



NAPCO®

333 Bayview Avenue
Amityville, New York 11701

For Sales and Repairs, (800) 645-9445

For Technical Service, (800) 645-9440 or visit us at

<http://tech.napcosecurity.com/>

(Note: Technical Service is for security professionals only)
Publicly traded on NASDAQ Symbol: NSSC

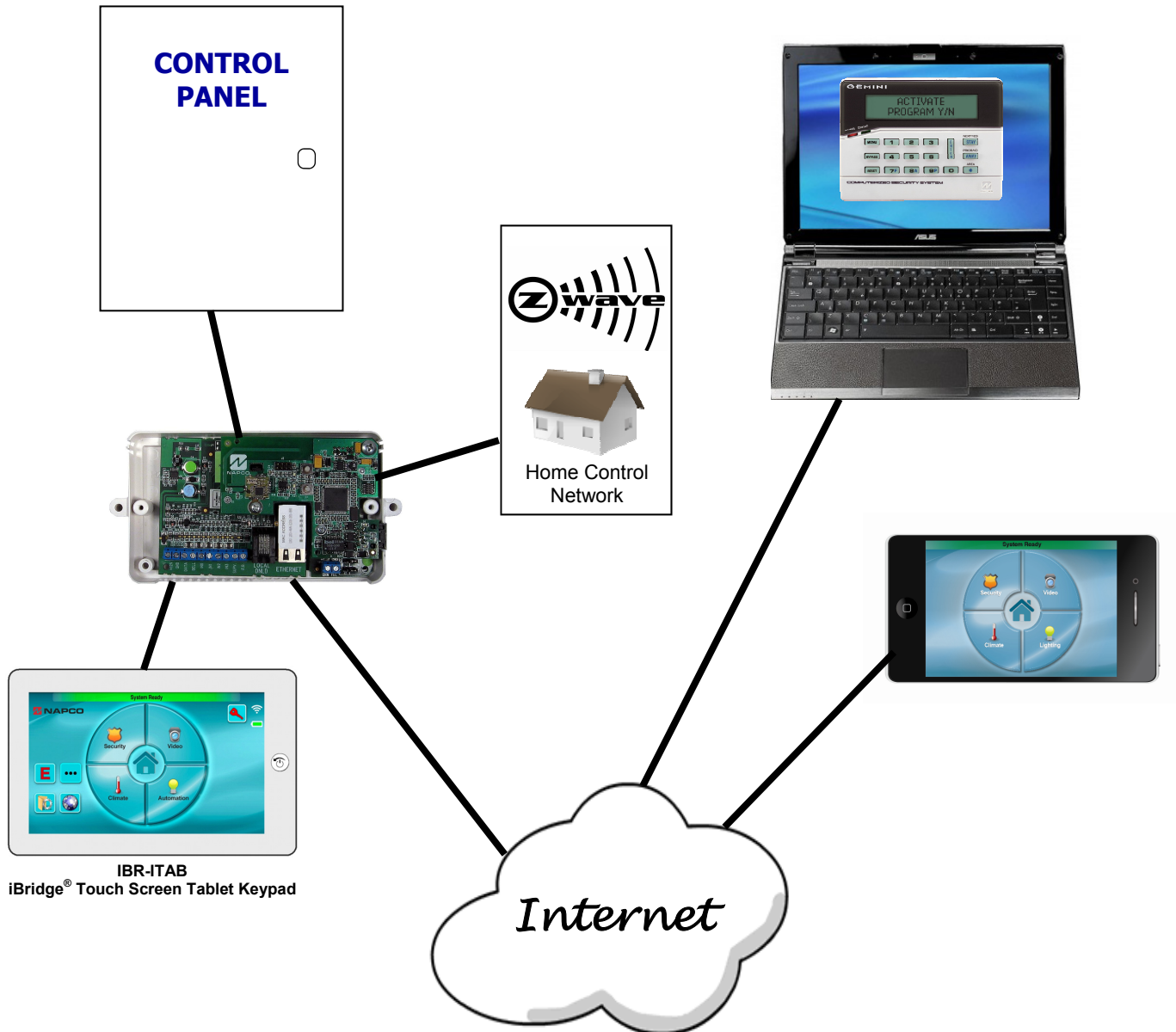
© NAPCO 2013

iBridge® Suite Quick Start

Installing the IBR-ZREMOTE Z-Wave® Controller, ISEE-WAP Wireless Access Point and the IBR-ITAB Wireless Touchscreen Tablet

WI1980B draft .09 05/13

iBridge®



Overview of the NAPCO iBridge® IBR-ZREMOTE Z-Wave® Controller

General Overview

The iBridge® IBR-ZREMOTE is a Local and Remote Control Module and Z-Wave® Controller that allows control of security, video, locking, lighting and climate control from inside or outside your home. Z-Wave devices may be enrolled, removed and formed into a Z-Wave wireless home control network, and also integrated with Napco's iBridge suite of services that includes access to the iSee Video remote video Internet monitoring system.

Compatibility with the iSee Video VideoAlert system allows an email or text message to be sent when a selected control panel event occurs. In addition, acting as a wireless Z-Wave controller, the IBR-ZREMOTE can trigger Z-Wave network devices upon control panel events. For example, upon system arming the IBR-ZREMOTE can turn lights on or off, adjust thermostats, email video clips, etc.

The IBR-ZREMOTE is wired to the control panel keypad bus, and continually monitors all changes to the status of the system and triggers actions based on user or dealer entered programming.

Note: Z-Wave enabled devices displaying the Z-Wave logo can usually be used with the IBR-ZREMOTE module regardless of manufacturer, and the IBR-ZREMOTE module can also be used in other manufacturer's Z-Wave enabled networks. For an **iBridge Z-Wave Evaluated Device List**, see our website at www.napcosecurity.com/ibridge.html.

iBridge Online

To access the IBR-ZREMOTE remotely via PC, tablet or smart phone, or to provide remote services for a customer, the dealer must have an iBridge online account. Go to www.ibridgeonline.com/ibridge to access your existing account or register for a new account. Device apps are available for iPhones, iPads and Android devices from their respective app markets.

Remote Control

With the IBR-ZREMOTE, *actions performed at the keypad can be performed remotely*. Add the IBR-ZREMOTE to a Napco control panel by simply programming an additional keypad address into the control panel, set the IBR-ZREMOTE to this new keypad address and enroll the IBR-ZREMOTE into your subscribers account.

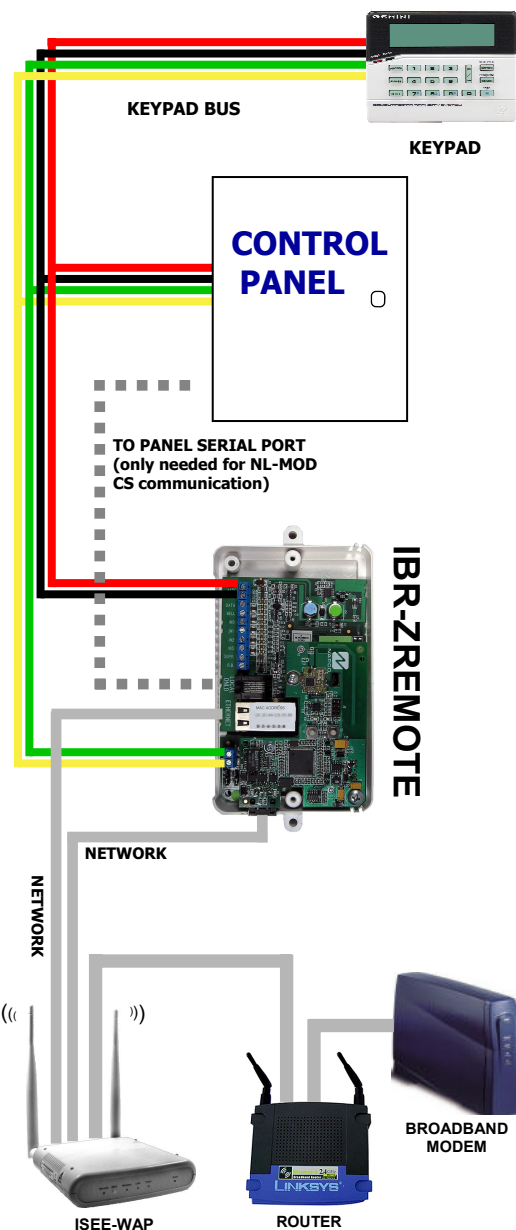
Alarm Reporting

The IBR-ZREMOTE is also an Internet reporting module, capable of reporting alarms and events to any central station equipped with the Napco NetLink NL-RCV-RMPCUL central station receiver or NetLink NL-CSRCV central station software application. The IBR-ZREMOTE also permits high speed upload/download of the control panel through the Internet. Refer to manuals WI1491 (NL-RCV-RMPCUL) and OI294 (NL-CSRCV) for details.

Overview: Home Control Network

A home control network is a system used for controlling lights, appliances, air conditioning, heating, burglary alarm systems and other devices within a home or office. Z-Wave is a reliable and robust wireless home control network standard created by Zensys, Inc. (www.zen-sys.com), operating within an interconnected "mesh" network where at least two pathways exist for each device (thus if one pathway fails, another is still available). In addition, Z-Wave devices operate within the 902-928 MHz band, and therefore will not interfere with Wi-Fi and other devices using the 2.4 GHz band.

The simplest Z-Wave network consists of a primary "controller" and single controllable device or "node" such as a light switch, thermostat, etc. Additional controllers and devices can be "included" into (or "excluded" from) the network at any time, usually by means of button presses on both the controller and the device. The IBR-ZREMOTE module can act as a "primary" controller to setup and maintain the network, or can act as a "secondary" controller within an existing Z-



Wave network previously started by a "primary" controller (from any manufacturer).

Note: As the signal strength between the IBR-ZREMOTE controller and its devices is crucial, *we recommend all devices be mounted in their final installed locations before they are included into the network.*

Ordering Information

- **IBR-ZREMOTE:** Bus-Mount Module for remote control, up/download of security system, plus control of Z-Wave devices, lights, locks, thermostats, etc.
- **IBR-ITAB:** iBridge Wireless Touchscreen Tablet with mounting frame and charging station.
- **IBR-ITABKIT** Kit: iBridge Wireless Touchscreen Tablet with mounting frame/charging station plus Wireless Access Point (ISEE-WAP).
- **IBR-ITAB-HW:** Hardwired iBridge Touchscreen Tablet version for permanent mounting and for a more conventional hardwire installation.
- **ISEE-WAP:** Wireless Access Point for wireless communication between IBR-ITAB and wireless cameras.
- **IBR-ITABSTAND:** Angled tabletop stand/docking station for use with IBR-ITAB Touchscreen (not included). Décor-neutral and ideal for bedrooms, kitchens, desks, etc.
- **IBR-WIFI-MOD:** Wireless Panel Interface, communicates between Internet, Gemini Control Panel and IBR-ITAB Touchscreen Tablet, when NO remote services or Z-Wave are required (**Note:** For remote services and Z-Wave, use the IBR-ZREMOTE).

For an **iBridge Z-Wave Evaluated Device List**, see our website at www.napcosecurity.com/ibridge.html. Although all Z-Wave appliances should comply with the Z-Wave standard, we recommend that you install only Napco evaluated devices, especially the more complex devices such as thermostats and door locks.

Specifications

Dimensions: 1½" x 7" x 4¾" (HxWxD)

Input Voltage: 13.0-10.0VDC.

Input Current: Maximum current (@ 8VDC) = 185mA

Nominal current: @ 12VDC = 185mA (supplied by control panel connections).

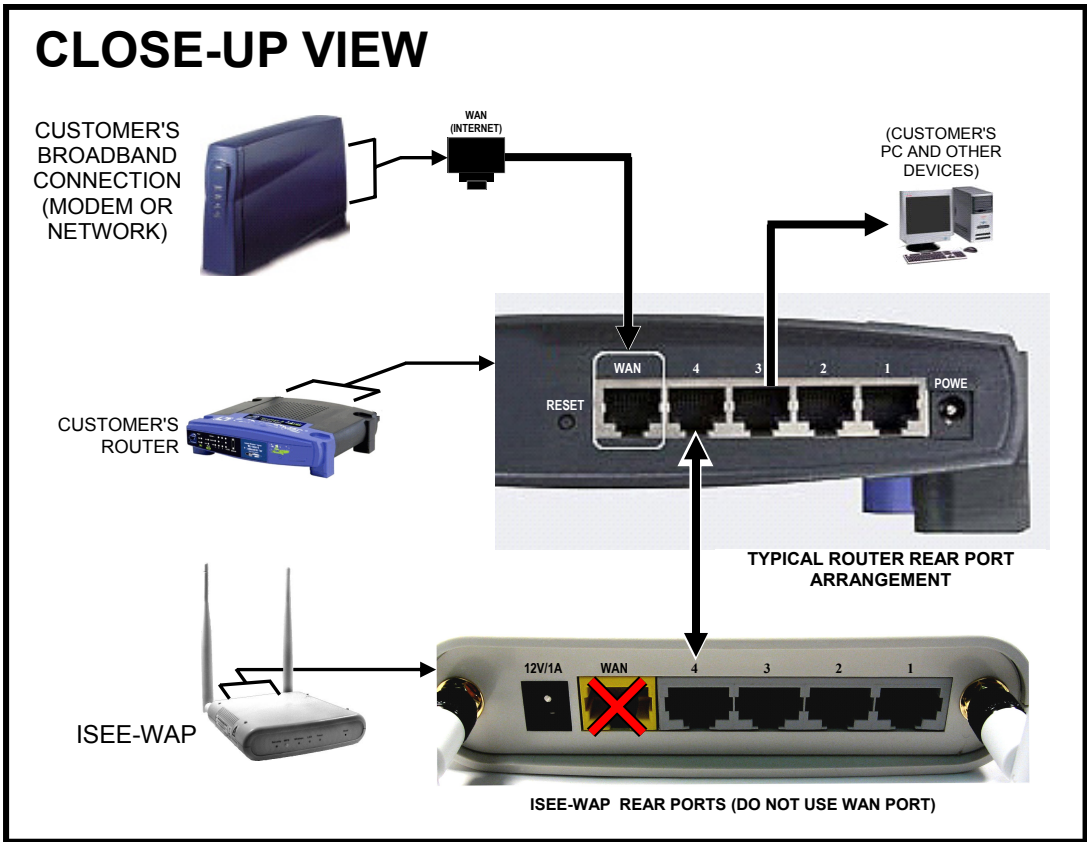
Available panel combined auxiliary current is reduced by 185mA.

Outputs: PGM-style open collector (negative trigger) with a maximum sink current of 50mA.

Factory Default Settings

The IBR-ZREMOTE factory default settings for the NL-MOD and NL-RCM modules are:

- Account ID = FFFFFFFF
- Dealer ID = NAP0000
- Keypad Address = 1
- Keypad Type = RP1CAe2
- PC Preset / DNS IP Address = 72.3.180.2
- PC Preset / DNS Port = 5002
- PC Preset / DNS Check-In Time = 1
- iBridge Server IP Address = 208.109.208.163
- iBridge Server Port = 5011



The system can be installed out of the box without any configuration changes. First ensure the alarm control panel is wired and working with a standard wired keypad as KP ADDR #1 before you continue. Be sure to use the same "type" of keypad (either "Classic" or "K Series" Stay/Away) that you plan to configure the system to use. Do not wire the IBR-ZREMOTE yet.

STEP 1: PREPARE THE IBR-ITAB

The IBR-ITAB has an internal battery that may need recharging. Press and hold the "Back/Power" button (shown at right) until the display starts to turn on (then release the button). After the IBR-ITAB tablet starts, observe the battery indicator icon (upper right); if green or yellow, the battery has enough charge to complete the installation. Press and hold the "Back/Power" button again until the power off message appears and turn off the tablet. If the battery indicator icon is red, you can install and mount the charging plate as described in W11944 or just connect the power adapter to the charger plate (observing polarity) and power the IBR-ITAB to continue.



Back / Power Button

STEP 2: CONFIGURE THE CONTROL PANEL

The alarm control panel must have the correct firmware version installed to utilize all features of the IBR-ZREMOTE. Required are:

- **PCD-Windows Quickloader:** V6.12 or greater (located on the enclosed IBR-ZREMOTE support CD)
- **Control panels GEM-X255, GEM-P9600 and GEM-P3200:** Firmware version 60A22-4 or greater (included in IBR-ZREMOTE box)
- **Control panels GEM-1664, GEM-P1632 and GEM-P816:** Firmware version 30R-9 or greater (included in IBR-ZREMOTE box)

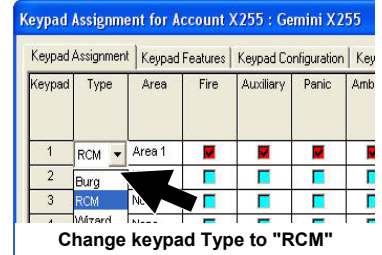
Note: The following version control panels may be upgraded for iBridge compatibility:

- GEM-P3200 and P9600 controls running firmware version 20 or greater, released in May of 1999.
- GEM-P816, P1632 and P1664 controls running firmware version 30 or greater, released in August of 1999 (V10 can be used if a 32 pin socket is available on the control panel motherboard).

Perform the following:

2A. If installing the IBR-ZREMOTE on a previously programmed control panel, launch Quickloader 6.12 and upload the control panel program configuration to an account on your PC. In all cases ensure a conventional keypad is connected at keypad address 1 for steps that follow.

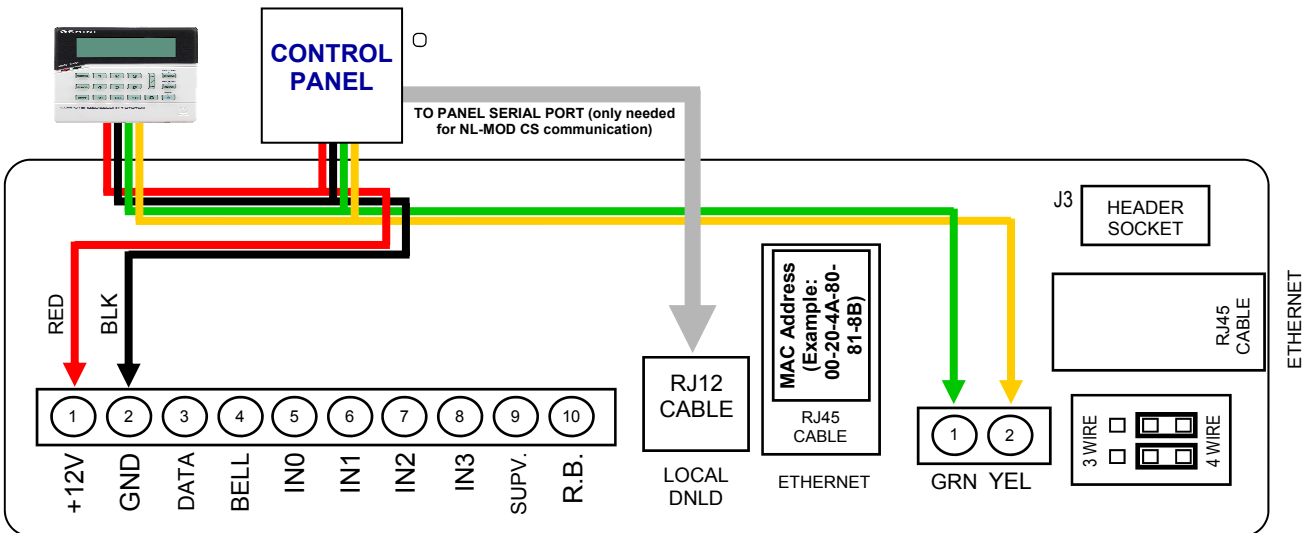
- 2B. Remove power from the control panel, disconnect the battery wires and replace the EPROM with the new version.
- 2C. Power up the control panel and reconnect the battery wires. Enter Direct Address Program Mode and Cold Start the control panel (refer to the enclosed programming instructions WI2052 for the procedure).
- 2D. Download the saved control panel program configuration back into the control panel or create and download new control panel programming.
- 2E. In PCD-Windows Quickloader, select the keypad address to be used for the IBR-ZREMOTE; change the keypad **Type** for that keypad address to "RCM" (as shown in the image at right), select **EZ Arm** (6 columns to the right on the same screen). In the **Keypad Features** tab, check "**Disable Code-Required-for-FM-Level 1**". Download to the control panel (all IBR-ZREMOTE modules are factory defaulted as keypad #1). Change the conventional wired burglary keypad that was keypad #1 to keypad #2.



Note: If this is your first installation, we suggest you leave the IBR-ZREMOTE at KP ADDR #1 and change the conventional wired keypad to ADDR #2 as described in these instructions.

STEP 3: INSTALL AND WIRE THE IBR-ZREMOTE

The IBR-ZREMOTE requires a unique keypad address on the NAPCO keypad bus. The IBR-ZREMOTE is factory configured as control panel keypad address #1 and as a Napco "Classic" keypad. Place the panel configuration jumper into **CONFIG** mode and leave this jumper there for now. The keypads will be configured in step 5. Disconnect power from the control panel (AC and battery) and connect the keypad bus wires as shown below to the +12V, GND, GRN and YEL terminals.



STEP 4: WIRE THE NETWORK CONNECTION

Use standard CAT5 network cables as follows: Plug one end of a CAT5 cable into an open LAN socket on the customer's existing router and the other end into an open LAN socket of the ISEE-WAP. Plug one end of a second CAT5 cable into another open LAN socket on the ISEE-WAP, and the other end into the IBR-ZREMOTE receptacle labeled "**ETHERNET**". Then plug one end of a third CAT5 cable into another open LAN socket on the ISEE-WAP, and the other end into the other IBR-ZREMOTE receptacle located on the right side of the IBR-ZREMOTE. Refer to the diagram on page 4 if needed. **Note: Customer's router must support DHCP.**

Reconnect the battery connection and power the control panel. Wait two (2) minutes for all devices to fully power and complete their network connections. Remember, the panel configuration jumper is set to **CONFIG** mode, so the keypads will power up and display "OUT OF SYSTEM".

STEP 5: CONFIGURE THE IBR-ZREMOTE AND KEYPAD ADDRESSES

- 5A. If the IBR-ZREMOTE is to be keypad address #1 and set as a Napco "Classic" keypad, then set the keypad address in the conventional wired keypad to keypad address #2 as you normally would using Keypad Configuration Mode (press 11123 **FUNCTION**). If you have more than one conventional wired keypad, verify each address is unique. If not changing the IBR-ZREMOTE, then move the panel **CONFIG** jumper back to **NORM** and go to step 7. If the IBR-ZREMOTE is changing, then the basic procedure is to enter Keypad Configuration Mode and set the KP ADDR and Keypad Type to the desired values.

5B. The IBR-ZREMOTE keypad address and Keypad Type can be configured in one of three ways:

- Use an IBR-ITAB
- Use an app on your iPhone, iPad or Android device
- Use a Napco GEM-RP1CAe2 or GEM-K1 keypad with a special programming cable

USING THE IBR-ITAB

If step 4 was completed properly, the IBR-ZREMOTE and ISEE-WAP should have obtained IP addresses and be ready for use. Power up an IBR-ITAB and it will connect to the ISEE-WAP and IBR-ZREMOTE automatically (this process may take several minutes the first time it is performed). The top status bar will display "Not Ready To Arm" when it is ready for the next step.



Back / Power Button

First set the keypad skin for the IBR-ITAB. On the IBR-ITAB, **press and hold** the button with the **System Settings** "gear" icon on the lower left corner of the display for 4 seconds. Tap the empty field and in the keyboard type the administrator password "admin"; tap **Done** and then tap **OK**. Tap **Yes** to the "Making System Changes..." popup, then tap **Security**. Tap the first menu entry **Keypad Skin**, then tap either **Classic** or **K Series Stay/Away**. Press the **Back/Power** button twice to return to the keypad display. Next, set the keypad type in the IBR-ZREMOTE.

Tap **Security > Other Options > Keypad Mode**. The keypad will display "01 Out of System". Tap **1 1 1 2 3 FUNCTION** to enter Dealer Mode. Tap **FUNCTION** or **MENU** repeatedly until the configuration keypad displays "Keypad Address". Enter the correct address and tap **ON/OFF** or **ENTER** to set. Tap **FUNCTION** or **MENU** repeatedly until the configuration keypad displays "KEYPAD TYPE RP1CAE2" (tap **INTERIOR / STAY** or **NEXT** to toggle between the keypad model names. **Note:** If using a physical K Series ("Stay/Away") keypad connected with a wire harness, **press and hold STAY** until it beeps to toggle between the keypad model names). When selected, tap **ON/OFF** or **ENTER** to set, then tap **RESET** to exit.

Return the **CONFIG** jumper on the control panel back to **NORM** ("System Ready" should appear on the keypad if all zones are closed).

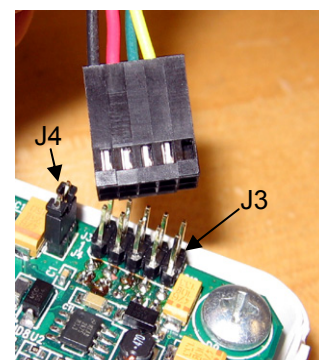
USING AN APP

If you have already loaded the iBridge App on your device, then connect to the ISEE-WAP Wi-Fi access point "IBRIDGE" using the WEP key **1234567890**. Repeat the same steps in the section "USING THE IBR-ITAB" above. If for any reason you cannot connect with the IBR-ITAB or the phone app, then the "USING A CONFIGURATION KEYPAD" procedure (below) can be used.

Apps can be obtained from Google Play or the Apple Store.

USING A CONFIGURATION KEYPAD

A GEM-RP1CAe2 or GEM-K1 keypad (henceforth called a "configuration keypad") can be plugged into the IBR-ZREMOTE "Header Socket" receptacle (marked "J3" on the PC board; see the image at right). When connected, the IBR-ZREMOTE can be configured exactly the same way as a physical Gemini keypad. Connect one end of the provided RCM-PROGCABLE keypad bus cable to the Gemini keypad, then connect the other end to the IBR-ZREMOTE circuit board receptacle marked "J3" (keying tab faces away from unit).



RCM-PROGCABLE plugs into the "Header Socket" (J3) Jumper J4 also shown.

Configuration Procedure

Use the "configuration keypad" to program the IBR-ZREMOTE KP ADDR and Keypad Model as follows:

- a. Ensure both jumpers marked **J2** and **J3** located on the lower PC board (next to the blue bus connector) are set closer to the "4-WIRE" printing on the PC board (this is the default shipping configuration).
- b. Remove jumper **J4** on the Z-Wave PC board (located on the top PC board in the IBR-ZREMOTE housing, next to silver battery).
- c. Connect one end of the special keypad bus cable (RCM-PROGCABLE) to the back of the configuration keypad and connect the other end to the IBR-ZREMOTE "Header Socket" receptacle (marked "J3" on the PC board). The control panel **CONFIG** jumper should still be set to **CONFIG** from step 4. When the configuration keypad powers up, its display will read "XX OUT OF SYSTEM". **IMPORTANT:** After the display reads "XX OUT OF SYSTEM", you **MUST** stop and wait the IBR-ZREMOTE components to reset and prepare for communication; only after the display changes to "XX OUT OF SYSTEM RCM-MODULE" may you proceed with the next step (the words "RCM-MODULE" must be in the display text).

Repeat the same steps in the section "USING THE IBR-ITAB" above. When finished, disconnect the cable **and be sure to reinstall jumper J4.**

At this point you should have a functioning system and be able to arm and disarm the panel using the IBR-ITAB. The next step is to integrate video cameras (if applicable).

STEP 6: ENROLL VIDEO CAMERAS (Optional)

If you already have iSeeVideo cameras installed, then jump to the next paragraph "Discovering Cameras" below.

Installing Cameras

Mount and wire cameras in accordance with the work instructions included with the camera. Make note of the MAC address of each installed camera. Once the cameras are installed (wired or wireless), power them and wait at least two (2) minutes for the cameras to acquire IP addresses and stabilize.

Discovering Cameras

On the IBR-ITAB Touchscreen, tap the **VIDEO** "pie shape", then tap the magnifying glass that appears on the next screen to discover the newly installed cameras (or the existing iSeeVideo cameras installed previously). It may be necessary to re-run this discovery process more than once if all cameras are not found.

STEP 7: ACTIVATE AN IBR-ZREMOTE ACCOUNT FOR "REMOTE SERVICES"

Once the IBR-ZREMOTE has been completely wired to the control panel, configured and powered up, a consumer iBridge subscriber account is ready to be created for remote services (remote access through the web and smartphones), if desired. These activation steps include adding Subscribers, cameras and an IBR-ZREMOTE to a customer account.

NEW ACTIVATION

7A. To create your new **iBridge** subscriber accounts, simply type the following Internet address into your Web browser:

www.ibridgeonline.com/ibridge

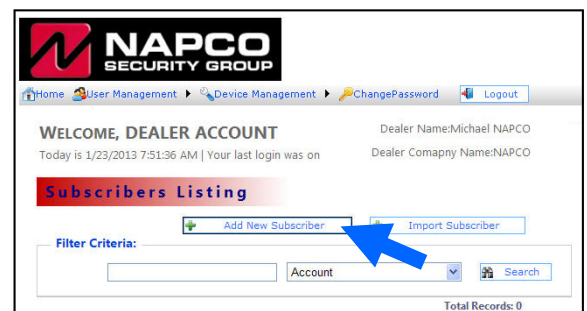
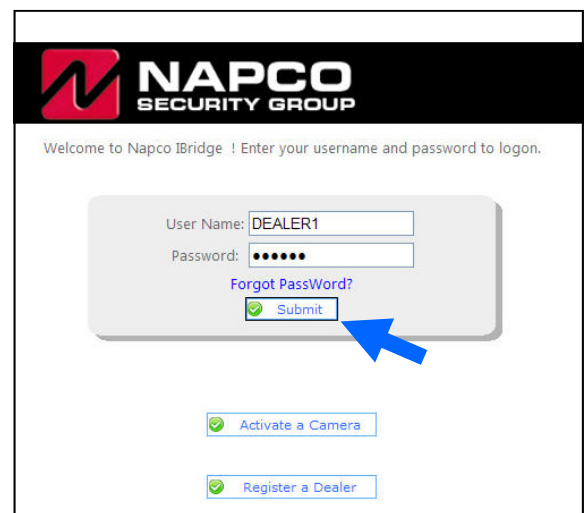
...and the following web page appears:

- If you are *not yet* registered as a Dealer, simply click **Register a Dealer** to submit a registration request (you must be a registered dealer to create subscriber accounts)
- If you *already have* a Dealer account, type your **User Name** and **Password** and click **Submit** and the **Welcome** screen appears

7B. In the **Welcome** screen, click **User Management > Manage Subscribers**. The **Subscribers Listing** page appears.

Click **Add New Subscriber**. In the **Subscriber Registration** form, type the subscriber's name, address, telephone number and other information in the appropriate fields as shown in the image at right. When finished, click **Create**.

Note: After clicking **Create**, scroll below the **Subscriber Information** to find the subscriber automatically added as a new "**Master**" **End User** (the person having administrative privileges, i.e. the ability to program Advanced Settings and add new End Users to the account).



7C. Near the bottom of the screen, click **Add / Replace New i/z Remote Device**.

In the popup that appears, type the unique **MAC Address** of the IBR-ZREMOTE printed on the label on the jack marked **ETHERNET**. Type the complete 12-digit code (do not enter dashes).



Keypad Selection

Click the **Keypad** selection pull-down menu to select the keypad type of the installation. This should be the same keypad type installed in step 5. **Note:** For the -2AS, the -3DGTL and -4RF series, the corresponding full alpha keypad will be displayed, allowing the entry of zone descriptions, if desired.

Click **Submit** → and the new IBR-ZREMOTE will be added to the account.

7D. Next, add any video cameras to the account by typing the MAC address of the cameras you wish to view remotely. This step is required even if the cameras are existing iSeeVideo cameras. Above the **zRemote** entry field you will see the **Add New Camera** button shown at right:

Simply click on **Add New Camera** and type the MAC address in the field provided. If you previously enrolled cameras to your Dealer account but did not assign them to a Subscriber account, then you can select "**Add from Existing Camera Device List**" to find the cameras and assign them to the Subscriber.

Click **Submit** and then add additional cameras if needed.

7E. Be sure to select the services to be made available to your customer by checking the appropriate boxes. By checking **Video**, **Security** and/or **Z-Wave**, customers can control these functions via the web. Only by checking **Remote Access** can your customers remotely log in and connect using Apple and Android devices ("Remote Services").

7F. Verify the user account is functioning by logging in to the following Internet address using your Web browser:

www.ibridgeonline.com/ibridge

Enter the customer User Name and Password created in

step 7B above, and verify that the image shown at right appears.

Verify the system can be armed and disarmed and that the cameras, if installed, are visible. The consumer can change the User Name and Password by accessing the web account.



STEP 8 – SECURING THE SYSTEM

Up to this point the iBridge system auto-configured using the default Wi-Fi settings. The ISEE-WAP has two default SSIDs (network access point names) broadcasting to devices within signal range of the ISEE-WAP; these SSIDs can easily be seen with any iPhone or Android device. The names are **PUBLIC** and **IBRIDGE**. SSID1 is named **PUBLIC** and is used by the IBR-ITABs and cameras to automatically join the network. SSID2 is named IBRIDGE, uses the WEP security protocol and a 10-digit Key of "1234567890". SSID2 can be changed to a new name and a **secret** Key so that only the customer has access. After this step is completed, PUBLIC can be disabled so that no one else can connect to the system. **Note:** This process is reversible to accommodate future changes.

The following steps will ensure that the IBR-ITAB will **only** wirelessly connect to the intended ISEE-WAP by adding the unique SSID name and (secret) key to the ISEE-WAP.

With the Home Screen displayed, using your finger, **press and hold** the **System Settings** "gear" icon (shown at right).



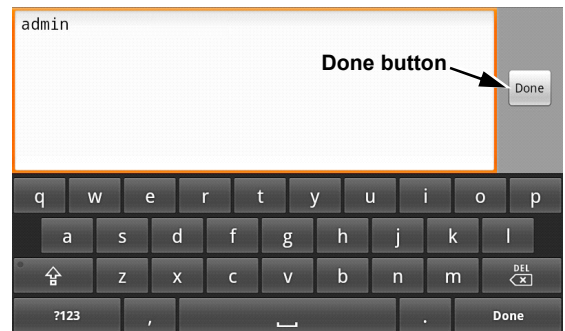
Press and hold the "System Settings" "gear" icon

The **Please enter password** popup appears (shown at right). If this popup does not appear, press the **Back/Power Button** and try again. Remember, be sure to **press and hold** the **System Settings** "gear" icon.



In the **Please enter password** popup, tap the blank (empty) field with the flashing cursor, and the following keyboard will appear on the screen:

Using the keyboard keys, tap each letter to type the word "**admin**" (all lowercase). When finished typing, tap the **Done** button (see image at right).



The word "admin" is now placed in the **Please enter password** popup, as shown:



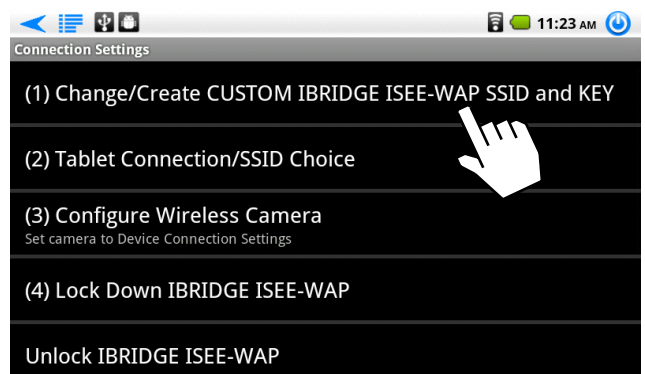
Tap **OK**. The following warning popup appears:



Tap **Yes** and the following **User Settings** menu appears:



Tap **Tablet**, then tap **Connection**. The following **Connection Settings** appears:

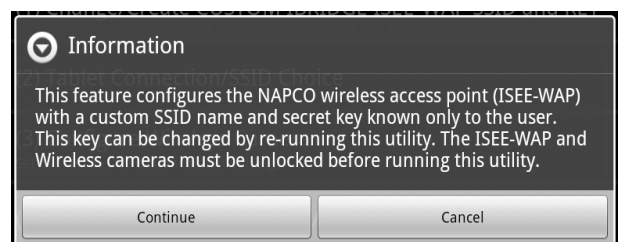


Change the SSID and Key.

Tap **(1) Change/Create CUSTOM IBRIDGE ISEE-WAP SSID and KEY**.

Note: The following only needs to be performed once to configure or change the ISEE-WAP. If enrolling a second IBR-ITAB, jump to the next step.

An **Information** popup appears:



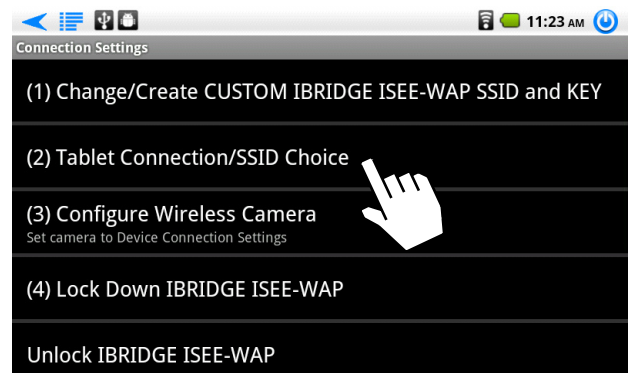
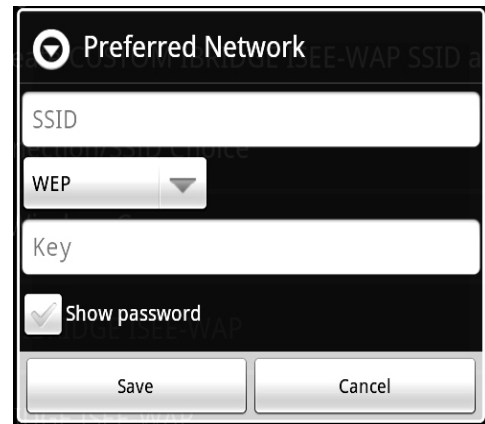
Tap **Continue**. In the **Preferred Network** dialog that appears (shown at right), type a new **SSID** name, ensure the default security protocol is **WEP**, then type a new secret **Key** (check **Show Password** to view the password text as you type). The **Key** MUST be one word (no spaces) 10 digits in length using only 0-9, A, B, C, D, E or F as digits. **DO NOT use the same SSID name and secret Key as the customer's router. Again, do not use spaces!**

When finished, tap **Save**. This action adds this unique **SSID** and this unique **Key** to the ISEE-WAP. A popup will display that reads, "**Command completed successfully -- OK**". Tap OK to close; wait two (2) minutes for the ISEE-WAP to restart and the IBR-ITAB to reconnect.

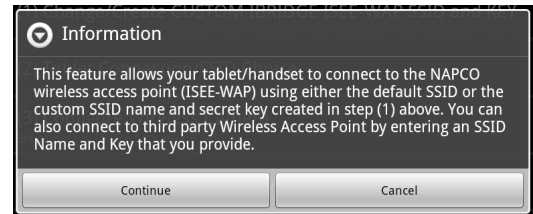
Next, you must configure the IBR-ITAB to hereafter **ONLY** connect to the ISEE-WAP with this unique **SSID** and this unique **Key**. Proceed as follows:

Choose the Tablet Connection/SSID.

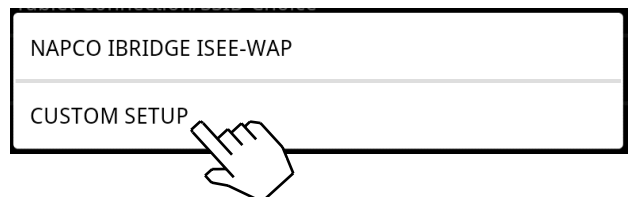
At the **Connection Settings** menu that appears (shown at right), tap **(2) Tablet Connection/SSID Choice**.



In the following **Information** popup that appears, tap **Continue**.

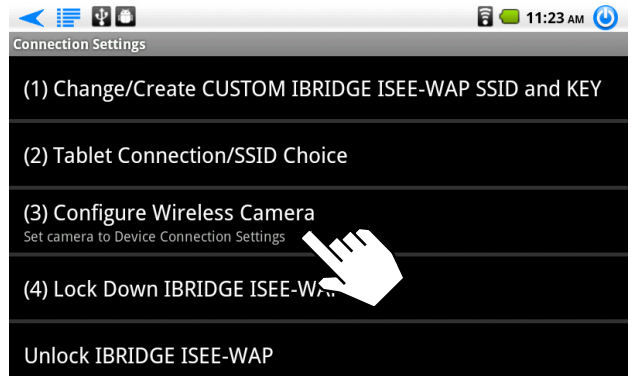


In the screen that appears, tap **CUSTOM SETUP**.



Under **CUSTOM SETUP** you will be presented with the same **Preferred Network** dialog above. The data entered previously will still exist; tap **Join** to accept this data. Note: If enrolling a second IBR-ITAB, these fields will have to be completed using the same data you entered previously with the first IBR-ITAB.

Configure the Wireless Cameras. Be sure all wireless cameras are powered, then tap **(3) Configure Wireless Camera**.



A confirmation popup appears; tap **Yes** to proceed (or tap **No** to exit without saving changes).

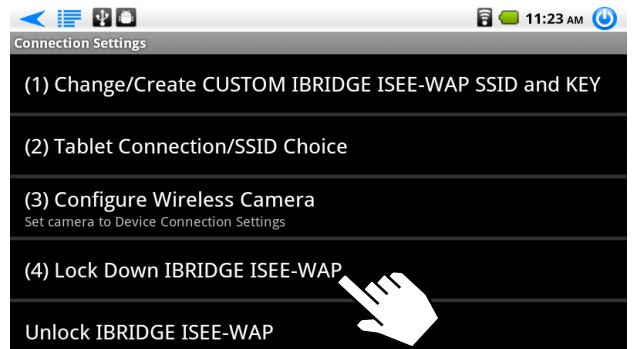


Wait while the IBR-ITAB searches for all cameras. When finished searching, the IBR-ITAB lists all the discovered cameras by IP address. Tap to select each camera one at a time and tap **"Lock"** to lock the camera. Exit when complete.

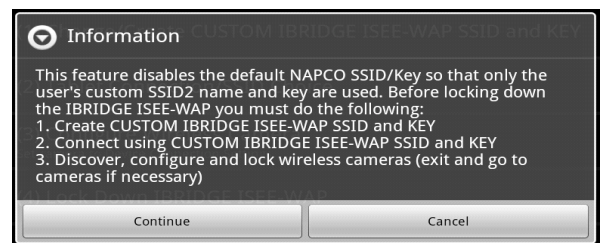
Lock Down the ISEE-WAP.

In the **Connection Settings** menu, tap **(4) Lock Down IBRIDGE ISEE-WAP**.

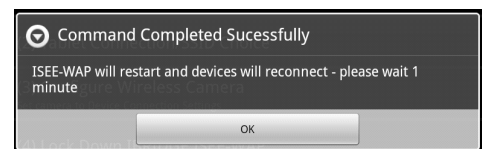
Locking the ISEE-WAP turns off the default "PUBLIC" SSID so no other systems can connect to your equipment. Any new IBR-ITABs will have to use the new SSID and Key entered in the **Preferred Network** dialog above.



In the **Information** popup that appears, tap **Continue**.



Wait several seconds until the following popup appears:



Tap **OK** to close.

Test the keypad. To ensure the IBR-ITAB is connected with the correct ISEE-WAP, press the **Back/Power Button** repeatedly until the Home Screen appears, then press the **Security** button. A screen with your arming choices appears:

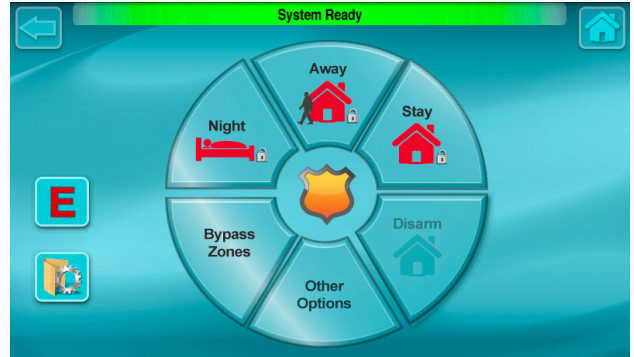
Arm the system by first pressing **AWAY**, then press the User Code in the keypad that appears. Ensure the keypad text on the IBR-ITAB matches the keypad text that appears on the standard wired keypad.

In the Home Screen, when connected, a connection strength indicator appears at the top right (1-4 bars, as shown). If you wish to verify the connection, press this icon and text appears at the bottom of the IBR-ITAB screen confirming the validity of the connection. For example, the text may read:



Signal Strength Indicator

"Connected with ssid: WAP345, Level: Excellent, IP: 192.168.50.102, Port: 8003, Gateway: 192.168.50.2"



At this point you have successfully installed, configured and locked down the iBridge system. Additional manuals are included with this system as follows:

Z-WAVE PROGRAMMING AND USER GUIDE (OI378)

If your customer plans to use Z-WAVE devices, then consult OI378, "Using your iBridge IBR-ITAB Series Home Automation System". This user guide describes how to enroll and control Z-Wave devices. As a Dealer, you have the choice to either allow or disable access to Z-WAVE configuration menus by the end user. This setting is discussed in the following WI1944.

CONFIGURING THE IBR-ITAB (WI1944)

The IBR-ITAB Installation, Mounting and Programming instructions describes how to physically install the IBR-ITAB to the wall and also describes the three (3) types of menus in the IBR-ITAB. They are:

1. **User Settings:** User Settings are options that your customer can set to control the IBR-ITAB. Tap the **System Settings** "gear" icon once (lower left corner of the Home screen) to access this menu. Descriptions of each feature are described in the IBR-ITAB Security System User Guide OI372.
2. **Dealer Settings:** Dealer Settings are options that the Dealer configures. These menus are accessed via the same "gear" icon but by pressing and holding the "gear" icon for 3 seconds (a password is required to access these menus).
3. **Android Settings:** Within Dealer Settings there is an option to access the Android menu system. The Android menus should not be accessed by the Dealer; these menus exist for troubleshooting purposes when in contact with our Technical Support department.

IBR-ITAB SECURITY SYSTEM USER GUIDE (OI372)

This user guide describes how to use the security keypad on the IBR-ITAB screen, and perform tasks such as arming Stay (protecting yourself at home), arming Away (setting the alarm when leaving), arming Night (protecting yourself when sleeping), bypassing zones, and all other aspects of the customer's security alarm system.

NOTES

THE FOLLOWING STATEMENT IS REQUIRED BY THE FCC:

This equipment generates and uses radio-frequency energy and, if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for a Class-B computing device in accordance with the specifications in Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: reorient the receiving antenna; relocate the computer with respect to the receiver; move the computer away from the receiver; plug the computer into a different outlet so that computer and receiver are on different branch circuits. If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful: "How to Identify and Resolve Radio-TV Interference Problems". This booklet is available from the U.S. Government Printing Office, Washington, DC 20402; Stock No. 004-000-00345-4. Changes and Modifications not expressly approved by NAPCO can void your authority to operate this equipment under Federal Communications Commissions rules.

FCC NOTICE (FOR U.S. CUSTOMERS):

This device complies with Part 15 of the FCC Rules:
Operation is subject to the following 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.

THIS DEVICE COMPLIES WITH INDUSTRY CANADA LICENCE-EXEMPT RSS STANDARD(S). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

NAPCO LIMITED WARRANTY

NAPCO SECURITY SYSTEMS, 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.