RISCO
A LIFETIME OF SECURITY

LightSYS Air

Installation and Programming Manual

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

Important Notice

This guide is delivered subject to the following conditions and restrictions:

This guide contains proprietary information belonging to RISCO Group. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the system. No part of its contents may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of RISCO Group.

The information contained herein is for the purpose of illustration and reference only.

Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein belong to their respective owners.

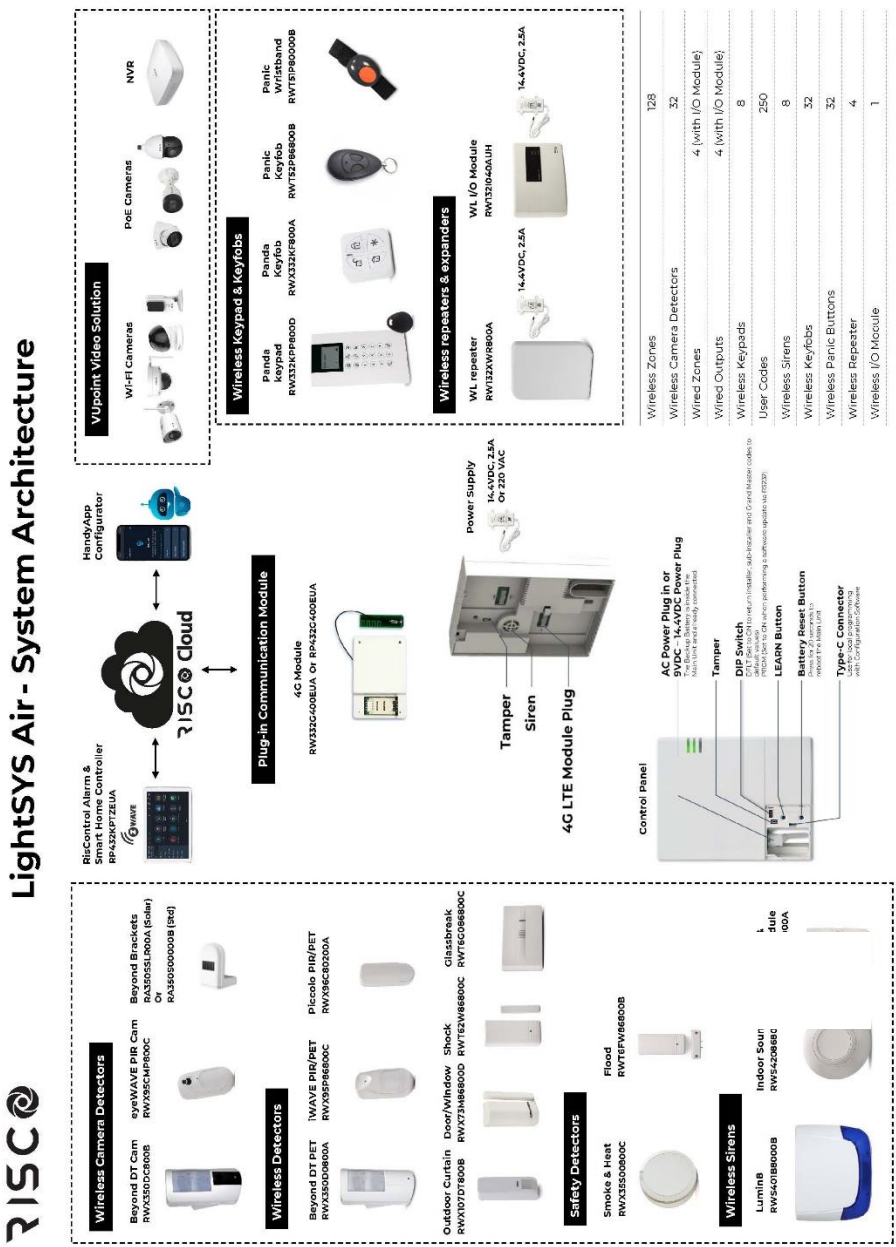
Contents

Introduction

The ideal solution for residential, commercial, and enterprise sectors, LightSYS Air is a Grade 2 compatible security system that offers communication flexibility and advanced system control via Smartphone and Web user apps, scalable up to 128 zones – using various combinations of wireless detectors and accessories. LightSYS Air offers the following:

- ✓ Various system connectivity options, including via the RISCO Cloud – for user control, operation and notification via RISCO's Smartphone and Web user apps, for communicating and reporting to the monitoring station, and for utilizing RISCO's VUpoint IP cameras – for real-time, live video verification of events
- ✓ One or more multi-socket communication modules (IP, or GSM 4G) that provide multiple, simultaneous communication channels for direct communication, and for communication via the Cloud
- ✓ Additional communication modules – multi-socket GSM/GPRS/4G and built-in IP Module
- ✓ A system supporting installation of any combination of RISCO peripherals: wireless devices (2-way)
- ✓ Advanced tests and diagnostics for the system and for individual peripherals
- ✓ Support for SIA IP
- ✓ Advanced remote/local configuration & diagnostics via Configuration Software

System Architecture



Capabilities	Description
Communication modes	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) iRISCO App
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)

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.

Main Features

Live Video Verification with VUpoint IP Cameras

LightSYS Air supports VUpoint – RISCO's revolutionary, live video verification solution for residential and commercial installations that seamlessly integrates an unlimited number of IP cameras to provide an unprecedented level of security and live video monitoring capabilities for monitoring stations and end-users alike.

- VUpoint offers seamless integration of LightSYS Air with IP cameras
- A unique solution that offers real-time video verification of alarms and events for monitoring stations, business & home owners
- Live video available on-demand
- VUpoint may be added to any LightSYS Air system connected to the RISCO Cloud, and is not dependant on the firmware version installed

VUpoint Indoor Cube IP Camera

VUpoint Outdoor Bullet IP Camera

Powered by the RISCO Cloud, VUpoint enables live video streaming from IP cameras to be viewed "on-demand" using the iRISCO Smartphone or Web user application. VUpoint can be configured so that any event—intrusion, safety, or panic—can activate the IP camera.

For verification purposes, live viewing of video of events can greatly assist monitoring stations in identifying costly false alarms, and enabling a greater operational efficiency.

Download the iRISCO app from the Apple Store for iOS devices and the Play Store for Android devices. For more information contact your RISCO distributor or go to: **www.riscogroup.com**

Flexible Communication Options

LightSYS Air offers a multitude of communication channels and reporting formats, enabling monitoring, notification & operation and maintenance for end users, installers and monitoring stations.

Advanced Communication Modules

System communication is enabled by easy-to-install plug-in GSM communication modules and a built-in IP module:

- **Multi-socket GSM 4G module**
- **Multi-socket IP**

Multiple Reporting Destinations

- **System Users:** System users can use the Cloud-based iRISCO smartphone and Web User interface for receiving event notifications. Also, multiple Follow-Me recipients are notified of events via SMS or e-mail.
- **Monitoring Station**: Events are reported to monitoring station(s) directly or via the RISCO Cloud, in any of the supported channels. LightSYS Air supports all major monitoring station reporting formats and protocols - including direct connection to the monitoring station using SIA IP, or via the Cloud with the RISCO IP Receiver installed at the monitoring station.
- **Installer:** According to how the system is programmed, installers can also receive Follow-Me reporting, just like system users.

Cloud Communication

Cloud communication is available either from a private server or hosted by the RISCO Cloud – RISCO's application server that enables communication to monitoring stations and to end users utilizing event reporting, self-monitoring and operational functions via the iRISCO Smartphone app and Web user interface. The Configuration Software can also be connected via the RISCO Cloud to perform remote system configuration and diagnostics.

Monitoring, Notification, Operation and Control via the RISCO Cloud

Self-Monitoring for System Users via Smartphone & Web Applications

Powered by the RISCO Cloud, the iRISCO Smartphone app and Web User Interface empower system users with self-monitoring, notification, control, and operation of their systems remotely – anywhere, anytime, with or without a monitoring station.

iRISCO Smartphone App

The iRISCO Smartphone app provides smart and easy control of the system, enabling on-the-go users to receive event notifications, view the system status and event history, arm/disarm the system, activate home automation devices, bypass zones, and utilize IP cameras for visual verification and self-monitoring. iRISCO is available for iOS and Android.

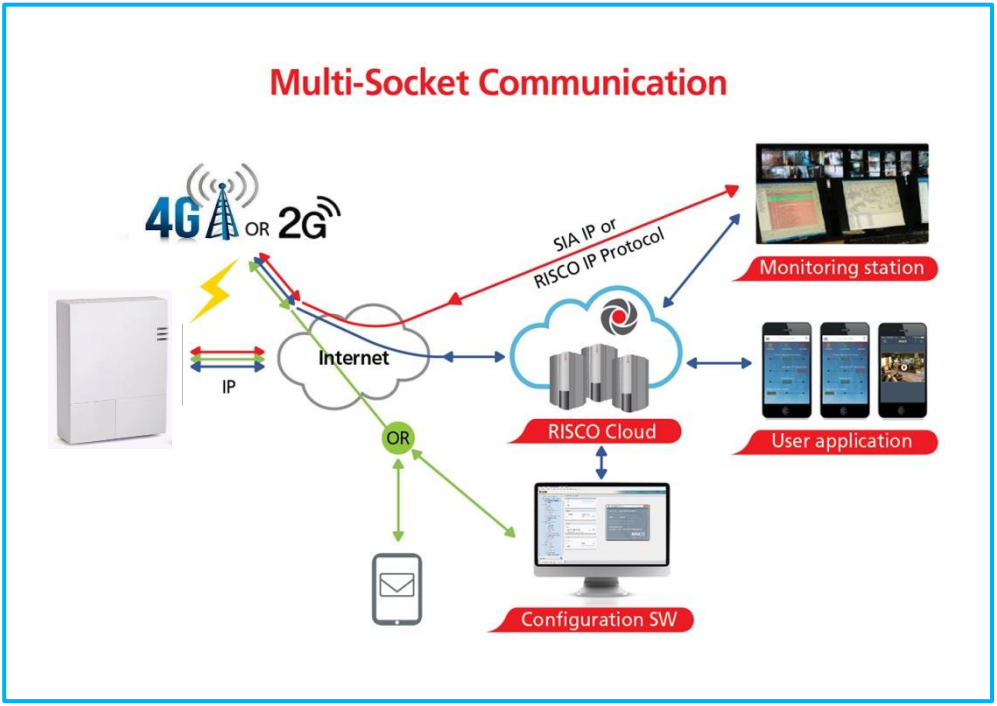
Web User Interface

RISCO's Web user interface enables system users to monitor, control and configure their system via their computer's Web browser. In addition to the capabilities of the iRISCO Smartphone app, the Web user interface enables registering the system, adding system users, and more.

Enhanced Capabilities of Multi-Socket Communication Modules

Multi-socket communication modules each provide multiple, simultaneous communication channels for services and reporting (for example to the user and monitoring station) – directly, or via the Cloud. Multi-socket module services and reporting abilities include:

- **iRISCO Smartphone app & Web user interface:** Connected via RISCO Cloud
- **Monitoring Station:** Direct connection using SIA-IP, or with the RISCO IP Receiver installed at the monitoring station
- **Configuration Software:** Connection with panel via RISCO Cloud or directly using various channels, including GSM & IP networks – see CS documentation
- **Follow-Me:** Events are sent to FM destinations by E-mail or SMS



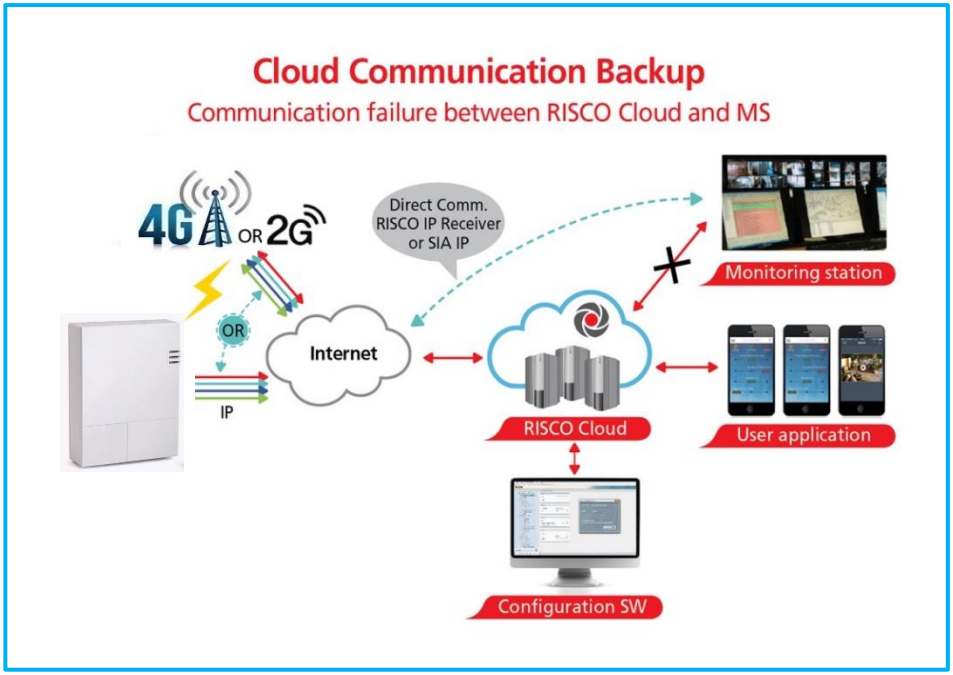
Parallel Communication

Parallel communication is accomplished using multiple communication channels (Wi-Fi/IP, GSM 4G) simultaneously ("in parallel") – for example, for user reporting via the Cloud while simultaneously reporting to the monitoring station directly. If two multi-channels (Wi-Fi/IP and GSM) are installed, each channel provides its own parallel communication capabilities.

Backup Communication

Backup communication can be accomplished as follows:

- **If using multi-socket modules** (Wi-Fi/IP, GSM 4G), any individual multi-socket installed can provide multiple, simultaneous communication channels with a variety of reporting frameworks, both directly and through the RISCO Cloud – for example, one channel reporting to the user via the Cloud, while the other channel simultaneously reporting directly to the monitoring station. If both Wi-Fi/IP and GSM multi-sockets are installed, when utilizing direct communication either of the modules can take over and connect as a communication failure backup if the other fails.



System Configuration Interfaces

- **Keypad**
- **Configuration Software**
- **HandyApp Application**

Installation and Device Allocation Tools

- **Background noise-level threshold & calibration:** For wireless devices, you can measure ("calibrate") the background noise that the main panel detects (to provide an indication whether the main panel is mounted at a good location), and also define the acceptable threshold value (to decide how much background noise your system will tolerate before it generates jamming events).
- **Wireless Communication Test:** This tests and displays the signal strength between the wireless device tested and the main panel, as an indicator of whether the mounting location of the wireless device is adequate.

Diagnostic Tests and Maintenance Features

Various tests are available to perform during and after installation, such as the **Walk Test, Follow-Me Test, GSM Signal Strength Test, Monitoring Station Test,** and more (see *Testing the System, page 164,* and the respective sections in this manual).

Service Mode silences all tamper alarms at the main panel and peripheral devices/accessories for the duration of time required for device battery replacement.

Event Logging

The LightSYS Air has the capability of storing up to 2000 events, including alarms, arming, disarming, bypassing, troubles, restores, and resets, and up to 2000 events for access control. These events are logged in order, according to date and time – and when applicable, according to zone, partition, area, user code, keypad, etc. Events are viewed on the keypad. Installers can also view events with the Configuration Software, and system users can also view events with the iRISCO Smartphone app and the Web user interface.

False Alarm Reduction Features

Features to help reduce false alarms include:

- Zone crossing
- Swinger limit (swinger shutdown) programmable by zone
- Audible exit/entry delay & exit restart
- Audible exit fault
- Soak test by zone
- Pulse count by zone
- Transmission delay
- Arm/disarm bell squawk
- Double verification of fire alarms
- Sequential alarm confirmation

Home Automation

LightSYS Air supports RISCO's Cloud-based Home Automation services.

Safety Warnings and 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

Main Tasks for Initial System Setup

Installing and setting up the system should be performed by a professional alarm system installer. Presented here is a typical order of performing these tasks:

System Installation

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

System Initialization, Device Allocation & General Configuration

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

Installer Programming

- Defining Parameters – Installer Programming Menu
- Exiting Installer Programming Menu after Initial System Programming
- Defining Parameters – Additional Installer Menus

System Testing

Various system tests are available for the LightSYS Air. Relevant tests should be performed for verifying system operability during initial system setup, as well as after completion of the initial system setup (before system handover to the client). Tests are also available for system diagnostics. See *Testing the System, page 164.*

Installer Responsibilities in Assisting the Client

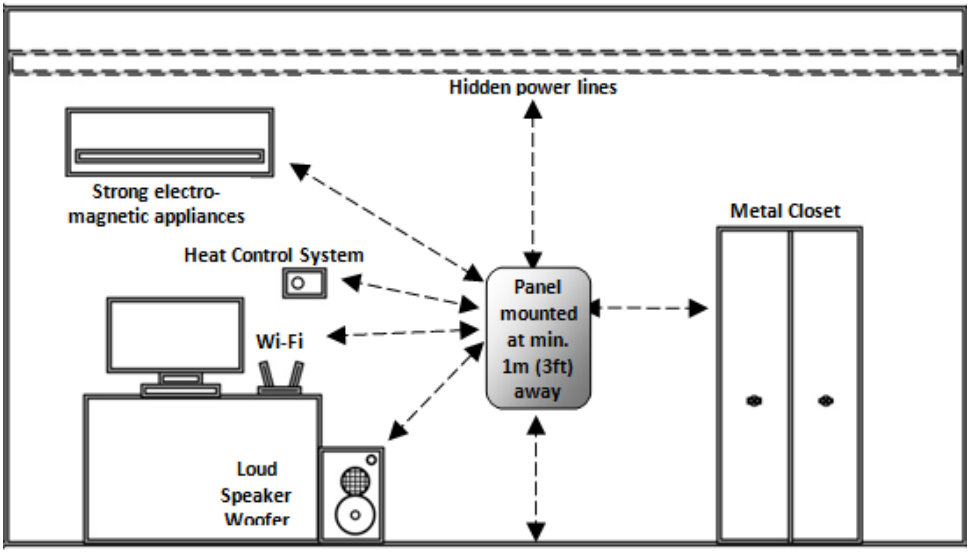
Upon handing over a fully configured and fully tested system to the client, a checklist is provided listing some of the main areas that the installer should assist the client with. See *Installer Responsibilities for Assisting the Client, page 165.*

Step 1: Creating a Plan for Mounting the System

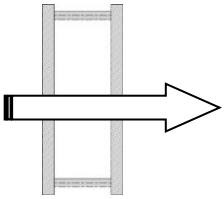
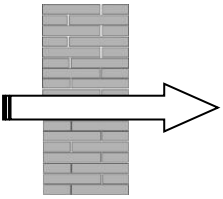
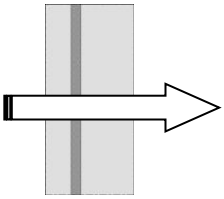
Before you mount the main panel and peripheral system components, make a plan for obtaining the most optimal location. Depending on the configuration requirements, the main panel should typically be:

- 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 disturbance (including electrical, RF and heat), and not near large metal objects which may hinder reception

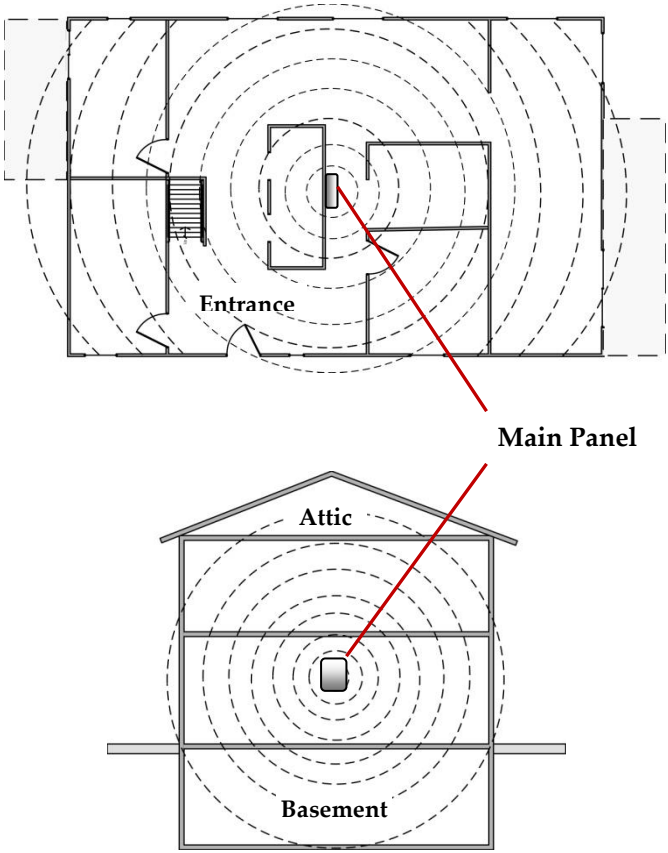
Main Panel Mounting Considerations – Wireless Systems



RF Signal Loss Due to Common Building Materials

		
Wallboard and wood	**Light concrete or brick**	**Heavy concrete and steel reinforcement**
0%—10% loss of signal	**5%—35% loss of signal**	**70%—90% loss of signal**

Central Mounting Location – Wireless Systems



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

NOTE: Not applicable to Australia and New Zealand.

IMPORTANT:

- Electrical AC wiring should be performed by a certified electrician, and in compliance with applicable electrical code, laws and regulation.
- The main panel should be connected to an easily-accessible wall outlet so that electrical 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.

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  . **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)

Installing Plug-In Communication Modules

See the installation instructions included with each module for installation details.

⚠ **CAUTION:** Before installing any communication 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.**

Installing a GSM Module

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

➢ **To install a GSM module:**

1. Ensure the main panel is powered off.
2. Install the GSM module according to the installation instructions packaged with the module for the module's connection location on the main panel.
3. Ensure the antenna is attached onto its connector on the GSM module, and then slide the antenna into place on the box/enclosure housing according to the instructions packaged with the specific box/enclosure being used.
4. Insert the dedicated SIM card and, if required, enter its enabling PIN. You can disable the SIM PIN in advance by placing it in a cell phone and then disabling it, or you can disable it later during installer programming (where you can enter or disable the PIN) and also manually define the APN, if needed (see *Defining APN Automatically and Manually, page 29*).

IMPORTANT:

- Ensure that you remember the PIN for the SIM card. If you forget it and the SIM is locked, you may need to contact your cellular provider to unlock it.
- Do not install SIM card while power is applied to the LightSYS Air.
- Do not touch SIM card connectors/circuitry. Doing so may release an electrical discharge that could damage the SIM card.
- Once the SIM card is installed, it is recommended to test the operation of the SIM by conducting a call and testing the GSM signal strength.

Connecting to IP

IP provide data communication over TCP/IP.
Connect the incoming LAN cable to its jack on the IP connector, and ensure network connectivity.

Connecting to Wi-Fi

➢ **To Connect 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 Allocations & General System Configuration

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

Step 1: Describing Keypad Controls and Installer Menus

Describing Dynamic Keypad Menus

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

Table of Keypad Buttons

The following describes the typical Panda keypad buttons used for programming:

NOTE: On other keypad the buttons may differ. See their packaged instructions.

Panda 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
	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 (such as Yes and No)
A, B, C, D	To select the corresponding group (A—D)

Designating Labels

The following table describes all the available characters at the Elegant/Panda keypad that can be used for labels (names/descriptions).

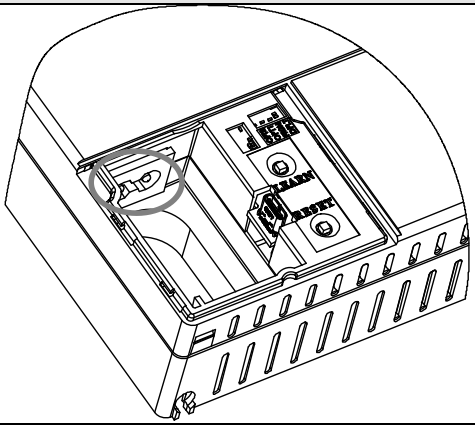
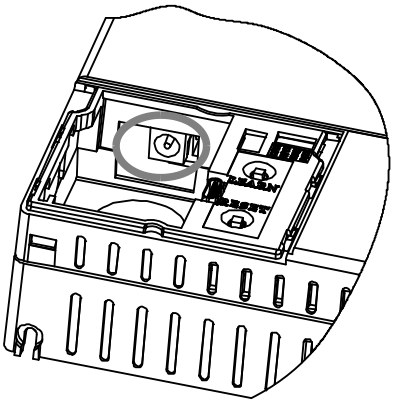
Key	Character Options	Key	Character Options
1	1 . , ' ? ! \ " — < > @ / : _ + * #	**7**	7 P Q R S
2	2 A B C	**8**	8 T U V
3	3 D E F	**9**	9 W X Y Z
4	4 G H I	**0**	0 (also use for blank space)
5	5 J K L	**A**	To toggle between lower case and capital letter
6	6 M N O	 	To scroll through all possible characters, to toggle through options (Yes/No)

Entering the Installer Programming Menu at Initial System Setup

After initial system power-up, language/time/date setting, viewing enabled zones and defining system partitions, you'll be in the installer Programming menu.

IMPORTANT: After you finish initial system setup programming tasks from the installer Programming menu, you must exit the installer Programming menu (see *Exiting Installer Programming Menu after Initial System Programming, page 156).*

Step 2: Powering-Up and Initializing the System

Configuration A: AC Connection	Configuration B: DC Connection
	

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.

System Power-Up and Language Selection

➢ **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 **Exit** when prompted, then scroll to select a language & press OK.

   NOTES:

   - During regular system operation (after initial system power-up & settings) the language can be subsequently changed by pressing **Exit** + **9** simultaneously.
   - If powering up subsequently (after initial power-up and system initialization), language, time & date settings will not automatically appear. Instead, you will be prompted to enter the installer code to access the Installer menus for programming.

Defining Partitions

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

Keypad Timeout

When in installer Programming, if no entry is made to a keypad after the pre-defined time period (see installer Programming menu), it will beep and display TIME OUT, HIT ANY KEY. Press any key to stop the beeping, then re-enter your installer code to get back in the installer Programming menu.

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  ; 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.
3. Press **OK**.

Entering or Deleting a SIM Card PIN

If your SIM card required 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-
2. 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.
3. You can manually define APN definitions if you don't have them configured automatically (default), see *Defining APN Automatically and Manually, page 29.*

   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 164.*

Defining APN Automatically and Manually

After the SIM card is installed and upon establishing GSM/GPRS/4G 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, username, 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),** and then press **OK** (✓).
2. Enter the **APN code** and then press **OK**.
3. Scroll to **2) APN User Name**, press **OK**, enter the **username** and then press **OK**.
4. Scroll to **3) APN Password,** press **OK**, enter the **password** and then press **OK**.

Setting Dynamic IP / Static IP

To set IP communication to Dynamic IP or Static IP, go to: **5 → 1 → 3 → 1 → 1,** scroll to either **1) Dynamic IP** or **2) Static IP,** and then press **OK (✓).**

Step 3: Allocating Wireless Devices

Multiple 2-way wireless detectors and accessories are connected to the system.

NOTE: To set additional parameters, see *Installer Programming, page 56*.

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 for 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.”

NOTE: The panel will sound each time you enter or exit the Learn mode.

During Learn mode the status show on keypad is “System in RF Allocation Mode”.

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).

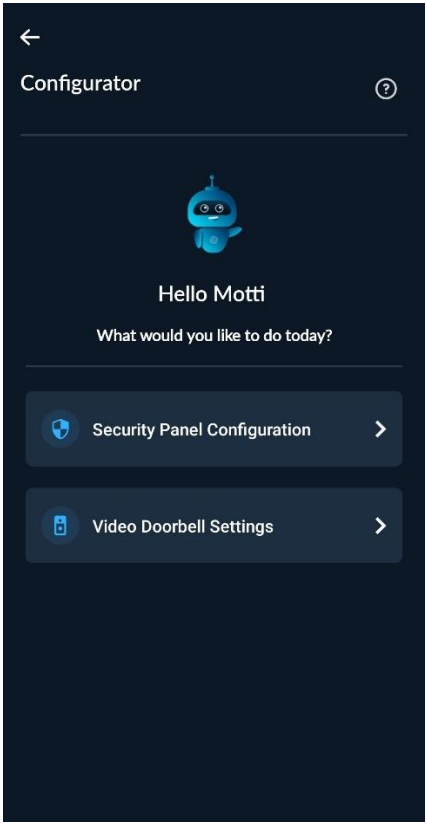
   NOTE: For future use, it is recommended to write down the device assignment / zone and installation location of each allocated device.

Access Point Mode

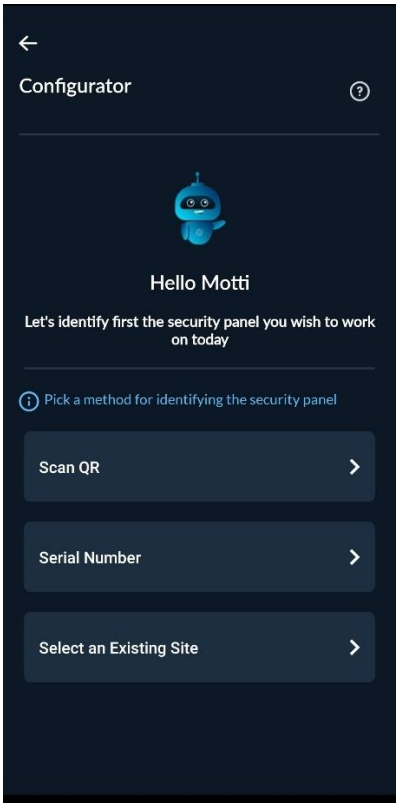
This feature enables the setup of the WiFi connection of the LightSYS Air panel that is configured without a keypad to the local network using the Handy App application.

Connecting the Control Panel to the Local Network

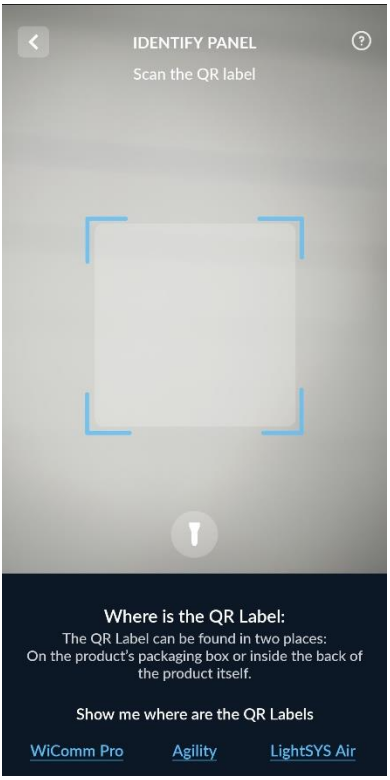
1. Open the Handy App Application.
2. From the menu, select “Configurator”.
3. Select “Security Panel Configuration”.



4. Select “Scan QR” and scan the Panel’s QR Code or select “Serial Number” and enter the Panel’s Serial Number.

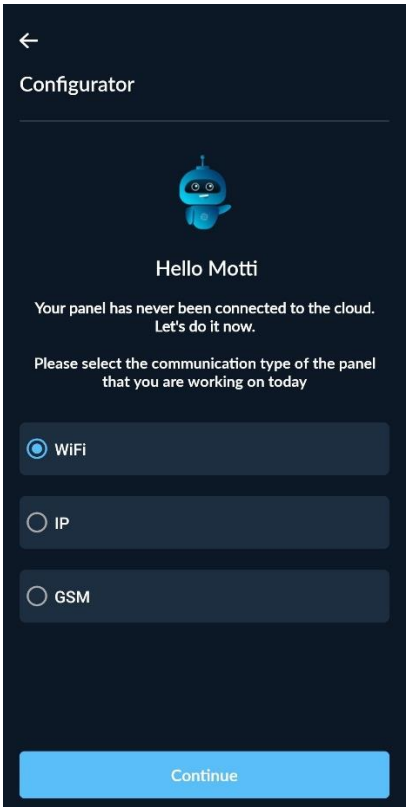


If the Scan QR option is selected, the following screen is displayed.

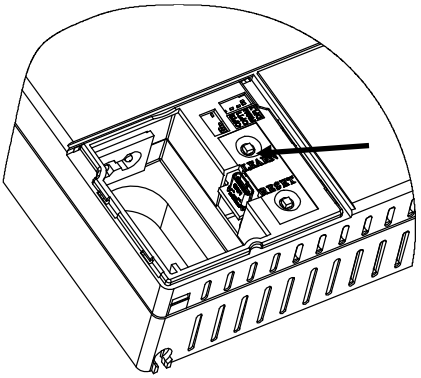


Note: *To locate the QR Code, under "Show me where are the QR Labels" click "LightSYS Air".*

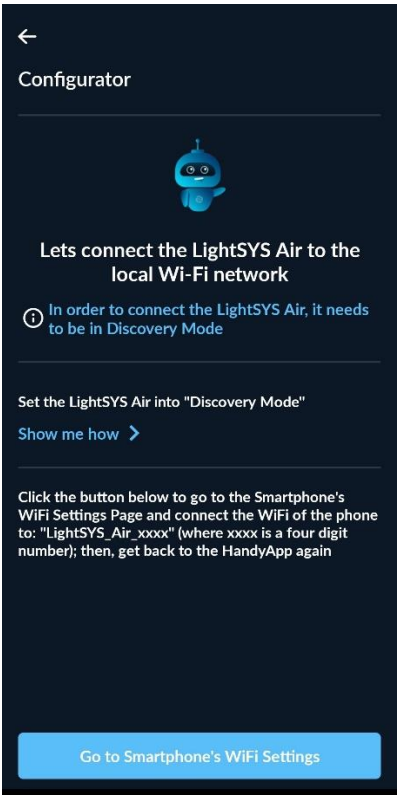
5. Click the "Next" button and then select the "WiFi" option.



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.



NOTE: If no connection has been established within 10 min, while in Access Point mode, exit the IP card from the Access Point mode.

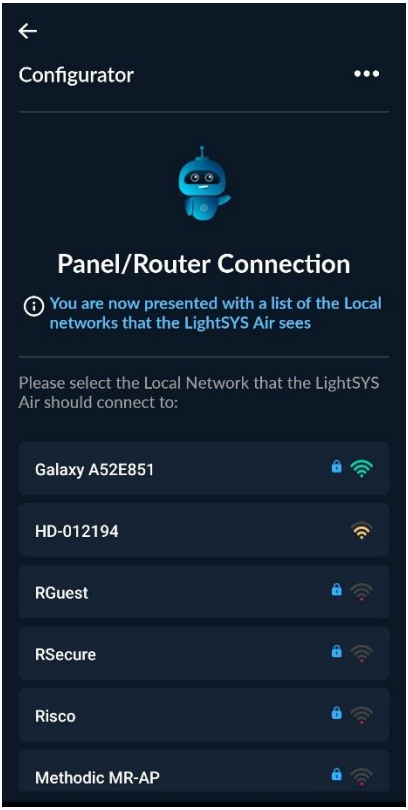


8. Click the “Go to Smartphone’s WiFi Settings” button and connect the Wi-Fi to “LightSYS_Air_xxxx”.where “xxxx” is the last four digits of the panel’s ID No. A list of local networks will open that the LightSYS Air “sees”.

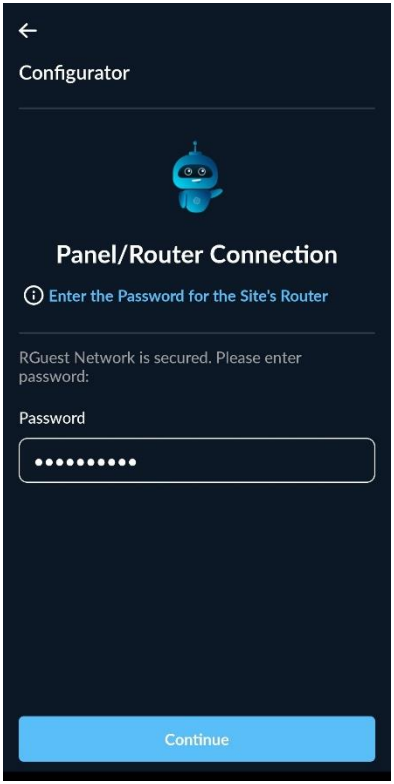
9. Select the “LightSYS_Air_xxxx” network; the password is "Riscoyyyy" where “yyyy” is the Grand Master Code. For example, in the default panel the password is “Risco1234”.
10. Return to the HandyApp Configurator.

Connecting to a Panel Network

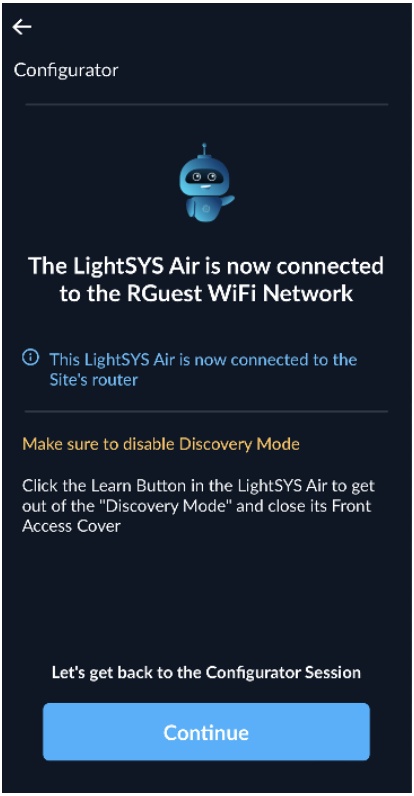
1. When prompted by the App, connect the panel to a local network by selecting the network that was scanned via the panel.



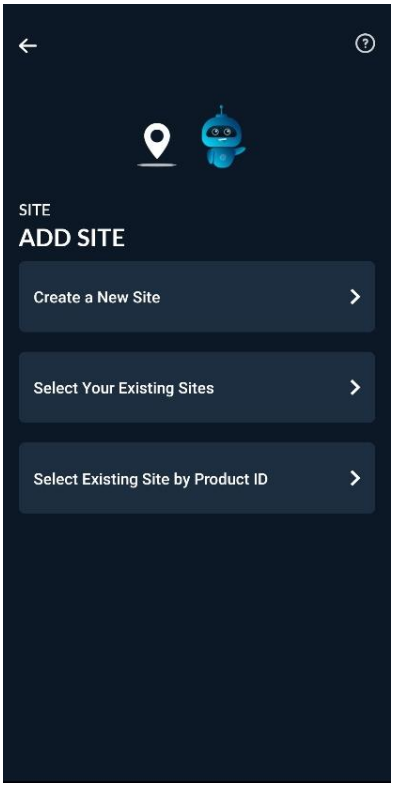
2. Enter the password of the local network.
3. Click the “Continue” button.



When connected successfully, the following screen is displayed.



4. Click the “Continue” button.



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 has to be pressed).
2-Button Panic Keyfob	Press both buttons for at least 7 seconds
Wrist Band Panic Transmitter	Press the button for at least 7 seconds.

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.

Allocate each wireless transmitting device via keypad or CS – either by sending an RF transmission or enter the device's 11-digit code (see sticker on device for code).

Allocating Wireless Devices via RF Transmission

- **To allocate a wireless device via RF transmission:**

1. From the installer **Programming menu,** go to **7 → 2 → 2 → 1 → 1 (Install → WL Device → Allocation →By RF → Zone).**
2. If you have multiple wireless receivers, scroll to the first one for which you want to allocate its wireless devices, and then press OK; 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.

It may be beneficial at a later stage to perform advanced programming such as measuring and setting the background noise threshold level, followed by performing a wireless communication test (seeAdvanced Programming for Wireless Zones page *47).*

Allocating Wireless Devices via Code

➢ **To allocate a wireless device via the device's code:**

1. From the **installer Programming menu,** go to **7 → 2 → 2 → 2 (Install → WL Device → Allocation →By code)**
2. Scroll to the zone or wireless device type [keyfob, keypad, sounder]).
   NOTE: See table above for specific wireless device types.
3. If you have multiple wireless receivers scroll to the first one for which you wish to allocate it's respective wireless devices.
4. Press **OK** (✓); Each zone/device appears in the following format:

002: ZONE 002
SN:5415

   Results display as per this example:
   - 002 is the zone number of the device
   - **5415** is the device Serial Number

   NOTE: If you try to allocate the same wireless zone number/device twice, the second allocation will over-write the prior allocation
5. Scroll to the zone number/device you want to allocate (or enter the zone number using 3 digits – for example enter 022 for zone 22), and then press **OK**; Z=xxx (RE) WRITE: 00000000000 displays (whereas xxx = the zone number). For devices, the device name, number and (RE) WRITE: 00000000000 display.
6. Enter the 11-digit code of the wireless device to enroll, and then press **OK**; the zone number and device description appears if successfully allocated.

Step 4: Basic Zone Configuration for All Zone Types

Defining Basic Parameters

You can define basic parameters for all types of zones. The relevant parameters display dynamically according to the respective zone type.

You can define all the various zone parameters for one zone at a time by using the **"One By One"** option, or you can take a specific parameter and define it accordingly for multiple zones by using the **"By Category"** option.

After defining the basic zone parameters, you can define advanced parameters for wireless zones (see *Step 5: Advanced Zone Configuration for Wireless Zones, page 47*).

Describing Zone Information Displayed at the Keypad

At the keypad you will be entering the zone information which will be displayed as per this example:

001 RWX107D 2-W
RSSI:99%

EXPLANATION:

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

Defining Zone Parameters using the "One-By-One" Option

This option lets you to define all zone parameters, for one zone at a time.

➢ **To define zone parameters using the One-By-One option:**

1. From the **installer Programming menu** go to: **2 →1 → 1 (Zones → Parameters → One by One);** the first zone (Z=001) displays in the format described above**.**
2. Using the numeric keys, you can change the zone's 3-digit zone number to the one for which you want to define its parameters, and then press **OK** (✓).
3. You can now define the following parameters for this specific zone (moving from one parameter type to another by pressing **OK**):
   a. **[Labels]:** Give the zone a descriptive "label" by typing over the default "ZONE" (see *Designating Labels, page 25*), and then press **OK**.
   a. **[Partitions]:** To select partitions (up to 32) to associate with the zone, scroll to the partitions, which are grouped in blocks: the first block contains partitions 01—08 (the default) if that is what was enabled. If additional partitions were enabled, scroll to all the blocks (of ten) they are located in: block 01—10, 11—20, 21—30, and 31—32. In each block, enter the relevant partition number/s (each will display as P=#) and then before pressing **OK**, scroll to the next blocks and do the same. When finished, press **OK**.
   b. **[Group]:** A group is a specific area (zone) that can be armed within a specific partition – up to 4 groups [A—D] maximum per each partition. For each group letter, toggle between **Y** (select) and un-select, then scroll to the next group letter, if needed. When finished press **OK**.
   c. **[Zone Type]:** Scroll to select the zone type (35 zone types), then press **OK**.
   d. {Arm Sound]: Scroll to select an arming sound, and then press **OK**. Options: silent, bell only, buzzer only, bell+buzzer, door chime.
   e. [**Stay (Partial Arm) Sound**]: Scroll to select a partial arming sound, then press **OK**. Options: silent, bell only, buzzer only, bell+buzzer, door chime.
   f. **[Disarm Sound]:** Scroll to select the disarming arm sound for this zone, and then press **OK**. Options: **silent, door chime.**
4. Press **OK** to go to the next zone and repeat the procedure for all other zones.

Defining Zone Parameters using the "By Category" Option

For a specific parameter type, this lets you to define it accordingly for multiple zones (as you go from one to another, scrolling through all zones in the system).

- **To define zone parameters using the By-Category option:**

1. From the **installer Programming menu** go to: **2 → 1 → 2 (Zones →Parameters →By Category).**
2. Scroll to arrive to the parameters and their respective options to modify. Parameters: **Label, Partition, Type, Sound, Advanced.** Press **OK** (✓) to confirm after each selection. Use the numeric keys to enter the zone number (or numeric values) where needed.

Step 5: Advanced Zone Configuration for Wireless Zones

NOTE: To set additional parameters, see *Installer Programming, page 56.*

Advanced Programming 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),** 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 the 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 49*).

Measuring the background noise level provides an indication whether the main panel is mounted at a good location.

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)**; 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. To re-calibrate (re-measure) the background noise, toggle to **Y** (yes), and then press **OK**; the new result ("NEW THOLD") displays.
4. 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 the following procedure).

- **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. 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 **1—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 *Exiting Installer Programming Menu after Initial System Programming, page 156*).
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 **1** (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 6: Configuring System Communication

NOTE: To set additional parameters, see *Installer Programming, page 56.*

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 communication channel: **(GSM or IP/Wi-Fi),** then press **OK**.
3. Scroll through the respective parameters (see the table below), and define the relevant ones, pressing **OK** after each parameter that is set.

NOTES:

- You can connect to the Cloud and additional destinations/monitoring station in parallel, using a single multi-socket communication module (IP or GSM 4G).
- For setting the backup communication channel to the monitoring station, see *Defining Monitoring Station Account Parameters, page 51*.
- LightSYS Air menus reflect only the communication modules that are installed.
- For IP communication, you can set it to Dynamic IP or Static IP. See *Setting Dynamic IP / Static IP, page 29.*
- To establish GPRS/4G communication, a SIM card must be installed.

Primary Comm. 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** **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/4G.

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 that if "GSM Only," or "IP Only" is selected, it will not have a backup communication channel.
5. Enter any needed parameters, and then press **OK**. Note that "GSM Only" means there will be no backup communication channel for this primary channel.
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 7: 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 the Smartphone and Web apps). Cloud communication enables remote monitoring and control of the system, sending event notifications, and viewing real-time video verification via RISCO's VUpoint IP cameras.

NOTE: To set additional parameters, see *Installer Programming, page 56.*

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].**
2. 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 (default), from the **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** or **GSM Only,** depending on the installed communication modules in the panel.
   - **5) Controls:** Toggle between **Y** and **N** to enable/disable MS Call All, FM Call All, App Arm, and App Disarm.

Step 8: Configuring Common System Parameters

NOTE: In addition to defining these common system parameters, see *Installer Programming, page 56* for programming all other parameters in the Installer Programming menu, as well as in the other installer menus.

Defining System Users

As the installer, you must set up the user codes for all the **system users** (up to 128 codes total, which includes 127 users including the Grand Master, plus the installer).

Performed from a keypad or from the CS, you configure the code length and the authority levels (permissions) for the system users as determined by the Grand Master (the default authority level is **User**). The Grand Master will select the numerical codes for each user from a keypad or the Web user interface. The installer can also change the default installer and Grand Master codes.

NOTE: You designate the code lengths to be either 4 or 6 digits in length. If defined as 6 digits, the length applies for everybody - all users/installers. However, if defined as 4 digits, Grand Master, Installer, and Sub-Installer must have 4-digit codes, while the system users can have codes of various lengths, from 1—4 digits.

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 partition(s) this user will be allowed to operate, do the following:
   a. While scrolling through each increment of 10 partitions, select partition(s) to allow operation by this user. Enter a partition number to select it (it will display) or enter 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 scroll to the authority level for this user **(User, Arm Only, Maid, Unbypass, Guard, Duress, UO/DOOR CONTROL, Master)**, then press **OK**.

NOTE: "Duress" is not an authority level, but a feature available to all users. By selecting this option (use any available user index number) the Grand Master will then assign a code that all users can use in times of duress, where they are forced to disarm the system. The monitoring station is sent an alarm, but the panel is silent.

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 as you overwrite with a new code, and 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 documentation).

➢ **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 over them, and then press **OK**.

Resetting the Installer, Sub-Installer and Grand Master Codes to Default Codes

You can reset the Installer, Sub-Installer and Grand Master Codes to default codes.

➢ **To change to default codes:**

1. Restart the panel.
2. Press  + 8 simultaneously on the keypad; a unique 15-digit number displays.
3. Obtain the required reset key (8 digits) from the HandyApp, RISCO Cloud or RISCO Customer Support.
4. Enter the reset key in the keypad.

The Installer/Sub-Installer/Grand Master Code will be set to the default code.

Defining Follow Me Destinations

You can enable and define up to 64 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,** 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

➢ **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.

Defining All Additional Parameters

For defining all additional system parameters in the installer Programming menu, as well as in other installer menus, see the next section (Installer Programming).

IMPORTANT:

- After you have finished programming all relevant parameters in the Installer Programming menu **at the time of initial system setup,** you must then perform the procedure to exit the installer Programming mode. See *Exiting Installer Programming Menu after Initial System Programming, page 156*.
- For accessing the Installer Programming menu again after initial system setup (after you have performed the procedure to exit installer Programming mode) see *page 156*.
- To restore the system's factory defaults, see *Restoring Manufacturer's Programming Defaults, page 157*.

Installer Programming

LightSYS Air can be programmed by the installer using the following:

- **Keypad**
- **Configuration Software** (locally or remotely connected – see the CS documentation).
- **HandyApp Application**

When performing installer programming in the various installer menus, some of the parameters display dynamically, meaning that the keypad will only display the parameters for the respective modules/hardware that are installed.

IMPORTANT: After finishing to work in the Installer Programming menu the first time (for initially programming the system), you must then exit the menu. See *Exiting Installer Programming Menu after Initial System Programming, page 156.*

Defining Parameters – Installer Programming Menu

This section describes all parameters contained in the Installer Programming menu, including the common definitions described prior in this manual.

The Installer Programming menu consists of the following sub-menus:

① System
② Zones
③ Outputs
④ Codes
⑤ Communication
⑦ Install
⑧ Devices
⓪ Exit

① System

The System sub-menu contains the following programmable parameters:

- **Timers**
- **Controls**
- **Labels**
- **Sounds**
- **Settings**
- **Automatic Clock**
- **Service Information**
- **Firmware update**

①① Timers

The Timers parameters specify the time duration of an operation.

System → Timers

Quick keys	Parameter	Default	Range
①①⓪①	**Exit/Entry Delay 1**		
	Exit/Entry delays (Group 1).		
①①⓪①❶	**Entry Delay 1**	30 seconds	01—255 seconds
	Duration of entrance delay 1.		
①①⓪①❷	**Exit Delay 1**	45 seconds	01—255 seconds
	Duration of exit delay 1.		
①①⓪②	**Exit/Entry Delay 2**		
	Exit/Entry delays (Group 2).		
①①⓪②❶	**Entry Delay 2**	30 seconds	01—255 seconds
	Duration of entrance delay 2		
①①⓪②❷	**Exit Delay 2**	45 seconds	01—255 seconds
	Duration of exit delay 2.		
①①❶❸	**Bell Timeout**	04 minutes	01—90 minutes
	Duration of the external sounder(s) during alarm.		

Quick keys	Parameter	Default	Range
①①⓪❹	**Bell Delay**	00 minutes/seconds	00—90 minutes/seconds
	The time delay before the keypad sounder and the external sounder operate after the onset of an alarm.		
①①⓪❺	**Switch Aux Break**	10 seconds	00—90 seconds
	The time that the power supplied to the system's smoke detectors through the programmable output is interrupted during a user-initiated smoke detector reset, typically performed after a fire alarm or automatically when the fire verification is defined in the system control (see *Double Verification of Fire Alarms, page 64* for additional details). **Note** This feature is supported through any programmable output that is defined as Switch AUX.		
①①⓪⑥	**Wireless**		
	Specifies the time intervals relating to the operation of the wireless module.		
①①⓪⑥❷	**RX Supervise**	0	0—7 hours
	Specifies how often the system expects to get a signal from the system's transmitters. If a signal from a zone is not received during the specified time the zone will be regarded as lost, the system will send a report code to the monitoring station, and the system status will be "Not Ready." **Note** Setting to 0 hours disables supervision. It is recommended to set the supervision time to a minimum of 3 hours		
①①⓪⑥❸	**TX Supervise**	058	1-255 minutes
	Specifies how often a 2-way wireless device generates a supervision request to the system. If any accessory doesn't respond to the request at least once during the RX Supervision time, the system will regard the accessory as Lost. **Note** Device will generate the supervision message according to the time defined. **Important** The RX Supervision time should be higher than the TX Supervision time in order to eliminate a false lost event.		
①①⓪⑥❹	**Service Mode**	020	1–255 minutes

Quick keys	Parameter	Default	Range
	The time period that all tampers (main unit and accessories) can be opened for purposes of battery replacement without triggering a tamper alarm.		
①①❼	**AC Off Delay**	30	000–255 minutes
	In the case of a loss of AC power, this parameter specifies the delay period before reporting the event or operating the programmable output. If the delay time is set to zero, there will be no delay period.		
①①❽	**Guard Delay**	30	01–99 minutes
	Specifies the time period that the system will be unarmed after an authorized user enters a Guard code.		
①①❾	**Swinger Limit**	00	00–15 times
	A swinger is a repeated violation of the same zone, often resulting in a nuisance alarm and usually due to a malfunction, an environmental problem, or the incorrect installation of a detector or sensor. This parameter specifies the number of violations of the same zone reported during a single armed period, before the zone is automatically bypassed. **Notes** • Enter **00** to disable the swinger shutdown. • The zone will be unbypassed automatically after 24 hours or at disarm. • EN 50131 compliance with swinger limit of no more than 10 times		
①①❶❼	**Redial Wait**	30	0–255 seconds
	The number of seconds between attempts at redialing the same phone number. Applies to the parameter MS Retries, page 132, and Follow Me Retries, page 146.		
①①❶❶	**Last Exit Sound**	10	01–255 seconds
	Defines the final seconds of the Exit Time for which the beep sound will change (at keypads), indicating that Exit Time period is about to expire.		
①①❶❷	**Buzzer at Stay**	15	01—99 seconds
	Defines how much time the keypad's buzzer will sound before the external sounders start to operate while an alarm occurs in Stay (partial arming) mode. The timer is relevant only if the system control Bell→Buzzer is defined as Yes.		
①①❶❸	**Status Timer**	000	0—255 seconds
	Defines if the system status will be displayed while the system is armed. When the time is defined as 0, the system status will be displayed during the arming period. When the time is not 0, the system status will be displayed only during this interval after the arming period starts.		

Quick keys	Parameter	Default	Range
①①❶❹	**Service Timer**	000	0—255 weeks
	Use this timer to periodically generate a "service required" message so that the user is reminded that a service call is required. The user may continue to arm and disarm the system. When this time is other than 0, the panel will count down the time. When the time expires, a service message will be displayed on all LCD keypads whenever the keypad is on Disarm display. To clear the message, the installer needs to reset the time, enter a code from the Anti Code menu or perform a "remote reset" to the panel.		
①①❶❻	**Pulse Open**	00 sec	0—255 seconds
	This timer is relevant only for zones defined with a pulse counter greater than one. See *Pulse Counter, page 92* (②①②⑦❷).		
	If such a zone is regarded as **not ready** for the time defined under this timer, then the zone will be tripped and act according to its type definition.		
①①❶❼	**Inactivity Timer**	0	0—255 minutes
	This timer relates to the Automatic Arm/Disarm scheduler. If there is no signal from any of the zones located in a partition that is defined under an Arm/Disarm scheduler for the time defined as **Inactive Timer,** then the automatic schedule will be activated and the relevant partitions will be auto-armed (according to the schedule definition).		
	Note Inactive Timer of scheduling program should be defined as ON under: **User Menu → Clock → Scheduler → Weekly → Schedule# → Arm/Disarm → 6)Inactive**		
①①❶❽	**Timeout Beeps**	15	0-60 minutes
	When the system is in programming mode and you have not performed any operation within the time set in Timeout Beeps, the keypad will start beeping to alert you that the system is in programming mode. When the time is defined as 0, the timeout beeps will be disabled.		

①② Controls

The Controls sub-menu has the following configurable parameters:

- **Basic**
- **Advanced**
- **Communication**
- **EN 50131**
- **PD6662**
- **CP-01**
- **Device**

System → Controls → Basic

Quick keys	Parameter	Default	Range
①②①	**Basic Programming**		
	This section refers to the most common controls in the system.		
①②① ⓪❶	**Quick Arm**	Yes	Yes/No
	YES: Eliminates the need for a user code when arming (full or partial). **NO**: A valid user code is required for arming (full or partial).		
①②① ⓪❷	**Quick UO**	Yes	Yes/No
	YES: A user can activate a utility output without the need to enter a user code. **NO**: A user code is required to activate a utility output.		
①②① ⓪❸	**Allow Bypass**	Yes	Yes/No
	YES: Permits zone bypassing by authorized system users after entering a valid user code. **NO**: Zone bypassing is not permitted.		
①②① ⓪❹	**Quick Bypass**	No	Yes/No
	YES: Eliminates the need for a valid user code when bypassing zones. **NO**: Qualified users must enter a valid user code to bypass zones.		

Quick keys	Parameter	Default	Range
①②① ❼❺	**False Code Trouble**	Yes	Yes/No
	YES: A false code report is sent to the monitoring station after three successive attempts at arming or disarming in which an incorrect user code is entered. No alarm sounds at the premises, but a trouble indication appears on the keypads. **NO**: A false code report is sent to the monitoring station and a local alarm is sounded at the premises. **NOTE:** Above Grade 2, after 10 invalid code entry attempts the keypad will lock for 90 seconds (relevant for all user codes and operations – arming, disarming, etc.). This feature is automatically activated, and there are no parameters to set for it.		
①②① ❼❻	**Bell Squawk**	Yes	Yes/No
	YES: Arming or disarming the system using a remote control, wireless keypad or a keyswitch produces a brief "chirp" and activates the strobe as follows: **1.** One chirp indicates the system is armed **2.** Two chirps indicate the system is disarmed. **3.** Four chirps indicate the system is disarmed after an alarm. **NO**: No "chirp" is produced.		
①②① ❼❽	**Audible Panic**	No	Yes/No
	YES: The sirens operate when a "panic alarm" is initiated (if defined) at the keypad, at the remote control, or when a panic zone is activated. **NO**: No siren operation occurs during a panic alarm, making the alarm truly "silent" at the premises (Silent Panic). **Note** The system always transmits a panic report to the monitoring station.		
①②① ❼❾	**Buzzer → Bell**	No	Yes/No
	YES: If an alarm occurs when the system is armed in the Stay arm (partial arm) mode, a buzzer sounds for the time defined under Buzzer At Stay (see *Buzzer at Stay page 59*) before the external sirens operate. **NO**: An alarm in the Stay Arm (partial arm) mode causes sirens to operate simultaneously.		
①②① ❶❼	**Enable Jamming**	No	Yes/No
	YES: Enables jamming alarm in system. **NO**: Disables jamming alarm in system.		
①②① ❶❶	**Audible Jamming**	No	Yes/No

Quick keys	Parameter	Default	Range
	YES: Once the specified 30 seconds time is reached, the main panel activates any internal sounders and sends a report code to the monitoring station. **NO**: Same as above, except the internal sounders do not operate.		
①②① ❶❷	**Exit Beeps at Stay**	No	Yes/No
	Determines whether the system will sound beeps during the exit time when in Stay arming (partial arming). **YES**: Exit beeps will sound. **NO**: Exit beeps will not sound.		
①②① ❶❸	**Forced Keyswitch Arming**	Yes	Yes/No
	YES: Keyswitch, Keyfob or Proximity Key arming (only from PKR) is performed on any partition. Any violated ("Not Ready") zones in the partition will be bypassed automatically. The partition is then "force-armed," and all intact zones are capable of producing an alarm. **NO**: The partition cannot be armed until all violated ("Not Ready") zones are secured.		
①②① ❶❹	**Arm Pre-Warning**	No	Yes/No
	Related to auto arm/disarm operation. **YES**: For any partition(s) set up for auto arming, an audible exit delay (warning) countdown will commence 4:15 minutes prior to the automatic arming. During this period, exit delay beeps will be heard. You can enter a valid user code at any time during the countdown to delay the partition's automatic arming by 45 minutes. When an "Auto-Arm" partition is disarmed, as described above, it can no longer be automatically armed during the current day. The extended 4:15 minutes warning does not apply to automatic partial arming. **NO**: Auto arming for any programmed partition(s) takes place at the designated time.		

System → Controls → Advanced

Quick keys	Parameter	Default	Range
①②②	**Advanced**		
	This section refers to the advanced controls in the system.		
①②② ⓪❶	**Double Verification of Fire Alarms**	No	Yes/No
	YES: Implemented on detection of smoke or fire for verification. Power to the smoke detector(s) in the affected zone is cut off and restored after the time defined in the Switch Aux Break delay (Switch Aux Break, page 58). If a subsequent detection occurs in the same zone within one minute at the end of the Switch Aux time, the system emits a fire alarm. **NO**: No fire alarm verification takes place.		
①②② ⓪❸	**Code Grand Master**	No	Yes/No
	YES: Only a user with the Grand Master authority level can change all user codes, along with the time and date. **NO**: Grand Master as well as those with the Master authority level can change their own user codes and all codes of those with lower authority levels – in addition to allowing changing the time and date. Also enables those with User and Unbypass authority levels to change their own codes.		
①②② ⓪❹	**Area**	No	Yes/No
	Changes the system operation to area instead of partition, which then changes only the operation of a common zone. **YES**: When selected, the following apply: • A common zone will be armed after any partition is armed. • A common zone will be disarmed only when all partitions are disarmed. **NO**: When selected, the following apply: • A common zone will be armed only when all partitions are armed. • A common zone will be disarmed when any partition is disarmed.		
①②② ⓪❺	**Global Follower**	Yes	Yes/No
	YES: Specifies that all zones (that are programmed to follow an Exit/Entry delay time) will follow the Exit/Entry delay time of any armed partition. **NO**: Specifies that all zones (that are programmed to follow an entry delay time) will follow the entry delay time of only the partitions to which they are assigned.		

Quick keys	Parameter	Default	Range
①②② ⓪❻	**Summer/Winter**	No	Yes/No
	YES: The LightSYS Air automatically sets its Time of Day clock one hour ahead in the spring (on the last Sunday in March) and one hour back in the Autumn (on the last Sunday in October). **NO**: No automatic time accommodation is made.		
①②② ⓪❼	**24-Hour Bypass**	No	Yes/No
	YES: It is possible for the user to bypass a 24-hour zone. **NO**: It is not possible for the user to bypass a 24-hour zone.		
①②② ⓪❽	**Technician Tamper**	No	Yes/No
	YES: It is necessary to enter the installer code to reset a tamper alarm ( ). Therefore, resetting a tamper alarm requires the intervention of the alarm company. However, the system can still be armed although the tamper indication is on. **NO**: Correcting the problem resets a tamper alarm, requiring no alarm company assistance.		
①②② ⓪❾	**Technician Reset**	No	Yes/No
	YES: It is necessary to enter the installer code to reset an alarmed partition after it has been disarmed. This requires the intervention of the alarm company technician/installer. **Note** Before the Ready LED (✓) can light, all zones within the partition must be secured. **NO**: Once an alarmed partition is reset the Ready LED lights when all zones are secured.		
①②② ❶⓪	**Installer Tamper**	Yes	Yes/No
	For above Grade 2, the system control bit "INSTALLER TAMPER" shall be defined as **YES.** **YES:** A Tamper event causes a lockout condition which can only be reset by the installer code or by anti-code. **NO:** A Tamper event does not cause a lockout condition		
①②② ❶❶	**Low Battery Arming**	Yes	Yes/No
	YES: Allows system arming when a low battery condition is detected (also in the power supply expansion module). **NO**: System arming is disabled when a low battery condition is detected.		

Quick keys	Parameter	Default	Range
①②② ❶❷	**Bell 30/10**	No	Yes/No
	YES: Any internal sounders cease to sound for 10 seconds after each 30 seconds of operation. **NO**: Any internal sounders operate without interruption.		
①②② ❶❸	**Fire Temporal Pattern**	No	Yes/No
	YES: During a fire alarm, the sirens produce a pattern of three short bursts followed by a brief pause. **NO**: During a fire alarm, the flow of sounds produced by the siren is a pattern of two seconds ON, then two seconds OFF.		
①②② ❶❹	**IMQ Install**	No	Yes/No
	YES: Causes the following parameters to function as follows: • **Auto Arm Bypass**: If there is an open zone during the auto arm process, the system will be armed, and a silent alarm will be activated (unless the open zone is closed). • A utility output defined as "Auto Arm Alarm" is activated. • A utility output defined as "Zone Loss Alarm" is activated • **Guard User**: If a Guard user disarms a partition, the system will be armed automatically after the predefined time period (see *Guard Delay page 59*). If there is an open zone during the arming process, the system will be armed, and an alarm will be sounded (unless the open zone is closed). **NO**: Causes the following parameters to function as follows: • Auto Arm Bypass: If the Auto Arm programming arms the system and there is an open zone during the auto arm, the system will bypass the open zones and arm the system.		
①②② ❶❻	**Disable Keypad When Auto Disarm Exists**	No	Yes/No
	YES: When a partition is armed manually or in auto arm mode, and an auto disarm time is defined, this parameter specifies that all the keypads that are masked to this partition will not function and that it will be impossible to disarm the relevant partition. **Note** The partition can be disarmed only by using the Configuration Software or the Auto Disarm function. **NO**: When a partition is armed manually or in Auto Arm mode, and an auto disarm time is defined, the relevant keypads will function normally.		

Quick keys	Parameter	Default	Range
①②② ❶❼	**Buzzer Delay**	No	Yes/No
	YES: The keypad buzzer will be silent during the bell delay time. **NO**: The keypad buzzer will be audible immediately when a system alarm occurs.		
①②② ❶❽	**Speaker = Buzzer**	No	Yes/No
	YES: The internal sounder will follow the operation of any keypad's buzzer. **NO**: The internal sounder will follow the external sounder operation (and not the keypad's buzzer).		
①②② ❶❾	**Confirmation Speaker**	No	Yes/No
	YES: A confirmed alarm triggers the internal sounder. **Note** A confirmed alarm actually eliminates the buzzer delay time, causing the internal speaker to trigger immediately. **NO**: The internal speaker will trigger normally (at the end of bell delay time).		
①②② ❷❿	**Bell Confirmation**	No	Yes/No
	YES: A confirmed alarm triggers the external bell. **Note** A confirmed alarm actually eliminates the bell delay time, causing the external alarm to start immediately. **NO**: The external bell will trigger normally (at the end of bell delay time).		
①②② ❷❶	**Error Speaker Time Out**	No	Yes/No
	This option determines the duration of the alarm that is generated via the internal sounders (speakers) when the exit door is programmed as "Final Exit", and it is not closed once the exit time expires (an "EXIT ERROR"). **YES**: The "EXIT ERROR" alarm in the internal speaker matches the alarm bell timeout setting. **NO**: The "EXIT ERROR" alarm in the internal speaker sounds continuously until user reset.		
①②② ❷❷	**AC Trouble Arm**	Yes	Yes/No
	YES: The system can be armed with an AC trouble detected in the main panel. **NO**: The system cannot be armed with an AC trouble.		

Quick keys	Parameter	Default	Range
①②② ❷❸	**Strobe Arm**	No	Yes/No
	This option allows the strobe (internal or external activated by a utility output - **Utility Output → Follow Partition → Strobe Trigger**) to confirm the final arming of the system. **YES**: A ten-second strobe indication will occur after the system is armed. **NO**: There will be no strobe indication when the system is armed.		
①②② ❷❹	**Final Night**	Yes	Yes/No
	This option determines the behavior of a final exit zone when the system is armed at partial (Stay) arming. **YES**: There is no need to open and close the door, if the door is closed, in order to arm the system in partial (Stay) arming. The zone behaves like a regular "EXIT(OP)" zone type**.** **NO**: There will be no change in the operation of a final exit zone in partial (Stay) arming.		
①②② ❷❺	**Stay Strobe**	No	Yes/No
	YES: For partial (Stay) or group arming, a squawk indication will be made by the strobe activated by an output **(Utility Output →Follow Partition →Strobe Trigger)** at the end of the exit delay time. **NO**: For partial (Stay) arming or group arming, no indication will be made by the strobe at the end of the exit delay time.		
①②② ❷❻	**Blank display**	No	Yes/No
	YES: Two minutes after the last keypad operation, the display will appear blank. After pressing any key, an "Enter Code" message will be displayed. The user should enter his code or pass his proximity tag. The display returns to the normal operation mode. Select this option for keypads that can be viewed from outside the protected area to disguise the system status. **NO**: The keypad display operates normally.		
①②② ❷❼	**Disp.Sys.Lb**	No	Yes/No
	This option allows you to determine whether to display the system's label on the keypad display instead of the keypad's status. **YES:** The keypad displays system's label instead of Partition status. **NO**: The keypad does not display system's label.		
①②② ❷❽	**PRES LOG N**	No	Yes/No
	YES: Presence will be recorded in the event log.		

Quick keys	Parameter	Default	Range
	No: Presence will not be recorded in the event log.		
①②② ❷❾	**Wireless Lost as Tamper**	No	Yes/No
	Sets the behavior of the sound when a wireless loss zone is detected. **YES:** The sound can be activated as in a tamper condition. **No:** The sound can be activated as in a fault condition.		

System → Controls → Communication

Quick keys	Parameter	Default	Range
①②③	**Communication**		
	This section refers to controls of the systems communication capabilities.		
①②③ ❶	**Monitoring Station Enable**	Yes	Yes/No
	YES: Enables communication with the monitoring station to report alarms, trouble, and supervisory events. **NO**: Disables communication with the monitoring station. Select NO for installations that are not monitored by a monitoring station.		
①②③ ❷	**Follow Me Enable**	Yes	Yes/No
	YES: Enables Follow-Me communication. If both the monitoring station report and the FM report are defined, the system will first call the monitoring station phones and then the FM destinations. **NO**: Disables Follow-Me communication.		
①②③ ❸	**Configuration Software Enable**	Yes	Yes/No
	YES: Enables communication between the alarm company (installer) and the LightSYS Air main panel using the Configuration Software. This enables modifying an installation's configuration, obtaining status information, and issuing main panel commands, all from a remote location. **NO**: Disables communication, as detailed above.		
①②③ ❹	**Cloud Enable**	Yes	Yes/No
	YES: Enables communication between the LightSYS Air system and the Cloud. **NO:** Disables Cloud communication.		

Quick keys	Parameter	Default	Range
①②③ ❺	**External Communication**	Yes	Yes/No
	YES: Enables RS-232 External Communication. **NO:** Disables RS-232 External Communication.		

System → Controls → EN 50131

Quick keys	Parameter	Default	Range
①②④	**EN 50131**		
	This section refers to controls that apply to EN 50131 approvals.		
①②④ ❶	**Authorize Installer**	No	Yes/No
	This option limits the installer and sub-installer authorization to access the programming menu. **YES**: A Grand Master code is required to authorize the installer to enter the programming mode for one hour. **NO**: The installer does not need an authorization code.		
①②④ ❷	**Override Trouble**	Yes	Yes/No
	Specifies if the system/partition can be armed when there is a trouble in the system. **YES**: The system will arm even if there is a trouble in the system. **NO**: When the user starts the arming process and there is a system-trouble, the user must confirm that he is aware of all troubles before continuing with the arming process. The user needs to scroll the list of troubles. At the end of the list the following question will appear: "Override Trouble?" Toggle to **Y** (yes) and then press **OK.**		
①②④ ❸	**Restore Alarm**	No	Yes/No
	YES: The user must confirm that s/he is aware that alarm occurred in the system before rearming the system. The system/partition will be in "Not Ready" status until it confirms the alarm. The user needs to confirm the alarm by going to **View → Alarm Memory** **NO**: The user does not need to confirm the alarm before rearming the system.		
①②④❹	**Mandatory Event Log**	No	Yes/No
	YES: Only mandatory events (specified in the EN standard) will be displayed in the event log.		

Quick keys	Parameter	Default	Range
	NO: All the events will be displayed in the event log.		
①②④❺	**Restore Troubles**	Yes	Yes/No
	For above Grade 2, the system control bit "Restore Troubles" shall be defined as **YES**. **YES:** A System Trouble condition must be acknowledged by the user. **NO:** A System Trouble condition will reset automatically when clear.		
①②④❻	**Exit Alarm**	Yes	Yes/No
	YES: A violated zone outside the exit route will generate an alarm during the exit time. A report to the monitoring station for arming the system is sent at the beginning of the arming procedure. **NO**: A violated zone outside the exit route that remains open at the end of the exit timer will cause a system fail-to-set condition. A report to the monitoring station is sent at the end of a successful arming procedure.		
①②④ ❼	**Entry Alarm**	No	Yes/No
	This feature is used to reduce false alarm reports to the monitoring station. **YES**: The report to the monitoring station and the siren alarm will be delayed for 30 seconds or until the end of the predefined entry delay (the shorter time of the two) following a violation of a zone outside the entry route. **NO**: A violated zone outside the entry route will generate an alarm during the entry time and a report will be sent to the monitoring station.		
①②④ ❽	**20 Minutes Signal**	No	Yes/No
	YES: Prior to arming the system, the system will check for zones that did not send a signal for more than 20 minutes. These zones will be regarded as not ready. A partition assigned with a not ready zone cannot be armed. **NO**: Prior to arming, the system will not check whether a zone did not send a signal for more than 20 minutes.		
①②④ ❾	**Attenuation**	No	Yes/No
	YES: The LightSYS Air device will be attenuated by 8dB during the Walk test using installer code. **NO**: The LightSYS Air device works in normal operation mode.		

System → Controls → PD6662

Quick keys	Parameter	Default	Range
①②⑤	**PD6662**		
	If the PD6662 standard has been selected (see procedure on *page 77),* then the configurable controls for this standard (listed below) can be set as needed. **NOTE:** For the non-configurable "Hold-Up Alarm Confirmation" parameter, see *page 77*.		
①②⑤ ❶	**Bypass Exit/Entry**	Yes	Yes/No
	YES: It is possible for the user to bypass an Exit/Entry zone. **NO**: An Exit/Entry zone cannot be bypassed.		
①②⑤ ❷	**Entry Disable**	No	Yes/No
	YES: Alarm confirmation process will be disabled when entry time starts. **NO**: Alarm confirmation process will start when the entry time starts.		
①②⑤ ❸	**Route Disable**	No	Yes/No
	YES: The panel disables the entry route zones (EX/EN, EX (OP)/EN, followers and Final Exit) from participating in the alarm confirmation process when the entry time starts. **Note** Sequential confirmation can still be established from two confirmed zones, located off the entry route. **NO**: The entry route zones will participate in the alarm confirmation process when the entry time starts.		
①②⑤ ❹	**Installer Confirmation**	No	Yes/No
	YES: An installer confirmation is required in order to reset the system after a confirmed alarm. The system cannot be armed until an installer reset confirmation is performed. The reset can be done by entering the Anti Code or entering the installation mode or by performing an "Installer reset" from the keypad. **NO**: Any means can be used to arm or disarm the system (keypad, remote phone operation etc.).		

Quick keys	Parameter	Default	Range
①②⑤ ❺	**Key Switch Lock**	No	Yes/No
	YES: Only a latched key switch zone can arm or disarm the system. **Note** When the system has more than 1 zone defined as latch key switch the arm / disarm operation will occur only after all these zones are armed or disarmed **NO**: Any means can be used to arm or disarm the system (keypad, remote phone operation, etc.).		
①②⑤ ❻	**Entry Disarm**	No	Yes/No
	Determines if the system's disarming depends on the entry time. **YES**: Only a remote control or Proximity tag can disarm the system during the entry time. **Note** System can't be disarmed with a remote control while the system is armed. **NO**: System can be disarmed during any time using any disarming device.		
①②⑤ ❼	**Proximity Disarm All Partitions**	Yes	Yes/No
	Determines which partitions can be armed/disarmed using a proximity tag. **YES**: The system arms/disarms all partitions that the proximity tag has authority of. **NO**: Enables you to select which partitions can be armed or disarmed depending on the authority of the partitions.		

System → Controls → CP-01

Quick keys	Parameter	Default	Range
①②⑥	**CP-01**		
	This section refers to controls that apply to comply with SIA CP 01.		
①②⑥ ❶	**Exit Restart**	No	Yes/No
	This parameter is used to define if an exit time shall restart one additional time while an entry/exit zone is tripped twice during exit time. **YES**: Exit time will restart for one time only when an entry/exit zone is tripped during exit time. **NO**: Exit time will not be affected if an entry/exit zone is tripped during exit time.		
①②⑥ ❷	**Auto Stay**	No	Yes/No

Quick keys	Parameter	Default	Range
	This parameter is used to define the system's arming mode when using a keypad and no exit/entry zone is tripped during exit mode. **YES**: If no exit/entry zone is tripped during exit time the system will be armed in partial (Stay) arming mode. **NO**: If no exit/entry zone is tripped during exit time the system will be armed in full (Away) arming mode.		

System → Controls → Device

Quick keys	Parameter	Default	Range
①②⑦	**Device**		
①②⑦ ❶	**Anti Mask = Tamper**	No	Yes/No
	Used to determine the operation of anti-masking detection. **YES**: Anti mask violation will activate tamper alarm. **NO**: Anti mask violation will be regarded as trouble event.		
①②⑦ ❷	**Proximity Anti Mask =Tamper**	No	Yes/No
	Used to determine the operation of the proximity anti masking detection indicated by the microwave channel. **YES**: Proximity anti mask detection will activate the tamper alarm. **NO**: Proximity anti mask detection will be regarded as a fault event. **Notes** • The Proximity Anti Mask operates for approximately 2.2 seconds when the detector is approached in close proximity. • Ensure that Proximity Anti Mask has been enabled when configuring the zone parameters.		
①②⑦ ❺	**Siren Pre-Alarm**	No	Yes/No
	Specifies if the system will send a pre-alarm message to the siren while an entry delay starts. **YES**: The system sends a pre-alarm signal to the siren at the beginning of the entry delay. If the siren does not receive a cancellation signal from the system at the end of the entry time, the siren goes into alarm. **NO**: Pre-Alarm disabled.		
①②⑦❻	**RF Wake-Up**	No	Yes/No
	Toggle between **Y** (yes) and **N** (no) to define whether the system can wake up the 2-way wireless Slim keypad during exit/entry times, or when failing to arm the system. **YES:** The system wakes up the keypad.		

Quick keys	Parameter	Default	Range
	NO: The system cannot wake up a 2-way keypad (this saves battery life).		
①②⑦❼	**Keyfob Instant Arm**	No	Yes/No
	YES: Away arming from any 2-way remote control will be instant. **NO**: Away arming from any 2-way remote control will be delayed, following exit delay 1.		
①②⑦❽	**Keyfob Instant Stay**	No	Yes/No
	YES: Stay arming from any 2-way remote control will be instant. **NO**: Stay arming from any 2-way remote control will be delayed, following exit delay 1.		
①②⑦❾	**Disarm using Code**	No	Yes/No
	Defines if a PIN code is required to perform the disarm operation while using any of the 2-way remote controls.		

①③ Labels

Define global system and partition labels.

System → Labels

Quick keys	Parameter	Default	Range
①③❶	**System**	Security System	Any 16 characters
	Edit the global system label		
①③❷	**Partitions (01-32)**	Partition 01 – 32	Any 16 characters
	Edit the label of the partitions		

①④ Sounds

Define the following system sound parameters:

- **Tamper**
- **Speaker Volume**

System → Sounds → Tamper

Quick keys	Parameter	Default	Range
①④①	**Tamper Sound**		
	Sets the sound(s) produced by a tamper violation of a keypad and/or an expansion module, as follows: ❶ Silent — Produces no sound ❷ Bell Only (external siren) ❸ Buzzer Only (keypad piezo) ❹ Bell + Buzzer		
①④① ❶	**During Disarm**	Buzzer	1—4
	Sets the sound produced by tamper violation while the system is disarmed.		
①④① ❷	**During Arm**	Bell only	1—4
	Sets the sound produced by tamper violation while the system is armed.		

System → Sounds → Speaker Volume

Quick keys	Parameter	Default	Range
①④②	**Speaker Volume**		
	Sets the volume of internal sounder (speaker) connected to the Bells/LS (+ and –- terminals) according to different system modes. Volume range is between 0 (silent) and 9 (maximum). After changing the volume, sound will be emitted by the internal sounder to enable evaluation of the selected volume level.		
①④② ❶	**Trouble**	9	0—9
	Determines the volume of the internal sounder beeps while there is trouble in the system.		
①④② ❷	**Chime**	9	0—9
	Determines volume of internal sounder chime sound. The Chime sound is used as an audible indication to a zone violation while system is disarmed.		
①④② ❸	**Exit/Entry**	9	0—9

Quick keys	Parameter	Default	Range
	Determines the volume of the beeps sounded from the internal sounder during the Exit/Entry times.		
①④② ❹	**Alarm**	9	0—9
	Determines the volume of the beeps sounded from the internal sounder during an alarm.		
①④② ❺	**Squawk**	9	0—9
	Determines the volume of the squawk sounded from the internal sounder during an alarm.		

①⑤ Settings

Set the System Settings parameters as needed.

System → Settings

Quick keys	Parameter	Default	Range
①⑤❷	**Default Panel**		
	Restores programming options to factory defaults.		
①⑤❸	**Erase Wireless**		
	Erases wireless devices without changing the system current programmed parameters. Select the wireless device to be erased. **Note** This entry appears only if a wireless device is allocated in the system.		
①⑤ ④	**Standard**		
	Sets the panel programming options in compliance with the selected standard.		
①⑤ ④ ❶	**EN 50131 (G2)**		
	For EN 50131 (G2), see page 70.		
①⑤ ④ ❷	**PD6662**		
	By selecting this standard: • **Configurable parameters** applicable for this standard can be set as needed (see *page 72*).		

Quick keys	Parameter	Default	Range
	• Parameters for the HU (Hold-Up) Alarm Confirmation are **automatically set**, and any respective outputs are activated accordingly. **NOTE:** See below for HU Alarm Confirmation description and the required action for non-reinstated HU devices. **HU Alarm Confirmation Description:** Part of the BS 8243:2010 standard, "HU alarm confirmation" automatically sends a "confirmed" alarm notification to the monitoring station when at least 2 separate, sequential HU (panic) alarms occur during the "HU confirmation time period" – which is fixed at 8 hours. The alarms must be triggered from different HU devices – for example, 2 panic alarms that are each triggered from a different keypad, or that are triggered from 1 keypad and 1 keyfob (the keyfob must be installer-configured to be used for panic alarms). At the expiration of the HU confirmation time period, if only one HU (panic) alarm has occurred – but not the second one that is required for confirmation - then the system is automatically reinstated (restored to a normal state). At the end of the HU confirmation time period, all non-reinstated HU devices are automatically bypassed – which will appear in the system's event log, the monitoring station will be notified, and there will be an indication at the panel to notify the user. **IMPORTANT: As these non-reinstated (now bypassed) devices are still in an alarm state, perform a system restore per the system's definition.**		
①⑤ ④ ❸	**CP01**		
	For CP01, see page 73		
①⑤ ④ ❹	**EN 50131 (G2)**		
	For EN 50131 (G2) see page 70		
①⑤ ❺	**Customer**		
	Sets the panel programming options in compliance with the selected customer code. Each customer has its predefined parameters. **Note** Selecting a customer that is different than the one in use will automatically default the panel.		

Quick keys	Parameter	Default	Range
①⑤ ❻	**Language**		
	Sets the system language (e-mail, SMS and keypad interface language) ❶ Text - Change the interface keypad language		
①⑤ ❼	**Partition Qty**	8	08—32
	Set the Partition Quantity parameter to define the number of partitions allocated to the system (up to 32). Press **OK** to view the number of partitions. Default is 08 (meaning up to 8). To change number of partitions, enter the number of partitions over the number that currently displays.		
①⑤ ❽	**Bypass tamper**	Yes/No	
	This option allows you to bypass the bell/box. 1. Bell tamper (default=No) 2. Box tamper (default=No)		

①⑥ Automatic Clock

Set the Automatic Clock parameters to retrieve automatic time updates (NTP or Daytime) through IP or GPRS/3G/4G.

System → Automatic Clock

Quick keys	Parameter	Default	Range
①⑥①	**Server**	Daytime	
	Select the internet time protocol: ❶ NTP (Network Time Protocol) ❷ DAYTIME		
①⑥❷	**Host**	99.150.184.201	
	The IP address or server name.		
①⑥❸	**Port**	00013	
	The NTP server port.		
①⑥❹	**Time Zone (GMT)**		
	Scroll through the available selections (GMT-12:00 - GMT+13:00).		

①⑦ Service Information

Enter the service information details of the monitoring station.

System → Service Information

Quick keys	Parameter	Default	Range
①⑦ ❶	**Name**	Any 16 characters	
	Enables you to insert and/or edit the name of the monitoring station from where service may be obtained.		
①⑦ ❷	**Phone**	Any 16 characters	
	Enables you to insert and/or edit the service phone number.		

①⑧ Firmware Update

Set parameters when updating the system firmware.

Note
The firmware update menu option series is visible only if the IP or GSM module is installed.

System → Firmware Update

Quick keys	Parameter	Default	Range
①⑧❶	**Server IP**	firmware.riscogroup.com	
	Enter the IP address of the router/gateway where the upgrade file is located.		
①⑧❷	**Server Port**	80	
	Enter the port on the router/gateway where the upgrade file is located		
①⑧❸	**File Name**	CMD.TXT (case sensitive)	
	Enter the firmware update file name. **NOTE:** Please contact Customer Support services for the file name parameters		
①⑧④	**Download File**		
	Select the communication path for the upgrade. ❶ Via IP ❷ Via GPRS/3G/4G		

② Zones

Configure the following "**basic**" zone parameters. The attributes for each zone vary according to the zone's type. The following sub-menus are available:

- **Parameters**
- **Testing**
- **Cross Zones**
- **Alarm Confirm**

②① Parameters

Configure the **basic parameters** for all zone types by the following method(s):

- **One-By-One:** Define all the relevant parameters for one zone at a time
- **By Category:** Define a specific parameter accordingly for multiple zones (as you go from one zone to another, scrolling through all zones in the system)

Note

Advanced parameters are also available for wireless zones – see *Step 5: Advanced Zone Configuration for Wireless Zones, page 47*.

One-By-One

Zones → Parameters → One-By-One

Quick keys	Parameter	Default	Range
②①①	**One-By-One**		
	See *Defining Zone Parameters using the "One-By-One" Option, page 46*.		

By Category

Zones → Parameters → By Category

Quick keys	Parameter	Default	Range
②①②	**By Category**		
	See *Defining Zone Parameters using the "By Category" Option, page 47* for an explanation, and see below for defining the parameters:		

Quick keys	Parameter	Default	Range
	❶ Label ❷ Zone Partition (and Group) ❸ Type ❹ Sound ❺ ❼ Advanced		

Zones → Parameters → By Category → Label

Quick keys	Parameter	Default	Range
②①② ❶	**Label**		
	The label identifies the zone in the system. Up to 16 characters. Type a descriptive label over the default "ZONE"		

Zones → Parameters → By Category → Zone Partition (and Group)

Quick keys	Parameter	Default	Range
②①② ❷ ZZZ	**Zone Partition**		
	1. Use scroll keys and enter a zone number (ZZZ), then press **OK.** If a zone displays with "(--:-- -- --: -- --)" it means that zone has not yet been allocated. 2. After you have selected an allocated zone, enter the number of the partition and then press **OK.** If you had defined more than 8 (default) partitions to be available in the system, you will need to scroll to get to the partition that you want the zone to be in. As there are 32 partitions maximum, the available partitions are in blocks of partitions. When you scroll to the appropriate block, enter the partition number; it will display as P=## (whereas ## is the partition). 3. Press **OK.**		
②①② ❷ ZZZ ABCD	**Group**		
	A group is a specific area (zone) that can be armed within a specific partition. There are up to 4 groups possible per partition (groups A—D). 1. Select zone partition (see procedure directly above). 2. For each applicable group letter (A—D), toggle to select it (**Y**), or to clear it. 3. Press **OK**.		

Zones → Parameters → By Category → Type

Quick keys	Parameter	Default	Range
②①② ❸	**Type**		
	The Zone Type menu contains parameters that enable you to program the zone type for any zone. 1) Select the zone (ZZZ) and then press **OK.** 2) Then scroll to select the zone type (35 types – see below) and press **OK.** **Note** Zones for partial arming ("Stay" arming) must be defined as **Interior** type. Available options: ❼❼: Interior+Exit/Entry 1, ❶❶: Interior +Entry follower ❼❽: Interior+Exit/Entry 2, ❶❷: Interior+Instant ❼❾: Interior+Exit(OP)/Entry		
Quick keys	**Parameter**	**Default**	**Range**
②①②③ZZZ ❼❼	**Not Used**		
	Disables a zone. All unused zones should be given this designation		
②①②③ZZZ ❼❶	**Exit/Entry 1**		
	Used for Exit/Entry doors. Violated Exit/Entry zones do not cause an intrusion alarm during the Exit/Entry delay. If the zone is not secured by the end the delay expires it will trigger an intrusion alarm. To start an arming process, this zone should be secured. When system is armed, this zone starts the **entry delay** time (see ①①⓪①).		
②①②③ZZZ ❼❷	**Exit/Entry 2**		Arm/Stay
	Same as above, except that the Exit/Entry 2 time period applies		
②①②③ZZZ ❼❸	**Exit (OP)/Entry 1**		
	Used for an exit/entry door, open during the armed period. This zone behaves as described in the **Exit/Entry 1** parameter, shown above, except that, if faulted when the system is being armed, it does not prevent arming. To avoid an intrusion alarm, it must be secured before the expiration of the **Exit Delay** period.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ❼❹	**Exit (OP)/Entry 2**		
	Same as above, except that the Exit (Op)/Entry 2 time period applies.		
②①②③ZZZ ❼❺	**Entry Follower**		
	Usually assigned to motion detectors and to interior doors protecting the area between the entry door and the keypad. This zone(s) causes an immediate intrusion alarm when violated unless an Exit/Entry zone was violated first. In this case, Entry Follower zone(s) will remain bypassed until the end of the Entry Delay period.		
②①②③ZZZ ❼❻	**Instant**		
	Usually intended for non-exit/entry doors, window protection, shock detection, and motion detectors. Causes an immediate intrusion alarm if violated after the system is armed or during the Exit Delay time period. When Auto Arm and Pre-Warning are defined, the instant zone will be armed at the end of the Pre-Warning time period.		
②①②③ZZZ ❼❼	**I+ Exit/Entry 1 (Interior+ Exit/Entry 1)**		
	Used for Exit/Entry doors, as follows: • If the system is armed in the Away (full) arming mode, the zone(s) provide a delay (specified by Exit/Entry 1) allowing entry and exit to and-from the armed premises. • If the system is armed in the Stay mode, the zone is bypassed. **Important** For greater security when arming in the partial (Stay) arming mode, it is possible to eliminate the Entry Delay period associated with any zone(s), classified as Exit/Entry Delay 1 by pressing the [⌂] key twice, one after another. In effect, this makes it an instantly-armed zone.		
②①②③ZZZ ❼❽	**I + Exit/Entry 2** **(Interior + Exit/Entry 2)**		
	Same as the **I+Exit/Entry 1** parameter, described above, but the **Exit/Entry 2** time period is applicable.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ❼❾	**I + Exit(OP)/Entry 1** **Interior + Exit(OP)/Entry 1)**		
	Used for an exit/entry door that, for convenience, may be kept open when the system is being armed, as follows: • In full (Away) arming mode behaves as an Exit (Op)/Entry 1 zone (see ②①ZZZ❼❸ above). • In partial (Stay) arming mode, the zone will be bypassed.		
②①②③ZZZ ❼❶❼	**I + Exit(OP)/Entry 2** **Interior + Exit(OP)/Entry 2)**		
	Used for an exit/entry door that, for convenience, may be kept open when the system is being armed, as follows: • In full (Away) arming mode behaves as an Exit (Op)/Entry 2 zone (see ②①ZZZ❼❹ above). • In partial (Stay) arming mode, the zone will be bypassed.		
②①②③ZZZ ❼❶❶	**I+ Entry Follow** **(Interior + Entry Follower)**		
	Generally used for motion detectors and/or interior doors (for example, foyer), which would have to be violated after entry in order to disarm the system, as follows: • In full (Away) arming mode behaves as an Entry Follower zone. (see ②①ZZZ❼❺ above). • In partial (Stay) arming mode, the zone will be bypassed.		
②①②③ZZZ ❼❶❷	**I + Instant (Interior + Instant)**		
	Usually intended for non-exit/entry doors, window protection, shock detection and motion detectors. • In full (Away) arming) mode behaves as an intruder (instant) zone. • In partial (Stay) arming mode, the zone is bypassed.		
②①②③ZZZ ❼❶❸	**UO/REX Trigger**		
	For a device or zone, which if violated at any time triggers a previously programmed utility output, and can activate an external indicator, relay, appliance, and so on.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ❼❶❹	**Day**		Arm
	Usually assigned to an infrequently used door, such as an emergency door or a movable skylight. Used to alert the system user if a violation occurs during the unset period (fault by day; Intruder at night), as follows: • With the system partially or fully armed (Stay or Away), the zone acts as an intruder zone. A violation of this zone after the system is armed or during the exit delay time period causes an immediate intrusion alarm. • With the system disarmed, a violation of this zone attempts to alert the user by causing the POWER/ ⏻ indicator on all keypads to flash rapidly. This directs the user to view the system's trouble indications. • Optionally, such a violation can be reported to the monitoring station as a zone trouble. See *Appendix E: Report Codes → Miscellaneous (page.181).*		
②①②③ZZZ ❼❶❺	**24 Hours**		
	Usually assigned to protect non-movable glass, fixed skylights, and cabinets (possibly) for shock detection systems. A violation of such a zone causes an instant intrusion alarm, regardless of the system's state		
②①②③ZZZ ❼❶❻	**Fire**		
	For smoke or other types of fire detectors. This option can also be used for manually-triggered panic buttons or pull stations (if permitted), as follows: • If violated, it causes an immediate fire alarm, and the Fire/ 🔥 indicator is lit (steady). • A fault in the wiring (wire open) to any fire zone causes a Fire Trouble signal (a rapid flashing of the keypads' Fire / 🔥 indicator). A short in the wires will cause an immediate alarm.		
②①②③ZZZ ❼❶❼	**Panic**		
	Used for external panic buttons and wireless panic transmitters. If violated, an immediate panic alarm is sounded (if the zone sound is not defined as silent or audible panic system control is enabled), regardless of the system's state, and a panic report is sent to the monitoring station. An alarm display will not appear on the keypads. If violated, an immediate panic alarm is sounded, regardless of the system's state.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ❶❽	**Special**		
	For external auxiliary emergency alert buttons and wireless auxiliary emergency transmitters. If violated, an immediate auxiliary emergency alarm is sounded, regardless of the system's state and a report is sent to the monitoring station.		
②①②③ZZZ ❶❾	**Key Switch**		
	Used to arm/disarm the system. Connects an external momentary action key switch to any zone terminals given this designation.		
②①②③ZZZ ❷❼	**Final Exit**		
	Zones of this type must be the last detector to be activated on exit or the first detector to be activated on entry. When arming the system, the related partition arms 10 seconds after this zone is closed, or opened and then closed. After triggered once the zone acts as an exit (open)/entry 1 zone.		
②①②③ZZZ ❷❶	**Latch Key Switch**		
	Connect an external SPST latched (non-momentary) key switch to any zone terminals given this designation and operate the keyswitch, as follows: • After arming one or more partitions using the key switch and then disarming using the keypad, the related partitions will be disarmed. In order to arm the partition using the key switch again, turn the key to the disarm position and then to the arm position.		
	• If a key switch latch is assigned to more than one partition and one of the partitions is armed by using the keypad (the key switch stays in the disarm position), then: o When changing the position of the key switch to the arm position, all the disarmed partitions, which belong to this key switch, will be armed. o When turning the key switch to the disarm position, all the partitions will be disarmed.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ⓿❷❷	**Entry Follower + Stay**		All
	Assigned to motion detectors and to interior doors protecting the area between the entry door and the keypad, as follows: • In partial (Stay) arming mode, a zone(s) given this designation behaves like an Exit/Entry zone and is subject to the Entry and Exit Delay time periods specified under Exit/Entry Delay 1. See *Exit/Entry Delay 1*, above (②①②③ZZZ⓿❶) and ①①⓪①. • In full (Away) arming mode, a zone(s) given this designation behaves like an Entry Follower Zone and causes an immediate intrusion alarm when violated unless an Exit/Entry zone was violated first. • If so, an Entry Follower + Stay zone(s) remains bypassed until the end of the Entry Delay period.		
②①②③ZZZ ⓿❷❸	**Key Switch Delay**		
	Used to apply the **Exit/Entry Delay 1** parameter to the momentary key switch operation. See *Exit/Entry Delay 1*, above (②①②③ZZZ⓿❶) and ①①⓪①.		
②①②③ZZZ ⓿❷❹	**Latch Key Switch Delay**		
	Used to apply the Exit/Entry Delay 1 parameter to the latched key switch operation. See *Exit/Entry Delay 1*, above (②①②③ZZZ⓿❶) and ①①⓪①.		
②①②③ZZZ ⓿❷❺	**Tamper**		
	For tamper detection. This zone operates the same as 24 hours zone, but it has a special reporting code. **Note** For this zone type the zone sound is determined according to the Tamper Sound defined under **1) System → 4) Sound → 1) Tamper**		
②①②③ZZZ ⓿❷❻	**Technical**		
	This zone operates the same as 24 hours zone, its report code should be manually set according to the relevant detector connected to the zone.		

Quick keys	Parameter	Default	Range
②①②③ZZZ ❼❷❼	**Water**		
	For flood or other types of water detectors. This zone operates the same as 24 hours zone, but it has a special flood report code.		
②①②③ZZZ ❽❷❽	**Gas**		
	For Gas (natural gas) leak detector. This zone operates the same as 24 hours zone, but it has a special gas report code.		
②①②③ZZZ ❾❷❾	**CO**		
	For CO (Carbon Monoxide) gas detectors. This zone operates the same as 24 hours zone, but it has a special CO report code.		
②①②③ZZZ ❿❸❿	**Exit Term**		
	This zone is normally connected to a push button outside the protected premises, which can be used to finally arm the system or area. The exit time is infinite and the related partition is not armed until this zone is triggered. When triggered, the exit time resets to 10 seconds. Use this zone to arm the system. It cannot trigger an alarm. If the partition is not secured when the exit time expires, the system stays disarmed and the keypad displays: "Fail to Arm". No "Fail to Arm" report is sent to the Monitoring Station.		
②①②③ZZZ ❶❸❶	**High Temperature**		
	For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code.		
②①②③ZZZ ❷❸❷	**Low Temperature**		
	For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code.		
②①②③ZZZ ❸❸❸	**Key Box**		
	This zone is mainly used in Scandinavia. Triggering this zone will be recorded in the event log. It can also be reported to the monitoring station. No alarm is triggered.		

Quick keys	Parameter	Default	Range
	When using this zone you should connect the alarm wiring of this zone (usually the auxiliary contact of a door) to an external key box and the tamper wiring to the housing switch.		
②①②③ZZZ ❼❸❹	**Key Switch Arm**		
	This zone is used by financial institutions such as cash distribution centers and banks to control the arming of the vault door or treasury department entrance. Use this zone for instant arming of the partition in which the zone is allocated. This zone cannot perform disarming operation.		
②①②③ZZZ ❼❸❺	**Key Switch Delayed Arm**		
	Same as the **Key Switch Arm** type (see above), but the arming will be delayed following exit delayed time.		

Zones → Parameters → By Category → Sound

Quick keys	Parameter	Default	Range
②①② ❹	**Sound**		

	This menu enables you to program the sound produced when a systems zone triggers and alarm. Reporting to the central station is not affected by the option of this menu.
	The following sound can be selected:
	• **Silent**: Produces no sound
	• **Bell Only**: Activates the bell sounders for the duration of the Bell Timeout period, or until a User Code is entered
	• **Buzzer Only**: Activates each keypad's internal piezo buzzer
	• **Bell + Buzzer**: Activates the bell sounders and the keypads' buzzers simultaneously
	• **Door Chime**: The Door Chime parameter is used as an audible sounder to indicate the violation of a zone(s), as follows:
	  ○ If the system is disarmed, the system's keypad buzzers make three momentary sounds whenever the zone is violated.
	  ○ If the system is armed, only the bell sounders produce the alarm.
	A different sound can be defined according to the system status as follows		

②①②④ ❶	**At Arm**		

Quick keys	Parameter	Default	Range
	Set the sound produced when a system's zone triggers an alarm while the system is fully (Away) armed.		
②①②④ ❷	**At Stay**		
	Set the sound produced when a system's zone triggers an alarm while the system is partially (Stay) armed.		
②①②④ ❸	**At Disarm**		
	Set the sound produced when a system's zone triggers an alarm while the system is disarmed.		

Zones → Parameters → By Category → Advanced

The following Advanced zone parameters are available for configuration:

- **Advanced**
- **Wireless Zone Configuration**

Quick keys	Parameter	Default	Range
②①②❼	**Advanced**		
②①②⑦❶	**Forced arming**		
	This option enables or disables the use of forced arming for each of the system's zones, as follows: • If forced arming is enabled for a particular zone, it allows the system to be armed even though this zone is faulty. • When a zone(s) enabled for forced arming is faulted, the red LED blinks during disarm period. • After arming, all zones enabled for forced arming are bypassed at the end of the exit delay time period (see ①①⓪① *page 57*). • If a faulted zone (one enabled for force arming) is secured during the armed period, it will no longer be bypassed and will be included among the system's armed zones. 1. Select the zone (ZZZ) and then press **OK.** 2. Then scroll to select either DISABLE or ENABLE. 3. Press **OK.**		

Quick keys	Parameter	Default	Range
②①②⑦❷	**Pulse Counter**	01	01—15
	• Specifies that the zone will count the number of open and close pulses received. If the zone exceeds the predefined number of pulses, the zone will be tripped and act according to its type definition. After a 25-second timeout the pulse counter is restarted. Select the pulse count, and then press **OK.**		
②①②⑦❸	**Abort Alarm**		
	This parameter defines whether a zone alarm report to the monitoring station will be immediate or delayed: 1. Select the zone (ZZZ) and then press **OK.** 2. Then scroll to select either: ❶ **ENABLE**: A report to the MS will be delayed according to the Abort Time Delay parameter ⑤②⑥② **(Communication → MS → MS Times →Abort Alarm)**. ❷ **DISABLE**: A report to the MS will be sent immediately 3.. Press **OK.**		

Zones→Parameters→By Category→Advanced→Wireless Parameters

Quick Keys	Parameter	Default	Range
②①②⑦ ⑤	**Wireless Parameters**		
	The Wireless Parameters menu contains parameters that enable you to program the special parameters of a 1-way or 2-way wireless zone. The options are determined according to the wireless detector type. For example: • **2-Way WatchOUT**: A dual technology outdoor detector with signal processing based on two Passive Infrared (PIR) channels and two Microwave (MW) channels. • **2-Way Magnet: Contact detector (x73)** – models include shutter and universal • **2-Way Smoke detector** • **2-Way PIR** • **Also Shock, Flood, Gas, CO, and Curtain detectors** Use the instructions below to set parameters for the relevant wireless zone detector. Also see the instructions packaged with each detector.		

Wireless Zones: 2-Way Smoke

Quick Keys	Parameter	Default	Range
②①②⑦⑤ZZZ❶	**Serial No.**		
	The identifying 11-digit number on the detector sticker		
②①②⑦⑤ZZZ②	**Control**		
②①②⑦⑤ZZZ②❶	**Supervision**	No	Yes/No
	Determines if this zone will be supervised by the system expander according to the time defined under the timer RX Supervision (see *RX Supervise, page 58*).		
②①②⑦⑤ZZZ②❷	**LED Enable**	Yes	Yes/No
	Defines whether or not the LEDS operation mode is enabled		
②①②⑦⑤ZZZ❸ **(2-Way Smoke Only)**	Operation Mode	Smoke & Heat	S/H/S&H
	Defines the detector operation mode. ❶ SMOKE ❷ HEAT ❸ SMOKE & HEAT		

Wireless Zones: 2-Way PIR, WatchOUT

Quick Keys	Parameter	Default	Range
②①②⑦⑤ZZZ❶	**Serial No.**		
	The identifying 11-digit number on the detector sticker		
②①②⑦⑤ZZZ②	**Control**		
②①②⑦⑤ZZZ②❶	**Supervision**	No	Yes/No
	Determines if this zone will be supervised by the system expander according to the time defined under the timer RX Supervision (see *RX Supervise, page 58*).		
②①②⑦⑤ZZZ②❷	**LED Enable**	Yes	Yes/No
	Defines whether or not the LEDS operation mode is enabled		
②①②⑦⑤ZZZ②❸	**Anti Mask**	No	Yes/No
	Defines the operation of anti-masking detection and behaves according to the settings defined in quick keys ②①②⑦④ZZ⑦		
②①②⑦⑤ZZZ③	**Detection Mode**	2.5 Min	2.5 min/ 2.5 sec
	❶ Normal 2.5 Min ❷ Fast 2.5 Sec		

Quick Keys	Parameter	Default	Range
	If automatic detection mode is enabled, designate here the polling periodicity of alarm generating events.		
②①②⑦⑤ZZZ④	**Sensitivity**		
	• Defines the visual sensitivity of the detector. ❶ LOW ❷HIGH ❶ LOW ❷MEDIUM ❸HIGH ❹MAXIMUM **(WatchOUT only)** • (For IR Beam) Defines the sensitivity of the detector (how long must the beam transmission be interrupted to generate an alarm event) ❶LOW 900 mSEC ❷MEDIUM 675 mSEC ❸ HIGH 450 mSEC ❹MAXIMUM 225 mSEC		

Wireless Zones: 2-Way Magnetic Contact Detector (X73)

Quick Keys	Parameter	Default	Range
②①②⑦⑤ZZZ❶	**Serial No.**	Normal	
	The identifying 11-digit number on the detector sticker		
②①②⑦⑤ZZZ②	**Control**		
②①②⑦⑤ZZZ②❶	**Supervision**	No	Yes/No
	Determines if this zone will be supervised by the system expander according to the time defined under the timer RX Supervision (see *RX Supervise, page 58*).		
②①②⑦⑤ZZZ②❷	**LED Enable**	Yes	Yes/No
	Defines whether or not the LEDS operation mode is enabled		
②①②⑦⑤ZZZ⑤	**(M&F Univ only) Magnet Enable**	Yes	Yes/No
	❶ Yes (Enable) or ❷ No (disable) the transmitter's magnet.		
②①②⑦⑤ZZZ⑥	**Alarm Hold On**	On	On/Off
	Use this parameter to define the minimum period between alarm broadcasts. **ON**: Only one alarm message is transmitted in any 2.5 minute time-period **OFF**: Alarm detection is immediately transmitted		

②①②⑦⑤ZZZ⑦	**Input Termination**	N/O	N/O, N/C, DEOL
	Use this parameter to program the connection type used for each of the system's zones ❶ (F Shutter only) Shutter: Specifies that the Input 2 will count the number of open and close pulses received. If the zone exceeds the predefined number of pulses, the zone will be tripped and act according to its type definition. After a 25-second timeout, the pulse counter is restarted. The pulse length is the currently defined Loop Response time period. ❷ N/O: Uses normally-open contacts and no terminating End-of-Line Resistor ❸ **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. ❹ **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions		
②①②⑦⑤ZZZ⑧	**Input Response Time**	500	10/500mSEC
	❶ 10 mSEC ❷500mSEC Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
②①②⑦⑤ZZZ⑨	**(F Univ. only) Anti-Sabotage**	Disable	Enable/Disable
	❶ Enable or ❷ disable the transmitter's anti-sabotage magnet.		
②①②⑦⑤ZZZ❿	**(F SP only) Shutter Pulse**	02	01—16
	Define here the number of pulses for the input.		

Presence

Quick Keys	Parameter	Default	Range
②①②⑦⑥ZZZ	**Zone=001 (0:E00:01)**	Disable	Enable/Disable
	A zone that is set as Presence will send a push notification to the end-user when triggered during disarm state. **NOTE:** Presence is applicable to all wireless detectors except for		

Beyond/PIR Camera Detectors.

❶ Enable or ❷ Disable sending a push notification to the end-user.

Notes

- The Presence push notifications option must also be selected in the RISCO Cloud for the notifications to be sent to the end-user's smartphone.
- The Presence zone can also be muted via the RISCO Cloud.

②② Testing

The Testing sub-menu has the following system tests. Also see *Testing the System, page 164.*

- **Self Test**
- **Soak Test**

Zones → Testing → Self Test

Quick keys	Parameter	Default	Range
②②❶	**Self Test**		
	This feature provides an automated self-test for a selected group of localized intrusion sensors (for example, glass break detectors, sound discriminators and shock sensors) which respond to an artificial source of noise and/or vibration. Automated self-testing is especially useful when sensors are placed in high security areas where failure cannot be tolerated. Up to 16 zones can be designated for self-testing. A sound or vibration generator should be used that can be placed close enough to the sensors to trigger them when the noise source is activated. A Programmable Output acts as the source of switched power for the noise/vibration generator (see Sensors Test, *page 103*). This is set to conform to the testing schedule. The schedule defines the time and day for the first test, and sets the times for repeated tests over a 24-hour period. A message is sent to the monitoring station if all the related sensors are triggered during the test (if a report code has been defined).With successful completion of the self-test, an entry is also placed in the event log. If one or more of the sensors fails to trip during the test period, a self-test failure message is generated and sent to the monitoring station. A record of the failure is also entered in the event log.		

Zones → Testing → Soak Test

Quick keys	Parameter	Default	Range
②②❷	**Soak Test**		

The Soak Test feature is designed to allow false alarms for predefined detectors to be bypassed from the system, while any alarms generated are displayed to the user for reporting to the monitoring station. This is especially useful to prevent unnecessary police response and when a particular zone is causing unidentified problems.

Up to 20 zones can be placed on Soak Test. Any zone placed in the Soak Test list is bypassed from the system for 14 days and is automatically reinstated after that time if no alarms have been generated by it.

If a zone in the Soak Test list has an alarm during the 14-day period, the keypad indicates to the user that the test has failed. After the user looks at the View Trouble option the trouble message will be erased. This will be indicated in the event log, but no alarm will be generated. The alarmed zone's 14-day Soak Test period is then reset and restarted.

1. From the installer Programming menu, press ②②②. The following appears:
   ZONES FOR TEST:
   001) ZONE 001 N
2. Scroll to the zone you wish to perform the Soak Test for, and then toggle to **Y** (to perform the test), or **N**.
3. Press **OK.**
4. To add other zone(s) to be tested, repeat the procedure for all additional zone(s).

EN 50131-3 Note

The Soak Test function is not in compliance with EN50131-3.

②③ Cross Zones

The Cross Zones menu is used for additional protection from false alarms and contains parameters that enable you to link together two related zones. Both must be violated within a designated time period (between 1 and 9 minutes) before an alarm occurs. This type of linking is used with motion detectors in hostile or false-alarm prone environments. The LightSYS Air allows 50 unique sets of zone links (pairs of zones), which can be manually specified, as required. Zones crossed with themselves are valid pairs. They need to register a violation twice to trigger the alarm. This process is known as Double Knock. You may want to establish a number of zone links, but leave them deactivated at this time (see below).

Zones → Cross Zones

Quick keys	Parameter	Default	Range
②③	**Cross Zones**	**None**	

1. From the installer Programming menu, press ②③. The following appears:
   ZONES CROSSING:
   01) 001 S 001
2. You are at the first **set** of zone links**(01)** – or scroll to go to the next set of zone links (50 sets maximum) ; the following displays:
   CROSSING SET 01:
   1ST = 001 2ND=001
3. Select the zone sets manually, as required, by making changes to the number of the first zone in the set, followed by the number of the second zone. If necessary, toggle between all the possibilities for each digit (you can also scroll to them).

Note
Zones crossed with themselves are valid pairs. They need to register a violation twice to trigger the alarm. This process is known as Double Knock.

4. Press **OK** to display the correlation type screen where you select how the system will process violations of the paired zones:
   ❶ NONE– Not correlated: Temporarily disables any associated zone pairings
   ❷ ORDERED–Correlated: Effects an alarm so the first listed zone is tripped before the second
   ❸ NOT ORDERED–Correlated: Affects an alarm in which either zone in the pair may be tripped first. In this case, the specified zone order (1st, 2nd) has no bearing on the alarm activation.
5. Press **OK** to display the alarm violation differential screen:
   T.SLOT: XXX,YYY
   SIZE=1 MINUTES
6. Enter the time slot, meaning the maximum amount of time allowed between the triggering events for them to be considered a valid violation (**XXX, YYY** indicate the crossed zones).
   Default: 1 min
   Range: 1 to 9 minutes
7. Repeat the entire process, as required, for any additional zone links (up to 50).

②④ Alarm Confirm

The Alarm Confirm sub-menu enables you to define the following that can be used for alarm verification:

- **Confirm Partition**
- **Confirm Zones**

Zones → Alarm Confirm → Confirm Partition

Quick keys	Parameter	Default	Range
②④❶	**Confirm partition**		
	Defines which partitions are to be defined for alarm sequential confirmation (relevant for intrusion alarms, not HU Confirmation alarms). Each confirmed partition has a separate timer (time period), which is equivalent to the confirmation time defined in "Confirmation Time Window" (see *Confirm Time , page 134*). A confirmed intrusion alarm will be reported to the monitoring station if two separate alarm conditions are detected in the same confirmed partition, during the period of the confirmation time window. • Cycle through the partitions and toggle to **Y/N** for each.		

Zones → Alarm Confirm → Confirm Zones

Quick keys	Parameter	Default	Range
②④❷	**Confirm zones**		
	Define which zones are to be defined for alarm sequential confirmation (relevant for intrusion alarms, not HU Confirmation alarms). When the first zone goes into alarm the system transmits the first zone alarm. When the second zone goes into alarm, during the confirmation time, the panel transmits the zone alarm and the police code. **Notes** • A confirmed zone will be part of the sequential confirmation only if the partition in which the alarm occurs is defined as confirmed partition as well. • Any code can reset a confirmed alarm. • If the first zone is violated and not restored until the end of the confirmation time (no second zone alarm), then this zone will be excluded from the confirmation process until the next arming. • Cycle through the zones and toggle to **Y/N** for each.		

③ Outputs

The Utility Output menu provides access to the following submenus and their related programming parameters that enable you to choose among the following event types that will trigger a selected Utility Output, as well as the manner in which the output will be applied:

- **Nothing**
- **System**
- **Partition**
- **Zone**
- **Code**

③⓪ Nothing

This parameter is for disabling a previously enabled utility output.

Note

When selecting output utility output number (1—10), if the UO number appears with a 0 first (for example 0xx, whereas xx is the UO number) that indicates the UO is connected directly to the terminal block and not assigned to an output expander.

1. From the installer Programming menu go to **3)Outputs** and then press **OK** (✓).
3. Scroll to a UO number to disable (1—10), and press **OK**.
4. Scroll to **0)Nothing** and then press **OK**.
5. Scroll to additional programmed outputs to disable, then press **OK** after each.

Outputs → Nothing

Quick keys	Parameter	Default	Range
③xx ① ⓪	**Nothing**		
	Disables a previously enabled programmable output		

③① System

Define parameters that follow system events.

Note

When selecting output utility output number (1—10), if the UO number appears with a 0 first (for example 0xx, whereas xx is the UO number) that indicates the UO is connected directly to the terminal block and not assigned to an output expander.

1. From the installer Programming menu go to **3)Outputs** and then press **OK** (✓).
2. Scroll to a UO number to configure (1—10), and press **OK**.
3. Scroll to **1)System** and then press **OK**.
4. Scroll to a parameter to configure in the table below, and then press **OK**.
5. Scroll to the pattern of operation option (see Pattern of Operation for Utility Outputs, page 111) and then press **OK**.
6. Set other parameters as relevant (such as pulse duration and UO label), and then press **OK** after each.

Outputs → System

Quick keys	Parameter
③xx ① ⓪❶	**Bell Follow**
	Activates when a bell is triggered. If a bell delay was defined, the utility output will be activated after the delay period.
③xx ① ⓪❷	**No Telephone Line**
	Activates when a bell is triggered. If a bell delay was defined, the utility output will be activated after the delay period.
③xx ① ⓪❸	**Communication Failure**
	Activates when communication with the monitoring station cannot be established. Deactivates after a successful call is established with the MS.
③ xx ① ⓪❹	**Trouble Follow**
	Activates when a system trouble condition is detected. Deactivates after the trouble has been corrected
③ xx ① ⓪❺	**Low Battery Follow**
	Activates when the LightSYS PlusLightSYS Air panel's rechargeable standby battery has insufficient reserve capacity and the voltage decreases to 11 V or following an accessory low battery indication.

Quick keys	Parameter
③ xx ① ❻❻	**AC Loss Follow**
	Activates when the source of the main panel's AC power is interrupted. This activation will follow the delay time defined in the system control times and the AC Off Delay Time parameter (see *AC Off Delay page 59*).
③ xx ① ❼❼	**Sensors Test**
	Relates to the LightSYS PlusLightSYS Air Zone Self-Test (Quick Keys ②②①) This option is selected if the designated utility output is part of the circuit providing switched power for the source of noise (or vibration) used in the sensors test procedure.
③ xx ① ❽❽	**Battery Test**
	A pulsed utility output will follow the battery test only once a day at 9:00 AM. The pulse interval is ten seconds. This parameter is usually used to perform an overload test on the system by using an external device.
③ xx ① ❾❾	**Bell Burglary**
	Activates the utility output after any bell burglary alarm in any partition in the system.
③ xx ① ❶❶	**Scheduler**
	The utility output will follow the predefined time programming that is defined in the scheduler of the weekly programs for utility output activation. For additional details, refer to the LightSYS PlusLightSYS Air User Manual.
③ xx ① ❶❶	**Switched Aux**
	Activates the utility output when a fire zone is activated (for fire detection) according to the time defined in double verification of fire alarms (see *Double Verification of Fire Alarms, page 64*). This utility output will not have the option to choose pulse or latch in the Utility Output: Code. The pulse time is defined in *Switch Aux Break, page 58*.
Quick keys	**Parameter**
③ xx ① ❶❷	**GSM Error**
	Relates to the installed GSM module. Activates the utility output in the following cases:

Quick keys	Parameter
	1. There is no SIM card in the GSM module or SIM is faulty 2. GSM RSSI signal level is low 3. GSM network fault
③ xx ① ❶❸	**Bell Test**
	Activates the output when the "Bell Test" option is selected and deactivates when the "Bell Test" option is finished.
③ xx ① ❶❹	**Installation**
	Activates the output following the system installation status. It activates when the system is in installer programming mode and deactivates when exiting installer's mode.
③ xx ① ❶❺	**Walk Test**
	Activates the output when the "Walk Test" option is selected and deactivates when the "Walk Test" option is finished.
③ xx ① ❶❻	**Burglary**
	Activates the output (Pulsed only) following any intruder activation in the system (Regardless the bell time out timer). The maximum number of times an output can be activated from the same zone is defined according to the Swinger Limit Timer (Quick key ①①❼❾)
③ xx ① ❶❼	**Panic**
	Activates the output (Pulsed only) following any panic activation in the system. The maximum number of times an output can be activated from the same zone is defined according to the Swinger Limit Timer (Quick key ①①❼❾).
③ xx ① ❶❽	**Fire**
	Activates the output (Pulsed only) following any fire activation in the system. The maximum number of times an output can be activated from the same zone is defined according to the Swinger Limit Timer (Quick key ①①❼❾).
③ xx ① ❶❾	**Special**
	Activates the output (Pulsed only) following any special emergency activation in the system. The maximum number of times an output can be activated from the same zone is defined according to the Swinger Limit Timer (Quick key①①❼❾).

Quick keys	Parameter
③ xx ① ❷❼	**24 Hour**
	Activates the output (Pulsed only) following any 24 Hour zone activation in the system. The maximum number of times an output can be activated from the same zone is defined according to the Swinger Limit Timer (Quick key ①①❼❾).

③② Partition

Define parameters that follow partition events.

Note

When selecting output utility output number (1—10), if the UO number appears with a 0 first (for example 0xx, whereas xx is the UO number) that indicates the UO is connected directly to the terminal block and not assigned to an output expander.

1. From the installer Programming menu go to **3)Outputs** and then press **OK** (✓).
2. Scroll to a UO (utility output) to configure (1—10), and press **OK**.
3. Scroll to **2)Partition** and then press **OK**.
4. Scroll to a parameter to configure in the table below, and then press **OK**.
5. Select the partition/s by entering the numbers (you can enter a number again to clear it), and then press **OK**.
6. Scroll to the pattern of operation option (see Pattern of Operation for Utility Outputs, page 111), and then press **OK**.
7. Set other parameters as relevant (such as pulse duration and UO label), and then press **OK** after each.

Outputs → Partition

Quick Keys	Parameter
③ xx ② ❼❶	**Ready Follow**
	Activates the output when all selected partition(s) are in a "ready" state.
③ xx ② ❼❷	**Alarm Follow**
	Activates the output when an alarm occurs in the selected partition(s).
③ xx ② ❼❸	**Arm Follow**
	Activates the utility output when the selected partition(s) is armed in either the full (Away) or partial (Stay) arming mode. The utility output will be activated immediately, regardless of the exit delay time period.

③ xx ② ❿❹	**Burglary Follow**
	Activates the output when an intruder (intrusion) alarm occurs in the selected partition(s).
③ xx ② ❿❺	**Fire Follow**
	A\ctivates the utility output when a fire alarm is triggered in the selected partition(s) from the keypads or a zone defined as Fire.
③ xx ② ❿❻	**Panic Follow**
	Activates the utility output when a panic alarm is triggered in the selected partition(s) from the keypads, remote controls or a zone defined as Panic.
③ xx ② ❿❼	**Special Follow (Emergency)**
	Activates the utility output when a special alarm is triggered in the selected partition(s) from the keypads or a zone defined as Special.
③ xx ② ❿❽	**Buzzer Follow**
	Activates the output when a keypad in the selected partition(s) sounds its buzzer during auto setting, Exit/Entry delays, and alarm conditions.
③ xx ② ❿❾	**Chime Follow**
	Activates the output when a keypad in the selected partition(s) sounds its chime.
③ xx ② ❶❿	**Exit/Entry Follow**
	Activates the output when the selected partition(s) initiates an Exit/Entry delay period.
③ xx ② ❶❶	**Fire Trouble Follow**
	Activates the output when a Fire Trouble is detected in the selected partition(s).
③ xx ② ❶❷	**Day Trouble (Zone)**
	Activates when a day zone trouble is detected in the selected partition(s).
③ xx ② ❶❸	**Trouble Follow (General)**
	Activates the output when a fault condition is detected in the selected partition.

③ xx ② ❶❹	**Stay Follow**
	Activates the utility output when the selected partition(s) is armed in the partial (Stay) arming mode.
③ xx ② ❶❺	**Tamper Follow**
	A latched output activated when a tamper occurs in the selected partition(s) and follows any type of tamper. The output deactivates at tamper reset.
③ xx ② ❶❻	**Disarm Follow**
	Activates the utility output when the selected partition(s) is disarmed.
③ xx ② ❶❼	**Bell Follow**
	This output enables the connection of different external sounders to different partitions. Activates the output when one of the defined partitions is in alarm mode and the bell is triggered. It will be activated for the programmed bell time or until the alarm is unset. **Note** The external sounder will not generate any squawk sounds
③ xx ② ❶❽	**Bell Stay Off**
	This parameter causes the output to function as follows: In full (Away) arming mode, the output will follow the bell activation in the defined partitions. In partial (Stay) arming mode, the output will not be activated. **Note** If an alarm occurs in a zone that shares more than one partition and one of the partitions is in full (Away) arming mode (while the other is in partial (Stay) arming mode, the output will be activated, as described above. In partial (Stay) arming mode, a 24-hour zone will not activate this output.
③ xx ② ❶❾	**Zone Bypass**
	Activates the output when the relevant partitions are in full (Away) arming mode or partial (Stay) arming mode, and any zone in the relevant partitions is bypassed.
③ xx ② ❷❿	**Automatic Arm Alarm**
	Activates the utility output when there is a not ready zone at the end of the pre warning time during an auto-arm process. The output restore shall be on Bell- Timeout or at user Disarm.
③ xx ② ❷❶	**Zone Loss Alarm**
	Activates the utility output when there is a lost wireless zone in the

	system. The output restore shall be on Bell-Timeout or at user Disarm.
③ xx ② ❷❷	**Bell Trigger**
	Mainly used for the connection of different external sounders to different partitions in the UK. Activates the output when one of the defined partitions is in alarm mode and the bell is triggered. It will be activated for the programmed bell time out or until alarm is disarmed. This output generates squawk sounds and has a special sound for fire alarms. **Note** In fire alarm the output will not follow the bell delay time (see *Bell Delay, page 58*) but will trigger immediately. It will be triggered in pulsed sequence: five seconds on and two seconds off.
③ xx ② ❷❸	**Strobe Trigger**
	A latched output that is used to trigger a strobe. The output is activated when one of the defined partitions is in alarm mode or during squawks. The output will be activated until the alarm is disarmed. The output is also activated in test mode. **Note** A tamper alarm will not activate the output if all partitions are disarmed.
③ xx ② ❷❹	**Fail To Arm**
	Activates when one of the defined partitions fails to arm and deactivates at user reset.
③ xx ② ❷❺	**Confirm Alarm**
	The output activates when a confirmed alarm occurs in a partition and deactivates at the restore of the alarm confirmation. RISCO recommends using this output for the Red-Care STU Confirmed Alarm channel.
③ xx ② ❷❻	**Duress Follow**
	Activates the Utility Output when a duress alarm is initiated at the keypad related to the selected partition(s).
③ xx ② ❷❼	**HU Confirmation Al. (Hold Up Confirmation Alarm)**
	Activates the output when "Hold-Up Alarm Confirmation" occurs in the selected partition(s). See *page 72*.
③ xx ② ❸❷	**Zone Exclude**
	Activates the output when any zone is excluded from the confirmation procedure.

③③ Zone

Define parameters that follow zone events. Each utility output can be activated by a group of up to five zones.

Note

When selecting output utility output number (1—10), if the UO number appears with a 0 first (for example 0xx, whereas xx is the UO number) that indicates the UO is connected directly to the terminal block and not assigned to an output expander.

1. From the installer Programming menu go to **3)Outputs** and then press **OK** (✓).
2. Scroll to a UO (utility output) to configure (1—10), and press **OK**.
3. Scroll to **3)Zone** and then press **OK**.
4. Scroll to a parameter to configure in the table below, and then press **OK**.
5. For each utility output, you can define a group of up to five zones. Select the 1st through 5th zone numbers to be in the group, pressing **OK** after each (press **OK** even if you don't specify a zone number for all of the five). If you choose a zone that's not in the system, the keypad will beep - scroll back and enter a valid zone.
6. Scroll to the pattern of operation option (see Pattern of Operation for Utility Outputs, page 111), and then press **OK**.
7. Set other parameters as relevant (such as pulse duration and UO label), and then press **OK** after each.

Outputs → Zone

Quick keys	Parameter
③ xx ③ ❶	**Zone Follow**
	Activates the utility output when the selected zone is tripped. The tripped zone need not be armed to trigger the utility output.
③ xx ③ ❷	**Alarm Follow**
	Activates the utility output when the selected zone causes an alarm.
③ xx ③ ❸	**Arm Follow**
	Activates the utility output when the selected zone is armed by the system.
③ xx ③ ❹	**Disarm Follow**
	Activates the utility output when the selected zones are disarmed.

③④ Code

Outputs → Code

Define parameters for enabling codes (for system users) to activate / deactivate utility outputs.

Notes

- The utility output is activated by entering a user code only if the **Quick UO** parameter under System Control is defined as Disabled. When the Quick UO is defined as Enabled, no user code is required.
- When selecting output utility output number (1—10), if the UO number appears with a 0 first (for example 0xx, whereas xx is the UO number) that indicates the UO is connected directly to the terminal block and not assigned to an output expander.

Quick keys	Parameter
③ xx ④ ❶	**U.Output**
	Activates the utility output when entering a user code.

Pattern of Operation for Utility Outputs

The Pattern of Operation enables you to set activation/deactivation options for utility outputs. When the UO is following more than one partition, zone, or user you can choose the logic of the UO activation or deactivation, as follows:

Latch N/O & Latch N/C

For Latch N/O and Latch N/C, you can choose the **activation and deactivation** logic of the utility output to follow either after all the partitions/zones/user codes or after any of the partitions/zones/user codes.

Pulse N/O & Pulse N/C

If the pattern of operation is defined as Pulse N/O or Pulse N/C, you can choose **only the activation** logic of the utility output to follow either after all the partitions/zones/user codes or after any of the partitions/zones/user codes. The deactivation operation follows the defined time period.

Pattern of Operation	Default	Range
Pulse N/C	05 seconds	01—90 seconds
The utility output is always activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates for the pulse duration specified below and then reactivates automatically. 1. Choose the desired pulse duration, between **01—90 seconds.** 2. Press **OK** (✓) and set the activation by toggling to **ALL** or **ANY**. 3. Press **OK** and define a label (max 10 characters) for the UO.		
Latch N/C		
The utility output is always activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates and remains deactivated (latched) until the operation is restored. 1. Toggle to either **ALL** or **ANY** to set the activation, and then press **OK** (✓). 2. Toggle to either **ALL** or **ANY** to set the deactivation, and then press **OK**. 3. Define the output label (max 10 characters), and then press **OK**.		
Pulse N/O	05 seconds	01—90 seconds
The utility output is always deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (is pulled down) for the pulse duration specified below, then deactivates automatically. 1. Choose the desired pulse duration, between **01—90 seconds.** 2. Press **OK** (✓) and set the activation by toggling to **ALL** or **ANY**. 3. Select a label for the UO (max 10 characters), and then press **OK**.		

Latch N/O		
The utility output is always deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (is pulled down) and remains activated (latched) until the operation is restored. 1. Toggle to select **ALL** or **ANY** to set the activation, and then press **OK** (✓). 2. Toggle to select **ALL** or **ANY** to set the deactivation, and then press **OK**. 3. Define the output label (max 10 characters), and then press **OK**.		

④ Codes

Define code parameters for the following:

- **User:** Assign to each system user
- **Grand Master:** For the system-responsible, or chief user
- **Installer code:** for the installer/technician
- **Sub-installer:** for an installer/technician sent to carry out restricted tasks (restricted access) that are defined at the time of system installation by the primary installer/technician
- **Code length:** Configure code length for Grand Master, installer and sub-installer (also configure per Grade requirement)
  NOTE: The installer designate codes to be either 4 or 6 digits in length. If defined as 6 digits, the length apply for everybody - all users/installers, however if defined as 4 digits, Grand Master, Installer, and Sub-Installer must have 4-digit codes, while system users can have codes of various lengths, from 1—4 digits.

The installer typically performs the following for the user codes:

- Determines the authority level for each system user (default level is **User**)
- Designates which partitions can be operated (armed/disarmed) per user code
- Changes the Grand Master, installer, and sub-installer codes
- Modifies code length as necessary (see note above under Code Length)

④① User

Define user codes by assigning each user a specific authority level and specific partitions. Up to 499 codes for system users (including Grand Master) can be defined in the system.

Note

For defining user codes, see *Defining User Codes, page 53*.

Codes → User

Quick keys	Parameter	Default	Range
④① YYY❶	**Partition**		
	Specify the partition(s) for which the designated user can have access by using. Press a number to assign, or press the same number again to clear it.		
④① YYY❷	**Authority Level**		
	Assign the authority level of each user (for each user code). There are 8 authority levels (not including the Grand Master level). Toggle between the different levels: • **Master**: There are no restrictions in the number of master codes (as long as they do not exceed the number of codes remaining in the system). o Restricted to assigning and changing user codes belonging to those with authority levels of master and below (user, arm only, maid, unbypass, guard, UO/Door control) o Restricted access to designated partitions • **User**: There are no restrictions in the number of user codes (as long as they do not exceed the number of codes remaining in the system). The user has access to the following: o Arming and disarming o Bypassing zones o Accessing designated partitions o Viewing system status, trouble, and alarm memory o Resetting the switched auxiliary output o Activating designated utility outputs o Changing his/her own user code • **Arm Only**: There are no restrictions in the number of Arm Only codes (as long as they don't exceed the number of codes remaining in the system). Arm Only codes are useful for workers who arrive when the premises are already open, but because they are last to leave, they're given the responsibility to close the premises and arm the system. The users with Arm Only codes have access for arming one or more partitions, and cannot change their own code.		

Quick keys	Parameter	Default	Range
	• **Maid**: The maid code is a temporary code, which is automatically and immediately deleted from the system as soon as it is used to arm. This code is typically used for maids, home attendants, and repairmen who must enter the premises before the owner(s) arrive. These codes are used as follows: o For one-time arming in one or more partitions. o If first used to disarm the system, the Maid code may be used once for subsequent arming. o After deleted, the code will need to be redefined by the Grand Master for the next usage. o Cannot change own code • **Unbypass**: This user has access to all the user's privileges apart from bypassing zones. • **Guard**: This user can arm/disarm the system. After entering the Guard code, the system will be disarmed for the predefined time period. The user can also decide to arm the system before the automatic predefined time period (See: *Guard Delay page 59*). • **Duress**: When forced to disarm the system (under duress), the system sends a duress alarm to the monitoring station, but the panel is silent. The duress code can be used by all system users, regardless of authority level. • **UO/Door Control:** o Used to operate Utility Output(s) o Used to operate Door Control o Cannot change own code		

④② Grand Master

Codes → Grand Master

Default = **1234.** The Grand Master code is used by the system-responsible (for example, the owner), and has the highest authority level. The Grand Master can change the Grand Master code (in the User menu).

Notes

- The Grand Master is index number 00.
- The Grand Master, the installer and the sub-installer can enter and change their codes, but the new codes entered don't display at the keypad – instead **** displays .

④③ Installer

Codes → Installer

Default = **1111.** The Installer code provides access to the installer Programming menu as well as all other installer menus, allowing modification of system parameters. The installer can change the installer code.

④④ Sub Installer

Codes → Sub-installer

Default = **2222.** The sub-installer code allows limited access to selected installer programming parameters. It is recommended to change the code to one that is unique. The sub-installer is prohibited from accessing the following parameters:

- **Default enable** (to change the panel back to default factory settings)
- **Code length**
- **Installer code**
- **Communication menu**
- **Customer ID**
- **Standards**

④⑤ Code Length

Codes → Code Length

The installer, sub-installer, and Grand Master can define the number of digits. The installer designates the codes to be either 4 or 6 digits in length. If defined as 6 digits, the length apply for everybody - all users/installers, however if defined as 4 digits, Grand Master, Installer, and Sub-Installer must have 4-digit codes, while the system users can codes of various lengths, from 1—4 digits.

Notes

- When you change the code length parameter, all user codes are deleted and must be re-programmed or downloaded.
- For a 6-digit code length system, 4-digit default codes like 1-2-3-4 (Grand Master), 1-1-1-1 (Installer), and 2-2-2-2 (Sub-Installer) become 1-2-3-4-0-0, 1-1-1-1-0-0, and 2-2-2-2-0-0, respectively.
- If you change the code length back to 4 digits, the system codes are restored to the default 4-digit codes.

EN 50131 Notes

- If EN 50131 Grade 2 is selected, all users code length must be exactly 4 digits: xxxx
- In any configuration, UO Controller code length are up to 6 digits.
- For each digit 0-9 can be used
- Invalid codes cannot be created since after 4/6 digits are input, the "Enter" is automatic.
- Codes are rejected when trying to create a code in the wrong format.

⑤ Communication

Define the following parameters for establishing system communication:

- **Method**
- **Monitoring Station**
- **Configuration Software**
- **Follow Me**
- **Cloud**

⑤① Method

Define communication channel parameters for the following methods:

- **GSM**
- **IP**

Communication → Method → GSM

Quick Keys	Parameter	Default	Range
⑤①②	**GSM**		
	The GSM screen contains parameters for the communication of the system over the GSM/GPRS/3G/4G network.		
⑤①②①	**Timers**		
	Allows to program timers related to operation with the GSM module		
⑤①②①❶	**GSM Lost**	1 minute	001—255 minutes
	The period length during which the reception is below the minimum threshold (defined by the GSM Network Sensitivity parameter) that triggers the panel to send a report of GSM Lost. (⑤①②⑤ ❹)		
⑤①②①❷	**GSM Network Loss**	10 minutes	001—255 minutes
	The period length after which the panel will send a report of GSM network loss to the monitoring station.		

⑤①②①❸	**SIM Expire**	0 months	00—36 months
	A pre-paid SIM card has a defined life length defined by the provider. After each charging of the SIM, the user will have to manually reset the expiration time of the SIM card. Thirty days before the expiring date, a notification will be displayed on the keypad's LCD. Set the SIM expiring date (in months) using the numeric keys, according to the time given by the provider.		
⑤①②①❹	**MS Polling**	00000	0—65535 times

The time period that the system will establish automatic communication (polling) with the monitoring station over GPRS/3G/4G, in order to check the connection.

3 polling times can be defined: Primary, Secondary and Backup. For each time period define the number of units between 1- 65535. Each unit represents a time frame of 10 seconds.

Notes

- When using the polling feature through GPRS/3G/4G the MS channel parameter must be defined as GPRS/3G/4G only.
- The report code for MS polling is 999 (Contact ID) or ZZ (SIA)
- When the GPRS/3G/4G Primary polling time is defined as 0, no polling message is sent to the MS

The use of these time periods depends on the reporting order to the MS defined by the Report Split MS Urgent parameter. See: ⑤①② (**Communication → MS → Report Split**).

The following table describes how the three MSs use the primary, secondary and backup time intervals in the various MS report split options.

MS report Urgent events	MS 1 Polling State	MS 2 Polling State	MS 3 Polling State
Do not call	N/A	N/A	N/A
Call 1st	Primary	N/A	N/A
Call 2nd	N/A	Primary	N/A
Call 3rd	N/A	N/A	Primary
Call All	Primary	Primary	Primary

1st Backup 2nd	Primary	If (MS 1 is OK) Secondary else (MS#1 Fails) Backup	N/A
1st Backup 2nd3rd	Primary	If (MS#1 is OK) Secondary else (MS#1 Fails) Backup	If (MS#2 is OK) Secondary else (MS#2 Fails) Backup
1st Backup 3rd Call 2nd	Primary	Primary	If (MS#1 is OK) Secondary else (MS#1 Fails) Backup
2nd Backup 3rd Call 1st	Primary	Primary	If (MS#2 is OK) Secondary else (MS#2 Fails) Backup

MS Polling example:
When selecting MS 1 (GPRS/3G/4G), MS 2 (GPRS/3G/4G) and split report option 1st Backup 2nd (using the default primary, secondary and backup time intervals), the report process will be as follows:
In a normal state:
Polling through the GPRS/3G/4G network using the GSM module will occur every 90 seconds according to the primary time interval to MS 1 and every 3600 seconds (1 hour) according to the secondary time interval to MS 2.
When communication to MS 1 fails, polling occurs every 90 seconds according to the backup interval to MS 2. When communication returns to MS 1, polling reverts back to the secondary time interval and occurs every 3600 seconds (1 hour) to MS#2.

⑤①②②	**GPRS**		
	Allows programming parameters that relate for the communication over the GPRS/3G/4G network.		
⑤①②②❶	**APN Code**		
	To establish a connection to the GPRS/3G/4G network an APN (Access Point Name) code is required. The APN code differs from country to country and from one provider to another (the APN code is provided by your cellular provider). The LightSYS Air supports an APN code field of up to 30 alphanumeric characters and symbols (!, &, ? etc.).		
⑤①②②❷	**APN User Name**		
	Enter user name for the GPRS/3G/4G network (if required). The user name is provided by your provider. The LightSYS Air supports a user name field of up to 20 alphanumeric characters and symbols (!, &, ? etc.).		
⑤①②②❸	**APN Password**		
	The password to the GPRS/3G/4G network as provided by your provider (if required). The LightSYS Air supports a user name field of up to 20 alphanumeric characters and symbols.		
⑤①②③	**Email**		
	The following programming parameters are used to enable sending Follow Me event messages by e-mail through GPRS/3G/4G. **Note** To enable e-mail messaging, the GPRS/3G/4G parameters have to be defined.		
⑤①②③ ❶	**Mail Host**	000.000.000.000	
	The IP address or the host name of the SMTP mail server.		
⑤①②③ ❷	**SMTP Port**	00000	00000—65535
	The port address of the SMTP mail server.		
⑤①②③ ❸	**Email Address**		
	The Email address that identifies the system to the mail recipient.		

⑤①②③ ❹	**SMTP User Name**		
	A name identifying the user to the SMTP mail server The user name field can include up to 10 alphanumeric characters and symbols (!, &, ? etc.).		
⑤①②③ ❺	**SMTP Password**		
	The password authenticating the user to the SMTP mail server The password can include up to ten alphanumeric characters and symbols (!, &, ? etc.).		
⑤①②④	**Controls**		
	Allows controlling timers related to operation with the GSM module.		
⑤①②④❶	**Caller ID**	No	Yes/No
	The Caller ID function enables to restrict SMS remote control operations to the predefined Follow Me phone numbers. If the incoming number is recognized as one of the Follow Me numbers, the operation will be executed.		
⑤①②④❷	**LED Enable**	No	Yes/No
	Defines whether or not the LEDS operation mode is enabled		
⑤①②⑤	**Parameters**		
	Allows to program timers related to the operation with the GSM module.		
⑤①②⑤❶	**PIN Code**		
	The PIN (Personal Identity Number) code is a 4 to 8 digit number giving you access to the GSM network provider. **Note** You can cancel the PIN code request function by inserting the SIM card into a regular mobile phone and according to the phone settings, disable this function.		
⑤①②⑤❷	**SIM Number**		
	The SIM phone number. The system uses this parameter to receive the time from the GSM network in order to update the system time.		
⑤①②⑤❸	**SMS Center Phone**		
	A telephone number of the message delivery center. This number can be obtained from the network operator.		

⑤①②⑤❹	**GSM RSSI**		Disabled/Low/High
	Set the minimum acceptable network signal level (RSSI level). Options: Disabled (No troubles for low signal reception) / Low signal / High signal		
⑤①②⑥	**Prepay SIM**		
	Allows programming parameters that will be used when a prepaid SIM card is used in the system.		
⑤①②⑥❶	**Get Credit by**		
	Depending on the local network provider, the user can receive the credit level of the prepaid SIM card by sending a predefined SMS command to a defined number. The activation of the credit request can be done by the Grand Master. • **SMS Credit Message**: Enter the message command as defined by the provider and the provider's phone number to which the credit level SMS message request will be sent. • **Service Command**: Enter the service command message as defined by the provider.		
⑤①②⑥❷	**Phone To Send**		
	The provider's phone number to which the credit level SMS message request will be sent to or a call will be established, depending on the selection in the Get Credit by parameter.		
⑤①②⑥❸	**Phone To Receive**		
	The provider's telephone number from which an automatic SMS credit status message will be sent from.		
⑤①②⑥❹	**SMS Message**		
	When performing manual Credit Level check this message will be sent to the provider in order to receive the SIM card credit. The message is predefined (for example "BILL") by your service provider. * When using a service command this field is ignored.		

Communication → Method → IP

Quick Keys	Parameter	Default	Range
⑤①③	**IP**		
	The IP menu contains parameters for the communication of the system over the IP network.		
⑤①③❶	**IP Config**		

	The IP menu contains parameters for the communication of the system over the IP network.		
⑤①③①❶	**Obtain IP**		
	Defines automatically whether the IP address, which the LightSYS Air refers to, is dynamic or static.		
⑤①③①①❶	**Dynamic IP**		
	The system refers to an IP address provided by the DHCP.		
⑤①③①①❷	**Static IP**		
	The system refers to a static IP Address.		
⑤①③①❷	**Panel Port**		
	The LightSYS Air Port address.		
⑤①③①❸	**Panel IP (Only for Static IP)**		
	The LightSYS PlusLightSYS Air static IP address		
⑤①③①❹	**Subnet Mask (Only for Static IP)**		
	The subnet mask is used to determine where the network number in an IP address ends.		
⑤①③①❺	**Gateway (Only for Static IP)**		
	The IP address of the local Gateway, which enables communication settings to other LAN segments. This address is the IP address of the router connected to the same LAN segment as the LightSYS PlusLightSYS Air.		
⑤①③①❻	**DNS Primary (Only for Static IP)**		
	The IP address of the primary DNS server on the network.		
⑤①③①❼	**DNS Secondary (Only for Static IP)**		
	The IP address of the secondary DNS server on the network.		

⑤①③①❽	**WiFi Scan**		
	Scans for Wi-Fi Network		
⑤①③①❾	**Add WiFi Net**		
	Add Wi-Fi Network		
⑤①③①⑨❶	**Name**		
	Add Wi-Fi Network Name		
⑤①③①⑨❷	**Security type**		
	Add Wi-Fi Security type		
⑤①③①⑨❸	**Connect**		
	Connect to the Wi-Fi		
⑤①③①❶⓿	**WPS Button**		
	Press the WPS button on the router to establish a connection. A "Successfully Connected" to network message will appear within 2 min.		
⑤①③②	**Email**		
	Allows programming parameters that enable the system to send e-mail messages following Follow Me events		
⑤①③②❶	**Mail Host**	000.000.000.000	
	The IP address or the host name of the SMTP mail server.		
⑤①③②❷	**SMTP Port**	00000	00000—65535
	The port address of the SMTP mail server		
⑤①③②❸	**Email Address**		
	The e-mail address that identifies the system to the mail recipient.		
⑤①③②❹	**SMTP Name**		
	A name identifying the user to the SMTP mail server. Its field can include up to 10 alphanumeric characters and symbols (!, &, ? etc.).		
⑤①③②❺	**SMTP Password**		
	The password authenticating the user to the SMTP mail server. It can include up to 10 alphanumeric characters and symbols (!, &, ? etc.).		

⑤①③③	**Host Name**	Security System	Up to 32 Characters
	IP address or a text name used to identify the LightSYS Air over the network. Default: **Security System**		
⑤①③④	**MS Polling (Keep Alive)**		

The time period that the system will establish automatic communication (polling) with the monitoring station over the IP network, in order to check the connection. Three polling times can be defined: primary, secondary and backup. For each time period, define the number of units between 1–65535. Each unit represents a time frame of 10 seconds.

Note

When using the polling feature through IP, the MS channel parameter must be defined as IP only.

The use of these time periods depends on the reporting order to the MS defined by the report split MS urgent parameter (see *MS Urgent, page 135*). The following table describes how the three MSs use the primary, secondary & backup time intervals in the various MS report split options:

MS report Urgent events	MS 1 Polling State	MS 2Polling State	MS 3 Polling State
Do not call	N/A	N/A	N/A
Call 1st	Primary	N/A	N/A
Call 2nd	N/A	Primary	N/A
Call 3rd	N/A	N/A	Primary
Call All	Primary	Primary	Primary
1st Backup 2nd	Primary	If (MS 1 is OK) Secondary else (MS#1 Fails) Backup	N/A
1st Backup 2nd3rd	Primary	If (MS#1 is OK) Secondary else (MS#1 Fails) Backup	If (MS#2 is OK) Secondary else (MS#2 Fails) Backup
1st Backup 3rd Call 2nd	Primary	Primary	If (MS#1 is OK) Secondary else (MS#1 Fails) Backup
2nd Backup 3rd Call 1st	Primary	Primary	If (MS#2 is OK) Secondary else (MS#2 Fails) Backup

	MS Polling example: When selecting MS 1 (IP Only), MS 2 (IP only) and split report option 1st Backup 2nd (using the default primary, secondary and backup time intervals), the report process will be as follows: In a normal state: Polling through the IP network using the IP will occur every 30 seconds according to the primary time interval to MS 1 and every 3600 seconds (1 hour) according to the secondary time interval to MS 2. When communication to MS 1 fails, polling occurs every 30 seconds according to the backup interval to MS 2. When communication returns to MS 1, polling reverts back to the secondary time interval and occurs every 3600 seconds (1 hour) to MS#2		
⑤①③⑤	**Controls**	No	Yes/No
	Enable or disable IP Communication		

⑤② Monitoring Station

Define the following, which enable the system to establish communication with up to three monitoring station accounts:

- **Report Type**
- **Accounts**
- **Communications Format**
- **Controls**
- **Parameters**
- **MS Timers**
- **Report Split**
- **Report Codes**

Communication → Monitoring Station → Report Type

Quick Keys	Parameter
⑤②⓪	**MS Mode**
	Select to Enable or Disable the MS mode
⑤②①	**Report Type ⓪**
	Defines the communication type that the system will establish with each monitoring station account. The system can report in these (optional) communication channels: IP, SMS, LRT, SIA IP. **NOTE:** If there is a communication fault with the monitoring station the panel will not be ready to arm.
⑤②① ❶–❸	**Select MS**
	Scroll to select the monitoring station account (MS 1—MS 3) for which you want to define the reporting type, and then press **OK.**
⑤②①①–③ ❶–❺	**MS Channel**
	Scroll to select the communication channel to use for reporting to the monitoring station account, and then press **OK:** ② IP ③ SMS ⑤ SIA IP
⑤②①①–③ ❷	**IP**

Quick Keys	Parameter
	Encrypted events are sent to the monitoring station over the IP or GPRS/3G/4G network using TCP/IP protocol. 128 BIT AES encryption is used. RISCO Group's IP/GSM Receiver Software located at the MS site receives the messages and translates them to standard protocols used by monitoring station applications (For example; contact ID). **Note** To enable GPRS/3G/4G communication the SIM card has to support GPRS/3G/4G channel. Reporting by IP can be established through different channels. The optional channels depend on the hardware installed in your system. Select the required channel via the Configuration Software as follows: 1. **IP/GPRS**: The panel checks for the availability of the IP network. During regular operation mode all calls and data transmission are carried out using the IP network line. In the case of trouble in the IP network, the report is routed to the GPRS/3G/4G network. 2. **GPRS/IP**: The panel checks for the availability of the GPRS/3G/4G network. During regular operation mode all calls and data transmission are carried out using the GPRS/3G/4G. In 7the case of trouble the report is routed to the IP network. 3. **IP Only**: The report is executed through the IP network only. 4. **GPRS Only**: The report is executed through the GPRS/3G/4G network. Enter the relevant IP and Port numbers for the MS that will receive reports from the system (See IP and Port)
⑤②①①–③ ❸	**SMS**
	Enter the relevant phone numbers for the monitoring station that will receive reports from the system via encrypted SMS Events are sent to the monitoring station using encrypted SMS messages (128 BIT AES encryption). Each event message contains information including the account number, report code, communication format, time of event and more. The event messages are received by RISCO's IP Receiver software located at the monitoring station site. The IP Receiver translates the SMS messages to standard protocols used by the monitoring station applications (For example; contact ID). This channel requires that RISCO Group's IP/GSM receiver has to be used at the MS side.

Quick Keys	Parameter
⑤②①✪ ❺	**SIA IP**
	NOTE: ✪ = monitoring station (MS) account Reports to the monitoring station can be transmitted using the SIA IP protocol to standard SIA IP receivers. Using SIA IP enables transmission of visual imagery from PIR cameras. Reporting by SIA IP can be established through the hardware channels installed in your system. Reporting of the SIA IP is 128 BIT AES encrypted. SIA IP reports also support labels reporting. Usage of SIA IP requires setting. See: ⑤②⑤③ • Encryption Key • SIA IP Receiver Number • SIA IP Receiver Line Number

Communication → Monitoring Station → Accounts

Quick Keys	Parameter
⑤②②	**Accounts**
	The number that recognizes the customer at the monitoring station, you can define an **account number** for each monitoring station (1—3 possible). Account numbers are 6-digitnumbers in length, and are assigned by the central station. ➢ **To edit an MS account number (code):** 1. From the **installer Programming menu,** go to: **5 → 2 → 2** 2. Scroll to the MS account (❶, ❷ or ❸), and then press **OK** (✓). 3. Define/modify the code as needed, per the communication format notes below: **Notes** **Notes for Account Number in Contact ID Communication Format**: • The account number will always be reported as 4 digits, for example: A number defined as 000012 will be reported as 0012 • If more than 4 digits were defined, the system always sends the last 4 digits of the account number, for example: Account number that was defined as 123456 will be sent as 3456. • In Contact ID you can place digits and letters A–F. The A character is always sent as 0 for example: Account number that was defined as 00C2AB will be sent as C20B. **Notes for Account Number in SIA Communication Format:**

Quick Keys	Parameter
	• Account number for SIA should be defined as a decimal number (Only digits 0..9) • Account number can be reported as 1 to 6 digits. To send an account number with less than 6 digits use the "0" digit, for example: For account number 1234 enter 001234. In this case the system will not send the "0" digit to the monitoring station. • In order to send the "0" digit in SIA format, located at the left side of the number, use the "A" digit instead of the "0" digit. For example, for account number 0407 enter 00A407, for a 6 digit account number such as 001207 enter AA1207.
⑤②② ❶	**Partition (MS Accounts per Partition)**
	You can specify the monitoring station account(s) to notify upon events that occur for the partitions you select (there are 32 partitions maximum per system). If you selected partition(s) from 1—3, you then choose the monitoring station account(s) to notify (1—3) for each, followed by entering the respective account numbers (codes). If you selected partition(s) from 4—32, you then enter the account numbers (codes); all monitoring station accounts will be automatically notified for events occurring in these partitions. ➢ **To designate MS accounts per partition:** 1. From the **installer Programming menu,** go to: **5 → 2 → 2 (Communication →MS → Accounts)** 2. Scroll to **01)Partition,** and then press **OK** (✓). 3. Select a partition number and then press **OK.** 4. [If you selected partition 1—3]: Scroll to the MS account (❶, ❷ or ❸), press **OK**, enter the MS account number (code), and press **OK.** 5. [If you selected partition 4—32]: Enter the MS account number (code) and press **OK.** 6. Repeat this procedure for all additional monitoring station accounts-per-partition designations **NOTE:** Advanced configuration options are also available from the Configuration Software.

Communication → Monitoring Station → Communications Format

Quick Keys	Parameter
⑤②❸	**Communications Format**
	Enables the system to communicate to the monitoring station. **Note** See *Appendix E:* *, page 177*. ❶ **Contact ID:** The system allocates Report Codes supporting Contact (Point) ID ❷ **SIA:** The system allocates Report Codes supporting SIA (Security Industry Association) format

Communication → Monitoring Station → Controls

Quick Keys	Parameter	Default	Range
⑤②④	**Controls**		
	Programmable controls related to communication between the system and the monitoring station		
⑤②④❶	**Call Save**	No	Yes/No
	YES: For reducing MS traffic congestion, the system holds all non-urgent events (for example, opening/closing reports, test transmissions) for up to 12 hours (programmable) and sends them as a batch at a less busy time, for example, at night (see *Periodic Test, page 133*). **NO**: All events are transmitted as they occur.		
⑤②④❷	**Show Kissoff**	No	Yes/No
	YES: The keypad indicates when the dialer receives the kissoff signal from the MS's receiver. **NO**: The keypad does not indicate on receipt of the kissoff signal.		
⑤②④❸	**Show Handshake**	No	Yes/No
	YES: The keypad indicates when the dialer receives the handshake signal from the monitoring station's receiver. **NO**: No indication for establishing communication with the MS's receiver		

Quick Keys	Parameter	Default	Range
⑤②④❹	**Audible Kissoff**	No	Yes/No
	YES: There is an audible sound emitted from the keypad when the dialer receives the kissoff signal from the monitoring station's receiver. **NO**: There is no audible sound on receipt of the kissoff signal.		
⑤②④❺	**SIA Text**	No	Yes/No
	Yes: SIA format report to monitoring station will support text transmission over the voice channel. **Note** The monitoring station receiver should support the SIA Text protocol **No**: SIA format will not support text		
⑤②④❻	**Random MS Testing**	No	Yes/No
	Yes: At power-up the panel randomly set a test time between 00:00 and 23:59. Once the hour is set, this will be the fixed report hour of this panel. The time can be viewed under the Periodic test timer fields (⑤②⑥❶). The interval of sending the test will be as defined under the Periodic Test timer **No**: The periodic test will be according to the time defined under the MS periodic timer (⑤②⑥❶).		
⑤②④❼	**SIA W/Partition**	No	Yes/No
	Indicates the partition when reporting to the monitoring station in SIA over the voice channel (GSM). **Yes**: SIA format report to MS will support text transmission over the voice channel. **Note** The monitoring station receiver should support the SIA Text protocol **No**: SIA format will not support text		
⑤②④❽	SIA CH Info	No	Yes/No
	When the panel transmits events to the monitoring station, additional MS channel type information (whether by IP or GPRS) is provided with the transmitted event. **Yes**: Additional MS channel type information is provided with the transmitted event. **No**: Additional MS channel type information is not provided with the transmitted event.		

Communication → Monitoring Station → Parameters

Quick Keys	Parameter	Default	Range
⑤②⑤	**Parameters**		
	Programmable parameters related to operation with the MS		
⑤②⑤❶	**MS Retries**	08	01—15
	The number of times the LightSYS Air redials the monitoring station after failing to establish communication. **NOTE:** If there is a communication fault with the monitoring station the panel will not be ready to arm.		
⑤②⑤❷	**Alarm Restore**		
	Specifies under what conditions an Alarm Restoral is reported. This option informs the MS of a change in the specified condition(s) during an alarm restore. These reports need a valid Report Code. ❶ **ON BTO (Bell Time Out) –** Reports the restoral after the audible alarm times out. ❷ **FOLLOW ZONE –** Reports the restoral when the zone in which the alarm occurs returns to its non-violated (secured) state. ❸ **AT DISARM** – Reports the restoral when system (or the partition in which the alarm occurs) is disarmed, even if the siren has timed out.		
⑤②⑤❸	**SIA IP Param.**		
	Define the following SIA IP parameters for each monitoring station account (MS1, MS2, and MS3): **1) Encryption Key** **2) Receiver Number** **3) Line Number**		
	❶ Encryption Key A 32-digit digital signature and authentication for purposes of safeguarding data transmission to and from the monitoring station. The key must be defined for both the panel and monitoring station. For use when SIA IP report type is in effect. A unique key can be defined for each of up to three monitoring stations.		
	❷ Receiver Number A 4 digit number which states the SIA IP receiver number as supplied from the monitoring station. A unique key can be defined for each of up to three monitoring stations.		
	❸ Line Number A 4 digit number which states the SIA IP receiver line number as		

Quick Keys	Parameter	Default	Range
	supplied from the monitoring station. A unique key can be defined for each of up to three monitoring stations.		

Communication → Monitoring Station → MS Timers

Quick Keys	Parameter	Default	Range
⑤②⑥	**MS Times**		
	Allows programming timers related to operation with the monitoring station.		
⑤②⑥❶	**Periodic Test**		HR = 0--24 MIN = 0—59 D = per table below
	The Periodic Test enables you to set the time period that the system will automatically establish communication to the monitoring station in order to check the connection. The periodic test involves sending the account number and a valid test report code (Contact ID 602, SIA TX). Set the test time and daily interval for Periodic Test Reporting. Use the table below to specify the daily testing intervals (D)-effective from the day of programming:		

D	Meaning
0	Never
H	Every hour
1	Every day
2	Every other day
3	Every 3rd day
4	Every 4th day
5	Every 5th day
6	Every 6th day
7	Once a week

Quick Keys	Parameter	Default	Range
⑤②⑥❷	**Abort Alarm**	15 secs	00-255 seconds
	Defines the time delay before reporting an alarm to the monitoring station. If the alarm system is disarmed within the abort window, no alarm transmission shall be sent to the monitoring station.		
⑤②⑥❸	**Cancel Delay**	5 mins	00-255 minutes
	If an alarm is sent in error, it is possible for the monitoring station to receive a cancel alarm code, sent subsequently to the initial alarm code. This happens if a valid user code is entered to reset the alarm in the cancel delay time window that starts after the defined abort alarm time is over. **Note** Ensure that Cancel Alarm report code is defined.		
⑤②⑥⑤	**Confirmation**		
	These confirmation times relate to the zone's sequential confirmation (see ②④) - *Alarm Confirm, page 100*).		
⑤②⑥⑤❶	**Confirm Start (Confirm delay time)**	000	1—120 minutes
	Specifies that the system cannot start a sequential confirmation process until the timer has expired. This time starts when the system has been armed and will prevent confirmed alarms being generated in situations when a person has been accidentally locked in the building.		
⑤②⑥⑤❷	**Confirm Time (Confirmation Time Window)**	030	30—60 minutes
	Specifies a time period that starts when an intrusion alarm is triggered for the first time. If a second intrusion alarm is triggered before the end of the time period (the "confirmation time window"), the system will then send a "confirmed" alarm notification to the monitoring station.		

Communication → Monitoring Station → Report Split

Quick Keys	Parameter	Default	Range
⑤②⑦	**Report Split**		
	The Report Split menu contains parameters that enable the routing of specified events to up to three monitoring station (MS) receivers.		
⑤②⑦❶	**MS Arm/Disarm**	1st backup 2nd	
	Reports Arming/Disarming (meaning Closings/Openings) events to the monitoring station (MS): ❶ **Do not call** (no report). ❷ **Call 1st:** Reports Openings and Closings to MS 1. ❸ **Call 2nd:** Reports Openings and Closings to MS 2. ❹ **Call 3rd:** Reports Openings and Closings to MS 3. ❺ **Call all:** Reports Openings and Closings to the all defined MS. ❻ **1st Backup 2nd:** Reports Openings and Closings to MS 1. If communication is not established, calls MS 2. ❼ **1st Backup 2nd 3rd**: Reports to MS 1. If communication is not established calls MS 2. If communication is not established again calls the MS. ❽ **1st Backup 3rd Call 2nd:** Reports MS 1. If communication is not established calls to MS 3. In addition it will also call MS 2. ❾ **2nd Backup 3rd Call 1st:** Reports to MS 2. If communication is not established calls MS 3. In addition it will also call MS 1.		
⑤②⑦❷	**MS Urgent**	1st backup 2nd	
	Reports urgent (alarm) events to the monitoring station (MS): ❶ **Do not call** (no report) ❷ **Call 1st:** Reports Openings and Closings to MS 1. ❸ **Call 2nd:** Reports Openings and Closings to MS 2. ❹ **Call 3rd:** Reports Openings and Closings to MS 3. ❺ **Call all:** Reports Openings and Closings to the all defined MS. ❻ **1st Backup 2nd:** Reports Openings and Closings to MS 1. If communication is not established, calls MS 2. ❼ **1st Backup 2nd 3rd:** Reports to MS 1. If communication is not established calls MS 2. If communication is not established again calls the MS. ❽ **1st Backup 3rd Call 2nd:** Reports MS 1. If communication is not established calls to MS 3. In addition it will also call MS 2. ❾ **2nd Backup 3rd Call 1st:** Reports to MS 2. If communication is not established calls MS 3. In addition it will also call MS 1.		

Quick Keys	Parameter	Default	Range
⑤②⑦❸	**MS Non Urgent**		
	Reports non-urgent events (supervisory troubles and test reports) to the monitoring station (MS): ❶ Do not call (no report) ❷ **Call 1st:** Reports Openings and Closings to MS 1. ❸ **Call 2nd**: Reports Openings and Closings to MS 2. ❹ **Call 3rd**: Reports Openings and Closings to MS 3. ❺ **Call all**: Reports Openings and Closings to the all defined MS. ❻ **1st Backup 2nd**: Reports Openings and Closings to MS 1. If communication is not established, calls MS 2. ❼ **1st Backup 2nd 3rd**: Reports to MS 1. If communication is not established calls MS 2. If communication is not established again calls the MS. ❽ **1st Backup 3rd Call 2nd**: Reports MS 1. If communication is not established calls to MS 3. In addition it will also call MS 2. ❾ **2nd Backup 3rd Call 1st:** Reports to MS 2. If communication is not established calls MS 3. In addition it will also call MS 1.		

Communication → Monitoring Station → Report Codes

Quick Keys	Parameter	Default	Range
⑤②⑧	**Report Codes**		
	Enables you to view or program the codes transmitted by the system to report events (for example, alarms, troubles, restores, supervisory tests, and so on) to the monitoring station. The codes specified for each type of event transmission are a function of the central station's own policies. Before programming any codes, it is important to check the central station protocols. Reporting codes are assigned by default, according to the selected communication format SIA or contact ID. Assigns a specified report code for each event, based on the reporting format to the monitoring station. An event that is not assigned with a report code will not be reported to the monitoring station. For list of report events see *Monitoring Station Report Codes, page 178*. **NOTE:** Using a double-zero (00) for any event will prevent a report from being generated.		
⑤②⑧❶	**Edit Codes**		

Quick Keys	Parameter	Default	Range
	For each code type, edit their respective parameters as needed.		
⑤②⑧①❶	**Alarms**		
⑤②⑧①❶❶	**Panic**		
⑤②⑧①❶❷	**Fire**		
⑤②⑧①❶❸	**Medical**		
⑤②⑧①❶❹	**Duress**		
⑤②⑧①❶❺	**Confirm Alarm**		
⑤②⑧①❶❻	**Box Tamper**		
⑤②⑧①❶❼	**Bell Tamper**		
⑤②⑧①❶❽	**Recent close**		
⑤②⑧①❶❾	**HU Confirm**		
⑤②⑧①❷	**Main Troubles**		
	Common system trouble parameters.		
⑤②⑧①❷❶	**Low Battery**		
⑤②⑧①❷❹	**AC Loss**		
⑤②⑧①❷❻	**Clk Not Set**		
⑤②⑧①❷❽	**False Code**		
⑤②⑧①❷❾	**GSM Trouble**		
⑤②⑧①❷10	**IP Net Trbl**		
⑤②⑧①❷11	**MS 1 Trouble**		
⑤②⑧①❷12	**MS 2 Trouble**		
⑤②⑧①❷13	**MS 3 Trouble**		
⑤②⑧①❸	**Arm/Disarm**		
	Set arming/disarming parameters.		
⑤②⑧①❸❶	**User**		
⑤②⑧①❸❷	**Automatic**		

Quick Keys	Parameter	Default	Range
⑤②⑧①❸❸	**Remote**		
⑤②⑧①❸❹	**Force Arm**		
⑤②⑧①❸❺	**Quick Arm**		
⑤②⑧①❸❻	**Keyswitch**		
⑤②⑧①❸❼	**Auto Arm Fail**		
⑤②⑧①❹	**Zones**		
	Set zone-related parameters.		
⑤②⑧①❹❶	**By Zone**		
⑤②⑧①❹❷	**Zone Lost**		
⑤②⑧①❹❸	**Soak Fail**		
⑤②⑧①❹❹	**Self Test**		
⑤②⑧①❺	**Accessories**		
	Edit parameters for system peripheral devices/accessories.		
⑤②⑧①❺❶	**Keypad**		
⑤②⑧①❺❸	**Util. Output**		
⑤②⑧①❺❺	**Keyfob**		
⑤②⑧①❻	**Miscellaneous**		
	Edit codes and other miscellaneous parameters		
⑤②⑧①❻❶	**Enter Prog.**		
⑤②⑧①❻❷	**Exit Prog.**		
⑤②⑧①❻❸	**MS Periodic Test**		
⑤②⑧①❻❹	**System Reset**		
⑤②⑧①❻❺	**Abort Alarm**		
⑤②⑧①❻❼	**MS Polling**		
⑤②⑧①❻❽	**Cancel Rprt.**		

Quick Keys	Parameter	Default	Range
⑤②⑧①❻❾	**Walk test**		
⑤②⑧①❻10	**Exit Error**		
⑤②⑧①❻11	**Fail Cloud**		
⑤②⑧①❻12	**Entry Service Mode**		
⑤②⑧①❻13	**Exit Service Mode**		
⑤②⑧❷	**Delete All**		
	Clears all codes (reverts to factory defaults)		

⑤③ Configuration SW

Configure the following parameters for communication between the Configuration Software and the system:

- **Security**
- **Controls**
- **Gateway**

Communication → Configuration SW → Security

Quick Keys	Parameter	Default	Range
⑤③①	**Security**		
	Enables you to set parameters for remote communication between the technician and the system using the Configuration Software		
⑤③①❶	**Access Code**	5678	
	Enables you to define an up-to six-alpha-numeric-character installation access code. In order to enable communication between the alarm company and the system the same access code must subsequently be entered into the corresponding account profile created for the installation in the Configuration Software. For successful communication, the access code along with the ID code must match between the Configuration Software and the system.		

Quick Keys	Parameter	Default	Range
⑤③①❷	**Remote ID**	0001	
	Defines an ID code that serves as an extension of the access code. In order to enable communication between the alarm company and the installation, the same remote ID code must be entered into the account profile in the Configuration Software. For successful communication, the ID code along with the access code must match between the Configuration Software and the main panel. Dealers often use the customer's monitoring station account number for the ID code, but you can use any 4-digit code unique to the installation.		
⑤③①❸	**MS Lock**	000000	
	MS Lock is a security function used in conjunction with the Configuration Software. It provides greater proprietary security when viewing monitoring station parameters. The same 6-digit code, which will be stored in the panel, must be entered into the corresponding account profile created for the installation in the Configuration Software. If there is no match between the MS Lock code defined in the main panel and the MS Lock code defined in the Configuration Software, the installer will not have permission to change the following monitoring station parameters from the Configuration Software: MS Lock, Installer Code, MS IP Port, MS IP Address, MS Phone, Default Enable, MS Account, MS Format, MS Channel, MS Backup, MS Enable, Remote ID, Access Code.		

Communication → Configuration SW → Controls

Quick Keys	Parameter	Default	Range
⑤③③	**Control**		
⑤③③ ❶	**User Initiated Call**	Yes	Yes/No
	YES: For a remote Configuration Software session to take place, the Grand Master must first enter specific keypad commands in the User Functions mode. **NO**: Configuration Software operations are possible without requiring the user's participation.		

Communication → Configuration SW → Gateway

Quick Keys	Parameter	Default	Range
⑤③④	**IP Gateway**		
	The IP and port address of the configuration's software PC. If you have a router connected to the PC of the Configuration Software, then you should enter the IP of the router. This definition will be used when there is a request to create a remote connection from the panel to the Configuration Software. The connection can be done over IP or GPRS/3G/4G. **Note** In the configuration software, under **Communication → Configuration → GPRS**, enter the IP address of the PC that the software is installed in.		
⑤③④❶	**IP Address**		
⑤③④❷	**IP Port**		

⑤④ Follow Me

In addition to reporting to the monitoring station, the Follow-Me feature enables reporting system events to pre-defined follow me user destinations using SMS message or E-mail. Up to 64 Follow Me destinations can be defined in the system. The following FM parameters can be defined:

- **Define FM**
- **Controls**
- **Parameters**

Communication → Follow Me → Define FM

Quick Keys	Parameter	Default	Range
⑤④①	**Define FM**		
	Up to 64 Follow Me destinations can be defined in the system. Select a follow destination from the list		
⑤④①✪①	**Report Type**		
	Defines the type of reporting events to a Follow Me destination. **NOTE:** ✪ = FM number		

Quick Keys	Parameter	Default	Range
⑤④①✪①②	**EMAIL**		
	Report to Follow Me will be done by e-mail thorough IP or GPRS/3G/4G (or GSM – depending which modules are installed). Each e-mail contains information including the system label. Event type and time. Enter the e-mail address for Follow Me destination defined as IP type. ❶ **IP/GPRS (or IP/GSM)**: The system checks for the availability of the IP network. During regular operation, emails will be sent using the IP network line. In case of trouble in the IP network, the email is routed to the GPRS/3G/4G network. ❷ **GPRS/IP (or GSM/IP)**: The system checks for the availability of the GPRS/GSM network. During regular operation mode emails will be sent using the GPRS/3G/4G/GSM. In case of trouble, the email is routed to the IP network. ❸ **IP Only**: The report is executed through the IP network only ❹ **GPRS Only (or GSM Only)**: The report is executed through the GPRS/3G/4G/GSM network only		
⑤④①✪①③	**SMS**		
	Report to Follow Me will be done by SMS. Each event message contains information including the system label, event type and time. Enter the telephone number including area code or special letters.		
⑤④①✪❷	**Partition**		
	Assign the partitions from which events will be reported to the Follow Me number.		
⑤④①✪③	**Events**		
	Each Follow Me destination can be assigned with its own set of events. Choose the events that will be reported to each Follow Me		

Event	Description	Default
①**Alarms**		
❶ Intruder	Intruder alarm in the system	Yes
❷ Fire	Fire alarm in the system	Yes
❸ Emergency	Emergency alarm in the system	Yes
❹ Panic (S.O.S)	A panic alarm in the system	Yes
❺ Tamper	Any tamper alarm in the system	No
❻ Duress Alarm	Duress alarm in the system from user xx	Yes
❼ Confirmed alarm	Confirmed alarm indication	No

Quick Keys	Parameter	Default	Range
	②**Arm/Disarm**		
	❶ Arm	Arming operation has been performed in the system	No
	❷ Disarm	Disarming operation has been performed in the system	No
	③**Troubles**		
	❶❶ False Code	After three unsuccessful attempts of entering an incorrect code.	No
	❶❷ Main Low Battery	Low battery indication from the LightSYS Air main panel (below 11V)	No
	❶❸ Wireless Low Battery	Low battery indication from any wireless device in the system	No
	❶❹ Jamming	Jamming indication in the system	No
	❶❺ WL Lost	Wireless device lost. When no supervision signal is received from a wireless device	No
	❶❻ AC Off	Interruption in the source of the main AC power. This activation will follow the delay time predefined in the AC Loss Delay timer	No
	❶❼ Siren low Battery	Low battery indication from any sounder in the system	
	❶❾ IP Network	Communication trouble with the IP network.	No
	❶❶ Charge Trouble	Trouble while charging battery	No
	④ **GSM**		
	❶ GSM Trouble	General GSM trouble (Network availability, Network Quality, PIN code error, Module communication, GPRS/3G/4G password, GPRS/3G/4G IP fault, GPRS/3G/4G Connection, PUK code fault	No
	❷ SIM Trouble	Any trouble with the SIM card	No
	❸ SIM Expire	Report to Follow Me will be established 30 days before the SIM Expiration Time defined for a prepaid SIM card.	No

Quick Keys	Parameter	Default	Range
	❹ SIM Credit	An automatic SMS credit message (or any other message) received from the provider's number predefined in SMS Receive Phone will be transferred to the Follow Me number	No
	⑤ **Environmental**		
	❶ Gas Alert	Gas (natural gas) alert from a zone defined a Gas detector	No
	❷ Flood Alert	Flood alert from a zone defined as flood type	No
	❸ CO Alert	CO (Carbon Monoxide) alert from a zone defined a CO detector	No
	❹ High Temperature	High Temperature alert from a zone defined a Temperature detector	No
	❺ Low Temperature	Low Temperature alert from a zone defined a Temperature detector	No
	❻ Technical	Alert from the zone defined as Technical	No
	⑥ **Miscellaneous**		
	❶ Zone Bypass	Zone has been bypassed	No
	❷ Periodic test	Follow Me test message will be established following the time defined in the Periodic Test parameter under the MS parameters	No
	❸ Remote programming	System is in remote installation mode	No

Quick Keys	Parameter	Default	Range
⑤④①✪④	**Restore Events**		

Choose the restore events that will be reported to each Follow Me destination.

Event	Description	Default
① **Alarms**		
❶❶ Intruder Alarm	Intruder alarm in the system restored	Yes
❶❷ Tamper	Tamper alarm in the system restored	No
② **Troubles**		
❶❶ Main Low Battery	Low battery indication from the LightSYS Air main panel restored	No
❶❷ WL Low Battery	Low battery indication from any wireless device in the system restored	No

Quick Keys	Parameter	Default	Range
	⓪❸ Jamming	Jamming indication in the system restored	No
	⓪❹ WL Lost	Wireless device lost restored	No
	⓪❺ AC Off	Interruption in the source of the main AC power restored	No
	⓪❼ Siren low Battery trouble	Siren low Battery trouble restored	
	⓪❾ IP Network	Communication trouble in the IP restored	No
	❶⓪ Charge Trouble	Trouble while charging battery restored	No
	③ **GSM**		
	❶ GSM Trouble	General GSM trouble restored	No
	④ **Environmental**		
	❶ Gas Alert	Gas Alert restored	No
	❷ Flood Alert	Flood Alert restored	No
	❸ CO Alert	CO Alert restored	No
	❹ High Temperature	High Temperature Alert restored	No
	❺ Low Temperature	Low Temperature Alert restored	No
	❻ Technical	Technical Alert restored	No

Quick Keys	Parameter	Default	Range
⑤④①✪❺	**Remote Control**		Yes/No
⑤④①✪❺①	**Remote Listen**	No	Yes/No
	Enables the user of the Follow Me phone to perform remote listen and talk operation with the premises.		
⑤④①✪❺②	**Remote program**	No	Yes/No
	Enables the user of the Follow Me phone to enter the remote operation menu and perform all available programming options. For more details see the LightSYS Air User Manual.		

Communication → Follow Me → Controls

Quick Keys	Parameter	Default	Range
⑤④②	**Controls**		
	Programmable controls related to Follow Me operation		
⑤④②❶	**Disarm Stop Follow Me**	Yes	Yes/No
	YES: The Follow-Me reports will stop when the partitions are disarmed by a user code **NO**: The Follow-Me reports will continue to be made when the partitions are disarmed by a user code		
⑤④②❷	**Disable Report at Stay**	No	Yes/No
	YES: No follow me report during partial (Stay) or Group arming for alarm or tamper **NO**: Follow Me report for alarm or tamper will be established during partial (Stay) arming.		

Communication → Follow Me → Parameters

Quick Keys	Parameter	Default	Range
⑤④③	**Parameters**		
	Allows to program parameters related to operation with the Follow Me		
⑤④③❶	**Follow Me Retries**	03	01—15
	Edit the number of times the Follow Me phone number is redialed		
⑤④③❸	**Follow Me Periodic Test**		(see *Periodic Test, page 133*).
	Set the time period that the system will automatically establish communication to a Follow Me destination defined with the Periodic Test event (see *Periodic Test, page 133*).		

⑤⑤ Cloud

Define the following parameters for Cloud communication:

Communication → Cloud

Quick Keys	Parameter	Default	Range
⑤⑤	**Cloud**		
	Define here the server settings for communication with the LightSYS Air system. **NOTE:** For Cloud connectivity, Cloud must be enabled (default). To enable/disable Cloud connectivity go to: **1)System → 2)Controls → 3)Communication → 4)Cloud Enable** and then select **Y** (yes) to enable or **N** (no) to disable.		
⑤⑤❶	**IP Address**	www.riscocloud.com	
	The IP address or server name. If the LightSYS Air system is connected to the RISCO Cloud for self-monitoring, then use: riscocloud.com. Otherwise enter the IP address or name where the private Cloud server is located.		
⑤⑤❷	**IP Port**	33000	
	The server port address		
⑤⑤❸	**Password**	AAAAAA	Up to 6 characters (case sensitive)
	Specify the password for server access. This password should be identical to the **CP Password** defined in the server under the Control Panel Page definition.		
⑤⑤❹	**Channel**		
	Communication with the Cloud can be established through an IP or GSM channel, depending on your system installed hardware. Utilizing the standard single-channel communication modules, communication with the Cloud can be established through an IP or GSM channel, depending on the installed system hardware. Utilizing the generation multi-socket communication modules, communication with the Cloud can be established with either the IP or 3G modules. **Available Communication Options:**		

Quick Keys	Parameter	Default	Range
	• **IP Only**: Communication is executed through the IP network only. • **GSM (or GPRS) Only**: Communication is executed through the GSM or GPRS/3G/4G network only • **IP/GSM:** Communication is executed through the IP network (primary channel) or through the GSM network (backup channel) • **GSM/IP:** Communication is executed through the GSM network (primary channel) or through the IP network (backup channel)		
⑤⑤❺	**Controls**		01–05
	The LightSYS Air supports parallel channel reporting (via IP, GPRS, GSM, SMS) to both the monitoring station and FM when connected in Cloud mode. Use this setting to decide if the panel reports events to the monitoring station or Follow-Me in parallel to the report to the Cloud or only as a backup when the communication between the LightSYS Air and the Cloud is not functioning. **NOTE:** When the backup mode is functioning, the monitoring station specifications are as defined under MS menu (see *Monitoring Station, page 126 and Follow Me, page 141*).		
	❶ MS Call All		
	YES: Parallel reporting to the MS can be established via both the Cloud and non-Cloud channels. **NO:** Communication to the Monitoring station via the non-Cloud channels can be established only in backup mode (when LightSYS Air – Cloud connection is down)		
	❷ FM Call All		
	YES: Parallel reporting to the Follow Me destination can be established via both the Cloud and non-Cloud channels. **NO:** Communication to the Follow Me destination via the non-Cloud channels can be established only in backup mode (when LightSYS Air – Cloud connection is down)		
	❸ App Arm		
	Yes: Enables remote system arming from user app and Web user interface **No:** Disables remote system arming from user app and Web user interface		
	❹ App Disarm		
	YES: Enables remote system disarming from user app, Web user interface **NO:** Disables remote system disarming from user app, Web user interface		
	❺ App Exit Delay		

Quick Keys	Parameter	Default	Range
	YES: Enables remote Exit Delay from user app, Web user interface **NO:** Disables remote Exit Delay from user app, Web user interface		
	❻ Encryption		
	YES: Enables encrypted communication with the cloud **NO:** Disables encrypted communication with the cloud		

⑦ Install

The following enable adding, removing or testing accessories in the system:

- **Wireless Device**

⑦② Wireless Devices

The following parameters can be defined for wireless devices:

- **RX Calibration**
- **Allocation**
- **Delete**

Note

Allocation of wireless devices can be performed only if a wireless expander module has been defined in the system.

Install → Wireless Devices → RX Calibration

Quick Keys	Parameter	Default	Range
⑦②❶	RX Calibration		
	See *Measuring Background Noise Level and Defining the Threshold Limit, page 47*.		

Install → Wireless Devices → Allocation

Quick keys	Parameter	Default	Range
⑦②②	**Allocation**		
	See *Step 3: Allocating Wireless , page 30*.		
⑦②② ❶	**By RF**		
	See *Allocating Wireless Devices via RF Transmission, page 43*.		
⑦②②❷	**By Code**		
	See *Allocating Wireless Devices via Code, page 44*.		

Install → Wireless Devices → Delete

Quick keys	Parameter	Default	Range
⑦②❸	**Delete**		
	Use this sub-menu to delete the allocation of a wireless device.		

Note

When deleting a wireless Panda keypad after entering the Installer Programming Menu

from the same keypad, the panel will save the data and will automatically exit the installer Programing mode.

⑧ Devices

Manually configure and modify installed system devices:

- **Keypad**
- **Keyfob**
- **Sounder**

⑧① Keypad

Devices → Keypad

Quick keys	Parameter	Default	Range
⑧①	**Keypad**		
	NOTE: ✪ = keypad number Select a keypad, press **OK.** The following can be defined for each keypad:		
⑧①✪❶	**Label**		
	Enter a label identifying the keypad in the system.		
⑧①✪❷	**Partition**		
	Enter a partition (01--32) for the keypad		
⑧①✪❸	**Masking**		
	Specifies the partitions that are controlled by the specified keypad. Enter a number to clear it. Enter the number again to display it.		
⑧①✪❹	**Controls**		
	Define these parameters: ❶ Emergency (**Y/N**) – to enable (Y) or disable (N) the keypad's emergency keys per keypad. ❷ Multi view **YES:** The keypad will display the status of all masked partitions and will activate its buzzer in case of alarm from any of the masked partitions. **NO:** The keypad will display the status and activate its buzzer only of its partition. ❸ Exit beeps (for a 2-Way Slim keypad with bypass) **YES:** Exit / Entry beeps will sound. **NO:** Exit / Entry beeps will not sound. ❹ Supervision **(Y/N)** – to enable (Y) or disable (N) supervision for a		

Quick keys	Parameter	Default	Range
	wireless keypad		
⑧①✪❺	**Serial Number**		
	Displays the identifying 11-digit number of the allocated keypad		

⑧② Keyfob

Devices → Keyfob

Quick keys	Parameter	Default	Range
	Options for Keyfob The available programmable functions for the buttons: ❺ **Serial No** ❻ **Masking:** Specifies the partitions that are controlled by the device. ❼ **Controls** ❶❷**Button ARM: Used to arm away** ❶❸**Button DISARM: Used to disarm** ❶❹**Button *: Used** ❶❺**Button STAY: Used to arm home** ❶❻**Select ASSIGN: Select the assigned device (repeater or control panel)**		

⑧③ Sounder

Define the following for an external siren that is connected to the LightSYS Air:

- **Parameter**

Note

Access to this sub-menu requires that a sounder device is installed on your site.

Device → Sounder → Parameter

Quick Keys	Parameter	Default	Range
⑧③①	**Parameters**		
	Use this menu to define all parameters of the siren. Note that some parameters are only relevant for specific siren models. Select a sounder and press **OK.**		

Device → Sounder → Parameter

Quick Keys	Parameter	Default	Range
⑧③①✪①	**Label**		
	As assign the sounder a label (description)		
⑧③①✪②	**Masking**		
	Use this menu to define parameters relating to masking		
⑧③①✪③	**Strobe**		
	Use this menu to define parameters relating to the sounder strobe		
⑧③①✪③❶	**Strobe Control**	Follow Bell	
	Defines the strobe operation mode. ❶ ALWAYS OFF - The strobe is deactivated. ❷ FOLLOW BELL — The strobe is activated when the siren bell is triggered. ❸ FOLLOW ALARM — The strobe is activated when an alarm occurs in the selected siren's partitions.		
⑧③①✪③❷	**Strobe Blink**	40	
	Defines the number of times that the strobe will blink in a minute. ❶ 20 [Times/Min] ❷ 30 [Times/Min] ❸ 40 [Times/Min] ❹ 50 [Times/Min] ❺ 60 [Times/Min]		
⑧③①✪③❸	**Arm Squawk**	01	01-20 (seconds)
	The time that the strobe will blink when the system is armed. **Note** If the siren's squawk strobe is defined as **NO** (see the add/delete module, ⑦①②❶❽) this parameter will be ignored.		
⑧③①✪⑦	**Volume**	9	0—9 (seconds)
	Sets the Alarm volume. The volume ranges between 0 (silent) to 9 (max volume). After setting/changing the volume, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.		
⑧③① ✪①②	**Serial Number**		
	(Only for Lumin8)		

Quick Keys	Parameter	Default	Range
	The identifying 11-digit number of the sounder (display only)		
⑧③① ✪①③	**Supervision**		
	(Only for Lumin8) Determines if this zone will be supervised by the system expander according to the time defined under the timer RX Supervision (see *RX Supervise, page 58*).		
⑧③① ✪①④	**Select Assign**		
	Select the assigned device (repeater or control panel)		

Device → Sounder → Parameter → 2-Way WL Sounders

Quick Keys	Parameter	Default	Range
⑧③① ✪❶❶	**Label**		
	You can define a label(name/description) for a sounder		
⑧③① ✪⓪②	**Strobe**		
	Use this menu to define parameters relating to the sounder strobe		
⑧③①✪⓪②①	**Control**	Follow Bell	
	Defines the strobe operation mode: ❶ ALWAYS OFF - The strobe is deactivated. ❷ FOLLOW BELL — The strobe is activated when the siren bell is triggered. ❸ FOLLOW ALARM — The strobe is activated when an alarm occurs in the selected siren's partitions.		
⑧③①✪⓪②②	**Blink**	40	
	Defines the number of times that the strobe will blink in a minute. ❶ 20 [Times/Min] ❷ 30 [Times/Min] ❸ 40 [Times/Min] ❹ 50 [Times/Min] ❺ 60 [Times/Min]		
⑧③① ✪⓪②❸	**Arm Squawk**	01	01—20 (seconds)
	The time that the strobe will blink when the system is armed.		

Quick Keys	Parameter	Default	Range
	Note If the siren's squawk strobe is defined as **NO**, then this parameter will be ignored.		
⑧③① ✪⓪③	**Volume**		
	Sets the WL siren's internal speaker Alarm volume - range is between 0 (silent) to 9 (maximum). After setting, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.		
⑧③① ✪⓪③❶	**Alarm**	9	(1—9)
	General alarm volume		
⑧③① ✪⓪③❷	**Squawk**	9	(1—9)
	Squawk sound alarm		
⑧③① ✪⓪③❸	**Exit Entry**	9	(1—9)
	Notification of system status in exit or entry delay.		
⑧③① ✪❶❹	**Serial No.**		
	The identifying 11-digit number of the sounder (display only)		
⑧③① ✪❶❺	**Supervision**		
	Determines if this zone will be supervised by the system expander according to the time defined under the timer RX Supervise, page 58).		

Device → Repeater

⑧ Repeater

Devices → Repeater

Quick Keys	Parameter	Default	Range
⑧⑤✪①	**Serial Number**		
	Scroll to Serial Number and then press OK, the Repeater 11-digit serial number displays.		
⑧⑤✪①	**Label**		
	A label identifying the Repeater		
Quick Keys	**Parameter**	**Default**	**Range**
⑧⑤✪①	**Supervision**	Yes	Yes/No
	Choose if the Repeater will be supervised or not		

⓪ Exit

When exiting installer Programming menu, go to **0) Exit** and then press **OK** (✓). Note that if exiting after programming in the installer Programming menu the very first time (at initial system configuration), perform the following procedure:

Exiting Installer Programming Menu

Exiting Installer Programming Menu after Initial System Programming

IMPORTANT: After you have finished programming all relevant parameters in the installer Programming menu **the first time – at the time of initial system setup,** you must then perform the following procedure to exit the installer Programming mode. Afterwards you can then program additional parameters as needed from the same menu, or from other installer menus.

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

1. Close the main panel box/enclosure in order to prevent a front tamper alarm.
2. At the keypad, press **Exit** () repeatedly to return to the start of the current menu.
3. Press **0** to exit, toggle 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 **Exit,** then toggle to **Y** (yes), and then press **OK**.

   NOTE: If you select **N** (no), you will not be able to exit installer Programming mode until the tamper trouble condition has been restored to normal.

Restoring Manufacturer's Programming Defaults

You can revert to manufacture defaults for all system parameters.

- **To restore the main panel to the manufacturer's defaults:**

1. From the installer Programming menu, select **1→ 5→ 2 (System→Setting→ Default Panel).**
1. To restore the system labels to the manufacturer defaults (delete all labels), toggle to **Y** (yes) and then press **OK** (✓) to confirm**.**
2. To revert to the default panel and keep existing labels, toggle to **N,** and then press **OK**.
   NOTE: It may take a minute or two to process, but wait until SETTINGS: 2) DEFAULT PANEL displays.
3. To save your settings exit the Programming mode.

Defining Parameters – Additional Installer Menus

You can program additional system parameters in installer menus (other than the Programming menu):

Activities Menu

Activities parameters
Keypad Sound
Chime **Keypad Chime**—Use the scroll buttons to turn the keypad's internal sounder ON or OFF for any function utilizing the chime. **Partition Chime**—Use the scroll buttons to turn internal sounders ON or OFF for all keypads in the partition (for all functions utilizing the chime). **Buzzer ON/OFF**—Use the scroll buttons to turn the keypad's internal buzzer ON or OFF during both Entry and Exit Delay time periods, and during all fire and intrusion alarms.
Advanced **Service Mode**—Press **OK** to activate / deactivate the service mode, which silences alarms in order to enable battery replacement for detectors and accessories. For setting Service Mode parameters, see *Service Mode on page 134*. **MS Test** — Press **OK** to initiate a test message to the monitoring station according to EN50131 requirements. **Wi-Fi Scan-**The Control panel scans for Wi-Fi networks and shortly after available networks appear in a list (the connected network is marked and appears first in the list). The rest of the list is sorted from high RSSI to low, with a max. 20 networks. Scroll to your Router's Wi-Fi network, select the desired network and then press [enter]. Enter the Password, if required, and press [enter]. If connection is successful, a successful message is displayed. If there is a connection failure, an error message is displayed. **Note:** Your Router's Wi-Fi must be activated for the Control Panel to recognize and communicate with the Router. **Wi-Fi WPS Button**-Press the WPS button on the router to establish a connection. A "Successfully Connected" to network message will appear within 2 min.

Follow Me Menu

Follow Me parameters
Define – Press **OK,** and then scroll to a FM destination number (up to 64) to define
For the selected FM destination number, enter the Follow Me destination information, according to its type (SMS or E-mail), and then press **OK.** For more information, see *Follow Me, page 141.*
Label – For the selected FM destination number, scroll to enter (over the existing or default label) an identifying description, and then press **OK.**
Terminate Follow Me – A Follow Me destination can be terminated (deleted).
Test FM – For testing Follow Me reporting

View Menu

View parameters
Trouble (⚠) – Scroll to view system troubles.
Alarm Memory – Displays the 5 most recent alarm conditions stored in the system
Partition Status – Scroll to view partition status and NR (not ready) zones in the system.
Note • Pressing on the scroll keys from the normal operation mode displays the status of the partition to which the keypad is assigned • For each user code, displays the status of all respective partitions assigned to that user
Zone Status – Scroll to view all system zones and their current status.
Service Information – Scroll to the following options: **Installer** – View any previously entered service / installer information **System Version** – View the version number and date of the installed system software **Serial Number –** View the 11-digit serial number of the main panel **Panel ID –** View the 15-digit panel ID number **Cloud Status- Scroll to view the Cloud Status** **Wi-Fi Status- Scroll to view the Wi-Fi Status**

Clock Menu

Clock parameters
Time & Date – To set the system time and date, scroll to each space and enter/re-enter the time and date definitions (required for all Scheduler programming – see below).
Scheduler **NOTE:** For complete Scheduler and Vacation procedures, see the *LightSYS Air User Manual*. You can configure the following automated system operations according to schedules (and other criteria) that you define: • Arming/disarming the system **one-time** only within the next 24 hours • Up to 64 **re-occurring weekly schedules** for arming/disarming the system, activating/deactivating up to 4 UOs (utility outputs). • Up to 99 **vacation schedules** for UO activation and system arming **One-Time**: Define a one-time automatic arm/disarm of the system at a specific time within the next 24 hours. **Weekly Schedules:** Define up to 64 weekly schedules for automatic arming/disarming and automatic activation/deactivation of utility outputs. Each schedule can be defined with up to 2 time intervals (2 separate start & stop times) per day. For automatic arming/disarming, you have the option to set a "user limitation" safeguard that prevents users that you define from disarming the system during time intervals that you specify.
Vacation – To set up to 99 vacation schedules for automatic arming & UO activation (with respective dates/ times as well as partitions for arming)

Event Log Menu

Event Log parameters
View of up to 2000 system events. Each event displays with the date and time. Scroll to an event number, and then press **OK** to view its details.
Notes • The events memory cannot be erased • To skip to blocks of 100 events backward or forward, use [🏠] [🔒] respectively

Maintenance Menu

Maintenance parameters
Walk Test – Test and evaluate the operation of selected zones in the system. A walk test is set for up to 60 minutes. During the last 5 minutes, the keypad used to activate the test will indicate that the test is about to end. • **Full Walk Test** (areas activated) – Displays the activated zones and type of detector • **Quick Walk Test** (areas not activated – Displays the non-activated zones.
Keypad Test – Activates the keypads and momentarily tests the keypad indicators.
Siren Test –Activates utility outputs defined as Bell Trigger (③② ❷❷).
Strobe Test –activates utility output defined as Follow Strobe (③② ❷❸).
Wireless Test – For all allocated keyfobs, wireless zones, and wireless keypads: **Comm.Test** – Displays the last measurement taken at the last transmission (last detection or last supervision signal) of the selected device. To receive the updated signal strength, activate the detector prior to performing the communication test. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the panel (see *Performing a Wireless Comm. Test for Measuring Signal Strength, page 49*). **Battery Test** – Displays the last battery test results of the selected device taken at the last transmission. A confirmation message displays if the test was successful. In addition, you can activate the device.
Diagnostics
You can activate the following tests for system diagnosis: • **Main Battery Test** – Tests the level of the main panel's backup battery. Press **OK** to start the test; the result displays. • **Siren** – Tests installed sirens and displays information regarding each siren (depending on siren type). Press **OK,** scroll to the siren to test, and then press **OK** again. Now scroll to either view the results for DIAGNOSTICS or VERSION, and press **OK;** the corresponding information displays. • **GSM module** – Tests the following for the installed GSM module: ❖ **Signal (RSSI)** – Displays the signal level measured by the GSM module (0 = no

signal, 5 = very high signal)

- ❖ **Version** – Displays information regarding the GSM module version
- ❖ **IMEI** – Displays the IMEI number of the GSM module. This number is used for identification of the LightSYS Air at the RISCO IP Receiver when using GSM or GPRS/3G/4G communication

- **IP–** Performs a diagnostic test for the following parameters of the plug in IP:
  - ❖ **IP Address** – View the system's IP address
  - ❖ **MAC Address** – View the MAC address of the IP. This number is used for identification of the system at the RISCO IP Receiver when using the IP communication module.
  - ❖ **WIFI MAC Address** – View the MAC address of the IP. This number is used for identification of the LightSYS Air at the RISCO IP Receiver when using Wi-Fi Communication.
- **WME Version** – Displays the selected wireless expansion module's software version/date
- **Panel Version** – Displays the main panel (system) software version/date
- **Keypad Version** – Displays the selected keypad's software version/date
- **W2W Zone Version** – Displays the wireless 2-Way zone version
- **W2W KF Version** – Displays the wireless 2-Way Keyfob version
- **Repeater** - Displays the wireless 2-Way Repeater version

Macro Menu

Macro parameters
Test a selected macro, if it has been pre-programmed. Scroll to select the respective macro **(A—D),** and then press **OK.** For more information on programming macros, see the *LightSYS Air User Manual*.

Stand Alone Keyfob Menu

Stand Alone Keyfob parameters
Standalone keyfobs are used for gate control (with a dedicated wireless expander module). Scroll to select the wireless expander module used for the standalone keyfobs/gate control, and then press **OK.** For the respective keyfobs supported, select from the following parameters to configure. For more information on standalone keyfobs, see the LightSYS Air User Manual. • **New Keyfob** – To allocate a new keyfob • **Delete Keyfob** – To delete the allocation of a keyfob • **Delete All** – To delete all keyfob allocations • **UO Buttons** – To change the keyfob buttons that control utility outputs

Testing the System

It is important to fully test the system. Here are typical, recommended system tests that should be performed at system installation, and subsequently as needed:

- ✓ **Background noise-level threshold & calibration for wireless devices:** See *Measuring Background Noise Level and Defining the Threshold Limit, page 47.*
- ✓ **Wireless Communication Test:** For testing the signal strength of wireless devices. See *Performing a Wireless Comm. Test for Measuring Signal Strength, page 49.*
- ✓ **Walk Test (for zones):** Arm the system, and then enter the protected area in order to trigger alarm events at each detector to ensure operability. See the installer **Maintenance menu → Walk test,** *page 161.*
- ✓ **Monitoring Station Test:** See **View Menu → Advanced → MS Test,** *page 159.*
- ✓ **GSM signal strength (RSSI)**: View the signal strength result measured by the GSM module (from 0—5). Go to: **installer Maintenance menu → Diagnostics → GSM → Module,** *page 161.*
- ✓ **Additional tests at the** installer **Maintenance menu**: For keypads, sirens, strobes, wireless, and diagnostics. See from *page 161.*
- ✓ **Follow-Me Test:** After programming FM destination(s), go to: installer **Follow Me Menu → Test.** Trigger an alarm activation (for example, as done during a Walk Test), and see if the FM notification is received at the FM destination(s). See *Follow Me Menu, page 159.*

Installer Responsibilities for Assisting the Client

Here are some typical, recommended areas for you to assist the client, upon handing over system after installation:

- ✓ Advise client to change the default 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 destinations.
- ✓ Instruct how to do the following from keypads and keyfobs:
  - Full arm, partial arm, disarm
  - Send a duress disarm (silent alarm) to the monitoring station
  - Activate a panic alarm
  - Check system status
  - Use SMS for remote operation

Appendix A: Technical Specification

Configuration	
Communication modes	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	100-240 VAC, 50/60Hz,0.1A Max.
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 Module (RP512G4, RP512G4T, RP512G4L)	
Current consumption	30 mA standby, 300 mA communicating
WL Panda Keypad for LightSYS Air/LightSYS Plus:(RW432KPP2/ RW432KPP2BL)	
Current consumption	30μA standby current, 150 mA maximum

Appendix B: Installer Event Log Messages

Event Message	Description
AC Low PS=y	Loss of AC power from power supply ID=y
AC RST PS=y	AC power restore on power supply ID=y
Activate UO=xx	UO XX activation
Actv UO=xx KF=zz	UO XX is activated from remote control ZZ
AL.ReinstateP=Y	Alarm reinstatement on partition Y
Alarm Z=xx	Alarm in zone no. XX
Alrm Cancel P=y	Alarm is cancelled in partition ID=Y
ARM A:P=y C=zz	Group A on partition Y is armed by user ZZ
ARM A:P=y KF=zz	Group A on partition Y is set by wireless keyfob ZZ
ARM B:P=y C=zz	Group B on partition Y is armed by user ZZ
ARM B:P=y KF=zz	Group B on partition Y is set by wireless keyfob ZZ
ARM C:P=y C=zz	Group C on partition Y is armed by user ZZ
ARM C:P=y KF=zz	Group C on partition Y is set by wireless keyfob ZZ
ARM D:P=y C=zz	Group D on partition Y is armed by user ZZ
ARM D:P=y KF=zz	Group D on partition Y is set by wireless keyfob ZZ
ARM FAIL P=y	Fail to Arm Partition X by Guard due to not ready zones
ARM:P=y C=zz	Partition Y armed by user ZZ
ARM:P=y KF=zz	Partition Y armed by wireless keyfob ZZ
Aut tst fail	Failure of zone self-test
Auto test OK	Automatic zone self-test OK
Aux RS PS=y	Restore of Aux power on power supply ID=Y
Aux RS ZE=y	Restore of S. Aux power on zone expander Y
Aux TRBL RS S=y	Auxiliary trouble restore on the siren ID=Y
Aux TRBL SIR.=y	Auxiliary trouble on the siren ID=Y
Bat Load RS S=y	Battery load trouble restore from siren ID=Y
Bat Load SIR.=y	Battery load trouble from siren ID=Y
Bat Rst PS=y	Low battery trouble restore from power supply ID=Y
BELL RS PS=y	Bell trouble restore in power supply ID=Y
Bell tamper	Bell tamper alarm
Bell tmp rs	Bell tamper alarm restore
Box tamper	Box tamper alarm from main unit
Box tmp rs	Box tamper alarm restore
Bypass Box+Bell	Box tamper is bypassed
Byp Trbl C=xx	System troubles were bypassed by user XX
Bypass Zn=xx	Zone no. XX is bypassed

Event Message	Description
Charge Curr S=y	Battery charging trouble in siren ID=Y
Chng code=xx	Changing user code XX
Change FM=yy	Changing Follow-Me number YY
Charge Current RS S=y	Battery charging trouble restore in siren ID=Y
Clk not set	Time is not set
Clk set C=xx	Time defined by user no. XX
Cloud Comm.Trbl	Communication problems with the Cloud channel
Cloud Connected	Cloud communication channel is functioning
Cloud Disconnect	Cloud communication channel is not functioning
Cloud Login Err	Login problems with the Cloud channel
CO Alarm Z=xx	CO alert from zone XX defined as a CO detector
CO Rst. Z=xx	CO alert restored from zone XX defined as a CO detector
Comm OK IP	Communication OK between the LightSYS Air and IP
Comm OK Siren=y	Communication OK between the LightSYS PlusLightSYS Air and Siren Y
Comm. OK GSM	Communication OK between the LightSYS Air and GSM
Comm.OK LRT	Communication OK between the LightSYS Air and the long range transmitter
Conf. Z=xx	Confirmed alarm occurred from zone XX
Conf. alarm P=y	Confirmed alarm occurred in partition Y
Conf.holdup P=y	Confirmed holdup occurred in partition Y
Confirm rs Z=xx	Restore zone confirmed alarm
CP reset	The control panel has reset
Dat set C=xx	Date defined by user no. XX
Day A:P=y	Daily arm on partition Y
Day Arm:p=y	Daily Arm on Partition Y
Day b:p=y	Arm by scheduler of group B on partition Y
Day c:p=y	Arm by scheduler of group C on partition Y
Day d:p=y	Arm by scheduler of group D on partition Y
Day dis:P=y	Daily disarm on partition Y
Day hom:P=y	Daily Stay or Group arming in partition Y
Dis:P=y C=zz	Partition Y disarmed by user ZZ
Dis: P=y KF=zz	Partition Y disarmed by remote control ZZ
Duress P=y C=xx	Partition Y duress alarm from user no. XX
EE AC.UPLOAD	Load new parameters from PTM accessory
Enter progrm	Entering installer programming from keypad or configuration software

Event Message	Description
Exit program	Exiting installer programming from keypad or configuration software
F.Tr OK Z=xx	Trouble restore in fire zone no. XX
F.Trbl Z=xx	Trouble in fire zone no. XX
Fire Zone=xx	Fire alarm in zone no. XX
False code kp=y	False code due to 3 incorrect keypad attempts
False code kr=y	False code due to 3 incorrect Access Control attempts
False rest.kp=y	False code is restored for keypad
False rest.kr=y	False code is restored for key reader
Fault z=xx	Trouble in zone XX
Fire z=xx	Fire alarm in zone XX
Fire kp=y	Fire alarm from keypad (ID=XX) (keys 3 & 4)
Foil ok Z=xx	Restore in foil (Day) zone no. XX
Foil Z=xx	Trouble in foil (Day) zone no. XX
Forced P=y	Partition Y is force armed
Found Z=xx	Wireless zone found, zone no. XX
Func=xx C=yy	Quick key function XX by user YY
Gas Alarm Zn=xx	Gas (natural gas) alert from zone XX defined as a gas detector
Gas Rst. Z=xx	Gas (natural gas) alert restored from zone XX defined as a gas detector
GSM:GPRS PW ERR	Authentication password is incorrect
GSM:GPRS PW OK	Authentication password is correct
GSM:IP OK	IP connection OK
GSM:IP Trouble	IP address is incorrect
GSM:Mdl comm.OK	Communication between the GSM/GPRS/3G/4G Module and the LightSYS Air is OK
GSM:MS OK	GPRS/3G/4G communication to the MS is OK
GSM:MS trouble	GPRS/3G/4G communication failure to the MS
GSM:NET avail.	GSM network is not available
GSM:NET avai.OK	GSM Network is available
GSM:NET qual.OK	GSM Network quality is acceptable
GSM:NET quality	The GSM RSSI level is low
GSM:PIN cod.err	PIN code entered is incorrect
GSM:PIN code OK	PIN code is correct
GSM:PUK Cod err	PUK code required
GSM:PUK Code OK	PUK Code entered is correct
GSM:SIM OK	SIM Card in place
GSM:SIM trouble	SIM card missing or not properly sited

Event Message	Description
H.Temp rst Z=xx	High temperature alert restored from zone XX defined as a temperature detector
High Temp. Z=xx	High temperature alert from zone XX defined as a temperature detector
HOM:P=y C=zz	Partition Y is armed in Stay mode by user ZZ
HOME:P=y KF=zz	Partition Y is home armed using keyfob ZZ
HU.ReinstateP=y	Hold-Up Reinstatement in partition y
IP:DHCP error	Failed to acquire an IP address from the DHCP server
IP:DHCP OK	Succeeded to acquire an IP address from the DHCP server
IP: downld err	IP generated a download error
IP: download OK	IP download was OK
IP: evnt log ER	IP generated an event log error
IP: evnt log OK	IP event log generated no error
IP: hardware OK	IP hardware is OK
IP: hardware error	IP generated a hardware error
IP: mail error	IP generated a mail error
IP: mail OK	IP mail is OK
IP:MS=y error	IP Monitoring station ID=Y generated an error
IP:MS=y OK	IP Monitoring station ID=Y was OK
IP: Network err	Failed to connect to IP network
IP: Network OK	Successful connection to IP network
IP:NTP error	Failed to acquire time data from the time server
IP:NTP ok	Succeeded to acquire time data from the time server
IP: upgrade err	The IP upgrade generated an error
IP: upgrade OK	The IP upgrade was OK
JAMM. WME=y	Jamming in wireless module expander ID=Y
KeyBox Open Zxx	Zone XX of type key box is open
KeyBox Rst Z=xx	Zone XX of type key box is restored
KP=$ Lost	Keypad is lost
KP=$ Lost Rs	Lost keypad has been restored
KP=$ LOW BAT.	Low Battery trouble for the keypad
KSW A: Z=xx P=Y	Group A in partition Y is armed by keyswitch zone XX
KSW ARM:Z=xxP=Y	Partition Y is armed by keyswitch zone XX
KSW B: Z=xx P=Y	Group B in partition Y is armed by keyswitch zone XX
KSW C: Z=xx P=Y	Group C in partition Y is armed by keyswitch zone XX
KSW D: Z=xx P=Y	Group D in partition Y is armed by keyswitch zone XX
KSW DIS:Z=xxP=Y	Partition Y is disarmed by keyswitch zone XX
LB rstr KF=yy	Low battery trouble restore from wireless remote control YY

Event Message	Description
L.Temp rst Z=xx	Low temperature alert restored from zone XX defined as a temperature detector
LB RSTR Z=xx	Low battery restore from wireless zone XX
Lost Z=xx	Wireless zone lost, zone no. XX
Low Bat KF=xx	Low battery trouble from wireless remote control ID=XX
Low Bat PS=y	Low battery trouble from power supply ID=Y
Low Bat RS Z=xx	Low battery trouble restored from wireless zone no. XX
Low Bat Siren=y	Low battery trouble from siren ID=Y
Low bat Z=xx	Low battery trouble from wireless zone no. XX
Low Temp. Z=xx	Low temperature alert from zone XX defined as a temperature detector
LRT:ACCOUNT ERR	The long range transmitter account generates an error
LRT:ACCOUNT OK	The long range transmitter account is OK
LRT:HARDWARE OK	The long range transmitter hardware is OK
LRT:HARDWRE ERR	The long range transmitter hardware generates an error
LRT:LOW BAT	The long range transmitter is experiencing low battery trouble.
LRT:LOW BAT OK	The long range transmitter low battery in not troubled
LRT:NO BAT	The long range transmitter is experiencing no battery
LRT:NO BAT OK	The long range transmitter no battery is not troubling.
LRT:SYSTEM ERR	The long range transmitter is generating a system error.
LRT:SYSTEM OK	The long range transmitter system status is OK
Main Bell RS	Bell trouble restore in Main Panel
Main:AC Rstr	AC power restore on main panel
Main Aux Rst	Restore of Aux power on Main Panel
Main: Bat Rst	Low battery trouble restore from the main panel
Main: Low AC	Loss of AC power from the main panel
Main: Low Bat	Low battery trouble from the main panel
Main:No aux	Failure in the Aux power on Main Panel
Main:No bell	Bell trouble in Main Panel
Masked Z=XX	Anti mask trouble from zone XX
MS=y call error	Communication fail trouble to MS phone no. Y
MS=y restore	Communication fail trouble restore to MS phone no. Y
MW restore z=xx	Trouble restore in the MW channel of BUZ zone XX
MW trouble z=xx	Trouble in the MW channel of BUZ zone XX
Next arm:p=y	Partition Y armed in Next Arm mode
Next dis:p=y	Partition Y disarmed in Next Disarm mode
No aux ps=y	Failure in the Aux power on power supply ID=X

Event Message	Description
No aux ze=y	Failure in the S. Aux power on zone expander Y
No bell ps=y	Bell trouble in power supply ID=Y
No Com IPC	Communication failure between the LightSYS Air and IP card
No com kp=y	Communication failure between the LightSYS Air and keypad ID=Y
No com kr=y	Communication failure between the LightSYS Air and Key Reader ID=Y
No com WME=y	Communication failure between the LightSYS Air and wireless module expander ID=Y
No comm PS=y	Communication failure between the LightSYS Air and power supply Y
No comm Siren=y	Communication failure between the LightSYS Air and siren Y
No comm. GSM	No communication between the GSM/GPRS/3G/4G Module and the LightSYS Air
No comm. LRT	No communication between long range transmitter and system
No jam wme=y	Jamming restore on wireless module expander ID=Y
No mask z=xx	Anti mask trouble restore from zone XX
Nxt hom:p=y	Partition Y is armed in Next Stay mode
Phone fail	If the phone line is cut or the DC level is under 1V
Phone restore	Phone line trouble restore
Police KF=yy	Police (panic) alarm from remote control YY
Police KP=y	Police (panic) alarm from keypad Y
POT.LD RS PS=y	Potential overload restore of 3A SMPS joined by 3A SMPS Y
POT.OVRLD PS=y	Potential overload of SMPS joined by 3A SMPS Y
PROX FAIL S=y	Fail in the proximity anti approach protection in siren Y
PROX OK SIREN=y	Proximity anti approach protection is restored in siren Y
PROX TMP RS S=y	Proximity tamper restore from siren ID =Y
PRX TMP SIREN=y	Proximity tamper from approaching siren ID=Y
Radio l.bat S=y	Radio low battery trouble from siren Y
Radiol.bat rS=y	Radio low battery restore from siren Y
Remote Prog	The system has been programmed from the configuration software
Reset: P=y C=zz	Reset of partition ID=Y and user ID=ZZ
Restore Z=xx	Alarm restore in zone no. XX
Rmt Arm:P=y	Partition Y armed from the configuration software
Rmt Dis:P=y	Partition Y disarmed from the configuration software
RMT Hom:P=y	Partition Y armed in Stay mode from the CS software

Event Message	Description
Siren=$ Lost	Siren is regarded as lost following supervision test
Siren=$ Lost Rs	The LightSYS Air received a signal from siren after it has been regarded as lost
Soak fail Z=xx	Zone XX has failed in the soak test
Spec. KP=y	Special alarm from the from wireless keypad Y
Spk Trbl RS S=y	Speaker low battery restore from siren Y
Spkr Trbl Sir=y	Speaker low battery trouble from siren Y
Spkr l.bat S=y	Speaker low battery trouble from siren Y
Spkr l.batrsS=y	Speaker low battery restore from siren Y
Start exit P=y	Exit time started in partition Y
STU=Y Line Rstr	STU adapter Y line restoration
STU=Y Line Trbl	STU adapter Y line trouble
STU=Y R.RESET	STU adapter Y line restoration reset
Tamper Kp=y	Tamper alarm from keypad ID=Y
Tamper LRT	Tamper alarm from long range transmitter
Tamper PS=y	Tamper alarm from power supply Y
Tamper Siren=y	Tamper alarm from wireless siren Y
Tamper UO=y	Tamper alarm from utility output expander Y
Tamper WME=y	Tamper alarm from wireless module expander Y
Tamper ZE=y	Tamper alarm in zone expander ID=X
Tamper Zn=xx	Tamper alarm from zone no. XX
Tech alarm Z=xx	Alarm from zone XX defined as Technical
Tech rstr Z=xx	Alarm restored from zone XX defined as Technical
TMP RS KP=y	Keypad tamper restore
TMP RS PS=y	Tamper alarm restore from power supply expander ID=Y
TMP RS UO=y	Tamper alarm restore from UO expander ID=Y
TMP RS WME=y	Tamper alarm restore from wireless module expander ID=Y
TMP RS ZE=y	Tamper alarm restore in zone expander ID=Y
TMP RS ZN=xx	Tamper alarm restore on zone XX
TMP RST LRT	Long Range transmitter tamper alarm reset
Tmp rst Siren=y	Tamper alarm restore from wireless siren Y
Unbyp Box+Bell	Box reinstated from bypass
Unbyps Zn=xx	Zone no. XX is reinstated from bypass
Unknown evnt	Unknown event alert
UO REST ZN=xx	A zone defined as “UO/REX Trigger” has been deactivated
UO TRIG ZN=xx	A zone defined as “UO/REX Trigger” has been activated
Water Alrm Zn=xx	Flood alarm from zone no. XX

Event Message	Description
Water rstr Z=xx	Flood alarm restore on zone no. XX
WEAK BAT PS=y	Weak battery indication joined by 3A SMPS Y
Weak Bat RS PS=y	Weak battery restore indication joined by 3A SMPS Y
Z=xx aut bad	Zone self-test failed, zone no. XX
Z=xx auto ok	Zone self-test OK, zone no. XX

Appendix C: Troubleshooting

Troubleshooting and diagnostics can be done by performing by the various systems tests that are available (see *Testing the System, page 164*) and with the Configuration Software. Additional information is available through RISCO University. For additional assistance, contact RISCO Group Technical Support.

GSM Module LEDs

Note

After 15 minutes all LEDs will turn off.

LED/Function	State	Status	
LD1	(not in use)		
LD2	ON	Module is ON	
	OFF	Module is OFF	
LD3	ON	Communicating with the main panel	
	OFF	No communication with the main panel	
LD4	ON	**Data call:** Connected to remote party or exchange of parameters while setting up or disconnecting a call.	
	OFF	Module is OFF	
	Blink slow	600 ms ON / 600 ms OFF:	1. No SIM 2. No PIN 3. Network search in progress 4. Ongoing user authorization 5. Network login in progress
		500 ms ON / 25 ms OFF:	Packet switch data in progress
	Blink fast	75 ms ON / 3 sec OFF:	Registered to GSM network

Appendix D: Monitoring Station Report Codes

Parameter	Contact ID	SIA	Report Category
Alarms			
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Fire alarm	115	FA	Urgent
Fire alarm restore	115	FH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
Duress alarm	121	HA	Urgent
Duress alarm restore	121	HH	Urgent
Box tamper	137	TA	Urgent
Box tamper restore	137	TR	Urgent
Confirmed alarm	139	BV	Urgent
Confirmed alarm restore	139		Urgent
Confirmed hold up alarm			Urgent
Confirmed hold up alarm restore			Urgent
Recent Close	459		Non-urgent
Main Troubles			
Bell trouble	321	YA	Non-urgent
Bell trouble restore	321	YH	Non-urgent
Auxiliary failure	300	YP	Non-urgent
Auxiliary restore	300	YQ	Non-urgent
Low battery	302	YT	Non-urgent
Low battery restore	302	YR	Non-urgent
AC loss	301	AT	Non-urgent
AC restore	301	AR	Non-urgent
Clock not set	626		Non-urgent
Clock set	625		Non-urgent
False code	421	JA	Non-urgent
False code restore	421		Non-urgent
RF Jamming	344	XQ	Non-urgent
RF Jamming restore	344	XH	Non-urgent

Parameter	Contact ID	SIA	Report Category
GSM trouble	330	IA	Non-urgent
GSM trouble restore	330	IR	Non-urgent
GSM Pre-Alarm			Non- urgent
IP Network trouble			Non-urgent
IP Network trouble restore			Non-urgent
Arm/Disarm			
User Arm	401	CL	Arm/Disarm
User Disarm	401	OP	Arm/Disarm
Stay arm	441	CG	Arm/Disarm
Disarm after alarm	458	OR	Arm/Disarm
Keyswitch Arm	409	CS	Arm/Disarm
Keyswitch Disarm	409	OS	Arm/Disarm
Auto Arm	403	CA	Arm/Disarm
Auto Disarm	403	OA	Arm/Disarm
Remote Arm	407	CL	Arm/Disarm
Remote Disarm	407	OP	Arm/Disarm
Forced Arm	574	CF	Arm/Disarm
Quick Arm	408	CL	Arm/Disarm
Auto Arm fail	455	CI	Arm/Disarm
Detectors (Zones)			
Burglary alarm	130	BA	Urgent
Burglary alarm restore	130	BH	Urgent
Fire alarm	110	FA	Urgent
Fire alarm restore	110	FH	Urgent
Foil alarm	155	BA	Urgent
Foil alarm restore	155	BH	Urgent
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
24 Hour alarm	133	BA	Urgent
24 Hour alarm restore	133	BH	Urgent
Entry/Exit	134	BA	Urgent
Entry/Exit restore	134	BH	Urgent

Parameter	Contact ID	SIA	Report Category
Water (Flood) alarm	154	WA	Urgent
Water (Flood) alarm restore	154	WH	Urgent
Gas alarm	151	GA	Urgent
Gas alarm restore	151	GH	Urgent
Carbon Monoxide alarm	162	GA	Urgent
Carbon Monoxide alarm restore	162	GH	Urgent
Low Temperature (Freeze alarm)	159	ZA	Urgent
Low Temperature restore	159	ZH	Urgent
High Temperature	158	KA	Urgent
High Temperature restore	158	KH	Urgent
Zone trouble	380	UT	Urgent
Zone trouble restore	380	UJ	Urgent
Burglary trouble	380	BT	Urgent
Burglary trouble restore	380	BJ	Urgent
Zone bypass	570	UB	Urgent
Zone bypass restore	570	UU	Urgent
Burglary bypass	573	BB	Urgent
Burglary bypass restore	573	BU	Urgent
Zone supervision loss	381	UT	Urgent
Zone supervision restore	381	UJ	Urgent
Tamper	144	TA	Urgent
Tamper restore	144	TR	Urgent
Zone lost	381	UT	Urgent
Zone lost restore	381	UJ	Urgent
Low battery	384	XT	Non-urgent
Low battery restore	384	XR	Non-urgent
Soak fail	380	UT	Urgent
Soak fail restore	380	UJ	Urgent
Zone Alarm	134	BA	Urgent
Zone Alarm restore	134	BH	Urgent
Zone confirm alarm	139	BV	Urgent
Zone confirm alarm restore	139		Urgent

Parameter	Contact ID	SIA	Report Category
No activity	393	NC	Urgent
No activity restore	393	NS	Urgent
Wireless Keypad			
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Keypad lost	355	BZ	Urgent
Keypad lost restore	355		Urgent
Keypad low battery	384	XT	Non-urgent
Keypad low battery restore	384	XR	Non-urgent
Wireless Keyfob			
Arm	409	CS	Arm/Disarm
Disarm	409	OS	Arm/Disarm
Low battery	384	XT	Non-urgent
Low battery restore	384	XR	Non-urgent
Wireless Siren			
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Low battery	384	XT	Non-urgent
Low battery restore	384	XR	Non-urgent
Siren bell trouble	321	YA	Non-urgent
Siren bell trouble restore	321	YH	Non-urgent
Siren lost	355	BZ	Urgent
Siren lost restore	355		Urgent
Siren auxiliary failure	300	YP	Non-urgent
Siren auxiliary restore	300	YQ	Non-urgent
Miscellaneous			
Enter programming (local)	627	LB	Arm/Disarm
Exit programming (Local)	628	LS (LX)	Arm/Disarm
Enter programming (Remote)	627	RB	Arm/Disarm
Exit programming (Remote)	628	RS	Arm/Disarm
MS periodic test	602	RP	Non-urgent
MS keep alive (polling)	999	ZZ	Urgent
System reset	305	RR	Urgent
Cancel Report	406	OC	Urgent

Parameter	Contact ID	SIA	Report Category
Walk Test	607	BC	Non-urgent
Walk Test restore	607		Non-urgent
Exit Error	374		Non-urgent
Enter Service Mode	393	LB	Non-urgent
Exit Service Mode	393	LX	Non-urgent
Fail Cloud Communication			Non-urgent

Appendix E: Remote Software Upgrade

This appendix explains how to perform remote upgrade of your LightSYS Air main panel software using the LightSYS Air keypad or SMS command. Remote software upgrade is performed via IP or GPRS/3G/4G.

Notes

1. It is recommended to perform the upgrade process from keypad 1 (not from a wireless keypad).
2. Software upgrade does not delete all previous parameters of the panel.

Step 1: Set parameters for IP/GPRS/3G/4G communication

Define all parameters required to set GPRS/4G or IP communication as explained in the Communication section of the LightSYS Air (See *page 116*).

Step 2: Enter the location of the firmware update file

- Go to: **1 → 8 (**installer **Programming menu → System → Firmware Update),** and enter the relevant information regarding the location of the F/W update file:
  - ❶ **Server IP**: Enter the IP address of the router/gateway where the F/W update file is located. Default: **firmware.riscogroup.com**
  - ❷ **Port**: Enter the port on the router/gateway where the F/W update file is located. Default: **00080**
  - ❸ **File Name**: Enter the F/W update file name. Default: **CMD.TXT**

Notes

1. The file name is case sensitive.
2. Please contact RISCO Group Customer Support services for the file name parameters.

Step 3: Activate the Remote Upgrade from the keypad

1. Go to: **1 → 8 → 4 (**installer **Programming menu → System → Firmware Update → Download File).**
2. Select the communication path as follows:
   - ❶ **Via IP**
   - ❷ **Via GPRS**

Notes

Each option appears only if the relevant module (IP or GPRS//4G module) is installed in the system.

If your panel is equipped with an IP or GSM module you can start the download file procedure by sending an SMS command to the panel in the following format:
(If address and port are configured and updated)

a. Via IP 97239637777IPFILE.
b. Via GSM (GPRS/3G/4G) 97239637777GSMFILE.

(Address and port can be added to the SMS command string as per the following. If specified, these parameters also override any existing panel settings)

a. Via IP 97239637777IPFILE10.10.10.6:80.
b. Via GSM (GPRS/3G/4G) 97239637777GSMFILE212.150.25.223:80.

3. Once selected, the LightSYS Air will start downloading the required files. The upgrade procedure may take approximately 40 minutes to complete. This will vary according to whether the procedure is performed via GPRS/3G/4G or IP. Once the files are downloaded the panel automatically starts with the upgrade procedure of the units connected to the system.

Notes

- During the upgrade process of the panel firmware there will be no display on the keypad.
- While downloading the files for the upgrade procedure the green STATUS LED on the main panel will flash slowly. When the upgrade procedure starts, it will start to flash rapidly.

Step 4: Verify the upgrade was successful

1. From the main display press **Exit** ( ) and enter the installer code followed by **OK** (✓).
2. Scroll to **Maintenance → Diagnostics→ Panel Version.** The upgraded version of the main panel will appear.
3. To view the other accessories version navigate to the required menus under the **Maintenance → Diagnostics** menu.

Note

If upgrade has failed, the previous software version of the main panel / accessory version will appear.

Appendix F: Compliance

Possible logical key calculations

- Logical codes are codes punched in the wireless keypad to allow Level 2 (users) and Level 3 (installer) access.
- All codes - 6 digits structure: xxxxxx
- 0-9 can be used for each digit.
- There are no disallowed codes - codes from 000001 to 999999 are acceptable.
- Invalid codes cannot be created due to the fact that after the code 4th digit has been punched, "Enter" is automatically applied. Code is rejected when trying to create a non-existing code.

Possible physical key calculations

- Physical keys are implemented in the wireless keyfobs.
- It is assumed that only a user possesses a keyfobs, therefore a physical key is considered as access Level 2
- Each keyfob has 24 bit identification code comprising 2^24 options.
- A keyfob has to be recognized and registered by the LightSYS Air, therefore, a "write" process must be performed.
- A valid keyfob is one "Learned" by the panel and allowing arm/disarm
- A non-valid keyfob is one not "learned" by the panel and not allowing arm/disarm.

System Monitoring

- The main unit is monitored for AC trouble, battery fault, low battery and more.
- All other wireless elements are monitored for low voltage battery.

Setting the LightSYS Air to comply with EN 50131 Requirements

1. Access the Installer programming mode.
2. From the ① System menu select ⑤ to access the Settings menu.
3. From the Settings menu select ④ to access the Standard option.
4. Select EN 50131. Once selected, the following changes will occur in the LightSYS Air software:

Feature	**EN 50131 Compliance**	
Timers	**Quick Key**	**Required Value:**
Entry Delay	①①⓪① ❶, ①①⓪② ❶	45 seconds (maximum allowed)
AC Delay	①①⓪② ❼	Immediate (0 minutes)
RX Supervision	①①⓪⑥ ❷	2 hours
System Controls	**Quick Key**	**Required Value:**
Quick Arm	①②① ❿❶	Set to NO
False Code Trouble	①②① ❿❺	Set to Yes
Forced Arming	①②① ❶❷	Set to NO
Authorize installer	①②④ ❿❶	Set to YES
Override Trouble	①②④ ❿❷	Set to NO
Restore Alarm	①②④ ❿❸	Set to YES
Mandatory Event Log	①②④ ❿❹	Set to YES
Restore Trouble	①②④ ❿❺	Set to YES
Exit Alarm	①②④ ❿❻	Set to NO
Entry Alarm	①②④ ❿❼	Set to YES
20 minutes signal	①②④ ❿❽	Set to YES
Attenuation	①②④ ❿❾	Set to YES

- After configuring the system to EN 50131, indications are made inaccessible and the display will show only "Enter code:" To show indications, you must enter a valid code.
- After entering 3 invalid user codes, an 'invalid code' signal will be alerted to the monitoring station and recorded in the event log. The invalid code will continue to alert in the system until restored by a user with a code

Appendix G: LightSYS Air Accessories

Part number	Description	Comments
Main Panel		
RW432MV8000A	LightSYS Air Panel (Voice&WiFi&IP),868MHz	
RW432M08000A	LightSYS Air Panel,WiFi&IP,868MHz	
RW432MV4000A	LightSYS Air Panel (Voice&WiFi&IP),433MHz	
RW432M04000A	LightSYS Air Panel,WiFi&IP,433MHz	
RW432MV4100A	LightSYS Air Panel(Voice&WiFi&IP),433/916,Ext. DC	
RW432MV8B00A	LightSYS Air Panel (Voice&WiFi&IP), 868MHz, Black	
RW432M04100A	LightSYS Air Panel,WiFi&IP,433/916,Ext.DC	
RW432M08B00A	LightSYS Air Panel,WiFi&IP, 868MHz, Black	
GSM Communication Modules		
RW432G4TVEUA	4G Module for LightSYS Air,VOICE,EU	
RW432G4K1EUA	4G for LightSYS Air,VOICE,EU+RISCO SIM	
RW432G4V1EUA	4G Module for LightSYS Air,VOICE,EU,LC	
Keypads		
RW432KPP802A	WL Panda KP LightSYS+/Air&Prox For 868MHz System	
RW432KPP402A	WL Panda KP LightSYS+/Air&Prox For 433MHz System	
RW432KPP8B2A	WL Panda KP LightSYS+/Air&Prox, 868MHz Sys, Black	

Part number	Description	Comments
Wireless Devices		
RW132KL1P00A	2-Way Black Ext. WL Slim KP+Prox	Black Proximity keypad 868 MHz
RW132KL2P00A	2-Way White Int. WL Slim KP+Prox	White Proximity keypad 868 MHz
RW132KL2P00H	2-Way White Int. WL Slim KP, 433 MHz	Black Proximity keypad 433 MHz
RW132KL1P00H	2-Way Black Ext. WL Slim KP, 433 MHz	Outdoor White Proximity keypad 433 MHz
RWX515PR080A	2 Way WL BWare PIR, 868MHz	
RWX515DT080A	2 Way WL BWare DT, 868 MHz	
RWX95086800C	2-Way WL iWAVE PIR, 868 MHz MHz	
RWX95P86800C	2-Way WL iWAVE Pet, 868 MHz	
RWX95P86800D	2-Way Wireless iWAVE PET/PIR,868MHz	
RWX95DT0800B	2 Way WL iWave DT, 868 MHz	
RWX95DTP800B	2 Way WL iWave DT Pet, 868 MHz	
RWX95P868BLD	2-Way Wireless iWAVE PET/PIR, 868MHz, Black	
RWX95CMP8BLC	2-Way WL eyeWAVE Pet Cam, 868MHz, Black	
RWT312PR400B	WL WatchOUT PIR, 433 MHz	
RWX10680200A	2-Way WL Curtain PIR, 868MHz	
RWX10640200A	2-Way WL Curtain PIR, 433MHz	
RWX73F8BL00C	2-Way Multi Contact,868, Black	
RWX96P40200A	2 Way WL Piccolo PET 433MHz	
RWX96C40200A	2 Way WL Piccolo PIR 433MHz	
RWX96C80200A	2 Way WL Piccolo PIR 868MHz	
RWX96P86800A	1&2 Way WL Piccolo Pet 868 MHz	
RWX96P80200A	2 Way WL Piccolo Pet 868MHz	
RWX73M8BL00D	2-Way Door/Win Contact, 868 MHz, Black	
RWX73M86800D	2-Way Door/Window Contacts, 868 MHz	
RWX73F8BR00C	2-Way Multi Contact, 868 MHz, Brown	

Part number	Description	Comments
RWX107DT800C	WL Outdoor DT Curtain 868+Swivel	
RWX107DT400A	WL Outdoor DT Curtain 433 MHz	
RWX73F86800C	2Way Multi-Function Contacts, 868 MHz	
RWX350D0800A	WL Beyond DT, 868 MHz	
RWX350DC800B	WL Beyond DT Cam, 868.65/869.525 MHz	
RWX350D0400A	WL Beyond DT, 433MHz	
RWX350DC400B	WL Beyond DT Cam, 433/916MHz	
RWX73M43300D	2Way Door/Window Contacts, 433 MHz	
RWX73F43300C	2Way Multi-Function Contacts, 433 MHz	
RWX34S43300B	Smoke & Heat Detector1&2 Way 433 MHz	
RWX780868M3C	2-way Slim Contact X73 868MHz	
RWX7808BLM3C	2-Way Slim Contact X73 868MHz, Black	
RWX35S00400C	WL Smoke & Heat, 433 MHz	
RWX35S00800C	WL Smoke & Heat, 868 MHz	
RWT6GS41100A	WL GAS Detector 433 MHz, 110V	
RWT6FW43300B	WL Flood Detector 433 MHz-White	
RWX132KF800A	2-Way WL Remote Control, 868 MHz	
RWX332KF800B	Panda 2-Way KeyFob 868MHz	
RWX332KF400A	Panda 2-Way KeyFob 433MHz	
RWX332KF8BLB	Panda 2-Way KeyFob 868MHz, Black	
RWT52P86800A	2 Button Panic Keyfob, 868 MHz	
RWT52P43300A	2 Button Panic Keyfob, 433 MHz	
RWT51P80000A	Wristband Panic Transmitter, 868 MHz	
RWS42086800B	WL Indoor Sounder, 868 MHz, Round	
RWS42043300B	WL Indoor Sounder, 433 MHz, Round	

Part number	Description	Comments
Wireless External Sirens		
RWS50B868UKB	WL External Sounder, Blue 868 MHz UK	
RWS20A86800B	Wireless ProSound, 868 MHz	
RWS401A8000B	WL Lumin8, Amber 868 MHz	
RWS401B4000B	WL Lumin8, Blue, 433 MHz	
RWS401B8000B	WL Lumin8, Blue 868 MHz	
RWS401R8000B	WL Lumin8, Red, 868MHz	

Appendix H: Installer Programming Maps

Installer Programming Menu

1) System			
1) Timers			
	01) Ex/En Delay 1		
	02) Ex/En Delay 2		
	03) Bell Timeout		
	04) Bell Delay		
	05) Switch Aux Break		
	06) Wireless		
	07) AC Off Delay		
	08) Guard Delay		
	09) Swinger Limit		
	10) Redial Wait		
	11) Last Exit Sound		
	12) Buzzer at Stay		
	13)Status Timer		
	14) Service Timer		
	16) Pulse Open		
	17) Inactivity Timer		
	18) T.O. Beeps		
2) Controls			
	1) Basic		
		01) Quick Arm	
		02) Quick UO	
		03) Allow Bypass	
		04) Quick Bypass	
		05) False Code Trouble	
		06) Bell Squawk	
		08) Audible Panic	
		09) Buzzer → Bell	
		10) Enable Jamming	
		11) Audible Jamming	
		12) Ex..St. Beep	
		13) Forced KSW	
		14) Arm Prewrn	
	2) Advanced		
		01) Dbl Verification Fire	
		03) Code Grand Master	
		04) Area	
		05) Global Follow	
		06) Summer/Winter	
		07) 24 Hour Bypass	
		08) Technician Tamper	

		09) Technician Reset	
		10) Engineer Tamper	
		11) Low battery Arming	
		12) Bell 30/10	
		13) Fire Temporal Pattern	
		14) IMQ Install	
		16)Disable. Keypad Auto Arming	
		17) Buzzer Delay	
		18) Speaker=Buzzer	
		19) Confirm Speaker	
		20) Bell Confirmation	
		21) Error Speaker Time On	
		22) AC Trouble Arm	
		23) Strobe Arm	
		24) Final Night	
		25) Stay Strobe	
		26) Blank Display	
		27) Display System Label	
		28) Presence Log Event	
		29) Wireless Lost as Tamper	
	3) Communication		
		1) Monitoring Station Enable	
		2) Follow Me Enable	
		3) CS Enable	
		4) Cloud Enable	
		5) External Communication	
	4) EN 50131		
		1) Authorize Installer	
		2) Override Trouble	
		3) Restore Alarm	
		4) Mandatory Event Log	
		5) Restore Troubles	
		6) Exit Alarm	
		7) Entry Alarm	
		8) 20 minutes signal	
		9) Attenuation	
	5) PD6662		
		1) Bypass Exit/Entry	
		2) Entry Disable	
		3) Route Disable	
		4) Installer Confirmation	
		5) Key switch Lock	
		6) Entry Disarm	
		7) Proximity Disarm	
	6) CP-01		
		1) Exit Restart	
		2) Auto Stay	
	7) Device		
		1) Anti Mask = Tamper	
		2) Proximity Anti Mask =	

		Tamper	
		5) Siren Pre-Alarm	
		6) RF wake-up	
		7) KF Instant Arm	
		8) KF Instant Stay	
		9) KF Dis+Code	
3) Labels			
	1) System		
	2) Partitions (1—32)		
4) Sounds			
	1) Tamper Sound		
		1) During Disarm	
			1) Silent
			2) Bell only
			3) Buzzer (main) only
			4) Bell + Buzzer
		2) During Arm	
			1) Silent
			2) Bell only
			3) Buzzer (main) only
			4) Bell + Buzzer
	2) Speaker Volume		
		1) Trouble	
		2) Chime	
		3) Exit/Entry	
		4) Alarm	
		5) Squawk	
5) Settings			
	2) Default Panel		
		With labels?	
	3) Erase Wireless		
	4) Standard		
		1) EN 50131 (G2)	
		2) PD6662	
		3) CP-01	
	5) Customer		
		1) 0EN	
		2) 0IT	
		3) 0IL	
		4) 0HU	
		5) 0UK	
		6) 0SP	
		7) 0PL	
		8) 0GR	
		9) 0BR	
		10) 0RU	
		11) 0NL	
		12) 0FR	
		13) 0CN	

		14) 0DK	
		15) 0CZ	
		16) 0AU	
		17 0TH	
		18) 0DE	
		19) 0IE	
		20) 0GT	
	6) Language		
		1) Text	
			(language selection)
	7) Partition Quantity		
	8) Bypass Tamper		
6) Automatic Clock			
	1) Server		
		1) NTP	
		2) DAYTIME	
	2) Host		
	3) Port		
	4) Time Zone (GMT)		
7) Service Info.			
	1) Name		
	2) Phone		
8) Firmware Update			
	1) Server IP		
	2) Server port		
	3) File name		
	4) Download Files		
		1) Via IP	
		2) Via GPRS	

2) Zones				
1) Parameters				
	1) One By One			
		Label		
		Partition/s		
		Group/s		
		Type		
			00) Not used	
			01) Exit/Entry 1	
			02) Exit/Entry 2	
			03) Exit(OP)/Entry 1	
			04) Exit(OP)/Entry 2	
			05) Entry Follower	
			06) Instant	
			07) I+ Exit/Entry 1	
			08) I+ Exit/Entry 2	
			09) I+Exit(OP)/Entry1	

			10) I+Exit (OP)/Entry2	
			11) I + Entry Follow	
			12) I+ Instant	
			13) UO/REX Trigger	
			14) Day Zone	
			15) 24 Hours	
			16) Fire	
			17) Panic	
			18) Special	
			19) Key switch	
			20) Final Exit	
			21) Latch Keyswitch	
			22) EN.Foll + Stay	
			23) Pulsed Keyswitch Delay	
			24) Latch Keyswitch Delay	
			25) Tamper	
			26) Technical	
			27) Water	
			28) Gas	
			29) CO	
			30) Exit Term	
			31) High temp	
			32) Low temp.	
			33) Key box	
			34) Keyswitch Arm	
			35) Keyswitch Delayed Arm	
		Arm sound		
			1) Silent	
			2) Bell only	
			3) Buzzer only	
			4) Bell + buzzer	
			5) Door chime	
		Stay sound		
			1) Silent	
			2) Bell only	
			3) Buzzer only	
			4) Bell + buzzer	
			5) Door chime	
		Disarm sound		
			1) Silent	
			2) Bell only	
			3) Buzzer only	
			4) Bell + buzzer	
			5) Door chime	
	2) By Category			
		1) Label		
		2) Partition		
		3) Type		
			00) Not used	
			01) Exit/Entry 1	

			02) Exit/Entry 2	
			03) Exit(OP)/Entry 1	
			04) Exit(OP)/Entry 2	
			05) Entry Follower	
			06) Instant	
			07) I+ Exit/Entry 1	
			08) I+ Exit/Entry 2	
			09) I+Exit(OP)/Entry1	
			10) I+Exit (OP)/Entry2	
			11) I + Entry Follow	
			12) I+ Instant	
			13) UO/REX Trigger	
			14) Day Zone	
			15) 24 Hours	
			16) Fire	
			17) Panic	
			18) Special	
			19) Key switch	
			20) Final Exit	
			21) Latch Keyswitch	
			22) EN.Foll + Stay	
			23) Pulsed Keyswitch Delay	
			24) Latch Keyswitch Delay	
			25) Tamper	
			26) Technical	
			27) Water	
			28) Gas	
			29) CO	
			30) Exit Term	
			31) High temp	
			32) Low temp.	
			33) Key box	
			34) Keyswitch Arm	
			35) Keyswitch Delayed Arm	
		4) Sound		
			1) At Arm	
				1) Silent
				2) Bell only
				3) Buzzer only
				4) Bell+buzzer
				5) Door chime
			2) At Stay	
				1) Silent
				2) Bell only
				3) Buzzer only
				4) Bell+buzzer
				5) Door chime
			3) At Disarm	
				1) Silent
				2) Bell only

				3) Buzzer only
				4) Bell+buzzer
				5) Door chime
		7) Advanced		
			1) Forced Arming	
				1) Enable
				2) Disable
			2) Pulsed Counter	
			3) Abort Alarm	
				1) Enable
				2) Disable
			5) Wireless Zone Parameters	
			6) Presence	
2) Testing				
	1) Self Test			
		1) Times		
		2) Zones		
	2) Soak Test			
3) Cross Zones				
	Pair			
		1) None		
		2) Ordered		
		3) Not ordered		
4) Alarm confirm				
	1) Confirm partition			
	2) Confirm zones			

3) Outputs			
0) Follows Nothing			
1) Follows System			
	01) Bell follow		
	02) No. Tel Line		
	03) Comm. failure		
	04) Trouble follow		
	05) Low battery follow		
	06) AC loss follow		
	07) Sensors test		
	08) Battery Test		
	09) Bell Burglary		
	10) Scheduler		
	11) Switched Aux		
	12) GSM Error		
	13) Bell Test		
	14) Installation		
	15) Walk Test		
	16) Burglary		
	17) Panic		
	18) Fire		

	19) Special		
	20) 24 Hour		
2) Follows Partition			
	01) Ready follow		
	02) Alarm follow		
	03) Arm follow		
	04) Burglary follow		
	05) Fire follow		
	06) Panic follow		
	07) Special follow		
	08) Buzzer follow		
	09) Chime follow		
	10) Exit/Entry follow		
	11) Fire Trouble		
	12) Day (Zone) Trouble		
	13) Trouble follow		
	14) Stay follow		
	15) Tamper follow		
	16) Disarm follow		
	17) Bell follow		
	18) Bell Stay Off		
	19) Zone Bypass		
	20) Auto Arm Alarm		
	21) Zone Loss Alarm		
	22) Bell Trigger		
	23) Strobe Trigger		
	24) Fail To Arm		
	25) Confirm Alarm		
	26) Duress follow		
	27) HU Confirm Alarm		
	32) Zone Exclude		
3) Follows Zone			
	1) Zone Follow		
	2) Alarm Follow		
	3) Arm Follow		
	4) Disarm Follow		
4) Follows Code			
	1) U. Output		

4) Codes			
1) User			
	1) Partition		
	2) Authority		
2) Grand Master			
3) Installer			
4) Sub Installer			
5) Code Length			
	1) 4 digits		
	2) 6 digits		

5)Communication				
1) Method				
	2) GSM			
		1) Timers		
			1) GSM Lost	
			2) GSM Net Loss	
			3) SIM Expire	
			4) MS Polling	
				1) Primary
				2) Secondary
				3) Backup
		2) GPRS		
			1) APN Code	
			2) APN User Name	
			3) APN Password	
		3) Email		
			1) Mail Host	
			2) SMTP Port	
			3) Email Address	
			4) SMTP User name	
			5) SMTP Password	
		4) Controls		
			1) Caller ID	
			2) LED Enable	
		5) Parameters		
			1) PIN Code	
			2) SIM Number	
			3) SMS Center Phone	
			4) GSM RSSI	
				1) Disable
				2) Low Signal
				3) High Signal
		6) Prepay SIM		
			1) Get Credit by	
				1) Credit SMS
				3) Service Cmnd
			2) Phone To Send	
			3) Phone To Receive	
			4) SMS Message	
	3) IP			
		1) IP Configuration		
			1) Obtain IP	
				1) Dynamic ID
				2) Static ID
			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) Email		
			1) Mail Host	
			2) SMTP Port	
			3) Email Address	
			4) SMTP Name	
			5) SMTP Password	
		3) Host Name		
		4) MS Polling		
			1) Primary	
			2) Secondary	
			3) Backup	
		5) Controls		
			1) Disable IP N/Y	
2) Monitoring Station				
	0) MS Mode			
	1) Report Type			
		1) MS 1 2) MS 2 3) MS 3		
			2) IP	
				1) IP/GPRS
				2) GPRS/IP
				3) IP Only
				4) GPRS Only
			3) SMS	
				MS Phone Number
			5) SIA IP	
				1) IP/GPRS
				2) GPRS/IP
				3) IP Only
				4) GPRS Only
	2) Accounts			
		1)Partition		
	3) Comm. Format			
		1) Contact ID		
		2) SIA		
	4) Controls			
		1) Call Save		
		2) Show Kissoff		
		3) Show Handshake		
		4) Audible Kissoff		
		5) SIA Text		
		6) Random MS Testing		
		7) SIA w/part		

		8) SIA CH INFO		
	5) Parameters			
		1) MS Retries		
		2) Alarm Restore		
			1) On Bell Time out	
			2) Follow Zone	
			3) At Disarm	
		3) SIA IP Parameters		
			1) MS 1 2) MS 2 3) MS 3	
				1) Encryption Key
				2) Receiver Number
				3) Line Number
	6) MS Times			
		1) Periodic Test		
		2) Abort Alarm		
		3) Cancel Delay		
		5) Confirmation		
			1) Confirm Start	
			2) Confirm Time	
	7) Report Split			
		1) MS Arm/Disarm		
			1) Do Not Call	
			2) Call 1st	
			3) Call 2nd	
			4) Call 3rd	
			5) Call All	
			6) 1st Bkup 2nd	
			7) 1st Bk 2nd 3rd	
			8) 1 Bk 3 Call 2	
			9) 2 Bk 3 Call 1	
		2) MS Urgent		
			1) Do Not Call	
			2) Call 1st	
			3) Call 2nd	
			4) Call 3rd	
			5) Call All	
			6) 1st Bkup 2nd	
			7) 1st Bk 2nd 3rd	
			8) 1 Bk 3 Call 2	
			9) 2 Bk 3 Call 1	
		3) MS Non Urgent		
			1) Do Not Call	
			2) Call 1st	
			3) Call 2nd	
			4) Call 3rd	
			5) Call All	
			6) 1st Bkup 2nd	
			7) 1st Bk 2nd 3rd	

			8) 1 Bk 3 Call 2		
			9) 2 Bk 3 Call 1		
	8) Report Codes				
		1) Edit Codes			
			1) Alarms		
				1) Panic	
				2) Fire	
				3) Medical	
				4) Duress	
				5) Confirm Alarm	
				6) Box Tamper	
				7) Bell Tamper	
				8) Recent Close	
				9) HU Confirm.	
			2) Main Troubles		
				01) Low Battery	
				04) AC Loss	
				06) Clk not set	
				08) False code	
				09) GSM trouble	
				10) IP net trbl.	
				11) MS 1 trouble	
				12) MS 2 trouble	
				13) MS 3 trouble	
			3) Arm/Disarm		
				1) User	GM (000) User: (001-- 499)
				2) Automatic	
				3) Remote	
				4) Force Arm	
				5) Quick Arm	
				6) Keyswitch	
				7) Auto Arm Fail	
			4) Zones		
				1) By zone	1) Alarm 2) Trouble 3) Bypass 4) Tamper 5) Low Battery
				2) Zone lost	
				3) Soak fail	
				4) Self test	
			5) Accessories		
				1) Keypad	1) Tamper

					2) Low Battery 3) Lost
				3) Utility Output	1) Tamper
				5) Keyfob	1) Arm/Dis 2) Low bat
			6) Miscellaneous		
				01) Enter prog.	
				02) Exit prog.	
				03) MS per. test	
				04) System reset	
				05) Abort alarm	
				07) MS polling	
				08) Cancel report	
				09) Walk test	
				10) Exit error	
				11) Fail Cloud	
				12) Ent. Serv. Mod	
				13) Ex. Serv. Mod	
		2) Delete All			
3) Configuration					
	1) Security				
		1) Access code			
		2) Remote ID			
		3) MS Lock			
	3) Control				
		1) User Initiate			
	4) IP Gateway				
		1) IP Address			
		2) IP Port			
4) Follow Me					
	1) Define FM				
	(Select FM 01—64)				
		1) Report Type			
			1) Voice		
				1) PSTN/GSM 2) GSM/PSTN 3) PSTN only 4) GSM only	
			2) Email		

				1) IP/GPRS 2) GPRS/IP 3) IP only 4) GPRS only
			3) SMS	
		2) Partition		
		3) Events		
			1) Alarms	
				1) Intruder alarm
				2) Fire alarm
				3) Emergency alarm
				4) Panic alarm
				5) Tamper alarm
				6) Duress alarm
				7) Confirm alarm
			2) Arm/Disarm	
				1) Arm
				2) Disarm
			3) Troubles	
				01) False code
				02) Main low battery
				03) WL low battery
				04) Jamming
				05) WL lost
				06) AC off
				07) Siren low battery
				9) IP network
				10) Charge Trouble
			4) GSM	
				1)GSM trouble
				2)SIM trouble
				3)SIM expire
				4)SIM credit
			5) Environmental	
				1) Gas alert
				2) Flood alert
				3) CO alert
				4) High temp.
				5) Low temp
				6) Technical
			6) Miscellaneous	
				1) Zone bypass
				2) Periodic test
				3)Remote programming
		4) Restore Events		
			1)Alarms	
				1) Intruder alarm
				2) Tamper alarm
			2) Troubles	
				01) Main low battery

				02) WL low battery
				03) Jamming
				04) WL lost
				05) AC off
				07) Siren low battery
				09) IP network
				10) Charge Trouble
			3) GSM	
				1) GSM trouble
			4) Environmental	
				1) Gas alert
				2) Flood alert
				3) CO alert
				4) High temperature
				5) Low temperature
				6) Technical
		5) Remote Control		
			1) Remote Listen	
			2) Remote Program	
	2) Controls			
		1)Disarm Stop FM		
		2) Disbl. report at Stay		
	3) Parameters			
		1) FM retries		
		3) Periodic Test		
5) Cloud				
	0) Cloud Mode			
	1) IP Address			
	2) IP Port			
	3) Password			
	4) Channel			
		1) IP Only		
		2) GSM Only		
		3) IP/GSM		
		4) GSM/IP		
	5) Controls			
		1)MS Call All		
		2)FM Call All		
		3)App Arm		
		4)App Disarm		
		5)App Exit Delay		
		6) Encryption		

7) Install				
2) Wireless Device				
	1) RX Calibration			
		Receiver		
			Re-calibrate?	

	2) Allocation			
		1) By RF		
			1) Zone	
			2) Keyfob	
			3) Keypad	
			4) Sounder	
			5) Repeater	
		2) By code		
			1) Zone	
			2) Keyfob	
			3) Keypad	
			4) Sounder	
			5) Repeater	
	3) Delete			
8) Devices				
1) Keypad				
	1) Label			
		Assign to partition		
		Masking		
		1) Emergency		
		2) Multi view		
		3) Exit Beeps		
		4) Supervision		
	2) Partition			
		Assign to partition		
		Masking		
		1) Emergency		
		2) Multi view		
		3) Exit Beeps		
		4) Supervision		
	3. Masking			
		Masking		
		1) Emergency		
		2) Multi view		
		3) Exit Beeps		
		4) Supervision		
	4) Controls			
		1) Emergency		
		2) Multi view		
		3) Exit Beeps		
		4) Supervision		
	5) Serial Number			
2) Keyfob Button 1—8:				
	5) Serial No.			
	6) Masking			
	7) Controls			
	12) Button ARM			

	13) Button DISARM			
	14) Button *			
	15) Button STAY			
	16) Select ASSIGN			
3) Sounder				
	1) Parameter			
		01) Label		
		02) Masking		
		03) Strobe		
			1) Control	
				1) Always Off
				2) Follow Bell
				3) Follow Alarm
			2) Blink	
				1) 20[Times/Min]
				2) 30 [Times/Min]
				3) 40 [Times/Min]
				4) 50 [Times/Min]
				5) 60 [Times/Min]
			3) Arm Squawk	
		07) Volume		
			S=01 Volume Level 9 (0-9)	
		12) Serial Number		
		13) Supervision		
		14) Select Assign		
7) Repeater				
	1) Serial Number			
	3) Label			
	3) Supervision			
0) Exit				

Additional Installer Menus

Activities Menu				
Keypad Sound				
	Chime			
		Keypad Chime		
		Partition Chime		
	Buzzer On/Off			
Advanced…				
	Service Mode			
	MS Test			
Wi-Fi…				
	Wi-Fi Scan			
	Wi-Fi WPS Button			
Follow Me Menu				
Define				
Test FM				
View Menu				
Trouble				
Alarm Memory				
	All Partitions Disarmed			
Partition Status				
	(zone number)			
Zone Status				
	(zone number)			
Service Info				
	Installer			
	System Version			
	Serial Number			
	Panel ID			
	Cloud Status			
	WiFi Status			
Clock Menu				
Time and Date				
Scheduler				
	Weekly (schedules 1--64)			
		1) Arm/Disarm		
			1) ON/OFF	
			2) Partition	
			3) Arming Mode	
				1) Arm
				2) Stay
				3) Group (A, B, C, D)
			4) Day/ Time	
				1) Monday Arm/Disarm times

				2) Tuesday Arm/Disarm times
				3) Wednesday Arm/Disarm times
				4) Thursday Arm/Disarm times
				5) Friday Arm/Disarm times
				6) Saturday Arm/Disarm times
				7) Sunday Arm/Disarm times
				8) All Arm/Disarm times
			5) Label	
				Schedule label
			6) Inactive	
				Inactive Timer OFF/ON
		2) UO ON/OFF		
			1) ON/OFF	
				Schedule(s) ON/OFF
			2) Utility Outputs	
				Utility Outputs Y/N
			3) Day/Time	
				1) Monday Start/Stop times
				2) Tuesday Start/Stop times
				3) Wednesday Start/Stop times
				4) Thursday Start/Stop times
				5) Friday Start/Stop times
				6) Saturday Start/Stop times
				7) Sunday Start/Stop times
				8) All Start/Stop times
			4) Vacation	
				UO Vacation Y/N Vac.start/stop times
			5) Label	
				Schedule label
		3) USER LIMIT		
			1)ON/OFF	
				Schedule ON/OFF
			2) Users number	
				00) Grand Master Y/N
				(01—) User
			3) Day/Time	
				1) Monday Start/Stop times

				2) Tuesday Start/Stop times
				3) Wednesday Start/Stop times
				4) Thursday Start/Stop times
				5) Friday Start/Stop times
				6) Saturday Start/Stop times
				7) Sunday Start/Stop times
				8) All Start/Stop times
			4) Label	
				Schedule label
	One Time			
		Next Arm		
			Next Arm partition/s	
			Next Arm Time	
		Next Disarm		
			Next disarm partition/s	
			Next disarm time	
Vacation				
	Partitions			
		(partition number/s)		
	Dates			
		Start time & date		
		Stop time & date		
Event Log Menu				
Event/s				
	Security Log			
	AC Event Log			
Maintenance Menu				
Walk test				
	Full Walk Test			
		Results (per event)		
	Quick Walk Test			
		Results per zone		
Keypad test				
Siren test				
Strobe test				
Wireless test				
	Zones			
		Communication Test		
		Battery Test		
	Keyfobs			
		Communication Test		
		Battery Test		
	WL Keypads			
		Communication Test		

		Battery Test		
	WL Sirens			
		Communication Test		
		Battery Test		
	Repeaters			
		Communication Test		
		Battery Test		
Diagnostics				
	Main battery test			
		0) Main Board		
		1) Siren 1		
		2) Siren 2		
	Siren			
		Select Siren		
			Siren Version	
			Siren Calibration	
				New threshold
	GSM			
		Signal (0—5)		
		Version		
		IMEI		
	IP			
		IP Address		
		MAC Address		
		WiFi MAC Address		
	WME Version			
	Panel Version			
	Keypad Version			
	W2W Zone Version			
	W2W KF Version			
	Repeaters			
Macro Menu				
Macro (A, B, C, D)				
	Start/stop macro			
Standalone Keyfob Menu				
Select Receiver				
	New Keyfob			
		Start/stop Learn mode		
	Delete Keyfob			
		Start Erase mode		
	Delete All			
	UO Buttons			

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

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.

Installer Notes

Contacting RISCO Group

RISCO Group is committed to customer service and product support. You can contact us through our website (www.riscogroup.com) or at 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 from: