DSC

From Tyco Security Products

IoTega
Self-Contained Wireless Security System

User Manual

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

Table of Contents

1.0 About Your Security System **3**
1.1 Fire Detection 3
1.2 Carbon Monoxide Detection 3
1.3 Testing 3
1.4 Monitoring 3
1.5 Maintenance 4
2.0 General System Operation **5**
2.1 Integrated Keypad 5
2.2 Panel Indicators 5
2.3 Important Notice 9
2.4 Language Selection 9
2.5 System Models 9
3.0 Arming the System **10**
3.1 Stay Arming 10
3.2 Silent Exit Delay 10
3.3 Away Arming 10
3.4 Quick Exit 11
3.5 Arming Errors and Exit Faults 11
3.5.1 Arming Error 11
3.5.2 Audible Exit Fault 11
3.6 Alarm Cancel Window 11
3.7 Bypass Zones 12
3.8 Bypass Group 12
4.0 Disarming the System **13**
4.1 Disarming Error 13
5.0 Using Wireless Keys **14**
6.0 User Access Codes **15**
6.1 Access Code Types 15
6.2 Level 1 Access (Supervisor/Administrator) 15
6.3 Level 2 Access (Basic/Standard User) 16
6.4 Level 3 Access (Maintenance/Guest) 16
6.0 Additional Features **16**
6.5 Burglary Verification 16
6.6 Swinger Shutdown 16
6.7 Fire Alarm Verification 16
7.0 Emergency Keys **17**
7.1 Two-Way Audio Operation 17
7.2 Intrusion (Burglary) Alarm Continuous Siren 17
7.3 When Alarm Sounds 18
7.4 Fire Alarm Pulsed Siren (Temporal 3) 18
7.5 Carbon Monoxide (CO) Alarm 18
8.0 Using the Smartlink User App and Web Portal **19**
8.1 Accessing Your Account 19
8.2 Managing Users 19
8.2.1 Account Lockout 20
8.3 App Main Screen 20
8.4 Security 21
8.4.1 Arming 21
8.4.2 Disarming 21
8.4.3 Viewing and Bypassing Zones 21
8.5 Viewing System Status 21
8.6 Viewing System Activity and Troubles 22
8.7 Adding a Camera 22
8.7.1 Editing or Removing a Camera 23

8.7.2 Viewing Live Video and Recordings 23
8.8 Setting Event Recordings 24
8.9 Creating an Event Schedule 25
8.10 Creating Scenes 25
8.11 Running a Scene 26
8.12 Controlling Lights and Appliances 26
8.13 Controlling a Thermostat 27
8.14 Managing Notifications 27
9.0 Using Z-Wave Devices 28
9.1 Z-Wave Alliance Certification 28
9.2 Adding or Removing a Controller 28
9.3 Replicating a Controller 28
9.4 Controller Learn Mode 29
9.5 Changing the Primary Controller 29
9.6 Adding a Device 29
9.6.1 Editing or Removing a Device 29
9.7 Device Interoperability 29
9.8 Z-Wave Association Groups 29
9.9 Z-Wave Reset 30
10.0 Viewing Troubles on the Integrated Keypad 31
10.1 Alarm Memory 32
11.0 Testing Your System 33
11.1 System Test 33
12.0 Safety Instructions 34
12.1 Removing the Battery 34
12.2 Regular Maintenance and Troubleshooting 36
12.3 Cleaning and Maintenance 36
13.0 Locating Detectors and Escape Plan 37
13.1 Smoke Detectors 37
13.2 Fire Escape Planning 38
13.3 Carbon Monoxide Detectors 39
14.0 Installer Warning 40
14.0 Regulatory Agency Statements 41
15.0 Reference Sheets 43
15.1 System Information 43
15.2 Service Contact Information 43

1.0 About Your Security System

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

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

1.1 Fire Detection

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

Note: Your installer must enable and configure this feature.

1.2 Carbon Monoxide Detection

This system can monitor carbon monoxide detectors and provide a warning if carbon monoxide is detected. Read the Family Escape Planning guidelines in this manual and the instructions for the carbon monoxide detector.

Note: Your installer must enable and configure this feature.

1.3 Testing

Test your system weekly to ensure that your system functions as intended. Refer to the Testing your System section in this manual. If your system does not function properly, call your installation company for service.

1.4 Monitoring

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

Note:

- Your installer must enable the monitoring function before it is functional.
- Consult with your installer to determine if your system is configured with a communicator delay. A communicator delay prevents a report to the central station if the control panel is unset within 30-45 seconds after an intrusion alarm is triggered. Note that fire-type alarms are normally reported without a delay.
- Ensure that your installer verifies that your system is compatible with the Central Station Receiver format at yearly intervals.

1.5 Maintenance

With normal use, the system requires minimum maintenance. Note the following points:

- Do not wash the security equipment with a wet cloth. Light dusting with a slightly moistened cloth removes normal accumulations of dust.
- Replace the standby battery every 3-5 years.

WARNING! Do not attempt to replace the battery or open the enclosure, as there is a risk of electric shock or fire.

For other system devices such as smoke detectors, passive infrared, ultrasonic or microwave motion detectors, or glass break detectors, consult the manufacturer's literature for testing and maintenance instructions.

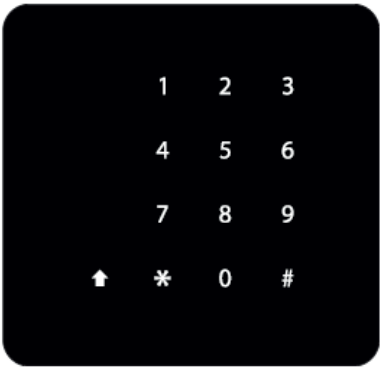
2.0 General System Operation

Your security system comprises an integrated alarm control/panel and various sensors and detectors. The panel is mounted by the main entry/exit location. The system is self-contained; electronics and standby battery are housed within the unit.
Note: Ensure that only the installer or a service professional has access to the system.

The security system has several zones of area protection. Each of these zones communicates to one or more wireless sensors, such as motion detectors, glass break detectors, door contacts, etc. A sensor in alarm is indicated by messages on the IoTega mobile phone user application.
Additional features include Automatic Inhibit (Swinger Shutdown) for alarm, Tamper and Trouble signals after three occurrences in a given set period, and a programmable Keypad Lockout option. For SIA CP-01 classified installations, the swinger shutdown feature is programmed such that one or two trips shuts down the zone. The zone is restored after a manual reset by entering the access code at the time of disarming the alarm system, or it is reset automatically after 48 hours with no trips on any zones.
Note: The mobile phone user application feature was not evaluated by UL/ULC.

2.1 Integrated Keypad

The IoTega system includes a capacitive touch integrated keypad with 16 keys: numbers 0 thru 9, *, #, Fire, Auxiliary, Panic (FAP), and shift (up arrow).
In normal operation, the keypad remains dim when not in use. When a user is in close proximity, the number keys illuminate.
Note: The FAP keys do not illuminate unless the shift key is tapped. See the Emergency Keys section for more information.

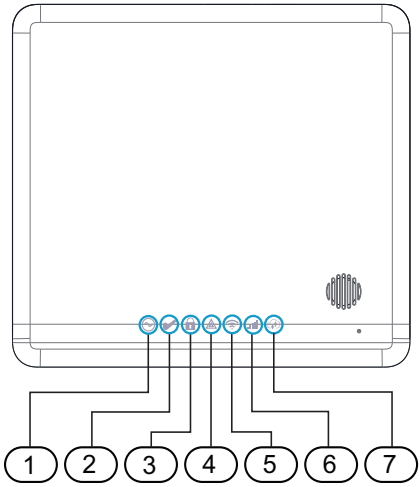


Note: The keypad can only be used for arming, disarming, and the local FAP. The same functions are available when switching between partitions.

2.2 Panel Indicators

The IoTega system includes a series of illuminated point source status indicators. There is a minimum of seven indicators:

- Four single-color LEDs
- Three bi-color LEDs (red and green)



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

Power

Status Light	LED indicator	Description
	ON Steady	AC power is connected to the system.
	Flashing	System Test All status LEDs flash at the same time.
	OFF	There is no AC or battery power to the system.

Ready to Arm

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

Armed

Status Light	LED indicator	Description
	ON Steady	The partition is armed..
	Flashing	The system in Alarm. **Note:** Silent alarms or panic do not flash the Alarm LED.
		System Test All status LEDs flash at the same time.
		Installer Walk Test Ready, Trouble, and Arm LEDs flash at the same time.
	OFF	The partition is disarmed

Trouble

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

WiFi Signal Strength

Status Light	LED indicator	Description
	ON Steady (green)	The radio is active with a strong signal connection.
	ON Steady (yellow)	The radio is active with a weak signal connection.
	ON Steady (red)	There is no signal.
	ON Flashing (red).	There was hardware network reset.
	Flashes red for several seconds, then flashes green	System Test All status LEDs flash at the same time.
	OFF	Client Mode is OFF.

Cellular Signal Strength

Status Light	LED indicator	Description
	ON Steady (green)	Cellular is active with a strong signal connection.
	ON Steady (yellow)	Cellular is active with a weak signal connection.
	ON Steady (red)	A communicator is installed but there is no signal or connection.
	Flashes red for a few seconds, then flashes green	System Test All status LEDs flash at the same time.
	OFF	A communicator is not installed or not configured.

Remote Connection Status

Status Light	LED indicator	Description
	ON Steady (green)	The link is active with a server.
	ON Flash (red)	The link activates but fails to communicate with the server.
	OFF	The link is not yet active with any server.
	ON Flash (green)	The link is active with a server and Installer Access is available.
	Flashes red for a few seconds, then flashes green	System Test All status LEDs flash at the same time.

2.3 Important Notice

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

Note: When the panel is in Sleep Mode, it is saving battery life. The panel will not be turned on until there is a specific reason, such as a hand wave in front of the panel, or the start of an entry delay.
In this mode the keypad is still functioning and nothing will be visible; however if desired, your installer can enable the armed status to be visible while in Sleep Mode.

2.4 Language Selection

The system supports the following three languages:

- English
- French
- Spanish

You can select the language on the touchscreen keypad.

2.5 System Models

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

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

(*) These devices are UL/ULC listed.

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

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

3.0 Arming the System

You can arm the system using the following options:

- Integrated keypad
- Touchscreen keypad
- User app (Operation with the user app was not evaluated by UL/ULC.)
- Wireless key (Refer to section 5.0 for a list of UL/ULC listed compatible wireless keys.)

3.1 Stay Arming

Stay Arming arms the perimeter of the premises while permitting movement inside.

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

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

When exit delay is active , the Armed and Ready indicators turn on and the keypad is silent. When the exit delay expires, the system is armed and indicated by the following conditions on the keypad:

- The Ready indicator turns off.
- The Armed indicator stays on.

Note: For SIA CP-01 listed panels, the Stay Arming exit delay will be twice as long as the Away Arming exit delay.
If your system is installed in accordance with SIA CP-01 Standard for False Alarm Reduction, the security system arms in the Stay Armed mode if the exit delay time expires and there is no exit.

3.2 Silent Exit Delay

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

3.3 Away Arming

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

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

1. Ensure all protected doors and windows are secure or bypassed and that the Ready ✔ indicator is on.
2. Enter a valid user code and exit the premises through a door programmed as entry/exit type. Exit delay begins.
3. When exit delay is active, the Armed and Ready indicators turn on and the keypad beeps once per second. Depending on your system configuration, you have ____ seconds to exit the premises. Your installer can program this time.
4. The keypad buzzer emits a distinct pulsating rate during the last 10 seconds of the exit delay to indicate that the time is expiring.
5. To cancel the arming sequence, enter your access code.

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

- The Ready indicator turns off.
- The Armed indicator stays on.
- The keypad is silent.

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

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

Note: This function is available on the touchscreen keypad and user app.

3.4 Quick Exit

If the system is armed and you must exit, use the Quick Exit function to avoid disarming and rearming the system. Using this function gives you 2 minutes to exit the premises. When the door is closed after exiting, the remaining exit time is cancelled.

3.5 Arming Errors and Exit Faults

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

3.5.1 Arming Error

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

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

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

3.5.2 Audible Exit Fault

To reduce false alarms, the Audible Exit Fault notifies you of an improper exit when arming the system. If the entry/exit door is not securely closed during the programmed exit delay, the system will sound the alarm to indicate an improper exit.

Note: Your installer must enable this feature.

To correct and exit fault, do the following steps:

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

3.6 Alarm Cancel Window

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

Note:

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

3.7 Bypass Zones

Use the zone bypassing feature when you need access to a protected area while the system is armed, or when a zone is temporarily out of service, but you need to arm the system. Bypassed zones are not able to sound an alarm. As a result, bypassing zones reduces the level of security. If you are bypassing a zone because it is not working, call a service technician immediately to resolve the problem an restore your system to proper working order.
Ensure that no zones are unintentionally bypassed when arming your system. Zones cannot be bypassed once the system is armed. Bypassed zones, except for 24-hour zones, are automatically cancelled each time the system is disarmed and must be bypassed again before the next arming.
Note:

- Two-hour zones can only be unbypassed manually.
- This function is available on the touchscreen keypad and user app.
- For UL listed installations, zones can only be bypassed manually.

To bypass an active zone on the touchscreen keypad or user app, do the following steps:

1. Tap the main menu icon  to access the main menu.
2. Tap **Sensors**.
3. Slide the switch from right to left to bypass the active zone.

3.8 Bypass Group

A bypass group is a selection of zones programmed into the system. If you bypass a group of zones on a regular basis, you can program them into a bypass group, so that you do not have to bypass each zone individually. Note that you can only program one bypass group at a time.

Note:

- This feature is not to be used in UL Listed installations.
- This function is available on the touchscreen keypad.
- For UL listed installations, zones can only be bypassed manually.

4.0 Disarming the System

You can arm the system using the following options:

- Integrated keypad
- Touchscreen keypad
- User app (Operation with the user app was not evaluated by UL/ULC.)
- Wireless key (Refer to section 5.0 for a list of UL/ULC listed compatible wireless keys.)

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

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

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

4.1 Disarming Error

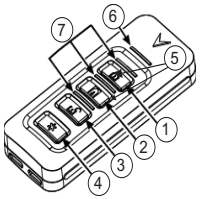
If your code is invalid, the system will not disarm and the system emits a 2-second error tone. If this happens, press [#] and try again.

5.0 Using Wireless Keys

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

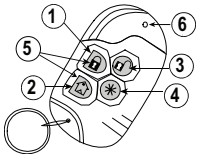
The following wireless keys are compatible with the IoTega system:

PG4929/PG8929/PG9929



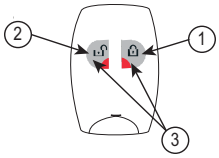
1. Away Arm
2. Stay Arm
3. Disarm
4. Panic
5. Command Output 1
6. Message LED
7. Status LEDs

PG4939/PG8939/PG9939



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

PG4949/PG8949/PG9949



1. Away Arm
2. Disarm
3. Panic

Note: The panic feature is disabled on PG9929 and PG9939 for SIA CP-01 certified installations.

A user at Master or Administrator level can assign wireless keys to users on the touchscreen keypad.

To assign a wireless key, complete the following steps:
1. From the main menu, tap Users.
2. On the upper right corner of the screen, tap the wireless key icon.
3. Tap a wireless key, then tap user to assign the key.

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

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

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

6.0 User Access Codes

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

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

User codes are 4-digits and must be unique; the system does not recognize duplicate codes. If you program a duplicate code, the system errors and rejects the code. If you try to change an existing user code to a one that is already programmed, the system errors and rejects the change.
Refer to the **Managing Users** section for more information.

6.1 Access Code Types

The IoTega system provides the following user access code types:

Master Code	This is the system master code. You cannot disable or delete this code, but you can change it in the user app. Use this code to program all other access codes, including the duress codes. You can use this code to do all user-level functions, except to access Installer mode.
User Codes	There are three access levels for user codes: • Level 1 - Supervisor/Administrator • Level 2 - Basic/Standard User • Level 3 - Maintenance/Guest Each level has different permissions. See User Code Access Levels for descriptions of each level.
Duress Codes	Use duress codes to disarm the system only in an emergency situation. When used, an emergency disarm event transmits to the central monitoring station. The system supports two duress codes, one for each partition. These codes are excluded from the total number of available codes. They have the access level of a Level 2 Basic User.

6.2 Level 1 Access (Supervisor/Administrator)

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

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

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

- Initiate system test
- Enable installer or remote access
- Language selection
- View event buffer
- View images
- Program zone and partition labels
- Schedule Auto Arming

- Initiate firmware updates
- Update the system WiFi SSID and password
- Create new users and user labels
- Program duress codes

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

6.3 Level 2 Access (Basic/Standard User)

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

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

6.4 Level 3 Access (Maintenance/Guest)

Users at this level are limited to reduced system access on their partition assignment. Users can do the following actions on their partitions:

- Arm/disarm
- Chime enable/disable
- View system troubles
- View alarm memory

6.0 Additional Features

6.5 Burglary Verification

The Control Panel includes cross zone and sequential detection features that require a trip on two or more zones within a given time period, to generate a confirmed alarm and immediate police response.
Note: Must be enabled and configured by installer.

6.6 Swinger Shutdown

The Control Panel has a swinger shutdown feature that when enabled a programmable number of trips shall shut down the zone. All burglary zone types have this feature enabled in CP-01 installations.
Note: Must be enabled and configured by installer.

6.7 Fire Alarm Verification

Fire Alarm Verification is an available option for Fire zones. If configured, once the conditions for alarm verification are met the fire alarm will sound and an alarm transmission will be sent to the monitoring station.
Note: Must be enabled and configured by installer.

7.0 Emergency Keys

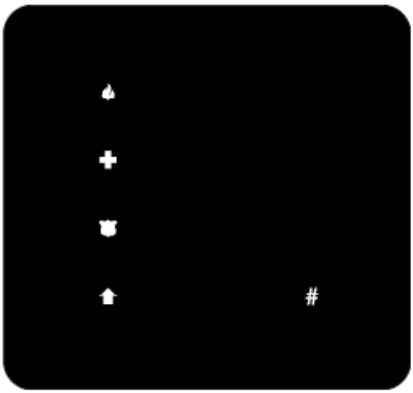
IMPORTANT: EMERGENCY USE ONLY!
The emergency keys generate a fire, auxiliary, or panic alarm and alerts the central monitoring station.
To use the emergency keys, do the following steps:

1. Tap the shift key on the keypad. The emergency keys illuminate.

   Fire Alarm

   Auxiliary Alarm

   Panic Alarm



2. Touch the Fire, Auxiliary, or Panic key for 2 seconds, as needed. The system beeps to indicate that the alarm input has been accepted and sent to the monitoring station.
3. To return to the number keypad without using the emergency keys, tap the [#] key.

Note: Depending on your system configuration, your installer can disable any of the emergency keys.

7.1 Two-Way Audio Operation

This feature is used to verify the nature of an alarm and to determine the type of assistance the occupant needs. When the central monitoring station receives an alarm, they initiate a two-way audio session.
Note:

- Only the central monitoring station can initiate a two-way audio session when they receive an alarm.; the user cannot initiate a session.
- The two-way audio feature was not evaluated by UL/ULC.

7.2 Intrusion (Burglary) Alarm Continuous Siren

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

If the alarm was accidental, enter your access code to silence the alarm. If the alarm system is disarmed within the programmed transmitter delay time, no alarm transmission is sent to the central monitoring station. Check with your installer to see if this option has been enabled on your system and for the transmitter delay time.
Following the transmitter delay time, you have 5 minutes to enter your user code to cancel an alarm that has been previously transmitted. A cancel signal is sent to the central monitoring station and the system indicates that the cancel signal was transmitted. Call your central monitoring station to avoid a dispatch.

7.3 When Alarm Sounds

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

1. Fire Alarm = Temporal/pulsed siren
2. Carbon Monoxide Alarm = four beeps, 5-second pause, four beeps
3. Intrusion (Burglary) Alarm = Continuous siren

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

7.4 Fire Alarm Pulsed Siren (Temporal 3)

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

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

7.5 Carbon Monoxide (CO) Alarm

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

 **Activation of your CO alarm indicates the presence of carbon monoxide (CO), which can be fatal.**
An alarm is indicated by the following conditions:

- The red LED on the CO detector flashes rapidly and buzzer sounds with a repeating cadence of 4 quick beeps, 5-second pause, 4 quick beeps.
- The siren connected to the control panel produces the same cadence as above.
- The system provides audible and visual indication of the CO alarm.

If the CO alarm sounds, do the following steps:

1. Press the button on the CO detector to silence the alarm.
2. Call emergency services or your fire department.
3. Immediately move outdoors or to an open door/window.

8.0 Using the Smartlink User App and Web Portal

You can manage your system with the Smartlink user app and web portal. Both provide access to several features on your system, including the following functions:

- Viewing the system status and activity
- Arming and disarming
- Bypassing zones
- Viewing the system status and troubles
- Managing devices and cameras

The web portal includes all functions that are available on the app and additional functions, including the following:

- Setting event recordings
- Creating scenes
- Managing Users and Passwords

Note: Your installer must create your customer account and configure your system before you can access it on the Smartlink app or in the web portal.

8.1 Accessing Your Account

Your installer provides a username and password you can use to log on to the app and the web portal. You can change these details at any time in the web portal. Refer to **Managing Users** for more information.

Download and install the Smartlink user app from the iOS App Store or the Google Play Store.
After downloading and installing the app, log on to your customer account with your username and password .If you have more than one system connected with your account, choose which system you want to view.

To access your account in the Smartlink web portal, enter the follwing URL in your browser:

smartlink.secure.direct

Enter your username and password and choose which system you want to view.

8.2 Managing Users

All users must have an account before they can access the system on the app or in the web portal. You can only create and edit user accounts in the web portal.

To add a new user account, complete the following steps:

1. In the web portal, go to the **Contacts** page from the left side menu.
2. Click **Add Contact** and complete the form with at least one phone number.
3. Click **Check Availability** to make sure the username is not already in use.
4. In the **Alarm User** section, the new user is automatically assigned a User ID. Enter a 4-digit panel access code for the new ID. The user needs this code to disarm the system.
5. Click **Save**.

When you save the user account, it appears on the **Contacts** page. The user can now access the system through the app and the web portal.

To edit a user account, click the **Edit** icon next to the user in the **Contacts** list.

8.2.1 Account Lockout

You have three log-on attempts before your account is locked. When this happens, your IP address is blocked for 20 minutes. After that time, the account is unlocked and you can log on again.

If you forget your password, you can avoid being locked out by resetting your password before your third log-on attempt.

To reset your password, complete the following steps:
1. On the login screen, tap **Forgot Password?**
2. Enter the following details, then tap **Next**:
   - Username
   - Phone number
   - E-mail address

An e-mail is then sent to your e-mail address with a link to reset your password.

8.3 App Main Screen

The main screen of the Smartlink app shows the current system status and lists the options available to manage your system and connected devices.

Icon	Description
	**Activity** lists system, events, such as alarms, arming, disarming, and troubles.
	**Lights &Appliances** lists controllable Z-Wave devices, such as lights and switches, and options to manage them.
	**Locks** lists controllable door locks.
	**Other Devices** lists non-controllable devices on the system, such as Z-Wave powered sensors, sirens, or range extenders.
	**Security** shows arm or disarm options.
	**Video** shows cameras and options to view live or recorded video.
	**Scenes** lists your personalized scenes you can run.
	**Thermostat** lists the options used to control your thermostat.
	**Garage Door** lists the options to control your garage door.
	**Energy** lists non-controllable devices on which you can monitor energy usage. **Note:** An energy specific device must be installed to use this feature.
	**Settings** - Manage system settings and notifications, detect cameras, and add or delete devices.

The main screen icons also appear in a footer navigation bar on most pages. Slide the bar left to right to see additional options.

8.4 Security

The **Security** screen includes functions and options for you to control your system.
From this screen, you can access the following options:

- View current system status
- Arm or disarm the system
- Access zone options
- Silence the alarm
- Turn the entry delay ON/OFF
- Access door locks

8.4.1 Arming

You can arm your system in **Stay** or **Away** mode from the **Security** screen.

To arm the system, tap the **Stay** or **Away** icon.
When the exit delay expires, the system is armed and indicated by the **Armed Stay** or **Armed Away** icon.

To cancel the arming sequence during exit delay, tap the **Arming** icon.

If a zone is open when you arm the system, a prompt appears to bypass the zone or to cancel arming. Refer to **Viewing and Bypassing Zones** for more information.

8.4.2 Disarming

To disarm your system, tap the **Armed Away** or **Armed Stay** icon and enter your panel access code followed by [#]. The system status bar changes to show the system is disarmed and the screen shows the arming options.
Note: You can set or change your panel access code in the web portal. Refer to **Managing Users** for more information..

8.4.3 Viewing and Bypassing Zones

You can view and bypass zones when the system is disarmed.
To view the zone status, tap the **Zones** icon under the **Options** tab from the **Security** screen.

To bypass a zone, tap the **Active** box next to the zone you want to bypass. The system status and the zone status change to show the bypassed zone.

To make the zone active, tap the box again.

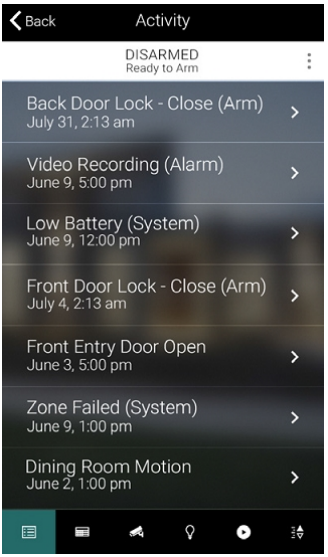
8.5 Viewing System Status

The system status and any warnings or errors on the system appear in the **Status Bar** on the app. You can tap the bar from any screen to access the system status.

On the **System Status** screen, tap one of the options to see the status of each item under that option.
.

8.6 Viewing System Activity and Troubles

The **Activity** screen lists system, events, such as alarms, arming, disarming, and troubles. Tap an event to see more information.



8.7 Adding a Camera

The Smartlink user app supports SNET cameras only, from which you can monitor your system through live footage or recordings. You can add cameras on the app and in the web portal.

Before you add a camera on the app, make sure your smartphone is connected to your home WiFi network.
To add a camera, complete the following steps:

1. From the **Settings** screen, tap **Add Camera** and tap on the image that matches your camera.
2. Enter a name for your camera.
3. Tap **Scan QR code** to use your smartphone to scan the unique device ID on the camera. Alternatively, you can enter the ID manually. Enter the device ID, including dashes and characters, then tap **Next**.
4. Plug the camera into a power outlet
5. Use one of the following methods to connect your camera:
   - Connect via IP
   - WiFi via IP
   - WiFi via Soundwave (indoor cameras only)

Connect via IP

To use the **Connect via IP** option, connect your camera to your router with the Ethernet cable. The camera automatically connects to your local network over IP.
Note: When connected, the IP/Ethernet indicator light on the back of the camera stays on.

WiFi via IP

When you use the **WiFi via IP** option, you can push the WiFi settings to the camera and remove the Ethernet cable when the camera is connected.

To use this option, wait 90 seconds after connecting power to the camera, then tap **Check Connection**.

WiFi via Soundwave (indoor cameras only)
For indoor cameras, you also have the option to **Connect via Soundwave**.
To use this option, hold your smartphone near the camera and make sure the volume on your phone is turned up.
Your phone plays an audible sound and passes your WiFi network information to the camera. The WiFi indicator light flashes slowly while the camera is in listen mode.

When the WiFi connection is successful, indoor cameras beep twice and the WiFi indicator light stays on. If using **WiFi via IP**, you can now disconnect the Ethernet cable.

8.7.1 Editing or Removing a Camera

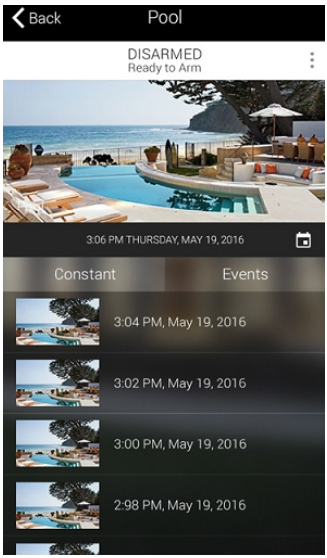
To edit a camera, complete the following steps:
1. From the **Settings** screen, tap **Edit Camera** and tap on the one you want to edit.
2. Update the camera name and tap **Done** to save the changes.

To remove a camera, tap **Remove Camera**.

To update your WiFi or network settings, tap **Update Network Connection**. This repeats the connection process, where you can update the WiFi network credentials.

8.7.2 Viewing Live Video and Recordings

The **Video** screen lists all cameras installed on your system. Tap on a camera to view the live video from that camera.

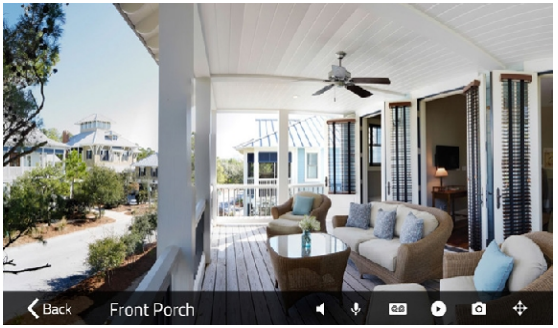


When viewing the footage vertically on your smartphone, there are tabs for **Constant** and **Event** recordings below the footage.

Constant recordings are stored on the local microSD card in supported cameras. If there is no microSD card installed, the **Constant** recording list shows a prompt to insert a blank one.

Event recordings are stored in the cloud. Security events, such as an alarm, arming, disarming, or a scene that is set on an event schedule trigger event recordings.. Refer to **Setting Event Recordings** for more information.
Note: The **Constant** and **Event** recordings are only available on supported cameras.

You can also search for recordings by date and time using the **Calendar** filter, located above the **Constant** and **Events** tabs. Tap the **Calendar** icon next to the time stamp, to select a date and time. A list of the most recent recordings prior to that time is displayed.



Rotate your phone horizontally to switch to full-screen viewing and to see the following video controls:

Mute toggles on and off the volume through the camera.

Microphone launches a **Push to Talk** button. Touch and hold the button to speak from your smartphone through the camera's built-in speaker.

Recordings displays and overlay of the **Constant** and **Event** recordings.

Control shows and overlay list of your device, which you can control while you are viewing live video.

Snapshot saves an image of the current video frame to your smartphone.

Pan/Tilt launches the pan and tilt overlay controls on supported cameras.

For **Constant** recording playback, tap on a recording in the list to start playback of the video. Tap the screen to pause or continue playback, or drag the slider to a particular point in the video.
You can choose another video from the recording list, or tap the **Back** icon to return to live viewing.

8.8 Setting Event Recordings

In the web portal, you can set your cameras to record certain events, such as alarms, arming and disarming, or scenes.
To set an event recording, complete the following steps:

1. In the web portal, go to the **Camera Settings** page from the left side menu.
2. Click the down arrow, then click **Edit** on the camera that you want to record.
3. Click **Edit** again to see the camera settings.
4. Check **Enable record on arms** and **Enable record on disarms** to start recording for those events.
5. Check all the listed sensors under the **Recording on Zones** header to record alarm events when a sensor triggers an alarm condition.

Note: Alarm events only record for sensors that you check on the **Recording on Zones** page.

You can also trigger event recordings on an individual sensor, time, or Z-Wave events by creating an event schedule. Refer to **Creating an Event Schedule** for more information.

8.9 Creating an Event Schedule

Event schedules are event-based triggers used to run scenes or individual devices automatically. You can create event schedules in the web portal.

To create an event schedule, complete the following steps:

1. In the web portal, go to the **Event Schedule** page.
2. Enter a name and choose a trigger type. Trigger types are as follows:
   - Alarm events
   - Time (one-time event or repeated)
   - Individual zones
   - Z-Wave devices

When you select a trigger type, the page updates so you can select a specific device and condition for time, zone, alarm event, or just a device.

3. In the **Actions** section, choose your desired devices and scenes and corresponding actions to run on this event schedule.
4. Click **Save** to create and activate the event schedule.

8.10 Creating Scenes

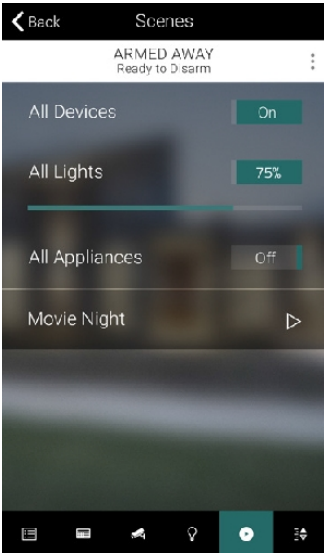
A scene is a group of device actions set to run collectively that can be triggered by an event schedule or on-demand from the app or web portal. You can create scenes in the web portal.

To create a scene, complete the following steps:

1. In the web portal, go to **Personalize Scene** and click **Create Scene**.
2. Enter a name and click **Next**.
3. Select an **Action Type**, device, and state or action, as follows:
   - Alarm
   - Z-Wave
   - Camera
4. Click **Add** to add the device and action to the scene.
5. Repeat steps 2 and 3 to add more devices and actions.
6. Click **Save** to create the scene.

8.11 Running a Scene

You can run a scene on-demand from the app or the web portal. On the app, the **Scenes** screen contains your created scenes and system preset scenes such, **All Lights**, **All Devices**, or **All Appliances**.

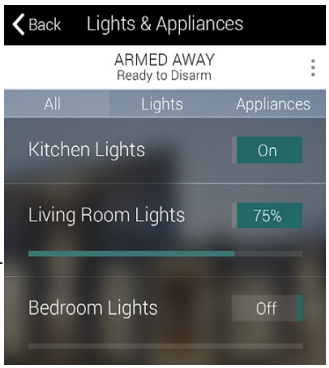


To run your created scene, tap the **Play** ▶ icon next to the scene name.

To control a preset scene, use the slider or toggle switches next to the scene.

8.12 Controlling Lights and Appliances

The **Lights & Appliances** screen lists your controllable Z-Wave devices, including lights and switches.

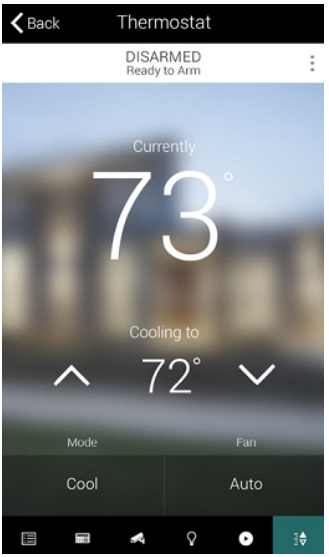


Lights are devices with dimmer functionality. Use the toggle switch next to the device name, to turn the light on and off. Control the brightness of the light by using the slider under the device name.

Appliances are devices that have only on and off capability, such as a smart switch. Use the toggle switch to turn the appliance on and off.

8.13 Controlling a Thermostat

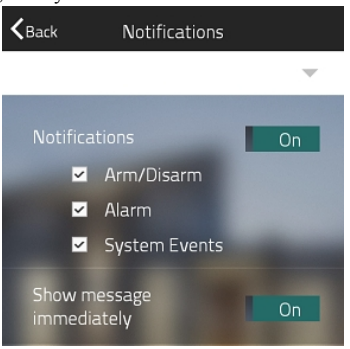
The **Thermostat** screen shows the current temperature reading. Adjust the target temperature by tapping the up and down arrows.



Tap on the **Mode** or **Fan** options to switch to Heat/Cool/Off mode and On/Auto fan.

8.14 Managing Notifications

You can receive notifications for arming, disarming, alarms, and system events.



To set your notifications, complete the following steps:

1. From the **Settings** screen, tap **Notifications**.
2. Tap the toggle switch to turn all notifications on or off.
3. To receive individual notifications, select the box beside that type.

You can also manage notifications for each user in the web portal.

To set notifications for a system user, complete the following steps:

1. From the **Contacts** page, click the down arrow to expand the contact.
2. Click the buttons for **Text Alert** and **Email Alert** to turn them on or off.

9.0 Using Z-Wave Devices

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

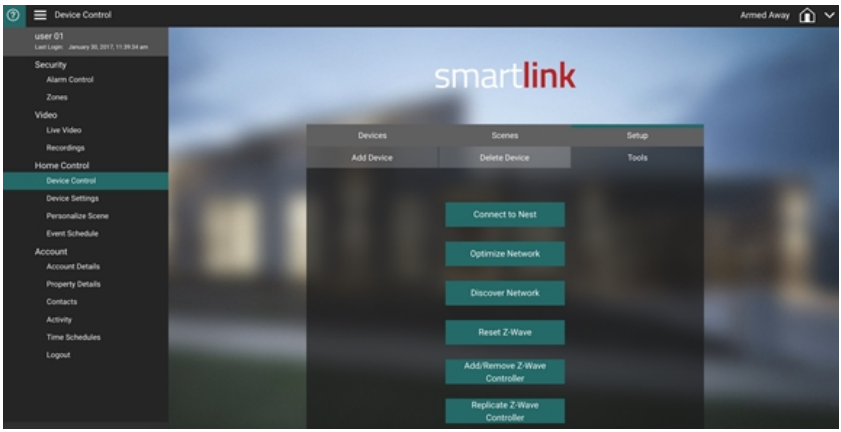
9.1 Z-Wave Alliance Certification

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

9.2 Adding or Removing a Controller

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

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



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

9.3 Replicating a Controller

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

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

9.4 Controller Learn Mode

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

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

9.5 Changing the Primary Controller

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

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

9.6 Adding a Device

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

To add a device on the app, tap the applicable option and complete the following steps:
1. Power up your device per the manufacturer's instructions.
2. From the **Settings** screen, tap **Add Z-Wave Device** to initialize learn mode.
3. Follow the instructions onscreen to bind your device. Refer to the device instructions, if necessary.
4. When enrollment completes, enter a device name and tap **OK**. Your device is ready to use.

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

9.6.1 Editing or Removing a Device

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

9.7 Device Interoperability

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

9.8 Z-Wave Association Groups

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

Bit	Property
0	Low Battery
1	AC Failure

Bit	Property
2	No Battery
3	Tamper

9.9 Z-Wave – Responding to the Basic Command

If this device receives a Basic Get request, it will respond with the BASIC REPORT detailed in section Z-Wave Association Groups.

This device ignores the z-wave Basic SET command.

9.10 Z-Wave Reset

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

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

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

10.0 Viewing Troubles on the Integrated Keypad

When the system detects a trouble condition, the Trouble  indicator turns on and the system beeps once every 10 seconds. Tap any key to silence the beeps.
Note: For UL Listed installations, your access code is required to view system troubles.

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

1. When the keypad illuminates, tap [*][2].
2. Enter your access code, if required. The Trouble indicator flashes if an access code is required.

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

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

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

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

Top Level Device Type		Second Level Trouble Type		Third Level Device ID
01	System Trouble	01	AC	
		02	Battery Trouble (low battery, no battery)	
		03	Tamper	
		04	Hardware Fault	
		05	Future Use	
		06	RF Jam	
02	Zone	01	AC	1-128
		02	Battery Trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not Networked	
		06	Fire/CO Trouble	
03	Siren	01	For future use	1 to 16
		02	Battery Trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not Networked	

Top Level Device Type		Second Level Trouble Type		Third Level Device ID
04	Keypad	01	AC (Power G only)	1 to 4
		02	Battery Trouble (Power G only)	
		03	Tamper (Power G only)	
		04	Fault (supervision) (Power G, WiFi keypads)	
		05	Not Networked (Power G only)	
05	Repeater	01	AC	1 to 8
		02	Battery Trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not Networked	
		06	RF Jam	
06	Wireless key	01	For future use	1 to 32
		02	Battery Trouble	
		03	Tamper	
		04	Fault (supervision)	
		05	Not Networked	
07	Communication	01	Receiver not available	
		02	FTC Trouble	1- receiver 1 2- receiver 2 3- receiver 3 4- receiver 4
		03	Receiver supervision trouble	
		04	Cellular Trouble	
		05	Ethernet/WiFi Trouble	
		06	Remote shutdown	

10.1 Alarm Memory

When an alarm occurs while the system is armed, it is stored in the alarm memory when you disarm the system. The system sounds a different tone than normal during entry delay. After disarming the system, the zone number on the keypad flashes for 5 minutes to indicate an alarm in memory.
Note: If disarming the system with a 2-way wireless key, the system squawks three times to indicate an alarm in memory.

 Proceed with caution, as an intruder can still be within the premises.

To arm the system again, wave your hand in front of the keypad. The zone numbers stop flashing and you can then arm the system. The alarm memory clears the next time you arm and disarm the system.

11.0 Testing Your System

Inform your Monitoring Station when you begin and end system testing.
Household fire alarm systems shall be tested by a qualified service technician at least every 3 years in accordance with NFPA72. It is the user's responsibility to test the system weekly (excluding smoke detectors). Ensure you follow all the steps identified in the following sections.
Should the system fail to function properly, call your installer immediately for service.

11.1 System Test

The system test activates a 4-second check of the system status indicators, keypad lights, buzzer, and siren. It is a partition-based test must be done when the system is disarmed.

To start a system test from the touchscreen keypad or the user app, do the following steps:

1. Tap the main menu icon  to access the main menu.
2. Tap **Advanced**, then tap Execute System Test.

The following conditions indicate a system test is in progress:

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

12.0 Safety Instructions

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

WARNING! This equipment has no mains on/off switch; if the equipment must be quickly disconnected, the plug of the direct plug-in power supply is intended to serve as the disconnecting device; it is imperative that access to the mains plug and associated mains socket/outlet, is never obstructed.

When using equipment connected to the mains and/or to the telecommunication network, there are basic safety instructions that must always be followed. Refer to the safety instructions provided with this product and save them for future reference. To reduce the risk of fire, electric shock and/or injury, observe the following:

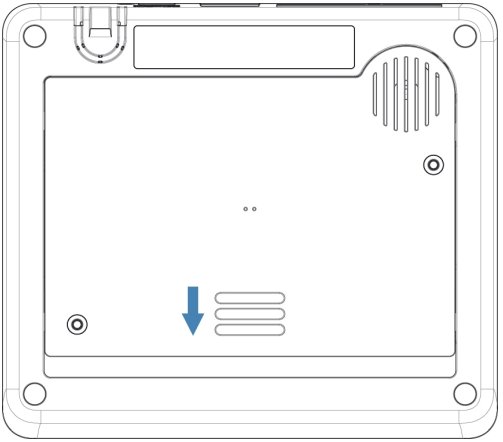
- Use authorized accessories only with this equipment!
  DO NOT leave and/or deposit ANY object on the top of the cabinet of this equipment!
  The cabinet is not designed to support any supplementary weight!
- Do not touch the equipment and its connected cables during an electrical storm; there may be a risk of electric shock.
- Never touch un-insulated wires or terminals unless the equipment has been disconnected from the mains supply!
- Ensure that cables are positioned so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain. Do not spill any type of liquid on the equipment.
- Do not use the Alarm system to report a gas leak if the system is near a leak.

These safety instructions should not prevent you from contacting the distributor and/or the manufacturer to obtain any further clarification and/or answers to your concerns.

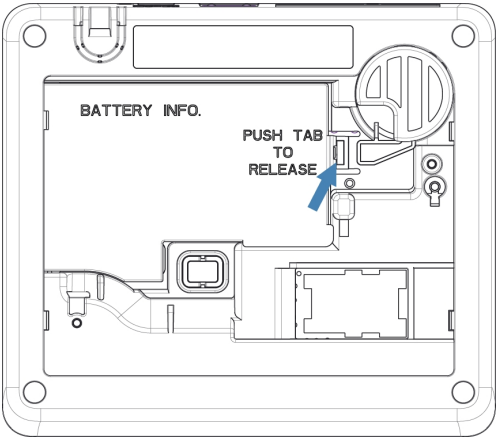
12.1 Removing the Battery

To completely disconnect power to the equipment, you must disconnect the direct plug-in power supply and remove the battery.

To remove the battery, do the following steps:
1. On the bottom of the panel, slide the cover in the direction shown and remove it.



2. .Gently push the tab on the side of the battery to release it.



3. Lift and slide the battery out of the compartment.

12.2 Regular Maintenance and Troubleshooting

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

12.3 Cleaning and Maintenance

- Clean the units by wiping with a damp cloth only.
- Do not wipe the front cover with alcohol.
- Do not use any water or any other liquid.
- Do not use abrasives, thinners, solvents or aerosol cleaners (spray polish) that may enter through holes in the Alarm Controller and cause damage.
- Use the system test described in "Testing Your System" to check the battery condition. We recommend, however, that the standby batteries be replaced every 3-5 years.
- For other system devices such as smoke detectors, passive infrared, ultrasonic or microwave motion detectors or glass break detectors, consult the manufacturer's literature for testing and maintenance instructions.

13.0 Locating Detectors and Escape Plan

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

13.1 Smoke Detectors

Research has shown that all hostile fires in homes generate smoke to a greater or lesser extent. Experiments with typical fires in homes indicate that detectable quantities of smoke precede detectable levels of heat in most cases. For these reasons, smoke alarms should be installed outside of each sleeping area and on each storey of the home.

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

It is recommended that additional smoke alarms beyond those required for minimum protection be installed. Additional areas that should be protected include: the basement; bedrooms, especially where smokers sleep; dining rooms; furnace and utility rooms; and any hallways not protected by the required units. On smooth ceilings, detectors may be spaced 9.1m (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 38ºC (100ºF) or falls below 5ºC (41ºF).
- Smoke detectors must always be installed in USA in accordance with Chapter 29 of NFPA 72, the National Fire Alarm Code: 29.5.1.1.

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

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

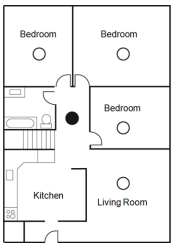


Figure 1

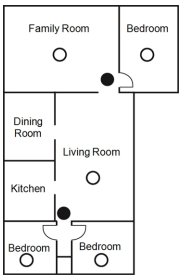


Figure 2

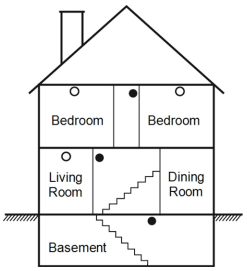


Figure 3

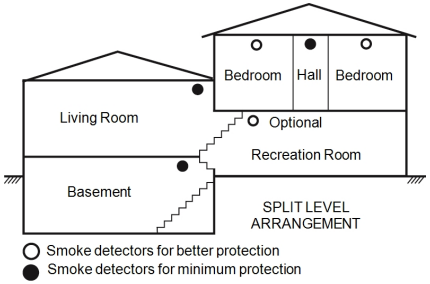


Figure 3a

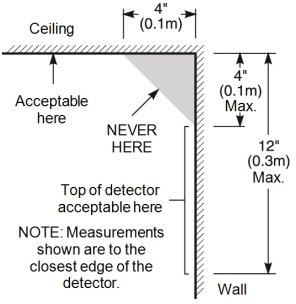


Figure 4

13.2 Fire Escape Planning

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

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

Consider the following when making your escape plans:

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

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

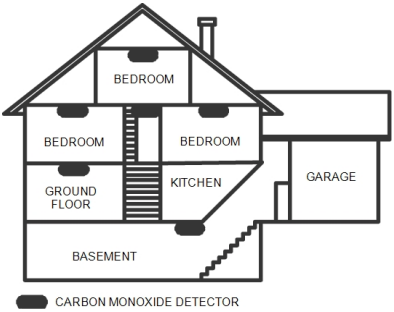


Figure 5

13.3 Carbon Monoxide Detectors

Carbon monoxide is colorless, odorless, tasteless, and very toxic, it also moves freely in the air. CO detectors can measure the concentration and sound a loud alarm before 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.

Do NOT place the CO alarm in the following areas:

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

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

14.0 Installer Warning

Warning Please Read Carefully

Note To Installers:

This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the 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 these reasons may be:

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.

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 a security system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

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.

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.

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.

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.

System Users

A user may not be able to operate a panic or emergency switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm.

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.

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, barbeques, fireplaces, sunlight, steam vents, lighting and so on.

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 or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a hearing-impaired person.

Telephone Lines

If telephone lines are used to transmit alarms, they may be out of service or busy for certain periods of time. Also an intruder may cut the telephone line or defeat its operation by more sophisticated means which may be difficult to detect.

Insufficient Time

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

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.

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.

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.

14.0 Regulatory Agency Statements

FCC MODIFICATION STATEMENT

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

FCC AND ISED CANADA INTERFERENCE STATEMENT

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

FCC CLASS B DIGITAL DEVICE NOTICE

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

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

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

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

FCC/ISED CANADA WIRELESS NOTICE

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

Antenna gain must be below:

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

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

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

Gain de l'antenne doit être ci-dessous:

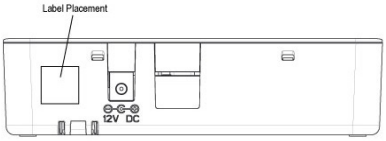
Frequency band	3G4000
GSM 850 / FDD V	2.1 dBi
PCS 1900 / FDD II	3.7 dBi
LTE B4 (1700 MHz)	1.5 dBi
LTE B13 (700 MHz)	2.2 dBi

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

FCC/IC LABEL

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

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



Hereby, DSC, declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The complete R&TTE Declaration of Conformity can be found at http://www.dsc.com/listings_index.aspx

(CZE) DSC jako výrobce prohlašuje, že tento výrobek je v souladu se všemi relevantními požadavky směrnice 1999/5/EC.

(DAN) DSC erklærer herved at denne komponenten overholder alle viktige krav samt andre bestemmelser gitt i direktiv 1999/5/EC.

(DUT) Hierbij verklaart DSC dat dit toestel in overeenstemming is met de eisen en bepalingen van richtlijn 1999/5/EC.

(FIN) DSC vakuuttaa laitteen täyttävän direktiivin 1999/5/EC olennaiset vaatimukset.

(FRE) Par la présente, DSC déclare que ce dispositif est conforme aux exigences essentielles et autres stipulations pertinentes de la Directive 1999/5/EC.

(GER) Hierdurch erklärt DSC, daß dieses Gerät den erforderlichen Bedingungen und Vorrausetzungen der Richtlinie 1999/5/EC entspricht.

(GRE) Δία του παρόντος, η DSC, δηλώνει ότι αυτή η συσκευή είναι σύμφωνη με τις ουσιώδης απαιτήσεις και με όλες τις άλλες σχετικές αναφορές της Οδηγίας 1999/5/EC.

(ITA) Con la presente la Digital Security Controls dichiara che questo prodotto è conforme ai requisiti essenziali ed altre disposizioni rilevanti relative alla Direttiva 1999/05/CE.

(NOR) DSC erklærer at denne enheten er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

(POL) DSC oświadcza, że urządzenie jest w zgodności z zasadniczymi wymaganiami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE.

(POR) Por este meio, a DSC, declara que este equipamento está em conformidade com os requisitos essenciais e outras determinações relevantes da Directiva 1999/5/EC.

(SPA) Por la presente, DSC, declara que este equipo está en conformidad con los requisitos esenciales y otros requisitos relevantes de la Directiva 1999/5/EC.

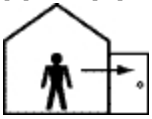
(SWE) DSC bekräftar härmed att denna apparat uppfyller de väsentliga kraven och andra relevanta bestämmelser i Direktivet 1999/5/EC.

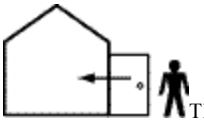
15.0 Reference Sheets

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

15.1 System Information

Mark if Buttons are Enabled
[F] FIRE [M] Medical [P] PANIC

 The Exit Delay Time is _____ seconds.

 The Entry Delay Time is _____ seconds.

15.2 Service Contact Information

Central Station Information
Account #: _____ Telephone #: _____
Installer Information:
Company: _____ Telephone #: _____
Battery Installation / Service Date:

_____
_____
_____

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

Tech Support: 1-800-387-3630 (Canada & U.S.) or 905-760-3000
• www.dsc.com

DSC
From Tyco Security Products

29009783R001