Lyric™ Gateway

Honeywell
THE POWER OF **CONNECTED**

User Reference Guide

Ref: LCP300-L/LCP300-LC

800-21670 10/16 Rev B

IMPORTANT!
PROPER INTRUSION PROTECTION

For proper intrusion coverage, sensor should be located at every possible point of entry to a home or commercial premises. This would include any skylights that may be present, and the upper windows in a multi-level building.

In addition, we recommend that radio backup be used in a security system so that alarm signals can still be sent to the Central Monitoring Stations in the event that the internet connection is interrupted or not working correctly (alarm signals are normally sent over the Wi-Fi and internet network.

EARLY WARNING FIRE DETECTION

Early warning fire detection is important in a home. Smoke and heat detectors have played a key role in reducing fire deaths in the United
States. With regard to the number and placement of smoke/heat detectors, we subscribe to the recommendations contained in the National Fire Protection Association's National Fire Alarm Code (NFPA 72). These recommendations can be found on page 57 of this manual.

System Compatibility Notice

Your Honeywell security system is designed for use with devices manufactured or approved by Honeywell for use with your security system. Your Honeywell security system is not designed for use with any device that may be attached to your security system's control or other communicating bus if Honeywell has not approved such device for use with your security system. Use of any such unauthorized device may cause damage or compromise the performance of your security system and affect the validity of your Honeywell limited warranty. When you purchase devices that have been manufactured or approved by Honeywell, you acquire the assurance that these devices have been thoroughly tested to ensure optimum performance when used with your Honeywell security system.

Lyric™ Lock

Your system supports advanced features designed to keep it functioning optimally. These capabilities include: the ability to interact with Honeywell and your dealer's network for the setup and programming of its features, support for remote software updates and the ability (when enabled by your monitoring dealer) to enhance your security by preventing an unauthorized takeover of the system by another monitoring company. In the event that your dealer has enabled the feature to prevent an unauthorized takeover and you wish to authorize a new company to take over your system, you may request that Honeywell remotely disable this feature. Honeywell will require documentation that you have attempted to contact your existing security dealer and that they have failed to respond, or failed to agree to your request.

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

TABLE OF CONTENTS

Overview

The Lyric™ Gateway combines a security system and home automation with flexibility to operate your system locally using Wi-Fi® connection or remotely over the internet using mobile (smart) devices and easy to use Apps.

Your system can include wireless sensors to provide burglary protection and smoke and combustion detectors to provide early fire and carbon monoxide (CO) warnings (if installed).

Your Gateway system monitors sensors and system status to initiate alarms and generate alerts. The system can also send alarm and status messages to a central monitoring station via the cellular phone network or the Internet, if programmed to do so.

Convenient methods of operating the Gateway include the following:

- The Gateway's touchpad
- Your **Total Connect™ Remote Services** account (for local and remote access)
- The **MyHome™ Gateway** App (for local access)
- Optional wireless keys (key fobs), Lyric keypads and smart devices.

Download and install the free **MyHome Gateway**™ and **Total Connect**™ Apps from your smart device's App Store.

NOTE: The **MyHome Gateway** App requires connection to the Gateway via the premise's Wi-Fi® router (Ethernet cable or Wi-Fi). The **Total Connect** App requires internet or cellular connection for remote access to the Gateway.

Note for Android Mobile Device Users: Before using the MyHome Gateway App, disable Power Saving mode on your device. Failure to do so may cause the app to lose connection to the Gateway if the mobile device enters power save mode.

About This Guide

Throughout the User Reference Guide, icons help you easily identify which control options are available for different system features:

This icon	Means, you can operate the feature…
	from the Gateway touchpad.
	locally from your smart device using the **MyHome Gateway** App.
	locally or remotely from your computer or smart device using your **Total Connect Remote Services** account. For smart devices, download the **Total Connect** App.
	Using optional wireless keys (key fobs), Lyric keypads, or smart devices

In the Operating your Gateway with the MyHome Gateway App section, various menu commands are also listed for operating different system features. For example, if you see:

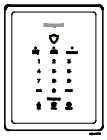
Home > Security > Tools > Users

This means: From the **MyHome Gateway** App **Home** screen, select **Security**.
From the Security menu, select **Tools**.
From the Tools menu, select **Users**.

Note that the illustrations in this document may differ slightly from your system.

Basic System Functions

Security



	Press	
Arm in Home mode	ARMED Home	and enter your user code
Arm in Away mode	ARMED Away	and enter your user code
Disarm system & **silence** alarms	Disarmed	and enter your user code; repeat to silence alarms/alerts
Emergency	Emergency	Then press:
	Fire / Police or Medical	notifies the monitoring company of the emergency type (if programmed to do so)

	Press	
Access Security features		on the Home screen
Arm in Away mode		and enter your user code
Arm in Home mode		and enter your user code
Disarm system & **silence** alarms		and enter your user code; repeat to silence alarms/alerts
Emergency (Panic) [Not available from the MyHome Gateway App]		Use the Gateway Touchpad **Emergency** options or, if programmed to do so, use your wireless key (key fob) to signal an emergency.

Video

Press on the Home screen to view and configure Wi-Fi cameras

Control Panel Settings

Press (Settings) on the Home screen

Gateway key brightness	Select **Brightness** and use the slider
Gateway volume	Select **Panel Volume** and use the slider
Voice announcements volume	Select or deselect **PANEL VOICE**
Chime volume (count-down beeps, other sounds)	Select or deselect **CHIME**

Automation Features

	Press
Operate & manage Z-Wave® devices	on the Home screen
Create & manage Smart Scenes	on the Home screen

Common Master User Functions

	Press
	(Security) then , (Tools) and enter your **Master User** code.
Add, delete or modify user codes	(Users)
View a list of System Events	(Events)
System tests	(Advanced) and select Walk Test or Comm. Test
View a list of mobile (smart) devices paired to your Gateway	(Paired Devices)
Network (Wi-Fi) Configuration	(Network Config)
Edit Chime Sounds	(Edit Chime)

False Alarm Prevention

Many false alarms are caused by minor problems, such as a door or window left open when exiting the home. Gateway includes several features to help prevent false alarms. Note that some are optional or must be programmed by the installer. Disabling these features may increase security, but may also increase the chance of false alarms.

Your installer can help you decide how to use and customize these features. A brief explanation of false alarm prevention features follows, along with advice on what to do if false alarms occur.

Exit/Entry Delays	Programmed delay times allow you to leave after arming the system or disarm it after entering without setting off an alarm. Exceeding a delay period causes an alarm. After a false alarm, disarm the system and contact your monitoring company. They will verify your security code or password, preventing unnecessary calls for emergency response.
Entry Delay	When the system is armed, Entry Delay is the time period allowed to disarm the system with a user code after an entry door is opened. Failure to disarm the system during the Entry Delay causes an alarm. *The delay period is set by your installer.*
Exit Delay	When arming the system, the Exit Delay period begins, allowing household members to exit through entry/exit doors without triggering an alarm. Entry/exit doors must be closed before the exit delay ends. *The delay period is set by your installer.*
Exit Time Restart	If you leave the premises and enter again before the exit delay has expired, the exit delay restarts, giving you more time to leave without causing an alarm. With 10 seconds left to exit, the Gateway begins beeping quickly, indicating that an alarm will occur if you don't exit or disarm the system immediately.
Exit Delay Restart/Reset	If this occurs, disarm the system and arm it again when you are ready to leave. You can restart the Exit Delay by pressing **Restart Timer** on the **MyHome Gateway** App screen.
Alarm Reporting Delay	Gateway is programmed to wait for a brief period between sounding a burglary alarm on the premises and sending an alarm message to your monitoring company. This delay allows you to disarm the system before an alarm message is sent in error.
Exit Alarms	False alarms can be caused by leaving the house and forgetting to close the door. If this happens, Gateway sounds an alarm and displays an Exit Error. The alarm reporting delay gives you time to disarm the system before an alarm message is sent.
Silent Exit	Press **Silent Exit** on the **MyHome Gateway** App screen to mute the beeping sound for exit countdowns in most situations. Voice confirmation of arming status is not muted. Silent Exit doubles the Exit Delay time.
Quick Exit	Press **Quick Exit** on the **MyHome Gateway** App screen when the system has been armed and someone needs to leave the premises. This restarts the exit delay, allowing you to exit the premises without having to disarm and re-arm the system.

Security Features

NOTES:
- For the Gateway to report alarms over the internet, your Wi-Fi network MUST have power at all times.
- You must arm your security system in order for it to sound alarms.

Sensors and Zones

Your system's sensors are assigned to numbered zones that correspond to areas of your home. For example, the sensor on an entry/exit door might be assigned to Zone 03, a device in a bedroom to Zone 06, and so on.

When alarms or trouble conditions occur, you can find information about the zone number and a description of the sensor involved using the MyHome Gateway App. [Home > Security > Tools . Master User Code > Events]

Fire Protection

Fire protection is always active when the system is operating normally. An alarm sounds if a fire condition is detected. See the Fire/CO Alarm System section for important information about fire protection, smoke detectors and planning emergency exit routes.

Carbon Monoxide

Carbon monoxide (CO) detectors, if installed, are always active and sound an alarm if a carbon monoxide condition is detected. See the Fire/CO Alarm System section for more information.

Burglary Protection

Gateway provides HOME and AWAY burglary protection.

HOME mode protects windows and exterior doors, allowing you to move around inside your home without setting off an alarm. (This mode may be referred to As STAY mode in Total Connect.)

AWAY mode protects the entire premises, including interior motion detectors, if present.

Both modes offer an entry delay period that allows you to reenter the home without setting off an alarm. For long periods such as vacations, the entry delay can be turned off while arming the system.

Gateway also allows you to **Bypass** selected sensors before arming the system.

The system also features **Chime** mode, which can alert you to the opening of protected doors and windows while the system is disarmed.

Alarms

When there is an Alarm, the system's sounders turn on: Internal sounders on the **Gateway Touchpad** and any smart devices running the **MyHome Gateway** App; also any external sirens (if used).

The Gateway Touchpad's status shield and **Alert** blink red. If open, the MyHome Gateway App screen indicates **Alarm** and shows the zone(s) where the alarm has occurred.

After 15 seconds, the sounder stops temporarily and the system begins voice announcements of relevant zone information. After the zones are announced, the system's sounder resumes sounding. Alarm sounds and voice announcements alternate until the system is disarmed or until alarm bell timeout occurs.

If the system is connected to central monitoring, an alarm message is sent.

To silence the sounder, disarm the system. The zone(s) causing the alarm remain displayed on the MyHome Gateway App screen, indicating *Memory Of Alarm is held in memory*. See Clearing Alarms for more about clearing memory of alarm.

Security (User) Codes

A user code is required when arming or disarming and for some other functions.

When the system is installed, you are asked to choose a personal 4-digit security code, known as the "Master User code".

Other users can be added, typically with less control over the system than the Master User. See Users and Security Codes.

User Code Error (Touchpad Lockout)	The system locks out user code entries for 15 minutes if six invalid codes are attempted (24 keystrokes without a valid user code detected). Additional code entry attempts will not be accepted until the lock out period ends. **NOTE**: The system can be Quick Armed while in Lockout mode, but cannot be disarmed.
Audio Alarm Verification	Allows your central monitoring station to listen to or talk with individual(s) on the premises (if programmed to do so).

Getting Started

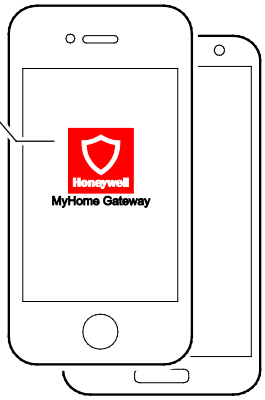
Your installer will have set up your system and helped you install the **MyHome Gateway**™ App on at least one mobile (smart) device. Up to 8 mobile devices can be used to manage your System Security, Automation, Smart Scenes, Video and Settings. Each mobile device you want to use to manage your system with the MyHome Gateway App must be added to the system.

Adding (enrolling) mobile devices in your system

1. Download the Honeywell **MyHome Gateway** App to the mobile device(s) that will be used to control your system.

MyHome Gateway App
Gateway and device must be on the same Wi-Fi network

This free App lets you operate your Security, Video and Automation Functions; Change system settings; add mobile devices and Z-Wave® components



2. Ensure each smart device is connected to the same local Wi-Fi network as the Gateway (check Settings > Wi-Fi on the device).
3. Launch the **MyHome Gateway** App on a device.
4. Enter your **Master user code** then **2 1** on the **Gateway** Touchpad.
5. The App displays a six-digit "Pairing key" number. Enter that number on the **Gateway** Touchpad.
6. When prompted, enter a valid user code on the **MyHome Gateway** App screen to complete the enrollment. The screen confirms the enrollment success and opens the App **Home** screen.

Refer to the Operating your Gateway with the MyHome Gateway App section in this User Reference Guide to operate your system with the **MyHome Gateway** App.

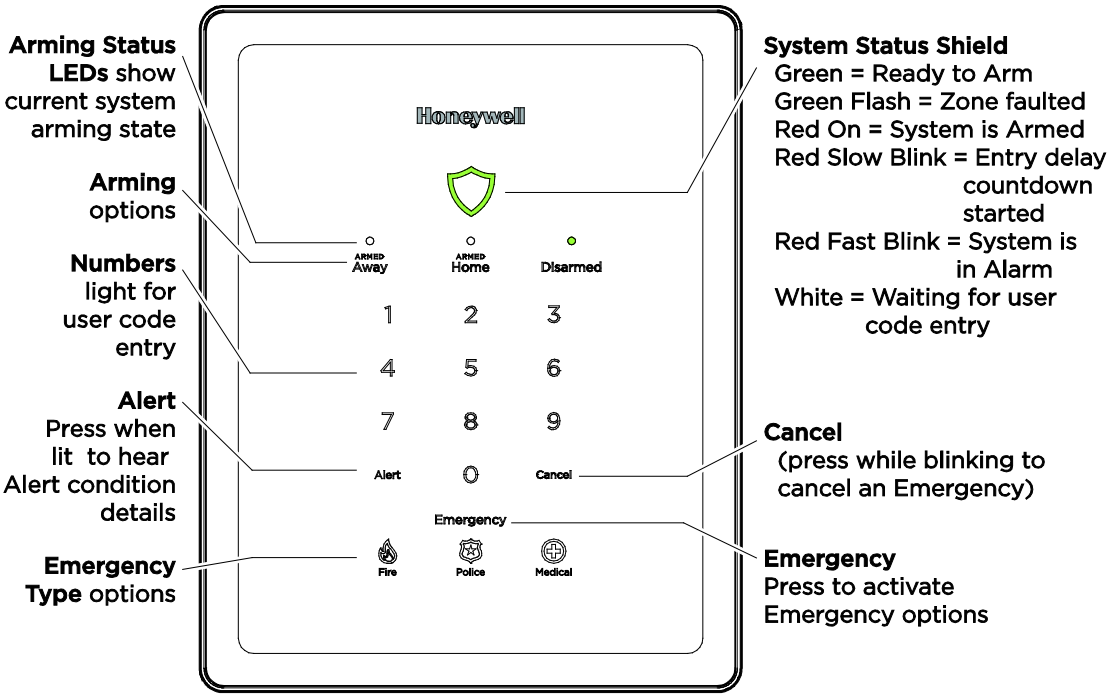
Gateway Menu Modes

The Gateway provides a Menu Mode with options to add and delete smart devices from your system or change the system Wi-Fi network.

Access the Menu Mode when the System is disarmed and the numbers are off. Enter the **Master user code then the two-digit code** for the desired mode option:

Enter Code...	To...
1 1	hear the list of available menu mode options.
2 0	delete all enrolled MyHome Gateway App devices from your Gateway. NOTE: You will need to re-enroll any devices you want to use to operate your Gateway with the MyHome Gateway App.
2 1	enroll or re-enroll devices with the MyHome Gateway App in your Gateway
3 1	Enters the Gateway in Access Point mode; used to change your Wi-Fi setup if your network connection/router changes. See Manually Configure Access Point in Wi-FI (Network) Configuration section for details.
4 1	Enter the Gateway in WPS enrollment mode; used to change or set your Wi-Fi network connections/router to a router that supports WPS. Enter the **Master User code** then **4 1** on the Gateway touchpad, then press the WPS button on the router. The Gateway announces when the connection is complete.

Operating your system using the Gateway Touchpad



The Gateway Touchpad is designed to operate your basic security features. It also lets you quickly see your system status by which items on the Touchpad are lit.

The Status Shield and arming options are always lit and color coded to show system status at a glance. Emergency is also always lit, so it is easy to find, when needed. The other options on the touchpad light only when needed.

System Status Shield

The Status Shield indicates system status with these behaviors:

	Green, steady	System is ready to be armed
	Green Flash	A zone is faulted
	Red, steady	System is armed
	Red, blinking slowly	Entry delay countdown started; enter your user code to disarm the system
	Red, blinking rapidly	System is in Alarm If programmed to do so, two-way Voice Communication may be active when the system is in Alarm. [See your installer to program this feature.]
	White, steady	System is waiting for a user code

See the Emergency section for information on silent alarms.

System Alert

If the system experiences a condition such as AC power loss, connectivity or a communication problem, the **Alert** blinks.

Press **Alert** and the Gateway announces the system Alert condition and suggested actions.

NOTE: If the Gateway loses AC power, **Alert** begins to blink slowly after 15 minutes on battery backup and all other lights on the Gateway are off. In this situation, although the Emergency light is off, **Emergency** functions remain available.

System Sounds

If you hear…	It means…
Beeping	The Gateway touchpad is being pressed to enter codes or other functions, an entry/exit delay is in process, or a trouble condition exists (for example, a low battery condition).
Announcements or Chime	A system condition exists, or a zone has been faulted.
System sounders or sirens	The system is in Alarm. Alarm volume is **not** adjustable.

NOTES:
- The system volume for voice announcements, chimes and most sounds is adjustable through the **MyHome Gateway**™ App
- A beep every 45 seconds indicates one of your wireless devices has a low battery condition. Use the **MyHome Gateway** App to see which device(s) need new batteries.

Arming Options and LEDs

Press any of the arming options and the numbers light. Basic security functions include:

To…	Press	
Arm in Away mode (typically when no one is home)	ARMED **Away** and enter your user code	
Arm in Home (Stay) mode (typically when someone is home)	ARMED **Home** and enter your user code	
Quick Arm without a code in Away mode or Home mode	ARMED **Away** or ARMED **Home** For 3 seconds	
Disarm the system	**Disarmed** and enter your user code	

Switching Arming Modes

You can easily switch between arming modes without having to first disarm the system. When the system is armed or while arming or disarming, simply press the desired arming option and enter your user code. (This feature is available only from the Gateway Touchpad or a Wireless Key.)

Auto-Home Mode Operation: If your system is programmed to do so, it automatically arms in Home mode when you select Armed Away but no one opens an exit-delay door. [This mode is not available when arming using Total Connect.]

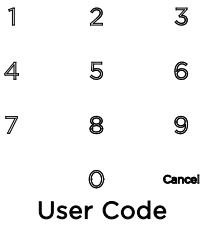
Emergency Options

Depending on your system set up, when an Emergency Type option is pressed, emergency messages can be sent to your monitoring company (if programmed to do so).

Refer to the Emergency Alarms section of *Operating your Gateway with the MyHome Gateway App* for additional details.

Press	Then…
Emergency	The system Emergency Type options appear.
Fire **Police** or **Medical**	The system sends an emergency message to the monitoring company, if programmed up to do so.
Cancel	Press **Cancel** when it is blinking to cancel the Emergency before it is sent.

To Cancel and Clear an Emergency Alarm that has been triggered



Enter your User Code The Alarm silences and the system announces the status.

Check for alarm details on MyHome Gateway App or Total Connect Remote Services.

Enter a User Code again to clear alarms.

Network Configuration from the Gateway

If your network connections or router change, you can connect to the network via the Gateway or using the MyHome Gateway App. To configure the network via the Gateway touchpad:

WPS Enrollment Method

To connect to a WPS router:

1. Enter the **Master User code** then **4 1** on the Gateway touchpad.
2. Press the **WPS** button on your router.
3. When done, the system announces the network connection is complete.

Gateway AP Enrollment Method

Gateway AP Enrollment Method:

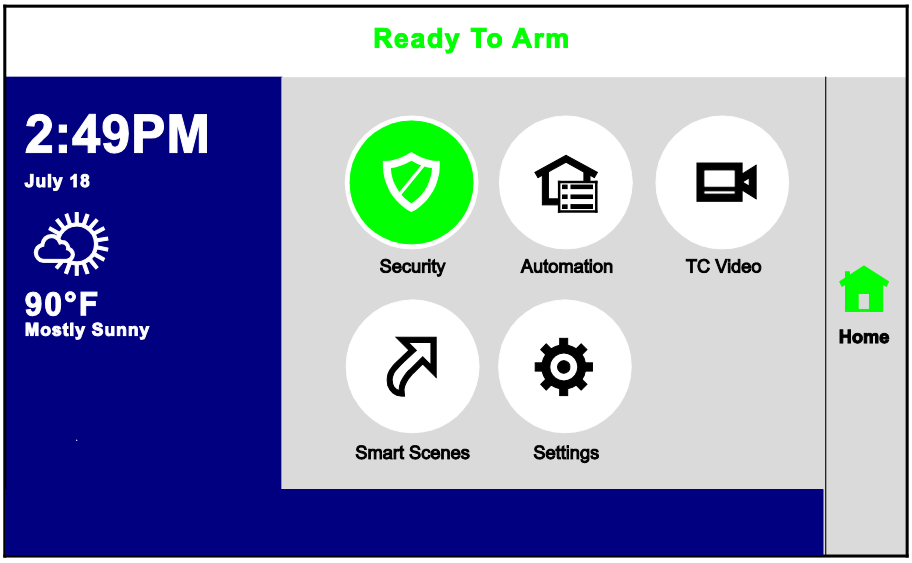
1. Enter **Master User code** then **3 1** on the Gateway touchpad. (Once in this mode, the MyHome Gateway App disconnects because it is no longer on the same network.)
2. On your mobile device, go to the System Wi-Fi Settings and change the Wi-Fi setting to the Gateway AP.
   a. Select the Gateway SSID and, press CONNECT. (The SSID **OPTGW_####** is listed on a label on the bottom of the Gateway.)
   b. When prompted, enter Gateway's 8-Digit case sensitive WPA2 Password. (The password is also on the SSID label.)
3. Launch the **MyHome Gateway** App on a device.
4. Enter your **Master user code** then **2 1** on the **Gateway** Touchpad.
5. The App displays a six-digit "Pairing key" number. Enter that number on the **Gateway** Touchpad and the system announces when Enrollment is completed.
6. When prompted, enter a valid user code on the **MyHome Gateway** App screen. The App screen confirms enrollment success and opens the App **Home** screen.
7. Navigate to the Network Configuration list of Wi-Fi options screen and press **Manual Config AP**. The Wi-Fi enrollment menu appears. (Fields include **Network Type**, which cannot be changed.)
8. Press **SSID Name,** enter your network's name, press **Done** and **Save**.
9. Press **Security,** choose the same security protocol as your router. Options include **Open**, **WPA/WPA2** and **WPA2**. (WEP is not supported.)
10. If a password is required, press **Key**, then enter the password, press **Done** and **Save**.
11. Press **JOIN** and a confirmation screen appears.
12. Press **Yes**. The system announces connection to the network.

NOTE: Network Configuration can also be managed using the MyHome Gateway App. See WI-Fi (Network) Configuration in the Systems Settings section.

Operating your Gateway using the MyHome Gateway App

Use the **MyHome Gateway**™ App to manage your System Security, Automation, Smart Scenes, Video and Settings:

Home Menu Overview



NOTE: Pressing **Home** from any screen returns you to this Home screen.

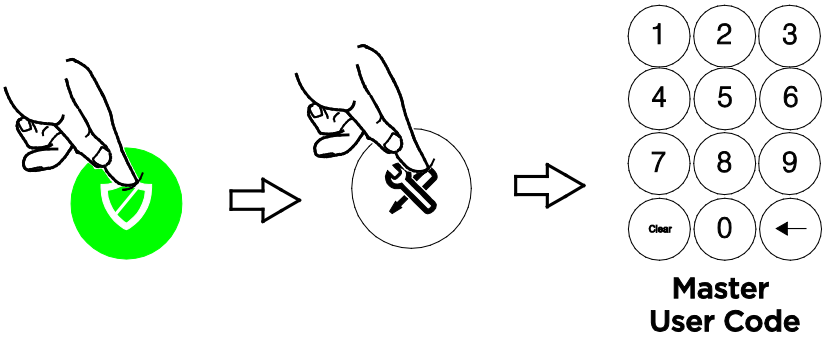
Option	Allows you to…	To Navigate, Press…
Security	Operate and manage the security features and access other features of your Gateway system.	and select from the options on the next screen.
Automation	Manually operate your Z-Wave devices Add or delete Z-Wave Devices	and select the device then **Setup** and . See the Automation section for details
TC Video	View and configure system cameras; manage video recovery functions	See Video section for details
Smart Scenes	View and run automation scenes to operate your system for convenience, comfort, energy savings and security*	and enter your Master User Code. See the Smart Scenes section for details.
Settings	Adjust the Gateway touchpad and LED brightness and the announcements and chime volume	See the Systems Settings section for details.

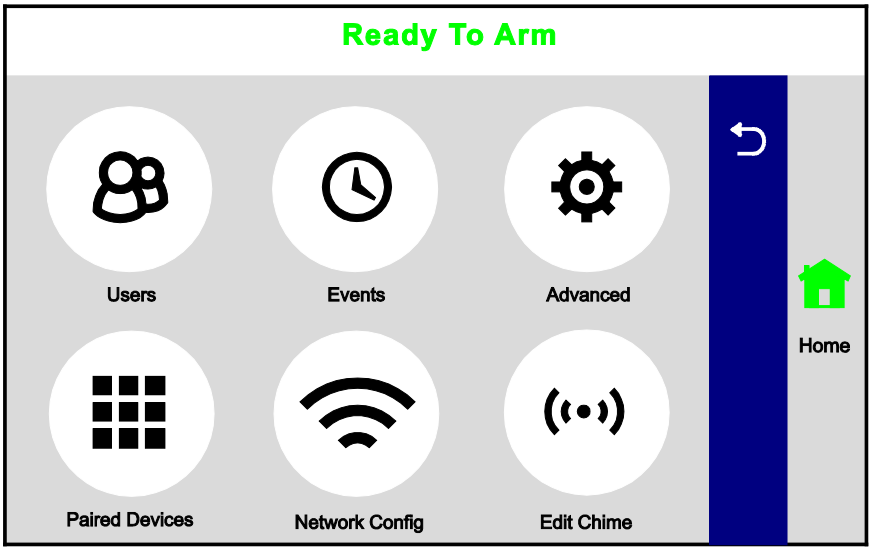
* Smart Scenes are created and deleted using **Total Connect Remote Services.**

The Tools Menu Overview

Home > Security > Tools

NOTE: The **Master User code** is required to access Tools.





This menu offers access to most of Gateway's important settings and maintenance functions:

Option	Allows you to…
Users	Add/remove users, control user's access to system features. The Master User code is required. Seethe Users and Security Codes section for details.
Events	View system event logs. See Events in the System Settings section
Advanced	Access software upgrades, tests and user maintenance functions. Includes features found in the Maintenance and System Settings sections.
Paired Devices	Manage smart devices paired to your Gateway. See Paired Devices in the System Settings section
Network Config	Configure Wi-Fi connection to the Gateway. See the Wi-Fi (Network) Configuration in the System Settings section.
Edit Chime	Change Chime sounds for select zones. See Edit Chime in the System Settings section.
(Back Arrow)	Return to the previous screen or menu.

Security

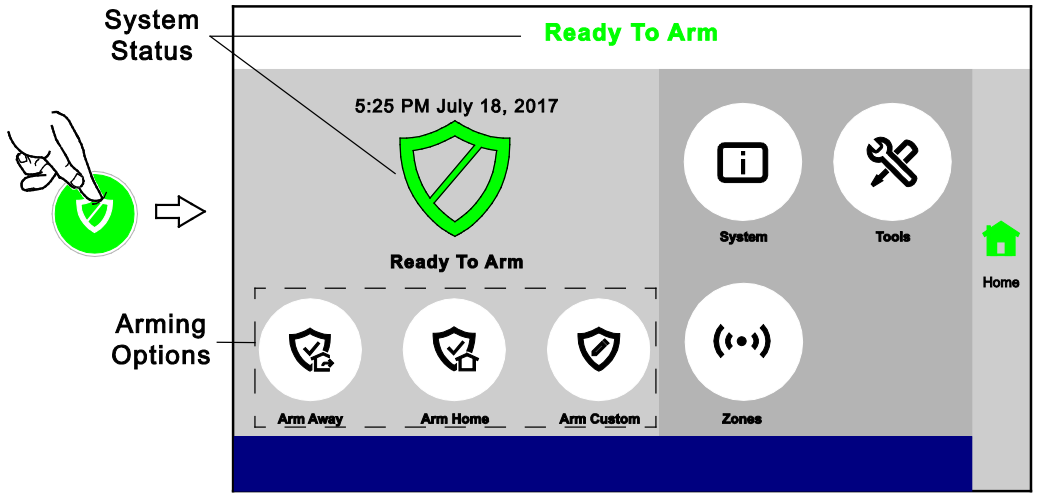
IMPORTANT

If the Gateway is beeping rapidly when you enter the premises, an alarm has occurred and an intruder may still be nearby.

LEAVE IMMEDIATELY and CONTACT THE POLICE from a safe location.

Security Menu Overview

NOTES:
- For the Gateway to report alarms over the internet, your Wi-Fi network MUST have power at all times.
- You must arm your security system in order for it to sound alarms.



The MyHome Gateway App displays the system arming status, top and center of the screen:

Ready to Arm = the system is ready to be armed.

Not Ready To Arm-Fault = one or more zones are faulted. The system cannot be armed until all zone faults are fixed or bypassed.

Armed [Home, Away, Custom, etc.] = the system is armed, and arming mode description.

Arming the System

Before arming your system, all protected doors, windows, and other protection zones should be closed or bypassed (see Bypassing Protection Zones).

To change the volume of countdown sounds and security status voice announcements, see System Settings.

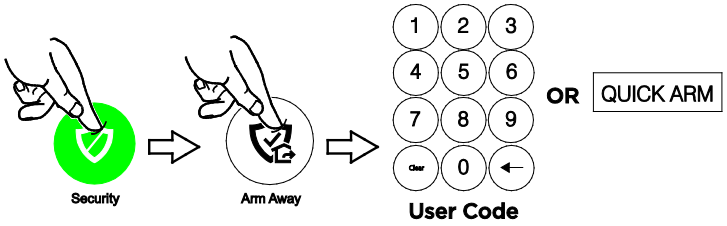
Arming states include

Arm Away	For times when no one is home; protects all perimeter (doors and windows) and interior zones.
Arm Home	For times when the house is occupied; protects only perimeter zones.
Arm Custom	Arms the system with pre-selected zones bypassed.
Bypass	This feature allows you to arm the system while intentionally leaving selected zones unprotected.
Arm Night	For times when the house is occupied; protects perimeter zones and selected interior motion sensors if used. Other interior zones are unprotected. *Enabled by your installer and only used with interior motion sensors.*
Instant	For times when Entry/Exit doors are not expected to open at all. Entry Delay is eliminated. When the system is armed, an alarm occurs **immediately** if an exterior door is opened.
Quick Arm	Used to arm the system in any mode without entering a user code, *if programmed.* NOTE: A user code is always needed to **disarm** the system.
Auto Home	If you arm the system in the "Away" mode but no one exits, the alarm system automatically changes to the "Home" mode. This helps to prevent unwanted alarms when someone remains on the premises. Disarm the system and Arm Away again when you are ready to leave. *This option is enabled by your installer.*

Arm Away

Security > Arm Away

By default, this mode's exit delay countdown is accompanied by a beeping sound.



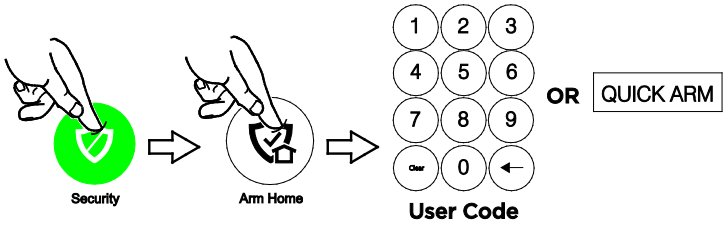
For a silent exit, press **Silent Exit** first.

- The system beeps twice and announces "Armed Away; exit now". The exit delay countdown begins.
- Press **Restart Timer** if you need more time to leave.
- Leave the premises and close the door before the countdown ends.
- The system arms in Away mode. (Door and window sensors and interior motion sensors are active.)

Arm Home

Security > Arm Home

By default, this mode's exit delay countdown is silent.



- The system beeps three times and announces "Armed Home; exit now". The exit delay countdown begins.
- Press **Restart Timer** if you need more time to leave.
- The system arms in Home mode. Door and window sensors are active, but interior motion sensors are not active.

Arm Custom

Security > Arm Custom

Use this option to pre-set zones for bypass when arming the system. You can also enable or disable the entry delay.

1. Select Arm Custom to display a list of zones.
2. Select the zones you wish to bypass when arming the system.
3. Select Arm Custom on the zone list screen.
4. A numerical keypad appears.
   Select **Entry Delay** if desired. (See Instant Mode for more about disabling Entry Delay.)
5. Arm the system by entering a user code.
6. The exit delay countdown begins.
7. If leaving, exit the premises and close the door.

   Bypassed zones are left unprotected.

   NOTE: The next time Arm Custom is used, the same zones that were previously selected are highlighted on the zone list screen. If desired, select different zones for custom arming.

Instant Mode

Security > Arm Custom

In Instant mode, an alarm occurs immediately when a protected Entry/Exit is opened. There is no Entry delay during which a code can be entered to disarm the system.

1. Select Arm Custom to display the zone list screen.
2. If any zones have been previously set for bypass, deselect them.
3. Press **Arm Custom**.
4. When the keypad appears, **de-select Entry Delay**.
5. Enter a user code to arm the system and leave the premises during exit delay.

Arm Night

Security > Arm Home

Arm Night must be enabled by your security installer.

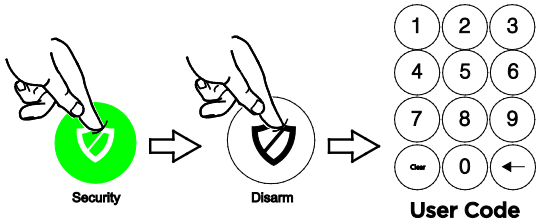
1. Select **Arm Home** to display the keypad.
2. Select **Arm Night** and then enter a user code.
3. The system beeps and announces "Armed Night Home mode". Exit delay begins.
   Press **Restart Timer** if you need more time to leave.
4. The system arms in **Arm Night** mode. Doors and windows and pre-selected interior zones are active.

Disarming the System

Security > Disarm

NOTE: Disarming the system also silences audible alarms and trouble alerts.

To disarm your security system:



- The system beeps and announces “Disarmed”, followed by alerts about system readiness, if any.
- A “Check system” announcement indicates a faulted sensor or problems in the Gateway itself.

In most situations, if a valid user code is not entered within 30 seconds of pressing **Disarm**, the Home screen reappears, and the system remains armed.

NOTES:
- If a valid code is not entered by the time the entry delay ends, an alarm occurs.
- The Guest code and the Installer code can only disarm the system if that code was used to arm the system. If the Quick Arm option has been used, neither the Guest Code nor Installer Code can disarm the system.

User Code Error (Touchpad Lockout)

When the screen displays **User Code Error**, it means too many invalid user codes have been entered. The system will not accept additional user code entries for 15 minutes (lockout period).

Bypassing Protection Zones

Any zones with faults must be cleared before arming the system.

Bypass allows arming the system while intentionally leaving selected zones unprotected.

Bypassed zones will not trigger an alarm.

To Bypass zones:

1. Before arming the system, press **Zones** on the Security menu. A list of your system’s zones appears. Faulted (open) zones are shown in red or orange.

   To choose which zone list to view (All, Alarm, Trouble, Fault or Bypassed zones), press **Select** on the bottom, right of the screen.

   Use the up and down arrows to scroll through the list of zones.
2. Select the zone(s) to be bypassed.
3. Press **BYPASS** and enter a user code.

   If programmed, you can select **BYPASS FAULTED** and enter a user code. This selects and bypasses all zones with faults or other issues.

   A Bypass icon [⛔] appears on Bypassed zones on the zone lists.
4. Arm the system as usual.

   NOTES:
   - Fire and Carbon Monoxide (CO) and Emergency zones cannot be bypassed.
   - Bypassed zones are automatically un-bypassed when the system is disarmed.

Press **Clear Bypass** to un-bypass any previously bypassed zones.

Entry and Exit Delays

NOTE: Entry and exit delay times are programmed by your installer. There is room to jot them down in Your System Information, near the end of this guide.

Entry Delay

Entry delay allows time to disarm the system when entering the premises. If the system is not disarmed before the entry delay period ends, an alarm occurs. If programmed, the Gateway beeps during the entry delay period as a reminder to disarm the system.

Two different entry delay periods can be programmed. The first is for the primary entrance, typically, the front door. The second can be used for a secondary entrance, where more time might be needed to walk to the Gateway to disarm the system.

Exit Delay

Exit delay begins immediately after the system is armed, providing time to leave through the designated exit door without causing an alarm. In most situations, the MyHome Gateway App screen displays a countdown of the remaining time. The exit door must be closed before the end of the exit delay.

Typically, the system beeps slowly when counting down to Arm Away and the beeping speeds up during the last 10 seconds of the delay period. The exit beeps cannot be silenced unless **Silent Exit** is selected.

Restart Exit Delay

The **Restart Timer** option appears only if the option has been programmed by the installer.

Exit delay can be restarted **once**.

Exit Alarm

This option helps minimize false alarms sent to the monitoring company. Exit Alarm is always enabled.

Exit delay begins whenever the system is armed.

- If an exterior door or protected interior zone is faulted during the exit delay (and remains faulted when the exit delay ends), an exit alarm occurs and an **entry delay** countdown begins.
- If the system is disarmed before the entry delay ends, the alarm sound stops and the message **Alarm Exit Error** and any faulted zones appear.
- **No message is sent to the monitoring company**. Any open zones must be secured before the exit alarm condition can be cleared.

To clear the display, press **Disarm** and enter a security code.

- If the system is not disarmed before the entry delay ends, and an entry/exit door or interior zone is still open, the alarm sound continues and an **Exit Alarm** message is sent to the alarm monitoring company, along with a “Recent Close” message (the Recent Close option is always enabled).
- The message **Alarm Exit Error** appears. Faulted zones are also displayed. The alarm continues to sound until the system is disarmed or timeout occurs.

To stop the alarm, disarm the system. The message **Not Ready to Arm-Fault** is displayed and faulted zones continue to be displayed.

To clear the display, press Disarm and re-enter the security code.

An exit alarm (“Alarm – Entry Exit”) also occurs if an entry/exit door or interior zone is faulted within two minutes after the end of the exit delay.

Emergency Alarms

Available Emergency modes may vary, depending on the options programmed by your installer.

IMPORTANT
Use the Gateway Touchpad to trigger an Emergency. An Emergency can be canceled or cleared from the Gateway Touchpad, the MyHome Gateway App or Total Connect.

Activating an Emergency Alarm

1. Press **Emergency** on the Gateway.
2. Press the appropriate Emergency type option on the Touchpad.

Depending on the Emergency mode selected, an alarm tone sounds and the appropriate alarm icon appears on the MyHome Gateway screen.

Pressing **Police** can send a **silent** message to your monitoring company if programmed to do so. Verify this setting with your installer.

Common Emergency Types

Fire	Alerts the monitoring company that a fire condition exists. (Displays Fire Alarm 995 Main Fire)
Police	Alerts the monitoring company that a police emergency exists. (Displays Alarm 999 Police, default is silent)
Medical	If programmed, alerts the monitoring company to other types of emergency. (Displays Alarm 996 Main Medical)

Types of Emergency Alarms

Silent emergency (silent alarm)	Sends an alarm signal to the monitoring company, but triggers no audible alarms or display (on either the Gateway Touchpad or MyHome Gateway screen.) **Requires connection to a monitoring company.**
Audible emergency (audible alarm)	Sends an emergency message to the monitoring company, if connected. A loud, steady tone sounds at the Gateway and external sounders if connected, and an alarm appears on the MyHome Gateway App screen.
Personal emergency or **Aux alarm**	Sends an emergency message to the monitoring company if connected and sounds at the Gateway and MyHome Gateway App, but not at external sounders. An alarm icon appears on MyHome Gateway.
Fire alarm	Sends a fire alarm message to the monitoring company if connected. A pulsing tone (three pulses – pause – three pulses – pause – etc.) sounds at the Gateway, on MyHome Gateway and external sounders are activated if connected. A Fire alarm icon appears on MyHome Gateway.

Canceling Alarms from MyHome Gateway

Depending on the **type** of alarm in effect, a keypad may appear immediately after the alarm is initiated.

1. Enter a user code to cancel the alarm.
2. The audible alarms stop and **Alarm Cancel** appears.

If a silent alarm has been activated and the Home screen is displayed:

1. Select Security on the Home screen. Typically, a “Not Ready to Arm” message and the Disarm icon appears.
2. Press **Disarm** and enter a user code.
3. The screen changes to the normal Security menu.

Clearing Alarms

After an alarm is canceled, the MyHome Gateway App continues to display zone information associated with the alarm (this feature is known as **Memory of Alarm**).

To clear memory of alarm, press Disarm and enter the user code again.

Memory of alarm can also be dismissed with these steps:

1. Cancel and silence the alarm as above.
2. Press **Zones** on the Security menu. The zone number associated with the type of alarm appears.
3. Press **CLEAR ALARMS** and enter a user code.
4. Press ⮌ to return to the Security menu or press the Home button.

NOTE: If any Emergency is canceled and cleared before a report is sent, an alarm will not be sent to the monitoring company.

Chimes/Voice Annunciations

IMPORTANT
The Chime feature is intended for convenience and is not intended for life safety purposes or pool alarm and does not meet the requirements of UL 2017.

Volume/Mute

Home > Settings

Gateway can be set to give audible notifications when a protected zone opens **while the system is disarmed**.

On the **Settings** screen:

1. Select **CHIME** and **PANEL VOICE** to enable chime sounds and voice annunciations.
   De-select **PANEL VOICE** for chime sounds only.
   De-select **CHIME** to mute these audible notifications.
2. Adjust **Panel Volume** with the slider.
3. Press **Save**.

NOTES:

- The system must be disarmed to change chime and voice settings.
- Chime related Voice annunciations are controlled by enabling or disabling CHIME.
- Voice annunciations should not be confused with Gateway's Two-Way Voice (Audio Alarm Verification) feature.
- With Chime enabled, the Gateway sounds a selectable tone when a protected zone is opened. See Selectable Chime Sounds below
- General voice annunciations, such as arming and disarming notifications, are controlled by enabling or disabling PANEL VOICE.only.

Selectable Chime Sounds

Chime sounds are set by your installer and can be changed using the MyHome Gateway App. See Edit Chime.

Chime tones may not be selectable for some devices, such as those associated with smoke and CO detectors.

Audio Alarm Verification (Two-Way Voice)

This feature allows your central monitoring station to listen to or talk with individual(s) on the premises when an alarm has occurred (if programmed to do so).

NOTES:
- System announcements are disabled when this feature is active.
- Fire and CO alarms prevent Audio Alarm Verification from operating.
- New Fire or CO alarms terminate Audio Alarm Verification operation.
- Burglar alarms occurring during Audio Alarm Verification operation do not interrupt operation and are reported immediately after operation concludes.
- Audio Alarm Verification modes are controlled by the central station.

Automation: Z-Wave and Other Devices

IMPORTANT
Automation can ONLY be used for lifestyle enhancement. It must not be used for personal safety or property protection.

Working with Z-Wave Devices

NOTE **Z-Wave automation functionality is supplementary only and has not been evaluated by compliance agency.**

Z-Wave technology is designed to automate devices in a home control network. The Lyric™ Gateway is a security enabled Z-Wave Plus device that uses encrypted Z-Wave Plus messages to communicate to other Z-Wave Plus products; it also supports Z-Wave Network Wide Inclusion (NWI) Mode.

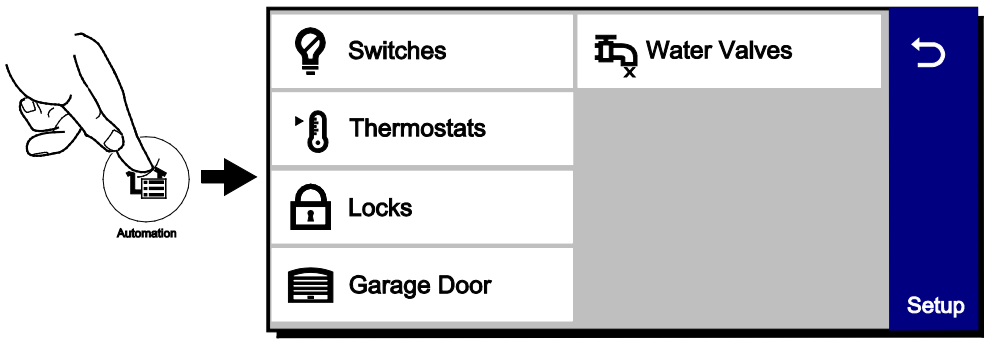
The Gateway and Z-Wave devices added to your system are linked together in a wireless network. Each device in the network is assigned a unique address and cannot be activated by a neighbor's Z-Wave controller. The Z-Wave network supports multiple controllers, allowing remote control of Z-Wave devices throughout the home.

This product can be included and operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers and/or other applications.

All non-battery operated nodes within the network act as repeaters, regardless of vendor, to increase the network reliability.

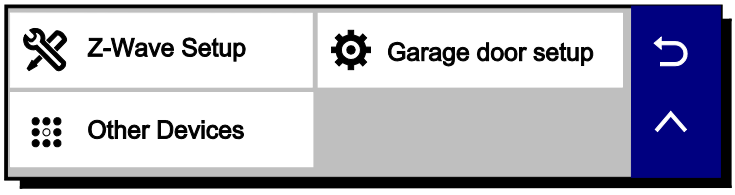
NOTES:
- Z-Wave Grouping Identifier of Gateway is 1 and used for the Lifeline association.
- The maximum number of devices that can be added to the group is 1.
- Any received BASIC commands will be ignored.
- In some cases, a Z-Wave device might not report its status to the Gateway and/or Total Connect when an action is initiated at the device itself (ex. Thermostat low battery message or manual change of thermostat status). This varies with the manufacturer.

Press **Automation** on the Home screen. The Automation (Z-Wave Device) Management screen appears, initially displaying categories of Z-Wave devices. (*Your MyHome Gateway App's display may differ from these illustrations.)*



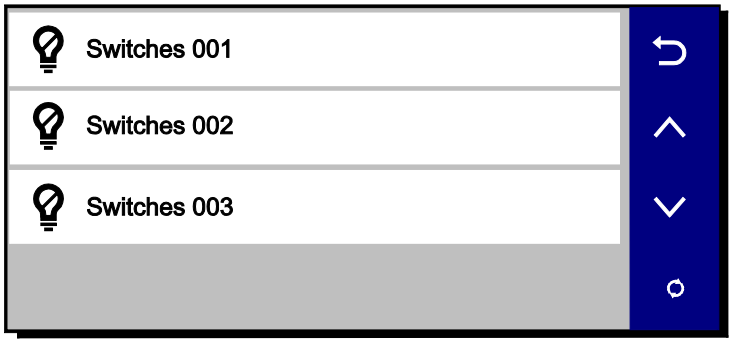
This screen may also display "Press to see Failed Devices". See Failed Devices (Failed Nodes) for more information.

Press **Setup** for more options:



Consult your installer about the options available in your system.

Selecting a device category opens a list of devices in that category. An example of the **Switch** category is pictured.



For most devices, status is indicated by the color of the icon.

The **Refresh** button updates device status indications on the display.

Operating Z-Wave Devices Manually

1. On the Z-Wave Device Management screen, select one of the device categories.
2. Select the device you wish to operate. Controls appear.
3. The options shown will vary with your device: Lighting controls might offer an On/Off button or a slide control for dimmers, Thermostats may display temperature set points and energy-saving features.
4. Operate the device as desired.
5. Press ⮌ to return to the previous screen.

Adding Z-Wave Devices (Include Devices)

NOTE: When adding a device, it may be necessary to perform the **Exclude** procedure before the device can be Included successfully.

1. On the Z-Wave Device Management screen, press **Setup**.
2. Press **Z-Wave Setup**.
3. Options appear, including **Include Devices**, **Exclude Devices** and **Advanced Tools**. (**View Failed Devices** and **Replace Failed Devices** may also appear.)
4. Select **Include Devices**.

   After the Gateway enters Inclusion mode, the screen displays “Ready to Include Device. Press the function button on the device”.
5. Press the device’s Function button within 60 seconds. (Note that the location of the Function button and inclusion process varies with the device you are adding. See the device’s instructions.)

   The panel displays “Device Found. Please Wait”.
6. To include additional devices, repeat step 5.

   OR

   Press **Abort** to complete the Inclusion process.
7. Press ⮌ to return to the previous screen.

Including Light Switches or Outlet Modules

Install the receptacle, wall switch or lamp/appliance module **before** Including it in your system. Refer to the device’s instructions for more information about installation.

Z-Wave switches and outlet modules may vary. Refer to the device’s instructions to ensure that it is Included properly in your system.

Including Door Locks

IMPORTANT
For security, Z-Wave door locks are encrypted; they enroll at low power transmission range (approximately 6 feet). This requires Including the lock before its installation in a door.

Assemble the lock, connect necessary cables and install batteries according to the device's instructions. **Be sure the door lock's orientation/handedness is correct**.

Z-Wave door locks vary. Refer to the device's instructions to ensure that it is Included properly. See the Users and Security Codes section for more information.

After Inclusion, install the lock within recommended Z-Wave range (see Wireless Range for more information).

NOTES:
- Program the 4-digit user code into the Gateway. When programming user codes into the Gateway determine if the user will have access to the Z-Wave lock. If so, the user code will be transferred to the lock.
- If using a lock with Smart Scenes, automatic locking/re-locking features should be disabled.
- Due to Low Power Inclusion Mode of secure devices, Include the Z-Wave Lock first, if not using an Inclusion Tool/Remote Control. The lock should be installed before including other devices.
- During operation, the system displays "JAMMED" and reverts to "Unlocked" status if a jammed lock is detected.

Including Thermostats

Install and **test** the thermostat before Including it in your system. Refer to the device's instructions for more information about installation.

IMPORTANT
Honeywell is not responsible for property damages due to improper setting of thermostat modes.

NOTES:
- Some thermostats may not update temperature status displayed on the MyHome Gateway App.
- When using Z-Wave thermostat control on the Gateway, make sure the thermostat's scheduling feature is disabled on the thermostat itself.
- When the HOLD button on the MyHome Gateway's thermostat control screen is highlighted, neither Scheduled nor Triggered Smart Scenes will affect thermostat operation. **Manually** running Scheduled or Triggered Smart Scenes, however, will change thermostat settings.
- If your system is connected to remote services, the remote 7-day schedules will also not affect thermostat operation.
- For **threshold monitoring** to be configurable on the remote services and/or a Z-Wave thermostat, the respective zones must first be programmed with an appropriate response type. Verify with your installer which thermostats are programmed for threshold monitoring.
  NOTE: Threshold monitoring is not available on all thermostats.
- Program both zones for each thermostat used (as many as 6):

Zone Pairs	Thermostat	Zone Pairs	Thermostat
280 & 281	1	286 & 287	4
282 & 283	2	288 & 289	5
284 & 285	3	290 & 291	6

- When temperature is represented in Celsius, Gateway matches the temperature increment of the particular thermostat for Heat, Emergency Heat and Cool set points. Increments can be one degree or half degree, depending on the thermostat.

Including Thermostats (continued)

- If Celsius scale is used in the thermostat, the Gateway must also be set to Celsius scale.
- For thermostats that support Multilevel Sensor Command Class, press the current air temperature to show the sensor type and value, even though not supported.
- If the Energy Saving mode is set, the MyHome Gateway displays Energy Saving Heat/Cooling Setpoint Temperatures that are programmed at the thermostat.
- An additional "Energy Saving" function in the thermostat is used to set/unset the Energy Saving mode.

Gateway Z-Wave Thermostat Functions

Control	Function
Mode	Select between HEAT, COOL and OFF; other options may also be available, such as AUXILIARY mode, if supported.
Fan	Select between ON, CIRCULATE and AUTO. *The Mode and Fan settings available will vary with your thermostat.*
HOLD	Allows temporary override of programmed Smart Scenes that may operate the thermostat.
NORMAL	Allows selected thermostat to run programmed Smart Scenes.
NO SCHED	Prevents Scheduled Smart Scenes from operating the selected thermostat
Threshold Monitoring	Enable/Disable Threshold Monitoring Feature (if available)
Saving Off-Saving On	Enables/disables the thermostat's Energy Saving Function.
EDIT	Used to edit the thermostat's name.
BACK	Used to return to Thermostats screen.

Thermostat Energy Saving Mode

1.	On the Z-Wave Device Management screen, select **Thermostats**.
2.	Select the desired thermostat from the displayed list.
3.	On the thermostat control screen, press the "Saving Off" button OR "Saving On" to activate or deactivate the thermostat's Energy Saving Schedule Function when a heating or cooling operation is selected.

Deleting Z-Wave Devices (Exclude Devices)

To delete (Exclude) a Z-Wave device:

1. On the Z-Wave Device Management screen, press **Setup**.
2. Press **Z-Wave Setup**.
3. Select **Exclude Devices.**
4. The panel enters Exclusion mode. Next, the MyHome Gateway screen displays "Ready to Exclude device. Press the function button on the device."
5. Press the device's Function button.

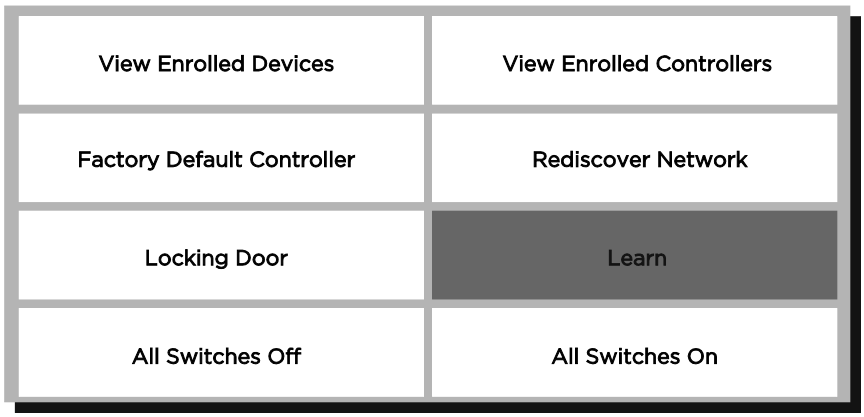
   The device is excluded from the system and its information is displayed.
6. To delete another device, press **Exclude** on the right side of the screen.
7. Press ⮌ to return to the previous screen(s).

Editing Z-Wave Device Names

1. On the Z-Wave Device Management screen, select the category that includes the device you want to rename.
2. Select the device in the displayed list.
   The device's controls appear, showing the device's default name.
3. Press **Edit** on the right side of the screen; a keyboard appears on the screen.
4. Use the keyboard to enter a custom name, up to 14 characters.
5. **Save** the device's new name.
6. Press ⮌ to return to the previous screen(s).

Advanced Tools

1. From the Z-Wave Device Management screen, press **Setup** and then **Z-Wave Setup**.
2. Select **Advanced Tools**.
3. Enter the Master User code. The Advanced Tools screen appears:



View Enrolled Devices

Press to display Z-Wave device information: System Index/name, Secured or Non-Secured, device type, device ID, manufacturer, node number.

View Enrolled Controllers

Press to display controller information: Primary or Secondary, Z-Wave Library Rev., Home ID, device type, device ID, node number, manufacturer, Secured or Non-Secured.

Factory Default Controller

Press to delete all Z-Wave nodes in the Gateway, and reset the Gateway's Home ID. When prompted, press **Yes** to confirm.

Important! Defaulting the Controller does **not** delete/Exclude individual Z-Wave devices. Therefore, each device must be Excluded before being added/Included in the Gateway again. Also, if the controller is used as a secondary controller in the network, use the above procedure to default the controller only when the primary controller is missing or otherwise inoperable.

Rediscover Network

Press to refresh communication paths between new and old Z-Wave devices or repair communication paths for Failed Devices.

NOTE: Some devices may not be included in the network path, such as devices that have been moved outside of the network range, battery devices that are in sleep mode to conserve energy or with low battery conditions.

Advanced Tools (Continued)

Locking Door

Press to have your system **arm** automatically when a Z-Wave door lock is locked. Press repeatedly to select the desired arming option: **Home** mode, **Away** mode, **Arm without Auto-Home (Stay)** mode or **Disabled**. Then press **Save**.

Learn

This option is intended for future use.

All Switches Off

Press to manually turn off all Z-Wave devices. (See the following Note.)

All Switches On

Press to manually turn on all Z-Wave devices. (See the following Note.)

NOTE: **All Switches On/Off** commands broadcast messages over the Z-Wave network and are intended for testing device communication. They should not be used for basic operation as each Z-Wave device reacts differently to these commands and unintended results may occur. For Example:

- Some Z-Wave enabled thermostats may enter or exit their Setback (or energy saver) modes.
- Z-Wave enabled water valves will open (enabling water flow), however, the **All Switches Off** command is not processed.

Failed Devices (Failed Nodes)

When the system tries to operate a Z-Wave device that has no AC power or other problems, it is identified as a **Failed Device**. The system may take up to a minute after the operation to recognize the failure.

Failed Z-Wave devices are also indicated by a ⚠ symbol on the Z-Wave Device Management screen or the symbol appears in gray on the Home screen.

To view Failed Devices:

1. On the Z-Wave Device Management screen, select **View Failed Devices**

   OR press **Setup**, **Z-Wave Setup** and then **View Failed Devices**.
2. The device's information is displayed. If multiple devices are listed, use the up and down arrows at right to view the entire list.

NOTE: When troubleshooting a failed device, first make sure that power has been restored and try the Rediscover Network option from the Z-Wave Advanced Tools menu.

3. If a device is defective or otherwise unavailable, use the **Fix All** option. Press **Fix All** and "**This will delete all failed nodes**" appears. Press **Yes** to confirm.

Devices deleted with Fix All must be added to the system again. See Adding Z-Wave Devices (Include).

To Replace Failed Devices:

1. From the Z-Wave Device Management screen, press **Setup**, then **Z-Wave Setup.**
2. Press **Replace Failed Devices**.
3. When a failed device is highlighted and the "**Replace**" button is selected, the screen displays "Entering Inclusion Mode. Please Wait...". Next, "Ready to include device, select the function button on the device" appears.
4. **Within one minute** press the device's Function button or activate the switch, as applicable. If the module has been successfully enrolled, the panel displays "Device Found! Please Wait". After successfully including a device, the device is removed from the failed devices list.

Garage Doors

Home > Automation > Garage Door

Garage door operation from the Gateway requires installation of a garage door control kit. Consult your security professional for more information.

The Gateway can remotely operate and monitor as many as four garage doors. The system can be armed when the garage door is opened. After it is closed, the zone will be monitored without providing burglary protection.

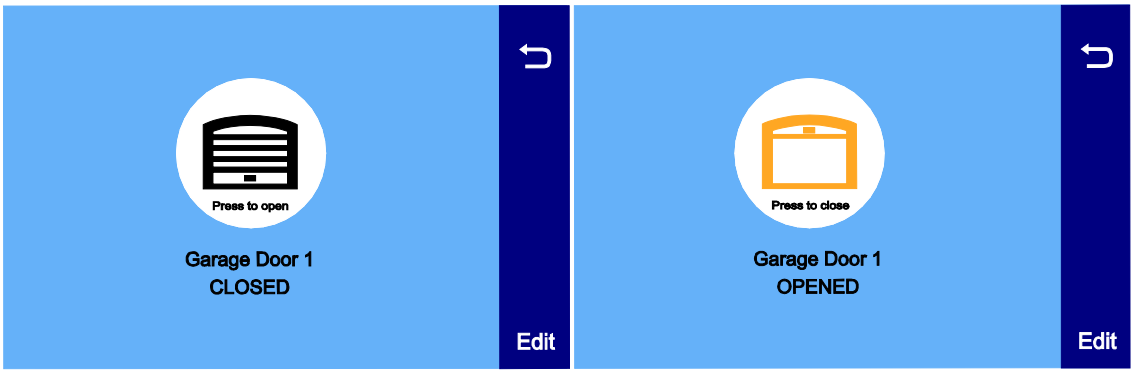
IMPORTANT

Do not use Gateway's 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.

NOTE: Press **Switches** on the Z-Wave Device Management menu to configure new Z-Wave binary garage door openers. Ask your security professional for more information.

Garage Door Operation from the MyHome Gateway App

1. On the Home screen, select **Automation**.
2. On the Z-Wave Device (Automation) Management menu, press **Garage Door**. The MyHome Gateway App screen displays the Open/Closed status of your connected garage doors.
3. Select the garage door you wish to operate.
4. Press the button in the middle of the screen to open or close the garage door.



Edit	Press to rename the selected garage door. Use the on-screen keypad and press **Save.**

Important Notes About Z-Wave Devices

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 of medical and/or life support equipment.

Wireless Range

This device complies with the Z-Wave® standard of open-air, line of sight transmission distances of 328 feet (100 meters). Actual performance in a home depends on the number of walls between the Gateway and the destination device, the type of construction and the number of Z-Wave enabled devices installed in the control network.

Note that 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 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 (refrigerators, large TVs, etc.) between the remote and the destination device can reduce the maximum range of 100 feet (30 meters) 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 suffer a significant loss of range (approximately 20%) since the metal box blocks a large part of the RF signal.

Additional Z-Wave Information

- Gateway can control up to **72** Z-Wave devices.
- The system supports a maximum of 232 nodes. Note that a node is created every time a device is Included, even if the device is being re-added to the system after being Excluded. This can cause the number of nodes in the system to exceed the number of actual devices.
- If the limit of 232 nodes is met and you need to add or re-Include more Z-Wave devices, use the Factory Default Controller function. Be aware that defaulting the controller deletes all of the system's nodes, requiring all devices to be Included again. Node numbers can be viewed by selecting Automation > Tools > Advanced Tools > View Enrolled Devices. Remember that the system may require the Master User code for access to Advanced Tools.
- **The system is not aware** of door locks being enabled with any temporary user shutdown feature such as Vacation Mode. The system continues to unlock a door if programmed to do so via Smart Scenes.
- Z-Wave door locks with thumbturns: Certain models allow a brief period in which the thumbturn can be operated manually before the device locks automatically. Locks of this type are not recommended for use with Smart Scenes.

Z-Wave Compatibility

Z-Wave devices vary; follow the instructions provided with the specific device when including and excluding devices into your Z-Wave network.

NOTE: Not all Z-Wave devices have been tested. Some functions may produce unpredictable results.

Z-Wave Compatibility (Continued)

Appliance	Lights
HomeManageables Appliance Module	Leviton®/ViziaRF+® Switches
Wayne Dalton Small Appliance Module	Leviton/ViziaRF+ Dimmers
GE® Wireless Lighting Control Plug-In Appliance Module	Leviton/ViziaRF+ Plug-In Appliance Modules
Cooper In-Wall Duplex Receptacle Module (Model RF9505-TDS)	GE Wireless Lighting Control Dimmers
Door Locks	GE Wireless Lighting Control Switches
Yale® Real Living Push-Button Lever Lock	GE Wireless Lighting Control Plug-In Appliance Modules
Yale Real Living Touchscreen Lever Lock	Cooper Plug-in Lighting Switch Module (Model RFAPM)
Yale Real Living Push-Button Deadbolt Lock	AEON Labs Lamp/Dimmer Module (Model DSC06106-ZWUS)
Yale Real Living Touchscreen Deadbolt Lock	Remotec Lamp Dimmer Module (Model ZDS-100US)
Schlage® Link Deadbolt Lock	Intermatic In-Wall Receptacle (Model HA01)
Schlage Link Lever Lock	**Siren**
Kwikset® Smartcode Lever lock	FortrezZ SSA1/SSA2 Wireless Siren & Strobe Alarm
Kwikset Smartcode Deadbolt Lock	**Water Valve**
Thermostats	FortrezZ WV-01 Wireless Z-Wave Water Valve
Honeywell Z-Wave Thermostat (ZWSTAT)	**Garage Door**
Wayne Dalton Z-Wave Thermostat	Linear GDZ-004 Garage Door Module
Trane® Z-Wave Thermostat	**Window Shades**
Residential Control Systems Thermostat (Model TZ45)	Somfy® ILT Series
Intermatic InTouch Thermostat (Model CA8900)	Somfy Z-Wave to Digital Motor Interface (ZDMI)
Radio Thermostat Company of America (Model CT30, CT32, CT100, CT101 and CT110)	

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

USE OF THESE PRODUCTS IN COMBINATION WITH NON-HONEYWELL 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

Automation: Smart Scenes

Home > Smart Scenes

Smart Scenes are used to automate Gateway functions for comfort, energy savings and security. Multiple settings can be put into effect with a single command. For example, selected lights can respond to a door opening or movement in the middle of the night. Climate settings can be controlled by your schedule and the security system can disarm automatically for expected visitors or babysitters. Selected functions can be restricted to the homeowner, and limited access given to children or guests.

IMPORTANT

When the Gateway is connected to Honeywell Total Connect™ (or other compatible remote services), Smart Scenes can be created and modified ONLY via remote services.

* If your system is **not** set up with remote services, Smart Scenes can be created and deleted using the MyHome Gateway App as described in the following sections

Smart Scenes can be created, deleted or edited ONLY by the Master User. See Smart Scenes and User Access for more about **types** of users and their access to different functions.

Three types of Smart Scene can automate combinations of security and lifestyle settings:

- **Anytime**: Initiated by users.
- **Triggered**: Initiated by the system in response to user-defined conditions.
- **Scheduled**: Initiated by the system's calendar and clock.

Smart Scenes are frequently used in pairs. For example, a Smart Scene might be set to operate multiple devices, turning on lights and opening blinds or shades. A second Smart Scene could be used to return these devices to their off or closed states.

NOTES:
- As many as 100 Smart Scenes can be created.
- You can modify (Edit), manually start (Run)* and review (Show)* Smart Scenes prior to operation.
- Scheduled* and Triggered Smart Scenes can be paused with the Hold function.
- Setup details vary with each type of Smart Scene.
- Many options in Smart Scenes can be pressed repeatedly to toggle through different option choices.
- The system treats security (Arm/Disarm) actions separately from changes to devices such as lights, locks and thermostats. Setup details with options of both types display them in different categories called Security and Devices.

* Smart Scenes options such as Run, Show and placing Scheduled scenes on Hold can also be done using the **MyHome Gateway** App.

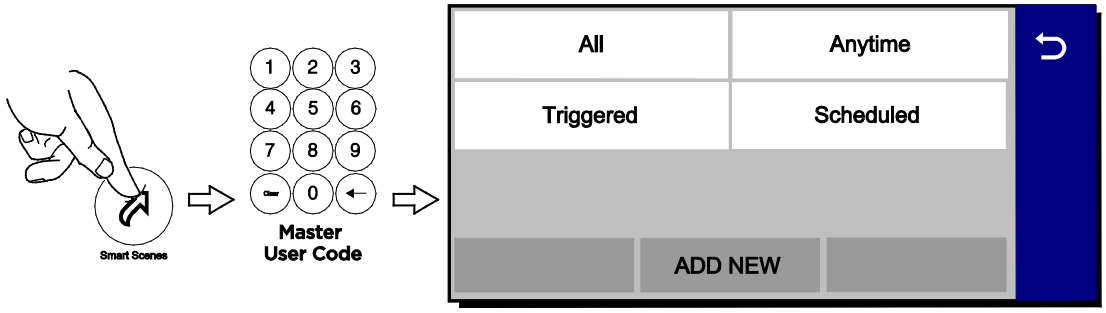
Smart Scenes and User Access

NOTES:
- The Master User designates which types of user have access to each Smart Scene. See Users and Security Codes for more information on different types of users.
- Smart Scenes can be created, deleted or edited ONLY by the Master User.
- The **Add New** button is available only to the Master User.

From the MyHome Gateway App, Master users can Run and Show all Smart Scenes. Regular users can Run and Show Smart Scenes created for Regular Users, Guests and those designated for "All Users". Guests can Run and Show Smart Scenes created for Guests and those designated for "All Users".

To work with Smart Scenes:

1. Select **Smart Scenes** on the Home screen. A keypad appears.
2. Enter a user code to display the Smart Scenes menu. From here, Smart Scenes can be created* or viewed by type.



Creating a Smart Scene using the MyHome Gateway App

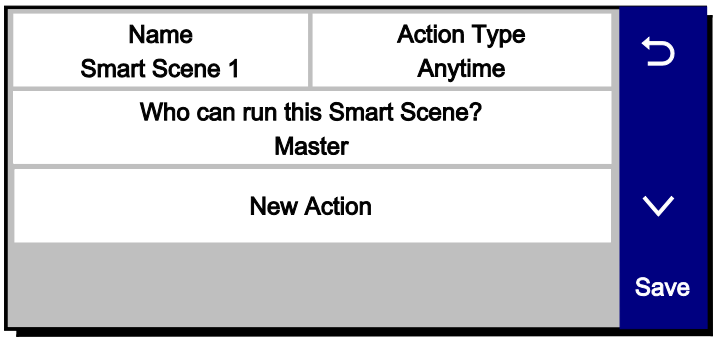
These instructions apply to the creation and operation of Smart Scenes from the MyHome Gateway App. If your system is connected to Total Connect remote services, you can create Smart Scenes only through Total Connect. Working with Smart Scenes from Total Connect differs slightly. (*Note that **Anytime** scenes are labeled as "When you manually run this scene" or "When you click it" in Total Connect.)*

Creating any Smart Scene involves these settings:

- Name
- The type of trigger that initiates the Smart Scene
- The type of user who can manually run the Smart Scene
- The resulting action(s) that take place when the triggering events or conditions occur

NOTE: Creating a Smart Scene should begin with giving it a **Name**.

1. Select **Add New**. (The default name that appears may differ from the illustration.)



2. Press **Name**.
3. Use the onscreen keyboard to enter a name and **Save** it.
4. Select the type of user who can run the Smart Scene. Choices include:
   - Master
   - Regular Users
   - Guest
   - All Users
5. Press **Action Type** to toggle through the types of Smart Scene.
   a. **Anytime**: Go to Step 6.
   b. **Scheduled**: Go to Step 7.
   c. **Triggered**: Go to Step 8.

6. Select **Anytime**. These options appear:
   - Name
   - Action Type
   - Who can run this Smart Scene? (User type)
   - New Action

   a. Press **New Action** to define the system's response when the Smart Scene is triggered.

   b. When settings are complete, press ⮌ until the Smart Scene appears with its name displayed.

   c. Press **Save**. Press ⮌ to return to the main Smart Scenes menu.
7. Select **Scheduled**.

   a. Select the type of user who can run the Smart Scene.

   b. Select **Scheduled** to display clock and calendar settings.

   c. Set a time when the Smart Scene will start. Be sure to specify AM or PM.

   You can select **Sunrise** or **Sunset** instead of setting a time on the clock. Selecting Sunrise or Sunset overrides the clock controls.

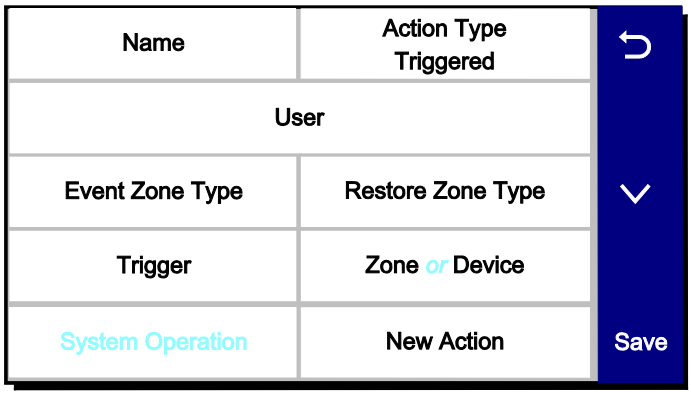
   NOTE that updated Sunrise and Sunset times may depend on the system's connection to the internet or cellular phone network. Ask your installer for more information.

   d. Set the days of the week for the Smart Scene to take place.

   e. Press **Save**. The schedule settings are displayed.

   f. Press **New Action** to define the response when the scheduled time occurs (see Step 8).

   g. Press ⮌ to return to the Smart Scenes menu.
8. Select **Triggered Action**. These options appear:



Smart Scenes can be started by one or a combination of the following options:

- Event Zone Type
- Restore Zone Type
- Trigger
- System Operation

NOTE: **Event Zone Type**, **Restore Zone Type** and **Trigger** can be different kinds of conditions.

For example, a given Smart Scene can be triggered by a Fire alarm OR by an Entry/Exit event. Smart Scenes can also be triggered by Trouble conditions (Trouble as the Trigger in one of the system's zones).

Device-related events (such as Light On, Light Off, Door Locked, Door Unlocked) set the button at right to **Device**. Choices depend on the devices installed in your system.

a. **Event Zone Type** starts the Smart Scene in response to any event (Fault, Trouble or Alarm) in any protected Zone of a specific zone type. Select the desired option. Examples of some typical zone types include:
   - Entry/Exit (front and back doors)
   - Perimeter (typically window sensors)
   - Interior Follower (typically motion sensors)
   - Day/Night (Usually assigned to sensitive areas where immediate notification of an entry is always wanted.)
   - 24 Hour Silent (Emergency (Panic) button)
   - 24 Hour Audible (Emergency (Panic) button)
   - Silent Burglary (typically a sensor)
   - Fire No Verification (smoke detector)
   - Fire With Verification (smoke detector)
   - Carbon Monoxide (CO detector)

   NOTE: Your system may include Zones that do not offer every Zone Type response.

b. **Restore Zone Type** starts the Smart Scene when any zone with the selected Zone Type returns to its normal state (such as a door closing). The options are the same as **Event Zone Type** options.

   NOTE: Event Zone Type and Restore Zone Type are **separate settings**. For example, a given Smart Scene can be triggered by a Fire Alarm (Fire No Verification as the Event Zone Type) OR by an open door closing (Entry/Exit as the Restore Zone Type).

c. **Trigger** starts the Smart Scene in response to a Fault, Trouble or Alarm in a particular zone or changes to connected devices.

   A note about triggering events:
   Any change in the state of a security system zone is known as a **Fault**. Faults can include **Trouble** and **Alarm** conditions. Trouble can include low battery or loss of communication with the device. Alarm conditions include zone faults while the system is armed and fire/CO detectors. Fault, Trouble and Alarm conditions can be used to trigger a Smart Scene.

   Fault: Any change in the state of a sensor triggers the Scene.
   Trouble: Only **Trouble** conditions trigger the Scene
   Alarm: Only **Alarm** conditions trigger the Scene.

   Choosing one of these events sets the button at right to display **Zone** options.

   Smart Scenes can also be triggered by changes in connected **devices** such as lights and locks. These events include:

   Light On
   Light Off
   Door Locked
   Door Unlocked

   Choosing one of these events sets the button at right to display **Device** options.

d. Choose **Zone** or **Device**, depending on your selection of a Trigger above. Security zone sensors or devices such as lights and locks are listed.

e. Select the zone or device and **Save**.

f. **System Operation** starts Smart Scenes in response to security-related events. Examples of some available options include:
   - Arm Away
   - Arm Home
   - Disarm
   - Any Burglary Alarm
   - Bell Timeout (end of the programmed time for which an alarm sounds)
   - Start of Entry Delay
   - End of Exit Delay
   - Any Fire Alarm

g. Select New Action to define the response when the triggering event occurs.

NOTE: The 24 Hour Silent Alarm or 24 Hour Auxiliary Alarm Zone types will not trigger the selected Smart Scene if the **Any Burglary Alarm** option is programmed.

9. **New Action** defines the response when the triggering event occurs. This includes users manually running **Anytime** Smart Scenes, the time of **Scheduled** Smart Scenes and the conditions for **Triggered** Smart Scenes. You can choose both Security and automation device responses. The Security choices are:
   - Arm the system in Away mode.
   - Arm the system in Home mode.
   - Disarm the system.

   a. After choosing a Security setting, press ↩ and then **Save**.

   b. If you choose to work with Devices, a list of the system's automation devices appears.

   c. Select one or more devices and set the device's desired operation. (For example, set switches to on or off, or locks to locked or unlocked.)

   d. After adding a device and its desired operation to the Smart Scene, press **Save**. Other available devices are displayed again so that they can be added to the Smart Scene.

   NOTE: In most situations, specific Security and Device information is displayed by pressing the Down arrow.

10. Press **Save**.
11. Press ↩ to return to the Smart Scenes menu.

Hold / Run / Show

These controls allow you to pause, preview/execute and review Smart Scenes from the MyHome Gateway App.

NOTE: You **can** use the **Hold, Run** and **Show** functions from the MyHome Gateway App, even when set up with Total Connect remote services.

Hold

Hold allows Scheduled and Triggered Smart Scenes to be temporarily suspended.

A **Scheduled** Smart Scene can be put on Hold **before** programmed operations take place.

1. Select a Scheduled or Triggered Smart Scene.
2. Press **Hold**. The button is highlighted, and programmed operation will not take place.

To remove a Hold:

1. On the Smart Scenes menu, enter a user code with access to the desired Smart Scene.
2. Select the Smart Scene and un-highlight **Hold**. Programmed operation resumes.

Run

Smart Scenes can be manually started with the **Run** button. The Smart Scene's results are displayed when the programmed operations have been performed.

NOTE: The **Run** option can be used to check the outcomes of Scheduled Smart Scenes and Triggered Smart Scenes, regardless of programmed triggers.

1. Select the Smart Scene.
2. Press **Run**. The system performs the programmed operations and the results are displayed. Successful operations are displayed with device information and a check mark. Failed operations are displayed with an empty circle.

Show (Review)

Use the **Show** button to see the programmed details of a Smart Scene without running it.

1. Select the Smart Scene.
2. Press **Show**. The scene's category, authorized users and included devices are displayed.

Video

The Gateway can display live video from as many as eight Wi-Fi-connected cameras.

NOTE: Gateway and its cameras must be on the same Wi-Fi network.

Viewing and Naming Cameras

1. Press **TC Video** on the Home screen. Video appears in windows or the cameras appear in a list.

   OR

   The system may **scan** for cameras; when the scan is complete, the camera list appears.

   From these screens, you can:
   - Press ⮌ to return to the Home screen.
   - View live video.
   - Name cameras.
   - Add cameras to the system.
2. Select one or more cameras (as many as four) in the list.
   - When multiple cameras are available, you may select as many as four.
   - Selected cameras are highlighted and the **Display** option appears.
   - You can also press **Scan** to search for other available cameras.
   - Press a camera's name again to de-select it.
3. Select **Display** to see video from the selected camera(s).
   - Select **Camera List** to return to the list view.
   - With multiple cameras displayed, you can select one to work with by tapping its video window.
4. Viewing a single camera displays its details, which vary with the camera selected.

For all compatible cameras, you can:

- Name the camera. Select **Name** above the video display or **Edit** at right.
- Press **Save** on the on-screen keyboard.
- Press ⛶ to show the camera full-screen.
- Press ⛶ to return to the detail view.

Some cameras offer additional options such as pan/tilt and built-in lighting.

Adding a Camera

- **Make sure** that the camera is on the **same Wi-Fi network** as the Gateway system.
- Install the camera according to its instructions.

With the camera installed:

1. View or list cameras as above.
2. Press **Scan**. The system looks for available cameras.
3. When the new camera is found, you can name it as described above.

Users and Security Codes

Home > Security > Tools > Users

Gateway uses 4-digit codes to restrict certain functions to selected users. A special 4-digit code can be set to trigger the system's **Duress** function.

User codes can be used interchangeably when performing system functions (a system armed with one user's code can be disarmed by another user's code), with the exception of the Guest Code described below.

All users are automatically assigned a **user number**, which cannot be changed. Do not confuse these user numbers with user codes.

User Codes

Master User	This code is usually set when the system is installed, and can be changed later. Typically, the Master User is a household member who can perform all system functions. **Only** the Master User can add and remove users or modify their settings. Settings include assigning security codes and user names. **Only** the Master User can create Smart Scenes. Access to Smart Scenes for other users is controlled by the Master User.
User	Typical users are household members and other authorized persons who can arm and disarm the security system, with controlled access to other system features.
Guest	Visitors and others who are authorized to arm/disarm the system only at certain times or on a temporary basis. [Examples: babysitters, cleaning people, etc.] The Guest's user code can be used to **arm** the system, but cannot **disarm** it unless the system was armed using the Guest code. The Guest's user number is **47**.

Duress Code

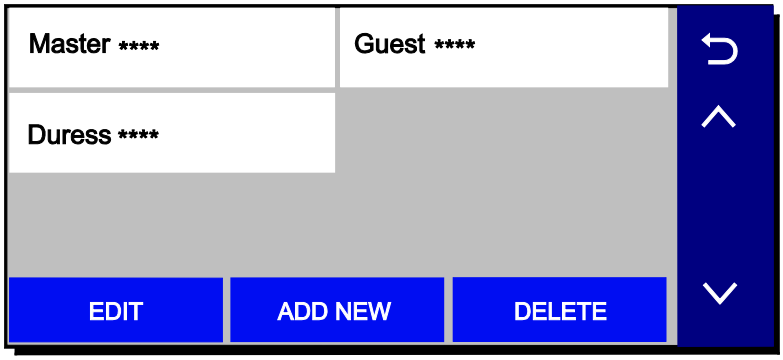
IMPORTANT
The Duress function requires connection to an alarm monitoring service.

Household members and authorized visitors can enter this code if forced to disarm or arm the system under threat. When the Duress code is entered, the Gateway and keypads appear to behave normally, but the system silently notifies your alarm monitoring service. The Duress Code user number is **48**.

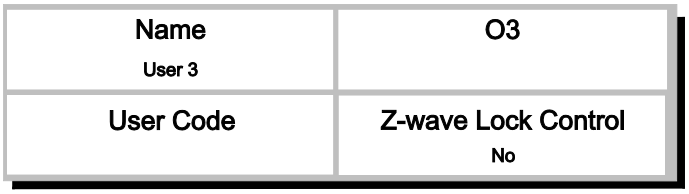
NOTES:
- A security code cannot be assigned more than once. If an existing code is entered, the system displays the warning **User code not accepted!** If this occurs, press **OK** to return to user settings and assign a different code.
- The system should be disarmed before you work with user codes.
- Limited-access users such as guests and cleaning staff should not be instructed on system functions other than those they will be using.
- The number of user codes supported by a Z-Wave door lock can vary between manufacturers. To ensure compatibility with Gateway, set the length of the Master User code on the door lock to be greater than four digits.

Adding Users and Assigning Codes

1. On the Home screen, press **Security**.
2. Press **Tools**, and enter the Master User code.
3. Select **Users**. Existing Users are displayed, along with the Guest and Duress code listings. Four asterisks appear on each listing that has a security code already established. See User Settings for full details.



4. Create and change settings in the menu shown here (the details may vary):



   a. **Create User**: Press **Add New** and a new user screen like the one pictured above appears. Set the details as desired.
   b. **Define/Change Guest Settings**: Press **Guest** and then **Edit**.
   c. **Set/Change Duress Code**: Press **Duress** and then **Edit**. Enter a 4-digit code.
5. **Save** after making settings. The list of user codes reappears.
6. Press ⮌ to return to the Tools menu.

Changing Security Codes or the Duress Code

The Master User can change other users' names and security codes as well as delete users from the system.

1. Access the **Users** screen as shown above.
2. Select one of the listed users.
3. At the bottom of the screen, press **Edit**. User details appear. **Note** that a user's number in the system, seen at upper right in the user details, cannot be changed.

Deleting a User

The Master user can delete secondary users from the system.

1. Select one of the listed users.
2. At the bottom of the screen, press **Delete**. Gateway requests confirmation.
3. Press **Yes**.

User Settings

User Name

Newly-created users are given a default name. To customize a user's name:

1. Press **Name** at upper left on the display. A keyboard appears.
2. Press **Clear** to delete the default name.
3. Enter the desired name, using as many as 10 characters.
4. **Save**. User details appear.
5. Press **Save** again. The list of users appears, displaying your changes.

User Code

Newly-created users have no security code. To assign a code:

1. Press **User Code**. A keypad appears.
2. Press **Clear** if you are changing an existing code.
3. Enter a four-digit code.
4. Press **Done**. User details appear.
5. **Save**. The list of users appears.

Users and Z-Wave Lock Control

NOTE: This option appears only if Z-Wave devices are connected.

Each user can be given the ability to disarm the system by entering their code to open a Z-Wave lock.

When creating or editing a User:

1. Set **Z-Wave Lock Control** to **Yes**. **Z-Wave Unlocking Door** appears.
2. Select **Disarm**.
3. Press **Save**.

With this setting, entering a user code at any Z-Wave door lock in the system unlocks the door and disarms the security system.

System Settings

Brightness/Volume

Home > Settings

Adjust voice and system sounds with the **Volume** slider. System sounds include zone alert chimes and countdown beeps.

Adjust the Gateway touchpad brightness with the **Brightness** slider.

NOTES:
- Move the brightness and volume sliders and press Save to adjust the settings.
- Voice annunciations are controlled by enabling or disabling PANEL VOICE and CHIME.

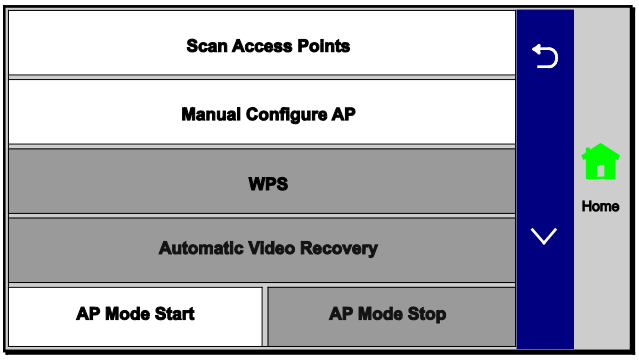
Wi-Fi (Network) Configuration

Home > Security > Tools > enter Master User Code > Network Config

Manage your system's router here. Remember that the Gateway, all mobile devices used to operate the Gateway and all Wi-Fi cameras must be on the same network.

To View or Join Available Wi-Fi Networks

1. On the Tools menu, select **Network Config** then **Configure Network**. A list of Wi-Fi options appears. (If the option is gray, it is not currently available.)



List of Wi-Fi Options

2. Press **Scan Access Points**. A list of available networks is displayed. Use the up and down arrows to scroll through the list. Press ⮌ to return to the previous screen.
3. Select the desired network and press **Edit**. The network information is displayed.
4. If a password is required, press **Key,** enter the password, press **DONE** and **Save**.
5. Press **JOIN** and a confirmation message appears.
6. Press **YES** and the system announces when connected to the network.

Manually Configure Access Point

IMPORTANT
The Security setting below must match the security protocol used by your network router.

1. From the list of Wi-Fi options select **Manual Config AP**. The Wi-Fi enrollment menu appears. (**Network Type** cannot be changed.)
2. Press **SSID Name**, enter your network's name, press **DONE** and **Save**.
3. Press **Security** and choose the same security protocol as your router. Options include **Open**, **WPA/WPA2** and **WPA2**. (WEP is not supported.)
4. If a password is required, press **Key**, enter your network password, press **DONE** and **Save**.
5. Press **JOIN**. A confirmation screen appears.
6. Press **YES** and wait. The Gateway announces when it has connected to the Wi-FI network.

Manually Configure Access Point (Continued)

7. The MyHome Gateway App attempts to connect. Change network settings on all mobile devices that have the MyHome Gateway App to the same network as the Gateway. If necessary re-enroll the device in your system (see Adding (enrolling) mobile devices in your system).

Software Updates

Home > Security > Tools > Advanced

Gateway

Software updates for the Gateway are published periodically. Certain critical updates are installed automatically.

You can see the current version of the Gateway's software at Security > Tools > Advanced > System Information.

Key Fob Firmware *(Wireless Keys)*

SiX™ Series wireless keys:

We recommend that you have the wireless key handy so you can work with it as instructed during this procedure.

1. On the **Advanced** menu, press **Update Keyfob Firmware**.
2. Press **Start** and follow the instructions on the screen.
3. Press **Stop** when the update is complete.
4. Press ⮌ to return to the **Advanced** menu.

Other types of Wireless Keys:

Ask your installer about updating your system's other wireless keys.

Events

Home > Security > Tools > Events

The Gateway keeps a log of system events such as:

- Arm/Disarm
- Alarm, Trouble and Fault
- Changes in status of Z-Wave devices

The system can save up to 6000 events. When the log is full, the oldest 2000 entries are deleted to make room for logging new events.

Logs can be viewed at the MyHome Gateway App or on Total Connect Remote Services.

See Event Log Codes for a list of logged events and how they are displayed.

Viewing Events

On the Tools menu, press **Events**. The MyHome Gateway App Events screen lists all events, sorted chronologically.

Paired Devices

Home > Security > Tools > Paired Devices

This menu displays the name of mobile devices connected to Gateway via the **MyHome Gateway** app.

The mobile device name is listed here when the app is first configured for use with Gateway.

To disconnect a device, touch its listing on the screen and press **Delete**.

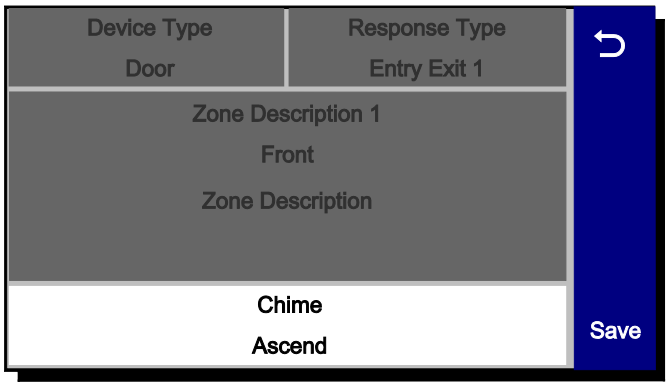
Press **Yes** to confirm.

Edit Chime

Home > Security > Tools > Edit Chime

This menu lets you edit chime sounds for select zones.

To change the chime sound for a zone, select a zone from the Zone list and press **Edit.** Press the Chime button until the desired sound is displayed and press **Save**.



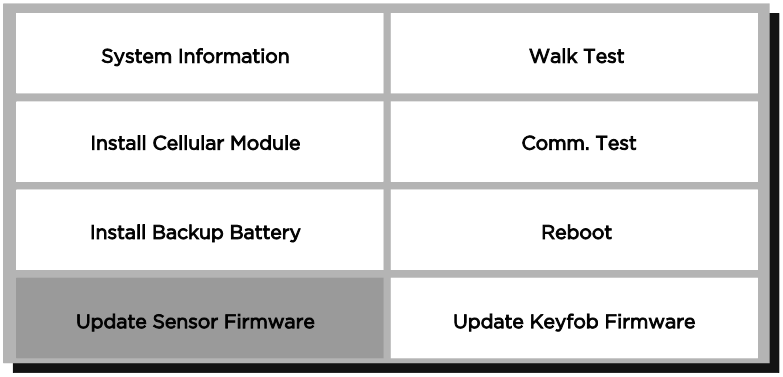
Testing Your System

NOTE: TESTING SHOULD BE PERFORMED WEEKLY.

Before testing, the system should be disarmed and all protected doors and windows closed. The systems should be in Ready to Arm state.

No alarm messages are sent to your alarm monitoring company during these tests.

Press **Tools** and enter the 4-digit Master User code. Press **Advanced**.



Testing Sensors (Walk Test)

Home > Security > Tools > Advanced > Walk Test

Start by pressing **Walk Test**.

The Gateway's internal sounder loudly sounds and **Walk Test – Home to Quit** appears. The Gateway then beeps every 30 seconds as a reminder that the system is in Test mode.

Note that Walk Test mode automatically quits after 4 hours.

Doors and Windows	Open each protected door and window in turn and listen for the set device chime from the Gateway. If PANEL VOICE is enabled, each zone's voice descriptor is announced. Identification of protection points with problems should appear on the MyHome Gateway App screen. Notifications of problem zones clear when the door or window is closed.
Motion Sensors	Walk in front of each sensor and listen for three beeps and/or voice descriptors. The device's identification should appear on the display when it is activated. The display clears when no motion is detected. **NOTE**: If wireless motion detectors are in use, there is a 3-minute delay between activations, which helps preserve battery life.
Fire/Carbon Monoxide sensors	Follow the manufacturer's instructions to test these devices. When a device is activated, its identification should appear on the MyHome Gateway App screen.

IMPORTANT

When testing smoke detectors, keep the Gateway in test mode for **at least one minute (60 seconds)** after testing the detector to avoid sending unwanted alarm messages to your central station monitoring company.

If there is a problem with any sensor (no confirming sounds, no display), notify your service company.

When all sensors have been checked (and doors and windows closed), no zone identification numbers should be displayed.

Finish by pressing **Home** and entering the Master User code.

Testing Communications

Home > Security > Tools > Advanced > Comm. Test

These tests check the system's cellular network and internet (Wi-Fi/Ethernet) connections.

On the Advanced menu, press **Comm. Test**. The options may vary with the devices installed in your system. Select the desired option to test connectivity and/or send test messages to the Central Station.

If the test is successful, the MyHome Gateway App screen displays **Service OK** or **ACK Received**. Details of the test may be shown.

Test Ethernet	Checks internet connectivity without sending test messages.
Send Any	Sends test messages via all available connections.
Send Cellular Message	Sends test messages via cellular network.
Send Ethernet Message	Sends test messages via internet.

Finish by pressing ⮌ to run a different test or by pressing **Home**. Enter the Master User code if prompted.

Reboot

Home > Security > Tools > Advanced > Reboot

Press **Reboot** to restart the Gateway if required.

Press **Yes** to proceed.

Maintenance

The Gateway is designed to require little maintenance. However, testing your system is strongly recommended, and regular cleaning is suggested.

- Test the system weekly.
- Test your system after any alarm occurs.

See Testing Your System for more information.

Care and Cleaning

- Do not slam sensor-protected doors or windows.
- Keep dust from accumulating on the Gateway and sensors, particularly motion sensors and smoke or carbon monoxide detectors.
- The Gateway and sensors should be cleaned carefully with a soft, dry cloth. Do not clean the components with water or any other liquids.

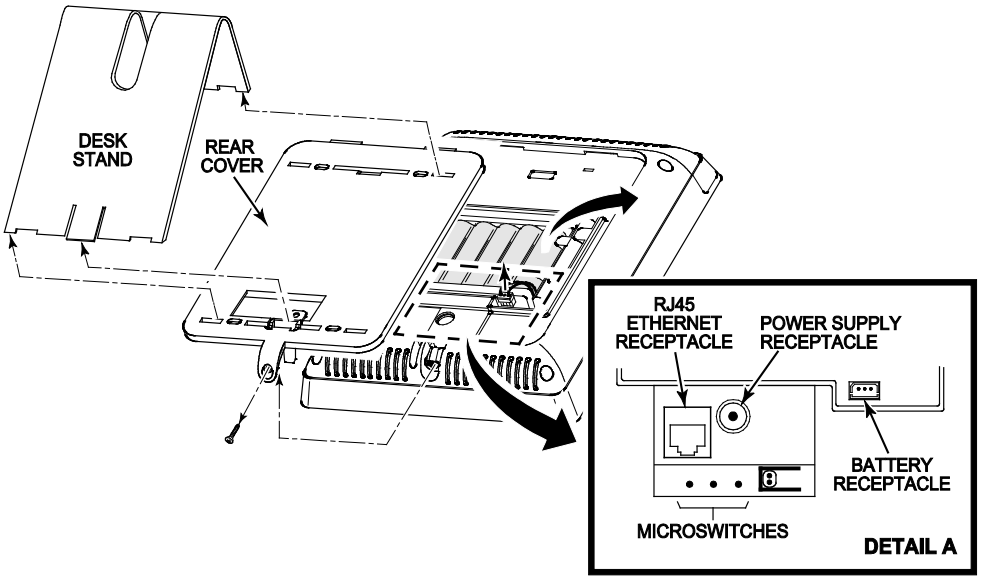
Battery Replacement

Home > Security > Tools > Advanced > Install Backup Battery

IMPORTANT
Replace the battery pack when the Security menu displays **Low Battery** with no zone number specified.
Use only batteries recommended by the installer or the manufacturer.
Disarm the system before changing the Gateway's battery pack.
Remember that you must enter the Master User code for access to the Tools menu.

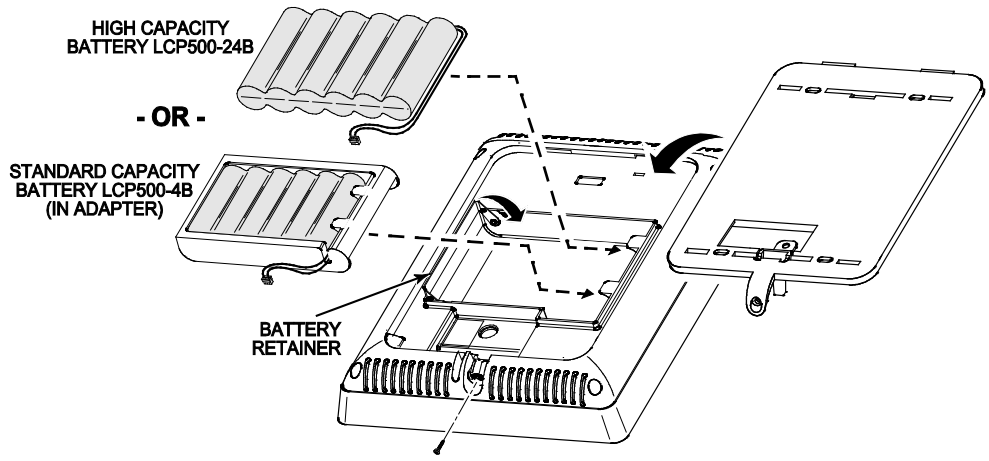
Gateway

1. On the **MyHome Gateway** App, navigate to the **Advanced** menu and select **Install Backup Battery.** A confirmation request appears; press **Yes** and **leave the battery installation procedure screen open.**
2. If mounted on a wall, remove the screw from the rear cover and separate the Gateway from the rear cover.
3. If using a desk stand, remove the desk stand from the back of the Gateway, then remove the bottom screw and separate the Gateway from the rear cover.
4. Unplug the power cord (and Ethernet cable, if used) from the back of the Gateway.



Gateway Battery Replacement (Continued)

5. Disconnect the battery pack from the battery receptacle, raise the battery retainer and remove the battery pack from the battery compartment.
6. Install the new battery pack in the battery compartment and secure with the battery retainer.



7. Connect the battery to the battery receptacle inside the battery compartment.
8. Reattach the rear cover to the Gateway and secure it in place with the screw.
9. Plug the power cord (and Ethernet cable, if used) back into the receptacle(s).
10. Return the Gateway to its mounting location (on the wall, or reattach the desk stand).
11. On the MyHome Gateway App screen, press OK on the battery installation procedure screen. The system confirms “Battery successfully installed".
12. Press OK. The system returns to the Advanced menu.
13. Press ⮌ to return to the previous screen(s).

Sensors

IMPORTANT
The Gateway beeps every 40-45 seconds when a sensor reports a low battery. A sensor with a low battery will continue to operate for up to 30 days. However, the battery must be replaced within 30 days of this audible warning beginning to sound.

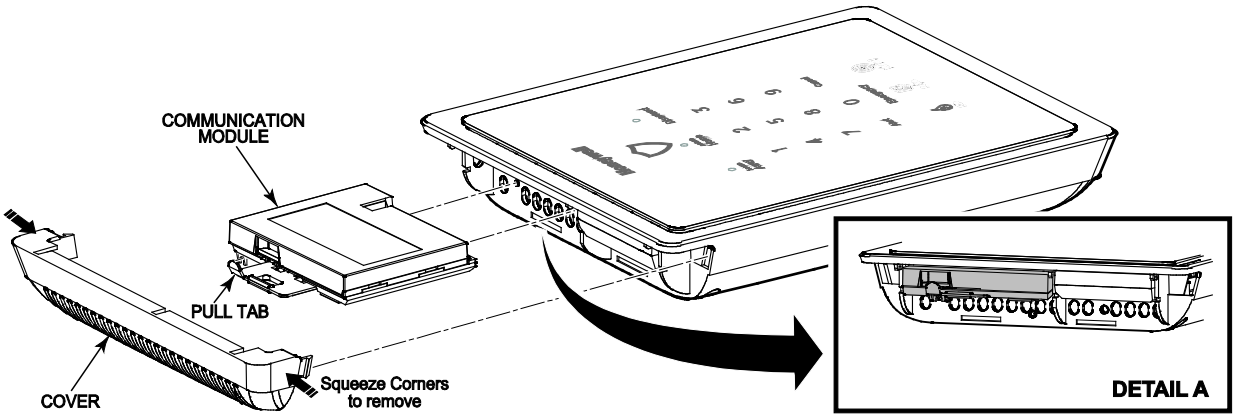
Clear sensor low-battery warnings by entering a user code on the Gateway. Follow the sensor’s battery replacement instructions.

NOTES: For SiX™ series sensors and wireless keys, remove the battery and wait about 10 seconds before installing the replacement battery.

Communication Module Replacement

Home > Security > Tools > Advanced > Install Cellular Module

Refer to the illustrations below and follow these steps to replace a communication module:



1. Make sure the system is disarmed.
2. From the MyHome Gateway App, select **Security**, then **Tools**.
3. Enter the 4-digit Master User code.
4. Select **Advanced**, then **Install Cellular Module**.

   Follow the on-screen instructions for changing the module.
5. Squeeze inward on the corners of the top cover and remove the top cover as shown.
6. Use the Communication Module pull tab to remove the old module.
7. Insert the replacement Communication module as shown.
8. Press **OK** on the **MyHome Gateway App** screen and the system confirms installation.
9. Press **OK**. The system returns to the **Advanced** menu.
10. Reboot the Gateway (Home > Security > Tools > Advanced > Reboot).

MyHome Gateway App Symbols

Zone numbers, location and other information may be displayed with status indications. Failure and Trouble indications and panel **Emergency** indications appear in red.

System Status and Security

Alarm		Bypassed Zone		Automation Failure (Z-Wave problem)	
Fire Alarm		Restart Timer (more Exit time)		Door Open	
CO Alarm		Trouble/Alert Details on Security menu		Window Open	
Arm Away		Communication Trouble		Glass Break	
Arm Home		AC Power Loss		Fire or Heat Sensor	
Arm Custom		Low Battery		Flood Sensor	
Arm Night Home		No Battery			
Disarm					

Features/Various

Icons may appear in red or orange to indicate device status. Problems involving Z-Wave devices are indicated by the Automation icon appearing in gray on the Home screen.

Tools		Network (Wi-Fi). Configuration		Locks	
Users		Automation		Garages	
Events		Switches		Water Valves	
Advanced		Thermostats			
Paired Devices		View Zones or Edit Chime			

Date and Time Gateway's clock and calendar are updated via the Gateway's network connections.

Event Log Codes

The Gateway's Event Log can record and display as many as 6000 system events. Events are stored locally in the Gateway, in chronological order and sent to your monitoring company as needed. When the maximum number of stored events is reached, the oldest 2000 entries are deleted to make room for logging new events.

The Event log, viewed from the MyHome Gateway App, provides a description of the event and an event code. The tables below provide definitions of the events/codes that may be transmitted to the Central Station and/or displayed by the MyHome Gateway App. ("E" Codes indicate an Event and "R" codes indicate the event was Restored.)

NOTE: If the Gateway's backup battery is exhausted after AC power is lost, any system activity occurring after Low Battery notification is not saved. Additionally, the Gateway reverts to the status condition as before the low battery notification.

Event Log Codes		
Event Code	**Definition**	**Event Log Display**
110	Alarm, Fire	Fire
121	Alarm, Duress	Duress
122	Alarm, Silent	Silent
123	Alarm, Audible	Audible
131	Alarm, Perimeter	Perimeter
132	Alarm, Interior	Interior
134	Alarm, Entry/Exit	Entry/Exit
135	Alarm, Day/Night	Day Night
137	Alarm, Tamper	Tamper
145	Expansion Module Tamper	Expansion Module Tamper
146	Silent Burglary	Silent Burglary
150	24-Hour Non-Burglary	24 Hour Non-Burglary
162	Carbon Monoxide Detected	Carbon Monoxide Detected
301	Trouble, AC Loss	AC Loss
302	Trouble, Low System Battery	Low system battery
305	Trouble, System Reset	System Reset
308	System shutdown	System shutdown
316	System Tamper*	System Tamper
341	Trouble, Case Tamper	Cover Tamper
344	Trouble, RF Receiver Jam Detect	RF Jam Detect
350	Long Range Radio Reset	Long Range Radio Reset
353	Trouble, Long Range Radio Transmitter Fault	Comm. Trouble
354	Failure to Communicate Event	Failure to Communicate Event
373	Trouble, Fire Trouble	Fire trouble
374	Trouble, Exit Error Alarm	Exit error alarm
380	Trouble, Sensor	Sensor trouble
381	Trouble, Loss of Supervision RF	Superv Loss-RF
383	Trouble, Sensor Tamper	Sensor Tamper

Continued next page

Event Log Codes		
Event Code	**Definition**	**Event Log Display**
384	RF Low Battery	RF Low Battery
401	Open/Close by User	Arm Away/Disarmed
403	Open/Close Automatic	Automatic O/C (or Scheduled Arming)
406	Cancel	Cancel
407	Remote Arm/Disarm	Remote Arm/Disarm
408	Quick Arm	Quick arm
441	Armed Home	Arm Home/Disarmed
455	Auto-Arm Failed	Auto-arm Failed
459	Recent Close	Recent Closing
461	Wrong Code Entry	Wrong Code Entry
570	Zone/Sensor Bypass	Zone Bypass
601	Manual Trigger Test Report	Manual Trigger Test Report
602	Periodic Test Report	Periodic test report
606	Listen-in to follow	Listen-in to follow
607	Walk Test	Walk Test Mode
623	Event 90% Full	Event Log 90% Full
627	Program Mode Entry	Program mode entry
628	Program Mode Exit	Program mode exit
654	System Inactivity	System Inactivity
655	Reset Master Code	User Code
759	Resident Monitor Zone Response	Resident Monitor Zone Response
760	Resident Response Zone Response	Resident Response Zone Response
761	General Monitor Zone Response	General Monitor Zone Response
762	General Response Zone Response	General Response Zone Response
3000	Binary Switch Off	Switch Off (Z-Wave Device)
3001	Binary Switch On	Switch On (Z-Wave Device)
3100	Multi Level Switch Change Level (Off)	Multilevel Switch Off (Z-Wave Device)
3101	Multi Level Switch Change Level (On)	Multilevel Switch On (Z-Wave Device)
3200	Garage Door Close	Garage Door Close
3201	Garage Door Open	Garage Door Open
3300	Door Lock Unlocked	Door Unlocked (Z-Wave Device)
3301	Door Lock Locked	Door Locked (Z-Wave Device)
3302	Door Lock Jammed	Door Lock Jammed (Z-Wave Device)
3400	Thermostat Mode Off	Thermostat Mode Off
3401	Thermostat Mode Heat	Thermostat Mode Heat
3402	Thermostat Mode Cool	Thermostat Mode Cool
3403	Thermostat Mode Auto	Thermostat Mode Auto
3404	Thermostat Mode Aux /Em Heat	Thermostat Mode Aux /Em Heat
3405	Thermostat Fan Mode Auto	Thermostat Fan Mode Auto

Continued next page

Event Log Codes		
Event Code	**Definition**	**Event Log Display**
3406	Thermostat Fan Mode Manual On	Thermostat Fan Mode Manual On
3407	Thermostat Fan Mode Circulate	Thermostat Fan Mode Circulate
3408	Thermostat Set Heat Point	Thermostat Set Heat Point (and temperature)
3409	Thermostat Set Cool Point	Thermostat Set Cool Point (and temperature)
3410	Thermostat Hold	Thermostat Hold
3411	Thermostat No Scheduling	Thermostat No Scheduling
3412	Thermostat Normal Mode	Thermostat Normal Mode
3500	Low Battery	Low Battery (Z-Wave Device)
3501	Low Battery Restore	Low Battery Restore (Z-Wave Device)
5000	Critical Panel Firmware Update Downloaded	Critical Panel Update Downloaded

*If your Central Monitoring Station receives a “Comm. Fail” message (E316), your system has been tampered with and may have been compromised. This occurs if no signal is heard from the alarm panel within 15 minutes following a delayed alarm.

Glossary

Arm Away	Enables all exterior and interior security protection provided by door and window sensors and motion detectors.
Arm Custom	Allows authorized users to arm the system with selected zones bypassed or with entry delays disabled.
Arm Home	Enables exterior protection; sounds an alarm if protected doors or windows are disturbed. Allows bypassing of selected zones, permitting movement within the home without unwanted alarms.
Bypass	Allows authorized users to exclude selected protection zones when arming the system.
Disarm	Turns off the security portion of the system. Silences alarms and trouble indicators.
Duress	Special code that can be entered into the system instead of a normal user code. Sends a silent call for assistance while the Gateway appears to behave normally. Requires connection to a central monitoring service.
Emergency	Special keys on the Gateway activate sounders on the premises and optionally send alert messages in various types of emergency. Connection to a central monitoring service is required for outside emergency calls.
Quick Arm	Allows household members to arm the system without entering a user code. This feature can only be enabled by an authorized user.
Quick Exit	Allows an outside door to be opened for a set time period. This feature is used for checking the mailbox, retrieving the newspaper, etc.
Zone	Specific areas of protection in your home. Sensing devices are assigned to these numbered Zones, with designations such as front door, kitchen window, etc. Zone numbers appear on the MyHome Gateway App display when an alarm or fault occurs.

Z-Wave

Controller	The **primary** controller is the main device used to set up and control the Z-Wave network. There can only be one primary controller and it must be used to add/Include or delete/Exclude devices. A primary controller can be a portable device such as a hand-held remote, a permanently mounted control panel, a Z-Wave enabled PC or a Z-Wave enabled Ethernet router/bridge. A **secondary** controller cannot be used to add or delete devices. If the secondary controller is the same model as the primary, it has all of the primary's capabilities, but cannot be used to add or delete devices.
Exclude	When a device is Excluded, it is removed from the system. Excluding the device also removes the network pairing from the device's memory. In this document, the term Exclude is used interchangeably with "Delete".
Include	Including a device pairs it with the Gateway so the two can communicate. In this document, the term Include is used interchangeably with "Add".

Important Note: A device must be Excluded before it can be moved to another network or re-Included after using the Defaulting the Controller option.

Fire/CO Alarm System

Your fire alarm system (if installed) is active 24 hours a day, providing continuous protection. In the event of an emergency, the installed smoke, heat and/or carbon monoxide detectors automatically activate your security system, triggering a loud, intermittent tone from the Gateway and the mobile device when using the MyHome Gateway App. The sound alternates with the voice announcement, sounding every 15 seconds. A "FIRE" or "CO" message announces on the Gateway, or appears on the MyHome Gateway screen and remains on until you silence and clear the alarm display.

In Case of Fire

1. Should you become aware of a fire emergency before your detectors sense the problem, go to the Gateway touchpad and press **Emergency** and then press **Fire**. The alarm sounds and an alarm is transmitted to the central station (if programmed to do so).
2. Evacuate all occupants from the premises.
3. If flames and/or smoke are present, leave the premises and notify your local Fire Department immediately.
4. If no flames or smoke are apparent, investigate the cause of the alarm. The zone number of the zone(s) in an alarm condition appears on the MyHome Gateway screen.

In Case of Carbon Monoxide Alarm

1. If a high level of carbon monoxide is detected you should evacuate all occupants from the premises and immediately move to a location where fresh air is available, preferably outdoors.
2. From a safe area, contact your central monitoring company for further instructions.

Silencing a Fire/Carbon Monoxide Alarm

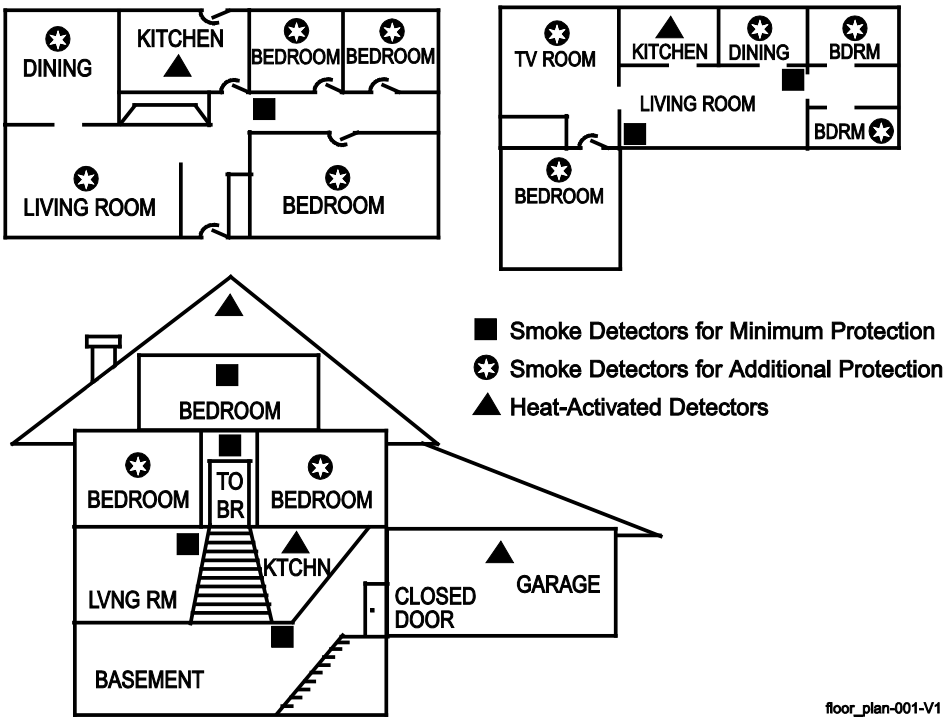
1. Silence the alarm by entering a valid User code.
2. To clear the alarm, enter a valid User code again.
3. If the MyHome Gateway App screen indicates a trouble condition after entering the Master User code a second time, check that smoke detectors are not responding to smoke- or heat-producing objects in their vicinity. Should this be the case, eliminate the source of heat or smoke.
4. If this does not remedy the problem, there may still be smoke in the detector. Clear it by fanning the detector for about 30 seconds.
5. When the problem has been corrected, clear the display by entering a valid User code again.

National Fire Protection Association Smoke Detector Recommendations

With regard to the number and placement of smoke and heat detectors, we subscribe to the recommendations contained in the National Fire Protection Association's (NFPA) Standard #72 noted below.

Early warning fire detection is best achieved by the installation of fire detection equipment in all rooms and areas of the household. The equipment should be installed as follows: A smoke detector installed outside of each separate sleeping area, in the immediate vicinity of the bedrooms and on each additional story of the family living unit, including basements and excluding crawl spaces and unfinished attics.

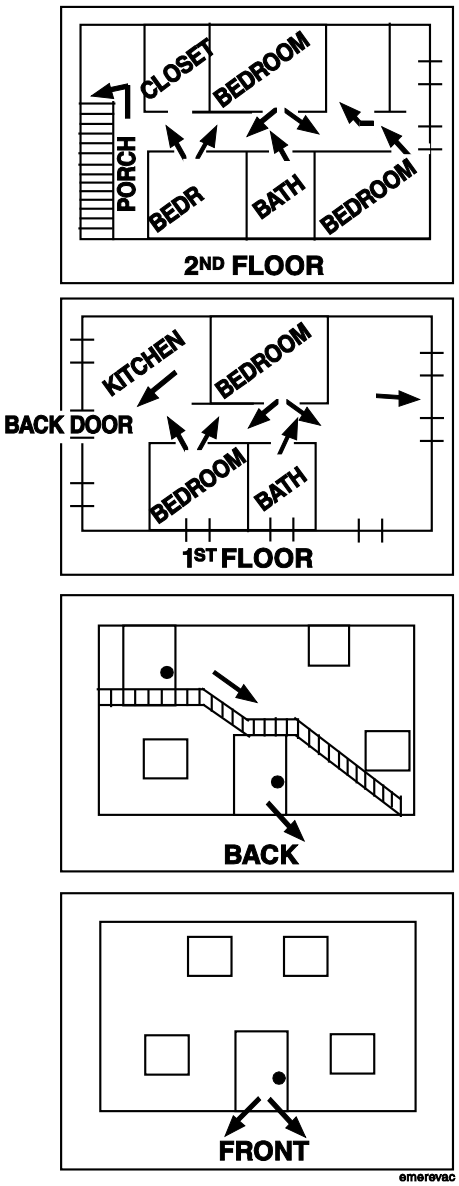
In addition, the NFPA recommends that you install heat or smoke detectors in the living room, dining room, bedroom(s), kitchen, hallway(s), attic, furnace room, utility and storage rooms, basements and attached garages.



Emergency Evacuation

Establish and regularly practice a plan of escape in the event of fire. The following steps are recommended by the National Fire Protection Association:

1. Position your detector or your interior and/or exterior sounders so that they can be heard by all occupants.
2. Determine two means of escape from each room. One path of escape should lead to the door that permits normal exit from the building. The other should be an alternative escape, such as a window, should your path to that door be impassable. Station an escape ladder at such windows if there is a long drop to the ground.
3. Sketch a floor plan of the building. Show windows, doors, stairs and rooftops that can be used to escape. Indicate escape routes for each room. Keep these routes free from obstruction and post copies of the escape routes in every room.
4. Assure that all bedroom doors are shut while you are asleep. This will prevent deadly smoke from entering while you escape.
5. Try the door. If the door is hot, check your alternate escape route. If the door is cool, open it cautiously. Be prepared to slam the door if smoke or heat rushes in.
6. When smoke is present, crawl on the ground. Do not walk upright, since smoke rises and may overcome you. Clearer air is near the floor.
7. Escape quickly; don't panic.
8. Establish a place outdoors, away from your house, where everyone can meet and then take steps to contact the authorities and account for those missing. Choose someone to assure that nobody returns to the house — many die going back.



Regulatory Agency Statements

FEDERAL COMMUNICATIONS COMMISSION (FCC) & 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.

CLASS B DIGITAL DEVICE 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 Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Cet appareil est conforme à la partie 15 des règles de la FCC et exempt de licence RSS d'Industrie 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 antenna(s) used for this device must be installed to provide a separation distance of at least 7.8 inches (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: La/les antenne(s) utilisée(s) pour cet émetteur doit/doivent être installée(s) à une distance de séparation d'au moins 20 cm (7,8 pouces) de toute personne 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 ISED.

IMPORTANT NOTE ABOUT EXTERNAL ANTENNAS

If an external cellular radio antenna is used, the antenna may be installed or replaced ONLY by a professional installer.

TO THE INSTALLER

Lyric-3G, Lyric-3GC: The external antenna must not exceed a maximum directional gain (including cable loss) of 6.0 dBi at 850 MHz and 2.5 dBi at 1900 MHz. Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified in FCC Parts 22H and 24E and 27, and IC RSS-130, RSS-132, RSS-133, and RSS-139.

Lyric-CDMA: The external antenna must not exceed a maximum directional gain (including cable loss) of 9.3 dBi at 850 MHz and 8.2 dBi at 1900 MHz. Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified in FCC Parts 22H and 24E and 27.

LYRICLTE-A, LYRICLTE-C: This device is to be used in mobile or fixed applications only. For mobile and fixed operating configurations the antenna gain, including cable loss, must not exceed 3.25 dBi (US) or 0.6dBi (Canada) at 850 MHz, 5.5 dBi at 1700 MHz, 2.5dBi at 1900 MHz for satisfying RF exposure compliance. Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified in Part 22H and 24E and 27, and IC RSS-130, RSS-132, RSS-133, and RSS-139.

LYRICLTE-V: This device is to be used in mobile or fixed applications only. For mobile and fixed operating configurations the antenna gain, including cable loss, must not exceed 7.31 dBi at 780 MHz, 7.35 dBi at 1700 MHz for satisfying RF exposure compliance. Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified in Part 22H and 24E and 27.

Wireless Keys

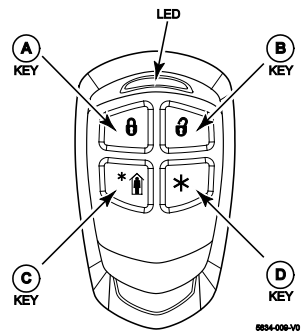
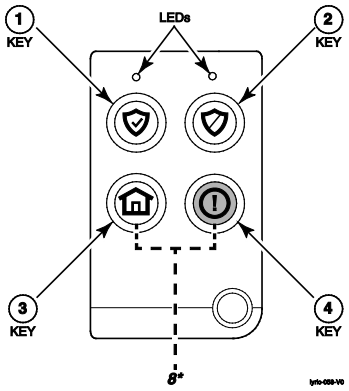
IMPORTANT SECURITY NOTICE

Your wireless key (key fob) is similar to your keys or access card. If lost or stolen, another person can compromise your security system. Immediately notify your Dealer/Installer of a lost or stolen wireless key. The Dealer/Installer will then remove the wireless key programming from the security system.

Key Assignments

Your wireless keys (key fobs) are set up by your installer. It is advisable to write down each button's preprogrammed function in the space below.

NOTES: • One or more buttons may have been programmed for Emergency function.
• To activate a button function, press and hold the button for 1-2 seconds.

Button A: _____ Button B: _____ Button C: _____ Button D: _____	5800 Series wireless key 
Button 1: _____ Button 2: _____ Button 3: _____ Button 4: _____ Button *8**: _____ *(press and hold BOTH buttons to activate)*	SiX™ Series wireless key 

SiXFOB Wireless Key Status Indications

Press and release any key for system status. Status is indicated by the LEDs at the top of the key fob.

Green LEDs	Red LEDs	Sounder	System Status
Rapid Flash – Alternating about 8-20 seconds, then ON for 3 seconds	Off	Chirp for confirmation	Device Enrollment
Off	ON 2-3 seconds	2 Beeps	System Armed (any mode)
Off	Slow Flash for 2-3 seconds	4 Beeps	Alarm in progress or System is in Audible Emergency (Panic) Mode
ON 2-3 seconds	Off	1 Beep	Disarmed, Ready to Arm
Slow Flash for 2-3 seconds	Off	Silent	Disarmed, Not Ready to Arm
Flash once (both LEDs)	Off	Silent	RF Transmission
Off	Off	1 Second beep	Not Hearing from the Gateway
Rapid Flash for 2 seconds	Off	Silent	Deleting wireless key from system

Your System Information

Your local Honeywell dealer is the person best qualified to service your alarm system. Arranging a program of regular service is advisable.

Security Company/Installer:

Name: _____ Phone: _____

Address: _____

_____

DELAY DURATIONS, ARMING OPTIONS AND EMERGENCY TYPES

Exit Delay time _____ Entry Delay 1 time _____ Entry Delay 2 time _____

ARM NIGHT enabled ☐ Yes ☐ No Zones _____

AUTO HOME enabled ☐ Yes ☐ No Restart Exit Delay enabled ☐ Yes ☐ No

QUICK ARM enabled ☐ Yes ☐ No QUICK EXIT enabled ☐ Yes ☐ No

CHIME mode enabled ☐ Yes ☐ No Audio Alarm Verification enabled (Two-Way Voice) ☐ Yes ☐ No

FIRE ☐ Yes ☐ No

MEDICAL ☐ Yes ☐ No

POLICE ☐ Yes ☐ No ☐ Silent

Alarm Reporting Delay _____

SYSTEM USERS			
Keep track of authorized system users in the chart below. This record should be kept secure by the Master User.			
User #		**User Code**	**Comment/Description**
02 (preset)	Master User		Can add and modify Users. Can add, modify, edit and run all Smart Scenes.
47 (preset)	Guest		The Guest user code can be used to arm the system, but cannot disarm it unless the system was armed using the Guest code.
48 (preset)	Duress		Enter this code if forced to disarm/arm the system under threat. System appears to behave normally, but silently notifies alarm monitoring service.
03			
04			
05			
06			
07			
08			
09			
10			
11			
12			
13			
14			

ZONES	
Zone Number	Location and Description

SMART SCENES	
Smart Scene Name	Description

Z-WAVE DEVICES		
Type	Name	Location

Notes

Notes

Notes

Notes

Index

OWNER'S INSURANCE PREMIUM CREDIT REQUEST

This form should be completed and forwarded to your homeowner's insurance carrier for possible premium credit.

A. GENERAL INFORMATION:

Insured's Name and Address: _____

_____

Insurance Company: _____ Policy No.: _____

Lyric™ Gateway Other _____

Type of Alarm: ☐ Burglary ☐ Fire ☐ Both

Installed by: _____ Serviced by: _____

Name Name

_____

Address Address

B. NOTIFIES (Insert B = Burglary, F = Fire)

Local Sounding Device _____ Police Dept. _____ Fire Dept. _____

Central Station ☐ Name: _____

Address: _____

Phone: _____

C. POWERED BY: A.C. with Rechargeable Power Supply

D. TESTING: ☐ Quarterly ☐ Monthly ☐ Weekly ☐ Other _____

E. SMOKE DETECTOR LOCATIONS

☐ Furnace Room ☐ Kitchen ☐ Bedrooms ☐ Attic

☐ Basement ☐ Living Room ☐ Dining Room ☐ Hall

F. BURGLARY DETECTING DEVICE LOCATIONS:

☐ Front Door ☐ Basement Door ☐ Rear Door ☐ All Exterior Doors

☐ 1st Floor Windows ☐ All Windows ☐ Interior Locations

☐ All Accessible Openings, Including Skylights, Air Conditioners and Vents

G. ADDITIONAL PERTINENT INFORMATION:

_____

_____

_____

_____

_____

Signature: _____ Date: _____

Limitations of This Alarm System

WARNING!

While this system is an advanced design security system, it does not offer guaranteed protection against burglary or fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

- Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
- Intrusion detectors (e.g. passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Battery operated devices will not work without batteries, with dead batteries, or if the batteries are not put in properly. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.
- Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
- A user may not be able to reach a panic or emergency button quickly enough.
- While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second floor detector, for example, may not sense a first floor or basement fire. Moreover, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson. Depending upon the nature of the fire and/or the locations of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.
- Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of protected area approaches the temperature range of 90° to 105°F, the detection performance can decrease.
- Alarm warning devices such as sirens, bells or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices sound on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm warning devices, however loud, may not warn hearing-impaired people or waken deep sleepers.
- Communication paths needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily out of service. Communication paths are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.
- This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 10 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly.

Installing an alarm system may make one eligible for lower insurance rates, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property.

We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

For patent information, see www.honeywell.com/patents

TWO YEAR LIMITED WARRANTY

Honeywell International Inc., acting solely through its Security and Fire 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.

Ref: LCP300-L/LCP300-LC

800-21670 10/16 Rev B

Honeywell

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

www.honeywell.com/security