TIMELY, SECURE, UNINTERRUPTED OR ERROR-FREE; (ii) THAT ANY FILES, CONTENT OR INFORMATION OF ANY KIND THAT MAY BE ACCESSED THROUGH THE PRODUCT SHALL REMAIN SECURED OR NON DAMAGED. CUSTOMER ACKNOWLEDGES THAT NEITHER RISCO NOR ITS LICENSORS CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, GSM OR OTHER MEANS OF COMMUNICATIONS AND THAT RISCO'S PRODUCTS, MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH MEANS OF COMMUNICATIONS. RISCO IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. RISCO WARRANTS THAT ITS PRODUCTS DO NOT, TO THE BEST OF ITS KNOWLEDGE, INFRINGE UPON ANY PATENT, COPYRIGHT, TRADEMARK, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT IN ANY EVENT RISCO SHALL NOT BE LIABLE FOR ANY AMOUNTS REPRESENTING LOST REVENUES OR PROFITS, PUNITIVE DAMAGES, OR FOR ANY OTHER INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, EVEN IF THEY WERE FORESEEABLE OR RISCO HAS BEEN INFORMED OF THEIR POTENTIAL.

UKCA and CE RED Compliance Statement

Hereby, RISCO Group declares that this equipment is in compliance with the essential requirements of the UKCA Radio Equipment Regulations 2017 and CE Directive 2014/53/EU.

For the UKCA and 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 RISCO branches:

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

This RISCO product was purchased at: