RISCO

A LIFETIME OF SECURITY

LightSYS Plus

User Manual

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

Important Notice

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

This document 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.

Copyright Information

RISCO Group 2022. All rights reserved. No part of this document may be reproduced in any form without prior written permission from the publisher.

Contents

LIGHTSYS PLUS MAIN FEATURES 1

Flexible, Scalable, Hybrid System 1
Advanced Features for System Users 1
Empowered by the RISCO Cloud 2
Self-Monitoring, Operation and Notification via the RISCO Cloud 2
iRISCO Smartphone App 2
Web User Interface 2
System Capabilities 3
Alarm Receiving Centre Partnership 5
Operational Devices & Interfaces for System Users 6

IMPORTANT SAFETY PRECAUTIONS 8

GETTING STARTED 8

INITIAL SETUP TASKS FOR THE GRAND MASTER 9

Who Can / Can't Perform the Procedures? 9
Step 1: Changing the Default Grand Master Code 10
Step 2: Registering the System to the RISCO Cloud 10
Viewing the Panel ID at the Keypad 11
Step 3: Logging into the RISCO Cloud / Web User Interface 11
Step 4: Downloading the iRISCO Smartphone App 11
Logging into the iRISCO App 11
Step 5: Working with Keypads and User Menus 12
Keypad Buttons 12
User Menus 13
Step 6: Defining User Codes and Proximity Tags 13
Describing User Authority Levels 14
Table of User Authority Levels 14
Describing User Codes 16
Creating or Editing User Codes 16
Creating or Editing the Duress-Unsetting Code 17
Creating or Editing Labels 19
Deleting Codes 19
Describing Proximity Tags 20
Defining and Enrolling Proximity Tags 21
Enrolling My Own Proximity Tag 21
Deleting Proximity Tags 22
Deleting a Proximity Tag by its Index Number 22
Deleting a Proximity Tags by its Tag 23

Deleting My Own Proximity Tag 23
STEP 7: DEFINING FOLLOW-ME DESTINATIONS 24
Examples of Follow-Me Notifications *24*
Creating or Editing Follow Me Destinations *25*
Special Dialing Characters for Voice Notifications 25
Deleting Follow Me Destinations *26*
Testing Follow-Me Destinations *26*
STEP 8: DEFINING KEYFOBS FOR OUTPUT (GATE) CONTROL 27
Registering New Keyfobs for Output Control *27*
Changing the Keyfob Buttons for Output Control *28*
Deleting the Registration for a Single Output Control Keyfob *28*
Deleting Registrations for all Output Control Keyfobs *29*
STEP 9: PERFORMING AN ALARM RECEIVING CENTRE TEST 29
STEP 10: PERFORMING A WI-FI SCAN 29
STEP 11: TRAINING SYSTEM USERS 30

OPERATING THE SYSTEM 31

MODES OF OPERATION 31
Remote Operational Modes *31*
Local Operational Modes *31*
Receiving and Acknowledging a Follow-Me Status Call *31*
Acknowledgement Menu 31
Operations Menu 32
OPERATING REMOTELY BY SMS 33
SMS Commands *33*
OPERATING THE LISTEN-IN & SPEAK UNIT 34
OPERATING LOCALLY BY KEYPADS, REMOTE CONTROLS/KEYFOBS, AND PROXIMITY 34
Working with Keypads *34*
Keypad Display Options 34
Using the "Multi View" Keypad Display 34
Using the "Blank" Keypad Display 35
OBTAINING SYSTEM INFORMATION 35
Obtaining System Status – Requested from Remote Controls *37*
Obtaining System Status – Requested from Keypads *37*
Obtaining System Information – Requested from, and Viewed at Keypads *38*
Viewing the Event Log 38
Viewing Alarm Memory 39
Viewing System Faults 39
Viewing Zone Status 39
Viewing Partition Status 40
Viewing IP Address 40
Viewing Service Information 40
Engineer Information 41
System Version 41

Serial Number 41
Panel ID 41
OMITTING ZONES 42
Viewing Not-Ready Zones *42*
Defining Zone Omit Status *43*
Quickly Omitting/Un-Omitting Zones on a One-Time Basis *44*
SETTING & UNSETTING THE SYSTEM 45
Setting/Unsetting Modes *45*
Before Setting the System *45*
Setting Procedures *46*
Full Setting 46
Part Setting 48
Partition Setting 50
Setting All Partitions 51
Setting an Individual Partition 52
Group Setting 54
Automatic Setting and Unsetting 55
Setting with System Faults 55
Omitting Zones (Setting with Manually-Omitted Zones) 55
Keyswitch Setting 55
Forced Keyswitch or Proximity Setting 55
Low-Battery Setting 56
Strobe Setting 56
Unsetting Procedures *56*
Unsetting All Partitions 57
Unsetting an Individual Partition 58
Duress Unsetting 59
Unsetting with Alarm Activation (Silencing an Alarm) 59
RETURNING THE SYSTEM TO NORMAL OPERATION AFTER ALARM ACTIVATION 60
Resetting the System with Engineer Intervention *60*
Anti-Code Reset (Engineer Reset) 61
Configuration Software Reset 61
Enabling Engineer CS Access for Resetting the System 61
Resetting latched devices *62*
Restoring the System upon Power Supply Overload *63*
ACTIVATING EMERGENCY ALARMS 64
Activating a Panic ("Police") Alarm *65*
Activating a Fire Alarm *65*
Activating an Auxiliary ("Emergency") Alarm *66*
Activating a Duress-Unsetting Alarm *66*
DESCRIBING UTILITY OUTPUTS 67
UO Operational Modes *67*
MANUALLY OPERATING UTILITY OUTPUTS 68
DEFINING AUTOMATICALLY-OPERATED UOS AND SETTING OPERATIONS 69

Defining a "One-Time" Schedule for Automatic Setting *69*
Defining Weekly Schedules for Automatic Setting and UOs *70*
Configuring the Set/Unset Option 70
Turning a Setting/Unsetting Schedule On or Off 70
Defining Partitions for the Setting/Unsetting Schedule 70
Selecting a Setting Mode for the Setting/Unsetting Schedule 71
Setting the Day & Time for the Setting/Unsetting Schedule 71
Defining a Label for the Setting/Unsetting Schedule 71
Turning the Inactivity Timer On or Off for the Setting/Unsetting Schedule 71
Configuring the UO Option 72
Turning a UO Schedule On or Off 72
Defining the Utility Output(s) for the Schedule 72
Setting the Day and Time for the UO Schedule 72
Defining a UO Schedule as a "Holiday" UO Schedule 72
Defining a Label for the UO Schedule 72
Configuring the User Limitation Option 73
Applying/Removing a User Limitation 73
Describing Holiday Schedules *73*
Setting Dates/Times and Activating a Holiday Schedule 74
Defining Partitions for a Setting Holiday Schedule 74
USING MACROS 75
Recording Macros *75*
Activating Macros *75*
PERFORMING MAINTENANCE TASKS 76
Defining the Time and Date Manually *76*
Replacing Detector & Accessory Batteries in Service Mode *76*
Performing SIM Card Maintenance *77*
Checking the SIM Credit Level 77
Resetting the SIM Card 77
Enabling / Disabling Keypad Sounds *77*
Enabling / Disabling the Current Keypad's Chime 78
Enabling / Disabling All Keypad Chimes 78
Enabling / Disabling the Current Keypad's Buzzer 78
Terminating Follow-Me Notifications *79*
Cancelling Alarm Receiving Centre Notification upon Engineer Programming *79*
TESTING THE SYSTEM 79
Performing a Walk Test *80*
Testing ARC Communication *80*
Testing Follow-Me Destinations *81*
Performing a Keypad Test *81*
Performing a Sounder Test *81*
Performing a Strobe Test *82*

APPENDIX A: SCHEDULING CHART FOR AUTOMATIC UO & SETTING OPERATIONS 83

APPENDIX B: USER MENU MAPS 84

APPENDIX C: SYSTEM INDICATORS 85

SOUND INDICATORS 85
"Beep" and "Squawk" Sound Indicators 85
Voice Announcements 87
VIEWED INDICATORS 87
Keypad Indicators 87
Slim Keypad Indicators 87
Narrow Keypad Indicators 88
Panda Keypad Indicators 88
Elegant Keypad Indicators 89
Remote Control Indicators 89
8-Button Remote Control Indicators 89
4-Button Panda Keyfob Indicators 89

LightSYS Plus Main Features

Flexible, Scalable, Hybrid System

The ideal security solution for both residential and commercial sectors, LightSYS Plus offers communication flexibility and advanced system control and operation for small and large installations using state-of-the-art RISCO detectors and accessories – including remote user operation via Smartphone and Web user apps.

A flexible hybrid system that is scalable according to your needs, LightSYS Plus empowers you to utilize up to 512 zones and 500 system users.

LightSYS Plus utilizes a wide range of RISCO peripherals in almost any combination, including wireless detectors, bus detectors and wired relay detectors – as well as a multitude of other security and safety accessories.

LightSYS Plus is compatible for multi-site projects that utilize SynopSYS – RISCO's "In-House Central" security management solution.

Advanced Features for System Users

- ✓ **Live video verification** using RISCO's revolutionary Cloud-enabled VUpoint P2P cameras – for real-time verification of alarms and events, as well as live video on demand
- ✓ **User monitoring & event notification** via the Cloud-based iRISCO Smartphone app and the Web User Interface
- ✓ **Follow-Me reporting** for sending event notifications up to 64 recipients — via SMS, e-mail or voice messages
- ✓ **Event logging** of up to 2000 system events, including alarms, setting/unsetting, Omitting, faults, restores, and resets. View events on keypads, via the iRISCO Smartphone app, and with RISCO's Web user interface.
- ✓ **Scheduling automatically-operated operations** for setting and activation of external devices and appliances via utility outputs – for a one-time occurrence, on a reoccurring weekly basis, or for vacations

Empowered by the RISCO Cloud

Cloud communication is available either from the RISCO Cloud – RISCO's application server, or from a privately-hosted server.

Self-Monitoring, Operation and Notification via the RISCO Cloud

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 an Alarm Receiving Centre. The RISCO Cloud also enables operating RISCO's Home Automation services.

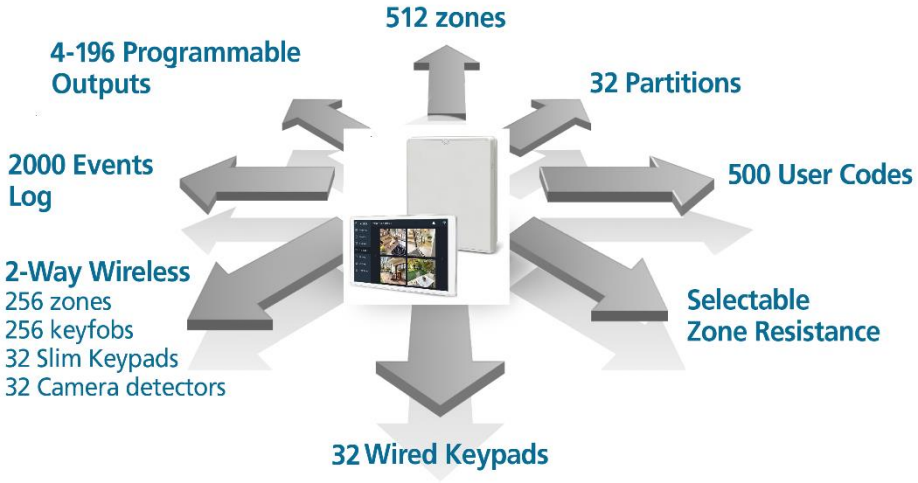
iRISCO Smartphone App

The iRISCO Smartphone app provides smart and easy control of the system, enabling on-the-go users to receive event notifications, view the system's status and event history, set/unset the system, activate home automation devices, omit zones, and utilize IP cameras for real-time, live visual verification and self-monitoring. iRISCO is downloadable from the Apple App Store for iOS devices and from the Play Store for Android devices.

Web User Interface

RISCO's Web User Interface enables system users to monitor, control and operate 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.

System Capabilities



Capabilities	Description
Users (user codes)	500 (with a selection of authority levels)
Total zones	512 (of varied combinations)
Bus zones	512
Hard wired zones	512
Wireless zones	256 (1-way & 2-way)
Partitions & groups	• 32 partitions (any zone can be associated to any partition) • Up to 4 groups per partition
Utility outputs	196
User codes	• 500 user codes, with choice of authority levels • 1 code each for Engineer, sub-Engineer and Grand Master
Event log capacity	2000
Wired keypads	32
Wireless keypads	32
Wireless keyfobs / remote controls	256 (1-way, 2-way) including RISCO's Panic keyfob
Proximity key readers	64

Capabilities	Description
Communication channels / modules	• Built-in IP • GSM/GPRS/2G/3G/4G module • Built-in Wi-Fi • STU module (UK) • LRT (Long-range Radio Transmitter) module (Non UK)
Audio Modules	• Voice Module • Listen-In Unit
Expansion capabilities	• Wireless Expander (868MHz) • Wireless Video Expander • Wireless Security Module • Bus Zone Expanders • Zone Expanders (for relay detectors): 16-zone, 8-zone, single-zone • Output Expanders (4 X 3A, 8 X 100mA) • Power Supply Expanders (3A)
Monitoring station	Up to 3 Alarm Receiving Centres (ARC)
Follow-Me	Up to 64 destinations, reporting via SMS, E-mail, or voice
SynopSYS connectivity	Via IP / GPRS/3G/4G
Power input	2.5-4.5A
Power Output Fault	8.3V
Output Voltage Range	11V—13.8V (ripple 200 mV)
Wired sirens	32
Operating temperature	-10°C—55°C (14°F—131°F)
Wireless sirens	32
Automatic program schedules	64
Number of invalid codes before user interface is disabled	After 3 invalid codes

Compliance Statement

Hereby, RISCO Group declares that the LightSYS Plus is designed to comply with:

- EN50131-1
- EN50131-3 Grade 3, Environmental Class II for Housing RP512B and RP432BP3
- EN50131-3 Grade 2, Environmental Class II for Housing RP432BP
- 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 2G/3G/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 Plus IP and GSM communication modules to be in compliance with the information security and substitution security requirements of EN50136.

Alarm Receiving Centre Partnership

For extra security monitoring, LightSYS Plus can be used with up to 2 separate Alarm Receiving Centres. When a system event such as an alarm takes place, the Alarm Receiving Centre is automatically notified. This helps enable rapid around-the-clock resolution in notifying responding agencies (police, fire, medical, etc.) for resolution of a false alarm, or in resetting the system, for example.

The system Engineer configures the Alarm Receiving Centre account(s) to be notified for the specific event types and partitions selected.

Operational Devices & Interfaces for System Users

Device/interface	Description & model numbers
	RisControl Touchscreen Keypad: RP432KPT
	Panda Wired Keypad: RP432KPP2 (with Proximity) RP432KP02 **Panda Wireless:** RW432KPP
	Elegant Keypad: RPKEL (Black)/(White) RPKELP (Black with Proximity)/(White with Proximity)
	Narrow LCD Keypad: RP432KP RP432KPP (with Proximity)
	ProSYS LCD Keypad: ProSYS KCL ProSYS KCLP (with Proximity)
	2-Way Wireless Slim Keypad: RW132KL1 (Outdoor, black) RW132KL1P (Outdoor, black, with Proximity) RW132KL2 (Indoor, white) RW132KL2P (Indoor, white, with Proximity)

Device/interface	Description & model numbers
	Panda 2-Way KeyFob: RW332KF1
	4-Button Rolling-Code Keyfob RWT4RCP (868 MHz, with 2-button Panic feature)
	2-Way 8-Button Remote Control: Agility 132KF2 / 868 MHz)
	Web User Interface
	iRISCO app for Smartphones (both iOS and Android)
	SMS notifications (for mobile phones)

Important Safety Precautions

⚠ **WARNING:** Usage of this product that is not in accordance with the intended use and manufacturer instructions can result in damage, injury or death.

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

⚠ **WARNING:** Do not open the main panel nor service this product yourself. Always call a professional alarm system Engineer for servicing and repair.

⚠ **WARNING:** 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.

⚠ **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 Engineer.

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

Getting Started

This manual describes how to setup and operate your LightSYS Plus system, and contains the following main sections:

- **Initial Setup Tasks for the Grand Master:** The required, initial system setup tasks that are typically performed by the Grand Master – the principal system user
- **Operating the System:** The user operations, such as setting, unsetting, and Omitting zones -- which may vary per user
- **Reference Materials (Appendixes)**

Initial Setup Tasks for the Grand Master

Before operating the system, the Grand Master (chief system user) must perform some initial setup tasks. Below is a list of the Grand Master tasks most commonly performed, shown in a typical order (depending on the system requirements, not all of these tasks may be necessary):

Step 1: Changing the Default Grand Master Code

Step 2: Registering the System to the RISCO Cloud

Step 3: Logging into the RISCO Cloud / Web User Interface

Step 4: Downloading the iRISCO Smartphone App

Step 5: Working with Keypads and User Menus

Step 6: Defining User Codes and Proximity Tags

Step 7: Defining Follow-Me Destinations

Step 8: Defining Keyfobs for Output (Gate) Control

Step 9: Performing a Alarm Receiving Centre Test

Step 10: Performing a Wi-Fi Scan

Step 11: Training System Users

Who Can / Can't Perform the Procedures?

Although this chapter is intended for the Grand Master, some of the procedures can also be performed by the Engineer and other system users – whether at initial setup, or during regular system operation.

In order to show at-a-glance who can/can't perform the procedure, at the start of each procedure the two most common user authority levels (level of permissions) are indicated – **Grand Master** and **User,** as well as the **Engineer/Technician.** Their respective icons are as follows, and if an icon is not listed, it means that person does not have permission to perform the procedure:

- **Grand Master:**
- **User:**
- **Engineer/Technician:**

NOTE: For Engineer/technician-indicated procedures, although they can perform the procedures (locally at the premises or remotely via Configuration Software), the procedures in this manual are specifically for Grand Master and system users.

For a detailed description of all user authority levels and their respective permissions, see *Describing User Authority Levels, page 14*.

Step 1: Changing the Default Grand Master Code

IMPORTANT: The default Grand Master code is **1234,** which can be changed by both the Engineer and Grand Master. After the Engineer is finished installing and programming the system, it is recommended that the Grand Master change this code to be one that is unique, and confidential.

Step 2: Registering the System to the RISCO Cloud

Registering to the RISCO Cloud is a one-time procedure that allows you to use the iRISCO Smartphone app and Web User Interface. This procedure should be performed by the system Engineer, after you supply the Engineer with the required information, such as an e-mail address.

- **To register the system to the RISCO Cloud:**

1. After the RISCO Cloud has been Engineer-enabled during system configuration, go to **www.riscocloud.com**

   NOTE: The Engineer can change the Grand Master Code but cannot see the one programmed.

2. Fill in your first name and last name.
3. Enter your e-mail address as the Login Name (required for 1st-time activation).
4. Define the password (must be: a minimum of eight characters; contain at least one capital letter and one lower case letter; contain at least one number; and contain at least one special symbol) and then confirm.
5. Enter the 15-digit panel ID as it appears on the postcard packaged with the panel or supplied by the Engineer. You can also view it on the keypad (see the procedure below).
6. Complete registration form, and then press **Register.**
7. Open the e-mail received at the email account you had defined as the Login Name in step 3, and then click the link to activate your registration to the Cloud.

- **To register to the iRISCO Smartphone App:**

Download the iRISCO Smartphone app from the Apple App store or the Android Play Store.

Viewing the Panel ID at the Keypad

➢ **To view the main panel ID at the keypad:**

1. Enter your Grand Master or user code, and then press **OK.**
2. Scroll to the **View menu** and then press **OK.**
3. Scroll **Service Info** and then press **OK.**
4. Scroll to **Panel ID** and then press **OK;** the 15 digit panel ID displays.

Step 3: Logging into the RISCO Cloud / Web User Interface

You must log into the RISCO Cloud after registration. In addition, the Grand Master and other system users (according to user authority level) can access and use the Web User Interface, which offers basic and advanced remote operation, control, and management operations for the system. Each time you log in to the Web User Interface, you connect to the RISCO Cloud.

➢ **To log into the RISCO Cloud / Web User Interface:**

1. Go to **www.riscocloud.com**
2. Enter your **username** and **password** (as you defined during the registration process – see *Step 2: Registering the System to the RISCO Cloud, page 10*).
3. Enter the system **PIN code** (user code), and then click **Enter.**

Step 4: Downloading the iRISCO Smartphone App

For system users with Smartphones, the iRISCO Smartphone app can be downloaded from the Apple App store for iOS devices and from the Play Store for Android devices.

Logging into the iRISCO App

Whenever you access the iRISCO app, you typically need to enter your PIN only. However if you manually log out from iRISCO, then to subsequently access it, you must first log into the RISCO Cloud (at the iRISCO Login screen).

Step 5: Working with Keypads and User Menus

Keypad Buttons

Familiarize yourself with the keypad buttons for Grand Master setup tasks as well as the buttons used for the operational procedures performed by system users. Also see the packaged keypad instructions and the respective procedures in this manual.

This describes the main functions of keypad buttons for both Grand Master setup tasks and the operational commands available for all system users. For further details, see the packaged keypad instructions and also the respective procedures in this manual.

Panda Keypad	Elegant Keypad	Narrow Keypad	ProSYS Keypad	Slim Keypad	For Grand Master Setup	For User Operations
Buttons 0—9	**Buttons 0—9**	**Buttons 0—9**	**Buttons 0—9**	**Buttons 0—9**	For entering numeric data/values, for use as quick keys	For user operations and commands
				– –	**EXIT:** Exit a menu, back a step, or return to beginning of a menu	**EXIT:** Exit a menu, back a step, or return to beginning of a menu
				– –	**OMIT:** Omit zones	**OMIT:** Omit zones
				# ?	**OK:** Ok / confirm / save	**OK:** Ok / confirm / save **STATUS:** For Slim only, also status via its LEDs
				– –	**SCROLL:** Scroll through menus & options, also for toggling (such as between ON/OFF)	**SCROLL:** Scroll through menus & options, also for toggling (such as between ON/OFF). **STATUS:** view partition status before setting.
				– –	**SCROLL:** Scroll or toggle backward	**PARTITION STATUS:** Displays the status of the partition to which the keypad is assigned
					TOGGLE: To toggle between options (not applicable for Slim)	**PART SET:** For partial (home/stay) setting
					TOGGLE: To toggle between options (not applicable for Slim)	**FULL SET:** For full setting

Panda Keypad	Elegant Keypad	Narrow Keypad	ProSYS Keypad	Slim Keypad	For Grand Master Setup	For User Operations
					– –	**UNSET:** For unsetting the system
Buttons 4 and 6	**Buttons 4 and 5**	**Buttons 4 and 6**	**Buttons 4 and 5**	**Buttons 3 and 4**	– –	**FIRE ALARM:** To activate a fire alarm
Buttons 7 and 9	**Buttons 7 and 8**	**Buttons 7 and 9**	**Buttons 7 and 8**	**Buttons 5 and 6**	– –	**EMERGENCY:** To activate an emergency alarm
			Buttons 1 and 2	**Buttons 1 and 2**	– –	**PANIC:** To activate a panic alarm
1 = A **2 = B** **3 = C** **5 = D**	**A** **B** **C** **D**	**1 = A** **2 = B** **3 = C** **5 = D**	**A** **B** **C** **D**	– –	**GROUP:** To select group/s for group setting	**GROUP:** To select group/s for group setting

User Menus

From a wired keypad, the Grand Master is the one who typically performs the system setup tasks (the tasks geared for system users) from the user menus. Each menu's configurable options display for the devices connected in the system. User menus are as follows:

Activities	**Follow Me**	**View**	**Codes / Tags**	**Clock**
Event Log	**Maintenance**	**Macro**	**Stand Alone Keyfob**	

NOTE: For a detailed list of all user-programmable settings for all user menus, see *Appendix B: User Menu Maps, page 84*.

Step 6: Defining User Codes and Proximity Tags

Before assigning user codes, it is important to understand the available authority levels (permissions levels) that need to be assigned for each system user.

Describing User Authority Levels

Each user-initiated command or procedure for operating the system requires the system user to have permission to perform it. Various levels of permissions ("user authority levels") are available to assign to each user, which designates which, out of all the system operations, the user can or can't perform. The Grand Master (only one allowed) has the highest level, and is responsible for determining the appropriate user authority level for each other system user, and then communicating it to the Engineer – who in turn programs it in the system. If the Grand Master ever decides to restrict the permissions or grant additional permissions for a user, the Engineer may need to re-program the authority level in the system.

Table of User Authority Levels

This table lists all user authority levels, and describes their respective permissions. The **Grand Master** can perform all of the user operations, while system users with the **User** authority level (the default) can perform most of the common operations.

Authority level	Description of permissions
Grand Master	○ Can perform all operations for all partitions ○ Grand Master code can be changed by the Grand Master or Engineer only ○ Only 1 Grand Master code allowed in the system (has index number **000)**.
Master	Can perform all operations like the Grand Master, except the following: ○ Can only assign and change codes belonging to those with authority levels of Master and below ○ Restricted access to designated partitions ○ No restriction on the amount of Master codes
User	○ Can perform the following for one or more partitions: ▪ Setting and unsetting ▪ Omitting zones ▪ Accessing designated partitions ▪ Viewing system status, fault, and alarm memory ▪ Resetting the switched auxiliary output (e.g. for resetting wired latched devices) ▪ Activating designated utility outputs ▪ Changing one's own code ○ No restriction on the amount of User codes

Authority level	Description of permissions
UnOmit	o All permissions of User level, except without the ability to omit zones
Duress	o Duress is not really an authority level but a special programmable code for all system users – used for activating a "Duress-Unsetting" alarm. Both the Engineer and Grand Master have a role in defining the Duress Unsetting code (see *Creating or Editing the Duress-Unsetting Code, page 17*).
Set Only	o Can only perform setting (for one or more partitions) o Useful for workers who arrive when the premises are already open, but are the last to leave, and thus have the responsibility to close the premises and set the system o Cannot change one's own code o No restriction on the amount of Set Only codes
Maid	o Typically used for cleaners and home attendants who may need to enter the premises at times when the owner is not present o For one-time setting of one or more partitions o A temporary code, it is automatically and immediately deleted from the system as soon as it is used to set (the code will then need to be redefined by the Grand Master) o Cannot change one's own code o If first used to unset the system (for example, to enter the premises), the code may be used once more for subsequent setting
Guard	o Can only unset the system o After entering the code, the system will be unset for the predefined time period. After this period expires, the system is automatically set again. o Cannot change one's own code
UO Control	o Can only operate utility output(s) o Cannot change one's own code

Describing User Codes

In order to perform system operations and commands, all system users must enter their personal user code at the keypad. Up to **500** different codes are available, to be used for the Engineer, sub-Engineer, Grand Master and all other system users.

The Grand Master assigns a unique, numeric user code for each system user from a wired keypad, or via the Web user interface.

IMPORTANT:

- All system users should keep their personal codes confidential, so as to prevent unauthorized system access.
- The Engineer defines the codes for the Engineer and sub-Engineer but can also define the code for the Grand Master – it is therefore recommended that the Grand Master define a new, confidential Grand Master code after system installation (one other than the default, or an Engineer-defined code).

The Grand Master determines a "user authority level" for each system user. There are 9 levels to choose from, each of which has its own set of specific permissions for operating the system. The Engineer in turn programs the user authority level for each system user. See *Table of User Authority Levels, page 14*. The Grand Master can also assign a unique identifying "label" (such as a name) for each system user.

NOTES:

- At the time of installation, the Engineer designates the codes to be either 4 or 6 digits in length. If defined as **6 digits** the length apply for everybody – all users and Engineer/sub-Engineer, however if defined as **4 digits** then the Grand Master, Engineer, and sub-Engineer must have 4-digit codes.
- Other than the Grand Master, some users (according to their authority levels) can change their own codes – see *Table of User Authority Levels, page 14*.
- After the Grand Master enters a code, for reasons of confidentiality, the digits will not be visible, but will display with asterisks (****). The number of asterisks that display represent the code length.
- You can also define user codes with the Web User Interface.

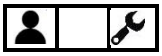
Creating or Editing User Codes

➢ **To create or edit a user code from a wired keypad:**

1. If not known, find out from the Engineer what the code length requirement is for system users.

2. Enter your Grand Master or user code, and then press **OK.**
3. Scroll to the **Codes/Tags** menu**,** and then press **OK.**
4. At **Define** press **OK.**
5. Scroll to one of the available user index numbers (**User 001—499**), or scroll to **Grand Master,** and then press **OK.**
6. At **Edit Code** (for Grand Master) or at **Edit My Code** (for other users), press **OK.**
7. Enter a unique code, and then press **OK;** a single beep with ACCEPTED displaying indicates a successful code designation, while 3 beeps with REJECT CONFLICT displaying, which indicates an unsuccessful code designation.
8. If not defining a label, press **Exit.**
9. **[Grand Master only]:** To define a label (name/description), scroll to **Edit Label** and press **OK.**
10. For instructions on editing a label, see *Creating or Editing Labels, page 19*. When finished, press **OK,** and then repeat the procedure for defining additional user codes.

Creating or Editing the Duress-Unsetting Code



A Duress-Unsetting code is a common code to be used if needed by **all system users** – for the purpose of unsetting the system in an emergency situation only (typically when a user is forced to unset against their will). When activated, the Alarm Receiving Centre is notified, but at the premises there are no visual or audible indications (no alarms will sound).

Both the Engineer and Grand Master have a role in defining the Duress-Unsetting code:

1. Before performing the procedure below for the Grand Master, the Engineer must first designate the **duress** "authority level" to **one** of the available user index numbers, and then inform the Grand Master which user index number it is.
2. The Grand Master then defines the actual numerical code for that user index number (the actual Duress Unsetting code), and then notifies all system users of the code.

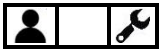
➢ **To create or edit a numerical Duress-Unsetting code:**

1. If not known, find out from the Engineer which **user index number** was assigned the "Duress" authority level, as well as the **code length** requirement.
2. Enter your Grand Master code, and then press **OK.**
3. Scroll to the **Codes/Tags** menu**,** and then press **OK.**
4. At **Define** press **OK.**
5. Scroll to the Engineer-provided user index number (user number) that had been defined with the "Duress" authority level, and then press **OK.**
6. At **Define,** press **OK.**
7. At **Edit Code**, press **OK.**
8. Enter a unique code (cannot be the same as any existing user code) – with the same

length that was Engineer-set for the user codes, and then press **OK;** a single beep with ACCEPTED displaying indicates a successful code designation, while 3 beeps with REJECT CONFLICT displaying indicates an unsuccessful code designation.

9. If not defining a label, press **Exit** (see table in Keypad Buttons, page 12)**.**
10. To define a label (such as "Duress"), scroll to **Edit Label** and press **OK.**
11. See the table below for instructions on editing a label. When finished, press **OK,** and repeat the procedure for defining additional user codes.

Creating or Editing Labels



➢ **To create or edit a label:**

- Using the scroll buttons to move the cursor, at each cursor position enter (or over-write) a character/symbol by pressing the appropriate button (perhaps repeatedly) to cycle through the button's various options, as listed in the table below. Note that after a few seconds the cursor will automatically advance to the next position. Alternatively, at each cursor position, you can use the toggle keys to go forward/backwards through all possible characters (this may take longer).

Button	Respective characters/symbols
1	**1 . , ' ? ! " – ( ) @ / \ : _ + & * # (blank)**
2	**a b c 2 A B C (blank)**
3	**d e f 3 D E F (blank)**
4	**g h i 4 G H I (blank)**
5	**j k l 5 J K L (blank)**
6	**m n o 6 M N O (blank)**
7	**p q r s 7 P Q R S (blank)**
8	**t u v 8 T U V (blank)**
9	**w x y z 9 W X Y Z (blank)**
0	**0 (blank)**
Set and **Part Set** buttons	Used to toggle through all possible symbols and alpha-numeric characters (including upper and lower cases).

Deleting Codes

NOTES:

- The Grand Master can delete the user code for any system user.
- Other system users may be able to delete their own code (per authority level)
- Only the Grand Master can delete a Duress-Unsetting code

➢ **To delete your (or another) code from a wired keypad:**

1. Enter your Grand Master or user code, and then press **OK.**
2. Scroll to the **Codes/Tags** menu**,** and then press **OK.**
3. **[Grand Master only]:** Scroll to **Define**, and then press **OK.**
4. **[Grand Master only]:** Scroll to the user number corresponding to the code you want to delete (or scroll to Grand Master to delete your code), then press **OK.**
5. At **Edit My Code ("Edit Code**" for Grand Master), press **OK.**

6. Enter a single **zero (0)** and then press **OK;** ACCEPTED displays, which indicates the code has been deleted.

Describing Proximity Tags

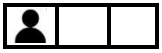
Proximity-enabled RISCO keypads allow using Proximity tags to operate the system (per user authority level – see *Describing User Authority Levels, page 14*). By holding a personal Proximity tag close to the Proximity sensor of any Proximity-supported keypad, it functions the same as entering a personal user code. The system supports up to 500 Proximity tags—maximum one tag per user.

From keypads with Proximity, the Grand Master can define all aspects of Proximity tags, while system users have a separate procedure in which they can only enroll or delete their own personal tags (they cannot define a label).

NOTES:

- For those with user codes already defined, Proximity tags subsequently assigned to them will automatically have the same authority levels as their respective user codes.
- Defining and enrolling Proximity tags can be performed at any keypad except the Slim keypad, however users can operate the system with Proximity tags at any Proximity-compatible keypad – including the Slim keypad.
- For those with the **Maid** authority level**,** they can **only** operate Proximity tags if they already have user codes defined.
- Those with the **User** authority level can only change or delete their own personal Proximity tags, whereas the Grand Master can create and modify Proximity tags for all system users.

Defining and Enrolling Proximity Tags



- **To define and enroll Proximity tags:**

1. Enter your Grand Master code, and then press **OK.**
2. Scroll to the **Codes/Tags** menu**,** and then press **OK**.
3. At **Define** press **OK**.
4. Scroll to the user index number (001—499) for which you will define a Proximity tag – or scroll to **Grand Master** to define your Proximity tag, and then press **OK.**
5. To give a label (name/description), scroll to **Edit Label** and press **OK.** Now define the label (see *Creating or Editing Labels, page 19*).
6. Scroll to **(Re)Write Tag,** and then press **OK.**
7. Within 10 seconds, hold the tag about 2 cm (1 inch) directly above the keypad's built-in Proximity sensor; DEFINED FOR RF ID displays and the keypad sounds a beep, indicating the successful registration of the tag.

   NOTE: If a Proximity tag is already registered to another user, USER TAG ALREADY IN MEMORY displays.

Enrolling My Own Proximity Tag

- **To enroll your own (non-Grand Master) Proximity tag:**

1. Enter your user code, and then press **OK.**
2. Scroll to **Codes/Tags,** and then press **OK.**
3. To enroll your Proximity tag, scroll to **Write My Tag,** and then press **OK.**
4. Within 10 seconds, hold your tag about 2 cm (1 inch) directly above the keypad's built-in Proximity sensor; DEFINED FOR RF ID displays and the keypad sounds a beep, indicating the successful registration of the tag.

   NOTE: If the Proximity tag is already registered to another user, USER TAG ALREADY IN MEMORY displays.

Deleting Proximity Tags

Proximity tags can be deleted by the Grand Master, and also by the system user (his/her tag only).
The Grand Master can delete Proximity tags (including the Grand Master's) by the following methods:

- **By index number**—if the user's index number is known
- **By tag**—if the user's index number is not known

System users (not including Grand Master) can delete their own Proximity tags by a different procedure – see *Deleting My Own Proximity Tag, page 23*.

Deleting a Proximity Tag by its Index Number

➢ **To delete a Proximity tag by its index number:**

1. Enter your Grand Master code, and then press **OK.**
2. Scroll to the **Codes/Tags** menu**,** and then press **OK**.
3. At **Define** press **OK**.
4. Scroll to the user index number (001—499) for which you will delete a Proximity tag – or scroll to **Grand Master** to delete your Proximity tag, and then press **OK**.
5. Scroll to **Delete Tag,** and then press **OK.**
6. At the confirmation prompt, use the Part Set button (see table in Keypad Buttons, page 12) to toggle to **Y** (yes) to delete, or to **N** (no) to cancel the operation, and then press **OK;** the system sounds a beep to confirm the deletion.

Deleting a Proximity Tags by its Tag

- **To delete a Proximity tag by its tag:**

1. Enter your Grand Master code, and then press **OK.**
2. Scroll to the **Codes/Tags** menu**,** and then press **OK**.
3. Scroll to **Delete By Tag,** and then press **OK**.
4. Within 10 seconds, hold the tag about 2 cm (1 inch) directly above the keypad's built-in Proximity sensor; TAG DELETED displays and the keypad sounds a beep, indicating the successful deletion.

   NOTE: If a tag is not registered, if you position it over the keypad's Proximity sensor TAG NOT DEFINED IN MEMORY displays.

Deleting My Own Proximity Tag

- **To delete your own (non-Grand Master) Proximity tag:**

1. Enter your user code, and then press **OK**.
2. Scroll to **Codes/Tags,** and then press **OK**.
3. Scroll to **Delete My Tag,** and then press **OK.**
4. At the "ARE YOU SURE?" prompt, use the Part Set button (see table in Keypad Buttons, page 12) to toggle to **Y** (yes) to delete it, or to **N** (no) to cancel the operation.
5. Press **OK;** if deleted, the keypad beeps and DELETED displays.

Step 7: Defining Follow-Me Destinations

The Grand Master can define up to 64 Follow-Me (FM) destinations ("user-recipients") that will receive notification of system events such as alarm activations:

- **If system is Cloud-connected** (for example if using a Smartphone with the Cloud-connected iRISCO app): a FM user can receive notifications by **E-mail, push-notification, SMS-notification or voice, simultaneously**.
- **If system is not Cloud-connected** (for example if using a mobile phone without the iRISCO app): FM notification is transmitted from the main panel (instead of via the Cloud), and a FM user can receive notification by either **e-mail, SMS,** or **voice message**.

IMPORTANT: Ensure the system Engineer configures the Follow Me notification type(s) for each FM recipient. The Grand Master, in turn, inputs the respective telephone numbers and e-mail addresses.

NOTES:

- FM requires specific modules installed in the system – ask your Engineer.
- The ability to transmit FM notifications are disabled/enabled by the Engineer.

Examples of Follow-Me Notifications

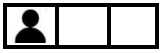
Typical FM notification via SMS:

Security System:
06/03/2022
Intruder Alarm
Partition 1
Entrance

Typical FM notification via e-mail:

Subject: Alarm Security Message: Fire Alarm
System Name: Falafel-Hut Restaurant
Event: Fire alarm, zone 2, kitchen door
Time: 06 January, 2022; 10:12
Partition: Partition 1, first floor
Service Contact: Alarm Receiving Centre 03, 714-5551212

Creating or Editing Follow Me Destinations



➢ **To create or edit a FM destination:**

1. Enter your Grand Master code, and then press **OK.**
2. Scroll to the **Follow Me** menu**,** and then press **OK**.
3. At **Define** press **OK**
4. Scroll to an available FM index number (**01—64**) -- or scroll to an existing FM index number that you want to edit**,** and then press **OK**.
5. To create or edit a label (name/description), scroll to **Label** and press **OK.** Now define the label by entering text and then press **OK** (see *Creating or Editing Labels, page 19*).
6. Scroll to **Destination**, and then press **OK.**
7. Create/edit the FM destination as per the following types and follow the same instructions as in step 5 for creating a label.
   - **[For e-mail notification]:** "EDIT MAIL" will display. Enter an e-mail address. When finished, press **OK.**
   - **[For SMS and voice message notifications]:** "EDIT PHONE" will display. Enter a phone number, including area code, of up to 32 characters in length (including special dialing characters for SMS – see table below). When finished, press **OK.**

   NOTE: To utilize a combination of FM notification types for different users (e-mail, SMS, voice announcement), it must be Engineer-configured.

Special Dialing Characters for Voice Notifications

If required, when defining a telephone number you can include these special dialing characters for SMS, to achieve the functions described:

Special character	Description of function
W	Stops dialing and **w**aits for a new dial tone
,	Waits a fixed period before continuing dialing
#	Sends the # character
*	Sends the ∗ character.
(blank – no character)	Deletes the number/character from the cursor position

Deleting Follow Me Destinations

You can delete existing FM destinations (telephone numbers, e-mail addresses) and labels of FM recipients who are no longer authorized to receive FM notification.

NOTE: During system operation, in the event of a false alarm for example, the Grand Master can terminate Follow-Me notification transmissions to the recipients (see *Terminating Follow-Me Notifications, page 79*).

➢ **To delete a Follow Me destination and label:**

1. Enter your Grand Master code, and then press **OK.**
2. Scroll to the **Follow Me** menu**,** and then press **OK**.
3. At **Define** press **OK**.
4. Scroll to the FM index number to delete**,** and then press **OK**.
5. **[To delete the destination]:**
   a. Scroll to **Destination,** and then press **OK.**
   b. Press and hold down the **Exit** button (see table in Keypad Buttons, page 12). While pressing it, also press **0**.
   c. Press **OK;** the destination (telephone number or E-mail) is deleted.
6. **[To delete the label]:**
   a. Scroll to **Label,** and then press **OK.**
   b. Scroll to each character to delete, and then press **0** to delete it.
   c. Press **OK.**

Testing Follow-Me Destinations

You can test to ensure notifications sent to FM destinations are received. It is recommended to test every FM destination after it is defined. See *Testing Follow-Me Destinations, page 81.*

Step 8: Defining Keyfobs for Output (Gate) Control

Systems equipped with a dedicated wireless expander set to standalone mode can support up to 200 "standalone keyfobs," each of which can be used to activate up to two outputs for gate / parking control. For this purpose, the wireless expander can be used in either "bus mode" (installed inside the main panel enclosure) or in the wireless "standalone mode" configuration, where it is housed in a separate plastic enclosure, outside of the main panel. Each standalone keyfob has a dedicated Engineer-programmable button for each of the 2 possible outputs.

For output control, the standalone keyfobs and wireless expander used are not the same ones used to operate other functions of the system (setting/unsetting, etc.), although the same keyfob/wireless expander models are used for both purposes.

NOTES:

- The following procedures are only for standalone keyfobs (for output control)
- See the packaged wireless expander instructions for standalone usage details

Registering New Keyfobs for Output Control

Each keyfob for output control must be "learned" (registered to the system) by the Grand Master before it can be used.

➢ **To register a keyfob:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Stand Alone KF** (keyfob), and then and press **OK.**
3. Scroll to select the wireless expander ("receiver") that you want to assign the keyfob to and press **OK.**
4. Scroll to **New Keyfob,** and then press **OK.**
5. Press **OK** to start the Learn mode.
6. At the 4-buton keyfob, press for about 3 seconds until the keypad beeps.
7. Back at the keypad, press **OK** to stop Learn mode.
8. Repeat from **step 4** for each additional keyfob.

Changing the Keyfob Buttons for Output Control

[For the 4-button keyfob]: By default the small and large circular/oval buttons are used for controlling the outputs. After registering, either the Grand Master or Engineer can change the functionality of the keyfob buttons so that the buttons with printed "locked" and "unlocked" symbols will be used for output control instead.

[For the 8-button remote control]: Only the Engineer defines the buttons used for output control.

➢ **To change the keyfob buttons used for output control:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Stand Alone KF** (keyfob), and then and press **OK.**
3. Scroll to select the wireless expander ("receiver") that you want to assign the keyfob to and press **OK.**
4. Scroll to **UO Buttons**, and then press **OK;** ARE YOU SURE? displays.
5. Toggle to **Y** (yes), or to cancel the operation toggle to **N** (no), and then press **OK;** the keypad sounds a confirmation beep.

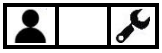
Deleting the Registration for a Single Output Control Keyfob

The Grand Master must delete the registrations for all output control keyfobs/remote controls that are no longer used, to prevent unauthorized usage.

➢ **To delete a keyfob/remote control registration:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Stand Alone KF** (keyfob), and then and press **OK.**
3. Scroll to select the specific wireless expander ("receiver") that the keyfob is assigned to, and then press **OK.**
4. Scroll to **Delete Keyfob,** and then press **OK.**
5. Press **OK** to start Erase mode (registration deletion mode).
6. At the keyfob, do the following:
   - **[4-button keyfobs]:** Press for about 3 seconds until the keypad beeps.
   - **[8-button remote controls]:** Press and simultaneously for about 3 seconds until the keypad beeps.
7. Back at the keypad, press **OK** to stop Erase mode.

Deleting Registrations for all Output Control Keyfobs



The Grand Master can delete the registrations for all output control keyfobs/remote controls at the same time.

- **To delete registrations for all keyfobs/remote controls:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Stand Alone KF** (keyfob), and then and press **OK.**
3. Scroll to select the specific wireless expander ("receiver") that the output control keyfobs are assigned to, and then press **OK.**
4. Scroll to **Delete All,** and then press **OK;** ARE YOU SURE? displays.
5. Toggle to **Y** (yes), or to cancel the operation toggle to **N** (no), and then press **OK;** the keypad sounds a confirmation beep.

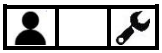
Step 9: Performing an Alarm Receiving Centre Test

This procedure sends a test message to the Alarm Receiving Centre, according to requirements for EN50131 standards**.**

- **To perform an ARC test:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Advanced**, and then press **OK.**
4. Scroll to **ARC Test,** and then press **OK;** DONE HIT ANY KEY displays and a confirmation beep sounds, indicating the test message was sent.
5. Press any key to exit the test mode.

Step 10: Performing a Wi-Fi Scan



This procedure displays the available networks to connect to**.**

- **To perform a Wi-Fi Scan:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Wi-Fi**, and then press **OK.**

4. Scroll to **Wi-Fi Scan,** and then press **OK;** from the available networks that appear, scroll to your Router's Wi-Fi network and then select the desired network.
5. Press [enter].

Step 11: Training System Users

Typically performed by the Grand Master, all system users must be educated and trained in the operational and security aspects of the system, including, for example:

- Responsibility to safeguard portable user devices (keyfobs, remote controls) and the confidentiality of user codes
- All operational procedures – those performed at the premises and remotely (such as obtaining system status, and usage of iRISCO, Web User Interface, SMS, and remote telephone operation)
- Policy for responding to actual alarms (for example intrusion or emergency)
- Activating emergency alarms, including Duress Unsetting
- Follow-Me notification (and cancellation of FM for false alarms)
- Usage of Listen-In & Speak communication
- Silencing an alarm after a false alarm
- Engineer/technician and Alarm Receiving Centre contact information – for example, if an Engineer/technician-assisted system reset is required after alarm activation

Operating the System

This chapter contains all the operational procedures available for system users.

Modes of Operation

The system can be operated by authorized users either remotely or locally (at the premises).

Remote Operational Modes

- **Smartphones via the iRISCO app** (see the app for instructions)
- **Computer browsers via the Web User Interface** (see the website for instructions)
- **Cellphones via SMS**

Local Operational Modes

- **Keypads**
- **Remote controls and keyfobs**
- **One-way or two-way "Listen-In & Speak" communication** between user at premises and Alarm Receiving Centre

Receiving and Acknowledging a Follow-Me Status Call

➢ **To acknowledge you received a system-generated Follow-Me status call:**

1. When the telephone rings, answer and verify if the call is system-generated (if so, nobody will be on the line and you'll hear a system-generated voice announcement for an event occurrence at the premises).
2. Press **#.**
3. Select options from the following **Acknowledgement Menu** and if necessary, from the subsequent **Operations Menu** for performing system operations:

Acknowledgement Menu

For this:	Press this:
Acknowledge you received the event message and allow the system to dial the next Follow-Me number.	**1**
Acknowledge you received the event message, and then stop the system from dialing other Follow-Me numbers.	**2 ➢ Grand Master code ➢ #**
Acknowledge you received the event message, and then access the Operations Menu (see *Operations Menu*, below)	**3 ➢ user code ➢ #**
Use "Listen-In and Talk" for 2-way communication	**6 ➢ 3 ➢user code**

Repeat the event message	#
Return to the Acknowledgement menu	*

Operations Menu

For this:	Press this:
Set all partitions	**1 ➢ 1**
Set by partition (set selected partition)	**1 ➢ 9 ➢ partition number**
Unset all partition	**2 ➢ 2**
Unset by partition (unset selected partition)	**2 ➢ 9 ➢ partition number**
Change zone omit (un-omit a zone)	**3 ➢ zone number ➢ # ➢ 9**
Operate utility output(s)	**4 ➢UO number**
Change Follow-Me telephone numbers	**5 ➢ FM number ➢ # ➢ 2 ➢ new phone number ➢ # ➢ 1**
Listen-in to premises only (Listen-In and Talk feature)	**6 ➢ 1**
Talk to premises only (Listen-in and Talk feature)	**6, ➢2**
Listen and talk to-and-from premises (Listen-In and Talk feature)	**6 ➢ 3**
Record messages	**7**
Exit the system	**0**
Repeat the menu options	#
Return to the previous menu	*

Operating Remotely by SMS

You can operate the system remotely by sending SMS commands.

NOTES:

- To utilize SMS a GSM module must be installed – ask your Engineer.
- Commands entered are not case sensitive (upper and/or lower case are ok).
- A separator between command words may be used, or not used.
- To receive an acknowledgement reply (an "operation confirmed" or "operation failed" message), add **RP** to the end of a command (for example 1234 S RP). This can be used for: **setting, unsetting, omitting, activating output, changing Follow-Me definition**.

SMS Commands

Command name:	Enter this:
Full set	code + S (Example: 1234S)
Part set	code + P
Group set	code + G + select group A--D
Full unset	code + S
Partition full set	code + S + partition number
Partition partial set	code + P + partition number
Partition unset	code + US + partition number
Get system status	code + ST
Omit zone	code + OM + zone number
Un-omit zone	code + UNOM + zone number
View last alarm	code + AL
Change FM number	code + FMPHONE + FM serial number + NEW + new phone number
Activate output	code + POON + PO number
Deactivate output	code + POOFF + PO number
Get SIM credit level	code + CR

Operating the Listen-In & Speak Unit

The Listen-In & Speak Unit is an audio accessory that provides 2-way “listen-in" and/or "talk” communication to and from the premises (such as between a system user at the site and the Alarm Receiving Centre). The Listen-In & Speak Unit is also used to broadcast status in the form of voice announcements (for system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only – see *Voice Announcements, page 87*). Multiple Listen-In & Speak units can be used in the system.

- For operational usage, see the relevant entries in the *Acknowledgement Menu, page 31* and the *Operations Menu, page 32*.

Operating Locally by Keypads, Remote Controls/Keyfobs, and Proximity

Working with Keypads

For a description of keypad buttons used for user operations, see *Step 5: Working with Keypads and User Menus, page 12*.

Keypad Display Options

Using the "Multi View" Keypad Display

[For wired keypad models with LCD displays]: The keypad displays each partition number, with date, and time. If Engineer-defined, a letter can also display to indicate the partition’s status, as follows:

Letter	Partition Status
A	Partition is fully set
S	Partition is partially set
N	Partition is not ready for setting
R	Partition is ready for setting
L	Partition is in an alarm state

Using the "Blank" Keypad Display

[For wired keypad models with LCD displays]: If Engineer-defined, two minutes after the last keypad operation the keypad display will appear blank, other than the text "ENTER CODE." This feature prevents the system status from displaying for unintended viewers – for example, from keypads that are located outside the premises. Any user can view status as needed on a "blank display" keypad by entering their code.

NOTE: When in blank display mode, the "Ready" indicator will still indicate faults in the system.

➢ **To view status on a "blank display" keypad:**

- Enter your Grand Master or user code (or place Proximity tag), and then press **OK;** the status will display at the keypad.

  NOTE: To enable viewing status on the keypad at all times, the Engineer must disable the Blank Display mode for the keypad.

Obtaining System Information

System information/status can be requested and received from keypads and remote controls. As well, system information can be obtained via the iRISCO app and the Web user interface.

Depending on your system configuration, system information/status types received can be visual **(viewed)** or audible **(sound):**

- **Viewed indicators:** keypad text and indicators, keypad and remote control LEDs, iRISCO and Web User Interface texts
- **Sound indicators:** "beeps" and "squawks" from keypads and sirens respectively, or "voice announcements" heard when operating the system when broadcast from Listen-In & Speak units – for system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only.

NOTES:

- For a description of all viewed indications, see *Viewed Indicators, page 87*.
- For a description of all sound indications, see *Sound Indicators, page 85*.

Information requested from:	Types of information that can be received:
Narrow, Panda and Elegant keypads	• Keypad display indicators (icons and/or text) • Keypad beeps (setting/unsetting, entry/exit countdown) • Single sounder "squawk" for setting confirmation only • Voice announcements broadcast from the Listen-In & Speak unit (for system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only)
Slim keypad	• Keypad's LEDs • Keypad beeps (setting/unsetting, entry/exit countdown) • Voice announcements broadcast from the Listen-In & Speak unit (for system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only) • Single sounder "squawk" for setting confirmation only
8-button remote control	• Remote control's LEDs and beeps • Single sounder "squawk" for setting confirmation only
4-button Panda keyfob	• Remote control's LEDs • Single sounder "squawk" for setting confirmation only
4-button keyfob	• Single sounder "squawk" for setting confirmation only

Obtaining System Status – Requested from Remote Controls

When requested from an 8-button remote control, you can get system status via the remote control's LED indicators, and via "beeps" and "squawks" from the remote control and sounder respectively (see *"Beep" and "Squawk" Sound Indicators, page 85*).

Remote Control	Procedure:	Status indications received:
2-Way, 8-button	**Sound status indication:** • **Quick mode:** Press 4|? for 2 seconds • **High Security mode:** Press 4|? for 2 seconds ➤ press **PIN code**	• Beep indication from the remote control • Confirmation squawk from sounder See *"Beep" and "Squawk" Sound Indicators, page 85*.
	LED status indication: • Press * ➤ 4|?	See *8-Button Remote Control Indicators, page 89*.
2-Way, 4-button	**Sound status indication:** • **Quick mode:** Press 4|? for 2 seconds • **High Security mode:** Press 4|? for 2 seconds ➤ press **PIN code**	• Beep indication from the remote control • Confirmation squawk from sounder See *"Beep" and "Squawk" Sound Indicators, page 85*.
	LED status indication: • Press * ➤ 4|?	See4-Button Panda Keyfob Indicators, *page 89*.

Obtaining System Status – Requested from Keypads

When requested from a keypad, you can get **both audible and visual system status** – viewed via the keypad's display (or via the Slim keypad's LED indicators), and heard via keypad "beeps" and sounder "squawks" (see *"Beep" and "Squawk" Sound Indicators, page 85*). You can also hear "voice announcements" broadcast from a Listen-In & Speak unit for system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only. See *Voice Announcements, page 87*.

Keypad	Procedure:	Status indications received:
Panda	Press scroll keys	Partition status (R=ready/NR=not ready).
Elegant	Press scroll keys △	Partition status (R=ready/NR=not ready).
Slim	• **Quick mode:** Press #? for 2 seconds • **High Security mo**de: Press #? for 2 seconds ➢ enter **code** or use **Proximity tag**	• LED indications from the keypad **(**see *Slim Keypad Indicators, page 87*) • Sound (beeps) from keypad (*see "Beep" and "Squawk" Sound Indicators, page 85*).
Narrow	Press scroll keys	Partition status (R=ready, NR=not ready).
ProSYS	Press scroll keys	Partition status (R=ready, NR=not ready).

Obtaining System Information – Requested from, and Viewed at Keypads

The following system information is **viewed only** – on keypad displays (not relevant for the Slim keypad):

- **Event Log**
- **Alarm Memory**
- **System Faults**
- **Zone Status**
- **Partition Status**
- **IP Address**

NOTE: For Slim keypads, see *Slim Keypad Indicators, page 87* for a description of the system information provided by the keypad's LED indicators.

Viewing the Event Log

View all types of system events, are stored in chronological order. The event log holds up to 2000 events.

NOTE: The event memory cannot be completely erased. When the event log exceeds the maximum (2000) events, the oldest events will be over-written by the newest events.

➢ **To view the event log:**

1. At the keypad, enter your Grand Master code, and then press **OK**.
2. Scroll to **Event Log,** and then press **OK.**
3. Scroll through the various events to view their description and time/date of occurrence.

   NOTE: Use the Part Set (toggle) button (see table in Keypad Buttons, page 12) to skip 100 events, either forwards or backwards.

Viewing Alarm Memory

View the 5 most recent alarms stored in the system memory.

➢ **To view the 5 most recent alarms:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Alarm Memory** and then press **OK.**
4. Scroll to view the alarms.

Viewing System Faults

A flashing power icon (⏻) on the keypad indicates there are current faults in the system that you can view.

➢ **To view all system faults:**

1. At the keypad, enter your Grand Master or user code, and then press **OK.**
2. Scroll, to **View** and then press **OK.**
3. Scroll to **Fault** and then press **OK.**
4. Scroll to view current faults found in the system.

Viewing Zone Status

View the status of all zones in the system.

➢ **To view zone status:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll**,** to **View** and then press **OK.**
3. Scroll to **Zone Status** and then press **OK.**
4. Scroll through the zones to view their current status.

Viewing Partition Status

View the status for individual partition(s) or all partitions to which the keypad is assigned (according to your user authority level).

➢ **To view partition status for the keypad-assigned partition:**

1. At the keypad, press the **scroll** button to view all status information for the first block of partitions (partitions 1—10), such as **R** (ready to set) or **NR** (not ready to set).
2. Press **scroll** again to view the status for the next block of partitions –you can repeat this to view the status of all partitions (32 maximum).

➢ **To view partition status for all partitions:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Part. Status** and then press **OK.**
4. While scrolling through the partitions, for each you can view its status, such as **R** (ready to set) or **NR** (not ready to set).

Viewing IP Address

View the IP address of the system.

➢ **To view the IP address:**

1. At the keypad, enter your Grand Master code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **View IP Address** and then press **OK;** the IP address displays.

Viewing Service Information

View the following types of service information (per user authority level):

- **Engineer/technician information**
- **System Version**
- **Serial Number**
- **Panel ID**

Engineer Information

- **To view Engineer/technician information:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Service Information** and then press **OK.**
4. Scroll to **Engineer** and then press **OK,** Engineer-input information displays.

System Version

- **To view the system software version**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Service Information** and then press **OK.**
4. Scroll to **System Version**, then press **OK;** the system software version displays.

Serial Number

- **To view the main panel serial number:**

1. At the keypad enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Service Information** and then press **OK.**
4. Scroll to **Serial Number** and then press **OK,** the main panel's 11-digit serial number displays.

Panel ID

- **To view the main panel ID number:**

1. At the keypad enter your Grand Master or user code, and then press **OK**.
2. Scroll to **View** and then press **OK.**
3. Scroll to **Service Information** and then press **OK.**
4. Scroll to **Panel ID** and then press **OK,** the panel's 15-digit ID number displays.

Omitting Zones

If Engineer-enabled, you can set a partition – even if a zone within that partition is not secured – by **manually** Omitting that zone.

If not omitted, when a zone is not secured, or "open" (OP) for whatever reason, by default it will be in a "not-ready" (NR) state, meaning the system is not ready to be set, and the keypad's "ready" indicator will not display.

Typical reasons for Omitting a zone are, for example, to set the system while allowing access a zone in an otherwise protected area, or to set the system while temporarily circumventing the setting of a specific zone.

NOTE: If Engineer-configured, you can "force set" which **automatically** omits specific zone(s) upon setting. See ***Error! Reference source not found.***, *page* ***Error! Bookmark not defined.***.

CAUTION: Zone Omitting, whether manual or automatic, may compromise the level of protection the system can offer.

Viewing Not-Ready Zones

Before considering whether to omit zones, first view the non-secured/not-ready zones in the system.

NOTE: Users can only view the "not-ready" zones that they are allowed to operate, according to their user authority level (see *Describing User Authority Levels, page 14)*.

- **To view not-ready zones:**

1. At the keypad, enter your Grand Master or user code, and then press **OK.**
2. Scroll, to **View** and then press **OK.**
3. Scroll to **Zone Status,** and then press **OK.**
4. Scroll to view the zones, which will display as READY or NOT READY.

Defining Zone Omit Status

If Engineer-configured, you can perform either the following procedure to omit zones, or the quick procedure for one-time-only Omitting (see *Quickly Omitting/Un-Omitting Zones on a One-Time Basis, page 44*).

➢ **To define a zone's omit status:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. Scroll to **Activities** and then press **OK.**
3. At **Omit** press **OK.**
4. At **Zones** press **OK.**
5. Scroll to select from the following omit options:
   - **One Time Only:** Omits the selected zone once only – at the next system setting (the zones will then not be omitted at subsequent settings)
   - **Permanent Omit:** Omits the selected zone on a continual basis, upon each system setting
   - **Omit Reset:** Un-omits (removes the omit) for all zones
   - **Omit Recall:** Reverts to the most recent zone-omit state (if a Omit Reset was recently performed)
6. Perform the following additional steps in the table below, according to the option you select:

   NOTES:

   - The default for all zones is **N** (not omitted)
   - If a zone is omitted, the full setting indicator does not display on the keypad when in full setting mode

Omit Option	Procedure:
One-Time-Only	a. At the One-Time-Only option, press **OK**. b. Scroll through the zones to one for which you want to change its omit status. c. Toggle to either **Y** (to omit) or **N** (to un-omit), and then press **OK.**
Permanent Omit	a. At the Permanent Omit option, press **OK.** b. Scroll through the zones to one for which you want to permanently omit. c. Toggle to either **Y** (to omit) or **N** (to un-omit), and then press **OK**.
Omit Reset	a. At the Omit Reset option, press **OK.** b. Press **OK** again to confirm; the keypad beeps, indicating that all zones have been reset to a not-omitted (default) state.
Omit Recall	a. At the Omit Recall option, press **OK,** then press **OK** again to confirm. b. Scroll through the zones to view that previously un-omitted zones are again omitted. You can also toggle to **N** at any zone to cancel its omit state. c. Press **OK;** the keypad beeps, indicating the successful operation.

Quickly Omitting/Un-Omitting Zones on a One-Time Basis

If Engineer-configured, you can quickly access the "**one-time-only**" omit option (see table above). This may be useful, for example, if you want to omit zone(s) on a one-time basis, or if you have previously permanently omitted zone(s) and you want to un-omit them on a one-time basis.

- **To perform a quick "one-time-only" Omitting/un-Omitting of zones:**

1. At the keypad, enter your Grand Master or user code **(don't** enter OK after).
2. Press a **scroll** key; you will be prompted to omit the first zone (zone 1).
3. Scroll to the zone you want to omit, and then toggle using the Part Set button to either **Y** to omit or **N** to un-omit.
4. Scroll to additional zone(s) as needed and repeat step 3 for each.
5. When finished, press **OK.**

Setting & Unsetting the System

System setting protects the premises by triggering alarms and sending notifications upon detection from any installed detector. System users can set/unset the system according to their user authority level.

Setting/Unsetting Modes

LightSYS Plus offers the following modes of setting/unsetting the system:

Setting Modes
✓ **Full setting**
✓ **Part setting**
✓ **Partition setting**
✓ **Group setting**
✓ **Automatic setting and unsetting**
✓ **Setting with system faults**
✓ **Forced setting (setting with automatically- omitted zones)**
✓ **Omitting zones (setting with manually omitted zones)**
✓ **Keyswitch setting**
✓ **Forced keyswitch or Proximity setting**
✓ **Low-battery setting**
✓ **Strobe setting**
Unsetting Modes
✓ **Unsetting all partitions**
✓ **Unsetting an individual partition**
✓ **Duress unsetting**
✓ **Unsetting with alarm activation (silencing an alarm)**

Before Setting the System

IMPORTANT: Before setting the system, do the following:

- ✓ **Ensure the premises have been vacated.** Note that the **entry/exit delay** provides a specific period of time to exit the premises before alarms are activated.
- ✓ **Observe the system's status indicators, faults, and READY status:**
  - **Check status indicators** – View icon indicators on keypad displays, or LED indicators on Slim keypads and remote controls. Also listen to any audible system status (beeps/squawks, or voice announcements). See *Appendix C: System Indicators, page 85*.

- **Check that all zones are ready to be set (no open zones)** –view the READY indicator on the keypad (see *Keypad Indicators, page 87)*
- **Check for system faults.** It is good practice to scroll through and view all faults, whether or not your system is configured to require viewing them before setting**.**

CAUTION: Depending on the system configuration, you may be able to set the system while omitting all (or specific) open zones, and/or set while overriding system faults, however, depending on the circumstances these arrangements may compromise the level of protection that the system offers.

Setting Procedures

- For setting/unsetting via SMS, see *Operating Remotely by SMS, page 33*
- For setting/unsetting via iRISCO and Web User Interface, see the respective applications.

Full Setting

Full setting requires that all of the premises be vacated.

➢ **To fully set the system:**

1. Verify that the premises are vacated, and that the system is ready to be set (view the READY indicator).
2. If not ready to set, secure (or omit) any open zones s*ee Omitting Zones (Setting with Manually-Omitted Zones), page 55* and also ***Error! Reference source not found.****, page* ***Error! Bookmark not defined.***.
3. If unable to set, scroll to view system fault messages, and resolve accordingly. If Engineer-defined, you can set while overriding all current faults (see *Setting with System Faults, page 55*).
4. Perform the following setting procedure in the table below.

   NOTES:

   - If you enter your code incorrectly, three short beeps will sound. Re-enter the code.
   - Keyfob and remote control buttons can have different functions and are Engineer-defined.
   - Proximity setting is Engineer-defined and can vary per system user.

Device	Full-Setting procedure:
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢ press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢ press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢ press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢ press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press . ❖ **High security mode:** Press ➢ enter **code** ❖ **Proximity mode:** Press ➢ place **Proximity tag** **NOTE:** If needed, press * to "wake-up" the Slim keypad
	❖ **Quick mode:** Press .
	❖ **Quick mode:** Press . ❖ **High Security mode:** Press ➢ enter **PIN code** (not user code)
	Press

5. Leave the premises before the end of the exit delay period. During the exit delay period, you can observe the following indicators at the keypad:

   - The keypad beeps slowly and repeatedly, followed by faster beeps at end of exit delay time period
   - The exit-delay countdown appears on the keypad display, and the full set icon flashes. On the Narrow keypad the red LED is flashing.

   NOTE: You can press the current keypad's **Exit** button during the exit delay time period to silence the beeps (other keypads in the system will still beep).

6. At the end of the exit delay time period, the **Full-Set** icon appears without blinking and SET displays. On the Narrow keypad, the red LED is lit without flashing.

Part Setting

Part setting allows the non-set areas of the premises to be inhabited.

➢ **To partially set the system:**

1. Verify that the system is ready to be set (view the READY indicator).
2. If not ready to set, secure (or omit) any open zones s*ee Omitting Zones (Setting with Manually-Omitted Zones), page 55* and also ***Error! Reference source not found.***, *page* ***Error! Bookmark not defined.***.
3. If unable to set, scroll to view system fault messages, and resolve accordingly. If Engineer-defined, you can set while overriding all current faults (see *Setting with System Faults, page 55*).
4. Perform the following setting procedure in the table below.

   NOTES:

   - If you enter your code incorrectly, three short beeps will sound. Re-enter the code.
   - Keyfob and remote control buttons can have different functions and are Engineer-defined.
   - Proximity setting is Engineer-defined and can vary per system user.

Device	Part-Setting procedure:
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢ press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick Set mode:** Press ❖ **High Security mode:** Enter **code** ➢press ❖ **Proximity mode:** Place **Proximity tag**
	❖ **Quick mode:** Press ❖ **High security mode:** Press ➢ enter **code** ❖ **Proximity mode:** Press ➢ place **Proximity tag** **NOTE:** If needed, press * to "wake-up" the Slim keypad
	❖ **Quick mode:** Press .
	❖ **Quick mode:** Press . ❖ **High Security mode:** Press ➢ enter **PIN code** (not user code)
	Press

5. Leave the premises before the end of the exit delay period. During the exit delay period, you can observe the following indicators at the keypad:
   - The keypad beeps slowly and repeatedly, followed by faster beeps at end of exit delay time period
   - The exit-delay countdown appears on the keypad display, and the full set icon flashes. On the Narrow keypad the red LED is flashing.

NOTE: You can press the current keypad's **Exit** button during the exit delay time period to silence the beeps (other keypads in the system will still beep).

6. At the end of the exit delay time period, the **Part-Set** and **Full Set** icons both appear without blinking, and AT HOME SET displays. On the Narrow keypad, the red LED is lit without flashing.

Partition Setting

Each partition in the system (32 maximum) is a separate entity, whereas it can be independently set/unset (fully or partially) by those users with the appropriate authority level – regardless of the state of the other partitions in the system.

Each zone (detector) of any type – whether a bus zone, hard-wired zone or wireless zone – is associated with (assignable to) one or more partitions.

A partitioned system may have one or more **common zones** ("shared zones") **–** for example, a common front door with a contact detector that is used by multiple offices.

NOTES:

- A common zone is **set** only if **all partitions** to which the zone is associated are set (may be set differently, depending on the Engineer's configuration).
- A common zone is **unset** if **any of the partitions** to which the zone is associated are unset (may be unset differently, depending on the Engineer's configuration).

The Grand Master has access to all partitions and can use any keypad to access any partition. Other users can use only designated keypads for the partitions they are authorized to access, according to user authorization level and configuration.

You can set either ALL partitions (with full-setting or partial-setting for each partition's zone/s) or set 1 INDIVIDUAL partition at a time (with full-setting or partial setting for that partition's zone/s).

Setting All Partitions

Set all partitions at the same time, as either fully-set or partially-set.

➢ **To set all partitions:**

1. Verify that the areas of the premises to be set are vacated, and that the system is ready to be set (view the READY indicator).
2. If not ready to set, secure (or omit) any open zones, s*ee Omitting Zones (Setting with Manually-Omitted Zones), page 55* and also ***Error! Reference source not found.***, *page* ***Error! Bookmark not defined.***.
3. If unable to set, scroll to view system fault messages, and resolve accordingly. If Engineer-defined, you can set while overriding all current faults (see *Setting with System Faults, page 55*).
4. Perform the following setting procedure for **ALL** partitions as either fully-set or partially-set:

For this:	Do this to set ALL partitions:
	❖ **Fully-set-all partitions:** Enter **code** ➢press **full set button** ➢If only 1 partition, it is now fully-set. For all partitions, at the All? prompt press **full set button**. ❖ **Partly-set all partitions:** Enter **code** ➢press **partial set button** ➢ If there is only 1 partition, it's now partially-set. For all partitions, at the All? prompt press **partial set button**. ❖ **Fully or partially set all partitions with Proximity:** Place tag at keypad ➢ at "All?" prompt press either **full set button** or **partial set button**. **NOTE:** The number of partitions (32 maximum) that can be set using a Proximity tag is Engineer-configured per user.
	❖ **Quick mode:** Press (full-set) or (partial-set). ❖ **High security mode:** Press (full-set) or (partial-set).➢ enter **code** ❖ **Proximity setting:** Press (full-set) or (partial-set) ➢ place tag at keypad **NOTE:** The number of partitions (32 maximum) that can be set using a Proximity tag is Engineer-configured per user.

For this:	Do this to set ALL partitions:
	❖ **Quick mode:** Press
	❖ **Quick mode:** Press ❖ **High security mode:** Press ➢ enter **code** **NOTE:** You can select only a single partition 1, 2 or 3, even if you have access to more partitions.

Setting an Individual Partition

Set an individual partition, as either fully-set or partially-set. For multiple partitions, repeat this procedure as needed.

➢ **To set an individual partition:**

1. Verify that the areas of the premises to be set are vacated, and that the system is ready to be set (view the READY indicator).
2. If not ready to set, secure (or omit) any open zones, s*ee Omitting Zones (Setting with Manually-Omitted Zones), page 55* and also ***Error! Reference source not found.**, page **Error! Bookmark not defined.***.
3. If unable to set, scroll to view system fault messages, and resolve accordingly. If Engineer-defined, you can set while overriding all current faults (see *Setting with System Faults, page 55*).
4. Perform the following setting procedure for **1 INDIVIDUAL** partition, as either fully-set or partially-set.
5. Repeat the following procedure for each additional individual partition to set:

For this:	Do this to set an INDIVIDUAL partition:
   	❖ **Fully-set an individual partition:** Enter **code** ➢press **full set button** ➢ enter the 2-digit partition number (example 03) ➢press **full set button**. ❖ **Partly-set an individual partition:** Enter **code** ➢press **partial set button** ➢ enter the 2-digit partition number (example 03) ➢press **partial set button**. ❖ **Fully or partially set 1 partition with Proximity:** Place tag at keypad ➢ at "All?" prompt scroll to the partition to set ➢press either **full set button** or **partial set button**. **NOTE:** The number of partitions (32 maximum) that can be set using a

For this:	Do this to set an INDIVIDUAL partition:
	Proximity tag is Engineer-configured per user.
	❖ **Quick mode:** Press partition number (**1—3**) ➢ press (full-set) or (partial-set). ❖ **High security mode:** Press partition number (**1—3**) ➢ press (full-set) or (partial-set). ➢ enter **code** ❖ **Proximity setting:** Press partition number (**1—3**) ➢ press (full-set) or (partial-set) ➢ place tag at keypad **NOTES:** • The number of partitions (32 maximum) that can be set using a Proximity tag is Engineer-configured per user. • You can select only partition **1, 2** or **3** to unset only that specific partition. Other partitions cannot be separately unset from the keypad.
	❖ **Quick mode:** Press button **1, 2,** or **3** for partition number ➢ press (full-set) or (partial-set). ❖ **High Security mode:** Press button **1, 2,** or **3** for partition number ➢ press (full-set) or (partial-set) ➢ enter **PIN code.** **NOTES:** • The 8-button remote control can set up to 32 partitions • You can select only partition **1, 2** or **3** to unset only that specific partition. Other partitions cannot be separately unset from the keyfob.

Group Setting

In each partition the zones are assignable to up to 4 **groups,** enabling 4 levels of partial-setting in each partition. Group setting can be performed at the following keypads:

- **Narrow keypad**
- **ProSYS Keypad**
- **Elegant keypad**
- **Panda keypad**

NOTE: Group setting can require entering the user code or it can be Engineer-configured to be "quick set" (not requiring a user code).

➢ **To set a group:**

1. Verify that the areas of the premises to be set are vacated, and that the system is ready to be set (view the READY indicator).
2. If not ready to set, secure (or omit) any open zones, see *Omitting Zones (Setting with Manually-Omitted Zones), page 55* and also ***Error! Reference source not found.**, page **Error! Bookmark not defined.***.
3. If unable to set, scroll to view system fault messages, and resolve accordingly. If Engineer-defined, you can set while overriding all current faults (see *Setting with System Faults, page 55*).
4. Enter your **code** (unless Engineer-configured to not require it), then perform the following procedure:

For this:	Do this to GROUP set:
	❖ **If user has permission for 1 partition:** Press the group to set (**A, B, C,** or **D)** key for 2 seconds. To set another group for this single partition, repeat this procedure. ❖ **If user has permission for multiple partitions:** Enter Code: Press the group to set (**A, B, C,** or **D)** for 2 seconds ➢ enter the partition number (example 03) ➢ press the group again for 2 seconds. To set another group for this or another partition, repeat this procedure. **NOTE:** If configured for **quick setting**, press the group letter button for 2 seconds corresponding to the group(s) you want to set; the selected groups are set.

Automatic Setting and Unsetting

You can have the system set and unset automatically for re-occurring weekly schedules, one-time schedules, and holiday schedules (see *Defining Automatically-Operated UOs and Setting Operations, page 69*).

Setting with System Faults

If Engineer-configured, you can set the system while overriding all current faults, provided you first view and confirm all the faults.

CAUTION: Depending on the type of faults, setting while overriding faults may compromise the level of protection the system can offer.

➢ **To set the system while overriding faults:**

1. If you do not succeed to set, use the scroll buttons to view all the system faults; after viewing them all, OVERRIDE FAULT? will appear.
2. Toggle to the **Y** (yes) option to override them all, or toggle to **N** (no) to cancel the override request.
3. Press **OK.**

Omitting Zones (Setting with Manually-Omitted Zones)

See *Defining Zone Omit Status, page 43* and *Quickly Omitting/Un-Omitting Zones on a One-Time Basis, page 44*.

Keyswitch Setting

If the system is equipped with a keyswitch, perform set and unset operations by "toggling" through the respective modes.

Forced Keyswitch or Proximity Setting

When using a keyswitch or Proximity you can force-set any partition that has one or more open zones (these zones will be automatically omitted upon setting). See ***Error! Reference s ource not found.***, *page* ***Error! Bookmark not defined.***.

Low-Battery Setting

If Engineer-configured, low battery setting enables setting the system when a low battery condition is detected in the main panel backup battery, or in a power supply expansion module battery.

Strobe Setting

If Engineer-configured, strobe setting enables the internal or external strobe (upon automatic activation by a UO) to provide a 10-second strobe confirmation after setting.

Unsetting Procedures

Unsetting deactivates all zones/detectors in the partitions, so they don't trigger alarms. Unsetting also resets the system to normal operation, unless the system is configured to require the intervention of a technician/Engineer for performing a system reset (see Restoring the System upon Power *Supply Overload.*

Resetting the System with Engineer Intervention, *page 60).*

When unsetting at keypads, for security purposes all users are always required to input their user codes. When unsetting at remote controls and keyfobs, a built-in "rolling code" feature provides extra security without the need for the user code, although a unique PIN code may be used with an 8-button remote control.

Unsetting All Partitions

You can unset all fully-set or partly-set partitions at the same time (per your user authority level – **"all" refers to the maximum partitions a user's authority level enables him/her to operate)** – which may not necessarily be all the partitions in the system.

➢ **To unset all partitions:**

1. If outside the premises, open a designated "entry" door. The keypad beeps, indicating that the entry delay time period has started.
2. Before the end of the entry delay time period, perform the following procedure:

NOTES:

- If you enter your code incorrectly, three short beeps will sound. Re-enter the code.
- Upon unsetting, a confirmation beep or squawk may sound**.**

For this:	Do this to unset ALL partitions:
	❖ **Unset all partitions:** Enter **code** ➢ press **unset button** ➢ if only 1 partition, it is now unset. For all partitions, at the "All?" prompt press **unset button** again. ❖ **Proximity unset:** Place **tag** ➢ press **unset button**
	❖ **Unset all partitions:** Press ➢ enter **code** ❖ **Proximity unset all partitions:** Press ➢place **tag**
	❖ **Fully unset all partitions:** Press . ❖ **Fully unset all partitions with PIN:** Press ➢ enter **PIN code**
	Press

Unsetting an Individual Partition

You can unset 1 individual partition at a time (as fully-set or partly-set).

➢ **To unset an individual partition:**

1. If outside the premises, open a designated "entry" door. The keypad beeps, indicating that the entry delay time period has started.
2. Before the end of the entry delay time period, perform the following procedure:

   NOTES:

   - If you enter your code incorrectly, three short beeps will sound. Re-enter the code.
   - Upon unsetting, a confirmation beep or squawk may sound**.**

For this:	Do this to unset an INDIVIDUAL partition:
	❖ **Unset an individual partition:** Enter **code** ➢ press **unset button** ➢ enter the 2-digit partition number (example 03) ➢ press **unset button.** ❖ **Proximity unset:** Place **tag** ➢ enter the 2-digit partition number (example 03) ➢ press **unset button** **NOTE:** You can select only partition **1, 2,** or **3** to unset only that specific partition. Other partitions cannot be separately unset from the keypad.
	❖ **Unset partition:** Enter the 2-digit partition number (example 03) ➢Press **unset button** ➢ enter **code** ❖ **Proximity unset partition:** Press ➢ place **tag**
	❖ **Unset a partition:** Press button **1,2,** or **3** for partition number ➢ press . ❖ **Unset a partition with PIN:** Press button **1,2,** or **3** for partition number ➢ press ➢ enter **PIN code** **NOTE:** You can select only partition **1, 2,** or **3** to unset only that specific partition. Other partitions cannot be separately unset from the keyfob.
	❖ Press

	❖ Press

3. Repeat the procedure for additional individual partitions to delete.

Duress Unsetting

See *Activating a Duress-Unsetting Alarm, page 66*.

Unsetting with Alarm Activation (Silencing an Alarm)

Depending on the system configuration, alarms will typically sound and have visual indications at the keypad. If you unset the system during an alarm activation, it will also serve to silence the alarm.

CAUTION: Before you unset with an alarm, ensure that it is a false alarm, or that no danger will result by silencing the alarm.

Once the cause of the alarm has been determined (and any steps for resolution taken, if needed), depending on the configuration, the system may require a "Technician Reset" – the intervention of an Engineer/technician to reset the system (see *Resetting the Alarm with Engineer/ Technician Intervention*).

IMPORTANT: If the alarm was triggered by a heat/smoke detector, in addition to the audible alarm, the fire indicator will display on the keypad indicating the fire system must first be reset before it can return to normal operation, and before one can re-set the system (see *Resetting latched devices, page 62*)**.**

CAUTION: During or after any type of alarm activation (manual or automatic), before approaching or entering the premises, first be certain that there is no danger present. You may need to contact responding agencies (police, fire, etc.) in order to confirm whether it is safe to return to the premises.

➢ **To unset with an alarm:**

1. If outside the premises, open a designated "entry" door; the keypad beeps, indicating that the entry delay time period has started.
2. Observe the following alarm activation indicators:
   - The sounder sounds
   - On keypads with displays, the **full-set** icon flashes and the activated **zone** displays (for multiple activations, the first activation displays).
   - On Slim keypads, the red LED flashes rapidly
   - A voice announcement may broadcast: "Alarm occurred in the system"
3. Enter your code (or place Proximity tag near the keypad's Proximity sensor).

4. Press the **Unset** button.
5. For keypads with displays, scroll to view all zones with alarm activations.
6. If Engineer-intervention is required to reset the system after an alarm, see *Resetting the System with Engineer/Technician Intervention*.

Returning the System to Normal Operation after Alarm Activation

After an alarm activation, returning the system to normal operation requires one of the following:

- A system unsetting performed by the Grand Master or system user with appropriate user authority level. See *Unsetting with Alarm Activation (Silencing an Alarm), page 59*.
- A system unsetting by Grand Master or system user, followed by the Engineer/ technician resetting the system (required after each alarm activation). See *Resetting the Alarm with Engineer/ Technician Intervention.*
- A procedure for the Grand Master to disable and reset Smoke/Heat detectors after a smoke/heat alarm activation. See *Resetting latched devices, page 62*.
- A procedure for the Grand Master or Engineer/technician to restore the system upon power-supply overload for the 3 amp power supply module. See *Restoring the System upon Power Supply Overload.*
- Resetting the System with Engineer Intervention

The following methods of resetting the system require Engineer/technician intervention (note that a system user must contact the Engineer/technician after each alarm activation):

- **Anti-Code reset** (also known as "**Technician reset")**
- **Configuration Software reset**

Anti-Code Reset (Engineer Reset)

If Engineer-enabled, upon alarm activation the system will not be ready to set until the Engineer provides you with a code that allows you to reset the system.

➢ **To perform an anti-code system reset:**

1. Ensure the system is unset.
2. After an alarm activation, while you see CALL ENGINEER displaying on the keypad, press the **Exit** button to access the Anti-Code menu.
3. At the **Anti-Code** option press **OK**.
4. Call the technician/Engineer and read the randomly generated code that displays on the keypad; the technician/Engineer will then give you an anti-code number.
5. Enter the anti-code number you received, and then press **OK;** the system resets.

Configuration Software Reset

Upon alarm activation, the system will not be ready to set until the Engineer performs a remote system reset using a computer with the **CS** (Configuration Software). Only a 1-hour single access to the CS is allowed per alarm activation.

NOTE: Depending on the system's configuration, the Grand Master may need to first authorize (enable) the Engineer to access the CS.

Enabling Engineer CS Access for Resetting the System

➢ **To enable the Engineer CS access for resetting the system:**

1. Ensure the system is unset.
2. Discuss with the Engineer which communication channel (**IP or GSM**) to utilize for his/her computer to remotely communicate with the system, for the purpose of performing a system reset using the CS.
3. At the keypad, enter your Grand Master code, and then press **OK.**
4. At **Activities** press **OK.**
5. Scroll to **Config SW,** and then press **OK;** either CS CONNECT or ENABLE CS displays:
   - **[If ENABLE CS displays]:** The system is **not** currently configured to allow the technician/Engineer to access the CS. For you to authorize the technician/Engineer a one-time access to the CS, press **OK,** scroll to **CS Connect**, and then proceed to step 6.
   - **[If CS CONNECT displays]:** The system is currently configured to allow the technician/Engineer to access to the CS. Proceed to step 6.

6. At **CS Connect** press **OK.**
7. Scroll to the communication channel that the technician/Engineer computer will utilize to communicate with the system (**IP or GSM**).
8. Press **OK;** DONE displays, and the technician/Engineer now has a 1-hour time limit to perform a CS reset of the system.

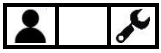
Resetting latched devices

The Grand Master can reset latched devices if configured to do so by the Engineer.

- **To reset latched devices:**

1. At the keypad, press menu, then enter your Grand Master code, and then press **OK**.
2. At **Activities** press **OK.**
3. Scroll to **Advanced** and then press **OK.**
4. At **Switch Aux** press **OK;** the keypad beeps and the latched device is reset.

Restoring the System upon Power Supply Overload



[For the 3-amp Power Supply Module only]: In the event of an overload of the system's power supply**,** you can attempt to restore the system by yourself.

IMPORTANT: If the following procedure does not resolve the situation, it will require the intervention of a technician/Engineer**.**

WARNING: Do not ever attempt to open the system's main panel or perform any service/repair yourself, as doing so can result in death, injury or damage – always contact a professional alarm system technician/Engineer.

- **To restore the system after a power supply overload:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Advanced** and then press **OK.**
4. Scroll to **Overload Restore** and then press **OK.**

Activating Emergency Alarms

All RISCO keypads are equipped with specific buttons to use for quick activation of emergency alarms:

- **Panic ("Police") alarm**
- **Fire alarm**
- **Auxiliary / emergency alarm**
- **Duress-Unsetting alarm**

NOTE: RISCO 4-button keyfobs and 8-button remote controls can also be used to also activate Panic alarms – ask your Engineer.

Upon alarm activation, Alarm Receiving Centre(s) can be automatically notified, which in turn contact responding agencies (fire, police, etc.). See *Compliance Statement*

Hereby, RISCO Group declares that the LightSYS Plus is designed to comply with:

- EN50131-1
- EN50131-3 Grade 3, Environmental Class II for Housing RP512B and RP432BP3
- EN50131-3 Grade 2, Environmental Class II for Housing RP432BP
- 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 2G/3G/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 Plus IP and GSM communication modules to be in compliance with the information security and substitution security requirements of EN50136.

Alarm Receiving Centre Partnership, *page 4*.

CAUTION: During or after any type of alarm activation (manual or automatic), before approaching or entering the premises, first be certain that there is no danger present. You may need to contact responding agencies (police, fire, etc.) in order to confirm whether it is safe to return to the premises.

Activating a Panic ("Police") Alarm

Keypad:	Press this:
Panda	
Elegant	
Slim	Buttons 1and 2
Narrow	
ProSYS	Buttons 1and 2

Activating a Fire Alarm

Keypad:	Press this:
Panda	Buttons 4 and 6
Elegant	Buttons 4 and 5
Slim	Buttons 3 and 4
Narrow	Buttons 4 and 6
ProSYS	Buttons 4 and 5

Activating an Auxiliary ("Emergency") Alarm

Keypad:	Press this:
Panda	Buttons 7 and 9
Elegant	Buttons 7 and 8
Slim	Buttons 5 and 6
Narrow	Buttons 7 and 9
ProSYS	Buttons 7 and 8

Activating a Duress-Unsetting Alarm

Activated from keypads only, a Duress-Unsetting alarm can be activated by all system users during a "duress" emergency situation (typically, where a user is forced to unset the system against their will). Duress unsetting "silently" disarms the system (no alarms will sound at the premises) while it simultaneously sends a duress alarm to the Alarm Receiving Centre, which in turn can quickly notify responding agencies, such as the police.

Instead of entering a user code, the user enters the special Duress-Unsetting code instead (see *Creating or Editing the Duress-Unsetting Code, page 17*).

[For Proximity Users]: If a user has already set the system using a Proximity tag, the user can activate a Duress-Unsetting alarm by using the **duress code only** (the user should not use the tag).

IMPORTANT: The same code is used by all system users, and it should be kept confidential from non-users.

CAUTION: A Duress-Unsetting alarm should be activated only when needed and not haphazardly, as Alarm Receiving Centres and responding agencies treat duress alarms seriously and may take immediate action.

Keypad:	Do this:
Panda	Enter **duress code** ➢ press OK
Elegant	Enter **duress code** ➢ press
Slim	Press ➢ enter **duress code**
Narrow	Enter **duress code** ➢ press
ProSYS	Enter **duress code** ➢ press #/6

Describing Utility Outputs

The system supports up to 196 programmable utility outputs (UOs) in the system. UOs typically automatically activate **external devices and appliances** such as lighting and air conditioning, or system **setting/unsetting** – in response to Engineer-defined activation criteria, such as events and other triggers related to alarms, zones, partitions, system events, user actions, and scheduled operations. Ask your Engineer about configuring UOs in your system.

To schedule the automatic operation of a UO, the user inputs specific criteria, such as the time and dates for activation/deactivation (s*ee Defining Automatically-Operated UOs and Setting Operations, page 69*). The Engineer can designate a label for each UO (the default is entitled "OUTPUT").

NOTE: Utility outputs can also be manually activated locally from keypads, or remotely via either SMS (see *Operating Remotely by SMS, page 33*).

UO Operational Modes

When a UO appliance/device is activated, it operates in one of the following Engineer-configured modes:

- **Latched:** The appliance/device remains activated until it is deactivated.
- **Pulsed:** The appliance/device remains activated for a predefined time, after which it is automatically deactivated.

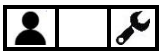
Manually Operating Utility Outputs

NOTES:

- All UOs are Engineer-configured
- Proximity and keyfobs/remote controls can be used if Engineer-configured

Device	Manual UO activation procedure:
	❖ Press **Exit** button ➢ enter **code** and press **OK** ➢ scroll to **Activities menu** and press **OK** ➢ scroll to **Output Control** and press **OK** ➢scroll to relevant **UO number** and press **OK** ➢ press **OK** again to activate (or deactivate) the utility output. ❖ **Proximity activation/deactivation:** Place tag to activate the Engineer-defined UO. Place tag again to deactivate the UO. **NOTE:** Proximity activation/deactivation is enabled only for tags that are specifically configured to operate a UO. A Tag that is configured to set/unset cannot operate the UO.
	❖ **Quick mode:** Press **UO button (1,2, or 3)** for 2 seconds ❖ **High-Security mode:** Press **UO button (1,2, or 3)** for 2 seconds ➢ enter **code** **NOTE:** You can activate from 1—3 UOs from the Slim keypad.
	❖ **Quick mode:** Press **UO button (1, 2,** or **3)** for 2 seconds ❖ **High Security mode:** Press **UO button (1, 2,** or **3)** for 2 seconds ➢ enter **code** **NOTE:** You can activate from 1—3 UOs from the 8-button remote control
	❖ Press button **3** or **4** (per Engineer definition) **NOTE:** You can activate 1 UO from the 4-button keyfob

Defining Automatically-Operated UOs and Setting Operations

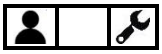


The Grand Master can configure the following automated system operations according to schedules and other criteria that the Grand Master defines:

- **One-time system setting/unsetting:** (For setting within the next 24 hours
- **Re-occurring weekly schedules:** Up to 64, for setting/unsetting the system and/or activating/deactivating up to 4 UOs
- **Holiday schedules:** Up to 99, for UO activation and system setting

NOTE: When defining schedules for automatically-operated UOs or setting operations, you may find it handy to use the scheduling chart for listing the details (see *Appendix A: Scheduling Chart for Automatic UO & Setting Operations, page 83*).

Defining a "One-Time" Schedule for Automatic Setting



➢ **To define a "one-time" system setting/unsetting:**

1. At the keypad, enter your Grand Master code, and then press **OK**.
2. Scroll to **Clock** and then press **OK**.
3. Scroll to **Scheduler** and then press **OK**.
4. Scroll to **One Time** and then press **OK.**
5. Scroll to **Next Set** and then press **OK.**
6. Select the partitions to set. As the partitions are grouped in blocks of 10, scroll to the relevant block and then select the partition(s) by entering the respective partition numbers.
7. Press **OK,** and then enter the time for the setting to occur (within the next 24 hours); the keypad sounds a confirmation beep.
8. Scroll to **Next Unset** and then press **OK.**
9. Select the partitions to unset. As the partitions are grouped in blocks of 10, scroll to the relevant block and then select the partitions by entering the respective partition numbers.
10. Press **OK.**
11. You can now enter an unsetting time; the keypad sounds a confirmation beep.

Defining Weekly Schedules for Automatic Setting and UOs

You can define up to 64 re-occurring weekly schedules for **automatic UO activation/deactivation** and **automatic system setting/unsetting.** Each schedule can have up to 2 separate start and stop time intervals per day. For an automatic setting/unsetting, you can also set a "user limitation" safeguard to prevent the users you specify from unsetting the system during the times you specify.

➢ **To define a weekly schedule:**

1. At the keypad, enter your Grand Master code, and then press **OK**.
2. Scroll to **Clock** and then press **OK**.
3. Scroll to **Scheduler** and then press **OK**.
4. Scroll to **Weekly** and then press **OK**.
5. Scroll to select the schedule number you are defining (**1—64**), then press **OK.**
6. Scroll to select from the following options for the selected schedule, then press **OK,** and then proceed to perform the respective configuration procedures in the tables below.
   - **1)SET/UNSET**
   - **2)UO ("UO ON/OFF")**
   - **3)USER LIMIT**

   NOTE: When finished configuring an option, you can select and configure from the other options above.

Configuring the Set/Unset Option

Turning a Setting/Unsetting Schedule On or Off

1. Scroll to **1)ON/OFF,** and then press **OK.**
2. Toggle to **ON** or **OFF** to turn the automatic setting schedule on or off respectively, and then press **OK.**

Defining Partitions for the Setting/Unsetting Schedule

1. Scroll to **2)PARTITION,** and then press **OK.**
2. Select partitions to set/unset. As the partitions are grouped in blocks of 10, scroll to the relevant block and then select the partitions by entering the respective partition numbers.
3. Press **OK.**

Configuring the Set/Unset Option

Selecting a Setting Mode for the Setting/Unsetting Schedule

1. Scroll to **3)SETTING MODE,** and then press **OK.**
2. Scroll to a setting mode: **SET** (full setting), **PART** (partial setting), or **GROUP** (group setting), and then press **OK.**
3. **[For Group mode]:** Select the group letter(s) to automatically set (each selected group displays as **Y**). To undo a selection, press the respective group letter again. Now press **OK.**
4. **[For all three modes]:** Select the day/time (required) and define a label for a setting/unsetting schedule (optional) – see the following procedures:

Setting the Day & Time for the Setting/Unsetting Schedule

1. Scroll to **4)DAY/TIME,** and then press **OK.**
2. Scroll to a day to assign SET and UNSET time periods – or scroll to **8)ALL** to assign those time periods to all days of the week, then press **OK.**

   NOTE: If you don't want to schedule time periods for any day(s), make sure the respective SET/UNSET times are set to the defaults (00:00).
3. Enter the SET time for the 1st time period, and then press **OK.**
4. Enter the UNSET time for the 1st time period, and then press **OK.**
5. Repeat the prior two steps for the 2nd time period if applicable**.**
6. Set SET/UNSET time periods for other days of the week as needed.

Defining a Label for the Setting/Unsetting Schedule

1. Scroll to **5)LABEL,** and then press **OK.**
2. Enter a label (see *Creating or Editing Labels, page 19*), and then press **OK.**

Turning the Inactivity Timer On or Off for the Setting/Unsetting Schedule

If there is no detection from any of the zones in partitions with an automatic schedule (that has the Set/Unset option defined by the Grand Master with the Inactivity Timer set to ON), then those partitions will be automatically set according to the (Engineer-set) Inactivity Timer parameter definition.

1. Scroll to **6)INACTIVE,** and then press **OK**.
2. Toggle to **ON** (to turn the Inactivity Timer on) or **OFF** (to turn it off), and then press **OK.**

Configuring the UO Option

Turning a UO Schedule On or Off

1. Scroll to **1)ON/OFF,** and then press **OK.**
2. Toggle to **ON** or **OFF** to turn the UO schedule on or off respectively, and then press **OK.**

Defining the Utility Output(s) for the Schedule

1. Scroll to **2)UTIL OUTPUTS,** and then press **OK.**
2. Scroll through the utility outputs (up to 4 can be defined for the schedule), and for each toggle to either **Y** (to select) or **N** (to not select/remove).
3. Press **OK.**

Setting the Day and Time for the UO Schedule

1. Scroll to **3)DAY/TIME,** and then press **OK.**
2. Scroll to a day to assign START and STOP time periods – or scroll to **8)ALL** to assign those time periods to all days of the week, and then press **OK.**

   NOTE: If you don't want to schedule time periods for any day(s), make sure the respective START/STOP times are set to the defaults (00:00).
3. Enter the START time for the 1st time period, and then press **OK.**
4. Enter the STOP time for the 1st time period, and then press **OK.**
5. Repeat the prior two steps for the 2nd time period if applicable**.**
6. Set START/STOP time periods for other days of the week as needed

Defining a UO Schedule as a "Holiday" UO Schedule

See *Describing Holiday Schedules, page 73*.

1. Scroll to **4)HOLIDAY,** and then press **OK.**
2. Toggle to **Y** (to set the schedule as a holiday schedule) or **N** (to not set it as a holiday schedule/remove a holiday schedule), and then press **OK.**
3. Now set the applicable dates (see *Setting Dates/Times and Activating a Holiday Schedule, page 74*)..

Defining a Label for the UO Schedule

1. Scroll to **5)LABEL,** and then press **OK**.
2. Enter a label (see *Creating or Editing Labels, page 19*), and then press **OK**.

Configuring the User Limitation Option

You can apply a "user limitation" mechanism to prevent selected users from unsetting the system during 1 or 2 specified time intervals per day. By default, users do not have a user limitation applied.

Applying/Removing a User Limitation

1. Scroll to **3)USER LIMIT,** and then press **OK.**
2. Scroll to **1)ON/OFF** and then press **OK.**
3. Toggle to **ON** to apply a scheduled user limitation or **OFF** to remove a scheduled user limitation, and then press **OK.** Continue with the following steps only if you are applying a user limitation.
4. Scroll to **2)USER NUMBER**, and then press **OK.**
5. Scroll through the users starting with Grand Master (or enter the user number) and for each user toggle to either **Y** (to apply a user limitation) or **N** (to not apply/remove an existing user limitation).
6. When finished configuring the users, press **OK.**
7. Press the **Exit button ( ),** then scroll to **3)DAY/TIME,** and then press **OK.**
8. Scroll to a day to assign the user limitation time periods – or scroll to **8)ALL** to assign those time periods to all days of the week, and then press **OK.**
   NOTE: If you don't want to schedule time periods for any day(s), make sure the respective START/STOP times are set to the defaults (00:00).
9. Enter the START time for the 1st time period, then press **OK.**
10. Enter the STOP time for the 1st time period, then press **OK.**
11. Repeat the prior two steps for the 2nd time period if applicable.
12. Set START/STOP time periods for other days of the week as needed.
13. Scroll to **4)Label,** and then press **OK.**
14. Enter a label (see *Creating or Editing Labels, page 19*), and then press **OK.**

Describing Holiday Schedules

Define up to 99 different holiday schedules that are ready to activate when needed. A holiday schedule is simply an additional schedule for **automatic UO activation/deactivation** or **automatic system setting/unsetting** for which you assign holiday-specific criteria as needed, such as dates/times, and partitions.

The start holiday will set the system and will only be unset at the end of the holiday schedule. An existing schedule defined to set/unset the same partition will not override the holiday schedule and, therefore, will not be activated before the end of the holiday schedule.

Setting Dates/Times and Activating a Holiday Schedule

This procedure is for both UO holiday schedules and setting holiday schedules.

- **To set the date/time and activate a UO or setting holiday schedule:**

1. **[For a UO holiday schedule only]:** First perform the following procedure: *Defining a UO Schedule as a "Holiday" UO Schedule*
2. **[For a UO holiday schedule or setting holiday schedule]:** At the keypad, enter your Grand Master code, and then press **OK**.
3. Scroll to **Clock** and then press **OK**.
4. Scroll to **Holiday** and then press **OK.**
5. Scroll to **Dates** and then press **OK;** the first holiday schedule (01) appears first by default.
6. Press the **unset button** for this holiday schedule (01), or scroll to another holiday schedule (from 01—99), and then press **OK.**
7. Enter a start time.
8. Scroll to the date field and enter a date (in a **day/month** format), and then scroll to the activation status **(Y** or **N)** and toggle to change it accordingly –Y activates the holiday schedule and N deactivates the holiday schedule.
9. **[For a setting holiday schedule only]:** If you are defining partitions, perform the following procedure now: *Defining Partitions for a Setting Holiday Schedule, page 74.*

Defining Partitions for a Setting Holiday Schedule

You can define up to 32 partitions for a setting holiday schedule.

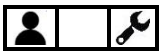
- **To define partitions for a setting holiday schedule:**

1. Directly after you performed the prior procedure, press the **Exit button,** then scroll to **Partitions,** and then press **OK.**
2. The 32 partitions are grouped in blocks of 10. Scroll to the relevant block and then select the partition(s) by entering the respective partition number(s). To delete a previously selected partition, re-enter the partition number.
3. Press **OK.**

Using Macros

System users can activate macros, which are custom commands for controlling and operating the system. Up to four macros (A, B, C, D) can be recorded (programmed) locally using any RISCO keypad except Slim models.

Recording Macros



➢ **To record a macro:**

1. At the keypad, enter your Grand Master code, and then press **OK**.
2. Scroll to **Macro** and then press **OK.**
3. Scroll to select one of the available (not-yet recorded) macro options -- **A, B, C,** or **D,** and then press **OK.**
4. Press the macro option you selected in the prior step (A, B, C, or D) for 5 seconds to start the recording sequence.
5. Enter a sequence of characters according to the following table:

Character	Represents the following
0--9	Numerical buttons from 0—9
A, B, C, D	Macro keys A, B, C, and D
*****	Exit button
#	OK button
a, b, c, d	Groups A, B, C, and D
r	Full setting button
s	Part setting button

6. After you finished entering the series of characters, scroll so that the cursor is located **after** the last character in the series, and then press the macro option you had selected in step 3; the macro is saved.

Activating Macros

➢ **To activate a pre-recorded macro:**

- On the keypad, press the macro option **(A—D)** for 2 seconds to activate the respective macro.

Performing Maintenance Tasks

Defining the Time and Date Manually

For systems connected to the Cloud, the time and date are updated automatically, however, regardless of whether your system is Cloud-connected or not, the time and date can be manually set as needed.

- **To manually define the time and date:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Clock,** and then press **OK.**
3. At **Time & Date** press **OK.**
4. Using the scroll keys to move the cursor, enter the time and date in the format as shown on the keypad display. When finished, press **OK.**

Replacing Detector & Accessory Batteries in Service Mode

Activating **Service mode** silences all tamper alarms from detectors and accessories for an Engineer-defined period of time, which enables you to replace wireless detector and accessory batteries without the tamper alarms sounding.

- **To activate and deactivate Service mode:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Advanced,** and then press **OK**.
4. Scroll to **Service Mode,** and then press **OK;** a confirmation beep sounds and SERVICE MODE ACTIVATED displays.
5. Proceed to replace detector/accessory batteries as required.
6. When you've finished replacing batteries, press **OK** to deactivate Service mode.

   NOTE: If the keypad has timed out (after 90 seconds – when SERVICE MODE and the time/date display), in order to deactivate Service mode first press **Exit**, and then repeat **steps 1—4** in this procedure; a confirmation beep sounds and SERVICE MODE DEACTIVATED displays.

   NOTE: After the Service mode time period expires, if you did not yet exit the mode, the system will automatically exit and any open detectors/accessories may trigger tamper alarms.

Performing SIM Card Maintenance

Checking the SIM Credit Level

Receive information on the available credit level of the prepaid SIM card via SMS or voice (Engineer-configured).

➢ **To check the SIM credit level:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Prepaid SIM,** and then press **OK**.
4. Scroll to **Check Credit,** and then press **OK;** SENDING MESSAGE appears as the system communicates to the service provider, and you will receive notification of the SIM credit status accordingly (via SMS or voice message).

Resetting the SIM Card

After replenishing the SIM card's credit level, it must be manually reset.

➢ **To reset the SIM card:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Prepaid SIM,** and then press **OK**.
4. Scroll to **Reset SIM,** and then press **OK.**
5. Press **OK** again; RESET SIM CARD COUNTER appears to inform of the reset.

Enabling / Disabling Keypad Sounds

At the keypad, you can turn the following sounds on or off:

- **Keypad chime** [for the internal chime of the current keypad]: Turn the chime **ON** or **OFF** for all functions that have the chime feature.
- **Partition chime** [for the internal chime of all keypads in the partitions]: Turn all the chimes **ON or OFF** for all functions that have the chime feature.
- **Buzzer** [for the internal buzzer of the current keypad]: Turn the buzzer **ON** or **OFF** – used Entry & Exit Delay time periods, and for fire and intrusion alarms.

Enabling / Disabling the Current Keypad's Chime

➢ **To enable/disable the internal chime of the currently-used keypad:**

1. At the keypad, enter your Grand Master or user code, and then press **OK.**
2. At Activities press OK.
3. Scroll to **Keypad Sound,** and then press **OK.**
4. At **Chime** press **OK.**
5. Scroll to **Keypad Chime** and then press **OK.**
6. Scroll to **ON** or **OFF,** then press **OK;** LOCAL CHIME ON (or OFF) displays.

Enabling / Disabling All Keypad Chimes

➢ **To enable/disable the internal chime of all keypads in all partitions:**

1. At the keypad, enter your Grand Master or user code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to **Keypad Sound,** and then press **OK.**
4. At **Chime** press **OK.**
5. Scroll to **Partition Chime** and then press **OK.**
6. Scroll to **ON** or **OFF**, then press **OK;** GLOBAL CHIME ON (or OFF) displays.

Enabling / Disabling the Current Keypad's Buzzer

➢ **To enable/disable the internal buzzer of the currently-used keypad:**

1. At the keypad, enter your Grand Master or user code, and then press **OK**.
2. At Activities press **OK**.
3. Scroll to **Keypad Sound,** and then press **OK**.
4. At **Chime,** scroll to **Buzzer On/Off,** and then press **OK.**
5. Scroll to **ON** or **OFF,** then press **OK;** LOCAL BUZZER ON (or OFF) displays.

Terminating Follow-Me Notifications

You can terminate the transmission of FM notifications to the recipients – for example, for a false alarm, where you don't want the recipients to get notified.

- **To terminate Follow Me notifications:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Follow Me** and then press **OK.**
3. Scroll to **Terminate FM** and then press **OK; notification** transmissions to all remaining FM destinations are stopped.

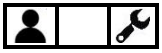
Cancelling Alarm Receiving Centre Notification upon Engineer Programming

If the system is configured to require the Grand Master to notify the Alarm Receiving Centre when an Engineer/technician configures programs the system (for any time after initial system setup and programming), the Grand Master can select **Void Report Programming** to cancel sending the notification report to the Alarm Receiving Centre, and still allow the Engineer to program the system. The Engineer will then have 5 minutes to gain access to the Engineer Programming menu.

- **To allow Engineer programming without Alarm Receiving Centre notification:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. At **Activities** press **OK.**
3. Scroll to Advanced, and then press **OK.**
4. Scroll to **Void Report Programming,** and then press **OK;** the Engineer has 5 minutes to gain access to the Programming menu.

Testing the System



The following tests are recommended to be performed at system installation, and subsequently, as needed. Ask your Engineer if they have already been performed during the system installation.

Performing a Walk Test

A walk test checks the detection ability of all detectors (PIR and Magnetic Contact detectors) in all zones, to ensure correct operation. Test results are displayed on the keypad. A walk test can be a relatively a quick procedure, depending on the scope of the installation and premises, however if needed, up to 60 minutes is allotted for the test. The following walk tests can be performed:

- **Full Walk Test:** This test displays the activated zones (the zones where all detections occurred) and the types of detection.
- **Quick Walk Test:** This test displays the non-activated or open ("not-ready") zones (the zones where detections didn't occur).

NOTES:

- Both full and quick walk tests must be performed with the system unset.
- A walk test cannot be performed using a Slim keypad

➢ **To perform a full or quick walk test:**

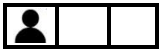
1. Ensure the system is unarmed.
2. At the keypad, enter your Grand Master code, and then press **OK.**
3. Scroll to **Maintenance** and then press **OK.**
4. Scroll to **Walk Test** and then press **OK.**
5. Scroll to either **Full Walk Test** or **Quick Walk Test,** and then press **OK;** MAKE WALK TEST AND HIT ANY KEY display.
6. During the allotted time period of 60 minutes, walk through all the zones in order to trigger activations from all the detectors in those zones.

   NOTE: During the last five minutes of the time period, the keypad used to initiate the test will indicate that the time period is about to end.
7. When you have finished walking through the zones, press any key on the keypad to end the test; the results display on the keypad.

Testing ARC Communication

This tests the communication between the system and the Alarm Receiving Centre(s). See *Step 9: Performing an Alarm Receiving Centre Test, page 29*.

Testing Follow-Me Destinations

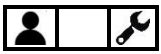


This tests if notifications sent to Follow-Me destinations (recipients) are received. It is highly recommended to test every FM destination.

➢ **To test a FM destination:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Follow Me** and then press **OK.**
3. Scroll to **Test FM** and then and press **OK.**
4. Scroll to select a FM destination to test, and then press **OK;** FM TEST ACTIVATED displays and a test message is sent to the selected FM destination.

Performing a Keypad Test



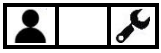
This tests a keypad's indicators.

NOTE: This test is not relevant for the Slim keypad.

➢ **To perform a keypad test:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Maintenance** and then press **OK.**
3. Scroll to **Keypad Test** and then press **OK;** all the keypad's indicators display for a few seconds.

Performing a Sounder Test



This tests a sounder's' sounding mechanism.

➢ **To perform a sounder test:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Maintenance** and then press **OK.**
3. Scroll to **Sounder Test** and then select the sounder to test.
4. Press **OK;** the sounder sounds.
5. Press **Exit** to end the sounder test.

Performing a Strobe Test

This tests a sounder's strobe light.

➢ **To perform a strobe test:**

1. At the keypad, enter your Grand Master code, and then press **OK.**
2. Scroll to **Maintenance** and then press **OK.**
3. Scroll to **Strobe Test** and then select the strobe to test.
4. Press **OK;** the strobe activates.
5. Press **Exit** to end the strobe test.

Appendix A: Scheduling Chart for Automatic UO & Setting Operations

You can use this chart (optional) to list the details of an automatic UO or setting schedule – it can be used for reoccurring weekly schedules, or weekly holiday schedules.

Schedule name / number: _____

Reoccurring weekly schedule: ☐ **Holiday schedule:** ☐

Schedule Type	Details			
Set / Unset ☐	**Partition(s)** _____			
	Setting Mode: ☐ Full ☐ Part ☐ Group	**Group:** ☐ A ☐ B ☐ C ☐ D		
Utility Output ☐	**UO number(s):**_____			
	Note: Up to 99 different holiday schedules can be defined.			
User Limitation ☐	**User Number**	**Name**	**User Number**	**Name**
	Note: Default is without user limitation applied.			

Day	Start Time 1 HH:MM	Stop Time 1 HH:MM	Start Time 2 HH:MM	Stop Time 2 HH:MM
Sunday				
Monday				
Tuesday				
Wednesday				
Thursday				
Friday				
Saturday				

Appendix B: User Menu Maps

The following user menus and respective options will display according to the system installation, as well as the authority level of the user.

User menu	Menu options and respective settings
Activities	○ **Omit** ➢ Zones ➢ One Time Only, Omit Reset, Omit Recall, Permanent Omit ○ **Output control** ➢ Output 001 ○ **Keypad sound** ➢ Chime, Buzzer ON/OFF ○ **Config SW** ➢ CS Connect ○ **Prepaid SIM** ➢ Check credit, Reset SIM ○ **WiFi** ➢ WiFi Scan, WiFi WPS Button ○ **Advanced** ➢ Switch AUX, Void Rep. Prog., Service mode. ARC Test
Follow Me	○ **Define** ➢ FM number ➢ Report Type, Partition, Events, Restore Event, Remote Control, Label ○ **Test FM** ○ **Terminate FM**
View	○ **Fault** ➢ (view faults) ○ **Alarm Memory** ○ **Partition Status** ○ **Zone Status** ○ **Service Info** ➢ Engineer, System version, Serial number, Panel ID ○ **View IP Address** ○ **Cloud Status** ○ **Wi-Fi Status**
Codes/Tags	○ **Define** ➢ GM, user, ➢ Edit code, Authority, Partition, (Re)Write Tag, Delete Tag, Edit Label ○ **Delete By Tag**
Clock	○ **Time & Date** ○ **Scheduler** ➢ Weekly, One Time ○ **Holiday** ➢ Partitions, Dates
Event Log	○ **Event number / user**
Maintenance	○ **Walk test** ➢ Full Walk Test, Quick Walk Test ○ **Keypad test** ○ **Sounder test** ○ **Strobe test**
Macro	○ **Macro** ➢ A, B, C, D
Stand Alone Keyfob	○ **Select receiver** ➢ New keyfob, Delete keyfob, Delete All, UO buttons

Appendix C: System Indicators

Various audible (sound) indicators and visual (viewed) indicators are available, depending on the system configuration.

Sound Indicators

Sound indications are available for system status, operations and events:

- **Beeps and squawks**
- **Voice announcements**

Sound indicators are requested / initiated from keypads and remote controls, and the sounds can be heard from the keypads, remote controls and external sirens.

"Beep" and "Squawk" Sound Indicators

The following table below shows the "beep" and "squawk" sound indications that are heard when requested / initiated from keypads, remote controls and keyfobs:

Requested / initiated from: 8-button remote control		
Operation / event	**Sounds from remote control**	**Sounds from sounder**
Confirmation	1 beep	No sound
Error	3 beeps	No sound
Alarm	5 beeps	No sound
Setting / unsetting	1 beep	Set = 1 squawk Unset = 2 squawks (or 4 if unset after an alarm)

Requested / initiated from: 4-button keyfob		
Operation	**Sounds from keyfob**	**Sounds from sounder**
Setting / unsetting	No sound	Set = 1 squawk Unset = 2 squawks (or 4 if unset after an alarm)

Requested / initiated from: Slim keypad		
Operation / event	**Sounds from keypad**	**Sounds from sounder**
Confirmation	1 long beep	No sound
Wrong code	3 short beeps	No sound
Entry/exit beeps	Slow repeating beeps until end of delay period [2] Fast beeps at end of delay period.	No sound

Requested / initiated from: Slim keypad		
Each key press	1 short beep	No sound
Setting / unsetting	1 long beep	Set = 1 squawk Unset = 2 squawks (or 4 if unset after an alarm)

Requested / initiated from: Narrow, Elegant, Panda keypad		
Operation / event	**Sounds from keypad**	**Sounds from sounder**
Intrusion alarm	Fast beeping	Sounder sound (fast beeping)
Fire alarm	Fast beeping	Repeated sequence of 2 sounder beeps followed by short interval
Duress Unsetting alarm	No sound (1)	No sound (1)
Emergency alarm	A single beep	No sound
Setting / unsetting	Long "confirmation" beep (can be Engineer-configured to be without sound).	Set = 1 squawk Unset = 2 squawks (or 4 if unset after an alarm)
Confirm operation	Long "confirmation" beep	No sound
Reject command / incorrect operation	3 fast beeps (2,3)	No sound
Chime sound	Long beep (4)	None
Entry Delay countdown	Slow repeating beeps until end of delay period (2) Fast beeps at end of delay period.	No sound (unless Engineer-configured)
Exit Delay countdown	Slow repeating beeps until end of delay period (2) Fast beeps at end of delay period.	No sound (unless Engineer-configured)

Footnotes:

1. As defined by the Engineer, during system installation.
2. Keypad beeps may be enabled/disabled by user (see *Enabling / Disabling Keypad Sounds, page 77*).
3. Press the OK button on the keypad for two seconds to stop fault beeps
4. As defined by the Engineer, for any intrusion zone violated when the system is unset. It can be disabled when not required.

Voice Announcements

Requested/initiated from keypads, **Voice Announcements** enable users to hear LightSYS Plus-supplied voice clips (short voice recordings) that are broadcast through Listen-In & Speak Units – for announcing system events such as alarms, and as confirmation for user-initiated commands at the time of setting/unsetting only.

NOTE: To utilize voice announcements, specific modules need to be installed –ask your Engineer.

Viewed Indicators

Requested/initiated from the keypads and remote controls, the following viewed indicators are provided for system status, operations and events:

- **Texts and messages** on keypad displays
- **Icon status indicators** on keypad displays
- **LED status indicators** on keypads and 8-button remote controls

For the procedures to view system status, see *Obtaining System Information, page 35*.

Keypad Indicators

NOTE: For wired keypad display options, see *Keypad Display Options, page 34*.

Slim Keypad Indicators

LED Indicators	LED Color	State	Status
	Blue	Blinking	Keypad is communicating with the panel
	Red	On	System is fully or partially set
		Slow flashing	During an exit delay
		Rapid flashing	During an alarm
	Green	Blinking	Fault indication is in the system while the system is unset
	Green/Red	Toggling	Waiting for code to be entered

Narrow Keypad Indicators

POWER **On**: Power OK **Off**: No power **Rapid flash:** System fault	**SET** **(Also red LED on Narrow keypad)** **On**: System set – either fully or partially. **Off**: System is unset **Slow flash:** System is in Exit Delay **Rapid flash:** Alarm	**PART/OMIT** **On**: System is in part set or zone-omit mode **Off**: No omitted zones
READY **On**: Ready to set **Off**: Not ready to set **Slow flash:** Ready to set with open Exit/Entry zone	**FIRE** **On**: Fire alarm **Off**: No fire alarm **Flash:** Fire alarm fault (fire circuit fault)	**TAMPER** **On**: Tamper alarm **Off:** No tamper alarm

Panda Keypad Indicators

FAULT **On:** System Fault **Off:** System operating normally	**READY** **On:** Ready to set **Off:** Not ready to set **Slow flash:** System is ready to be set while exit/entry zone is open	**SET** **On:** System is set in Full Set or Stay Set mode **Off:** System unset **Slow flash:** System in Exit Delay **Rapid flash:** Alarm
PART SET / OMIT **On:** System is Stay Set mode (Part Set) or Zone Omit mode **Off:** No omitted zones	**TAMPER** **On:** Zone / keypad / external module has been tampered **Off:** All zones are operating normally	**CLOUD CONNECTIVITY** **On:** System connected to cloud **Off:** No cloud connection configured / No cloud connectivity **Slow flash:** Cloud connectivity fault

Elegant Keypad Indicators		
POWER **On:** Power OK. **Off:** No power **Rapid flash:** System fault. **Slow flash:** System is in programming	**READY** **On:** Ready to set **Off:** Not ready to set **Slow flash:** Ready to set with open Exit/Entry zone	**SET** **On:** System in fully set mode **Off:** System unset **Rapid flash:** Alarm **Slow flash:** System in Exit Delay
PART SET / OMIT **On:** System is in partially-set or zone-omit mode **Off:** No omitted zones	**TAMPER** **On:** Tamper alarm **Off:** No tamper alarm	**FIRE** **On:** Fire alarm **Off:** No fire alarm **Flash:** Fire alarm fault (fire circuit fault)

Remote Control Indicators

8-Button Remote Control Indicators		
Operation	**LED for Send Commands**	**LED for Receive Status**
Full Setting	Green*	Red
Part Setting	Green*	Orange
Unsetting	Green*	Green
Alarm	Green*	Flashing LED
* If the LED changes to orange, it indicates the remote control battery is low.		

4-Button Panda Keyfob Indicators		
Operation	**LED for Send Commands**	**LED for Receive Status**
Full Setting	Green*	Red
Part Setting	Green*	Orange
Unsetting	Green*	Green
Alarm	Green*	Flashing LED
UO activation	Green*	Blinks according to panel status
* If the LED changes to orange, it indicates the remote control battery is low.		

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

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.

Contacting RISCO Group

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

This RISCO product was purchased from:

© RISCO Group. All rights reserved. 2022