DSC
From Tyco Security Products

iotega Wireless Security and Automation System

V1.0 Reference Manual

Models:
WS900UL/WS901

ALARM.COM

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

Table of Contents

Safety Instructions for Skilled Persons

Warning: When using equipment connected to the telephone network, always follow the basic safety instructions provided with this product. Save these instructions for future reference. Inform the end-user of the safety precautions that must be observed when operating this equipment.

Before Installing The Equipment

Ensure your package includes the following items:

- Installation and User manuals, including the SAFETY INSTRUCTIONS. READ and SAVE these instructions!
  Follow all WARNINGS AND INSTRUCTIONS specified within this document and/or on the equipment.
- iotega alarm controller
- Power Supply, direct plug-in
- Ethernet cable
- Mounting hardware

Selecting A Suitable Location For The Alarm Controller

Use the following list as a guide to find a suitable location to install this equipment:

- Locate near a power outlet.
- Select a location free from vibration and shock.
- Place alarm controller on a flat, stable surface and follow the installation instructions.

Do NOT locate this product where people may walk on the secondary circuit cable(s).

Do NOT connect alarm controller to electrical the same circuit as large appliances.

Do NOT select a location that exposes your alarm controller to direct sunlight, excessive heat, moisture, vapors, chemicals or dust.

Do NOT install this equipment near water. (e.g., bath tub, kitchen/laundry sink, wet basement, near a swimming pool).

Do NOT install this equipment and accessories in areas where risk of explosion exists.

Do NOT connect this equipment to electrical outlets controlled by wall switches or automatic timers.

AVOID interference sources.

AVOID installing equipment near heaters, air conditioners, ventilators, and refrigerators.

AVOID locating equipment close to or on top of large metal objects (e.g., wall studs).

See "Locating Detectors and Escape Plan" on page 40 for information on locating smoke and CO detectors.

SAFETY Precautions Required During Installation

- **NEVER** install this equipment during a lightning storm.
- Position cables so that accidents can not occur. Connected cables must NOT be subject to excessive mechanical strain.
- Use only the power supply provided with this equipment. Use of unauthorized power supplies may cause damage.

WARNING: THIS EQUIPMENT HAS NO MAINS ON/OFF SWITCH. THE PLUG OF THE DIRECT PLUG-IN POWER SUPPLY IS INTENDED TO SERVE AS THE DISCONNECTING DEVICE IF THE EQUIPMENT MUST BE QUICKLY DISCONNECTED. IT IS IMPERATIVE THAT ACCESS TO THE MAINS PLUG AND ASSOCIATED MAINS SOCKET/OUTLET IS NEVER OBSTRUCTED.

IMPORTANT NOTE FOR NORTH AMERICA!

This alarm system must be installed and used within an environment that provides the pollution degree max 2 and over-voltages category II NON-HAZARDOUS LOCATIONS, indoor only. The equipment is DIRECT PLUG-IN (external transformer) and is designed to be installed, serviced and/or repaired by skilled persons only; (skilled person is defined as a person with relevant education or experience to enable him or her to identify hazards and to take appropriate actions to reduce the risks of injury to themselves and others).

There are no parts replaceable by the end-user within this equipment. The wiring (cables) used for installation of the alarm system and accessories, shall be insulated with PVC, TFE, PTFE, FEP, Neoprene or Polyamide.

(a) Internal wiring must be routed in a manner that prevents:

- Excessive strain or loosening of wire on terminal connections;

- Damage of conductor insulation

(b) Disposal of used batteries must be made in accordance with local waste recovery and recycling regulations.

(c) Before servicing, DISCONNECT the power.

(d) DO NOT route any wiring over circuit boards.

(e) The installer is responsible to ensure that a readily accessible disconnect device is incorporated in the building for permanently connected installations.

The power supply must be Class II, FAIL SAFE with double or reinforced insulation between the PRIMARY and SECONDARY CIRCUIT/ENCLOSURE and be an approved type acceptable to the local authorities. All national wiring rules must be observed.

Section 1: Introduction

1.1 About the System

The iotega is an easy to use, wireless security and home automation panel. iotega supports a range of wireless devices via PowerG or Z-Wave.

Installers set up and configure the panel through a smartphone app or cloud-based portal. End users also interact with the iotega using an intuitive smartphone app, web portal or optional wirefree and touchscreen keypads.

1.2 Compatible Devices List

The following table lists all devices compatible with the iotega.

Note: Only models with^{UL} are UL/ULC listed. For UL/ULC certified installations use only UL/ULC listed devices.

Note: 'x' refers to detector frequency: 4 = 433MHz, 9 = 868MHz, 9 = 915MHz

Product Type	Model
Modules	
Touchscreen Keypad*	WS9TCHW
Wirefree LCD Keypad	WS9LCDWF
Cellular Communicator	3G7090E-EU
PowerG	
Wireless vanishing door/window contact	PGx975^{UL}
Wireless door/window contact w/ AUX	PGx945^{UL}
Wireless smoke detector	PGx926^{UL}
Wireless smoke and heat detector	PGx916^{UL}
Wireless CO detector	PGx913^{UL}
PIR/Pet Immune Motion Detector	PGx914
Wireless PIR motion detector	PGx904(P)^{UL}
Wireless PIR + camera motion detector	PGx934(P)^{UL}
Wireless Outdoor PG PIR + camera motion detector	PGx944
Wireless curtain motion detector	PGx924^{UL}
Wireless dual tech motion detector	PGx984(P)
Wireless mirror motion detector	PGx974(P)^{UL}
Wireless outdoor motion detector	PGx994^{UL}
Wireless glass break detector	PGx912, PGx922^{UL}
Wireless shock detector	PGx935^{UL}
Wireless flood detector	PGx985^{UL**}

Product Type	Model
Wireless temperature detector (indoor use)	PGx905^{UL**}
Wireless 4-button key	PGx939 ^{UL}PGx929^{UL}
Wireless panic key	PGx938
Wireless 2-button key	PGx949^{UL}
Wireless indoor siren	PGx901^{UL}
Wireless outdoor siren	PGx911^{UL}
Wireless repeater	PGx920^{UL}
IP Devices		
Touchpad	Wi-Fi Touchscreen (dedicated as a system keypad)	WS9TCHW
Phone	Cellular Phone w/Wi-Fi	iOS/Android based
Z-Wave Devices		
See the portal for a complete list of supported Z-Wave devices.		
Central Monitoring Station Receivers		
Receiver	Sur-Gard System I-IP Receiver	SG-System I-IP
Receiver	Sur-Gard System II Receiver	SG-System II
Receiver	Sur-Gard System III Receiver	SG-System III
Receiver	Sur-Gard System IV Receiver	SG-System IV
Receiver	Sur-Gard System 5 Receiver	SG-System 5

1.3 Specifications

Zone Configuration

- 128 wireless zones
- 18 zone types and 4 programmable zone attributes
- 4 touchscreen keypads supported
- 4 wirefree keypads
- 16 wireless sirens
- 32 wireless keys supported
- 8 wireless repeaters. Note that more than one wireless repeater shall be installed in a given fire alarm signaling system to provide a redundant RF transmission path.

Access Codes

- Up to 99 access codes, plus one master code and two duress codes
- Programmable user access levels and partition assignment for each user code

Warning Device Output

- Integral sounder capable of 85 dB @ 3m
- 2 remote, wireless indoor/outdoor warning devices supported: models PGx901 (indoor), PGx911 (outdoor)

- Programmable as steady, pulsed, temporal three (as per ISO8201) or temporal four (CO alarm)
- Warning device sounds alarms in the following priority: Fire, CO, Burglary

Memory

- 128MB RAM
- 4GB eMMC solid-state drive
- 128MB embedded FLASH memory

Power Supply

Transformer:

Primary: 120VAC, 0.35A, 60Hz Class II

Secondary: 12VDC, 1.16A

Standard Battery

- Model: DSC model 17000178, 7.4V,1.0Ah lithium-Ion, rechargeable
- Backup time: 4 hours
- Recharging time to 85%: 24 hours
- Low battery threshold: 7.3V
- Low battery restore: 7.4V
- Battery Critical Shutdown: 6.5V
- Battery lifespan: 3-5 years

Extended Battery

- Model: DSC model 17000179, 7.4V, 4.5Ah, lithium-Ion, rechargeable
- Backup time: 24 hours
- Recharging time to 85%: 24 hours
- Low battery threshold: 7.3V
- Low battery restore: 7.4V
- Battery Critical Shutdown: 6.5V
- Battery lifespan: 3-5 years

Operating Environmental Conditions

- Temperature range: 0°C to +49°C (32°F-120°F)
- Relative humidity: <93% non condensing

Alarm Transmitter Equipment (ATE) Specification

- Communications over cellular or Ethernet
- Supports SIA and Contact ID
- Complies with TS203 021-1, -2, -3 Telecom equipment requirements

System Supervision Features

The iotega continuously monitors a number of possible trouble conditions and provides audible and visual indication at the keypad if a trouble is present. Trouble conditions include:

- AC power failure
- Zone trouble
- Fire trouble
- Communicator trouble
- Low battery condition
- RF jam
- Failure to communicate
- Module fault (supervisory or tamper)

Additional Features

- 2-way audio Talk/Listen support*
- Quick arming

- User, partition, module, zone and system labels
- Z-WAVE-based home automation support*

* Not evaluated by UL.

Section 2: Installation

2.1 Alarm Controller Installation

Installing the iotega consists of connecting and powering up the hardware, as well as configuring the device using the installer portal.

A typical installation includes the following steps:

1. Create a customer account
2. Install the hardware
3. Power up the panel
4. Confirm communication
5. Enroll and install devices
6. Connect to Wifi router
7. Test the system

To install the iotega:

1. Locate the panel on a flat surface in close proximity to AC power and a wireless router.
2. Remove the plastic pull tab from the access cover on the back of the panel to activate the battery. If the battery is not installed, see Installing a new Battery.
3. Connect the Ethernet cable to the port on the back of the panel. Connect the other end of the cable to the wireless router. Installation and configuration can be done over cellular without the need for an Ethernet connection.
4. Connect the barrel jack of the plug-in adapter to the power connector on the back of the panel. Route the power cable through the strain relief channel on the bottom of the panel then plug the adapter into an AC outlet. The iotega powers up once connected to AC.

   The power-up sequence is as follows:

    - The integrated keypad numbers illuminate in sequence until power-up is complete.
    - The system powers up after approximately 2 minutes.
    - The Ethernet Link Speed LED illuminates steady green and the Ethernet Link Activity LED flashes rapidly to indicate that a connection is being made to the network.
    - After several minutes, depending on network speed, the Remote Connection LED illuminates steady green, indicating that a connection has been established.

    Note: If the Remote Connection Status LED flashes red, the panel may be having difficulty connecting to the remote servers. Restarting the panel may remedy the issue.

    For more information on LED indicators, see "Controls and Indicators" on page 6.

5. [Optional] Connect the iotega to the customer's WiFi network. To do this, enable WPS on the router, then enable WPS on the iotega either via the Alarm.com MobileTech app or the local keypad ([*][8][Installer Code]).

    If WPS is not available, connect to a valid 2.4 GHz WiFi network via the Alarm.com MobileTech app or from the panel's local webpage. The local webpage is accessed via [*][8][Installer Code], connecting to the iotega's access point and navigating to http://iotega. The password is the installer code twice (e.g., if Installer code is 5555, the password is 55555555)."

Figure 2-1 Panel Connections
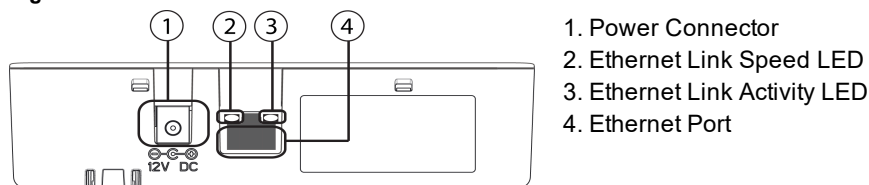
1. Power Connector
2. Ethernet Link Speed LED
3. Ethernet Link Activity LED
4. Ethernet Port

Figure 2-2 Panel Bottom
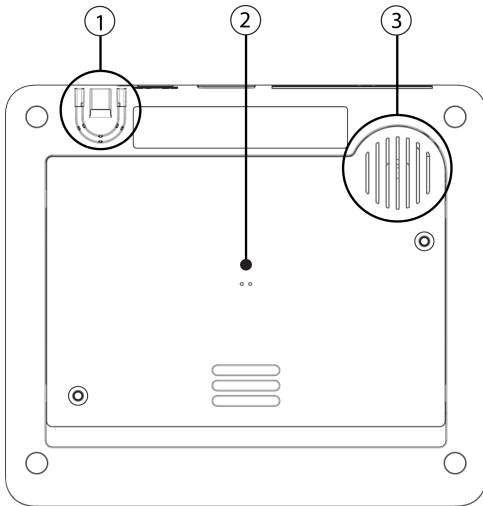
1. Power cable Strain Relief
2. Access Cover for Battery, SIM Card and Reset Button
3. Speaker

Figure 2-3 Battery Compartment
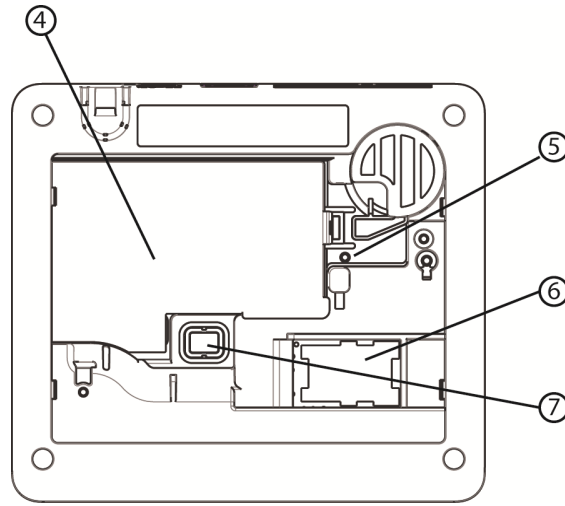
4. Battery
5. Reset button
6. SIM card
7. Tamper switch

Removing the Battery

1. Remove the access cover from the back of the panel.
2. Push the battery retention tab in the direction of the arrow in Figure 2-4 .
3. Lift the battery from the front, then pull up and slide out.

Figure 2-4 Battery Removal

Push tab to release
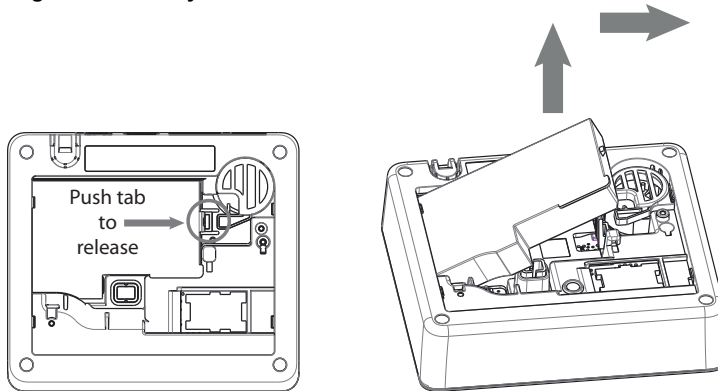
Installing a new battery

1. Remove the access cover from the back of the panel.
2. Insert the battery, back end first, as shown in Figure 2-4 .
3. Press the front of the battery down until the retention tab clicks into place.
4. Replace the back cover of the panel.

Note: When replacing the battery, use battery pack suitable for the application. Refer to on page 2.

2.2 Controls and Indicators

The iotega provides a series of LED indicators to notify users of system status.

Figure 2-5 LED Indicators
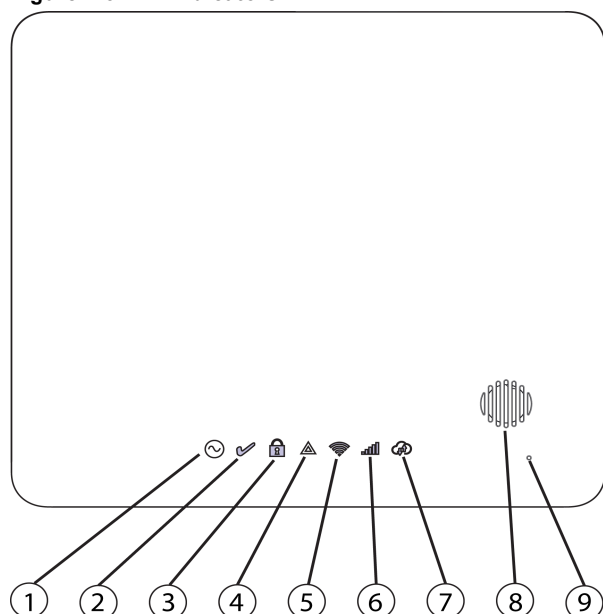
1. Power LED
2. Ready to Arm LED
3. Armed LED
4. Trouble LED
5. WiFi Signal Strength LED
6. Cellular Signal Strength LED
7. Remote Connection LED
8. Siren
9. Microphone

Table 2-1 LED Indicator Operation

LED	Indicator	Description
⊘ Power	ON Steady [Green]	AC power is connected to the system
	OFF	· System is not powered On · NO AC connected, and system is operating on backup battery · NO AC connected and backup battery is discharged
	Flashing	System test in progress (Ready, Trouble and Arm LED's flashing at same time)
✔ Ready	ON Steady [Green]	Partition is ready to arm
	OFF	Partition is not ready to arm. Not all zones are secure or an alarm is present.
	Flashing [Green]	Installer Walk Test (Ready, Trouble and Arm LED's flashing at same time) or system test in progress (Ready, Trouble and Arm LED's flashing at same time)

LED	Indicator	Description
🔒 Armed	ON Steady [Red]	Partition is armed
	Flashing [Red]	System in Alarm. [Note: this LED does not flash for silent alarms or panic alarms]
	Flashing [Red]	Installer Walk Test (Ready, Trouble and Arm LED's flashing at same time) or system test in progress (Ready, Trouble and Arm LED's flashing at same time)
	OFF	Partition is disarmed or audible alarm annunciation is deactivated
⚠ Trouble	ON Steady [Amber]	System trouble is present
	Single flash [Amber]	[*][2] System Trouble menu level 1
	Two flashes [Amber]	[*][2] System Trouble menu 2
	Three Flashes [Amber]	[*][2] System Trouble menu 3
	Flashing [Amber]	Access code is required to view Trouble menu, Installer Walk Test (Ready, Trouble and Arm LED's flashing at same time) or a system test is in progress (Ready, Trouble and Arm LED's flashing at same time)
	OFF	No system troubles
📶 Wi-Fi Signal Strength	ON Steady [Green]	Strong Signal Connection
	ON Flashing [Green]	Wi-Fi active in WSA mode (for AP mode)
	ON Steady [Amber]	Radio active with weak signal connection
	ON Flashing [Amber]	Z-Wave is active in learn pair mode
	On Steady [Red]	No Signal
	Flashing [Amber]	System Test (AC, Ready, Trouble, Arm LED's, WiFi Trouble, Cellular Trouble & System Remote Status flashing at same time)
	OFF	WiFi disabled
📶 Cellular Signal Strength	ON Steady [Green]	Strong signal connection
	ON Steady [Amber]	Weak signal connection
	ON Steady [Red]	No Signal or no connection
	Flashing [Amber]	System Test (AC, Ready, Trouble, Arm LED's, WiFi Trouble, Cellular Trouble & System remote status flashing at same time)
	OFF	Cellular is disabled

LED	Indicator	Description
Remote Con-nection Status	ON Steady [Green]	Link to remote server is active
	ON Flash [Red]	Link to remote server is active but has failed to communicate
	OFF	Link to remote server is not active or the panel has not been activated with Alarm.com
	Flashing [Amber]	System Test (AC, Ready, Trouble, Arm LED's, WiFi Trouble, Cellular Trouble & System Remote Status flashing at same time) **Note:** If the Remote Connection status LED flashes red, the panel may be having difficulty connecting to the remote server. Restarting the panel may remedy the issue. If the problem persists, contact technical support

Note: During a system test, All LEDs flash.

Reset Button

Pressing and holding the Reset button, located under the battery cover (see figure 3-3), for a minimum of 10 seconds defaults the interactive app to factory settings. The iotega beeps once to confirm successful reset.

Pressing and holding the Reset button for a minimum of 20 seconds resets the panels network configuration to factory defaults. The iotega beeps twice to confirm successful reset.

Note: The system must be disarmed with no alarms in memory in order for the Reset button to function as described above.

Tamper Switch

The panel includes a tamper switch under the back battery cover. If the battery cover is removed while the system is dis-armed, the tamper condition must be cleared before arming is permitted. If the battery cover is removed while the system is armed, the bell sounds, a system tamper is logged and communicated to the central monitoring station, and a system tem-per trouble is displayed in the Trouble menu.

Low Power Operation

In the event of an AC power outage, all Wi-Fi and home automation functions are discontinued. The panel uses battery power to communicate alarms or critical conditions.

2.3 Enrolling Wireless PowerG Security Devices

Device enrollment and configuration is done using the installer portal.

To enroll wireless devices, navigate to *Equipment > Sensors > Add a Sensor* to put the panel into Add mode. Select Auto-Learn or Remote Add.

Auto-Learn mode

1. Power up the sensor or device and trigger it according to the instructions in the device manual. Enrolled devices are displayed on the Mobile Tech page in the Added Devices section.
2. Once all devices are added, choose Exit.
3. Edit the device name, group, and partition as needed.
4. Click Save to finish.

Add Sensor and Peripheral Devices (Remote Add)

1. Enter the device ID, zone definition, partition, name, and ESN into the appropriate fields.
2. Click Add Sensor to finish.

The device may need to be tampered when in range of the panel in order to start functioning.

The wireless devices in the table below each have a dedicated Enroll button, located on the circuit board inside the plastic casing. A Phillips screw must be removed on most devices to gain access. Refer to the installation instructions provided with the device for more information.

PGx901	Indoor siren		PGx924	Curtain motion detector
PGx904	PIR/Pet Immune motion detector		PGx926	Smoke detector
PGx914	PIR/Pet Immune motion detector		PGx935	Shock detector and magnetic contact
PGx905	Temperature detector		PGx944	Tower Cam motion detector
PGx911	Outdoor siren		PGx945	Magnetic contact with Aux.
PGx913	Carbon Monoxide detector Note: enrolls automatically on power-up		PGx974	Mirror PIR with anti-masking
PGx912	Glassbreak detector		PGx975	Magnetic contact (vanishing)
PGx916	Smoke and heat detector		PGx984	Mirror PIR motion detector
PGx920	Wireless repeater Note: hold Enroll button until red and green LEDs light steady		PGx985	Flood detector
PGx922	Glassbreak detector		PGx994	Outdoor PIR motion detector

To enroll wireless keys:

PGx929/PGx939 4-button wireless key	Press and hold [*] button until LED lights steady then release.
PGx949 2-button wireless key	Press and hold unlock button until LED lights steady then release.
PGx938 Panic key	Press and hold button until LED lights steady then release.

Section 3: Operation

This section describes how to use the iotega's integrated keypad.

3.1 Using the Integrated Keypad

The iotega includes a built-in, touch sensitive keypad that activates by proximity. From the keypad, users can arm and disarm the system, view system troubles, and activate the Fire (F), Auxiliary (A) and Panic (P) keys.

The integrated keypad can be configured to work on any partition.

Figure 3-1 Keypad - Normal Operating Mode   **Figure 3-2 Keypad - Shift Mode**
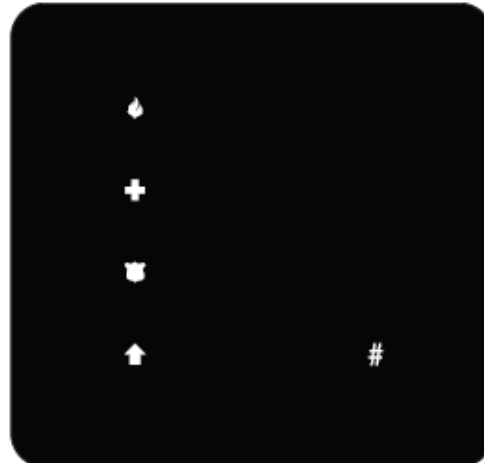
3.1.1 Key Functions

The following keys are enabled during normal operating mode:

Key	Description
(0-9)	numeric entry (access code)
#	clear entries, return to previous screen
*	[*] 2 for Troubles, see "Viewing Troubles from the Integrated Keypad" on page 35. [*] 8 to enable WiFi access point (to add IP devices, i.e.,touchscreen keypad). See "WPS Mode ([*]8)" for more information. [*] 7 to initiate a phone test with ADC.
↑	Shift mode switches between numeric and Emergency keys

3.1.2 Emergency Keys

The Fire, Auxiliary and Panic keys can be enabled independently by the installer. All three are enabled by default. The Emergency keys behave as follows:

Key	Alarm Type	Indication	Reporting Code
🔥	Fire	Keypad beeps 3 times. Siren sounds. Signal sent to monitoring station	Fire Alarm (if programmed)
✚	Auxiliary	Keypad beeps 3 times when activated and 10 times when the event is successfully received by the central monitoring station.	Auxiliary alarm

	Panic	Keypad beeps three times and a signal is sent to the monitoring station. Can be configured as audible or silent	Panic alarm

To use the Emergency keys:
1. Press the Shift key (↑). The Emergency keys are illuminated (if enabled). If an Emergency key is not pressed within 10 seconds, the keypad returns to normal operating mode.
2. Press and hold an Emergency key for 2 seconds to activate the alarm.

3.1.3 Phone Test ([*][7])

The Phone test sends a test transmission from the iotega to the monitoring station. This test helps installers determine if the panel is communicating properly. Successful completion of the test is indicated on the installer portal. If the test fails, an FTC error is logged. The Phone test can be initiated by installers and the system master user, and may take several minutes to complete.

To perform a Phone test:
- Press [*][7][01][installer code], or [*][7][02][master code]

3.1.4 WPS Mode ([*][8])

WPS (WiFi Protected Setup) mode activates iotega's WiFi access point to facilitate connection with IP devices, such as the touchscreen keypad and IP cameras.

To enable WPS mode:
1. At the installation site, tap [*] 8 on the integrated kaypad.
2. Enter a valid installer code. The WiFi signal strength LED flashes for two minutes to indicate the system is in WPS mode.

    The WPS window expires after 2 minutes.

3.1.5 Local Webpage ([*][8])

This mode is used to connect the iotega to the local WiFi router, configure static/dynamic ip address, configure WiFi settings and to view panel, cellular status/information and firmware versions.

Note: WLAN Client Mode and Access Point must be enabled to use this feature.

The access window expires after 10 minutes.

To enable Local Webpage mode:
1. At the installation site, tap [*] 8 on the integrated kaypad.
2. Enter a valid installer code. The WiFi signal strength LED flashes for two minutes to indicate the system is in local webpage mode.

To access the local webpage:
1. On your local device (mobile/laptop), locate the Guest AP network and join.
2. Enter your password (installer code twice. e.g., 55555555).
3. Use a web browser to access http://iotega.

    Note: The access window timer can be restarted by pressing [*][8][installer code] again.

3.2 Arming and Disarming Methods

This section describes the arming methods available on the iotega.

3.2.1 Away Arming

Away Arming arms the entire system, including the perimeter and interior devices. The Ready light must be on to arm the system. If the Ready light is off, ensure all protected doors and windows are secure or bypassed.

To arm the system, enter a valid access code. To disarm, enter a valid access code.

During exit delay, the Armed and Ready indicators turn on and the keypad beeps once every second during the exit delay (and three times a second during the last 10 seconds) to alert the user to leave via a delay zone. The Ready light turns off when the Exit Delay ends.

When the exit delay has expired, the system is armed as indicated by the following conditions:

- the Ready indicator turns off.
- the Armed indicator stays on.
- the panel is silent.

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

3.2.2 Stay Arming

Note: Requires at least one zone defined as Interior Stay/Away or Delay Stay/Away for this function to work.

Stay Arming is intended to arm the perimeter of the premises while permitting movement within. The Ready light must be on to arm the system. If the Ready light is off, ensure all protected doors and windows are secure or bypassed. To Stay arm the system, enter a valid user code and stay within the premises (do NOT violate a zone programmed as Delay). The Armed light turns on once a function key is pressed or an access code is entered. The Ready indicator turns off and the Armed indicator turns on when the exit delay ends.

Note: In Stay Arming mode, all bypassed stay/away zones are logged and communicated to the central monitoring station.

3.2.3 Quick Arming

Quick arming enables users to arm the system via touchscreen or wirefree keypad without entering an access code. This provides a fast method of arming for regular users and allows users without an access code to arm the system. The Quick Arming feature must be enabled in order for this function to operate. See "Quick Arm" on page 18.

3.2.4 Disarming

The user must enter through a door programmed as Delay. Upon entering, the panel emits a steady entry delay tone (and a pulsing tone during the last 10 seconds of entry delay) to alert the user to disarm the system. To disarm the system, enter a valid user code or use a wireless key. If an alarm occurred while the panel was armed, the keypad numbers corresponding to the violated zones are illuminated. If the system is disarmed using a method other than the keypad (e.g., wireless key), the panel emits three squawks to indicate alarm in memory.

Section 4: Programming Options

This section provides descriptions of all alarm controller options, both programmable and read-only. Programming options are accessed through the Installer portal.

4.1 Integrated Keypad Options

This section describes programmable options for the iotega's integrated keypad.

Keypad Partition Assignment

This section is used to select the partition that the built-in keypad will operate on.

Default:	1
Valid range:	1-2

Fire Button Options

This function is used to enable or disable the Fire [F] button on the integrated keypad. When enabled, pressing and holding the [F] button for 2 seconds triggers a Fire alarm. The system sounds 3 beeps to acknowledge the valid alarm and the siren sounds with a pulsing tone. An alarm reporting code is transmitted to the central monitoring station.

Default:	Enabled
Valid range:	Enabled, Disabled

Auxiliary Button Options

This function is used to enable or disable the Auxiliary [A] button on the integrated keypad. When enabled, pressing and holding the [A] button for 2 seconds sends an emergency alarm reporting code to the central monitoring station. When the emergency reporting code is received, the keypad beeps 10 times.

Default:	Enabled
Valid range:	Enabled, Disabled

Panic Button

This function is used to enable or disable the Panic [P] button on the integrated keypad. When enabled, pressing and holding the [P] button for 2 seconds sends an emergency alarm reporting code to the central monitoring station.

Default:	Enabled
Valid range:	Enabled, Disabled

Internal Buzzer Control

This option is used to set the tone of the internal buzzer. The tnoe ranges from lowest (1) to highest (15). Programming (0) turns off the buzzer.

Default:	7
Valid range:	0-15

4.2 System Configuration Options

This section describes programmable options for the alarm controller.

System Area Label

Use this option to program a custom label for the security system. This label is used in the event buffer when system events occur.

Default:	System Area
Valid range:	32 Characters

System Account Number

The system account number is used to identify the alarm system when communicating system events to the central monitoring station. The system account number can be either 4 or 6 digits long. Program a 6-digit code only when using the SIA reporting format. SIA uses this account number for all partitions and system events. All other reporting formats use a 4-digit system account number to report system maintenance (e.g., low battery, zone fault) and test transmission events. To program a 4-digit system account number, enter 4 digits followed by FF.

Note: This field is mandatory for communication with the central monitoring station.

Default:	FFFFFF (disabled)
Valid range:	000001 to FFFFFF (Hexadecimal)

Event Reporting Format

The panel has an assigned communicator protocol for transmitting zone alarms, tampers, faults and other signals to the central monitoring station.

View the assigned protocol on the portal by navigating to Monitoring Settings and clicking View Additional Receiver Information.

SIA Format - Level 2 (Hard Coded)

The SIA communication format used in this product follows the level 2 specifications of the SIA Digital Communication Standard - October 1997. This format sends the account code along with its data transmission. The transmission appears similar to the following at the receiver:

N ri1 BA 01

N = New Event

ri1 = Partition /Area Identifier

BA = Burglary Alarm

01 = Zone 1

A system event uses the Area Identifier ri00.

Bell Squawk on Arming

With this option enabled, the iotega chirps the sirens briefly at full volume when the system is successfully armed. The following options are provided to customize this option:
None: Sirens do not chirp when the system is armed.
All RF: Sirens chirp when armed by any wireless device.
RF Wireless Key: Sirens chirp only when armed by a wireless key.
RF Keypad: Sirens chirp only when armed by a wirefree keypad.

Default:	RF Wireless Key
Valid range:	None, All RF, RF Wireless Key, RF Keypad

Chime on Zone Opening

When this option is enabled, the door chime sounds each time an appropriately configured zone is opened.
The Door Chime attribute must be set to ON for every zone that requires a chime on opening.

Default:	Enabled
Valid range:	Enabled, Disabled

Chime on Zone Closing

When this option is enabled, the door chime sounds each time an appropriately configured zone is closed.
The Door Chime attribute must be set to ON for every zone that requires a chime on opening.

Default:	Disabled
Valid range:	Enabled, Disabled

Trouble Beeps (Audible/ Auto-silent)

When this option is enabled, trouble beeps are not sounded for any trouble condition except Fire/CO. For these, trouble beeps sound every 10 seconds for the duration of the trouble.
When this option is disabled, the system announces troubles through the keypad buzzer every 10 seconds. Pressing any key on the keypad silences the trouble beeps; however, new troubles will restart trouble beeps. For troubles that have been silenced but are still present, trouble beeps restart daily at 7AM.

Default:	Enabled
Valid range:	Enabled, Disabled

Burglary Bell Time-out

This option determines the length of time the system siren sounds for. System tampers follow this timer, but Fire alarms and keypad buzzers do not.

Default:	4 Minutes
Valid range:	0 to 255 Minutes

Fire Bell Time-Out

This option determines the maximum activation time for fire alarm sirens. Each partition has a dedicated Fire Bell Time-out timer.

Fire Bell Time-out takes priority over Burglary Bell Time-out.

Default:	5 Minutes
Valid range:	0 to 255 Minutes

Audible Panic

This option is used to set internal buzzer behavior when the Panic key is pressed. When set to Audible, pressing the Panic key causes the buzzer to sound a series of 3 beeps to acknowledge the alarm. The buzzer then sounds a steady tone for the length of the bell time-out or until an access code is entered.
When set to Silent, pressing the Panic key causes the buzzer and the bell output to remain silent, but the alarm is still transmitted (if programmed).

Default:	Silent
Valid range:	Audible, Silent

Access Code Required For Bypassing

When this option is enabled, an access code is required to view the zone bypass menu.
When this option is disabled, the zone bypass menu is accessible to anyone.

Default:	Disabled
Valid range:	Enabled/Disabled

RF Jam

When this option is enabled, the alarm panel detects and reports continuous wireless signals that could interfere with the operation of the alarm system.
UL: The iotega detects and reports continuous RF interference using UL 20/20 requirements for wireless jam detection (20 seconds of continuous jam detection is required).

Default:	Disabled (Note: RF Jam shall be enabled for UL/ULC applications)
Valid range:	00: Disabled, 01: UL 20/20, 02: EN 30/60, 03: Class 6 30/60

Access Code Required to View/Silence Troubles

This option is used to enable and disable the need to enter an access code before viewing and silencing system troubles.

Default:	Disabled
Valid range:	Enabled, Disabled

Cellular Low Signal Trouble

This option is used to determine if the system will generate a trouble event when a weak cellular signal is detected.
When enabled, a trouble event is generated if the radio signal level falls below threshold level (average CSQ level 4 or less).

Default:	Enabled
Valid range:	Enabled, Disabled

Lockout Attempts

This option is used to program the number of invalid access code entries allowed before the keypad is locked. When keypad lockout occurs, the system is inaccessible by keypad for the programmed duration. If the number of invalid attempts is not reached within one hour, or if a valid access code is entered, the counter is reset to 0 after 5 minutes. Each keypad keeps track of its own lockout count and time.

Note: The FAP keys are not locked.

Default:	0
Valid range:	0 to 255

Keypad Lockout Duration

This section displays the length of time that the integrated keypad remains locked after the programmed number of access code attempts has been exceeded.

Default:	5 minutes
Valid range:	Read-only

Fire Supervision

This option is used to control system supervision of smoke, CO and heat detectors. When this option is enabled, fire detection devices are monitored over a four-hour period. If a device fails to report within the four-hour window, a hardware fault trouble is logged for the zone.

With this option disabled, fire detection devices follow the programmed supervisory window up to a maximum time of 18 hours. After 18 hours, fire detection devices go into fault, regardless of the programmed supervisory window.

Default:	Disabled
Valid range:	Enabled/Disabled

Wireless Supervisory Window

Use this option to program the time window for reception of supervision (keep alive) signals from wireless devices enrolled on the system. If a device does not report at least once within the programmed time window, a hardware fault trouble is generated.

Default:	24 Hours
Valid range:	1 Hour, 2 Hours, 4 Hours, 8 Hours, 12 Hours, 24 Hours, Disabled

Wi-Fi Low Signal Trouble

This option is used to determine if the system will log and report low Wi-Fi signals.

Default:	Enabled
Valid range:	Enabled, Disabled

Communication Cancel Window

This option is used to program the length of the Communication Cancel window.

Entering an access code during the communicaiton cancel window sends a code to the central monitoring station, informing them that the previous event should be disregarded.

The communications cancel window begins after the transmission delay expires and a zone alarm is transmitted. If an access code is entered during this window, a reporting code is communicated and logged. If the window expires without an access code entry or a code is entered after the window, the communications canceled event is not logged or communicated.

Note: The cancel window does not start after an Emergency key alarm.

Default:	0 Minutes (Standard)
Valid range:	0 to 255 Minutes (Standard)

Swinger Shutdown

This value defines the number of communication attempts made before the event goes into swinger shutdown. Once the programmed number of alarm/restore events have been communicated for an event, no further alarm/restore events are sent until swinger shutdown is reset. The last restore event is not communicated until swinger shutdown is cleared.

Default:	003 (Standard)
Valid range:	000-014 (Standard)

Communication Delay

This value defines the delay before an alarm is transmitted. The delay is for zones which have the Transmission Delay attribute enabled. Each partition shares the same active timer. If the delay is already active due to an alarm on a different partition, any new activity on another partition does not restart the communications delay timer. Burglary Verified events are postponed until after the transmission delay expires. When a valid disarming procedure is used while the transmission delay is active, a communications canceled message is briefly displayed on the keypad when the delay is canceled.

Default:	000 (Standard)
Valid range:	000-255 Seconds (Standard)

AC Failure Communication Delay

This value determines the delay before an AC failure or restore is logged and reported. The AC failure or restore is still displayed immediately in the Trouble menu.

Default:	030 Minutes
Valid range:	000 to 255 Minutes

Wireless Low Battery Communication Delay

When a zone reports a low battery condition, the trouble is indicated immediately in the Trouble menu, but transmission to the monitoring station and logging to the event buffer is delayed by the number of days programmed in this section. If the low battery condition is not corrected before the delay

expires, the condition is transmitted and logged to the event buffer. The Low Battery Restore transmission is not delayed.

Default:	007 days
Valid range:	000 to 255 days

[A] Key Alarm control (for 2-way Voice) - Read Only

When this option is enabled, a 2-way talk/listen-in session is initiated when the Auxiliary [A] key is tapped.

Default:	Enabled
Valid range:	Enabled

[P] Key Alarm Control (for 2-way Voice) - Read Only

When this option is enabled, a 2-way talk/listen-in session is initiated when the Panic [P] key is tapped. Note that the [P] key must be programmed as audible in order to initiate 2-way audio. If the [P] key is programmed as silent, a listen-in only session is initiated when the Panic [P] key is tapped.

Default:	Enabled
Valid range:	Enable

Duress Alarm Control (for 2-way Voice) - Read Only

When this option is enabled, a Listen-in session is initiated when a Duress alarm occurs.

Default:	Enabled
Valid range:	Enabled

Wireless Siren Control During 2-way Voice

When this option is enabled and an audible alarm is present, the wireless siren activates during a 2-way audio session.

When disabled, the wireless siren is silent when a 2-way audio session begins. This allows the user to better hear the operator. The sounder resumes operation for the timeout duration if the panel has not been disarmed at the end of the 2-way session.

Default:	Enabled
Valid range:	Enabled, Disabled

Onboard Siren Control During 2-way Voice

When this option is enabled and an audible alarm is present, the panel's onboard siren activates during a 2-way audio session.

When disabled, the onboard siren is silent when a 2-way audio session begins. This allows the user to better hear the operator. The sounder resumes operation for the timeout duration if the panel has not been disarmed at the end of the 2-way session.

Note: This option shall be enabled for UL/ULC.

Default:	Disabled
Valid range:	Enabled, Disabled

4.3 ADC Events to Forward

This section is used to configure monitoring station and receiver settings for the panel. ADC Events to Forward is accessed via the Alarm.com Partner Portal or Mobile Tech app under Monitoring Settings.

The following events are selectable:

- Alarms
- Bypass
- Crash & Smash
- Panics
- Phone Tests
- All Events
- Sensor Tampers
- Trouble Restorals
- Armings (Openings/Closings)
- Cancels
- Panel Not Responding
- Phone Communication Failures
- Troubles
- RF Receiver Jamming
- Sensor Tests

4.3.1 Network Configuration Options

LAN/WAN Obtain IP Address

This option is used to determine how an IP address for LAN/WAN communication is obtained. When DHCP is selected, the iotega is automatically assigned an IP address by the network. When
Static IP is selected, a consistent IP address is used.

Default:	DHCP (Automatic)
Valid range:	DHCP, Static IP

LAN/WAN IP Address

This section is used to program a static IP address. To use a static IP address, the option LAN/WLAN Obtain IP Address must be set to Static IP address.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

LAN/WLAN IP Subnet Mask

This section is used to program a LAN/WLAN subnet mask. To use the subnet mask, the option LAN/WLAN Obtain IP Address must be set to Static IP address.

Default:	255.255.255.255
Valid range:	000.000.000.000 to 255.255.255.255

LAN/WLAN Gateway IP Address

This section is used to program the IP address for the network's default gateway. To use this gateway, the option LAN/WLAN Obtain IP Address must be set to Static IP address.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

Panel's Preferred DNS Server

This section is used to program the name of the preferred Domain Name System server.

Note: To use the panel's preferred DNS server, the option LAN/WLAN Obtain IP Address must be set to Static IP address.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

Panel's Alternate DNS Server

This section is used to program the name of an alternate Domain Name System server to be used if the preferred DNS server is unavailable.

Note: To use the panel's alternate DNS server, the option LAN/WLAN Obtain IP Address must be set to Static IP address.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

WLAN SSID

This section is used to program a network name (unique identifier) for the panel.

Default:	None
Valid range:	Alphanumeric

WLAN Client Control

This option is used to control WiFi client mode.

Default:	Enabled
Valid range:	Enabled/Disabled

WLAN Security Type

This option is used to select which encryption protocol the system uses to secure the wireless network.

Default:	WPA2 PSK AES
Valid range:	WPA PSK TKIP WPA PSK AES WPA PSK TKIP AES WPA2 PSK TKIP WPA2 PSK AES WPA2 PSK TKIP AES

WLAN Security Key

This section is used to program a password for the Wi-Fi network.

Default:	None
Valid range:	32 character ACCII

Time Zone

This option defines the time zone that the alarm system will operate in.

Default:	US Eastern
Valid range:	US-Alaska, US-Aleutian, US-Arizona, US-Central, US-Eastern, US-Hawaii, US-Indiana-East, US-Indiana-Starke, US-Michigan, US-Mountain, US-Pacific, US-Samoa, CA-Atlantic, CA-Central, CA-Eastern, CA-Mountain, CA-Newfoundland, CA-Pacific, CA-Saskatchewan, CA-Saskatchewan-East, CA-Yukon

Time zone is set automatically by ADC based on the installation address provided in the customer setup.

4.4 Central Monitoring Station Programming Options

The following section provides descriptions of all programming options for communications between the iotega and the central monitoring station.

Communication Path

Use this option to select the method by which the panel communicates to the central monitoring station. Choose one of the following:

Cellular: The system communicates to the central monitoring station via cellular connection only.

Ethernet and Cellular: The system communicates to the central monitoring station via Ethernet as the primary path and cellular as the secondary path.

Default:	None
Valid range:	Cellular, Ethernet and Cellular

4.4.1 Other Communicator Related Options

Cellular Test Transmission Time

Enter a 4-digit number (0000-2359) using the 24-hour clock format (HHMM) to set the time of day a cellular test transmission is sent. Programming a value of 9999 disables the test transmission time.

Note: The internal date and time will automatically be programmed when the unit communicates with the primary receiver.

Default:	9999
Valid range:	0000 to 2359, 9999 to disable

Cellular Test Transmission Cycle

This option is used to program how often, in minutes, cellular test transmissions are sent. Once the initial test transmission is sent, all future test transmissions are offset by the programmed number of minutes.

Default:	0 minutes.
Valid range:	000000 to 999999 minutes

Note: Programming an interval of less than 5 minutes or a value greater than 999999 disables the test transmission.

4.5 Partition Configuration Options

This section describes programming options used to configure individual partitions.

Partition Label

This option is used to add a unique label to each partition on the system. This label is displayed on partition keypads and event messages.

Default:	Blank
Valid range:	32 character ASCII

Partition Account Number

This option is used to add a unique account number to a partition. When using formats other than SIA, the account number identifies the alarm system to the central monitoring station when communicating partition-specific events.

Note: The iotega will not communicate if the account number is not programmed.

Default:	FFFF
Valid range:	0001 to FFFF (FFFF to disable communication)

Entry Delay 1

This value determines the entry delay time for Delay 1 type zones.

Default:	30 seconds. Max. 45 seconds required for UL/ULC
Valid range:	0 to 255 (standard) 30 to 255 Seconds (UL/ULC)

Entry Delay 2

This value determines the entry delay time for Delay 2 type zones.

Default:	45 seconds (standard) Max. 45 seconds required for UL/ULC
Valid range:	0 to 255 (standard) 30 to 255 Seconds (UL/ULC)

Exit Delay

This value determines the length of time given to exit the premises before the system becomes fully armed.

Default:	120 seconds (standard). Note: Minimum 45 seconds required for UL/ULC
Valid range:	0 to 255 (standard) 45 to 255 seconds (UL/ULC)

Closing Delinquency Delay

This value determines the time the alarm system delays before transmitting a close delinquency event to the central monitoring station.

Default:	30 Days
Valid range:	0 to 255 Days

Cross Zone Delay

If another zone with the Burglary Verification attribute enabled is violated within the duration of this timer, a Burglary Verified event is communicated and logged.

Default:	0 Seconds
Valid range:	0 to 255 Seconds

Quick Arm

When this option is enabled, the iotega can be armed without entering an access code.

Note: Quick arming cannot be initiated from the integrated keypad.

Default:	Enabled
Valid range:	Enabled/Disabled

Quick Exit

When this option is enabled, users can temporarily bypass a Delay 1 or Delay 2 zone to exit the premises when the system is armed. Only one delay zone may be activated. Activity on another delay zone initiates the appropriate alarm sequence. If the delay zone is still open two minutes after being bypassed, entry delay is initiated. If armed in Stay mode, the automatic bypass on Stay/Away zones remains.

Note: Quick Exit cannot be initiated from the integrated keypad.

Default:	Disabled
Valid range:	Enabled/Disabled

Internal Siren

When this option is enabled, The iotega's built-in siren activates during an alarm.

Default:	Enabled
Valid range:	Enabled/Disabled

Internal Buzzer

When this option is enabled, the iotega's built-in buzzer provides auditory feedback (e.g., key presses, door chime).

Default:	Enabled
Valid range:	Enabled/Disabled

Chime Control

When this option is enabled, the iotega sounds door chime beeps whenever a zone with the Door Chime attribute ON is opened.

Default:	Disabled
Valid range:	Enabled/Disabled

Duress Access Code (Pin)

This section is used to program an access code designated as Duress. When this code is used to perform any function on the partition, a Duress reporting code is sent to the central monitoring station.

Default:	Blank
Valid range:	4-digit, 0-9

4.6 Primary Temperature Zone

Primary Temperature Zone

Use this option to select the primary temperature zone to display on partition tablets and keypads. This option can be programmed by level 1 users via remote app or local tablet.

Default:	000 (no temperature zone selected)
Valid range:	000-128

Secondary Temperature Zone

Use this option to select the secondary temperature zone to display on partition tablets and keypads. This option can be programmed by level 1 users via remote app or local tablet.

Default:	000 (no temperature zone selected)
Valid range:	000-128

4.7 Wireless Device Configuration Options

This section describes programming options used to configure supported wireless PowerG devices.

4.7.1 Wirefree Keypad Configuration Options

The following sections describe programming options used to configure the available wirefree keypad.

Keypad Label

This section is used to program a user-friendly name for the keypad.

Default:	Blank
Valid range:	32 character ASCII

Keypad Partition Assignment

This section is used to program the partition that the wirefree keypad is assigned to.

Default:	1
0 to 255	1-4, ALL

Panic Button Options

This feature is used to enable and disable the Fire, Medical, and Panic keys on the wirefree keypad. Programming is done through the installer portal under *Command Catalog>Keypad/Screen Settings>Panic Button Options*.

Default:	Fire, Medical and Police panic
Valid range:	Fire panic only, Medical panic only, Police panic only, Fire and Medical panic, Fire and Police panic, Fire, Medical and Police panic, None

Internal Buzzer Control

This option is used to set the volume level of the keypad's internal buzzer. The volume ranges from lowest (1) to highest (15). Programming (0) turns off the buzzer.

Default:	7
Valid range:	0-15

Keypad Tamper

When this option is enabled, the wirefree keypad tamper switch generates tamper alarms and restores when activated.

Default:	Disabled
Valid range:	Enabled/Disabled

Armed LED Power Save Option

This option is used to control the Armed LED on/off state. If enabled, the Armed LED does not illuminate when the system is armed to conserve battery life.

Default:	Disabled
Valid range:	Read-only

Auto Scroll Open Zones Option

When this option is enabled, the keypad automatically scrolls through and displays all open zones.

Default:	Enabled
Valid range:	Read-only

Alarms Displayed While Armed Option

When this option is enabled, the keypad displays alarms on affected zones while the system is armed.

If disabled, zones in alarm are not displayed while the system is armed.

Default:	Enabled
Valid range:	Read-only

Power LED AC Present Option

When this option is enabled, the Power LED illuminates when the iotega has electrical power.

When disabled, The Power LED illuminates when the iotega does not have electrical power.

Default:	Enabled
Valid range:	Read-only

Auto Alarm Scroll Option

When this option is enabled, the keypad scrolls automatically and displays all alarms when the bell is active or when an alarm is in memory while armed.

Default:	Enabled
Valid range:	Read-only

Local Clock Display Option

When this option is enabled, the keypad displays the time and date when not in use.

Default:	Enabled
Valid range:	Read-only

4.7.2 User Configuration Options

This section describes programming options for configuring system users.

User Partition Assignment

This section is used to assign system user 2-100 to an available partition. Users may be assigned to multiple partitions. Basic/Standard users may only assign new users to partitions they themselves have permission to access.

Default:	1
Valid range:	1, 2, 3, 4, All

User Access Code (Pin)

This section is used to program a 4-digit code used to access the panel. Each user requires a code. Duplicate codes are not permitted.

Default:	Blank
Valid range:	0000 to 9999

User Access Level

Each system user is assigned an access level that determines the features they can use. All codes are 4-digit decimal entries. Duplicate codes are not permitted.

The following access levels may be available on your panel:

Master User

Has access to all system functionality. These functions include:

- Bypass/unbypass zones
- Chime enable/disable
- View troubles
- View alarms in memory
- Create new users (via user app)
- Initiate a system test
- Update Panel WiFi (client mode) SSID & password
- Adjust keypad settings sucha as buzzer tone and volume, display contrast and brightness
- Assign wireless keys to users

Level 0: Professional Installer

Has permission to enable WPS mode (to enable local programming access to the panel via the installer app) and also initiate phone test.

Level 1: Supervisor/Administrator

Users assigned to this level have similar privileges to the Master Code user but are limited based on the partition assignment. This user can perform the following actions on the partitions they are assigned to:

- Arm/Disarm
- Bypass/Unbypass
- Enable/disable chime
- Access home automation menu
- View troubles, initiate a system test
- Select a display language
- View the event buffer
- Program zone labels
- Update WiFi SSID and password
- Create new users
- Program a duress code
- Program user labels

Supervisor users can only add, edit or delete users assigned to the same partitions as they are.

Level 2: Basic/Standard User

Has permission to access basic security functions, including:

- Arm/disarm
- Bypass/unbypass zones
- Enable/disable chime
- View system troubles
- View alarm in memory

Level 3: Maintenance/Guest

Users assigned to this level are limited to an assigned partition and have reduced system access. These functions include:

- Arm/disarm
- Enable/disable chime
- View system troubles

Duress code:

Has access to all features of Basic/Standard user, including:

- Arm/disarm
- Bypass/unbypass zones

When this code is used for any function, a duress code event will be generated.

User Name (label)

This option is used to program a system user name.

Default:	Blank
Valid range:	32 character ACSII

4.7.3 Wireless Siren Configuration Options

The following section provides descriptions of all wireless siren programming options.

Siren Label

This option is used to program a label for the device.

Default:	Siren 1
Valid range:	32 character ASCI

Siren Enable/Disable

This option is used to enable and disable the wireless siren.

Default:	Enabled
Valid range:	Enabled/Disabled

Siren Partition Assignment

This option is used to assign the wireless siren to an available partition.

Default:	1
Valid range:	1-4

Fire Alarm

When this option is enabled, the wireless siren sounds during fire alarms.

Default:	Enabled
Valid range:	Enabled/Disabled

CO Alarm

When this option is enabled, the wireless siren sounds during CO alarms.

Default:	Enabled
Valid range:	Enabled/Disabled

Burg Alarm

When this option is enabled, the wireless siren sounds during burglary alarms.

Default:	Enabled
Valid range:	Enabled/Disabled

Flood Alarm

When this option is enabled, the wireless siren sounds for flood alarms.

Default:	Enabled
Valid range:	Enabled/Disabled

Auto Tamper Alarm

When this option is enabled, the wireless siren sounds during tamper alarms.

Default:	Disabled
Valid range:	Enabled/Disabled

Activity LED

When this option is enabled, the Activity LED flashes every few seconds to indicate that the siren is enrolled and active.

Default:	Disabled
Valid range:	Enabled/Disabled

Volume Control

This option is used to control the volume of the wireless siren.

Default:	Medium.
Valid range:	Low, Medium, High

Squawk Control

This option is used to control wireless siren behavior during an alarm.

Default:	Sounder Only
Valid range:	Disabled, Sounder Only, Strobe Only, Sounder and Strobe

Exit/Entry Beeps

When this option is enabled, the wireless siren beeps whenever entry/exit zones are tripped.

Note: When set to Disable in Stay Mode, the siren still beeps on entry/exit when the system is armed in Away mode.

Default:	Disabled
Valid range:	Disabled, Enabled, Disable in Stay Mode

Siren Strobe Alarm

This option is used to control the behavior of the wireless siren strobe light during an alarm.

Default:	Active Until Bell Time-out
Valid range:	Disabled, Active Until Disarmed, Active Until Bell Time-out

4.7.4 Wireless Key Configuration Options

The following sections are used for programming wireless keys.

Wireless Key Enable/Disable

When this option is enabled, the alarm panel receives commands from the enrolled wireless key.

Default:	Enabled
Valid range:	Enabled/Disabled

Wireless Key Partition Assignment

This option is used to assign the wireless key to an available partition.

Default:	1
Valid range:	1-4, ALL

Wireless Key Button Programming

This option is used to program functionality for all available buttons on the wireless key. The number of buttons varies depending on the model.

Note: Panic shall be disabled for PGx929 and PGx939 for SIA installations.

Default:	Button 1 = Away Arm*
	Button 2 = Stay Arm*
	Button 3 = Disarm*
	Button 4 = Panic**
	Button 5 = Quick Exit
Valid range:	Null, Disarm, Stay Arm, Away Arm, Global Stay Arm, Global Away Arm, Global Disarm, Quick Exit, Auxiliary Alarm, Panic Alarm

*Not applicable for PGx938.

**Not applicable for PGx938 and PGx949.

Supervision

This option is used to control battery supervision of the wireless key. When enabled, the iotega detects and reports a wireless key low battery condition.

This feature is only applicable for PGx938.

| Default: | Disabled (Must be enabled for UL) |
| Valid range: | Enabled/Disabled |

User ID

All wireless keys are assigned to the Master user by default. Assignment to another user is done via the touchscreen keypad. Assigning wireless keys to specific users aids in tracking and logging system events.

Not applicable for PGx938

| Default: | None |
| Valid range: | 001-100 |

4.7.5 Wireless Smoke and CO Configuration Options

The following sections are used for programming wireless smoke and CO detectors.

Device Enable/Disable

This option is used to enable and disable wireless smoke and CO detectors.

| Default: | Enabled |
| Valid range: | Enabled/Disabled |

Device Partition Assignment

This option is used to assign wireless smoke and CO detectors to an available partition.

| Default: | 1 |
| Valid range: | 1-4 |

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

| Default: | Beeps |
| Valid range: | Beeps, Bing Bing, Ding Dong, Alarm Tone |

Zone Type

This programming option is used to program a zone type for the device.

| Default: | 24-hour standard fire |
| Valid range: | 24-hour standard fire, Auto-verified fire |

Device Label

This section is used to program a custom label for the device.

| Default: | Zone ZZZ |
| Valid range: | 32 character ASCII |

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Disabled (read-only)
Transmission Delay	Disabled (read-only)
Bell Audible	Enabled (read-only)
Bell Steady	Disabled (read-only)
Bypass Enable	Disabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Disabled (read-only)
Two Way Audio	Disabled (read-only)
Talk Listen	Disabled (read-only)

Supervision

This section is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

| Default: | Enabled (Must be enabled for UL) |
| Valid range: | Enabled/Disabled |

4.7.6 Wireless Glassbreak Configuration Options

The following sections are used for programming glassbreak detectors.

Device Enable/Disable

This option is used to enable and disable the wireless device.

| Default: | Enabled |
| Valid range: | Enabled/Disabled |

Device Partition Assignment

This option is used to assign the wireless device to an available partition.

Default:	1
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Beeps
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Type

This programming section is used to program a zone type for the device.

Default:	Interior Follower
Valid range:	Instant, Interior Follower, Interior Stay/Away, Delay Stay/Away, 24 Hour Supervisory Buzzer, 24 Hour Non Alarm

Device Label

This section is used to program a custom label for the device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Enabled
Alarm Report	Enabled
Burglary Verified	Enabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Enabled (read-only)
Two Way Audio	Enabled (read-only)
Talk Listen	Enabled (read-only)

Supervision

This section is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

4.7.7 Wireless Temperature Configuration Options

The following sections are used for programming wireless temperature sensors.

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Device Partition Assignment

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Disabled
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Type

This option is used to program a zone type for the device.

Default:	24-hour Temperature
Valid range:	24-hour Temperature

Device Label

This option is used to program a custom label for the wireless device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Disabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Disabled (read-only)
Two Way Audio	Disabled (read-only)
Talk Listen	Disabled (read-only)

Supervision

This option is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

Temperature Format
This section is used to select the scale temperature is displayed in.

Default:	F
Valid range:	F (Fahrenheit), C (Celsius)

High Temperature Warning
This option is used to set the temperature threshold for activating the High Temperature warning indicator. A high temperature warning sounds an audible alert but does not send a trouble to the central monitoring station.
This option is disabled by entering -999 or 999.

Default:	999
Valid range:	-999 to 999

High Temperature Alarm
This option is used to set the temperature threshold for activating the High Temperature alarm.
This option is disabled by entering -999 or 999.

Default:	999
Valid range:	-999 to 999

Low Temperature Warning
This option is used to set the temperature threshold for activating the Low Temperature warning indicator. A low temperature warning sounds an audible alert but does not send a trouble to the central monitoring station.
This option is disabled by entering -999 or 999.

Default:	999
Valid range:	-999 to 999

Low Temperature Alarm
This option is used to set the temperature threshold for activating the Low Temperature alarm.
This option is disabled by entering -999 or 999.

Default:	999
Valid range:	-999 to 999

4.7.8 Wireless Flood Configurations

The following sections are used for programming wireless flood sensors.

Device Enable/Disable
This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Device Partition Assignment
This option is used to assign the wireless device to an available partition.

Default:	1
Valid range:	1-4

Chime Tone
This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Disabled
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Type
This programming section is used to program a zone type for the device.

Default:	Interior Follower
Valid range:	Instant, Interior Follower, Interior Stay/Away, Delay Stay/Away, 24 Hour Supervisory Buzzer, 24 Hour Non Alarm

Device Label
This section is used to program a custom label for the device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Attribute

This option is used to customize zone operation. The following attributes are available for the temperature sensor:

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Disabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Disabled (read-only)
Bypass Enable	Disabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Disabled (read-only)
Two Way Audio	Disabled (read-only)
Talk Listen	Disabled (read-only)

Supervision
This section is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

4.7.9 Wireless PIR CAM Configurations

The following sections are used to program wireless PIR Camera motion detectors.

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Device Partition Assignment

This option is used to assign the wireless device to an available partition.

Default:	1
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Beeps
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Device Label

This section is used to program a custom label for the device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Type

This programming section is used to program a zone type for the device.

Default:	Interior Follower
Valid range:	Instant, Interior Follower, Interior Stay/Away, Delay Stay/Away, 24 Hour Supervisory Buzzer, 24 Hour Non Alarm

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.
See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Enabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Enabled (read-only)
Two Way Audio	Enabled (read-only)
Talk Listen	Enabled (read-only)

Supervision

This section is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

Alarm LED

This option is used to enable/disable the device's onboard LED. When enabled, the LED activates when an alarm occurs.

Default:	Enabled
Valid range:	Enabled/Disabled

High Traffic Shutdown

Activating this feature helps conserve battery power when the system is disarmed by configuring a reporting timer. When motion is detected, the device transmits an alarm to the receiver and does not report any further events until the timer expires. Any motion detected during the configured period is reported once the timer expires. No Delay causes the device to report an alarm each time the detector is tripped.

Default:	Not Active
Valid range:	Not Active, No Delay, 5 Second Delay, 15 Second Delay, 30 Second Delay, 1 Minute Delay, 5 Minute Delay, 10 Minute Delay, 20 Minute Delay, 60 Minute Delay

Event Counter

This option is used to set the number of alarm events required to activate the alarm.

Default:	Low
Valid range:	Low/High

Image Brightness

This option is used to lighten or darken the camera image.

Default:	0
Valid range:	-3, -2, -1, 0, 1, 2, 3

Image Contrast

This option is used to lighten or darken the contrast of the camera image.

Default:	o
Valid range:	-3, -2, -1, 0, 1, 2, 3

Color

When this option is enabled, the camera captures color images. When disabled, the camera captures black and white images.

Default:	Enabled
Valid range:	Enabled/Disabled

High Resolution

When this option is enabled, the camera captures high resolution images (320 x 240 dpi). When disabled, image resolution is 160 x 128 dpi.

Default:	Enabled
Valid range:	Enabled/Disabled

Normal Quality

When this option is enabled, the camera captures lower resolution images (160 x 128 dpi).

Default:	Disabled
Valid range:	Enabled/Disabled

Audio (mic)

This option is used to enable/disable the built-in microphone on the device.

Default:	Disabled
Valid range:	Enabled/Disabled

4.7.10 Wireless PIR (NO CAM) Configurations

The following sections are used to program wireless motion detectors.

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Device Partition Assignment

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Beeps
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Type

This option is used to program a zone type for the device.

Default:	Follower
Valid range:	Instant, Interior, Follower, Interior Stay/Away, Delay Stay/Away, 24 Hour Supervisory Buzzer, 24 Hour Non-Alarm

Device Label

This option is used to program a custom label for the wireless device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Enabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Enabled (read-only)
Two Way Audio	Enabled (read-only)
Talk Listen	Enabled (read-only)

Supervision

This option is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

Alarm LED

This option is used to enable/disable the device's onboard LED. When enabled, the LED activates when an alarm occurs.

Default:	Enabled
Valid range:	Enabled/Disabled

24 Hour PIR

This option is used to define if motion alarms are always enabled or only enabled at night.

Default:	Enabled
Valid range:	Enabled/Disabled

High Traffic Shutdown

Activating this feature helps conserve battery power when the system is disarmed by configuring a reporting timer. When motion is detected, the device transmits an alarm to the receiver and does not report any further events until the timer expires. Any motion detected during the configured period is reported once the timer expires. No Delay causes the device to report an alarm each time the detector is tripped.

Default:	Not Active
Valid range:	Not Active, No Delay, 5 Second Delay, 15 Second Delay, 30 Second Delay, 1 Minute Delay, 5 Minute Delay, 10 Minute Delay, 20 Minute Delay, 60 Minute Delay

Detection Range

This option is used to select the sensitivity of the detector. The higher the sensitivity, the further the range of the detector.

Default:	High
Valid range:	Low, High, UL

4.7.11 Wireless Door Window Configurations

The following sections are used to program wireless door/window contacts.

Device Label

This option is used to program a custom label for the wireless device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Zone Type

This option is used to program a zone type for the device.

Default:	24-hour Temperature
Valid range:	Delay 1, Delay 2, Instant (Perimeter), Interior Follower, Interior Stay/Away, Delay Stay/Away, Day Zone, 24Hour Burglary, 24Hour Silent Holdup, 24Hour Audible Panic, 24Hour Medical Alarm, 24Hour Supervisory Buzzer, 24Hour Non-Alarm

Device Partition Assignment

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Beeps
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Disabled
Alarm Report	Enabled
Burglary Verified	Enabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Enabled (read-only)
Two Way Audio	Enabled (read-only)
Talk Listen	Enabled (read-only)

Supervision

This option is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

Alarm LED

This option is used to enable/disable the device's onboard LED. When enabled, the LED activates when an alarm occurs.

Default:	Enabled
Valid range:	Enabled/Disabled

Reed Switch

This option is used to enable/disable the device's built-in reed switch. The reed switch is used in conjunction with the separately mounted magnet as part of the trigger mechanism.

If the reed switch is enabled and a device is hardwired to the external input terminals, both sensors transmit simultaniously. However, the iotega treats both devices as the same zone. Disable the reed switch to have the hardwired device funciton independently.

Default:	Enabled
Valid range:	Enabled/Disabled

Zone EOL Configuration

This option is used to configure end of line resistors for the external input terminals. The alarm panel uses EOL resistors to monitor for fault or alarm conditions.

Default:	EOL Disable
Valid range:	Single, EOL Disable, Normal Open, Normal Close

4.7.12 Wireless Shock Sensor Configurations

The following sections are used to program wireless shock sensors.

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

Device Partition Assignment

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	1-4

Chime Tone

This option is used to select the tone emitted by the device when the zone is tripped.

Default:	Beeps
Valid range:	Beeps, Bing Bing, Ding Dong, Alarm Tone

Zone Type

This option is used to program a zone type for the device.

Default:	Instant (Perimeter)
Valid range:	24 Hour Burglary, Day Zone, Instant (Perimeter)

Device Label

This option is used to program a custom label for the wireless device.

Default:	Zone ZZZ
Valid range:	32 character ASCII

Zone Attribute

This section is used to customize zone behavior for the device. The table below specifies the status of each attribute for this device.

See "Available Zone Attributes" on page 32 for attribute definitions.

Door Chime	Enabled
Alarm Report	Enabled
Burglary Verified	Enabled
Transmission Delay	Enabled
Bell Audible	Enabled (read-only)
Bell Steady	Enabled (read-only)
Bypass Enable	Enabled (read-only)
Force Arm	Disabled (read-only)
Swinger Shutdown	Enabled (read-only)
Two Way Audio	Enabled (read-only)
Talk Listen	Enabled (read-only)

Supervision

This option is used to enable/disable wireless supervision of the device. Supervision monitors the presence of the wireless device on the alarm system.

Default:	Enabled
Valid range:	Enabled/Disabled

Alarm LED

This option is used to enable/disable the device's onboard LED. When enabled, the LED activates when an alarm occurs.

Default:	Enabled
Valid range:	Enabled/Disabled

Reed Switch

This option is used to enable/disable the device's built-in reed switch. The reed switch is used in conjunction with the separately mounted magnet as part of the trigger mechanism.

If the reed switch is enabled and a device is hardwired to the external input terminals, both sensors transmit simultaniously. However, the iotega treats both devices as the same zone. Disable the reed switch to have the hardwired device funciton independantly.

Default:	Disabled
Valid range:	Enabled/Disabled

Zone EOL Configuration

This option is used to configure end of line resistors for the external input terminals. The alarm panel uses EOL resistors to monitor for fault or alarm conditions.

Default:	EOL Disable
Valid range:	Single, EOL Disable, Normal Open, Normal Close

Shock Accumulation

Shock accumulation is used to count a series of low level impacts that fall below the programmed alarm threshold (see Shock Sensitivity) over a ten-second period.

If the total energy of the low level impacts surpasses the threshold, an alarm is triggered. If not, the accumulation level is reset.

Default:	Enabled
Valid range:	Enabled/Disabled

Shock Sensitivity Level

This option is used to adjust the sensitivity of the sensor. The lower the number, the more sensitive the device. Use the lowest settings for hard surfaces such as concrete.

Default:	8
Valid range:	1-19

4.7.13 Repeater Configuration Options

The following sections are used to program wireless repeaters.

Device Label

This section is used to program a custom label for the device.

Default:	Repeater X
Valid range:	32 character ASCII

Device Enable/Disable

This option is used to enable and disable the wireless device.

Default:	Enabled
Valid range:	Enabled/Disabled

4.8 Available Zone Types

Delay 1	Commonly assigned to primary points of entry. Follows entry delay 1 and exit delay timers. Arming the alarm system starts the exit delay timer. After the exit delay has expired, opening the door starts the entry delay timer. During entry delay, the keypad buzzer prompts the user to disarm the system.
Delay 2	Commonly assigned to secondary points of entry (further from the keypad). Follows entry delay 2 timer.
Instant	Commonly used for perimeter doors and windows, this zone type follows the exit delay. The alarm is triggered instantly if the zone is tripped after the exit delay expires.
Interior	Commonly assigned to interior motion sensors near a point of entry, such as a foyer or hallway, that must be accessed to reach the keypad. The alarm is activated if the system is armed and a delay type zone (e.g., front door) is not tripped first, or if the entry/exit timer expires before the alarm is disarmed. Otherwise, the zone is instant if tripped.
Interior Stay/Away	Similar to Interior zone type except that the system bypasses the zone when armed in Stay mode. Commonly used to activate perimeter zones while permitting free movement throughout the interior.
Delay Stay/Away	Similar to delay 1 except that the zone is bypassed when armed in Stay mode. Commonly used with motion detectors that cover an entry point.
Day Zone	Commonly used in areas where immediate notification of entry is desired. When disarmed, tripping this zone activates the keypad buzzer but does not log or report the event. When armed, tripping this zone activates the siren then logs and reports the event. **Note:** An alarm during exit delay causes the siren to activate and remain on when exit delay expires.
Standard 24-Hour Fire	This zone is used with smoke detectors. The siren sounds instantly when the smoke detector is activated. If enabled, the communicator immediately transmits the alarm to the monitoring station. A tamper or fault of this zone type causes a fire trouble to log and transmit.
Auto Verify Fire	This 24 hour zone type validates an alarm condition by looking for a second alarm transmission or the absence of an alarm restoral condition on wireless smoke detectors. When the zone is activated, a 40-second delay begins. If the zone is still faulted after 40 seconds, the system goes into full alarm. The bell sounds and the event is logged and communicated. If another fire zone is activated during the auto verify sequence, alarms are immediately generated for all pending zones. This applies to all other fire zone types and to [F] key alarms. If the zone is no longer in alarm at the end of the 40 second delay, an 80-second verification timer begins. If another fire zone is activated during the auto verify sequence, both zones go into alarm immediately. **Note:** Wireless smoke detectors used with this zone type must have a built in siren to act as a pre-alert to the system alarm.
24-Hour CO	This zone type is used with CO detectors. In the event of an alarm, a distinctive siren cadence is sounded. This is followed by a 5-second pause and then repeated. After 4 minutes, the 5-second pause is extended to 60 seconds; however, BTO must be programmed with a value of 5 minutes or higher. The siren is silenced when an access code is entered or the siren times out.
24-Hour Burglary	This zone type is active at all times. It reports an alarm if the alarm system is armed or disarmed. This zone type sounds the siren for the length of Bell time-out if the audible attribute is enabled.
24-Hour Holdup	Instant alarm when activated, silent alarm at default. **Note:** Not for use in UL listed installations.
24-Hour Panic	Instant alarm when activated, audible alarm at default.
24-Hour Medical	Instant alarm when activated, audible alarm at default.
24-Hour Supervisory	This zone is active and reports alarms at all times when tripped. The siren and keypad buzzer do not activate.
24-Hour Temperature	This zone type is used with temperature sensors and is activated when the temperature rises above a programmed threshold. Instant alarm when activated, audible alarm at default. This zone type generates an alarm when the system is armed or disarmed. **Note:** The temperature threshold includes a 3 °C (5-6 °F) difference between a given state and its restored condition. For example, an alarm at 6 °C is restored at 3°C (High temperature) or 9°C (Low temperature), depending upon the zone type selected.
24-Hour Flood	Instant alarm when activated, audible alarm at default.
24-Hour Non-Alarm	This zone is active at all times but does not cause an alarm. Zone attributes such as Zone Bypassing and Door Chime affect the functionality of this zone. This zone type can also be assigned to a temperature sensor if indoor/outdoor temperature display is required without temperature warnings or alarm conditions.

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.

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)
This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

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

FCC/ISED CANADA WIRELESS NOTICE

This equipment complies with FCC and ISED Canada radiation exposure limits set forth for an uncontrolled environment. The antenna should be installed and operated with minimum distance of 20 m between the radiator and your body. Antenna gain must be below:

Frequency band	3G7090
GSM 850 / FDD V	2.1 dBi
PCS 1900 / FDD II	3.7 dBi
Frequency band	LT7090
LTE B4 (1700 MHz)	1.5 dBi
LTE B13 (700 MHz)	2.2 dBi

This transmitter can be co-located or operating in conjunction with any other antenna or transmitter.

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
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.

NIST Validation of encryption algorithm AES128 certificate No. 4053

FCC/IC LABEL

The modular transmitter 3G7090 or LT7090 is labeled with its own FCC ID and IC number. When the module is installed inside the host device WS900-19 or WS900- 29 and the FCC ID/IC of the module is not visible, the host device displays the provided label referring to the FCC ID and IC of the enclosed module. This 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.

4.9 Available Zone Attributes

The following table defines each available zone attribute.

Alarm Report	When this attribute is enabled, zone alarm and restore events are transmitted. When disabled, zone alarm events are not transmitted but are logged to the event buffer.
Chime	When this attribute is enabled, the keypad chimes when the zone is opened or closed.
Burglary Verified	When this attribute is enabled, zone alarms are not communicated until a burglary verified event occurs.
Transmission Delay	When this attribute is enabled, reporting of zone alarms is delayed for the programmed time. If a valid access code is entered within this time, no alarm signal is communicated. When disabled, reporting codes are transmitted immediately.
Bell Audible	The siren activates on alarm. This is a read-only option.
Bell Steady	Siren output is steady rather than pulsed when in alarm. This is a read-only option.
Bypass Enable	Zones can be manually bypassed. This is a read-only option.
Force Arm	The system can be armed with the zone open. The zone is temporarily bypassed and, when secured, is monitored by the system. If Open Zone Cancels Arming is enabled, the system can begin arming with an open, Force Arm zone, but if the zone is still open when the exit delay timer expires, arming is cancelled. This is a read-only option.
Swinger Shut-down	A zone that goes into alarm for the number of times programmed in the Swinger Shutdown Counter shuts down with no further transmissions sent to the monitoring station. The siren follows swinger shutdown if programmed. This is a read-only option.
Two-Way Audio	The panel is able to initiate a 2-way audio session. This is a read-only option.
Talk Listen	The central station operator and the end user can communicate through the panel's microphone and speaker. This is a read-only option.

4.10 Diagnostics - Read Only

Radio Version#

This section displays the software version of the cellular radio.

Primary Telephone Number

This section displays the cellular telephone number of the SIM.

IMEI number

This section displays the unique 15-digit International Mobile Equipment Identity (IMEI) of the radio. The format of the IMEI is: Reporting Body Identifier (2 digits), Allocation Number (4 digits); Final Assembly Code (2 digits); Serial Number (6 digits); and a check digit.

SIM Number

This section displays the Subscriber Identity Module (SIM) number of the SIM card installed in the communicator. The format of the SIM number is: Major Industry Identifier (2 digits); Mobile Country Code (2 or 3 digits); Mobile Network Code (2 - 3 digits); Unique Number (10 -12 digits); and Checksum (1 digit). Valid SIM numbers range is: 18 - 21 numbers. This number is printed on the SIM and the outside of the communicator carton.

Note: The checksum digit is omitted on 19-digit SIM card numbers.

Cellular Device Type

This section displays the type of cellular module used by the system. E.g., UE910-N3G, LE910-SVG

Cellular Signal Strength

This section displays the strength of the cellular signal: Strong, Weak, None.

Radio Network Technology

This section displays the mobile wireless telecommunications technology used by the cellular radio.

Provider ID#

This section identifies number of the telecommunications service provider.

4.11 System Control

Use this section to perform the following diagnostic tests.

System Test

This test is used to check that the iotega's siren and LEDs are operating correctly. This is a hardware test only. No signals are transmitted to the monitoring station. During the test, the LEDs flash.

Alarm Control Panel Placement Test

This test is used to check the panel location for signal noise that could interfere with the proper operation of the alarm system. If the location is good, "No noise" is displayed. If the location has signal noise beyond system tolerance, "noise" is displayed.

Walk Test

This mode tests the operation of each detector in the system. While in Walk Test, the Ready, Armed, and Trouble LED's on the keypad flash to indicate that the test is active.
When a zone is violated during the test, a 2-second tone sounds on all system keypads to indicate that the zone is working correctly. The system automatically ends the test after 15 minutes without zone activity. An audible warning (5 beeps every 10 seconds) is sounded, beginning 5 minutes before the test ends.

Placement Test

This test is used to determine the RF signal status for wireless devices and can be performed on the installer portal or at the individual device. For instructions on placement testing at the device, refer to the installation sheet included with the wireless equipment.

Two test results are provided:

24 Hour: The iotega displays RF test results from the enrolled device received over a 24 hour period.

Now: The iotega displays RF test results from the last placement test.

Note: For vanishing door contacts and wireless keys, the device must be triggered in order to get a result.

Status	Definition
Strong	Strong signal strength
Good	Good signal strength
Poor	Poor signal strength
1-Way	The alarm panel can see the device but cannot configure or control it.
2-Way	The alarm panel can configure and control the device.
0-Way	The alarm panel cannot see or control the device.
Missing	The device has not received any communications from the panel during the supervision monitoring period.
Not Networked	The device is registered but not activated on the network.
NA	The device is not registered.

4.11.1 Network

Cellular Test Transmission

Ethernet and Cellular test transmissions check to see if the selected communication path between the iotega and the central monitoring station is functioning correctly.

Both Ethernet/Cellular 1 (primary receiver) and Ethernet/Cellular 2 (secondary receiver) can be tested separately based on individual reporting configurations. Test transmissions can also be configured to alternate between primary and secondary receivers. For details, see "Alternate Test Transmission" on page 1.

Test transmission time and test transmission cycle can be programmed for both primary and secondary receivers. See "Central Monitoring Station Programming Options" on page 17 for more details.

Section 5: Troubleshooting

5.1 Testing

- Power up the system
- Program options as required (see programming section)
- Trip then restore zones
- Verify correct reporting codes are sent to the central monitoring station

5.2 Viewing Troubles from the Integrated Keypad

1. Move your hand over the iotega to illuminate the keypad.
2. Press * 2 .
3. Enter your access code if required. The Trouble LED on the keypad flashes if an access code is needed to view troubles. Entering a valid access code silences trouble beeps.
4. The keypad displays top-level troubles present on the system by illuminating numbers on the keypad. Refer to the table below for the meaning of each trouble code. When in the top level trouble display, the trouble LED flashes once, pauses, then repeats.
5. If additional details are available for the trouble, the [*] key illuminates. Press any illuminated number to display the second level troubles.
6. The keypad displays a second level of detail for the trouble code selected in step 5 by illuminating numbers on the keypad. Refer to the table below for the meaning of each trouble code. When in the second level trouble display, the trouble LED flashes two times, pauses, then repeats.
7. If additional details are available for the trouble, the [*] key illuminates. Press any illuminated number to display the third level trouble detail.
8. The keypad displays the device number with the trouble condition. If more than one device has this trouble at the same time, the keypad cycles though each one. When in the third level trouble display, the trouble LED flashes three times, pauses, then repeats.
9. Press the [*] key to acknowledge a trouble.

Note: Pressing the # key returns you to the previous level. Pressing the # key while in the top-level exits the trouble menu.

Trouble Summary

- Trouble [01] - System Trouble
- Trouble [02] - Zone
- Trouble [03] - Siren
- Trouble [04] - Keypad
- Trouble [05] - Repeater
- Trouble [06] - Wireless Key
- Trouble [07] - Communication
- Trouble [00] - Integrator Trouble

Table 7-1 Trouble Indications

1st Layer		2nd Layer		3rd Layer
01	System Trouble	01	AC	
		02	Battery Trouble	
		03	Tamper	
		04	Hardware Fault	
		05	Loss of Time	
		06	RF Jam	
02	Zone	01	AC Trouble	1-128
		02	Battery Trouble	1-128
		03	Tamper	1-128
		04	Fault (Supervision)	1-128

		05	Not Networked	1-128
		06	Fire/CO Trouble	1-128
03	Siren	01	Future Use	1-16
		02	Battery Trouble	1-16
		03	Tamper	1-16
		04	Fault (Supervision)	1-16
		05	Not Networked	1-16
04	Keypad	01	AC	1-9
		02	Battery Trouble	1-9
		03	Tamper	1-9
		04	Fault (Supervision)	1-9
		05	Not Networked	1-9
05	Repeater	01	AC	1-8
		02	Battery Trouble	1-8
		03	Tamper	1-8
		04	Fault (Supervision)	1-8
		05	Not Networked	1-8
		06	RF Jam	1-8
06	Wireless Key	01	Future Use	1-32
		02	Battery Trouble	1-32
		03	Future Use	1-32
		04	Future Use	1-32
		05	Not Networked	1-32
07	Communication	02	FTC Trouble	
		04	Cellular Trouble	
		05	Ethernet/WiFi Trouble	
00	Integrator Trouble	01	Z-Wave Trouble	

Appendix 8: Reporting Codes

The following tables contain Contact ID and Automatic SIA format reporting codes.

Contact ID

Each of the digits indicate specific information about the signal. For example, if zone 1 is an entry/exit point, the event code contains [34]. The central monitoring station would receive the following:

*BURG - ENTRY/EXIT - 1 where the "1" indicates which zone went into alarm.

see "Contact ID and SIA Zone Alarm/Restore Event Codes" on page 37 for code definitions.

SIA Format - Level 2 (Hard Coded)

The SIA communication format used in this product follows the level 2 specifications of the SIA Digital Communication Standard - October 1997. This format sends the account code along with its data transmission. The transmission appears similar to the following at the receiver:

    N ri1 BA 01

    N = New Event

    ri1 = Partition /Area Identifier

    BA = Burglary Alarm

    01 = Zone 1

A system event uses the Area Identifier ri00.

Contact ID and SIA Zone Alarm/Restore Event Codes

Section #	Definition	Dialer Direction*	Automatic Contact ID Codes	SIA Auto Rep Codes**
Sensor Events				
	Sensor alarms	A/R	see "Contact ID & SIA Zone Alarm/Restore Event Codes" on page 38" for details.	
	Sensor restores	A/R		
	Sensor tamper/restore	MA/R	E(3)83-ZZZ / R(3)83-ZZZ	TA-ZZZ / TR-ZZZZ
	Sensor trouble/restore	MA/R	E(3)8A-ZZZ / R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
Tamper Events				
	Sensor tamper/restore	T/R	E(3)17-000 / R(3)17-000	ES-000 / TR-000
	Panel tamper/restore	T/R	E(1)37-000 / R(1)37-000	ES-000 / EJ-000
	Touchpad tamper - keystroke	T/R	E(4)61-000	JA-000
Opening Events				
	Opening report	O/C	E(4)A1-UUU	OP-UUUU
Closing Events				
	Closing report	O/C	R(4)A1-UUU	CL-UUUU
	Partial closing	O/C	E(4)56-000	CG-0000
	Exit alarm	O/C	E(3)74-ZZZ	EA-ZZZZ
System Trouble Events				
	Sensor tamper/restore	MA/R	E(1)37-000/ R(1)37-000	ES-0000/EJ-0000
	CPU low battery trouble/restore	MA/R	E(3)A2-000 / R(3)A2-000	YT-0000 / YR-0000
	Battery absent trouble/restore	MA/R	E(3)11-000 / R(3)11-000	YM-0000 / YR-0000
	Battery charging trouble/restore	MA/R	E(3)14-000/ R(3)14-000	YP-0000/ YQ-0000
	AC power fail/restore	MA/R	E(3)A1-000 / R(3)A1-000	AT-0000 / AR-0000
Communication				
	Receiver jammed/restore	MA/R	E(3)AA-001 R(3)AA-001	YX-0001 / YZ-0001
	Dual path supervision failure/restore	MA/R	E(3)500-xxx R(3)500-xxx	YS-0001 / YZ-0001
	FTC trouble/restore	MA/R	E(3)54-RRR/ R(3)54-RRR	YC-RRR/YK-RRR
	2-Way voice session start	MA/R	E(6)06	LF-000
Sensor Events				
	Sensor low battery trouble/restore.	MA/R	E(3) 84-ZZZ R(3) 84-ZZZ	XT-ZZZZ / XR-ZZZZ

Section #	Definition	Dialer Direction*	Automatic Contact ID Codes	SIA Auto Rep Codes**
	Sensor trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
	Sensor bypass/restore	MA/R	E(5)7A-ZZZ R(5)7A-ZZZ	UB-ZZZZ / UU-ZZZZ
	Heat or probe trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	KT-ZZZZ / KJ-ZZZZ
	Freeze ESM module/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	ZT-ZZZZ / ZJ-ZZZZ
	Repeater 1-8 AC fail/restore	MA/R	E (3)A1-901 R (3)A1-901	AT-0901 / AR-0901
	RF jam trouble/restore		E(3)AA-0000 R(3)AA-000	XQ-0000/XH-0000
Miscellaneous Alarms				
	Duress zlarm - code entered at keypad	A/R	E(1)21-000	HA-0000/ HH-0000
	Opening after alarm - disarmed with alarm in memory	A/R	E(4)58-000	OR-0000
	Recent closing - alarm occurs within two minutes of system arming	A/R	E(4)59-UUU	CR-UUUU
	Cross zone alarm	A/R	E(1)39-000	BV-0000
	Two trip error	A/R	E(3)78-000	BG-0000
	Cancel report	A/R	E(4)A6-UUU	OC-UUUU
Priority Alarm and Restoral Events				
	[F] Key alarm/restore	A/R	E(1)1A-000 R(1)1A-000	FA-0000 / FH-0000
	[A] Key alarm/restore	A/R	E(1)AA-000 R(1)AA-000	MA-0000 / MH-0000
	[P] Key alarm/restore	A/R	E(1)2A-000 R(1)2A-000	PA-0000 / PH-0000
	Silent police panic/cancel	A/R	E(1)20-0000/ R(1)20-0000	PA-0000/PH-0000
Miscellaneous Closing				
	Sensor bypass	O/C	E(5)7A-ZZZ	UB-ZZZZ
	Sensor bypass restore	O/C	R(5)7A-ZZZ	UU-ZZZZ
Testing				
	Sensor test start/end	T	E(6)A7-UUU R(6)A7-UUU	TS-UUUU/TE-UUUU
	Auto-phone test	T	E(6)A2-000	RP-0000 / RY-0000
	Test transmission with trouble	T	E(6)A8-000	RY-0000
	Manual phone test	T	E(6)A1-000	RX-0000
Maintenance				
	Partition fire trouble/restore	MA/R	E(3)73-992 R(3)73-992	FT-992 / FJ-992
	Smoke detector low sensitivuty trouble/restore	MA/R	E(3)73-000 R(3)73-000	FT-0000 / FJ-0000
	Panel programming	MA/R	E(6)27-000	LB-0000
	Panel programming exited	MA/R	E(6)28-000	LS-0000
	Lack of usage	MA/R	E(6)54-000 R(6)54-000	CD-000
*	A/R = alarms/restores; T/R = tampers/restorers; O/C = openings/closings; MA/R = maintenance alarms/restores; T = test transmissions			
**	UUU = user number. Note that for CID, enter 999 for user 1000. ZZZ/ZZZZ = zone number.			
***	Zones and panic pendants are identified, wireless keys can be identified for openings and closings.			

Contact ID & SIA Zone Alarm/Restore Event Codes

(as per SIA DCS: 'Contact ID' 01-1999):

The table below defines the meaning of all Contact ID and SIA zone alarm/restore event codes.

Zone Definition	SIA Auto Rep Codes	Contact ID Auto Rep Codes
Delay 1	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Delay 2	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Instant	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Interior	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Interior stay/away	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Delay stay/away	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Day Zone	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
24-Hr. Burglary	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
Standard 24-Hr. Fire (wireless)	FA-ZZZZ / FH-ZZZZ	E(1) 1A - ZZZ / R(1)1A - ZZZ
24-Hr Temperature	KA-ZZZZ / KH-ZZZZ	E(1) 58 - ZZZ / R(1)58 - ZZZ
24-Hr. Non alarm (walk test only)	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A- ZZZ
24-Hr. Supervisory buzzer	UA-ZZZZ / UH-ZZZZ	E(1) 5A - ZZZ / R(1)5A - ZZZ
24-Hr. Auto verified fire (wireless)	FA-ZZZZ / FH-ZZZZ	E(1) 1A - ZZZ / R(1)1A - ZZZ
24-Hr. CO alarm	GA-ZZZZ / GH-ZZZZ	E(1) 62 - ZZZ / R(1)62 - ZZZ
24-Hr. Holdup	HA-ZZZZ / HH-ZZZZ	E(1) 22 - ZZZ / R(1)22 - ZZZ
24-Hr. Panic	PA-ZZZZ / PH-ZZZZ	E(1) 2A - ZZZ / R(1)2A - ZZZ
24-Hr. Flood	WA-ZZZZ / WH-ZZZZ	E(1) 54 - ZZZ / R(1)54 - ZZZ
24-Hr. Auxiliary	MA-ZZZZ / MH-ZZZZ	E(1) AA - ZZZ / R(1)AA - ZZZ
ZZZ/ZZZZ = zones 001-128		

Appendix 1: Guidelines for Locating Smoke Detectors and CO Detectors

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.

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 9.1m (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°C (100°F) or falls below 5°C (41°F).

Smoke detectors should 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 other governing 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 21 ft (6.4 m) of any door to a sleeping room, with 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.
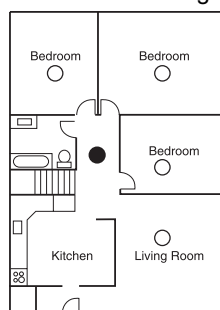6. In the living area(s) of a residential board and care occupancy (small facility).
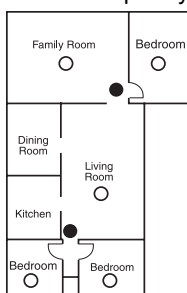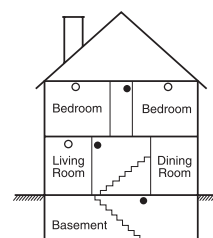

Figure 1

Figure 2

Figure 3

Figure 3a

○ Smoke detectors for better protection
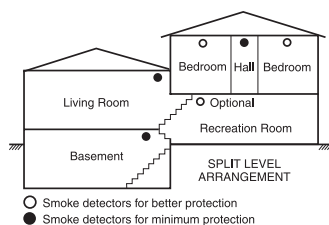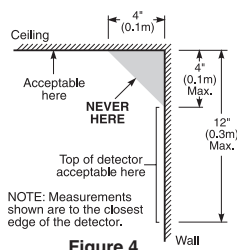● Smoke detectors for minimum protection

Figure 4

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 a potentially harmful level is reached. The human body is most vulnerable to the effects of CO gas during sleeping hours; therefore, CO detectors should be located in or as near as possible to sleeping areas of the home. For maximum protection, a CO alarm should be located outside primary sleeping areas or on each level of your home. Figure 5 indicates the suggested locations in the home.
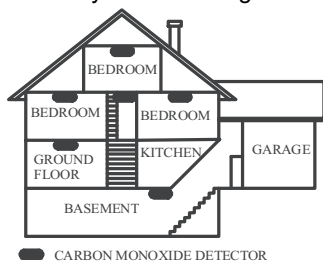
Figure 5

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10ºC or exceed 40ºC
- Near paint thinner fumes
- Within 5 feet (1.5m) 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; this will damage the detector

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

Household Fire Safety Audit

Read this section for important information about fire safety. Most fires occur in the home. To minimize this danger, we recommend that a household fire safety audit be conducted and a fire escape plan be developed.

1. Are all electrical appliances and outlets in a safe condition? Check for frayed cords, overloaded lighting circuits, etc. If you are uncertain about the condition of your electrical appliances or household service, have a professional evaluate these units.
2. Are all flammable liquids stored safely in closed containers in a well-ventilated cool area? Cleaning with flammable liquids should be avoided.
3. Are fire-hazardous materials (e.g., matches) well out of reach of children?
4. Are furnaces and wood-burning appliances properly installed, clean and in good working order? Have a professional evaluate these appliances.

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 neighbour'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.

Appendix 2: Regulatory Information

This product has been tested and found in compliance with the following standards:

- UL1023 Household Burglar-Alarm System Units
- UL985 Household Fire Warning System Units
- ULC-S545-02 Residential Fire Warning System Control Units
- ORD-C1023-1974 Household Burglar-Alarm System Units

This product has also been tested and found in compliance with the ANSI/SIA CP-01-2014 Control Panel Standard – Features for False Alarm Reduction.

This product is UL/ULC listed under the following categories:

- UTOU/UTOUC Control Units and Accessories, Household System Type
- NBSX/NBSXC Household Burglar Alarm System Units
- AMTB Control Panels, SIA False Alarm Reduction

The product is labeled with the UL and ULC listing marks along with the SIA CP-01 compliance statement (Also Classified in accordance with SIA-CP-01 Standard) as proof of compliance with the above mentioned standards. For further information on this product's listings please also refer to the official listing guides published at the UL web site (www.ul.com) under Certifications Section.

UL/ULC Residential Fire and Burglary Installations:

For ULC Installations refer to the Standard for the Installation of Residential Fire Warning Systems, CAN/ULC-S540.

- Use at least one PG9916 or PG9926 Smoke Detector for Fire Installations (refer to Installer portal > Panel Settings> Zones> Add Device (Enter Device Serial # or Auto Enroll) > Type >Standard Fire)
- The entry delay shall not exceed 60 seconds (refer to Installer portal > Panel Settings>Panel Configuration>Partition Configuration> Entry Delay 1)
- The exit delay shall not exceed 120 seconds (refer to Installer portal > Panel Settings>Panel Configuration>Partition Configuration> Exit Delay)
- The minimum Bell Time-out is 4 minutes (refer to Installer portal > Panel Settings>Panel Configuration>System Configuration> Burglary Bell Time-out)

Note: For ULC Residential Fire Installations the minimum Bell Time-out is 5 minutes

- Temporal Three Fire Signal shall be enabled (hardcoded ON)
- Arm/Disarm Bell Squawk shall be enabled when using wireless key PG9929, PG9939 or PG9949 (refer to Installer portal > Panel Settings>Panel Configuration>System Configuration> > Local arm shall be ON)
- A code shall be required for bypassing (refer to Installer portal >Panel Settings>Panel Configuration>System Configuration> Access Code Is Required for Bypassing)
- Trouble beeps shall be enabled (refer to Installer portal >Panel Settings>Panel Configuration>System Configuration> Trouble Beeps Auto Silence)

Note: This product is programmed to perform 5 attempts for communication of an event to the supervising station. If unsuccessful, a Fail To Communicate (FTC) trouble is generated.

- Test transmission cycle shall be set for monthly transmission (refer to Installer portal > Panel Settings>Panel Configuration>Comms Configuration> Ethernet Test Transmission Cycle & Cellular Test Transmission Cycle)
- For UL installations, 2 repeaters (model PG9920) must be used for proper signal routing.

Note: For ULC Residential installations set for daily test transmission

- Wireless Supervision window shall be enabled (refer to Installer portal > Account Details > Panel Configuration > Ethernet Supervision, Cellular Supervision)
- Wireless Supervision window shall be set to 4 hours for Fire Installations (refer to Installer portal > Panel Settings>Panel Configuration>Comms Configuration > Ethernet Supervision, Cellular Supervision)
- Wireless Supervision window shall be set to 24h for Burglary Installations only (refer to Installer portal > Panel Settings>Panel Configuration>Comms Configuration > Ethernet Supervision, Cellular Supervision)
- RF Jam detection shall be enabled (refer to Installer portal > Panel Settings>Panel Configuration>System Configuration> RF Jam Detection and Reporting)
- Bells will be active During 2-way Audio (refer to Installer portal > Panel Settings > Panel Configuration > System Configuration > Wireless Siren Control)
- New Alarms will Disconnect 2-way Audio (refer to Installer portal > Panel Settings > Panel Configuration > System Configuration > New Alarms Disconnect 2-way Audio for 2G)
- When the 2- way audio feature is enabled(refer to Installer portal > Panel Settings > Zones > 2-Way Audio) ensure that New alarms will not Disconnect 2-Way Audio is OFF and Wireless Siren During 2-Way Audio is ON

Programming

The notes in the programming sections describing the system configurations for UL/ULC listed installations shall be implemented.

Bell Location

The alarm sounding device (bell) shall be located where it can be heard by the person operating the security system during the daily arming and disarming cycle.

Casual Users

The installer should caution the user(s) not to give system information (e.g., codes, bypass methods, etc.) to casual users (baby-sitters or service people).

User Information

The installer should advise the users and note in the User's Manual:

- Service organization name and telephone number
- The programmed exit time
- The programmed entry time
- Test system weekly

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.

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)

This Class B digital apparatus complies with Canadian ICES-003. Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

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

FCC/ISED CANADA WIRELESS NOTICE

This equipment complies with FCC and ISED Canada radiation exposure limits set forth for an uncontrolled environment. The antenna should be installed and operated with minimum distance of 20 m between the radiator and your body. Antenna gain must be below:

Frequency band	3G7090
GSM 850 / FDD V	2.1 dBi
PCS 1900 / FDD II	3.7 dBi
Frequency band	LT7090
LTE B4 (1700 MHz)	1.5 dBi
LTE B13 (700 MHz)	2.2 dBi

This transmitter can be co-located or operating in conjunction with any other antenna or transmitter.

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

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.

NIST Validation of encryption algorithm AES128 certificate No. 4053

FCC/IC LABEL

The modular transmitter 3G7090 or LT7090 is labeled with its own FCC ID and IC number. When the module is installed inside the host device WS900-19 or WS900- 29 and the FCC ID/IC of the module is not visible, the host device displays the provided label referring to the FCC ID and IC of the enclosed module. This 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.

SIA False Alarm Reduction Installations: Quick Reference

Caution

Fire Alarm Verification feature (Auto Verified Fire Zone) is supported on the DSC Wireless Smoke Detector, Model PGx916 and PGx926. The fire alarm delay is 40s.

Notes:

Programming at installation may be subordinate to other UL requirements for the intended application.

Cross zones have the ability to individually protect the intended area (e.g. motion detectors which overlap).

Cross zoning is not recommended for line security Installations nor is to be implemented on exit/entry zones.

There is a communication delay of 30 seconds in this control panel. It can be removed, or it can be increased up to 45 seconds at the option of the end user by consulting with the installer.

The security system shall be installed with the sounding device activated and the communicator enabled for transmission using SIA or CID format.

SIA Feature Programming Section	Comments	Range/Default	Requirement
Exit Delay Panel Settings>Panel Configuration>Partition Configuration> Exit Delay (select 45s, 60s, 90s, or 2 min)	Access to Entry and Exit delays and Bell Time Out for the system	Range: 45- 120 sec. Default: 60 sec.	Required (programmable)
Exit Time Restart (hardcoded ON)	Enables the exit delay restart feature	Default: Enabled	Required
Auto Stay Arm on Un-vacated Premises Zones must be programmed as stay/Away	Function Key: Stay Arming. All Stay/Away type zones will be automatically bypassed	If no exit after full arm Default: Enabled	Required
Entry delay(s) Panel Settings>Panel Configuration>Partition Configuration > Entry Delay (select 30s, 45s, 60s, 2mins, 3mins or 4mins)	Access to Entry and Exit delays and Bell Time Out for the system Note: Combined Entry delay and Communications Delay (Abort Window) shall not exceed 60s	Range: 30 sec. to 4 min. Default: 30 sec.	Required (programmable)
Abort Window for Non-Fire zones	Transmission Delay zone attribute must be enabled	May be disabled by zone or zone type Default: Enabled	Required
Abort Window Time for Non-Fire zones Panel Settings>Panel Configuration>System Configuration > Communication Delay	Access to the programmable delay before communicating alarms Note: Combined Entry delay and Communications Delay (Abort Window) shall not exceed 60s	Range: up to 45 sec. Default: 30 sec.	Required (programmable)
Abort Annunciation	An audible tone is generated when an alarm is aborted during the Abort window	Annunciate that no alarm was transmitted Default: Enabled	Required
Communications Canceled Window Panel Settings>Panel Configuration>System Configuration>Communication Cancel Window	Access to the programmable Cancel Window.	Range: minimum 5 min. Default: 5 min. Note: minimum 5 min. for UL installations	Required

SIA Feature Programming Section	Comments	Range/Default	Requirement
Cancel Annunciation Panel Settings>Panel Con-figuration>System Configuration>> Reporting	Access to the reporting code for Alarm Canceled	Annunciate that a Cancel was transmitted. Default: Enabled	Required
Duress Feature	Do not derive code from an existing Master/User code (e.g., Master code is 1234, the duress code should not be 1233 or 1235)	No automatic derivative of another user code. No duplicates with other user codes Default: Disabled	Allowed
Cross Zone Timer Panel Settings>Panel Con-figuration>Partition Configuration>Cross Zone Delay	Access to the programmable Cross Zone timer	May program Range: 001-255 seconds. Default: 0 seconds	Allowed
Swinger Shutdown for Alarms Panel Settings>Zones> Swinger Shutdown	Access to the swinger shutdown limit for zone alarms.	For all non-fire zones shut-down at 1 or 6 trips Default: 2 trips	Required (programmable)
24 hour auto verified Fire	Access to 24 hour auto verified Fire	Activates If a restore is Not received within the spe-cified time Default: dis-abled	Required

System Test: Panel Settings> Dia-gnostics> Sys-tem>System Test	The system activates all keypad sounders, bells or sirens for 2 seconds and all keypad lights turn on. Refer to the User Manual.
Panel Settings> Dia-gnostics> System> Device> Begin Walk Test	This mode is used to test each zone on the system for proper functionality.

Appendix 3: EULA

IMPORTANT - READ CAREFULLY: DSC Software purchased with or without Products and Components is copyrighted and is purchased under the following license terms:

This End-User License Agreement ("EULA") is a legal agreement between You (the company, individual or entity who acquired the Software and any related Hardware) and Digital Security Controls, a division of Tyco Safety Products Canada Ltd. ("DSC"), the manufacturer of the integrated security systems and the developer of the software and any related products or components ("HARDWARE") which You acquired.

If the DSC software product ("SOFTWARE PRODUCT" or "SOFTWARE") is intended to be accompanied by HARDWARE, and is NOT accompanied by new HARDWARE, You may not use, copy or install the SOFTWARE PRODUCT. The SOFTWARE PRODUCT includes computer software, and may include associated media, printed materials, and "online" or electronic documentation.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to You under the terms of that license agreement.

By installing, copying, downloading, storing, accessing or otherwise using the SOFTWARE PRODUCT, You agree unconditionally to be bound by the terms of this EULA, even if this EULA is deemed to be a modification of any previous arrangement or contract. If You do not agree to the terms of this EULA, DSC is unwilling to license the SOFTWARE PRODUCT to You, and You have no right to use it.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE This EULA grants You the following rights:

Software Installation and Use - For each license You acquire, You may have only one copy of the SOFTWARE PRODUCT installed.

Storage/Network Use - The SOFTWARE PRODUCT may not be installed, accessed, displayed, run, shared or used concurrently on or from different computers, including a workstation, terminal or other digital electronic device ("Device"). In other words, if You have several workstations, You will have to acquire a license for each workstation where the SOFTWARE will be used.

Backup Copy - You may make back-up copies of the SOFTWARE PRODUCT, but You may only have one copy per license installed at any given time. You may use the back-up copy solely for archival purposes. Except as expressly provided in this EULA, You may not otherwise make copies of the SOFTWARE PRODUCT, including the printed materials accompanying the SOFTWARE.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Limitations on Reverse Engineering, Decompilation and Disassembly - You may not reverse engineer, decompile, or disassemble the SOFTWARE PRODUCT, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to the Software, without the written permission of an officer of DSC. You may not remove any proprietary notices, marks or labels from the Software Product. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA.

Separation of Components - The SOFTWARE PRODUCT is licensed as a single product. Its component parts may not be separated for use on more than one HARDWARE unit.

Single INTEGRATED PRODUCT - If You acquired this SOFTWARE with HARDWARE, then the SOFTWARE PRODUCT is licensed with the HARDWARE as a single integrated product. In this case, the SOFTWARE PRODUCT may only be used with the HARDWARE as set forth in this EULA.

Rental - You may not rent, lease or lend the SOFTWARE PRODUCT. You may not make it available to others or post it on a server or web site.

Software Product Transfer - You may transfer all of Your rights under this EULA only as part of a permanent sale or transfer of the HARDWARE, provided You retain no copies, You transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades and this EULA), and provided the recipient agrees to the terms of this EULA. If the SOFTWARE PRODUCT is an upgrade, any transfer must also include all prior versions of the SOFTWARE PRODUCT.

Termination - Without prejudice to any other rights, DSC may terminate this EULA if You fail to comply with the terms and conditions of this EULA. In such event, You must destroy all copies of the SOFTWARE PRODUCT and all of its component parts.

Trademarks - This EULA does not grant You any rights in connection with any trademarks or service marks of DSC or its suppliers.

3. COPYRIGHT

All title and intellectual property rights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, and text incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT, are owned by DSC or its suppliers. You may not copy the printed materials accompanying the SOFTWARE PRODUCT. All title and intellectual property rights in and to the content which may be accessed through use of the SOFTWARE PRODUCT are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This

EULA grants You no rights to use such content. All rights not expressly granted under this EULA are reserved by DSC and its suppliers.

EXPORT RESTRICTIONS - You agree that You will not export or re-export the SOFTWARE PRODUCT to any country, person, or entity subject to Canadian export restrictions.

CHOICE OF LAW - This Software License Agreement is governed by the laws of the Province of Ontario, Canada.

ARBITRATION - All disputes arising in connection with this Agreement shall be determined by final and binding arbitration in accordance with the Arbitration Act, and the parties agree to be bound by the arbitrator's decision. The place of arbitration shall be Toronto, Canada, and the language of the arbitration shall be English.

LIMITED WARRANTY

NO WARRANTY - DSC PROVIDES THE SOFTWARE "AS IS" WITHOUT WARRANTY. DSC DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

CHANGES IN OPERATING ENVIRONMENT - DSC shall not be responsible for problems caused by changes in the operating characteristics of the HARDWARE, or for problems in the interaction of the SOFTWARE PRODUCT with non-DSC-SOFTWARE or HARDWARE PRODUCTS.

LIMITATION OF LIABILITY; WARRANTY REFLECTS ALLOCATION OF RISK - IN ANY EVENT, IF ANY STATUTE IMPLIES WARRANTIES OR CONDITIONS NOT STATED IN THIS LICENSE AGREEMENT, DSC'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS LICENSE AGREEMENT SHALL BE LIMITED TO THE GREATER OF THE AMOUNT ACTUALLY PAID BY YOU TO LICENSE THE SOFTWARE PRODUCT AND FIVE CANADIAN DOLLARS (CAD$5.00). BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

DISCLAIMER OF WARRANTIES - THIS WARRANTY CONTAINS THE ENTIRE WARRANTY AND SHALL BE IN LIEU OF ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED (INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE) AND OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF DSC. DSC MAKES NO OTHER WARRANTIES. DSC NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MOD8IFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE PRODUCT.

EXCLUSIVE REMEDY AND LIMITATION OF WARRANTY - UNDER NO CIRCUMSTANCES SHALL DSC BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL THEORY. SUCH DAMAGES INCLUDE, BUT ARE NOT LIMITED TO, LOSS OF PROFITS, LOSS OF THE SOFTWARE PRODUCT OR ANY ASSOCIATED EQUIPMENT, COST OF CAPITAL, COST OF SUBSTITUTE OR REPLACEMENT EQUIPMENT, FACILITIES OR SERVICES, DOWN TIME, PURCHASERS TIME, THE CLAIMS OF THIRD PARTIES, INCLUDING CUSTOMERS, AND INJURY TO PROPERTY.

DSC recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this SOFTWARE PRODUCT to fail to perform as expected.

Appendix 4: Limited Warranty

Digital Security Controls warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Digital Security Controls shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original purchaser must promptly notify Digital Security Controls in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period. There is absolutely no warranty on software and all software products are sold as a user license under the terms of the software license agreement included with the product. The Customer assumes all responsibility for the proper selection, installation, operation and maintenance of any products purchased from DSC. Custom products are only warranted to the extent that they do not function upon delivery. In such cases, DSC can replace or credit at its option.

International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Digital Security Controls shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of Digital Security Controls such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- damage caused by peripherals (unless such peripherals were supplied by Digital Security Controls);
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the products for purposes other than those for which it was designed;
- damage from improper maintenance;
- damage arising out of any other abuse, mishandling or improper application of the products.

Items Not Covered by Warranty

In addition to the items which void the Warranty, the following items shall not be covered by Warranty: (i) freight cost to the repair centre; (ii) products which are not identified with DSC's product label and lot number or serial number; (iii) products disassembled or repaired in such a manner as to adversely affect performance or prevent adequate inspection or testing to verify any warranty claim. Access cards or tags returned for replacement under warranty will be credited or replaced at DSC's option. Products not covered by this warranty, or otherwise out of warranty due to age, misuse, or damage shall be evaluated, and a repair estimate shall be provided. No repair work will be performed until a valid purchase order is received from the Customer and a Return Merchandise Authorisation number (RMA) is issued by DSC's Customer Service.

Digital Security Controls's liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty. Under no circumstances shall Digital Security Controls be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property. The laws of some jurisdictions limit or do not allow the disclaimer of consequential damages. If the laws of such a jurisdiction apply to any claim by or against DSC, the limitations and disclaimers contained here shall be to the greatest extent permitted by law. Some states do not allow the exclusion or limitation of incidental or consequential damages, so that the above may not apply to you.

Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) And of all other obligations or liabilities on the part of Digital Security Controls Digital Security Controls neither assumes responsibility for, nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

Digital Security Controls recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs

Digital Security Controls will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Digital Security Controls must first obtain an authorization number. Digital Security Controls will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Digital Security Controls determines to be repairable will be repaired and returned. A set fee which Digital Security Controls has predetermined and which may be revised from time to time, will be charged for each unit repaired.

Products which Digital Security Controls determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

WARNING: Installer please read carefully

Note to Installers

The warnings on this page contain vital information. As the only individual in contact with system users, it is the installer's responsibility to bring each item in this warning to the attention of all users of this system.

System Failures

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some, but not all, of the reasons may be:

Access by Intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a warning device, or interfere with or prevent the proper operation of the system.

Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

Compromise of Radio Frequency (Wireless) Devices

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent radio signal interference.

Criminal Knowledge

This system contains security features which were known to be effective at the time of manufacture. It is possible for persons with criminal intent to develop techniques which reduce the effectiveness of these features. It is important that your security system be reviewed periodically to ensure that its features remain effective and that it is updated or replaced if it is found that it does not provide the protection expected.

Failure of Replaceable Batteries

This system's wireless transmitters have been designed to provide several years of battery life under normal conditions. The expected battery life is a function of the device environment, usage, and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

Inadequate Installation

A security system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a security professional to ensure that all access points and areas are covered. Locks and latches on windows and doors must be secure and operate as intended. Windows, doors, walls, ceilings and other building materials must be of sufficient strength and construction to provide the level of protection expected. A reevaluation must be done during and after any construction activity. An evaluation by the fire and/or police department is highly recommended if this service is available.

Inadequate Testing

Most problems that would prevent an alarm system from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an earthquake, an accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices, and any other operational devices that are part of the system.

Insufficient Time

There may be circumstances when the system will operate as intended, yet the occupants will not be protected from an emergency due to their inability to respond to the warnings in a timely manner. If the system is remotely monitored, the response may not occur in time to protect the occupants or their belongings.

Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beams. They cannot detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbecues, fireplaces, sunlight, steam vents, lighting and so on.

Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be charged, in good condition and installed correctly. If a device operates only by AC power, any interruption, however brief, will render that device inoperative while it does not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment such as a security system. After a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

Security and Insurance

Regardless of its capabilities, an alarm system is not a substitute for property or life insurance. An alarm system also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation.

Smoke Detectors

Smoke detectors that are a part of this system may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls or roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke produced and the rate of burning. Smoke detectors cannot sense all types of fires equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

Warning Devices

Warning devices such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. If warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened. Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners, other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

SIMPLIFIED EU 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: WS900-19, WS900-29, 3G7090, LT7090 (used in North America only), WS901-14, WS901-24EU, WS901-18, WS901-28, WS911-18, WS911-28, 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
Product specifications:

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

European single point of contact
Tyco Safety Products, Voltaweg 20, 6101 XK Echt, Netherlands

The WS912-28 Control Panel with 3G7090E-EU cellular communicator has been certified by Telefication according to EN50131-1:2006+A1:2009+ A2:2017, EN50131-3:2009, EN50131-4: 2008, EN50131-10: 2014, EN50131-6:2017 (Type A) and EN50136-1:2012 (SP2,DP2) for Grade 2, Class II. For EN50131 compliant installations, with alarm control panels WS912-28 only the intrusion portion of the alarm system may be activated.

The Tyco cloud collects 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.

29010132R001