

riscogroup.com



LightSYS™2

User Manual

Register with RISCO Cloud (if enabled)

Registering with RISCO Cloud enables you to monitor and control your LightSYS™2 system.

Note: Registration and connection of your system to www.riscocloud.com may depend on your installer.

1. Go to www.riscocloud.com/register.
2. Enter your first name and last name.
3. Enter your email address as Login Name (required for 1st time activation).
4. Define password (minimum of 6 characters and at least one digit) and confirm.
5. Enter in the 15 digits Panel ID as it appears: on the postcard that arrived with the panel or supplied by the installer (also available in the keypad menu as described below)
6. Complete registration form and click Register.
7. To complete registration open the email message received on the email account you defined as Login Name.

Login to RISCO Cloud






1. Go to www.riscocloud.com.
2. Enter User Name and Password (same as supplied during the registration process).
3. Enter Passcode/PIN (LightSYS™2 User Code).
4. Click **Enter**.

iRISCO – RISCO's Smartphone Application

Homeowners can now enjoy the iRISCO Smartphone app for smart and easy control of their LightSYS™2 system from any location.











































Download the iRISCO app from the Apple App store or Android Play Store (Search for "iRISCO").

Locating Panel ID in Keypad

1. From the main display press .
2. Enter master code (default code 1234) followed by .
3. Scroll to the option "View" and press .
4. Scroll to "Service Info" and press .
5. Scroll to "Panel ID" and press . 15 digit Panel ID is now displayed.






Interface:

LCD Keypad (432KP)

Full (Away) Arm	Code > 
Part (Stay) Arm	Code > 
System Disarm and Silence an Alarm	Code> 
Partition Away Arm	Code >  > Partition No. > 
Partition Stay Arm	Code >  > Partition No. > 
Partition Disarm	Code>  > Partition No. > 
Duress Unset	Duress Code > 
Panic Alarm	Pressing   simultaneously for 2 seconds
Fire Alarm	Pressing   simultaneously for 2 seconds
Medical Alarm	Pressing   simultaneously for 2 seconds
Quick Zones Bypass	Code >  [Zone No.]
Activate Output	 [Code]  [Activities]  [Util Output Num]
Define Follow-Me	 > [Code]  [Follow Me]  [Define]
View Trouble	 [Code]  [View]  [Trouble] 
View Event Log	 [Code]  [Event Log] 
Keypad Chime On/Off	 [Code]  [Activities]  [Keypad sound]  [Chime]
Edit User Code	 [Code]  [Codes/Tags]  [Define]
Zone Testing (Walk Test)	 [Code]  [Maintenance]  [Walk Test]  



2-way Slim keypad

Operation	Quick	High-Security Mode ¹
Full Arm – System		 > [Code] ²
Full Arm – Partition	Select partition [1/2/3] > 	Select partition [1/2/3] >  > [Code] ²
Full Disarm	 > [Code] or Proximity tag (after waking)	



Partial Arm – System ³			> [Code]
Partial Arm – Partition	Select partition	Select partition	
	[1/2/3] >	[1/2/3] >	> [Code]
Partition Disarm	Select partition 1/2/3/4 and press		followed by [Code]
Panic alarm	Press	+	simultaneously for 2 seconds
Fire alarm	Press	+	simultaneously for 2 seconds
Emergency/Med alarm	Press	+	simultaneously for 2 seconds
Status Request	Press for 2 seconds to view LED display of system status (see Indicators below)	Press for 2 seconds followed by code ² to view LED display of system status (see Indicators below)	
Output Control	Press 1/2/3 for 2 seconds	Press 1/2/3 for 2 seconds followed by code ²	
Wake up keypad	Press		

2-way Remote Control keyfob


Operation	Quick	High Security Mode ¹
Full Arm		> [Code]
Partial Arm*		> [Code]
Full Disarm		> [Code]
System Status	for 2 seconds	for 2 seconds > Code



Output Control A/B/C	/ / for 2 seconds	/ / for 2 seconds > [Code]
Panic Alarm	+ simultaneously for 2 seconds	
Clear Operation	>	

*For Part setting with no entry delay, press and hold for two seconds

Notes:

- 1. Consult your installer for the operations defined with a code.
- 2. The proximity tag can be used instead of code.
- 3. For Part Setting (Stay Arming) with no entry delay press  for 2 seconds.
- 4. Light sensor is used to save battery by turning on/off the keypad backlight.
- 5. Needs to be defined by your installer.

Smartphone

Full Arm – System



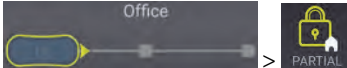
Full Arm – Partition



Partial Arm – System



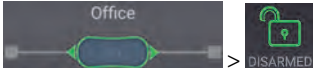
Partial Arm – Partition



System Disarm



Partition Disarm



Detector Bypass (On/Off toggle)



Web Application

SET/UNSET sub-tab

Full Arm All Partitions or PARTITION x > Full Set

Full Arm – Group [Group Letter] > Full Set
(if supported) Or PARTITION x > [Group Letter]

Part Arm All Partitions or PARTITION x > Partial Set

Disarm All Partitions or PARTITION x > [Code] > UNSET







SETTINGS sub-tab

System user and codes	Edit, Delete and ADD NEW USERS
Web interface users and codes	EDIT user fields and access credentials
Change Password	Enter Old/New/Confirm > SET NEW PASSWORD
Quick Zone Bypass	Select ZONE xx > Omit > Update
Change Appearance	Select Color Scheme
Alerts/Add New Contact	Enter Name, Email/Mobile phone #. Select Alert Language, Partition association, and toggle Set/Unset Email and SMS
Time Zone	Select system time zone


HISTORY sub-tab

Review activity log and export

AUTOMATION sub-tab

Utility Outputs	Toggle ON/OFF > Update
1-way Remote Control keyfob	
Full Arm	Press 
Disarm	Press the  button. All partitions assigned to the button will be disarmed
Stay Arm	Press  button or button 4 (if defined)
Partition Arm	Press  button or button 4 (if defined)



SMS	For a full list of SMS operations, refer to <i>Appendix D – SMS Operation</i> .	
Full Arm	[Code][A], example, 1234A	
Full Disarm	[Code][D], example, 1234D	
Stay Arm	[Code][H], example, 1234H	
Partition Arm	[Code][A] [Partition No.] examples: To arm partitions 1: 1234A1 To arm partitions 1 and 2: 1234A12	
Partition Disarm	[Code][D] [Partition No.] Example 1234D1	

Indicators:

LCD and Touchscreen Keypads



(Power):

On: Power OK, No troubles

Off: No power

Rapid Flash: System trouble

(Ready):

On: Ready to arm

Off: Not ready to arm

Slow Flash: Ready to arm with open Exit/Entry zone



(Arm) / RED LED

On: System armed (Away or Stay)

Off: System disarmed

Slow Flash: System is in Exit Delay

Rapid Flash: Alarm



(Tamper) :

On: Tamper alarm

Off: No tamper alarm



(Stay / Bypass):

On: System armed at Stay / Bypass zones in the system

Off: No bypass zones



(Fire):

On: Fire alarm

Off: No fire alarm

Flash: Fire trouble



(Proximity) [Touchscreen only]

Flashing: Indicates keypad has a proximity reader

2-way Slim Keypad

Blue Red Green



LED Indicator

Color	State	Status
Blue	Blink	During communication with the panel
Red	On	System fully or partially armed
	Slow flash	During exit delay
	Rapid flash	During alarm
Green	Blink	Trouble indication in the system while the system is unset*
Green/Red	Toggle	Waiting for code to be entered

2-way Keyfob

Operation	LED* (Send command)	LED* (Receive Status)
Full Setting (Away)	Green	Red
Part Set (Stay Arm)	Green	Orange
Unset (Disarm)	Green	Green
Alarm	Green	Flash LED

* If the LED changes to orange, it indicates a low battery condition.

Table of Contents

Chapter 1 Mastering Your System	9
Introduction	9
Main System Capabilities	9
LightSYS™2 Architecture	10
User Operating Tools	11
System Monitoring	13
System Tones	15
Chapter 2 Arming and Disarming	17
Arming your system	17
Disarming your system	22
Additional Arm/Disarm Capabilities	26
Emergency Alarms	26
Chapter 3 User Functions and Settings	27
User Codes	27
Proximity Tags	30
Setting and Changing System Time and Date	32
Setting Follow Me Destinations	33
Bypassing zones	34
Scheduling Weekly Programs	35
Macro Keys	36
Parking Control with LightSYS™2 Gate Control Keyfobs	38
Complete List of User Functions	40
Appendix A – System Troubles	47
Appendix B – Glossary	48
Appendix C – Scheduling Tables	50
Appendix D – SMS Operation	51
Appendix E – System Testing and Maintenance	52

Chapter 1 Mastering Your System

Introduction
















Congratulations on your purchase of RISCO Group's **LightSYS™2** Security System. The LightSYS™2 has been specifically designed to meet a wide range of security needs for residential and commercial applications.

LightSYS™2 is designed to recognize abnormal conditions and inform the system of the status of any protected door, window, hallway, room, or area. It supports the capabilities of communicating with a Central Monitoring Station or to your mobile phone using friendly and easy to understand verbal messages as well as SMS, E-mail messages or cloud channel reporting.

The **LightSYS™2** contains a variety of programming features including smartphone apps and web control. Ask your installer which features have been programmed for your system.

This manual describes how to operate your system. It will guide you through programming instructions for main system features as well as basic arming and disarming commands for the system

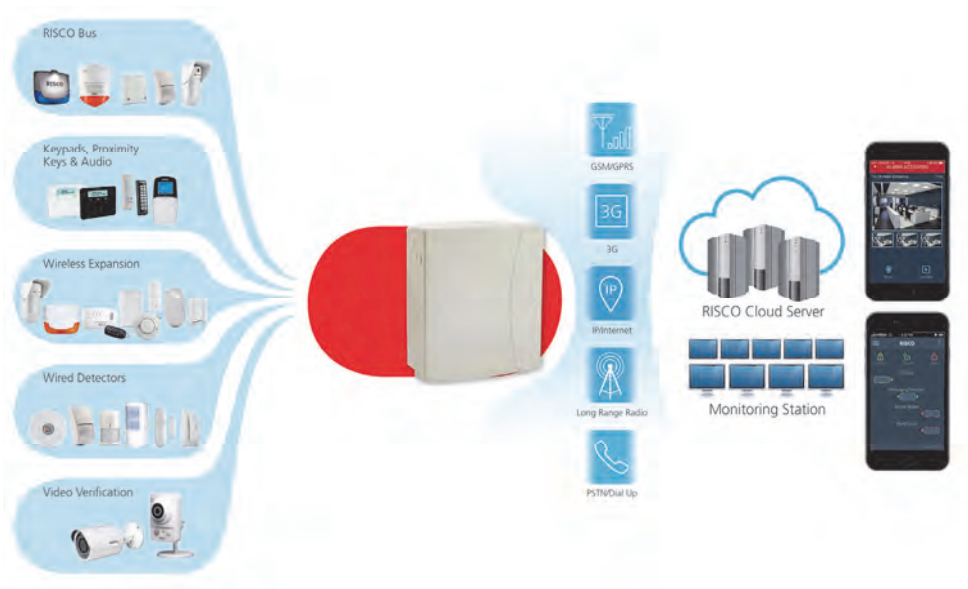
Main System Capabilities

-  Up to 32 sensor devices
-  16 User codes + Grand Master code
-  4 authority levels for different system users
-  Optional user proximity tag to be used instead of a code
-  Up to 4 partitions
-  4 wired / wireless keypads
-  Up to 4 sirens
-  Up to 16 full control remote controls
-  Up to 200 gate control remote controls
-  500 Events Log
-  16 Follow Me destinations
-  Up to 14 outputs
-  X-10 support for home automation
-  4 automatic scheduling programs
-  Smartphone operation of principal functions



LightSYS™2 Architecture

Your **LightSYS™2** controls and monitors a variety of sensors, detectors, and contacts placed throughout the premises, which provide external, perimeter and internal burglary protection. The system is supervised, meaning that the panel checks the status of each sensor to detect problems. If trouble is detected, you are notified both with panel beeps and indicator lights as well as remote messaging. The following diagram shows the components that make up the system:



User Operating Tools

LightSYS™2 can easily be managed locally or remotely depending on your system configuration.

You can issue commands to the system and in turn, the system will communicate information to you via its display, indicators, voice messages, SMS messages, Email messages and by the sounds it makes.

Depending on your purchased supplementary modules, you can operate your system via the following:



LightSYS™2 Keypad and proximity tag:

Locally through its LCD keypad(s), you can issue commands to your system. In turn, the system can communicate information to you through its display, indicators and by the sounds it makes.



2-Way Slim Keypad

With support for up to three bi-directional wireless communication, 2-Way slim keypads, LightSYS™2 now offers an outdoor-certified tamper-proof power-saving option. The slim keypad offers the entire range of arming and disarming as well as alarming options



2-Way 8 Button Remote Control:

Using the bi-directional 8 button remote control you can arm, disarm, send a panic alarm, activate outputs and more. Being bi-directional the remote control receives a reply status indication, via its 3 colored LEDs and internal buzzer siren, from the panel for each command that it has sent to the panel. For higher security, commands can be defined to be activated with a 4 digit PIN code.



Smartphone Operations:

Homeowners can now enjoy the iRISCO Smartphone App for smart and easy control of their LightSYS™2 system. The app enables users to arm/disarm the system on-the-go, activate home automation devices, bypass detectors, view the system's status and history, and much more. Available for iPhone, iPad and Android.

Note: Registration and connection of your system to www.riscocloud.com may depend on your installer

Mastering Your System



Web Application:

RISCO Group's interactive web application enables you to monitor, control and configure your LightSYS™2 system from any location. As with the Smartphone app, the application is powered by the RISCO Cloud server.

Note: Registration and connection of your system to www.riscocloud.com may depend on your installer



4 Button Keyfob:

Using the wireless 4 button keyfob you can arm, disarm, send a panic alarm and activate outputs.



Remote Phone Operation:

If your system includes the voice module, it can provide audible information about system status, and enable any remote, touch-tone (DTMF) telephone to act as a keypad for the system. Upon event occurrence, such as alarm activation, the voice module informs you by calling you and playing a prerecorded event announcement, as described in the *5IN1545 LightSYS Voice Module Programming and Operations Guide*.



SMS:

If your system is equipped with RISCO Group's GSM/GPRS module it can provide information about the system by SMS and enable operation of the system using SMS commands for arming the system, disarming the system and more.



Configuration Software:

RISCO Group's Configuration Software enables the installer to program the system and manage the system locally or remotely.

System Monitoring

Report to Monitoring Station

When a system event occurs, the control system sends a message to your monitoring service describing the exact nature of the event. This enables the monitoring service to perform the required action. Monitoring service notification can be implemented through either regular telephone cellular communication or IP network.



Caution:

Remember that no security system can prevent emergencies. This system is only intended to alert you in case of an emergency and should not take the place of prudent security practices or life and property insurance.

Follow Me Messaging

When an alarm or event, the system can initiate a report message of up to 16 predefined designated destinations using a voice announcement, SMS, smartphone app, or email to express the active event.

SMS Example:

Security System:
21/01/2011
Intruder Alarm
Partition 1
Entrance



Email Message Example:

Subject: Alarm Security Message: Intruder Alarm
System Name: John's Residence
Event: Fire Alarm, Zone 5, Entrance door
Time: 01 April 2011; 16:12
Partition: Partition 1, First floor
Service Contact: Monitoring Station 01, 03-5676778

Your installer defines the type of reporting to a Follow Me destination. Consult your installer for the report type for each destination.

The definition of the telephone number or Email address for each destination is defined by the grand master (see page 33).

Notes:

- Voice messaging requires using the LightSYS™2 voice module. This module also enables the LightSYS™2 to announce various local messages to residents.
- SMS messaging requires the use of the LightSYS™2 GSM/GPRS module.
- Email messaging requires the use of the LightSYS™2 IP module.

LCD Status Display

The LCD status display will vary depending on the number of partitions in your system. If your system is defined with only one partition, the LCD displays the partition name, time and date.

If your system has two or three partitions, the LCD displays the system name, date, time and the status of each partition. A status letter represents the partition's status, as follows:

A: Partition Armed

N: Partition Not Ready

L: Partition in Alarm

S: Partition Stay Armed

R: Partition Ready

LCD Blank Display

If defined by your installer, two minutes after the last keypad operation the keypad will be disabled and the following display will appear on the LCD:

Enter code:

To release the keypad and return to normal operation mode press: [CODE] + .

Note:

During blank display mode the Ready LED indicates a trouble in the system.


System Tones

In addition to the visual indications provided by your keypad(s), your system is designed to produce audible annunciation after certain events. Depending on the circumstance, such sounds may be made by your system's keypad(s) or sounders (for example, a siren or bell).

Note:
If defined by your installer, internal bell annunciation can be generated to accompany any of the keypad sounds.

Event	Keypad Sound	Internal Bell	External Siren
Intrusion Alarm	Rapid beeping	Rapid beeping	Rapid beeping
Fire Alarm	Rapid beeping	Rapid beeping	YES (staggered)
Keypad Police Emergency	No sound (1)	No sound (1)	No Sound (1)
Keypad Emergency / Medical	A momentary chirp	No sound	No sound
Arming or Disarming	No Sound	System is armed: 1 chirp System is disarmed: 2 chirps (Keyfob) Disarm after alarm: 4 chirps (Keyfob)	System is armed: 1 chirp
Confirm Operation	A one-second tone, if completed correctly	No sound	No sound
Reject Operation	Three rapid error beeps, if incorrect (2,3)	No sound	No sound
Entry Delay Countdown	Slowly repeating tones until the entry delay time period expires (2)	No sound	No sound
Exit Delay Countdown	Slowly repeating tones until the exit delay time period expires (2)	No sound	No sound
Chime Sound	2 second buzzer beep (4)	No sound	No sound

Notes:

1. Based on decisions made at the time your alarm system installation, keypads may beep during this type of alarm.
2. Keypad beeps may be disabled at the user's discretion, see Buzzer On/Off, page 41.
3. Press  for two seconds to stop the fault beeps
4. Any intrusion zone, if selected for the chime feature, will, when violated during the disarm period, cause the keypad to annunciate the event. The chime can also be disabled when not required.

Chapter 2 Arming and Disarming

The following chapter describes how to operate your LightSYS™2 locally from the LCD keypad. For system operation from other accessories, refer to the instructions supplied with the product.

As a user of your security system, you'll mostly be concerned with the keypad.

The LightSYS™2 LCD keypad is the primary system interface. Each keypad in your system reports its status via its LCD icons, as described below. Through its keys, you can enter commands to arm and disarm the system, bypass intrusion zones, report emergencies, and more, as described in the subsequent chapters of this manual. For detailed information regarding the keypad interface, refer to the instruction supplied with the keypad.

Notes:

1. There are two types of LCD keypads, with and without proximity for non-contact arming and disarming.
2. Each keypad in the system is assigned to a particular partition, meaning that commands entered in a keypad are implemented only in the partition to which it is assigned. For example, pressing the Quick Arm key on a keypad assigned to partition 1 arms only partition 1

Arming your system

Arming your system causes the intrusion detectors to trigger an alarm when violated. You can arm your system by code arming, in which you need to use your user code, or you can use quick arming (without using a code).

Note:

If during code setting you enter a wrong user code, the keypad produces three short beeps. Simply re-enter the correct sequence.


Remember, fire protection and the protection offered by the keypad's emergency keys are always armed and always available (if authorized by your installer).

Before arming the system:

1. Verify that the ✓ (ready) icon is lit or flashing indicating that system is READY to be armed.
2. Make sure that the system includes no violated zones and is ready to be armed.
3. If the system is NOT ready to be armed, secure or bypass the violated zone(s) (see page 34), and then proceed.


Arming and Disarming

Notes:




- If you are unable to arm the system, press  to view system messages.
- If defined by your installer, your system can be defined to accept force arming. This definition arms the system regardless of open zones when using a keyswitch or automatic arming. Note that force arming the system results in leaving partition(s) unsecured.
- If defined by your installer, it might be required that all troubles in the system should be confirmed to enable the arming operation.

Your **LightSYS™2** supports the following kinds of arming:

Away (Full) arming

Away arming () prepares all of the system's intrusion detectors to activate an alarm if violated, and is used when leaving the premises. Once you have armed the system, exit via the designated final exit door.


To fully arm your system:

1. Verify that the system is ready to be armed.
2. Enter your user code followed by  or hold the tag close to the keypad's keys.
3. Leave the premises and close the door. The keypad beeps and the  icon flashes while the system counts down the exit delay time period.
4. When the exit delay time period has expired, the  icon lights steadily.


Note:




If defined by your installer, system sirens can sound one chirp, indicating that the system is armed.

Stay (Home) arming




Stay arming () activates only perimeter detectors (as defined by your installer), enabling individuals to remain inside and move about the premises while the system is partially armed.

To stay arm your system:

1. Verify that the system is ready to arm.
2. Enter your user code followed by .

3. During the exit delay time period:
 - the keypad beeps
 - the  icon flashes
 - the  icon lights indicating that the interior zones are being bypassed.
4. When the exit delay time period has expired, the  icon lights steadily.

Notes:



1. Press   to cancel the Entry Delay time period for the current STAY arming.
2. Press  during the exit delay time period to silence the keypad beeps.

Partition arming




A key **LightSYS™2** advantage is its ability to divide the system into up-to-four partitions. Each partition can be managed as a separate security sub-system, that is, armed and disarmed individually, regardless of the condition of the others



Partitions can be armed or disarmed one at a time, or all at once, and each partition can be armed as stay or away. Only users who have been defined to operate multiple partitions can operate more than one partition and simultaneously arm/disarm all partitions.

To arm specific partitions:

1. Verify that the system is ready to arm.
2. For away arming enter your user code followed by  or hold the tag close to the keypad's keys. For stay arming, press .
3. Select the number of the partition you want to arm.

Notes:

If your user code is assigned to more than one partition, use the  or  keys to select the required partition(s) and press . Select "0" to arm all partitions assigned to a code.

4. Press  / Present Tag (For away arm) or press  (stay arm) to arm the selected partition(s).
5. Repeat the above steps to arm additional partitions

Arming and Disarming

Examples:

- To away arm partition 3 with user code: 1234:

1-2-3-4  3  or 1-2-3-4 [] 3 []

- To arm all partitions:

1-2-3-4  0 

- To arm partitions 3 and 4:

1-2-3-4  3 4 

- To arm partition 3 in stay mode:

1-2-3-4  3 

Notes:





Keypads and Partitions — Each keypad is assigned to different partition(s). The grand master and the manager (with access to all partitions) can use any keypad to access any partition. Other users can use only designated keypads.

Common Zones — Partitioned systems have to share common zones. For example, a shared front door to two family houses must be available to both families and is therefore shared between them.





A common zone(s) is armed only if all partitions sharing the zone(s) are armed. The common zone(s) is disarmed if any of the partitions, to which the zone(s) is assigned, are disarmed.

If the system is defined to work in area mode, the common zone will be armed if any partition sharing the zone is armed. The common zone will be disarmed if all the partitions sharing the zone are disarmed.

Group Arming

Group arming enables you to arm a number of zones within a partition, using the function keys , , , . Ask your installer about group definition in the system. Each partition can be defined with up to four groups.











To arm a group (if the system has one partition):

1. Verify that the system is ready to arm.
2. Enter your code, followed by pressing for two seconds the key for the corresponded group you want to arm (A , B , C , D ). The selected group is armed.

For example, to arm group C, enter: [Code] [ for two seconds].

3. To arm another group, repeat the above steps .

To arm a group (if your user code is assigned to more than one partition):

1. Verify that the system is ready to arm.
2. Enter your user code, then the group letter (, , , ) , then the partition number, and the group letter again (, , , ) .
For example, to arm group C, enter:
[Code] [ for two seconds] [Partition No] [ for two seconds] .
3. To arm another group, repeat above steps .




Note:

If your system supports Quick Arming, press the function key for two seconds corresponding to the group(s) you want to arm. The selected groups are armed.

Arming With Troubles in the System

If required, and defined by your installer, all troubles in the system may require confirmation to enable the arming operation.

When trying to arm the system with troubles, the display will show the system troubles.




Scroll through the list of troubles using the  key. At the end of the list the following question will appear: « Override Trouble? » Use the  key to toggle the option to Y and press .

Keyswitch Arming

If your system is equipped with a special keyswitch, it can, with the twist of a key, be toggled through arm (away) and disarm modes.

Arming in Blank Display Mode

To perform arming while the system is in blank display mode:

1. Release the keypad by pressing [CODE] + 
2. Within 2 minutes time press:
 For away arming
 For stay arming

Arming and Disarming

Disarming your system

Disarming your system causes the detectors not to trigger an alarm when violated.


Disarming deactivates the partitions assigned to the specified user code.

You can disarm your system by code, for which you need to use your user code or a proximity tag.

When you enter the premises, the entry delay count-down period begins. You must disarm the system within the entry delay period to prevent it from triggering an alarm. The disarming operation will be followed by a local message announcement (if defined).

LightSYS™2 disarming varieties include the following:

Full Disarming

1. If outside the premises, open an "entry" door. The keypad(s) beeps, indicating that the entry delay time period has begun.
2. Before the entry delay time period expires, enter your user code followed by  or present the proximity tag.



Note:

1. If you make a mistake entering your user code, the keypad produces three short beeps. If so, simply re-enter the above sequence correctly.
2. If defined by your installer, system sirens sounding two siren chirps indicate that the system is disarmed.







Partition Disarming

Partition disarming enables you to disarm individual partitions within an armed system.

To disarm specific partitions:

1. Enter user code followed by  or present the proximity tag.
2. Select the partition number (1-4) OR- to disarm all partitions at once, select 0.
3. Press  to confirm. A confirmation message will be displayed for several seconds.
4. Repeat the above steps to disarm other partitions.







Examples:

1. To disarm partition 3 with code 1234: 1-2-3-4  3 .
- To disarm ALL partitions: 1-2-3-4  0 .
- To disarm partitions 3 and 4 with a tag: 1-2-3-4  3 4 .

Disarming after an Alarm

If an alarm has occurred, it will be indicated by the keypad. Once the cause of the alarm has been established the system must be reset.

To disarm the system after an alarm:

1. If outside the premises, open an "entry" door. The keypad(s) beeps, indicating that the entry delay period has begun.
2. Observe the keypad. If the  icon is flashing, and the display shows the activated partition, an alarm activation has occurred. Pressing the  key will show the activated partition and zone.
3. Hold the tag close to the keypad's keys OR enter your user code and press . If an alarm occurred:
 - a) The  icon will flash
 - b) The sirens will sound four siren chirps, indicating that an alarm occurred in the system.
 - c) If your system is equipped with the voice module, an announcement message will be broadcast: "Alarm occurred in the system".
4. Scroll through the list of alarm zones. To exit the alarm memory mode before the timeout has expired, press  (which will clear the alarm memory) or  (which will not clear the alarm memory)
5. If required, proceed to "Resetting after an alarm" (see below).


Note:

If an alarm occurred in the system, it is recommended to leave the premises. Only after police investigation should you consider that the burglar is no longer on your premises and you can re-enter. In special cases (if programmed by your installer) arming the system after an alarm might require a technician code. On the LCD, a Not ready - technician reset message may appear. For more information, consult with your installer.

Arming and Disarming





Important:

If the alarm was caused by a tripped smoke detector(s), the keypad's **Fire**  indicator will remain lit, providing an indication that the fire system must be reset before it will be capable of detecting subsequent infractions. Furthermore, until it is reset, you will be prevented from setting your system.

To reset a smoke detector, press  > User Code >  > Activities >  > Advanced >  > Switch Auxiliary > .

Note: You may need to perform this procedure several times in order to prevent the smoke detector(s) from re-detecting any remaining smoke

Press   to exit the user functions mode.

Resetting after an alarm




Your installation company can configure the reset of the system to a normal operation mode to require the intervention of your monitoring station or installer. In this case, after an alarm condition, the system will be regarded as not ready and the display will show a Call Installer message.

Consult your installer regarding whether your system reset mode is Remote or Installer.







Note:

Before attempting to reset your system ensure that the system is disarmed.

To remotely (anti-code) reset after an alarm

1. Press  key while the Call Installer display is on will enter you to the Anti Code section.
2. Press  to enter the Anti Code option.
3. Call your monitoring station (MS) or installer and quote the RANDOM CODE displayed on your keypad. The MS or installer will give you a return Anti-Code.
4. Enter this Anti code followed by  to reset the system.

To locally (from the keypad) or remotely reset your system (by your MS or installer)

1. Press  Code  Activities  Config SW  CS Connect  Via GPRS/IP? [if both GPRS and IP are available, you must select which]. Press  to confirm
2. Done is displayed. A one hour time window is opened for the installer to program user functions and be able to reset your system.

Duress Disarming

If you are ever coerced into disarming your system, you can comply with the intruder's wishes while sending a silent duress alarm to the monitoring station. To do so, you must use a special duress code, which when used, disarms the system in the regular manner, while simultaneously transmitting the duress alarm. Confirm with your installer which of the user codes is defined as a duress code:

Note:

Under no circumstances must the duress code be used haphazardly or without reason. Central stations, along with police departments, treat duress codes very seriously and take immediate action.






Disabling a Fire Alarm (Switch Auxiliary)

Unsetting the fire alarm interrupts the power supplied to the system's smoke detector(s) for a predetermined interval, thus resetting and "readying" them for subsequent alarms.

Note:

You may need to perform this procedure several times in order to prevent the smoke detector(s) from re-detecting any remaining smoke.

To disable a fire alarm

1. Press  and enter your grand master code followed by .
2. Using the arrow keys, scroll to the option **Activities** and press .
3. Scroll to **Advanced** and press .
4. Scroll to **Switch AUX** and press .
5. The fire alarm is disabled for a predefined amount of time.

Arming and Disarming

Additional Arm/Disarm Capabilities

Automatic Arm/Disarm

The LightSYSTM2 has the ability to define automatic system arming at a predefined time of a day. An Arm/Disarm program automatically arms and disarms the system during your required time intervals. When defining the automatic arming/disarming program, you need to define the following parameters: Partition, Arming Mode (Away/Stay), Time, and Label.

Arm /Disarm from your Wireless Keyfob

The system can be armed using a wireless keyfob (If equipped with a wireless module expansion). For detailed information regarding the keyfob operation consult with your installer .

Remote Arm/Disarm Using a Phone



If your LightSYSTM2 is equipped with the voice module you can perform arming/disarming operations and operate the system from a remote touch-tone phone by initiating a telephone call to or from the system and interacting with voice menus that guide you through your required remote operation. For detailed information refer to the 5IN1545 LightSYS Voice Module Instructions.

Emergency Alarms

Your keypad provides three sets of emergency keys, which can be pressed whenever the police, fire department, or auxiliary assistance is required.



Police Emergency



Pressing   simultaneously, and for at least two seconds, activates a police emergency alarm (panic alarm).



Fire Emergency



Pressing   simultaneously, and for at least two seconds, activates a fire emergency alarm.

Auxiliary Emergency





Pressing   simultaneously, and for at least two seconds, activates an auxiliary emergency alarm.

The resulting annunciation, along with other system sounds is configurable. If your system has been programmed to do so, it will communicate any or all of these alarms to the station monitoring your installation. System programming also determines whether these emergency alarms are audible and/or capable of being communicated to the monitoring station.






Chapter 3 User Functions and Settings

Your LightSYS™2 comes with a variety of selectable user functions that become available when you enter the *User Functions* mode. This chapter describes in detail the most frequent user functions and also lists the complete menu of user functions.

To enter the *User Functions* mode, press  and enter your code followed by .

To exit the *User Functions* mode and return to *Normal Operation* mode, press   quickly.

When using the keypad during the programming mode use the following table to familiarize yourself with the functionality of the keys:

Function	Sequence
	Exits from the current menu
	Terminates commands and confirms data to be stored
	Used to browse through the menu; Scrolls up a list or moves the cursor
	Changes data
	Numerical keys are used to input the numeric codes that may be required for arming, disarming, or used to activate specific functions

User Codes

To perform many of the **LightSYS™2** functions, a security code (often called a user code) must be input. **LightSYS™2** can support up to 16 different user codes. User codes may have variable lengths of up to six digits.

Each individual using the system is assigned a user code, which, in turn, is linked to an authority level. Those with a "higher authority" have access to a greater number of system functions, while those with a "lower authority" are more restricted in what they may do.

LightSYS™2 supports up to nine authority levels.

Notes:

Consult with your installer to configure authority levels.

Authority Levels







Level	Description
GRAND MASTER	All operations for all partitions. There is only one grand master code in the system, and it is designated as user index number 00. This code can be changed by the installer or the grand master.
Notes:	
Your LightSYS™2 was given a grand master code of 1-2-3-4 during manufacturing. RISCO advises that you modify this code to one that is unique and personalized as herein described, unless your alarm company has already done so.	
MASTER	All operations but only for designated partitions. The user holding the master code can change the master code and the codes of all authority levels lower than master. LightSYS™2 supports an unlimited numbers of master codes.
USER	Only basic operations for one or more partitions.
DURESS	Like USER except that when disarming the system a duress alarm message is sent to the monitoring station.
ARM ONLY	Arming one or more partitions. Arm only codes are useful for workers who arrive when the premises are already open but, because they are the last to leave, are given the responsibility to close and secure the premises at the day's close.
CLEANER	Used only for one-time arming and disarming, after which the code is automatically erased and should be redefined. This code is typically used residentially for maids, home attendants, and repairmen who must enter the premises before the owner(s) arrive.
UNBYPASS	Basic operations to one or more partitions without the ability to bypass zones.
GUARD	Typically used to enable a guard to disarm the system for a predefined amount of time. After this period, the system is automatically armed again.
UO ONLY	Typically used to enable the operation of a device controlled by a utility output (UO) (for example, a door). These codes are used only to operate a utility output.

Setting / Changing User Codes

The user assigned the grand master authority level can change all user codes but cannot view the digits in the user code fields. Users with other authority levels can only change their own codes. The system must be disarmed in order to set or change user codes.


Note: User codes can also be defined from the web application

To set/change a user code:

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Codes/Tags and press .
3. Scroll to Define and press .
4. Select the user index number and press .
5. Select Edit Code and press .

Note:

In the **LightSYS™2** system, the User Index number range is from 00 to 15. (00=Grand master)


6. Enter the new code followed by .
If successful, a single confirmation beep is sounded; if not, three quick error beeps are sounded
7. Repeat the above steps for additional codes until you have completed your list

Deleting User Codes

At times, you may want to completely delete a user code. Note that it is impossible to delete the grand master code (although it can be changed).

The system must be disarmed in order to delete user codes.

To delete a user code:


1. Follow steps 1-4 of the previous procedure (See *Setting/Changing User Codes*)
2. Scroll the menu to the option Delete and press .
3. If successful, a single confirmation beep is sounded; if not, three quick error beeps are sounded.
4. Repeat the above steps for deleting additional codes.


User Functions and Settings

User Code Labels

You can rename the labels that identify users by changing the default labels (User 1, User 2, and so on) to the names of the users themselves.

To enter a user label:

1. Follow steps 1-4 of the previous procedure (See *Setting/Changing User Codes*)
2. Scroll to Edit Label. Press .
3. Use the keys on the keypad to produce characters according to the table below.
Pressing a particular key toggles between the characters available for that key:

Key	Data Sequence
1	1 . , ' ? ! " - () @ / : _ + & * #
2	2 a b c A B C
3	3 d e f D E F
4	4 g h i G H I
5	5 j k l J K L
6	6 m n o M N O
7	7 p q r s P Q R S
8	8 t u v T U V
9	9 w x y z W X Y Z
0	0
	Use these keys to toggle forwards and backwards through all the available characters.

Proximity Tags

The proximity keypad enables you to use a proximity tag to arm and disarm the security system or to activate and deactivate home appliances and utilities, such as heating and lights.






Notes:

- Users can define or delete their individual proximity tags. The grand master can define or delete **any** user's tag.
- Each proximity tag can be assigned to only one user.

Adding a New Proximity Tag


You can add a new proximity tag for each user in the system, as required.

To add a new proximity tag:

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Codes/Tags and press .
3. Scroll to Define and press .
4. Select the user to which you want to assign the proximity tag and press . Each proximity tag can be assigned to only one user.

Note:

A display of (****) indicates that a user has already been assigned to a specific proximity tag.

5. Scroll to (Re)write Tag. Press .
Within 10 seconds, approach the proximity tag at a distance of 4 cm. from the front of the keypad bottom. The keypad automatically reads the proximity tag and saves it into the system's memory.
Once the proximity tag has been successfully recorded, a long confirmation beep sounds, and a confirmation message is displayed.
If the proximity tag is already stored in the system's memory, the following message is displayed:
USER TAG ALREADY IN MEMORY



Notes:

- Once a proximity tag is recognized, it will be functional from all keypads.
- The programmed proximity tag has the same permissions that are defined for the specified user code.
- If a user is defined as having the Cleaner security level, then the proximity tag can operate only if a security code was previously defined for that user.




User Functions and Settings

Deleting a Proximity Tag





Deleting proximity tags can be performed in either of two manners:

-  **By user number:** Use this option to delete a tag for which the user is known
-  **By tag:** Use this option to delete a tag for which the user is not known

To delete a proximity tag by user serial number:

1. Follow steps 1-4 of the previous procedure (See *Adding a new proximity Tag*)
2. Scroll to Delete Tag and press . The following question appears:
Delete, Are you sure?
3. Toggle Y or N by using the  key and then pressing . If you select Y, the following confirmation message is displayed:
USER XX: TAG DELETED









To delete a proximity tag by user tag:

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Codes/Tags and press .
3. Scroll to Del By Tag and press .
4. Within 10 seconds, approach the proximity tag at a distance of 4 cm. from the front of the keypad bottom. If the proximity tag was deleted, the following confirmation message is displayed: USER TAG XX DELETED.
If the system does not recognize the proximity tag, the following message is displayed: TAG NOT DEFINED IN MEMORY.

Setting and Changing System Time and Date

The correct time and date must be set to ensure proper operation of LightSYS™2.

To set/change the system time:










1. Press  and enter grand master code followed by .
2. Using the arrow keys, scroll to the option Clock and press .
3. The display will show Time and Date. Press .
4. Enter the correct time in 24-hour format and date. For entering the date use the  keys to move the cursor and the  /  key to toggle among the choices.
5. Press  to save your settings.



Setting Follow Me Destinations







In the case of an alarm or event, the system can initiate a phone call to a designated telephone, send an SMS/email and employ unique tones or messages to express the active event or perform push notification to your smart phone application. Consult your installer for configuring event reporting to a Follow Me destination.

Note:
When the LightSYS™2 is connected in cloud mode (depending on system settings) the system may only be able to send emails or push notification to Smartphone applications.

To enter/edit a Follow Me destination:

- 1. Press  and enter your code followed by .
- 2. Using the arrow keys, scroll to the option Follow Me and press .
- 3. Select the Follow Me index number you want to define and press .
- 4. The display will show Destination. Press .
- 5. Enter the phone number, including the area code (if required) or email address. To enter an email address, use the  and  keys to obtain the required characters and use the  and  keys to move to the required character position in the address.


Note
If required, when defining a telephone number (maximum 32 digits), include the special functions described below to achieve the related effect. You can press the  or  keys to toggle to the required character.

Function	Sequence	Results
Stop dialing and wait for a new dial tone	 1	W
Wait a fixed period before continuing.	 2	,
Switch from Pulse to Tone (or from Tone to Pulse).	 3	C
Send the DTMF * character.	 7	*
Send the DTMF # character		#
Delete numbers from the cursor position		[*] @

simultaneously

When done with your complete entry, press  to store it.

Bypassing zones

When an intrusion zone is not secured, the keypad's **Ready/**  icon will not light, nor can the system be readily armed. Bypassing a zone enables you to arm a partition even if a zone within that partition is open (not secured).

You may want to bypass a zone when access is needed to one zone in an otherwise protected area, or to cause the system to temporarily circumvent a zone containing damaged wiring until repairs can be made.





Warning:








A bypassed zone may reduce the system's security capability.

To view Not Ready zones:



Before performing the following procedure, identify the violated zone(s) as follows:

1. Enter your user code followed by .
2. Scroll down with the  key to view all "not ready" zones. The LCD only displays "not ready" zones that belong to the user code that was entered.

To change a zone's bypass status:

1. Press  and enter your code followed by .
2. Scroll to **Activities** and press .
3. Select **Bypass** and press .
4. Select **Zones** and press .
5. For bypassing a zone only for the next system arming select **One Time Only**. If you want to bypass the zone permanently select **Permanent Byp**.
6. Scroll down the list of zones and using  to select the zones to be bypassed.
7. To confirm press .

Notes:

- You can access the one-time bypass option in a quick way by pressing [Code][].
- Zones defined for **One Time Only** bypass are automatically un-bypassed when the system is armed and then subsequently disarmed.
- The  icon turns off when arming in *away* mode.







Scheduling Weekly Programs

The LightSYS™2 enables you to automate some system operations. Each program can be defined with up to two time intervals per day, during which the system automatically performs one of the following functions:


- **Automatic Arming/Disarming:** This program automatically arms and disarms the system during your required time intervals.
- **Automatic UO Activation:** A UO (home appliance) activation program automatically activates and deactivates UOs during your required intervals.
- **User Limitation:** A user limitation program automatically prevents certain users from disarming the system during specified time intervals.

Up to four scheduling programs can be defined. Use the table in *Appendix C – Scheduling Tables* to define your date.

Automatic Arming/Disarming

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Clock and press .
3. Using the arrow keys, scroll to the Scheduler option and press .
4. Using the arrow keys, scroll to the Weekly option and press .
5. Select the Schedule program index number.
6. Select Arm / Disarm and press .
7. Follow the LCD display messages that will guide you through the programming procedure. When defining Arm/Disarm program, you need to define the following parameters: Partition, Time Schedule, Arming mode, and Label


Notes:

- When defining the Day/Time intervals for each day of the week you can select 8 All to set the same time intervals for every day in the week.
- Use  key to enter Y when requested. For example when defining a partition that will be automatically armed and disarmed
- Leave the time at 00:00 if you do not want to perform the automation during the current interval for the current day

Automated Output Operation

A UO (home appliance) activation program automatically activates and deactivates UOs during your required intervals. In each program, you can define four UOs to operate simultaneously. When defining a UO activation program, you need to define the following parameters: UOs, Time Schedule, Vacation, and Label

User Functions and Settings

1. Repeat stages 1- 5 of the Arming/Disarming schedule programming procedure
2. Select UO On/Off and press .
3. Follow the LCD display messages that will guide you through the programming procedure.

Note:


The Vacation option for the UO scheduling program defines the way in which the group of UOs are activated during a vacation:

N: During vacation, UOs are activated in the same way as defined in the time windows of the week.








Y: UOs are activated during the vacation according to the time schedule defined in the next step (vacation definition).

User Limitation Program

A user limitation program automatically prevents certain users from disarming the system during specified time intervals. By default, all users of the system operate without this limitation. When defining a user limitation program, you need to define the following three parameters: Users, Time Schedule, and Label

1. Repeat stages 1- 5 of the Arming/Disarming schedule programming procedure
2. Select User Limit and press .
3. Follow the LCD display messages that will guide you through the programming procedure

Quick Activation/Deactivation of a Weekly Program

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Clock and press .
3. Using the arrow keys, scroll to the Scheduler option and press .
4. Using the arrow keys, scroll to the Schedule Enable option and press .
5. Select the Schedule program index number.
6. Use the  key to toggle activate /deactivate and press .

Macro Keys





Programming Macro Keys

LightSYS™2 enables the installer or grand master to record a series of keystrokes and assign them to a macro. When the macro is invoked, the recorded commands are executed from beginning to end. Up to four macros can be programmed to a system using the LightSYS™2 keypad or the LightSYS™2 Configuration Software.

Notes:





- The default function for all function keys is group arming, as described on page 20. If group setting is used, this option is not available.
- Macros cannot be programmed to perform disarming commands.





Before programming a function key, it is recommended to note the keystroke sequence. These keys will be entered in the form of characters in step 5 (below) of the procedure for programming the macro key.

For example, to arm partitions 1 and 2 in a 3-partitioned system, you would press the following keys in step 5: [Code]    

This example requires the following sequence of characters: 1234r12r





To program a Macro:

1. Press  and enter your code followed by .
2. Using the arrow keys, scroll to the option Macro and press .
3. Select a macro (A, B, C, or D) and press .
4. Press A (or the macro key you selected in step 3) for five seconds to start the recording sequence
5. Enter the sequence of characters according to the following table:

Character	Represents	
0-9	The Numerical keys from 0 to 9.	
A-D	The macro keys from A to D (obtained by depressing the 1,2,3 or 5 key for five seconds).	
*	The  key.	r  Away (full) arm
#	The  key.	s  Stay arm
a-d	Group A to D	

6. When you have finished entering the series of characters, ensure that the cursor is placed in the field after the last character in the series, and press A (or the function key you selected in step 4) again. The series of characters is saved and assigned to the selected function key

Activating a Macro

Press  /  /  /  on the keypad for two seconds to activate the macro A/B/C/D respectively.

Parking Control with LightSYS™2 Gate Control Keyfobs









If your system is equipped with a wireless expander it can support up to 200 keyfobs that can be used for controlling two outputs for gate and parking control. These keyfobs are additional to the keyfobs that can be used to control the security applications of the system. Each keyfob had a dedicated button to support each output.

The grand master or the installer can control the management of these keyfobs





Notes:

The following procedures are relevant only for stand-alone keyfobs. The keyfobs that control the security system can be defined and programmed only by your installer. Your installer must define the outputs and the way they will operate so you can perform the following procedures.




Assign New Keyfob

1. Press  and enter Grand Master code followed by .
2. Using the arrow keys, scroll to the option Stand Alone KF and press .
3. Select the receiver that you want to assign the keyfob to and press .
4. Using the arrow keys, scroll to the New Keyfob option and press .
5. Press the  key to start the keyfob registration mode.
6. Press the keyfob  key for 3 seconds.
7. Repeat step 6 for additional keyfobs. When finished press  to exit registration mode.

Delete a keyfob




1. Follow steps 1-3 of the previous procedure (See *Assign New Keyfob*)
2. Using the arrow keys, scroll to the Delete Keyfob option and press .
3. Press the  key to start the keyfob erase mode.
4. Press the keyfob  key for 3 seconds.
5. Repeat above steps for additional keyfobs. When finished press  to exit Erase mode

Delete All keyfobs

1. Follow steps 1-3 of the previous procedure (See *Assign New Keyfob*)
2. Using the arrow keys, scroll to the **Delete All Keyfobs** option and press .
3. Use the  key to toggle to Y and press .

Change keyfob buttons that controls the outputs

By default, button 3 (small round key) of the keyfob controls output 1 and button 4 (egg shape) controls output 2. This can be changed for all the keyfobs that are already assigned to the wireless receiver.

1. Follow steps 1-3 of the previous procedure (See *Assign New Keyfob*)
2. Using the arrow keys, scroll to the **UO Buttons** option and press .
3. Use the  key to toggle to Y and press . This will replace button 3 to button 1 and button 4 to button 2.

Complete List of User Functions

This section lists the complete menu of user functions.
The following table shows full Keypad Operations according to users.
√ : User is able to perform this function (GM=grand master or master, U=user, and In.=installer)
- : User is unable to perform this function

Note:
Although these functions are in the User Functions menu, you can ask your installer to program some of them for you

Menu Structure	GM	U	In.
-----------------------	-----------	----------	------------

Activities

<i>Bypass</i>	√	√	-
---------------	---	---	---

Zones: Provides the ability to bypass any of the system's intrusion zones as described on page 34.

One Time only— Single bypass for the next arming.

Bypass Reset— Removes any bypass(es) previously placed on an intrusion zone(s).

Bypass Recall— Recalls the most recent zone bypass(es).


Permanent Bypass: Bypasses (and reset bypassing) any of the system's intrusion zones permanently. This feature is different from regular zone bypassing. While in regular bypassing, the zone returns to be Not Bypassed after it is armed, in permanent bypass the zone remains bypassed until its status is changed.




Tamper bypass: Provides the ability to bypass bell or box tamper conditions. If Bypass Tamper is selected and a tamper condition occurs, the tamper LCD icon (🔔) will light, there will be no alarm, no indication to the Monitoring Station and no record in the event log.
Note that this feature should be enabled by your installer.

<i>Outputs</i>	√	√	-
----------------	---	---	---

Allows user control of previously designated external devices. Consult with your installer as to which outputs can be activated. If no outputs are defined, this option will not appear on the list.



Menu Structure	GM	U	In.
Keypad Sound	√	√	√
<i>Chime</i>			
<i>Keypad Chime</i> — Allows to control (turning ON and OFF) of the current keypad's internal sounder for any function involving the Chime feature.			
<i>Partition Chime</i> — Allows to control (turning ON and OFF) of all keypad buzzers in the partition for any function involving the Chime feature.			
<i>Buzzer On/Off:</i> Used to control (Turning ON and OFF) the current keypad's internal buzzer during both Entry and Exit Delay time periods and all fire and burglar alarms.			
Anti Code	√	√	-
Some systems (defined at the time of their installation) are not ready to be reset after an alarm or tamper condition. To restore the system to normal operation mode, an installer code or anti-code must be entered. Entering the code supplied by the technician at this location will restore the system to the normal operation mode.			
Configure SW	√	-	-
<i>Enable CS:</i> Each time this function is enabled, your alarm company may subsequently gain a single remote access to your system to make any required programming changes.			
<i>CS connect (Initiate Call):</i> Enables to establish communication between your system and your alarm company to allow them to perform a remote programming operation on your system using the remote configuration software. Select the communication method (IP or GPRS) as guided by your installer.			
Prepaid SIM	√	-	-
<i>Check Credit:</i> Use this function to receive information by SMS or voice of the credit level in your prepaid SIM card. For more information consult your installer.			
<i>Reset SIM:</i> After charging a prepaid SIM card, the user has to reset the SIM expire time manually. The time period duration for expiration is defined by your installer.			

Menu Structure		GM	U	In.
<p>User call: Use this function to receive the SIM credit level using the voice channel. Upon accessing this option, a dial tone is received and the LightSYS™2 keypad functions as a GSM telephone. You can dial and listen to messages as with a regular telephone. To end the call press the  key.</p>				
<p>Notes:</p> <ul style="list-style-type: none">• The outgoing call will always be executed through the GSM channel.• Talking is not optional during the call.• This option can be used to get any provider information.• The call can be established to any phone number				
<p>Advanced...</p>		√	-	√
<p>Switch AUX: Interrupts the power supplied to the system's smoke detector(s) for a predetermined interval, thus resetting and "readying" them for subsequent alarms</p>				
<p>Void Report Programming</p>		√	-	√
<p>Some protocols have a report code to the monitoring station for entering and exiting the installer programming. To avoid the entering report and save time, this function postpones the report for two minutes during which the installer can enter the programming menu and no report will be made.</p>				
<p>Service Mode</p>		√	-	√
<p>Used to silence an alarm initiated by any tamper for a <i>Service Time</i> period specified by your installer. Use this option when replacing the accessory battery.</p>		√	-	√
<p>Overload restore: Use this option to restore overloading of the system's switched power supply. If the overload condition is still present, disconnect all loads from AUX.</p>				
<p>Follow Me</p>				
<p>Define</p>		√	-	√
<p>Destination: Used to define (up-to-16) Follow Me destinations according to its type: Voice message, SMS or E-mail. For more information refer to page 33.</p>				
<p>Label: Identifying labels for the Follow Me destination. Enter the labels according to the instruction defined for user label on page 30</p>				

Menu Structure	GM	U	In.
Terminate Follow Me	√	-	-
If Follow Me destination(s) were chosen, their operation can be terminated. Use this function when an alarm has been tripped and there is no need to utilize the Follow Me feature.			
Test Follow Me	√	-	√
Used to test Follow Me reporting.			
View			
Trouble	√	√	√
Should be used when the system has detected a problem, which is evidenced by the rapid flashing of the  power icon, as described on page 7.			
Alarm Memory	√	√	√
Displays the five most recent alarm conditions stored by the system.			
Partition Status	√	√	√
Displays the partitions' status, the troubles in the system and all “not ready” zones. Pressing on the  key from the normal operation mode displays the status of the partition to which the keypad is assigned. Pressing the sequence [CODE]  from the normal operation mode displays the status of all the partitions assigned to the user code.			
Zone Status	√	√	√
Allows the display of all system zones and their current status.			
Service Info	√	√	√
Allows the display of any previously entered service information and the system version			
[Sytem Entry Level] Status of current user			
System Version The installed firmware version of LightSYS™2.			
Serial Number The 11-digit number used by the cloud to identify the panel			
Panel ID The 15-digit number used by the end-user for self-registration to the RISCO cloud (See page 2)			

User Functions and Settings

Menu Structure	GM	U	In.
<i>IP Address</i>	√	-	√
Use this option to view the IP address of the LightSYS™2. This option is available only if IP module is defined in the system			
<i>Advanced</i>	√	-	√
MS Test- Use this option to initiate a test message to the Monitoring Station according to IMQ and EN50131 requirements			
Codes/Tags			
<i>Define</i>	√	√	-
Codes: <i>Edit Code</i> — Use this menu to edit user codes in the system. For detailed information refer to page 31. <i>Erase Code</i> — Use this menu to delete user codes in the system			
Proximity Tag: <i>(Re)write Tag</i> — Assigns user codes to proximity tags. For detailed information refer to page 30 <i>Delete Tag</i> — Deletes a proximity tag of the selected user. <i>Edit Label</i> — Assigns labels to users (16 characters long). These labels are presented in the event log.			
<i>Delete By Tag</i>	√	-	-
Use this option to delete a proximity tag when the user of the tag is unknown.			
Clock			
<i>Time & Date</i>	√	-	√
Allows the setting of the system time and dates, as described on page 32. This definition is required for setting the scheduler programming in the system.			
<i>Scheduler</i>	√	-	√

Menu Structure		GM	U	In.
<p>Weekly — Enables you to define up to four weekly programs with up to two time intervals per day, during which the system automatically arms/disarms, activates utility output , or prevents users from disarming.</p> <p>One Time — Enables a one-time operation of automatic Arm/Disarm of the system at a specific time within the next 24 hours.</p> <p>Schedule Enable — Enables you to activate or deactivate predefined schedules.</p>				
<i>Vacation</i>		√	-	√
Enables defining up to 20 holiday periods and the partitions that will be set automatically during the holiday.				
Event Log		√	-	√
Allows the viewing of significant system events including date and time.				
<p>Notes:</p> <p>The events memory cannot be erased.</p> <p>To skip 10 event at a time backward or forward use the  and  keys consecutively.</p>				
Maintenance				
<i>Walk test</i>		√	-	√
<p>Enables to easily test and evaluate the operation of selected zones in your system. Walk test is set for up to 60 minutes. During the last five minutes of walk test mode, the keypad used to perform the walk test will indicate that the walk test period is about to end.</p> <p>Full walk test — The test displays the detected zones and type of detection.</p> <p>Quick walk test — The test displays the undetected zones.</p>				
<i>Keypad test</i>		√	-	√
Momentarily tests the keypad indicators.				
<i>Siren test</i>		√	-	
Activates the squawk sound in the selected siren.				
<i>Strobe test</i>		√		
Activates the strobe light in the selected siren.				

User Functions and Settings

Menu Structure	GM	U	In.
Macro	√	-	√
LightSYS™2 enables the installer or GM to record a series of commands and assign them to a macro. For more information, refer to section page 35.			
Stand Alone Keyfobs	√	-	√
LightSYS™2 enables the installer or GM to assign up to 200 keyfobs that can be used for gate control. For addition information refer to page 38.			

Appendix A – System Troubles

The following table lists possible trouble conditions, their descriptions, and recommended responses.

Trouble	Description	Response
Low Battery	The capacity of the battery is low or missing and needs to be recharged or replaced. Replace rechargeable batteries according to the battery manufacturer.	Contact your dealer.
Loss of AC Power	The commercial power has been interrupted; the system will continue to operate on its standby battery as long as possible. Loss of AC Power will be displayed on the LCD.	Check the connection of the panel's transformer to its AC source. Be sure that power has not been interrupted or switched off.
Auxiliary Failure	The auxiliary power, used to supply electric current to designated devices (e.g. motion detectors, keypads, and smoke detectors), has failed (either form panel or the optional power supply module(s)) .	Contact your dealer.
False Code Trouble	If enabled by your dealer, your system will report a false code as a trouble.	Once the trouble has been displayed (LCD keypad only), it will automatically be removed from the system.
Phone Line Failure	The telephone line used for monitoring station communication is either disconnected or inoperative.	If all premises telephones are operating properly, contact your security dealer.
Bus Failure	A fault has been detected in the wiring supporting system peripherals. The trouble indicates the device with the communication trouble.	Contact your dealer.
Clock Not Set	The system's clock has lost track of the time and/or date.	Set the system's time and date.
Bell Trouble	Trouble has been detected in a bell connected to the main panel or to the power supply expander.	Contact your dealer.
Zone Trouble	A zone has been faulted during the arm/disarm period.	Check the integrity of the indicated zone.
Day Zone Trouble	A zone designated as a DAY ZONE has been faulted during the disarm period.	Check the integrity of the indicated zone.

Appendix B – Glossary

[Terms and Definitions] Understanding the following terms will help you to better manage and operate your system.

Authority Level: Each individual using the system is assigned a user code, which, in turn, is linked to an authority level. Those with a "higher authority" have access to a greater number of system functions, while those with a "lower authority" are more restricted in what they may do. There are nine different authority levels available for users of the LightSYS™2, as described on page 27.

Chime: The chime is a series of three short keypad tones, which can be set up to announce, during the disarmed period, the violation of selected intrusion zone(s). For example, the chime tone can be used to announce the arrival of a customer each time the front door opens. The chime can be disabled or enabled at your discretion.

Configuration Software: Software used by the installer for programming the LightSYS™2 and by the user for operating the system and viewing system status.

Event Log: A list of system events can be displayed on an LCD keypad or uploaded to the monitoring station via the configuration software and printed for further analysis.

Exit/Entry Delay: Your security system must incorporate an entry/exit delay to allow proper entry and exit to and from the premises without causing inadvertent alarms.

Follow-Me Destinations: In addition to the standard event reporting to the monitoring station, the system can send event messages to a designated system user's telephone/email.

Group: A number of zones gathered as one unit to allow partial arming. Each zone can be assigned to any one (or a combination) of four groups (A, B, C or D). Each partition can be divided into a maximum of four groups.

Keyswitch: Your system may also be equipped with a keyswitch, which is useful for simple arming and disarming operations (usually at a remote location).

Monitoring Station: Your system is set up to report alarms to a monitoring station, which is a facility that continually monitors the activities of many security systems (usually via the telephone network) and dispatches the proper authorities.

Partition: One of the LightSYS™2 advantages is its ability to divide any system into a number of partitions. You can think of each partition as a separate security system that can be armed and disarmed individually.

Proximity: A technology that enables a keypad to sense when a proximity key tag is near it. This provides an easy and user-friendly way to arm or disarm the security system.

Tamper: A device that prevents system hardware from being tampered with by triggering an alarm whenever a hardware component is opened.

Trouble Reporting: If required, your security system may also report to the monitoring station any troubles or malfunctions it senses, so that a service call can be made.

User Code: Up to a four-digit or six-digit code that is used to perform many of the LightSYSTM2 functions.

Utility Output (UO): A household appliance. In addition to your system's normal operation, it is possible to place a household appliance or premises lighting under the control of the LightSYSTM2 where it can be conveniently turned on and off automatically, or by user command from any system keypad.

Weekly Schedules: Through the use of the system's built-in clock, it is possible to schedule automatic operations such as arming and disarming, UO activation, and user limitation.

Zone: A single detector, or collection of detectors, usually relating to a certain area of the premises or type of protection. Zones that use devices designed to detect break-ins are called intrusion zones. Another kind of zone may contain one or more smoke detectors. Such zones are called fire zones. An environmental zone typically protects the premises from gas leaks and/or flooding.

Appendix C – Scheduling Tables

Use the following table to define each of the weekly schedules.

Weekly Schedule: _____

Schedule Name: _____

Schedule Type		Parameter Definitions							
Arm / Disarm <input type="checkbox"/>	Partition	1	2	3	4	5	6	7	8
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Arm Mode: <input type="checkbox"/> Arm <input type="checkbox"/> Home <input type="checkbox"/> Group	Select Group: <input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D							
Utility Output <input type="checkbox"/>	1st UO No: _____				3rd UO No: _____				
	2nd UO No: _____				4th UO No: _____				
		Note: For the UO weekly schedule, you can define a separate time definition during vacation.							
User Access Authorization <input type="checkbox"/>	User #	Name		User #	Name				
	Note: You can choose any user in the system.								
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 D – SMS Operation

The **LightSYS™2** enables you to perform remote control operations using simple SMS commands. The following section describes the SMS commands and the response of the system to these commands.

Note: This application is available only if a GSM/GPRS module is installed in your system.

Operation	SMS Message Structure	Example
Full Away Arm	[Code] A	1234A
Home Arm	[Code] H	1234H
Group Arm	[Code][G][Select a one Group A/B/C/D))	1234GA
Full disarm	[Code] D	1234D
Arm by partition	[Code] A [Partition No.]	1234A1
Home Partition Arm	[Code] H [Partition No.]	1234H1
Group Arm by Partition	[Code] G [Select one Group A/B/C/D] [Select partitions]	
Disarm by Partition	[Code] D [Partition No.]	1234D1
Bypass a zone	[Code] B [zone number]	1234B05
Un-bypass a zone	[Code] UB [zone No.]	1234UB05
Activate Output	[Code] UOON [UO No.]	1234UOON1
Deactivate Output	[Code] UOOFF [UO No.]	1234UOOFF1
Change FM number	[Code] FMPHONE [FM serial number] NEW [New Phone No.]	1234FMPHONE 3 NEW0529692345
Get system status	[Code] ST	1234ST
Get last alarm	[Code] AL	1234AL
Get SIM credit level (for prepaid cards)	[Code] CR	1234CR

Notes: SMS commands are not case sensitive (they can contain both capital, small or mixed letters).
A separator between command words is not required, although it is accepted.

SMS Confirmation Message

A confirmation message following a SMS operation is sent to the user, upon request, by adding the letters “**RP**” at the end of the SMS messages listed below.

Example:







1234 A RP - A confirmation message following an arming operation is sent to the user.
Confirmation or Fail operation messages can be assigned to the actions of arming, disarming, bypassing, activating outputs or changing follow me definitions.

Appendix E – System Testing and Maintenance

The LightSYS™2 should be tested once a week. Also, the system should be checked by a qualified technician at least every 3 years. Your weekly test should include:





- System arming • System disarming • Creating an alarm
- Testing the zones in the system through a Walk Test, allowing you to open and then close each protected door and window while listening for the keypad to beep confirming its operation

To perform a Walk Test:

1. Make sure the system is disarmed.
2. Press  and enter your code followed by .
3. Using the arrow keys, scroll to the option Maintenance and press .
4. Select Walk Test and press .
5. Select Full Walk test and press .
6. A beep is heard and the following display appears:
**MAKE WALK TEST
AND HIT ANY KEY**
Walk throughout the protected area and make sure you test every zone in the system. You have 60 minutes to perform the test.
7. When done, press any key. A list of the tripped zones during the walk test appears. Use the arrow keypad's keys to scroll through the list of the zones logged during the test
8. Press  to confirm and exit the walk test mode.

Important Notice

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

-  This guide contains proprietary information belonging to RISCO Group. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the system.
-  No part of its contents may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of RISCO Group.
-  The information contained herein is for the purpose of illustration and reference only.
-  Information in this document is subject to change without notice.

Corporate and individual names and data used in examples herein belong to their respective owners

Standard Limited Product Warranty (“Limited Warranty”)

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

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

RED Compliance Statement:

Hereby, RISCO Group declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. For the CE Declaration of Conformity please refer to our website: www.riscogroup.com.

Contacting RISCO Group

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

United Kingdom

Tel: +44-(0)-161-655-5500
E-mail: support-uk@riscogroup.com

Italy

Tel: +39-02-66590054
E-mail: support-it@riscogroup.com

Spain

Tel: +34-91-490-2133
E-mail: support-es@riscogroup.com

France

Tel: +33-164-73-28-50
E-mail: support-fr@riscogroup.com

Belgium (Benelux)

Tel: +32-2522-7622
E-mail: support-be@riscogroup.com

USA

Tel: +1-631-719-4400
E-mail: support-usa@riscogroup.com

China (Shanghai)

Tel: +86-21-52-39-0066
E-mail: support-cn@riscogroup.com

Israel

Tel: +972-3-963-7777
E-mail: support@riscogroup.com

Australia

Tel: +1-800-991-542
E-mail: support-au@riscogroup.com

RISCO product was purchased from



© 2017 RISCO Group. All rights reserved.

RISCO Group 11/2017

5IN2052 C