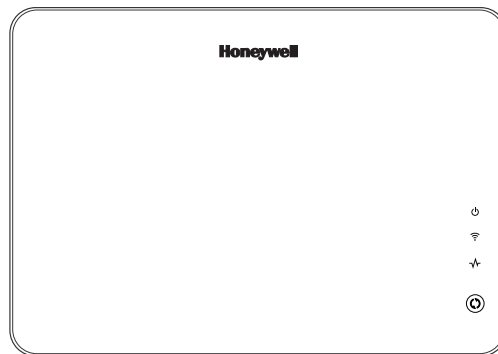


Honeywell

VISTA® Automation Module

User Guide



PLEASE GO TO THE BOTTOM OF
PAGE 35 FOR FCC / IC AGENCY
STATEMENTS.

TABLE of CONTENTS

INTRODUCTION	5
VAM Features.....	5
Memory Card.....	6
Navigating the VAM Menus	6
Navigation Button Descriptions.....	7
LED Functions.....	8
 USING CAMERAS (MULTIMEDIA MENU).....	 9
Viewing Cameras	9
Adding Cameras to the System.....	9
Removing Cameras from the System.....	10
 AUTOMATION AND USING Z-WAVE DEVICES (AUTOMATION MENU)	 11
Manually Operating Devices.....	11
Adding (Include/Add) Z-Wave Devices.....	11
Editing Z-Wave Device Names.....	13
Removing (Exclude/Delete) Z-Wave Devices.....	Error! Bookmark not defined.
Abort a Z-Wave Action	13
 CREATING SCENES	 16
Definitions of Trigger, Condition, and Action	16
Steps To Create a Scene	18
Creating Groups & Rooms	18
Z-Wave Troubleshooting	14
 USING THE SECURITY SYSTEM (SECURITY MENU)	 19
User Codes.....	19
Introduction to Arming and Disarming the System.....	19
Steps to Arm the System.....	19
Arming Multiple Partitions.....	20
Steps to Disarm the System	20
How to Display Faults (Zones).....	21
How to Bypass Zones.....	21
How to Clear Bypassed Zones	22
Console Emulation Mode	22
How to Enter Console Emulation Mode.....	22
 USING TOTAL CONNECT WITH VAM (REMOTE SERVICES).....	 23

SYSTEM SETUP26
 Email Setup26
 Remote Access Log In Setup (Account Setup).....27
 Time and Date Setup.....27
 Options and ECP Address (for Installer use only) .. **Error! Bookmark not defined.**
 Changing the Home Router (Wi-Fi Setup).....28

SOFTWARE UPGRADES.....30
 System Information.....30
 Manual Software Upgrades30
 Automatic Software Updates30
 Compatible Z-Wave Devices31

NOTES32

NOTE: This device is a Security Enabled Z-Wave Controller.

Introduction

The VISTA Automation Module (herein after referred to as “VAM”) provides Z-Wave automation features to your VISTA® security system, allowing control of various Z-Wave devices including cameras, lights, door locks, and thermostats. VAM does not have a physical keypad interface, but instead is controlled by using a web browser on a Wi-Fi® enabled computer device that is connected to your home Wi-Fi network.

VAM Features

Feature	Description
Wi-Fi® Connection	VAM uses your home Wi-Fi network to communicate with a Wi-Fi enabled device such as a Smartphone, i-Pad™, Android™ Tablet, Blackberry® or laptop PC. Your installer connected the VAM to your Wi-Fi router during installation. However, if you later install a new router, you will need to reconnect the VAM to the new router. Refer to Wi-Fi Network Setup in the System Setup section for details on connecting VAM to a different router.
Home Automation	Control lights, thermostats, door locks, and other Z-Wave devices automatically and easily add or remove Z-Wave devices to the system.
Create Automation Scenes	Define system actions to automatically start when certain conditions occur. Supports up to 10 scenes.
View Cameras	View up to four cameras at the same time. Supports up to 32 cameras.
Security System	Control your security system via VAM menus.
Remote Access	Control VAM when away from the premises using a computer device connected to the Internet.
Remote Services	VAM supports remote services so you can control VAM using Honeywell’s Total Connect™.
Email Notification	Receive email notifications when certain events occur. Notifications can be sent to up to four email addresses.
Switchable Themes	Switch from normal view to mobile view depending on the type of device used with the VAM.
Setup Menus	If needed, program various system settings, including time and date, new router, and remote access log in. Refer to the System Setup section for details.

UL	Wi-Fi has not been evaluated by UL.
-----------	-------------------------------------

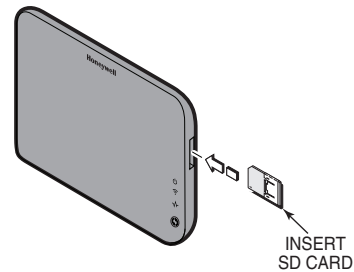
Memory Card

The VAM supports automatic software upgrades. However, an SD memory card must be installed and left in the VAM to upgrade the software. Your installer may have installed the SD memory card for you. See Software Upgrades section later in this manual for more information about automatic software upgrades.

If not already installed, insert the memory card (SD/SDHC Card) as shown.

- 4GB SD card supplied
- Supports up to 16GB SD Card

IMPORTANT: Avoid touching the contacts on the SD card.

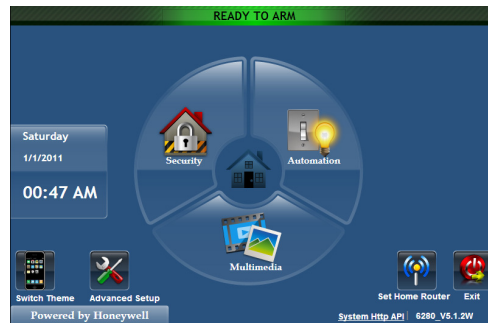


Navigating the VAM Menus

VAM is controlled by using a web browser on a Wi-Fi enabled computer device. Your installer will have shown you the URL to enter into the browser's address bar that opens VAM's Main menu, and perhaps made a bookmark (favorite) for easy access later. Navigation begins from the Main menu. Navigate through various sub-menus by clicking graphical buttons (buttons) to perform a selected function.

From the Main menu you can:










- control your security system
- control/view your cameras
- control home automation such as lighting, thermostat, and door locks
- switch from PC view to mobile view by clicking **Switch Theme** button.
- go to advanced setup menus.



NOTE: Depending on the type of computer device being used to access the VAM, options are selected by either clicking a mouse pointer or touching/tapping the screen. In this manual, the term "click" is used to indicate this function.

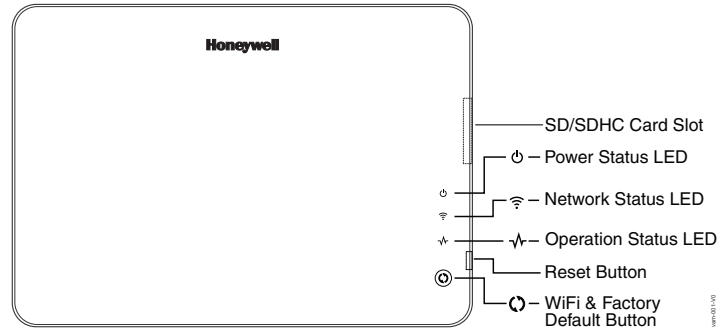
Navigation Button Descriptions

To aid in the navigation through the VAM menus, a set of user-friendly icons (buttons) has been provided. The appearance and function of these buttons are described below.

BUTTON	BUTTON TITLE	FUNCTION
	Automation	Used to perform Z-Wave setup, Scene setup, and Group setup screens to control Z-Wave devices.
	Security	Used to control the security portion of the system.
	Multimedia	Used to view cameras and/or add cameras to the system.
	Home	Returns to the Main menu ("Home") screen.
	Back	Returns to the previous screen.
	Setup	Used to set various system settings, including email notification and remote access log in credentials, time & date, and Wi-Fi setup.
	Set Home Router	Accesses the "Set Home Router" screen and used to connect VAM to your home router.
	Exit	Exit the VAM menu.
	Switch Theme	Used to set the screen for use on a mobile device or PC.

LED Functions

The VISTA Automation Module has three LEDs as follows:

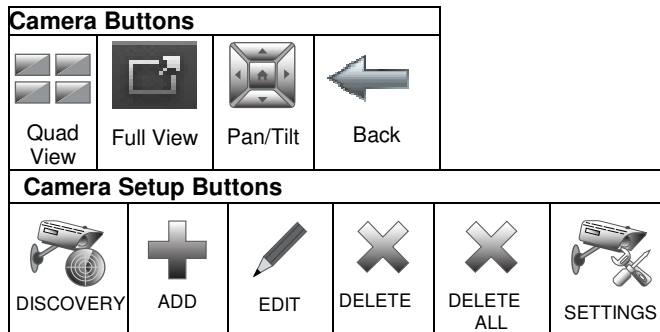


LED/BUTTON	MEANING
Power Status (green)	Indicates power status. This LED blinks when it is powering up and booting. Solid green indicates it is fully functional.
Network Status (blue)	When the Wi-Fi is connected to the VAM, it will show the Wi-Fi status through the blue LED. The LED is blinking when VAM is booting and solid blue when VAM is ready as AP mode (acting as an Access Point) or connects to the internet as STA mode (station mode, device is connected to the Wi-Fi router).
Operation Status (yellow)	Normally off. It will blink slowly if there is no communication with the control panel or if the Z-wave controller is not responding. Fast blinking indicates Z-wave is in enrollment or deletion status.
Reset Button	Press to reset the device. The Reset button can also be used to restore factory default settings. During power up, press and hold the reset button for more than 5 seconds, the unit will restore factory default settings. (The Wi-Fi & Factory Default button can also be used to restore factory defaults.)
Wi-Fi & Factory Default Button	<ul style="list-style-type: none"> • Wi-Fi Network Reset: Press and hold down for more than 5 seconds to clear the VAM's Wi-Fi network connection. You will then need to reconnect the VAM to your home Wi-Fi network. • Factory Default Reset: Double press this button, then, while the green, blue, and yellow LEDs blink in sequence, press and hold down this button for more than 5 seconds to set the VAM to its factory default settings.

Using Cameras (MultiMedia menu)

The Multi-Media feature allows you to view up to four cameras at once from the VAM camera screen.

UL Camera functionality is supplementary only and has not been evaluated by UL.



Viewing Cameras

Your installer may have installed one or more cameras at the time of installation. If you want to add cameras to the system, see the Adding Cameras to the System section.

1. Select **Multimedia**.
2. Images from installed cameras appear. Use the Quad View button to view up to four cameras on the same screen. Select a quadrant area on the screen (this area is highlighted) and then select the camera that you want to appear in that quadrant. For pan/tilt style cameras, use the Pan/Tilt button to change the angle of the selected camera.

IMPORTANT: Use the web browser to view cameras for non-security purposes only. Camera streams viewed from the web browser can stop without indication due to network connection issues.

Adding Cameras to the System

NOTE: VAM must be Wi-Fi connected to the home router before adding cameras.

1. Before mounting your camera, connect a Cat5/6 cable to the back of the camera and connect the opposite end to the Ethernet port on your router. Initial camera setup cannot be performed over a wireless connection.
2. Apply power to the Camera. It may take a few seconds for initial power-up of camera.

3. Click **Multimedia** and then click the **Camera Setup** button to display the “Camera List” screen.
4. Click the **Discover** button to locate the camera. Once located, highlight the camera address and go to Step 6 below.
5. If the camera information is not automatically obtained, click the **Add** button to manually enter the appropriate wireless information for SSID, security mode, N/W type, domain, and channel.
6. To edit camera information, highlight the listed camera name and click the **Edit** button; enter the desired name for the camera. Enter the appropriate information (**NAME, IP Address, RTSP, MJPEG, MOBILE, RTSP PORT#, MODEL,**) if known.
7. Click **OK**.
A pop-up window displays “**cam (name) wireless set OK**”, if successful. Or, “**cam (name) wireless set Failed**”.
8. If successful, the Cat5/6 cable can now be removed from the wireless camera,, and once power has been recycled to the camera you can view wirelessly via the VAM’s Multimedia menu.

NOTES:

- QuickTime® media player must be installed on your PC.
- Maximum suggested camera resolution = 640 x 480.
- Maximum suggested frame rate = 5 fps.
- Camera viewing is not compatible if using Opera web browser.

Removing Cameras from the System

1. To delete a camera, highlight the camera name and click the **Delete** button.
2. To delete all cameras, click the **Delete ALL** button.
3. Click the **Save** button.

Automation and Using Z-Wave Devices (Automation menu)

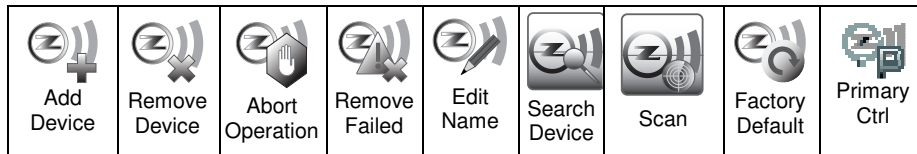
The VISTA Automation Module lets you control installed Z-Wave devices such as lights, thermostats, door locks, etc. To use Z-Wave devices, they first must be added (“included”) to the system. Follow the instructions below to Include Z-Wave enabled devices into a home control network using the VAM and follow the instructions in the Z-Wave device User Guide for your specific device.

EXISTING NETWORK NOTE: Z-Wave products from other manufacturers can be included (added) into the VAM network. Z-Wave devices that are always powered can serve as repeaters regardless of manufacturer.



- Automation functionality is supplementary only and has not been evaluated by UL.
- Z-Wave applications have not been evaluated by UL.

Z-Wave Device Management Buttons



Manually Operating Devices

Devices can be programmed to operate automatically based on scenes you define (refer to the Creating Scenes section). Alternatively, you can manually control a device using the Z-Wave Management screen (**Automation > Z-Wave Setup**).

Adding (Include/Add) Z-Wave Devices

Each device must be installed according to the manufacturer’s instructions. Before starting, make sure light modules are on, door locks are assembled and have their batteries installed, and thermostats are installed and operating.

WARNING: Automation is intended for lifestyle convenience. Do not use automation for life safety and property protection.

1. Go to the **Z-Wave Device Management** screen (**Automation > Z-Wave Setup**).
2. Click the **Z-Wave Include/ Add** button.
3. At the Z-Wave device, press the appropriate Function button depending on the type of device being added. Refer to the Device sections that follow.

Light, Switch or Outlet Module

Be sure the power switch on the device module is **ON**. Press the **Function Key** on the device.

NOTE: Z-Wave light modules may vary; follow the instructions in the Users Guide for your specific device to include properly into the Z-Wave network.

- If a dimmer module (multi-level switch) was included, an On/Off button and a slide bar (to control dimmer) are displayed.
- If an on/off light/appliance module (binary switch) was included, an On/Off button (to control the device) is displayed.

The screen displays a series of messages:

“Start add device. Please press function key on device”
“Adding Slave Unit”
“Device added successfully”

Door Locks

Assemble the Z-Wave door lock.

IMPORTANT: Be sure the door lock orientation/handedness is correct before Including into the system.

Door lock devices may vary; follow the instructions in the *User Guide* for your specific door lock to include properly and to program a new user code. Refer to the Door Lock's *Instruction Guide* and connect necessary cables, then install batteries.

NOTES:

- Program the user code in the control panel prior to programming that user code into the door lock. User Codes must be 4-digits.
- If software is upgraded on the VAM, re-include the door lock and re-set the user code in the door lock

Include a door lock device into VAM as follows:

- a) Press the ***Function Key** on the door lock.
- b) Program the selected user code assigned in the panel; refer to Door Lock *User Guide*.

The screen displays a series of messages:

“Please press *function key on device”
“Adding Slave Unit:
“Adding to Security Network”

UL	Access control functionality has not been evaluated by UL and may not be used in UL Listed applications.
-----------	--

Honeywell Thermostat

Install Honeywell Thermostat according to the manufacturer's instructions. The device should be mounted in the final location and tested before adding it to the system.

NOTES:

- Honeywell is not responsible for property damages due to improper setting of the thermostat modes.
- If installing another brand of thermostat, follow the instructions in the User Guide for that specific thermostat to include properly into the Z-Wave network.
- If not using a Honeywell thermostat, enrollment procedure may vary. Refer to the thermostat instructions for enrollment procedure.

1. At the Z-Wave thermostat:
 - a) Select **Thermostat**; set Time/Date.
 - b) Follow the instructions in the thermostat Installation Guide for "Z-Wave enrollment".
 - c) To complete inclusion, Click **Done**.
 - d) Click **Exit** to return to normal operation.
2. At the VAM:
 - a) To verify activation, Click the **Back** button and wait 30 seconds. Click the **Refresh** button; the new device is displayed.

The screen displays a series of messages:

"Please press function key on device"
"Adding Controller Unit"
"Adding Slave Unit"
"Device added successfully"

Editing Z-Wave Device Names

To edit a device name, do the following:

1. Go to the Z-Wave Management screen (**Automation > Z-Wave Setup**).
2. Highlight the device name and click the **Z-Wave Edit** button.
3. Enter a new name.
- d) Click **OK**.

Abort a Z-Wave Action

If you inadvertently make a wrong selection, (add, delete, or remove failed device) click the **Abort** button to stop the process.

Removing All Z-Wave Devices

To remove all Z-Wave devices, do the following:

1. Click **Automation > Z-Wave Setup** to display the “Z-Wave Device Management” screen.
2. Click **Z-Wave Default** to delete all devices from the controller.
3. Select **Yes** or **No**. The following message is displayed:

This Z-WAVE controller is about to be factory defaulted and will lose all devices in the enrolled list.




All Z-WAVE devices must be re-enrolled after this reset.

Yes or No

Z-Wave Notes

1. Motorized door lock bolts physically lock and unlock when activated, but if the door lock installed is a non-motorized type, activation allows the door to be manually unlocked without a key. See “Compatible Devices” section for further information.
2. Some thermostats do not update temperature status automatically (i.e., Wayne Dalton).
3. When using a Kwikset Smartcode electronic deadbolt door lock (in a Scene that is programmed to trigger when unlocked) the Scene does not trigger if using a key; enter a user code.

Z-Wave Troubleshooting

PROBLEM	SOLUTION	
Cannot add new device.	Make sure the Z-Wave device is within range of the VAM. You may need to move the device closer to the VAM. Refer to the Z-Wave device Instruction Guide for proper range.	
Device is within proper range but still is not included.	 	<ol style="list-style-type: none"> 1. Go to the Z-Wave Device Management” screen. (Automation > Z-Wave Setup). If the device does not appear on the screen, click the Z-Wave Exclude/Delete button. 2. At the Z-Wave device, Click the Function Key. The screen will display a message “Device Removed”. 3. Include the device again.
Highlighted device will not delete.		When deleting a device, if the selected device remains on the screen, highlight the device name and click the Removed Failed Device button.

Using VAM as a Secondary Controller

VAM can be used as a secondary controller when connected to another Z-Wave network.

1. Remove any Z-Wave devices previously included in VAM.
Click **Automation > Z-Wave Setup** to display the Z-Wave Management screen, then click **Z-Wave Reset** and select **Yes**.
2. Press the Z-Wave Primary button to switch VAM to secondary controller. The Z-Wave Primary icon changes to Z-Wave Secondary accordingly.
3. Start the inclusion process at the other network's primary controller (see controller's manual), then click the **Add Device** button in VAM's Z-Wave Management screen to add (include) VAM to the controller. To remove (exclude) VAM from the primary controller, start the exclusion process at the other network's primary controller, then click the **Remove Device** button in VAM.

Creating Scenes

The system can automatically activate various devices when certain events occur. The programming of these triggers and actions is called Scenes. Up to 10 scenes can be defined.

A scene consists of a trigger, an optional condition, and up to three actions.

Definitions of Trigger, Condition, and Action

Trigger Defines the event that triggers the programmed action(s).

Triggers include the following categories:

Time	Choose the time option the action should begin: Repeated (choose the days of the week) Once (enter the date) Sunrise/Sunset (region must be set) By Clock (set the time the scene should begin)
Security	Choose the security mode upon which the action begins: Disarm (action starts when the system is disarmed) Away (action starts when the system is armed Away mode) Stay (action starts when the system is armed Stay mode) Night (action starts when the system is armed Night mode) Away Secured (action starts after exit delay has expired) Alarm (action starts if an alarm occurs) Enter User Code:
Thermostat	Choose the temperature at which the action begins: Above (set the temperature) Below (set the temperature)
Door	Choose the door status at which the action begins: Locked (action starts when the door is locked) Unlocked (action starts when the door is unlocked) Code Unlocked (action starts when door is unlocked by code)
Zones	Choose the zone condition to cause the action to begin: Restore (for trigger only; not for use with conditions) Alarm (upon an alarm from a specific zone or zones) Fault (upon a fault from a specific zone or zones)

Condition Defines an optional event that adds a condition to the trigger. Conditions include the same categories as triggers, however, conditions cannot be set with the same category as the trigger. (ex., if setting a trigger event for security, you cannot use a security event as a condition).

Action Defines the desired device action(s) when the trigger event occurs.
Actions include the following categories:









Security	Choose the security mode to occur upon the trigger event: Disarm Away Stay Night Enter User Code	NOTE: A valid user code is required for the system to perform any of the actions listed. Enter the code at the prompt. If the user code is later deleted from the security system, you will need to reenter a valid code at this screen.
Thermostat	Choose the thermostat action to occur upon the trigger event: Off Heat Cool Set point Set energy mode (normal/savings)	
Light	Choose the light option to occur upon the trigger event: On/Off On for Time	
Door	Choose the door status to occur upon the trigger event: Unlocks Locks	
E-Mail	If an email message is to be sent upon the trigger event, choose the recipient and enter a custom message. The Configure E-Mail ID's button lets you create email accounts if not previously set up via the Email Setup menu.	

Example: You want the lights to turn on when you arrive back home and disarm the system, but only at night.

Trigger: "when the system disarms:" Set the Trigger to **Security: System Disarm**

Condition: "only at night:" Set the **TIME** condition (enter the **Start Time** and **Duration**)

Action: "Turn the lights ON:" Set the Action to **LIGHT: ON**.

Scene Buttons			
 ADD	 DELETE	 EDIT	 LOG
Condition/Trigger/Action Buttons			
 Add	 Edit	 Delete	 Save





Steps To Create a Scene

1. Go to the Scene Setup menu (**Automation > Scene Setup**).
2. Click **Add**.
3. Click **Scene Name**; enter a name and click **OK**.
4. Assign the desired “Condition,” “Trigger,” and “Action” for this scene. For each category, use the appropriate device drop-down menu to choose the specific device(s).
5. After each selection click **Save**.

Creating Groups & Rooms

Groups and rooms are defined collections of Z-Wave devices that can be used in scenes. A **group** is a defined collection of the same type of Z-Wave devices (only light modules, or only door locks, etc.). When used in a scene and the scene activates, all devices assigned to that group activate.

A **room** is a defined collection of different types of Z-Wave devices (light modules, door locks, thermostat, etc.). When used in a scene and the scene activates, all devices assigned to that “room” activate. (The Room feature might not yet be available.)

Group Setup Buttons			
 Delete	 Edit	 Add	 Save

Steps to Create a Group

1. Click **Automation > Group Setup**.
2. Click the **Add** button and enter a group name > **GO**.
3. Choose the **Group Type** (Binary Light, Door Lock, Thermostat) from the drop-down list.
4. Choose the device(s) to be part of this group from the drop-down list.
Use the edit button to change the name of a group if desired.
5. Click **Save**.

Steps to Create a Room

1. Click **Automation > Room Setup**.
2. Click the **Add** button and enter a room name > **GO**.
3. Select the device(s) to be part of this room from the drop-down list.
4. Click **Save**.

Using the Security System (Security Menu)

You can control your security system using VAM's Security menu, including arming, disarming, and bypassing zones.




Refer to the control panel's user guide for details on specific security system functions.

User Codes

Each user was be assigned a name and 4-digit user code by your installer at the time of installation. To add additional user codes, refer to your security system user guide.

Introduction to Arming and Disarming the System

You can arm your system in one of three arming modes: Away, Stay, and Night. The following table lists the three different arming modes and the results of each.

MODE	NOTES
AWAY 	Use when no one is staying on the premises. When armed in AWAY mode, the system sounds an alarm if a protected door or window is opened, or if any movement is detected inside the premises. IMPORTANT: On certain VISTA-Turbo systems, "Away Auto Stay" mode is shown as "Away" mode (with all zones monitored). However, some interior zones may not be armed.
STAY 	Use when you are staying home, but might expect someone to use the entrance door later. When armed in STAY mode, the system sounds an alarm if a protected door or window is opened, but you may otherwise move freely throughout the premises.
NIGHT 	Use when you are staying home and do not expect anyone to use the entrance door. <i>Your installer may have configured NIGHT Mode differently; have the installer describe the actual settings of this mode.</i>

Steps to Arm the System

Arming the system in any mode is performed in the same way, as described below.

NOTE: Close all perimeter windows and doors before arming and make sure the system is "Ready to Arm." Or, bypass zones you want left open to make the system Ready to Arm.

1. From the "Home" screen, select **SECURITY**.
2. Choose the desired arming mode. You may be prompted to enter your user code.
3. The screen displays the exit delay countdown. When exit delay expires, the screen displays "Armed."

Arming Multiple Partitions

NOTE: Some systems may not have multiple partitions and the “Arm Multi-Partitions” option may not be available. In addition, your code must be authorized to arm multiple partitions.

1. From the “Home” screen, select **Security** and then select **Arm Multi-Partition**.
2. Choose the desired arming mode.
3. Enter the User Code authorized to access other partition(s).
4. Select the partition from the list on the screen, and press **OK**.
5. If desired, select **ALL** to arm all partitions listed.

NOTES:

- A user may have access to some or all of the available partitions.
- If the user code is accepted, the system displays the partitions that the user has access to.

Steps to Disarm the System

IMPORTANT: If you return to your home or business and the main burglary sounder is on, **DO NOT** enter the premises, but call the police from a nearby safe location. If you return to your home or business after an alarm has occurred and the main sounder has shut itself off, the keypad beeps rapidly upon entering, indicating that an alarm has occurred during your absence. **LEAVE IMMEDIATELY and CONTACT THE POLICE** from a nearby safe location.

If armed in **AWAY** mode:

1. When you enter the premises, the Entry Delay Active message appears.
2. Enter your 4-digit user code. The system disarms.

If armed in **STAY** or **NIGHT** mode:







1. Select the **Disarm** button.
2. Enter your 4-digit user code. The system disarms.

Steps to Disarm Multi-Partitions

1. Select **Security**.
2. Choose **Arm Multi-Partition**.
3. Click the **Disarm** button.
4. Enter your 4-digit user code.
5. Highlight the partition(s) to disarm and press **OK**, or press **ALL** to disarm all partitions.

How to Display Faults (Zones)

If the system shows the “Not Ready Fault” message, it means a zone or zones are open (faulted). Zones must be closed or bypassed before you can arm the system.

Distressed Zones Buttons					
 Alarm	 Troubles	 Faults	 Bypass Zones	 Low Battery	 All





To display the open zone(s), do the following:

1. Select **Security**, then click the **SHOW ZONES** button.
2. Click the **DISTRESSED ZONES** button, and then click the **FAULTS** button.
A listing of faulted and/or bypassed zones is displayed. As applicable, take corrective action such as closing a window or door to correct the fault.
3. If the fault cannot be corrected, you may choose to bypass the zone. by selecting the zone then click the **BYPASS SELECTED** button. Refer to the How to Bypass Zones section for more details on bypassing zones.

How to Bypass Zones

The Bypass function is used when you want to arm your system with one or more zones left open. Bypassed zones are unprotected and do not cause an alarm when violated while your system is armed.

- Some systems do not allow you to bypass fire, carbon monoxide or emergency zones. On certain fire control systems, a specified user may be allowed to bypass fire, carbon monoxide and system zones if the user was enabled by your system installer.
- Limits apply as to how many zones can be bypassed at one time. See your installer for these limits.

Show Zones Buttons			
 Show Zones	 Refresh Data	 Bypass Selected	 Distressed Zones

1. Select **SECURITY**.
2. Click the **SHOW ZONES** button.
3. Choose the zone(s) to be bypassed and click the **BYPASS SELECTED** button.
4. Enter your 4-digit user code.

5. Click the **BACK** button to return to the “Arming” screen, and then arm the system in the desired arming mode.

How to Clear Bypassed Zones

A bypassed zone is automatically unbypassed when you disarm the system. If a zone is bypassed, you can manually remove the bypass as follows:

1. Click the **SHOW ZONES** button.
2. Click the **CLEAR BYPASSES** button.
3. Enter your 4-digit user code. The system should now be Ready to Arm.

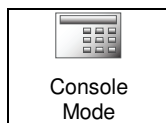
NOTE: If the system is armed and you unbyypass a zone, it disarms the system. If zones are still faulted (not ready) the system will indicate the status as “Not Ready Fault”.

Console Emulation Mode

Console Emulation Mode allows you to use the web browser as a keypad interface just as you would a regular system keypad. All commands shown in Console Emulation mode can also be performed from a standard alpha keypad.

NOTES:

- It is recommended that you **do not** use Console Emulation Mode to enter GOTO commands, because unsatisfactory operation may result.
- Two button panics (1 & *, 3 & #, and * & #) **do not** function in the Console Emulation Mode. The A, B, C, and D buttons do function if programmed as panic keys. Check with your system installer for details.



How to Enter Console Emulation Mode

To start Console Emulation Mode, do the following:

1. From the Home screen, press the **SECURITY** button.
2. Press the **CONSOLE MODE** button.
3. Perform functions as you would from a standard alpha keypad.

Using Total Connect with VAM (Remote Services)

The VISTA Automation Module supports Remote Services for controlling Z-Wave devices and scenes remotely from an associated Total Connect account. Ask your installer if a Total Connect account has been set up for you.

The following describes the related features:

- VAM can be controlled from a smart phone, i-Pad™, Android™ Tablet, Blackberry® or PC using Total Connect and includes webpage support for iOS6 and Google-TV
- Automation scenes can be created in both Total Connect and VAM (Scenes created in Total Connect can be edited only via Total Connect)
- Scenes created in Total Connect can be viewed from either Total Connect or directly from VAM using the Remote selection on the VAM scenes page
- Scenes created in VAM cannot be viewed from Total Connect.

The following table summarizes the relationships between Total Connect scenes and VAM scenes:

Controlling Device	Scenes created in Total Connect		Scenes created in VAM	
	View	Edit Scenes	View	Edit Scenes
Total Connect	yes	yes	no	no
VAM	yes	no	yes	yes

NOTE: For troubleshooting purposes, Total Connect server information (including IP addresses) can be viewed on the **Total Connect Server Setup** screen by clicking the **TC Server** button (see next page).

Controlling Automation (Z-Wave) Devices Remotely

Use Total Connect to control Z-Wave devices: lamp modules (binary switch), dimmer modules (multilevel switch), thermostats, etc., from a smart phone, i-Pad™, Android™ Tablet, Blackberry® or PC.

1. Access the Total Connect account and navigate to the Automation section of the dashboard.
2. Select a displayed device and click the desired action. Refer to the Total Connect online help guide for further details on controlling Z-Wave devices.

Creating Scenes in Total Connect

Use the Automation section of the dashboard in Total Connect to create up to 20 scenes. Refer to the Total Connect Online Help Guide for further details and device limitations for creating an automation scene.

1. Access the Total Connect account and navigate to the Automation module. Click **Create New**. Enter a name for the scene, select an button, and then click on the check boxes for the various device actions desired for that scene. Set the thermostat, if used, to the desired mode and/or temperature for that scene. Click **Save** when done.

NOTE: Scenes created in Total Connect can be edited only from Total Connect.

2. After scenes have been created, follow the Total Connect prompts to synchronize the data with VAM. Syncing is required before scenes created in Total Connect will display in VAM's menus.

Viewing and Controlling Total Connect Scenes from VAM

Use the **Scenes** button to display and control scenes that have been created in Total Connect.

1. From the Main menu, Click the **Automation** and **Scene Setup** buttons, then Click the **Remote** button. The screen displays a list of scenes created in Total Connect.

NOTE: The **Local** button allows you to view a list of scenes created in VAM.

2. To control a Remote scene, select the desired scene, then click the appropriate action (ex. Run).

Enabling Devices for Total Connect

1. From the Main menu, click **Setup > System > TC Server**.
2. Click the **TC Enable** button; the "Z-Wave Device Management for Total Connect" screen is displayed.
3. Select the device that you want to enable/disable in Total Connect.

NOTE: Devices are defaulted to Enable.

4. Click **Save** when done.
5. After devices have been enabled for Total Connect, follow the Total Connect prompts to synchronize the data with VAM. Syncing is required before the enabled devices will display in Total Connect.

NOTES:

1. Device IDs for Z-Wave devices could be different on VAM and Total Connect web pages.
2. On Total Connect, the maximum number of supported devices is 40 switches, 3 thermostats, and 4 door locks.

Total Connect Server Screen for Troubleshooting

The TC Server screen displays the current server information and Z-Wave device status. This information is typically used for IP connection troubleshooting purposes in collaboration with a service technician.

To access Total Connect Server Information and Z-Wave Status from the VAM, do the following:

1. From the Main menu, click the **Setup** button and then click **System**; enter the installer code (if required). Click the **TC SERVER** button.
2. The Total Connect Server Setup screen is displayed with the current Server information and Z-Wave Status (enabled/disabled).

NOTE: These fields are for reference only and cannot be edited.

3. Click the **Connect** button to test the connection to the AlarmNet servers.

System Setup

Use the setup menus to program email notifications, create a remote access login, set the time and date, and connect VAM to a new wireless router.

Email Setup

Email setup allows you to receive email notifications when one or more system events occur. Your installer may have already set up email notifications for you.

NOTE: Email notification requires that you have an active email address.

- An SMTP account needs to be assigned to establish the email server domain (i.e., the “from” address).
- There are four programmable sets of events (labeled “Event 1 – Event 4”).
- Each event 1-4 can send notifications to up to four email addresses (notification messages are pre-defined by the system based on the event).
- For each event 1-4, choose the conditions that will trigger notification:

Event Type	Conditions that Trigger Notification
Security	Disarm, Arm Away, Arm Stay
Zones	Alarms, Troubles, Restores
Thermostat	Temp Above or Temp Below an assigned temperature
Door Lock	Unlocked or Locked

1. Click **Setup** then select **Email**.
2. Click the **User SMTP** button to assign the user’s email server information. This establishes the email server domain (the “from” address).
 - a. Select the email server name (email provider). Choose from GMAIL, OUTLOOK, YAHOO, or Add New.
 - b. Enter the email ID (user name) and password for the chosen email server.
 - c. The Email Server and SMTP port number fields are automatically filled unless “Add new” was selected.
If Add new email server was selected, enter the appropriate SMTP and port number information (see your email provider for details).
 - d. Click **Save**.
3. Click **Event 1** to define the event types and conditions that will trigger notifications to the chosen email address(es).
4. Enter up to four email address(es) to which Event 1 will send notifications.
5. Click **Save**.
6. Repeat steps 3 -5 for Events 2-4 if desired.

Remote Access Log In Setup (Account Setup)

Remote access lets the user access VAM's menus directly via the Internet when away from home. The home router must first be configured for port forwarding. Refer to the router's instructions for details on port forwarding.

You can assign up to five user logins.

To set up a remote access log in, do the following:

1. Click **Setup > Account**.
2. Enter the desired user name and password.
Passwords must be a minimum of 8 alphanumeric characters, and must include at least one uppercase letter, one lowercase letter, and one number.
3. Click **Save**. The new user is displayed.
To clear a user's login, click the **CLEAR** button.

To access VAM remotely, use a web browser and VAM's network IP address to go to the login screen. Enter the assigned user name and password to open the main menu.

NOTE: Remote login is blocked after 3 failed attempts. To reset remote access, you must first connect to VAM locally via the home router, then re-enable remote access. Click **Setup > Account**, then click the appropriate **Enable** button and click **Save**.

Time and Date Setup

VAM can get the time from the control panel, or you can set the time manually. Set the time and date from the **Set Time & Date** screen.

- When the time is set it is stored in the keypad and sent to the control panel when you Click the **Apply** button and answer **Yes** to the following prompt. Additionally, when using the keypad with a residential panel, the panel downloads its time into the keypad once an hour after the clock is set.
- If **Get Time** is clicked, the keypad downloads the time and date from the control panel and exits the Set Time & Date screen.

Steps to Set the Time and Date

1. Click **Setup > System > Time/Date Setup**.
2. Select the Month, Year, Hour, and Minutes using the drop-down menus for each.
3. Select **AM** or **PM** (selection toggles by clicking)
4. Select the desired date format using the **MMDDYY** drop-down menu. Choose 12-hour (select the 12 Hour checkbox) or 24-hour format (uncheck the checkbox).
5. If Daylight Saving Time is used in the installation time zone, click **DST** and set the appropriate start and end DST month, weekend and hour. VAM will automatically adjust the time when Daylight Saving Time starts and ends.
6. Click **Apply** to save the settings.
7. A choice (checkmark = Yes; X = No) to copy the time to the control panel may appear. Choosing "yes" sets the control panel to the time entered in VAM.

Changing the Home Router (Wi-Fi Setup)

To set up the WiFi network for VAM, you will need the following:

- WiFi enabled computer device (Tablet PC, laptop, Smartphone, etc.)
- VAM SSID and WPA2 password (located on the VAM's label)
- VAM default IP address: 192.168.2.1
- Home router SSID and WPA2 password (typically located on the home router's label); home router must use WPA2 encryption and have a password (key) assigned.

1. Connect a WiFi computer device to VAM.

- a. Power up the VAM and reset it to factory settings. Using the Wi-Fi and Factory Default button, press and hold down for more than 5 seconds to reset the WiFi network settings to the original default settings.
- b. Connect the computer to the VAM using the computer's WiFi settings menu (VAM is a wireless access point).

Enter the VAM SSID: **VAM_xxxx**

NOTE: xxxx = the last 4 digits of the MAC address
SSID is case-sensitive

Enter the Key (found on the VAM label "WPA2 pw" line)

2. Access VAM's home screen.

- a. Open a web browser on the computer device.
- b. Go to VAM's default IP address: **192.168.2.1**

3. Connect the VAM to the home router.

- a. From the main menu, click the **Set Home Router** button.
- b. Enter the home router SSID and security key.
(SSID and security key are case-sensitive)
- c. Click **Connect**. A countdown begins and displays "Trying to connect to the Router: xxxx, please stay in this page and wait..."
- d. VAM can take about 2 minutes to connect to the home router. During this time, VAM reboots twice and a new network IP address is assigned to the VAM. When done, VAM automatically connects to the home router.

4. Retrieve and save VAM's network IP address.

- a. Leave the browser page open (minimize, but don't close, if needed).
- b. Reconnect the computer to the VAM using the computer's Wi-Fi settings menu.
- c. When connected to the VAM, return to the open browser page and click the **Show IP Info** link.
- d. The home router's SSID and VAM's new IP address is shown. Note the IP address for future reference.
- e. Keep the **Fixed IP** option unchecked and click the **Save** button (Fixed IP is

intended for network administrators).

- f. At the "...do you want to continue?" prompt, click the checkmark (yes). VAM reboots, then automatically connects to the home router and opens the main menu.
5. **Complete the network setup and bookmark VAM's URL.**
 - a. VAM should now be connected to the home network router.
 - b. Bookmark the URL displayed in the browser's address bar for easy access to VAM later.
 - c. To access VAM's main menu at a later session, simply go to the bookmarked address, or go to the following URL:
<http://VAM.tuxconnect.info> or
<http://vam.mylanconnect.com> (future use)

Options and ECP Address (for Installer use only)

IMPORTANT: The Options menu is intended for the installer only and the settings should not be changed by the user. Changing these settings can disconnect communication between VAM and the control panel and cause system errors.

Software Upgrades

Software upgrades may be available for this product. To ensure you have the latest version, check the version in your system (see System Information below). Software upgrades can be done manually, or you can set VAM to notify you automatically that an upgrade is ready.

System Information

To view the current software version installed on your system, do the following: Click the **Setup** button then click the **System Info** button.

Manual Software Upgrades

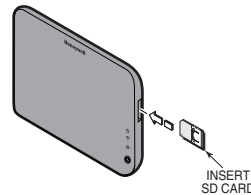
Go to the Toolkit site located at: <http://www.tuxedotouchtoolkit.com/index.html> to download the latest software to an SD card.

1. Copy the software upgrade file to the SD card.
2. Insert the SD card then reset the VAM (use a paper clip to depress the Reset button then release). The yellow Operation LED flashes during the upgrade process.
3. The LEDs show solid green and blue indicating the default/upgrade process is done.

Automatic Software Updates

To receive automatic remote updates, select the **Enable Remote Upgrade** checkbox on the system information screen and install an SD card.

1. Click **Setup > System Info**, then select the **Enable Remote Upgrade** checkbox.
2. Make sure a blank SD card is installed (minimum 200 MB of available space is required).
3. When updates are available, the system will automatically update the system.



Compatible Z-Wave Devices

Z-Wave devices may vary; follow the instructions in the *Users Guide* for your specific device when adding and deleting devices into the Z-Wave network. Refer to the table below for some of the compatible devices.

Door Locks
Yale Real Living Push Button Lever Lock
Yale Real Living Touchscreen Lever Lock
Yale Real Living Push Button Deadbolt Lock
Yale Real Living Touchscreen Deadbolt Lock
Schalge Link Deadbolt Lock
Schlage Link Lever Lock
Kwikset Smartcode Lever lock
Kwikset Smartcode Deadbolt Lock
Thermostats
Honeywell ECC
Wayne Dalton Zwave thermostat
Trane Zwave Thermostat
Appliance
HomeManageable Appliance Module
Wayne Dalton Small Appliance Module
GE Wireless Lighting Control Plug In Appliance Module
Lights
Leviton/ViziaRF+ Switches
Leviton/ViziaRF+ Dimmers
Leviton/ViziaRF+ Plug in Modules
GE Wireless Lighting Control Dimmers
GE Wireless Lighting Control Switches
GE Wireless Lighting Control Plug in Lamp Modules

Not all Z-wave devices have been tested and some features may produce unpredictable results.

NOTES

Wireless Range

This device complies with the Z-Wave® standard of open-air, line of sight transmission distances of 100 feet. Actual performance in a home depends on the number of walls between the controller and the destination device, the type of construction and the number of Z-Wave enabled devices installed in the control network.

Please Note: Z-Wave home control networks are designed to work properly alongside wireless security sensors, Wi-Fi, Bluetooth and other wireless devices. Some 900 MHz wireless devices such as baby cams, wireless video devices and older cordless phones may cause interference and limit Z-Wave functionality.

Things to consider regarding RF range:

- Each wall or obstacle (such as refrigerator, big screen TV, etc.) between the remote and the destination device will reduce the maximum range of 100 feet by approximately 25-30%.
- Brick, tile or concrete walls block more of the RF signal than walls made of wooden studs and drywall.
- Wall mounted Z-Wave devices installed in metal junction boxes will suffer a significant loss of range (approximately 20%) since the metal box blocks a large part of the RF signal.

WARNING: NOT FOR USE WITH MEDICAL OR LIFE SUPPORT EQUIPMENT!

Z-Wave enabled devices should never be used to supply power to, or control the On/Off status or medical and /or life support equipment.

Controlling Devices:

The features and functions that can be controlled vary by manufacturer and you will need to review the user manual that was provided to determine capabilities of each device.

Z-Wave devices are identified by the Z-Wave logo and can be purchased from your local retailer.

Z-Wave® is a registered trademark Sigma Designs, Inc. and/or its subsidiaries.



PLEASE GO TO THE BOTTOM OF
PAGE 35 FOR FCC / IC AGENCY
STATEMENTS.

– NOTES –

– NOTES –

**FEDERAL COMMUNICATIONS COMMISSION (FCC) AND
INDUSTRY CANADA (IC) STATEMENTS**

The user shall not make any changes or modifications to the equipment unless authorized by the Installation Instructions or User's Manual. Unauthorized changes or modifications could void the user's authority to operate the equipment.

FCC CLASS B STATEMENT

This equipment has been tested to FCC requirements and has been found acceptable for use. The FCC requires the following statement for your information:

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 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:

- If using an indoor antenna, have a quality outdoor antenna installed.
- Reorient the receiving antenna until interference is reduced or eliminated.
- Move the radio or television receiver away from the receiver/control.
- Move the antenna leads away from any wire runs to the receiver/control.
- Plug the receiver/control into a different outlet so that it and the radio or television receiver are on different branch circuits.
- Consult the dealer or an experienced radio/TV technician for help.

INDUSTRY CANADA CLASS B STATEMENT

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

FCC / IC STATEMENT

This device complies with Part 15 of the FCC Rules, and RSS 210 of IC. Operation is subject to the following two conditions: (1) This device may not cause harmful interference (2) This device must accept any interference received, including interference that may cause undesired operation.

Cet appareil est conforme à la partie 15 des règles de la FCC & de RSS 210 des Industries Canada. Son fonctionnement est soumis aux conditions suivantes: (1) Cet appareil ne doit pas causer d'interférences nuisibles. (2) Cet appareil doit accepter toute interférence reçue y compris les interférences causant une réception indésirable.



RF EXPOSURE

Warning -- The VAM must be installed to provide a separation distance of at least 7.8 in. (20 cm) from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

Mise en Garde -- Exposition aux Fréquences Radio: L'antenne (s) utilisée pour cet émetteur doit être installée à une distance de séparation d'au moins 7,8 pouces (20 cm) de toutes les personnes.

TWO YEAR LIMITED WARRANTY

Honeywell International Inc., acting through its Security & Communications business ("Seller"), 2 Corporate Center Drive, Melville, New York 11747 warrants its products to be free from defects in materials and workmanship under normal use and service, normal wear and tear excepted, for 24 months from the manufacture date code; provided, however, that in the event the Buyer presents a proper invoice relating to the purchased product and such invoice bears a date later than the manufacture date, then Seller may at its discretion, reflect the warranty period as commencing at invoice date. Except as required by law, this Limited Warranty is only made to Buyer and may not be transferred to any third party. During the applicable warranty period, Seller will repair or replace, at its sole option and as the exclusive remedy hereunder, free of charge, any defective products.

Seller shall have no obligation under this Limited Warranty or otherwise if the product:

- (i) is improperly installed, applied or maintained;
- (ii) installed outside of stated operating parameters, altered or improperly serviced or repaired by anyone other than the Seller/Seller's Authorized Service/Repair Center;
- (iii) damage is caused by outside natural occurrences, such as lightning, power surges, fire, floods, acts of nature, or the like; or
- (iv) defects result from unauthorized modification, misuse, vandalism, alterations of serial numbers, other causes unrelated to defective materials or workmanship, or failures related to batteries of any type used in connection with the products sold hereunder.

Exceptions to Warranty With Respect to Honeywell Products listed below:

Hardwire Contacts and PIRs – Seller warrants parts for hardwire contacts and PIRs in accordance with the terms of the above limited warranty for a period of five (5) years from the manufacture date code.

EXCLUSION OF WARRANTIES, LIMITATION OF LIABILITY

THERE ARE NO WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. TO THE FULLEST EXTENT PERMITTED BY LAW, IN NO CASE SHALL SELLER BE LIABLE TO ANYONE FOR ANY (i) CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR RELATING IN ANY WAY TO THE PRODUCT AND/OR FOR BREACH OF THIS OR ANY OTHER WARRANTY OR CONDITION, EXPRESS OR IMPLIED, OR UPON ANY OTHER BASIS OF LIABILITY WHATSOEVER, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY SELLER'S OWN NEGLIGENCE OR FAULT AND EVEN IF SELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES. Any product description (whether in writing or made orally by Seller or Seller's agents), specifications, samples, models, bulletin, drawings, diagrams, engineering sheets or similar materials used in connection with the Buyer's order are for the sole purpose of identifying the Seller's products and shall not be construed as an express warranty or condition. Any suggestions by Seller or Seller's agents regarding use, applications, or suitability of the products shall not be construed as an express warranty or condition unless confirmed to be such in writing by Seller. Seller does not represent that the products it sells may not be compromised or circumvented; that the products will prevent any personal injury or property loss by burglary, robbery, fire or otherwise, or that the products will in all cases provide adequate warning or protection. Buyer understands that a properly installed and maintained alarm may only reduce the risk of a burglary, robbery or fire without warning, but it is not insurance or a guarantee that such will not occur or will not cause or lead to personal injury or property loss. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON ANY CLAIM AT ALL INCLUDING A CLAIM THE PRODUCT FAILED TO GIVE WARNING. However, if Seller is held liable whether directly or indirectly for any loss or damage with respect to the products it sells, regardless of cause or origin, its maximum liability shall not in any case exceed the purchase price of the product, which shall be fixed as liquidated damages and not as a penalty, and shall be the complete and exclusive remedy against the Seller. Should your product become defective during the warranty, please contact your installer to facilitate repair or replacement with Seller pursuant to the terms hereof. Seller reserves the right to replace any defective product under warranty with new, refurbished, or remanufactured product.



800-15629 12/13 Rev. A Beta 4

Honeywell

2 Corporate Center Drive, Suite 100
P.O. Box 9040, Melville, NY 11747
Copyright © 2013 Honeywell International Inc.
www.honeywell.com/security