iSecure
Systems by Napco

Professional Cellular Alarm System

Installation & Programming Instructions

WI2240LF 12/19

DOCUMENT REVISION HISTORY

Date	Revision	Description of Changes
Dec 2019	WI2240LF	•Original release.
		•
		•
		•
		•
		•
		•
		•
		•
		•

Napco Security Technologies, Inc. (NAPCO) makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Further, Napco reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Napco to notify any person of such revision or changes.

Information furnished by Napco is believed to be accurate and reliable. However, no responsibility is assumed by Napco for its use; nor for any infringements of other rights of third parties which may result from its use. No license is granted by implications or otherwise under any patent or patent rights of Napco. *Changes Or Modifications Not Expressly Approved By The Party Responsible For Compliance Could Void The User's Authority To Operate The Equipment.*

For systems that include CO detectors, the system must be monitored by a central station.

Compliance Statement

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory. Napco Security Technologies, Inc., reserves the right to make product improvements and changes to product specifications at any time. While every precaution was taken during the preparation of this document to ensure its accuracy, Napco assumes no responsibility for errors or omissions.

Fire Alarm System Limitations

Automatic fire alarm systems can not guarantee against property damage, loss of property, or loss of life. An automatic fire alarm system's ability to provide early warning of a developing fire may be limited for a variety of reasons, but mainly due to improper installation or maintenance. The best way to minimize system failures is to perform regularly scheduled preventive maintenance in accordance with national and local fire codes. All system components and wiring should be tested and maintained by trained fire alarm system professionals. *All wireless devices, including Z-Wave devices, must be signal tested with all enclosure covers fully closed, including the Go-Anywhere Hub.*

Microsoft® and Windows® are registered trademarks of the Microsoft Corporation.

All other trademarks cited in this manual and all other © Napco manuals are for reference only and are the property of their respective owners.

This document contains proprietary information of Napco. Unauthorized reproduction of any portion of this manual without the written authorization of Napco is prohibited. The information in this manual is for informational purposes only. It is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. Napco assumes no responsibility for incorrect information this manual may contain. Refer to our website for the latest revisions of the documentation.

Caution: Verify all components including those adhered to walls with double-sided tape are secure and remain firmly adhered. Regularly inspect components that could cause injury; in addition, swallowing small components, such as magnets or batteries, could injure small children; keep all components away from children.

333 Bayview Avenue, Amityville, New York 11701
Publicly traded on NASDAQ Symbol: NSSC
Visit our website at www.napcosecurity.com
For Sales and Repairs: (800) 645-9445
For Technical Service: (800) 645-9440 or visit us at tech.napcosecurity.com
(**Note:** Technical Service is for security professionals only)
Fax: 631-789-9292

Table of Contents

Overview

INTRODUCTION

NAPCO's **iSecure Security System** is an easy to install, state-of-the-art microcomputer-based burglary alarm system with integral cellular communicator. Installation allows for wall mounting or placement on a table top. **iSecure** supports up to 80 wireless protection zones that may be divided into 1 or 2 Areas, each containing their own protection zones. The basic system can be easily expanded, with all Kits compatible with the following standard devices:

Go-Anywhere Hub™

- **IBR-TOUCH-WL** *Smart 7" Wireless IoT Touchscreen Keypad*
- **ISEC-WL-TOUCH** *Wireless 4.3" Full Color Security Touchscreen Keypad*
- **ISEC-WL-KEYPAD** *Wireless Battery-Powered Standard Keypad*
- **ISEC-WL-SIREN** *Wireless Siren*
- **ISEC-WL-MODULE** *Wireless 8-Zone Takeover Module*
- **ISEC-DW-XMITTER** *Low Profile Window/Door Transmitter*
- **ISEC-KEYFOB** *4-Button Pendant/Keychain Transmitter*
- **ISEC-SMOKE** *Supervised Wireless Digital Smoke Sensor*
- **ISEC-MOTION** *Passive Infrared Motion Sensor*
- **ISEC-GLASSBREAK** *Wireless Glass-Break Sensor*
- **ISEC-CARBON MON** *Supervised Wireless Carbon Monoxide Sensor*
- **ISEC-PANIC** *Single Button Waterproof Panic*
- **ISEC-HEAT** *Wireless Heat Detector with Rate of Rise*
- **ISEC-ZWAVE** *Z-Wave Module*
- **ISEC-WIFI** *Internet Module*
- **ISEC-2WF-MOD** *2-Wire Fire Sensor Module*
- **SLE-EXTANT-KIT** *Adapter Cable for ANTEXT Kits:*
  - **SLE-ANTEXT30** *30' Remote Antenna Kit*
  - **SLE-ANTEXT50** *50' Remote Antenna Kit*
  - **SLE-ANTEXT75** *75' Remote Antenna Kit*
  - **SLE-ANTEXT100** *100' Remote Antenna Kit*

See page 73 for ordering and additional information. Refer to our website for the latest revisions of the documentation

FEATURES

- iPhone and Android phone apps allow for local and remote arm / disarm, system status and Z-Wave control
- Integral 319MHz wireless receiver allows for compatibility with all NAPCO 319MHz wireless transmitters
- Integral 4-wire bus terminals that support the **GEMWV-RECV** (additional peripherals require power supply)
- Integral Ethernet 10/100 network connection for central station communication, notifications and **IBR-TOUCH-WL** operation
- Integral siren with Burg, Fire and CO Alarm cadences capable of 85dBA at 10 feet
- Integral voice prompts with 4 volume levels
- All Kits support up to six (6) **ISEC-WL-KEYPAD**s and/or **ISEC-WL-TOUCH**s, combined. When the **Go-Anywhere Hub** is connected to a network with a Wi-Fi access point, up to four (4) **IBR-TOUCH-WL** tablet keypads can be used.
- Powered by 16.5VAC transformer (included). Provision for rechargeable 4AH or 5AH 12V backup battery (not supplied) that automatically provides power during AC power outages
- System fully monitors AC power and charges the backup battery
- LTE cellular radio module for wireless central station communication, notifications, remote programming and firmware downloads
- Integral supervised bell output
- Integral PGM output initiated by a keyfob button press (toggle on/off or momentary on for 5 seconds)
- Cloud-based programming in the **iSecure Cloud Web Portal** (www.iSecureByNapco.com)
- 900MHz Wireless Transceiver Module for adding other wireless system peripherals, including the **ISEC-WL-KEYPAD**, the **ISEC-WL-TOUCH** *Touchscreen*, the **ISEC-WL-MODULE** *Takeover Module* and the **ISEC-WL-SIREN**.
- Optional **ISEC-ZWAVE** *Z-Wave Module* for programming/control of Z-Wave home automation controls such as Z-Wave-enabled lights, outlets, thermostats, garage door operators and door locks
- Optional **ISEC-WIFI** *Internet Module* for central station communication and notifications (supplied in KIT 3; see page 73 for kit ordering information).
- Optional **SLE-ANTEXT30** / **50** / **75** / **100** *Extended Range Remote Indoor/Outdoor Antenna* to increase LTE cellular transmission signal strength (see WI2230 for instructions)
- Optional **ISEC-2WF-MOD** *2-Wire Fire Sensor Module* that supports 2 Fire zones (connect to **Fire Power [+]**, **Zone 7 [–]** and **Zone 8 [–]** terminals)

See page 73 for ordering and additional information.

Note: Not all pages in this manual apply to all systems. Use the instructions for the peripherals and devices included with the iSecure kit or for any additional devices purchased, as required. ***All wireless devices, including Z-Wave devices, must be signal tested with all enclosure covers fully closed, including the Go-Anywhere Hub***.

Note: iSecure, Gemini Wave (GEMWV) and Gemini (GEM) transmitters are compatible with the iSecure system; however, iSecure and Gemini Wave (GEMWV) transmitters are not compatible with Gemini GEM-Receivers.

To simplify the installation process, the **Go-Anywhere Hub** can be programmed either through the programming screens in the iSecure phone app or by accessing the same programming screens in the **iSecure Cloud Web Portal** (www.iSecureByNapco.com). In addition, a log containing up to 800 events monitors Go-Anywhere Hub activity referenced to a precision real-time clock. This detailed event history may be displayed in the website page or in the app, as needed.

New User Pre-Installation and Configuration Steps

Open the box and locate **OI404LF**, a card that specifies the system **Radio ID** number, **Network MAC** address and **Master Code**. Keep this card handy during the installation process, *but always store in a secure location*.

Account and Central Station Activation

1. Visit (www.NapcoComNet.com)
2. Enter your **iSecure ID #** and the select your service plan
3. Access the iSecure Cloud Web Portal at www.iSecureByNapco.com. Click **Dealer Login**. Refer to the OI404LF card and enter your **Dealer User ID**, **Password** and **Radio ID** ("**iSecure LTE ID#**"). Click **Submit**.
4. Click **General Settings** and in the **Master Security Code** field, enter the **Master Code** (also refer to the OI404LF card).
   - (Optional) Enter a **Download Security Code** and a **Dealer Keypad Programming Code** in the fields provided.
5. Click **Save**. Any changes to the Master Security Code require that you exit and re-enter the iSecure Cloud Web Portal. Therefore, quit your browser and log back in.
6. Click **Central Station Reporting** and enter your central station account and telephone number. Click **Save**.
7. Download the Kit configuration into your Go-Anywhere Hub: Click **Upload/Download** > **Full Download** and click **Yes** to confirm. While waiting for the download to complete, the yellow "IP Network Wi-Fi" LED will be on steady during the download process and the Hub will beep when the download is complete.

After you have downloaded the Kit configuration into your Go-Anywhere Hub, you can add and easily configure any additional devices as detailed further in this manual (see the Table of Contents for the device you wish to add).

Hardware Installation Instructions

1. Open box and remove all components from the Kit and place on a clean table top. Be sure that **OI404LF** (the card that specifies the system **Radio ID**, **Master Code**, etc.), is in a secure location.
2. Power all battery-powered devices, either by inserting batteries or by removing battery ribbons/fishpaper. With the Kit 1 keypad (**ISEC-WL-KEYPAD**), insert battery (provided) into 1 of the 2 battery holders. Place magnets next to **ISEC-DW-XMITTERs** to make them appear to the system as "closed" (see page 18 for where to locate the magnet).
3. Separate the Go-Anywhere Hub housing: With a flat head screwdriver, push in the two tabs at the bottom to unhook, then carefully separate the two parts of the housing.
4. Place a 12V, 4AH (or 5AH) battery (not supplied) into its bracket, terminals facing the rear of the unit. Secure using the Velcro strip. Connect flying leads to battery terminals "red to red" and "black to black".
5. Re-join the front and rear Go-Anywhere Hub housing, thus powering the unit. Verify that the bottom right green LED on the Hub flashes for about 10 seconds.
6. Wire the supplied 16VAC transformer wires: Remove the wiring cover on the back of the Hub and connect each wire to each of the bottom two screw terminals. **Note:** The transformer is a required part of a working system.
7. Wait at least 30 seconds until the "Cellular Signal Strength" green LED (right side, second from top) flashes a signal strength of 3 or higher.
8. Confirm keypad operation by arming and disarming the system (use the default User Code **1 2 3**).
9. With the system disarmed, test each transmitter (one at a time) by removing and replacing its magnet.
10. Test the PIR by facing it towards a wall, or upside down so that no motion is detected for at least 5 minutes. Ensure the keypad displays a faulted zone when the PIR is triggered by pointing the PIR towards the tester.
11. If additional wireless devices were added to the system (programmed using the iSecure Cloud Web Portal and downloaded to the Hub) ensure the devices are similarly tested.
12. After confirming operation of all parts of the system, physically install each device in their desired location as detailed in this manual (see the Table of Contents for each device).
13. Determine the installation location noise level: After installing the Go-Anywhere Hub in its final location, remove power (unplug AC and open the Hub enclosure to momentarily disconnect the battery), wait 10 seconds, then snap the Hub enclosure back together and plug the Hub transformer into a wall outlet. This momentary removal of power will allow the Go-Anywhere Hub to determine the relative wireless noise level of each device at each of their selected installation locations. **IMPORTANT:** All wireless devices, including Z-Wave devices, must be signal tested with all enclosure covers fully closed, including the Go-Anywhere Hub.

Now install and launch the iBridge smartphone app to confirm the signal strength of each transmitter:

iOS / Android Phone App Installation

- Purchase and install the free smartphone app (search for "**iBridge**" in your online app store)
- Launch the app and tap **System** (the "gears" icon)
- Tap **Configure Remote Logins** > **New User**
- In the **Username** field, enter the **Radio ID** ("**iSecure LTE ID#**") located on the card (OI404LF)
- In the **Password** field, enter the default Password **1 2 3 4**
- Type a **Display Name**
- Tap **Log In** (when connected, the bottom right will indicate "**Connected...**"
- Tap **Security**
- Enter the **Master Code** located on the card (OI404LF), then tap **MENU**, **BYPASS**, (tap **Next/Yes** to DISPLAY RF XMITTER STAT Y/N).
- Tap **Next/Yes** to scroll forward through each zone (or tap **Prior/No** to scroll through the previous zones). Signal strength should be at least 3; we recommend 4 or greater)

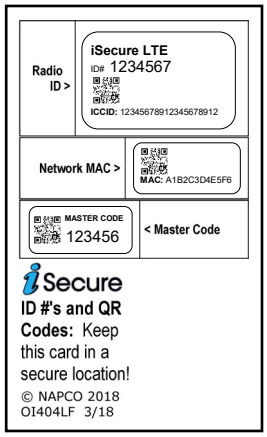
Dealer Account Activation & Programming

Dealer Account Activation

The iSecure system requires activation before it can be used. Before powering the Go-Anywhere Smart Hub, you must:

1. Be an active NapcoComNet dealer and have an account. To activate, go to www.NapcoComNet.com and log in to your NapcoComNet account in the "**Existing Customer**" section.
   If you are not yet registered as a NapcoComNet dealer, please complete the "**New Customer**" section. Dealer accounts are approved Monday-Friday 8:30 AM - 4:30 PM (please allow up to 1 business day for approval).

2. Click the **Add Device** tab at the top of the screen, click **Service Plans** and then enter the seven-digit **Radio ID** number on the card provided with your iSecure system to register and activate the Radio ID number. Enter the **Radio ID** without dashes or spaces (see sample shown at right).



3. Select: **iSecure Service Plans**

4. Click **Go** to view the applicable service plans and add them to your cart. If any optional services are available, they will appear on this screen. You will be asked to enter basic subscriber information, review your order and then check out by clicking **Process Order**.

   The iSecure product will be ready for use within 15 minutes of checkout.

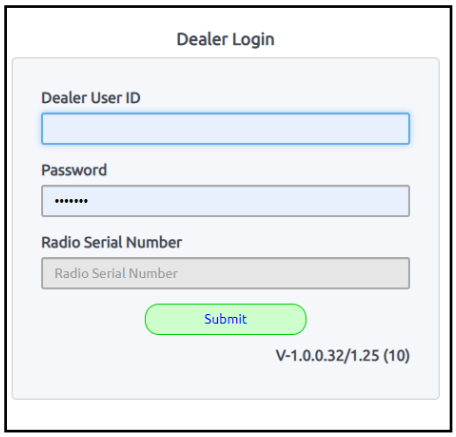
   With iSecure, a *new* subscriber account will automatically be created. A **Dealer User ID** and temporary **Password** will be emailed to you (the dealer) upon activation. This temporary **Password** *must* be changed by the customer (owner of the installation site premises) after the installation is complete. **Note:** For existing subscribers, the system will NOT generate an email with a **Dealer User ID / Password**.

Dealer Programming

When you purchase an iSecure kit (see page 73 for ordering information), all devices included in the kit are already programmed into the **iSecure Cloud Web Portal** (www.iSecureByNapco.com). Simply add extra devices or make changes to the existing devices as needed. To log into the **iSecure Cloud Web Portal**, proceed as follows:

1. Open your browser and go to the **iSecure Cloud Web Portal** at www.iSecureByNapco.com. An initial login screen appears:

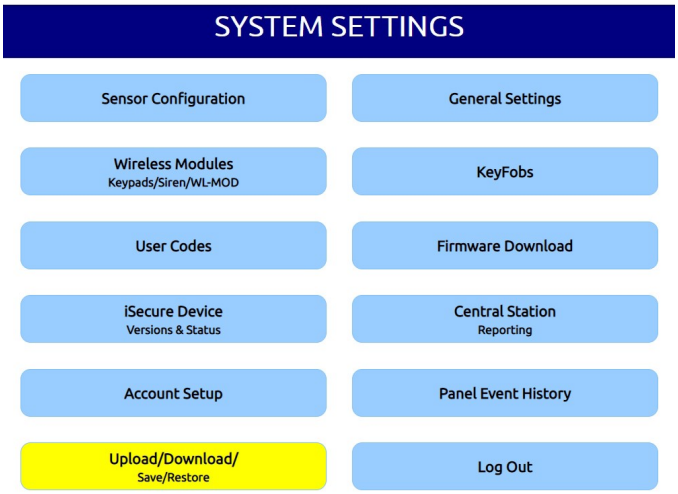
2. Click **Dealer Login** and the iSecure login screen appears:



3. In the email sent to you (see the section "**Dealer Account Activation**", above), enter the **Dealer User ID** and temporary **Password** in the fields provided.

   In the **Radio Serial Number** field, enter the **Radio ID** number printed on the iSecure card that came with your iSecure system (sample card shown above).

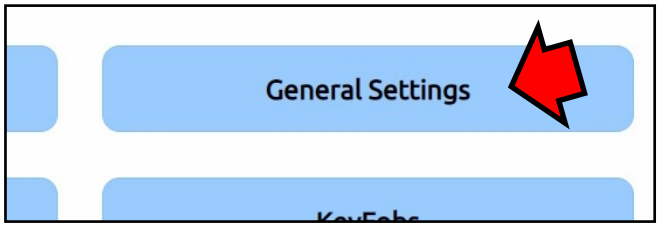
   Click **Submit** and the main programming "**SYSTEM SETTINGS**" screen appears:



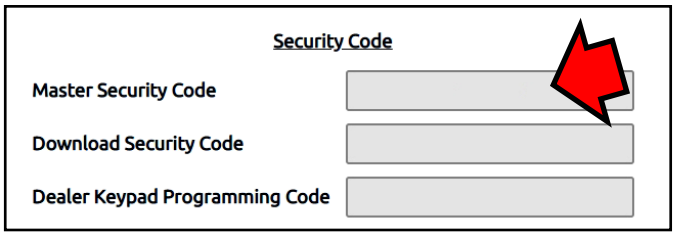
For new accounts accessed for the first time, a message will appear requesting that you first enter the six-digit **Master Code** located on the card provided with your iSecure system (see sample shown previously).

Dealer Account Activation & Programming (cont'd)

4. In the main programming "**SYSTEM SETTINGS**" screen, select **General Settings**.



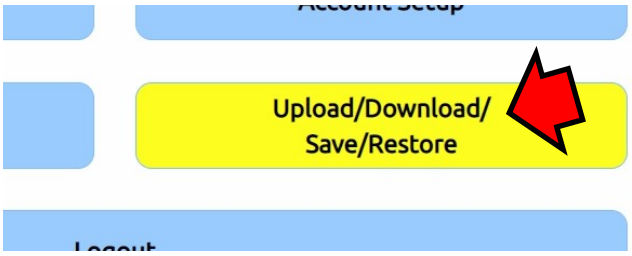
Enter the **Master Code** printed on the iSecure card in the **Master Security Code** field, then click **Save**.



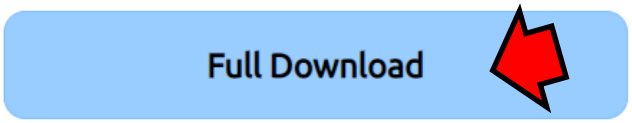
Any changes to the **Master Security Code** requires that you exit and re-enter the **iSecure Cloud Web Portal**.

5. Click **Log Out** to exit, then log back in to the iSecure Cloud Web Portal (www.iSecureByNapco.com) as described in step 1 and step 2. Exiting and re-entering ensures that the **iSecure Cloud Web Portal** and the **Master Security Code** are synchronized and the system is fully protected by your secure account password.

   When changes are made to the system, the **Upload/Download/Save/Restore** button on the main programming screen will appear yellow.



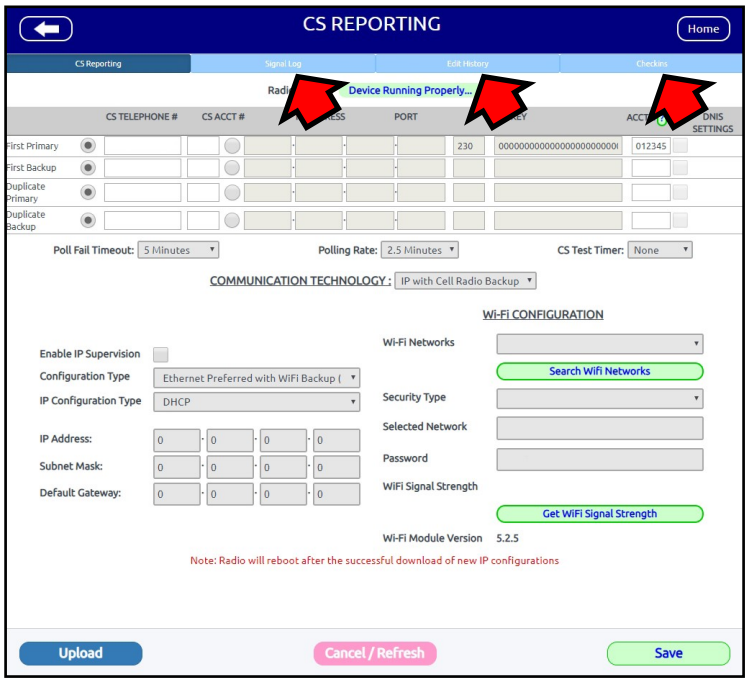
6. Click this yellow button, and click **Download All Changes**. (or click **Full Download** for new accounts accessed for the first time).



In the confirmation popup, click **Yes, download!** to send all changes to the **Go-Anywhere Smart Hub**.

Now that the system is synchronized with the **Master Security Code**, proceed to the next section to set up the central station communications.

Central Station CS Reporting Screen



At the top of this screen, three "tabs" are available (arrows): **Signal Log**, **Checkins** and **Edit History** logs for status and reporting information

Central Station Reporting Screen

Select **Central Station Reporting** and the above screen opens. In this screen you can change the reporting data, central station account numbers, supervision timeout durations and other selections appropriate for the installation and the service plan purchased. Always check that the radio communicator is active by ensuring the **Radio Status** indicates "**Device Running Properly…**", verify the correct **Radio #** appears at the very top of the screen, and to the right of the **Radio #**, enable the **Central Station Reporting** radio button.

Note: To ensure that the iSecure Cloud Web Portal has the latest configuration data stored in the Hub, click the **Upload Radio Status** button. Use this button the first time a radio communicator is to be managed by the Cloud Web Portal.

At any time you can change the reporting central station receiver telephone numbers, account numbers, IP reporting information and other settings by simply entering alternate data and clicking **Save**. Enable the appropriate radio button if backup or duplicate reports are to be sent, i.e. "**First Primary**", "**First Backup**", "**Duplicate Primary**", "**Duplicate Backup**". Other selections include:

CS TELEPHONE #
Enter all digits of the central station receiver telephone number including area code.

CS ACCT #
Enter all digits of the central station account number. **Note:** Both a **CS TELEPHONE #** and **CS ACCT #** must be entered in the fields, otherwise the **Save** button remains disabled.

IP-Based Reporting (to an IP Receiver)
In the **COMMUNICATION TECHNOLOGY** pull-down, there are three selections:

- **Cell Radio Only** (default)
- **IP with Cell Radio Backup**
- **IP Only**

If you wish to use IP-based reporting (radio or Dual Path) instead of telephone-based reporting, contact your central station and ask for the specific IP information (for example, Sur-Gard System II, Sur-Gard System V, Bosch D6100IPV6 or Bosch D6600 Receiver, with ITS-D6686 Ethernet Adapter via TCP/IP using standard line security central station receivers). To enter the required information for their receiver, including the **IP ADDRESS**, **PORT** number, encryption **KEY** characters, central station **ACCT #** (also known as *Account Code Field*, click the **"?"** icon and contact your central station for specific details regarding how they programmed their receiver to accept data) and **DNIS SETTINGS** number (if used). **Note:** For IP reporting, each digit if the **IP ADDRESS** must be 0-9 (do not use hex).

Poll Fail Timeout
The duration set determines how long the system will wait for a radio check-in packet. If not received, a Supervision signal will be sent to the specified central station. Select from the pull-down the appropriate **Poll Fail Timeout** duration available, depending on the service plan purchased.

CS Test Timer
The selections are Non, Daily or Weekly. If enabled, an automatic test report will be transmitted to the central station on the schedule selected when **First Primary** central station telephone number is configured. If **Cell Radio Only** is selected, Hub generated **Test Timers** are reportable signals and are forwarded to the central station.
Example: If a signal is sent to the central station, the supervision time counter will reset to that day. For example, if the supervision time is supposed to occur on March 25, but an alarm signal was tripped earlier on March 15, if no other signals are sent, the next time the radio will check in is in 30 days after the March 15 date.
The iSecure Cloud Web Portal also has the ability to send emails and text messages to dealers and/or customers (only available if supported by your service plan).

Enable IP Supervision
Check to enable the IP path of the integral dual path radio communicator (this selection is available depending on plan purchased).

Configuration Type
Click the **Configuration Type** pull-down to select the reporting pathway preference:

- Ethernet Preferred with Wi-Fi Backup
- Wi-Fi Preferred with Ethernet Backup
- Wi-Fi is Only IP Path
- Ethernet is Only IP Path

IP Configuration Type

- DHCP
- Static

Click the pull-down to select how the IP settings are configured. Select **DHCP** to have the IP address automatically assigned when the radio connects to the Internet, or select **Static** if you wish to manually designate a specific IP address that will remain permanently assigned to the radio.

Central Station Reporting Screen (cont'd)

IP Address
Subnet Mask
Default Gateway
Contact your central station for their **IP Address**, **Subnet Mask** (if used) and **Default Gateway**. The Default Gateway is the router used to forward all network data addressed outside the local network or local subnet, usually to the cable or DSL modem connected to the Internet service provider (ISP), and vice versa.

WI-FI CONFIGURATION
Wi-Fi Networks
Initially this pull-down field is blank; therefore click the **Search Wi-Fi Networks** button to look for the various Wi-Fi networks available in your area. **Note:** The search process may take up to 3 minutes (a warning popup will appear to confirm this duration). When the search process ends, select the Wi-Fi network you wish to use from the populated pull-down list. The selected Wi-Fi network name will appear in the **Selected Network** field (described below).

Security Type
From the pull-down, select the Wi-Fi security protocol to provide authentication and encryption between the Hub's internal radio communicator and the customer's Wi-Fi router; select either **Unknown**, **Disable**, **WEP** or **WPA2-Personal** (supported devices only).

Password
Type the password of the selected Wi-Fi network.

Selected Network
When the Wi-Fi network name is selected using the **Wi-Fi Networks** pull-down (described above), the selected Wi-Fi network name will appear in this field.

Wi-Fi Module Version
Displays the **ISEC-WIFI** module firmware version (installed inside the Hub) as retrieved from the firmware installed in the PC board circuitry.

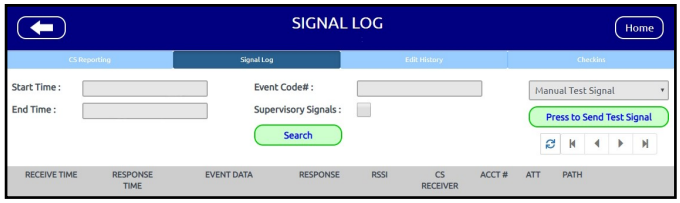
Upload Radio Status (button)
Click to ensure that the iSecure Cloud Web Portal has the latest configuration data stored in the Hub. This is rarely needed but should be used (button clicked) the first time a radio communicator is to be managed by the iSecure Cloud Web Portal. **Note:** Radio will reboot after the successful download of new IP configurations. **IMPORTANT:** Some police and/or fire departments require alarm permits (contact each department (do not dial 911) for confirmation).

Signal Log
Edit History
Checkins

At the top of the **CS Reporting** screen, click one of the three "tabs": **Signal Log**, **Checkins** (Check-in Log) or **Edit History** logs for status and reporting information, as follows:

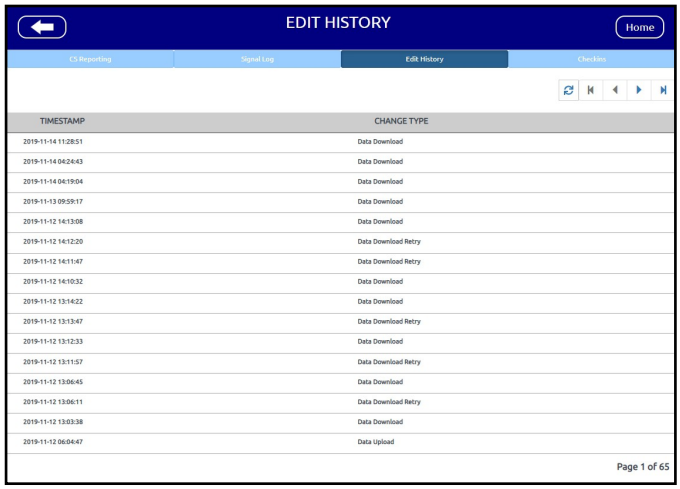
Signal Log

The Signal log displays the date and time reportable signals, troubles and alarms were received at the iSecure Cloud Web Portal. It also displays the event data received if the signal was processed without error (marked "OK"); the signal strength of the radio at the time the signal was received, the CS telephone number dialed and the number of attempts the radio made to deliver the signal. Select Press to Send Test Signal to manually initiate a test signal. For each signal the radio delivers, the system will try 8 times to reach the central station programmed. If the radio does not receive a kiss off, it will re-transmit the alarm and display a "2" in the log. After (another) 8 unsuccessful tries by the Cloud Web Portal to contact the central station, the radio will then output a "Fail to Communicate" signal.



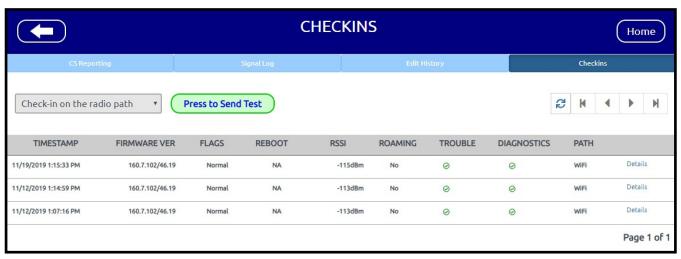
Edit History

This screen displays any time a radio has its configuration either uploaded or downloaded.



Checkins

The Check-in log displays radio transmissions that are not routed to the central station. These signals are used by the iSecure Cloud Web Portal to monitor the radio and indicate its status. Dealers can see the last check-in time (look at the **Timestamp** column). The remaining columns are for NAPCO technical support use. Radio "Check-in's" are dead-ended at the iSecure Cloud Web Portal, i.e. they are not sent to the central station but are tracked when IP reporting is not utilized ("**Cell Radio Only**" selected). If they are not received within the supervision time window, the system sends a *Loss of Supervision* signal to the central station.



1. Install the *Go-Anywhere Hub*

Place your ***Go-Anywhere Hub*** in a protected *central location* inside the premises, preferably in an elevated area (not on the floor) and near a standard un-switched / uninterruptable 120VAC electrical outlet.

- Place on a shelf, desk or wall mount
- Avoid proximity to electrical junction boxes, wireless telephones, wireless routers and transmitters (including baby monitors)
- Do not place in attics, utility, AV or computer closets
- Basement installation is NOT preferred
- Locations with proper ventilation and climate control are preferred

Go-Anywhere Hub

WALL MOUNTING

1. Mark the four mounting hardware locations. Use a level to ensure horizontal mounting.
2. Using #8 screws appropriate for the mounting surface, install the top two screws into mounting surface. **Note:** When mounting to hollow drywall or similar surface, we recommend using wall anchors or similar hardware appropriate for the installation.
3. Separate the Go-Anywhere Hub housing: With a flat head screwdriver, push in the two tabs at the bottom to unhook, then carefully separate the two parts of the housing .
4. Hang the rear housing by placing the top two keyhole-shaped holes over the two screws installed in step 2. Use the pre-installed Hanger Clip (see image below) to hang the front cover.
5. Install the two bottom screws (use #8 screws appropriate for the mounting surface) and tighten the two top screws. Do not over-tighten (to prevent the housing from distorting).
6. Power up using an un-switched 120VAC outlet (power wires can be snaked through the wall). Install and connect the 4AH or 5AH battery (not supplied), observing polarity; secure battery with Velcro strap.
7. Remove the plastic protective film from the face of the Go-Anywhere Hub.

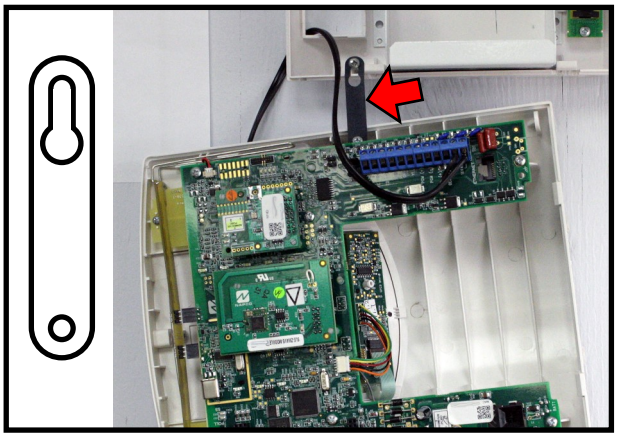
STAND-ALONE INSTALLATIONS

- If placing on a shelf or desk, install the supplied rubber feet on the bottom of the Go-Anywhere Hub
- Run the power adapter wiring to the nearest un-switched 120VAC outlet and plug in
- Install and connect the 4AH or 5AH battery (not supplied), observing polarity; secure battery with Velcro strap
- Remove the plastic protective film from the face of the Go -Anywhere Hub.

Voice Prompt Volume

To control the Hub *voice prompt volume*, press the following keys at any keypad in the system:

- ***On/Off*** = **1** + **ENTER**
- ***Louder*** = **2** + **ENTER**
- ***Softer*** = **3** + **ENTER**



Use Hanger Clip to simplify wall mounting and wiring

Go-Anywhere Hub Rear Access Descriptions

Note: The rear terminals, headers and sockets are not accessible after wall mounting.

TERMINAL DESCRIPTIONS

Configure all inputs and outputs using the iSecure Cloud Web Portal at www.iSecureByNapco.com. Located at the bottom of the Go-Anywhere Smart Hub PC board, the 11 terminals are described as follows:

Z7 (–): Connects to the negative terminal of the two-wire smoke sensor (zone 7). Requires **ISEC-2WF-MOD** *2-Wire Fire Sensor Module*.

FIRE PR+: Connects to the positive terminal of the two-wire smoke sensor. Requires **ISEC-2WF-MOD** *2-Wire Fire Sensor Module*.

Z8 (–): Connects to the negative terminal of the two-wire smoke sensor (zone 8). Requires **ISEC-2WF-MOD** *2-Wire Fire Sensor Module*.

GND: Common ground terminal.

GRN: Remote Bus connection, see wiring diagram.

YEL: Remote Bus connection, see wiring diagram.

PGM (+): This terminal is a low current continuous +12V output. Wired with the active trigger terminal **PGM (–)** below, this PGM output can be programmed to either toggle on/off or remain momentarily energized (for about 5 seconds) upon a keyfob button press. Program in **KEYFOB SETTINGS**, **KEY FUNCTIONS** column (for **Key #3** or **Key #4**, select **AuxOutput/PGM Toggle** or **AuxOutput/PGM Momentary**). This terminal can be wired to an LED or to the red (+) of the model RB1000 Relay Board (the RB1000 is a low-current Form-C relay that provides an additional dry contact output). This RB1000 relay may be used to activate access control devices, locks, etc.

PGM (–): The active trigger for the PGM (when triggered, changes from open collector to active). This terminal can be wired to the black (–) of the model RB1000 Relay Board (see description of terminal **PGM (+)**, above).

BELL (+): Connect the alarm sounding devices (self-contained sirens, speakers or a mechanical bells) this terminal and **BELL (–)**. Any self-contained external siren requiring a 12V supply can be connected. When connecting a mechanical bell, it must be supervised using a 2.2k Ohm resistor. To connect 8 Ohm speakers, use a Siren Driver with the proper polarity observed. **Note:** Refer to the Standby-Battery Calculation Worksheet (page 72) for standby and alarm current specifications. **Note:** In NFPA Household Fire and carbon monoxide installations, only a single siren or bell can be used on this bell circuit.

BELL (–): Wire this terminal to the black (–) of the model RB1000 Relay Board. See terminal **BELL (+)**, above..

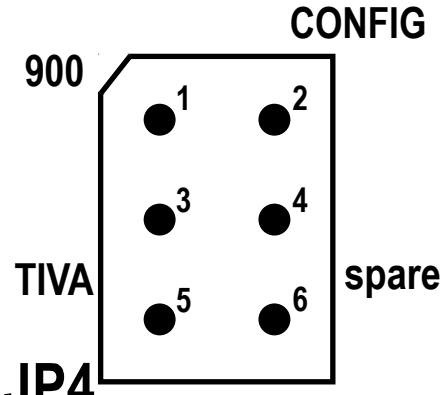
16VAC: (see **16VAC**, below)

16VAC: AC In (2 non-polarized terminals). Connect to the supplied 20VA TRF12 Class 2 transformer using appropriate gauge wire. **Important:** Do NOT connect the wall adapter to a switched AC outlet.

HEADER / SOCKET DESCRIPTIONS

Also refer to the Wiring Diagram on page 79.

J1 Optional Z-WAVE Board insert
J2 Optional Wi-Fi PC Board insert
J3 Wi-Fi PC Board Insert
J4 LTE Radio PC Board insert (for pre-installed LTE radio module)
J5 LTE Radio PC Board insert (for pre-installed LTE radio module)
J7 LTE Radio PC Board insert (for pre-installed LTE radio module)
J9 900MHz Transceiver Board insert
J11 2-Wire Fire PC Board insert
J15 Voice prompt mini-sounder socket
J14 Local keypad socket (reserved for future use)
J16 Siren socket
J19 Optional 345MHz receiver socket (reserved for future use)



Go-Anywhere Hub "JP4"

JUMPER / SHUNT DESCRIPTIONS

Also refer to the Wiring Diagram on page 79.

J8 Cut to enable Control tamper as keypad 1 tamper
JP2 Insert shunt on power up to create Cold Start, then remove (see page 61 for the full Cold Start procedure)
JP4 Configuration jumper (Technical Support use only)

2. Install the Keypad

SELECT MOUNTING LOCATION

Keypad installation is basically identical for all models. The **ISEC-WL-KEYPAD** (in Kit 1) is battery powered, requiring one CR123 Lithium battery (with optional 2nd battery for extended life). Both the **ISEC-WL-TOUCH 4.3" Color Touchscreen Keypad** (in Kit 2) and the **IBR-TOUCH-WL 7" Wireless IoT Touchscreen** (in Kit 3) require an un-switched 120VAC electrical wall outlet to supply power to the 12V@1A power adapter (select a location that allows the power wires to be hidden within the mounting surface). Mount keypads within easy reach of the exit/entry door(s) to simplify entry or exit. To ensure a constant wireless connection, mount the keypad between approximately 15 and 100 feet of the Go-Anywhere Smart Hub, where you find good signal strength between the keypad and the Go-Anywhere Hub. Mount the keypad indoors only, avoiding high condensation areas such as bathrooms. Avoid mounting where direct sunlight or bright light shines directly on the display screen. Install in indoor locations only. Environmental temperature limits: **ISEC-WL-KEYPAD** LCD keypad: 32°F to 122°F. **ISEC-WL-TOUCH** 4.3" Color Touchscreen Keypad: -10°F to 140°F. **IBR-TOUCH-WL** 7" Wireless IoT Touchscreen: 32°F TO 122°F.

ISEC-WL-KEYPAD
Wireless Battery-Operated Standard Keypad

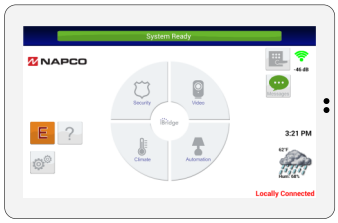
ISEC-WL-TOUCH Keypad Diagnostics (Optional)

See **ISEC-WL-TOUCH "System Diagnostics"** on page 65 to help you find the optimum mounting location for your **ISEC-WL-TOUCH** keypad by displaying the signal strength of the 900MHz radio signal link between the **Go-Anywhere Hub** and the **ISEC-WL-TOUCH** keypad.

ISEC-WL-TOUCH
Wireless 900MHz Touchscreen

KEYPAD INSTALLATION

1. Detach the keypad rear case by inserting a flat head screwdriver into the two slots at the bottom, then push and turn the screwdriver to unhook the two plastic tabs.
2. At the final mounting location, use the keypad rear case as a template to mark the mounting holes (always use a level to ensure horizontal mounting). For keypads powered by the wall adapter, mark the center hole for the power wire.
3. Install the Sliding Label Plate (Kit 1 **ISEC-WL-KEYPAD** model only):
   - With the handle facing forward, affix the label and felt backing.
   - With the handle facing forward, push the Plate down the guides at the rear of the keypad until it snaps into place.
4. Drill the two keypad mounting holes (four holes with the **IBR-TOUCH-WL**) in the mounting surface. When mounting to hollow drywall or similar surface, we recommend using wall anchors or similar hardware appropriate for the installation.



IBR-TOUCH-WL
Smart 7" IoT Touchscreen (Requires network connection)

For keypads powered by the power adapter:

- Using a 1/2" drill bit, drill the center hole and snake the power wire inside the wall and out through the drilled center hole. Do not connect the power adapter to the electrical wall outlet at this time.
- Firmly connect the power wire connectors and then push the wire and the connectors back into the drilled wall center hole until the rear case is flat against the wall surface. Insert screws through the rear case mounting holes and secure. **Important:** Do not over-tighten the mounting screws; over-tightening may distort the rear case.

5. Power the keypad: For the battery-powered **ISEC-WL-KEYPAD**, insert battery (provided) into 1 of the 2 battery holders; otherwise, power up the power adapter.
6. Assemble the keypad by placing the top edge of the keypad front case over the two hooks at the top of the rear case. Push the bottom of the keypad until it snaps together.
7. Power the Go-Anywhere Hub and test the keypad signal strength: The system will not allow arming and disarming without a valid Wi-Fi link. Test the keypad by arming STAY (press **1 2 3 STAY**, and the keypad display will read **ARMED STAY**) and disarming (press **1 2 3 ENTER**, and the keypad display will read **READY**). **Note:** The keypad factory default User Code is **1 2 3**; this can be changed later.

ADD AN ADDITIONAL KEYPAD

Program the Go-Anywhere Hub by entering the "**RF ID #**" (printed on the sticker to located on the back of the keypad) into the iSecure Cloud Web Portal, as follows: Click **Wireless Modules** > **Keypads**, then complete all of the fields for each additional keypad. When finished, click **Save** and click **Upload/Download** to send the data to your **Go-Anywhere Hub**.

IMPORTANT: All wireless devices, including Z-Wave devices, must be signal tested with all enclosure covers fully closed, including the Go-Anywhere Hub.

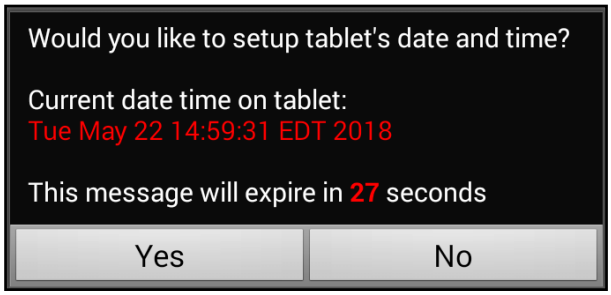
IMPORTANT: The **ISEC-WL-TOUCH** LCD display is made of glass, therefore avoid excessive mechanical shock or that application of strong pressure on the LCD surface. In addition, the polarizer used on the LCD surface can be scratched if proper care is not taken. To clean dust or dirt, wipe gently with a lint-free cloth that is damp with isopropyl or ethyl alcohol only. ***Do NOT use water, ketone or aromatics and never scrub the surface***!

Configure the IBR-TOUCH-WL 7" Touchscreen

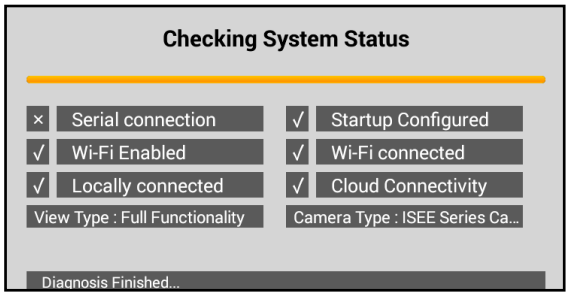
1 With power applied to the Go-Anywhere Smart Hub, power the IBR-TOUCH-WL. The unit will start within about 5 seconds (the unit can be manually powered by pressing and holding the small button on the right side for 10 seconds). Upon power up, the **Setup Wizard** will automatically start (follow the sequence of images starting with step 5). If the **Setup Wizard** does not automatically start, press and hold the **System Settings** ("gear") icon, enter your Dealer password, then tap **Setup Wizard**.

System Settings button

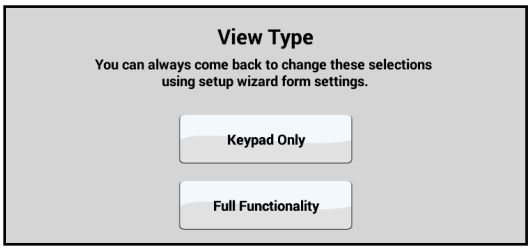
2 Tap **Yes** and set the date, time and Time Zone (if necessary). **IMPORTANT:** Outdated digital certificates will disallow connection to your security system, as well as inhibiting necessary automatic firmware downloads.



3 Wait for the system diagnostics process to complete. Functional components are marked with a check; items not configured or disabled are marked with an "x". Selections are blank when the **Setup Wizard** is run for the first time. Tap **Configure** to continue.

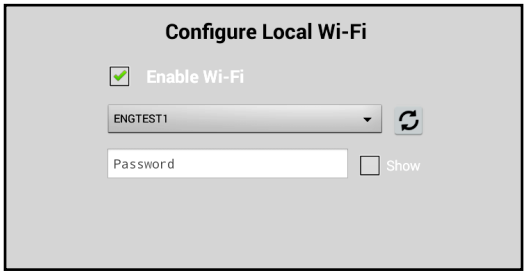


4 Select how the IBR-TOUCH-WL will be used. If it will only be used as a security system keypad, tap **Keypad Only** (jump to step 6). To include video camera and Z-Wave functions, tap **Full Functionality**.

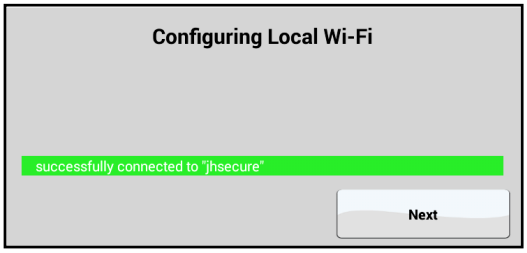


5 If you have an ISEE-WAP with existing older iSeeVideo cameras, tap **ISEE Series Cameras**; if your system includes the newer **ISV2** models, tap **ISV2 Series Cameras**; for systems without cameras, tap **No Cameras** (cameras can always be added later). **Note:** **ISEE** and **ISV2** cameras cannot be combined.

6 To connect through the customer's wireless router, check **Enable Wi-Fi**; select the router name from the pull-down and have the customer type their router Password (tap the "Refresh" button to the right of the pull-down if the customer's router is not listed). When finished, tap **Save & Next>>**.

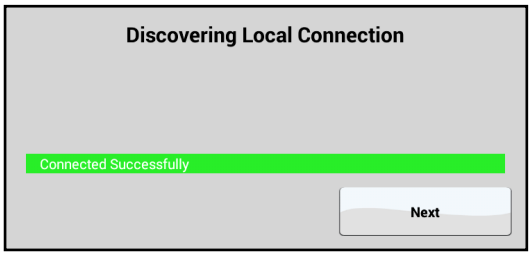


7 Wait until the message indicates the connection to the customer's wireless router is complete, then tap **Next**.

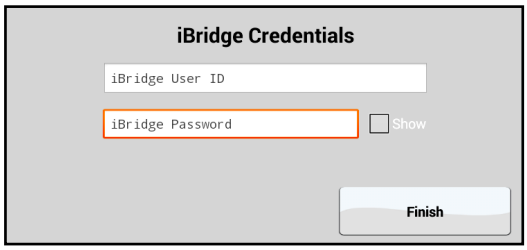


Configure the IBR-TOUCH-WL (cont'd)

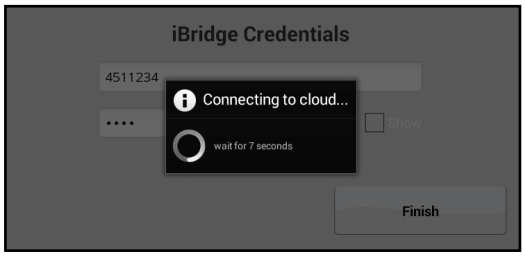
8 As shown in the image below, the system will then automatically try to connect the IBR-TOUCH-WL locally through Wi-Fi, provided the Hub is connected either by the wired Ethernet connection or the Wi-Fi connection. When connected, tap **Next**. If you selected **Keypad Only**, jump to step 11.



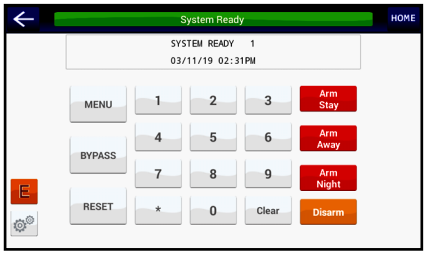
9 The IBR-TOUCH-WL will automatically attempt to connect, through the "cloud", to the NAPCO iSecure account. Enter your administrator account **User ID** and **Password** and tap **Finish**.



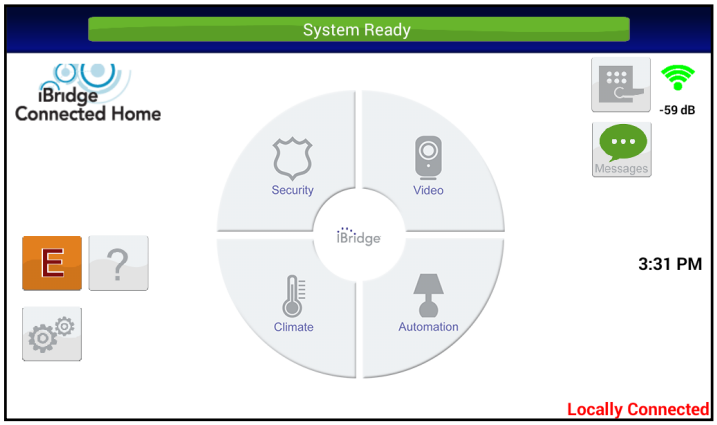
10 Upon connection to the Internet-based account for the iSecure system, the resulting keypad shown in step 12 will be configured for the payment plan selected by the customer. For example, smart phone notifications and camera video.



11 If you selected **Keypad Only** in step 7, the virtual security system keypad will appear (shown below). Stop here -- you're finished!
If you selected **Full Functionality**, you're almost finished...go to next step...



12 Be sure to verify the touchscreen display reflects the current status of the security Hub. **Note:** The red text at the bottom right describes the connections. In this example, the IBR-TOUCH-WL is connected to the Go-Anywhere Smart Hub through its Wi-Fi connection.



3. Install Motion Sensors

The **ISEC-MOTION** provides protection by detecting motion in protected areas.

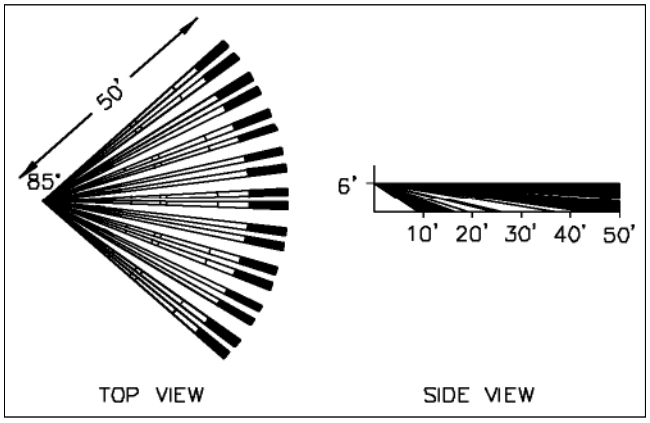
GENERAL DESCRIPTION

The ISEC-MOTION is an advanced PIR sensor designed for use with Napco's wireless receivers. The unit is powered by two supplied 3-volt lithium batteries (estimated battery life 3 years). When battery voltage drops below normal, a low-battery report will be sent to the receiver (replace with Duracell DL123A, Varta/ Power-One CR123A or Panasonic CR123A only). Coding switches are not used in the ISEC-MOTION. Each transmitter has a unique factory-programmed RF ID code (printed on the unit) that distinguishes itself to the receiver. (**Note:** Be sure to enter all numbers and/or letters, including leading zeros, if any).

SPECIFICATIONS

PIR Coverage (l x w): 50' x 50' (15.2m x 15.2m) at 20°C (68° F), typical.
Operating Temperature: 0° to +50°C (32° to 122°F)
Mounting: Wall or corner, 10' (3m) max.
Dimensions: 4.5" x 2.5" x 1.7" (11.4cm x 6.4cm x 4.3cm) (HxWxD)
Shipping Weight: 6.4oz (181gm)

STANDARD LENS



Standard Lens coverage pattern for 6' mounting height.

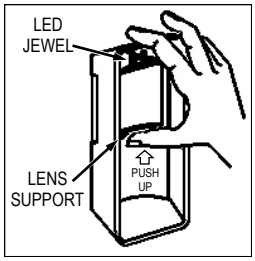
FEATURES

- Signal Selective Processing for reliable operation
- Unique circuit design protects against false alarms due to radio-frequency interference
- Vertical and horizontal aiming capabilities
- Dual-element sensor
- Lens Bank of optional accessory lenses
- Large lens area assures high sensitivity
- Small size with ample wiring space
- Corner mountable
- Built-in Tamper microswitch

REPLACING THE LENS

The lens is "sandwiched" between the front case and a Lens Support insert, which also serves to hold the LED jewel in place. To install one of the accessory lenses, proceed as follows.

1. To open the case, insert a small screwdriver in the slot at the bottom and push up slightly. Remove the front cover.
2. Push up on the lower edge of the Lens Support until it is clear of its retainers, then pull out the support from the bottom. Be careful not to dislodge the LED jewel. Note: If the LED jewel pops out, reinsert it with the small index key positioned at the top.
3. Slide out the lens and install the replacement.
4. Replace the Lens Support: Slip the Lens Support under the top guides with its two tabs straddling the LED jewel, then push in at the bottom until the Lens Support snaps into place. Removing Lens Support.

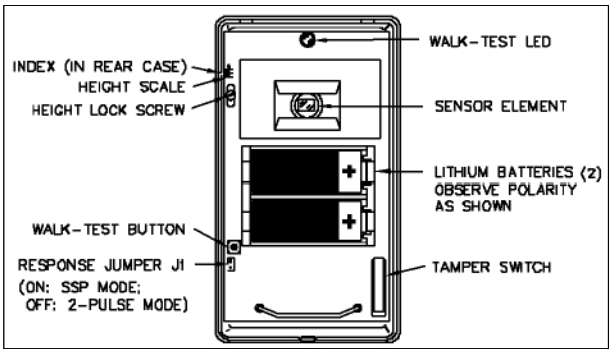


INSTALLATION

An assortment of "push-thru" holes is provided in the rear case for wall or corner mounting. Install the two lithium batteries as shown in the illustration below. Loosen the Height Lock Screw and set the board's height scale to the mounted height of the unit. Retighten the screw. To reduce range if necessary, set height scale at a higher number than actual mounting height of unit. Do not point the unit at sources of heat, such as radiators, space heaters, etc.

WALK TESTING

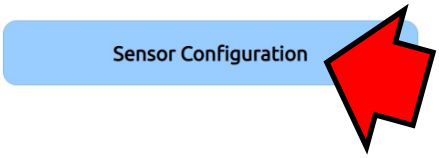
The LED will light in the Walk-Test Mode only. Allow at least 3 minutes for the unit to settle. Press the Walk-Test Button to access the Walk-Test Mode for 5 minutes.
Walk out to the maximum range and walk across the field of coverage. The LED will light whenever motion is detected. Check for environmental disturbances with all disruptive devices (heaters, air conditioners) on and no human activity within the coverage area. Adjust beams laterally by removing the Lens Support (see REPLACING THE LENS) and sliding the lens slightly left or right. To block a problem zone, apply a piece of lens foil (supplied) to the inside segment of the lens representing that zone.



SETTING THE OPERATING MODE

The ISEC-MOTION comes set for operation in the Signal Selective Processing (SSP) Mode. To change to the fixed 2-pulse bipolar mode for use with the Long-Range Lens (LENS840), Barrier Lens (LENS818) or other lens with a limited number of beams, remove the Response-Mode Jumper, J1.

- To program the Motion sensor in the iSecure portal, see page 45.



4. Install Glass-Break Sensors

The **ISEC-GLASSBREAK** is an advanced wireless acoustic glass-break sensor for use with all iSecure-Series *Go-Anywhere Hubs* and receivers. Each sensor has a unique RF ID code (printed on the rear housing) that distinguishes itself to only your *Go-Anywhere Hub*.

The **ISEC-GLASSBREAK** is an advanced wireless acoustic glass-break detector for use with the iSecure **Go-Anywhere Smart Hub** and receivers. Each transmitter has a unique RF ID code (printed on the sensor module and on the rear case) that distinguishes itself to the receiver. Refer to Go-Anywhere Smart Hub instructions for entering this code and its checksum digit into the Hub. Be sure to enter all numbers and/or letters, including leading zeros, if any.
The detector is powered by two type DL123A or CR123A 3-volt lithium batteries, which are factory installed. To energize the unit, simply install the supplied Power-Up Jumper across pins JP1 near the positive terminals of the batteries.

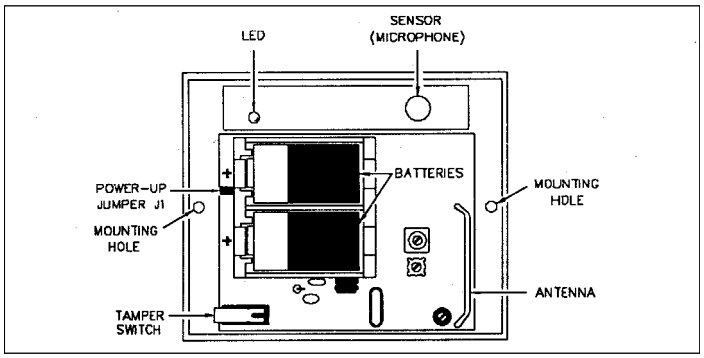


Fig. 1. ISEC-GLASSBREAK detector, cover removed.

SPECIFICATIONS

Microphone: Electret, omnidirectional
Temperature Range: 32°F to 120°F (0°C to + 50°C)
Range of Coverage (radius distance from sensor):
Plate Glass, 25' (7.6m)
Tempered, Wired, or Laminated Glass, 20' (6m)
Note: (1) Use 20' (6m) radius if unsure of glass type. (2) If not using a Sentrol 5709-C Tester to verify range, reduce range to 15' (4.5m) for windows with blinds or unlined drapes. (3) Reduce coverage 50% for armor-coated glass.
Glass Thickness:
Plate Glass, 3/32" to 1/4" (2.4 to 6.4mm)
Tempered Glass, 1/8" to 1/4" (3.2 to 6.4mm)
Wired Glass, 1/4" (6.4mm)
Laminated Glass, 1/8" to 1/4" (3.2 to 6.4mm)
Dimensions: 3.13 x 4.24 x 1.7" (8.0 x 10.8 x 4.3cm)
(h x w x d) Shipping Weight: 7.5oz (213gm)

FEATURES

- Superior immunity to false alarms
- Excellent detection, even through blinds and light drapes
- 25' radius
- Automatic test for easy installation
- "Hand-clap" test for sensor verification
- Includes lithium batteries

MOUNTING

Note: The ISEC-GLASSBREAK may be mounted in any position with no degradation in performance. However, for reference purposes in this text, the unit will be considered oriented with the antenna at the right, as shown above.
The detector mounts with two #6 screws (supplied). The rear case may be used as a template to mark mounting holes on the wall.
The sensor must be in direct line of sight of all windows being protected. Reliable detection cannot be expected around corners, in other rooms, etc.
For optimum false-alarm immunity, avoid installing the unit

- in rooms with lined, insulating, or sound-deadening drapes;
- in rooms with closed wooden window shutters inside;
- in rooms smaller than 10' x 10' (3m x 3m), and in rooms with multiple sounds, such as kitchens, glass booths, noisy areas, garages, etc.
- within 4' (1.2m) of noise sources such as televisions, speakers, sinks, doors, etc.
- on ceilings higher than 15' (4.5m), if mounting on ceiling;
- on 24-hour loop applications (perimeter loop okay);
- where white noise (such as air compressor noise) is present (may cause false alarms by saturating glass-break frequency spectrum).

Wall Mounting

Since the sound of breaking glass travels outward from the source, the best location for the ISEC-GLASSBREAK detector is on the wall opposite the windows being protected (assuming, of course, that the wall is within the sensor's range). Detection is reduced with same-wall mounting since such detection is partially dependent upon sound reflected off the opposite wall.

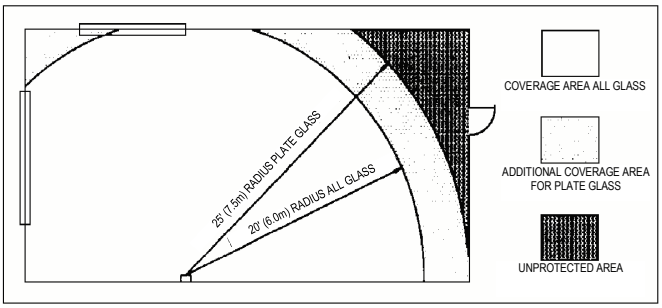


Fig. 2. Typical coverage pattern for wall-mounted units.

Ceiling Mounting

Similarly, a ceiling-mounted sensor will detect better if mounted 6' to 10' (2—3m) away from the glass, rather than directly above it. Mount the detector on any type of ceiling in direct line of sight of the windows being protected, at least 1' (0.3m) and preferably 3' (1m) from the glass. See Fig. 3.

Installation Notes

1. The unit is designed to detect the shattering of framed glass mounted in an outside wall. Testing the sensor with unframed glass, broken bottles, etc. may not trip the sen-

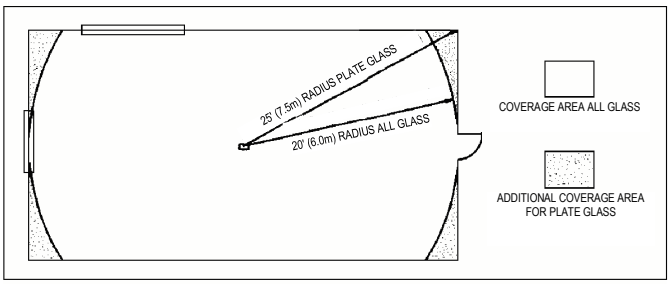


Fig. 3. Typical coverage pattern for ceiling-mounted units.

sor. The unit typically does not trip to glass-break tests in the middle of a room, as such breaks are false alarms.

2. False alarms are most likely to occur when installed on a 24-hour loop in glass airlocks and glass vestibule areas, when mounted above sinks, when used in residential car garages, and in other small, acoustically live rooms and rooms where multiple sound can reflect and eventually duplicate the glass-break frequency pattern. For occupied-area glass-break protection in such applications, the use of shock sensors is recommended.
3. Installing the unit on 24-hour loops will increase false alarms. The ISEC-GLASSBREAK is recommended for perimeter loops and is designed to function without false alarms in occupied areas. On a 24-hour loop, which is armed all day, all night, every day, the false alarm technology will be pushed to its limit since some sounds in some conditions can duplicate the points on the glass-break pattern that the unit detects. Install the unit on a perimeter loop, which is armed whenever the door and window contacts are armed. For occupied-area installations, the ISEC-GLASSBREAK's false-alarm immunity is best in rooms with only moderate noise.
4. The unit detects the shattering of glass. As with all glass-break detectors, it may not consistently detect cracks in glass or bullets that break through the glass or break out the glass. Glass-break detectors should always be backed up by interior protection.

TESTING

Preliminary

Use a Sentrol Model 5709-C hand-held tester (available separately) to place the detector into its test mode and for all functional testing.

Set the tester for tempered glass. Holding the tester speaker directly over the sensor, activate the tester. The detector will go into alarm (LED will come on for about 4 seconds), then go into the test mode for one minute. While in the test mode, the detector's LED will blink continuously. Extend test-mode time by firing the tester at least once a minute.

Testing the Sensor

The 5709-C tester has a setting for each type of glass. The tester should always be set for Tempered or Laminated glass (either is correct and both have the same range) unless the installer is certain that the glass to be protected is plate glass. Holding the tester near the surface of the glass, aim the tester at the detector and hold down test button. If drapes or blinds are present, test with the hand-held tester behind the closed drapes or blinds (do not use detector with heavy or lined drapes). If the detector is mounted on the same wall as the glass, point the tester at the opposite wall.

If the LED on the detector comes on for about 4 seconds when the tester is triggered, the glass is within detection range. If the LED does not come on but just continues to blink, reposition the detector closer to the windows and retest. This may require the use of additional detectors in order to achieve the desired coverage. In the unlikely event that the detector does not respond within its stated range of coverage, check the battery in the tester; a new battery will likely restore range.

The ISEC-GLASSBREAK detector will automatically revert to its normal operating mode approximately 1 minute after the last test.

Note: Room acoustics can artificially extend the range of a glass-break sensor. The specified range of the ISEC-GLASSBREAK detector has been established for worst-case conditions. While the sensor will likely function at additional range, it may miss a minimum output break, or room acoustics may be changed at some future time, bringing sensor range back into normal 20' (6m) conditions. Do not exceed the rated range of the sensor, regardless of what the tester shows.

Test-Mode Operation

The ISEC-GLASSBREAK ignores most false alarm sounds, including glass break testers. In order to test the ISEC-GLASSBREAK detector, a test mode is used. In its test mode, sensor processing of the glass-break pattern in the upper and lower frequencies is disabled, thus the sensor is listening only for the midrange frequencies, which the tester produces. It is the midrange frequencies that determine sensor range.

In the normal operating mode, the LED does not blink unless the sensor hears a loud sound. In normal operation, the ISEC-GLASSBREAK detector will not be tripped by the tester unless the tester is held right up against the sensor.

Note: Each time the detector goes into alarm, it also goes into the test mode for one minute.

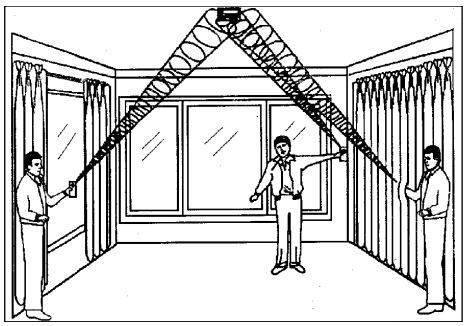
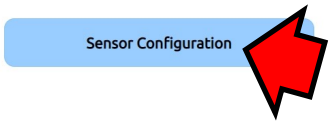


Fig. 4. Testing the sensor.

Hand-Clap Test

The ISEC-GLASSBREAK can be tested by the installer or the end user while in its normal mode simply by clapping loudly under the sensor. The LED will blink twice, but the detector will not trip. This verifies visually that there is power to the detector and that the microphone and circuit board are functioning. The hand-clap activation is momentary so there is no appreciable effect on battery life.

See page 46 for full programming information.



5. Install Window / Door Transmitters

GENERAL DESCRIPTION

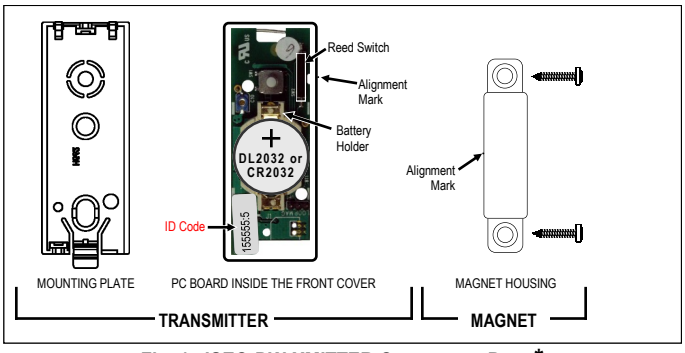


Fig. 1. ISEC-DW-XMITTER Component Parts*

The ISEC-DW-XMITTER is a low profile window/door transmitter designed for use in Napco iSecure wireless systems. Used with the supplied magnet, the transmitter functions as a window/door sensor. The ISEC-DW-XMITTER is powered by a 3-volt lithium battery (Energizer CR2032 or Duracell DL2032), that powers the transmitter for up to 5 years. When the battery cell voltage drops below normal, a low-battery report is sent to the **Go-Anywhere Smart Hub** and "E05" (followed by the zone number) will appear on the keypad display.

INSTALLATION

The PC board is factory installed in the transmitter front cover **and must not be removed**. The magnet and transmitter can be mounted in any orientation as long as the alignment marks are placed side-by-side and the magnet is placed up to 5/8" of the transmitter, depending on mounting surface (for reference purposes in this text, the transmitter will be considered oriented with the reed switch at the top, as shown in Fig. 1).

1. **Open the case.** Remove the ISEC-DW-XMITTER transmitter cover from its Mounting Plate by pressing the tab and lifting the Mounting Plate from the cover.
2. **Remove silk strip to activate battery cell.** Battery is preinstalled. Ensure cell remains inserted in its holder after removing silk strip. **Note:** When replacing a weak battery, always remove the old battery from the edge of the battery holder without touching its metal terminals. Always observe polarity; with the positive (+) terminal facing up, press the cell into the holder (see Fig. 1). ***Do not insert upside down***.
3. **Select transmitter location.** Avoid mounting the transmitter near the floor. Low level mounting can reduce transmission range and may subject the transmitter to damage.
4. **Install transmitter Mounting Plate and Magnet.** Use #6 flat-head screws or double-sided tape (supplied) to secure. Do not overtighten the screws securing the Magnet Housing. Observe internal magnetic reed switch alignment marks on both the transmitter Front Cover and Magnet Housing. Mount Magnet up to 5/8" of the transmitter Front Cover. If mounting the Magnet with double-sided tape, the Magnet Housing tabs may optionally be removed--***use a utility knife only***--***do not bend or break off tabs*** (see Fig. 2).

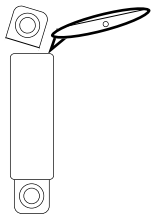


Fig. 2. Remove Magnet Housing tabs with utility knife only.

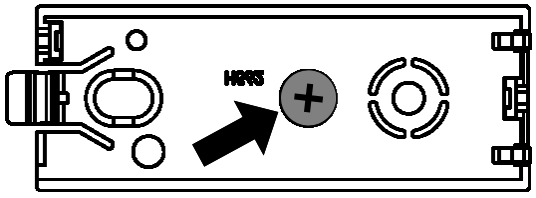
5. **Make note of the 6-digit ID code** with checksum digit printed on the inside sticker. Be sure to make note of ALL numbers and/or letters, including leading zeros, if any. This data will be used when programming the Go-Anywhere Smart Hub in step 7.
6. **Close the transmitter case.** Close by engaging the retaining tabs near the reed switch, then snapping the Front Cover to the Mounting Plate.
7. **Program the Go-Anywhere Smart Hub.** Each transmitter has a unique factory-programmed ID code that distinguishes itself to the receiver. The ID code is located on the rear of the Mounting Plate. **Note:** The ISEC-DW-XMITTERs included with the ISEC-KITs are pre-programmed; only new transmitters require the following programming steps: Enter (a) the zone number to which the transmitter will be mapped; (b) the 6-digit ID code with checksum digit; and (c) the wireless point number. See the Go-Anywhere Smart Hub installation instructions for how to enter the ID code and checksum digit; be sure to enter all numbers and/or letters, including leading zeros, if any.

Caution: Changes or Modifications not approved by NAPCO may void the user's authority to operate the equipment. This device may not cause interference. This device must accept any interference, including interference that may cause undesired operation of the device.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. **Caution:** Changes or modifications not expressly approved by manufacturer could void the user's authority to operate the equipment.

APPLY LABEL OVER SCREW HEAD

Place small individually supplied label (.375" dia., part # LA2867LF) over screw head (see arrow) to prevent shorting battery terminals.



***Note:** Plastic housing and PCB design may vary from images in this document.

6. Install Smoke Sensors

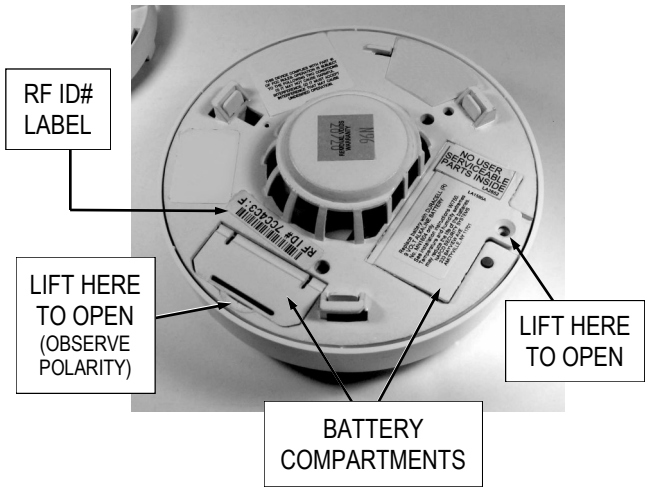
Description: The ISEC-SMOKE is a high-quality photoelectric smoke detector with built-in supervised digitally-coded radio transmitter. It is compatible with Napco's iSecure-series system that monitor alarms, restores, low battery and status.

During normal operation, the LED on the ISEC-SMOKE flashes once every 30 seconds. As soon as smoke is detected, the ISEC-SMOKE sounds a local alarm and the transmitter sends an alarm signal to the supervised receiver. The alarm signal is repeated every 10 seconds thereafter as long as smoke is still present. A restore report is sent when the smoke detection chamber clears. Supervisory status reports are sent from the ISEC-SMOKE every hour.

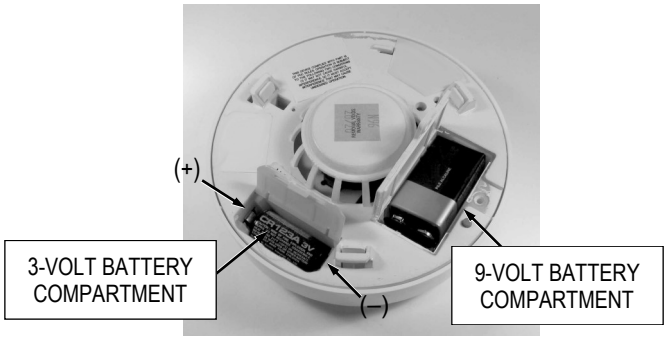
Coding switches are not required or used in the ISEC-SMOKE. Each transmitter is assigned a unique identification code number at the factory.

Step 1. Remove the mounting plate. Remove the ISEC-SMOKE mounting plate by turning the plate counter-clockwise and pulling it up.

Step 2. Identify components. Examine the ISEC-SMOKE to identify the component locations.



Step 3. Install battery. Place one 3-volt lithium Duracell DL123A, Varta/Power One Model CR123A or Panasonic CR123A NEGATIVE END FIRST in its battery compartment, observing correct polarity (**see page 21**). Connect one 9-volt Duracell MN-1604 alkaline battery and place it into its battery compartment. **Install batteries and enroll the ISEC-SMOKE into the Hub before mounting**.



The smoke detector and transmitter are powered by one 9-volt alkaline battery and one 3-volt lithium battery (supplied) which can power the unit for at least one year. If the battery voltage drops below normal, a low-battery report will be sent to the receiver with any status or alarm transmission. If a low-battery condition is indicated, always replace both batteries.

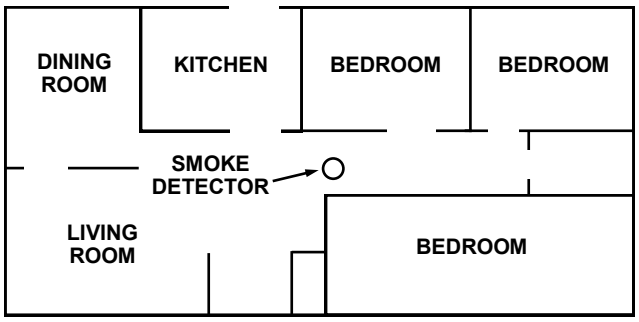
NOTE: Temperature and humidity extremes may reduce the life of the batteries. In addition, the ISEC-SMOKE detector is designed to prevent re-mounting to the mounting plate without the detector battery installed.

Use Only Batteries Specified In Marking. Use of A Different Battery May Have A Detrimental Effect On Detector Operation.

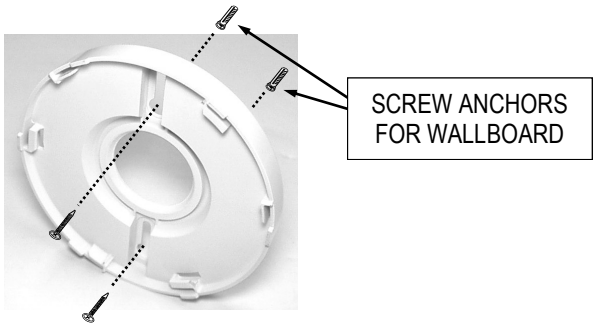
continued ⟶

6. Install Smoke Sensors (cont'd)

Step 4. Pick smoke-detector location. Referring to the NFPA standard on page 22, select a suitable location to mount the ISEC-SMOKE.
Note: *Mounting the ISEC-SMOKE on foil-backed wallpaper is NOT recommended because the radio range will be reduced.*



Step 5. Install mounting plate. Use the two screws and anchors provided to attach the mounting plate to the wall or ceiling.

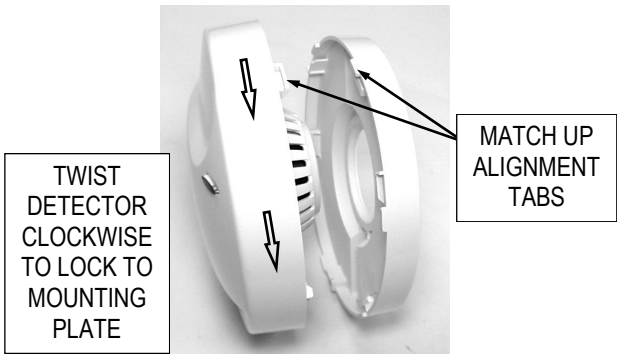


Step 6. Map the ISEC-SMOKE Transmitter. Enter the following:

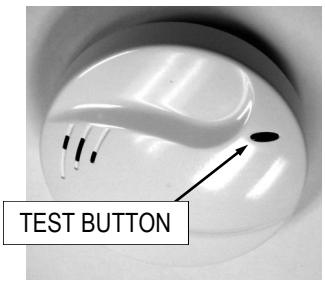
- the zone to which the transmitter will be mapped;
- the 6-digit RF identification number/1-digit checksum number printed on the transmitter (include all numbers and/or letters and leading zeros, if any); and
- the transmitter point number ("1").

NOTE: In fire alarm installations, the Hub must be programmed to activate the fire alarm bells or horns upon detection of a fire.

Step 7. Attach the ISEC-SMOKE to mounting plate. Match up alignment tabs on detector and plate. Turn detector clockwise until it locks into place.



Step 8. Test system weekly with unit mounted. If the system is monitored, notify central station of impending test. Press and hold the **Test** button for about 5 seconds and release when the sounder turns on. While holding the button down, the LED will start to flash rapidly indicating it is about to go into alarm. Do not hold the button down longer than 10 seconds or you will *Silence* the unit after the alarm is sounded (see **Silencing the Unit / Silence Mode** at right). Verify that the ISEC-SMOKE triggers the correct zone on the Hub and that the correct report is sent to the central station.



NOTE: Smoke detectors are not to be used with detector guards unless the combination has been evaluated and found suitable for that purpose.

Silencing the Unit / Silence Mode
If the unit is in alarm due to a smoke condition, it will stop sounding when the smoke condition has cleared. However, if you want to *temporarily silence* the sounder, press and hold the **Test** button for more than 10 seconds. During this *Silence Mode*, the unit will not react to any smoke nor report any alarms but will chirp every 30 seconds (without a simultaneous LED flash) to remind you it is in *Silence Mode*. It will exit *Silence Mode* after approximately 5 minutes or less on its own. **Note:** If smoke is still present in the chamber after exiting Silence mode, the detector will go into alarm again. **CAUTION:** When the unit is **not** in alarm, pressing the **Test** button will transmit an alarm, activate the sounder and then place the unit in *Silence Mode* if held for more than 10 seconds. Once the unit enters *Silence Mode*, the **Test** button is disabled until it exits *Silence Mode* on its own.

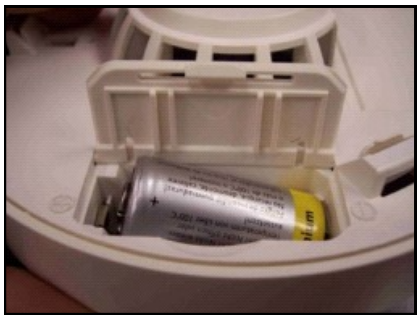
Low Battery Warning
Sounder chirps and the LED flashes simultaneously.

Maintenance Warning
The unit will warn that it must be cleaned when the unit chirps (without a simultaneous LED flash) but the LED flashes between chirps. To clean, vacuum the outside of the unit at least once a year (preferably every six months) using a soft brush attachment. *Do not attempt to clean the unit in any other way.* If this maintenance procedure fails to clean the unit sufficiently, call for service and/or replace the unit.

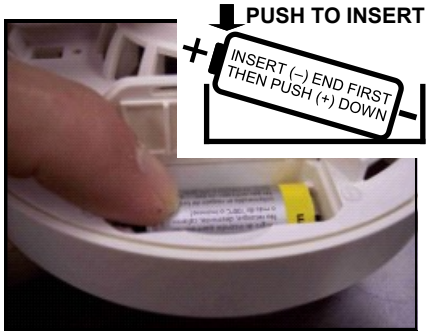
continued ⟶

6. Install Smoke Sensors (cont'd)

IMPORTANT! Use proper polarity when installing the 3V lithium battery. **Always** install the *negative* end first as shown below:



1. Place negative end in first.



2. Push down on positive end

(To remove battery, pull up on pos [+] end)

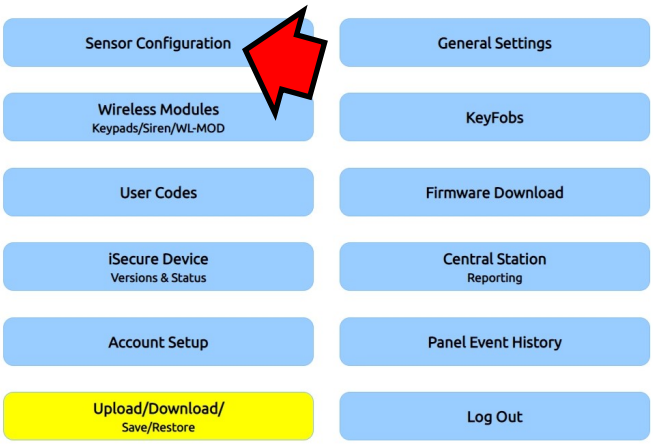
3. **Press and hold TEST** button for 5 seconds to activate the internal sounder, send a supervisory check-in (but NOT an alarm), and clear the low battery trouble from the ISEC-SMOKE.

4. **Separate Test (optional):** Press and hold **TEST** button (see page 20 for location) for 10 seconds to activate the internal sounder, send an alarm and clear the low battery trouble. Notify central station of impending test (if system is monitored). **Note:** While holding the button down, the LED will start to flash rapidly indicating it is about to go into alarm. Test system weekly with unit mounted.

This smoke detector has a *Silence* feature that will allow the User to temporarily silence the sounder of a detector in alarm. To activate *Silence*, hold down the **TEST** button for 10 seconds. **IMPORTANT:** The detector will chirp every 30 seconds while in *Silence* mode and will automatically exit this mode after 5 minutes. (**Note:** If smoke is still present in the chamber after exiting *Silence* mode, the detector will go into alarm again).

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. **Caution:** Changes or modifications not expressly approved by manufacturer could void the user's authority to operate the equipment.

- See page 48 for full programming information



continued ⟶

6. Install Smoke Sensors (cont'd)

NFPA STANDARD FOR SMOKE-DETECTOR LOCATION

The ISEC-SMOKE should be installed in accordance with the National Fire Protection Association (NFPA) Standard 72. For your information, the National Fire Protection Association's Standard 72, reads as follows:

11.5.1 One- and Two-Family Dwelling Units.

11.5.1.1 Smoke Detection Where required by applicable laws, codes, or standards for the specified occupancy, approved single- and multiple-station smoke alarms shall be installed as follows: (1) In all sleeping rooms. Exception: Smoke alarms shall not be required in sleeping rooms in existing one- and two- family dwelling units. (2) Outside of each separate sleeping area, in immediate vicinity of the sleeping rooms. (3) On each level of the dwelling unit, including basements. Exception: In existing one- and two-family dwelling units, approved smoke alarms powered by batteries are permitted.

11.8.3 Are More Smoke Detectors Desirable? The required number of smoke detectors might not provide reliable early warning protection for those areas separated by a door from the areas protected by the required smoke detectors. For this reason, it is recommended that the householder consider the use of additional smoke detectors for those areas for increased protection. The additional areas include the basement, bedrooms, dining room, furnace room, utility room, and hallways not protected by the required smoke detectors. The installation of smoke detectors in kitchens, attics (finished or unfinished), or garages is not normally recommended, as these locations occasionally experience conditions that can result in improper operation.

There exist certain situations where the presence of a smoke alarm is not effective, such as smoking in bed, the testing of gas leaks with a flame or for warning against the existence of high carbon monoxide levels inside a family living unit. Current studies have shown smoke alarms may not awaken all sleeping individuals; it is therefore the responsibility of individuals in the household that are capable of assisting others to provide assistance to those who may not be awakened by the alarm sound and to provide assistance to those who may be incapable of safely evacuating the area unassisted.

For family living units with one or more split levels (i.e., adjacent levels with less than one full story separation between levels), a smoke detector required as above shall suffice for an adjacent lower level, including basements. Exception: Where there is an intervening door between one level and the adjacent lower level, a smoke detector shall be installed on the lower level.

- Ceiling-mounted smoke alarms should be located in the center of the room or hall, or not less than 4 inches from any wall. When the detector is mounted on a wall, the top of the detector should be 4 to 12 inches from the ceiling.
- Do not install smoke alarms where normal ambient temperatures are above 100°F (37.8°C), below 40°F (4.4°C) or greater than 92% humidity unless the alarm has been determined to be capable of being used at installation points with higher or lower ambient temperatures. Also, do not locate alarm in front of air conditioners, heating registers, or other locations where normal air circulation will keep smoke from entering the detector. Installing smoke detectors in kitchens, garages or furnace rooms is NOT recommended.

All installation wiring must be in accordance with the provisions of Article 210 of the National Electrical Code, ANSI / NFPA 70. All protected premises fire alarm systems shall be maintained and tested (at least once every month) in accordance with NFPA 72.

FIRE PREVENTION AND ESCAPE

The purpose of an early warning smoke alarm is to detect the presence of fire in its early stages, and sound an alarm giving the occupants more time to exit the premise before the smoke reaches a dangerous concentration level.

Fires start even with the best of housekeeping and fire-prevention procedures. Fire is an unexpected event. Early warning detection alerts occupants in time to act.

KNOW FIRE HAZARDS. No detection device can protect life in all situations. Therefore, safeguards should be taken to avoid such potentially dangerous situations as smoking in bed, leaving children home alone, cleaning with flammable liquids such as gasoline. The best fire protection is minimizing fire hazards through proper storage of materials and general good housekeeping techniques. A cluttered basement, attic, or other storage area is an open invitation to fire.

Careless use of combustible materials and electrical appliances, or overloading of electrical outlets are other prime causes in starting fires.

It is most important that explosive and/or fast-burning materials be eliminated from the home if at all possible. Even after proper precautions have been taken, fires can start. Be prepared.

IN CASE OF FIRE. Leave immediately. Don't stop to pack or search for valuables. In heavy smoke, hold your breath and stay low -- crawl if necessary. The clearest air is usually at the floor.

If you have to go through a closed door, carefully feel the door and door knob to see if undue heat is present. If they seem relatively cool, brace your foot against the bottom of the door with your hip against the door and one hand against the top edge. Open it slightly. If a rush of hot air is felt, slam the door quickly and latch it. Unvented fire tends to build up considerable pressure. Be sure all the household realizes and understands this danger.

Use your neighbor's phone or a street fire alarm box. The job of extinguishing the fire should be left to the professionals. Too many unforeseen things can occur when inexperienced people try to extinguish afire.

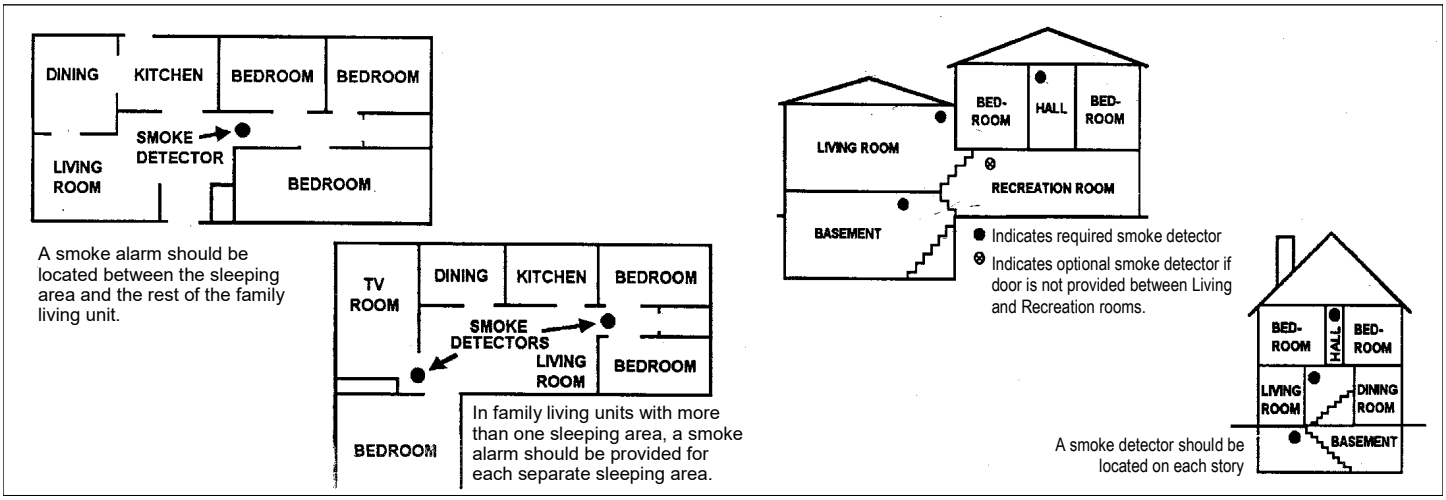
BE PREPARED. Perform fire drills regularly. Use them to assure recognition of an alarm signal. For your protection, simulate different circumstances (smoke in hall, in living room, etc.). Then have everyone react to the situation.

Draw a floor plan and show two exits from each room. Frequently, a knotted rope or ladder from a window will serve this purpose. It is important that children be instructed carefully, because they tend to hide in times of crisis.

It is imperative that one meeting place outside the home be established. You should insist that everyone meet there during an alarm. This will eliminate the tragedy of someone reentering the house for a missing member who is actually safe.

If you have children and/or invalids residing in your household, you can help your fire department. Most fire departments have window decals available for use in children's or invalid's bedrooms. Properly used, these decals will quickly identify sleeping quarters of these individuals and show the department where to look first for members of your household.

Additional information on Household Fire Warning is available at nominal cost from The National Fire Protection Agency, Batterymarch Park, Quincy, MA 02269. Request Standard No. NFPA 72.



7. Install Heat Sensors

DESCRIPTION

The ISEC-HEAT is a high-quality 135°F (57°C) fixed temperature detector with Rate of Rise. It is compatible with the NAPCO iSecure-series supervised security system.

The ISEC-HEAT incorporates circuitry which will transmit an alarm signal upon an alarm condition, generate an hourly supervisory test signal to the receiver and also monitor and annunciate low battery.

Coding switches are not required or used in the ISEC-HEAT. Each transmitter is assigned a unique identification code number at the factory. The transmitter is powered by one 3V Lithium battery (supplied) which can power the unit for up to two years. If the battery voltage drops below normal, a low-battery report will be sent to the receiver with any status or alarm transmission. If a low-battery condition is indicated, replace the battery.

OPERATION

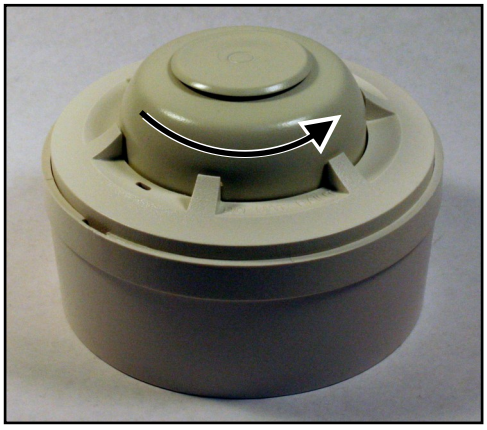
Rate-of-Rise Feature: A temperature increase of 15°F or more per minute will result in an alarm transmission. When the rate-of-rise element alone has been activated, the detector is self-restoring.

Fixed Temperature: If the temperature of the center disk rises to the detector's rated temperature (135°F / 57°C) an alarm transmission will result. When actuated by the fixed temperature element, the detector is non-restorable and must be replaced. The need for replacement is indicated when the center disk has fallen free; order System Sensor model 5601P to replace detector.

When the ISEC-HEAT detects an alarm as described above, the integral transmitter will send an alarm signal to the receiver. The alarm signal will be repeated every 10 seconds thereafter as long as the alarm condition is present. A restore report will be sent when the condition clears.

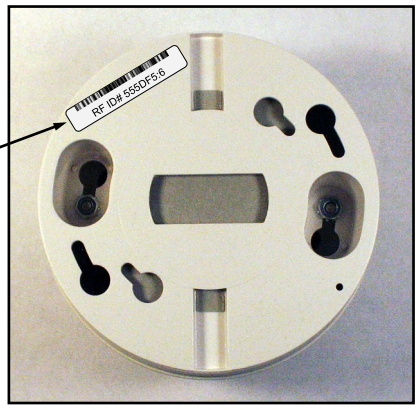
WARNING: NOT A LIFE SAFETY DEVICE - USE FOR PROPERTY PROTECTION ONLY

Step 1. Remove the mounting base.
Lift the ISEC-HEAT from the base by turning the top of the heat detector counter-clockwise while holding the base stationary.



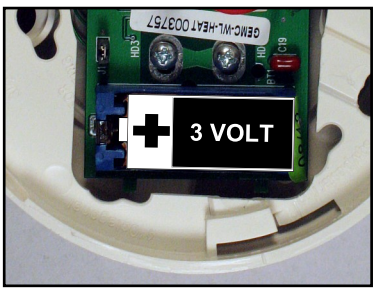
Step 2. Locate the RF ID#
Locate the RF ID# on the rear of the unit. **NOTE:** The RF ID# on the label must be accurately recorded in order to map the transmitter into the system (see Step 7).

NOTE: RF ID# is located on the label placed on the rear of the unit



Step 3. Install the battery
Observing polarity, install the supplied battery as shown.
NOTE: A Tamper zone trouble will result when the batteries are replaced. *Replace battery with a 3V Duracell DL123A, Varta/Power-One CR123A or Panasonic CR123A only. Use of another battery may present a risk of fire or explosion*.

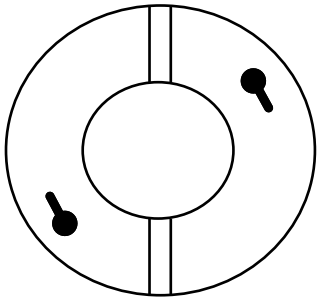
CAUTION: Risk of Fire, explosion and burns. Do not recharge, disassemble, heat above 100°C., or incinerate. Dispose of used batteries promptly. Keep away from children.



Step 4. Mounting the base to the ceiling
Select mounting location for detector on ceiling; maximum spacing (10ft ceiling) is 50-feet x 50-feet*. Do not locate in direct path of hot or cold air flow. Mark holes using the accompanying mounting template. Use the two screws and anchors provided to attach the mounting plate to the wall or ceiling.

NOTE: The mounting plate may be attached to a *plastic* single-gang electrical outlet box. Do not attach to metallic outlet boxes.

*Refer to NFPA 72 guidelines for spacing reductions when the ceiling height exceeds 10 feet.



continued ⟶

7. Install Heat Sensors (cont'd)

Step 5. Reinstall the ISEC-HEAT into the mounting base.
Insert the ISEC-HEAT into the base and turn the top clockwise while holding the base stationary until the ISEC-HEAT gently snaps into place.

Step 7. Testing the system
Test system with unit mounted. If the system is monitored, notify the central station of the impending test.

The rate-of-rise feature may be tested by a quick application of heat from any convenient source. A portable hair dryer is recommended. However, do not apply heat that exceeds the fixed temperature rating of the detector. If the fixed temperature is exceeded, the center disk of the detector will drop and the detector MUST be replaced.

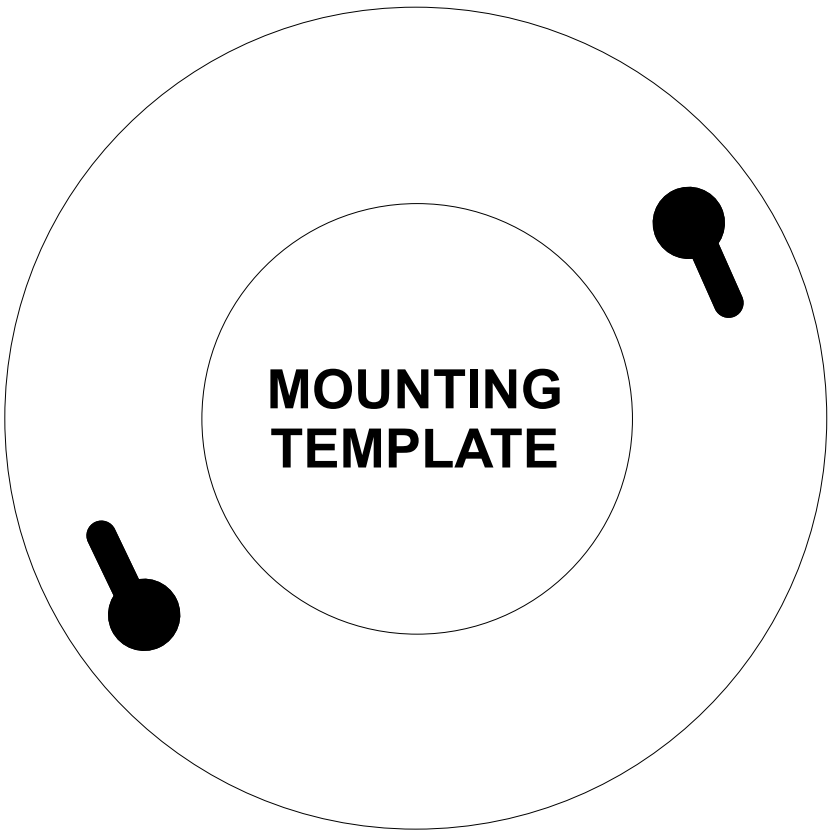
Apply the heat until the local alarm sounds. Verify that the ISEC-HEAT has triggered the correct zone and that the correct report has been transmitted to central station. Wait a few minutes and reset the fire circuit. Ensure that the system returns to a normal status.

Step 6. Map the ISEC-HEAT Transmitter
Referring to the installation instructions for the Hub and keypad in use, enter the following:

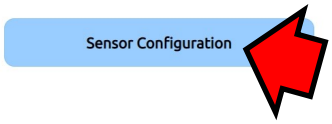
- The zone to which the transmitter will be mapped.
  Note: This zone must be programmed as a Fire Zone.
- The 6-digit RF identification number / 1 digit checksum number printed on the transmitter (include all numbers and/or letters and leading zeros, if any);
- The transmitter point number ("1").

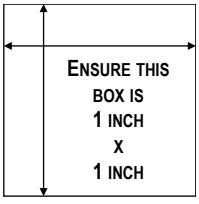
WARNINGS

- HEAT DETECTORS ARE NOT LIFE SAFETY DEVICES: USE FOR PROPERTY PROTECTION ONLY.
- WHERE LIFE SAFETY IS REQUIRED, SMOKE DETECTORS MUST ALSO BE USED.
- BATTERY BACK-UP: HEAT DETECTORS SHOULD BE ELECTRONICALLY SUPERVISED WITH BATTERY BACKUP AT THE HUB.
- THE RATE-OF-RISE MECHANISM MAY BE SUBJECT TO REDUCED SENSITIVITY OVER TIME. ANNUAL TESTING OF THE RATE-OF-RISE OPERATION IS RECOMMENDED.
- REFER TO NFPA STANDARD 72 FOR APPLICATION REQUIREMENTS, TESTING AND MAINTENANCE.
- DO NOT PAINT THE ISEC-HEAT.
- A TAMPER ZONE TROUBLE WILL RESULT WHEN THE BATTERIES ARE REPLACED.



• See page 49 for full programming information





8. Install Carbon Monoxide Sensors

OVERVIEW

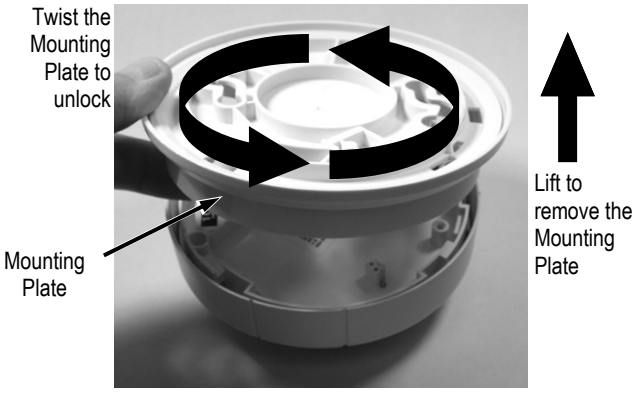
The ISEC-CARBON MON is a high-quality carbon monoxide (CO) detector with built-in supervised digitally-coded radio transmitter. Up to 80 CO detectors can be added to the system.

During normal operation, when unit is in standby mode and is within proper sensitivity limits, the green LED on the ISEC -CARBON MON flashes once every 10 seconds. When CO is detected, the ISEC-CARBON MON sounds a local alarm and the transmitter sends an alarm signal to the supervised receiver. The alarm signal is repeated as long as CO is still present. A restore report is sent when the CO detection chamber clears. Supervision status reports are sent from the ISEC-CARBON MON every minute.

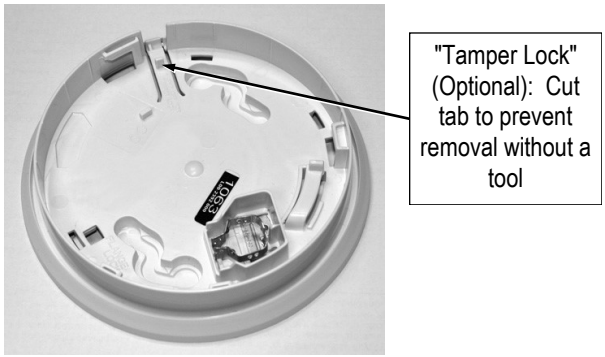
Note: Coding switches are not required or used in the ISEC-CARBON MON; each transmitter is assigned a unique identification code number at the factory.
The ISEC-CARBON MON must be installed in accordance with the National Fire Protection Association (NFPA) Standard 720.

INSTALLATION STEPS

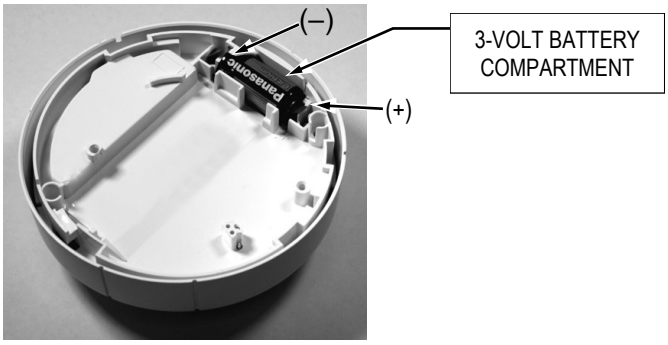
1. **Remove the Mounting Plate.** Remove the ISEC-CARBON MON Mounting Plate by turning the Plate counter-clockwise and pulling it up.



2. **Identify components.** Examine the ISEC-CARBON MON to identify the component locations. Take note of the "Tamper Lock" tab located on the inside of the Mounting Plate (see image below). Optionally, cut this "Tamper Lock" tab to prevent the removal of the ISEC-CARBON MON from the Mounting Plate without using a tool (such as a screwdriver).

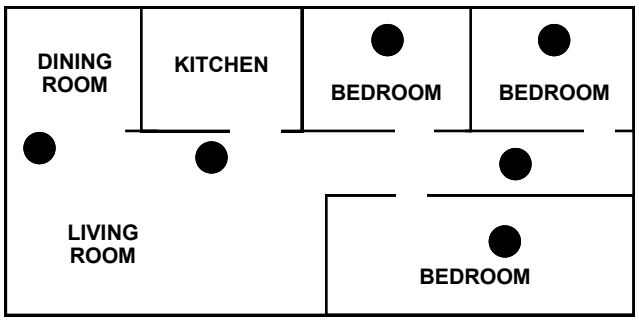


3. **Install battery.** Place one 3-volt lithium *Duracell*, *Panasonic*, *Varta* or *Sanyo* type "123A" battery in its compartment, observing correct polarity. Enroll the ISEC-CARBON MON into the Hub before mounting. During power up and status initialization, both the green and red LED's blink four times every 10 seconds in unison. Then look for the "standby" indication where the green LED blinks once every 10 seconds.



Low Battery Warning
The CO detector and transmitter are powered by one 3-volt lithium battery (supplied) that can power the unit for at least one year. If battery voltage drops below normal, the red LED will flash every 45 seconds and a low battery report will be sent to the Hub. If the voltage is still below normal after 7 days, the detector sounder will chirp. The battery should be replaced immediately. Operation of the detector cannot be assured after an additional 7 days of low-battery indication. A low-battery report is sent to the receiver with any status transmission.
NOTE: Temperature and humidity extremes may reduce the life of the battery.
Use Only Battery Specified In Marking. Use of A Different Battery May Have A Detrimental Effect On Detector Operation.

4. **Pick CO-detector location.** The ISEC-CARBON MON must be installed in accordance with the National Fire Protection Association (NFPA) Standard 720. Refer to figures in "**Recommended Installation Locations**" (on page 27) and all text on pages 27 through 29.
Note: *Mounting the ISEC-CARBON MON on foil-backed wallpaper is NOT recommended because the radio range will be reduced.*

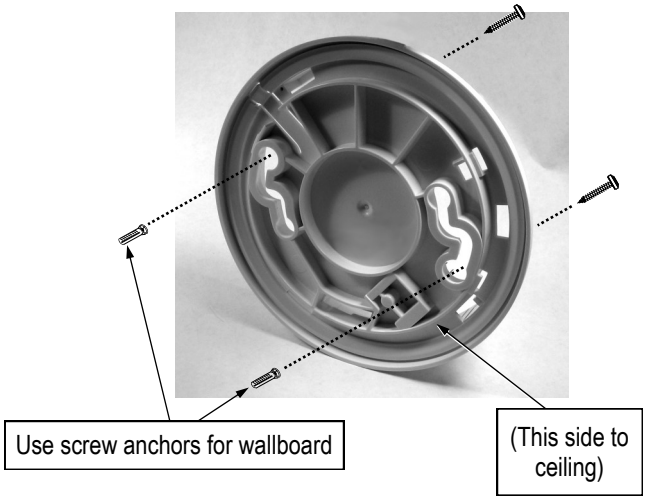


5. **Install mounting plate.** Use two screws and hardware appropriate for the mounting surface to secure the

continued →

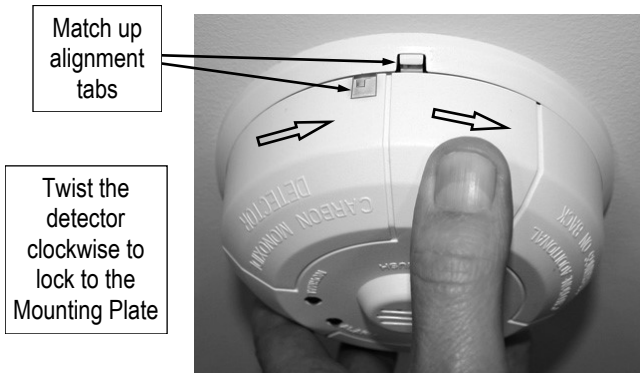
8. Install Carbon Monoxide Sensors (cont'd)

mounting plate to the wall or ceiling. **NOTE:** Do not install on removable surfaces such as ceiling tiles.

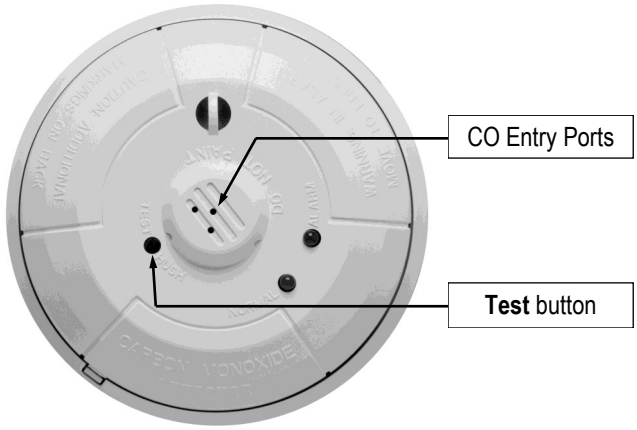


6. **Map the ISEC-CARBON MON Transmitter.** Referring to the installation instructions for the Hub and keypad in use, enter the following:
   - the zone to which the transmitter will be mapped
   - the 6-digit RF identification number / 1-digit checksum number printed on the transmitter (include all numbers and/or letters and leading zeros, if any)
   - the transmitter point number "1"

7. **Attach the ISEC-CARBON MON to Mounting Plate.** Match up alignment tabs on the detector and the Mounting Plate. Turn detector clockwise until it locks into place (see next image).



8. **Test system weekly with unit mounted** and by pressing the **TEST** button (shown in next image). Perform the **FUNCTIONAL GAS TEST** annually (if required by the AHJ) as described in the next section.



FUNCTIONAL GAS TEST MODE

Note: Check with local codes and the AHJ to determine if a functional gas test is desired for an installation. If the system is monitored, notify central station of the impending test. A canned CO testing agent may be used to verify the ability of the ISEC-CARBON MON to sense CO by utilizing the Functional Gas Test Mode. To perform the functional gas test, follow these steps:

a. With a small screwdriver, depress and hold the recessed "**TEST**" button for approximately 2 seconds. The detector will temporarily go into alarm and the red LED will illuminate.
b. Within a few seconds the green LED will start to blink rapidly indicating the detector is in a speed up, functional test mode, awaiting gas entry.
c. Spray a very small amount of Solo brand C6 canned CO into one of the 3 small gas entry holes located on the top center of the detector.
d. Upon successful gas entry and if functioning properly, the detector will alarm by sounding in a Temporal-4 pattern with the red LED blinking. An alarm signal will be sent to the Hub, providing verification of the alarm signal.
e. The alarm condition at the detector will time out in 20 to 60 seconds or when the CO gas has cleared.
f. If gas entry is unsuccessful, the test will time out after 27 seconds.

VISIBLE & AUDIBLE INDICATIONS

(In priority order, starting with highest priority)

- Red and green LED blink every 10 seconds for a total of 4 times (no sound produced) = "Power On Reset**" condition**.
- Sounder and red LED on once a second = **Carbon Monoxide Alarm!** The Hub produces the standard CO Alarm repeating cadence of "4 beeps, 5-second pause, 4 beeps", repeatedly, until the CO condition is cleared. **To Temporarily Silence:** Press and hold the recessed **TEST / HUSH** button for 10 seconds to temporarily silence the unit for 5 minutes.
- Red LED blinks once every 5 seconds; sounder chirp every 45 seconds = **CO Trouble / Calibration**. (**Note:** Transmits a trouble to the Hub).

continued ⟶

8. Install Carbon Monoxide Sensors (cont'd)

- Green LED blinks once every 10 seconds = **Tamper condition**. (**Note:** Transmits a trouble to the Hub).
- Red LED blinks once every 10 seconds; sounder chirp every 45 seconds = **End of Life Warning**. The unit has reached the end of its operational life and will no longer detect the presence of carbon monoxide. The unit can NOT be made operational and therefore MUST be replaced. (**Note:** Transmits a trouble to the Hub).
- Red LED blinks once every 45 seconds; chirps after 7 days = **Low Battery**. Chirp Silence: Press recessed **TEST / HUSH** button to temporarily disable the Low Battery Chirp ("sleep") for 12 hours.
- Green LED blinks every 10 seconds (sounder is silent) = **Normal** standby operation.

CO ALARM PROCEDURE

When a carbon monoxide alarm occurs:

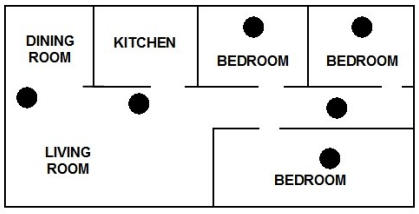
1. Immediately evacuate the premises and move to fresh air, either outdoors or by an open door or window.
2. Call emergency services (Fire Department or 911)
3. Ensure that all persons previously within the premises are accounted for. **Do not re-enter the premises until authorized by emergency service responders.**
4. If the CO alarm reactivates, repeat steps 1-3 and call a qualified service technician to investigate all possible sources of carbon monoxide, such as from fuel burning appliances and other equipment, and repair all problems found immediately. Note any equipment not inspected and refer to the equipment manufacturer's documentation, or contact the manufacturer's directly for more information about how the equipment can leak carbon monoxide into the premises. Ensure all motor vehicles are not, and have not been, operating in an attached garage, operating adjacent to the premises, or operating next to ventilation fresh air intake vents. Never restart the source of a CO problem until it has been corrected.
5. If the CO condition that caused the alarm continues, the alarm will reactivate. Never ignore the sound of the alarm! If the CO alarm resounds, the detector is sensing levels of CO that can quickly become a dangerous situation. **EVACUATE IMMEDIATELY** (repeat steps 1-4).

MAINTENANCE

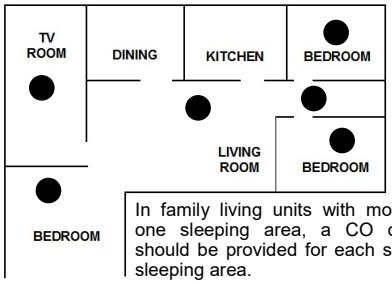
To keep your detector in functioning correctly, you must:

- Test the unit once a week by pressing the Test/Hush button (insert a non-conductive pointed object, such as a toothpick)
- Carefully vacuum the unit cover once a month to remove accumulated dust
- Never use detergents or solvents to clean the unit. Chemicals can permanently damage or temporarily contaminate the sensor

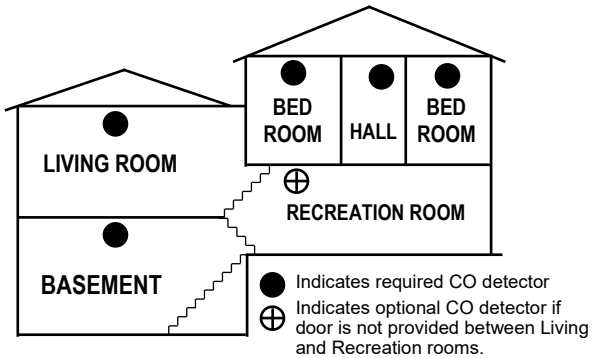
RECOMMENDED INSTALLATION LOCATIONS

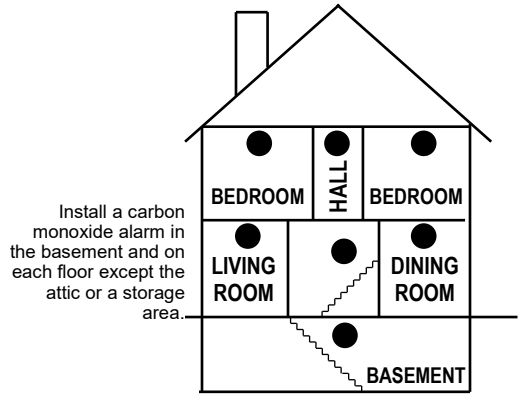


A CO detector should be located in every sleeping area, in each of the other family living units, but just outside the kitchen.



In family living units with more than one sleeping area, a CO detector should be provided for each separate sleeping area.





Install a carbon monoxide alarm in the basement and on each floor except the attic or a storage area.

continued ⟶

8. Install Carbon Monoxide Sensors (cont'd)

- Do not spray air fresheners, hair spray, paint or other aerosols near the unit
- Do not paint the unit, as paint will seal the vents and interfere with proper sensor operation

Move the CO detector to a safe and remote location to prevent damage or contamination prior to performing any of the following:

- Staining or stripping floors or furniture, painting or wallpapering
- Using aerosols or adhesives

Note: A Tamper / Trouble signal will be sent to the Hub when the detector is removed from the base. **IMPORTANT:** Reinstall the CO detector as soon as possible to assure continuous protection.

The following lists possible substances that at some levels can damage the sensor or cause false alarms:

- Ethylene, ethanol, alcohol, iso-propanol, benzene, toluene, ethyl acetate, hydrogen, hydrogen sulfide and sulfur dioxide
- Most aerosol sprays, alcohol based products, paint, thinners, solvents, adhesives, hair spray, after shave, perfume, auto exhaust, cleaning agents, etc.

LOCATIONS TO AVOID

IMPORTANT: Improper mounting locations can damage the electronic components within the detector. To avoid damage, to provide optimum performance and to avoid false alarms, proceed as follows:

- Do NOT install in kitchens, garages, furnace rooms or in areas that may expose the sensor to substances that could damage or contaminate it
- Do NOT install in areas where the temperature is colder than 32°F (0°C) or hotter than 122°F (49°C) such as crawl spaces, attics, porches and garages
- Do NOT install within 5 feet of heating or cooking appliances. (we recommend 15 feet to prevent false alarms)
- Do NOT install near vents, flues, chimneys or any forced/unforced air ventilation openings
- Do NOT install near ceiling fans, doors, windows or areas directly exposed to the weather
- Do NOT install in dead air spaces, such as peaks of vaulted ceilings or gabled roofs, where CO may not reach the sensor in time to provide early warning
- Do NOT install this unit near deep-cell large batteries, as these batteries may have emissions that can cause the detector to perform at less than optimum performance
- Do NOT obstruct the vents located on the unit
- Do not mount the unit where drapes, furniture or other objects can block the flow of air to the detector

GENERAL WARNINGS

- Read these installation instructions in their entirety before installing the ISEC-CARBON MON detector. Leave these instructions with the owner/user of the detector.
- The ISEC-CARBON MON is intended for use in indoor locations only
- Failure to properly install, test and/or maintain the ISEC-CARBON MON may cause it to fail, potentially resulting in loss of life
- Installation of this detector is not a substitute for proper installation, use, and maintenance of fossil fuel-burning appliances, including appropriate ventilation and exhaust systems
- To reduce the risk of carbon monoxide poisoning, test detector operation weekly
- Do not paint the detector

Carbon monoxide detectors are NOT smoke detectors. A carbon monoxide detector is NOT a substitute for smoke detectors. This carbon monoxide detector is specifically designed to detect the presence of carbon monoxide gas and is NOT designed nor intended to detect smoke, fire or any other gas. In addition, this detector will only indicate the presence of carbon monoxide *at the sensor*; carbon monoxide gas may be present within other areas of the premises.

CARBON MONOXIDE POISONING

The following are some of the possible carbon monoxide poisoning symptoms that should be presented to and discussed with all occupants of the protected premises:

- **Mild exposure**: "Flu-like" symptoms, including but not limited to slight headache, nausea, vomiting, fatigue, runny nose and sore eyes
- **Medium exposure**: Severe throbbing headache, dizziness, drowsiness, confusion, fast heart rate
- **Extreme exposure**: Loss of consciousness, brain damage, convulsions, cardio-respiratory failure, death

Often cases of reported CO poisoning indicate that while victims are aware they are unwell, they become so disorientated that they are unable to save themselves by either exiting the building or calling for assistance. Young children and pets may be the first affected.

SOURCES OF CARBON MONOXIDE

Potential carbon monoxide sources include fuel-fired appliances (space heaters, furnaces, water heaters, ranges, ovens, clothes dryers); other sources (kerosene-burning stove or heater, or gas log fireplace); or internal combustion engines. In addition, excessive exhaust spillage or reverse venting of fuel-burning appliances can produce dangerous transient levels of CO. This can be caused by external conditions, such as:

- Wind direction, velocity, or a combination of both, including high gusts of wind or insufficient draft in vent pipes
- Temperature inversions that can trap exhaust gases near the ground
- Negative pressure differential resulting from the use of exhaust fans

continued ⟶

8. Install Carbon Monoxide Sensors (cont'd)

- Simultaneous operation of several fuel-burning appliances competing for limited internal air
- Vent pipe connections vibrating loose from dryers, furnaces, or water heaters
- Obstructions in vent pipes or unconventional vent pipe designs that can amplify the above situations
- Poorly designed or maintained chimneys and/or vents
- Extended operation of unvented fossil fuel-burning devices (range, oven, fireplace, etc.)
- Idling cars in an open or closed attached garage, or near the premises

GENERAL LIMITATIONS OF CARBON MONOXIDE DETECTORS

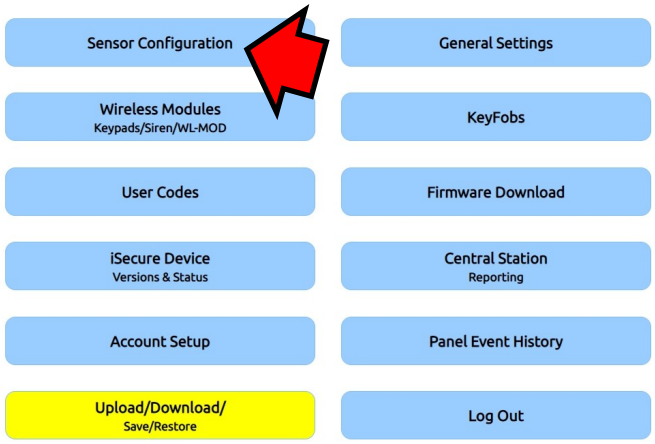
This detector is designed to protect individuals from the severe effects of CO exposure. It will not fully safeguard individuals with specific medical conditions. If in doubt, consult a medical practitioner.

If the unit is in trouble or has arrived at the end of its life, it may not sense CO and cannot be relied upon to monitor CO levels. Replace the CO detector by the date specified on the unit or when the detector indicates an end of life condition, whichever comes first. CO detectors are not a substitute for designated life safety devices. Napco does not warrant or imply in any way that a CO detector will protect lives from CO poisoning. These detectors should only be considered as an integral part of a comprehensive safety program.

SPECIFICATIONS

Electrical Ratings

Input Power:	Powered by a 3-volt lithium battery. Use one 3-volt lithium Duracell DL123A, Varta CR123A, Panasonic CR123A or Sanyo CR123A.
Dimensions (W×L×D)	5-3/8 x 5-3/8 x 2-1/8" (13.7 x 13.7 x 5.4cm)
Operating Environment	
Temperature	32°F to 122°F (0°C to 49°C)
Relative humidity	15% - 95% RH
Regulatory Information	
Manufacturer:	Napco Security Technologies, Inc. 333 Bayview Avenue, Amityville, NY 11701
Environmental class	Indoor, in accordance with the Operating Environment specifications.



- See page 50 for full programming information

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. **Caution:** Changes or modifications not expressly approved by manufacturer could void the user's authority to operate the equipment.

9. Install Panic Button

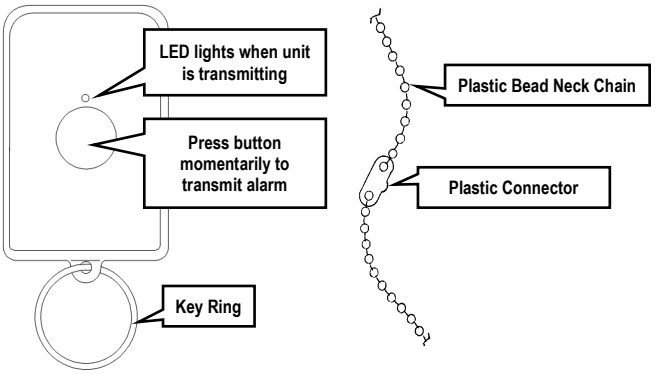
GENERAL DESCRIPTION

The ISEC-PANIC Panic is an single function pendant / key-chain transmitter compatible with the NAPCO iSecure security system. The ISEC-PANIC serves as an emergency device for use as a police panic and/or auxiliary emergency transmitter. Two replaceable Energizer 386 1.5V silver oxide cells power the transmitter. A flashing LED signals a low-battery warning. To operate, simply press the button momentarily until the red LED lights. **Note:** When the button is pressed, the ISEC-PANIC will transmit the respective signal to the Central Station, if so programmed. The LED lights while the unit is transmitting. See page 51 for full "**Sensor Configuration**" programming information.

Low-Battery Check: The power cells are checked automatically during any transmission. A low-battery condition causes the LED to turn on for twice the normal time, then start pulsing about once every 1.5 seconds; a low-battery report will be sent to the receiver. Replace batteries every 3 years.

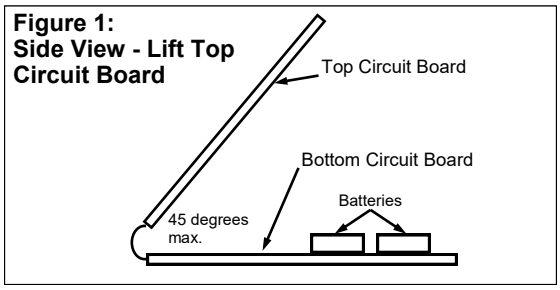
BATTERY REPLACEMENT

1. Remove the screws on the bottom of case and turn over. Lift off the top cover, exposing the circuit boards.
2. *Carefully* lift the top circuit board away from the bottom circuit board **no more than 45 degrees** (see Figures 1 and 2) to allow removal of batteries from the bottom circuit board.
3. Slide the bottom battery out and away from the circuit board. Replace the battery as shown (see Fig. 3 and 4).
4. Replace the top battery by sliding it out to the right. Replace the battery as shown (see Figures 3 and 4).
5. Carefully press the top circuit board back toward the bottom circuit board. Reassemble the case and slip the neck chain through the eyelet.
6. Test the button to verify its function. **Note:** Inform the Central Station about the test or disable the transmission of panic during the test.



ADJUSTING CHAIN LENGTH

The ISEC-PANIC has a plastic bead neck chain included. To adjust its length, simply disconnect the chain from one end of the plastic connector by removing a plastic bead, use scissors to cut the chain to the desired length, then reconnect the chain by inserting a bead into the connector.



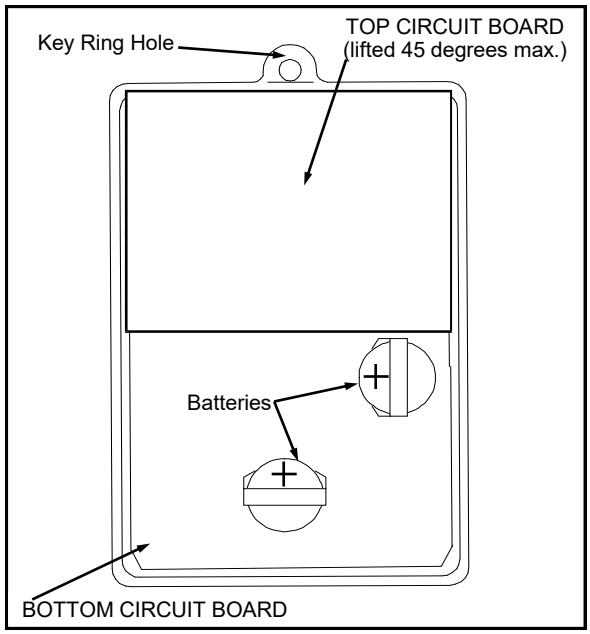


Figure 3: Top View of Bottom Circuit Board for Battery Replacement with Top Circuit Board lifted

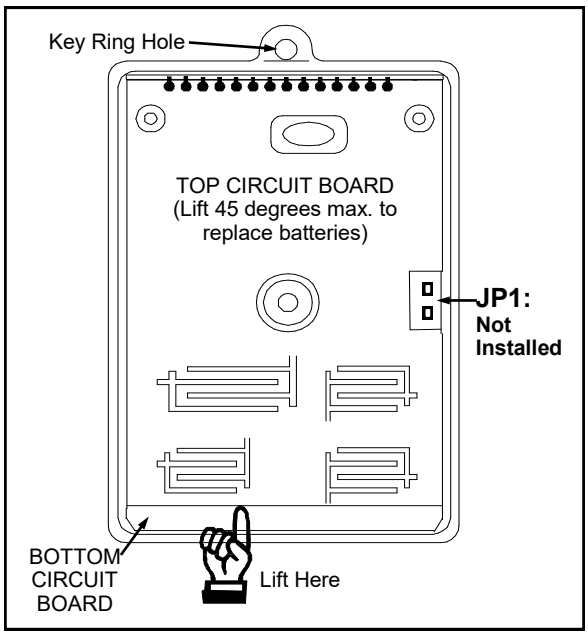


Figure 2: Top View of Top Circuit Board

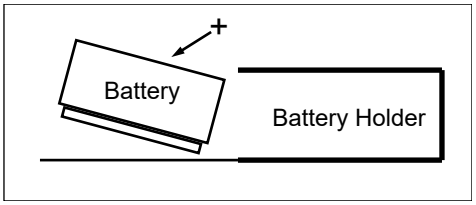


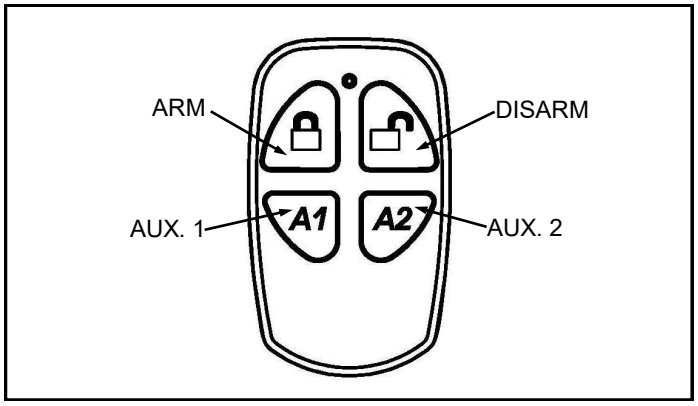
Figure 4: Angle the Battery on Entry

10. Install Keyfobs

The **ISEC-KEYFOB** is a multifunction pendant/keychain transmitter compatible with Napco iSecure-Series wireless systems. It serves as an area arm/disarm device with two auxiliary functions, and may be used as a police panic and/or auxiliary emergency transmitter. A 3V Lithium coin cell battery powers the ISEC-KEYFOB transmitter (use type CR2032 or Duracell DL2032 only; use of another battery may present a risk of fire or explosion). A flashing LED indication signals a low-battery warning to replace the unit.

The ISEC-KEYFOB leaves the factory as a remote area arm/disarm transmitter with two Auxiliary buttons, A1 and A2. Auxiliary functions are selected by programming keyfob Aux 1 and Aux 2 options: None, Panic, Instant , Aux Output Toggle, Aux Output Momentary, Arm Stay or Bypass Interior.

Note: The Aux 1 Button and Aux 2 Button must each be held down for approximately 2 seconds before the respective signal will be sent. The LED will light while the unit is transmitting.



Factory-Supplied Functions: Arm, Disarm, Aux. 1 and Aux. 2

LOW-BATTERY CHECK. THE BATTERIES ARE CHECKED AUTOMATICALLY DURING ANY TRANSMISSION. A LOW-BATTERY CONDITION WILL CAUSE THE LED TO COME ON AND START PULSING FOR APPROXIMATELY 30 SECONDS; A LOW-BATTERY REPORT WILL BE SENT TO THE RECEIVER.

SPECIFICATIONS

Electrical Ratings

Input Power: Powered by a 3-volt lithium battery.
Operating Frequency: 319.5Mhz

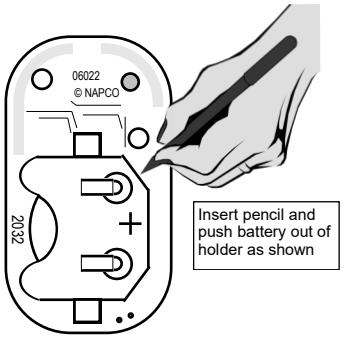
REQUIRED PROGRAMMING

The following information is required for each unit. See page 52 for full programming information.

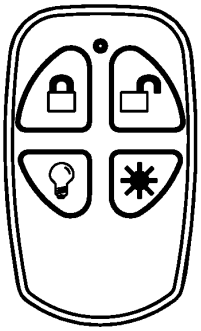
- An assigned keyfob transmitter number
- Area number(s) to which transmitter is applicable
- The 6-digit RF ID code with checksum digit printed on the transmitter (enter all numbers and/or letters, including leading zeros, if any)
- Aux-1 option and Aux-2 option

BATTERY REPLACEMENT

1. Remove the keyring from the keyfob case.
2. Carefully insert the edge of a small coin in the notch located in the bottom right corner of the keyfob (near the key ring loop). Open the case by gently twisting the coin. Lift off the top cover.
3. With the bottom half of the keyfob facing upwards, carefully remove the circuit board.
4. On the bottom side of the circuit board, push the battery out of its metal holder with a sharp pencil. The battery will slide out of its holder as shown in the image below. *Note the orientation of the battery polarity, with its positive side up, before fully removing the battery.*



Battery Replacement: Top View of Bottom Circuit Board



Button Replacement: Auxiliary buttons

5. Replace with a new battery, ***positive (+) side up***, by sliding the battery into its metal bracket. *Be certain of battery polarity before installation*.
6. Reassemble the case by first placing the circuit board, battery side down, into the keyfob base. Place the top of the keyfob (with its rubber button/gasket in place) on the keyfob base and press to snap the two keyfob pieces together.
7. Test the keyfob operation.

BUTTON REPLACEMENT

Factory supplied auxiliary buttons can be installed to operate other items, such as outdoor lights. Install as follows:

1. Open the keyfob as per the Battery Replacement instructions (above) step 1.
2. With the top cover off, lift and remove the rubber buttons from the inside of the top cover.
3. Replace the rubber buttons with the auxiliary buttons, (shown above) reassembling the keyfob in the reverse order of disassembly.
4. Test the keyfob operation.

11. Install Siren

Before You Begin

Install the **ISEC-WL-SIREN** in either of two ways:

- AC with batteries as backup if AC lost
- Batteries only ("mount anywhere")

ISEC-WL-SIREN
Wireless Siren

The unit is shipped from the factory with the 120VAC wall outlet prongs installed (see "**AC With Battery Backup**" instructions, below). To power the siren with batteries only, thus increasing the number of possible installation locations, skip to the section "**Batteries Only ('Mount Anywhere')**". Use the template (page 75 or 77) appropriate for the installation. We recommend the unit be oriented as shown in the accompanying image; however, the unit can be installed upside down if needed. **Warning:** When installing outdoors, *locate in shaded areas only, never in direct sun* (extreme temperatures affect battery life). In addition, do not mount upside down; for outdoor locations the weep hole must be located at the bottom of the unit to allow any condensed water to drip out.

The siren will "learn" AC presence upon first power up; this means that an AC Power Failure trouble will only be reported if the siren is powered by AC and then AC power is lost or if the siren is removed from the wall power socket. In addition, if the siren is powered by AC and the batteries are low (or not installed), a low battery trouble will be reported. Four 'C'-size batteries (not included) ***must always*** be installed (we recommend using Duracell alkaline; never use less than 4 fresh batteries).

Protection against tamper is provided by a Tamper Magnet; for wall outlet installations, install this Tamper Magnet with the provided double-sided tape and NOT the screws (DO NOT use screws near electrical wiring that runs inside walls). We recommend the use of ear protection should the siren activate inadvertently. The siren will "learn" the presence of the tamper magnet the first time the presence of the magnet is detected; subsequent removal of the magnet will trigger a tamper trouble.

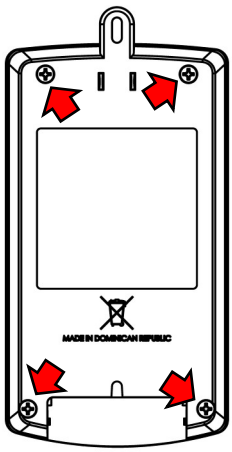


Fig. 1: Rear of the unit

AC With Battery Backup

For AC installations, be sure to select an un-switched 120VAC wall outlet and ALWAYS install the **required** four 'C'-size batteries (not included) that provide power if AC power fails.

1. Place a template (see page 75 or 77) over the 120VAC wall outlet socket, carefully aligning the template with the "**Center Line of Wall Socket**".
2. Mark the location of the ***Tamper Magnet***.
3. Use the supplied double-backed tape to secure the ***Tamper Magnet*** to the wall (do NOT use any screws near electrical wiring that runs inside walls).
4. At the wall outlet, remove the wall cover plate screw (only the screw; keep the cover plate in place). For wall outlets without a center cover plate screw, use the provided bracket and the template on page 77.
5. Plug the unit into the wall outlet, being certain the siren housing is placed over the ***Tamper Magnet***. The unit powers up*.
6. Secure siren to wall outlet by using the supplied screw (part #SC206LF) to replace the wall cover plate screw removed previously. Insert this new screw into the ***Screw Hole Tab*** shown on the page 75 template (or the page 77 template used for outlets without a center cover plate screw).
7. Install the ***Finisher Plate*** to conceal the ***Tamper Magnet*** (see Fig. 2).

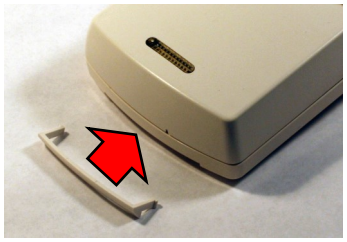


Fig. 2: Finisher Plate

Batteries Only ('Mount Anywhere')

1. Place the template over the mounting surface. Use a level to be sure the template is parallel with the floor. **WARNING:** Select a location that will ensure that screws are NOT used near electrical wiring that runs inside walls.
2. Mark the 2 holes for the ***Tamper Magnet***.
3. Mark the 1 hole for the ***Slide Screw***.
4. Heeding the **WARNING** noted in step 1, above, secure the ***Tamper Magnet*** to the wall using the two screws provided (part #SC596, #6 x ¾" self-tapping, Phillips flat head, U-cut, steel zinc, Type A).
5. Screw in the provided ***Slide Screw*** fully into the wall, then back the screw out 1 turn (part #SC265, #6 x ½" self-tapping, Phillips pan head, steel zinc, Type A).
6. On the back of the unit, remove the four (4) screws that secure the rear housing and pull off the rear housing (see Fig. 1).
7. Remove the two screws that secure the ***Wall Outlet PCB*** (see Fig. 3). Unplug the ***Wall Outlet PCB*** and place into the supplied anti-static bag/sheet for possible future use.
8. On the inside rear housing, insert the **Rubber Gasket** that covers the slots for the ***Wall Outlet PCB*** prongs (see Fig. 4).
9. Install batteries (observing polarity) and the unit powers up*.
10. Replace the rear housing; secure with the four (4) screws.
11. Secure unit to the wall by using a screw (appropriate for the mounting surface) inserted into the ***Screw Hole Tab*** shown on the templates.
12. Install the ***Finisher Plate*** to conceal the ***Tamper Magnet*** (see Fig. 2).

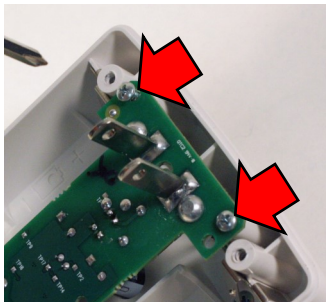


Fig. 3: Remove the two "Wall Outlet PCB" screws

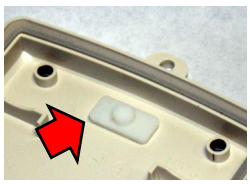


Fig. 4: Rubber Gasket

Note: In areas where power outages are common, we recommend a 5 minute sounder cutoff to maximize battery life.

Every time the siren is powered from an unpowered state, the unit ignores the tamper function until after the siren is placed over the tamper magnet. Subsequently, when the normally-closed tamper circuit opens (magnet removed), the siren reports a tamper trouble to the Go-Anywhere Hub. In addition, pressing the keypad **RESET button sends an updated status from the **ISEC-WL-SIREN** to the Go-Anywhere Smart Hub.*

12. Install Takeover Module

DESCRIPTION

The **ISEC-WL-MODULE** is a "takeover module", used to convert an existing wired security system to wireless. The **ISEC-WL-MODULE** will convert a total of 8 wired zones and convert them into 8 supervised wireless 900MHz zones. For example, if you have existing wired security system sensors such as motion detectors, glass break sensors and door/window transmitters, you can use the existing wiring for each of these devices and convert them into iSecure system wireless zones. Up to 4 **ISEC-WL-MODULE**s are allowed with each Go-Anywhere Smart Hub. **Note:** For existing 2-wire smoke detectors, the **ISEC-2WF-MOD** *2-Wire Fire Sensor Module* may be used if the detectors are compatible (see page 36 for the list of compatible detectors and additional information). **Note:** Pressing the keypad **RESET** button sends an updated zone status and module status from the **ISEC-WL-MODULE** to the Hub. In addition, LED1 turns on for 10 seconds. In addition, remove power from smoke detectors for 10 seconds to reset. See page 54 for full programming information.

WIRING

In general, the first step for wiring the **ISEC-WL-MODULE** is to connect all of the Zone data wires to a mounted and *unpowered* **ISEC-WL-MODULE**. Only after all zone and other wiring is connected should you then power the **ISEC-WL-MODULE** using either the existing wired 12VDC power connections from the existing security control panel or by an auxiliary power supply.

Connect the high side (positive) of each wired zone to its own screw terminal, labeled **Z1**, **Z2**, etc. on the **ISEC-WL-MODULE** terminal strip. Note that several sensors can be wired to a single zone provided they are wired in series. Connect the low side (negative) of each wired zone to any of the ground terminals (labeled **GND** next to each zone terminal).

After all zone wires are connected, connect the battery 12V positive lead to the **BATT+** terminal on the **ISEC-WL-MODULE**. Connect the battery ground lead to any **GND** terminal. After the battery is connected, then connect the 12V positive regulated control panel (or auxiliary supply) power to the **+12V** terminal followed by the negative ground connection to any **GND** terminal.

Wire all zone and power connections using 18-22AWG wire. Install end-of-line resistors on all zones, even if one or more zones are not used.

Note: If battery voltage falls below the minimum level, a battery trouble is triggered; if the voltage climbs above the minimum level, the trouble will restore 30 seconds after pressing the keypad **RESET** button. If **RESET** is not pressed, the battery trouble will self-restore in 4 hours if the battery voltage always remains above the minimum level during this time.

TERMINAL DESCRIPTIONS

Configure all inputs and outputs using the Management Center (the Napco "NOC" located at www.iSecureByNapco.com). Located at the bottom of the PC board, the 20 terminals are described as follows:

EARTH... This optional earth ground terminal provides protection from high-voltage transients (for example, nearby lightning discharges induce high-voltage transients into the field wiring of electronic equipment). Therefore, connect this terminal to a metal cold-water pipe or a long steel (or copper) ground rod driven deeply into the earth. Do not use a gas pipe, plastic pipe or AC ground connections. Use at least 16-gauge wire. Make the run as short and direct as possible, without any sharp bends in the wire.

16VAC SUPV ..... (Left terminal; some PC boards may indicate "**AC**" or "**ACL**") Non-polarized 16VAC terminal used for monitoring AC (**for supervision only, not power**). Connect to AC power source terminal (power supply or Hub power).

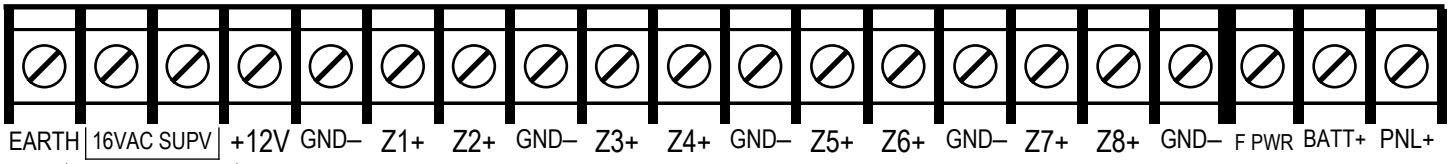
(Right terminal; some PC boards may indicate "**AC**" or "**ACN**") Non-polarized 16VAC terminal used for monitoring AC. Connect to AC power source terminal (power supply or Hub power).

+12V..... +12 volts DC to power the **ISEC-WL-MODULE**. Connect this terminal to the Hub + Auxiliary Power terminal or to the +12VDC terminal of the dedicated power supply

GND– ..... Common ground terminal for all sensors (all **GND** terminals are electrically equivalent). Therefore, connect the low side (negative) lead of each wired zone to the **GND** terminal next to each zone terminal (labeled **Z1**, **Z2**, etc.).
In addition, for the purpose of powering the **ISEC-WL-MODULE**, connect this terminal to the Hub (–) Auxiliary Power or to the (–) 12VDC of the dedicated power supply.

Z1+ - Z8+..... Connect the high side (positive) lead of each wired zone to its own screw terminal, labeled **Z1**, **Z2**, etc., for each zone 1 through 8, respectively.

F PWR.... Fire Reset (output). Pressing **RESET** on a system keypad causes this output to change state (on to off, off to on) for 10 seconds. Typically used to create a power output for latching 4-wire smoke detectors and similar devices that require power to be removed for reset. May also be used on door latches that normally require power, thus power is removed on a "Fire Alarm" event.



Some PC boards may indicate "**AC**" and "**AC**" or "**ACL**" and "**ACN**"

continued ⟶

12. Install Takeover Module (cont'd)

BATT+ ... Optional connection to the existing Hub battery + terminal (or + terminal of the power supply) for power supervision. Place shunt across **JP3** to enable supervision.

PNL+..... External +12VDC power input used to power the **FIRE** terminal (described above). Remove jumper **JP13** when **FIRE** output is powered by an external power source (for example, wired to the DC+ output of an external power supply). Install **JP13** to power the **FIRE** terminal from internal DC power. **IMPORTANT:** NEVER install wire to terminal **PNL+** when **JP13** is installed.

JUMPER DESCRIPTIONS

Jumper Block P2

These "Learn jumpers" are in the **P2** jumper block with positions numbered, from left to right, as **1** to **6**:

P2 Position 1 - Shunt position 1 to **DEFAULT** all board flash memory to the factory default settings (enters RF LEARN mode). Shunt position 1 before power up; after the **ISEC-WL-MODULE** is powered, remove jumper from position 1 and the LED marked **LED1** will flash, indicating the unit is waiting to be learned into the Go-Anywhere Hub.

When this learn process completes, **LED1** stops flashing and remains lit.

P2 Position 2 - Shunt position 2 to **DISABLE AC** monitoring of terminals **ACL** and **ACN**. If you wish to disable monitoring of the AC transformer that powers the DC power supply and you also wish to enable AC FAIL reporting, shunt this jumper 2. When **P2** is not shunted, the removal of AC will cause the system to annunciate.

P2 Position 3 - Shunt position 3 to **DISABLE BATTERY** monitoring on the terminal **BATT+**.

P2 Position 4 - Reserved for future use.

P2 Position 5 - Reserved for future use.

P2 Position 6 - Shunt position 6 to start an **END OF LINE RESISTOR LEARN** process for zone terminals **Z1** through **Z8** whereby the value of each normal zone condition is learned by the system. Within 3 seconds of shunting position 6, LED3 (at the top of the PC board) will blink to indicate the learn process is active. This learning process requires that the zone be wired to a sensor and **ZONE #** jumper (**JP5** to **JP12**; see below) be removed for a short time and re-installed. Each normal zone condition is learned by the system. If the zone is open, the zone condition will not be learned. When the zone learning process ends, remove jumper from position 6; in 3 seconds, LED3 will turn off to indicate the learning process has ended. **Note:** The factory default value of the zone terminating resistor is 2.2KΩ, *and therefore does NOT require this **END OF LINE RESISTOR LEARN** process*!

Zone Monitoring Jumpers (JP5 to JP12)

To enable zone monitoring for a zone, place a jumper one of the 8 jumper blocks labeled **JP5** (for **ZONE 1**) through **JP12** (for **ZONE 8**). Each zone 1 - 8 is assigned to terminals **Z1** through **Z8**, respectively.

Notice each jumper block labeled **JP5** through **JP12** contains vertical 4 pins:

- **FIRE** (top two pins): Selected zone reports as a Fire transmitter (for example, a model **ISEC-SMOKE** detector).
- **CO** (middle two pins): Selected zone reports as a carbon monoxide (model **ISEC-CARBON MON**) transmitter.
- **BURG** (lower two pins): Selected zone reports as a Burglary window / door transmitter (model **ISEC-DW-XMITTER**) with one point (i.e. reports the zone change from "normal" to "open").

SPECIFICATIONS

Electrical Ratings

Input Power: 12.5 - 7.5VDC, 60mA.
Zone Loop current: 4.7mA nominal, 5.5mA when shorted.
Maximum Zone Loop Resistance: 300 ohms.
2.2K End of line resistor (part number EOL2.2K required in Fire applications).
Output Power:
PGM Output (Active low): 5mA, 12V. Connect only to power-limited circuits less than 14VDC. Use only in Burglary applications.
Ground Faults Detected: 1.25KΩ to ground or less.

BATTERY MONITORING

When monitoring the battery is required, install the shunt across **P2 Position 2**.

Battery Wiring:

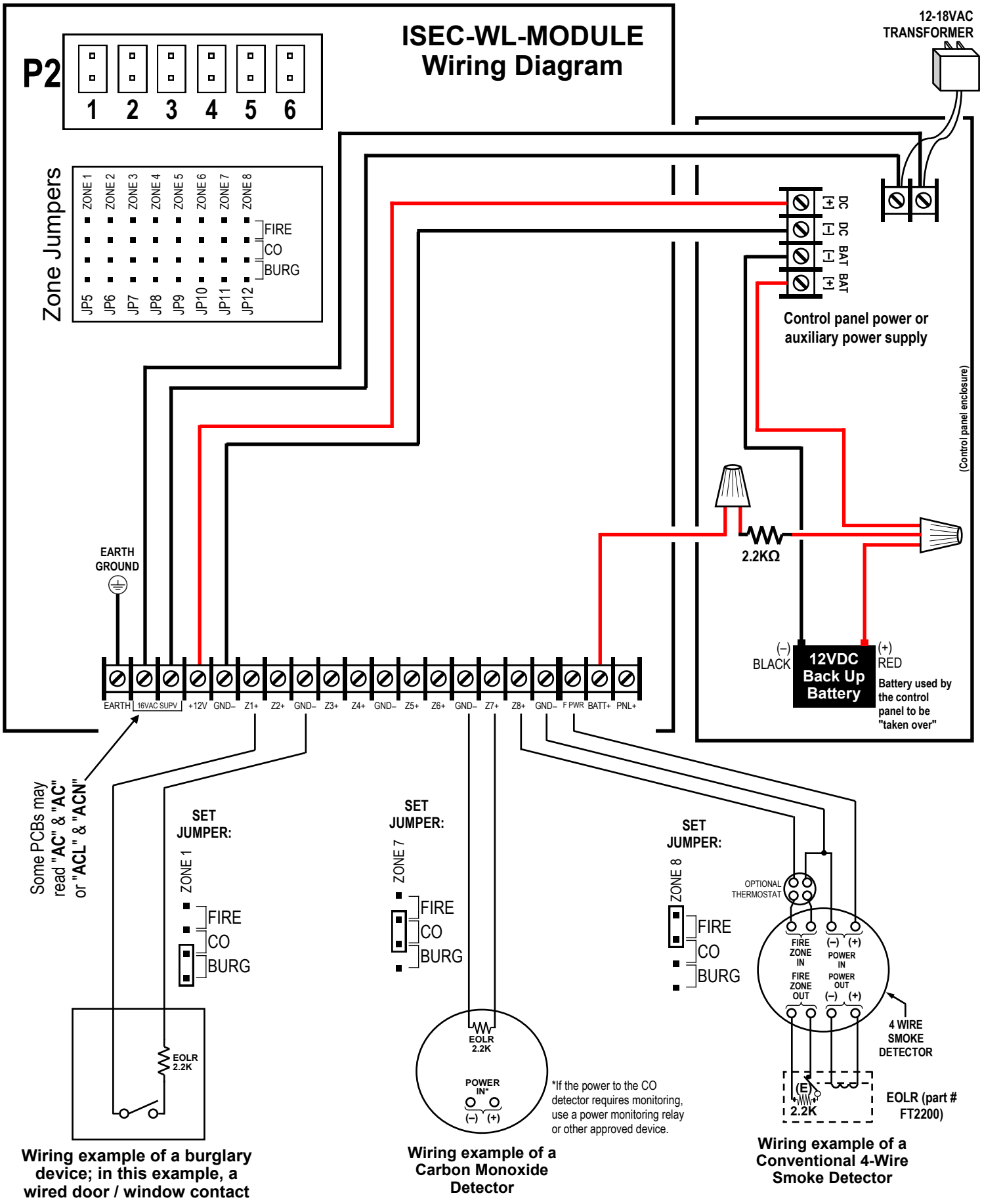
1. Disconnect the battery of the Hub to be taken over and unplug its AC transformer.
2. Cut the control panel's red battery flying lead approximately 3 inches from the battery terminal.
3. Strip both sides of the cut flying lead to expose wire.
4. Inside the panel housing, using a suitable wire connector, crimp both sides of the stripped flying battery lead and one side of the supplied EOLR2.2K.
5. Using a suitable connector, crimp the remaining side of the EOLR2.2k to the wire that extends outside the panel housing to the ISEC-WL-MODULE "**BATT+**" terminal.
6. Ensure the wires connected to the battery are separated by at least 1/4 inch from any non-power limited wire inside the panel housing.

Enable AC Fail Monitoring:

- Install shunt across header **P2 Position 1**.
- For the Hub to be taken over, connect the AC terminal to the ISEC-WL-MODULE "**ACL**" terminal.

continued ⟶

12. Install Takeover Module (cont'd)



13. Install the ISEC-2WF-MOD

OVERVIEW

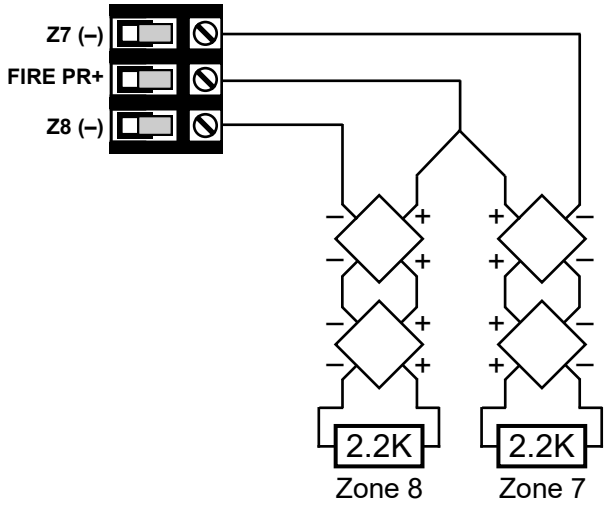
The **ISEC-2WF-MOD** *2-Wire Fire Sensor Module* allows your Napco iSecure Go-Anywhere Smart Hub to detect up to 20* *compatible* 2-Wire smoke detectors (10 per zone). The **ISEC-2WF-MOD** permits the use of existing compatible 2-Wire smoke detectors (see list of compatible smoke detectors, below), and all existing wiring to be used with your iSecure security system.

The **ISEC-2WF-MOD** requires 15mA standby current. The **ISEC-2WF-MOD** signals an alarm when the smoke detector initiates an alarm; refer to the smoke detector specifications for alarm current.

The 2-wire smoke detector wiring is connected to the Go-Anywhere Hub terminals for zones 7 and 8 as follows:

- **Z7 (–)**: Connects to the negative terminal of the two-wire smoke sensor (zone 7).
- **FIRE PR+**: Connects to the positive terminal of the two-wire smoke sensor.
- **Z8 (–)**: Connects to the negative terminal of the two-wire smoke sensor (zone 8).

Connect the 2-wire smoke detectors to the Go-Anywhere Hub terminals, as shown in the accompanying wiring diagram.



**Maximum Wire Length for use with 2WTA-B	
Solid FPLR ("Fire-Power Limited-Riser") or equivalent	**Maximum wire length for use with 2WTA-B**
18 AWG	150 feet (45.7m)
16 AWG	300 feet (91.4m)
14 AWG	350 feet (106.7m)

Based on 2 ohm line resistance.

Compatible 2-Wire Smoke Detector Models		
Manufacturer	**Model**	**Base**
NAPCO	FW-2, FW-2S (FW-RM1** required with the FW-2S** when more than 1 per loop)	N/A
Sentrol / ESL	711U, 712U, 721U, 721UT, 722U, 731U, 732U	701U, 702U, 702RE, 702RU
System Sensor	1100, 1151, 1400, 2100, 2100T, 2100S, 2100TS, 2151, 2400, 2400TH, 2WTA-B**	N/A

Note: Voltage Rating: 8.5 - 13.3VDC.

*Maximum five (5) model FW-2S detectors when using the FW-RM1.

The 300m alarm current supplied by the Go-Anywhere Smart Hub must be reduced by 60mA for each zone using a FW-2S without the FW-RM1. When using the FW-RM1, the standby current must be reduced by 30mA and the 300mA available alarm current reduced by 60mA for each FW-2S used. In addition, when using the FW-RM1, the 470Ω resistor supplied with the FW-RM1 must be placed across the **Bell + and **Bell –** terminals.

Prior to opening the **ISEC-2WF-MOD** PC board package or touching anything inside the iSecure Go-Anywhere Smart Hub enclosure, discharge any static electricity from your body or clothing. Use a grounded wrist strap or touch an unpainted, grounded metal object.

13. Install the ISEC-2WF-MOD (cont'd)

ISEC-2WF-MOD INSTALLATION

If the Go-Anywhere Smart Hub enclosure is not already open, open the enclosure as directed on page 10, step 3. Remove all A/C and battery power and install the **ISEC-2WF-MOD** into the iSecure Hub main PCB as follows:

1. Insert the plastic Standoff into the bottom of the **ISEC-2WF-MOD** (Fig. 1).

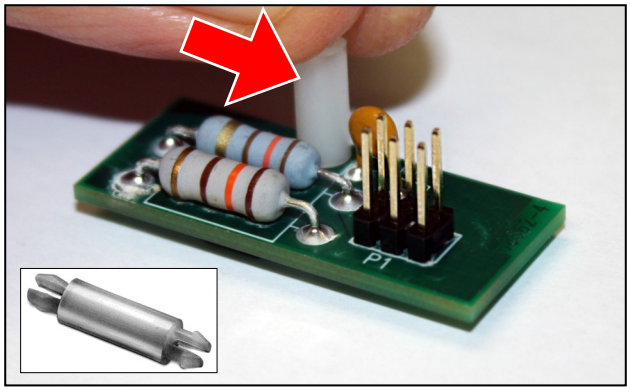


Fig. 1: Standoff (arrow)

2. Use Fig. 2 to locate the **Header Socket** located near the middle left side of the Hub PCB (circled). Also locate the Standoff hole (arrow).

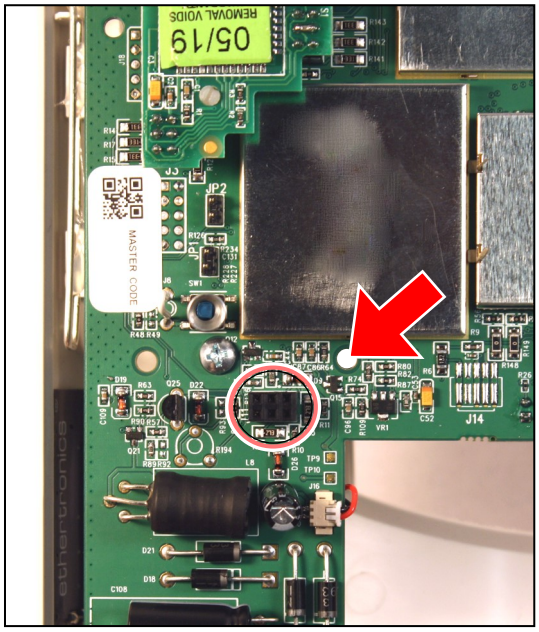


Fig. 2: "Header Socket" (circled)

3. Carefully align the Standoff with its hole, and align the **Header Plug** with its **Header Socket** (Fig. 3).

   Firmly press the **ISEC-2WF-MOD** into the PC board.

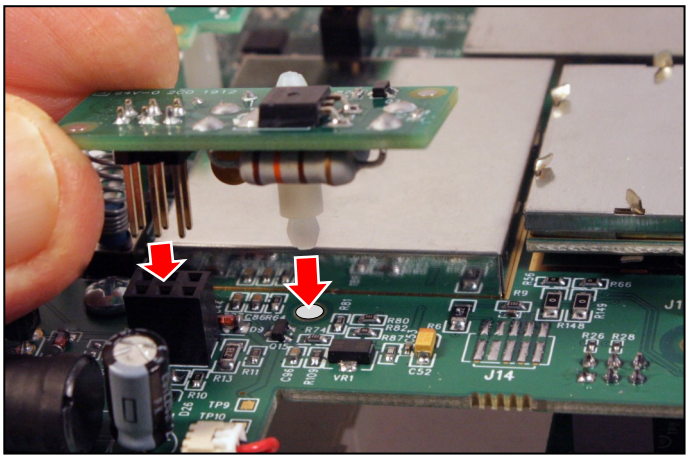


Fig. 3: Align and insert ISEC-2WF-MOD

PROGRAMMING

After the **ISEC-2WF-MOD** module is installed, program the Go-Anywhere Hub using the iSecure Cloud Web Portal:

1. Log into the iSecure Cloud Web Portal at www.iSecureByNapco.com as a Dealer (click **Dealer Login**).
2. Click **Sensor Configuration**.
3. In zone 7 or in zone 8, in the **Sensor Type** column, select **Wired Fire**.

14. Install the ISEC-WIFI

The **ISEC-WIFI** allows your Napco iSecure Go-Anywhere Hub to connect to the Internet by means of a wireless (Wi-Fi) link, eliminating a wired Ethernet cable connection. **Note:** The **ISEC-WIFI** requires 46mA (standby current); refer to the "**STANDBY - BATTERY CALCULATION WORKSHEET**" in this manual to verify that sufficient power is available.

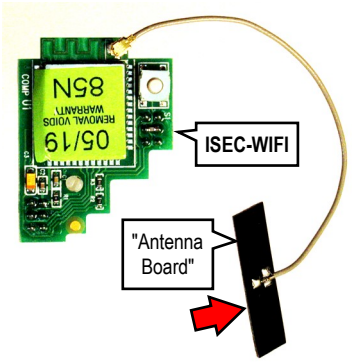


Fig. 1: ISEC-WIFI and Antenna Board (with adhesive). Arrow points to top edge.

Prior to opening the **ISEC-WIFI** PC board package or touching anything inside the iSecure Go-Anywhere Smart Hub enclosure, discharge any static electricity from your body or clothing. Use a grounded wrist strap or touch an unpainted, grounded metal object.

INSTALLATION STEPS

The **Antenna Board** (see Fig. 1) has "peel and stick" adhesive that secures it to the inside of the Go-Anywhere Hub front housing, **with its top edge facing up**). Keep the wire away from the "Top Antenna" at the top of the Hub.

1. **Remove AC power from the Go-Anywhere Smart Hub** by unplugging the AC transformer.
2. **Separate the Go-Anywhere Hub housing**. With a flat head screwdriver, push in the two tabs at the bottom to unhook, then carefully separate the two parts of the Hub housing (separating the housing disconnects the battery).
3. **Remove the six (6) screws** that secure the Go-Anywhere Hub motherboard PCB to the front housing. See the arrows in Fig. 2 for screw locations.
4. **The Antenna Board has "peel and stick" adhesive**. Peel off the protective paper without touching the adhesive.
5. **Carefully lift the motherboard** only until you have enough clearance for the following:
   - ***With the top edge of the Antenna Board facing up***, secure the antenna adhesive to the interior plastic, as shown in Fig. 3.

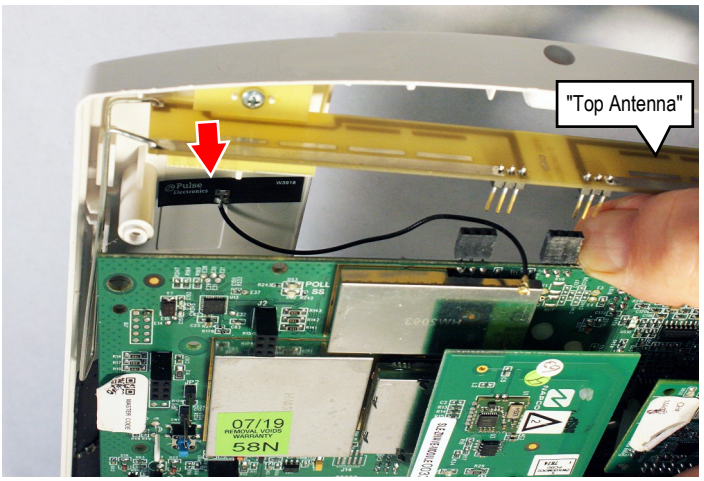


Fig. 2: Arrows show six (6) screws securing the motherboard. The Top Antenna, is also shown

Fig. 3: Carefully lift the motherboard. Note the location of the Antenna Board's "top edge" (arrow) .

Be careful not to lift the motherboard too far, ensuring all connections remain secure.

Note: Be aware the Top Antenna may become disconnected; its connectors can easily be re-inserted after the next step.

6. **Lower the motherboard**, re-aligning all mounting holes. *Gently pull the Antenna Board plug and wire toward the **front** of the motherboard* (this will assist with its connection to the **ISEC-WIFI** module in a future step).

   If the Top Antenna disconnects from the motherboard, be sure to carefully re-insert the connections.
7. **Replace the six (6) screws** that secure the Go-Anywhere Hub motherboard PCB to the front housing. See the arrows in Fig. 2 for screw locations.
8. **With the ISEC-WIFI PC board in hand**, connect the small **Antenna Board** plug to the **ISEC-WIFI** module socket (see Fig. 4).

   The antenna wire should freely rotate while remaining connected. **Important:** Handle this wire with care; do not twist, create sharp bends or apply excessive force.

14. Install the ISEC-WIFI (cont'd)

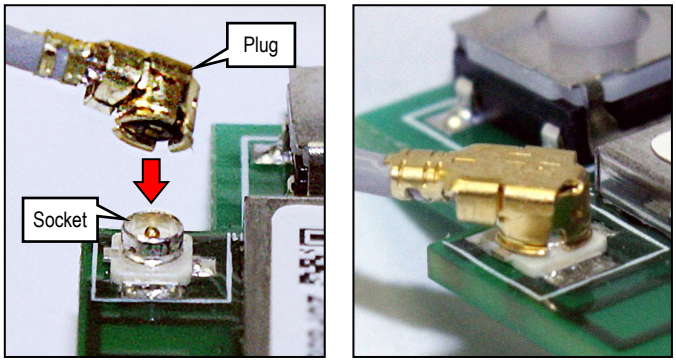


Fig. 4: Antenna Wire Plug and Socket

In addition, keep the wire away from the "Top Antenna" that runs along the top edge of the motherboard, as shown in Fig. 2.

9. Insert the plastic **Standoff** into the bottom of the **ISEC-WIFI** (see Fig. 5).

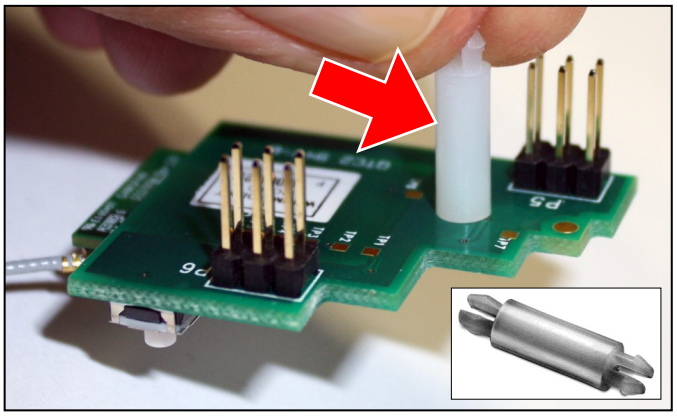


Fig. 5: Standoff (arrow)

10. Use Fig. 6 to locate the two **Header Sockets** located near the top left side of the Hub PCB (circled). Also locate the **Standoff hole** (arrow).

11. With the small Antenna Wire Plug located at the top of the **ISEC-WIFI** PC board, carefully align the Standoff with its hole, and align the two **Header Plugs** with their **Header Sockets** (Fig. 6). Firmly press the **ISEC-WIFI** into the PC board.

12. Re-assemble the Go-Anywhere Smart Hub enclosure as directed in "**Install the Go-Anywhere Hub**" on page 10.

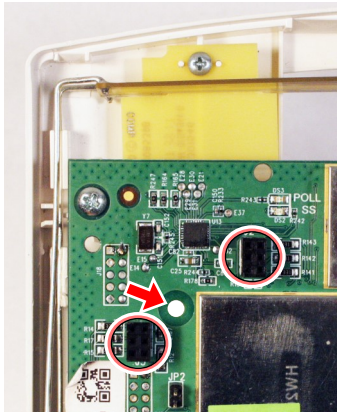


Fig. 6: "Header Sockets" (circled)

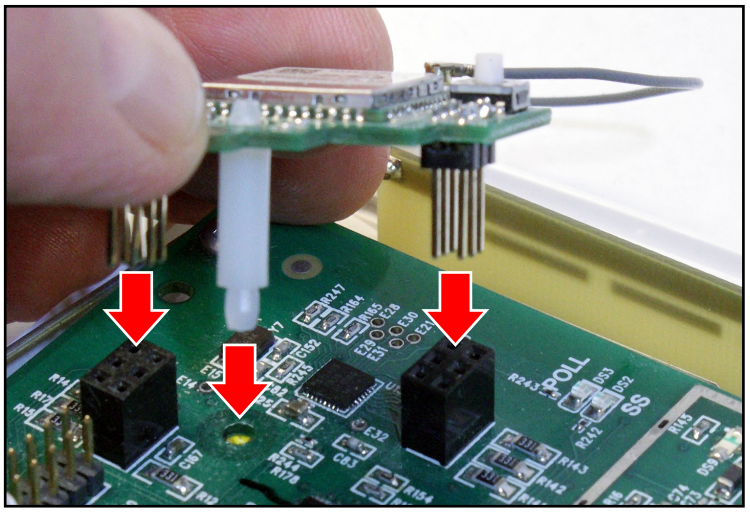


Fig. 7: Align and insert ISEC-WIFI (PC Board)

PROGRAMMING

After the **ISEC-WIFI** module is installed, program the Go-Anywhere Hub using the iSecure Cloud Web Portal:

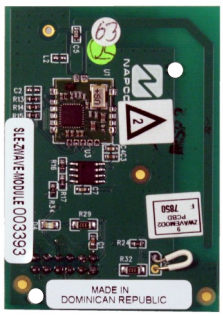
1. Log into the iSecure Cloud Web Portal at www.iSecureByNapco.com as a Dealer (click **Dealer Login**).
2. Enter the **Radio Serial Number** and click **Submit**.
3. Before Wi-Fi networks can be searched, click **Central Station Reporting** and perform the following:
   - At the top of the screen, click to select the **Central Station Reporting** radio button.
   - In the **COMMUNICATION TECHNOLOGY** pull-down, select **IP with Cell Radio Backup** or **IP Only**, depending on your installation.
   - Check **Enable IP Supervision**, if desired.
   - In **Configuration Type**, select **Ethernet Preferred with WiFi Backup (non-UL)**.
   - In **IP Configuration Type**, select **DHCP**.
   - Click **Save** to download your changes and restart the system.
   - In **Dealer Entered Programming**, click **Search WiFi Networks** (a popup will appear warning that scanning may take up to 3 minutes). Click **Yes** to continue.
   - In the **Wi-Fi Networks** pull-down, find and select the SSID name of the customer's network. Upon selection, the **Security Type** and **Selected Network** fields will automatically populate.
   - Type the **Password** of the customer's Wi-Fi network and click **Save**. **Note:** The **Wi-Fi Module Version** will not appear until connected.

ELECTRICAL RATINGS

Primary Operating Supply: 3.3VDC from Go-Anywhere Smart Hub motherboard. 46mA standby current draw.

15. Install the ISEC-ZWAVE

The **ISEC-ZWAVE** allows you to control your Z-Wave devices through your NAPCO iSecure system. **Note:** This and all other iSecure documents are available for download at our Technical Library: tech.napcosecurity.com.
The **ISEC-ZWAVE** requires 20mA; refer to the "**STANDBY - BATTERY CALCULATION WORKSHEET**" on page 72 to verify that sufficient power is available.



ISEC-ZWAVE

Prior to opening the **ISEC-ZWAVE** PC board package or touching anything inside the radio enclosure, discharge any static electricity from your body or clothing. Use a grounded wrist strap or touch an unpainted, grounded metal object. Install as follows:

ISEC-ZWAVE Installation

If the Go-Anywhere Smart Hub enclosure is not already open, open the enclosure as directed on page 10, step 3. Remove all A/C and battery power and install the **ISEC-ZWAVE** into the iSecure Go-Anywhere Smart Hub main PCB as follows:

1. Insert the two plastic Standoffs (red arrows "**A**" and "**B**"). into the bottom of the **ISEC-ZWAVE** (Fig. 1).

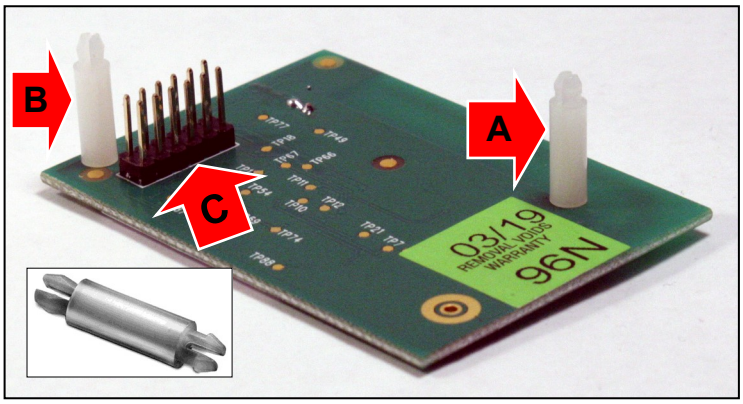


Fig. 1: Two Standoffs (red arrows "A" and "B") and Header Socket J1 (red arrow "C"). Standoff shown in bottom left image.

2. Re-verifying that the Go-Anywhere Smart Hub A/C and battery power are disconnected, use Fig. 2 to locate the two **Standoff Holes** located near the center of the Go-Anywhere Smart Hub PCB (red arrows "**A**" and "**B**") and locate the **Header Socket J1** (red arrow "**C**").

3. Carefully align the two **Standoffs** with their two holes, and align the **Header Plug** with its **Header Socket** (Fig. 3). Firmly press the **ISEC-ZWAVE** into the PC board.

4. Reconnect the Go-Anywhere Smart Hub A/C and battery power. Wait 2 minutes for all devices to fully power before proceeding.

For full programming information, see OI414.

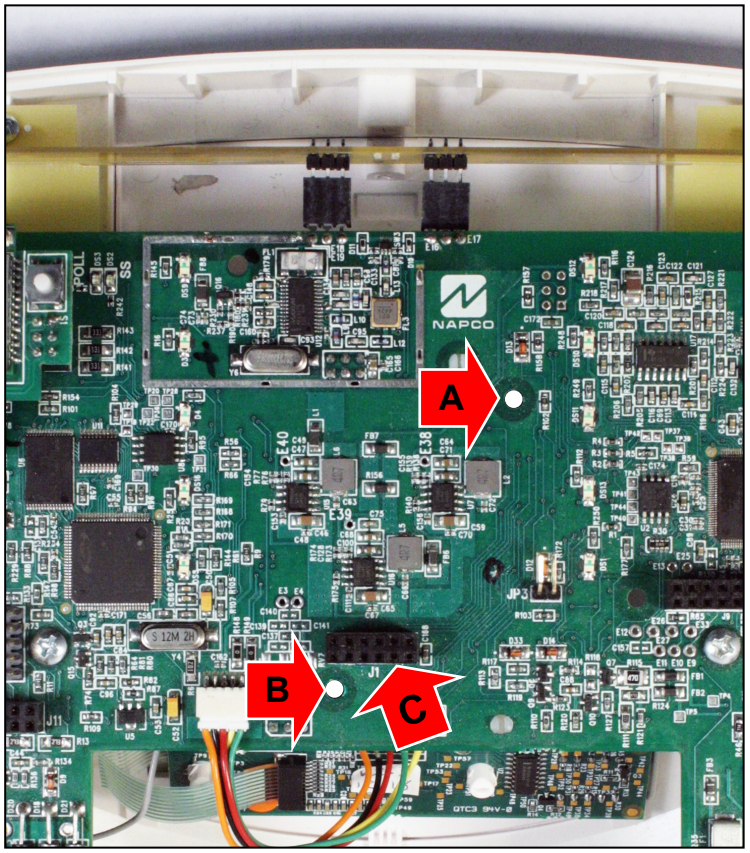


Fig. 2: Two standoff holes ("A" & "B") and "Header Socket J1" ("C").

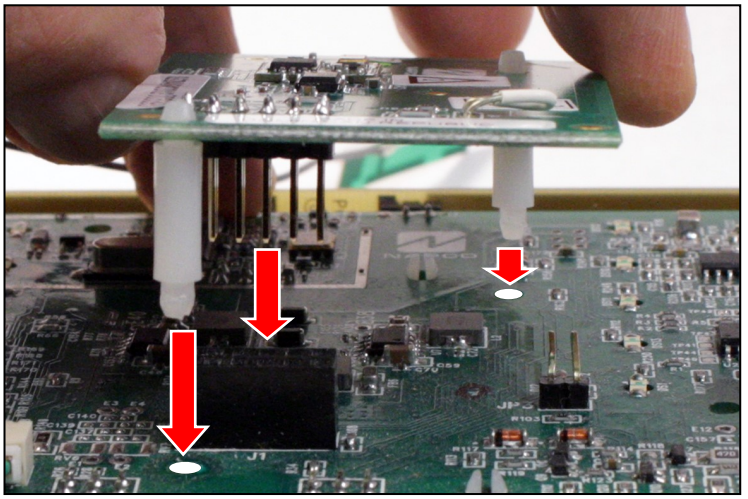


Fig. 3: Align and Insert the ISEC-ZWAVE.

Install the ISEC-EXTANT-KIT (optional)

The **ISEC-EXTANT-KIT Internal LTE Extended Antenna Bracket Kit** is installed inside the iSecure Go-Anywhere Hub to permit the connection of an external LTE antenna to improve reception in weak cellular signal areas. This **Bracket** assembly, pictured in Fig. 1, provides an alternate SMA connection to the LTE radio, allowing the use of Napco **SLE-ANTEXT** antenna kits. The remote-mounted antenna is a dual-wideband, indoor/outdoor LTE antenna that significantly improves cellular reception (**Note:** Mount the **SLE-ANTEXT** antenna before performing these instructions to allow its immediate use after installing the **ISEC-EXTANT-KIT** and the radio is re-powered). For details about the SLE-ANTEXT, see WI2230, available from the NAPCO Technical Library at tech.napcosecurity.com.

INSTALLATION STEPS

Bracket installation requires flat and Phillips head screwdrivers and a cable zip tie (supplied).

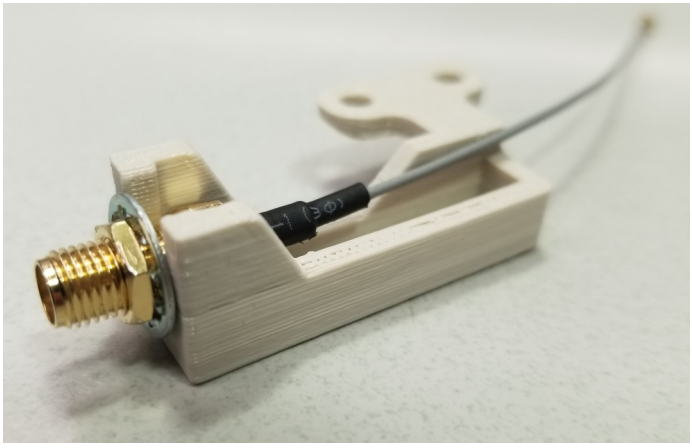


Fig. 1: Antenna Bracket Assembly ("Bracket")

1. **Remove AC power from the Go-Anywhere Smart Hub** by unplugging the AC transformer.
2. **Separate the Go-Anywhere Hub housing**. With a flat head screwdriver, push in the two tabs at the bottom to unhook, then carefully separate the two parts of the Hub housing. **Note:** Separating the housing disconnects the battery.
3. **Remove the top screw** at the top of the unit that secures the front LED Faceplate to the front housing.
4. **Remove the LED Faceplate**. From the front of the housing, pull out the LED Faceplate to remove. .
5. **On the inside of the LED Faceplate**, remove the screw that secures the *right side* light pipe (when viewing from the rear) as shown in Fig. 2.
6. **While keeping the light pipe in place**, position the Bracket on top of the light pipe boss . Re-install the screw removed in step 6 and install an additional screw as shown in Fig. 2.

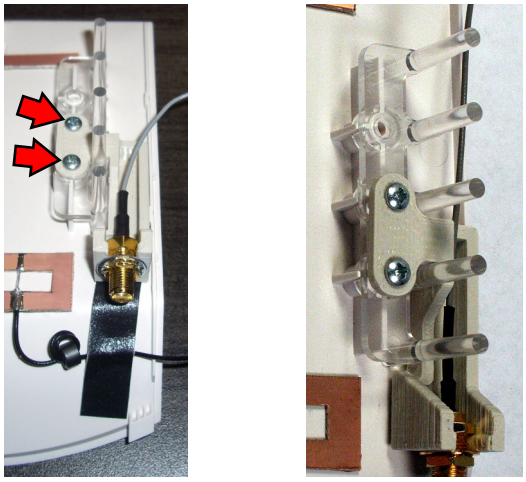


Fig. 2: Two views of rear LED Faceplate: Secure Bracket to right side with two screws (arrows) on top of light pipe.

7. **Connect the Antenna (SMA female) cable** end to the male threaded end of the Bracket (see Fig. 3). Route the cable through the Hub housing.

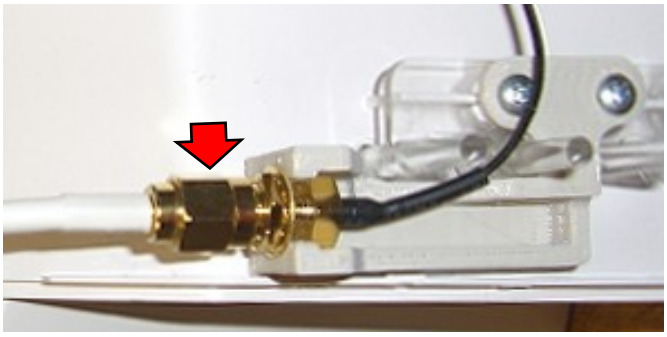


Fig. 3: Connect the cable to the Bracket.

8. **Insert the very small Antenna Plug** located at the end of the Bracket (shown in Fig. 4) into the correct PC board sockets as described in Fig. 5:

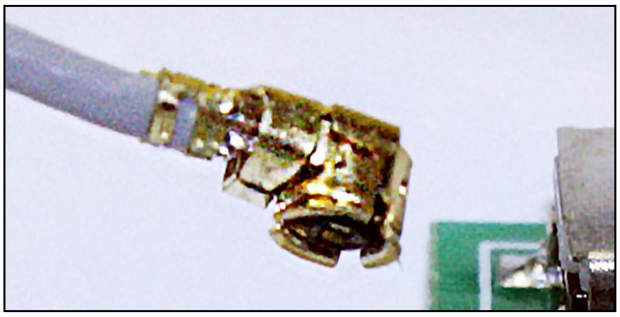


Fig. 4: Antenna Plug

Be sure the plug freely rotates but remains connected. If this plug should disconnect, simply insert and press firmly until connected. ***Handle wire with care; do not twist, create sharp bends or apply excessive force***.

9. **Replace the LED Faceplate**. Be careful to ensure both Antenna Plugs remain connected to their sockets.

Install the ISEC-EXTANT-KIT (cont'd)

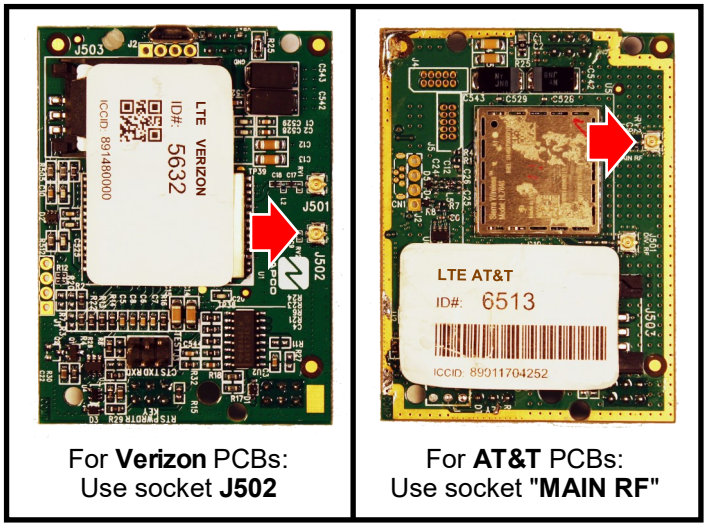


Fig. 5: Verizon and AT&T Antenna Socket Locations

10. **Route the cable through the Hub** and along the pathway shown in Fig. 6. Guide the cable to the right and around the side "ribs" shown in Fig. 7 and down along the bottom of the Hub PC board.

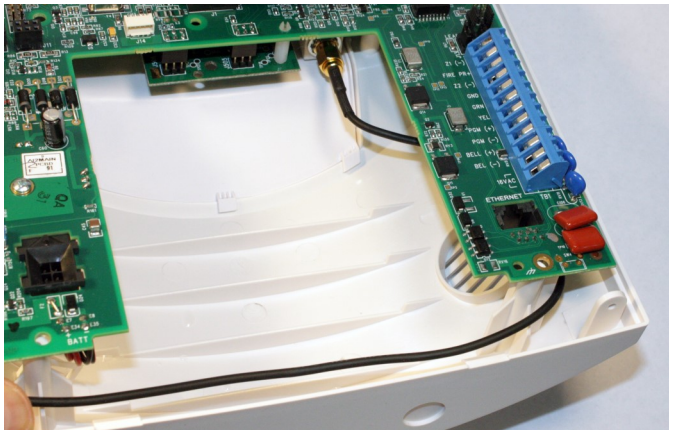


Fig. 6: Route the Antenna Cable to the right of the side "ribs" as shown in this image and in Fig. 7.

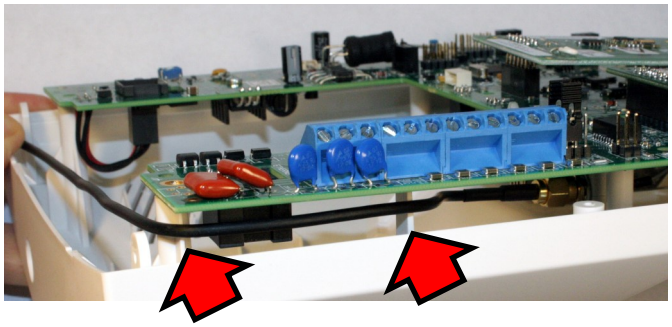


Fig. 7: Route the cable around the side "ribs" (arrows) as shown.

Important: To ensure maximum reception performance, the cable **must** be routed along this path.

11. **For strain relief**, secure the cable to the PCB by inserting the zip tie into the PCB hole shown in Fig. 8.

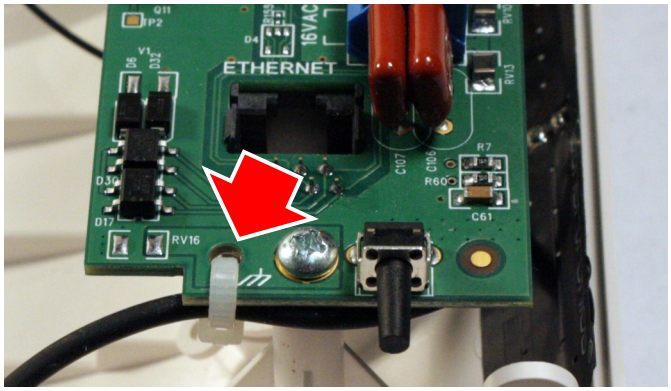


Fig. 8: For strain relief, secure antenna cable to the PCB with zip tie

Before proceeding, be sure the **SLE-ANTEXT** antenna is connected to allow its immediate use when the radio is re-powered in the next step.

12. **Close the two parts of the Hub housing, routing the cable** out the rear access door (see Fig. 9). Be sure not to crimp the wire between the PCB and the housing.

    Closing the two parts of the Hub housing will re-power the unit, and the antenna will immediately begin transmitting.

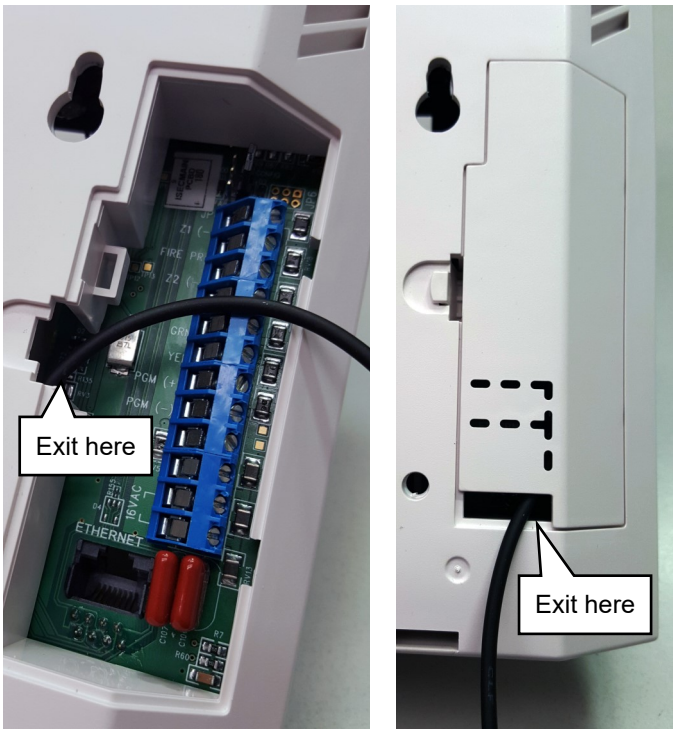


Fig. 9: Route cable through access door. With access door installed, route cable through the opening in the bottom of the door.

13. **Re-connect AC power to the Go-Anywhere Smart Hub** by plugging in the AC transformer. Test system operation.

Go-Anywhere Smart Hub Icons

"ARMED" Light (Red)
- Steady On: Armed
- Slow Flash: Alarm
- Rapid Flash: Instant
- Off: Disarmed

"STATUS" Light (Green)
- On Steady: Disarmed and all zones secured
- Off: Open Zone

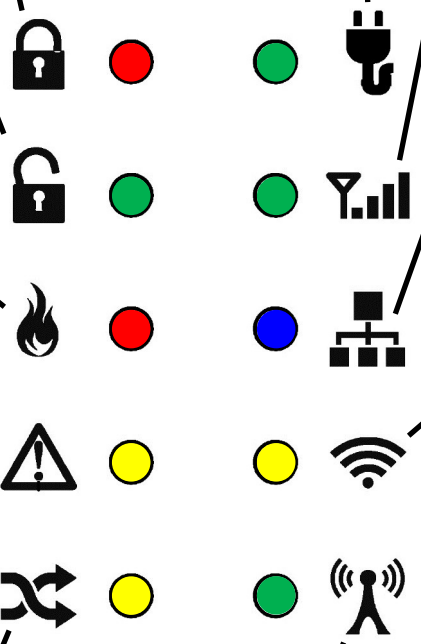
"Fire" (Red)
- On Steady: Fire Silenced
- Pulsing: Fire Alarm

"Trouble" (Yellow)
- Steady: System Trouble Acknowledged
- Flashing: System Trouble

"Bypassed" (Yellow)
- On: Zone(s) Bypassed

Wireless Sensor Transmissions (Green)
- On: Receiver trouble due to excessive radio noise in area. Try relocating the Smart Hub. Otherwise, call for service
- Rapid Flicker: Transmissions in progress
- Flashing: 900MHZ peripheral download Status
- Off: No transmissions

"Smart Hub AC" (Green)
- On: AC On
- Off: AC Off



"Cellular Signal Strength" (Green)
- Flashes: Smart Hub cellular signal strength 1-8

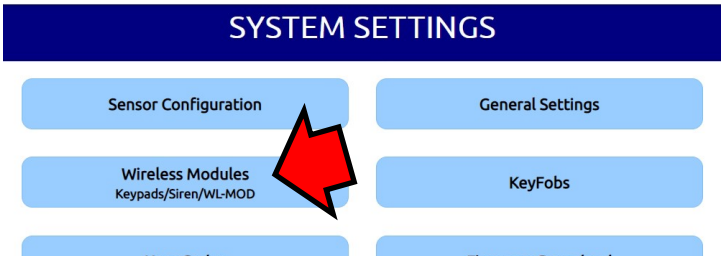
"Operational Status" (Blue)
- Normal: Momentary Blink every 10 seconds
- All Other Blinks: Cellular Communications in progress

"IP Network Wi-Fi" (Yellow)
- OFF: Network OK
- Rapid Flashes: No IP connection
- 1 blink: No network cable detected
- 2 blinks: No access to Internet via network cable
- 3 blinks: Ethernet failed to communicate
- 4 blinks: Ethernet poll / checkin failure
- 5 blinks: Wi-Fi enabled but no Wi-Fi installed
- 6 blinks: No Wi-Fi access to internet
- 7 blinks: Wi-Fi failed to communicate
- 8 blinks: Wi-Fi poll / checkin fail
- 9 blinks: Wi-Fi no serial data response
- 10 blinks: Wi-Fi security authentication failed

Programming: Keypads / Touchscreens

ISEC-WL-KEYPAD
Wireless Battery-Operated Standard Keypad

ISEC-WL-TOUCH
Wireless Touchscreen



1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Wireless Modules** > **Keypads**.
3. In the **KEYPADS** screen (shown below), program the installed keypads as indicated (when finished, click **Save**).

What are Emergency Buttons?
Scroll to the bottom of the **KEYPAD** screen to enable the use of *Emergency Buttons* for your security system. Emergency Buttons are used together with the keypad "Star" button to signal an emergency. With the **ISEC-WL-KEYPAD**:

- Press 7 & "Star" simultaneously for *Fire Emergency*.
- Press 8 & "Star" simultaneously for *Auxiliary Emergency*.
- Press 9 & "Star" simultaneously for *Police Emergency*.

(With the **ISEC-WL-TOUCH**, press and hold the appropriate **FIRE**, **AUX** or **PANIC** button, respectively; see the User's Guide for details). By default, Emergency Buttons are enabled for all keypads; to disallow their use, simply uncheck the selections for the keypad, as desired.

1
TYPE
- **ISEC-WL-TOUCH** (Select "**Color Touch**")
- **ISEC-WL-KEYPAD** (Select "**LCD**")

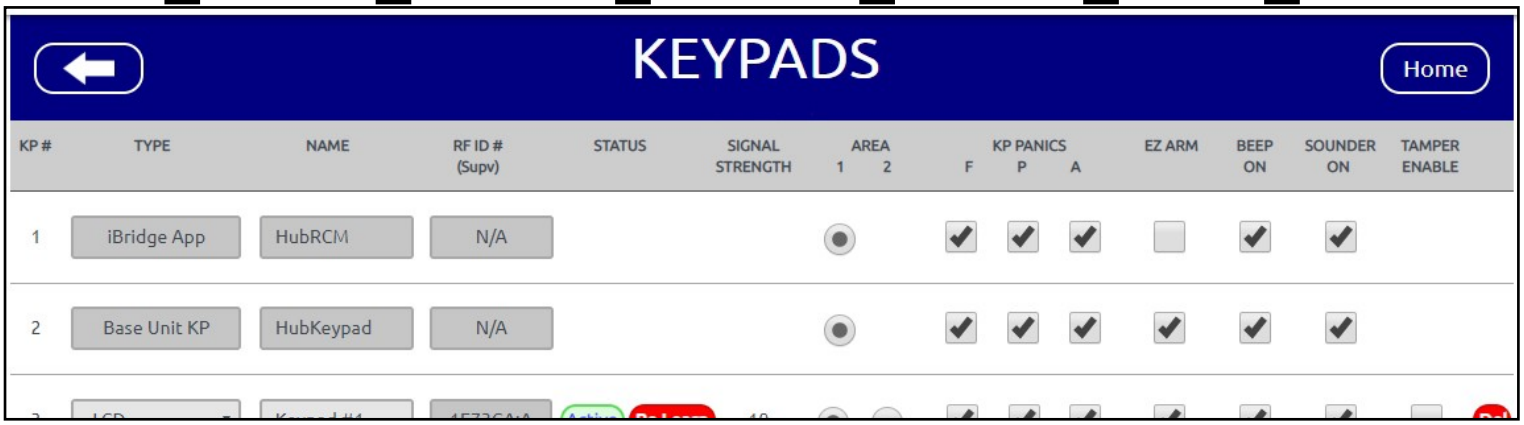
2
NAME
Type the keypad location (for example, "**Front Door**").

3
RF ID
Type in the 7 digit sensor ID # for the device

4
AREA
Default = 1. (See the keypad Operating Guide for "Area" definition).

5
KP PANICS
(See above "**What are Emergency Buttons?**")

6
EZ ARM
Permits quick arming by pressing and holding **ENTER** for 2 seconds.



SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the keypad closer to the Hub.

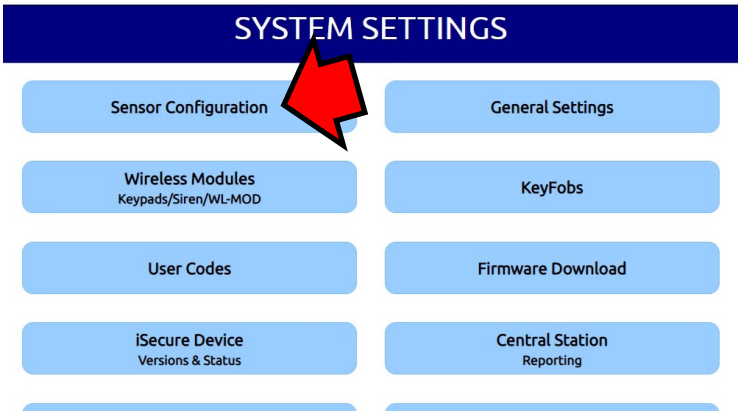
7
BEEP ON
Check to enable keypad feedback (button presses, etc.)

8
SOUNDER ON
Check to enable exit/entry keypad sounder.

9
TAMPER ENABLE
Check to enable the keypad tamper switch (removal from rear case or from wall)

Programming: Motion Sensors

ISEC-MOTION
Wireless Passive Infrared Motion Sensor



1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed motion sensors as indicated (when finished, click **Save**).

5

AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

CHIME
Check to sound a chime when motion is detected.

3

SENSOR FUNCTION
Select "**Instant**" or "**Interior**". When armed "**STAY**" (usually when sleeping), and you want the motion to ignore movement within the home, select "**Interior**". If you want the sensor to immediately trigger an alarm when motion is detected, select "**Instant**".

1

DESCRIPTION
Type the sensor description you wish to appear on the keypad display

2

SENSOR TYPE
Select "**Motion Sensor**".

4

SENSOR ID
Type in the 7 digit sensor ID # for the device

6

ENABLE REPORTING
Check to enable central station reporting

SENSOR CONFIGURATION

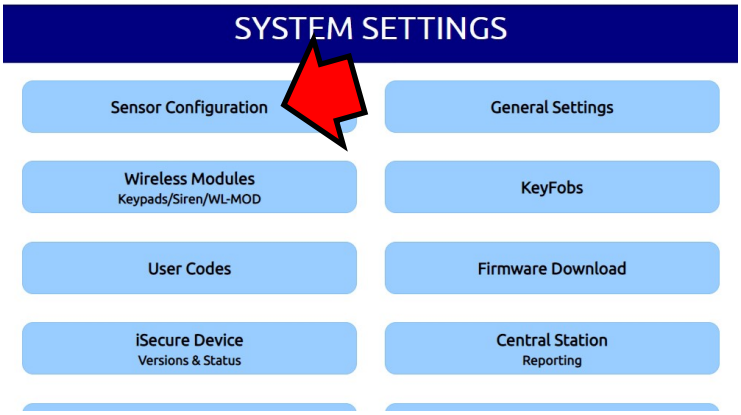
Home

ZONE #	DESCRIPTION	SENSOR TYPE	SENSOR FUNCTION	SENSOR ID #	AREA	CHIME	ENABLE REPORTING	SIGNAL STRENGTH
1	01-Trans LP-# 1154CEF:4	Door Window	Exit/Entry 1	154CEF:4	1, 2	1, 2	✓	10
2	02-Trans LP # 2 11C1F0:B	Door Window	Exit/Entry 2					10
3	03-TRANS 2 0D3E54:3	Door Window	Interior	0D3E54:3	1, 2	1, 2	✓	10
4	04-WL PIR 528A83:F	Motion Sensor	Interior	528A83:F	1, 2	1, 2	✓	10

SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

Programming: Glass-Break Sensors

ISEC-GLASSBREAK
Wireless Glass-Break Sensor



1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed glass break sensors as indicated (when finished, click **Save**).

3

SENSOR FUNCTION
For most installations, we recommend selecting "**Instant**". With "**Instant**", when the system is armed, the sensor will immediately trigger an alarm when the sound of glass breaking is detected. If you select "**24Hr Zone Audible**", the system will trigger an alarm when the sound of glass breaking is detected, whether the system is armed or disarmed.

5

AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

1

DESCRIPTION
Type the sensor description you wish to appear on the keypad display

2

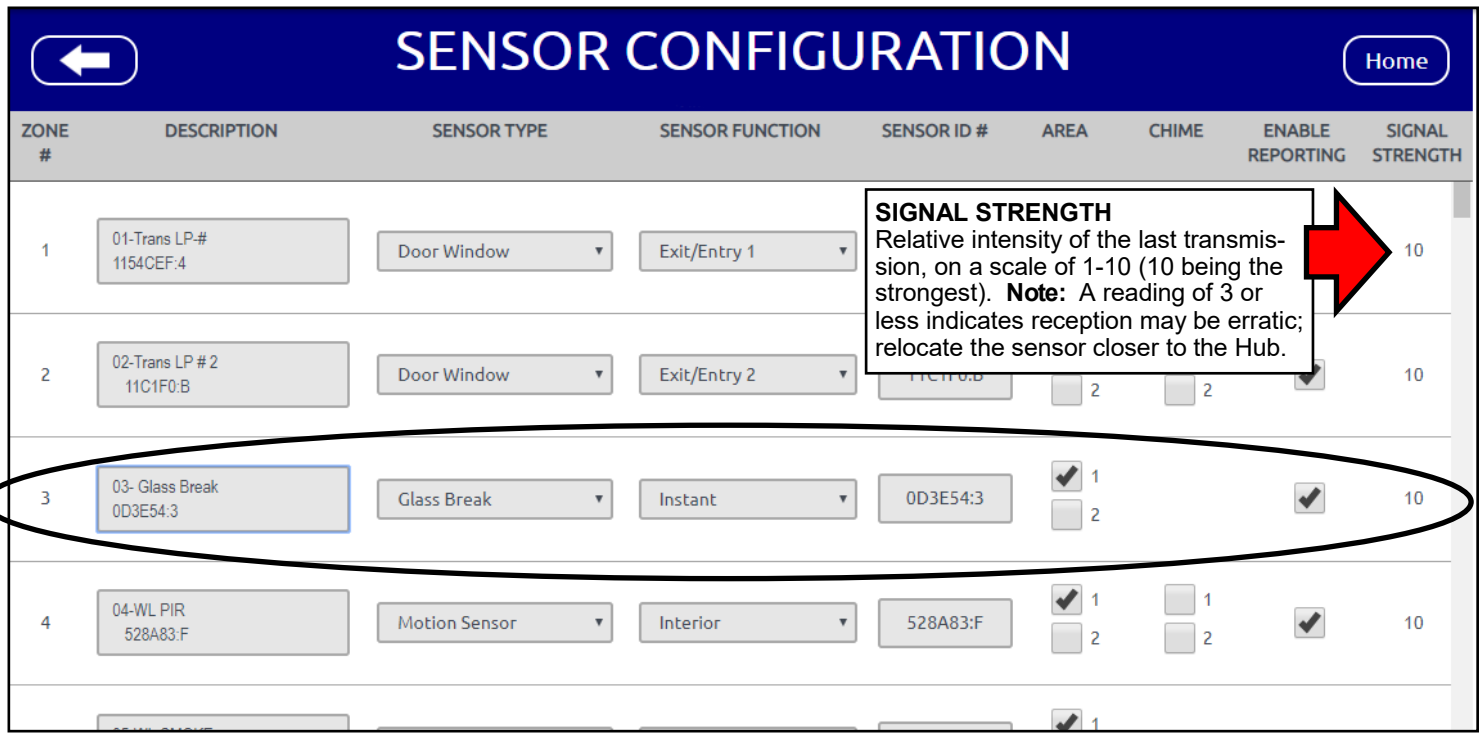
SENSOR TYPE
Select "**Glass Break**".

4

SENSOR ID
Type in the 7 digit sensor ID # for the device

6

ENABLE REPORTING
Check to enable central station reporting

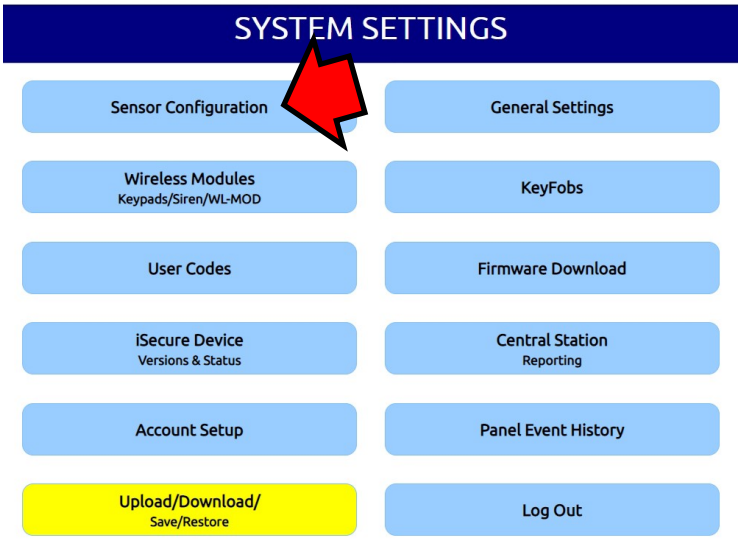


SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

Programming: Window / Door Transmitters

ISEC-DW-XMITTER *Window / Door Transmitter*

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed transmitters as indicated (when finished, click **Save**).



3

SENSOR FUNCTION
- **Exit/Entry 1 & 2:** Allows for exit delay (when leaving the premises) and entry delay (when entering) before triggering an alarm. One of two separate exit/entry combinations can be selected.
- **Interior:** Use when armed "**STAY**" (usually at night when sleeping), and you want the system to ignore this sensor. For example, use for an interior door that will be in use when armed "**STAY**" but protected when armed "**AWAY**".
- **Instant:** Allows for an immediate alarm when activated, providing instant protection while you or someone else is in the premises.
- **24Hr Zone Audible:** Provides protection at all times, whether or not the system is armed, by sounding an alarm when the door or window is opened.
- **24Hr Zone Silent:** Provides protection at all times, whether or not the system is armed. When armed and the door or window is opened, a silent alarm will be sent to the central station.
- **Audible Panic:** Triggers the siren to immediately sound and an emergency report sent to the central station.
- **Silent Panic:** Triggers a silent report to be sent to the central station (i.e. the user can silently signal an emergency).

5

AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

CHIME
Check to sound a chime when a door (or window) is opened in an unarmed system.

7

SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest).
Note: A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

1

DESCRIPTION
Type the sensor description you wish to appear on the keypad display

2

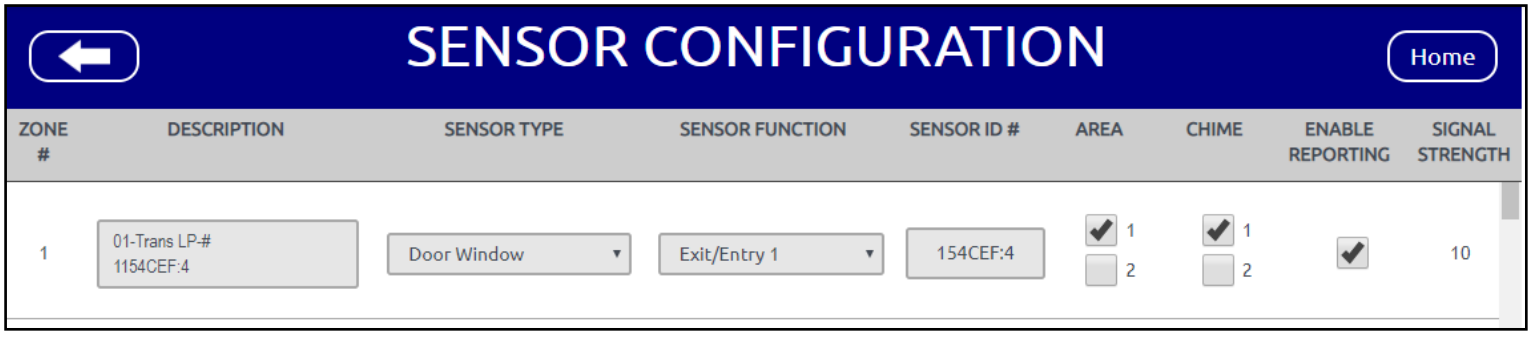
SENSOR TYPE
Select "**Door Window**".

4

SENSOR ID
Type in the 7 digit sensor ID # for the device

6

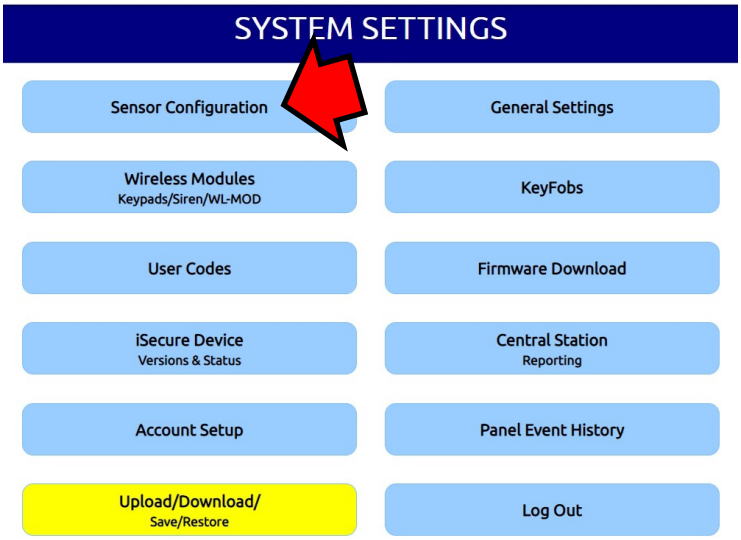
ENABLE REPORTING
Check to enable central station reporting



Programming: Smoke Sensors

ISEC-SMOKE *Supervised Wireless Digital Smoke Sensor*

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed sensors as indicated (when finished, click **Save**).



1
DESCRIPTION
Type the sensor description you wish to appear on the keypad display

2
SENSOR TYPE
Select "**Smoke Sensor**".

3
SENSOR FUNCTION
"**Smoke**" is automatically selected when "**Smoke Sensor**" is selected as the "**SENSOR TYPE**".

4
SENSOR ID
Type in the 7 digit sensor ID # for the device

5
AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

6
ENABLE REPORTING
Check to enable central station reporting

SENSOR CONFIGURATION — Home

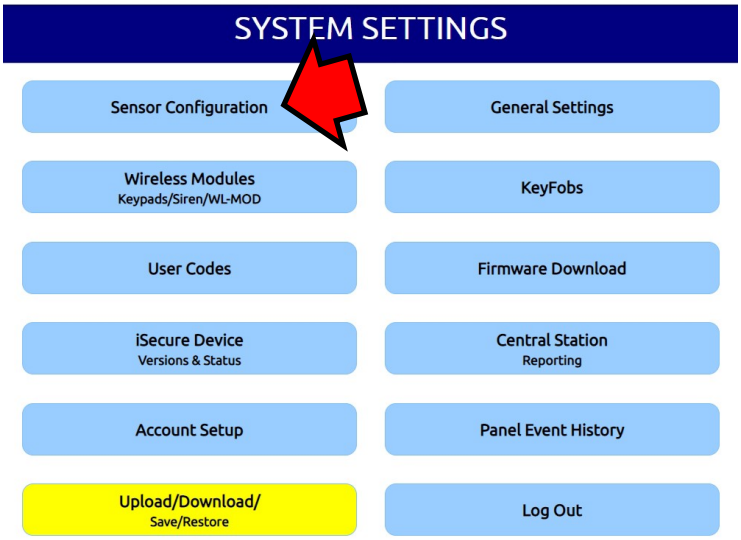
ZONE #	DESCRIPTION	SENSOR TYPE	SENSOR FUNCTION	SENSOR ID #	AREA	CHIME	ENABLE REPORTING	SIGNAL STRENGTH
1	01-Trans LP-# 1154CEF:4	Door Window	Exit/Entry 1					10
2	02-Trans LP # 2 11C1F0:B	Door Window	Exit/Entry 2		2	2		10
3	03- 2 Wire Smoke 0D3E54:3	Smoke Sensor	Smoke	0D3E54:3	1		✓	10
4	04-WL PIR 528A83:F	Motion Sensor	Interior	528A83:F	1	1	✓	10

SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

Programming: Heat Sensors

ISEC-HEAT
Wireless Heat Detector with Rate of Rise

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed sensors as indicated (when finished, click **Save**).



1
DESCRIPTION
Type the sensor description you wish to appear on the keypad display

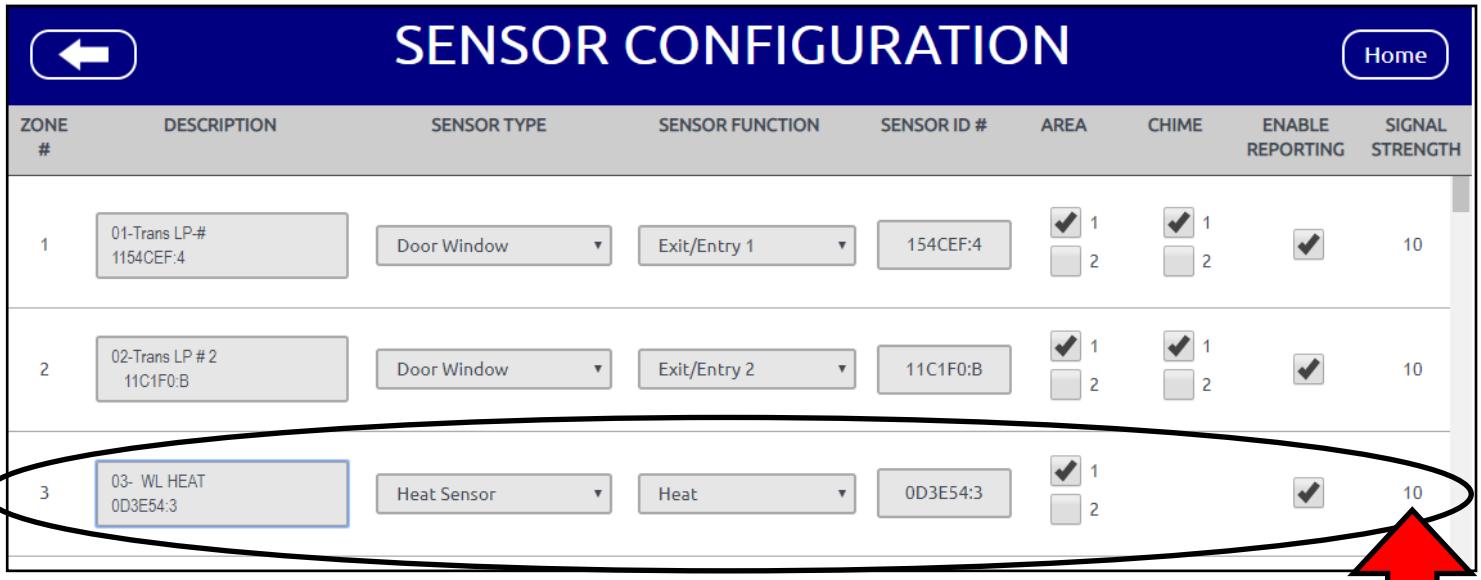
2
SENSOR TYPE
Select "**Heat Sensor**".

3
SENSOR FUNCTION
"**Heat**" is automatically selected when "**Heat Sensor**" is selected as the "**SENSOR TYPE**".

4
SENSOR ID
Type in the 7 digit sensor ID # for the device

5
AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

6
ENABLE REPORTING
Check to enable central station reporting

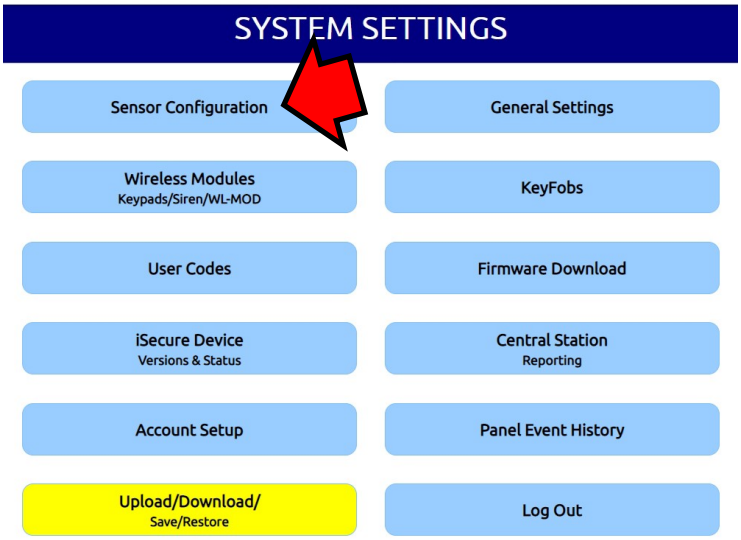


SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

Programming: Carbon Monoxide Sensors

ISEC-CARBON MON
Supervised Wireless Carbon Monoxide Sensor

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program the installed Carbon Monoxide sensors as indicated (when finished, click **Save**).



1
DESCRIPTION
Type the sensor description you wish to appear on the keypad display

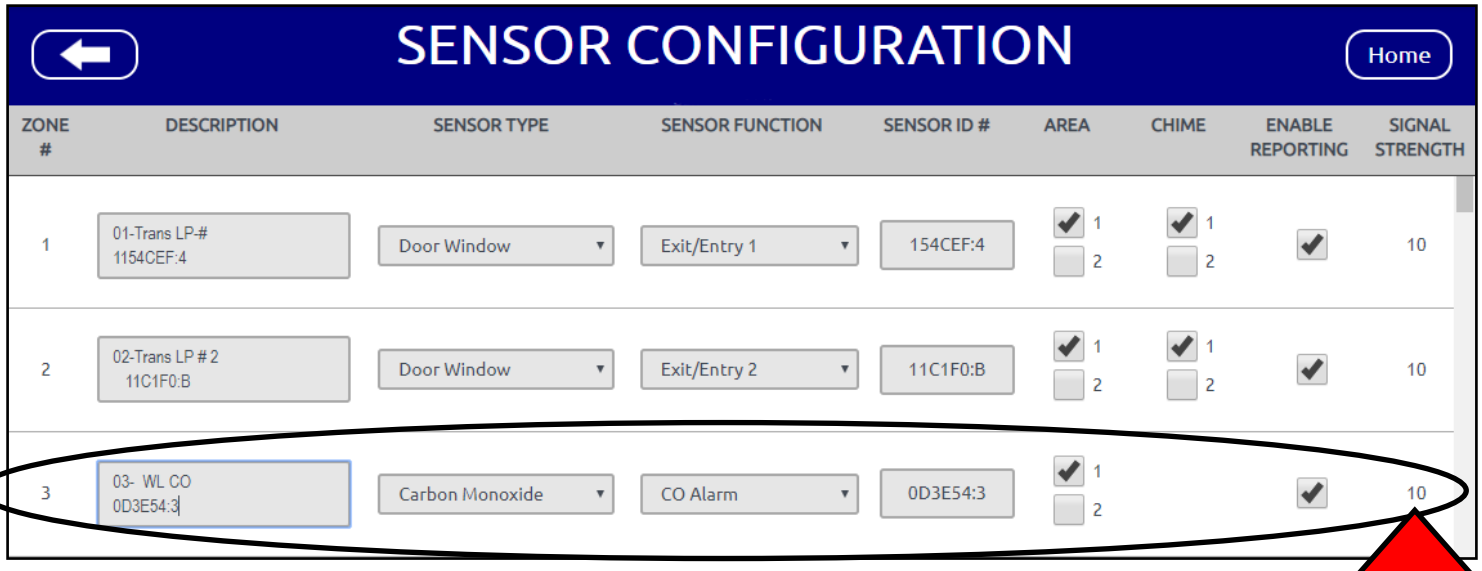
2
SENSOR TYPE
Select "**Carbon Monoxide**".

3
SENSOR FUNCTION
"**CO Alarm**" is automatically selected when "**Carbon Monoxide**" is selected as the "**SENSOR TYPE**".

4
SENSOR ID
Type in the 7 digit sensor ID # for the device

5
AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".

6
ENABLE REPORTING
Check to enable central station reporting

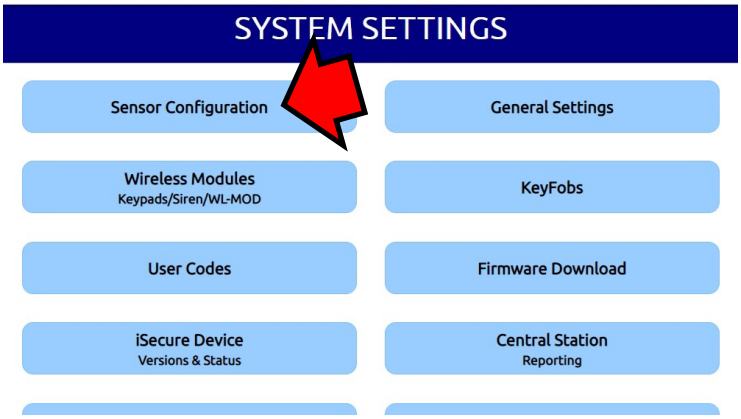


SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.

Programming: Panic Buttons

ISEC-PANIC *Single Button Waterproof Panic*

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Sensor Configuration**.
3. In the **SENSOR CONFIGURATION** screen (shown below), program each **ISEC-PANIC** as indicated (when finished, click **Save**).



3 **SENSOR FUNCTION**
Each transmitter can be designated to function in a particular manner. Select one of the following:
Instant: Allows for an immediate alarm when the panic button is pressed, providing instant protection.
24Hr Zone Audible: Provides protection at all times, whether or not the system is armed, by sounding a siren when the panic button is pressed. Reports as E150.
24Hr Zone Silent: Provides protection at all times, whether or not the system is armed. When the panic button is pressed; when armed and the panic button is pressed, a silent alarm is sent to the central station. Reports as E150.
Audible Panic: Pressing the panic button causes the siren to immediately sound and an emergency report sent to the central station. Reports as E123.
Silent Panic: Pressing the panic button causes a silent report to be sent to the central station (i.e. the user can silently signal an emergency). Reports as E122.

7 **SIGNAL STRENGTH**
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocating the Hub may be necessary.

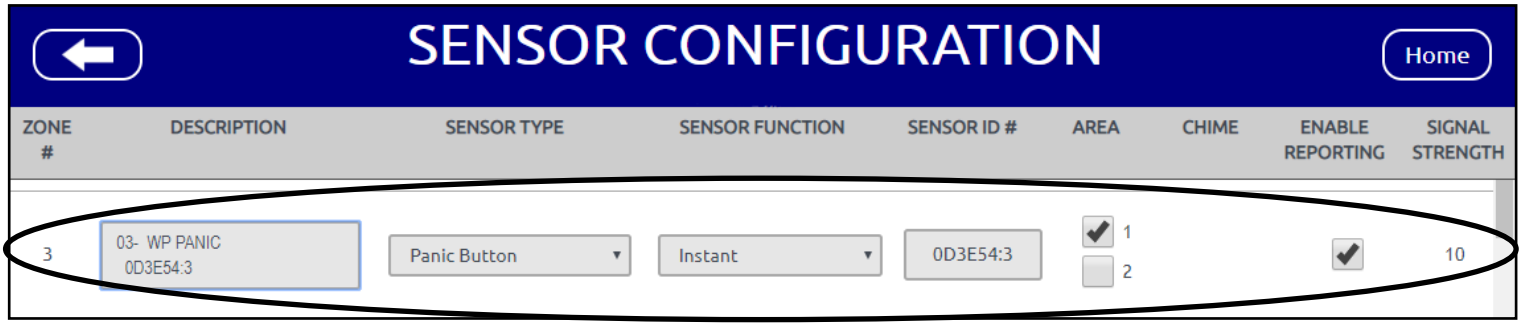
5 **AREA**
Default = 1. See the keypad Operating Guide for the definition of "Area".

1 **DESCRIPTION**
Type the sensor description you wish to appear on the keypad display

2 **SENSOR TYPE**
Select "**Panic Button**".

4 **SENSOR ID**
Type in the 7 digit sensor ID # for the device

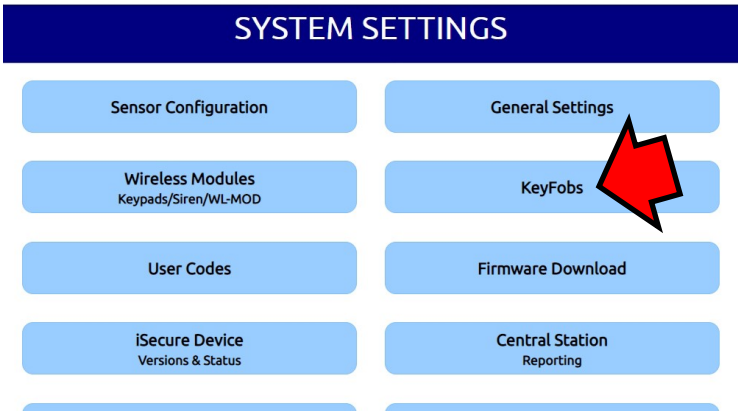
6 **ENABLE REPORTING**
Check to enable central station reporting



Programming: Keyfobs

ISEC-KEYFOB *4-Button Pendant / Keychain Transmitter*

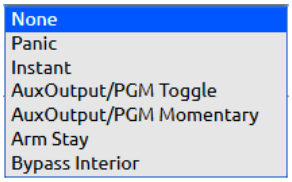
1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **KeyFobs**.
3. In the **KEYFOB SETTINGS** screen (shown below), program each **ISEC-KEYFOB** as indicated (when finished, click **Save**).



4 **KEY FUNCTIONS**

The "lock padlock" icon button is always used to arm AWAY (when you leave the premises). The "unlock padlock" button is always used to disarm the system. "**A1**" ("Key 3") and "**A2**" ("Key 4") can be set in any combination, as follows:

- **None:** Select to disable the designated key ("Key 3" and/or "Key 4").
- **Panic:** Pressing the designated key causes the siren to sound and sends a panic report to the central station.
- **Instant:** Pressing the designated key before arming allows for an immediate alarm when the system is armed, providing instant protection.
- **AuxOutput/PGM Toggle:** Press the designated button to toggle the Aux. Relay on or off.
- **AuxOutput/PGM Momentary:** Press the designated button to cycle the Aux. Relay for 4-5 seconds.
- **Arm Stay:** Press the designated button to arm "STAY" (usually at night when sleeping). Arming STAY provides partial protection by allowing free movement within the premises, while still protecting the perimeter zones (Exit/Entry doors are provided with Exit/Entry delays).
- **Bypass Interior:** Pressing the designated key before arming allows for partial protection when the system is armed by allowing free movement within the premises, while still protecting the perimeter zones (Exit/Entry doors are provided with Exit/Entry delays).



1

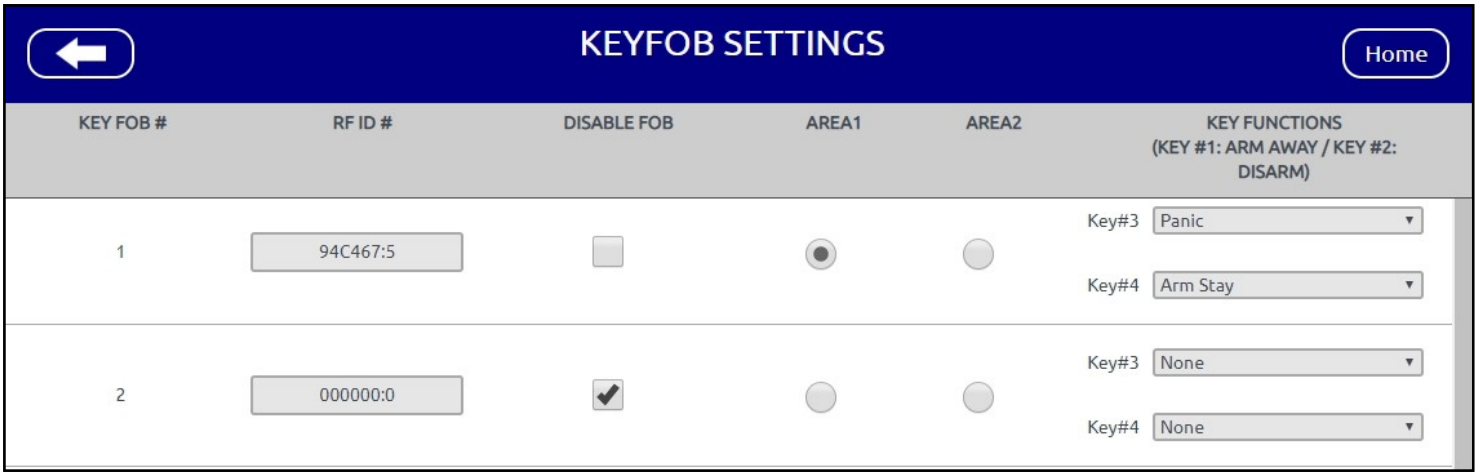
RF ID
Type in the 7 digit sensor ID # for the device

2

DISABLE FOB
Keep unchecked unless you wish to deactivate your KeyFob

3

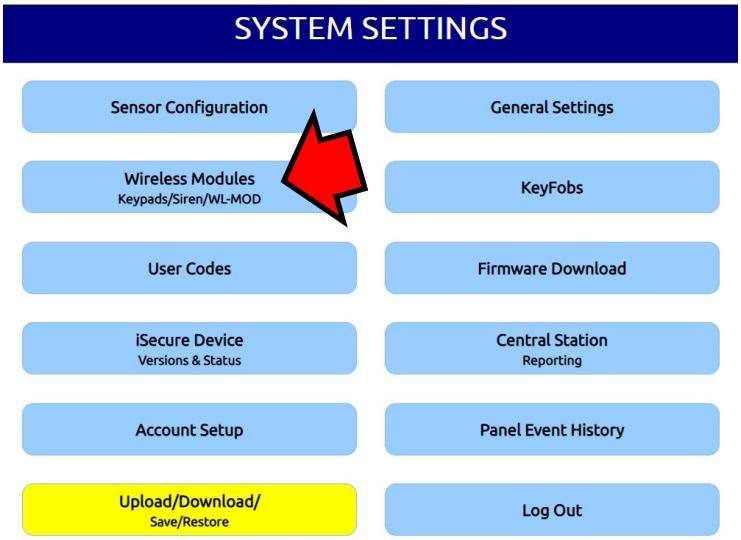
AREA
Default = 1. See the keypad Operating Guide for the definition of "Area".



Programming: Sirens

ISEC-WL-SIREN *Wireless Siren*

1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **Wireless Modules** > **Siren**.
3. In the **SIRENS** screen (shown below), program each siren in your system (up to 4 allowed) (when finished, click **Save**).



1

TYPE
Sirens can be powered by an AC power supply (plugged into a 120VAC unswitched wall outlet) or with batteries. Select the power type used by your siren.

2

NAME
Type the siren description you wish to appear on the keypad display

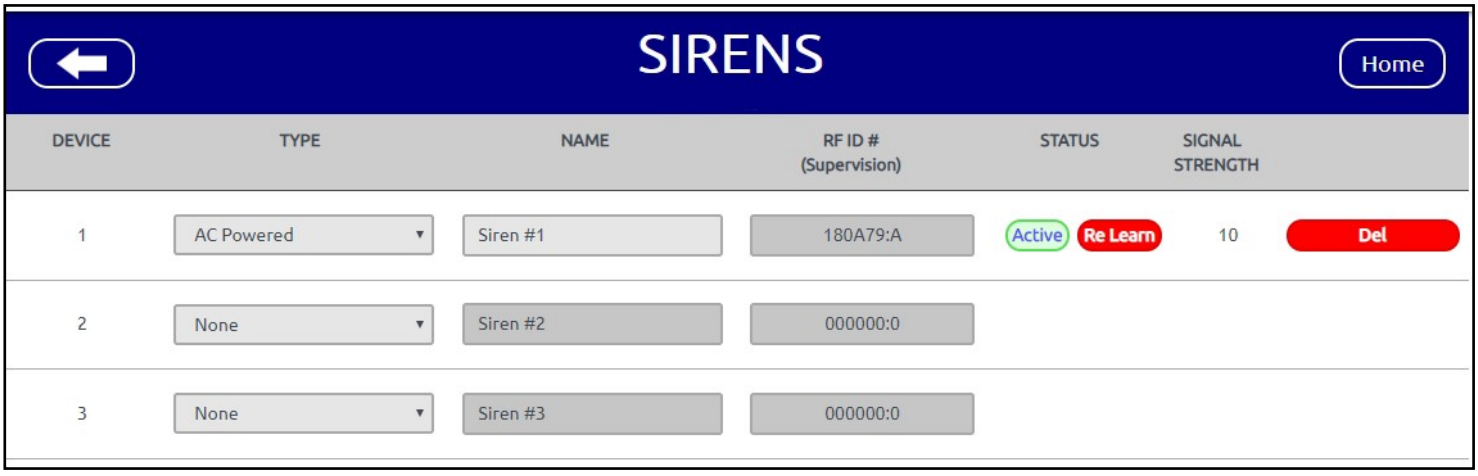
3

RF ID
Type in the 7 digit sensor ID # for the device

4

STATUS
Indicates the current condition of the siren, whether active or inactive; to relearn the unit, click **Relearn**.

SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the sensor closer to the Hub.



Programming: Takeover Modules

The **TAKEOVER** screen allows you to assign each existing wired zone to a supervised 900MHz wireless zone (up to 8 zones for each **ISEC-WL-MODULE**; up to 4 **ISEC-WL-MODULE** Takeover modules allowed for each *Go-Anywhere Smart Hub*).

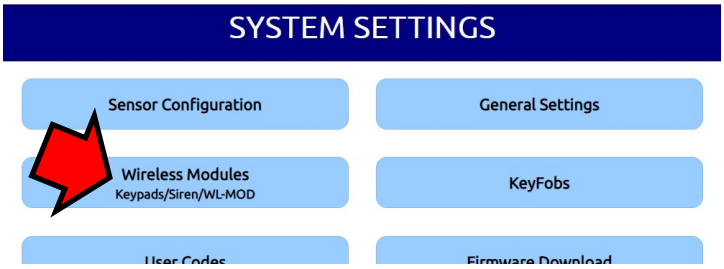
ISEC-WL-MODULE *Wireless 8-Zone Takeover Module*

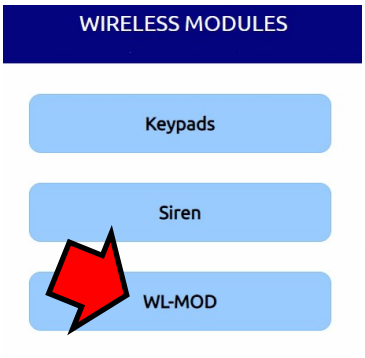
1. Go to www.iSecureByNapco.com and log into your iSecure account.

2. In the **SYSTEM SETTINGS** screen, click **Wireless Modules** > **WL-MOD** and the **TAKEOVER** screen opens (shown below).

   The **TAKEOVER** screen assigns each existing wired zone to the RF ID # of the supervised 900MHz wireless zone (up to 8 zones for each **ISEC-WL-MODULE**).

   In the **TAKEOVER** screen, shown below, for the "**Takeover Module #**" added previously, program each column, as detailed below





1

NAME
The two numbers (e.g. "1-1") refer to the number of the module (up to 4 allowed per Smart Hub) followed by the assigned wireless zone .

2

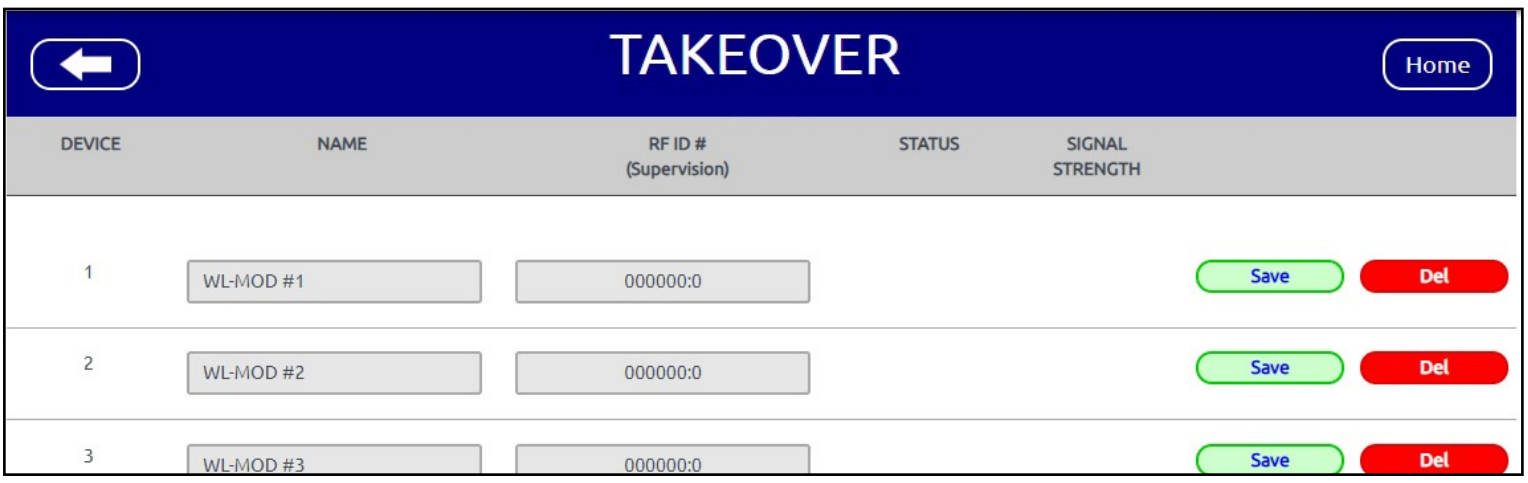
RF ID
Type in the 7 digit sensor ID # for the device

3

STATUS
Indicates the current condition of the module, whether active or inactive; to relearn the unit.

4

SIGNAL STRENGTH
Relative intensity of the last transmission, on a scale of 1-10 (10 being the strongest). **Note:** A reading of 3 or less indicates reception may be erratic; relocate the module closer to the Hub (or vice versa).

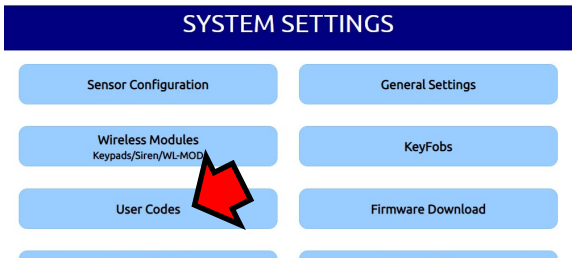


User Codes

Up to 96 personal User Codes may be added to the system using the keypad. Existing User Codes may also be erased, as well. Each User Code is assigned an Authority Level, controlling the range of tasks that Code (and therefore the User) is allowed to perform. Each User should be assigned their own unique Code and should be cautioned against divulging their Code to anyone else. Thus should it become necessary to remove a User from the system, that one User Code may be simply erased without affecting other User Codes, and that User would then be prevented from entry. **Note:** Duplicate User Codes are not allowed by the system. User Codes may contain up to six digits or as few as a two to allow for quick arming. In selecting your User Codes, do not program repetitive numbers (1111), consecutive numbers (1234), your birth date, address, or other obvious combinations.

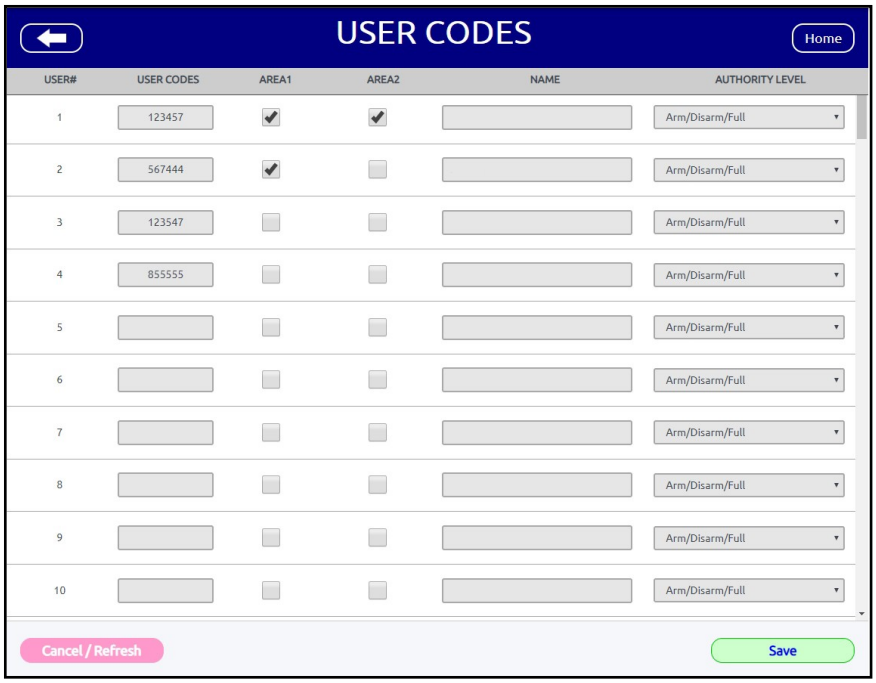
Programming / Reprogramming a User Code

Add new User Codes or erase / change / review existing User Codes, as follows:



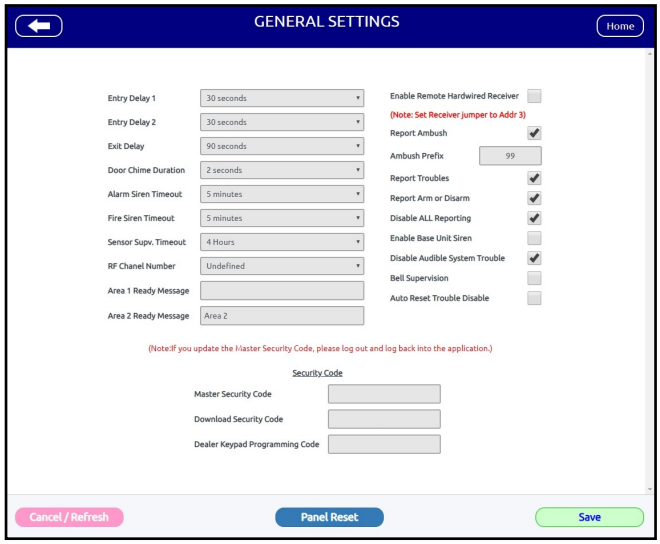
1. Go to www.iSecureByNapco.com and log into your iSecure account.
2. Click **User Codes**. The **USER CODES** screen appears.
   Note: With up to 96 User Codes allowed, each one is assigned a "**USER#**" (user number), as shown in the left column.
3. To add a new Code, click in a blank **USER CODES** field and enter the new User Code (up to 6 digits). To erase or change an existing Code, simply clear or re-enter the User Code.
4. Add a check to either or both checkboxes to select the **Area(s)** in which the User Code will be valid.
5. Click in the **NAME** field to add a descriptive name for the User Code.
6. Click the **Authority Level** pull-down to select the range of tasks the User Code (and therefore the User) is allowed to perform:
   - **Arm/Disarm/Full** - Code may be used to arm/disarm the Area(s) in which it is programmed, also allows entry into System Settings (gears icon) screens using the **ISEC-WL-TOUCH** or the **IBR-TOUCH-WL** keypads.
   - **Arm/Disarm** - Same as **Arm/Disarm/Full** without access to System Settings (gears icon).
   - **Arm-Only** - Code may only be used to arm the Area in which it is programmed; it has no disarm capability.
   - **Service/Maid** - An arm / disarm Code that is easily activated when needed, and dormant at other times. Intended for the occasional or temporary user (repairman, etc.) who would otherwise be denied access to the premises. It may then be used to arm and disarm just as any other User Code. A **Service/Maid** Code allows for arming/disarming from a disarmed state, but disallows arming / disarming from an armed state, after another non-**Service/Maid** Code has been entered.
7. When finished, tap **Save**.

Note: When using a system keypad or touchpad to enter/change/erase User Codes, the keypad **ARMED** and **STATUS** lights remain off and burglary and fire alarm functions are disabled.



GENERAL SETTINGS

Various system settings are available, including those to control system delays, timeouts, reporting and special system security codes. Each is described below.



Entry Delay 1
Entry Delay 2
Exit Delay
Separate delays that let you exit and enter your premises without setting off an alarm when the system is armed. The iSecure system has three programmable Entry Delay times available: 30, 45 and 60 seconds (default is 30 seconds). Exit Delay available times are 45, 60 and 90 seconds (default is 45 seconds).

Door Chime Duration
When Door Chime is enabled, a beep will sound while the system is disarmed to alert that the programmed zone (for example, an Entry Door) has been opened. Available times are 1, 1.5 and 2 seconds.

Alarm Siren Timeout
Fire Siren Timeout
Duration the siren will remain active (ON) unless the system is reset or silenced with a code entry.

Sensor Supv. Timeout
Specifies the length of time before a 319MHz transmitter supervisory trouble is triggered if no transmission is received from the transmitter. The default **Sensor Supv. Timeout** upon a Go-Anywhere Hub Cold Start is "Undefined", but available selections are 4 and 24 hours.

Enable Remote Hardwired Receiver
Add a check to allow the use of a GEMWV-RECV wireless receiver in the system. With 2 integral Hub receivers, this additional receiver would make a system total of 3. See the installation instructions supplied with the GEMWV-RECV (WI2316) to configure the receiver jumpers to enable the GEMWV-RECV as receiver #3.

Report Ambush
Ambush Prefix
Disarming with an Ambush Code will cause a silent report to be sent to a central station. Thus, should a user be forced to disarm, the user can silently signal an emergency while appearing to be merely disarming the system. Add a check to enable **Report Ambush**, and the Ambush Zone will automatically report. **Note:** The **Ambush Prefix** is a 2-digit code that is entered immediately prior to (and as part of) a regular valid User Code. **Important:** Do not program the first two digits of ANY User Code as the same digits entered for the "**Ambush Prefix**".

Report Troubles
Report Arm or Disarm
Disable ALL Reporting
Check **Report Troubles** to allow all system troubles to be reported to the central station. If **Report Troubles** is unchecked and **Report Arm or Disarm** is checked, only arm/disarm events will be reported to the central station. If **Disable ALL Reporting** is checked, all central station reporting will be stopped.

Enable Base Unit Siren
Check to enable (and uncheck to silence) the Go-Anywhere Smart Hub sounder and speaker (enabled by default).

Disable Audible System Trouble
Unchecked by default, add a check to silence all audible system trouble notifications at the Hub and at all keypads.

Master Security Code
This code is added to the Go-Anywhere Hub memory at the factory and is not changeable. This code is printed on a label placed on a card (OI404LF) that is included with the Go-Anywhere Hub. Entering this code at a keypad will provide access to ALL functions in the system. This code MUST be entered in this field and must match the code at the corresponding Hub. **Note:** All keypad programming must be performed at the keypad addressed as Keypad # 1. Retain the OI404LF card with the code in a secure place for reference. **Note:** Whenever you add or update the Master Security Code, you must log out and log back into the application (exiting and re-entering ensures that the iSecure Cloud Web Portal and the Master Security Code are synchronized and the system is fully protected by your secure account password).

Download Security Code
This code is not a keypad code, but is only used to permit local or remote connections to be established between the iSecure Cloud Web Portal and the Go-Anywhere Hub. Used during the connection process, if the code stored in the Hub does not match the code entered here (in the iSecure Cloud Web Portal), a data connection will be denied. Some dealers with multiple iSecure Cloud Web Portal accounts use the same Download Security Code for all accounts. When attempting to establish a connection, if this code is forgotten, the Master Security Code of the particular Go-Anywhere Hub can be used in its place.

Dealer Keypad Programming Code
This code is left blank in the Hub memory at the factory and may be added by the dealer (in possession of the **Master Security Code**). The **Dealer Keypad Programming Code** allows the same access to programming functions as the **Master Security Code**.

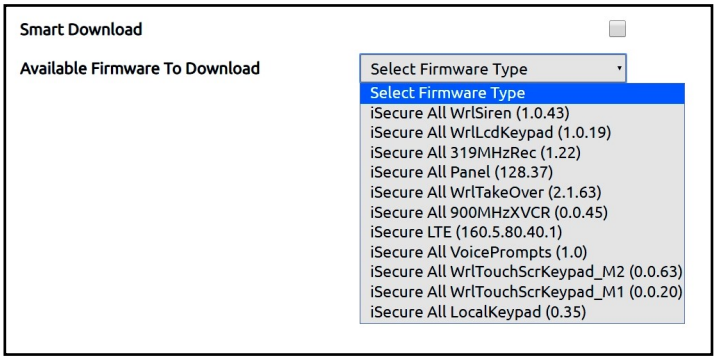
Bell Supervision
If checked, the Bell output, supervised with an EOLR, if shorted or opened the keypad will display an E51 trouble, with a report sent to the central station.

Auto Reset Trouble Disable
If this feature is checked (where "auto reset" is to be "disabled"), if the system detects a trouble and its condition is subsequently

cleared, the trouble will not reset until the **RESET** button is pressed.
If this feature is not checked, the trouble will reset automatically when the trouble condition clears.

FIRMWARE DOWNLOAD

This screen is used when you wish to manually update the Go-Anywhere Hub firmware, or keypad firmware.



Smart Download
A quick method of communications that compares the sum-checks of sections of the Go-Anywhere Hub program to determine if they are different from the account sections and only communicates data that is different, thus saving time (for LTE and Voice Prompts only). The iSecure Cloud Web Portal first compares the original account programming to the existing Hub programming. If they match, the new changes are downloaded to the Hub; if they differ, selected Hub programming areas are first uploaded into the iSecure Cloud Web Portal, then the iSecure Cloud Web Portal downloads the new changes into the Hub. If the iSecure Cloud Web Portal account is locked, the same comparison operation is performed (compares the original account programming to the existing Hub programming). If they match, the new changes are downloaded to the Hub; if they differ, the operation aborts.

Available Firmware To Download
Click this pull-down to select the Hub, keypad or device firmware you wish to update. **IMPORTANT:** Perform each update individually and wait for the update process to complete fully (do not interrupt). When updating keypads, the LCD keypad (ISEC-WL-KEYPAD) displays "**Su**" (for "System update"), and the color touchscreen keypad (ISEC-WL-TOUCH) displays "**Firmware Update In Progress**". However, during the update process, be aware that the keypad and the Cloud Web Portal screens do not always continually display the current real-time status of the process. See next section for more information.

To Update Firmware

The duration of the firmware update process varies depending on the size of the firmware file selected and the speed of the network connection.

1. Make note of both the existing and new version numbers before starting the update process (use the **ISECURE DEVICE VERSIONS & STATUS** screen).
2. Select the firmware from the pull-down and click **Start Download** and a download status popup appears. The firmware file sizes vary, therefore downloading the file to the Hub may take up to 5 minutes, depending on the speed of the network connection. **Note:** The firmware for the ISEC-WL-TOUCH Wireless Touchscreen Keypad (with "**M2**" in the file name as shown in the image above) may take up to 6 minutes or longer to complete.
3. When the download status popup closes, the update process will start. Wait a full 5 minutes. **Note:** Keypads may not always display the real-time status of the update process and may automatically reboot; do not interrupt the process.
4. The update process is complete when the keypad(s) all read, "**System Ready**", wait an additional 3 minutes before clicking the **Scan** button at the bottom of the **ISECURE DEVICE VERSIONS & STATUS** screen (see page 59). *Add another minute of waiting time for each additional device of the same type*.

Was the Firmware Update Successful?

If the **ISECURE DEVICE VERSIONS & STATUS** screen does not display the new version number that you noted in step 1, try relearning the device while monitoring the **ISECURE DEVICE VERSIONS & STATUS** screen.

When updating keypads, you can check the current firmware version numbers within the keypad itself:

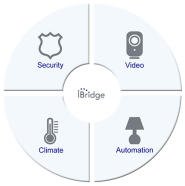
- With the ISEC-WL-KEYPAD LCD keypad, use the keypad "Local Functions" (perform the steps in the "**Keypad Attributes**" section on page 63).
- With the ISEC-WL-TOUCH color touchscreen keypad, view the "**System Diagnostics**" screen (tap the **Settings** ("gears") icon, then tap the **DIAG** button; see page 65).

If the new update is still not displayed, start again at step 2.

ACCOUNT SETUP

This screen allows you to enable certain account services and abilities. **Note:** All four services are available for selection in the "pie" (shown below) for all locally connected devices (the IBR-TOUCH-WL 7" touchpad or personal smart devices). For all remote connections, services not enabled are not selectable.

System Name
Type a descriptive name in this field that you wish to be used in text and email notification messages to help you identify the iSecure system installation.



- **Video**
- **Security**
- **Z-Wave**
- **Remote Access**

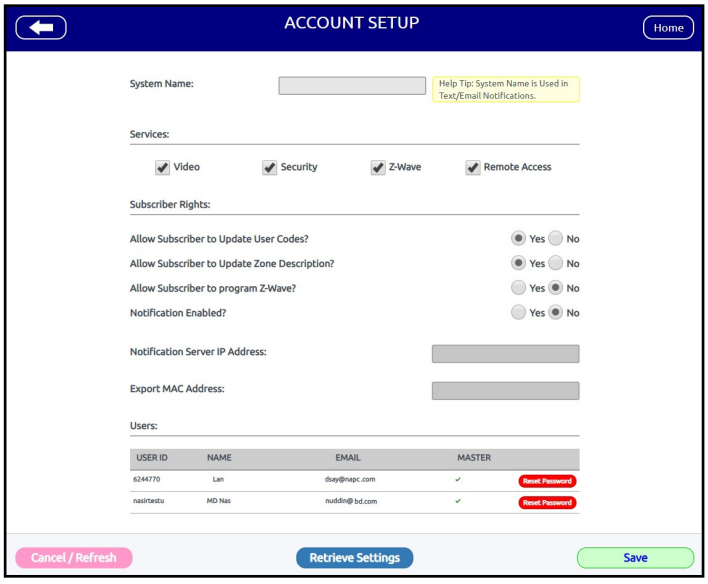
Check to enable access to each service from the Home Screen of the **IBR-TOUCH-WL** Smart 7" Wireless IoT Touchscreen. Check "**Remote Access**" to allow remote connectivity to your iSecure system using the iSecure app.

Other iSecure Cloud Web Portal Screens (cont'd)

Allow Subscriber to Update User Codes?
Click the **Yes** or **No** radio buttons to allow or disallow the homeowner (user) the ability to add/change/review User Codes using the touchscreen (in Notification Setup only).

Allow Subscriber to Update Zone Descriptions?
Click the **Yes** or **No** radio buttons to allow or disallow the homeowner (user) the ability to change Zone Description text using the touchscreen (in Notification Setup only).

Allow Subscriber to program Z-Wave?
(Appears if installed) Click the **Yes** or **No** radio buttons to allow or disallow the user the ability to add and program Z-Wave home automation devices. For more information about using Z-Wave with your iSecure system, see OI414LF, available for download at tech.napcosecurity.com



Notifications Enabled?
Click the **Yes** or **No** radio buttons to allow or disallow notification messages for this account.

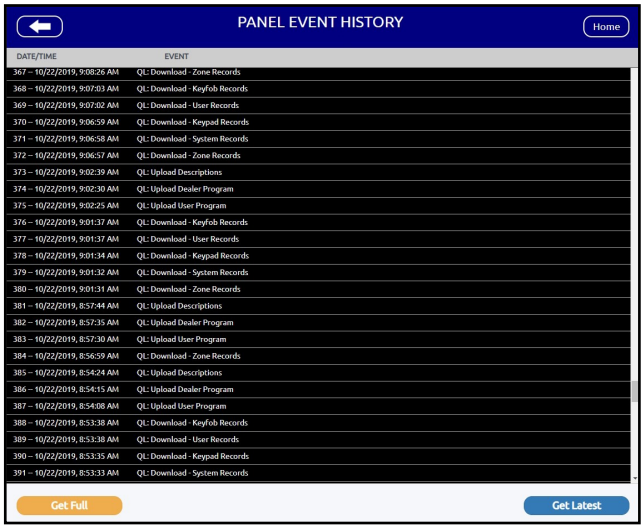
Notifications Server IP Address
Displays the IP address of the server used to send notification messages for this account.

Export MAC Address
Note: In addition to standard security passwords, some wireless routers can also be configured to allow Wi-Fi connections to only specific MAC Addresses. Displays the MAC Address of the Go-Anywhere Hub in an easy-to-copy field, should it be needed.

Users
Displays the **USER ID**, **NAME**, **EMAIL** address of those who can log into the iSecure Cloud Web Portal. **MASTER** is checked for those users authorized to make all changes to the account without restrictions. Click **Reset Password** to edit the password of the selected User.

PANEL EVENT HISTORY

Displays 800 of the most recent Hub events of all types, including alarm conditions, Fire events, and openings / closings (see example, above). Includes the event, date, time, Area, zone, User Code and other pertinent information, where necessary, depending upon event. When the number of events reaches the 800 maximum, the oldest events are overwritten.



UPLOAD / DOWNLOAD SAVE / RESTORE

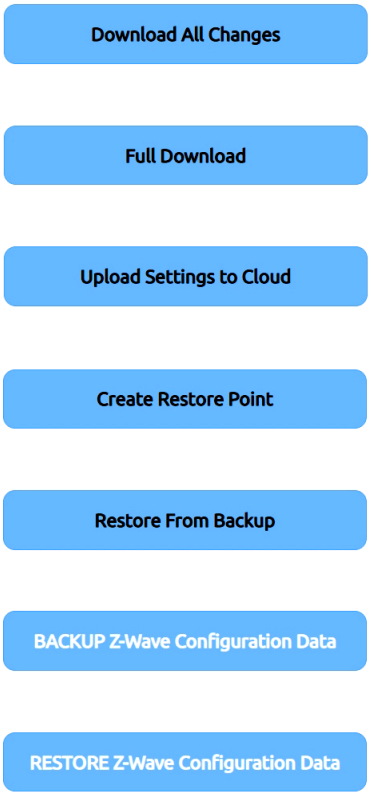
After making changes within the various iSecure Cloud Web Portal screens, click the **Upload / Download / Save / Restore** button to upload (i.e. back up) the existing Hub programming into the Cloud Web Portal, or send your changes to the Go-Anywhere Hub.

Download All Changes
Downloads all changes made in the iSecure Cloud Web Portal into the Go-Anywhere Hub.

Full Download
Performs a full download from the changes made in the iSecure Cloud Web Portal and overwrites ALL configuration data in the Go-Anywhere Hub.

Upload Settings to Cloud
Performs a full upload of all configuration data in the Go-Anywhere Hub and overwrites any existing configuration data in the iSecure Cloud Web Portal.

Create Restore Point
Creates a copy of the current iSecure Configuration data already in the iSecure Cloud Web Portal and retains it in the



Cloud Web Portal for later retrieval, if needed.

Restore From Backup
Click to restore the iSecure Cloud Web Portal to the previous configuration that will appear. To update the Go-Anywhere Hub, a full download must be performed after the restoral.

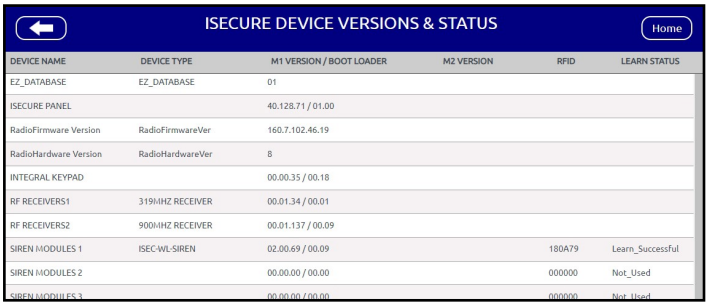
BACKUP Z-Wave Configuration Data
Click to back up all Z-Wave enrolled devices and programming into the iSecure Cloud Web Portal.

RESTORE Z-Wave Configuration Data
Click to restore all Z-Wave enrolled devices and programming into the Z-Wave device.

Last backup
Displayed under the appropriate button, this is the date and time (in 24-hour military format) the last complete and successful backup was performed for the associated configuration. The backup is sent from the Hub to the Cloud Web Portal.

ISECURE DEVICE VERSIONS & STATUS

Many different types of microprocessors and firmware are used within the iSecure system, some located within the Go -Anywhere Hub, others within each iSecure device. Some devices are required, some are optional; all are listed in this screen to display their related firmware for each. Use this screen to ensure that the firmware is the latest version (click the **Scan** button to retrieve the latest data). To manually update firmware, see the section "**FIRMWARE DOWNLOAD**" on page 57.



Entries located at the top of this screen include the various Go-Anywhere Hub hardware and firmware versions, including:

- "**EZ_DATABASE**" refers to the iSecure Cloud Web Portal database version.
- "**ISECURE PANEL**" refers to the microprocessor version within the Go-Anywhere Hub that controls most of the local alarm functions (arming/disarming, etc.).
- "**RadioFirmware Version**" refers to the microprocessor within the Go-Anywhere Hub that controls the radio communications between the Hub and the wireless device(s).
- "**RadioHardware Version**" refers to the version of the LTE Radio PC board that is plugged into the Go-Anywhere Hub motherboard. This PCB controls the LTE radio communication (reporting) functions.
- **INTEGRAL KEYPAD** (reserved for future use)
- **RF RECEIVERS1** refers to the integral Hub 319MHz receiver firmware that controls those devices, including the window/door transmitters, passive infrared motion sensors, etc.
- **RF RECEIVERS2** refers to the integral Hub 900MHz receiver firmware that controls those devices, including the keypads and other 900MHz peripherals.

Other entries include the versions and current status of the various optional iSecure devices that can be added to the system (sirens, keypads, sensors, etc.).

Device Name / Device Type
Description of each upgradable module or firmware version that exists or can exist within the iSecure system. The text names are derived from the current Hub firmware.

M1 Version / Boot Loader / M2 Version
Displays the version of the Hub firmware for microprocessor #1 and (under its own column) #2. The Boot Loader is the firmware that controls the remote download/upload processes.

RFID
Each wireless device (for example, a keypad) has a unique factory programmed ID code that distinguishes itself to the Hub. For example, "155E57:F". The first six characters of the ID code are displayed here.

Learn Status
Indicates whether the device was correctly and successfully entered into the Hub programming. **Note:** Although the device may be been correctly configured in the iSecure Cloud Web Portal and downloaded into the Go-Anywhere Hub without apparent errors, a "Learn Successful" status always requires a complete two-way synchronization and acknowledgement "handshake" between the Hub and the device. For example, a device with a "Learn Unsuccessful" status may not have been powered during the learn process, and thus is not successfully learned into the system. **Note:** Every re-learn process also refreshes the version information.
See "**FIRMWARE DOWNLOAD**" on page 57 for important information about the firmware update process.

Troubleshooting

Your iSecure system will warn you of any problems by flashing a yellow LED next to the triangle "!" (system trouble) icon located on the face of the *Go-Anywhere Smart Hub* (and with keypad indications). Here are some common warnings and recommended solutions:

"ZONES FAULTED"

At the **ISEC-WL-TOUCH** keypad, the green STATUS light must be lit in order to arm. If the green light is off, "ZONES FAULTED" will display in the window followed by the number and description of each faulted zone. Note each problem zone and secure it by closing a window, door, etc. When all zones are secure, the green STATUS light will come on and the window will display "SYSTEM READY".

" ** ALARM **** "**

If the red keypad light is flashing and **ALARM** is displayed, an alarm occurred while you were out. Proceed with caution! If you suspect that an intruder may still be on the premises, leave immediately and call authorities from a neighbor's phone. To silence an audible alarm:

1. Enter your code and press **ENTER**. After the system is disarmed, the window will continue to display **ALARM** followed by the zone(s) violated.
2. To reset the display, note the zones violated, then press **RESET**.

"E-04-NN" (Device has lost its connection)

When a wireless device loses its connection with the *Go-Anywhere Smart Hub*, an error "**E-04**" appears. The "**NN**" is a two-digit number representing the zone assigned to the wireless device (keypad, sensor, etc.). If you see this message regularly, your *Go-Anywhere Smart Hub* and wireless device may be too far apart for reliable communication. Either relocate the *Go-Anywhere Smart Hub* or the device so they are in closer proximity.

"E-05-NN" (Transmitter Low Battery)

When an RF device has a weak battery, an error "**E-05**" appears. The "**NN**" is a two-digit number representing the zone assigned to the keypad (numbers 83-88). In addition, the sounder will turn on and the triangle "!" (system trouble) icon will flash until the keypad **RESET** button is pressed (the trouble sounder will silence and the **TROUBLE** icon will turn on steady).

To change the ISEC-WL-KEYPAD battery: Open the keypad housing by inserting a flat head screwdriver into either slot at the bottom. Gently push up with a slight twisting motion to release the retainer tab (repeat for the other slot). Pull out at the bottom and lift off the two hooks at the top. Install one CR123A (3V) with optional 2nd battery, observing polarity.

"E-01" (AC Power Outage)

Inside the *Go-Anywhere Smart Hub* is a large rechargeable back up battery designed to keep the system fully powered and working normally for at least 8 hours without AC power. Press **RESET** to silence. When power is restored, this indication will clear and the system will return to normal operation. **Note:** An E93-96 trouble will be generated if the ISEC-WL-MODULE Takeover Module loses power. If the rest of your home still has power, check that the wall transformer is fully and tightly inserted into your wall outlet and check its plug connection at the *Go-Anywhere Smart Hub* socket. See "**Common Error Codes / Troubles**" on page 62 for more information.

"E-02" (*Go-Anywhere Smart Hub* Low Battery)

The large rechargeable back up battery located inside your *Go-Anywhere Smart Hub* is unable to maintain adequate charge and must be replaced. **Note:** An E93-96 trouble will be generated if the ISEC-WL-MODULE Takeover Module loses power. See "**Common Error Codes / Troubles**" on page 62 for more information.

Cold Start, Test and Reset Processes

Your iSecure Go-Anywhere Smart Hub and 900 MHz Keypads, Siren and take Over module can be reset back to their original "default" conditions, i.e. the state each was in when they first left the factory. Proceed as follows:

Cold Start the Go-Anywhere Hub (Factory Default)
The Go-Anywhere Smart Hub can be reset back to its original "default" condition, clearing all programming and settings, including all zones and keypads, and re-loading its factory default program.

1. Remove AC power from the Go-Anywhere Hub.
2. Separate the Go-Anywhere Hub front and rear housing by pushing in the two tabs at the bottom with a flat head screwdriver until the tabs unhook. Battery power is removed upon separation of the housing.
3. Add a jumper to the two (2) pins of **JP2** (located at the top left of the PC board).
4. Wait 60 seconds, or until error code **E09-00** appears on the keypad or touchpad display.
5. Remove jumper from **JP2**.
6. Reassemble the front and rear housing and re-connect AC power.
7. Perform a Full Download of the Hub programming.

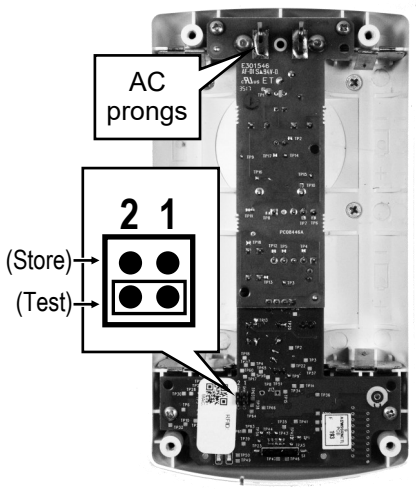
Factory Reset the ISEC-WL-SIREN

1. Remove power.
2. Place jumper on **J1**.
3. Power up siren. The siren will blink once with a strobe flash.
4. Remove jumper **J1**.
   If the default process is successful, upon power up the LED will blink three times.
   If unsuccessful, the LED will blink only once.

Test the ISEC-WL-SIREN (Strobe/Sounder Test)

Use hearing protection before testing! The siren is rated at 85dBA.

1. Remove AC and batteries.
   The jumper pins on the siren PCB are marked "**2 1**" (see image at right). With the unit oriented with the wall outlet AC prongs at the top, the factory storage position for the jumper is across the top two pins.
2. Place jumper across the two **bottom** pins as shown to begin the test process.
3. Install batteries, observing polarity.
   Upon the insertion of the 4th battery, the siren will sound and the strobe will flash.
4. Remove jumper and store in the top two pins for future use.
5. Remove batteries to silence; replace batteries and restore AC (if necessary).



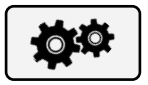
ISEC-WL-SIREN Strobe / Sounder Test Jumper Pins (jumper shown when starting test)

Factory Reset the ISEC-WL-MODULE *Takeover Module*

1. Remove power.
2. Place jumper on **J1**.
3. Power up the module.
4. Wait 10 seconds and remove jumper from **J1**.
   If the default process is successful, upon power up the LED will slowly blink.

Factory Reset the ISEC-WL-KEYPAD *Wireless Battery-Powered Standard Keypad*

1. Press and hold the **AREA** (✱) button until "**LF**" appears in the display.
2. Press **0**, **2**, **ENTER**.
   If the default process is successful, the "dot" in the left bottom corner of the display and the word **READY** will appear. If unsuccessful, only the "dot" in the left bottom corner of the display will appear. **Note:** This reset procedure can only be initiated either within 1 minute after power up, or when the keypad flashes "o#" (where # is the keypad address).



System Settings ("gears") icon

Factory Reset the ISEC-WL-TOUCH *Wireless 4.3" Full Color Security Touchscreen Keypad*

1. From the Home screen, press the **System Settings** ("gears") icon (shown at right).
2. Enter the Master Security Code (refer to the OI404LF card), then press **ENTER**.
3. In the **System Settings** screen that opens, press the **Dealer KP Config** button.
4. Press the **LearnOff** button. The **LearnStatus** will change from **ON** to **OFF**.
5. Press **Exit** twice to save and exit.
   Note: To verify the **LearnStatus**, re-enter the **System Settings** screen and press the **Dealer KP Config** button.

Common Error Codes / Troubles

E01 AC -- Power Failure
This trouble will occur if AC power is not present. Make sure system transformer is plugged into AC receptacle and check the circuit breaker, otherwise call installing company for service.
E01-89, E01-90, E01-91 and E01-92: AC loss for the ISEC-WL-SIREN (#1 through #4)
E01-93, E01-94, E01-95 and E01-96: AC loss for ISEC-WL-MODULE Takeover modules (#1 through #4).

E02 -- Low Battery
If there has been a recent power failure, the battery may be partially depleted and must be recharged by the Go-Anywhere Smart Hub. The Go-Anywhere Smart Hub performs an automatic test of the battery every 24 hours, at which time the trouble will clear if the battery has been recharged. If the trouble does not go away in 24 hours, call installing company for service.

E03 -- Communication Failure
The system was not able to report to the central station. If this is due to a temporary interruption in the radio or Internet (or both) service, the trouble can be cleared when the service is restored by performing a Communication Test:
1. While disarmed, enter your User Code followed by ENTER.
2. Answer NO until "15" (Telephone Test) appears in the window.
3. Press YES to send a test signal to the central station.
4. If the trouble continues, call installing company for service.

E04-NN -- Wireless Transmitter Supervisory Failure
A problem has been detected with a wireless transmitter. Call installing company for service.

E04-(83-88) -- Wireless Keypad Trouble Supervisory
A problem has been detected with a wireless keypad. Call installing company for service.

E04-(89-92) -- Wireless Siren Trouble Supervisory
A problem has been detected with a wireless siren. Call installing company for service.

E04-(93-96) -- Wireless Takeover Module Trouble Supervisory
A problem has been detected with a takeover module. Call installing company for service.

E05-(83-88) -- Wireless Keypad Trouble Low Battery
E05-(89-92) -- Wireless Siren Trouble Low Battery
E05-(93-96) -- Wireless Takeover Module Trouble Low Battery
The battery in a wireless device is low and should be replaced. The replacement battery for the **ISEC-WL-KEYPAD** is CR123A (use one for standard battery life, use two for extended battery life). The siren requires 4 alkaline C-size batteries. If a low battery is indicated for a takeover module, check the battery or power supply that is providing power to the module. Warning: Replace batteries only with the same type as specified above. Use of other types may present a risk of fire or explosion. Never recharge or disassemble a battery, or dispose of in fire.

E06-NN -- Receiver Response Failure
Call installing company for service.

E09-00 -- System Cold Start
For installer use only. (This indication always appears when a system "Cold Start" is performed. "Cold Starting" the Go-Anywhere Smart Hub resets it back to its original "default" condition, i.e. the state it was in when it left the factory).

E10-NNN -- Keypad Response Failure
Call installing company for service.

E11-NNN -- Keypad Tamper
The Go-Anywhere Smart Hub has been opened, or a wall-mounted keypad has been opened and/or removed from the wall. Call installing company for service if problem cannot be repaired.

E15-NNN -- RF Transmitter Tamper
Wireless transmitter cover removed (NN = transmitter number). Call installing company for service.

E16-NNN -- Wireless Receiver Jam
A problem has been detected with the wireless receiver. Call installing company for service.

E17-NNN -- Receiver Tamper Condition
Call installing company for service.

E18-NNN -- Keyfob Transmitter Low Battery
A keyfob transmitter has indicated its power cell(s) are weak and should be replaced. The 4-button ISEC-KEYFOB uses a 3V Lithium coin cell battery (replace with type CR2032 or Duracell DL2032 only). The 1-button ISEC-PANIC uses two Energizer 386 1.5V silver oxide cells (the unit will also flash its LED to warn of a low-battery). **Warning:** Replace batteries only with the same type as specified above. Use of another battery may present a risk of fire or explosion. Do not recharge or disassemble battery, or dispose of in fire.

E40-NNN -- RF Self-Test Failure
A wireless motion sensor on the zone indicated has failed its automatic self-test routine. Call installing company for service.

E41-NNN -- Fire Trouble
A problem has been detected on the fire zone indicated. Call installing company for service.

E42-NNN -- CO Zone trouble
A problem has been detected on the carbon monoxide zone indicated. Call installing company for service.

E51 -- Bell/Siren Trouble
There is a problem with the bell or siren. Call installing company for service.

E59-03 -- Ethernet failed to communicate
Call installing company for service.

E59-04 -- Ethernet poll/check-in failure
Call installing company for service.

E59-07 -- Wi-Fi failed to communicate
Call installing company for service.

E59-08 -- Wi-Fi poll/check-in fail
Call installing company for service.

E60-03 -- Radio failed to communicate
Call installing company for service.

E60-05 -- Radio Poll or Check in failure (RF only)
Call installing company for service.

ISEC-WL-KEYPAD "Local Functions"

The **ISEC-WL-KEYPAD** includes internal keypad "local functions" that display certain keypad attributes as well as allow for the adjustment of some internal settings.

Keypad Attributes

This function displays certain keypad attributes that may be helpful when installing and configuring the system.

1. Press and hold the keypad **AREA** (✱) button until "**LF**" appears in the Window.
2. Press the keypad **AREA** button once (✱), then press **ENTER**.

Data appears in the following order:

- **Keypad Address** - Displays the address assigned by the iSecure Cloud Web Portal when the keypad was added into the system. Up to 6 keypads may be installed in each iSecure system, and each must be assigned a unique Keypad Address number (that is, no two keypads may be numbered alike). Keypads must be numbered consecutively (missing numbers are permitted after keypad delete). Keypads are added to the iSecure Cloud Web Portal in the **KEYPADS** screen starting at Address number 3, and with up to 6 keypads allowed per system, the Keypad Address numbers therefore run from 3 through 8. **Note:** If the keypad is "out of system" (no wireless connection to the Hub), the Keypad Address will appear after a lowercase "o" (to signify "out of system").
- **Keypad Firmware Version** - The full version number is displayed in the iSecure Cloud Web Portal **ISECURE DEVICE VERSIONS & STATUS** screen, but the keypad displays only partial version numbers after the letters "**rE**", and in several segments. For example, if the full version number is "00.02.38 / 00.09", the (partial) version will appear in the keypad window as "**rE**, **02**, **d**, **38**" (the letter "**d**" signifies "dot").
- **Keypad Battery Voltage Level** - The keypad requires one 3V battery. A second 3V battery can be installed and is used only to extend the time between battery replacements, not to increase the voltage. The total battery level is always displayed in two digits with a decimal in-between. For example, if the level is 3.0 volts, "30" is displayed; if the level is 2.9 volts, "29" is displayed.
- **Keypad "Learn" Status** - Indicates whether the keypad is or is not currently paired with a Hub. Displayed after the letters "**Lr**" as either "**00**" (currently not paired) or "01" (currently paired).
- **Radio Frequency (RF) Channel** - Displayed after the letters "**CH**", the RF Channel is a number between **0** and **32**, and is assigned by the iSecure Cloud Web Portal or randomly by the Hub when the keypad was paired (zero assigned when the keypad is not yet paired).

Walk Test Mode

Use this function to verify that sufficient wireless signal strength exists between the keypad and the Go-Anywhere Hub, and is useful when selecting suitable (or optimal) keypad mounting and Hub installation locations. Increase the distance between the Hub and the keypad and the radio signal will grow weaker with a corresponding slowing of data rates and throughput. The keypad must be learned into the Hub for this test mode to function.

1. Press and hold the keypad **AREA** (✱) button until "**LF**" appears in the Window.
2. Press **4** and "**F4**" appears in the Window, then press **ENTER**.

ISEC-WL-KEYPAD
Wireless Battery-Operated Standard Keypad

When the test is initiated, data is transferred back and forth between the keypad and Hub. When finished, the signal levels of both the keypad and Hub are displayed and a beep is heard in the sequence listed below.

The descriptions below use the following characters as an example result:

"**LL**, **10**, **36**, **PL**, **10**, **45**, (**beep**)".

- **LL** - The numbers that follow correspond to the RF signal strength received by the (LCD) keypad sent from the Hub. **Note: LL** = "**L**CD **L**evel".
- **10** - Signal strength received by the keypad expressed on a scale from 1 (weaker) through 10 (stronger).
- **36** - Signal strength received by the keypad expressed in dBm units (signal level relative to 1 milliwatt), provided for those more familiar with signal readings expressed using standard radio communication terminology. Normally, dBm units are expressed in negative numbers, but this keypad omits the minus ("-") sign and only displays the two right digits. Therefore, with this keypad only, a "lower" number reflects a stronger signal. For example, a reading of "30" is stronger ("better") than "55". If the reading is -102dBm, the keypad will display the two right digits ("02"). If the reading is -99dBm, "99" will be displayed. Numbers in dBm scale are from -30dbm to -105dbm, with -30dbm as the strongest reading.
- **HL** - The numbers that follow correspond to the RF signal strength received by the Hub. **Note: HL** = **H**ub **L**evel.
- **10** - Signal strength received by the Hub expressed on a scale from 1 (weaker) through 10 (stronger).
- **45** - Signal strength received by the Hub expressed in dBm units (see "36", above).
- Beep - If the current data transfer was successful, the beep will sound. The beep failing to sound indicates a loss in the keypad/Hub wireless connection; thus the readings subsequently displayed without a beep will reflect the readings from the last time the keypad/Hub had a wireless connection.

After the beep, the test will repeat. If the subsequent test completes successfully, the keypad Window will display updated numbers. This test mode will keep repeating until **RESET** is pressed or until the mode automatically times out after four minutes.

Display Keypad RF Attributes

This feature displays the radio frequency (RF) characteristics of the keypad, for reference. **Note:** The keypad must be learned into the Hub for this test mode to function.

1. Press and hold the keypad **AREA** (✱) button until "**LF**" appears in the Window.
2. Press "**0**" and all keypad icons will briefly turn on at the same time (this is a test of the Window display).
3. Press **ENTER**.

All signal strength readings in this function are expressed in dBm units (signal level relative to 1 milliwatt), provided for those more familiar with signal readings expressed using standard radio communication terminology. Normally, dBm units are expressed in negative numbers, but this keypad omits the minus ("–") sign and only displays the two right digits. Therefore, with this keypad only, a "lower" number reflects a stronger signal. For example, a reading of "30" is stronger ("better") than "55". If the reading is -102dBm, the keypad will display the two right digits ("02"). If the reading is -99dBm, "99" will be displayed. Numbers in dBm scale are from -30dbm to -105dbm, with -30dbm as the strongest reading. **Note:** Unless otherwise noted, all readings displayed in this function reflect the latest sample readings that were automatically retrieved by the keypad every 15 minutes.

The signal strength readings always follow two letters, as follows:

- **FL** - The numbers that follow correspond to the weakest RF signal received by the (LCD) keypad from any device in the system (**FL** = "Floor Level").
- **LL** - Same as the "**LL**" description in the previous function, "**Walk Test Mode**", described earlier in this section.
- **OL** - In one of several efforts to save keypad battery power, the sensitivity level of the keypad is adjusted as needed, depending upon calculations based upon the "**LL**" signal (above), and is displayed here for reference. Depending on the "**LL**" signal level, if the keypad is adjudged to be in "close" proximity to its connected Hub and also to another, separate iSecure system, the keypad sensitivity threshold is adjusted to save battery power, and to also prevent the other, separate iSecure system from needlessly waking up the keypad when in an idle state.
- **HL** - Same as the "**HL**" description in the previous function, "**Walk Test Mode**", described earlier in this section.
- **LP** - Similar to "**OL**", above, this reading exists as a result of another effort to save keypad battery power. The transmission level of the keypad is adjusted as needed, depending upon calculations based upon the "**HL**" signal (above), and is displayed here for reference.
- **Operating Frequency** - Displays the radio operating frequency of the iSecure system, in MHz. For example, a frequency of 928.75MHz is displayed as "**Fr**, **92**, **87**, **50**".

Reset Microcontroller

Performing this feature is equivalent to removing the keypad battery power and then restoring battery power. All keypad settings are retained.

1. Press and hold the keypad **AREA** (✱) button until "**LF**" appears in the Window.
2. Press **RESET**, then press **ENTER**.

Keypad Window Backlight

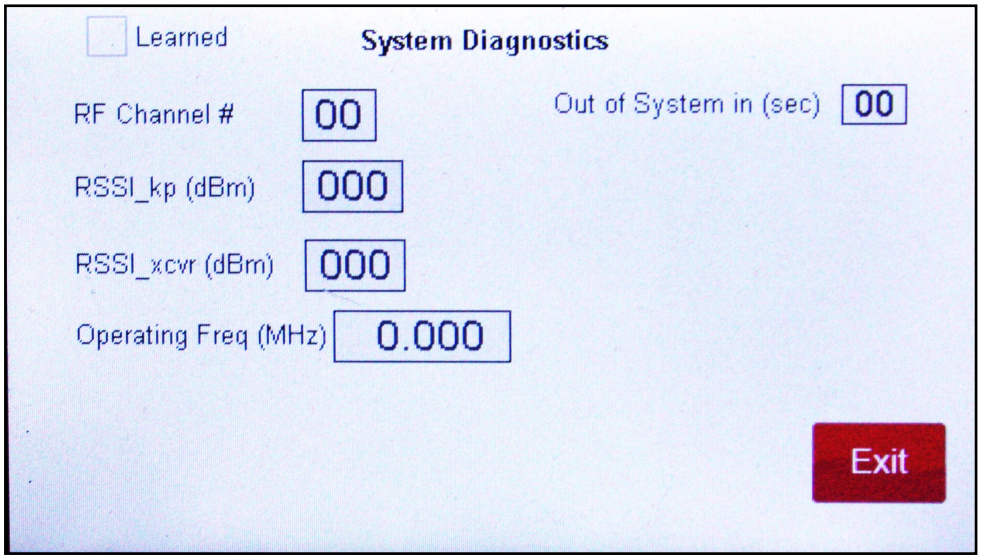
The keypad face contains a Room Light Sensor that automatically measures the ambient light level to determine if the keypad Window backlight needs to be turned on for a few seconds after a keypad button press. A lit backlight ensures the Window contents are displayed clearly in a dark room. In a bright room, the backlight is not needed and thus remains off to save battery power.

This Room Light Sensor threshold can be adjusted as well as enabled/disabled, as described in the *Operating Guide for the ISEC-WL-KEYPAD Wireless Battery-Powered Keypad* (OI400), in the section "**KEYPAD WINDOW BACKLIGHT**".

ISEC-WL-TOUCH "System Diagnostics"

The **ISEC-WL-TOUCH** "**System Diagnostics**" screen shown below is exclusive to the **ISEC-WL-TOUCH** 4.3-inch 900MHz Color Touchscreen Wireless Keypad. It is designed to help you find the optimum mounting location for your **ISEC-WL-TOUCH** keypad by displaying the signal strength of the 900MHz radio signal link between the Go-Anywhere Hub and the **ISEC-WL-TOUCH** keypad within the installation environment. This screen is accessed by tapping the **Settings** ("gears") icon, then tapping the **DIAG** button.

ISEC-WL-TOUCH
Wireless 900MHz Touchscreen



Each button and field in this screen is described below:

Learned
Checked when the status of the ISEC-WL-TOUCH keypad is paired into the iSecure system; otherwise unchecked.

RF Channel #
Displays the frequency of the channel used for communications between the Go-Anywhere Hub and the ISEC-WL-TOUCH keypad.

RSSI_kp (dBm)
RSSI (*Received Signal Strength Indicator*) is a measurement of the power present in a received radio signal. This field displays the 900MHz radio signal that the ISEC-WL-TOUCH keypad received from the Go-Anywhere Hub.

RSSI_xcvr (dBm)
The RSSI value that the Go-Anywhere Hub received from this ISEC-WL-TOUCH Keypad.

Operating Freq (MHz)
Displays the wavelength, in megahertz, of the radio frequency used in communications between the Go-Anywhere Hub and the ISEC-WL-TOUCH keypad.

Out of System in (sec)
Displays the number of seconds the communication link between the Hub and the ISEC-WL-TOUCH keypad was interrupted. If Out of System, this field will count down.

Keypad Dealer Function Menu

The keypad can provide a wide assortment of utility functions as summarized in the Function Menu. The functions are displayed in a prompting "YES/NO" format. The complete Function Menu list is provided here in its normal displayed sequence. However, since not all functions are designed for all systems (or intended for all users), only functions that are applicable and active are displayed (e.g. if no zones are bypassed, "DISPLAY ZN BYPASSED" will not appear). Furthermore, functions that are intended for use by the installer or servicer will not be displayed unless a valid Dealer Code is entered.

To return to normal keypad operation, press **RESET** (the keypad will automatically return to its normal operating mode if no activity is detected for longer than one minute). Note: Consult the keypad User Guide to determine which buttons allow for scrolling through the selections. For the **IBR-TOUCH-WL** *Smart 7" Wireless IoT Touchscreen*, see OI413. For the **ISEC-WL-TOUCH** *Wireless 4.3" Full Color Security Touchscreen Keypad*, see OI401. For the **ISEC-WL-KEYPAD** *Wireless Battery-Powered Standard Keypad*, see OI400.

DISPLAY ZN FAULTS

Displays all unsecured zones within the keypad's Area while disarmed. Zones may be bypassed in this mode by pressing **BYPASS**; manually bypassed zones will be indicated when displaying status.

DISPLAY ZN BYPASSED

Displays zones that have been deactivated ("bypassed").

DISPLAY ZN DIRECTORY

Displays a list of all programmed zone descriptions in the selected Area. To return to normal system operation, press **RESET** at any time.

ACTIVATE BELL (SIREN) TEST

Activates the alarm sounder (while disarmed) for about 2 seconds and performs a battery test. If the alarm does not sound, it may be defective. If the battery is low, "E02-00" will appear in the display indicating a low battery condition. Allow 24 hours for the battery to recharge.

DISPLAY SYS TRBL

Displays all system error codes/troubles (LOW BATTERY, AC POWER LOSS, etc.). Wait for the display to scroll through multiple system troubles.

DISPLAY FIRE ALARM (AFTER PERMISSION TO RE-ENTER THE PREMISES BY EMERGENCY RESPONDERS)

Displays Fire Zone(s) in alarm. Correct the cause of the alarm condition, then press **RESET** to restore the "SYSTEM READY" condition.

DISPLAY FIRE TRBL

Displays Fire Zone(s) in trouble. Correct the problem, then press **RESET** to restore the "SYSTEM READY" condition.

ACTIVATE CHIME

Sounds a tone at the keypad when the selected zone is violated (faulted) while disarmed. The duration of the tone is programmable. To turn off the Chime Mode, re-enter this Function Menu and select DEACTIVATE CHIME.

RESET SMOKE

If the unit is in alarm due to a smoke condition, it will stop sounding when the smoke condition has cleared. Press **RESET** to reset the system after a smoke alarm; "SYSTEM READY" will be displayed.

RESET SYSTEM TRBL

System troubles normally latch and display and sound at the keypad. Pressing **RESET** will silence the sounder and "**SYSTEM READY**" will be displayed. Correcting the trouble will clear most system trouble indications, however a keypad tamper system trouble requires a Level-2 or -3 code for manual reset (enter code and access **RESET SYS TRBL**).

Note: (1) If a system trouble is not corrected, it will re-display after 5 minutes. (2) If one or more of the above listed system troubles appear during the first 5 minutes after power-up, they will be cleared automatically.

FAULT FIND

This troubleshooting aid helps you locate "swingers" (a swinger is a fault on a communicator zone usually attributed to a malfunctioning device or relay that ultimately causes a large number of the same signals to be transmitted to the central station; i.e. a nuisance alarm).

When this menu selection is accessed, two things occur:

- The loop response of each zone is set for the fastest response time.

- Causing or repairing a fault activates the sounder for about 7 seconds.

Tapping and poking at suspect points, the installer can easily locate swingers by listening for the beep. This eliminates the need of returning to the keypad to visually check after each attempt. Press **RESET** to restore normal operation (arming the system automatically cancels the Fault Find mode). **Note:** When testing wireless systems, the keypad will not beep if the signal strength is less than 3, but the strength will still be displayed.

ACTIVATE LOCATE

Helps you find zone troubles and indicates when they are repaired. When this feature is accessed, the sounder will turn on and the keypad display will read "LOCATE", then scroll through the zones in trouble. As each zone is corrected, the sounder will stop momentarily, signaling its repair, and the display will indicate the remaining zones in trouble. The sounder and display will continue in this manner until all zones are repaired, or until **RESET** is pressed. **Note:** This feature will only operate with Zone Expansion Module(s); see the documentation for model GEM-EZM8 (eight point expansion module) in the Technical Library at https://tech.napcosecurity.com/.

DISPLAY ALARM LOG

Displays most recent alarm events. Includes the event, date, time, Area and zone.

DISPLAY TOTAL LOG

Displays most recent events of all types. Includes the event, date, time and, if applicable, Area and zone or user.

DISPLAY SYSTEM LOG

Displays most recent system events. Includes the event, date, time and other pertinent information, where necessary, depending upon the event.

TO ARM IN 1-4 HRS.

Use this function to (a) delay programmed auto-arming up to 4 hours, 15 minutes or (b) initiate auto-arming in 4 hours, 15 minutes.

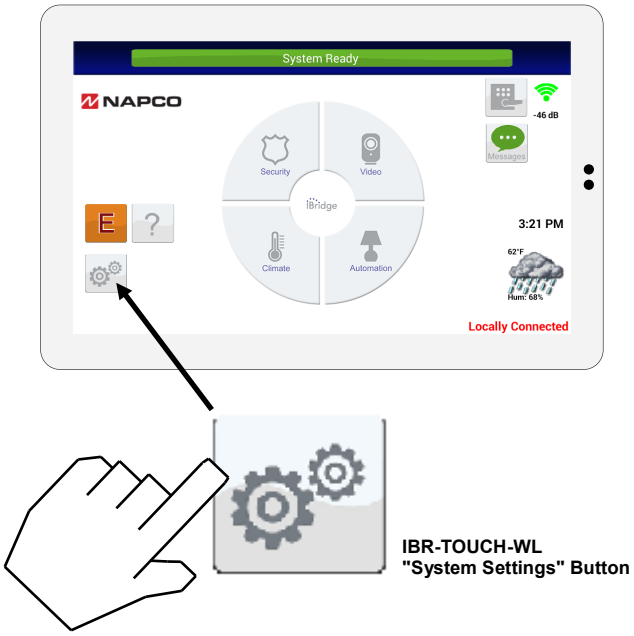
Fifteen minutes prior to arming, the siren will sound a 2-second warning and the keypad will begin a 15-minute countdown with the sounder pulsing (the sounder may be silenced by pressing **RESET**, but it will turn back on one minute before arming). Within this countdown window, arming may be delayed an additional 1 to 4 hours, as above, or auto-arming may be canceled by arming and disarming the Go-Anywhere Hub.

DISPLAY RF XMITTER STAT

Checks the status of up to 60 transmitters. The keypad will display:

- zone number (Z01-Z96)
- transmitter ID code number (6 digits)
- point number (PT1-PT4; "9" for unsupervised)
- status of transmitter:
  NODATA: Transmission not yet received
  NORMAL: Transmitter's zone normal;
  FAULT: Transmitter's zone open;
  LOBATT: Transmitter battery low;
  TAMPER: Transmitter case open;
  S.FAIL: Supervisory failure (test transmission not received within programmed time);
- relative signal strength of the last transmission, on a scale of 1-10 (10 being the strongest). ("**SS—**" indicates transmission not yet received). **Note:** A signal strength of 3 or less is an indication that reception may be unreliable. In such cases, the use of an additional receiver located closer to the transmitter is recommended. If two receivers are connected to the Go-Anywhere Hub, only the higher signal strength of the two will be displayed.

IBR-TOUCH-WL Dealer Settings Menu



IBR-TOUCH-WL "System Settings" Button

This "System Settings" button can display either a list of "user-only" selections (adapted for home/business owners), or a list of "dealer-only" selections (customized for installers), depending on the *how* this button is tapped and pressed:

- **Dealer Settings**: To display the list of "dealer-only" selections, *press and hold* this button (password required)
- **User Settings**: To display the list of "user-only" selections, simply tap this button once (see OI413)

When accessing the **Dealer Settings**, (again, by pressing and holding this button), a popup appears requesting a password. This password request signifies that the **Dealer Settings** menu will be displayed. Type the dealer password (default is "**admin**") and tap **OK**. Tap **Yes** to the warning popup that appears, and the **Dealer Settings** menu opens.

For Z-Wave menu selections, see the **Using your iBridge App to Program your Z-Wave Home Automation System** (OI414).

DEALER SETTINGS

Setup Wizard

Tap to re-start the Setup Wizard to configure how the IBR-TOUCH-WL will be used, its Wi-Fi connection settings to the customer's Wi-Fi network and iBridge radio, and optionally the NAPCO StarLink account(s). See page 13 for step-by-step instructions to help guide you through the Wizard.

Run Diagnostics

Tap to run a system diagnostics test for components selected the last time the **Setup Wizard** was run (typically when the touchscreen was first powered). Functional components are marked with a check; items not configured or not enabled are marked with an "x". Selections are blank when the Wizard is run for the first time. If you wish to continue through the **Setup Wizard** (described below), tap **Configure**; otherwise tap **Continue to App** to return to the Home Screen (or **Test Again** to repeat the test). See page 13 for step-by-step instructions to help guide you through the Wizard.

Security

EZ-ARM: Check to enable Easy Arming (ability to arm the alarm system quickly by simply tapping **ENTER** or **ON/OFF**, **Night**, **Away** or **Stay**). Each touchscreen may be individually programmed for Easy Arming. Disarming still requires entry of a valid user code. **Note:** The Hub must be programmed to support this feature.

EASY EXIT: Check to enable Easy Exit. While armed in the Interior Bypass/Stay Mode, Easy Exit can be initiated by pressing and holding the **Disarm** "pie wedge" button. Easy Exit restarts the Exit delay (the top banner on the touchscreen changes to read "**ARMING STAY**...") allowing a User to exit an armed premises without disarming and rearming the system. **Note:** The Hub must be programmed to support this feature.

Number of Zone Areas: Some systems may be divided, or partitioned, into smaller independent subsystems, which are referred to as Areas. Tap to select the number of Areas in the alarm system. **Note:** Each Area may be controlled by its own touchscreen or by a touchscreen of a different Area through Managers Mode (a low-security operating mode that allows arming by Area).

Connection Settings: Displays the network communication and automatic identification settings used between the IBR-TOUCH-WL and the customer's router.

Serial Interface: Reserved for future use.

IP Address: Displays the private TCP/IP protocol address used for communications between the IBR-TOUCH-WL and the customer's router.

Port No.: Displays the port number used for network activities.

Autodiscovery Options: "Enabled" allows for the ongoing automatic recognition of and connection between the IBR-TOUCH-WL and customer's router. Includes discovery and ports established during the initial handshake process.

IBR-TOUCH-WL Dealer Settings Menu (cont'd)

Time interval to request status: Displays the duration between autodiscovery process activations.

Connect using Wi-Fi Only

This selection MUST be checked (enabled).

Tablet

Connection:

(1) Change/Create CUSTOM IBRIDGE ISEE-WAP Wi-Fi Name and KEY: Select this feature to modify the factory default network settings of the touchscreen. The **Preferred Network** dialog appears, allowing a new **Wi-Fi Name** (SSID) and a new secret **Key** to be entered. Note that this information can be changed at any time by re-running this feature. **Note:** All wireless cameras in the system must be unlocked before using this feature.

(2) Configure Wireless Camera: When wireless cameras are first powered, they (by default) automatically attempt to connect with the first access point that answers using the default **SSID** of "PUBLIC". This feature requests all cameras within range to attempt to connect with a wireless router using the custom **SSID** and secret **Key** previously created in the menu item named "***(1) Change/Create CUSTOM IBRIDGE ISEE-WAP SSID and KEY***" described above. **Note:** All wireless cameras in the system must be unlocked before using this feature (will read "**Camera is unlocked**" in popup).

(3.a) Lock Down IBRIDGE ISEE-WAP: Tap to protect the wireless router / touchscreen connection by a "lock down" process, ensuring a fixed connection between the wireless router / touchscreen device pairs. This selection disables the automatic connection process that attempts to connect the touchscreen with the first wireless router that answers using the default **SSID** of "PUBLIC".

(3.b) Unlock IBRIDGE ISEE-WAP: To reverse the "Lock Down" process described in the previous menu selection.

(4) Restart Wi-Fi: Tap to perform a "warm boot" restart operation of the Wi-Fi, where the power is not turned off and back on, and with the app running.

Minutes to check connection integrity: Tap to set the number of minutes the touchscreen will automatically attempt a restoration of the wireless connection between the touchscreen and the wireless router should this connection be interrupted. Selectable durations are: 1, 3, 5, 7, 10, 15 and 20 (minutes).

BSSID used to LOCKDOWN IBRIDGE: Tap to enter a new "broadcast" SSID (named "BSSID" in this menu) to be stored in the touchscreen's memory, to be used by default when the touchscreen is rebooted, powered off/on or emerges from Screen lock.

Factory Default:

Tap to remove all user data and restore the IBR-TOUCH-WL back to its original out-of-box factory condition.

iBridge Updater

Update Server Address: Displays the IP Address and Port number used by the network server when the menu selection **Check For Updates** (described below) is tapped.

Check for Updates: Tap to automatically check to see if a newer version of the touchscreen firmware is available from the location specified in the "**Source**" menu item (described above). If a newer version is available, follow the on-screen prompts to load the firmware update files, as necessary.

Current Version: Displays the current version number of the IBR-TOUCH-WL firmware.

Update iBridge Application from USB: Select if the new firmware update is located on USB memory (such as a thumb drive, portable hard drive, memory stick, etc.), and you wish to use the USB socket located on the side of the IBR-TOUCH-WL to re-install the firmware. **Note:** The update file must be placed in a folder named "napco" (case sensitive) located in the top root directory.

Update Logo: Insert a USB thumb drive to add your logo image to the Home Screen and "Keypad Skin". The logo must be named "logo.png" (case sensitive) and must be located in a folder named "dealerLogo" (case sensitive) located at the top root directory of the thumb drive. When this logo is added successfully and later the logo is tapped, the touchscreen opens its default browser to the webpage specified in the **Update Infopage** menu selection, detailed below. **Note:** Although the touchscreen searches for the specific file name "logo.png", the image file itself may be a .png, .bmp or .jpeg format. However, the file must be renamed "logo.png".

Update Infopage: Insert a USB thumb drive to add an image that will display website or other corporate information. The file must be named "dealer.png" (case sensitive) and must be located in a folder named "dealerLogo" (case sensitive) located at the top root directory of the thumb drive. When a logo is added to the Home Screen and

"Keypad Skin" using the **Update Logo** menu selection (see above) and this logo is later tapped, the "dealer.png" image file will appear enlarged on the touchscreen.

Update Android OS via USB: Select to update the Android operating system. Be sure the update .zip file (WinZip) is located in the top root directory of the USB drive (such as a thumb drive, portable hard drive, memory stick, etc.). Use the USB socket located on the side of the IBR-TOUCH-WL to install the OS. Once inserted into the USB socket, tap this selection (if already inserted, remove and re-insert). Allow up to 15 seconds for the update process to begin; once started, DO NOT remove the USB drive!.

Password Configuration: Allows you to change the password used to access the **Dealer Settings** menu. In the **Change Settings password** popup that appears, press the empty field with the flashing cursor to open an onscreen keyboard, allowing you to type the new password. Check the optional "**Show password**" checkbox to view the populated characters. Press "**Change Password**" to enter or "**Cancel**" to exit without changing.

Video

Allows changes to the video data settings received by the IBR-TOUCH-WL. **Note:** This **Video** menu selection appears (and all of the selections below) only if "**ISEE Series Cameras**" is selected in the Setup Wizard (see page 13 for more information about the Setup Wizard).

Camera List

Camera Auto Discovery: Check to allow the touchscreen to automatically attempt to capture and display video stream data found within the network to which the touchscreen is connected. This feature is designed to operate within the iSeeVideo system. See http://www.napcosecurity.com/video.html for more information.

Configure Wireless Camera: Allows the touchscreen to remotely change the wireless settings of the selected camera. When this feature is selected, be aware that the network path from the touchscreen to the camera may take several seconds to be established. **Note:** When selected, a popup appears, that reads:

"Please make sure to first connect an Ethernet cable to the router and to then connect power to the camera. Do you wish to proceed with Wireless Camera Configuration?"

1. The camera must be powered and wirelessly connected to the network before proceeding.
2. Tap **Yes** to proceed or **No** to exit without saving any changes. If you tap **Yes**, the touchscreen will scan the network and all available cameras will be listed (by IP address) in the Camera List that appears. Tap to select a camera in the list, and a **Configure Wireless Camera** popup appears, allowing you to either Lock or Unlock the selected camera. Locking the camera will ensure a permanent connection between the camera and the touchscreen.
3. Select either the **Lock** or **Unlock** radio button, and tap **Configure** to proceed or tap **Cancel** to exit without saving changes.

Camera Manual Discovery: Allows you to browse for and select to use a specific camera attached to the iBridge network using the touchscreen. The following two steps ("**Select**…" and "**Discover**…" shown below are required:

1. **Select camera to discover:** (Step 1): Tap to select the camera you wish to discover and capture its video stream data.
2. **Discover IP Camera:** (Step 2): Tap to initiate the network scanning process to discover the selected camera. Upon discovery, the video will be available for display from the touchscreen Home Screen (**Video** button).

Launcher

(Reserved for NAPCO use only)

Home

Show Clock - Check to display the current time on the Home Screen.

Weather Options - Local weather reports can be displayed on the Home Screen.

Refresh Frequency: Tap to set how often to automatically update the weather report feed. Selections include 5, 10, 15, 20, 30, 40, 50, 70, 80, 90 and 100 minutes. More frequent updates increase data use and slightly decrease battery life between charges.

Weather Feed: Check to display a weather report feed on the Home Screen. Uncheck to remove the weather feed from the Home Screen. **Note:** To customize the weather report feed to a particular Zip Code, see the following menu entries below.

Zip code entry: Check to associate the weather report feed to the area of the United States specified by the Zip Code entered in the field below. Uncheck to disassociate the weather feed from this Zip Code.

IBR-TOUCH-WL Dealer Settings Menu (cont'd)

Zip Code: Tap to set the Zip Code to which the Weather Feed is associated.

Update Automation Clock - Synchronizes the clock within the customer's router with the same time as the IBR-TOUCH-WL touchscreen.

Lock Display on Keypad View - Enabled (checked) when "Keypad Only" is selected in the Setup Wizard (see below). When enabled, pressing **Security** in the Home Screen immediately displays the virtual security system Gemini keypad, and not the intermediary "pie wedges" that are displayed when "Full Functionality" is selected in the Setup Wizard.

Set Keypad as the Only View - When enabled, pressing the **Home** button immediately and continually displays the virtual security system Gemini keypad. **Note:** The User Setting "**Enable KeySwitch Arming**" (detailed above) must first be disabled.

Modify Z-Wave Settings

For dealers who wish to disallow customer changes to the home automation Z-Wave system, unchecking (disabling) this setting disables the **User Settings** menu feature named "**Automation Management (z-wave)**". Conversely, check this setting to enable the **User Settings** menu feature named "**Automation Management (z-wave)**", allowing control of the Z-Wave home automation components within the system using the "**User Settings**" menu (where an touchscreen Dealer Settings password is not required).

Automation Management (z-wave)

Opens the **Automation Management** screen, allowing the configuration of Z-Wave devices, including the assignment of devices to Groups, the creation of Z-Wave Events, etc. See the **Using your iBridge App to Program your Z-Wave Home Automation System** (OI414) for more information.

Emergency Button

Check to enable the "**E**" (Emergency) button on the IBR-TOUCH-WL Home Screen. If unchecked, although the "**E**" (Emergency) button will appear on the Home Screen, it will be disabled and the message, "**Permission Denied. Please Contact Dealer.**" will appear when tapped.

Change Login URL

Not Used; do not change this selection.

Standby-Battery Calculation Worksheet

Use the procedure given below to determine the required standby battery capacity in Ampere-Hours (AH). **Note:** It is not totally accurate to merely multiply the combined standby current (in amperes) by the standby time (in hours) to obtain the battery capacity (in ampere-hours), since other factors (Go-Anywhere Hub charging capabilities, temperature, battery condition, etc.) affect battery operation. The following calculations will yield the theoretical minimum required capacity:

1. STANDBY CURRENT

DEVICE	QTY		STANDBY CURRENT (Amps)		
			EACH		TOTAL
iSecure Kit 1*	1	X	0.146	=	
iSecure Kit 2*	1	X	0.155	=	
iSecure Kit 3*	1	X	0.200	=	
Network	1	X	0.006	=	
GEMWV-RECV		X	0.025	=	
ISEC-WIFI[1]		X	0.050	=	
ISEC-ZWAVE[2]		X	0.010	=	
		X		=	
		X		=	
		X		=	
TOTAL STANDBY CURRENT →					Amps

(Box 1)

ISEC-KIT1 Battery Standby Hours*

- 12V,4AH battery: No network connection, ~27 hours, with network connection, ~26 hours.
- 12V,5AH battery: No network connection, ~34 hours, with network connection ~32 hours.

ISEC-KIT2 Battery Standby Hours*

- 12V,4AH battery: No network connection, ~25 hours, with network connection ~24 hours.
- 12V,5AH battery: No network connection, ~32 hours, with network connection ~30 hours.

ISEC-KIT3 Battery Standby Hours*

- 12V,4AH battery: No network connection, ~19.5 hours, with network connection ~19 hours.
- 12V,5AH battery: No network connection, ~24 hours, with network connection ~23 hours.

With 4AH battery, a system without Wi-Fi, Z-Wave or transceiver without a network connection will last about 27.5 hours. With 5AH battery, the same system will last about 34 hours. **Note:** Battery not supplied.

X [Hours] = [AH.]

(Standby Time) (Box 2)

2. ALARM CURRENT

DEVICE	QTY		ALARM CURRENT (Amps)		
			EACH		TOTAL
TOTAL STANDBY CURRENT (from Box 1, above) →					
HUB INTEGRAL SIREN		X	0.200	=	
BELLS		X		=	
STROBES		X		=	
HORNS / STROBES		X		=	
SMK DETECTORS with sounders		X		=	
TOTAL ALARM CURRENT →					Amps

X [Hours] = [AH.]

(Alarm Time) (Box 3)

MINIMUM REQUIRED BATTERY CAPACITY = BOX 2 + BOX 3 → [AH.]

Maximum Alarm Current = 300mA.

*Actual standby time will vary with Kit, system components and network use. For components included in each kit and other details, see **Ordering Information** on page 73.
(1) iSecure Kit 1 and Kit 2 only, if added.
(2) iSecure Kit 1, if added.

ORDERING INFORMATION

Complete Professional System Kits

- **Kit 1 (ISEC-KIT1) with ISEC-WL-KEYPAD Wireless Battery-Powered Standard Keypad:** All-Inclusive system includes a Go-Anywhere Smart Hub with up to 80 zones, siren and integral dual path cell/IP LTE reporting, wireless LCD keypad (lithium battery-powered), security and notifications from consumer app, 50' wireless PIR and two wireless window/door contact transmitters. Provision for a 4AH or 5AH backup battery (not supplied) for power outage protection. 1 hour installation, dealer programming via cellphone or tablet.
- **Kit 2 (ISEC-KIT2) with ISEC-WL-TOUCH Wireless 4.3" Full Color Security Touchscreen Keypad:** All-Inclusive system includes a Go-Anywhere Smart Hub with up to 80 zones, siren and integral dual path cell/IP LTE reporting, wireless security touchscreen, integral Z-Wave control from consumer app, virtual keypad and SMS text notifications, 50' wireless PIR and two wireless window / door contacts. Provision for a 4AH or 5AH backup battery (not supplied) for power outage protection. 1 hour installation, dealer programming via cellphone or tablet.
- **Kit 3 (ISEC-KIT3) with Connected Home/Video/ Security IBR-TOUCH-WL Smart 7" Wireless IoT Touchscreen:** All-Inclusive system includes a Go-Anywhere Smart Hub with up to 80 zones/ points, siren and integral dual path cell/IP LTE reporting, integral Z-Wave control from touchscreen or app. Wireless multifunction 7" TFT security touchscreen controls smart automation, video-viewing and security functions. One 50' wireless PIR and two wireless window/door contact transmitters. Provision for a 4AH or 5AH backup battery (not supplied) for power outage protection. 1 hour installation, dealer programming via cellphone or tablet.

System Components

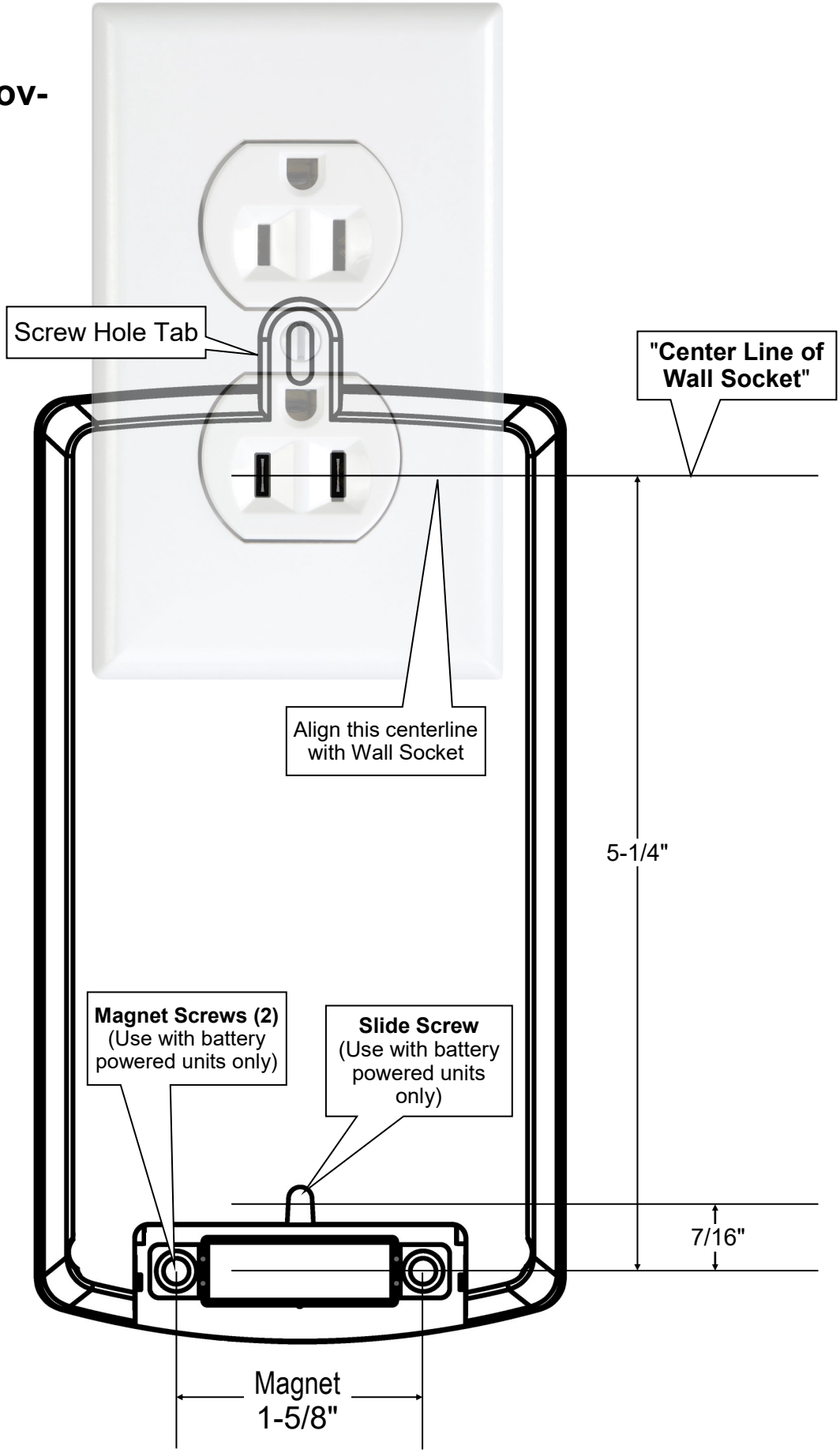
- **ISECURE GO-ANYWHERE SMART HUB**: Includes up to 80 wireless zones, in 1 or 2 discrete Areas, with keypad bus and other optional connections. Kits with the suffix "-V" use the Verizon network, "A" use the AT&T network.
- **IBR-TOUCH-WL Smart 7" Wireless IoT Touchscreen**: Wireless interface touchscreen with 7" color display. Requires 120VAC electrical wall outlet for power supply. Dimensions (WxHxD): 7⅞ x 5⅜ x ⅞ in. (13.7 x 20 x 2.2 cm).
- **ISEC-WL-TOUCH Wireless 4.3" Full Color Security Touchscreen Keypad**: 900MHz wireless interface touchscreen with 4.3" color display. Requires 120VAC electrical wall outlet for power supply. Dimensions (WxHxD): 5⅜ x 3¾ x 1⅜ inches (13.7 x 9.5 x 3.5 cm).
- **ISEC-WL-KEYPAD *Wireless Battery-Powered Standard Keypad***: 900MHz wireless interface with multi-line wide viewing angle ICON display for system status, "K Style" (**STAY**/**AWAY**) keypad buttons, battery powered by one CR123 Lithium battery, optional 2nd battery for extended life. Dimensions (WxHxD): 5⅜ x 3¾ x 1⅜ inches (13.7 x 9.5 x 3.5 cm).
- Optional **ISEC-2WF-MOD** *2-Wire Fire Sensor Module* that supports 2 Fire zones (connect to Fire Power [+], Zone 7 [–] and Zone 8 [–] terminals).
- Optional **StarLink Extended Range Antenna** to increase LTE cellular transmission signal strength.
- **ISEC-CARBON MON *Supervised Wireless Carbon Monoxide Sensor***: A high-quality carbon monoxide (CO) sensor with built-in supervised digitally-coded radio transmitter. It is compatible with Napco's iSecure series supervised receivers that monitor alarms, restores, low battery, tamper and status.
- **ISEC-DW-XMITTER *Low Profile Window/Door Transmitter***: A 1-point low profile window/door transmitter specially designed for use in iSecure series wireless systems. When used with the supplied magnet, the transmitter functions as a window/door sensor.
- **ISEC-GLASSBREAK *Wireless Glass-Break Sensor***: An advanced Commercial/ Residential wireless acoustic glass-break sensor designed for use with Napco iSecure series RECV wireless receivers. Equipped with a combination normally-closed (NC) cover and wall tamper, each unit is shipped with the cover tamper operational, and the wall tamper disabled.

Ordering Information (cont'd)

- **ISEC-HEAT** ***Wireless Heat Detector with Rate of Rise***: A high-quality 135°F (57°C) fixed temperature detector with Rate of Rise and built-in supervised digitally-coded radio transmitter. It is compatible with Napco's iSecure RECV series supervised receivers that monitor alarms, restores, low battery, tamper and status.
- **ISEC-KEYFOB** ***4-Button Pendant/Keychain Transmitter***: This multifunction transmitter serves as an Area arm / disarm device with two auxiliary functions, and may be used as a police panic and/or auxiliary emergency transmitter.
- **ISEC-WL-MODULE** ***Wireless 8-Zone Takeover Module***: Designed to make use of the wiring and power supply of an existing wired security system, the **ISEC-WL-MODULE** is designed to convert 8 *hardwired* zones into eight supervised *wireless* burglary, 4-wire Fire or CO zones, thus simplifying installation, including the ability to work with existing 12 volt power supplies. The module is commonly mounted next to the existing control panel, in close proximity to the existing hardwired zone connections. Wireless frequency is 900MHz.
- **ISEC-MOTION** ***Passive Infrared Motion Sensor***: An advanced PIR sensor designed for use with Napco's iSecure RECV series wireless receivers. The **ISEC-MOTION** is powered by two supplied 3-volt lithium batteries (estimated battery life 3 years). When battery voltage drops below normal, a low-battery report will be sent to the receiver.
- **ISEC-PANIC** ***Single Button Waterproof Panic***: A single-function pendant/keychain transmitter that serves as an emergency device for use as a police panic and/or auxiliary emergency transmitter. Two replaceable 1.5V silver oxide cells power this portable transmitter (it includes a flashing LED to warn when low batteries require replacement). To operate, simply press the button momentarily.
- **ISEC-WL-SIREN Wireless Siren**: Output provides 85dBA sound level at 10 feet, supports *Siren*, *Temporal Fire* and *CO* alarm audible cadences, with optional bright LED strobe. Operable from 110VAC with battery backup, or by battery power alone; mountable on flat wall or by AC outlet plug; for indoor or outdoor operation. The iSecure system can accommodate up to 4 wireless sirens. Wireless frequency is 900MHz.
- **ISEC-SMOKE** ***Supervised Wireless Digital Smoke Sensor***: A high-quality photoelectric smoke sensor with built-in supervised digitally-coded radio transmitter. It is compatible with Napco's iSecure RECV series supervised receivers that monitor alarms, restores, low battery, tamper and status.
- Optional **ISEC-WIFI** *Internet Module* for central station communication and notifications. Supplied in KIT 3 (see above).
- Optional **ISEC-ZWAVE** *Z-Wave Module* for programming/control of Z-Wave home automation controls such as Z-Wave-enabled lights, outlets, thermostats, garage door operators and door locks.

ISEC-WL-SIREN Wireless Siren Mounting Template

For Wall Outlets With a Center Cover Plate Screw



ENSURE THIS BOX IS 1 INCH X 1 INCH

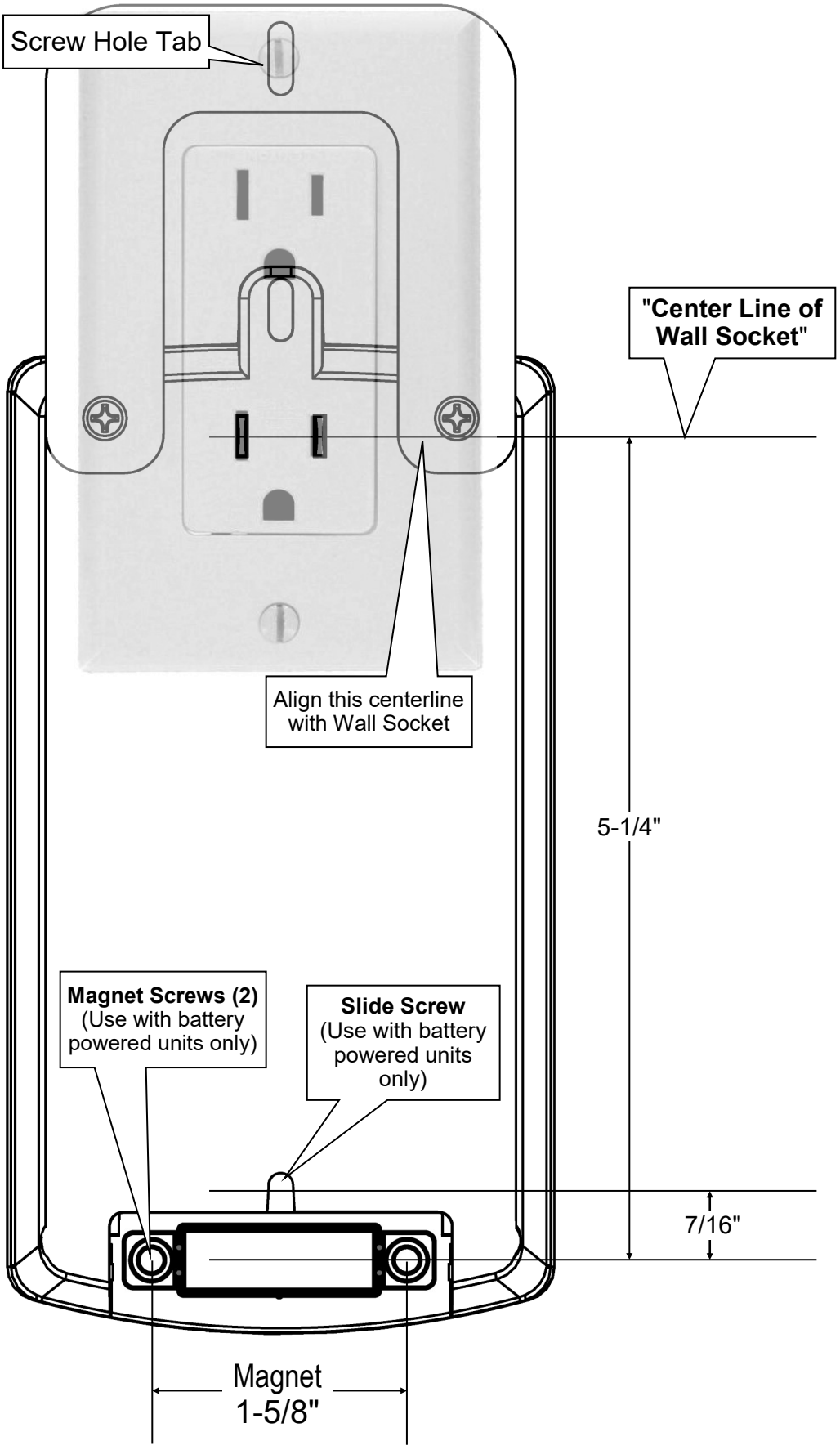
Notes

ISEC-WL-SIREN Wireless Siren Mounting Template

For Wall Outlets Without a Center Cover Plate Screw

This template shows the unit plugged into the bottom receptacle, but either can be used (or invert the unit as required).

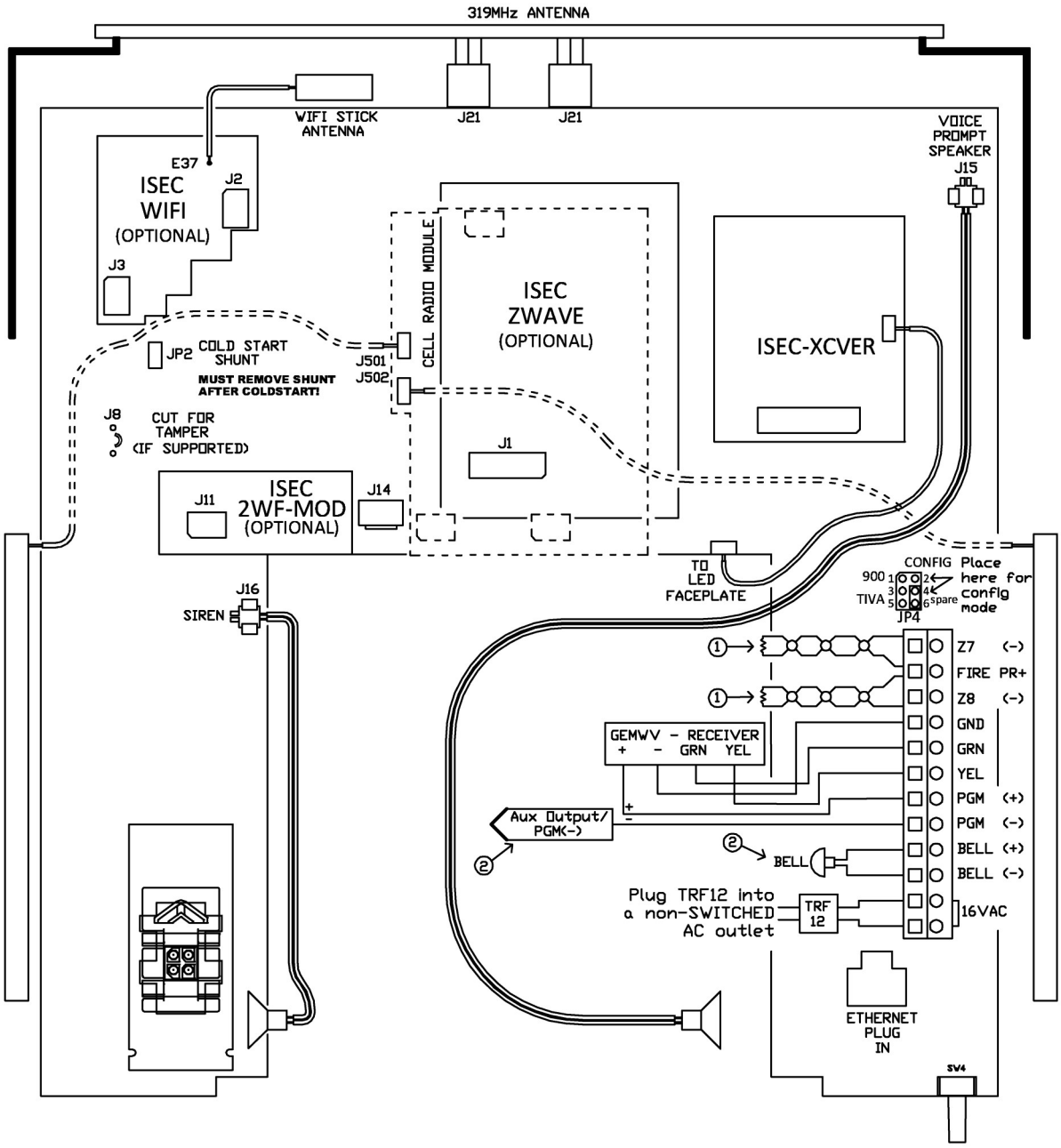
Remove the two screws from the siren housing and replace screws with bracket in place, as shown.



ENSURE THIS BOX IS 1 INCH X 1 INCH

Notes

iSecure Hub Wiring Diagram



NOTES:

1. REQUIRES ISEC-2WF-MOD
   USE ONLY LISTED 2 WIRE
   SMOKE DETECTORS, USE 2.2K EOLR
2. REFER TO WI2240 FOR MAX CURRENT
   AND BATTERY STANDBY.
   BELL CAN BE PROGRAMMED AND WIRED
   FOR SUPERVISION.
3. REFER TO WI2440LF FOR ADDITIONAL
   INFORMATION.

LA3550A2

NAPCO LIMITED WARRANTY

NAPCO SECURITY TECHNOLOGIES, INC. (NAPCO) warrants its products to be free from manufacturing defects in materials and workmanship for *thirty-six months* following the date of manufacture. NAPCO will, within said period, at its option, repair or replace any product failing to operate correctly without charge to the original purchaser or user.

This warranty shall not apply to any equipment, or any part thereof, which has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to acts of God, or on which any serial numbers have been altered, defaced or removed. Seller will not be responsible for any dismantling or reinstallation charges.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. THERE IS NO EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR A WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. ADDITIONALLY, THIS WARRANTY IS IN LIEU OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF NAPCO.

Any action for breach of warranty, including but not limited to any implied warranty of merchantability, must be brought within the six months following the end of the warranty period. IN NO CASE SHALL NAPCO BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT.

In case of defect, contact the security professional who installed and maintains your security system. In order to exercise the warranty, the product must be returned by the security professional, shipping costs prepaid and insured to NAPCO. After repair or replacement, NAPCO assumes the cost of returning products under warranty. NAPCO shall have no obligation under this warranty, or otherwise, if the product has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to accident, nuisance, flood, fire or acts of God, or on which any serial numbers have been altered, defaced or removed. NAPCO will not be responsible for any dismantling, reassembly or reinstallation charges.

This warranty contains the entire warranty. It is the sole warranty and any prior agreements or representations, whether oral or written, are either merged herein or are expressly cancelled. NAPCO neither assumes, nor authorizes any other person purporting to act on its behalf to modify, to change, or to assume for it, any other warranty or liability concerning its products.

In no event shall NAPCO be liable for an amount in excess of NAPCO's original selling price of the product, for any loss or damage, whether direct, indirect, incidental, consequential, or otherwise arising out of any failure of the product. Seller's warranty, as hereinabove set forth, shall not be enlarged, diminished or affected by and no obligation or liability shall arise or grow out of Seller's rendering of technical advice or service in connection with Buyer's order of the goods furnished hereunder.

NAPCO RECOMMENDS THAT THE ENTIRE SYSTEM BE COMPLETELY TESTED WEEKLY.

Warning: Despite frequent testing, and due to, but not limited to, any or all of the following; criminal tampering, electrical or communications disruption, it is possible for the system to fail to perform as expected. NAPCO does not represent that the product/system may not be compromised or circumvented; or that the product or system will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; nor that the product or system will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce risk of burglary, robbery, fire or otherwise but it is not insurance or a guarantee that these events will not occur. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE, OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. Therefore, the installer should in turn advise the consumer to take any and all precautions for his or her safety including, but not limited to, fleeing the premises and calling police or fire department, in order to mitigate the possibilities of harm and/or damage.

NAPCO is not an insurer of either the property or safety of the user's family or employees, and limits its liability for any loss or damage including incidental or consequential damages to NAPCO's original selling price of the product regardless of the cause of such loss or damage.

Some states do not allow limitations on how long an implied warranty lasts or do not allow the exclusion or limitation of incidental or consequential damages, or differentiate in their treatment of limitations of liability for ordinary or gross negligence, so the above limitations or exclusions may not apply to you. This Warranty gives you specific legal rights and you may also have other rights which vary from state to state.

RADIO AND TELEVISION INTERFERENCE: CAUTION:

Changes or modifications not expressly approved by manufacturer could void the user’s authority to operate the equipment.

This equipment has been tested and found to comply with the limits pursuant to Part 15 of the FCC rules. This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.