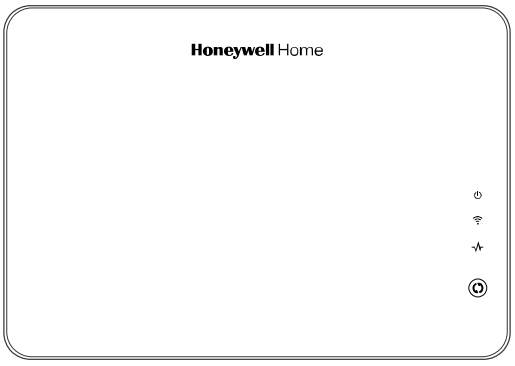
Honeywell Home

VISTA® Automation Module

User Guide



800-15629V3E 10/15 Rev. E

TRADEMARKS

Honeywell is a registered trademark of Honeywell International Inc.
Total Connect is a trademark of Resideo Technologies, Inc.
Windows and Windows Vista are trademarks, or registered trademarks of Microsoft Corporation in the United States and other countries.
Android™ is a trademark of Google Inc.
RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used as trademarks in the U.S., Canada, and countries around the world.
QuickTime® is a registered trademark of Apple Inc., registered in the U.S. and other countries.
iPad® and iPhone® are registered trademarks of Apple Inc.
iTunes® and iTunes Store® are registered trademarks of Apple Inc., registered in the U.S. and other countries.
All other trademarks and service marks are the properties of their respective owners.

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.

USE OF THESE PRODUCTS IN COMBINATION WITH NON-RESIDEO PRODUCTS IN A WIRELESS MESH NETWORK, OR TO ACCESS, MONITOR OR CONTROL DEVICES IN A WIRELESS MESH NETWORK VIA THE INTERNET OR ANOTHER EXTERNAL WIDE AREA NETWORK, MAY REQUIRE A SEPARATE LICENSE FROM SIPCO, LLC. FOR MORE INFORMATION, CONTACT SIPCO, LLC OR IPCO, LLC AT 8215 ROSWELL RD., BUILDING 900, SUITE 950, ATLANTA, GA 303350, OR AT WWW.SIPCOLLC.COM OR WWW.INTUSIQ.COM.

WARNING: Z-WAVE DEVICES 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 of medical and /or life support equipment.

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

The product should not be disposed of with other household waste. Check for the nearest authorized collection centers or authorized recyclers. The correct disposal of end-of-life equipment will help prevent potential negative consequences for the environment and human health.

Any attempt to reverse-engineer this device by decoding proprietary protocols, de-compiling firmware, or any similar actions is strictly prohibited.

TABLE of CONTENTS

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 lights, door locks, water valves, garage door controllers, thermostats, shades and others. VAM does not have a physical keypad interface, but instead is controlled by using a web browser on a Wi-Fi® enabled smart device that is connected to your home Wi-Fi network.

DISPLAY NOTE: For optimum viewing of the screens and menus, the tablet's font size setting may need to be adjusted.

VAM Features

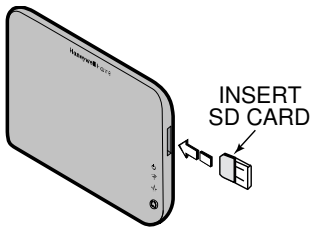
Feature	Description
Wi-Fi® Connection	VAM uses your home Wi-Fi network to communicate with a Wi-Fi enabled device such as a Smartphone, iPad®, Android™ Tablet or laptop PC. Your installer connected the VAM to your Wi-Fi router during installation. However, if you later install a new router, you will need to reconnect the VAM to the new router. Refer to Wi-Fi Network Setup in the System Setup section for details on connecting to a different router.
Home Automation	Control lights, thermostats, door locks, garage doors, water valves, shades 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 remote web enabled device connected to the Internet.
Remote Services	VAM supports remote services so you can control VAM using Resideo's Total Connect™ and Port forwarding.
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.

Wi-Fi has not been evaluated for applications which require agency compliances.

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



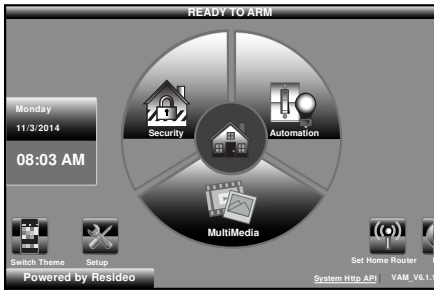
IMPORTANT: Avoid touching the contacts on the SD card.

Navigating the VAM Menus

The VAM is controlled using a web browser on a Wi-Fi enabled smart 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. If not, you can locate VAM by going to:
http://vam.mylanconnect.com.
Navigation begins from the Main menu. Navigate through various sub-menus by pressing the graphical buttons (icons) to perform a selected function.

From the VAM Home Page you gain access to:

- Control your security system
- Control/view your cameras
- Control home automation such as lighting, thermostat, water valves garage door openers, shades and door locks
- Switch from PC view to mobile view by pressing **Switch Theme**.
- Go to advanced setup menus.



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

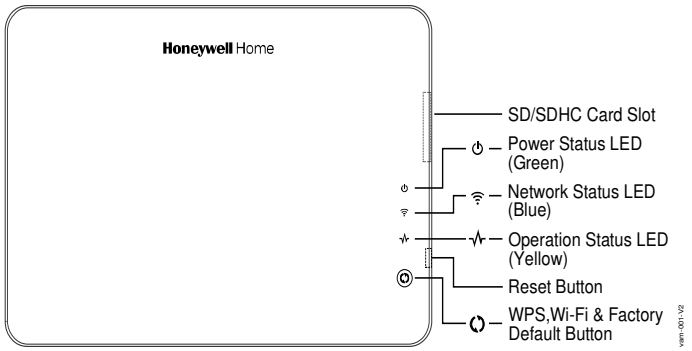
Navigation Icon Descriptions

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 icons are described below.

Icon	Icon Title	Function
	Automation	Used to control and set up 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 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	Exits 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. • Blinking when it is powered up and booting. • Solid green when 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. • In normal operation, the LED blinks when VAM is booting. • Solid blue when VAM is ready as AP mode (acting as an Access Point).
Operation Status (yellow)	In normal operation, the LED is normally off. • It will blink slowly when there is no ECP(including ECP error) or Z-wave controller not responding. • Fast blinking indicates Z-wave is in enrollment or deletion status.
Reset Button	Press to reboot the device.
Wi-Fi and Factory Default Button	The Wi-Fi and Factory reset options utilize the Reset Button to perform the required operation: • **Wi-Fi Network Reset**: Press and hold down for more than 5 seconds to clear the VAM's Wi-Fi network connection. You then need to reconnect the VAM to your 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 to factory defaults. • **WPS Enrollment:** Single press starts the WPS enrollment process.

Using the Security System Menu

You can control your security system using the VAM's Security menu, which includes 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 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 systems *"User Guide."*

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. Contact your installation company for more information.
 **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. *Your installer may have configured NIGHT Mode differently; have the installer describe the actual settings of this mode.*
 **Arm Multi Partition**	Use to arm more than one partition, if you are authorized to do so. Refer to the *"Arming Multiple Partitions"* section for details.
 **Console Mode**	This mode emulates a standard alpha keypad. If desired, you can use this mode to control the security system using standard keypad commands. Refer to the *"Console Emulation Mode"* section for details.
 **Show Zones**	Use to display the zones programmed in your system. From this menu you can view faulted zones (zones not ready to arm) and bypass zones. Refer to the *"How to Bypass Zones"* section for details.

Steps to Arm the System

Arming the system in any mode is performed in the same way.

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.

   Note: If the installer enables the **Quick Arming** feature pressing **Arm Away**/**Night**/**Stay** will not be prompted to enter a user code.
3. The screen displays the exit delay countdown. When exit delay expires, the screen displays *"Armed."*

Arming Multiple Partitions

NOTES:

- Some systems may not have multiple partitions. In addition, your code must be authorized to arm multiple partitions.
- Mobile view cannot be used to arm multiple partitions. Mobile view can control only the partition the VAM was assigned to when installed.

1. From the "Home" screen, press **Security** > **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.

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 valid 4-digit user code. The system disarms.

If armed in STAY or NIGHT mode

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

Steps to Disarm Multi-Partitions

1. Press **Security** > **Arm Multi-Partition > Disarm**.
2. Enter your valid 4-digit user code.
3. 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 Icons

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

1. Press **Security** > **SHOW ZONES.**
2. Press **DISTRESSED ZONES** > **FAULT.**

   A listing of faulted 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 pressing **BYPASS**. 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. Limits apply as to how many zones can be bypassed at one time. See your installer for these limits.

NOTE:

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.

Show Zones Icons

1. Press **SECURITY** > **SHOW ZONES**.
2. Choose the zone(s) to be bypassed and press **BYPASS SELECTED**.
3. Enter your valid 4-digit user code.
4. Press **BACK** to return to the *"Arming"* screen, and then arm the system in the desired arming mode.

How to Clear Bypassed Zones

For some control panels, a bypassed zone is automatically unbypassed when you disarm the system. Ask your installer if this is active for your system.

You can also manually remove the bypass as follows:

1. Press **SHOW ZONES**.
2. Press **CLEAR**.
3. Enter your valid 4-digit user code. The system should now be *"Ready to Arm."*

NOTE: If the system is armed and you unbypass 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 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.
- 2-button panic keys (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 **SECURITY** > **CONSOLE MODE**.
2. Perform functions as you would from a standard alpha keypad.

Setup Menu

Use the setup menus to create local/remote access logins (account icon), set the time and date, Language, User Profile, and connect the VAM to a new wireless router.

Language

The VAM supports 4 languages: English (default), Español, Português, Français. To change from the home screen, press **Settings** > **Language**, select the desired language, and then press **Save**.

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.

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). When an email is transmitted, the VAM will use this email to send the message.
- 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, Away Secured, Arm Stay
Zones	Alarm, Trouble, Restore
Thermostat	Temp Above or Temp Below an assigned temperature
Door Lock	Unlocked or Locked
Garage Door	Opened, Closed or Disabled/Failed
Water Valve	Opened or Closed

- **Current Part**. **Icon**: This is a reminder that email messages are based on actions occurring only in the partition to which the VAM is assigned.

1. Press **Setup** > **Email**.
2. Press **User SMTP** 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 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. Press **Save**.

3. Press **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. Press **Save.**
6. Repeat steps three through five for Events two through four if desired.

NOTES: If sending the e-mail, and it fails a failure notification icon will display on the *"User SMTP"* icon in *"Email Setup."* Verify your SMTP server settings and make sure there are no security protocols that need to be adjusted through your email provider's setup options.

Local/Remote Access Log In Setup (Account Setup)

Local/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. Press **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. Press **Enable local access authentication**, which enables the VAM to require a username and password from an internal LAN (Local Area Network) access.

   NOTE: ***"It is recommended this option is enabled."*** If this option is not enabled any persons with a smart device can access the VAM's webserver by typing in the IP Address.
4. Press **Save**. The new user is displayed.

   To clear a user's login, press **CLEAR**.

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.

NOTES:

- Local or Remote login is blocked after 3 failed attempts. To reset remote access, you must first connect to VAM locally via the home router, and then re-enable remote access. Press **Setup > Account**, then **Enable** for the appropriate user then press **Save**.
- Port 443 is the fixed port assigned to the VAM and cannot be changed. It is a secure login procedure; the URL must begin with HTTPS:// then the external IP address. If not, you may receive an error of *"There is a problem with this devices security certificate."*

Time and Date Setup

The VAM can get the time from the control panel (use **Get Time**), or the time can be set manually.

Set the time and date using the **Set Time & Date** option.

- When the time is set, it is stored in the keypad and sent to the control panel when you press **Apply**. Additionally, the control panel downloads its time into the VAM once an hour after the clock is set.
- If **Get Time** is pressed, the VAM downloads the time and date from the control panel and exits the Set Time & Date screen.
- **Automation Mode only**: The User or Installer can setup the time zone for the VAM manually or choose to synchronize with the internet.

Steps to Set the Time and Date

1. Press **Setup** > **System** > **Time/Date Setup.**
2. Select the **Month**, **Year**, **Hour**, and **Minutes** using the drop-down menus.
3. Select **AM** or **PM** (pressing toggles between AM or PM)
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 your time zone, press **DST** and set the start and end DST month, weekend and hour. VAM automatically adjusts the time when Daylight Saving Time starts and ends.
6. Press **Apply** to save the settings.
7. Select the Region from the **Region** drop-down menu and enter the appropriate ZIP or Postal code.
8. A choice (checkmark = Yes; X = No) to copy the time to the control panel may appear. *"Yes"* sets the control panel to the time entered in the VAM.

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 with the control panel and cause system errors.

User Profile

This page collects the user's data. The page data entries are as follows:

Name	Zip Code	Mobile Number
Region	Device Name	E-mail ID

NOTES:

- This page can be accessed from the home page by pressing **Setup** > **User Profile.**
- The data for Region and Zip Code/Postal Code synchronizes to the Time/Date setup page if completed during the initial setup. The e-mail address synchronizes to the e-mail setup page, if completed during the initial setup.
- The Zip Code option is needed for accessing daylight savings time for your Z-Wave scenes.

Configuring the Wi-Fi Settings

The **Change Wi-Fi Router** option is an alternative method of changing your router, but is recommended only for users with network administration experience. To accomplish this, the following will be needed:

• Wi-Fi enabled smart device (Tablet PC, laptop, Smartphone, etc.)

• Home router SSID and WPA2 password (typically located on the home router's label or assigned by the network administrator); home router must use WPA2 encryption and have a password (key) assigned.

NOTE: Before setting up the network, set your smart device for Wi-Fi operation only (turn off the smart devices "mobile data" option).

IMPORTANT!

The VAM supports only 2.4 GHz – B/G frequencies. If the VAM has problems connecting to the premise's Wi-Fi network check the router settings, verify it is trying to connect to the 2.4 GHz network (not 5 GHz). In addition, trouble connecting to the network can occur if the router's 5 and 2.4 GHz networks have the same SSID (network name).

Wi-Fi Protected Setup (WPS) Enrollment

To use the WPS enrollment you need a router with the WPS enrollment option and an internet connection.

1. Press the WPS button on the router, or Resideo WAP Plus, and verify it is in the enrollment mode (consult the WAP-Plus or router's installation instructions.)
2. Press the button on the VAM.
   a. The blue LED initially flashes three times every other second.
   b. The blue LED will flash slowly when the router and VAM are processing a secure connection.
   c. Once the blue LED is solid, the VAM is connected to the Wi-Fi network.
3. Go to vam.mylanconnect.com to display a list of devices, then select the desired VAM and press **GO**.
4. Navigate through the initial setup process as shown below.

NOTES:

- This process is recommended upon initial power up, or after a default, before accessing the VAM's easy setup mode.
- An internet connection is required for this process.

Manually Changing

1. Connect the smart device to the VAM using the normal process instructed by the installer.
2. Press **Setup** > **Network** > **Change WiFi Router** and Enter the new SSID and Password > **Connect**.
3. Accept the notification *"Are you sure you want to replace your router settings?"* This is a 1-minute process, after which VAM will return to the home screen once a successful connection has occurred. Bookmark this page (or access it through vam.mylanconnect.com).

NOTE: It may be necessary to default the Wi-Fi settings:

4. **Press and hold default/reset** button for more than 5 seconds (The VAM's LEDs blink in various patterns indicating that reboot is in progress. Reboot is complete when the blue and green LEDs light steady.)
5. **Connect Smart Device** to the VAM using the device's Wi-Fi settings menu (At this point the VAM is a wireless access point.)
6. **Enter the VAM's SSID**: **VAM_xxxx** (**NOTE**: xxxx = the last 4 digits of the MAC address [case-sensitive])
7. **Enter the Key** (found on the VAM label "WPA2 pw" line)
8. **Repeat** the connection process above.

Setting a Static Network Address.

1. Press **Setup > Network** to review the current Local Area WiFi Network Connection page to review the ip address. The default option is DHCP
2. Select the **Connection Type as Static IP** and replace the displayed IP address with the recommended network information.
3. At the "Save Success?" prompt, press the checkmark (yes).

Current blue LED is solid, press the button on the VAM:

Blue LED Status	Results
Double Flashing every other second -> Rapid flash -> solid	Connection Successful
Double Flashing every other second -> slow flash -> solid	Connection Failed
Double Flashing every other second -> Rapid flash -> slow flash -> solid	Connection Failed

Current blue LED is slow flash, press the button on the VAM:

Blue LED Status	Results
Double Flashing every other second -> Rapid flash -> solid	Connection Successful
Double Flashing every other second -> slow flash	Connection Failed
Double Flashing every other second -> Rapid flash -> slow flash	Connection Failed

NOTE: See **Appendix A** for troubleshooting.

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 automatically upgrade the software.

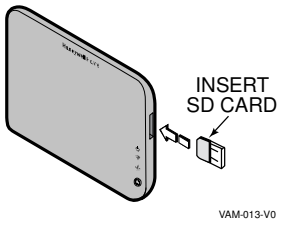
System Information

To view the current software version installed on your system:
Press **Setup** > **System Info**.

Automatic Software Upgrades

To receive automatic remote updates.

1. Make sure a blank SD card is installed (minimum 200 MB of available space is required.
2. When updates are available, the system will automatically update the system.



NOTE:
After a software upgrade, it is recommended that you delete your browser's Temporary Internet Files (cache). Undesired operation may occur if these files are not deleted.

Using Cameras (Multimedia Menu)

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

Camera functionality is supplementary only and has not been evaluated Agency Compliant applications.

Camera Icons


QUAD VIEW


FULL VIEW


PAN/TILT


BACK

Camera Setup Icons


DISCOVERY


ADD


EDIT


DELETE


DELETE ALL


SETTINGS


CAMERA WIFI

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.

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

1. Select **Multimedia.**
2. Images from installed cameras appear. Use the Quad View icon to view up to four cameras on the same screen:
   - Select a quadrant area on the screen (this area is highlighted)
   - Select the camera that you want to appear in that quadrant.
   - For full screen, press **Full View** (located on the lower right of a quad view image). For pan/tilt style cameras, use the Pan/Tilt icon to change the angle of the selected camera.

NOTES:

1. Certain browsers and/or devices may limit the number of cameras that can be viewed.
2. The **Test Camera** feature requires installation of QuickTime® on the smart device. Devices for Android do not currently support QuickTime.

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. Press **Multimedia** > **Camera Setup** to display the "Camera List" screen.
4. Press **Discovery** 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, press **Add** to manually enter. Refer to the cameras installation instructions for this information.

   To edit camera information, highlight the listed camera name and press **Edit**; enter the desired name for the camera. If known, enter the appropriate information (as seen below). Refer to the cameras installation instructions for this information.

• Name	• IP Address	• RTSP Path	• Resolution	• MJPEG Path
• Mobile Path	• HTTP Port #	• RTSP Port #	• Model	• Frame Rate

   NOTE: The camera's frame rate options are 1-30 frames per second, with a recommended rate of 1-8.

6. At this point if you have chosen to leave the camera using the Cat5/6 press **SAVE**.

Setting the Camera's Wi-Fi settings

The "Camera Wi-Fi" option sets the Wi-Fi options in the selected camera or all camera's if Wi-Fi options have changed.

NOTE: This option is only available for camera's that have a hardwired connection to the router, or switch, and are discoverable. The options are:

• SSID	• Security Mode	• N/W Type	• Domain	• Chanel

Once you select the "Security Mode" as WPA Personal or WPA2 personal, the option of "Passphrase/Shared Key" will appear. Enter the required password to connect to the entered SSID.

1. A pop-up window displays **"cam (name) wireless set OK",** if successful. Or, **"cam (name) wireless set Failed".** If successful, the Cat5/6 cable can now be removed from the wireless camera.
2. **Recycle power to the camera**. Once power has been recycled, you can view wirelessly via the VAM's Multimedia menu.

NOTES:

- QuickTime® media player must be installed on the smart device.
- For best performance, set camera resolution to 320 x 240 at 8 frames per second (fps), normal quality.
- Maximum suggest resolution is 640x480 with other options of 160x120 and 320x240.
- Maximum suggested frame rate = 15 fps with other options of 1-8, 10, 15, 20, 25, and 30.
- 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 press **Delete**.
   NOTE: After deleting a camera it cannot be rediscovered until a **Delete All** command is performed.
2. To delete all cameras, press **Delete ALL**.
3. Press **Save**.

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, garage door modules, water valves, shades, 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 the VAM controller's network. Follow the instructions in the Z-Wave device's User Guide.

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 for agency compliant applications.
- Z-Wave applications have not been evaluated for agency compliant applications

Z-Wave Device List Icons

Z-Wave Device Management Icons

Add Device	This icon is for including or adding a new device to the network
Remove Device	This icon is for removing, or excluding, a device from the devices current network (**NOTE**: the device does not have to be on the same network.)
Abort operation	Aborting a **Z-Wave Add Device** or **Remove Device** operation is used to cancel that operation.
Remove Failed	If a device, or node, is no longer operational or will not remove by using the **Remove Device** operation, **Removed Failed** device removes the device from the list.
Edit Name/Icon	Editing the device is for changing the defaulted name to a custom descriptor chosen by the installer or end user (**NOTE**: this is also the location for changing the icons picture of switches.)
Search Device	If a device is no longer functional, this option allows you to press the desired device, press **Search Device** and the VAM scans the network for the device. If successful the device route will be updated. If failed, then the device was not found by the VAM.

Scan Network	Then **Scan Network** operation rebuilds the entire Z-Wave network by taking note of each device and determining the best route for each. This helps improve Z-Wave network performance. Also known as Z-Wave network rediscovery
Z-Wave Reset	The ability to reset the Z-Wave controller without resetting the VAM, it power cycles the internal Z-Wave card.
Z-Wave Default	Press the icon to request a network ID, or remove all the existing devices. (**NOTE**: This does **NOT** remove each device. Once defaulted, you must use the "Remove Device" operation on each device. If this operation is not completed the device cannot be included into the new network.
Primary Controller	This icon will display the current role of the controller. If the device displays a "P" it is the **Primary Controller** and can add and remove devices. If the device displays an "S" it is the **Secondary Controller** and only displays and control devices. Example, if used in conjunction with a Tuxedo Touch™ keypad and experiencing network performance issues, the VAM can be used to extend the network by programming it in as a secondary controller to the Tuxedo Touch's network.
Secondary Controller	

Manually Operating Devices

Devices can be programmed to operate automatically based on scenes you define (refer to the *"Creating Scenes"* section). Or, you can manually control devices from the Device List screen (press **Automation**).

Adding (Include/Add) Z-Wave Devices

Each device must be installed according to the manufacturer's instructions. **Before starting, make sure each device is installed and functioning properly.**

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. **Press** Add Device.
3. At the Z-Wave device, press the appropriate Function key, depending on the type of device being added. Refer to the device installation sections that follow:

Light, Switch or Outlet Devices

i. Perform steps 1 & 2 above.

ii. Be sure the power switch on the device module is **ON**.

iii. Press the **Function Key** on the device.

NOTE: Z-Wave light modules may vary; follow the instructions in the User's Guide for your specific device to include properly.

- If a dimmer module (multi-level switch) was included, three lighting level icons (Low, Mid, High) are displayed.

- If an on/off light/appliance module (binary switch) was included, an On/Off icon (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 and Garage Door Control Devices (Entry Controller)

IMPORTANT!

Be sure the door lock orientation/handedness is correct before including the lock into the system.

NOTE: The VAM **cannot** synchronize panel users to the lock.

Door locking devices may vary; follow the instructions in the devices *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.

Include a door lock device into VAM as follows:

i. Perform steps 1 & 2 above.

ii. Press the **Function Key** on the door lock.

The screen displays a series of messages:

"**Please press function key on device**"
"Adding Slave Unit"
"Adding to Security Network"

Do not use any garage door automation with any garage door opener that lacks the safety features required by U.S. federal safety standards (this includes any garage door opener model manufactured before January 1, 1993). A garage door opener that cannot detect an object and stop and reverse the door – does not meet current U.S. federal safety standards. Your garage door opener also must signal before unattended door operation. For more information please consult your garage door opener manual.

Access control functionality has not been evaluated and may not be used in agency compliant applications.

Resideo Thermostat

Have a professional HVAC contractor install the Resideo 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:

- Resideo is not responsible for property damages due to improper setting of the thermostat modes, or improper wiring if not installed by a qualified technician.
- 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 Resideo thermostat, enrollment procedure may vary. Refer to the thermostat instructions for enrollment procedure.

i. Perform steps 1 & 2 above.

ii.. 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, press **Done**.

d) Press **Exit** to return to normal operation.

iii. At the VAM:

a) To verify activation, press **Back** and wait 30 seconds. Press **Refresh** and 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"

Z-Wave Water Valves

Have a professional plumber install the Z-Wave water valve the device should be mounted in the final location and tested before adding it to the system.

NOTE: Resideo is not responsible for property damages due to improper installation of the water valve.

i. Perform steps 1 & 2 above.

ii.. At the Z-Wave water valve press the function key to enroll

iii. At the VAM: The screen displays a series of messages:

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

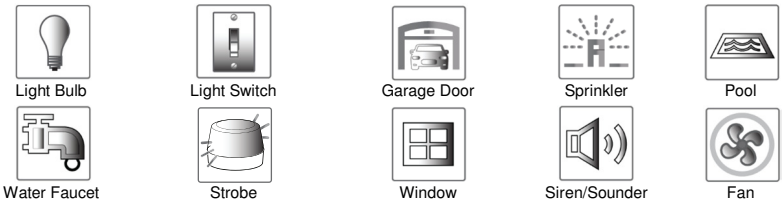
iv. To verify activation, press **Back** and wait 30 seconds. Press **Refresh** and the new device is displayed.

Editing Z-Wave Device Names and Icons

You can change the name of a device by using **Edit Name**:

Press **Automation** > **Z-Wave Setup** > Choose Device > **Edit Name** > Enter New Name > **OK.**

To display a different icon select the icon from the list below (**NOTE**: This only applies to binary and multilevel switches):



Abort a Z-Wave Action

If you inadvertently make a wrong selection, (**Add Device** or **Delete Device**) press **Abort** to stop the process.

Defaulting the Z-Wave Network

To default and remove all Z-Wave devices, press **Automation** > **Z-Wave Setup** > **Z-Wave Default** > **Yes**. 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. Each device will have to be excluded before it can be re-enrolled'
Yes or **No**

NOTE:

This defaults the Z-Wave network on the VAM and creates a new network ID; removes Z-Wave devices from the VAM only. This does not exclude devices from the network. Each device will need to be individually excluded before it can be re-included into the newly created network (or if the device is to be used on a different locations network).

Using VAM as a Secondary Controller

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

NOTE: If the VAM is configured as secondary controller, it cannot be used with Total Connect Remote Services.

1. Remove any Z-Wave devices previously included in VAM.

   Press **Automation** > **Z-Wave Setup** > **Z-Wave Default** > **Yes.**
2. Press **Z-Wave Primary Controller** (located on the bottom right of the Z-Wave Management screen) to switch VAM to secondary controller. The Z-Wave Primary icon (P) changes to Z-Wave Secondary icon (S) accordingly.
3. Start the inclusion process at the other network's primary controller (see controller's manual), then press **Add Device** 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 press **Remove Device** on the VAM.

NOTE: This action will automatically change the VAM back to a Primary Controller.

Z-Wave Advanced Setup (for Installer use only)

IMPORTANT!
The Z-Wave Advanced Setup menu is intended for the installer only and the settings should not be changed by the user. Changing these settings can cause system errors.

Z-Wave System 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.
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) some models will not trigger the scene if using a key, you must enter a user code.

NOTE ***"IF SYSTEM DEFAULT IS PERFORMED:"*** If the VAM is reset to factory defaults, all Z-Wave devices must be re-included into the system, even if they appear on the Device List. Remove all Z-Wave devices first, then re-include all desired devices (see Adding Z-Wave Devices section).

Z-Wave Troubleshooting

Problem	Solution
Cannot add new device.	Make sure the Z-Wave device is within range of the VAM. 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.	  1. Go to the Z-Wave Device Management screen. (**Automation** > **Z-Wave Setup**) If the device does not appear on the screen, press **Remove Device**. 2. At the Z-Wave device, press 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 press **Remove Device**.

Controlling Devices

The features and functions, which are controllable, vary by manufacturer. Refer to the user manual that is provided with the device to determine the limits of their capabilities.

Compatible Z-Wave Devices

Z-Wave devices may vary; follow the instructions in the *User's Guide* for your specific device when adding and deleting devices into the Z-Wave network.

Visit https://mywebtech.honeywellhome.com/ for a complete list of compatible Z-Wave devices. Refer to the document titled **"Z-Wave Compatibility Chart."**

NOTE: The listed companies in the document referenced online may manufacturer multiple Z-Wave devices. Installing 'like' modules not included on this list may produce unpredictable results.

Wireless Range for Z-Wave Devices

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.

NOTE: Z-Wave home control networks are designed to work properly alongside wireless security sensors, Wi-Fi, Bluetooth and other wireless devices. Some 900MHz wireless devices such as baby cameras, 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.

Defining Scenes

Z-Wave devices can automatically activate various devices when certain events occur. The programming of these triggers and actions are called Scenes and a total of 10 scenes can be defined.

A scene consists of a trigger, an optional condition, and up to five 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, which causes the action to 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, which causes the action to begin: • **Disarm** (action starts when the system is disarmed) • **Away** (action starts when system is armed Away mode) • **Stay** (action starts when system is armed Stay mode) • **Night** (action starts when system is armed Instant or Night mode) • **Away Secured** (action starts after exit delay expires) • **Alarm** (action starts on any alarm condition)
Thermostat	Choose the temperature, which causes the action to begin: • **Above** (set the temperature) • **Below** (set the temperature)
Door	Choose the door status, which causes the action to begin: • **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 manual code entry)
Zones	Choose the zone condition, which causes 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)
Garage Door	Choose the garage doors condition, which causes the action to begin: • **Opened** (action starts when door the status of the door changes to open) • **Closed** (action starts when door status of the door changes to close)
Water Valve	Choose the valves position, which causes the action to begin: • **Opened** (action starts when valve opening is finished.) • **Closed** (action starts when valve closing is finished)

Condition Defines an optional event that adds a condition to the trigger. If a condition is set, the condition must exist at the time of the trigger, in order for the action to occur. 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 mode to occur upon the triggering event: **Disarm** **Away** **Stay** **Night (arms Instant)** **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 action to occur upon the triggering event: **Off** **Heat** **Cool** **Set point** Set energy mode (normal/savings); if savings selected, see your local programming of the thermostat for settings.
Light	Choose the light option to occur upon the triggering event: **On/Off** **On for Time**
Door	Choose the door action to occur upon the triggering event: **Unlock** **Lock**
E-mail	Select the email recipient to have a custom message sent to, based on the triggered event.
Garage Door	Choose the door action to occur upon the triggering event: **Open** **Close**
Water Valve	Choose the valve action to occur upon the triggering event: **Open** **Close**

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:" Press **Trigger** > **Security** > **System Disarm.**

Condition: "Only at night:" Press **Condition** > **TIME** > **Start Time** > **Sunset** > **BY CLOCK** (continue pressing until **SUNSET** is displayed**.** Repeat the same for the end time and set as **SUNRISE.**)

Action: "Turn the lights ON**:"** Press **ACTION** > choose the light or group from the drop down options > **LIGHT** > **ON.**

Scene Icons			Condition/Trigger/Action Icons		
					
ADD	DELETE	EDIT	ADD	EDIT	DELETE

Steps To Create a Scene

Press **Automation** > **Scene Setup** > **Add** > **Scene Name** > enter a name > **OK** > **Save**.

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).

Creating Groups & Rooms

Groups and rooms are defined collections of Z-Wave devices that can be used to organize and activate using a scene.

A **Group** is a defined collection of the same type of Z-Wave devices (only light modules, 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.). Defining rooms can help organize your devices to make it easier to locate specific devices you may wish to control.

Group Setup Icons			
			
Delete	Edit	Add	Save

Steps to Create a Group

1. Press **Automation** > **Group Setup**  .
2. Press **Add** > enter a group name > **Back**.
3. Choose the **Group Type** (Binary Switches, Dimmer Lights, Door Locks, Shades, Thermostats, Garage Doors, Water Valves, and Others) from the drop-down list.
4. Choose the device(s) to be part of this group.
   Use the edit icon to change the name of a group if desired.
5. Press **Save**.

Steps to Create a Room

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

Using Total Connect with VAM (Remote Services)

The VAM supports Remote Services for controlling Z-Wave devices and scenes remotely from an associated Resideo Total Connect account. Ask your installer if a Total Connect account has been set up for you.
The following describes the related features:

- The VAM can be controlled from a smart phone, iPad®, 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 the VAM
- Scenes created in Total Connect can be viewed from either Total Connect or directly from the 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 pressing **TC Server** (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, garage door modules, water valves, etc., from a smart phone, iPad®, 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 press 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. Press **Create New** > enter a name for the scene > **Select a Device** > press 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. Press **Save** when done.
2. After scenes have been created, follow the Total Connect prompts to synchronize the data with the VAM. Initiating a *"Panel Sync"* is required before scenes created in Total Connect will display in the VAM's menus.

Viewing and Controlling Total Connect Scenes from VAM

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

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

   NOTES:

   - The **Local** icon allows you to view a list of scenes created in VAM.
   - Scenes created in Total Connect can be edited only via Total Connect.

2. To control a Remote scene, press or click the desired scene > press the appropriate action (ex. Run).

Enabling Devices for Total Connect

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

   NOTE: Devices are defaulted to *"Enable."*
4. Press **Save** when done.

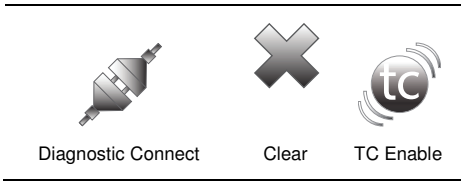
After devices have been enabled for Total Connect, follow the Total Connect prompts to synchronize the data with VAM. Syncing is required before the enabled devices will display in Total Connect.

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 press **Setup** > **System** > **TC SERVER**.

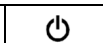
The Total Connect Server Setup screen is displayed with the current Server information and Z-Wave Status (enabled/disabled).

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

Press **Diagnostic Connect** to test the connection to the AlarmNet servers.

Appendix A

LED Status and Troubleshooting

	LED Indication (Green)	(Blue)	(Yellow)	Notes
Normal Operation				Boot Process, **VAM is inaccessible**
				**Slow Flashing**: Final Boot Process, VAM is inaccessible
				**Ready to Use**
				**Fast Flash:** Z-Wave is in the inclusion or exclusion process
				**All 3 LED's will scroll from top to bottom.** The VAM is currently in the default process
Trouble Shooting				**Slow Flashing:** a. Loss of ECP communication with the Security Panel (Check wiring and ECP Addressing) b. Internal Z-Wave module absent or loose from the slot
				**Slow Flashing:** a. Connecting to the Router b. Disconnected from the router (ex. Out of range, router power down, interference etc)
				**All Flashing in Unison:** Failed to configure the WiFi router (verify SSID/password, router has no internet connection if DHCP used, incorrect ip address if using Static)
				**Triple Flashing every other second:** WPS enrollment mode. The VAM is attempting to contact a router in a WPS enrollment state. **See page 6 for more information on the LED indicators.**

Legend		= Solid		= Flash
		= Solid		= Flash
		= Solid		= Flash

Appendix B

FEDERAL COMMUNICATIONS COMMISSION (FCC) AND ISED 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.

ISED 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 / ISED STATEMENT

This device complies with Part 15 of the FCC Rules, and ISED's license-exempt RSSs . 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 et exempt de licence RSS ISED . 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.

Responsible Party / Issuer of Supplier's Declaration of Conformity: Ademco Inc., a subsidiary of Resideo Technologies, Inc., 2 Corporate Center Drive., Melville, NY 11747, Ph: 516-577-2000

Partie responsable / Émetteur de la déclaration de conformité du fournisseur : Ademco Inc., une filiale de Resideo Technologies, Inc., 2 Corporate Center Drive., Melville, NY 11747, Tél. 516 577-2000

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 and ISED 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 20 cm (7,8 pouces) de toutes les personnes et ne pas être située(s) ni fonctionner parallèlement à tout autre transmetteur ou antenne, excepté en conformité avec les procédures de produit multi transmetteur FCC et ISEDs.

DECLARACIÓN IFETEL

La operación de este equipo está sujeta a las siguientes dos condiciones

1. Es posible que este equipo o dispositivo no cause interferencia perjudicial y
2. Este equipo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

DECLARACIÓN ANATEL

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

TWO YEAR LIMITED WARRANTY

Resideo Technologies Inc., is the company behind and the manufacturer of this product ("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 Resideo manufactured 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 Dealer 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.

resideo
www.resideo.com

Resideo Technologies, Inc
2 Corporate Center Drive, Suite 100
P.O. Box 9040, Melville, NY 11747

800-15629V3E 10/15 Rev E