iotega

DSC

From Tyco Security Products

Wireless Security and Automation System

User Manual

WARNING: This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer. Read the entire manual carefully.

Table of Contents

1.0 About your security system **3**
1.1 Fire detection 3
1.2 Carbon monoxide detection 3
1.3 Testing your system 3
1.4 Monitoring 4
1.5 Cleaning and maintenance 4
2.0 General system operation **5**
2.1 Integrated keypad 5
2.2 Panel indicators 5
2.3 Integrated keypad quick reference 8
2.4 Wireless LCD keypad 8
2.4.1 Wireless keypad symbols 9
2.4.2 Wireless keypad quick reference 9
2.5 Important notice 10
2.5.1 Power save mode 10
2.6 Language selection 10
2.7 System models 10
3.0 Arming the system **11**
3.1 Stay arming 11
3.1.1 Stay arming on the integrated keypad 11
3.1.2 Stay arming on the wireless keypad 11
3.2 Silent exit delay 12
3.3 No-entry arming 12
3.4 Away arming 12
3.4.1 Away arming on the integrated keypad 12
3.4.2 Away arming on the wireless keypad 12
3.5 Quick exit 13
3.5.1 Quick exit on the wireless keypad 13
3.6 Arming errors and exit faults 13
3.6.1 Arming error 13
3.6.2 Audible exit fault 13
3.7 Alarm cancel window 14
3.8 Bypass zones 14
4.0 Disarming the system **15**
4.1 Disarming on the integrated keypad 15
4.2 Disarming on the wireless keypad 15
4.3 Disarming error 15
5.0 Using wireless keys **16**
6.0 User access codes **17**
6.1 Access code types 17
6.1.1 Level 1 access (supervisor/administrator) 17
6.1.2 Level 2 access (basic/standard user) 18
7.0 Additional features **19**
7.1 System lockout due to invalid attempts 19
7.2 Burglary verification 19
7.3 Swinger shutdown 19
7.4 Fire alarm verification 19
8.0 Emergency keys **20**
8.1 Emergency keys on the integrated keypad 20
8.2 Emergency keys on the wireless keypad 20
8.3 When alarm sounds 20
8.3.1 Fire alarm pulsed siren (temporal 3) 21
8.3.2 Carbon monoxide (CO) alarm 21
8.3.3 Intrusion (burglary) alarm 21

9.0 Viewing troubles **22**
10.0 Using Z-Wave Devices **24**
10.1 Z-Wave Alliance Certification 24
10.2 Adding or Removing a Controller 24
10.3 Replicating a Controller 24
10.4 Controller Learn Mode 24
10.5 Changing the Primary Controller 24
10.6 Adding a Device 24
10.6.1 Editing or Removing a Device 25
10.7 Device Interoperability 25
10.8 Z-Wave Association Groups 25
10.9 Responding to the Basic Command 25
10.10 Z-Wave Reset 25
11.0 Safety instructions **26**
12.0 Locating detectors and escape plan **27**
12.1 Smoke detectors 27
12.2 Fire escape planning 28
12.3 Carbon monoxide detectors 29
12.0 Regulatory agency statements **30**
13.0 Reference sheets **32**
13.1 System information 32
13.2 Service contact information 32

1.0 About your security system

Read this manual carefully and have your installer instruct you on your system's operation and on which features have been implemented in your system. All users of this system must be fully instructed in its use. Fill out the **System Information** page with all of your zone information and access codes, and store this manual in a safe place for future reference.

Note: The iotega security system includes specific false alarm reduction features and is classified in accordance with ANSI/SIA CP-01-2014 Control Panel Standard - Features for False Alarm Reduction. Consult your installer for further information regarding the false alarm reduction features built into your system, as this manual does not cover all features.

1.1 Fire detection

If your installer enables this feature, this system can monitor fire detection devices, such as smoke detectors, and provide a warning if a fire condition is detected. Good fire detection depends on having an adequate number of detectors placed in appropriate locations. This equipment must be installed in accordance with NFPA 72 (N.F.P.A., Batterymarch Park, Quincey MA 02269). Carefully review the **Fire Escape Planning** section in this manual.

1.2 Carbon monoxide detection

If your installer enables this feature, this system can monitor carbon monoxide detectors and provide a warning if carbon monoxide is detected. Refer to the **Fire escape planning** and **Carbon monoxide detectors** sections for more information.

1.3 Testing your system

The system test activates a 4-second check of the system status LEDs, keypad LEDs, buzzer, and siren. It is a partition-based test and must be done when the system is disarmed.
You can perform a system test from the web portal.

The following events happen during a system test:

- All system status LEDs flash for 4 seconds.
- A system test transmits to the monitoring station.
- The system checks the backup battery level.
- The keypad LEDs illuminate for 4 seconds.
- The system buzzer sounds for 4 seconds, or the partition buzzer and siren sound for 2 seconds each in series.

Test your system weekly to ensure that it functions as intended. Inform your monitoring station when you begin and end system testing.
A qualified service technician must test household fire alarm systems at least every 3 years in accordance with NFPA72. It is your responsibility to test the system weekly, excluding smoke detectors.
If the system fails to function properly, call your installation company for service.

1.4 Monitoring

This system can transmit alarms, troubles and emergency information. If you initiate an alarm by mistake, immediately call the monitoring station to prevent an unnecessary response.

Notes:

- Your installer must enable the monitoring function before it is functional.
- Consult with your installer to determine if your system is configured with a communicator delay. A communicator delay prevents a report to the monitoring station if the control panel is disarmed within 30-45 seconds after an intrusion alarm is triggered. Note that fire-type alarms are normally reported without a delay.
- If enabled and configured, you cancel an alarm after the communication delay with the alarm cancel window. Refer to the **Alarm cancel window** section for more information.
- Contact your installer to verify that your system is compatible with the Central Station Receiver format at yearly intervals.

1.5 Cleaning and maintenance

Keep your Alarm Controller in optimal condition by following all the instructions that are included within this manual and/or marked on the product. It is the end-user's and/or installer’s responsibility to dispose of used batteries according to the waste recovery and recycling regulations applicable to the local market.

- Clean the unit by lightly dusting with a slightly moistened cloth.
- Do not wipe the front cover with alcohol.
- Do not use water or any other liquid.
- Do not use abrasives, thinners, solvents or aerosol cleaners (spray polish) that may enter through holes and cause damage.
- Replace the standby battery every 3-5 years.

For other system devices or sensors, consult the manufacturer’s literature for testing and maintenance instructions.

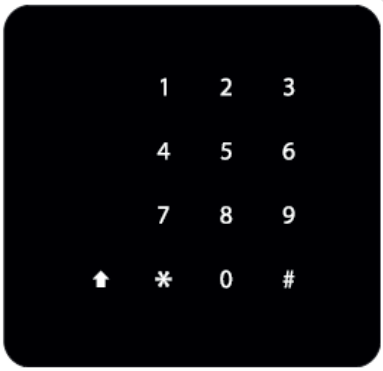
2.0 General system operation

Your security system comprises an integrated alarm control/panel and various sensors and detectors. The system is self-contained; the control panel, integrated keypad, and standby battery are all housed within the unit.

The security system has several zones of area protection. A zone is a sensor or detector that communicates with the panel. A sensor in alarm is indicated on the integrated keypad, wireless keypad, touchscreen keypad, and by messages on the mobile phone user application.

2.1 Integrated keypad

The iotega system includes a capacitive touch integrated keypad with 16 keys: numbers 0 thru 9, *, #, Fire, Auxiliary, Panic emergency keys, and shift (up arrow).
During power up, the number keys illuminate in sequence several times. In normal operation, the keypad remains off when not in use. When you wave your hand in close proximity to the keypad, the number keys illuminate.



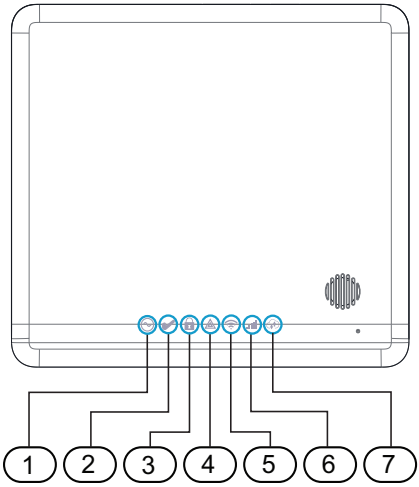
Notes:

- The emergency keys do not illuminate unless you tap the shift key. See the **Emergency Keys** section for more information.
- You can only use the keypad for arming, disarming, and the emergency keys. The same functions are available when switching between partitions.

2.2 Panel indicators

The iotega system includes seven LED status indicators:

- Four single-color LEDs
- Three multi-color LEDs (red, green, amber)



Item	Description
1	Power LED
2	Ready to Arm LED
3	Armed LED
4	Trouble LED
5	WiFi Signal Strength LED
6	Cellular Signal Strength LED
7	Remote Connection LED

Power

Status LED	Indication	Description
	ON (green)	AC power is connected to the system.
	Flashing (green)	System Test All status LEDs flash at the same time.
	OFF	There is no AC power to the system.

Ready to Arm

Status LED	Indication	Description
	ON (green)	The partition is ready to arm. There are no fire or CO alarm conditions.
	Flashing (green)	System Test All status LEDs flash at the same time.
		Installer Walk Test Ready, Trouble, and Arm LEDs flash at the same time.
	OFF	The system is not ready to arm. A fire or CO alarm condition is present.

Armed

Status LED	Indication	Description
	ON (red)	The partition is armed..
	Flashing (red)	The partition is in Alarm. **Note:** Silent alarms or panics do not flash the Alarm LED.
		System Test All status LEDs flash at the same time.
		Installer Walk Test Ready, Trouble, and Arm LEDs flash at the same time.
	OFF	The partition is disarmed

Trouble

Status LED	Indication	Description
	ON (amber)	A system trouble is present.
	Flashing (amber) [cadence of 500ms On/500ms OFF]	[*][2] The Trouble menu is accessed.
	Flashing (amber) [cadence of 250ms ON/250ms OFF/250ms ON/750ms OFF]	The system is in the second-level submenu.
	Flashing (amber) [cadence of 250ms ON/250ms OFF/250ms ON/250ms OFF/250ms ON/750ms OFF]	The system is in the third-level submenu.
	Flashing (amber)	System Test All status LEDs flash at the same time.
		Installer Walk Test Ready, Trouble, and Arm LEDs flash at the same time.
	OFF	System troubles are cleared.

WiFi Signal Strength

Status LED	Indication	Description
	ON (green)	The radio is active with a strong signal connection.
	ON (amber)	The radio is active with a weak signal connection.
	ON (red)	There is no signal.
	Flashing (green).	The radio is active in WiFi protected setup (WPS) mode for access point (AP) mode.
	Flashing (amber)	Z-Wave radio is active in learn pair mode
	Flashing (amber)	System Test All status LEDs flash at the same time.
	OFF	The radio is inactive or not connected to the network.

Cellular Signal Strength

Status LED	Indication	Description
	ON (green)	Cellular is active with a strong signal connection.
	ON (amber)	Cellular is active with a weak signal connection.
	ON (red)	A communicator is installed but there is no signal or connection
	Flashing (amber)	System Test All status LEDs flash at the same time.
	OFF	A communicator is not installed or not configured.

Remote Connection Status

Status LED	Indication	Description
	ON (green)	The link is active with a server.
	Flashing (red)	The link activates but fails to communicate with the server.
	Flashing (amber)	System Test All status LEDs flash at the same time.
	OFF	The link is not yet active with any server.
Note: If the Remote Connection status LED flashes red, the server may be undergoing maintenance or experiencing technical difficulties. Restarting the panel may remedy the issue. If the problem persists, contact your installer.		

2.3 Integrated keypad quick reference

Use the following table for quick reference of the integrated keypad options:

Action	Enter
Away arm	[Access Code]
Stay arm	[Access Code]
Disarm	[Access Code]
Abort arming sequence	[Access Code]
System troubles	
Silence troubles	[Any key] or [*][2] + [Access code[1]]
View troubles	[*][2] + [Access code[1]] + [Trouble code]

[1]For UL listed installations, you must enter your access code to silence trouble beeps and view system troubles.

2.4 Wireless LCD keypad

The iotega system supports the following keypad model:

WS9LCDWFx Wireless Alphanumeric LCD keypad

2.4.1 Wireless keypad symbols

Status LED		Indication	Description
	Ready to arm	ON (green)	The partition is ready to arm. There are no fire or CO alarm conditions.
	Armed	ON/flashing (red)	The partition is armed..
	Trouble	ON (yellow)	A system trouble is present.
		Flashing	Keypad low battery
	Power	ON (green)	AC power is connected to the keypad.

2.4.2 Wireless keypad quick reference

When using the wireless keypad, the iotega system uses shortcut keys to access options or features. Additionally, it uses a menu-based navigation system. Use the scroll keys to scroll through the list of options contained within the current menu.

Note: Your installer must enable and configure some features.

Action	Press
Away Arm	for 2 seconds + [Access Code[1]]
Stay Arm	for 2 seconds + [Access Code[1]]
Disarm	[Access Code]
Abort arming sequence	[Access Code]
Bypassing - All bypass commands begin with [*][1] + [Access Code[1]]	
Bypass individual zones	[3-digit zone #]
Common functions	
Turn chime ON/OFF	for 2 seconds
Change brightness	[*][6] + [Master code] + < >
Change contrast	[*][6] + [Master Code] + < >
View troubles	[*][2] + [Access code [2]] + < >
View alarms	[*][3] + < >
Buzzer volume	[*][6] + [Master Code] + < >
Language selection	[*][6] + [Master Code] + < >

[1]If configured by your installer

[2]For UL listed installations, you must enter your access code to silence trouble beeps and view system troubles.

2.5 Important notice

A security system cannot prevent emergencies. It is only intended to alert you and your monitoring station, if applicable, to an emergency situation. Security systems are generally very reliable, but they may not work under all conditions and they are not a substitute for prudent security practices or life and property insurance. Your security system must be installed and serviced by qualified security professionals. These professionals can instruct you on the level of protection that has been provided and on system operations.

2.5.1 Power save mode

When the panel is in Power Save mode, it is saving battery life. The integrated keypad is not turned on until there is a specific reason, such as a hand wave in front of the panel, or the start of an entry delay.
When initiated, the status indicators stay on for 30 seconds before turning off. In this mode, the panel is still functioning, but nothing is visible.

Note: For UL listed installations, the user app and touchscreen keypad functions are not available in this mode; therefore, you must use the integrated keypad or the wireless keypad to arm or disarm the system.

2.6 Language selection

The system supports the following three languages:

- English
- French
- Spanish

You can select the language on the touchscreen keypad or the wireless keypad.

2.7 System models

The reference to WS900 in this manual covers the following models:

WS900-29*	Alarm system with two-way audio support, operating in 912-919 MHz band
WS900-19*	Alarm system with two-way audio support, operating in 912-919 MHz band
3G7090*	3G Cellular Alarm Communicator
LT7090*	Verizon LTE Only Cellular Communicator

(*) These devices are UL/ULC listed.

WS900-28	Alarm system operating in 868 MHz band
WS901-18	Alarm system operating in 868 MHz band
WS901-24EU	Alarm system operating in 433 MHz band
WS901-14	Alarm system operating in 433 MHz band
3G7090-EU	3G Cellular Alarm Communicator

Note: Two-way audio support was not evaluated by UL/ULC.

WS901-29	Alarm system, operating in 912-919 MHz band

3.0 Arming the system

You can arm the system using the following options:

- Integrated keypad
- Wireless keypad
- Touchscreen keypad
- User app (Operation with the user app was not evaluated by UL/ULC.)
- Wireless key (Refer to the **Using wireless keys** section for a list of UL/ULC listed compatible wireless keys.)

3.1 Stay arming

Stay arming arms only the perimeter of the premises permitting movement inside.

Note: To arm the system in Stay mode, your installer must enroll and configure at least one zone as an Interior Stay/Away or a Delay Stay/Away type of zone.

3.1.1 Stay arming on the integrated keypad

To arm the system in Stay mode on the integrated keypad, complete the following steps:

1. Ensure all protected doors and windows are secure or bypassed and that the Ready indicator is on.
2. Enter your access code and do not leave the premises. The system automatically ignores bypassed zones and initiates the exit delay countdown.

To cancel the arming sequence, enter your access code.
When exit delay is active, the Armed and Ready indicators turn on and the keypad beeps once per second. When the exit delay expires, the system is armed and is indicated by the Ready indicator turning off and the Armed indicator staying on.

Note: For SIA CP-01 listed panels, the Stay arming exit delay will be twice as long as the Away arming exit delay.
If your system is installed in accordance with SIA CP-01 Standard for False Alarm Reduction, the security system arms in the Stay mode if the exit delay time expires and there was no exit.
If you arm the system remotely without exit delay, the security system arms in Away mode only.

3.1.2 Stay arming on the wireless keypad

Stay mode partially activates your alarm system by arming all perimeter sensors and bypassing all interior sensors.

To arm the system in Stay mode, complete the following steps:

1. Ensure all protected doors and windows are secure or bypassed and that the Ready indicator is on.
2. Enter your access code.
   OR
   Press and hold the Stay Arm function key for 2 seconds and enter your access code, if required.
   If zones have been bypassed, a warning appears

After successfully initiating the arming sequence, the following events occur:

- Armed indicator turns on.
- Ready indicator remains on.

- Exit Delay timer begins counting down.

When the exit delay timer expires, arming the system, the following events occur:

- Ready indicator turns off..
- Armed indicator remains on.
- Bypass or system indicator activates

To cancel the arming sequence, enter your access code.

3.2 Silent exit delay

If the system is armed in Stay mode or using the No-entry arming method, the keypad buzzer is silenced and the exit time is doubled for that exit period only. (SIA CP-01 only.)

3.3 No-entry arming

No-entry armingarms the system in Stay or Away mode after the exit delay expires and removes the entry delay.

Notes:

- All zones programmed as Delay function the same way as instant zones.
- This feature is only available on the touchscreen keypad and user app.

3.4 Away arming

Away arming arms the entire system, including the perimeter and interior devices.

3.4.1 Away arming on the integrated keypad

To arm the system in Away mode on the integrated keypad, complete the following steps:

1. Ensure all protected doors and windows are secure or bypassed and that the Ready indicator is on.
2. Enter your access code. Exit delay begins. Exit the premises through a door programmed as entry/exit type.

To cancel the arming sequence, enter your access code.

When exit delay is active, the Armed and Ready indicators turn on and the keypad beeps once per second. Depending on your system configuration, you have ____ seconds to exit the premises. Your installer can program this time.

The keypad buzzer emits a rapid pulsating rate during the last 10 seconds of the exit delay to indicate that the time is expiring.

When exit delay is active, the Armed and Ready indicators turn on and the keypad beeps once per second. When the exit delay expires, the system is armed and is indicated by the Ready indicator turning off and the Armed indicator staying on.

Note: In Away arming mode, manually bypassed zones are logged and communicated to the monitoring station.

If your system is installed in accordance with SIA CP-01 Standard for False Alarm Reduction, the following condition applies: Violation and restoral, followed by a second violation of the entry/exit zone before the end of the exit delay, restarts the exit delay.

3.4.2 Away arming on the wireless keypad

To arm the system in Away mode, complete the following steps:

1. Ensure all protected doors and windows are secure or bypassed and that the Ready indicator is on.

2. Enter your access code.
   OR
   Press and hold the Away Arm function key for 2 seconds and enter your access code, if required.
   If zones have been bypassed, a warning appears

To cancel the arming sequence, enter your access code.
Note: Your installer configures the exit delay time.

3.5 Quick exit

If the system is armed and you must exit, use the Quick Exit function to avoid disarming and rearming the system. Using this function gives you 2 minutes to exit the premises. When the door is closed after exiting, the remaining exit time is cancelled.
Note: This feature is not available on the integrated keypad.

3.5.1 Quick exit on the wireless keypad

To use the Quick Exit function on the wireless keypad, complete the following steps:

1. When system is armed and the Armed indicator is on, press and hold the Quick Exit key for 2 seconds..
2. Exit the premises before the exit delay timer expires. After exiting, the delay timer is canceled.

3.6 Arming errors and exit faults

Your security system audibly notifies you of any errors when you are attempting to arm the system or exit the premises.

3.6.1 Arming error

An error tone (long beep) sounds if the system is unable to arm. Arming errors occur under the following conditions:

- The system is not ready to arm, i.e. sensors are open
- The access code is incorrect.
- A trouble condition is present.

Ensure all sensors are secure and the system is ready to arm, then try again.

3.6.2 Audible exit fault

To reduce false alarms, the audible exit fault notifies you of an improper exit when arming the system. If the entry/exit door is not securely closed during the programmed exit delay, the system sounds the alarm to indicate an improper exit.

To correct an exit fault, complete the following steps:

1. Re-enter the premises.
2. Enter your access code to disarm the system before the entry delay timer expires
3. Ensure all sensors are secure and the system is ready to arm.
4. Repeat the Away arming procedure.

3.7 Alarm cancel window

There is a period of time in which you can cancel the alarm transmission. When the programmed alarm transmission delay expires, canceling an alarm sends a message to the monitoring station. When the cancellation message is successfully transmitted, the system beeps six times.

Note:

- Your installer must enable and configure this feature.
- For CP-01 systems, alarm transmission delay must not exceed 45 seconds.

3.8 Bypass zones

Use the zone bypassing feature when you need access to a protected area while the system is armed, or when a zone is temporarily out of service, but you need to arm the system. Bypassed zones are not able to sound an alarm. As a result, bypassing zones reduces the level of security. If you are bypassing a zone because it is not working, call a service technician immediately to resolve the problem and restore your system to proper working order.

Ensure that no zones are unintentionally bypassed when arming your system. Zones cannot be bypassed once the system is armed. Bypassed zones, except for 24-hour zones, are automatically unbypassed each time the system is disarmed and must be bypassed again before the next arming, if needed.

Notes:

- 24-hour zones can only be unbypassed manually.
- For UL listed installations, zones can only be bypassed manually.

4.0 Disarming the system

You can arm the system using the following options:

- Integrated keypad
- Touchscreen keypad
- Wireless keypad
- User app (Operation with the user app was not evaluated by UL/ULC.)
- Wireless key (Refer to the **Using wireless keys** section for a list of UL/ULC listed compatible wireless keys.)

4.1 Disarming on the integrated keypad

To disarm the system on the integrated keypad, complete the following steps:

1. Enter your access code.
2. If you open the entry/exit door, a continuous tone indicates that entry delay has started. Enter your access code within ____ seconds to avoid an alarm condition. Your installer can program this time.

Note: When disarming the system during entry delay, the tone is silenced when you enter the first digit of your access code. If your access code is invalid, the tone starts again.

4.2 Disarming on the wireless keypad

To disarm the system on the wireless keypad, complete the following steps:

1. Enter your access codewhen the system is armed. (Armed indicator is on).
2. If you walk through the entry door, the keypad beeps. Disarm within _____ seconds to avoid an alarm condition.

4.3 Disarming error

If your access code is invalid, the system does not disarm and emits a 2-second error tone. If this happens, press [#] and try again to ensure that you entered a valid access code. If it happens again, the access code may be invalid.

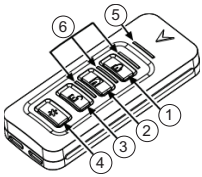
5.0 Using wireless keys

In addition to the keypad, you can control your system with two-way wireless keys. All wireless key buttons are programmable. Your installer can verify the functions for each key.
Using a two-way wireless key, you can arm or disarm the system while you are in close proximity to your house, or you can call for help.

The following wireless keys are compatible with the iotega system:

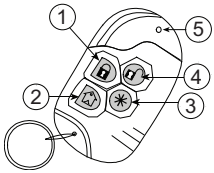
Note: The button functions listed are the default for each wireless key.

PG4929/PG8929/PG9929



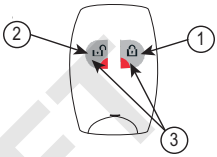
1. Away Arm
2. Stay Arm
3. Disarm
4. Panic
5. Message LED
6. Status LEDs

PG4939/PG8939/PG9939



1. Away Arm
2. Stay Arm
3. Disarm
4. Panic
5. LED

PG4949/PG8949/PG9949



1. Away Arm
2. Disarm
3. Panic

Note: The panic feature is disabled on PGx929 and PGx939 for SIA CP-01 certified installations.

A user at Master or Administrator level can assign enrolled wireless keys to other users.

To arm the system with a wireless key, press the desired arming mode button when the Ready indicator is on.
Note: When arming the system with a two-way wireless key, the system squawks once to indicate the system is armed.

To disarm the system with a two-way wireless key, complete the following steps:
1. Press the disarm button.
2. If you walk through the entry door, the keypad beeps. Press the disarm button within ____ seconds to avoid an alarm condition.

Note: When disarming the system with a two-way wireless key, the system squawks twice to indicate the system is disarmed.

6.0 User access codes

The iotega system supports up to 100 users, including the Master user. By default, user #1 is the Master user. You cannot disable or delete this user from the system. The system also supports an additional two duress codes, one for each partition.

From the touchscreen keypad, you can program and configure user types for users 2 through 100. You can assign a user to one or both partitions and enable or disable system interaction.

User access codes are four digits and must be unique; the system does not duplicate codes. If you program a duplicate code, the system errors and rejects the code. If you try to change an existing user code to a one that is already programmed, the system errors and rejects the change.

6.1 Access code types

The iotega system provides the following user access code types:

Master code This is the system master code. You cannot disable or delete this code, but you can change it in the user app or on the touchscreen keypad. Use this code to program all other access codes, including the duress codes. You can use this code to do all user-level functions, except to access Installer mode.

User codes There are two access levels for user codes:

- Level 1 - Supervisor/Administrator
- Level 2 - Basic/Standard User

Each level has different permissions. See the following sections for descriptions of each level.

Duress codes Use duress codes to disarm the system only in an emergency situation. When used, an emergency disarm event transmits to the monitoring station. The system supports two duress codes, one for each partition. These codes are excluded from the total number of available codes. They have the access level of a Level 2 Basic User.

6.1.1 Level 1 access (supervisor/administrator)

Users at this level have similar privileges to the master user but are limited based on their partition assignment. Users can do the following actions on their partitions:

- Arm/disarm
- Bypass/unbypass
- Chime enable/disable
- View troubles

Level 1 users can also do any user level functionality on the keypad or user app, as follows:

- Initiate system test
- Enable installer or remote access
- Language selection
- View event buffer
- View PowerG camera images
- Program zone and partition labels
- Schedule Auto Arming
- Initiate firmware updates
- Update the system WiFi SSID and password

- Create new users and user labels
- Program duress codes

Note: Users can only add, edit, or delete users that are assigned to the same partition as they are.

6.1.2 Level 2 access (basic/standard user)

Users at this level have access to basic security functions but are limited based on their partition assignment. Users can do the following actions on their partitions:

- Arm/disarm
- Bypass/unbypass
- Chime enable/disable
- View system troubles
- View alarm memory
- View event history

7.0 Additional features

The following sections list additional feature of your iotega system.

7.1 System lockout due to invalid attempts

If configured, your system automatically locks out inputs from all keypads for a specified duration if you enter too many invalid access codes. When you tap or press any keys, an error tone sounds. Emergency keys are still active during keypad lockout.
Note: Your installer must configure this feature and the lockout duration.

7.2 Burglary verification

The control panel includes cross zone and sequential detection features that require a trip on two or more zones within a given time period, to generate a confirmed alarm for police response.
Note: Your installer must enable and configure this feature.

7.3 Swinger shutdown

The panel has a swinger shutdown feature that shuts down a zone after a programmable number of trips. All burglary zone types have this feature enabled in CP-01 installations.

For SIA CP-01 classified installations, the swinger shutdown feature is programmed such that one or two trips shuts down the zone. The zone is restored after a manual reset by entering the access code at the time of disarming the alarm system, or it is reset automatically after 8 hours with no trips on any zones.

Note: Your installer must be enable and configure this feature.

7.4 Fire alarm verification

Fire alarm verification is an available option for fire zones. If configured, when the conditions for alarm verification are met the fire alarm sounds and an alarm transmission is sent to the monitoring station.
Note: Your installer must be enable and configure this feature.

8.0 Emergency keys

IMPORTANT: EMERGENCY USE ONLY!
The emergency keys generate a fire, auxiliary, or panic alarm and alerts the monitoring station.

8.1 Emergency keys on the integrated keypad

To use the emergency keys on the integrated keypad, complete the following steps:

1. Tap the shift key (up arrow) on the keypad. The emergency keys illuminate.

   Fire

   Auxiliary

   Panic

2. Touch and hold the Fire, Auxiliary, or Panic key for 2 seconds. The system beeps to indicate the alarm input was accepted and transmission is underway.
   The Fire key activates the siren in the pulsed fire pattern.
   For Auxiliary alarms, the system beeps again when the monitoring station acknowledges the signal.
   The Panic alarm is completely silent.
3. To return to the number keypad without using the emergency keys, tap the [#] key.

8.2 Emergency keys on the wireless keypad

To use the emergency keys on the wireless keypad, press both keys of the emergency type and hold for 2 seconds.

Fire

Auxiliary

Panic

The system beeps to indicate that the alarm input has been accepted and sent to the monitoring station.

Notes:

- Verify with your alarm company that your system is equipped with emergency keys.
- Depending on your system configuration, your installer can disable any of the emergency keys.

8.3 When alarm sounds

The system can generate the three different alarm sounds in this order of priority:

1. Fire alarm = temporal/pulsed siren
2. Carbon monoxide alarm = four beeps, 5-second pause, four beeps
3. Intrusion (burglary) alarm = continuous siren

Note: The panic alarm is silent and only results in an alarm transmission to the monitoring station.

8.3.1 Fire alarm pulsed siren (temporal 3)

In the event of a fire alarm, follow your emergency evacuation plan immediately!

The fire alarm temporal/pulsed siren sounds of three short pulses followed by a 1.5-second pause, then repeats. .
If the fire alarm was accidental, e.g. burnt toast, bathroom steam, etc., enter your access code to silence the alarm and call your monitoring station to avoid a dispatch.

Note: Verify with your alarm company that your system is equipped with fire detection.
For information on resetting smoke detectors see **Resetting Smoke Detectors**.

8.3.2 Carbon monoxide (CO) alarm

Activation of your CO alarm indicates the presence of carbon monoxide (CO), which can be fatal.

Carefully review your Carbon Monoxide Alarm Installation/User Guide to determine the necessary actions required to ensure your safety and ensure that the equipment is operating correctly. Incorporate the steps outlined in the guide into your evacuation plan.

An alarm is indicated by the following conditions:

- The red LED on the CO detector flashes rapidly and buzzer sounds with a repeating cadence of four quick beeps, 5-second pause, four quick beeps.
- The siren connected to the control panel produces the same cadence as above.
- The system provides audible and visual indication of the CO alarm.

If the CO alarm sounds, complete the following steps:

1. Immediately move outdoors or to an open door/window.
2. Call emergency services or your fire department.

8.3.3 Intrusion (burglary) alarm

If you are unsure of the source of the alarm, proceed with caution!

If the alarm was accidental, enter your access code to silence the alarm. If you disarm the alarm system within the programmed transmission delay time, no alarm transmission is sent to the monitoring station. Check with your installer to see if this option has been enabled on your system and for the transmission delay time.
Following the transmission delay time, enter your access code to cancel an alarm that was previously transmitted. The keypad sends a cancel signal to the monitoring station. When the monitoring station receives the signal, the keypad sounds eight beeps to confirm. Call your monitoring station to avoid a dispatch.

9.0 Viewing troubles

When the system detects a trouble condition, the Trouble indicator turns on and the system beeps every 10 seconds. Tap any key on the integrated keypad to silence the beeps. Alternatively, press the [*] key on the wireless keypad.
Note: For UL listed installations, you must enter your access code to view system troubles.

To view troubles on either keypad, do the following steps:

1. Enter [*][2].
2. Enter your access code, if required. The Trouble indicator flashes if an access code is required.

The system indicates top-level trouble codes by illuminating the corresponding numbers on the keypad, and the Trouble indicator flashes once with a pause, then repeats.

3. Tap or press one of the numbers to see the next level code. At the second level, the Trouble indicator flashes twice with a pause, then repeats.
4. Repeat step 3 to go to the next level. The system beeps if there is no third-level trouble condition. At this level, the Trouble indicator flashes three times with a pause, then repeats.

If there is more than one zone in trouble, each zone number flashes in sequence until you exit the trouble menu or when the time expires. At this level, the Trouble indicator flashes three times with a pause, then repeats.

5. Tap or press [#] to return to the previous level trouble code or to exit the trouble menu.

Top level Device type		Second level Trouble type		Third level Device ID
01	System trouble	01	AC	
		02	Battery trouble (all battery troubles)	
		03	Tamper	
		04	Hardware fault	
		05	Loss of time	
		06	RF jam	
02	Zone	01	AC	1-128
		02	Battery trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not networked	
		06	Fire/CO trouble	
03	Siren	01	Future use	1 to 16
		02	Battery trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not networked	

Top level Device type		Second level Trouble type		Third level Device ID
04	Keypad	01	AC (WiFi keypads only)	1 to 9
		02	Battery trouble (wireless only)	
		03	Tamper (wireless only)	
		04	Fault (supervision) (onboard, wireless , and WiFi keypads)	
		05	Not networked (wireless only)	
05	Repeater	01	AC	1 to 8
		02	Battery trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not networked	
		06	RF jam	
06	Wireless key	01	Future use	1 to 32
		02	Battery trouble	
		03	Future use	
		04	Future use	
		05	Not networked	
07	Communication	01	Receiver not available	
		02	FTC trouble	1- Receiver 1 2- Receiver 2 3- Receiver 3 4- Receiver 4
		03	Receiver supervision trouble	
		04	Cellular trouble	
		05	Ethernet/WiFi trouble	
		06	Remote shutdown	

10.0 Using Z-Wave Devices

The Smartlink user app and web portal supports Z-Wave-enabled devices, such as lights, door locks, and switches.

10.1 Z-Wave Alliance Certification

The iotega panel is a security-enabled Z-Wave Plus product that can use encrypted Z-Wave Plus messages to communicate to other Z-Wave Plus products.

10.2 Adding or Removing a Controller

To add the panel as a secondary controller to another Z-Wave network, complete the following steps:

1. Put the primary controller into Inclusion mode. Refer to the controller manual for more information.
2. In the Smartlink web portal, under **Home Control**, click **Device Control**.
3. Under **Setup**, click **Tools**, then click **Add/Remove Z-Wave Controller**.

To remove the panel as a secondary controller and re-establish it as primary, repeat the steps, changing the primary controller in step 1 to Exclusion mode.

10.3 Replicating a Controller

If the panel is established as a secondary controller on the Z-Wave network, you can request replication updates from the primary controller. This ensures that the Z-Wave information synchronizes from the primary controller to the panel.

To do this, click **Replicate Z-Wave Controller** under the **Tools** tab.

10.4 Controller Learn Mode

You can set the panel to receive network information from another Z-Wave controller using the Learn mode. Press the button on the controller to put it into Learn mode.

Some applications include adding the panel to or removing it from another network and changing primary controllers.

10.5 Changing the Primary Controller

If there are two or more controllers in the Z-Wave network, you can change the primary controller from the iotega panel to another controller.

To do this, click **Change Primary Controller** under the **Tools** tab, then set the other controller to Learn mode. Refer to the controller manual for more information..

10.6 Adding a Device

The Smartlink user app main screen has different options to add and control Z-Wave devices.

To add a device on the app, tap the applicable option and complete the following steps:
1. Power up your device per the manufacturer's instructions.
2. From the **Settings** screen, tap **Add Z-Wave Device** to initialize Learn mode.

3. Follow the instructions on-screen to bind your device. Refer to the device instructions, if necessary.
4. When enrollment completes, enter a device name and tap **OK**. Your device is ready to use.

If using a Z-Wave smart switch to control power to a light or appliance, such as a fan, simply plug it into an AC power outlet.
Note: Only use the dimmer function on supported devices to prevent damage to the device.

10.6.1 Editing or Removing a Device

To edit or remove a device, complete the following steps:
1. From the **Settings** screen, tap **Edit Device**, then select the device you want to edit or remove.
2. Update the device name and tap **Done** to save your changes. Alternatively, tap **Remove Device** to remove it from your system.

10.7 Device Interoperability

Your dealer can provide you with a list of currently supported Z-Wave devices. However, all Z-Wave Plus devices, supported and unsupported, are partially or fully operable. At a minimum, listening nodes function as message repeaters.

10.8 Z-Wave Association Groups

The iotega panel supports association group 1 with up to 100 nodes. Association group 1 notifies associated nodes of the device status. The panel sends a Z-Wave Basic Report as a bitmap with the following property values:

Bit	Property
0	Low Battery
1	AC Failure
2	No Battery
3	Tamper

10.9 Responding to the Basic Command

If this device receives a Basic Get request, it responds with the Z-Wave Basic Report. Refer to the **Z-Wave Association Groups** section for more information.

This device ignores the Z-Wave Basic SET command.

10.10 Z-Wave Reset

To remove all the Z-Wave devices and restore the Z-Wave controller to factory defaults, complete the following steps:

1. In the Smartlink web portal, under **Home Control**, click **Device Control**.
2. Under **Setup**, click **Tools**, then click **Reset Z-wave**.

Note: Use this procedure only when the network primary controller is missing or otherwise inoperable.

11.0 Safety instructions

This equipment is direct plug-in. It must be installed and used within an environment that provides the pollution degree max 2, over voltages category II, in non-hazardous, indoor locations only.

⚠ This equipment has no mains on/off switch. If you must quickly disconnect the equipment, the plug of the direct plug-in power supply is intended to serve as the disconnecting device. It is imperative that access to the mains plug and associated mains socket/outlet, is never obstructed.

When using equipment connected to the mains, you must always follow basic safety instructions. To reduce the risk of fire, electric shock and/or injury, observe the following instructions:

- Use only authorized accessories with this equipment.
- Ensure that cables are positioned so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain.
- Do not spill any type of liquid on the equipment.

12.0 Locating detectors and escape plan

The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke and CO alarms.

12.1 Smoke detectors

Research has shown that all hostile fires in homes generate smoke to a greater or lesser extent. Experiments with typical fires in homes indicate that detectable quantities of smoke precede detectable levels of heat in most cases. For these reasons, smoke alarms should be installed outside of each sleeping area and on each storey of the home.
The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke alarms.
It is recommended that additional smoke alarms beyond those required for minimum protection be installed. Additional areas that should be protected include: the basement; bedrooms, especially where smokers sleep; dining rooms; furnace and utility rooms; and any hallways not protected by the required units. On smooth ceilings, detectors may be spaced 9.1 meters (30 feet) apart as a guide. Other spacing may be required depending on ceiling height, air movement, the presence of joists, uninsulated ceilings, etc. Consult National Fire Alarm Code NFPA 72, CAN/ULC-S553-02 or other appropriate national standards for installation recommendations.

- Do not locate smoke detectors at the top of peaked or gabled ceilings; the dead air space in these locations may prevent the unit from detecting smoke.
- Avoid areas with turbulent air flow, such as near doors, fans or windows. Rapid air movement around the detector may prevent smoke from entering the unit.
- Do not locate detectors in areas of high humidity.
- Do not locate detectors in areas where the temperature rises above 38 ºC (100 ºF) or falls below 5 ºC (41 ºF).
- Smoke detectors must always be installed in USA in accordance with Chapter 29 of NFPA 72, the National Fire Alarm Code: 29.5.1.1.

Where required by applicable laws, codes, or standards for a specific type of occupancy, approved single- and multiple-station smoke alarms shall be installed as follows:

1. In all sleeping rooms and guest rooms.
2. Outside of each separate dwelling unit sleeping area, within 6.4 meters (21 feet) of any door to a sleeping room, the distance measured along a path of travel.
3. On every level of a dwelling unit, including basements.
4. On every level of a residential board and care occupancy (small facility), including basements and excluding crawl spaces and unfinished attics.
5. In the living area(s) of a guest suite.
6. In the living area(s) of a residential board and care occupancy (small facility).

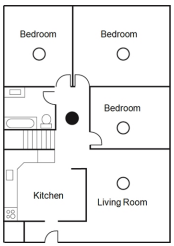


Figure 1

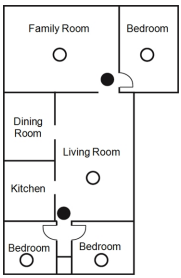


Figure 2

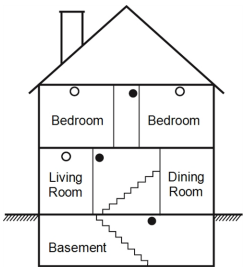


Figure 3

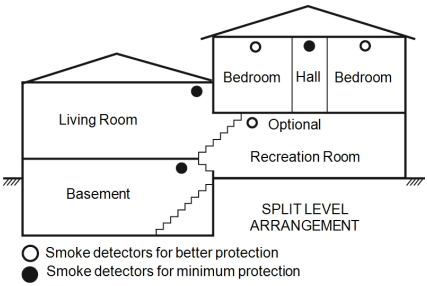


Figure 3a

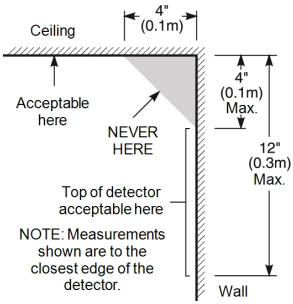


Figure 4

12.2 Fire escape planning

There is often very little time between the detection of a fire and the time it becomes deadly. It is thus very important that a family escape plan be developed and rehearsed.

1. Every family member should participate in developing the escape plan.
2. Study the possible escape routes from each location within the house. Since many fires occur at night, special attention should be given to the escape routes from sleeping quarters.
3. Escape from a bedroom must be possible without opening the interior door.

Consider the following when making your escape plans:

- Make sure that all border doors and windows are easily opened. Ensure that they are not painted shut, and that their locking mechanisms operate smoothly.
- If opening or using the exit is too difficult for children, the elderly or handicapped, plans for rescue should be developed. This includes making sure that those who are to perform the rescue can promptly hear the fire warning signal.
- If the exit is above the ground level, an approved fire ladder or rope should be provided as well as training in its use.
- Exits on the ground level should be kept clear. Be sure to remove snow from exterior patio doors in winter; outdoor furniture or equipment should not block exits.
- Each person should know the predetermined assembly point where everyone can be accounted for (e.g., across the street or at a neighbor's house). Once everyone is out of the building, call the fire department.
- A good plan emphasizes quick escape. Do not investigate or attempt to fight the fire, and do not gather belongings as this can waste valuable time. Once outside, do not re-enter the house. Wait for the fire department.
- Write the fire escape plan down and rehearse it frequently so that should an emergency arise, everyone will know what to do. Revise the plan as conditions change, such as the number of people in the home, or if there are changes to the building’s construction.
- Make sure your fire warning system is operational by conducting weekly tests. If you are unsure about system operation, contact your installer.

We recommend that you contact your local fire department and request further information on fire safety and escape planning. If available, have your local fire prevention officer conduct an in-house fire safety inspection.

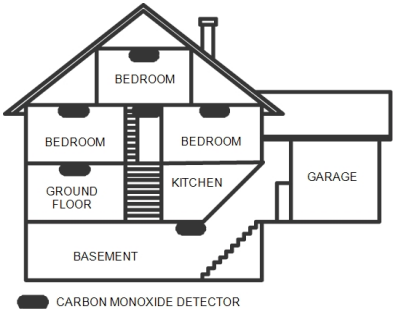


Figure 5

12.3 Carbon monoxide detectors

Carbon monoxide is colorless, odorless, tasteless, and very toxic, it also moves freely in the air. CO detectors can measure the concentration and sound a loud alarm before the CO reaches a potentially harmful level. The human body is most vulnerable to the effects of CO gas during sleeping hours; therefore, locate CO detectors in or as near as possible to sleeping areas of the home. For maximum protection, locate a CO alarm outside primary sleeping areas or on each level of your home. Figure 5 indicates the suggested locations in the home.

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10 ºC (14 ºF) or exceed 40 ºC (104 ºF)
- Near paint thinner fumes
- Within 1.5 meters (5 feet) of open flame appliances, such as furnaces, stoves, and fireplaces
- In exhaust streams from gas engines, vents, flues, or chimneys
- Do not place in close proximity to an automobile exhaust pipe; as this damages the detector.

REFER TO THE CO DETECTOR INSTALLATION AND OPERATING INSTRUCTION SHEET FOR SAFETY INSTRUCTIONS AND EMERGENCY INFORMATION.

12.0 Regulatory agency statements

FCC MODIFICATION STATEMENT

Digital Security Controls has not approved any changes or modifications to this device by the user. Any changes or modifications could void the user's authority to operate the equipment
.Digital Security Controls n'approuve aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

FCC AND ISED CANADA INTERFERENCE STATEMENT

This device complies with Part 15 of the FCC Rules and ISED Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'ISED Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, ême si le brouillage est susceptible d'en compromettre le fonctionnement.

FCC CLASS B DIGITAL DEVICE NOTICE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or experienced radio/television technician for help.

CAN ICES-3 (B) / NMB-3 (B)

The reference to the WS900-xx throughout this manual is applicable to the following model numbers: WS900-19 and WS900-29.
FCC ID:F5316WS90019
FCC ID:F5316WS900-29
IC: 160A-WS90019
IC: 160A-WS90029

The reference to the Cellular Communicator xx7090 throughout this manual is applicable to the following model numbers: 3G7090 and LT7090.
FCC ID:F53163G7090
FCC ID:F5316LT7090
IC: 160A-3G7090
IC: 160A-LT7090

FCC/ISED CANADA WIRELESS NOTICE

WARNING: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20cm or more must be maintained between the antenna of this device and persons during device operation.

Antenna gain must be below:

Frequency band	3G4000
GSM 850 / FDD V	2.1 dBi
PCS 1900 / FDD II	3.7 dBi
LTE B4 (1700 MHz)	1.5 dBi
LTE B13 (700 MHz)	2.2 dBi

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter, except as described in this user manual.

AVERTISSEMENT: Pour satisfaire aux recommandations d'exposition RF FCC des dispositifs de transmission mobile, un espace de séparation de 20 cm ou plus doit être maintenu entre l'antenne de l'appareil et les personnes pendant son fonctionnement.

Gain de l'antenne doit être ci-dessous:

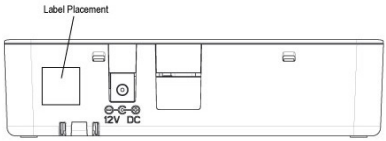
Frequency band	3G4000
GSM 850 / FDD V	2.1 dBi
PCS 1900 / FDD II	3.7 dBi
LTE B4 (1700 MHz)	1.5 dBi
LTE B13 (700 MHz)	2.2 dBi

Les antennes utilisées avec ce produit ne doivent pas être placées ni utilisées en association avec une autre antenne ou un autre émetteur, comme indiqué dans ce manuel

FCC/IC LABEL

A label is shipped together with the module and it is the responsibility of the integrator to apply it to the exterior of the enclosure, as displayed in the following figure.

Une étiquette est livré avec le module et il est de la responsabilité de l'intégrateur de l'appliquer à l'extérieur de l'enceinte, comme indiqué dans la figure suivante.



PRIVACY STATEMENT

The Tyco cloud collects the following Data from the iotega panel (public IP address, security events and statuses, security configuration, and system diagnostics) in order to [improve system performance, troubleshoot customer issues, and improve user experience]. You have the right to access, correct and request removal of your personal data by contacting info@tycosecurityproducts.com and the right to lodge a complaint with a supervisory authority. Tyco will not transfer this data to other parties, except for our cloud service provider in the US, with whom we have contractual Personal Data Processing Terms and EU Standard Contractual Clauses. Tyco uses industry-standard safeguards to protect your personal information. Find out more in our Privacy Statement at www.tyco.com/privacy. Your personal information will be retained as long as necessary to achieve the purpose for which it was collected and for any period thereafter as legally required or permitted by applicable law.

SIMPLIFIED DECLARATION OF CONFORMITY

Hereby, Tyco Safety Products Canada Ltd declares that the radio equipment type Wireless Alarm System with Integral Cellular Alarm Communicator is in compliance with Directive 2014/53/EU.
The following models are covered by this guide: WS900-14, WS900-24, 3G7090, LT7090 (used in North America only), WS901-14, WS901-24EU, WS901-18, WS901-28 and 3G7090-EU.

The full text of the EU declarations of conformity for the models mentioned below are available at the following internet addresses:
Model WS901-14: http://dsc.com/pdf/1707001
Model WS901-24EU: http://dsc.com/pdf/1707002
Model WS901-18: http://dsc.com/pdf/1707003
Model: WS901-28: http://dsc.com/pdf/1707004
Model: 3G7090-EU: http://dsc.com/pdf/1707009

Product specifications

Frequency	Maximum power
g1 433.04 MHz – 434.79 MHz	10 mW
h1.4 868.0 MHz – 868.6 MHz h1.5 868.7 MHz – 869.2 MHz	10 mW
2400 MHz-2483.5 MHz	100 mW
E-GSM/EDGE: 880 MHz – 915 MHz	Class 4 (2 W) @ 900 MHz, E-GSM Class E2 (0.5 W) @ 900 MHz, EDGE
DCS/EDGE: 1710 MHz – 1785 MHz	Class 1 (1 W) @ 1800 MHz, DCS Class E2 (0.4 W) @ 1800 MHz, EDGE
FDD Band VIII: 880 MHz – 915 MHz FDD Band I: 1920 MHz – 1980 MHz	Class 3 (0.25 W) @ 900/1800 MHz, FDD I/VIII

EUROPEAN SINGLE POINT OF CONTACT

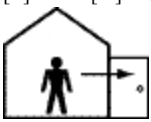
Tyco Safety Products, Voltaweg 20, 6101 XK Echt, Netherlands.

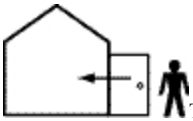
13.0 Reference sheets

Fill out the following information for future reference and store this guide in a safe place.

13.1 System information

Mark if buttons are enabled
[F] FIRE [A] AUXILIARY [P] PANIC


The exit delay time is _____ seconds.


The entry delay time is _____ seconds.

13.2 Service contact information

Monitoring station information
Account #: _____ Telephone #: _____
Installer information:
Company: _____ Telephone #: _____
Battery installation / service date:
_____
_____
_____

IMPORTANT: If you suspect a false alarm signal has been sent to the monitoring station, call the station to avoid an unnecessary response.

© 2017 Tyco Security Products. All Rights Reserved.
• www.dsc.com

The trademarks, logos, and service marks displayed on this document are registered in the United States and/or other countries. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products are the property of their respective owners, and are used with permission or allowed under applicable laws.
Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

DSC
From Tyco Security Products

29009891R001