

# Agility 4

## User Manual



**Model: RW132V**

## **Important Notice**

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

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



© 2019 RISCO Group. All rights reserved.

# Table of Contents

<b>INTRODUCTION</b> .....	<b>6</b>
VUPOINT – VIDEO VERIFICATION WITH IP CAMERA .....	6
SNAPSHOT FOLLOW EVENT .....	6
ADDITIONAL MAIN FEATURES .....	6
USER OPERATIONAL DEVICES.....	7
<b>IMPORTANT SAFETY PRECAUTIONS</b> .....	<b>8</b>
<b>SYSTEM STATUS INDICATIONS</b> .....	<b>9</b>
MAIN PANEL LED INDICATORS .....	9
MAIN PANEL SOUND INDICATORS.....	10
LCD KEYPAD LED INDICATORS.....	10
PANDA KEYPAD LED INDICATORS .....	10
REMOTE CONTROL LED INDICATORS.....	11
REMOTE CONTROL BUZZER INDICATORS .....	11
MESSAGE INDICATORS.....	12
<i>Viewing Last Alarm</i> .....	12
<i>Viewing and Hearing System Status</i> .....	13
<i>Hearing Voice Messages &amp; Announcements</i> .....	14
<i>Receiving SMS Messages</i> .....	14
<i>Receiving E-Mail Messages</i> .....	14
<b>ON-SITE USER OPERATION</b> .....	<b>15</b>
ARMING .....	15
<i>Away (Full) Arming</i> .....	15
<i>Stay / Home (Partial) Arming</i> .....	16
<i>Partition Arming – Stay or Away</i> .....	17
<i>Forced Arming</i> .....	18
<i>Arming with System Trouble (Trouble Bypassing)</i> .....	18
<i>Arming with Zone Bypassing</i> .....	19
DISARMING .....	19
<i>System Disarming</i> .....	20
<i>Disarming after Alarm Activation / Silencing an Alarm</i> .....	20
<i>Partition Disarming</i> .....	21
<i>Duress Disarming (Disarming while Sending a Duress Alarm)</i> .....	22
Granting User Permissions for Using the Duress Disarm .....	22
Defining Duress Disarm Codes .....	22
Sending a Duress Alarm (Duress Disarming) .....	23
RESETTING THE SYSTEM.....	23

<i>Installer or Monitoring Station Resetting after Alarm</i> .....	23
<i>"Anti-Code" Resetting by the User</i> .....	23
SENDING ALARMS (EVENTS) .....	24
<i>Sending a Duress Alarm</i> .....	24
<i>Sending a Panic Alarm</i> .....	24
<i>Sending a Fire Alarm</i> .....	24
<i>Sending a Medical / Emergency Alarm</i> .....	24
OPERATING OUTPUT CONTROL .....	25
VIEWING THE EVENT LOG .....	26
DESCRIBING TALK & LISTEN .....	26
<i>User-Initiated Talk &amp; Listen</i> .....	27
DESCRIBING LCD/PANDA KEYPAD BUTTONS .....	27
ADDITIONAL COMMON USER OPERATIONS AT THE LCD/PANDA KEYPAD .....	28
SYSTEM OPERATION BY REMOTE CONTROL .....	33
<i>Changing the Remote Control Code</i> .....	33
<i>Clearing a Remote Control Command</i> .....	33
<b>REMOTE USER OPERATION BY TELEPHONE .....</b>	<b>34</b>
ACCESSING THE SYSTEM BY TELEPHONE .....	34
RECEIVING FOLLOW-ME EVENT NOTIFICATION BY TELEPHONE .....	35
<i>Acknowledgement Menu</i> .....	35
<i>Telephone Operations Menu</i> .....	36
Talk & Listen .....	36
SMS OPERATION .....	37
<i>SMS Confirmation Reply</i> .....	37
<i>Table of SMS Commands</i> .....	37
<i>Operation</i> .....	37
<b>REGISTERING TO THE RISCO CLOUD .....</b>	<b>38</b>
LOGGING IN TO THE RISCO CLOUD / ACCESSING THE WEB USER APP .....	39
<b>SMARTPHONE / WEB USER INTERFACE OPERATION .....</b>	<b>40</b>
DOWNLOADING THE IRISCO SMARTPHONE APP .....	40
<i>Main iRISCO Operations</i> .....	40
<b>USER SETTINGS .....</b>	<b>41</b>
DEFINING USER CODES (SYSTEM USERS) .....	41
<i>Assigning or Editing Users (User Codes)</i> .....	41
<i>Deleting User Codes</i> .....	43
ADDING AND DELETING PROXIMITY TAGS .....	44
<i>Adding a Proximity Tag</i> .....	44

*Deleting a Proximity tag* .....44  
DEFINING FOLLOW ME DESTINATIONS .....45  
*Testing Follow Me Reporting* .....46  
ACTIVATING/DEACTIVATING AUTOMATIC ARMING & UTILITY OUTPUT PROGRAMS WITH SCHEDULER .47  
**SYSTEM TECHNICAL SPECIFICATIONS ..... 48**

# Introduction

This manual describes the user-operational procedures for the Agility 4 system. Agility 4 combines state-of-the-art wireless alarm security and safety features with advanced Cloud-based user-operation and monitoring via Smartphone and Web-based user apps.

## VUpoint – Video Verification with IP Camera

For end-users and monitoring stations alike, Agility 4 supports RISCO's revolutionary VUpoint video verification solution that seamlessly integrates an unlimited number of IP cameras to provide an unprecedented level of security together with live, real-time video monitoring capabilities – to help identify false alarms or actual intrusions-in-progress. Powered by the RISCO Cloud, VUpoint enables the initiation of live video streaming on-demand from any IP camera, which is viewed remotely using the iRISCO Smartphone or Web user apps. VUpoint can be configured so that any detected event – whether intrusion, safety or panic – can trigger the IP camera.

## Snapshot Follow Event

Agility 4 also supports advanced PIR camera functionality to “follow” event activations (to capture and send snapshots) – 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.

## Additional Main Features

- ✓ Supports 2-way wireless communication, compatible for 1-way and 2-way detectors
- ✓ 32 wireless zones
- ✓ 4 wired zones with selectable EOL resistance & 4 outputs (2 x 3A & 2 x 500 mA relays)
- ✓ 3 partitions per zone
- ✓ 16 Follow-Me destinations
- ✓ SMS-enabled with GSM/GPRS module
- ✓ Audio messaging / status announcements
- ✓ Remote telephone operation with PSTN module
- ✓ Event log capacity of 1000 events
- ✓ 2-way Listen & Talk capability between the premises and the monitoring station
- ✓ 31 possible user codes + 1 Grand Master code
- ✓ Up to three 2-way wireless keypads
- ✓ Supports 2-way wireless curtain detectors
- ✓ Supports magnetic door/contact detectors with shutter
- ✓ Up to 8 rolling-code keyfobs
- ✓ Supports the wireless I/O Expander module to control up to sixteen X10 devices

## User Operational Devices

Agility 4 can use several RISCO devices. The most typical ones are listed below.

---

**NOTE:** All RISCO devices available for system use come with their respective instructions.

---

### Smartphone



For Android and iOS, use the iRISCO Smartphone app for system operation and control. Via the RISCO Cloud, you can arm/disarm, visually verify alarms by viewing live video from the IP cameras and still images from the PIR cameras, activate home automation devices, view system status and much more.

### 4 Button Keyfob



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

### 4 Button Panda Keyfob



Using the wireless 4 button Panda keyfob you can arm, disarm, send a panic alarm and get system status.

### 2-Way, Wireless 8 Button Remote Control



Using the 2-way 8 button remote control you can arm /disarm, send a panic alarm, activate outputs and more. For higher security, some commands can be defined to be activated with a user code.

### Agility 2-Way Wireless LCD Keypad or Wireless Panda Keypad



Using the 2-way wireless keypad you can program and operate your system according to your needs. High-security mode functions are also available, using a user code or a proximity tag.



### Telephone



Use any touch-tone phone to perform remote operations such as arming, disarming, listening in and talking to the premises.



### SMS

If your system is equipped with a GSM/GPRS module it can provide information about the system, such as event notification via SMS to your mobile phone. You can also operate the system using SMS commands for system arming / disarming, and more.



### Web User App

The Web user app enables remote monitoring, control and configuration of the system from any location with Internet connectivity. It includes all the capabilities of the iRISCO Smartphone app and can also configure RISCO's PIR Camera settings such as the number of images taken, image resolution, and more. The app is powered by the RISCO Cloud.

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



**WARNING:** Risk of explosion exists if a battery is replaced by an incorrect type and does not have the UL recognized mark 



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



**CAUTION:** After any type of system alarm activation, to avoid any possible danger, it is recommended to avoid being present at the premises until the cause of the alarm can be verified. This may involve a monitoring station, police, other responding agencies/services, or utilizing VUpoint video verification, for example.



# System Status Indications

## Main Panel LED Indicators

### Power LED (Green)

Condition	Description
On	Power OK
Rapid flash	Indicates AC trouble
Slow flash	Indicates low battery trouble

### Away (Full) Arm & Alarm LED (Red)

Condition	Description
On	System is Away (Full) armed
Rapid flash	Alarm activation
Slow flash	System is in Exit delay
Off	System is disarmed

### Stay / Home (Partial) Arm LED (Red)

Condition	Description
On	System is Stay/Partial (Home) armed
Off	System is disarmed

### Ready LED (Green)

Condition	Description
On	System is ready
Off	Open zones
Slow flash	System is ready to be armed while a specially designated entry/exit door remains open

### Trouble LED (Orange)






Condition	Description
Rapid flash	Trouble
Off	No trouble

**NOTE:** If all LEDs flash one-after-the-other in sequence, the system is in learning mode (used for performing device enrollment).


## Main Panel Sound Indicators






Type	Description
Intrusion alarm	Continuous, rapid beeping
Fire alarm	Staggered, rapid beeping
Exit delay	Slow buzzer beeps until the Exit Delay time period expires
Entry delay	Slow buzzer beeps until the Entry Delay time period expires
Confirm operation	1-second tone
Reject operation	Three rapid error beeps
Arm/Disarm chirp	1 siren chirp = system armed 2 siren chirps = system is disarmed 4 siren chirps = system disarmed after an alarm

## LCD Keypad LED Indicators

LED	Description
 (green)	<ul style="list-style-type: none"> <li>♦ <b>On:</b> Power OK</li> <li>♦ <b>Rapid Flash:</b> AC trouble</li> <li>♦ <b>Slow Flash:</b> Low battery trouble</li> </ul>
✓	<ul style="list-style-type: none"> <li>♦ <b>On:</b> System ready</li> <li>♦ <b>Off:</b> Open zones</li> <li>♦ <b>Slow Flash:</b> Ready to arm with open entry/exit zone</li> </ul>
 (blue)	Communication with the main panel
 (red)	<ul style="list-style-type: none"> <li>♦ <b>On:</b> fully armed</li> <li>♦ <b>Slow flash:</b> exit delay</li> <li>♦ <b>Rapid flash:</b> alarm</li> </ul>
 (red)	<ul style="list-style-type: none"> <li>♦ <b>On:</b> partially armed (stay arm)</li> <li>♦ <b>Off:</b> disarmed</li> </ul>
 (orange)	Trouble in the system when system is disarmed

## Panda Keypad LED Indicators

LED	Description
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> System connected to cloud</li> <li>♦ <b>No:</b> No cloud connectivity</li> </ul>

	<ul style="list-style-type: none"> <li>♦ <b>Slow Flash:</b> Cloud connectivity trouble</li> </ul>
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> System ready</li> <li>♦ <b>Off:</b> Open zones</li> <li>♦ <b>Slow Flash:</b> Ready to arm with open entry/exit zone</li> </ul>
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> Zone/keypad/external module has been tampered</li> <li>♦ <b>Off:</b> Normal operation</li> </ul>
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> fully armed</li> <li>♦ <b>Slow flash:</b> exit delay</li> <li>♦ <b>Rapid flash:</b> alarm</li> </ul>
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> partially armed (stay arm)</li> <li>♦ <b>Off:</b> no bypassed zones</li> </ul>
	<ul style="list-style-type: none"> <li>♦ <b>On:</b> Trouble in the system</li> <li>♦ <b>Off:</b> No trouble</li> </ul>

## Remote Control LED Indicators





Operation	LED state (send command*)	LED state (receive status)
Away Arm	Green	Red
Stay Arm	Green	Orange
Disarm	Green	Green
Alarm	Green	Flashing Red
*If the Send command (green) LED changes to orange, it indicates a low battery condition.		

## Remote Control Buzzer Indicators
















Sound	Status
1 beep	Confirmation
3 beeps	Error
5 beeps	Alarm

## Message Indicators

### Viewing Last Alarm

Device	Procedure
	Press  for two seconds.
	<b>[Smartphone app]:</b> View last alarm from the event log
	<b>SMS:</b> Enter code + AL

## Viewing and Hearing System Status

Device	Procedure
	<p><b>NOTE:</b> Short-press for display, or long-press for display + announcement.</p> <p><b>Quick mode:</b> Press  </p> <p><b>High Security mode:</b> Press  , then enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p><b>NOTE:</b> Short-press for LCD display, or long-press for display + announcement.</p> <p><b>Quick mode:</b> Press </p> <p><b>High Security mode:</b> Press , then enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p><b>NOTE:</b> For both modes, pressing  before  will give status indication only with the remote control's LED, and not with a voice message at main panel.</p> <p><b>NOTE:</b> For LED and buzzer indication and code descriptions, see <i>Main Panel LED Indicators</i> on page 9, and <i>Main Panel Sound Indicators</i> on page 10.</p> <p><b>Quick mode:</b> Long-press </p> <p><b>High Security mode:</b> Long-press , then enter <b>code</b>.</p>
	<p><b>[Smartphone app]:</b> View system status</p>
	<p>Short-press the main panel button to hear a system status announcement (if installer-defined)</p>

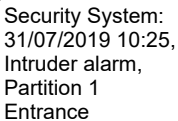
## Hearing Voice Messages & Announcements

Three types of voice messages can be heard— either locally at the main panel, or remotely via mobile phone:

- **Event notification messages:** The system calls the Follow Me telephone number(s) to notify the recipients of events with pre-recorded voice messages.
- **Status messages:** Upon accessing the system remotely by initiating a call from a remote telephone (or by receiving a call from the system), the system then announces the current system status with a pre-recorded message announcement.
- **Local Announcement messages:** The system can have various message announcements from the main panel.

## Receiving SMS Messages

When using the GSM/GPRS communication module, the system can send pre-defined SMS event messages to a Follow Me destination, to inform of the status of the security system and certain events that have occurred in the system. For example:

A screenshot of an SMS message displayed in a rounded rectangular box. The text inside the box reads: "Security System: 31/07/2019 10:25, Intruder alarm, Partition 1 Entrance".

Security System:  
31/07/2019 10:25,  
Intruder alarm,  
Partition 1  
Entrance

## Receiving E-Mail Messages

When the Agility 4 system is connected to the RISCO Cloud, the system can send the following system status and event notification messages to predefined e-mail addresses: Safety; Alarms; SOS; System Status; Faults; Maintenance; and Cloud Related. For example:

**Subject:** Alarm Security Message: Intruder Alarm

**System Name:** Dan's residence

**Event:** Intruder alarm, zone 5, entrance door

**Time:** 01 April 2019; 16:12

**Partition:** Partition 1, first floor

**Service Contact:** Monitoring Station 01, 05-7943452

# On-Site User Operation



**NOTE:** For user operations by telephone see *Remote User Operation by Telephone*, page 34. For user operations by SMS, see *SMS Operation*, page 37.

## Arming

Before arming the system check if the ✓ LED is on, which indicates the system is ready to arm. If not ready, secure or bypass the violated zone(s), and then proceed to arm.












Arming operations will be followed by a local message announcement if defined, and failure to arm will likewise be indicated by the system.







**NOTE:** If you're unable to arm the system, from the LCD/Panda keypad, short-press

 /  to view system status, or long-press to view and also hear the system status from the main panel.

## Away (Full) Arming














Full arming (also referred to as "Away" arming) is used when the protected premises is vacated, and all system detectors are therefore activated. After arming, you must exit via the designated exit door within the designated "exit delay" countdown time period.

Device	Procedure
	<p>[Smartphone app]: Press .</p>
	<p><b>NOTE:</b> For LED and buzzer indication and code descriptions, see <i>Main Panel LED Indicators</i> on page 9, and <i>Main Panel Sound Indicators</i> on page 10.</p> <p><b>Quick mode:</b> Press .</p> <p><b>High security mode:</b> Press , then enter <b>code</b>.</p>
	<p><b>Quick mode:</b> Press .</p> <p><b>High security mode:</b> Press , then enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p><b>Quick mode:</b> Press .</p> <p><b>High security mode:</b> Press , then enter <b>code</b> or use <b>proximity tag</b>.</p>





	Press 
	Press 
	[SMS]: Enter code + A Example: 1234A. For more information refer to <i>SMS Operation</i> , page 37.
	[Web app]: Click Full Arm

## Stay / Home (Partial) Arming

Partial arming (also referred to as “Stay” arming or “Home” arming) arms only part of the premises, while enabling people to remain in another disarmed part of the premises.





















Device	Procedure
	[Smartphone app]: Press 
	NOTE: For LED and buzzer indication and code descriptions, see <i>Main Panel LED Indicators</i> on page 9, and <i>Main Panel Sound Indicators</i> on page 10. Quick mode: Press  . High security mode: Press  , then enter code.
	Quick mode: Press  . High security mode: Press  , then enter code or use proximity tag.
	Quick mode: Press  . High security mode: Press  , then enter code or use proximity tag.
	Press 



	Press  or the small button if defined (installer-defined)
	<b>[SMS]:</b> Enter <b>code + H</b> Example: <b>1234H</b> . For more information refer to <i>SMS Operation</i> , page 37.
	<b>[Web app]:</b> Click <b>Part Arm</b>

## Partition Arming – Stay or Away

There can be up to 3 partitions. Each partition can be managed as a separate security system that can be armed and disarmed individually, regardless of the condition of the other. The partitions can be Stay or Away armed/disarmed one at a time or all at once. The permission levels of the users determine the number of partitions they can operate.

Device	Procedure
	<b>[Smartphone app]:</b> Partition arming (Away and Stay).
	NOTE: Pressing  before  will cancel the Entry Delay time. <b>Quick mode:</b> Press partition number (1–3), then press Away arming (  ) or Stay arming (  ). <b>High security mode:</b> Press partition number (1–3), press Away arming (  ) or Stay arming (  ), then enter <b>code</b> .
	<b>Quick mode:</b> Press partition number (1–3), then press Away arming (  ) or Stay arming (  ). <b>High security mode:</b> Press partition number (1–3), press Away arming (  ) or Stay arming (  ), then enter <b>code</b> or use <b>proximity tag</b> .
	<b>Quick mode:</b> Press partition number (1–3), then press Away arming (  ) or Stay arming (  ). <b>High security mode:</b> Press partition number (1–3), press Away arming (  ) or Stay arming (  ), then enter <b>code</b> or use <b>proximity tag</b> .
	Press  or small button 4 (installer-defined)



[SMS]: Enter **code + A** (Away) or **H** (Home/Stay). Now enter partition number (1–3). Example: **1234H3**. For more information refer to *SMS Operation*, page 37.

## Forced Arming

If the installer has enabled forced arming (for specific zones), you can arm the system regardless if those zones are open (not armed) or faulty.

- After arming, all zones enabled for forced arming are bypassed at the end of the Exit Delay time period.
- If a faulted zone that is enabled for forced arming is eventually secured (returned-to-normal state) during the armed period, it will no longer be bypassed and will be included among the system's armed zones.



**CAUTION:** Forced arming may result in leaving part of the premises unsecured.

## Arming with System Trouble (Trouble Bypassing)

If required, and defined by your installer, arming can take place from the wireless keypad even when there are system troubles occurring.

When arming the system with a simultaneous trouble, the display will show a system

trouble message. Press / and scroll to view a list of all current troubles.

















**CAUTION:** Arming with system troubles may result in leaving the premises unsecured.

### To bypass troubles and arm the system from the keypad:

1. Press / , then enter your **user code** to access the User menu.
2. Go to **Activities** and press / , scroll to **Bypass Trouble** and press / ; "Bypass troubles. Are you sure? N?" appears.
3. Press / to toggle to **Y** (yes), and then press / .
4. Press / / / to return to main display. You can now perform the arming operation.

## Arming with Zone Bypassing

Bypassing a zone enables you to arm a partition even if a zone within that partition is open (not secured). You may need to bypass a zone, for example, when access is needed to one zone in an otherwise protected area, or to cause the system to temporarily circumvent a zone.

Device	Procedure
	Press  and enter code, at <b>Activities</b> menu press  , at <b>Bypass Zone</b> press  , scroll to zone to bypass, press  to toggle between Y and N, and then press  .
	Press  and enter code, at <b>Activities</b> menu press  , at <b>Bypass Zone</b> press  , scroll to zone to bypass, press  to toggle between Y and N, and then press  .
	<b>[Smartphone app]:</b> Quick zone bypass
	<b>[Web app]:</b> On the Main Page menu, click <b>Settings</b> , and then <b>Zone Bypass</b>

## Disarming

When the system is disarmed, the system's devices will not detect events or trigger alarms.
















When entering an armed site, the installer-defined entry delay countdown begins, during which time you must disarm the system in order not to activate alarms. The disarming operation will be followed by a local message announcement (if installer-defined).

---

**IMPORTANT:** After any type of system alarm activation, to avoid any possible danger, it is recommended to avoid being present at the premises until the cause of the alarm can be verified. This may involve a monitoring station, police, other responding agencies/services, or utilizing video verification by a remote system user, for example.

---

## System Disarming




Device	Procedure
	<p>[Smartphone app]: Press .</p>
	<p><b>NOTE:</b> For LED and buzzer indication and code descriptions, see <i>Main Panel LED Indicators</i> on page 9, and <i>Main Panel Sound Indicators</i> on page 10</p> <p><b>Quick mode:</b> Press .</p> <p><b>High security mode:</b> Press , then enter <b>code</b>.</p>
	<p>Press  then enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p>Press  then enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p>Press .</p>
	<p>Press .</p>
	<p>[SMS]: Enter <b>code + D</b></p> <p>Example: <b>1234D</b>. For more information refer to <i>SMS Operation</i>, page 37.</p>
	<p>[Web app]: Enter <b>user code</b>, and then click <b>Disarm</b>.</p>

## Disarming after Alarm Activation / Silencing an Alarm

After an alarm activation, if you disarm the system it will also serve to silence the alarm.














### NOTES:

- After disarming, the system will sound 4 siren chirps to inform that an alarm has occurred, and then any alarms will be silenced.

- To view the last alarm information, at the LCD/Panda keypad press  for about 3 seconds.
- If an entry door is opened prior to disarming the system, "Alarm occurred in the system" will be announced.
- Short-press  /  to view the alarm type (system status), or long-press to view & also hear the status. Smartphone users can also view this information.

## Partition Disarming

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

Device	Procedure
	<p>[Smartphone app]: Partition disarming</p>
	<p><b>Quick mode:</b> Press partition number (1-3), then press .</p> <p><b>High security mode:</b> Press partition number (1-3), press , enter <b>code</b>.</p>
	<p>Press partition number (1-3), and then press . Now enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p>Press partition number (1-3), and then press . Now enter <b>code</b> or use <b>proximity tag</b>.</p>
	<p>Press  (for all assigned partitions)</p>
	<p>Press  (for all assigned partitions)</p>
	<p>[SMS]: Enter <b>code</b> + <b>D</b> + partition number (1-3). Example: <b>1234D2</b>. For more information refer to <i>SMS Operation</i>, page 37.</p>

## Duress Disarming (Disarming while Sending a Duress Alarm)

If a user is ever forced to disarm the system, they can comply while at the same time also send a silent duress alarm from the LCD/Panda keypad to the monitoring station. At the premises there are no audible alarms nor any visible indicators.

### Granting User Permissions for Using the Duress Disarm

















The Grand Master assigns permission for each user to use the Duress Disarm feature.

---

**NOTE:** Although the installer can also assign permissions for users to use Duress Disarm, only the Grand Master defines the confidential code(s) for the users to operate the feature.

---













#### To enable users to use Duress Disarm (to send a duress alarm):

1. Enter Grand Master code, then from User Menu scroll to **Codes/Tags** and press  /  .
2. From User Codes press , then scroll to **Parameters** and press  /  .
3. Scroll to select the user index number and then press  /  .
4. Scroll to **Authority** and then press  /  .
5. Scroll to **Duress** and then press  /  .

### Defining Duress Disarm Codes



Only the Grand Master can assign or change the code needed for operating the Duress Disarm feature. A code must be assigned for each system user with pre-defined permissions (it can be the same code, or it can be a different code). Make sure system users keep their codes confidential.

#### To define a Duress Disarm code for an authorized system user:

1. Enter Grand Master code, then from User Menu scroll to **Codes/Tags** and press  /  .
2. From User Codes press  /  , then scroll to **New/Change Code** and press  /  .
3. Scroll to select the user index number and then press  /  .
4. Enter a new code, then re-enter the same code; "Accepted" displays.

## Sending a Duress Alarm (Duress Disarming)

To disarm under duress (send duress alarm to monitoring station) via the LCD/Panda keypad:

- Press  /  , then enter the **duress code**

---

**NOTE:** Under no circumstances should the duress code be used haphazardly or without reason. Monitoring stations and responding agencies such as police departments treat duress codes very seriously and take immediate action.



---

## Resetting the System

The system can be installer-defined to be **not ready to arm** after an alarm or tamper condition. Resetting the system can be performed by the installer/monitoring station, or by the user (see “*Anti-Code*” Resetting by the User, below).

### Installer or Monitoring Station Resetting after Alarm









If resetting the system to normal operation requires the intervention of the monitoring station or installer (installer-defined), then after an alarm, the system will be in a “not ready to arm” state. You can view/hear a Technician Reset trouble message system status by pressing

 /  . You will then need to contact your monitoring station/installer to reset the system either remotely or locally from the keypad. To enable local resetting by your installer, you may need to grant the installer use of the Grand Master code. A one-hour time window is opened for the installer to program any user functions and reset your system locally.

### “Anti-Code” Resetting by the User

If the system is installer-defined to be “not ready to arm” after an alarm or tamper condition, an authorized user can restore the system to normal operation by entering an “anti code” which installer or monitoring station provides to the user.

To reset with an anti-code at the LCD/Panda keypad:

1. Press  /  and enter your user code.
2. At Activities press  /  , then scroll to **Anti Code** and press  /  ; a randomly-generated code displays.
3. Call your installer or monitoring station and read the code that displays; they will then provide you with an “anti code” number.
4. Enter the **anti code** number, and then press  /  ; the system will reset to normal operation, and you can then proceed to arm.














# Sending Alarms (Events)

## Sending a Duress Alarm

See *Duress Disarming (Disarming while Sending a Duress Alarm)*, page 22.

## Sending a Panic Alarm





In the event of an emergency you can send a panic notification to the monitoring station or to Follow-Me destinations. The panic alarm feature must be installer-enabled, and can also be installer-defined to be silent at the premises at the premises when sent from the LCD/Panda keypad. When sent from a keyfob or remote control, panic alarms are always silent.

Device	Panic Alarm Procedure
	Press  and  simultaneously <b>NOTE:</b> These buttons can be used for sending a panic alarm if installer-defined.
	Press  and  simultaneously <b>NOTE:</b> These buttons can be used for sending a panic alarm if installer-defined.
	Press  and  simultaneously for 2 seconds.
	Press the <b>small button</b> (if installer defined)
	Press  and  simultaneously

## Sending a Fire Alarm

You can send a fire alarm from the LCD/Panda keypad

To send a fire alarm from the LCD/Panda keypad:





- Press  and  (LCD Keypad) /  and  (Panda Keypad) simultaneously for 2 seconds.

## Sending a Medical / Emergency Alarm

You can send a medical / emergency alarm from the LCD/Panda keypad.




















**To send a medical / emergency alarm from the LCD/Panda keypad:**









- Press  and  (LCD Keypad) /  and  (Panda Keypad) simultaneously for 2 seconds

## Operating Output Control

Also known as Home Automation or Utility Output, this enables you to schedule multiple automated external (not system-connected) devices to be remotely turned on and off, such as lights, appliances, a garage door, etc.).

Device	Procedure
 	<p><b>Quick mode:</b> Press and hold button , , or  (for the respective automated device) for 2 seconds.</p> <p><b>High Security mode:</b> Press and hold button , , or  (for the respective automated device) for 2 seconds, then enter your <b>code</b> or swipe the <b>proximity tag</b>.</p> <p><b>NOTE:</b> Installer defines which output is assigned to each of the 3 buttons.</p>
	<p><b>[Web app]:</b> Operating output control [Automation tab]</p>
	<p><b>[Smartphone app]</b></p>
	<p><b>Quick mode:</b> Long-press , , or  (for outputs A, B, C respectively)</p> <p><b>High security mode:</b> Long-press , , or , then enter <b>code</b>.</p>








## Viewing the Event Log

Device	Procedure
	Press  then enter <b>code</b> and then scroll to <b>Event Log</b> and press 
	Press  then enter <b>code</b> and then scroll to <b>Event Log</b> and press 
	[Web app]: Viewing the Event Log (History tab)
	[Smartphone app]: Viewing the Event Log

## Describing Talk & Listen











The Talk & Listen feature enables 1-way or 2-way voice communication between the monitoring station and system users at the premises. Installer-defined, it can be activated by the monitoring station and also user-activated and operated from the keypad. The monitoring station, for example, can listen silently to the premises in order to verify an event or to talk to someone at the premises who needs assistance. For users at the premises, for example, they can place a service call to the monitoring station or call the monitoring station to prompt them to listen-in only (without any talking). The user at the premises communicates through the built-in microphone and speaker on the main panel, or alternatively via an external Talk & Listen unit – which must be located next to a keypad.

## User-Initiated Talk & Listen
























Device	Procedure
	<p>To activate/deactivate the Talk &amp; Listen feature at the Talk &amp; Listen unit (if installer-defined), at the keypad press  and  simultaneously.</p>
	<p>To activate/deactivate the Talk &amp; Listen feature at the Talk &amp; Listen unit (if installer-defined), at the keypad press  and  simultaneously.</p>
	<p>To activate/deactivate the Talk &amp; Listen feature at the main panel (if installer-defined), short-press the main panel button.</p>




























## Describing LCD/Panda Keypad Buttons






























The following controls are commonly used on the LCD/Panda keypad:







































Button (LCD Keypad)	Button (Panda Keypad)	Primary Function
		<p>To “wake-up” the keypad, go back one level, exit menus (similar to the Esc key).</p>
		<p>To select / confirm / OK (similar to the Enter key).</p>
		<p>To scroll between options. Also used to change (toggle) between options.</p>
		<p>To change (toggle) between options – such as Y (yes) and N (no).</p>
		<p>To exit the User menu, also to “go back” from within the User menu.</p>



























## Additional Common User Operations at the LCD/Panda Keypad

Keypad Operation	Procedure	Permissions		
		Grand Master	User	Installer
Set keypad contrast	<p><b>LCD Keypad:</b> Press and hold  for 2 seconds.</p> <p>Use   to adjust the display contrast, and then press .</p> <p><b>Panda Keypad:</b> Press and hold  for 2 seconds.</p> <p>Use   to select the  icon and press  then use   to adjust the display contrast, and then press .</p>	✓	✓	✓
System Chime On/Off (Chime indicates a zone violation when system is disarmed)	<p><b>LCD/Panda Keypad:</b> Without entering code, press  for 2 seconds to toggle between <i>System Chime On</i> and <i>System Chime Off</i>.</p>	✓	✓	✓
Wake up keypad	<p>Without entering code, press  /  .</p>	✓	✓	✓
Main Buzzer On/Off	<p>Press  /  , enter <b>code</b>, at Activities press  / , scroll to <b>Buzzer On/Off</b>, and then press  / ; keypad displays "Buzzer On" or "Buzzer Off". Repeat procedure to toggle between on &amp; off.</p>	✓	✓	✓

<b>Adjust speaker volume</b>	<b>LCD/Panda Keypad:</b> Press  for 2 seconds. Scroll to select volume level (0–4), and then press  / 	✓	✓	✓
<b>Adjust keypad volume</b>	<b>Panda Keypad:</b> / Press and hold  for 2 seconds. Use   to select the  icon and press  then use   to adjust the display contrast, and then press 	✓	✓	✓
<b>Change keypad and panel language</b>	Press  and  /   and  simultaneously for 2 seconds. Scroll to select a language, and then press  / 	✓	✓	✓
<b>Set Clock (Time &amp; date)</b>	Press  /   , enter <b>code</b> , scroll to <b>Clock</b> and press  /  , scroll to <b>Time &amp; Date</b> and press  /  , use scroll keys to enter the correct time and date, and then press  / 	✓		✓

<p><b>Service Mode</b> (Activate this mode when changing a device's battery to silence the tamper alarm for an installer-defined period of time)</p>	<p>Press  /  ↩, enter <b>code</b>, at Activities, press  / , scroll to <b>Advanced</b> and press  / , then scroll to <b>Service Mode</b> and press  ; "Service Mode Activated" displays. Remove device cover and replace battery. <b>NOTE:</b> To deactivate Service Mode (and return to normal operation after battery replacement), repeat the procedure; it automatically toggles to "Deactivated."</p>	✓	✓	✓
<p><b>Check SIM Credit</b> (Get credit level of your prepaid SIM card by SMS or voice)</p>	<p>Press  /  ↩, enter <b>code</b>, at Activities press  / , scroll to <b>Advanced</b> and press  / , scroll to <b>Prepaid SIM</b> and press  / , scroll to <b>Check Credit</b> and press  / , scroll to <b>Send Request</b> or <b>Get Results</b>, and then press  / .</p>	✓		
<p><b>Reset SIM</b> (After replenishing a prepaid SIM card, you must reset it)</p>	<p>Press  /  ↩, enter <b>code</b>, at Activities press  / , scroll to <b>Advanced</b> and press  / , scroll to <b>Prepaid SIM</b> and press  / , then scroll to <b>Reset SIM</b> and press  /  ; "Reset SIM Card Counter" displays.</p>	✓		

<p><b>Entry/Exit beeps</b> (Provides beep indication when in Entry Delay / Exit Delay modes)</p>	<p>Press  /  , enter <b>code</b>, at Activities</p> <p>press  / , scroll to <b>Advanced</b> and</p> <p>press  / , then scroll to <b>Ex/En</b></p> <p><b>Beeps</b> and press  /  ; “Ex/En Beeps On (or Off)” displays. Repeat procedure to toggle between <i>On</i> and <i>Off</i>.</p>	<p>✓</p>	<p>✓</p>	<p>✓</p>
<p><b>View Service Info</b> (View the installer’s name &amp; phone number)</p>	<p>Press  /  , enter <b>code</b> &gt; scroll to <b>Service Info.</b> and press  /  &gt; use the scroll keys to toggle between <i>Name</i> and <i>Phone</i> &gt; press  /  to select &gt; enter the information, using scroll keys to go to the next space.</p>	<p>✓</p>	<p>✓</p>	<p>✓</p>
<p><b>Restore Alarm</b> (If installer-enabled, user must confirm that an alarm occurred before rearming; the system will be in a not-ready state until confirming via this procedure)</p>	<p>Press  /  , enter <b>code</b>, at Activities</p> <p>press  / , scroll to <b>Advanced</b> and</p> <p>press  / , then scroll to <b>Restore Alarm</b> and press  / .</p>	<p>✓</p>	<p>✓</p>	<p>✓</p>
<p><b>Restore Trouble</b> (If installer-enabled, user must manually confirm the restoral of each trouble to a normal condition)</p>	<p>Press  /  , enter <b>code</b>, at Activities</p> <p>press  / , scroll to <b>Advanced</b> and</p> <p>press  / , scroll to <b>Restore Trbl.</b> and press  / , press  /  to toggle between <b>Y</b> and <b>N</b>, and then press  / .</p>	<p>✓</p>	<p>✓</p>	<p>✓</p>

<p><b>CS Connect</b> (Grants permission to installer / monitoring station to establish communication with the configuration software via IP or GPRS communication)</p>	<p>Press  /  ↩, enter <b>code</b>, at Activities</p> <p>press  /  , scroll to <b>Advanced</b> and</p> <p>press  /  , scroll to <b>CS Connect</b> and</p> <p>press  /  , scroll to <b>via IP</b> or <b>via GPRS</b>, and then press  /  ; "Connection Activated" displays.</p>	✓	✓	✓
<p><b>Enable CS</b> (Grants permission to installer / monitoring station to enable remote configuration and operation via the Configuration Software)</p>	<p>Press  /  ↩, enter code, at Activities</p> <p>press  /  , scroll to <b>Advanced</b> and</p> <p>press  /  , then scroll to <b>Enable CS</b> and press  /  ; "Connection Ready" displays.</p>	✓	✓	✓
<p><b>Walk Test</b> (To ensure correct detector operation for selected zones. After arming, walk through the zone(s) to ensure that the alarms are triggered.)</p>	<p> /  ↩, &gt; <b>code</b> &gt; at Activities menu</p> <p>press  /  &gt; scroll to <b>Walk Test</b> &gt;</p> <p>press  /  &gt; "at Start Walk Test"</p> <p>press  /  . Walk through the zone(s) and ensure detection by triggering the respective alarm(s).</p>	✓	✓	✓







## System Operation by Remote Control


### Changing the Remote Control Code

Each remote control can be defined by your installer to have a unique 4-digit code, which is used to perform operations in High Security mode. To change the remote control code, it is mandatory to perform the following procedure **in close proximity to the control panel**.

**To change the remote control code:**

1. Press  and  simultaneously for 2 seconds.
2. Enter the **current 4 digit code**.
3. Press , then enter a **new 4 digit code**.
4. Press ; the panel will send a confirmation message, the remote control will sound a long beep, and the green LED on the remote control will turn on. If no confirmation sound is heard the old code still remains. In that case, repeat the procedure again.

### Clearing a Remote Control Command

- When sending a command from a remote control, if you want to clear (cancel) the command before it is executed, press  twice.

# Remote User Operation by Telephone

You can remotely operate the system from a touch-tone phone by initiating a telephone call to the system and then interacting with voice menus that guide you through the operations. You can also receive voice notifications of events to your telephone, and from the menu options you can then perform system operations as well.

## Accessing the System by Telephone

Remotely accessing the system involves initiating a call to the system and entering your remote access code and the user code you usually enter at the LCD/Panda keypad.

### To remotely access the system:

1. From a remote touch-tone telephone, dial the number at the premises where Agility 4 is installed (for the telephone connected to the Agility 4 main panel).
2. If your system is connected to a landline telephone and an answering machine is in use at the premises, let it ring once then hang up, wait 20 seconds, and then call again.
3. If an answering machine is not in use at the premises, wait until the system picks up. After the system picks up a short tone is heard.

---

**NOTE:** When the system picks up, if there are multiple phones on the same line, all are effectively disconnected and cannot be used (depending on installer wiring).

---

4. Enter your **2-digit remote access code** within 5 seconds (default code = **00**); the following is announced: *"Hello, Please Enter Your User Code, Followed By #"*.
5. Enter your user code followed by # (default user code=**1234**).
6. After your code is accepted a system status message is announced, and you are now in the Operations menu (see next page).

## Receiving Follow-Me Event Notification by Telephone

Up to 16 users can receive Follow-Me event notifications (pre-recorded messages) to their telephones, which can be sent for any or all types of events (for example, intrusion, safety, or panic), depending on the installer-defined event type configuration for each Follow-Me user. Event notification enables system users and monitoring stations to respond appropriately – for example, by performing video verification, notifying responders, and also operating the system.

---

**NOTE:** Follow Me notifications are sent to system users only after first reporting the event to the Monitoring Station.

---

### To receive a Follow-Me event notification call:

1. Answer the phone and say "Hello" or press #; an event announcement informs you of the system event(s).

---

#### NOTES:

- Press # to play the event message again.
  - If no voice detected, the message will start playing 5 seconds after the phone picks up.
- 
2. Press \* to go to the Acknowledgement menu – where you must acknowledge that you heard the event message and can then perform other system operations as needed.

## Acknowledgement Menu

Acknowledgement menu item	User action
<b>Acknowledge message</b> After you acknowledge that you heard the event information, the system will call the next Follow-Me number	Press [1]
<b>Acknowledge message and stop all further FM notifications</b> This acknowledges the event and stops the system from calling the next Follow-Me numbers to report the event.	Press [2] + [code]
<b>Acknowledge message and access Operations menu</b> The Operations menu lists the available options for remotely operating your system (see <i>Telephone Operations Menu</i> , page 36).	Press [3] + [code]

---

#### NOTES:

- If an invalid code is entered 3 consecutive times, the system hangs up and that Follow-Me number will be locked for 15 minutes (during which time no calls will be initiated to the FM number).
  - If a valid user code is not entered within 10 seconds, the system hangs up.
-

## Telephone Operations Menu

The Operations menu announces the options and instructions for operating the system by telephone. The menu options vary, according to system status and user access rights.

<b>Operation</b>	<b>Procedure</b>
Arm all partitions	Press <b>[1][1]</b>
Arm a selected partition	Press <b>[1][9]</b> followed by the partition number
Disarm all partitions	Press <b>[2][2]</b>
Disarm a selected partition	Press <b>[2][9]</b> followed by the partition number
Change Zone Bypass status	Press <b>[3]</b> followed by the zone number, then <b>[#][9]</b>
Operate Utility Outputs	Press <b>[4]</b> followed by the output number
Change Follow Me numbers	Press <b>[5]</b> followed by the FM number and <b>[#][2]</b> . Enter the new phone number and press <b>[#][1]</b> .
Listen in to the premises	Press <b>[6][1]</b> See <i>Talk &amp; Listen</i> below.
Talk to the premises	Press <b>[6][2]</b> See <i>Talk &amp; Listen</i> below.
Listen and Talk to the premises	Press <b>[6][3]</b> See <i>Talk &amp; Listen</i> below.
Record messages that are not included in the message bank (up to 5 messages possible)	Press <b>[7][1 through 5]</b>
Record an opening message	Press <b>[7][6]</b>
Exit the System	Press <b>[0]</b>
Return to the previous menu	Press <b>[*]</b>
Repeat the menu options	Press <b>[#]</b>

### Talk & Listen

Talk & Listen enables 2-way communication (listening-in only, talking only, or both), and is used, for example, to remotely and silently listen in to the premises to verify the cause of an event occurrence, or to remotely talk to someone at the premises.

#### To use Talk & Listen:

1. From the Operations menu, press **[6]**; the following is announced: "To listen-in press [1], to talk press [2], to listen-in and talk (open channel) press [3], to return to the previous menu press [\*]."
2. Select an option.
3. Press **[\*]** to end the session and return to the Operations menu.

## SMS Operation

The following table describes user SMS commands for remote system operations.

---

**NOTE:** For SMS operation, the GSM/GPRS module must be installed in your system.

---

## SMS Confirmation Reply

An SMS sender can receive a confirmation (or fail) reply from the system upon request, by adding the letters **RP** at the end of any SMS command (see table below of SMS commands):

### Table of SMS Commands

Operation	SMS Command	Example
Away (Full) Arm	code + A	1234A
Home (Stay/Partial) Arm	code + H	1234H
Disarm	code + D	1234D
Partition Away (Full) Arm	code + A + partition number	1234A1
Partition Home (Stay/Partial) Arm	code + H + partition number	1234H1
Partition Disarm	code + D + partition number	1234D1
Bypass Zone	code + B + zone number	1234B05
Un-Bypass Zone	code + UB + zone number	1234UB05
Activate Output	code + UOON + UO number	1234UOON1
Deactivate Output	code + UOOFF + UO number	1234UOOFF1
Change FM Number	code + FMPHONE+ FM serial number + NEW +new phone number	1234FMPHONE3 NEW0529692345
Get system status	code + ST	1234ST
View last alarm	code + AL	1234AL
Get SIM credit level (for prepaid cards)	code +CR	1234CR

---

#### NOTES:

- SMS commands can be sent from any mobile phone or from an SMS website.
  - Command words are not case sensitive.
  - A separator between command words is not required although it is accepted.
-

# Registering the Agility 4 to the RISCO Cloud

To enable the use of GPRS/GSM communication and the iRISCO app, register your panel to the RISCO Cloud, and then log in.

---

**NOTE:** If using GPRS, verify with your installer that your panel is set to GPRS communication.

---

Registering to the Cloud can be done via self-registration or by the Installer, depending on the Cloud configuration.

---

**NOTE:** Before registering the panel, consult with your installer to check if the panel is already registered in the RISCO Cloud and is assigned to you. If so, open the email that was sent to you, then click on the confirmation link and follow the instructions to complete the registration.

---

If you were not invited by the Installer, you can perform registration yourself by following the instructions below.

## Registering to the RISCO Cloud

1. Go to **www.riscocloud.com** and click **register**
2. Fill in your **first and last name**.
3. Enter your **e-mail address** as the Login Name (required for 1st-time activation).
4. Define **password** (must be: a minimum of eight characters; contain at least one capital letter and one lower case letter; contain at least one number; and contain at least one special symbol) and then confirm.
5. Enter the **15 digits Panel ID** as it appear on the sticker located: on the postcard that arrived with the panel or supplied by the installer (also available in the keypad menu).
6. Complete registration form, and then press **Register**.
7. To complete the registration, open the email message received on the email account you defined as Login Name.

## Logging in to the RISCO Cloud / Accessing the Web User App

Here you can log in to the RISCO Cloud after registration and also log in to access the Web user app:

1. Go to **www.riscocloud.com**
2. Enter your **user name** and **password** (as defined during the registration process).
3. If you have more than one site, select the site you want to enter.
4. Enter the **PIN (user code)**.
5. Click **Login**.

# Smartphone / Web User Interface Operation

You must first be registered to the RISCO Cloud in order to operate your system using the Smartphone and Web apps.

For access to the Web User app, see the *Web User App User Guide*.

For access to the Smartphone app, see below.

## Downloading the iRISCO Smartphone App

The Smartphone app can be downloaded from the Apple App store for iOS devices or from the Android Play store for Android devices.

## Main iRISCO Operations

The following listing describes some of the main actions you can perform from the iRISCO Smartphone app:

- ✓ Full arming
- ✓ Stay/Home (partial) arming
- ✓ Full disarming
- ✓ Partition arming
- ✓ Zone bypassing
- ✓ Taking images upon request (Snapshot Follow Event)
- ✓ Video Verification
- ✓ Viewing history of images taken upon alarm event
- ✓ Viewing history of events
- ✓ Turning outputs on/off
- ✓ Notifications (App)/Followers(Web)



# User Settings

## Defining User Codes (System Users)

Using the LCD/Panda keypad or Web app, each system user is assigned a unique user code, which is needed to operate the system. Agility 4 can support the following: up to 31 different codes for system users and 1 Grand Master code. User codes are typically issued for:

- **Installer:** For system installation use only (installer code is for a temporary duration)
- **Grand Master:** One Grand Master code can be defined. A Grand Master is the primary system-responsible user with the highest level of user permissions). Although an installer may initially enable/disable permissions to have a user code, the Grand Master defines the actual numerical code for each user.
- **System Users:** For up to 31 other systems users















---

### NOTES:

- User codes (including Grand Master) may have either 4 or 6 digits (installer-defined).
  - The Grand Master default code is 1234. It is highly recommended to change it to a unique and confidential code after initial system setup.
  - The Grand Master can edit (change) the codes for all system users, but cannot view their currently-assigned codes.
  - Users with other authority levels can change their own codes only.
- 

## Assigning or Editing Users (User Codes)

To assign or edit a user code from an LCD/Panda keypad:

1. First make sure the system is disarmed.
2. Press  /  and then enter your **code** and then press  /  to access the **User Menu**.
3. Use   /   to scroll to **Codes/Tags**, and then press  / .
4. Scroll to **User Codes**, and then press  / .
5. Scroll to **New/Change Code**, and then press  / .

6. Scroll to select the **index number** (to designate to a system user), and then press



---

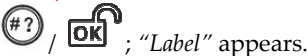
**NOTE:** Index number 00 is reserved for the Grand Master, while the other index numbers (01 through 31) are for all other system users.


---

7. Enter the **new code**.
8. Re-enter the **new code**; the system beeps and “Accepted” displays. If not re-entered correctly, the system sounds 3 beeps.
9. To edit parameters for the user such as Label (name), Partition, and Authority (level), do the following:
- Repeat steps 1–3 in this procedure, then scroll to **Parameters** and press





- Scroll to the index number (of the user you want to define), and then press






- Scroll between **Label**, **Partition**, and **Authority**, and press  to select:
  - For **Label**, edit by entering text over the existing description, then press



---

**NOTE:** Press each button repeatedly without pausing to toggle between all of its possible characters. Use  to scroll between spaces, and  to delete a character.

---

- For **Partition**, scroll between each partition (1, 2, and 3), and then for each, press  to toggle to either **Y** (to create partition) or leave it blank (to not partition), and then press .
- For **Authority**, scroll between the authority level options (**Arm only**, **Duress**, **Door Bypass**, **User**, or **Cleaner**), and then press  to select one of the options to assign to the user.

## Deleting User Codes



















User codes can only be deleted when the system is disarmed.

---

**NOTE:** It is not possible to delete the Grand Master code, although it can be changed.

---

### To delete a user code using an LCD/Panda keypad:

1. Press  /  and enter your **code** to access the **User Menu**.
2. Use   /   to scroll to **Codes/Tags**, and then press  / .
3. Scroll to **User Codes**, and then press  / .
4. Scroll to **Delete code**, and then press  / .
5. Scroll to the user index number of the code you want to delete, and then press  / .
6. At the “Delete User, Are You Sure?” prompt, press  /  to toggle to **Y** (yes), and then press  / ; the system beeps and “deleted” displays.

## Adding and Deleting Proximity Tags

At the LCD/Panda keypad you can use a proximity tag instead of entering your code – for performing arming/disarming or activating/deactivating functions.















The following Proximity tag operations can be performed:

- Adding a new proximity tag
- Deleting a proximity tag by the user's index number
- Deleting a proximity tag by the user's tag

### Adding a Proximity Tag

The Grand Master can assign a tag to any user in the system. Each proximity tag can be assigned to only one user.

To add a proximity tag:



















1. Press  /  and enter your **code** to enter the **User Menu**.
2. Use   /   to scroll to **Codes/Tags**, and then press  / .
3. Scroll to **Proximity Tags**, and then press  / .
4. Scroll to **New/Change**, and then press  / .
5. Scroll to select the user **index number** (to designate a tag to), and then press  /  ; "Approach Tag" displays.
6. Within 10 seconds, hold the tag 1–2 cm (.4–.8 in) from the LCD keypad buttons / at the right-hand side of the Panda Keypad display; the keypad then reads and saves the tag information. A long confirmation beep sounds, and a confirmation message is then displayed. If a proximity tag's information has already been saved in the system's memory, 3 error beeps will sound and a reject message will appear.

### Deleting a Proximity tag













Deleting proximity tags can be performed as follows:

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

### To delete by user index number:

1. Press  /  and enter your **code** to access the **User Menu**.
2. Use   /   to scroll to **Codes/Tags**, and then press  / .
3. Scroll to **Proximity Tags**, and then press  / .
4. Scroll to **Delete by User**, and then press  / .
5. Scroll to select the user **index number** (to delete), and then press  / .
6. At the “Delete User, Are You Sure?” prompt, press  /  to toggle to **Y** (yes), and then press  / ; the system beeps and a deletion message displays on the LCD/Panda keypad.

### To delete by tag:

1. Press  /  and enter your **code** to enter the **User Menu**.
2. Use   /   to scroll to **Codes/Tags**, and then press  / .
3. Scroll to **Proximity Tags**, and then press  / .
4. Scroll to **Delete by Tag**, and then press  / ; “Approach Tag” displays.
5. Within 10 seconds, hold the tag 1–2 cm (.4–.8 in) from the LCD keypad buttons / at the right-hand side of the Panda Keypad display; a deletion message displays.

## Defining Follow Me Destinations

The Grand Master can define FM destinations. In the case of an alarm or event, the system can send a “Follow-Me” event notification to a designated telephone number (voice message or SMS), to an e-mail address, or employ unique tones or custom event alert messages (push notification) to your Smartphone (if Cloud-connected – and defined through the iRISCO Smartphone app or the Web user app).

**To define a Follow Me destination using the LCD/Panda keypad:**

1. Press / and enter your **Grand Master code** to access the **User Menu**.
2. Use / to scroll to **Follow Me**, and then press / .
3. Scroll to select the user's **index number**, and then press / .
4. Scroll to **Define FM**, and then press / ; "Enter Phone" displays.
5. Enter the phone number (including area code) or e-mail address:
  - Use the scroll keys to go forward or backward, to edit each digit, as necessary.
  - Place the cursor at any digit/character you wish to delete, then press / and simultaneously for 2 seconds (you can also over-write any digit/character).

**NOTE:** Up to 32 digits/characters can be used for a Follow Me destination (phone number, e-mail address).

6. If required, incorporate the special functions listed below to achieve the described effect. Press or or to toggle to the required character.

<b>Special Function</b>	<b>Required character</b>
Stop dialing and wait for a new dial tone	W
Wait a fixed period before continuing to dial	,
Send the * character	*
Send the # character	#
User for calling internationally	+

7. When done with your entry, press / . "FM data saved" displays.

**Testing Follow Me Reporting**

The Grand Master and installer can test Follow Me reporting.

**To test Follow Me reporting:**

1. Press / and enter your **code** to enter the User Menu.
2. Use / to scroll to **Follow Me**, and then press / .
3. Scroll to select the user's index number, and then press / .
4. Scroll to **Test FM** and then press / ; "FM Test Activated" displays and a test event will be sent to the Follow Me destination.

# Activating/Deactivating Automatic Arming & Utility Output Programs with Scheduler

The Scheduler feature enables the Grand Master to activate or de-activate the following whenever needed:

- **Automatic system arming/disarming:** the Grand Master can activate (or deactivate) the system to be armed/disarmed at its pre-set time intervals.
- **Automatic activation of Utility Output (UO):** The Grand Master can activate (or deactivate) UO devices and appliances in order to operate automatically at their pre-set time intervals.











Before the Grand Master can activate/deactivate, the installer must first define the weekly program(s). Each program can be defined with up to two “ON” and “OFF” times per day.

---

### NOTES:

- Each program can be installer-defined to be activated in a different manner – for example, different scheduling days/times can be applied during a vacation
  - Automated programs can also be controlled with the Web user app.
- 

### To activate/deactivate an automated program from the LCD/Panda keypad:

1. Press  /  and enter your **Grand Master code**.
2. Scroll to **Clock**, and then press  / .
3. Scroll to **Scheduler En.**, and then press  / .
4. Scroll to select the (installer-defined) program index number, then press  /  to toggle between **Y** (activate) or **N** (deactivate), and then press  / .

# System Technical Specifications

---

## Electrical Characteristics

---

System power	230 V AC (-15%+10%), 50 Hz, 50 mA Optional: 9 V AC, 50-60 Hz
Units consumptions	Main board: Typical 130 mA GSM: Standby 35 mA, Communication 300 mA Modem: Standby 20 mA, Communication 60 mA IP Card: 115 mA (max)
Backup battery	Sealed lead acid battery 6 V, 3.7 Ah
Battery dimensions (HxWxD)	67 mm x 134 mm x 34 mm (2.64 in x 5.28 in x 1.34 in)
Internal siren intensity	100 dBA @ 1 m
Operating temperature	-10° C to 55° C (14° F to 131° F)
Storage temperature	-20° C to 60° C (-4° F to 140° F)

---

## Physical Characteristics

---

Dimension (HxWxD)	268.5 mm x 219.5 mm x 64 mm (10.57 in x 8.64 in x 2.52 in)
Weight (without battery)	1.31 Kg (full configuration)

---

## Wireless Characteristics

---

RF immunity	According to EN 50130-4
<b>Power Output</b>	868.65 MHz: 10mW Max. 869.525 MHz: 100mW Max.
Frequency	868.65 MHz or 433.92 MHz
<b>Camera Frequency</b>	869.525 MHz, 916 MHz, 430 MHz

---



## Standard Limited Product Warranty

RISCO Ltd., its subsidiaries and affiliates (“RISCO”) guarantee RISCO’s hardware 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 connection to the RISCO Cloud (for cloud connected products) or (ii) 24 months from production (for other products which are non-cloud connected), as the case may be (each, the “Product Warranty Period” respectively).

**Contact with customers only.** This Product Warranty is solely for the benefit of the customer who purchased the product directly from RISCO, or from any authorized distributor of RISCO. Nothing in this Warranty obligates RISCO to accept product returns directly from end users that 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. RISCO customer shall handle all interactions with its end users in connection with the Warranty, inter alia regarding the Warranty. RISCO’s customer shall make no warranties, representations, guarantees or statements to its customers or other third parties that suggest that RISCO has any warranty or service obligation to, or any contractual privity with, any recipient of a product.

**Return Material Authorization.** In the event that a material defect in a product shall be discovered and reported during the Product Warranty Period, RISCO shall, at its option, and at customer’s expense, either: (i) accept return of the defective Product and repair or have repaired the defective Product, or (ii) accept return of the defective Product and provide a replacement product to the customer. The customer must obtain a Return Material Authorization (“RMA”) number from RISCO prior to returning any Product to RISCO. 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 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 Products”), 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 Products.

**Entire Liability.** The repair or replacement of products in accordance with this warranty shall be RISCO’s entire liability and customer’s sole and exclusive remedy in case a material defect in a product shall be discovered and reported as required herein. RISCO’s obligation and the 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.** The Product 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, the Product Warranty does 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 delay or other failure in performance of the product attributable to any means of communications, 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 makes no other warranty, expressed or implied, and makes no warranty of merchantability or of fitness for any particular purpose. For the sake of good order and avoidance of any doubt:

**DISCLAIMER.** 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 LOSS OF DATA. 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 BY CUSTOMER OR END USER 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.

RISCO does not install or integrate the product in the end user security system and is therefore not responsible for and cannot guarantee the performance of the end user security system which uses the product.

RISCO does not guarantee 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.

Customer understands that a correctly installed and maintained alarm may only reduce the risk of burglary, robbery or fire without warning, but is not an assurance or a guarantee that such an event will not occur or that there will be no personal injury or property loss as a result thereof.

Consequently RISCO shall have no liability for any personal injury, property damage or loss based on a claim that the product fails to give warning.

No employee or representative of RISCO is authorized to change this warranty in any way or grant any other warranty.

## **RED Compliance Statement**

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

## **Contacting RISCO Group**

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

### **Belgium / Benelux**

Tel: +32-2522-7622

E-mail: [support-be@riscogroup.com](mailto:support-be@riscogroup.com)

### **China (Shanghai)**

Tel: +86-21-52-39-0066

E-mail: [support-cn@riscogroup.com](mailto:support-cn@riscogroup.com)

### **France**

Tel: +33-164-73-28-50

E-mail: [support-fr@riscogroup.com](mailto:support-fr@riscogroup.com)

### **Israel**

Tel: +972-3-963-7777

E-mail: [support@riscogroup.com](mailto:support@riscogroup.com)

### **Italy**

Tel: +39-02-66590054

E-mail: [support-it@riscogroup.com](mailto:support-it@riscogroup.com)

### **Spain**

Tel: +34-91-490-2133

E-mail: [support-es@riscogroup.com](mailto:support-es@riscogroup.com)

### **United Kingdom**

Tel: +44-(0)-161-655-5500

E-mail: [support-uk@riscogroup.com](mailto:support-uk@riscogroup.com)

### **United States**

Tel: +1-631-719-4400

E-mail: [support-usa@riscogroup.com](mailto:support-usa@riscogroup.com)

This RISCO product was purchased from:

