

iotega Wireless Security and Automation System

V1.2 Reference Manual



Models:
WS900^{UL}/WS901



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

Section 1: Introduction	2
1.1 About the System	2
1.1.1 Available Models	2
1.2 Compatible Devices List	2
1.3 Specifications	4
Section 2: Installation	6
2.1 Alarm Controller Installation	6
2.2 Controls and Indicators	8
2.3 Enrolling Wireless PowerG Security Devices	10
Section 3: Operation	12
3.1 Using the Integrated Keypad	12
3.1.1 Key Functions	12
3.1.2 Emergency Keys	12
3.1.3 WPS Mode ([*][8])	13
3.1.4 Local Webpage ([*][8])	13
3.2 Arming and Disarming Methods	13
3.2.1 Away Arming	13
3.2.2 Stay Arming	13
3.2.3 Quick Arming	14
3.2.4 Disarming	14
Section 4: Programming Options	15
4.1 Integrated Keypad Options	15
4.2 System Configuration Options	15
4.2.1 Reporting Configuration Options	19
4.2.2 Network Configuration Options	20
4.3 Central Monitoring Station Programming Options	21
4.3.1 Other Communicator Related Options	24
4.4 2-Way Voice Options	25
4.5 Partition Configuration Options	25
4.6 Wireless Device Configuration Options	27
4.6.1 Wirefree Keypad Configuration Options	27
4.6.2 User Configuration Options	28
4.6.3 Wireless Siren Configuration Options	29
4.6.4 Wireless Key Configuration Options	30
4.6.5 Wireless Smoke and CO Configuration Options	30
4.6.6 Wireless Glassbreak Configuration Options	31
4.6.7 Wireless Temperature Configuration Options	31
4.6.8 Wireless Flood Configurations	32
4.6.9 Wireless PIR CAM Configurations	33
4.6.10 Wireless PIR (NO CAM) Configurations	34
4.6.11 Wireless Door Window Configurations	35
4.6.12 Wireless Shock Sensor Configurations	36
4.6.13 Repeater Configuration Options	37
4.7 Available Zone Types	38
4.8 Available Zone Attributes	39
4.9 Diagnostics - Read Only	39
4.10 System Control	40
4.10.1 Network	40
Section 5: Troubleshooting	41
5.1 Testing	41
5.2 Viewing Troubles from the Integrated Keypad	41

5.3 Network Troubleshooting	43
Appendix 1: Guidelines for Locating Smoke Detectors and CO Detectors	44
Appendix 2: Reporting Codes	47
Appendix 3: Regulatory Information	52
5.4 SIA False Alarm Reduction Installations: Quick Reference	54

Safety Instructions for Skilled Persons

Follow all warnings and Instructions specified within this document and/or on the equipment.

IMPORTANT! Save these instructions for future reference. Inform the end-user of the safety precautions that must be observed when operating this equipment.

Before Installing

Ensure your package includes the following items:

- Installation and User manuals
- iotege alarm controller with mounting plate
- Ethernet cable
- Mounting hardware

SAFETY Precautions Required During Installation

Do not touch the equipment and its connected cables during an electrical storm; there may be a risk of electric shock.

Never touch uninsulated wires or terminals unless the equipment has been disconnected from the mains .

Position cables so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain.

Use authorized accessories only with this equipment

Do not place any object on the top of this equipment, it is not designed to support any supplementary weight

Do not spill any liquids on this equipment.

Do not attempt to service this product yourself. Opening or removing the cover may expose you to dangerous voltage or other risk. Refer servicing to skilled persons

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 48 for information on locating smoke and CO detectors.

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@tyco-securityproducts.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.

Data Collection Statement

The Tyco cloud collects Data from the iotege panel (public IP address, security events and statuses, security configuration, and system diagnostics) in order to improve system

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.

1.1.1 Available Models

The following alarm controller models are available:

Model	PowerG (MHz)	Wi-Fi (GHz)**	Z-Wave (MHz)*	2-Way Audio*
WS900-19 ^{UL}	912-919	2.4	No	Yes
WS900-29 ^{UL}	912-919	2.4	908.4	Yes
WS901-14	433	2.4	No	No
WS901-24EU	433	2.4	868.4	No
WS901-18	868	2.4	No	No
WS901-28	868	2.4	868.4	No

*Not evaluated by UL

** 802.11b/g/n

Note: Only models with ^{UL} designation are UL/ULC listed.

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, 8 = 868MHz, 9 = 912-919MHz

Product Type	Model
Modules	
Touchscreen Keypad*	WS9TCHW
Wirefree LCD Keypad	WS9LCDWF
Cellular Communicator	LT7090, 3G7090, 3G7090-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 smoke and heat detector	PGx936 ^{UL}
Wireless CO detector	PGx913 ^{UL}
Wireless CO detector	PGx933 ^{UL}
PIR/Pet Immune Motion Detector	PGx914
Wireless PIR motion detector	PGx904(P) ^{UL}

Product Type		Model
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**}
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		
These supplementary devices have not been evaluated by UL/ULC for compatibility with the alarm control panel.		
Camera	Wi-Fi IP Camera	See the Smarttech portal for available models
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.		
Note: These supplementary devices have not been evaluated by UL/ULC for compatibility with the alarm control panel.		
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

* Touchscreen device not evaluated by UL/ULC

**These devices shall not be used in UL/ULC listed installations.

1.3 Specifications

Zone Configuration

- 128 wireless zones
- 19 zone types and 4 programmable zone attributes
- 4 touchscreen keypads supported (not evaluated by UL/ULC)
- 4 wirefree keypads (not evaluated by UL/ULC)
- 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

- 100 access codes are available, including 99 for standard users and one for the system master user. One installer code is also provided for the panel, as well as one duress code per partition.
- 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 (Note: This battery pack shall not be used with UL/ULC Household Fire Alarm Signaling system)
- Backup time: 4 hours
- Recharging time to 85%: 24 hours (UL)
- 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 (UL)
- 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*
- Audio verification*
- 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. Install the hardware
2. Create an account for the panel
3. Assign a service plan
4. Add a gateway
5. Create a master contact
6. Enroll sensors and other devices
7. Select Go Live on the Accounts: Summary page to bring the iotega online.
8. Test panel operation

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.
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 8.

Note: The following UDP ports must be open: 1234, 1235, and 1236. If the problem persists, contact technical support.

Figure 2-1 Panel Connections

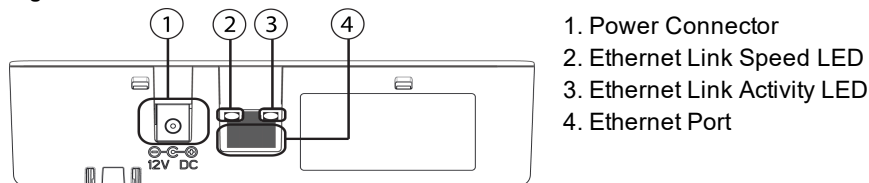
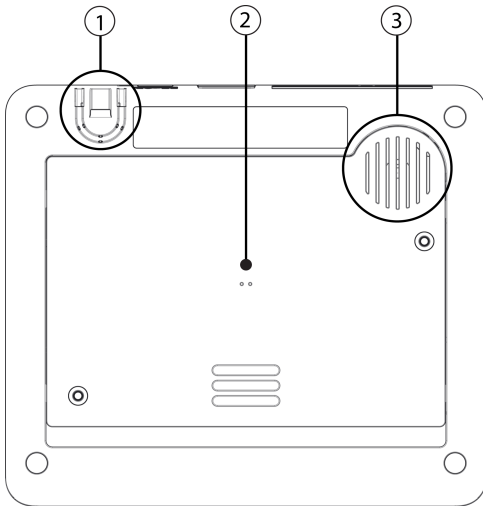
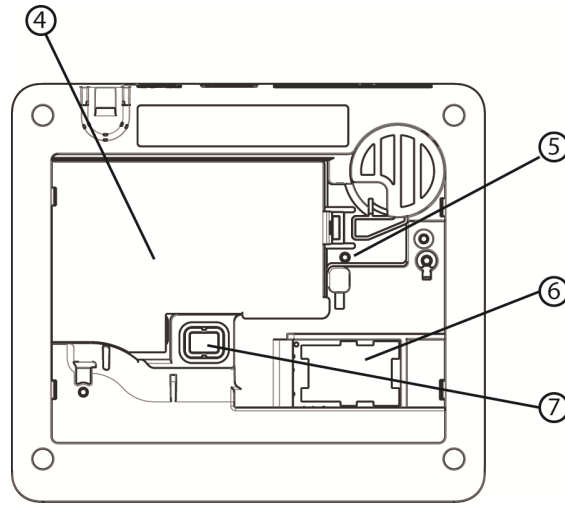


Figure 2-2 Panel Bottom



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

Figure 2-3 Battery Compartment

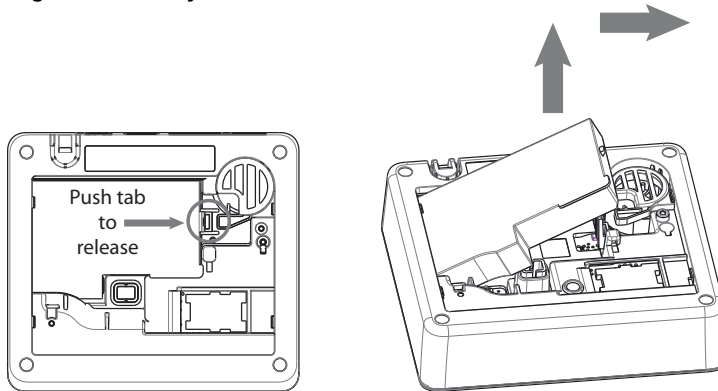


4. Battery
5. Reset button
6. SIM card
7. Tamper switch

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



Installing a new battery

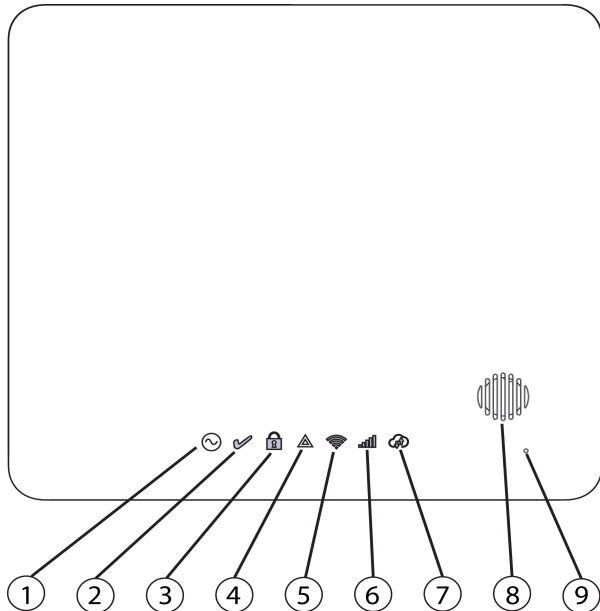
1. Remove the access cover from the back of the panel.
2. Insert the battery, back end first, as shown in Figure 2-4 .
3. Press the front of the battery down until the retention tab clicks into place.
4. Replace the back cover of the panel.

Note: When replacing the battery, use battery pack suitable for the application. Refer to on page 4.

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]	- The system is ready to arm, but Force Arm capable zones are open. - 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)

LED	Indicator	Description
 Remote Connection 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
	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 performs a vendor reset. WiFi configurations (client mode) are returned to default settings.

Pressing and holding the Reset button for a minimum of 20 seconds returns the following options to their default settings: SSID, security key, security type and reconnection to DHCP.

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 disarmed, 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 tamper 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.

Wireless devices are enrolled using one of the following methods:

- Manually entering a device-specific serial number then configuring the available options.
- Using auto enrollment.

To auto enroll:

1. Enable auto enroll using the installer portal.
2. Power up the wireless device and press the Enroll button until the on-board LED lights steady. The serial number is displayed.
3. Confirm you want to enroll the device then configure the available options.
4. Submit the settings to finish enrollment.
5. Continue the above process until all devices are enrolled.

To manually enroll:

1. Enable manual enrollment using the installer portal or app
2. Add the device zone type, partition, name, and electronic serial number (ESN).
3. When on site, power up the device. Note that some devices need to be tampered to complete enrollment. Refer to the installation instructions provided with the device for more information.

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.

Section 2: Installation

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.

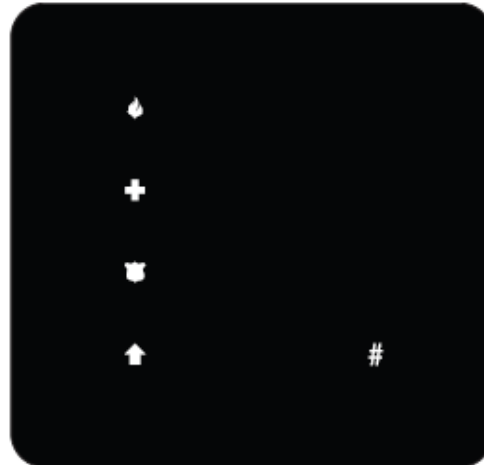
3.1 Using the Integrated Keypad

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 and return to previous screen Long press to switch partitions
*	[*] 2 for Troubles, see "Viewing Troubles from the Integrated Keypad" on page 41. [*] 8 to enable WiFi access point (to add IP devices, i.e., touchscreen keypad). See "WPS Mode ([*]8)" for more information.
↑	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 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 keypad.
 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.

3.1.4 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 keypad.
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 26.

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 Lockout Attempt

Keypad Lockout is a security measure designed to prevent unauthorized attempts to access the security system by limiting the number of attempts to enter a valid access code. Once the maximum number of attempts is reached, no functions can be performed on the keypad for 5 minutes (Lockout Duration).

If the maximum number of invalid attempts is not reached within one hour, or if a valid access code is entered, the counter is reset.

Default:	0 (disabled)
Valid range:	0 to 255

Keypad Partition Assignment

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

Default:	1
Valid range:	1-4

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 tone ranges from lowest (1) to highest (15). Programming (0) turns off the buzzer.

Note: Internal buzzer tone shall be at maximum setting for UL/ULC.

Default:	7
Valid range:	0-15

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

Ready LED Flashes for Force Arm

When this option is enabled, the keypad Ready LED flashes to indicate that a force arm zone is open but the system is still ready to be armed.

When this option is disabled, the keypad Ready LED operates as normal. It does not provide an indication of the open force arm zone.

Default:	Enabled
Valid range:	Enabled/Disabled

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 FFFFFFFF (Hexadecimal)

Event Reporting Format

This programming option is used to assign a communicator format for transmitting zone alarms, tampers, faults and other signals to the central monitoring station.

The following communicator formats are available:

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.

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.

Default:	SIA
Valid range:	SIA, CID

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 (Note: Burglary Bell Time-out shall be 4 minutes for UL/ULC)
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 (Note: Fire Bell Time-out shall be 5 minutes for UL/ULC)
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

Installer Access Window Permission

When this option is enabled, the installer is given access to the panel's programming sections for a 6-hour window, or until the install has been finalized.

When this option is disabled, the installer can access the panel's programming sections at any time.

This option is controlled by Level 1 users.

Default:	Enabled
Valid range:	Enabled, Disabled

Ethernet IP Address

This is the resolved value based on the DHCP address assignment.

Default:	000.000.000.000
Valid range:	Read-only

Ethernet IP Subnet

This is the resolved value based on the DHCP address assignment.

Default:	255.255.255.000
Valid range:	Read-only

Gateway IP Address

This is the resolved value based on the DHCP address assignment.

Default:	000.000.000.000
Valid range:	Read-only

DNS 1 IP Address

This is the resolved value based on the DHCP address assignment.

Default:	000.000.000.000
Valid range:	Read-only

DNS 2 IP Address

This is the resolved value based on the DHCP address assignment.

Default:	000.000.000.000
Valid range:	Read-only

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 (Note: Access Code Required to View/Silence Trouble shall be enabled for UL/ULC applications)
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

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 communication 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:	5 Minutes (UL/ULC) 0 Minutes (Standard)
Valid range:	5 to 255 Minutes (UL/ULC) 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:	002 (UL/ULC) 003 (Standard)
Valid range:	001 to 006 (UL/ULC) 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:	030 Seconds (UL/ULC) 000 (Standard)
Valid range:	000 to 045 Seconds (UL/ULC) 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

New Alarms Disconnect 2-Way Audio

When this option is enabled, a listen in/2-way audio session in progress is disconnected in favor of the incoming alarm. This option is useful when using a 2G network, as voice (2-way audio) and data (alarm) sessions cannot take place at the same time.

Note: Fire/CO alarms override this option and force a disconnect (if necessary) in order to communicate the event.

When this option is disabled, new alarms do not disconnect 2-way audio. If a new alarm is generated during the first 70 seconds of the two-way voice interval, the monitoring station operator has 20 seconds to begin another two-way voice interval.

If the new alarm is generated during the last 20 seconds of the two-way voice interval, the monitoring station operator has the remainder of the interval to begin another two-way voice interval.

Default:	Disabled
Valid range:	Enabled/Disabled

4.2.1 Reporting Configuration Options**Open/Close**

When this option is enabled, the following open/close events are reported to the central monitoring station when they occur. When disabled, open/close events are not reported.

- Away Arming (Close)
- Stay Arming (Close)
- Disarm (Open)
- Special Closing
- Auto Arming
- No Activity Arming
- Auto Arm Cancel Postponed

Default:	Enabled
Valid range:	Enabled/Disabled

Special Alarm Comms

When this option is enabled, the following special alarm events are reported to the central monitoring station when they occur. When disabled, special alarm events are not reported.

- Exit Error
- Recent Closing
- Local keypad Lockout
- Remote Lockout

Default:	Enabled
Valid range:	Enabled/Disabled

Maintenance

When this option is enabled, the following maintenance events are reported to the central monitoring station when they occur. When disabled, maintenance events are not reported.

- Event Buffer Full
- Close Delinquency
- Cold Start
- Installer Lead In/Out
- FW Update(Begin, Successful, Fail)

Default:	Enabled
Valid range:	Enabled/Disabled

System-Wide Troubles

When this option is enabled, the following system trouble events are reported to the central monitoring station when they occur. When disabled, system trouble events are not reported.

- AC Loss and restore
- Battery trouble and restore
- Tamper and restore
- Hardware fault and restore
- RF Jam trouble and restore
- RF Delinquency
- Loss of time trouble and restore
- Supervision trouble and restore
- Not networked trouble and restore
- Fire/CO trouble and restore
- Tamper trouble and restore
- Receiver not available trouble and restore
- FTC trouble and restore
- Receiver supervisiontrouble and restore
- Cellular trouble and restore
- Ethernet/WiFi trouble and restore
- Remote shutdown trouble and restore

Default:	Enabled
Valid range:	Enabled/Disabled

Alarms

The following alarm events are reported to the central monitoring station when they occur:

- Zone Alarm (including Heat/Freeze trouble)
- Alarm Cancel
- Duress Alarm
- Opening After Alarm
- Burglary Verified
- Burglary Not Verified
- Emergency Key Alarm
- Recent Closing

Default:	Enabled
Valid range:	Read-only

Alarm Restoral

When this option is enabled, the following alarm restoral events are reported to the central monitoring station when they occur. When disabled, alarm restoral events are not reported.

- Zone Alarm Restore
- Emergency Key Restore

Default:	Enabled
Valid range:	Enabled/Disabled

Test

When this option is enabled, the following test events are reported to the central monitoring station when they occur. When disabled, test events are not reported.

- System Test
- Installer Walk Test (Begin/End)

Default:	Enabled
Valid range:	Enabled/Disabled

Bypass

When this option is enabled, the following bypass events are reported to the central monitoring station when they occur. When disabled, bypass events are not reported.

- Bypass/Unbypass
- Partial Closing
 - Manually Bypassed Zones
 - Stay Zones
 - Force Arm Zones

Default:	Enabled
Valid range:	Enabled/Disabled

Periodic Test Transmissions

When this option is enabled, the following test transmission events are reported to the central monitoring station when they occur. When disabled, test transmission events are not reported.

- Periodic Test
- Periodic Test with Trouble

Default:	Enabled
Valid range:	Enabled/Disabled

4.2.2 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: Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems

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: Domain Name Service (DNS) programming is not permitted in UL/ULC listed systems

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

WiFi Country Code

This option is used to select the country of operation for the alarm system.

Default:	CA (Canada)
Valid range:	US, AU, CA, UK, FR, SE, IL, None

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 MIXED MODE TKIP MIXED MODE AES MIXED MODE TKIP AES

WLAN Security Key

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

Default:	None
Valid range:	32 character ASCII

Panel's Cellular Public APN

This section is used to program the Access Point Name of the network used for cellular-data connectivity.

Default:	Blank
Valid range:	32 ASCII characters or Null

Panel's Cellular Login User Name

This section is used to program a user name for cellular network connection.

Default:	Blank
Valid range:	32 ASCII characters or Null

Panel's Cellular Login Password

This section is used to program a user password for cellular network connection.

Default:	Blank
Valid range:	32 ASCII characters or Null

Time Zone

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

From the list of valid entries, locate and select the appropriate time zone.

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

4.3 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:

None: The system does not communicate to the central monitoring station via Ethernet or Cellular.

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

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:	None, Ethernet, Cellular, Ethernet and Cellular

CMS Ethernet 1 Account Code

This option is used to program an account code used by the central monitoring station to identify the ethernet transmitter. Programming all 0's or all F's causes a module configuration trouble.

Note: If both Ethernet Receiver 1 and Cellular Receiver 1 are the same receiver (IP and port number are identical), Ethernet Receiver 1 account is used for Ethernet and Cellular.

Note: An Ethernet account code is necessary in order for the iotega to communicate to the central monitoring station (if Ethernet communication path is selected).

Default:	0000000000
Valid range:	0000000000 to FFFFFFFF

CMS Ethernet 1 DNIS

The Dialed Number Information Service (DNIS) is used in addition to the account code to identify the communicator module at the central monitoring station.

Default:	000000
Valid range:	000000 to 0FFFFFF (first digit not used)

CMS Ethernet 1 IP Address

This option is used to program an IP address for the Ethernet receiver. When a valid IP address has been programmed, Ethernet receiver 1 is enabled and will communicate events over the Ethernet channel.

Ethernet Receiver 1 and Cellular Receiver 1 may be configured to communicate to the same central monitoring station receiver. To configure the device to operate using this common receiver mode functionality, program Ethernet Receiver 1 and Cellular Receiver 1, IP address and port number with identical values.

Note: When operating in common receiver mode, Ethernet Receiver 1 account code is used for Ethernet and Cellular.

Default:	127.000.000.001
Valid range:	000.000.000.000 to 255.255.255.255

CMS Ethernet 1 Local Port

Use this section to set the value of the local outgoing port. Set the value of this port when the installation is located behind a firewall and must be assigned a particular port number as determined by the central monitoring station system administrator.

Note: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 local ports with the same value.

Default:	3060 (0BF4)
Valid range:	0000 to 65535

CMS Ethernet 1 Remote Port

This section is used to program the port number used by Ethernet 1. Set the value of this port when the installation is located behind a firewall, and must be assigned a particular port number as determined by the central monitoring station system administrator.

Default:	3061 (0BF5)
Valid range:	0000 to 65535

CMS Ethernet 1 Domain Name

This information is provided by the central monitoring station system administrator.

Default:	Blank
Valid range:	32 characters ASCII

CMS Ethernet 2 Account Code

The account code is used by the central monitoring station to distinguish between transmitters. Programming all 0's or all F's causes a module configuration trouble.

Note: If both Ethernet Receiver 2 and Cellular Receiver 1 are the same receiver (IP and port number are identical), Ethernet Receiver 2 account will be used for Ethernet and Cellular.

Note: An Ethernet account code is necessary in order for the iotega to communicate to the central monitoring station (if Ethernet communication path is selected).

Default:	0000000000
Valid range:	0000000000 to FFFFFFFF

CMS Ethernet 2 DNIS

The Dialed Number Information Service (DNIS) is used in addition to the account code to identify the communicator module at the central monitoring station.

Default:	000000
Valid range:	000000 to FFFFFF (first digit not used)

CMS Ethernet 2 IP Address

Enter the Ethernet receiver 2 IP address. This address will be provided by the central monitoring station system administrator. Programming the Ethernet Receiver 2 IP address with 000.000.000.000 will disable Ethernet reporting.

Note: When a valid IP address has been programmed, Ethernet Receiver 2 is enabled and will communicate events over the Ethernet channel.

Ethernet Receiver 2 and Cellular Receiver 2 may be configured to communicate to the same central monitoring station receiver. To configure the device to operate using this common receiver mode functionality, program the Ethernet Receiver 2 and Cellular Receiver 2 IP address and port number with the same values. When operating in common receiver mode the Ethernet Receiver 2 account code will be used for communications over Ethernet and Cellular.

Note: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 to communicate to same receiver.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

CMS Ethernet 2 Local Port

Use this section to set the value of the local outgoing port. Set the value of this port when the installation is located behind a firewall and must be assigned a particular port number as determined by the central monitoring station system administrator.

Change the default value of this port when the installation is located behind a firewall and must be assigned a particular port number as determined by the central monitoring station system administrator.

Note: Do not program Ethernet Receiver 1 and Ethernet Receiver 2 local ports with the same value.

Default:	0000 to 65535
Valid range:	0000000000 to FFFFFFFF

CMS Ethernet 2 Remote Port

This section is used to program the port number used by Ethernet 1. Set the value of this port when the installation is located behind a firewall, and must be assigned a particular port number as determined by the central monitoring station system administrator.

Default:	3061 (0BF5)
Valid range:	0000 to 65535

CMS Ethernet 2 Domain Name

This information is provided by the central monitoring station system administrator.

Default:	Blank
Valid range:	32 characters ASCII

CMS Cellular 1 Account Code

The account code is used by the central monitoring station to distinguish between transmitters. Programming all 0's or all F's causes a module configuration Trouble.

A cellular account code is necessary in order for the iotega to communicate to the central monitoring station (if cellular communication path is selected).

Default:	0000000000
Valid range:	0000000000 to FFFFFFFF

CMS Cellular 1 DNIS

The DNIS is used in addition to the account code to identify the communicator module at the central monitoring station.

Default:	000000
Valid range:	000000 to 0FFFFF

CMS Cellular 1 IP Address

Enter the cellular receiver 1 IP address. This information will be provided by the central monitoring station system administrator.

Note: When a valid IP address has been entered, the cellular receiver is enabled and will communicate events over the cellular channel.

Default:	000.000.000.000
Valid range:	000.000.000.000 to 255.255.255.255

CMS Cellular 1 Remote Port

This section determines the port used by Cellular Receiver 1 for communication to the receiver.

Note: Programming this section with 0000 will disable the receiver.

Default:	3061 (0BF5)
Valid range:	0000 to 65535

CMS Cellular 1 APN

The Access Point Name (APN) determines the cellular network that the communicator will connect to. This information is available from the network carrier.

Note: When a SIM card with a custom APN is used, the unit will not have access to the Internet. DLS and remote flash can still be done if a valid public APN is programmed.

Default:	Blank
Valid range:	32 characters ASCII

CMS Cellular 1 Domain Name

This information is provided by the central monitoring station system administrator.

Default:	Blank
Valid range:	32 characters ASCII

CMS Cellular 2 Account Code

Default: 0 Not in valid range

Valid range: 0000000001 to FFFFFFFF

The account code is used by the central monitoring station to distinguish between different transmitters. This account code is used when transmitting signals to the central monitoring station receiver.

Note: Programming this section as all 0's or F's will cause a module configuration trouble (yellow LED = 12 flashes).

Note: A cellular account code is necessary in order for the iotega to communicate to the central monitoring station (if cellular communication path is selected).

Default:	0000000000
Valid range:	0000000000 to FFFFFFFF

CMS Cellular 2 DNIS

The DNIS is used in addition to the account code to identify the communicator module at the central monitoring station.

Default:	000000
Valid range:	000000 to 0FFFFF (first digit not used)

CMS Cellular 2 IP Address

Enter the Cellular receiver 2 IP address. This IP address will be provided by the central monitoring station.

Note: When a valid address has been entered, Cellular Receiver 2 is enabled and will communicate events over the cellular path.

Default:	000.000.000.000
Valid range:	000.000.000.000.to 255.255.255.255

CMS Cellular 2 Remote Port

Enter the cellular receiver 2 IP address. This IP address will be provided by the central monitoring station.

Note: When a valid address has been entered, cellular receiver 2 is enabled and will communicate events over the cellular path.

Default:	3061 (0BF5)
Valid range:	0000 to 65535

CMS Cellular 2 APN

The APN determines the cellular network that the communicator will connect to. This information is available from the network carrier.

Note: When a SIM card with a custom APN is used, the unit will not have access to the Internet. DLS and remote flash

can still be done if this option is programmed with a valid public APN.

Default:	Blank
Valid range:	32 characters ASCII

CMS Cellular 2 Domain Name

This information is provided by the central monitoring station system administrator.

Default:	Blank
Valid range:	32 characters ASCII

4.3.1 Other Communicator Related Options

Alternate Test Transmission

When this option is enabled, the test transmission alternates between primary and secondary receivers with each test transmission interval.

When disabled, the test transmission is sent to the programmed receivers, based on the settings of the periodic test transmission reporting codes.

Default:	Enabled
Valid range:	Enabled/Disabled

Ethernet Test Transmission Time

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

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

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

Ethernet Test Transmission Cycle

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

Default:	0 minutes. (Note: Test transmission shall be 24 hours for ULC and 7 days for UL)
Valid range:	000000 (disabled) to 999999 minutes.

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

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. (Note: When only cellular is used, test transmission shall be 24 hours for ULC and 7 days for UL.)
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.

Commercial Supervision

When this option is enabled, swap detection is provided on the supervisory packet. When disabled, only supervision of the communicator path to the receiver is provided.

Default:	Enabled
Valid range:	Enabled/Disabled

Ethernet Supervision Interval (Heartbeat)

This option is used to set the frequency (in seconds) when supervisory heartbeats are sent to the Ethernet receiver. If the programmed value is 000 seconds, supervision is disabled.

Note: Commercial Supervision must be enabled in order to test the communications path.

Default:	000
Valid range:	001 to 255 Seconds, 000 to Disable

Cellular Supervision Interval (Heartbeat)

This option is used to set the frequency (in seconds) when supervisory heartbeats are sent to the cellular receiver. If the programmed value is 000 seconds, supervision is disabled.

Note: Commercial Supervision must be enabled in order to test the communications path.

Default:	000
Valid range:	001 to 255 Seconds, 000 to Disable

CMS Event Heartbeat Interval

This option is used to program the periodic heartbeat interval between the alarm panel and the cellular communicator. The heartbeat is used to monitor for image/audio file requests.

Default:	15 Seconds, 0 to disable
Valid range:	000 to 255 Seconds

Communication Trouble Delay Time

This option is used to program the amount of time before the following troubles are transmitted to the central monitoring station:

- Ethernet trouble
- Cellular trouble
- Supervision trouble
- WIFI trouble

Default:	000
Valid range:	000 to 254 seconds, 000=Instant, 255=Disabled

Visual Verification

This feature enables the central monitoring station operator to view images captured via installed camera/motion detectors during an alarm.

Visual verification sessions are triggered by the following:

- Fire key
- Medical key
- Panic key
- Alarms detected by armed PIR cameras

Note: The microphone on the camera PIR can be disabled.

Default:	Enabled
Valid range:	Enabled/Disabled

Video on Demand

When this option is enabled, the central monitoring station can request a video image file from an installed camera/motion detector within 60 minutes of an alarm.

Default:	Enabled
Valid range:	Enabled/Disabled

Firmware update Over Cellular

Default: Disabled

Valid range: Enabled, Disabled

Enabled: Installers can perform remote firmware updates via cellular radio.

Disabled: Firmware updates cannot be performed via cellular radio.

4.4 2-Way Voice Options

Alternate Phone Number

This section is used to program the SIM phone number.

Default:	Blank or Auto-populated
Valid range:	32-Digit Phone Number

Two Way Voice

When this option is enabled, Talk/Listen-in capability for audio verification of alarms is available.

Default:	Disabled
Valid range:	Enabled/Disabled

Microphone Gain

This section is used to program the volume level of the built-in microphone. 001 is the lowest volume level. 000 disables the microphone.

Default:	001
Valid range:	000 to 255

Voice Volume

This option is used to program the volume level of the built-in speaker. 000 disables the speaker.

Default:	004
Valid range:	000 to 255

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. During exit delay, both the Ready and Armed LEDs illuminate. When the exit delay expires, both LEDs turn off.

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

Auto Arm

When this option is enabled, the iotega automatically arms in away mode (stay/away zones active) at a programmed time each day. The keypad emits three beeps to indicate the system is armed. All arming inhibit features such as latching tampers, AC inhibit, etc. also inhibit Auto Arming and send the Auto Arm Cancellation code.

Default:	Disabled
Valid range:	Enabled/Disabled

Auto Arming by Schedule

This option is used to program the time of day each alarm system partition automatically arms (in Away mode only). To program an auto-arm time, select a day of the week and then enter the time. At the programmed time, the keypad buzzers beep to warn that automatic arming is in progress. The siren also squawks once every 10 seconds during this warning period if programmed to do so. When the warning period is complete, the exit delay elapses and the system arms in away mode.

Default:	0000
Valid range:	0000 to 2359 (4-Digit HH:MM) for each day of the week

Auto Arm Postpone Timer (for schedule only)

This option is used to program a time delay before the Auto Arm sequence begins. Programming 0 cancels auto arming.

Default:	0 Minutes
Valid range:	0-255 minutes

No Activity Arm timer

This option is used to tell the iotega to arm in Away mode when no zone activity is detected during the programmed amount of time. The timer starts when a Delay type zone is restored.

Default:	0 Minutes (disables feature)
Valid range:	0 to 255 Minutes

Settle Delay

This timer enables a programmable, short duration bypass of all zones on the partition when arming. It allows motion detectors to restore when the system is armed to help prevent false alarms.

The typical value for this timer is 5 seconds, but can be increased if false alarms persist. Program 000 for no settle delay. The settle delay duration is programmed in seconds.

Default:	010
Valid range:	000 to 010 seconds

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

4.6 Wireless Device Configuration Options

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

4.6.1 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

Fire Button Options

When this option is enabled, pressing and holding the Fire [F] button on the wirefree keypad 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

When this option is selected, pressing and holding the Auxiliary [A] button on the wirefree keypad for 2 seconds sends an emergency alarm reporting code to the central monitoring station. When the emergency reporting code is

received at the central monitoring station, the keypad beeps 10 times.

Default:	Enabled
Valid range:	Enabled/Disabled

Panic Button

When this option is selected, pressing and holding the Panic [P] button for 2 seconds on the wirefree keypad 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 volume level of the keypad's internal buzzer. The volume ranges from lowest (1) to highest (15). Programming (0) turns off the buzzer.

Note: Internal buzzer volume shall be at maximum setting for UL/ULC.

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

12/24 Hour Clock

When this option is enabled, time is displayed in 24-hour clock format.

Default:	Disabled
Valid range:	Enabled/Disabled

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

Keypad Lockout Duration

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

Default:	5 Minutes
Valid range:	Read-only

4.6.2 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 or 6-digit code for accessing the panel. Each user requires a unique code. Duplicate codes are not permitted.

Default:	Blank
Valid range:	000000 to 999999

User Access Level

Each system user is assigned an access level that determines the features they can use. All codes are 4 or 6-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 such as buzzer tone and volume, display contrast and brightness
- Assign wireless keys to users

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
- Schedule auto arming
- Initiate firmware updates
- 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.

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

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.

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

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.

User Name (label)

This option is used to program a system user name.

Default:	Blank
Valid range:	32 character ASCII

User Enable (Locked)

This option is used to control access to the security system for the selected user. When enabled, the user can access all functionality available to their user level. When disabled, the user is locked out of the system.

Default:	Disabled
Valid range:	Enabled/Disabled

4.6.3 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 ASCII

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. (Note: UL/ULC installation use Medium setting.)
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

4.6.4 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

4.6.5 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 39 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

Interconnected Smoke Detector Operation

When a Fire zone goes into alarm, or when the [F] key is pressed, the sirens of all smoke detectors assigned to the affected partition are activated. Global fire alarms place all smoke detectors on the system into alarm.

Smoke detector alarms follows the Fire Bell Timeout setting of the panel.

4.6.6 Wireless Glassbreak Configuration Options

The following sections are used for programming glass-break 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:	Instant
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 39 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

4.6.7 Wireless Temperature Configuration Options

The following sections are used for programming wireless temperature sensors.

Note: Wireless temperature feature was not evaluated by UL/ULC.

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 39 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

4.6.8 Wireless Flood Configurations

The following sections are used for programming wireless flood sensors.

Note: Wireless Flood feature was not evaluated by UL/ULC.

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:	Instant
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

4.6.9 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:	Instant
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 39 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:	0
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

4.6.10 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 39 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. For UL/ULC installations, night mode is to be used to supplement protection of the detection area.

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

4.6.11 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:	Delay-1
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 39 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 simultaneously. However, the iotega treats both devices as the same zone. Disable the reed switch to have the hardwired device function 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

4.6.12 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 39 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 simultaneously. However, the iotega treats both devices as the same zone. Disable the reed switch to have the hardwired device function independently.

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

4.6.13 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

4.7 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.

4.8 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	When this attribute is enabled, an alarm activates the siren. When disabled, alarms are silent.
Bell Steady	When this attribute is enabled, siren output is steady when in alarm. When disabled, siren output pulses during an alarm.
Bypass Enable	When this attribute is enabled, the zone can be manually bypassed. When disabled, the zone cannot be bypassed.
Force Arm	When this attribute is enabled, the system can be armed with the zone open. The zone is temporarily bypassed and, when secured, is monitored by the system. Zones with this attribute disabled cannot be armed while the zone is open.
Swinger Shutdown	When enabled, 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. When disabled, all alarms are transmitted.
Two Way Audio	When this attribute is enabled, the panel is able to initiate a 2-way audio session. When not enabled, only the panel microphone turns on, initiating a listen-in only session. The speaker remains off.
Talk Listen	The central station operator and the end user can communicate through the panel's microphone and speaker.

4.9 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.

4.10 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.

4.10.1 Network

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 24.

Test transmission time and test transmission cycle can be programmed for both primary and secondary receivers. See "Central Monitoring Station Programming Options" on page 21 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 through 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 6-1 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	Future Use	
		02	Battery Trouble	1-128
		03	Tamper	1-128
		04	Fault (Supervision)	1-128
		05	Not Networked	1-128

Section 5: Troubleshooting

		06	Fire/CO Trouble	1-128
		07	RF Delinquency	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
		07	RF Delinquency	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
		07	RF Delinquency	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
		07	RF Delinquency	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	01	Receiver Unavailable	
		02	FTC Trouble	receiver 1-4
		03	Receiver Supervision Trouble	
		04	Cellular Trouble	
		05	Ehernet/WiFi Trouble	
		06	Remote Shutdown	

5.3 Network Troubleshooting

	Network Configuration	Connection Requirements	Comments
1	DHCP (default router settings)	None	Since the iotega can receive IP from the network and the network is not blocking any ports, DHCP must include the following items <ul style="list-style-type: none"> • IP • Subnet Mask • Gateway address • DNS Address
2	DHCP - MAC filtering enabled	Router must be programmed with iotega's MAC address	The MAC address of the iotega is listed on the label on the bottom of the panel.
3	DHCP - outbound port filtering	The router must have the required ports enabled for outbound traffic	Required ports: <ul style="list-style-type: none"> • FTP - 20/TCP/UDP • FTP - 21/TCP/UDP • DNS - 53/TCP/UDP • HTTP - 80/TCP (with the following sites allowed) <ul style="list-style-type: none"> www.johnsoncontrols.com www.tyco.com www.dsc.com www.amazon.com • NTP - 123/UDP • TycoOn - 443/UDP (configurable) • SecureNet - 1234/UDP • CMS - Programmable/UDP x2 Ethernet receivers
4	DHCP - with fixed IP address	Router must be programmed with iotega's MAC address	Router uses DHCP to assign a fixed IP address to the iotega based on the MAC address. This option may not be supported by all routers.
5	Static IP on unit (DHCP available)	The iotega can be configured for Static IP via the installer portal.	The iotega must be connected to the network with DHCP enabled. Once connected to the portal, a static IP can be assigned.
6	Static IP on unit (No DHCP - Ethernet/Wi-Fi only)	The iotega must be provisioned off-site.	iotega must be temporarily connected to a network with DHCP enabled. Once connected to the portal, a static IP can be assigned and the iotega taken to the site. Network setup details for the installation site are needed to assign a valid IP.
7	Static IP on unit (No DHCP - Ethernet/Wi-Fi only)	The iotega must be provisioned with a router between it and the customer network.	A router, with a static IP for the WAN interface, to the network is required. The LAN side must have DHCP. Connecting the IoTega to the LAN enables it to connect and route through to the servers. The Static IP can then be programmed and the unit reconnected directly to the customer network.
8	Static IP on unit (No DHCP - Ethernet/Wi-Fi and Cell backup)	The iotega must be configured off-site via Ethernet. Static IP is programmed via Cell once on-site.	Once the iotega is provisioned and cellular is active, the Static IP can be programmed via the cellular interface.
9	Wi-Fi only (Ethernet available during installation)	Ethernet is required for initial installation/configuration.	The iotega's Wi-Fi must be configured on the router/access point via Ethernet (or cellular after the initial installation is completed). After installation, Wi-Fi can be used by disconnecting Ethernet and placing the unit where desired.
10	Wi-Fi only (No Ethernet available during installation)	Ethernet is required to enable Wi-Fi setup	Same as setting up a Static IP, with no DHCP. Can be configured off-site if Wi-Fi information is known, or via another network interface such as a router and then placed back on Wi-Fi network.
11	Cellular only	Ethernet is required to enable Cellular setup	Same as setting up a Static IP, with no DHCP. Can be configured off-site if information is known.

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).

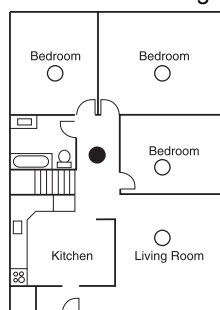


Figure 1

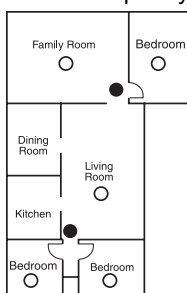


Figure 2

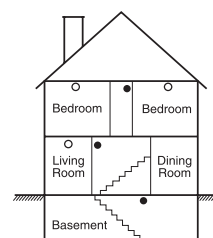


Figure 3

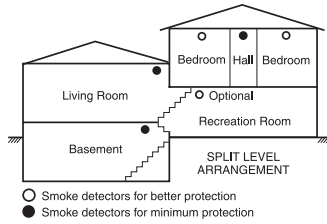


Figure 3a

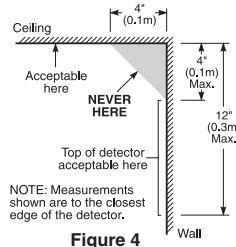


Figure 4

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.

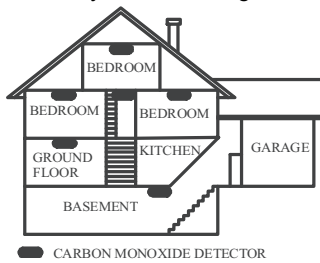


Figure 5

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10°C or exceed 40°C
- 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: 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 47 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**
Zone Events				
	Zone Alarms	A/R	see "Contact ID & SIA Zone Alarm/Restore Event Codes" on page 50" for details.	
	Zone Restores	A/R		
	Zone tamper/restore	MA/R	E(3)83-ZZZ / R(3)83-ZZZ	TA-ZZZ / TR-ZZZZ
	Zone fault/restore	MA/R	E(3)8A-ZZZ / R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
Tamper Events				
	Keypad 1 tamper/restore alarm	T/R	E(3)83-601 / R(3)83-601	TA-0601 / TR-0601
	Keypad 2 tamper/restore alarm	T/R	E(3)83-602 / R(3)83-602	TA-0602 / TR-0602
	Keypad 3 tamper/restore alarm	T/R	E(3)83-603 / R(3)83-603	TA-0603 / TR-0603
	Keypad 4 tamper/restore alarm	T/R	E(3)83-604 / R(3)83-604	TA-0604 / TR-0604
	Siren 1 tamper/restore alarm	T/R	E (3)83-801 / R (3)83-801	TA-0801 / TR-0801
	Siren 2 tamper/restore alarm	T/R	E(3)83-802 / R (3)83-802	TA-0802 / TR-0802
	Siren 3 tamper/restore alarm	T/R	E(3)83-803 / R (3)83-803	TA-0803 / TR-0803
	Siren 4 tamper/restore alarm	T/R	E (3)83-804 / R (3)83-804	TA-0804 / TR-0804
	Siren 5 tamper/restore alarm	T/R	E(3)83-805 / R (3)83-805	TA-0805 / TR-0805
	Siren 6 tamper/restore alarm	T/R	E(3)83-806 / R (3)83-806	TA-0806 / TR-0806
	Siren 7 tamper/restore alarm	T/R	E(3)83-807 / R (3)83-807	TA-0807 / TR-0807
	Siren 8 tamper/restore alarm	T/R	E(3)83-808 / R (3)83-808	TA-0808 / TR-0808
	Siren 9 tamper/restore alarm	T/R	E(3)83-809 / R (3)83-809	TA-0809 / TR-0809
	Siren 10 tamper/restore alarm	T/R	E (3)83-810 / R (3)83-810	TA-0810 / TR-0810
	Siren 11 tamper/restore alarm	T/R	E(3)83-811 / R (3)83-811	TA-0811 / TR-0811
	Siren 12 tamper/restore alarm	T/R	E (3)83-812 / R (3)83-812	TA-0812 / TR-0812
	Siren 13 tamper/restore alarm	T/R	E(3)83-813 / R (3)83-813	TA-0813 / TR-0813
	Siren 14 tamper/restore alarm	T/R	E (3)83-814 / R (3)83-814	TA-0814 / TR-0814
	Siren 15 tamper/restore alarm	T/R	E(3)83-815 / R (3)83-815	TA-0815 / TR-0815
	Siren 16 tamper/restore alarm	T/R	E (3)83-816 / R (3)83-816	TA-0816 / TR-0816
	Repeater 1 tamper/restore alarm	T/R	E(3)83-901 / R (3)83-901	TA-0901 / TR-0901
	Repeater 2 tamper/restore alarm	T/R	E(3)83-902 / R (3)83-902	TA-0902 / TR-0902
	Repeater 3 tamper/restore alarm	T/R	E(3)83-903 / R (3)83-903	TA-0903 / TR-0903
	Repeater 4 tamper/restore alarm	T/R	E(3)83-904 / R (3)83-904	TA-0904 / TR-0904
	Repeater 5 tamper/restore alarm	T/R	E(3)83-905 / R (3)83-905	TA-0905 / TR-0905
	Repeater 6 tamper/restore alarm	T/R	E(3)83-906 / R (3)83-906	TA-0906 / TR-0906

Appendix 2: Reporting Codes

Section #	Definition	Dialer Direction*	Automatic Contact ID Codes	SIA Auto Rep Codes**
	Repeater 7 tamper/restore alarm	T/R	E(3)83-907 / R (3)83-907	TA-0907 / TR-0907
	Repeater 8 tamper/restore alarm	T/R	E(3)83-908 / R (3)83-908	TA-0908 / TR-0908
	Keypad Lockout - Incorrect access code entry	T/R	E(4)61-000 / R(4)61-000	JA-0000
Opening Events				
	User Openings - Disarmed by user	O/C	E(4)A1-UUU	OP-UUUU
	Automatic Arming Canceled	O/C	E(4)64-UUU	CI-0000
	Special Opening - System disarmed using: keyswitch, maintenance code, DLS software, wireless key	O/C	E(4)AA-000	OP-0000
Closing Events				
	User Closings - System armed by user, wireless key	O/C	R(4)A1-UUU	CL-UUUU
	Partial Closing - 1 or more zones bypassed when armed	O/C	E(4)56-000	CG-0000
	Special Closing - System armed via: quick arm, keyswitch, function key, maintenance code, DLS software	O/C	R(4)AA-000	CL-0000
	Exit Fault	O/C	E(3)74-ZZZ	EA-ZZZZ
	Automatic (Schedule) Closing	O/C	R (4)A3-000	CA-0000
System Trouble Events				
	General system tamper/restore (while armed)	MA/R	E(1)37-000/ R(1)37-000	ES-0000/EJ-0000
	General system tamper/restore (while disarmed)	MA/R	E(1)37-000/ R(1)37-000	ES-0000/EJ-0000
	Battery trouble/restore - Main panel	MA/R	E(3)A2-000 / R(3)A2-000	YT-0000 / YR-0000
	Battery absent trouble/restore - Main panel	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
	Panel AC trouble/restore - Main panel	MA/R	E(3)A1-000 / R(3)A1-000	AT-0000 / AR-0000
	Battery over voltage charge/restore	MA/R	E(3)14-000/ R(3)14-000	YP-000/YQ-000
Alternate Communicator				
	Alternate Communicator radio/SIM trouble/restore	MA/R	E(3)AA-001 R(3)AA-001	YX-0001 / YZ-0001
	Alternate Communicator GSM Network trouble/restore	MA/R	E(3)AA-001 R(3)AA-001	YX-0001 / YZ-0001
	Alternate Communicator Ethernet trouble/restore	MA/R	E(3)AA-001 R(3)AA-001	YX-0001 / YZ-0001
	Alternate Communicator Receiver 1 absent/restore	MA/R	E(3)5A-001 R(3)5A-001	YS-0001 / YK-0001
	Alternate Communicator Receiver 2 absent/restore	MA/R	E(3)5A-002 R(3)5A-002	YS-0002 / YZ-0002
	Alternate Communicator Receiver 3 absent/restore	MA/R	E(3)5A-003 R(3)5A-003	YS-0003 / YZ-0003
	Alternate Communicator Receiver 4 absent/restore	MA/R	E(3)5A-004 R(3)5A-004	YS-0004 / YZ-0004
	Alternate Communicator Receiver 1 Supervisory trouble/restore	MA/R	E(3)5A-001/R(3)5A-001	YS-0001 / YK-0001
	Alternate Communicator Receiver 2 Supervisory trouble/restore	MA/R	E(3)5A-002/R(3)5A-002	YS-0002 / YK-0002
	Alternate Communicator Receiver 3 Supervisory trouble/restore	MA/R	E(3)5A-003/R(3)5A-003	YS-0003 / YK-0003
	Alternate Communicator Receiver 4 Supervisory trouble/restore	MA/R	E(3)5A-004/R(3)5A-004	YS-0004 / YK-0004
	Alternate Communicator SMS Config trouble/restore	MA/R	E(3)AA-001 R(3)AA-001	YX-0001 / YZ-0001
	Remote Programming Begin/End	MA/R	E(6)27-000 / E(6)28-000	LB-0000 / LS-0000
	FTC trouble/restore	MA/R	E(3)54-RRR/ R(3)54-RRR	YC-RRR/YK-RRR
	Receiver not available trouble/restore	MA/R	E(3)5A-RRR/ R(3)5A-RRR	YS-RRR/YK-RRR
	Receiver supervisory trouble/restore	MA/R	E(3)5A-RRR/ R(3)5A-RRR	YS-RRR/YK-RRR
Wireless Events				
	Wireless Zone Low Battery trouble/restore.	MA/R	E(3) 84-ZZZ R(3) 84-ZZZ	XT-ZZZZ / XR-ZZZZ

Appendix 2: Reporting Codes

Section #	Definition	Dialer Direction*	Automatic Contact ID Codes	SIA Auto Rep Codes**
	Wireless Device Low Battery trouble/restore.	MA/R	E(3) 84-ZZZ R(3) 84-ZZZ	XT-ZZZZ / XR-ZZZZ
	Wireless Zone AC trouble/restore	MA/R	E(3)A1-ZZZ R(3)A1-ZZZ	AT-ZZZZ / AR-ZZZZ
	Wireless Device fault/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
	Wireless device supervisory trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
	Wireless device force armed trouble/restore	MA/R	E(5)7A-ZZZ R(5)7A-ZZZ	UB-ZZZZ / UU-ZZZZ
	Wireless Temperature and Flood Probe trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	KT-ZZZZ / KJ-ZZZZ
	Freeze trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	ZT-ZZZZ / ZJ-ZZZZ
	Self test trouble/restore	MA/R	E(3)89-ZZZ R(3)89-ZZZ	YX-ZZZZ / YZ-ZZZZ
	Carbon monoxide trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	UT-ZZZZ / UJ-ZZZZ
	Repeater 1 AC fail/restore	MA/R	E (3)A1-901 R (3)A1-901	AT-0901 / AR-0901
	Repeater 2 AC fail/restore	MA/R	E(3)A1-902 R (3)A1-902	AT-0902 / AR-0902
	Repeater 3 AC fail/restore	MA/R	E (3)A1-903 R (3)A1-903	AT-0903 / AR-0903
	Repeater 4 AC fail/restore	MA/R	E (3)A1-904 R (3)A1-904	AT-0904 / AR-0904
	Repeater 5 AC fail/restore	MA/R	E(3)A1-905 R (3)A1-905	AT-0905 / AR-0905
	Repeater 6 AC fail/restore	MA/R	E (3)A1-906 R (3)A1-906	AT-0906 / AR-0906
	Repeater 7 AC fail/restore	MA/R	E (3)A1-907 R (3)A1-907	AT-0907 / AR-0907
	Repeater 8 AC fail/restore	MA/R	E (3)A1-908 R (3)A1-908	AT-0908/ AR-0908
	RF jam trouble/restore		E(3)44-0000	XQ-0000/XH-0000
	Wireless repeater 1-8 RF jam trouble/restore		E(3)44-901-908/ R(3)44-901-908	XQ-901-908/ XH-901-908
	Wireless keypad 1-8 trouble/restore		E(3)8A-601-608/ R(3)8A-601-608	UT-601-608/ UJ-601-608
	Wireless keypad supervisory trouble/restore		E(3)8A-601-608/ R(3)8A-601-608	UT-601-608/ UJ-601-608
	Wireless keypad 1-8 AC trouble/restore		E(3)A1-601-608/ R(3)A1-601-608	AT-601-608/ AR-601-608
	Wireless keypad 1-8 battery trouble/restore		E(3)84-601-608/ R(3)A1-601-608	XT-601-608/ XR-601-608
	Wireless repeater 1-8 trouble/restore		E(3)8A-901-908/ R(3)8A-901-908	UT-901-908/ UJ-901-908
	Wireless repeater 1-8 supervisory trouble/restore		E(3)8A-901-908/ R(3)8A-901-908	UT-901-908/ UJ-901-908
	Wireless siren 1-16 trouble/restore		E(3)8A-901-916/ R(3)8A-901-916	UT-901-908/ UJ-901-916
	Wireless siren 1-16 supervisory trouble/restore		E(3)8A-901-916/ R(3)8A-901-916	UT-901-908/ UJ-901-916
	Wireless siren 1-16 battery trouble/restore		E(3)8A-901-916/ R(3)8A-901-916	UT-901-908/ UJ-901-916
	Wireless repeater 1-8 battery restore		E(3)84-901-908/ R(3)A1-901-908	XT-901-908/ XR-901-908

Appendix 2: Reporting Codes

Section #	Definition	Dialer Direction*	Automatic Contact ID Codes	SIA Auto Rep Codes**
Miscellaneous Alarms				
	Duress Alarm - 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
	Burglary Verified	A/R	E(1)39-000	BV-0000
	Burglary Not Verified	A/R	E(3)78-000	BG-0000
	Alarm Canceled before expiry of alarm cancellation timer	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
	Fire alarm by wireless/ alarm restore	A/R	E(1)1A-0000/ R(1)1A-0000	FA-0000/FH-0000
	Auxiliary alarm by wireless/ alarm restore	A/R	E(1)AA-0000/ R(1)AA-0000	MA-0000/MH-0000
	Panic alarm by wireless/ alarm restore	A/R	E(1)2A-0000/ R(1)2A-0000	PA-0000/PH-0000
	Fire alarm by interactive/ alarm restore	A/R	E(1)11A-0000/ R(1)11A-0000	FA-0000/FH-0000
	Auxiliary alarm by interactive/ alarm restore	A/R	E(1)AA-0000/ R(1)AA-0000	MA-0000/MH-0000
	Panic alarm by interactive/ alarm restore	A/R	E(1)2A-0000/ R(1)2A-0000	PA-0000/PH-0000
Miscellaneous Closing				
]	Zone Bypass at time of arming	O/C	E(5)7A-ZZZ	UB-ZZZZ
	Zone unbypass	O/C	R(5)7A-ZZZ	UU-ZZZZ
Testing				
	Walk Test Begin/End	T	E(6)A7-UUU R(6)A7-UUU	TS-UUUU/TE-UUUU
	Periodic Test	T	E(6)A2-000	RP-0000 / RY-0000
	Periodic Test with Trouble	T	E(6)A8-000	RY-0000
	System Test	T	E(6)A1-000	RX-0000
Maintenance				
	General System trouble. An RF jam trouble occurred	MA/R	E(3) AA-000	YX-0000
	Fire trouble/restore	MA/R	E(3)73-000 R(3)73-000	FT-0000 / FJ-0000
	Heat trouble/restore	MA/R	E(3)8A-ZZZ R(3)8A-ZZZ	KT-ZZZZ / KJ-ZZZZ
	Cold Start - System has restarted after total power loss	MA/R	R(3) A5-000	RR-0000
	Smoke detector low sensitivity trouble/restore	MA/R	E(3)93-ZZZ	FT-0000/ FJ-0000
	Event Buffer 75% Full	MA/R	E(6)22-000	JL-0000
	Installer Lead In - Installer Programming has been entered	MA/R	E(6)27-000	LB-0000
	Installer Lead out - Installer Programming has been exited	MA/R	E(6)28-000	LS-0000
	Panel firmware update begin/ successful	MA/R	E(9)01-900 R(9)01-900	LB-0900 / LS-0900
	Panel firmware update fail	MA/R	E(9)02-900	LU-0900
	Periodic test with trouble	MA/R	E(6)A2-RRRR	RP-RRRR
*	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.

Appendix 2: Reporting 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. Low Temperature	ZA-ZZZZ / ZH-ZZZZ	E(1) 59 - ZZZ / R(1)59-ZZZ
24-Hr High 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
Push to Set (Walk Test Only)	BA-ZZZZ / BH-ZZZZ	E(1) 3A - ZZZ / R(1)3A - ZZZ
ZZZ/ZZZZ = zones 001-128		

Appendix 3: 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, même 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.

5.4 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 Con- figuration>Partition Con- figuration> 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

SIA Feature Programming Section	Comments	Range/Default	Requirement
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
Cancel Annunciation Panel Settings>Panel Configuration>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 Configuration>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 shutdown 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 specified time Default: disabled	Required
System Test: Panel Settings>Diagnostics>System>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> Diagnostics> System> Device> Begin Walk Test	This mode is used to test each zone on the system for proper functionality.
--	---

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 MODIFY 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.

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.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

