A LIFETIME OF SECURITY

WiComm Pro

Model: RW332M

Installation Manual

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 authorized WiComm Pro system installers. No part of this document or its contents may be used for any other purpose, disclosed to any person or firm, or reproduced in any form whatsoever, 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.

Table of Contents

CHAPTER 1: INTRODUCTION 1

MAIN FEATURES AND BENEFITS 1
Robust and Full-Featured System 2
WICOMM PRO ARCHITECTURE 3
Traditional 3
Cloud Communication 3
Parallel Communication 3
Back-up Communication 4
COMMUNICATION CHANNELS 4
GSM/GPRS 4
IP/Wi-Fi 4
MONITORING STATIONS 4
CONFIGURATION SOFTWARE 5
Video Verification with IP Camera 5
Snapshot Follow Event 5
PRODUCT SPECIFICATION 6
SAFETY PRECAUTIONS 7

CHAPTER 2: TYPICAL SYSTEM COMPONENTS 8

CHAPTER 3: DESCRIBING AND USING THE MAIN PANEL 10

WICOMM PRO MAIN COMPONENTS 10
Main Panel LEDs 12
Communication Modules 13
GSM/GPRS 13
IP 13
Wi-Fi 14
Installing Communication Modules 15

CHAPTER 4: INSTALLING THE WICOMM PRO 16

INSTALLING THE MAIN PANEL 16
Mounting Guidelines 16
Wall-Mounting the Main Panel 16

CHAPTER 5: INSTALLER PROGRAMMING 19

PROGRAMMING METHODS 19
Configuration Software 19
Allocating Installer Temporary Keypad 19
Allocating the Customer's Panda/LCD Keypad 21

Accessing the Installer Programming Menu *21*
WIRELESS DEVICE ALLOCATION OPTIONS 22
Quick Device Allocation at the Main Panel *23*
Wireless Device RF Transmissions *24*
Device Allocation using the Wireless LCD Keypad *25*
RF Allocation Method 25
Serial Number Method 25
Allocating Devices with the Configuration Software *26*
RF Allocation 26
Code Allocation 26
Clearing Device Allocation *27*
Clearing a Device Allocation from the Installer Keypad 27
Clearing a Device Allocation with the Configuration Software 27
Clearing All System Device Allocations with the Configuration Software 27
ESTABLISHING COMMUNICATION TO THE RISCO CLOUD 28
IRISCO APP 29
ACCESSING THE WEB APPLICATION 29

CHAPTER 6: PROGRAMMING THE INSTALLER MENUS 30

DESCRIBING INSTALLER KEYPAD BUTTONS 30
ACCESSING THE MAIN INSTALLER MENUS 30
PROGRAMMING MENU 31
System *31*
Timers 32
Controls 34
Labels 44
Sounds 45
System Settings 46
Service Information 47
Firmware Update 47
Picture Server 48
Radio Devices *49*
Allocation 49
Modification 49
Zones 50
Parameters 50
Alarm Confirmation 66
Soak Test 66
Zone Crossing 67
Remote Controls / Key Fobs 68
Wireless One-Way Key Fob Parameters 68
Wireless Two-Way Remote Control Parameters 69
Controls 70
Parent Control 70

Keypads 71
Parameters 71
Controls 72
Sirens 73
I/O Wireless Expander 74
Wired Zones 74
Output Parameters 76
X-10 Outputs 81
Parameters 81
Identification 82
Codes *83*
User 83
Codes: User Codes 83
Parameter 83
Grand Master 84
Installer 84
Guard 84
Code Length 84
DTMF Code 85
Parent Control 85
Communication *85*
Method 85
GSM 85
IP 89
Monitoring Station 92
Configuration Software 99
Follow-Me 101
Define Follow Me 102
Cloud 106
TESTING MENU 108
Main Unit *108*
Zone *109*
Remote Control *110*
Keypad *110*
Siren *111*
GSM *112*
IP Unit *112*
UO Unit *113*
ACTIVITIES MENU 113
FOLLOW ME MENU 115
CLOCK MENU 115
EVENT LOG MENU 116
MACRO MENU 116

Macro Keys *116*
Activating a Macro *117*

APPENDIX A: REPORT CODES **118**

APPENDIX B: INSTALLER EVENT LOG MESSAGES **123**

APPENDIX C: REMOTE FIRMWARE UPGRADE **128**

APPENDIX D: INSTALLER PROGRAMMING MAPS **133**

APPENDIX E: WICOMM PRO CERTITICATIONS **143**

EN 50131 & EN 50136 COMPLIANCE 143
SIA CP-01 COMPLIANCE 146
RED COMPLIANCE STATEMENT 148

RISCO GROUP LIMITED WARRANTY ..... ERROR! BOOKMARK NOT DEFINED.

CONTACTING RISCO GROUP **149**

Chapter 1: Introduction

The WiComm Pro wireless security alarm system is ideal for installation in any home or small business environment. It supports RISCO's extensive range of wireless security and safety devices, detectors, keypads, remote controls, key fobs, wireless sirens and other peripheral accessories.

Main Features and Benefits

- Connecting the system to a Cloud server enables remote control and remote configuration of the system, as well as "visual verification" – for monitoring stations and Web / smartphones users alike – to greatly assist in determining whether an alarm event is real or false by viewing photos in real-time. This feature can improve the efficiency of responding agencies and provide increased user-control and enhanced monitoring of secured premises.
- IP / Ethernet and GSM/GPRS communication channels. One can utilize a single communication channel, both channels simultaneously (using one channel as a backup), or no communication channel (for audible-only installations)
- Wireless 2-way accessories/peripherals, such as the wireless 2-way slim keypad, and wireless 2-way remote control with "rolling code" code protection, key-lock, as well as send-command and receive-command functions with LED indication
- Easy enrolling of wireless peripherals at the main panel or via the installer keypad or via Configuration Software. Remote enrolling of wireless peripherals can be performed according to device ID,or by RF allocation.
- Programming using Configuration Software or the installer keypad
- Ability to combine both one–way and two-way transmitting devices in the same system
- Separate main panel that can be hidden for higher security
- Input/output (home automation) capability

Robust and Full-Featured System

Detectors / Visual Verification

- Using up to 8 PIR detector / cameras – also "pet friendly" models
- False alarm reduction
- 2-way and 1-way wireless detectors that can be combined in the same system
- Image capturing and transmission via detector model with camera ("visual verification")

Monitoring Station

- Remote programming, diagnostics, and communication test
- Report up to 3 Monitoring Stations
- Encrypted GPRS and IP communication
- MS polling through GPRS network
- Flexible configuration for "split report" scenarios

Communication

- Flexible communication over GSM/GPRS, IP
- Backup capability between the communication methods
- Supports major reporting formats
- Cloud-based
- For smartphone app & Web application users

Installer Programming & Device Allocation

- Local / remote programming using Configuration Software
- Full programming using installer keypad
- Flexible device allocation (enrollment) by serial ID serial number or by RF allocation
- Keypad programming menu adjusted to existing hardware

Wireless 2-Way Slim Keypad

- S.O.S. / panic, 2-way communication emergency function)
- Model available with Proximity (tag reader)

VUpoint IP Cameras

- P2P - True plug and Play IP camera
- Various types
- Wi-Fi based
- Live video using App or Web

Codes

- 1 installer code
- 1 sub-installer code
- 1 grand master code
- 32 user codes maximum
- 4 authority levels
- Optional 4 or 6-digit code definition

Zones

- 32 wireless zones plus 4 additional zones via optional Wireless I/O Expander
- Multiple zone types
- Full zone supervision

Sirens

- Built-in siren on main panel
- Can be connected to up to 3 external and internal wireless sirens

False Alarm Reduction

- Swinger shutdown
- Zone crossing
- Report delays to MS
- Abort alarm feature
- Soak test
- Final exit zone

Follow Me

- Designate up to 16 Follow Me destinations
- Unlimited FM e-mails from Cloud server
- Follow me messaging can be defined as, SMS, e-mail or push notification over the cloud
- User control over the system
- Security code protection

User Operating Tools

- Wireless 2-way remote controls and key fobs
- Wireless 1-way key fobs
- Wireless 2-way Slim Keypad
- Self-monitoring from smartphone
- SMS
- Configuration software
- Web-based application

Wireless Features

- Signal jamming indication
- 868MHz / 433 MHz radio frequencies
- Programmable supervision time
- Tamper detection in transmitters
- Low-battery detection feature in transmitters

Home Automation

- 4 outputs for wireless I/O expander
- Up to 16 home automation ("X-10") devices – Outputs can follow system, partition, zone or user events
- Outputs scheduled, auto-activated, or by user command (SMS, Web or remote phone)

WiComm Pro Architecture

Traditional

WiComm Pro can communicate information to monitoring stations (and Follow Me destinations) through various communication channels, depending on the physical communication modules installed inside the main panel. Communication can be established through IP/Wi-Fi, or GSM/GPRS. Communication can be direct or through the RISCO Cloud.

All methods can be used for:

- Reporting events to monitoring stations
- Sending automatic notifications to the owner
- Remote system programming and maintenance
- Owner remote control

Cloud Communication

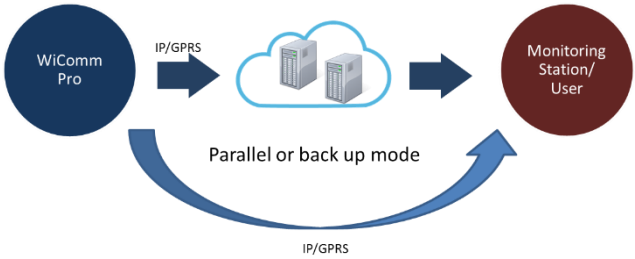
Wicomm Pro can be constantly connected to a dedicated application server (the "RISCO Cloud") via IP or GPRS.

The RISCO Cloud handles all communication between the WiComm Pro system, monitoring stations and Smartphone/Web users, enabling remote monitoring and control, as well as a RISCO's VUpoint video verification solution that utilizes IP cameras:

Cloud communication can be defined as either parallel or back-up.

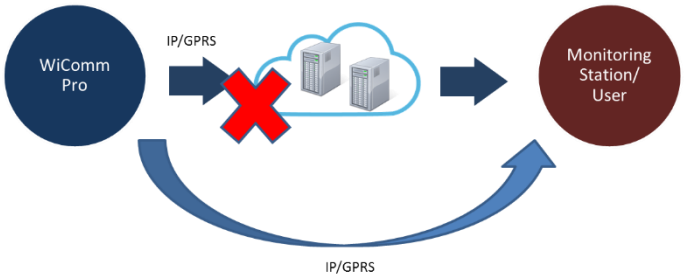
Parallel Communication

Reporting (event notification) can be sent in parallel through the Cloud and also straight from the system to the monitoring station and end- users (Follow Me, smartphone and Web application users) – via the designated communication channel (IP or GSM/GPRS).



Back-up Communication

Utilizing the Cloud as the main route for communicating (reporting) to the monitoring station and smartphone / Web application users. If the Cloud fails, the system utilizes the backup mode to communicate. Either GSM/GPRS or IP can be designated as the primary communication channel that is connected via the Cloud, and likewise, either GSM/GPRS or IP can be designated as the "backup."



Communication Channels

The WiComm Pro system communicates with monitoring stations and/or to designated contacts (smartphone / Web application users) via IP or GSM/GPRS communication channels, for the purposes of **remote monitoring, system-control and operation** (such as system setting/programming, arming, maintenance, receiving alarm event and status notification, viewing history log, bypassing detectors, and receiving visual verification).

GSM/GPRS

GSM/GPRS can be used as the primary communication channel, or as a back-up to the IP communication channel. The GSM /SPRS module support multi channels.

IP/Wi-Fi

Using IP/Wi-Fi as a communication channel enables system communication over a TCP/IP network. IP/Wi-Fi can be used as the primary communication channel or as a back-up channel to GSM/GPRS. The GSM /SPRS module support multi channels

Monitoring Stations

Reporting events to monitoring stations can be done via the Cloud (RISCO or OEM Cloud) or directly from the WiComm Pro system to the monitoring station using the RISCO IP Receiver. Events can be reported in SIA/IP, SIA and Contact ID monitoring protocols. In addition, WiComm Pro can send events in SIA IP protocol over TCP/IP to monitoring stations that have standard IP receivers.

Configuration Software

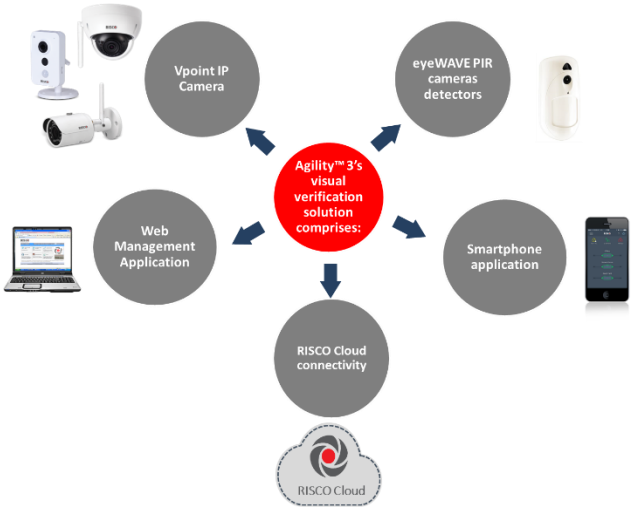
The system's Configuration Software enables remote system setting/programming by the user or by the monitoring station, via IP. Refer to the documentation for the Configuration Software.

Video Verification with IP Camera

WiComm Pro supports RISCOs revolutionary, live **VUpoint** video verification solution which seamlessly integrates an unlimited number of IP cameras to provide an unprecedented level of security and live video monitoring capabilities to monitoring stations and end-users alike. Powered by the RISCO Cloud, VUpoint enables the initiation of live video streaming on demand from any IP camera which can be viewed directly using the iRISCO smartphone or Web applications. VUpoint can be configured so that any detector or event, whether intrusion, safety or panic, can trigger the IP camera. For verification purposes, users can monitor intrusion events using snapshot images and live video, and monitoring stations can identify costly false alarms for higher efficiency.

Snapshot Follow Event

WiComm Pro also supports advanced PIR camera functionality to "follow" (capture and send snapshots) of event activations – other than those of the PIR camera itself – which occur within the PIR's partitions. This, together with video verification, enables comprehensive visual verification capabilities for your system.



Product Specification

Configuration	
Maximum number of partitions	3
Maximum number of wireless zones	32
Maximum rolling-code remote controls / key fobs	8
Maximum wireless 2-way slim keypads	3
Maximum Follow Me numbers	16
Maximum user codes	32
Grand Master, Installer, and Sub-Installer codes	1 each
Maximum events in event log	1000
Maximum alarm sounders (internal/external)	3
Electrical	
Electrical power requirement	230VAC, 50/60 Hz 0.6A max. or 14.4VDC, 2.5A
AC power supply cord	Diameter 14mm, conduit 16mm Safety-approved, in compliance with IEC 60227
DC Connector	DC plug, 5.5x2.1x12mm small magnetic ring
Current consumption (at main panel)	166mA standby
Backup battery (inside main panel)	Li-Polymer rechargeable battery pack 2350 mAh. Max. time to recharge to 80%: 34 hours Low voltage signal at 7.2 VDC
Operating Temperature	
Main panel, wireless PIR detector / camera	-10°c – 55°c (14°F to 131°F)
Physical	
Dimension (HxWxD) of main panel	197.5 mm x 152.5 mm x 52 mm 7.78 in x 6 in x 2.05 in
Weight	0.77 kg
Wireless	
RF immunity	According to EN 50130-4
Frequency	868.65 MHz, 433.92 MHz (Security)
Camera Frequency	869.525 MHz, 916 MHz, 430 MHz
GSM G2, GSM G3 & GSM G4 Modules (RP512G2, RP512G3, RP512G4)	
Current consumption	Average: 30 mA;Peak: 130 mA

Power Output	868.65 MHz, 10mW; 869.525 MHz, 100mW Max
IP Module (RP512IP)	
Current consumption	Average: 60 mA; Peak: 115 mA
Wi-Fi Module (RP51200W)	
Current consumption	Average: 60 mA; Peak: 115 mA

Safety Precautions

WARNING: Installation or usage of this product that is not in accordance with the intended use as defined by the supplier and as described in the instructional materials can result in damage, injury or death.

WARNING: Make sure this product is not accessible by children and those for whom operation of the system is not intended.

WARNING: Customer should never attempt to repair the wireless security alarm system or component, nor try to open the main panel casing, as doing so could result in damage, injury or death – customer should always contact your installer / supplier agent for service.

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

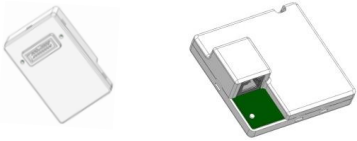
WARNING: Risk of explosion exists if a battery is replaced by an incorrect type.

CAUTION: Dispose of used system component batteries according to applicable law and regulations.

Chapter 2: Typical System Components

Main panel

Plug in Communication Modules: Single / Multi channels IP or GPRS



Wireless 2-way Keypads

Remote control (key fob). 1-way and 2-way models available

Magnetic door/window contact (includes sensor and magnet)

PIR motion detector (with or without camera). A "pet-friendly" model is also available

Safety detectors: Smoke,

Wireless Flood Detector and Sensor

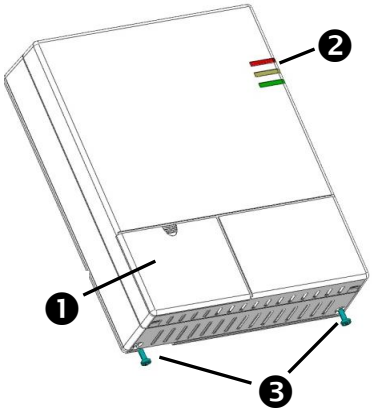
Wireless acoustic Glass Break Detector

Indoor Wireless Sounder

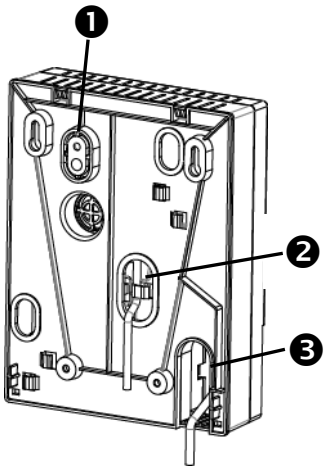
VUpoint IP Cameras:

Chapter 3: Describing and Using the Main Panel

WiComm Pro Main Components

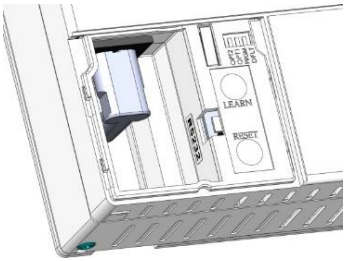


❶	Front access cover
❷	LED indicators
❸	Locking-screws (2)

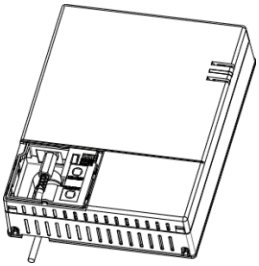


❶	Back tamper screw location
❷	Wiring channel for network cable (shown with cable routed via hook)
❸	Opening for AC or DC power cable (cable is installed onto the back of the panel only after the mounting bracket is secured to the wall)

AC Power Connection



DC Power Connection



LEARN Button	Used for local allocation of wireless device. To enter local programming mode, press the button for 5 seconds. The unit beeps once and enters "Learn" mode. The LEDs light up in Green one after the other. To exit "Learn" mode short-press the LEARN button; the unit beeps once and the LEDs stop flashing
RESET Button	Pressing on the RESET button for 20 seconds will reset the power supply for the main unit (Both AC and battery)
Front Tamper Switch	Used to indicate tamper alarm when opening the front cover.
RS232 Connctor	Use this connector for local programming using the configuration software
Dip Switches	**OPT1: Future use** **OPT2: Future use** **PRGM:** Enables loading local software updates to the WiComm Pro. • **ON**: software updates to the WiComm Pro can be loaded • **OFF** (Default): software updates to the WiComm Pro cannot be loaded **DFLT:** Default jumper: Used when performing the following: To return installer, sub-installer and grand master codes to their default factory values. Set this DIP switch to **ON**, disconnect all power and then reconnect the power. Note the code length does not change

Main Panel LEDs

LED	Color	State	Status
Upper LED (Power)	Green	On	Powered on
	Red	On	Electrical power supply trouble
	Orange	On	Low battery
Middle LED (Status)	Red	On	System armed (Full Arm or Partial Arm modes)
		Rapid flash	Alarm activation
		Slow flash	System is in entry/exit delay before disarming/arming the system
	Green	On	System is ready
		Slow flash	System is in exit delay with front door open
	Orange	On	System trouble
	OFF		System is not ready for arming
Buttom LED (Communication)	Green	On	GSM/IP communication ok
		Slow flash	GSM/IP connecting
	Orange	Slow flash	GSM/IP fault. Also, if only one communication mode is used (which is not a fault)
All 3 LEDs	Orange	Slow flash	Battery needs replacing (service mode)

Communication Modules

GSM/GPRS

The **easily**-installed GSM/GPRS plug-in module enables system communication over 2G/3G/4G networks for both users and monitoring stations, for event reporting, system control, and programming. GSM/GPRS can be used as the primary communication channel, or as a failure back-up for IP communication channel.

GPRS connectivity enables the system to be constantly connected to the RISCO Cloud, which in turn enables visual verification to end users and monitoring stations alike and provides end users with system control via the Smartphone and Web applications. Cloud-connected users can receive real-time push notification messages to Smartphones, or e-mail notifications.

Without Cloud connectivity, users can additionally control the system using SMS, and can also be configured to receive event notifications via SMS, and e-mail (in parallel to the Cloud-based notifications), depending on system configuration. Reporting events to monitoring stations is via GPRS or SMS (using the RISCO IP Receiver). Events can be reported in SIA, SIA IP, and Contact ID monitoring protocols.

IP

The easily-installed IP plug-in module enables system communication over a TCP/IP network. It can be used as the primary communication channel or as a failure back-up for GSM/GPRS communication channel.

Using IP connectivity, the system can be constantly connected to the RISCO Cloud server, which enables visual verification to end users and monitoring stations alike and provides end users with real-time event reporting and system control via the Smartphone and Web applications. The IP module also enables users to receive e-mail alerts and system status information.

The IP module supports common format protocols (SIA, Contact ID) to send alerts to monitoring stations using the RISCO IP Receiver. In addition, the system can send events in SIA IP protocol over TCP IP to monitoring stations that have standard receivers which support IP.

The IP module also enables remote programming of the system main panel using the Configuration Software over an IP line.

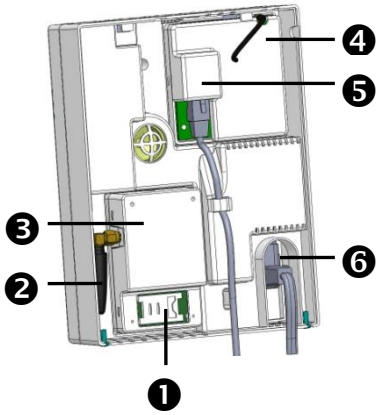
Wi-Fi

To Connect with Wi-Fi

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

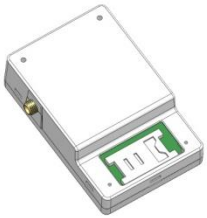
1. To connect via Wi-Fi network, you must select your Router's Wi-Fi network.
2. Go to Activities –> Wi-Fi screen: available networks appear in a list.
3. Select the desired network and enter the password (if required).

Installing Communication Modules



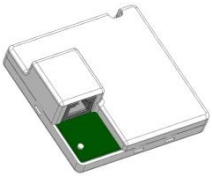
Plug in GSM Module

(front and back)



Plug in IP Module

(front and back)



❶	SIM holder on GSM module
❷	Antenna for GSM module (shown with internal antenna installed)
❸	GSM module
❹	IP module
❺	Network cable connector on IP module (shown with cable connected)
❻	AC or DC power cable (shown installed from the back of the main panel)

Chapter 4: Installing the WiComm Pro

Installing the Main Panel

IMPORTANT:

Only alarm system installers or similar professionals (such as electricians) should install and service the WiComm Pro

Mounting Guidelines

Install the main panel in consideration of the following guidelines:

- Install in a centrally-located place, between all the wireless devices in your system, for optimal communication
- Install in a protected area, that is not visible from outside of the premises
- Make sure it is not reachable by small children
- Install in a place where the alarm can be heard during Partial Arm mode
- Make sure it is installed where the GSM signal is good, as indicated by the communication LED lit up in green
- If an IP connection is used, install close to the router / wall IP connection
- Install near an uninterrupted 230V AC electrical outlet

⚠ **Do not install the main panel as follows:**

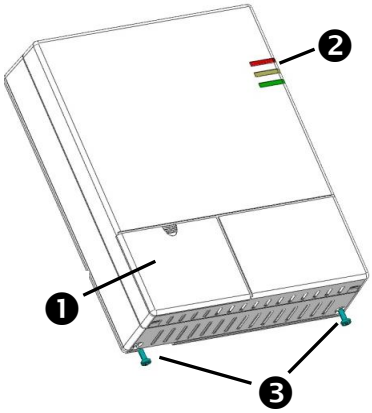
- Do not install near direct heat sources
- Avoid proximity to sources of electrical disturbance, such as computers and televisions
- Do not install near large metal objects, as they may hinder antenna performance

Wall-Mounting the Main Panel

The main panel can be wall-mounted either horizontally or vertically.

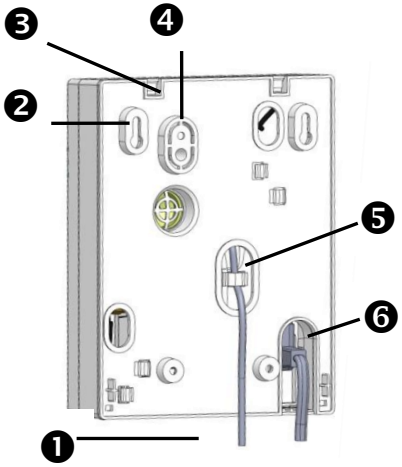
NOTE: For an EN50131-compliant installation, the main panel must be mounted horizontally (with LEDs facing upward)

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

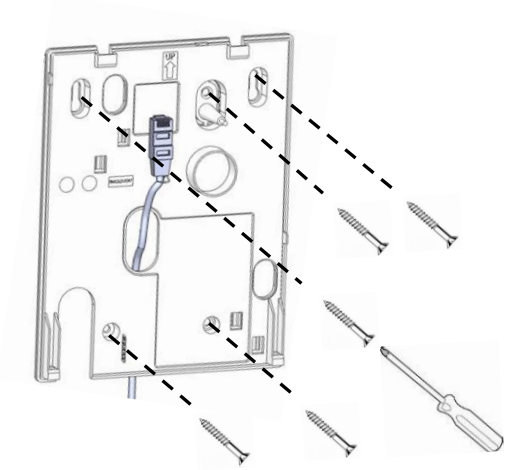


❶	Front access cover
❷	LED indicators
❸	Locking-screws (2)

2. Using the mounting bracket as a template, first mark and then drill all five holes on the wall (four mounting holes and one back tamper hole), then install the anchors.



Mounting bracket – back side



Mounting bracket – front side

❶	Lower mounting screw locations (2)
❷	Upper mounting screw locations (2)
❸	Grooves for placing tabs from front cover (2)
❹	Back tamper screw location
❺	Wiring channel for network cable (shown with cable routed via hook)
❻	Opening for AC or DC power cable (cable is installed onto the back of the panel only after the mounting bracket is secured to the wall)

3. Plug in the communication modules
    a. IP Module: If your WiComm Pro is equipped with an IP card Install the IP communication module in its cavity (back cover), with its connector fitting securely onto its respective socket. Make sure the network cable is first routed through the wiring channel on the mounting bracket (and via the fastening hook). Then plug the network cable into its jack on the module (see illustration above point 5).
    b. GSM/GPRS Module: If your WiComm Pro is equipped with a GSM/GPRS module, insert a SIM card into its holder to enable GSM/GPRS communication. Screw the antenna onto its connector on the GSM module. Install the GSM module in its cavity, with its connector fitting securely onto its respective socket

    NOTES:

    1. Do not install SIM card while the main panel is powered up.
    2. Do not touch SIM Card circuitry /connectors, as it could damage the SIM card

4. Route the AC or DC power cable (depending on the configuration) through the opening in the housing (back cover) and secure its plug onto the socket (see illustration).
5. Affix the main panel onto the mounting bracket by positioning its two plastic tabs (located at the top of the panel) onto their respective grooves (located at the top of the mounting bracket), and then press to close the housing.
6. Install the two locking screws at the bottom of the main panel.
7. Connect the main panel to the AC power supply (depending on the configuration).

    NOTE: The backup battery takes 24 hours to charge.

Chapter 5: Installer Programming

Programming Methods

There are available options for fully programming the WiComm Pro system:

- Via the system Configuration Software
- Via temporary "Installer" LCD Keypad (typically used for example, if customer's kit doesn't include an LCD keypad)
- Via Customer's Wireless Panda (2-Way LCD + Proximity) keypad

Configuration Software

The Configuration Software enables you to program the WiComm Pro from a computer. It enables the following:

- Working locally with a portable computer physically connected to the WiComm Pro via RS 232 cable
- Working at a remote site, communicating with the WiComm Pro via GPRS or IP address (Direct or through the RISCO Cloud)

For further information on programming via the Configuration software, refer to the Configuration Software documentation.

Allocating Installer Temporary Keypad

Although an installer can use a customer's wireless LCD keypad, RISCO Group offers the WiComm Pro installer a temporary "installer" wireless LCD keypad to be used for fully configuring the system. This LCD keypad will be allocated temporarily, and not as a permanent part of the system. After temporarily allocating the LCD keypad, the other system devices can then be allocated with it, and the system further configured.
When the temporary installer LCD keypad is allocated, it prompts the installer to define a default system language.

NOTES:

An hour after exiting the programming mode, the installer LCD keypad will be erased from the system's memory (also when power is lost to the system).

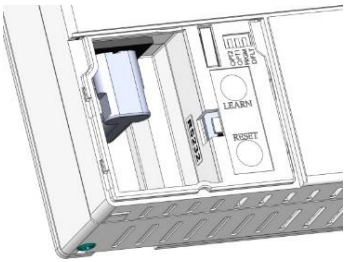
Installer programming can be performed using only one keypad at a time.

During installer programming, the keypad display will turn off after 4 minutes if no key entry has been made. Press any button to restore the current keypad display.

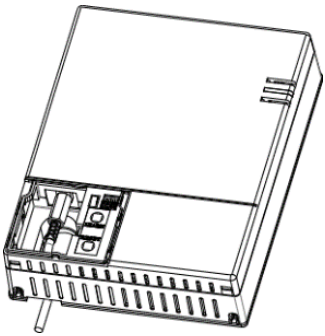
To (temporarily) allocate the installer keypad and define the system language:

1. After the main panel is connected to the power supply, short-press the LEARN button;

AC Power Connection



DC Power Connection



2. With battery installed, press the Panda/LCD keypad's buttons simultaneously during the status announcement until the following message appears:

   Select Language: Using the arrows scroll the options and press for the selected language.

3. Enter the Grand Master code (default is 1234) and then press ; you are now in the User Menu.

   NOTE: When a **wrong** Grand Master code is entered, the keypad will not be allocated. To continue this procedure, start the keypad allocation procedure again.

4. Press twice to exit the User Menu, and enter the system again using the installer code (default is 0132).

5. Now that you have temporarily allocated this "installer" LCD Keypad to the system, you can now allocate other system devices and perform system programming.

Allocating the Customer's Panda/LCD Keypad

WiComm Pro can be fully configured via the customer's wireless Panda/LCD keypad. New systems require that the LCD keypad be the first device to be allocated to the system, from which it then prompts the installer to define a default language. After the Panda/LCD keypad allocation, the other system devices can then be allocated with it, and the system further configured

To allocate the Panda/LCD keypad and define the system language:

1. After the main panel is connected to the power supply, press the LEARN button on the main panel for 5 seconds. The unit beeps once and enters "Learn" mode. The LEDs light up one after the other in Green.

2. Press and simultaneously for at least 2 seconds; the keypad will "beep" if allocated.

3. In the displayed language menu, select the system language (and customer default) settings, and then press to confirm.

4. Now that you have allocated this Panda/LCD Keypad to the system, you can now allocate other system devices with the Panda/LCD keypad and perform system programming

Accessing the Installer Programming Menu

After allocating the installer keypad and defining the system language, you can then start to allocate system devices from the Programming Menu on the installer keypad.

To access the Programming Menu:

1. Press and enter the installer code (default code is **0132**). The keypad will sound a confirmation beep, and the **Programming** menu will display on the keypad.

NOTE: If a Grand Master code is required to confirm the installer code, it should be entered at this stage (after entering the installer code).

---

2. From the Programming menu, press ; a confirmation sound will be heard and the three LEDs on the main panel will together flash on and off.

NOTE: If the keypad display shows "Unconfigured in learning mode" then wait a few minutes for the communication to be established, and then press again.

---

3. Use the buttons to scroll between the following Programming menu items ("sub-menus"):
    - **1) System**
    - **2) Radio Devices**
    - **3) Codes**
    - **4) Communication**
    - **0) Exit**
4. To exit the Programming sub-menus, press **zero** (**0**).

Wireless Device Allocation Options

All wireless devices (detectors and accessories) must also be allocated ("enrolled") to the system. This can be performed at:

- **Main panel:** Perform Quick Allocation of all devices by sending an RF signal transmission from each device to the main panel (see procedure below).
- **LCD keypad:** The following methods are available:

    For having devices assigned automatically (and sequentially): You can either perform this by the "RF Allocation" method, or by entering each device's unique 11-digit code (serial number) into the system.

    For manually selecting a specific device number to which a device is then allocated: You can perform this by the "Zone Allocation" method.
- **Configuration Software:** Refer to the Configuration Software documentation for details.

Quick Device Allocation at the Main Panel

You can quickly allocate all system devices at the main panel.

NOTE: For quick allocation at the main panel, the system bit Quick Learn must be enabled.

➢ **To quickly allocate all wireless devices at the main panel:**

4. Make sure batteries are installed in each device.
5. At the main panel press the **LEARN** button for 5 seconds; all three LEDs light up, one after the other, indicating the panel is in "Learn" (allocation) mode.
6. Send an RF signal transmission to the main panel from each device per the instructions in the *Table of Device Transmissions*, page 24. If a device is not listed in the table, refer to the device's packaged instructions.

NOTE: For future use, it is recommended to write down for the customer the device description, zone number, and installation location of each allocated device.

Wireless Device RF Transmissions

Wireless Device	Transmission procedure
2-Way LCD Keypad	Press and simultaneously for at least 2 seconds
2-Way Panda Keypad	Press and simultaneously for at least 2 seconds.
2-Way Slim Keypad	Press and simultaneously for at least 2 seconds.
PIR Detectors: • **PIR** • **PIR camera** • **PIR-pet** • **PIR-pet camera**	Press the tamper switch for 3 seconds.
Curtain Detector	After inserting battery, close the bracket and wait 3 seconds.
1-Way magnetic Contact Detectors	Press the tamper switch for 3 seconds.
2-Way Magnetic Contacts Detectors	Press the tamper switch for 3 seconds. **NOTE:** After programming parameters for this device and exiting Programming mode, press the Tamper switch for 3 seconds, and then wait 1 minute for the main panel to download the parameters from the detector.
2-Way Remote Control	Press and simultaneously for at least 2 seconds
1-Way Keyfob	Click for at least 2 seconds
Wireless 2-Way Smoke Alarm & Heat Detector	Press the tamper switch for 3 seconds.
WL 2-Way Indoor Siren	Press the tamper switch for 3 seconds.
Siren	Press the reset switch on the siren. After a squawk sounds, within 10 seconds press tamper switch for at least 3 seconds.
2-Button Panic Keyfob	Press both buttons for at least 7 seconds
Wrist Band Panic Transmitter	Press the button for at least 7 seconds.

When all the devices have been allocated, short-press the **LEARN** button to exit Learn mode; the LEDs stop flashing

Device Allocation using the Wireless LCD Keypad

RF Allocation Method

Using the RF Allocation method, zones are assigned automatically and sequentially.

To perform device allocation by RF Allocation:

1. Go to the Installer menu and select **Programming → Radio Device → Allocation → 1) RF Allocation.** The system immediately goes into Learn mode.
2. Send a transmission from the device. (See Wireless Device RF Transmissions, page 24.)
3. The main-panel will acknowledge the transmission with a beep and LCD keypad displays the device's automatically-assigned zone and index numbers, the device's 11-digit serial number, and the device's description.
4. When finished allocating the system device(s), press repeatedly until you arrive back to **Radio Device**, then press to Exit, and to confirm.

Serial Number Method

When performing allocation by entering the device's serial number ("code"), devices are assigned automatically and sequentially.

To perform device allocation by serial number:

1. Go to the Installer menu and select **Programming → Radio Device → Allocation → 2) By Code**.
2. Enter the device's 11-digit serial number ("code"), and then press .
3. The main panel will acknowledge the transmission with a beep and the LCD keypad displays the device's automatically-assigned zone and index numbers, the device's 11-digit serial number, and the device's description.
4. When finished allocating the system device(s), press repeatedly until you arrive back to **Radio Device**, then press to Exit, and to confirm.

Allocating Devices with the Configuration Software

The installer can perform wireless device allocation via the system Configuration Software by either RF allocation, or by entering the device's code (serial number).

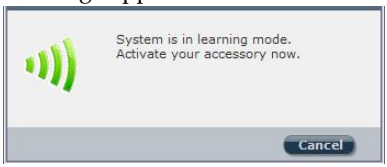
RF Allocation

To allocate a device by RF allocation:

1. Establish communication between the main panel and the Configuration Software. For more information refer to the documentation for the Configuration Software.

1. Open the **Activities > Radio Device Allocation** screen.

2. Click Allocate...; this sets the main panel to "learning" mode, and the following message appears:



3. Send a transmission from the device. See Wireless Device RF Transmissions on page 24; the main panel acknowledges the transmission with a beep, and the Radio Device Allocation screen indicates the allocation status as successful. The serial number, accessory type, and the system-assigned index number display.

NOTE: If required, you can change the index number assigned to the wireless device by selecting the corresponding index number and then pressing Allocate... again.

---

4. To allocate an additional wireless device, click Clear and then repeat this procedure from step 2.

Code Allocation

To allocate a device by code:

1. Establish communication between the main panel and the Configuration Software by selecting **Communication > Connect** from the main menu. For more information refer to the documentation for the Configuration Software.

2. Open the Radio Device Allocation screen, and then in the Allocation area enter the device's code (the 11-digit serial number found on the device).

3. Select the wireless device's index number. Selecting "**Automatic**" means that the index number will be automatically assigned by the system.

4. Click

; the main panel acknowledges the transmission with a beep, and the Radio Device Allocation screen indicates the allocation status as "successful."

Clearing Device Allocation

Clearing a device's allocation (deleting a wireless device) can be done either from the installer keypad or from the Configuration Software.

Clearing a Device Allocation from the Installer Keypad

To clear a device's allocation from the installer keypad:

1. Go to the Installer menus and select **Programming > Radio Device > Modification**.
2. Select the device category.
3. Go to the **Parameters** option.
4. Select the device index number.
5. Select the **Serial Number** option, and then enter **000000000000.**
6. Press

; the device will be deleted, a beep is sounded, and the words "deleted" appear on the installer keypad to confirm the deletion.

Clearing a Device Allocation with the Configuration Software

To clear a device's allocation using the Configuration Software:

1. Establish Communication between the main panel and the Configuration Software. For more information refer to the documentation for the Configuration Software.
2. From the **Radio Device Allocation** screen, in the Delete Accessories area, enter the device's serial number, and then click the **Delete** button.

Clearing All System Device Allocations with the Configuration Software

To clear allocations for all system devices using the Configuration Software:

1. Establish communication between the main panel and the Configuration Software by selecting **Communication > Connect** from the main menu. For more information refer to the documentation for the Configuration Software.
2. From the **Radio Device Allocation** screen, in the Delete Accessories area, click the **Delete All** button. When all accessories have been deleted, the screen indicates that the deletion has been successful.

Establishing Communication to the RISCO Cloud

WiComm Pro can be configured to be constantly connected to the RISCO Cloud, an application server that handles all communication between the system, service providers and Smartphone/Web users. The Cloud enables remote monitoring and control of the system, sending event notifications, and viewing real-time video clips via VUpoint IP cameras – for both monitoring stations and system users.

Step 1: Enabling Cloud Communication

- **From the Programming menu select:** 1) System > 2) Controls > 3) Communication > Cloud Enable > toggle to [Y] using , and then press OK to confirm.

Step 2: Defining the (GPRS or IP) Communication Channel

Connecting with GPRS

1. From Programming menu select: **4) Communication > 1) Method > 2) GSM > 2) GPRS**
2. Use to scroll between **1) APN Code** and **2) APN User Name** and then define the APN code and user name respectively. This information must correspond with that supplied by the SIM card service provider.

Connecting with IP

3. From Programming menu select: **4) Communication > 1) Method > 3) IP > 1) IP Config**
4. Now define whether the system's IP address is Static or Dynamic. If Dynamic select [**Y**] (the system refers to an IP address provided by the DHCP). If Static select [**N**] and define all other parameters in the menu.

Step 3: Defining Cloud Parameters for IP or GSM/GPRS

From the Installer Menu Programming select: **4) Communication > 5) Cloud,** and then define the following parameters:

5. **IP Address:** The server IP address (**www.riscoCloud.com**, or that of your organization's Cloud server)
6. **IP Port:** The server port is set to **33000.**
7. **Password**: The password for server access as provided by your provider (if required). This password should be identical to the main panel password as defined in the server under the Main Panel page definition.
8. **Channel:** Select the communication path for the Cloud (based on IP or GPRS communication) as appears in the available options.

NOTE: The SIM card must be installed (see *Wall-Mounting the Main Panel*, page 16).

9. **Controls:** The WiComm Pro supports parallel channel reporting (via IP, GPRS or SMS) to both the monitoring station and Follow Me users. Use this setting to decide if the panel reports events to the monitoring station or Follow Me in parallel to the report to the Cloud (assuming there is an additional communication channel available – IP, GPRS SMS,), or only as a backup when the communication between the WiComm Pro and the Cloud is not functioning.

Step 4: Registering to the RISCO Cloud

To be connected to the RISCO Cloud, the system must be registered. Registering to the Cloud can be done by the Cloud administrator or via self-registration by the customer, depending on the Cloud configuration. Registering with the RISCO Cloud enables the customer to monitor, control and configure your WiComm Pro system from any location. The self-registration process is as follows:

To Register to the RISCO Cloud

1. Go to **www.riscoCloud.com/register**
2. Fill in 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 sticker located on the side of the panel or as printed on the postcard that arrived with the panel. Do not enter hyphens.
6. Complete registration form and click the Register button.
7. To complete registration, click the link on the e-mail message received (the email account you defined as Login Name).

To Login to the RISCO Cloud

1. Go to **www.riscoCloud.com.**
2. Enter User Name and Password (as supplied during the registration process).
3. Enter Grand Master code. Click the **Enter** button.

iRISCO App

Once the self-registration is complete, users can enjoy the iRISCO Smartphone app for smart and easy control of their WiComm Pro system from any location. The next step is to download the iRISCO app from the Apple App store or Android Play Store

Accessing the Web Application

Once the Cloud registration and initial login have taken place, system users can enjoy the Web application. To access the Web Application**:**

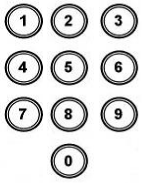
Enter the Web page address supplied by service provider into your Web browser

Chapter 6: Programming the Installer Menus

The installer menus and nested entities (sub-menus, options and parameters) are programmed by the installer using the installer keypad or the Configuration Software (refer to the Configuration Software documentation).

Describing Installer Keypad Buttons

The following buttons are commonly used for programming (the buttons shown are for the 2-Way Wireless Panda LCD & Proximity keypad):

Buttons	Description
	Used to input the numeric codes for arming, disarming, or to activate specific functions.
	To go back one level, exit menus (like the Esc key)
	To exit the programming mode (followed by to confirm)
	To select / confirm / OK (like the Enter key)
	To scroll between multiple options
	To toggle between options (such as Y / N)

Accessing the Main Installer Menus

To access the main installer menus from the installer keypad:

1. From an allocated keypad, press if needed (to go back in a menu), and then enter the installer code (default is **0132**).

NOTE: If the ***Authorize Installer*** **system bit** is defined as YES, a Grand Master code is required to authorize the installer to enter the programming mode. In this case the Grand Master code should be entered after the installer code via the ***Grand Master menu*** > ***Activities*** > ***Authorize Installer***.

2. Use the keys to scroll through all the **main installer menus:**

1) Programming
2) Testing
3) Activities
4) Follow Me
5) Clock
6) Event Log
7) Macro

3. Press to select a main installer menu.

4. Use the keys to scroll through the list of all the sub-menus.

Programming Menu

- After selecting the Programming Menu, you can scroll between the following list of its sub-menus:

1) System
2) Radio Devices
3) Codes
4) Communication
0) Exit

System

- The System sub-menu has the following options:

1) Timers
2) Controls
3) Labels
4) Sounds
5) Settings
6) Service Information
7) Firmware Update
8) Picture Server

Timers

The **Timers** option has the following parameters:

System: Timers		
Parameter	**Default**	**Range**
Exit/Entry Delay 1		
The amount of time before the system is armed/disarmed. Usually used on front entrance door.		
Entry Delay 1	45 sec	0-255 sec
Duration of entry delay 1 before the system is disarmed.		
Exit Delay 1	45 sec	0-255 sec
Duration of Exit Delay 1 before the system is armed.		
Exit/Entry Delay 2		
The amount of time before the system is armed/disarmed. Usually used on back door.		
Entry Delay 2	45 sec	0-255 sec
Duration of Entry Delay 2 before the system is disarmed.		
Exit Delay 2	45 sec	0-255 sec
Duration of Exit Delay 2 before the system is armed.		
Bell Timeout	03 min	01-90 min
Duration of the siren during an alarm.		
Bell Delay	00 min	00-90 min
The time delay before a siren sounds after an alarm is triggered.		
AC Off Delay	30 min	0-255 min
In the case of a loss of AC power, this parameter specifies the delay period before reporting the event or operating the programmable output. If the delay time is set to zero, there will be no delay period.		
Jamming Time	30	None, 10, 20 or 30 sec
Specifies the period that the system's receiver tolerates unwanted radio frequencies capable of blocking (jamming) signals produced by the system's transmitters. Once the specified time is reached, the system sends a report code to the monitoring station or activates a local siren, depending on the Audible Jamming system control. NONE: No jamming will be detected or reported.		
RX Supervision	2 hours	0-7 hours

System: Timers		
Parameter	**Default**	**Range**
Specifies how often the system expects to get a signal from the system's transmitters. If a signal from a zone is not received during the specified time the zone will be regarded as "lost," the system will send a report code to the monitoring station, and the system status will be "Not Ready".		
Notes: 0 hours disables supervision It is recommended to set the supervision time to a minimum of 3 hours		
TX Supervision	015	0-255 min
Specifies how often a bi-directional wireless device generates a supervision request to the system. If any of the accessories does not respond to the request at least once during the **RX Supervision** time, the system will regard the accessory as "lost."		
Note: The device will generate the supervision message according to the time defined.		
Important: The RX Supervision time should be higher than the TX Supervision time in order to eliminate false "lost "events.		
Redial Wait	30 sec	0-255 sec
The number of seconds between attempts at redialing the same phone number. Applies to both the **MS Retries** and **FM Retries** parameters.		
Note: Used for GSM.		
More		
Swinger Limit Shutdown	00	0-15 times
A swinger is a repeated violation of the same zone, often resulting in a nuisance alarm and usually due to a malfunction, an environmental problem, or the incorrect installation of a detector or sensor. This parameter specifies the number of violations of the same zone reported during a single armed period, before the zone is automatically bypassed.		
Note: 00 to disables the swinger shutdown		
No activity	00	0-99 hours
Determines the time limit for reception of signals from sensors used to monitor the activity of sick, elderly or disabled people. If no signal is received from a zone defined with the "No Activity" feature at least once within the defined time limit, a "No-Activity" alert can be send to the Follow Me destination, a local message can be heard, and a report to monitoring station can be defined to be send. Options: 0 =this parameter is inactive.		
Last Exit Sound	00	0-255 seconds

System: Timers		
Parameter	**Default**	**Range**
Entry Bypass	45 seconds	(15–240)
When the Wireless 2-Way Slim Keypad reader is defined as bypass mode, this timer defines the period during which an Open Delay Zone Type (typically a door) can be opened without triggering an alarm event.		
Service Time	20 minutes	0-240 minutes
The time period that all tampers (main panel and accessories) can be opened for purposes of battery replacement without triggering a tamper alarm (see Service Mode, under *Activities Menu*, page *113*).		

Controls

The **Control** menu contains parameters that control specific system operations.

System: Controls	
Parameter	**Default**
Basic programming	
Quick Arm	YES
YES: Eliminates the need for a user code when arming (full or partial) the system by a keypad or 2-way remote control. **NO**: A valid user code is required for arming using a keypad or remote control.	
Allow Bypass	YES
YES: Permits zone bypassing by authorized system users after entering a valid user code. **NO**: Zone bypassing is NOT permitted.	
Quick Status	YES
YES: A user code is not required before pressing the status button on your wireless keypad or bi-directional remote control. **NO**: A user code is required to activate the status key.	
False Code Trouble	YES
YES: A false code report is sent to the monitoring station after five successive attempts at arming or disarming in which an incorrect user code is entered. No alarm sounds at the premises, but a trouble indication appears. The wireless keypad will be locked for 30 minutes. **NO:** A local alarm is sounded at the premises.	

System: Controls	
Parameter	**Default**
Siren Squawk	YES

YES: Arming or disarming the system using a remote control, wireless keypad or a key fob produces a brief "chirp" and activates the strobe as follows:

- One chirp indicates the system is armed (also when arming with a keypad)
- Two chirps indicate the system is disarmed
- Four chirps indicate the system is disarmed after an alarm

NO: No "chirp" is produced

Audible Panic	NO

YES: The sirens operate when a "Police Alarm" is initiated at the keypad (if defined), at the remote control, or when a panic zone is activated.

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

Note: The system always transmits a panic report to the monitoring station.

Buzzer > Bell	YES

YES: If an alarm occurs when the system is armed in the Stay Arm (Partial Arm) mode, a buzzer sounds for 15 seconds before the sirens operate.

NO: An alarm in the Stay Arm (Partial Arm) mode causes sirens to operate simultaneously.

Audible Jamming	NO

Relates to the **Jamming Time** parameter.

YES: Once the specified time is reached, the system activates the siren and sends a report code to the monitoring station.

NO: Once the specified time is reached the sirens do not operate.

Exit Beeps at Stay	YES

Determines whether the system will sound beeps during exit time in Stay Arm (Partial Arm) mode.

YES: Exit beeps will sound

NO: Exit beeps will not sound

Forced Device Arming	YES

YES: Arming a partition, using a remote control or key-switch can be performed with violated (not ready) zones in the system. Any violated (not ready) zone(s) in the partition will be bypassed automatically. The partition is then "force armed," and all intact zones are capable of producing an alarm.

NO: The partition cannot be armed until all violated (not ready) zones are secured.

System: Controls	
Parameter	**Default**
Arm Pre-warning	YES

Related to auto Arm/Disarm operation.

YES: For any partition(s) set up for Auto Arming, an audible Exit Delay (warning) countdown will commence 4.25 minutes prior to the automatic arming. During this period, Exit Delay beeps will be heard.

You can enter a valid user code at any time during the countdown to delay the partition's automatic arming by 45 minutes.

When an "Auto-Arm" partition is disarmed as described above, it can no longer be automatically armed during the current day.

The extended 4.25 minutes warning does not apply to automatic Partial Arming.

NO: Auto Arming for any programmed partition(s) takes place at the designated time. The programmed Exit Delay period and any audible signal occur as expected.

Default Enable	YES

This option contains parameters that relate to what happens to the Installer, Sub-Installer and Grand Master codes if the main panel's DEFAULT Dip Switch is in place when power to the main panel is switched off and then on.

YES: The Installer, Sub-Installer and Grand Master codes will return to the original, factory default values.

NO: The Installer, Sub-Installer and Grand Master codes will **NOT** return to the original, factory default values by an unauthorized user.

Status-Y/Talk-N	YES

Main Button: Status-Y/Talk-N parameter determines the function of the button on the keypad.

YES: Status button – the system will relay the system status.

NO: Not applicable.

Quick Learn	YES

Enables the button on the surface of the main panel to perform quick allocation of wireless devices. (See *Quick Device Allocation at the Main Panel,* page 23.)

YES: Quick Learn mode is enabled. A long press on the main panel button will start the Learn mode, and the LEDs on the main panel will start flashing one after the other.

NO: Quick Learn mode is disabled. The main panel is not in Quick Learn mode.

System: Controls	
Parameter	**Default**
Advanced programming	
Area	NO

Changes the system operation to Area instead of Partition, which then changes only the operation of a common zone.

YES: When selected, the following points are relevant:

- A common zone will be armed after any partition is armed
- A common zone will be disarmed only when all partitions are disarmed

NO: When selected, the following points are relevant:

- A common zone will be armed only when all partitions are armed
- A common zone will be disarmed when any partition is disarmed

Global Follower	NO

YES: Specifies that all zones (that are programmed to follow an Exit/Entry Delay time) will follow the Exit/Entry Delay time of any armed partition.

NO: Specifies that all zones (that are programmed to follow an Entry Delay time) will follow the Entry Delay time of only the partitions to which they are assigned.

Summer/Winter	YES

YES: The system automatically sets its time of day clock one hour ahead in the spring (on the last Sunday in March) and one hour back in the Autumn (on the last Sunday in October).

NO: No automatic time accommodation is made.

24 Hour Bypass	NO

YES: It is possible for the user to bypass a 24-hour zone.

Note: When set, this parameter also applies to the zone's associated tamper settings. Thus, bypassing a zone, also bypasses its tamper.

NO: It is not possible for the user to bypass a 24-hour zone.

Technician Tamper	NO

YES: It is necessary to enter the installer code to reset a tamper alarm. Therefore, resetting a tamper alarm requires the intervention of the alarm company. However, the system can still be set.

NO: Correcting the problem resets a tamper alarm, requiring no alarm company intervention.

System: Controls	
Parameter	**Default**
Technician Reset	NO
YES: It is necessary to enter the installer code to reset an armed partition after it has been disarmed. This requires the intervention of the alarm company.	
Note: Before the "ready" LED can light, all zones within the partition must be secured.	
NO: Once an armed partition is reset, the "ready" LED lights when all zones are secured.	
Installer Tamper	NO
YES: After a tamper alarm, the system will not be ready to arm. This requires the intervention of the alarm company. **NO:** After a tamper alarm is restored the system will be ready.	
Low Battery Arm	YES
YES: Allows arming of the system when a low battery condition is detected in the main panel. **NO:** Arming the system is disabled when a low battery condition is detected.	
Siren Pre-Alarm	YES
Specifies if the system will send a pre-alarm signal to the siren while an entry delay starts. **YES**: The system sends a pre-alarm signal to the siren at the beginning of the entry delay. If the siren does not receive a cancellation signal from the system at the end of the entry time, the siren will sound. **NO**: Pre-Alarm is disabled.	
Bell 30/10	NO
YES: The sirens cease to sound for 10 seconds after each 30 seconds of operation. **NO**: The sirens operate without interruption.	
Fire Alarm Pattern	YES
YES: During a fire alarm, the sirens produce a pattern of 3 short bursts followed by a brief pause. **NO**: During a fire alarm, the flow of sounds produced by the siren is a pattern of 2 seconds ON, then 2 seconds OFF.	
IMQ	NO
YES: Causes the following parameters to function as follows: • **Auto Arm Bypass:** If there is an open zone during the Auto Arm process, the system will be armed, and a silent alarm will be activated (unless the open zone is closed) • A utility output defined as "Auto Arm Alarm" is activated • A utility output defined as "Zone Loss Alarm" is activated	

NO: Causes the following parameters to function as follows:

- **Auto Arm Bypass:** If the Auto **Arm** programming arms the system and there is an open zone during the Auto Arm, the system will bypass the open zones and arm the system
- A utility output defined as "Auto Arm Alarm" is deactivated
- A utility output defined as "Zone Loss Alarm" is deactivated

Bypass Unique Code NO

YES: Unique code for the purpose of the Door Bypass feature. The codes used for the Door Bypass feature are defined with Door Bypass authority level.

NO: The regular user code can be used as a bypass code (not including Arm only authority level). The same user codes will be used from a bypass keypad and from a regular keypad

Silent Remote Install

YES: During Configuration Software programming, all panel sounds are suppressed.

NO: The panel generates sounds during Configuration Software programming.

Anti Mask = Tamper NO

Used to determine the operation of Anti Masking detection in wirelss detectors

YES:. Anti mask violation will activate tamper alarm

NO: Anti mask violation will be regarded as trouble event

Power Management NO

Used for improved power managmant of the system**.**

YES: When lost od AC power is detected, the communcaiton to the cloud will be disconncted. Connection to the cloud wil be established once AC is back

NO: Connction to the cloud will no tbe affected by the AC power status.

Presence Log NO

YES: Presence will be recorded in the event log.

NO: Presence will not be recorded in the event log.

Secondary Alarm NO

YES: If smoke or heat is detected by one of the Smoke, Heat and PIR detectors in the system, the other Smoke, Heat and PIR detectors in the system will sound their sirens.

NO: If smoke or heat is detected by one of the Smoke, Heat and PIR detectors in the system, the other Smoke, Heat and PIR detectors in the system will not sound their sirens.

Note: This option applies only to the RWX35SP Smoke, Heat and PIR detector.

System: Controls	
Parameter	**Default**
Communication	
MS Enable	NO
YES: Enables communication with the monitoring station to report alarms, trouble, and supervisory events. **NO:** No communication with the Monitoring Station is possible. Choose **NO** for installations that are NOT monitored by a Monitoring Station.	
Configuration Software Enable	YES
YES: Enables communication between the alarm company and the system using the Configuration Software. This enables modifying an installation's configuration, obtaining status information, and issuing main panel commands, all from a remote location. **NO:** Disables communication, as detailed above.	
FM Enable	NO
YES: Enables Follow-Me communication. If both the monitoring station phones and the Follow Me phones are defined, the system will first call the monitoring station phones and then the Follow Me phones. **NO:** Disables Follow-Me communication.	
Cloud Enable	YES
Yes: Enables communication between the WiComm Pro system and the RISCO Cloud server. **NO:** Does not enable communication, as detailed above.	
EN 50131 programming	
Authorize Installer	NO
This option limits the installer authorization to access the Programming menu. **YES:** A Grand Master code is required to authorize the installer to enter the Programming mode for 1 hour. **NO:** The installer does not need an authorization code.	
Override Trouble	YES
Specifies if the system/partition can be armed when there is a fault in the system. **YES**: The system will arm even if there is a fault in the system. **NO:** When the user starts the arming process and there is a system-fault, the user must confirm that he is aware of all faults before continuing with the arming process. This is done via the **User menu > Activities >Bypass Trouble.** The system will not arm during forced arming if a fault occurred in the system.	

System: Controls	
Parameter	**Default**
Restore Alarm	NO
YES: The user must confirm that he/she is aware that alarm occurred in the system before rearming the system. The system will be in "Not Ready" status until the user confirms the alarm. This is done via the **User menu > Activities > Advanced > Restore Alarm.** **NO**: The user does not need to confirm the alarm before rearming the system.	
Mandatory Event Log	NO
YES: Only mandatory events (specified in the EN standard) will be displayed in the Event Log. **NO**: All the events will be displayed in the Event Log.	
Restore Troubles	NO
YES: The user must manually confirm the restoral of each trouble to a normal condition. This is done via the **User menu > Activities > Advanced > Restore Troubles.** **NO**: The restoral report of each trouble is automatic.	
Exit Alarm	YES
YES: A violated zone outside the exit route will generate an alarm during the exit time. A report to the monitoring station for arming the system is sent at the beginning of the arming procedure. **NO:** A violated zone outside the exit route will cancel the arming process. A report to the monitoring station is send at the end of a successful arming procedure.	
Entry Delayed Alarm	NO
This feature is used to reduce false alarm reports to the Monitoring Station. **YES**: The report to the monitoring station and the siren alarm will be delayed for 30 seconds or until the end of the predefined entry delay (the shorter time of the two) following a violation of a zone outside the entry route. **NO**: A violated zone outside the entry route will generate an alarm during the entry time and a report will be sent to the monitoring station.	
20 Minutes Signal	NO
YES: Prior to arming the system, the system will check for zones that did not send a signal for more than 20 minutes. These zones will be regarded as not ready. A partition assigned with a not ready zone cannot be armed. **NO:** Prior to arming, the system will not check whether a zone did not send a signal for more than 20 minutes.	

System: Controls	
Parameter	**Default**
Attenuation	NO
YES: The WiComm Pro receiver will be attenuated by 6 dB during the communication test. **NO**: The WiComm Pro receiver works in normal operation mode.	
DD243 programming	
Bypass Exit/Entry	YES
YES: It is possible for the user to bypass an Exit/Entry zone. **NO:** An Exit/Entry zone cannot be bypassed.	
Entry Disable	NO
YES: The alarm confirmation process will be disabled when the entry time starts. **NO:** The alarm confirmation process will start when the entry time starts.	
Route Disable	NO
YES: The panel disables the entry route zones (EX/EN, EX (OP)/EN, followers and Final Exit) from participating in the alarm confirmation process when the entry time starts.	
Note: Sequential confirmation can still be established from two confirmed zones, located off the entry route.	
NO: The entry route zones will participate in the alarm confirmation process when the entry time starts.	
Installer Reset Confirmation	NO
YES: An installer reset confirmation is required in order to reset the system after a confirmed alarm. The system cannot be armed until an Installer Reset Confirmation is performed. The reset can be done by entering the Anti code, by entering the installation mode, or by performing an "installer reset" from the keypad. **NO:** Any means can be used to arm or disarm the system (keypad, remote phone operation, etc.).	
Key Switch Lock	NO
YES: Only a latched Key Switch zone can arm or disarm the system**.**	
Note: When the system has more than 1 zone defined as Latch Key Switch, the arm/disarm operation will occur only after all these zones are armed or disarmed.	
NO: Any means can be used to arm or disarm the system (keypad, remote phone operation, etc.).	

System: Controls	
Parameter	**Default**
Entry Disarm	NO

Determines if the system's disarming depends on the entry time.

YES: A remote control or keypad proximity tag can disarm the system during the entry time.

Note: The system cannot be disarmed with a remote control while the system is armed. This parameter setting is relevant only for the Away Arm (Full Arm) state and not for Stay Arm (Partial Arm).

NO: The system can be disarmed during any time using any disarming device.

CP-01 programming	
Exit Restart	NO

This parameter is used to define if an exit time shall restart one additional time while an entry/exit zone is tripped twice during exit time.

YES: Exit time will restart for one time only when an entry/exit zone is tripped during exit time.

NO: Exit time will not be affected if an entry/exit zone is tripped during exit time.

Auto Stay	NO

This parameter is used to define the system's arming mode when using a keypad and no exit/entry zone is tripped during exit mode.

YES: If no exit/entry zone is tripped during exit time the system will be armed in STAY mode (Partial Arm mode).

NO: If no exit/entry zone is tripped during exit time the system will be armed in Away mode (Full Arm mode)

Exit Error	NO

This parameter is used to define what will happen if an Exit/Entry zone is left open at the end of the exit time.

YES:

- Local alarm will be activated at the end of the exit time
- Exit error report will be sent to the monitoring station together with an alarm report if the system has not been disarmed during the entry time that immediately started after the exit time expiration

NO:

- No local alarm will be activated at the end of the exit time
- Only an alarm report will be sent to the monitoring station if the system has not been disarmed during the entry time that immediately started after the exit time expiration

System: Controls	
Parameter	**Default**
3 Minute Bypass	NO
YES: Bypasses all zones automatically for 3 minutes when power is restored to an "unpowered" system. **NO:** No bypassing occurs.	

Labels

You can rename the labels that identify the system and partitions by changing the default labels (**Partition 1**, **Partition 2,** etc.) to meaningful names / location descriptions, for example, "**Sales Dept**," or "**Master Bedroom."**

Labels that can be renamed:

System: Labels		
Parameter	**Default**	**Range**
System	**G4S**	Any 16 characters
Edits the global (system) label		
Partition 1/2/3	Partitions 1 through 3	Any 16 characters
Edits partition labels		

To rename labels (using the keypad keys to produce characters), see the table below:

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 this key to toggle through all the available characters.

Sounds

Sounds contains parameters that enable you to set the sound(s) that will be produced by the system after the following system events:

System: Sounds		
Parameter	**Default**	**Range**
Tamper Sound	BELL/A Sil/D	1 to 6

Sets the sound(s) produced by a tamper violation according to the following options:

- **Silent**
- **Bell** (external/internal siren)
- **Buzzer** (main panel)
- **Bell + Buzzer**
- **Bell/A Buzzer/D:** Bell when system is armed, buzzer when system is disarmed
- **Bell/A S/Disarm:** Bell when system is armed, silence when system is disarmed

Local Speaker Alarm Volume	Level 5	0-5

Sets the main panel's internal speaker alarm volume. The volume ranges between 0 (silent) to 5 (maximum volume). After setting/changing the volume, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.

Local Speaker Squawk Volume	Level 3	0-5

Sets the main panel's internal speaker squawk volume. The volume ranges between 0 (silent) to 5 (maximum volume). After setting/changing the volume, sound will be emitted by the internal speaker to enable evaluation of the selected volume level.

Exit/Entry Beeps Volume	Level 2	0-5

Determines the volume of the beeps sounded from the main panel during the exit/entry times.

System Settings

This option enables setting the system settings for language, specific standardization, and more.

System: Settings		
Parameter	**Default**	**Range**
Default Panel		
Restores programming options to factory defaults. The Default Panel option will be followed by questions regarding the defaults of the labels and erasing wireless devices. Use to select your option.		
Erase Wireless Device		
Erase wireless devices without changing the system's current programmed parameters.		
Language		
Sets the system language (for e-mail, SMS, and keypad)		
Standards		
EN 50131	NO	
Sets the panel programming options in compliance with EN standards. See *Appendix F - EN 50131 & EN 50136 Compliance.*		
DD243	NO	
Sets the panel programming options in compliance with DD243 standards.		
CP-01	NO	
Sets the panel programming options in compliance with CP-01 standards.		
Customer		
Modify here the 3-character system Customer ID as per label format. Changing the Customer ID results in changing the system language and default settings according to the predefined factory Customer ID settings. Use this setting to alter the Customer ID specified upon first-time WiComm Pro start-up. Consult with your RISCO representative to acquire the appropriate Customer ID.		

Service Information

Service Information enables you to insert information accessible to the system's users of the alarm company from where the service is obtained.

System: Service Information		
Parameter	**Default**	**Range**
Name	Kontakt G4S	Any 16 characters
Enables you to insert and/or edit the name of the alarm company from where service may be obtained. The information can be viewed by the user using the LCD wireless keypad.		
Phone	70 33 00 40	Any 16 characters
Enables you to insert and/or edit the service phone number. The information can be viewed by the user using the wireless keypad		

Firmware Update

Firmware Update enables you to remotely upgrade the main panel firmware versions via IP or GPRS channels. Under Firmware Update you need to define the location of the upgrade file. The request to start the remote upgrade can be done from the installer keypad or via the Configuration Software. For detailed information refer to the Remote Software Upgrade Instruction Guide.

System: Firmware Update		
Parameter	**Default**	**Range**
Server IP	firmware.riscogroup.com	
Enter the IP address/URL of the router/gateway where the upgrade file is located.		
Server Port	80	
Enter the port on the router/gateway where the upgrade file is located.		
File Path	/ Wirelesspanels/4DK/FAT.txt	
Enter the upgrade file name.		

Please contact Customer Support services for the file name parameters.

Picture Server

Picture Server enables you to define a server on which to store and access images captured by system cameras. Use this feature for the http solution Web application and smartphone users.

System: Picture Server		
Parameter	**Default**	**Range**
Server IP		
Enter the IP address of the router/gateway of the server where the pictures are to be located.		
Server port		
Enter the port on the router/gateway of the server where the pictures are to be located.		
File Path		
Enter the upgrade file name. Please contact Customer Support services for the file name parameters.		
Username		
Enter user name (if required). The user name is provided the server administrator. The system supports a user name field of up to 32 alphanumeric characters and symbols (!, &, ? etc). • **Password:** Enter the password (up to 24 alphanumeric characters and symbols.) as provided the server administrator (if required).		

System: Picture Server		
Parameter	Default	Range
Image Channel		
Choose here the image transmitting channel for the http server, subject to the system's installed networks.		

Note: This feature requires that the monitoring station receiver supports the SIA IP protocol.

The four options are:

- **IP/GPRS**: The panel checks for the availability of the IP network. During regular operation mode images are transmitted using the IP network line. In the case of trouble in the IP network, the images are routed through the GPRS network.
- **GPRS/IP**: The panel checks for the availability of the GPRS network. During regular operation mode all image transmission are carried out using the GPRS. In the case of trouble, the images are routed through the IP network.
- **IP Only**: The images are transmitted through the IP network only
- **GPRS Only**: The images are transmitted through the GPRS network only

Radio Devices

The **Radio Devices** sub-menu provides access to its following options that are used for programming, defining and editing each of the system's wireless devices:

1. Allocation

2. Modification

3. Identification

4. Delete

Allocation

Each wireless device must be identified to the system receiver before its parameters can be configured. See Chapter 9 for further information on allocation procedures.

Modification

The **Modification** option is used to change the values of the parameters configured by the system for each wireless device. Modification is comprised of the following:

1. Zones

2. Remote Controls (key fobs)

3. Keypads

4. Sirens

5. I/O Expanders

NOTE: This list varies according to the devices that have been allocated to the system. Only devices that have been allocated can be configured or modified by the installer.

Zones

The **Zones** category has the following:

- **Parameters**
- **Alarm (Sequential) Confirmation**
- **Soak Test**
- **Zone Crossing**

Parameters

Note: The parameters displayed vary according to the type of zones connected to the system.

Zones: Parameters

Parameter	Default	Range
Label	Zone 01/02/03/ …	Any characters
A label identifies the zone in the system. Up to 16 characters.		
Serial Number		
The internal ID number of the zone. Each wireless device has its own unique ID number. Placing ID **00000000000** will delete the zone.		
Partition		
The partition (1 to 3) assignment for each zone.		
Type		
Each zone can be defined as one of the following types:		
Not Used		
Disables a zone. All unused zones should be given this designation.		
Exit/Entry 1		
Used for Exit/Entry doors. Violated Exit/Entry zones do not cause an intrusion alarm during the **Exit/Entry Delay.** If the zone is not secured by the end the delay expires, it will trigger an intrusion alarm. To start an arming process, this zone should be secured. When system is armed, this zone starts the entry delay time.		

Zones: Parameters		
Parameter	Default	Range
Exit/Entry 2		
Same as above, except that the Exit/Entry 2-time period applies.		
Exit(Op)/Entry 1		
Used for an Exit/Entry door. This zone behaves as described in the **Exit/Entry 1** parameter, shown above, except that, if faulted, the arming process is **not** prevented. To avoid an intrusion alarm, it must be secured before the expiration of the **Exit Delay** period.		
Exit(Op)/Entry 2		
Same as above, except that the Exit (Op)/Entry 2-time period applies.		
Entry Follower		
Usually assigned to motion detectors and to interior doors protecting the area between the entry door and the system. These zone(s) causes an immediate intrusion alarm when violated unless an Exit/Entry zone was violated first. In this case, Entry Follower zone(s) will remain bypassed until the end of the Entry Delay period.		
Intruder (Instant)		
Usually intended for non-exit/entry doors, window protection, shock detection, and motion detectors. Causes an immediate intrusion alarm if violated after the system is armed or during the Exit Delay period. When Auto Arm and Pre-Warning are defined, the instant zone will be armed at the end of the Pre-Warning period.		
Interior + Exit/Entry 1		
Used for Exit/Entry doors, as follows: • If the system is armed in the Away (Full Arm) mode, the zone(s) provide a delay (specified by Exit/Entry 1) allowing entry into and exit from an armed premises • If the system is armed in the Stay mode (Partial Arm), the zone is bypassed		
Interior + Exit/Entry 2		
Same as the **Interior + Exit/Entry 1** parameter, described above, but the Exit/Entry 2-time period is applicable.		

Zones: Parameters		
Parameter	Default	Range
Interior + Exit(Op)/Entry 1 Used for an exit/entry door that, for convenience, may be kept open when the system is being armed, as follows: • In Away (Full Arm) mode behaves as an **Exit (Op)/Entry 1** zone • In Stay mode (Partial Arm), the zone will be bypassed		
Interior + Exit(Op)/Entry 2 Same as the **Interior + Exit (Op)/Entry 1** parameter, described above, but the Exit/Entry 2-time period is applicable.		
Interior + Entry Follower Generally used for motion detectors and/or interior doors (for example, foyer), which would have to be violated after entry in order to disarm the system, as follows: • In Away (Full Arm) mode behaves as an Entry Follower zone. • In Stay mode (Partial Arm), the zone will be bypassed.		
Interior + Intruder (Instant) Usually intended for non-exit/entry doors, window protection, shock detection and motion detectors. • In Away (Full Arm) mode behaves as an Intruder (instant) zone • In Stay mode (Partial Arm), the zone is bypassed		
Entry Follower + Stay Assigned to motion detectors and to interior doors protecting the area between the entry door and the keypad, as follows: • In Away (Full Arm) mode behaves like an Entry Follower zone • In Stay mode (Partial Arm) behaves like an Exit/Entry 1 zone.		
24 Hours Usually assigned to protect non-movable glass, fixed skylights, and cabinets (possibly) for shock detection systems. A violation of such a zone causes an instant intrusion alarm, regardless of the system's state.		
Fire For smoke or other types of fire detectors. This option can also be used for manually triggered panic buttons or pull stations (if permitted), as follows: If violated, it causes an immediate fire alarm, fire report to the monitoring station.		

Zones: Parameters		
Parameter	Default	Range
Panic		
Used for external panic buttons and wireless panic transmitters. If violated, an immediate panic alarm is sounded (if the zone sound is not defined as silent or the Audible Panic system control is enabled), regardless of the system's state – and a panic report is then send to the monitoring station. An alarm display will not appear on the keypads.		
Special		
For external auxiliary emergency alert buttons and wireless auxiliary emergency transmitters. If violated, an immediate auxiliary emergency alarm is sounded, regardless of the system's state and a report is sent to the monitoring station.		
Tamper		
For tamper detection. This zone operates the same as 24 hours zone, but it has a special reporting code. **Note**: For this zone type the zone sound is determined according to the Tamper Sound defined under **System > Sound > Tamper**		
Water (Flood)		
For flood or other types of water detectors. This zone operates the same as 24 hours zone, but it has a special flood report code. See *Appendix A -- Report Codes*.		
Gas		
For Gas (natural gas) leak detectors. This zone operates the same as 24 hours zone, but it has a special gas report code. See *Appendix A -- Report Codes.*		
CO		
For CO (Carbon Monoxide) detectors. This zone operates the same as 24 hours zone, but it has a special CO report code. See *Appendix A -- Report Codes.*		
High Temperature		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code. See *Appendix A -- Report Codes.*		
Low Temperature		
For detector temperature (hot or cold). This zone operates the same as 24 hours zone, but it has a special report code. See *Appendix A -- Report Codes.*		

Zones: Parameters		
Parameter	Default	Range
Technical		
This zone operates the same as 24 hours zone, but its report code should be manually set according to the relevant detector connected to the zone.		
Final Exit		
Zones of this type must be for the last detector to be activated upon exit or the first detector to be activated upon entry. When arming the system, the related partition arms 10 seconds after this zone is closed or opened and then closed. After it is triggered once, the zone acts as an exit (open)/entry 1 zone.		
Exit Termination		
This type of zone is used to avoid a false alarm by acting like an Exit (OP)/Entry zone. When triggered (after arming the system and closing the door **or** opening the door, arming the system, and closing the door), the system's Exit Delay period will be shortened to 10 seconds. When you re-open the door, the entry time restarts. **Note:** Exit Termination requires allocation of at least one Exit/Entry zone type in the partition.		
UO Trigger		
For a device or zone, which if violated at any time triggers a previously programmed Utility Output, capable of activating an external indicator, relay, appliance, and so on.		
Day		
Usually assigned to an infrequently used door, such as an emergency door or a movable skylight. Used to alert the system user if a violation occurs during the disarmed period (trouble by day; burglary at night), as follows: • With the system armed (either Away [Full Arm] or Stay [Partial Arm]), the zone acts as an instant zone. A violation of this zone after the system is armed or during the Exit Delay time period causes an immediate intrusion alarm. • With the system disarmed, a violation of this zone attempts to alert the user by causing the trouble LED to flash rapidly This directs the user to view the system's status. Optionally, such a violation can be reported to the monitoring station as a zone trouble.		

Zones: Parameters		
Parameter	Default	Range
Pulsed Key Switch		
Connect an external momentary-action key switch to any zone given this designation. This zone will arm/disarm the partitions assigned to it.		
Pulsed Key Switch Delayed		
Used to apply the Exit/Entry Delay 1 parameter to the Pulsed Key Switch zone.		
Latched Key Switch		
Connect an external SPST latched (non-momentary) key switch as follows: ♦ After arming one or more partitions using the key switch and then disarming using the keypad, the related partitions will be disarmed. In order to arm the partition using the key switch again, turn the key to the disarm position and then to the arm position. ♦ If a key switch latch is assigned to more than one partition and one of the partitions is armed by using the keypad (the key switch stays in the disarm position), then: - When changing the position of the key switch to the arm position, all the disarmed partitions, which belong to this key switch, will be armed. - When turning the key switch to the disarm position, all the partitions will be disarmed.		

Zones: Parameters		
Parameter	Default	Range
Latch Key Switch Delay		
Used to apply the Exit/Entry Delay 1 parameter to the latched key switch zone.		
Keybox		
(Designed for the Danish market) A keybox is defined as a physical container in which to place the house keys. The WiComm Pro keybox zone behaves as follows: • Opening a key box zone (regardless of system arming status) sends a message to the monitoring station and recorded in the event log • There will be no indication on the screen that this zone is open • Tampering with a keybox causes a tamper alarm • If this zone is open, then the system can be armed		
Open Delay		
Use this zone for a door when used with wireless 2-way slim keypads defined as in bypass mode. This zone behaves as follows: • If the system is armed and the zone is opened without bypass code approval, the zone acts as an instant zone • If the system is armed and the zone is opened during the Entry Bypass timer (see page 34), it acts as an exit/entry zone • When the system is disarmed, this zone activates as an exit(open) /entry zone		
Sound	Bell+Buzzer	
Contains parameters that enable you to program the sound produced when a system zone triggers an alarm for the time defined under the Bell Time Out parameter.		
Silent		
Produces no sound.		
Bell		
Activates the wireless sirens (internal or external) and alarm from the main panel assigned to the partitions of the zone.		
Buzzer (main panel)		
Activates the internal buzzer on the main panel.		
Bell + Buzzer		
Activates the wireless sirens and siren on the main panel simultaneously.		

Zones: Parameters		
Parameter	**Default**	**Range**
Bell/Arm Buzzer/Disarm		
In a case of alarm, the following occurs: ♦ In Away mode (Full Arm) the wireless siren will operate ♦ In Disarm mode, only the buzzer on the main panel will operate		
Advanced programming		
Chime	None	
The **Chime** parameter is used as an audible indication to a zone violation while the system is disarmed.: **Options:** • None • Buzzer (Main panel) • Chime Sound 1 • Chime Sound 2 • Chime Sound 3: • Zone message: Not Applicable		
Controls		
Supervision		
Choose which zone will be supervised by the system receiver according to the time defined under the timer RX Supervision. See page *32*.		
Forced Arming Y/N		
This option enables or disables the use of forced arming for each of the system's zones, as follows: ♦ If forced arming is enabled for a particular zone, it allows the system to be armed even though this zone is faulty ♦ When zone(s) enabled for forced arming are faulted, the ✓ LED blinks during the disarm period ♦ After arming, all zones enabled for forced arming are bypassed at the end of the **Exit Delay** period ♦ If a faulted zone (one enabled for force arming) is secured during the armed period, it will no longer be bypassed and will be included among the system's armed zones		
No Activity		Y/N
Determines whether the zone participates in the No Activity function. The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people. See Timer "No Activity" on page *33*.		

Zones: Parameters		
Parameter	**Default**	**Range**
LED Enable Y/N (Only for 2 Way PIR and 2 Way WatchOUT)		Y/N
Defines the LED operation mode. YES: Detector's LED activated NO: Detector's LED deactivated		
Abort Alarm		Y/N
This parameter defines whether a zone alarm report to the monitoring station will be immediate or delayed: YES: A report to the MS will be delayed according to the Abort Time Delay parameter (**Communication > MS > MS Times > Abort Alarm**).		
Note: If a valid user code is entered to reset the alarm within the cancel delay time (**Communication > MS > MS Times > Cancel Report**), a cancel report alarm code will be sent to the monitoring station.		
NO: A report to the MS will be sent immediately.		
Detection Mode (Only for 2 Way Detectors)		Normal
• Fast (Walk Test): When the detector is in disarm it will transmit after each detection • Normal (Default): When the detector is in disarm, there will be 2.5 minutes of "dead time" between detection transmissions.		
Note: For both options, when the detector is armed it will transmit after each detection.		
Presence		Enable/Disable
A zone that is set as Presence will send a push notification to the end-user when triggered during disarm state: 1) Enable or 2) Disable sending a push notification to the end-user.		
Note: The Presence push notifications option must also be selected in the RISCO Cloud for the notifications to be sent to the end-user's smartphone. he Presence zone can also be muted via the RISCO Cloud.		
Sensitivity (Only for 2 Way PIR and 2 Way WatchOUT)		
Defines the PIR sensitivity of the detector. • Low • Medium (2 Way WatchOUT) • High • Maximum (2 Way WatchOUT)		
Camera Parameters (Only for 2 Way eyeWAVE PIR Cameras)		
Images at Alarm	3	(1–7)

Zones: Parameters		
Parameter	**Default**	**Range**
Specifies the number of images to be captured when an alarm event occurs.		
Image Interval	1.0	0.5, 1.0, and 2 seconds
Specifies the time in between image captures.		
Image Pre- Alarm	YES	YES/NO
Specifies if an image capture is to be performed upon each System Away arming. The picture is sent only in the event of an alarm occurrence, together with the alarm images.		
Image Resolution	QVGA	QVGA (320X240) VGA (640X480)
Specifies image quality, as defined by pixel resolution. A QVGA image file is approximately 7 Kb and VGA image file is 18 Kb		
Image Quality	High	High/Low
Specifies the extent of jpeg image lossy compression (Low=more compression, smaller file size; High=less compression, larger file size)		
Colored Image	YES	YES/NO
Specifies whether the captured and transmitted photographic image is to be color or black and white.		
X73 Parameters		
This section refers to the programming options of the two-way magnetic contact RWX73M and RWX73F. The programming options		
RWX73 M Parameters		
The RWX73M is a 2-way supervised transmitter that combines Magnetic/Door contact against opening doors and windows with additional universal input. The RWX73M operates with RISCO Group 2-Way wireless systems		
Magnet	Enable	**Enable/Disable**
Enable or disable the transmitter's magnet.		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm broadcasts. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period OFF: Alarm detection is immediately transmitted		

Zones: Parameters		
Parameter	**Default**	**Range**
Input Termination (IN 1):	NO	**NO**/NC/DEOL
Use this parameter to program the connection type used for each of the system's zones. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions.		
Input Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
RWX73 F Parameters (Universal/Shutter mode)		
The RWX73F is a 2-way multi-function supervised transmitter with two separate channels that combines Magnetic/Door contact (universal or shutter). The RWX73F has two reed switches for protection against opening doors and windows, and against any attempt to tamper the detector using large magnets. The RWX73F operates with RISCO Group 2-Way wireless systems		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm broadcasts. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period **OFF**: Alarm detection is immediately transmitted		
Input 2 Termination (External Zone):	NO	**NO**/NC/DEOL
Use this parameter to program the connection type used for Input 2. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions. **Shutter**: Specifies that the Input 2 will count the number of open and close pulses received. If the zone exceeds the predefined number of pulses, the zone will be tripped and act according to its type definition. After a 25-second timeout, the pulse counter is restarted. The pulse length is the currently defined Loop Response time period.		
Input 2 Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		

Zones: Parameters		
Parameter	**Default**	**Range**
Shutter Pulse	02	01-16
Define here the number of pulses for the input.		
RWX73 F Parameters (Universal mode)		
The RWX73F is a 2-way multi-function supervised transmitter with two separate channels that combines Magnetic/Door contact (universal). The RWX73F has two reed switches for protection against opening doors and windows, and against any attempt to tamper the detector using large magnets. The RWX73F operates with RISCO Group 2-Way wireless systems		
Magnet	Enable	**Enable/Disable**
Enable or disable the transmitter's magnet.		
Alarm Hold On	On	On/Off
Use this parameter to define the minimum period between alarm broadcasts. **ON:** Only one alarm message is transmitted in any 2.5 minute time-period OFF: Alarm detection is immediately transmitted		
Input 1 Termination (External Zone):	NNO	**NO**/NC/DEOL
Use this parameter to program the connection type used for Input 2. **N/O**: Uses normally-open contacts and no terminating End-of-Line Resistor. **N/C**: Uses normally-closed contacts and no terminating End-of-Line Resistor. **DEOL**: Uses normally-closed (NC) contacts in a zone using two 10 KΩ of End-of-Line Resistors to distinguish between alarms and tamper conditions.		
Input 1 Response Time	500	10–500 ms
Set the duration for which a zone violation must exist in order for the zone to trigger an alarm condition.		
Anti-Sabotage	Disable	Enable/**Disable**
Enable or disable the transmitter's anti-sabotage magnet.		
Two-way Smoke Detector Parameters		
Operation Mode		Smoke/Heat/ Smoke + Heat
Set operation mode of the two-way smoke detector (model RWX34S): • **Smoke Only:** Smoke alarm only • **Heat Only:** Heat alarm only • **Smoke + Heat:** Smoke or heat alarm		

RWX78M Parameters (2 way Slim Contact detectors)		
LED	On	On/Off
Defines the LED operation mode. On: Detector's LED activated Off: Detector's LED deactivated		
Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
RWX78S Detector Parameters (for 2 way Slim Shock detectors)		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
Shock Sensitivity	TBD	0-100%
Defines the detector's level of sensitivity.		
RWX78SM Detector Parameters (for 2 way Slim Shock and Contact detectors)		
Magnet		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
Hold On	On	On/Off
Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Shock		
Shock	Enabled	Enabled/Disabled
Defines whether to enable or disable shock detection		
LED Enabled	Yes	Yes/No
Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
Shock Sensitivity	TBD	0-100%

Defines the detector's level of sensitivity.

RWX78SM Detector Parameters (for 2 way Slim Shock and Contact detectors)

RWX78MU Detector Parameters (for 2 way Magnetic Contact and Universal detectors)			
Magnet			
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Hold On	On	On/Off
	Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Universal			
	Universal	Enabled	Enabled/Disabled
	Defines whether to enable or disable the universal zone input.		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	External Zone		NO/NC/DEOL/Shutter
	Defines the termination of the external zone input.		
	Response Time		10/500 ms
	Define the response time of the external zone input (applicable for NO and NC terminations only).		
	Hold On	On	On/Off
	Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination). **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
	Pulses number		2/4/6/8/10/12/14/16
	Defines the pulse number threshold for shutter input.		
	Input Protection	On	On/Off
	Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).		

RWX78SMU Detector Parameters (for 2 way Magnetic Contact, Shock and Universal detectors)			
	Magnet		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Hold On	On	On/Off
	Use this parameter to define the minimum period between alarm transmissions. **ON:** Only one alarm message is transmitted in any 2.5-minute time-period **OFF:** Alarm detection is immediately transmitted.		
Shock			
	Shock	Enabled	Enabled/Disabled
	Defines whether to enable or disable shock detection		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	Shock Sensitivity	TBD	0-100%
	Defines the detector’s level of sensitivity.		
Universal			
	Universal	Enabled	Enabled/Disabled
	Defines whether to enable or disable the universal zone input.		
	LED Enabled	Yes	Yes/No
	Defines the LED operation mode. Yes: Detector's LED activated No: Detector's LED deactivated		
	External Zone		NO/NC/DEOL/Shutter
	Defines the termination of the external zone input.		
	Response Time		10/500 ms
	Define the response time of the external zone input (applicable for NO and NC terminations only).		
	Hold On	On	On/Off

Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination).
ON: Only one alarm message is transmitted in any 2.5-minute time-period
OFF: Alarm detection is immediately transmitted.

Pulses number		2/4/6/8/10/12/14/16

Defines the pulse number threshold for shutter input.

Input Protection	On	On/Off

Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).

RWX78SU Detector Parameters (for 2 way Shock and Universal detectors)

Shock

LED Enabled	Yes	Yes/No

Defines the LED operation mode.
Yes: Detector's LED activated
No: Detector's LED deactivated

Shock Sensitivity	TBD	0-100%

Defines the detector's level of sensitivity.

Universal

Universal	Enabled	Enabled/Disabled

Defines whether to enable or disable the universal zone input.

LED Enabled	Yes	Yes/No

Defines the LED operation mode.
Yes: Detector's LED activated
No: Detector's LED deactivated

External Zone		NO/NC/DEOL/Shutter

Defines the termination of the external zone input.

Response Time		10/500 ms

Define the response time of the external zone input (applicable for NO and NC terminations only).

Hold On	On	On/Off

Use this parameter to define the minimum period between alarm transmissions (not applicable for shutter termination).
ON: Only one alarm message is transmitted in any 2.5-minute time-period
OFF: Alarm detection is immediately transmitted.

Pulses number		2/4/6/8/10/12/14/16

Defines the pulse number threshold for shutter input.

Input Protection	On	On/Off

Defines whether to generate a tamper message due to input wires shorted (applicable for shutter only).

Alarm Confirmation

Alarm Confirmation enables to define protection against false alarms and will be used for alarm verification.

Zones: Alarm Confirmation		
Parameter	**Default**	**Range**
Confirm Partition		
Defines which partitions will be defined for alarm sequential confirmation. Each confirmed partition has a separate timer, which is equivalent to the confirmation time defined in "Confirmation Time Window". A confirmed intruder alarm will be reported if two separate alarm conditions are detected in the same confirmed partition, during the confirmation time.		
Confirm Zones		
Define which zones will be defined for alarm sequential confirmation. When the first zone goes into alarm the system transmits the first zone alarm. When the second zone goes into alarm, during the confirmation time, the panel transmits the zone alarm and the Police code.		

Notes:

1. A confirmed zone will be part of the sequential confirmation only if the partition in which the alarm occurs is defined as confirmed partition as well.
2. Any code can reset a confirmed alarm.
3. If the first zone is violated and not restored until the end of the confirmation time (no second zone alarm), then this zone will be excluded from the confirmation process until the next arming.

Soak Test

The **Soak Test** feature is designed to allow false alarming for predefined detectors to be omitted from the system, while any alarms generated are displayed to the user for reporting to the monitoring center. This is especially useful if Police response withdrawal is being threatened and a particular zone is causing unidentified problems.

Each zone can be placed on Soak Test. Any zone placed in the Soak Test list is omitted from the system for 14 days and is automatically reinstated after that time if NO alarms have been generated by it.

If a zone in the Soak Test list has an alarm during the 14-day period, the keypad indicates to the user that the test has failed. After the user looks at the View Fault option, the fault

message will be erased. This will be indicated in the event log, but no alarm will be generated. The alarmed zone's 14-day Soak Test period is then reset and restarted.

Zone Crossing

Zone Crossing is used for additional protection from false alarms and contains parameters that enable you to link together two related zones. Both must be violated within a designated time period (between 1 and 9 minutes) before an alarm occurs.

This type of linking is used with motion detectors in *hostile* or *false-alarm prone* environments. **Default:** No cross zoning

Zones: Zone Crossing
Parameter
1st Zone
The 1st zone of a pair of zone defined for zone crossings.
2nd Zone
The 2nd zone of a pair of zone defined for zone crossings.
Time
The amount of time allowed between the triggering events for both zones to be considered a valid violation
Correlation Type
Determine how the WiComm Pro will process violations of the paired zones. • **Not correlate:** Temporarily disables any associated zone pairings • **Ordered correlate:** Effects an alarm so the first listed zone is tripped before the second • **Not ordered correlate:** Affects an alarm in which either zone in the pair may be tripped first. If this case, the specified zone order (1st, 2nd) has no bearing on the alarm activation.

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

Remote Controls / Key Fobs

Remote Controls / Key Fobs defines the operation of the remote controls / key fobs. Up to 8 remote controls / key fobs can be assigned to the system. The system supports 2 types:

- One-way (one-directional) key fobs (4-button model)
- Two-way (bi-directional) remote controls (8-button model)

The programming options under **parameters** vary according to the type of key fob or remote control (Wireless 1-Way Key Fob, or Wireless 2-Way Remote Control)

Wireless One-Way Key Fob Parameters

Each Wireless 1-Way Key Fob consists of 4 buttons, and each button can be programmed to a different mode of operation.

Remote Control Parameters – 1-Way Key Fob
Parameter
Label
A label identifying the user of the key fob.
Serial Code
The internal ID number of the key fob. Each wireless device has its own unique serial number. Placing ID **00000000000** will delete the key fob.
Partition
Assign the relevant partitions for the selected key fob.
Button 1 ( )
Set the operation of button 1 of the key fob from the following options: • **None:** Button disabled • **Arm:** The button is used for Away (Full) arming of the key fob's partitions • **Stay:** The button is used for Stay (Partial) arming of the key fob's partitions
Button 2 ( )
Set the operation of button 2 of the key fob from the following options: • **None:** Button disabled • **Disarm:** The button is used for disarming its assigned partitions
Button 3
Set the operation of button 3 (small blank button) of the key fob from the following options: • **None:** Button disabled • **Panic:** The button is used to send a panic alarm • **Status**: Main panel broadcast of system status • **UO Control (1-20):** The button is used to operate a single utility output

Remote Control Parameters – 1-Way Key Fob
Parameter
Button 4
Set the operation of button 4 (Large blank button) of the key fob from the following options: • **None:** Button disable • **Arm:** The button is used for Away (Full) arming of the key fob's partitions • **Stay:** The button is used for Stay (Home) arming of the key fob's partitions • **UO Control (1-20):** The button is used to operate a Utility Output

Wireless Two-Way Remote Control Parameters

The Wireless 2-Way Remote Control is an 8-button, rolling code wireless transmitter that is designed for remote system operation. Having bi-directional functionality enables each command that is sent to the panel to receive a reply status indication back from the panel using its multi-color LED and internal buzzer. For higher security, commands can be defined to be activated with a 4-digit PIN (personal ID number).

Remote Control Parameters –2-Way Remote Control
Parameter
Label
A label identifying the user of the remote control.
Serial Code
The internal ID number of the remote control. Each wireless device has its own unique serial number. Placing ID **00000000000** will delete the remote control.
Partition
Assign the relevant partitions for the selected remote control.
PIN Code
4-digit PIN code used for higher security when sending commands from the remote control. The code can be comprised from digits 1,2,3,4. **Note**: The use of the PIN code depends on the control *Quick UO or* system control *Quick Arm*
Panic Function
Define whether sending panic alarm from the remote control is permitted. If permitted, pressing on keys and simultaneously for 2 seconds on the remote control will send a panic alarm**.**

UO Key 1/2/3
Each remote control can activate up to 3 outputs. Assign to each of the keys 1-3 the relevant output.

Controls

Controls are relevant for both types of remote controls / key fobs.

Remote Controls / Key Fobs – Controls	
Control	
Instant Arm	NO
YES: Away arming (Full arming) from any remote control will be instant. **NO**: Away arming (Full arming) from any remote control will be delayed, following exit delay 1.	
Instant Stay	NO
YES: Stay Arming (Partial Arming) from any remote control will be instant. **NO**: Stay Arming (Partial Arming) from any remote control will be delayed, following exit delay 1.	
Disarm + Code (For 2 Way Remote Controls)	NO
Defines if a PIN code is required to perform the disarm operation while using any of the bidirectional remote controls.	

Parent Control

The Parent Control option is used to monitor the activity of children. This option allows you to monitor when the children arrive home and disarm the system or when they arm the system in Away, using a remote control or the keypad. With each activation/deactivation of the system a message is sent to a specified Follow Me number.

After selecting this option, using the key, define which of the remote controls are authorized with this feature and which are not.

Keypads

The system can support up to 3 wireless keypads. The types supported are the Wireless LCD keypad (for installer only), and the Wireless 2-Way Slim Keypad (both indoor and outdoor models).

For detailed information regarding the operation of the keypads refer to the instructions supplied with the product.

Parameters

Keypads: Parameters		
Parameter	**Default**	**Range**
Label		
A label identifying the keypad		
Serial Code		
The internal ID number of the keypad. Each wireless device has its own unique serial number. Placing ID **00000000000** will delete the remote keypad.		
Emergency Keys	YES	YES/NO
Defines whether the following keys will operate as emergency keys **LCD Keypad:** • Press Keys 4 and 5 simultaneously to send a **fire alarm** • Press Keys 7 and 8 simultaneously to send an **emergency alarm** **Slim Keypad:** • Press buttons 1 + 2 simultaneously for two seconds to send a **panic alarm** • Press buttons 3 + 4 simultaneously for 2 seconds to send a **fire alarm** • Press buttons 5 + 6 simultaneously for 2 seconds to send an **emergency / medical alarm**		
Function Key (Only for the Wireless LCD Keypad)	Panic	
Defines the operation of the ★ ★ keys for each keypad. • **Disable:** Keys disabled • **Panic:** Send a panic alarm to the monitoring station		

UO Control

Assign outputs that will be activated by a long press on keys on the bidirectional keypad.

Notes:

Outputs can be assigned only if I/O is assigned to the system.

Each keypad can activate different outputs.

Only outputs defined as *Follow Code* can be activated by the keypad keys

Mode (for the Wireless 2-Way Slim Keypad only)

Use this parameter to define the wireless 2-way slim keypad operation mode.

1. **Arm/Disarm:** the slim keypad is to have full user control of the system.
2. **Bypass:** designed for the Danish market; the slim keypad is to operate in bypass mode.

Door Bell Sound (only for slim keypad)

Use this parameter to define the chime sound (broadcast by the main panel) when the slim keypad door chime button ( ) is pressed as follows:

- None
- Chime sound 1/2/3

Controls

Controls defines programming options that are used for all keypads.

Keypads: Controls		
Parameter	**Default**	**Range**
RF Wake-up	NO	
Determines whether the system can wake the keypad up during exit/entry times or when failing to set the system. **YES**: The system wakes the keypad. **NO**: The system cannot wake up a keypad. Use this option to save battery life. (Default)		
Supervision	NO	
Choose if the keypad will be supervised or not		

Sirens

Sirens enables defining all parameters of external and internal wireless sirens that can be connected to the system. Up to 3 sirens can be added to the system.
For detailed information regarding the operation of the sirens refer to the instructions supplied with the product.

Wireless Device: Sirens		
Parameter	**Default**	**Range**
Label		
A label identifying the siren.		
Serial Code		
The internal ID number of the sirens. Each wireless device has its own unique serial number. Placing ID **00000000000** will delete the siren.		
Partition		
Assign the partitions that will effect the sounder operation.		
Supervision	YES	
Choose if the siren will be supervised or not.		
Volume	9	0-9
Define the volume of the sounder for the following scenarios in the system.		
Alarm Volume	9	0-9
The sound volume produced during an alarm (0 indicates silence).		
Squawk Volume	9	0-9
The sound volume produced during squawk sounds (0 indicates silence).		
Exit/Entry Volume	9	0-9
The sound volume produced during exit/entry time. (0 indicates silence).		
Strobe (External siren only)		
Defines the parameters for the strobe of the external siren.		
Strobe Control		
Defines the Strobe operation mode: • **Always off:** The strobe is deactivated • **Follow Bell:** The strobe is activated when the siren bell is triggered • **Follow Alarm:** The strobe is activated when an alarm event occurs in the system		

Wireless Device: Sirens		
Parameter	**Default**	**Range**
Strobe Blink	40	
Defines the number of times that the strobe will blink in a minute: • 20 times per minute • 30 times per minute • 40 times per minute • 50 times per minute • 60 times per minute		
Strobe Arm Blink	05	00-20
Defines the time that the strobe will blink when the system is armed.		

I/O Wireless Expander

The **Wireless I/O (Input/Output) Expander** is a self-powered device enabling system control of an additional 4 wired zones, with home automation capabilities. With the I/O Expander, the system has 4 physical outputs that can control 16 home-automation devices employing the X-10 protocol.

Wired Zones

The 4 inputs on the I/O Expander are regarded as zones 33-36 in the system.

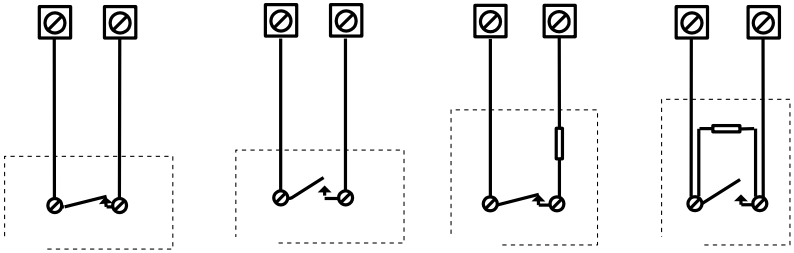
I/O Expander: Wired Zones		
Parameter	**Default**	**Range**
Label		
A label identifies the zone in the system (up to 16 characters).		
Partition	1	
The partitions assignment for each zone.		
Type	Intruder	
Contains parameters that enable you to program the zone type for any zone. Refer to the list of options for the Zone Type on page 50.		
Sound	Bell	
Not Applicable		
Advanced programming		
Chime	None	
The **Chime** parameter is used as an audible beep indication to a zone violation while the system is Disarmed.		
Control		
Forced Arm		

I/O Expander: Wired Zones		
Parameter	**Default**	**Range**
Define whether the zone can be force armed or not. For more information refer to page *57*.		
No Activity		
Determines whether the zone participates in the No Activity function. The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people. For more information refer to page *57*.		
Abort Alarm		
This parameter defines whether a zone alarm report to the monitoring station will be immediate or delayed. For more information refer to page *58*.		

Termination

The Termination menu enables you to program the connection type used for the wired zones 33-36. The actual (physical) termination for each zone must comply with that selected in the zone termination menu.

- **N/C** (Normally Closed)**:** Uses normally-closed contacts and no terminating end-of-line resistor
- **N/O** (Normally Open)**:** Uses normally-open contacts and no terminating end-of-line resistor
- **EOL**(End of Line)**:** Uses normally-closed (N/C) and/or normally-open (N/O) contacts in a zone terminated by a supplied 2200Ω (2200 ohm) end-of-line resistor



Loop response

Loop Response menu enables you to set the different times for which a wired zone violation must exist before the zone will trigger an alarm condition.

The following option are available:

Normal 400 ms	0.5 hours	2 hours	3.5 hours
Slow: 1 second	1 hour	2.5 hours	4 hours
Fast: 10 ms	1.5 hours	3 hours	

I/O Expander: Wired Zones		
Parameter	**Default**	**Range**
Detection Mode		

- **Normal** (Default): 2.5 minutes dead time between alarm detections transmissions
- **Fast** (Walk Test): Alarm detection is immediately transmitted

Output Parameters

The I/O Expander has 4 physical outputs on board: 2 relays (3 amp), and 2 transistor outputs (500 mA)

I/O Expander: Output Parameters		
Parameter	**Default**	**Range**
Label		
A label identifies the output in the system.		
Type		
There are 5 "types" of outputs in the system as follows • **Not Used** • **Follow System**: The utility output will follow a system event • **Follow Partition**: The utility output will follow a partition event • **Follow Zone**: The utility output will follow a zone event. Each utility output can be activated by a group of up to five zones • **Follow Code**: The utility output will be activated by a user defined as UO Control or from the user programming menu		
Follow System Events:		
Bell		
Activates when a bell is triggered. If a bell delay was defined, the utility output will be activated after the delay period.		
Monitoring Station Communication Fail		
Activates when communication with the Central Monitoring Station cannot be established. Deactivates after a successful call is established with the Monitoring Central Station.		
General Trouble		
Activates when a system trouble condition is detected. Deactivates after the trouble has been corrected		
Main unit Low battery		
Activates when the Pro battery has insufficient reserve capacity and the voltage decreases to 6V.		

I/O Expander: Output Parameters		
Parameter	Default	Range
AC Loss		
Activates when the source of the Main Panel's AC power is interrupted. This activation will follow the delay time defined in the system control times and the **AC Off Delay Time** parameter.		
Bell burglary		
Activates the Utility Output after any bell burglary alarm in any partition in the system.		
Scheduler		
The utility output will follow the predefined time programming that is defined in the scheduler of the weekly programs for utility output activation.		
Tamper		
Activates the utility output when a Tamper occurs in the system.		
Duress		
Activates the Utility Output when a duress alarm is initiated by any user defined as duress code.		
GSM Trouble		
Activates the utility output when there is GSM trouble in the GSM.		
Follow Open Delay		
This output is activated once an Entry Bypass timer starts (see page 34). The output is designed to be part of the bypass keypad solution for the Danish market. The output behavior depends on the output pattern as follows: **Pulsed**: Use this option to activate an electronic lock. The time duration is as defined by the installer under **Pulse Duration Length** (see page *81*). **Latched**: While the system is disarmed, entering a bypass code will activate the output like an access control reader. Output operation using the bypass code during disarm mode will not be registered in the event log. During Away (Full Arm) mode, opening an Open Delay zone (during the Entry Bypass time) will shorten the output time to 3 seconds.		
Door Bell		
Activates the utility output when a door button is pressed on a slim keypad. This output operates only as a pulse output (as defined by Pulse Duration Length (see page *81*).		
Follow Partition Events:		
Ready		

I/O Expander: Output Parameters		
Parameter	**Default**	**Range**
Activates the utility output when all the selected partition(s) are in the Ready state.		
Arm		
Activates the utility output when the selected partition(s) is armed in Away (Full Arm) mode. The utility output will be activated immediately, regardless of the Exit Delay time period.		
Disarm		
Activates the utility output Utility Output when the selected partition(s) is disarmed.		
Alarm		
Activates the utility output Utility Output when an alarm occurs in the selected partition(s).		
Intruder alarm		
Activates the utility output when an intrusion (Burglary) alarm occurs in the selected partition(s).		
Fire		
Activates the utility output when a fire alarm is triggered in the selected partition(s) from the keypads or a zone defined as Fire.		
Panic		
Activates the utility output when a panic alarm is triggered in the selected partition(s) from the keypads, remote controls or a zone defined as Panic.		
Special		
Activates the utility output when a special alarm is triggered in the selected partition(s) from the keypads or a zone defined as Special .		
Exit/Entry		
Activates the Utility Output when the selected partition(s) initiates an Exit/Entry Delay period.		
Zone Bypass		
Activates the utility output Utility Output when the relevant partitions are in ARM or STAY (Partial Arm) mode and any zone in the relevant partitions is bypassed.		
Auto Arm Alarm		
Activates the utility output when there is a not ready zone at the end of the pre- warning time during an auto-arm process. The output restore shall be on Bell-Timeout or at user Disarm.		

I/O Expander: Output Parameters		
Parameter	Default	Range
Zone Lost		
Activates the utility output when there is a lost wireless zone in the system. The output restore shall be on Bell-Timeout or at user Disarm.		
Stay Follow		
Activates the utility output Utility Output when the selected partition(s) is armed in Stay mode.		
Chime Follow		
Activates the utility output Utility Output following a chime sound in the selected partition(s)		
Bell Stay Off		
This parameter causes the utility output to function as follows: ♦ In Away arming mode, the utility output will follow the bell activation in the defined partitions. In Stay Arm (Partial Arm) mode, the utility output will not be activated.		
Bell		
♦ Activates the utility output when one of the defined partitions is in Alarm mode and the bell is triggered. This enables the connection of different sirens to different partitions.		
No Activity		
Activates the utility output when an event of NO ACTIVITY occurs in the system. . The No Activity function is for reception of signals used to monitor the activity of sick, elderly or disabled people		
Confirmed alarm		
Activates the utility output when a confirmed alarm occurs in the system.		
Follow Zone Events:		
Zone		
Activates the utility output when the selected zone is tripped. The tripped zone need not be armed to trigger the Utility Output.		
Alarm		
Activates the utility output when the selected zone causes an alarm.		
Arm		
Activates the utility output when the selected zones are armed.		

I/O Expander: Output Parameters		
Parameter	Default	Range
Disarm		
Activates the utility output when the selected zones are disarmed.		
Follow User Code:		
Defines the User Code(s) for triggering the selected utility output (UO). The activation of the UOUO is performed from the User Activities menu. Use the key to toggle between **[Y] YES** or **[N] NO** for each user chosen to trip the designated Utility Output.		
Pattern		
For each output you need to define the pattern of operation. The available options are:		
Pulse N/O (Normally Open)		
The utility output is always Deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (pulled down) for the Pulse Duration specified, then deactivates automatically.		
Latched N/O (Normally Open)		
The utility output Utility Output is always Deactivated (N/O) before it is triggered (pulled up). When triggered, it activates (pulled down) and remains activated (latched) until the operation is restored.		
Pulse N/C (Normally Closed)		
The utility output is always Activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates for the Pulse Duration specified below and then reactivates automatically.		
Latched N/C (Normally Closed)		
The utility output Utility Output is always Activated (N/C) before it is triggered (pulled down to negative). When triggered, it deactivates and remains deactivated (latched) until the operation is restored.		

I/O Expander: Output Parameters		
Parameter	Default	Range
Activation / Deactivation		
When the utility output is following more than one partition or zone, the installer can choose the logic of the utility output Utility Output activation as follows: • If the pattern operation of the output is defined as **Latch N/O** or **Latch N/C**, the activation and deactivation of the outputs can follow either after all the Partitions/Zones zones or after any of the Partitionspartitions/Zoneszones. If the Pattern operation of the output is defined as **Pulse N/O** or **Pulse N/C**, the activation of the outputs can follow either after all the Partitionspartitions/Zones zones or after any of the Partitionspartitions/Zoneszones. The deactivation operation follows the defined time period..		
Pulse Duration Length		
• The time that an output defined as Pulsed N.O or Pulsed N.C will be activated. At the end of the pulse duration the output reactivates automatically..		

X-10 Outputs

The wireless I/O Expander enables the system to control X–10 compatible devices. The I/O Expander converts the information sent from the programmable utility output into the X–10 protocol. Up to sixteen X-10 devices can be activated. These are recognized in the system as outputs 5-20.

I/O Expander: X-10 Outputs		
Parameter	Default	Range
Label		
A label identifies the output in the system		
Type		
Refer to the explanation under the utility output section.		
Pattern		
Refer to the explanation under the utility output section.		
Pulse Length	05 sec	01-90
Refer to the explanation under the utility output section.		

Parameters

The following table describes the general parameters for the I/O module.

I/O Expander: Parameters		
Parameter	Default	Range
Serial Code		

I/O Expander: Parameters		
Parameter	**Default**	**Range**
The internal ID number of the I/O Expander. Each wireless device has its own unique serial number.		
Controls		
I/O Expander Supervision Choose if the I/O Expander will be supervised or not.		
Quick Output Operation A user can activate a UO from the bidirectional remote control or keys on the wireless keypad without the need to enter his user code.		
X-10 House ID Defines the house code, which matches the code defined by the X-10 modules.		
UO DTMF Control The WiComm Pro enables to activate 8 utility outputs from remote DTMF phone. To operate a UO via the telephone you must assign a specific UO to a digit on the phone.		

Identification

This option provides the ability to identify the serial number of a wireless device in the system from a keypad or from the configuration software. When using a keypad, follow this procedure:

1. Go to **Programming > Radio Devices Menu > Identification** and press . The following message appears on the keypad LCD:

```
Please start RF
identification
```

2. Press the LEARN on the main panel to go into "Learn" mode. The serial number of the relevant device appears on the keypad LCD.

Codes

The **Codes** sub-menu enables defining parameters and codes for system users.

User

User rights can be defined by allocating each user a specific authority level and specific partitions. Up to 32 users can be defined in the system.

Codes: User Codes	
Parameter	Default
Labels	
Used to define the user name. Up to 32 characters can be used.	
Partition	
Enables you to assign the partition(s) in which all user codes (except for the Grand Master) can operate.	
Authority Level	
alocate an authority level to a user according to the following list: **User**: There are no restrictions in the number of user codes (as long as they do not exceed the number of codes remaining in the system). The user has access to the following: • Arming and disarming • Bypassing zones • Viewing system status, trouble, and alarm memory • Activating designated utility outputs • Changing his/her own user code • Setting keypad's settings **Cleaner**: The Cleaner code is a temporary code, which is to be immediately deleted from the system as soon as it is used to arm. This code is typically used for maids, home attendants, and repairmen who must enter the premises before the owner(s) arrive. These codes are used as follows: For one-time arming in one or more partitions If first used to disarm the system, the code may be used once for subsequent arming **Arm Only**: There are no restrictions in the number of Arm Only Codes (as long as they don't exceed the number of codes remaining in the system). Arm Only Codes are useful for workers who arrive when the premises are already open, but because they are last to leave, they're given the responsibility to close the premises and arm the system. The users with Arm Only codes have access for arming one or more partitions. **Duress**: When coerced into disarming the system, the user can comply with the intruder's wishes while sending a silent duress alarm to the Monitoring Station. To do so, a special duress code must be used, which when used, will disarm the system in the regular	

manner, while simultaneously transmitting the duress alarm. In any other situation the Duress authority level behaves as the same as the User authority level.

Door Bypass: Use this authority level when the slim keypad reader is defined in Bypass mode. The authorization code defined here initiates the Entry Bypass timer (see page 34). This authority is recognized only on a wireless 2-way slim keypad (not an installer's LCD keypad).

Grand Master

The Grand Master code is used by the system's owner and is the highest authority level. The owner can set/change the Grand Master code. Default is **1234**

Note: In the Configuration Software the Grand Master is identified as Code 00.

Installer

The installer code provides access to the installer Programming menu, allowing modification of all system parameters. The installer Code is used by the WiComm Pro installation company technician to program the system. The installer can change the installer code (default is **0132).**

Guard

The Guard code allows limited operations on the system. The Guard has permission to disarm the system after an alarm occurs in the system. The code will be valid only 2 minutes after alarm condition.

Default is **5678**

Note: The Guard User Code is available only for some Customer IDs.

Code Length

Code Length specifies the minimum number of digits requested. Default is 4 digits.

Notes:

When you change the **Code Length** parameter, all User Codes are deleted and must be re-programmed or downloaded.

For a 6-digit Code Length system, 4-digit default codes like **1-2-3-4** (Grand Master), **1-1-1-1** (Installer), and **5-6-7-8** (Guard) become **1-2-3-4-0-0**, **1-1-1-1-0-0**, and **5-6-7-8-0-0**, respectively.

If you change the **Code Length** back to 4 digits, the system codes are restored to the default 4-digit codes.

EN50131-3 standard specifications:

- All code length are 4 digits: xxxx
- For each digit 0-9 can be used
- All codes from 0000 to 9999 are acceptable

- Invalid codes cannot be created since after 4 digits are typed, the "Enter" is automatic. Codes are rejected when trying to create a code that does not exist.

DTMF Code

Not applicable

Parent Control

The Parent Control option is used to monitor the activity of children. This option allows all users to monitor when the children arrive home and disarm the system or when they arm the system in Away mode. With each activation/deactivation of the system a message is sent to a specified Follow Me number.

Use to toggle between **[Y] YES** or **[N] NO** for each user chosen to be assigned with the parent control feature.

Communication

The Communication sub-menu provides access to options and their related parameters that enable the system to establish communication with the monitoring station, Follow Me or Configuration Software.

The Communication sub-menu has the following options:

1. Method
2. Monitoring Station
3. Configuration Software
4. Follow-Me
5. Cloud

Method

This option allows you to configure the parameters of the following WiComm Pro communication methods (channels) :

2. GSM

3. IP

GSM

The GSM screen contains parameters for the communication of the system over the GSM/GPRS network.

Method: GSM		
Parameter	**Default**	**Range**
Timers		
Allows to program timers related to operation with the GSM module		
GSM Lost	10 min	001-255 min
The time after which the GSM module regards the GSM network as loss. Network loss is defined as RSSI level below the level defined GSM Network Sensitivity parameter.		
SIM Expire	00	00-36 months
A prepaid SIM card has a defined life length defined by the provider. After each charging of the SIM, the user will have to manually reset the expiration time of the SIM card. A notification will be displayed on the wireless keypad when asking for status indication. Set the SIM expiring date (in months) using the numeric keys, according to the time given by the provider.		
MS Keep Alive (Polling)	02160	0-65535 times
The time period that the system will establish automatic communication (polling) with the MS over GPRS, in order to check the connection. 3 polling times can be defined: Primary, Secondary and Backup. For each time period define the number of units between 1- 65535. Each unit represents a time frame of 10 seconds.		

Note: When using the polling feature through GPRS the MS channel parameter must be defined as GPRS only.
The report code for MS polling is 999 (Contact ID) or ZZ (SIA)

The use of these time periods depends on the reporting order to the MS defined by the Report Split MS Urgent parameter (See: **[4]Communication > [2]MS > [7]Report Split**)

- **Primary**: This time period is used when the MS channel is defined as ***GPRS Only*** and the Report Split parameter is <u>not</u> defined as ***1st backup 2nd***
- **Secondary**: This time period is used when the MS 2 channel is defined as ***IP>GPRS Only*** and the Report Split parameter is defined as ***1st backup 2nd***
- **Backup**: This time period will be assigned to the backup channel in the following case:
  - MS 2 channel is defined as ***IP>GPRS Only***
  - Report Split parameter is defined as ***1st backup 2nd***
  - The communication with MS 1 is disconnected

Method: GSM		
Parameter	**Default**	**Range**
GPRS		
Allows programming parameters that relate for the communication over the GPRS network.		
Access Point Network (APN) Code	internet	
To establish a connection to the GPRS network an APN (Access Point Name) code is required. The APN code differs from country to country and from one provider to another (the APN code is provided by your cellular provider). The system supports an APN code field of up to 30 alphanumeric characters and symbols (!, &, ? etc).		
APN User Name		
Enter APN user name (if required). The user name is provided by your provider. The system supports a user name field of up to 20 alphanumeric characters and symbols (!, &, ? etc).		
APN Password		
Enter the APN password (up to 20 alphanumeric characters and symbols.) as provided by your provider (if required).		
E-mail		
The following programming parameters are used to enable sending Follow Me event messages by e-mail through GPRS.		
Note: To enable e-mail messaging, the GPRS parameters have to be defined.		
Mail Host		
The IP address or the host name of the SMTP mail server		
SMTP Port		
The port address of the SMTP mail server		
Email address		
The Email address that identifies the system to the mail recipient .		
SMTP User Name		
A name identifying the user to the SMTP mail server. The user name field can include up to 10 alphanumeric characters and symbols (!, &, ? etc). Provision for future functionality		
SMTP Password		
The password authenticating the user to the SMTP mail server. The password can include up to 10 alphanumeric characters and symbols (!, &, ? etc). Provision for future functionality		

Method: GSM		
Parameter	**Default**	**Range**
Controls		
Allows to control timers related to operation with the GSM.		
Caller ID	NO	**NO/YES**
The Caller ID function enables to restrict SMS remote control operations to the predefined Follow Me phone numbers. If the incoming number is recognized as one of the Follow Me numbers, the operation will be executed.		
Disable GSM	NO	**NO/YES**
YES: The system will disable the GSM/GPRS from any activity. NO: GSM/GPRS is enabled in the system.		
CS via GPRS (out)	**YES**	**NO/YES**
YES: Enables to connect the panel to remote Configuration Software via the GPRS channel. The connection can be established either from the LCD keypad (**Installer Menu > Activities > 7)CS Connect > 2)Via GPRS)** or **via SMS** request command from the Configuration Software. **NO:** Communication between the Configuration Software and the panel via GPRS is disabled		
CS via GPRS (Listener mode)	**NO**	**NO/YES**
Not applicable		
CS via CSD	**YES**	**NO/YES**
YES: Configuration Software can attempt to contact the panel through the GSM CSD channel. **NO**: Configuration Software cannot attempt to contact the panel through the GSM CSD channel		
Parameters		
Allows to program timers related to the operation with the GSM module.		
SIM PIN Code		
The PIN (Personal Identity Number) code is a 4 to 8 digit number giving you access to the GSM network provider.		
Note: You can cancel the PIN code request function by inserting the SIM card into a regular mobile phone and according to the phone settings, disable this function.		
SMS Center Phone		
A telephone number of the message delivery center. This number can be obtained from the network operator.		

Method: GSM		
Parameter	**Default**	**Range**
GSM Network Sensitivity (RSSI) Set the minimum acceptable network signal level (RSSI level). Options: Disabled (No troubles for low signal reception) / Low signal / High signal		
SIM Number The SIM phone number. The system uses this parameter to receive the time from the GSM network in order to update the system time.		
Prepaid SIM Card Allows programming parameters that will be used when a prepaid SIM card is used in the system.		
Get Credit by Depending on the local network provider, the user can receive the credit level of the prepaid SIM card by sending a predefined SMS command to a defined number. The activation of the credit request can be done by the Grand Master. • **SMS Credit Message**: Type in the message command as defined by the provider and the provider's phone number to which the credit level SMS message request will be sent • **Voice Credit**: N/A • **Service Command**: Type in the service command message as defined by the provider		
Phone to Get Credit Message The provider's phone number to which the credit level SMS message request will be sent to or a call will be established, depending on the selection in the **Get Credit by** parameter.		
Phone to Receive SMS Credit Message: The provider's telephone number from which an automatic SMS credit status message will be sent from.		

IP

Communication Type: IP		
Parameter	**Default**	**Range**
IP Configuration		
Obtain Automatic IP	Dynamic IP	Dynamic IP/Static IP
Defines whether the IP address, which the WiComm Pro refers to, is static or dynamic. **Dynamic IP**: The system refers to an IP address provided by the DHCP. **Static IP**: The system refers to a static IP Address.		
Panel Port	01000	
Enter the WiComm Pro Port address.		
IP Address		
Enter the WiComm Pro IP address.		
Subnet Mask		
The subnet mask is used to determine where the network number in an IP address ends.		
Gateway IP		
The IP address of the local Gateway, which enables communication settings to other LAN segments. This address is the IP address of the router connected to the same LAN segment as the WiComm Pro.		
DNS Primary		
The IP address of the primary DNS server on the network.		
DNS Secondary		
The IP address of the secondary DNS server on the network		
Scan WiFi Net		
The Control panel scans for Wi-Fi networks and shortly after available networks appear in a list (the connected network is marked and appears first in the list). The rest of the list is sorted from high RSSI to low, with a max. 20 networks. Scroll to your Router's Wi-Fi network, select the desired network and then press [enter]. Enter the Password, if required, and press [enter]. If connection is successful, a successful message is displayed. If there is a connection failu re, an error message is displayed		
Add WiFi Net		
Add Wi-Fi Network		
WPS (Button)		

Communication Type: IP		
Parameter	**Default**	**Range**
Press the WPS button on the router to establish a connection and then press the WPS button on the panel within 2 min. A "Successfully Connected" to network message will appear.		
E-mail		
Allows programming parameters that enable the WiComm Pro to send Email messages following Follow Me events		
Mail Host The IP address or the Host name of the mail server.		
SMTP Port The port address of the SMTP mail server. Default: 00025		
E-mail address WiComm Pro E-mail address. Default: YourCompany.com		
SMTP User name If required by the mail server, fill in the Authentication User name		
SMTP User password If required by the mail server, fill in the Authentication User password		
Host Name	Security_System	(Up to 32 characters)
IP address or a text name used to identify the WiComm Pro over the network. Default: Security System		
MS Keep Alive (Polling)	00360	0-65535
The time period that the system will establish automatic communication (polling) with the MS over the IP network, in order to check the connection. 3 polling times can be defined: Primary, Secondary and Backup. For each time period define the number of units between 1- 65535. Each unit represents a time frame of 10 seconds.		

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

The use of these time periods depends on the reporting order to the MS defined by the Report Split MS Urgent parameter (See: **[4]Communication > [2]MS > [7]Report Split**)

- **Primary**: This time period is used when the MS channel is defined as ***IP Only*** and the Report Split parameter is not defined as ***1st backup 2nd.*** Default: 00003 (30 seconds).
- **Secondary**: This time period is used when the MS 2 channel is defined as ***IP>IP Only*** and the Report Split parameter is defined as ***1st backup 2nd.*** Default: 360 (3600 seconds).
- **Backup**: This time period will be assigned to the backup channel in the following case:
  - MS 2 channel is defined as ***IP>IP Only***
  - Report Split parameter is defined as ***1st backup 2nd***

- The communication with MS 1 is disconnected.

  Default is **00003** (30 seconds)

Controls		
Disable IP	NO	**YES/NO**
YES: The system will disable the IP from any activity. NO: The IP is enabled in the system.		
CS via IP	**YES**	**YES/NO**
YES: The system allows access to Configuration Software through an IP connection NO: The system does not allow access to Configuration Software through an IP connection		

Monitoring Station

The **Monitoring Station** option contains parameters that enable the system to establish communication with the monitoring stations (up to three) and transmit data.

Communication: Monitoring Station		
Parameter	Default	Range
Report Type		
Type		
Defines the communication type that the system will establish with each monitoring station. The system can report in 3 optional communication types: ♦ **SMS** ♦ **IP** ♦ **SIA IP**		

SMS

Events are sent to the monitoring station using encrypted SMS messages (128 BIT AES encryption). Each event message contains information including the account number, report code, communication format, time of event and more. The event messages are received by RISCO Group's IP/GSM Receiver Software located at the MS/ARC site. The IP/GSM Receiver translates the SMS messages to standard protocols used by the monitoring station applications (For example; Contact ID).This channel requires that RISCO Group's IP/GSM receiver has to be used at the MS side.
Enter the relevant phone numbers for the MS that will receive reports from the system (see page *102*).

Parameter	Default	Range

IP

Encrypted events are sent to the monitoring station over the IP or GPRS network using TCP/IP protocol. 128 BIT AES encryption is used. RISCO Group's IP/GSM Receiver Software located at the MS/ARC site receives the messages and translates them to standard protocols used by the monitoring station applications (For example; Contact ID).

Note: To enable GPRS communication the SIM card has to support GPRS channel

Reporting by IP can be established through different channels. Select the required channel via the Configuration Software as follows:

- **IP/GPRS**: The panel checks for the availability of the IP network. During regular operation mode all calls and data transmission are carried out using the IP network line. In the case of trouble in the IP network, the report is routed to the GPRS network.
- **GPRS/IP**: The panel checks for the availability of the GPRS network. During regular operation mode all calls and data transmission are carried out using the GPRS. In the case of trouble the report is routed to the IP network.
- **IP Only**: The report is executed through the IP network only.
- **GPRS Only**: The report is executed through the GPRS network. Enter the relevant IP and Port numbers for the MS that will receive reports from the system.

SIA IP

Reports to the monitoring station can be transmitted using the SIA IP protocol to standard SIA IP receivers. Using SIA IP enables transmission of visual imagery from PIR cameras. Reporting by SIA IP can be established through the hardware channels installed in your system. Reporting of the SIA IP is 128 BIT AES encrypted. SIA IP reports also support labels reporting. Usage of SIA IP requires setting:

- Encryption Key (see page 96)
- SIA IP Receiver Number
- SIA IP Receiver Line Number

Note: In the IP Address field you can enter up to 64 characters (for DNS Name of the monitoring software).

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Accounts		

Account Number

The number that recognizes the customer at the monitoring station. You can define an account number for each monitoring station. These account numbers are the 6-digit numbers assigned by the Monitoring Station.

Notes for Account Number in Contact ID Communication Format:

- The account number will always be reported as 4 digits, for example: A number defined as 000012 will be reported as 0012
- If more than 4 digits were defined, the system always sends the last 4 digits of the account number, for example: Account number that was defined as 123456 will be sent as 3456.
- In Contact ID you can place digits and letters A-F. The A character is always sent as 0 for example: Account number that was defined as 00C2AB will be sent as C20B.

Notes for Account Number in SIA Communication Format:

- Account number for SIA should be defined as a decimal number (Only digits 0..9)
- Account number can be reported as 1 to 6 digits. To send an account number with less than 6 digits use the "0" digit, for example: For account number 1234 enter 001234. In this case the system will not send the "0" digit to the monitoring station.
- In order to send the "0" digit in SIA format, located at the left side of the number, use the "A" digit instead of the "0" digit. For example, for account number 0407 enter 00A407, for a 6-digit account number such as 001207 enter AA1207.

Communications Format

Enables the system to contact the monitoring station in order to obtain details of the communication protocol used by the digital receiver for each account.

The codes are automatically uploaded when the communication format has been selected:

- **Contact ID:** The system allocates Report Codes supporting ADEMCO Contact (Point) ID
- **SIA:** The system allocates Report Codes supporting the SIA (Security Industry Association) format

Note: See Appendix A— Report Codes for the report codes list.

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Controls		
Allows to program control related to operation with the monitoring station.		
Handshake	NO	
YES: All LEDs on the WiComm Pro main panel light for one second when the handshake signal is received from the Monitoring Station's receiver. **NO:** No indication for establishing communication with the Monitoring Station's receiver.		
Kiss-Off Y/N	NO	
YES: All LEDs on the WiComm Pro main panel light for one second and an audible sound is emitted when the kissoff signal is received from the Monitoring Station's receiver. **NO:** No indication for establishing communication with the Monitoring Station's receiver.		
SIA Text		
Not Applicable		
Random MS Test		
YES: At First power up the system will set a random hour which then becomes the fixed hour for the panel to report periodic testing to the monitoring station. This time can be viewed under the Periodic test timer fields. **NO**: The periodic test will be according to the time defined by the installer defined under the MS periodic timer		
Parameters		
Allows to program parameters related to operation with the Monitoring Station.		
MS Retries	08	01-15
The number of times the system redials the Monitoring Station after failing to establish communication.		

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Alarm Restore	BTO	

Specifies under what conditions an Alarm Restoral is reported. This option informs the Monitoring Station of a change in the specified condition(s) during an alarm restore. These reports need a valid Report Code.

- **On Bell Time Out (BTO) -** Reports the restoral after the audible alarm times out.
- **Follow Zone -** Reports the restoral when the zone in which the alarm occurs returns to its non-violated (secured) state
- **At Disarm** - Reports the restoral when the system (or the partition in which the alarm occurs) is disarmed, even if the siren has already timed out

Encryption Key

A 32-digit digital signature and authentication for purposes of safeguarding data transmission to and from the monitoring station. The key must be defined for both the panel and monitoring station. For use when SIA IP report type is in effect. A unique key can be defined for each of up to three monitoring stations

Receiver Number

The receiver number as supplied from the monitoring station

Line Number

The receiver line number as supplied from the monitoring station

MS Timers

Allows to program timers related to operation with the monitoring station.

Periodic Test

The Periodic Test enables you to set the time period that the system will automatically establish communication to the Monitoring Station in order to check the connection. The periodic test involves sending the account number and a valid test report code (Contact ID 602, SIA TX). Set the test time and daily interval for Periodic Test Reporting.

Abort Alarm	15 sec	0-255 sec

Defines the time delay before reporting an alarm to the Monitoring Station. If the alarm system is disarmed within the Abort Window, no alarm transmission shall be sent to the MS.

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Cancel Delay	5 min	0-255 min
If an alarm is sent in error, it is possible for the Monitoring Station to receive a Cancel Alarm Code, sent subsequently to the initial Alarm Code. This happens if a valid User Code is entered to reset the alarm in the Cancel Delay time window that starts after the defined Abort Alarm time is over.		
Note: Cancel Alarm report code should be defined.		
Listen In	N/A	
Not Applicable		
Confirmation		
The confirmation times relate to the Zone Sequential Confirmation.		
Confirm Start (Confirm delay time)	0	0-120 min
Specifies that the system cannot start a sequential confirmation process until the timer has expired. This time starts when the system has set and will prevent confirmed alarms being generated in situations when a person has been accidentally locked in the building.		
Confirm Time Window	030	30-60 min
Specifies a time period that starts when an alarm is triggered for the first time. If a second alarm is triggered before the end of the confirmation time window, the system will send a confirmed alarm to the monitoring station.		
No Arm	0	0-12 weeks
A *No Arm* code will be sent to the Monitoring Station if no arming or disarming has been established during the time defined (1-12 weeks). (0=not activated)		

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Report Split		
The Report Split menu contains parameters that enable the routing of specified events to up to three Monitoring Station Receivers. (See *Appendix A – Report Codes*)		
MS Arm/Disarm		
Reports Arming/Disarming (meaning Closings/Openings) events to the Monitoring Station ♦ Do not call (no report) ♦ Send 1st: Reports Openings and Closings to MS 1 ♦ Send 2nd: Reports Openings and Closings to MS 2 ♦ Send 3rd: Reports Openings and Closings to MS 3 ♦ Send all: Reports Openings and Closings to the all defined MS ♦ 1st Backup 2nd: Reports Openings and Closings to MS 1. If communication is not established, calls MS 2		
MS Urgent		
Reports urgent (alarm) events to the Central monitoring station ♦ Do not call (no report) ♦ Call 1st: Reports urgent events to MS 1 ♦ Call 2nd: Reports urgent events to MS 2 ♦ Call 3rd: Reports urgent events to MS 3 ♦ Call all: Reports urgent events to the all defined MS. ♦ 1st Backup 2nd: Reports urgent events to MS 1. If communication is not established, calls MS 2		
MS Non Urgent		
Reports non-urgent events (troubles and test reports) to the MS ♦ Do not call (no report) ♦ Call 1st: Reports non-urgent events to MS 1 ♦ Call 2nd: Reports non-urgent events to MS 2 ♦ Call 3rd: Reports non-urgent events to MS 3 ♦ Call all: Reports non-urgent events to the all defined MS. ♦ 1st Backup 2nd: Reports non-urgent events to MS 1. If communication is not established, calls MS 2		

Communication: Monitoring Station		
Parameter	**Default**	**Range**
Report Codes		
Enables you to view or program the codes transmitted by the system to report events (for example, alarms, troubles, restores, supervisory tests, and so on) to the monitoring station. The codes specified for each type of event transmission are a function of the Monitoring Station's own policies. Before programming any codes, it is important to check the Monitoring Station protocols. Reporting codes are assigned by default, according to the selected communication format SIA or Contact ID Assigns a specified report code for each event, based on the reporting format to the monitoring station. An event that is not assigned with a report code will not be reported to the monitoring station. For list of report events refer to Appendix A -- Report Codes.		

Configuration Software

The **Configuration Software** option contains parameters that enable the configuration software to establish connection with the system.

Communication: Configuration software		
Parameter	**Default**	**Range**
Security		
Enables you to set parameters for remote communication between the technician and the system using the Configuration software		
Access Code Enables you to define an access code that is stored in the system. RISCO Group recommends using a different 4-digit access code for each installation. In order to enable communication between the alarm company and the system the same access code must subsequently be entered into the corresponding account profile created for the installation in the configuration software For successful communication, the access code along with the ID code must match between the configuration software and the system.	5678	

Communication: Configuration software		
Parameter	**Default**	**Range**
Remote ID		0001
Defines an ID Code that serves as an extension of the access code. In order to enable communication between the alarm company and the Installation, the same Remote ID code must be entered into the account profile in the configuration software. For successful communication, the ID code along with the access code must match between the Upload/Download software and the main panel. Dealers often use the customer's monitoring station account number for the ID Code, but you can use any 4-digit code unique to the installation		
MS Lock	000000	
MS Lock is a security function used in conjunction with the configuration software. It provides greater proprietary security when viewing monitoring station parameters. The same 6-digit code, which will be stored in the panel, must be entered into the corresponding account profile created for the installation in the Configuration software. If there is no match between the MS Lock Code defined in the Main Panel and the MS Lock Code defined in the Configuration software, the Installer will not have permission to change the following Monitoring Station parameters from the Configuration software: MS Lock, Installer Code, MS IP Port, MS IP Address, MS Phone, Default Enable, MS Account, MS Format, MS Channel, MS Backup, MS Enable, Remote ID, Access Code.		
Call Back		
Call Back Enabled	YES	
The call back feature requires the system to call back to a pre-programmed telephone number to which the alarm company's configuration software computer is installed. This provides more security for remote operations using the configuration software. **YES**: Call back is enabled **NO**: Call back is disabled		

Communication: Configuration software		
Parameter	Default	Range
Call Back Phones Define 3 numbers that the panel can call to perform Configuration Software communication. If no numbers have been defined, a call back can be performed to any phone. The installer will enter a phone number when establishing communication to the panel. If at least one number has been defined, it will be the only number that the call back can be established too. When the Configuration Software establishes communication to the panel, it sends the panel its calling phone number. (This number needs to be defined as *My Number* under the GSM Communication menu in the Configuration Software.) If the panel identifies one of the numbers as one of the numbers predefined in the panel, the call will hang up and the panel will call back to that same number.		
Configuration Software Port (IP Gateway)	00000	

The IP and port address of the configuration's software PC. If you have a router connected to the PC of the configuration software then you should enter the IP of the router.

This definition will be used when there is a request to create a remote connection from the panel to the configuration software. The connection can be done over IP or GPRS.

Note: In the configuration software, under Communication> Configuration>GPRS you should enter the IP address of the PC that the software is installed in.

IP Address

The IP address of the Configuration Software's PC

IP Port

The IP port of the Configuration Software's PC

Listener Port

The GPRS Port to which the Configuration Software can connect when GSM is in Listener mode.

Enter Host Subnet

The host subnet address (listener port number)

Follow-Me

In addition to reporting to the monitoring station, the WiComm Pro can notify end users of various system events. Reporting can be done directly from the WiComm Pro to the end user by SMS (up to 16). Reporting can also be by Email or Push Notification from the main unit or using the RISCO Cloud. When using the Cloud, the number is unlimited

Define Follow Me

Communication: Follow-Me		
Parameter	**Default**	**Range**
Label (via the Configuration Software)		
A label identifying the follow me destination		
Report Type		
Defines the type of reporting events to a Follow Me destination: • **Voice**: Not Applicable. • **SMS**: Report to Follow Me will be done by SMS. Each event message contains information including the system label, Event type and time. Type in the telephone number including area code or special letters for Follow Me destination. • **E-mail**: Report to Follow Me will be done by e-mail thorough IP or GPRS. Each e-mail contains information including the system label. Event type and time. (See *Channel > For E-mail report* below).Enter the e-mail address for Follow Me destination defined as e-mail type.		
Channel		
Email reporting events can be established through different channels. The optional channels depend on the hardware installed in the system. Select the required channel as follows: • **IP/GPRS:** The system checks for the availability of the IP network. During regular operation emails will be sent using the IP network line. In the case of trouble in the IP network, the email is routed to the GPRS network. • **GPRS/IP:** The system checks for the availability of the GPRS network. During regular operation mode emails will be sent using the GPRS. In the case of trouble, the email is routed to the IP network. • **IP Only:** The report is executed through the IP network only • **GPRS Only**: The report is executed through the GPRS network		

Events

Each Follow Me destination can be assigned with its own set of events. Choose the events that will be reported to each Follow Me

Event	Description	Default
Alarms		
Intruder	Intruder alarm in the system	Yes
Fire	Fire alarm in the system	Yes
Emergency	Emergency alarm in the system	Yes
Panic (S.O.S)	A panic alarm in the system	Yes
Tamper	Any tamper alarm in the system	No

Communication: Follow-Me		
Parameter		**Default Range**
Duress Alarm	Duress alarm in the system from user xx	Yes
No Movement	No movement report indication	No
Arm/Disarm		
Arm	Arming operation has been performed in the system	No
Disarm	Disarming operation has been performed in the system	No
Parent Control	System armed/disarmed by user/remote control defined with the Parent control feature	No
Troubles		
False Code	After 5 unsuccessful attempts of entering incorrect code.	No
Main Low Battery	Low battery indication from the WiComm Pro main panel (below 6V)	No
Wireless Low Battery	Low battery indication from any wireless device in the system	No
WL Jamming	Jamming indication in the system	No
WL Lost	Wireless device lost. When no supervision signal is received from a wireless device	No
AC Off	Interruption in the source of the main AC power. This activation will follow the delay time predefined in the AC Loss Delay timer	No
IP Network	Communication trouble with the IP network.	No
GSM		
GSM Trouble	General GSM trouble (SIM card fault, Network availability, Network Quality, PIN code error, Module communication, GPRS password, GPRS IP fault, GPRS Connection, PUK code fault	No
SIM Trouble	Any trouble with the SIM card	No
SIM Expire	Report to Follow Me will be established 30 days before the SIM Expiration Time defined for a prepaid SIM card.	No
SIM Credit	An automatic SMS credit message (or any other message) received from the provider's number predefined in *SMS Receive Phone* will be transferred to the Follow Me number	No
Environmental		
Gas Alert	Gas (natural gas) alert from a zone defined a Gas detector	Yes

Communication: Follow-Me		
Parameter	**Default Range**	
Flood Alert	Flood alert from a zone defined as flood type	Yes
CO Alert	CO (Carbon Monoxide) alert from a zone defined a CO detector	Yes
High Temperature	High Temperature alert from a zone defined a Temperature detector	Yes
Low Temperature	Low Temperature alert from a zone defined a Temperature detector	Yes
Technical	Alert from the zone defined as Technical	No
Miscellaneous		
Zone Bypass	Zone has been bypassed	No
Periodic test	Follow Me test message will be established following the time defined in the Periodic Test parameter under the MS parameters	No
Remote programming	System is in remote installation mode	No
Communication Info	The following information is sent by e-mail on power up and acquiring the GPRS and Ethernet communication parameters (assumption is that SMTP is predefined): • Panel UID • Panel version • Ethernet IP parameters • GPRS IP parameters	No
Restore Events:		
Alarms		
Intruder Alarm	Intruder alarm in the system restored	Yes
Tamper	Tamper alarm in the system restored	No
Troubles		
Main Low Battery	Low battery indication from the WiComm Pro main panel restored	No
WL Low Battery	Low battery indication from any wireless device in the system restored	No
Jamming	Jamming indication in the system restored	No
WL Lost	Wireless device lost restored	No

Communication: Follow-Me			
Parameter		**Default**	**Range**
AC Off	Interruption in the source of the main AC power restored		No
IP Network	Communication trouble in the IP restored		No
GSM Trouble	General GSM trouble restored		No
Environmental			
Gas Alert	Gas Alert restored		No
Flood Alert	Flood Alert restored		No
CO Alert	CO Alert restored		No
High Temperature	High Temperature Alert restored		No
Low Temperature	Low Temperature Alert restored		No
Technical	Technical Alert restored		No
Remote Control			
	Remote Listen	No	
	Not applicable.		
	Remote program	No	
	Enables the user of the Follow Me phone to enter the Remote Operation menu and perform all available programming options. For more details see the User manual.		
Partition			
Assign the partitions from which events will be reported to the Follow Me number.			
Controls			
Allows to program control related to operation with the Follow Me			
	Disarm Stop Follow Me	Yes	Yes/No
	YES: The Follow-Me calls will stop when the partitions are disarmed by a user code **NO**: The Follow-Me calls will continue to be made when the partitions are disarmed by a user code		
Parameters			
Allows to program parameters related to operation with the Follow Me			
	Follow Me Retries	08	01-15
	The number of times the Follow Me phone number is redialed		
	Voice Message Recurrence		N/A

Communication: Follow-Me			
Parameter		Default	Range
	Nor Applicable.		
	Follow Me Periodic Test		
	The Periodic Test enables you to set the time period that the system will automatically establish communication to a Follow Me destination defined with the Periodic Test event.		

Cloud

Define here the server settings for communication with the WiComm Pro system

	IP Address	91.221.51.215	
	The IP address or server name. If the WiComm Pro system is connected to the RISCO Cloud for self-monitoring, then use: **riscoCloud.com**. Otherwise enter the IP address or name where the Cloud server is located.		
	IP Port	33000	
	The server port address.		
	Password	AAAAAA	Up to 6 characters (case sensitive)
	Specify the password for server access. This password should be identical to the **CP Password** defined in the server under the Control Panel page definition.		
	Channel		
	Communication with the Cloud can be established through an IP or GPRS channel:. • **IP Only** • **GSM Only** • **IP/GPRS (Default)** • **GPRS/IP**		
	Controls		
	The WiComm Pro supports parallel channel reporting (via IP, GPRS or SMS) to both the monitoring station and Follow Me when connected via the Cloud. Use this setting to decide if the panel will report events to the monitoring station or Follow-Me in parallel to the report to the Cloud, or only as a backup when the communication between the WiComm Pro and the Cloud is not functioning. **Note:** When the backup mode is functioning, the monitoring station specifications are as defined under Monitoring Station (MS) menu and Follow-Me menu.		

MS Call All

Yes: Parallel reporting to the Monitoring Station can be established via both the Cloud and non-Cloud channels.

No: Communication to the Monitoring station via the non-Cloud channels can be established only in backup mode (when the WiComm Pro-to-Cloud connection is down)

FM Call All

Yes: Parallel reporting to the Follow Me destination can be established via both the Cloud and non-Cloud channels.

No: Communication to the Follow Me destination via the non-Cloud channels can be established only in backup mode (when the WiComm Pro-to-Cloud connection is down)

App Arm **YES**

Specifies if Arming operation will be active from the smartphone application

Yes: Arming from smartphone application is enabled

No: Arming from smartphone application is disabled

App Disarm **YES**

Specifies if Arming operation will be active from the smartphone application

Yes: Disarming from smartphone application is allowed

No: Disarming from smartphone application is disabled

Testing Menu

The following menu is used to perform tests on the system. Note that each test refers to the last time the device was activated. Tests can be performed on the following:

1. Main Unit
2. Zone
3. Keyfob
4. Remote Control
5. Siren
6. GSM
7. IP Unit
8. UO Unit

Main Unit

Main Unit
Parameter
Noise Level
This feature establishes the threshold noise level of the main panel ("main unit") receiver. The threshold noise level can be established automatically or manually (when using a keypad). **To establish the main unit receiver's noise level:** • **Automatic**: For automatic calibration select **[2] Calibration**. After the calibration process is accomplished, the new noise threshold level is displayed. • **Manual**: For manual calibration select **[1] View/Edit**. The value displayed is the last measured value. Set a new threshold level and press OK to confirm.
Siren
Activates the main panel siren.
Speaker
Not Applicable
Battery
Displays the battery voltage of the main panel.
Version
Displays the main panel's software version.
Serial Number
Displays the main panel's serial number.

Zone

Zone
Parameter
Comm Test
Displays the results of the last measurement performed after the last transmission (last detection or last supervision signal). To receive an updated signal strength, activate the detector prior to performing the communication test. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main panel.
Battery Test
Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.
Walk Test

Used to easily test and evaluate the operation of selected zones in your system. It is recommended to perform walk test after installing all wireless devices and also prior to performing Testing operation.
The keypad LCD displays the following information:
`Zone xx:`
` TRIP TMP TRBL`
• Zone number
• TRIP (successful detection)
• TMP (Tamper detection)
• Trbl (low battery)

Version
This menu displays software version of the selected 2-way detector.

Remote Control

Remote Control		
Parameter	**Default**	**Range**
Comm Test		
Displays the results of the last measurement performed after the last transmission. To receive an updated signal strength, activate the remote control prior to performing the communication test. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main panel.		
Battery Test		
Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.		
Version		
This menu displays information regarding the 2-way remote control's version.		

Keypad

Keypad		
Parameter	**Default**	**Range**
Comm Test		
Displays the results of the last measurement performed after the last transmission. To receive updated signal strength, activate the keypad prior to performing the communication test. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main panel		
Battery Test		
Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.		
Version		
This menu displays information regarding the keypad's version.		

Siren

Siren
Parameter
Comm Test
The siren communication test performs a communication test between the WiComm Pro and the selected siren. The value displayed indicates the siren's signal strength as received by the WiComm Pro. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main panel.
Battery Test
Speaker batteries voltage: Tests the selected siren's speaker batteries voltage. Radio (Transceiver) batteries voltage: Tests the selected siren's radio's batteries voltage.
Sound Test
Activates squawk sound in the selected siren.
Noise Level
This establishes the threshold noise level of the wireless siren receiver. The threshold noise level can be established automatically or manually (when using a keypad). **To establish a siren receiver's noise level:** 1. Select the siren for which you want to calibrate its receiver. 2. For automatic calibration select **[2] Calibration**. After the calibration process is accomplished, the new noise threshold level is displayed. 3. For manual calibration select **[1] View/Edit**. The value displayed is the last measured value. Set a new threshold level and press to confirm.
Version
This menu displays information regarding the siren's version.

GSM

GSM		
Parameter	**Default**	**Range**
Signal (RSSI)		
Displays signal level measured by the GSM module. (0=No signal, 5= Very high signal)		
Version		
Displays information regarding the GSM card version.		
IMEI		
View the IMEI number of the GSM module. This number is used for identification of the WiComm Pro at the RISCO IP receiver when using GSM or GPRS communication.		
IP Address		
The IP address given to the GSM when used in the Listener mode.		
IMSI		
International Mobile Subscriber Identity (IMSI) is a number that uniquely identifies every user of a cellular network. It is stored as a 64-bit field and is sent by the mobile device to the network.		
ICCID		
Integrated Circuit Card Identifier is a SIM card that contains its unique serial number (ICCID). ICCIDs are stored in the SIM cards and are also printed on the SIM card during a personalization process.		

IP Unit

IP Unit		
Parameter	**Default**	**Range**
IP Address		
View the IP address of the WiComm Pro		
Version		
View the version on the IP card		
MAC Address		
View the MAC address of the IP card. This number is used for identification of the WiComm Pro at the RISCO IP receiver when using IP communication.		
WiFi MAC Address		
View the Wi-Fi MAC address of the IP card. This number is used for identification of the WiComm Pro at the RISCO IP Receiver when using Wi-Fi communication.		
WiFi test		
View the received SSID (network name) and RSSI signal level: poor/fair/good/perfect.		

UO Unit

UO Unit		
Parameter	**Default**	**Range**
Comm Test		
Displays the results of the last measurement performed after the last transmission. To receive an updated signal strength, activate the UO unit prior to performing the communication test. For successful communication, the strength of the signal should be higher than the noise threshold level as measured during calibration of the main panel.		
Battery Test		
Displays the results of the last battery test performed after the last transmission. OK message is displayed for a successful test. For an updated value activate the device.		
Version		
This menu displays information regarding the UO unit's version.		

Activities Menu

The installer can perform special activities on the system via the Activities menu (some of these activities can also be performed by the user using the LCD keypad.

Activities		
Parameter	**Default**	**Range**
Main Buzzer On/Off		
Used to activate/deactivate the main panel buzzer.		
KP Sleep Time	10 seconds	00-60 seconds
Used to set the keypad's Sleep mode time. (The LCD display is turned off.)		
Service Mode		
Grand masters and Installers can silence any tamper (and suppress a report to the monitoring station) in the system from the main panel or any accessory for a period specified in Service Time (see page 34). Use this option, when system accessories require battery replacement.		
Avoid Report Programming		
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 engineer can enter the programming menu and no report will be made.		

Activities		
Parameter	**Default**	**Range**
Bypass Box Tamper		
Provides ability to bypass box tamper condition. When activated and tamper condition occurs, there will be no alarm, no indication to the Monitoring Station and no record in the event log.		
Note: To enable Bypass Box Tamper, both the **Allow Bypass** and **24-Hour Bypass** parameters must be set to **YES** (refer to page 52 and page 55 for more information).		
Installer Reset		
Use this option to reset an alarm.		
Configuration Software Connect		
Enables to establish remote communication with the configuration software at a predefined location through IP or GPRS.		
Note: The location of the configuration software should be predefined under **Communication>Configuration Software>IP Gateway**		
Firmware Update		
This option activates a firmware update process. The update can be established through IP or GPRS. The location of the new firmware should be predefined under Installer Programming> System>Firmware Update. 1. Once the communication method is selected (IP or GPRS) a special manufacturer password should be entered. Please refer to your local RISCO branch for this password.		
System Restart		
Enables to restart the main panel via the keypad.		

Activities		
Parameter	**Default**	**Range**
More		

1)WiFi

1)Scan Networks: The Control panel scans for Wi-Fi networks and shortly after available networks appear in a list (the connected network is marked and appears first in the list). The rest of the list is sorted from high RSSI to low, with a max. 20 networks.

Scroll to your Router's Wi-Fi network, select the desired network and then press [enter].

Enter the Password, if required, and press [enter]. If connection is successful, a successful message is displayed. If there is a connection failure, an error message is displayed

2)WPS(Button): Press the WPS button on the router to establish a connection and then press the WPS button on the panel within 2 min.

A "Successfully Connected" to network message will appear

Follow Me Menu

Follow Me	
Parameter	
Define	
Used to define Follow Me destinations phone number or E-mail address according to its type: SMS or E-mail	
Test FM	
Used to test Follow Me reporting.	

Clock Menu

Clock		
Parameter	**Default**	**Range**
Time + Date		
Allows the setting of the system time and date. This definition is required for setting the scheduler programming in the system.		
Scheduler		On/Off

Clock		
Parameter	**Default**	**Range**
Enables you to activate or deactivate preprogrammed schedules that were defined by your installer. Up to 8 weekly programs can be defined in the system during which the system automatically arms / disarms or activates utility outputs.		
Note: The definition of the scheduling programs is done from the configuration software.		
Automatic Clock		
Used to get an automatic time update (NTP or Daytime) through the IP network or GPRS.		
Server		
Select the Internet time protocol NTP or Daytime		
Host		
The IP address or server name.		
Port		
The server port.		
Time Zone (GMT/ UTC)		
Use the key to add an hour to the GMT/UTC time. Use the key to subtract an hour from the GMT/UTC time.		

Event Log Menu

Allows the viewing of significant system events including date and time. Scroll the list using the arrow keys to view the events in the system.

Macro Menu

Macro Keys

WiComm Pro enables the installer or Grand Master to record a series of commands and assign them to a macro. When the macro is pressed, the recorded commands are executed from beginning to end. Up to 3 macros can be programmed to a system using the LCD/Panda keypad or the WiComm Pro Configuration Software.

Before programming a macro, it is recommended to perform your required series of commands, making a note of every key you press while doing so.

NOTES:

- **Macros cannot be programmed to perform disarming commands**
- **Macros cannot be activated from slim keypad**

To program a macro:

1. In the Macro menu select a macro (**A, B** or **C**), and then press OK.
2. Enter the sequence of characters according to the following table:

Key	Represents
1 2 3 4 5 6 7 8 9 0	Used to enter numerical characters
	Used to move the curser to the left
	Used to move the curser to the right
Press **1** twice	Represents the ↑ character
Press **3** twice	Represents the ↓ character
Press **4** twice	Represents the key
Press **6** twice	Represents the key
Press **7** twice	Represents the ✱ character
Press **9** twice	Represents the # character
and **0** simultaneously	Deletes your entry from the cursor position forward
/	Use to toggle between , , ↑, ↓, #, ✱, and all of the numeric characters
OK	Used to end the sequence and save it to memory

3. Press OK to save your entry; the series of characters is saved and assigned to the selected macro. For example:

   To arm partition 1 with the code *1234*, enter the following sequence: 1 **1 2 3 4**

Activating a Macro

- Press **7/8/9** on the keypad for 2 seconds to activate the macro **A/B/C** respectively; the confirmation message "*[Macro X] activated*" will be announced.

Appendix A: Report Codes

Report Codes

Parameter	Contact ID	SIA	Report Category
Alarms			
Panic alarm	120	PA	Urgent
Panic alarm restore	*120*	*PH*	*Urgent*
Fire alarm	115	FA	Urgent
Fire alarm restore	115	FH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
Duress alarm	121	HA	Urgent
Duress alarm restore	121	HH	Urgent
Box tamper	137	TA	Urgent
Box tamper restore	137	TR	Urgent
Confirmed alarm	139	BV	Urgent
Confirmed alarm restore	139		Urgent
Recent Close	459		Non- urgent
Confirmed HU alarm (PD6662)	129	HV	Urgent
Main Troubles			
Low battery	302	YT	Non- urgent
Low battery restore	302	YR	Non- urgent
AC loss	301	AT	Non- urgent
AC restore	301	AR	Non- urgent
Clock not set	626		Non- urgent
Clock set	625		Non- urgent
False code	421	JA	Non- urgent
False code restore	421		Non- urgent
Main phone trouble	351	LT	Non- urgent
Main phone trouble restore	351	LR	Non- urgent
RF Jamming	344	XQ	Non- urgent
RF Jamming restore	344	XH	Non- urgent
GSM trouble restore	330	IR	Non- urgent
GSM Pre-Alarm			Non- urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
IP Network trouble			Non- urgent
IP Network trouble restore			Non- urgent
Arm/Disarm			
User Arm	401	CL	Arm/Disarm
User Disarm	401	OP	Arm/Disarm
Stay Arm (Partial Arm)	441	CG	Arm/Disarm
Disarm after alarm	458	OR	Arm/Disarm
Keyswitch Arm	409	CS	Arm/Disarm
Keyswitch Disarm	409	OS	Arm/Disarm
Auto Arm	403	CA	Arm/Disarm
Auto Disarm	403	OA	Arm/Disarm
Remote Arm	407	CL	Arm/Disarm
Remote Disarm	407	OP	Arm/Disarm
Forced Arm	574	CF	Arm/Disarm
Quick Arm	408	CL	Arm/Disarm
No Arm	654	CD	Arm/Disarm
Auto Arm fail	455	CI	Arm/Disarm
Detectors(Zones)			
Burglary alarm	130	BA	Urgent
Burglary alarm restore	130	BH	Urgent
Fire alarm	110	FA	Urgent
Fire alarm restore	110	FH	Urgent
Foil alarm	155	BA	Urgent
Foil alarm restore	155	BH	Urgent
Panic alarm	120	PA	Urgent
Panic alarm restore	120	PH	Urgent
Medical alarm	100	MA	Urgent
Medical alarm restore	100	MH	Urgent
24 Hour alarm	133	BA	Urgent
24 Hour alarm restore	133	BH	Urgent
Entry/Exit	134	BA	Urgent
Entry/Exit restore	134	BH	Urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
Water (Flood) alarm	154	WA	Urgent
Water (Flood) alarm restore	154	WH	Urgent
Gas alarm	151	GA	Urgent
Gas alarm restore	151	GH	Urgent
Carbon Monoxide alarm	162	GA	Urgent
Carbon Monoxide alarm restore	162	GH	Urgent
Environmental alarm	150	UA	Urgent
Environmental alarm restore	150	UH	Urgent
Low Temperature (Freeze alarm)	159	ZA	Urgent
Low Temperature restore	159	ZH	Urgent
High Temperature	158	KA	Urgent
High Temperature restore	158	KH	Urgent
Zone trouble	380	UT	Urgent
Zone trouble restore	380	UJ	Urgent
Burglary trouble	380	BT	Urgent
Burglary trouble restore	380	BJ	Urgent
Zone bypass	570	UB	Urgent
Zone bypass restore	570	UU	Urgent
Burglary bypass	573	BB	Urgent
Burglary bypass restore	573	BU	Urgent
Zone supervision loss	381	UT	Urgent
Zone supervision restore	381	UJ	Urgent
Tamper	144	TA	Urgent
Tamper restore	144	TR	Urgent
Zone lost	381	UT	Urgent
Zone lost restore	381	UJ	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Soak fail	380	UT	Urgent
Soak fail restore	380	UJ	Urgent
Zone Alarm	134	BA	Urgent
Zone Alarm restore	134	BH	Urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
Zone confirm alarm	139	BV	Urgent
Zone confirm alarm restore	139		Urgent
No activity	393	NC	Urgent
No activity restore	393	NS	Urgent
Wireless Keypad			
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Wireless Key Fob			
Arm	409	CS	Arm/Disarm
Disarm	409	OS	Arm/Disarm
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Wireless Siren			
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
Siren lost	355	BZ	Urgent
Siren lost restore	355		Urgent
Wireless I/O Expander			
Low battery	384	XT	Non- urgent
Low battery restore	384	XR	Non- urgent
I/O Expander lost	355	BZ	Urgent
I/O Expander lost restore	355		Urgent
Tamper	145	TA	Urgent
Tamper restore	145	TR	Urgent
AC trouble	301	AT	Non- urgent
AC trouble restore	301	AR	Non- urgent
RF Jamming	380	XQ	Urgent
RF Jamming restore	380	XH	Urgent

Report Codes			
Parameter	**Contact ID**	**SIA**	**Report Category**
Miscellaneous			
Enter programming (local)	627	LB	Arm/Disarm
Exit programming (Local)	628	LS (LX)	Arm/Disarm
Enter programming (Remote)	627	RB	Arm/Disarm
Exit programming (Remote)	628	RS	Arm/Disarm
MS periodic test	602	RP	Non- urgent
MS keep alive (polling)	999	ZZ	Urgent
Call back	411	RB	Non- urgent
System reset	305	RR	Urgent
Listen in begin	606	LF	Urgent
Cancel Report	406	OC	Urgent
Walk Test	607	BC	Non- urgent
Walk Test restore	607		Non- urgent
Exit Error	374		Non- urgent
Enter Quick Learn	627	LB	Urgent
Exit Quick Learn	628	LS	Urgent
Enter Service Mode	393	LB	Non- urgent
Exit Service Mode	393	LX	Non- urgent
Finished Uploading Pictures			Urgent
MS Trigger		ZY	Non- urgent
MS Trouble			Non- urgent
Fail Cloud Communication			Non- urgent

Appendix B: Installer Event Log Messages

* Event message display cannot be suppressed, as specified by EN50131-1-2006.

Event Message	Description
Activate UO=xx	UO XX activation
Actv UO=xx KF=zz	UO XX is activated from remote control ZZ
AL Reinstate P=y	Alarm reinstatement on partition Y
Alarm abort P=y	Alarm aborted on partition Y
* Alarm Zone=xx	Alarm in zone no. XX
* Anti-code reset	Remote reset
Auto Add GSM	GSM added to the main panel
Auto Add IP card	IP added to the main panel
Auto Add MODEM	Modem added to the main panel
Auto Del GSM	GSM was removed from the main panel
Auto Del IP card	IP removed from the main panel
Auto Del MODEM	Modem removed from the main panel
Auto test fail	Failure of zone self-test
Auto test OK	Automatic zone self-test OK
* Away fail P=y	Partition Y failed to arm
* Away:P=y C=zz	Partition Y armed by user no. ZZ
* Away:P=y KF=zz	Partition Y armed by remote control ZZ
* Bell tamper	Bell tamper alarm
Bell tamper rst	Bell tamper alarm restore
* Box tamper	Box tamper alarm from main panel
Box tamper rst	Box tamper alarm restore
* Bypass Box+Bell	Box + Bell tamper is bypassed
Bypass code=xx	Bypass code XX has been used
* Bypass Trbl C=xx	System troubles were bypassed by user XX
* Bypass Zone=xx	Zone no. XX is bypassed
Cancel Alarm P=x	Cancel alarm event has occurred from partition X. A valid user function is entered to reset the alarm after the defined Abort alarm time.
Change code=xx	Changing user code XX
Change FM=yy	Changing Follow-Me number YY
Change tag=xx	Changing keypad tag for user XX
Clock not set	Time is not set
Clock set C=xx	Time defined by user no. XX
Cloud Connected " ,	Cloud communication channel is functioning
Cloud Disconnect" , //	Cloud communication channel is not functioning
CO Alarm Zn=xx	CO alert from zone XX defined as a CO detector
CO Rst. Zn=xx	CO alert restored from zone XX defined as a CO detector
Com ok IP card	Communication OK between the WiComm Pro and IP card

Comm OK Siren=y	Communication OK between the WiComm Pro and Siren Y
Comm. OK GSM	Communication OK between the WiComm Pro and GSM
Comm.OK I/O Mdl.	Communication OK between the WiComm Pro and I/O module
* Conf. alarm P=y	Confirmed alarm occurred in partition Y
Conf. Hold-Up P=y	Confirmed Hold-Up Alarm in partition Y
Confirm rs Z=xx	Restore zone confirmed alarm
* Confirm Zone=xx	Confirmed alarm occurred from zone XX
CP reset	The control panel has reset
Date set C=xx	Date defined by user no. XX
* Day Away:P=y	Daily arm on partition Y
Day disarm:P=y	Daily disarm on partition Y
* Day stay: P=y	Daily Stay Arming (Partial Arming) in partition Y
Device Tmpr Byp	Device Tamper Bypass
* Disarm:P=y C=zz	Partition Y disarmed by user ZZ
* Disarm: P=y KF=zz	Partition Y disarmed by remote control ZZ
Duress C=xx	Duress alarm from user no. XX
Enter program	Entering installer programming from keypad or configuration software
Exit Error Zn=xx	Exit error event from zone XX The zone was left open at the end of the exit time
Exit program	Exiting installer programming from keypad or configuration software
False code	False code alarm
False restore	False code alarm restore
Fire Keypad=y	Fire alarm from wireless keypad Y
Fire main KP	Fire alarm from
Fire ok Zone=xx	Trouble restore in fire zone no. XX
Fire trbl Zn=xx	Trouble in fire zone no. XX
* Fire Zone=xx	Fire alarm in zone no. XX
Foil ok Z=xx	Restore in foil (Day) zone no. XX
Foil Zone=xx	Trouble in foil (Day) zone no. XX
Forced P=y	Partition Y is force armed
Found Zone=xx	Wireless zone found, zone no. XX
* Gas Alarm Zn=xx	Gas (natural gas) alert from zone XX defined as a gas detector
Gas Rst. Zn=xx	Gas (natural gas) alert restored from zone XX defined as a gas detector
GSM:IP OK	IP connection OK
GSM:IP Trouble	IP address is incorrect
GSM:Mdl comm.OK	Communication between the GSM/GPRS Module and the WiComm Pro is OK
* GSM: Module comm.	Internal GSM/GPRS BUS module trouble
* GSM:NET avail.	GSM network is not available

GSM:NET avail.OK	GSM Network is available
GSM:NET qual.OK	GSM Network quality is acceptable
GSM:NET quality	The GSM RSSI level is low
GSM:PIN code err	PIN code entered is incorrect
GSM:PIN code OK	PIN code is correct
GSM:PUK Code err	PUK code required
GSM:PUK Code OK	PUK Code entered is correct
GSM:SIM OK	SIM Card in place
GSM:SIM trouble	SIM card missing or not properly sited
H.Temp rst Zn=xx	High temperature alert restored from zone XX defined as a temperature detector
* High Temp. Zn=xx	High temperature alert from zone XX defined as a temperature detector
HU Reinstate P =Y	Hold-Up Reinstatement in partition y
I/O:AC Rstr	AC power restore on I/O module
I/O:AC Trouble	AC power trouble on I/O module
I/O: Battery Rstr	I/O module battery trouble restored
* I/O: Battery Trbl	I/O module battery trouble alert
* I/O: Jamming	I/O module jamming alert
I/O: Jamming Rstr	I/O module jamming alert restored
* I/O: Lost	I/O module is regarded as lost following supervision test
* I/O: Tamper	I/O module tamper alert
I/O: Tamper Rstr	I/O module tamper alert restored
IO: Lost Restore	The WiComm Pro received a signal from I/O module after it has been regarded as lost
IPC:DHCP error	Failed to acquire an IP address from the DHCP server
IPC:DHCP ok	Succeeded to acquire an IP address from the DHCP server
* IPC: Network err	Failed to connect to IP network
IPC: Network ok	Successful connection to IP network
IPC:NTP error	Failed to acquire time data from the time server
IPC:NTP ok	Succeeded to acquire time data from the time server
Jamming OK Zn=xx	Zone XX jamming OK
Jamming restore	Wireless receiver jamming restore
* Jamming Z=xx	Zone XX jamming trouble
KeyBox Open Z=!!	Zone XX defined as KeyBox type is open
KeyBox Rst Z=!!	Zone XX defined as KeyBox type is closed
KP=y Low Bat.Rst	Low battery trouble restored from keypad Y
* KP=y Low Battery	Low battery trouble from keypad Y
* Ksw away:P=y	Partition Y is armed by key switch
* Ksw disarm:P=y	Partition Y is disarmed by key switch
L.bat rstr KF=yy	Low battery trouble restore from wireless remote control YY

L.Temp rst Zn=xx	Low temperature alert restored from zone XX defined as a temperature detector
* Lost Zone=xx	Wireless zone lost, zone no. XX
Low Bat rs Z=xx	Low battery trouble restored from wireless zone no. XX
Low bat. Zn=xx	Low battery trouble from wireless zone no. XX
Low bat.KF=yy	Low battery trouble from wireless remote control XX
* Low Temp. Zn=xx	Low temperature alert from zone XX defined as a temperature detector
Main:AC restore	AC power restore on main panel
Main: Battery rst	Low battery trouble restore from the main panel
Main: Low AC	Loss of AC power from the main panel
Main: Low battery	Low battery trouble from the main panel
* MS=y call error	Communication fail trouble to MS phone no. Y
* MS=y restore	Communication fail trouble restore to MS phone no. Y
No Com IP card	Communication failure between the WiComm Pro and IP card
* No comm I/O Mdl.	Communication failure between the WiComm Pro and I/O module
* No comm Siren=y	Communication failure between the WiComm Pro and siren Y
* No comm. GSM	No communication between the GSM/GPRS Module and the WiComm Pro
* Phone fail	If the phone line is cut or the DC level is under 1V
Phone restore	Phone line trouble restore
* Police Keypad=y	Police (panic) alarm from wireless keypad Y
* Police KF=yy	Police (panic) alarm from remote control YY
PTM: Send Data	Load new parameters into the WiComm Pro from PTM accessory
* Radio l.bat S=y	Radio low battery trouble from siren Y
Radio l.bat rS=y	Radio low battery restore from siren Y
* Remote away:P=y	The system has been armed from the configuration software
* Remote program	The system has been programmed from the configuration software
* Remote stay:P=y	The system has been armed in STAY mode from the configuration software
Restore Zone=xx	Alarm restore in zone no. XX
* RF Jamming	Wireless receiver jamming
Rmt disarm:P=y	Partition Y disarmed from the configuration software
* Siren=y Lost	Siren Y is regarded as lost following supervision test
Siren=y Lost Rst	The WiComm Pro received a signal from siren Y after it has been regarded as lost
Soak fail Z=xx	Zone XX has failed in the soak test
Special KP=y	Special alarm from the from wireless keypad Y
Spkr l.bat rsS=y	Speaker low battery restore from siren Y
* Spkr low bat S=y	Speaker low battery trouble from siren Y
Start exit P=y	Exit time started in partition Y
* Stay:P=y C=zz	Partition Y Stay Armed (Partial Armed) by user ZZ

* Stay: P=y KF=zz	Partition Y Stay Armed (Partial Armed) by remote control ZZ
* Tamper I/O Mdl.	Tamper alarm from I/O module
Tamper I/O Mdl.	Tamper alarm restored from I/O module
* Tamper Keypad=y	Tamper alarm from keypad ID=Y
Tamper rs Zn=xx	Tamper alarm restore on zone no. XX
Tamper rst KP=y	Keypad Y tamper restore
* Tamper Siren=y	Tamper alarm from wireless siren Y
* Tamper Zone=xx	Tamper alarm from zone no. XX
* Tech alarm Zn=xx	Alarm from zone XX defined as Technical
Tech rstr Zn=xx	Alarm restored from zone XX defined as Technical
Tmp rstr Siren=y	Tamper alarm restore from wireless siren Y
Unbyp Box+Bell	Box + Bell reinstated from bypass
Unbypass Zone=xx	Zone no. XX is reinstated from bypass
Unknown event	Unknown event alert
User login C=xx	User XX has entered into programming mode. User 99 represents remote programming from the configuration software
* Water Alrm Zn=xx	Flood alarm from zone no. XX
Water rstr Zn=xx	Flood alarm restore on zone no. XX
Z=xx auto bad	Zone self-test failed, zone no. XX
Z=xx auto ok	Zone self-test OK, zone no. XX
Zn=xx Trouble	Zone trouble event from zone XX
Zn=xx Trouble OK	Zone trouble event restore from zone XX

Appendix C: Remote Firmware Upgrade

This appendix explains how to perform remote upgrade of your WiComm Pro main panel software using the WiComm Pro Configuration Software. Remote software upgrade is performed via IP or GPRS.

Prerequisites

- Configuration Software version 1.0.1.7 and later
- WiComm Pro Main Panel version 1.77 and later
- WiComm Pro system with GSM/GPRS or IP

IMPORTANT: Back up all client information (i.e. panel parameters) before performing a firmware upgrade with an established connection to the WiComm Pro main panel

Step 1: Verifying the current version of the main panel

In order to later confirm that the upgrade procedure has been successful (step 4), take note of the current version of your WiComm Pro main panel software.

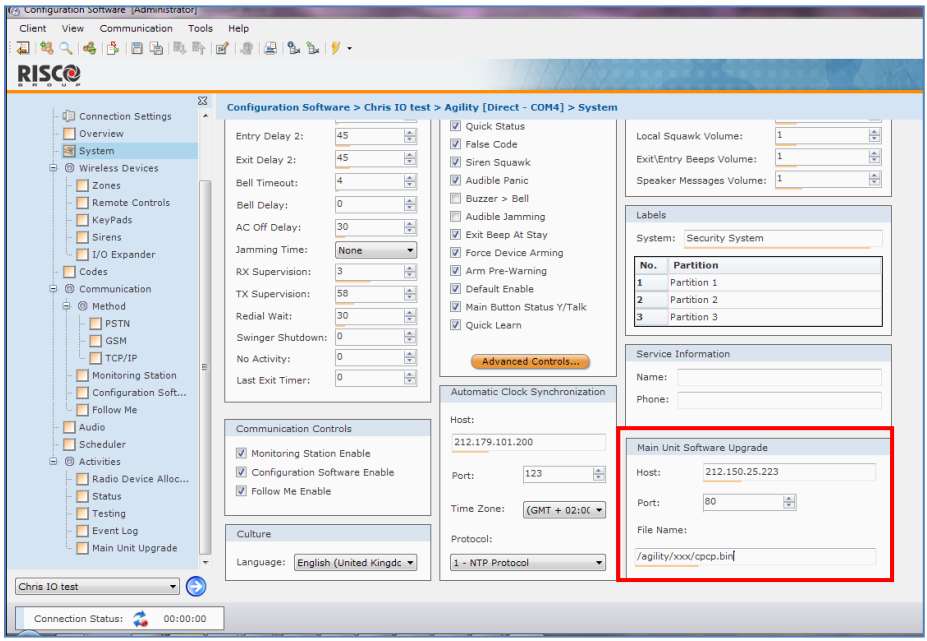
1. Login to the WiComm Pro Configuration Software program.
2. Select a client.
3. Click **Connect** to establish connection to the WiComm Pro main panel.
4. Go to the **Activities** > **Testing** screen.
5. In the Main Unit tab, click the **Test** button. The current version of the main panel appears in the Panel version textbox.

Step 2: Entering the location of the upgrade file

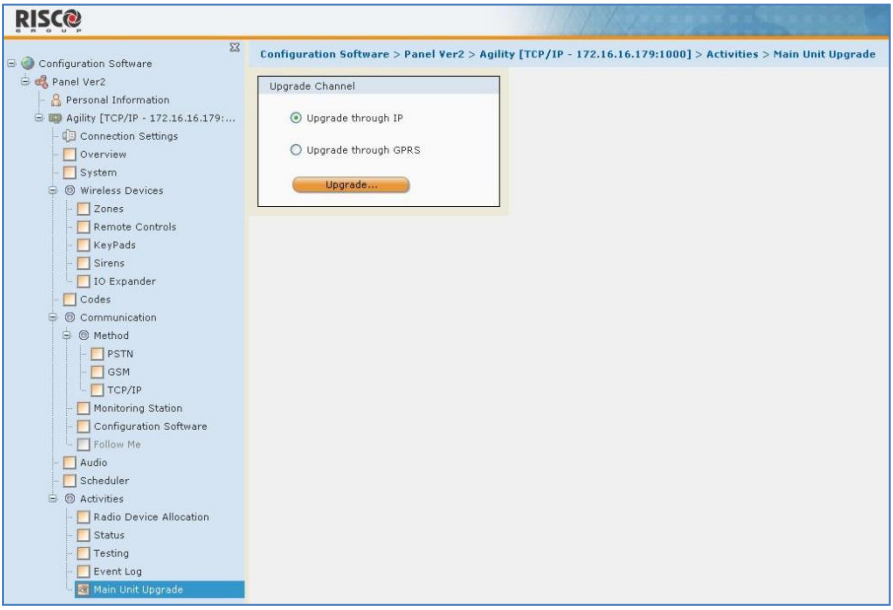
1. In the **System** screen, in the Main Unit Software Upgrade section, enter the relevant information regarding the location of the upgrade file:
   - **Host**: Enter the IP address of the router/gateway where the upgrade file is located (default is **212.150.25.223).**
   - **Port**: Enter the port on the router/gateway where the upgrade file is located (default is **80).**
   - File **Name**: Enter the upgrade file name. For example: **/ Wirelesspanels/4DK/FAT.txt**

NOTE: Please contact Customer Support services for the file name parameters.

2. Click **Send** .

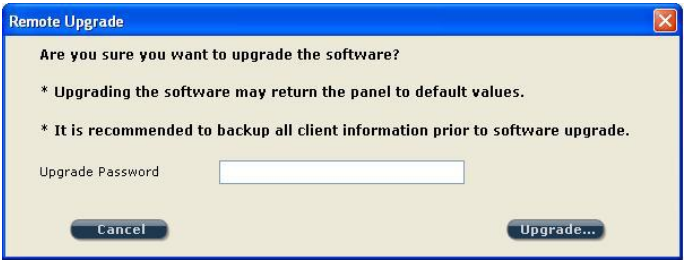


Step 3: Performing an upgrade



NOTE: Make sure you are online and connected to the WiComm Pro main panel (if not, click Connect).

1. In the **Activities > Main Unit Upgrade** screen, select the upgrade channel:
   - **Upgrade through IP**
   - **Upgrade through GPRS**
2. Click Upgrade... ; the following dialog box appears:



IMPORTANT: The message in the dialog box informs you that performing a remote software upgrade may result in returning the main panel to its default values, therefore it is recommended to backup all client information before performing the upgrade:

3. Enter the Upgrade Security password, and then click **Upgrade….** Please contact Customer Support services at your local RISCO Group branch for the password.

NOTE: For users with Configuration Software version 1.0.2.0 and above, when the following message appears "*The upgrade process will commence after disconnecting this session,*" click OK.

4. Disconnect from the current session by clicking to begin the upgrade procedure; the LEDs on the WiComm Pro main panel will begin to flash during the upgrade procedure as follows: The Power LED will light up and the other LEDs will flash rapidly.

NOTES:

- **The upgrade procedure may take approximately 13 minutes to complete. This will vary according to whether the procedure is performed via GPRS or IP.**
- **If upgrade fails, the previous WiComm Pro main panel software version is automatically recovered.**

Step 4: Restoring panel–system communication

In the event that the firmware upgrade involved a database change, the panel resets all parameters (except the saved **Communication parameters** as listed in the table below).

In this case, to re-enable the WiComm Pro—panel communication, reconnect to the panel from the Configuration Software and "Send All" parameters as follows:

- Select **Communication > Send > All**

List of Saved (Communication) Parameters	
a. System Parameters:	i. CS Enable ii. FM Enable. iii. MS Enable iv. Cloud Enable v. Disable incoming call vi. Random periodic test vii. SIA with text viii. CS Call back
b. MS Parameters:	i. MS LOCK
c. Configuration Software Parameters:	i. Access code ii. Remote ID iii. All the CS enable flags (IP, GSM in, out, SCD). 1. CS via GPRS (out) 2. CS via GPRS (List) 3. CS via CSD 4. CS via IP 5. CS via Modem
d. Codes:	i. Installer code ii. Sub installer code iii. GM Code
e. GSM Parameters:	i. GSM APN code ii. GSM APN user iii. GSM APN password iv. GSM PIN Code
f. IP Parameters:	i. IP Dynamic/Static ii. IP Address iii. IP Subnet iv. IP Gateway v. IP NetBIOS name vi. IP DNS1 vii. IP DNS2
g. Cloud Parameters:	i. Cloud CHANNEL ii. Cloud PASSWORDELAS PORT. iii. Cloud IP

Appendix D: Installer Programming Maps

1) Programming	See *Testing Menu* on page 108		
2) Testing			
	1) Main Unit		
		1) Noise Level	4) Battery
		2) Siren	5) Version
		3) Speaker	6) Serial Number
	2) Zone		
		1) Communication Test	3) Walk Test
		2) Battery Test	4) Version
	3) Remote Control		
		1) Communication Test	3) Version
		2) Battery Test	
	4) Keypad		
		1) Communication Test	3) Version
		2) Battery Test	
	5) Siren		
		1) Communication Test	4) Noise Level
		2) Battery Test	5) Version
		3) Sound Test	
	6) GSM		
		1) Signal	4) IP Address
		2) Version	5) IMSI
		3) IMEI	6) ICCID
	7) IP Unit		
		1) IP Address	4) WiFi Mac addr
		2) Version	5) WiFi test
		3) MAC Address	
	8) I/O Module		
		1) Communication Test	3) Version
		2) Battery Test	
3) Activities			
	1) Main Buzzer		
	2) KP Sleep Time		
	3) Siren TMP Mute		
	4) Avoid Report Prog		
	5) Bypass Box Tamp		
	6) Installer Reset		
	7) CS Connect		
	8) Firmware Update		
	9) System Restart		
	0) More		
		1)WiFi	
4) Follow Me			
	1) Define		
	2) Test Follow Me		

5) Clock			
	1)Time and Date		
	2) Scheduler Enable		
	3) Auto. Clock		
		1) Server	3) Port
		2) Host	4) Time Zone
6) Event Log			
7) Macro			

Installer Programming menu:

1) System				
1) Timers				
	1) Ex/En Delay 1			
	2) Ex/En Delay 2			
	3) Bell Timeout			
	4) Bell Delay			
	5) AC Off Delay			
	6) Jamming Time			
	7) RX Supervision			
	8) TX Supervision			
	9) Redial Wait			
	0) More			
		1)Swinger Shutdown		
		2) No Activity		
		3) Last Exit Sound		
		4) Entry Bypass		
		5) Service Time		
2) Controls				
	1) Basic			
		Quick Arm		
		Allow Bypass		
		Quick Status		
		False Code Trouble		
		Siren Squawk		
		Audible Panic		
		Buzzer > Bell		
		Audible Jamming		
		Exit Beeps At Stay		
		Forced Arming		
		Arm Pre-Warning		
		Default Enable		
		Main But: Status/Talk		
		Quick Learn		
	2) Advanced			
		Area		
		Global Follower		
		Summer/Winter		
		24 Hour Bypass		

		Technician Tamper		
		Technician Reset		
		Installer Tamper		
		Low Battery Arm		
		Siren Pre-alarm		
		Bell 30/10		
		Fire Alarm Pattern		
		IMQ		
		Disable Incoming Call		
		Bypass Unique Code		
		Silent Remote Install		
		AntiMask		
		Power Management		
		Presence		
		Secondary Alarm		
	3) Communication			
		MS Enable		
		Configuration Software Enable		
		FM Enable		
		Cloud Enable		
	4) EN 50131			
		Authorize Installer		
		Override Trouble		
		Restore Alarm		
		Mandatory Events		
		Restore Troubles		
		Exit Alarm		
		Entry Alarm		
		20 Minutes Signal		
		Attenuation		
	5) DD243 Prog			
		Bypass Exit/Entry		
		Entry Disable		
		Route Disable		
		Installer Confirmation		
		Keyswitch Lock		
		Entry Disarm		
	6) CP-01			
		Exit Restart		
		Auto Stay		
		Exit Error		
		3 Min. Bypass		
3) Labels				
	1) System			
	2) Partition 1			
	3) Partition 2			
	4) Partition 3			

4) Sounds				
	1) Tamper Sound			
		Silent		
		Bell		
		Buzzer (main)		
		Bell + Buzzer		
		Bell/A + Buzzer/D		
		Bell/A + S/Disarm		
	2) Local Alarm			
	3) Local Squawk			
	4) Ex/En Beeps			
	5) Speaker Volume			
5) Settings				
	1) Default Panel			
	2) Erase WL Device			
	3) Language			
	4) Standards			
		EN 50131		
		DD243		
		CP-01		
	5) Customer			
6) Service Info				
	1) Service Name			
	2) Phone			
7) Firmware Update				
	1) Server IP			
	2) Server Port			
	3) File Path			
8) Picture Server				
	1) Server IP			
	2) Server Port			
	3) File Path			
	4) Username			
	5)Password			
	6) Image Channel			
2) Radio Devices				
1) Allocation				
	1) RF Allocation			
	2) By Serial code			
	3) Zone Allocation			
2) Modification				
	1) Zones			
		1) Parameters		
			1) Label	
			2) Serial No.	
			3) Partition	
			4) Type	
			5) Sound	

			6) Advanced	
			1) Chime	
			2) Control	
			Supervision	
			Forced Arming	
			No Activity	
			LED Enable	
			Abort Alarm	
			Presence	
			3) Detection Mode	
			4) Sensitivity	
			5) Camera Parms	
			Images at Alarm	
			Image Interval	
			Image Pre-Alarm	
			Image Resolution	
			Image Quality	
			Colored Image	
			6) X73/X78 Contact	
			Magnet	
			Alarm Hold On	
			Input Termination	
			Input Response Time	
			Magnet	
			7) Two-way Smoke Detector	
			Operation Mode	
		2) Alarm Confirmation		
			1) Confirm Partition	
			2) Confirm Zones	
		3) Soak Test		
		4) Cross Zones		
	2) Keyfobs			
		1) Parameters		
			1-Way Keyfob	***2-Way Keyfob***
			1) Label	1) Label
			2) Serial No.	2) Serial No.
			3) Partition	3) Partition
			4) Button 1	4) PIN Code
			5) Button 2	5) Panic Enable
			6) Button 3	6) UO Button 1
			7) Button 4	7) UO Button 2
				8) UO Button 3
		2) Controls		
			Instant Arm	
			Instant Stay	
			Code Disarm	
		3) Parent Control		

	3) Keypads			
		1) Parameters	1) Label	
			2) Serial No.	
			3) Emergency Keys	
			4) Function Key (LCD Only)	
			5) UO Control	
			6) Mode (Slim only)	
			7) Door Bell Sound(Slim only)	
		2) Controls		
			RF Wake-up	
			Supervision	
	4) Sirens			
		1) Label		
		2) Serial Number		
		3) Partition		
		4) Supervision		
		5) Volume		
			1)Alarm	
			2) Squawk	
			3) Exit Entry	
		5) Strobe (Ext.l)		
			1)Strobe Ctrl	
			2) Strobe Blink	
			3)Strobe Arm Blink	
	5) I/O Modules			
		1) Wired Zones		
			1) Label	
			2) Partition	
			3) Type	
			4) Sound	
			5) Advanced	
			1) Chime	
			2) Control	
			3) Termination	
			4) Loop Response	
			5) Detection Mode	
		2) Outputs		
			1) Label	
			2) Type	
			3) Pattern	
			4) Pulse Length	
		3) X-10 Outputs		
			1) Label	
			2) Type	
			3) Pattern	
			4) Pulse Length	
		4) Parameters		
			1) Serial No.	

			2) Control	
				1) Supervision
				2) Quick UO/X10
			3) X10 House ID	
			4) UO DTMF Control	
3) Identification				
3) Codes				
1) User				
	1) Label			
	2) Partition			
	3) Authority			
		User		
		Cleaner		
		Arm Only		
		Duress		
		Door Bypass		
2) Grand Master				
3) Installer				
4) Sub-Installer				
5) Code Length				
	4 Digits			
	6 Digits			
6) DTMF Code				
7) Parent Control				
4) Communication				
1) Method				
	2) GSM			
		1) Timers		
			1) GSM Lost	
			2) SIM Expire	
			3) MS Keep Alive (Polling)	
		2) GPRS		
			1) APN Code	
			2) APN User Name	
			3) APN Password	
		3) Email		
			1) Mail Host	
			2) SMTP Port	
			3) E-mail Address	
			4) SMTP User Name	
			5) SMTP Password	
		4) Controls		
			Caller ID	
			Disable GSM	
			CS via GPRS (out)	

			CS via GPRS (Listener mode): N/A	
			CS via CSD	
		5) Parameters		
			1) SIM PIN Code	
			2) SMS Center Phone	
			3) GSM RSSI	
			4) SIM Number	
		6) Pre-Paid SIM		
			1) Get Credit by	
			2)SMS Receive Phone	
	3) IP			
		1) IP Configuration		
			1) Obtain Auto IP	
			2) Panel IP	
			3) IPAddress	
			4) Subnet Mask	
			5) Gateway	
			6) DNS Primary	
			7) DNS Second	
			8) Scan WiFi Net	
			9) Add WiFi Net	
			10) WPS (Button)	
		2) E-mail		
			1) Mail Host	
			2) SMTP Port	
			3) E-mail Address	
			4) SMTP Name	
			5) SMTP Password	
		3) Host Name		
		4) MS Keep Alive (Polling)		
		5) Controls		
			Disable IP	
2) Monitoring Station				
	1) Report Type			
		Voice: N/A		
		SMS		
		IP		
		SIA IP		
	2) Accounts			
	3) Comm Format			
		Contact ID		
		SIA		
	4) Controls			
		Handshake		
		Kissoff		
		SIA Text		
		Random MS Test		

	5) Parameters			
		1) MS Retries		
		2) Alarm Restore		
		3) Encryption Key		
	6) MS Timers			
		1) Periodic Test		
		2) Abort Alarm		
		3) Cancel Delay		
		4) Not applicable		
		5) Confirmation		
		6) No Arm		
	7) Report Split			
		1) MS Arm/Disarm		
		2) MS Urgent		
		3) MS Non Urgent		
	8) Report Codes			
		1) Edit Codes		
		2) Delete All		
3) Configuration s/w				
	1) Security			
		1) Access code		
		2) Remote ID		
		3) MS Lock		
	2) Call Back			
		Call Back Enabled		
		Call Back Phones		
	3) CS / IP Gateway			
	4)IP Address			
	5)IP Port			
	6)Listener Port			
	7)Ent Host Subent			
4) Follow-Me				
	1) Define			
		1) Report type		
			Voice : N/A	
			SMS	
			Email	
		2) Events		
		3) Restore events		
		4) Remote control		
			N/A	
			Remote program	
		5) Partition		
	2) Controls			
		Disarm stop FM		
	3) Parameters			
		1) FM Retries		
		2) N/A		
		3) Periodic test		

5) Cloud				
	1) IP Address			
	2) IP Port			
	3) Password			
	4) Channel			
	5) Controls			
0) Exit				

Appendix E: WiComm Pro Certitications

EN 50131 & EN 50136 Compliance

Compliance Statement

Hereby, RISCO Group declares that the WiComm Pro series of central units and accessories are designed to comply with:

- **EN50131-1**
- **EN50131-3 Grade 2, Environmental Class II**
- **EN50131-6 Type A**
- **EN50136-1**
- **EN50136-2**
- **EN50131-10 SPT Type Z**
- **EN50131-5-3**
- **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 (SP6)**
- **GSM primary and IP secondary (DP4),**
- **IP primary and GSM secondary (DP4)**

EN50136 Compliance:

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

- When IP and/or GSM are in use, IP Receiver software is also in use. The IP Receiver should be connected to automation software, which serves as the EN50136 annunciator. If connection between the IP Receiver and the automation software is lost, an error message will appear on the IP Receiver queue.
- In order to have an indication of ACK received from the receiving center transceiver, the parameter Kiss-Off Y/N (see page *95*) should be set to Y.

Possible Logical Keys Calculations

- Logical codes are codes punched in the wireless keypad to allow Level 2 (users) and Level 3 (installer) access.
- All codes - 4 digits structure: xxxx
- 0-9 can be used for each digit.
- There are no disallowed codes - codes from 0001 to 9999 are acceptable.
- Invalid codes cannot be created due to the fact that after the code 4th digit has been punched, "Enter" is automatically applied. Code is rejected when trying to create a non existing code.

Possible Physical Keys Calculations

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

System Monitoring

- The main panel is monitored for AC trouble, battery fault, low battery and more.
- The I/O Wireless Expander is monitored for AC trouble, battery fault, low battery and more.
- All other wireless elements are monitored for low voltage battery.

Setting the WiComm Pro to Comply with EN 50131 Requirements

1. Access the installer **Programming menu**.
2. From the **[1] System menu,** select **[5]** to access the Settings menu.
3. From the **Settings menu,** select **[4]** to access the Standard option.
4. Select **EN 50131;** once selected, the following changes will occur in the WiComm Pro software:

Report Codes Feature	EN 50131 Compliance
Timers	
Phone Line cut delay	Immediate (0 minutes)
Entry Delay	45 seconds (maximum allowed)
AC Delay	Immediate (0 minutes)
Jamming Time	0 minutes
RX Supervision	2 hours
System Controls	
Quick Arm	Set to NO
False Code Trouble	Set to Yes
Forced Arming	Set to NO
Authorize installer	Set to YES
Override Trouble	Set to NO
Restore Alarm	Set to YES
Mandatory Event Log	Set to YES
Restore Trouble	Set to YES
Exit Alarm	Set to NO
20 Minutes Signal	Set to YES
Entry Alarm	Set to NO
Attenuation	Set to YES

SIA CP-01 Compliance

Compliance Statement

Hereby, RISCO Group declares that the WiComm Pro series of central units and accessories are designed to comply with SIA CP 01.

The minimum requirement system for SIA-FAR Installations to comply with CP-01 standards:

- A minimum of 1 keypad must be installed
- 1 CP-01 Control Panel (WiComm Pro main panel)
- All system keypads must be audible (mute disabled).

Setting the WiComm Pro to comply with SIA CP 01 Requirements

1. Access the installer **Programming menu**.
2. From the **[1] System menu** select **[5]** to access the Settings menu.
3. From the **Settings menu** select **[4]** to access the Standard option.
4. Select **CP 01;** once selected, the following changes will occur in the WiComm Pro software:

Report Codes	
Feature	**CP 01 Compliance**
Timers	
Phone Line cut delay	Immediate (0 minutes)
Entry Delay	45 seconds (maximum allowed)
AC Delay	Immediate (0 minutes)
Jamming Time	0 minutes
RX Supervision	2 hours
System Controls	
Quick Arm	Set to NO
False Code Trouble	Set to Yes
Forced Arming	Set to NO
Authorize installer	Set to YES
Override Trouble	Set to NO
Restore Alarm	Set to YES
Mandatory Event Log	Set to YES
Restore Trouble	Set to YES
Exit Alarm	Set to NO
20 Minutes Signal	Set to YES
Entry Alarm	Set to NO
Attenuation	Set to YES

Feature	Range	Shipping default	Quick Key / Remark
Exit Delay time	45 sec - 255 sec	45 seconds	[1][1][1][2] / [1][1][2][2]
Progress annunciation	Not programmable	Enabled	
Exit Restore	For re-entry during exit delay	Enabled	[1][2][41]
Auto Stay arm Arm (Partial Arm) on un-vacated premises	If there is no exit after Full Arming	Enabled	[1][2][42]

Feature	Range	Shipping default	Quick Key / Remark
Entry Delay(s)	30 sec - 240 sec**	30 seconds	[1][1][1][1] / [1][1][2][1]
Abort Window - for non-fire zones	May be disabled by zone	Enabled	[2][0][4]
Abort window- for non-fire zones	15 sec - 45 sec**	30 seconds	[5][6][0][1]
Abort annunciation	Annunciate that no alarm was transmitted	Enabled	LCD Display message
Communication Cancel window	5-255 minutes	005 minutes	[5][6][0][2]
Duress feature	Not a duplicate of other user codes	Disabled	[4][1] Can define dedicated user with authority level
Cross zoning	(XX) sec 1-9 minutes	Disabled	[2][7]
Swinger shutdown	For all non-fire zones, shutdown at 1 or 2 trips	One trip	[5][6][8]
Fire alarm verification	Depends on sensors	Enabled	[1][2][10]
Call waiting cancel	Depends on user phone line	Disabled (Empty string)	[5][6][0][3] String required for activation
System test (test report + walk test mode + siren)	Test periodically	Disabled	[6][8][0][5] / [6][8][0][6] Report to Monitoring Station enabled when report code is entered
AC Power Loss indication		Enabled	LCD message display during AC power loss

UKCA and CE RED Compliance Statement

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

For the UKCA and CE Declaration of Conformity please refer to our website: www.riscogroup.com

Standard Limited Product Warranty ("Limited Warranty")

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

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

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

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

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

Limitations. This Limited Warranty is the only warranty made by RISCO with respect to the Products. The warranty is not transferable to any third party. To the maximum extent permitted by applicable law, this Limited Warranty shall not apply and will be void if: (i) the conditions set forth above are not met (including, but not limited to, full payment by customer for the Product and a proven weekly testing and examination of the Product functionality); (ii) if the Products or any part or component thereof: (a) have been subjected to improper operation or installation; (b) have been subject to neglect, abuse, willful damage, abnormal working conditions, failure to follow RISCO's instructions (whether oral or in writing); (c) have been misused, altered, modified or repaired without RISCO's written approval or combined with, or installed on products, or equipment of the customer or of any third party; (d) have been damaged by any factor beyond RISCO's reasonable control such as, but not limited to, power failure, electric power surges, or unsuitable third party components and the interaction of software therewith or (e) any failure or delay in the performance of the Product attributable to any means of communication provided by any third party service provider, including, but not limited to, GSM interruptions, lack of or internet outage and/or telephony failure. BATTERIES ARE EXPLICITLY EXCLUDED FROM THE WARRANTY AND RISCO SHALL NOT BE HELD RESPONSIBLE OR LIABLE IN RELATION THERETO, AND THE ONLY WARRANTY APPLICABLE THERETO, IF ANY, IS THE BATTERY MANUFACTURER'S WARRANTY. RISCO does not install or integrate the Product in the end user's security system and is therefore not responsible for and cannot guarantee the performance of the end user's security system which uses the Product or which the Product is a component of.

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

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

Contacting RISCO Group

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

Belgium (Benelux)
Tel: +32-2522-7622
support-be@riscogroup.com

China (Shanghai)
Tel: +86-21-52-39-0066
support-cn@riscogroup.com

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

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

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

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

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

© RISCO Group, 08/2023. All rights reserved. 5IN2772 E