Lyric® Gateway

Honeywell

THE POWER OF **CONNECTED**

Installation and Reference Guide

RECOMMENDATIONS FOR PROPER PROTECTION

The Following Recommendations for the location of fire and burglary detection devices help provide proper coverage for the protected premises.
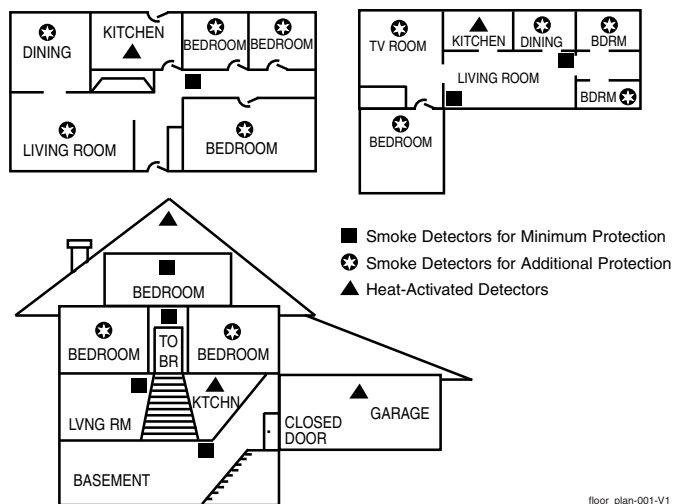
Recommendations for Smoke and Heat Detectors

With regard to the number and placement of smoke/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 as follows: For minimum protection a smoke detector should be installed outside of each separate sleeping area, and on each additional floor of a multi-floor family living unit, including basements. The installation of <u>smoke detectors</u> in kitchens, attics (finished or unfinished), or in garages is not normally recommended.

• For additional protection the NFPA recommends that you install <u>heat</u> or <u>smoke detectors</u> in the living room, dining room, bedroom(s), kitchen, hallway(s), attic, furnace room, utility and storage rooms, basements and attached garages.

In addition, we recommend the following:

• Install a smoke detector inside every bedroom where a smoker sleeps.

• Install a smoke detector inside every bedroom where someone sleeps with the door partly or completely closed. Smoke could be blocked by the closed door. Also, an alarm in the hallway outside may not wake up the sleeper if the door is closed.

• Install a smoke detector inside bedrooms where electrical appliances (such as portable heaters, air conditioners or humidifiers) are used.

• Install a smoke detector at both ends of a hallway if the hallway is more than 40 feet (12 meters) long.

• Install smoke detectors in any room where an alarm control is located, or in any room where alarm control connections to an AC source or phone lines are made. If detectors are not so located, a fire within the room could prevent the control from reporting a fire or an intrusion.

> **THIS CONTROL COMPLIES WITH NFPA REQUIREMENTS FOR TEMPORAL PULSE SOUNDING OF FIRE NOTIFICATION APPLIANCES.**

■ Smoke Detectors for Minimum Protection
✪ Smoke Detectors for Additional Protection
▲ Heat-Activated Detectors

floor_plan-001-V1

Recommendations for Proper Intrusion Protection

• For proper intrusion coverage, sensors should be located at every possible point of entry to a home or 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. This will ensure that alarm signals can be sent to the alarm monitoring station in the event that the communications are out of order (if connected to an alarm monitoring station).

Table of Contents

Table of Contents *(Continued)*

Lyric Lock

This system supports Lyric Lock, an advanced feature designed to keep it functioning optimally. Lyric Lock capabilities include: the ability to interact with Honeywell and your company's network for the setup and programming of system features, support for remote software updates and the ability to enhance the end user's security by preventing unauthorized takeover of the system by another monitoring company.

In the event that the end user wishes to authorize another company to take over the system, the end user may request that Honeywell remotely disable Lyric Lock. Honeywell will require documentation that the end user has attempted to contact your company three times and that your company has failed to respond, or failed to agree to the end user's request.

System Features

The Lyric Gateway is a self-contained, rechargeable wireless control/communicator that features easy installation and usage. A built-in speaker provides voice annunciation of system status along with voice descriptors of each zone. An internal module allows the Gateway to communicate with the Central Station via the Internet or (if installed) Cellular Wireless.

ETL	**Lyric Gateway is not intended for UL985 Household Fire applications unless a 24-hour backup battery (p/n 300-03866-AIO) is installed.**

System Features

- Voice Announcement of System and Zone Status
- 10 User-selectable Chime Sounds
- Automatic Stay Arming
- Arm Night Arming
- 48 User Codes (Installer, Master, Guest, Duress)
- Panic (Emergency) Functions (Police, Fire, Medical)
- Video Camera Control (requires Wi-Fi® connection)
- Supports Mobile Devices (Tablet, iPAD®, etc.) that duplicate functions of the Lyric Gateway (i.e.; Security, Web Content, Home Automation and Video Control). Requires Android Operating System Version 4.4 or higher or iOS Version 8.0 or higher.
- Wall or Desk mounting

Home Automation

- Integrated Z-Wave® Support
- Control up to 72 Z-Wave Home Automation Devices including:
  - Thermostats (up to 6)
  - Door Locks (up to 6)
  - Devices (outlets, switches, lamps/appliances) (up to 60)
  - Garage Doors (up to 4)
  - Water Valves (up to 4)
- Supports Z-Wave Network Wide Inclusion (NWI) Mode
- 100 programmable Smart Actions
- Up to 150 scheduled events

Zones and Devices

- 3 Panel Panic (Emergency) Zones
- 64 Wireless Protection Zones (5800 and SiX™ Series transmitters)
- 8 Monitored (Garage) Zones
- 32 Wireless Button (Wireless Key) Zones (5800 and SiX™ Series transmitters)
- 8 Wireless Keypad Zones (SiX™ Series)
- 8 Smart Device Zones
- 12 Temperature Zones
- Resident Monitor Zone Types
- Built-in Case Tamper

Communication

- ADEMCO Contact ID
- Integrated Wi-Fi Support
- Cellular (GSM or CDMA) Central Station communication
- Wi-Fi Central Station communication
- Ethernet Central Station communication
- Two-way Voice Communication
- Supports AlarmNet 360™ Cloud-based programming
- Supports TotalConnect ® Remote Services
- Supports MyHome Gateway app (iOS and Android™)

System Features *(Continued)*

System Power

- Primary Power: Plug-in Power Supply, 110VAC to 9VDC, 2.5A output p/n 300-05763V1 (300-05763V1 – CAN in Canada)
- Backup Battery: Rechargeable Nickel-metal Hydride Battery Pack rated at 7.2Vdc. LCP500-4B (p/n 300-03864-AIO) 1,100mAh or LCP500-24B (p/n 300-03866-AIO) 3,700mAh

Alarm Output

- Built-in (85dB) Sounder
- Steady Output for burglary/panic
- Temporal (3) Pulse Output for fire alarms
- Temporal (4) Pulse Output for carbon monoxide alarms
- Audio Alarm Verification (AAV)

Programming

- Options stored in EEROM
- Can be uploaded, downloaded or controlled via AlarmNet 360™ using capable Cellular or Wi-Fi Communications Module or Ethernet connection
- Flash Downloading

Other Features

- Exit Error feature (detects difference between an actual alarm and exit alarm caused by leaving a door open after the exit delay expires)
- Keypad Lockout (detects invalid code entries and locks out keypad for a 15 minute period)
- Event Log Storage (total 6,000 events)
- RF Jam Detection
- Advanced Protection Logic™ (APL) (Minimizes the likelihood of the system being disabled before notification can be sent to the Central Station indicating that the premises have been compromised.)
- Lyric Lock (Customer Retention Logic) Dealer selectable Lockout (anti-takeover) feature
- Dealer/Central Station Messages (requires TotalConnect Service)

Installing the Gateway

Backup Battery Installation

The Lyric Gateway is equipped with an integral, replaceable, rechargeable battery pack rated at 7.2Vdc. In the event of an AC power loss, the system is supported by the long life backup battery that is supervised for connection and for low voltage conditions. If the battery is missing, or a low battery condition is detected, a "low battery" message is displayed on the Smart Device and "Alert" will flash red on the Gateway. In addition, a System Low Battery report is sent to the Central Station. In addition, the system will beep once every 45 seconds to audibly indicate a low battery condition (press any key to stop the beeping). Select the appropriate battery pack, based on the installation's requirement, and install the battery pack. Follow the steps and refer to the figure below to install and connect the battery.

Battery Selection

Select the appropriate battery pack, based on the installation's requirement, and install the battery pack.

Battery Part Number	Battery StandbyTime	Low Battery Notification
LCP500-4B (300-03864-AIO)	4-hours (minimum)	Approximately 1-hour before battery depletion
LCP500-24B (300-03866-AIO)	24-hours (minimum)	At least 1-hour before battery depletion

Replacing the Rechargeable Backup Battery

1. Insert the battery pack into Gateway.
2. Close the hinged battery retainer.
3. Connect the battery pack connector to the receptacle on the Gateway.
4. Align the slots on the back of the Gateway with the hooks on the rear cover/wall mount as shown below.
5. Once attached, insert the screw to secure the rear cover/wall mount.
6. Plug the power supply into a 24-hour, 110VAC unswitched outlet. Upon power-up, the LEDs will flash alternately.
7. When the power-up sequence is complete, the green Disarmed LED and the green shield will be lit.
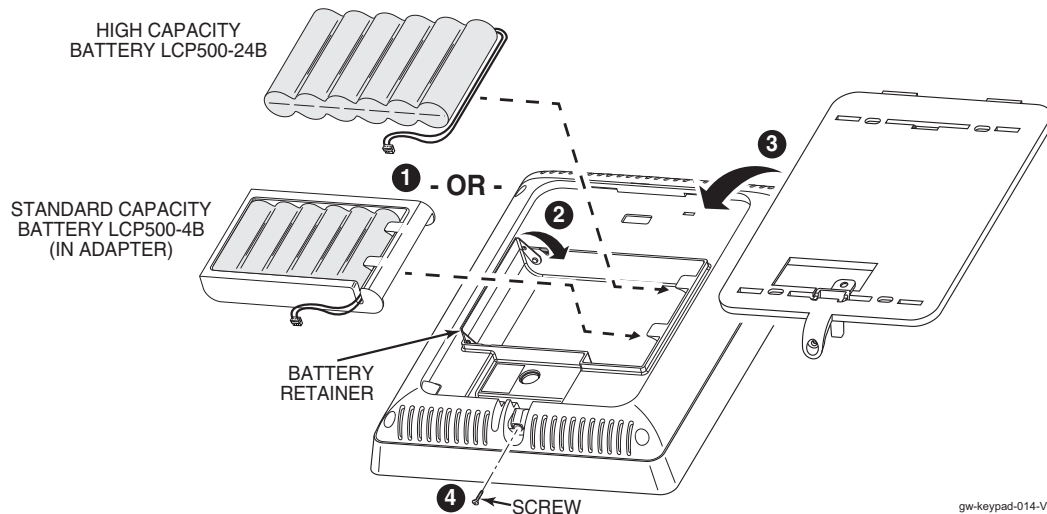
> Rechargeable batteries may take up to 48-hours to fully charge. The "Low Battery" message should clear within four hours or by entering Test Mode.

Replacing the Rechargeable Backup Battery

1. When battery replacement is required, at the Installer Tools screen on the AN360 App, select the "Advanced" icon.
2. Select "Install Backup Battery" and follow the displayed steps to replace the battery or follow the steps below.

Remove the battery

1. Remove the screw securing the Gateway to the rear cover/wall mount (if used).
2. Remove the back case or remove the Gateway from the rear cover/wall mount.
3. Disconnect the battery pack connector from the receptacle on the back of the Gateway.
4. Open the hinged battery retainer.
5. Remove the battery pack from the Gateway.

Installing the Gateway (Continued)

Install the replacement battery

1. Install a replacement battery pack (LCP500-4B [p/n 300-03864-AIO] OR LCP500-24B [p/n 300-03866-AIO]) into the Gateway.
2. Close the hinged battery retainer.
3. Connect the battery pack connector to the receptacle on the Gateway.
4. Align the slots on the back of the Gateway with the hooks on the rear cover/wall mount as shown below.
5. Once attached, insert the screw to secure the rear cover/wall mount.
6. Plug the power supply into a 24-hour, 110VAC unswitched outlet. Upon power-up, the LEDs will flash alternately.
7. When the power-up sequence is complete, the green Disarmed LED and the green shield will be lit.

NOTE: If a Cellular Communication Module is being installed, verify the module's signal strength before selecting a final mounting location. Refer to *Checking the Signal Strength* in the Communications Module section.

Wall Mounting

NOTE: When selecting a location for the Lyric Gateway, be sure to provide a separation of at least 10 feet between 2.4GHz devices such as Wi-Fi Routers/Access Points.

For wall mounting follow the steps and refer to the figure below.

1. Feed the field wiring through the appropriate openings in the wall mount.
2. Attach the wall mount to a sturdy wall using the four provided screws.
3. Install an additional mounting screw in the case tamper.
4. Align the slots on the back of the Gateway with the hooks on the wall mount as shown below.
5. Once attached, insert the screw to secure the Lyric to the wall mount.
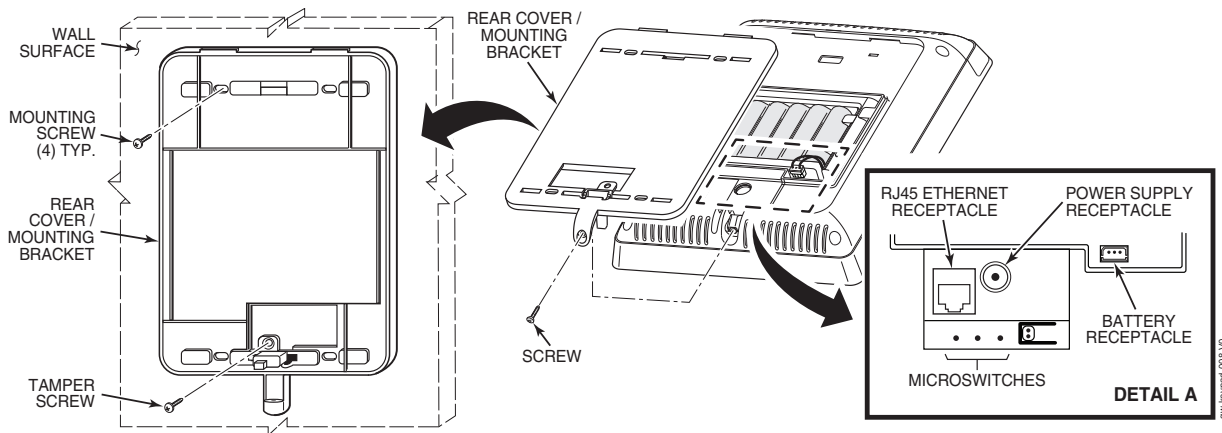
Desktop Mounting

NOTE: When selecting a location for the Lyric Gateway, be sure to provide a separation of at least 10 feet between 2.4GHz devices such as Wi-Fi Routers/Access Points.

The Desk Stand (LCP300-DK) can be installed in two positions that provide a viewing angle of 30 degrees or 60 degrees. Follow the steps and refer to the figures below.

Install the LCP300-DK Desk Stand

1. Align the slots on the back of the Gateway with the hooks on the desk stand as shown below.
2. Insert the stand into the slots on the rear case to provide the desired viewing angle and slide up to lock in place.
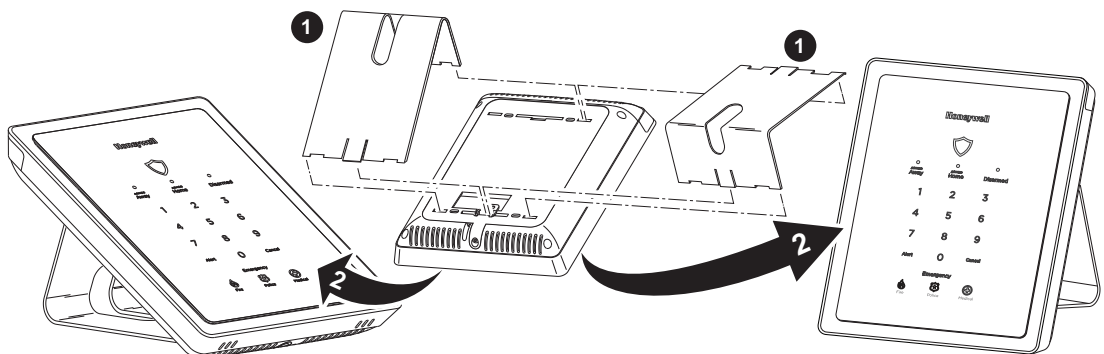
Installing the Gateway (Continued)

AC Power

The Lyric Gateway is powered by a 110VAC, 60 Hz/9 Volt DC, 2.5 Amp Plug-in Power Supply, 300-05763V1 (300-05763V1 –CAN in Canada). Refer to the wiring table below for wire gauge and length.

Use only the 300-05763V1 (300-05763V1-CAN in Canada) Power Supply. Do not plug the power supply into the AC outlet until after all wiring connections have been made.

Wiring Overview

The following summarizes the electrical connections associated with the Lyric Gateway. Follow the steps and refer to the figure below when making connections. Refer to the Summary of Connections diagram for additional information.

WIRING TABLE

Maximum Distance Between Power Supply and Gateway	Wire Gauge
Up to 8 feet (2.44 m)	# 22
Up to 13 feet (3.96 m)	# 20
Up to 20 feet (6.1 m)	# 18

Recessed Microswitch Functions

Location	Function
Left	Factory Default
Center	Reboot
Right	WPS
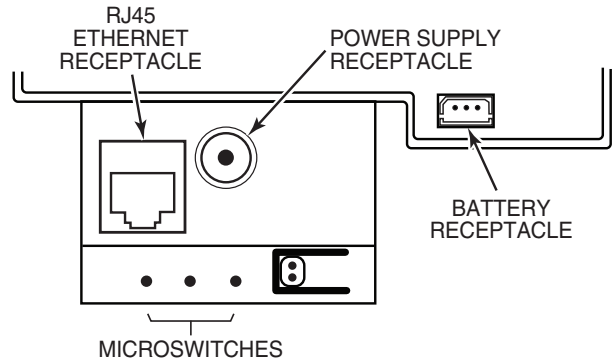
gw-keypad-020-V0

Before you begin

The Gateway can be connected to the internet via a hardwire connection or wirelessly via the premise's Wi-Fi® router. Programming is done via AlarmNet 360™ using a Smart (Mobile) Device or a laptop computer.

For Wireless Installations the following are required:

- A smart device with the AlarmNet 360 App loaded or a laptop (referred to as 'the set up device'). The App will be used to connect the Gateway panel to the customer's router onsite.
- Settings on the customer's smart device(s) must be set for Wi-Fi operation (Wi-Fi enabled).
- Access to the customer's router SSID and WPA or WPA2 password (typically located on the router's label).
- If you are not signed up for AlarmNet 360, click on "Dealer Signup" from the login screen to gain access to the Honeywell web-based programming.

Dealer Sign-Up Direct Link: https://services.alarmnet.com/AlarmnetDirectP_SignUp/Submission_Agree.aspx

Before starting the installation process, open the AlarmNet 360 App or go to the AlarmNet 360 website (www.AlarmNet360.com)

Connecting the Gateway

1. Temporarily hang the Gateway from the hook on the wall mount.
2. Connect the male end of the 110VAC, 60 Hz/9 Volt DC, 2.5 Amp Plug-in Power Supply, 300-05763V1 (300-05763V1-CAN in Canada) to the receptacle on the Gateway.
3. Install the rear cover on the Gateway OR align the slots on the back of the Gateway with the hooks on the rear cover/mounting bracket and attach the Gateway to the rear cover/mounting bracket.
4. Once attached, insert the screw to secure the Gateway to the rear cover/mounting bracket.
5. If used, connect the network cable to the Gateway's RJ45 receptacle.
6. Plug the power supply into a 24-hour, 110VAC unswitched outlet. The Gateway's Red and Green arming LEDs will blink alternately for approximately 2 minutes during power up.
7. If the Gateway's RJ45 ethernet connection is used, at the Gateway touchpad enter Installer Code + 31 to enter AP Mode and proceed to Step 12.
8. If the connection is via Wi-Fi, proceed to Step 9. When power up is complete the Gateway will be in Access Point [AP] mode.

   NOTE: The AP mode will remain active for approximately 30 minutes. To re-enter AP mode after it has expired, enter the Master Code and 31 on the Gateway touchpad.

9. If the customer's router is WPS-capable, at the Gateway touchpad enter Installer Code and 41. If not, proceed to Step 12.

Installing the Gateway (Continued)

Connecting the Gateway (Continued)

10. Press the WPS button on the customer's router.

11. Within approximately 3 minutes the Gateway confirms its connection to the Wi-Fi network and exits from WPS mode. Proceed to *"Programming the Lyric Gateway"*.

12. Change the Wi-Fi setting of the set up device, to the Gateway AP. Select the Gateway SSID, "OPTGW_####" (#### = Last 4 digits of the Gateway MAC ID#)" from the list of options and select "Connect". Enter the Gateway's 8-digit, case sensitive, WPA2 password when prompted and select Connect. (The Gateway SSID and Password are located on the bottom of the Gateway).

13. Open the AlarmNet 360 App on the set up device and select "Manage Lyric Gateway".

14. When prompted enter the Installer Code + "Done" + "Submit.

15. The Transfer Firmware, Transfer Panel Configuration, Configure Panel Wi-Fi and Advanced, options appear.
    a. Select Configure Panel WiFi to connect the Gateway to the customer's router.
       Enter the customer's SSID and WPA2 password when prompted.
    b. Select Transfer Firmware to transfer the latest firmware to the Gateway.
    c. Select Transfer Panel Configuration to transfer the panel configuration set up in AlarmNet 360 to the Gateway.
    d. Select Advanced to access Installer tools. Refer to the *Installation and Reference Guide* for additional information.

16 Select "Finish" when configuration is complete.

17. Select "Yes" to exit from the App. The Gateway exits from AP Mode and reconnects to the Wi-Fi network.

18. Select "Proceed to Panel Configuration".

19. Log in to AlarmNet 360.

Communication Modules

The Lyric Gateway supports Central Station reporting using wireless/cellular, ethernet and Wi-Fi communications devices. They also support upload/download programming capability via the Internet. This allows site maintenance independent of Central Station monitoring, and modification to sites globally via the Internet. Refer to the Quick Installation Guide (p/n 800-21668) for information regarding programming and registration. Additionally, an internal Z-Wave module allows the Lyric Gateway to support Home Automation functions. (refer to the Gateway User Reference Guide (p/n 800-21670 for additional information.) The Gateway is compatible with the following AlarmNet Communication Modules:

⚠️ **The LYRIC-CDMA Communications Module is only available in the continental United States, Alaska and Hawaii.**

Model	Description
LYRIC-3G/ LYRIC-3GC	GSM Cellular Communications Module
LYRIC-CDMA	CDMA Cellular Communications Module
LYRICLTE Series	LTE (Series) Cellular Communications Modules

Communications Module 24-Hour Standby Power

If 24-hour standby is required, the Super High Capacity battery (p/n 300-03866-AIO) must be installed.

RF Exposure

⚠️ **WARNING: The Lyric Gateway must be installed to provide a separation distance of at least 7.8 in (20 cm) from all persons and not co-located or operated in conjunction with any other transmitter except in accordance with FCC and ISED multi-transmitter product procedures.**

✓ **The Communications Module must be registered with AlarmNet 360™ before downloading or alarm reporting can take place.**

Install and Configure Communication Module

Follow the steps and refer to the figure to install the Communications Module.

Installing the Cellular Communications Module

1. At the AN360 app's Installer Tools screen, select "Advanced".

2. Select "Install Cellular Module" and follow the prompts displayed on the Smart Device or follow the steps below.

3. Remove Gateway upper cover (bezel).

4. Remove the existing Cellular Communications Module (if installed).

Installing the Gateway (Continued)

Communication Modules (Continued)

5. Install the Cellular Communications Module into the Gateway.
6. Ensure that the Communications Module is properly seated into the Gateway.
7. Insert the cover (bezel) into the top of the Gateway
8. Slide the cover (bezel) down to lock it in place and secure the Communications Module.
9. Select OK to complete the installation.

NOTE: The Communication Path dynamically adjusts when a Cellular Communication Module is installed or removed.

COMMUNICATION
MODULE

COVER

gw-keypad-010-V1

Installing Communications Modules

Install the Cellular Communication Module in a Registered Gateway

Follow the steps and refer to the figure to install the Communications Module in a Gateway that is already registered.
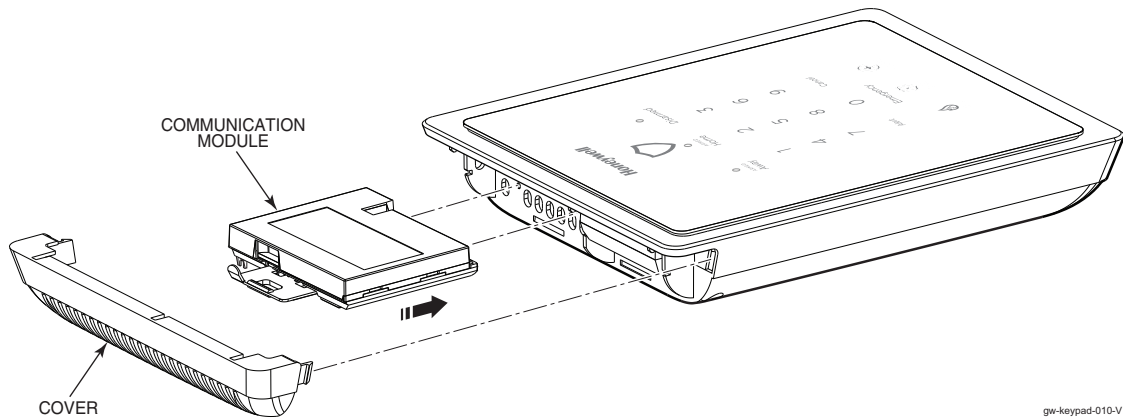
1. At the AN360 app's Installer Tools screen, select "Advanced".
2. Select "Install Cellular Module" and follow the prompts displayed on the Smart Device or follow the steps below:
3. Remove Gateway upper cover (bezel).
4. Install the Cellular Communications Module into the Gateway.
5. Ensure that the Communications Module is properly seated into the Gateway.
6. Insert the cover (bezel) into the Gateway.
7. Slide the cover (bezel) down to lock it in place and secure the Communications Module.
8. Go to the AlarmNet 360 "SETTINGS" Page->"COMMUNICATOR" Section and change Communication Path (Internal Device) to "Cellular" or "Cellular and IP".
9. Select "SAVE". The changes to the "Communication Path" will be reflected.
10. Select "SEND DATA".

Checking Signal Strength

When choosing a suitable mounting location, check the communications module's signal strength to ensure proper operation. For most installations, using the module's internal antenna, mounting the Lyric Gateway as high as practical, and avoiding large metal components provides adequate signal strength for proper operation. To check signal strength, perform the following test.

Check Signal Strength

1. At the AN360 app's Installer Tools screen, select "Advanced". The signal strength is displayed in bars (1 -5 bars) on the "Cellular Information" button.
2. Verify that adequate Signal Strength (greater than 1 bar) is available. If necessary, relocate the Gateway to obtain better signal strength (select "Cellular Information" again to refresh the reading).
3. If adequate signal strength cannot be achieved, External Antenna Kit model Cell-ANTST should be used.

Signal strength

4-5 bars..Excellent
2-3 bars ....Okay
1 bar...Poor

Wireless Zones

General Information

Zones
The Lyric Gateway supports up to 64 total wireless protection zones using 5800 and SiX™ Series transmitters, and wireless keys.

Range
The built-in RF receiver can detect signals from wireless transmitters within a nominal range of 200 feet.

Transmitters
5800 and SiX™ Series transmitters have built-in serial numbers that must be entered into the system via AlarmNet 360™. Each transmitter's zone number is also programmed into the system in the "Zones" programming section. Some transmitters, such as the 5816 can support more than one "zone" (referred to as loops or inputs). On the 5816, for example, the wire connection terminal block is loop 1; the reed contact is loop 2. Each loop must be assigned a different zone number.

For 5800 Series wireless keys such as the 5804E, 5834-4 and 5878, you must assign a unique zone number to each individual button used on the transmitter. Each button on the transmitter also has a pre-designated loop or input number, which is automatically displayed.

ETL	**The 5816 Transmitters do not have EOL supervision of their loop wiring, which must not exceed 3 feet.**
	The 5800PIR-OD, 5800SS1, 5804E, 5814, 5821, 5877 and 5878 wireless transmitters have not been evaluated by ETL.

Transmitter Supervision
With the exception of some transmitters/keypads that may be carried off-premises (5804E, 5834-4 and SiXFOB), each transmitter is supervised by a check-in signal that is sent to the receiver at 70–90 minute intervals. If at least one check-in is not received from each supervised transmitter within a 12-hour period, the "missing" transmitter zone number(s) and "Supervision" will be displayed. The supervision for a particular transmitter in the system that may also be carried off the premises may be turned off by entering it as an "Unsupervised" type. For additional information, refer to the "Zones" programming section in the Lyric Gateway Quick Installation Guide (p/n 800-21668). 5800 and SiX™ Series transmitters have built-in tamper protection and will annunciate as a fault condition if covers are removed. In Canada the RF supervision period is 3-hours for Fire zones and 12 hours for all other zone types.

Transmitter Input Types
Each transmitter has one or more unique factory-assigned input (loop/5800 Series or service/SiX™ Series) ID codes. Each of the inputs requires a programming zone (e.g., a 5804E's four inputs require four button zones). Transmitters can be entered as one of the following types (see transmitter's instructions for appropriate Supervision type):

Type	Description
RF Supervised	Sends periodic check-in signals, as well as fault, restore, and low battery signals. The transmitter must remain within the receiver's range.
RF Unsupervised	Sends all the signals that the Supervised type does, but the Gateway does not supervise the check-in signals. The transmitter may therefore be carried off-premises.
Button	Sends only fault signals. Does not send low battery signals until activated. The transmitter is unsupervised and may be carried off-premises.

Transmitter Battery Life
* Batteries in the wireless transmitters may last from 4–7 years, depending on the environment, usage, and the specific wireless device being used. Factors such as humidity, high or low temperatures, as well as large swings in temperature may all reduce the actual battery life in a given installation. The wireless system can identify a true low battery situation, thus allowing the dealer or user of the system time to arrange a change of battery and maintain protection for that point within the system.
* Button-type transmitters should be periodically tested for battery life. The 5804E, 5834-4, 5878 and SiXFOB button transmitters have replaceable batteries.

Transmitter (Sensor) Firmware Upgrade
The SiX™ Series transmitters (sensors) will receive updated firmware (if required) any time that the Gateway firmware is updated via AlarmNet 360. The Gateway will attempt to update the sensor firmware every 24 hours after its firmware has been updated.

Wireless Zones (Continued)

RF Transmitter Loop Numbers

(Refer to this information when programming 5800 Series transmitters)
The following illustration shows the compatible transmitters, their associated input types and loop designations.
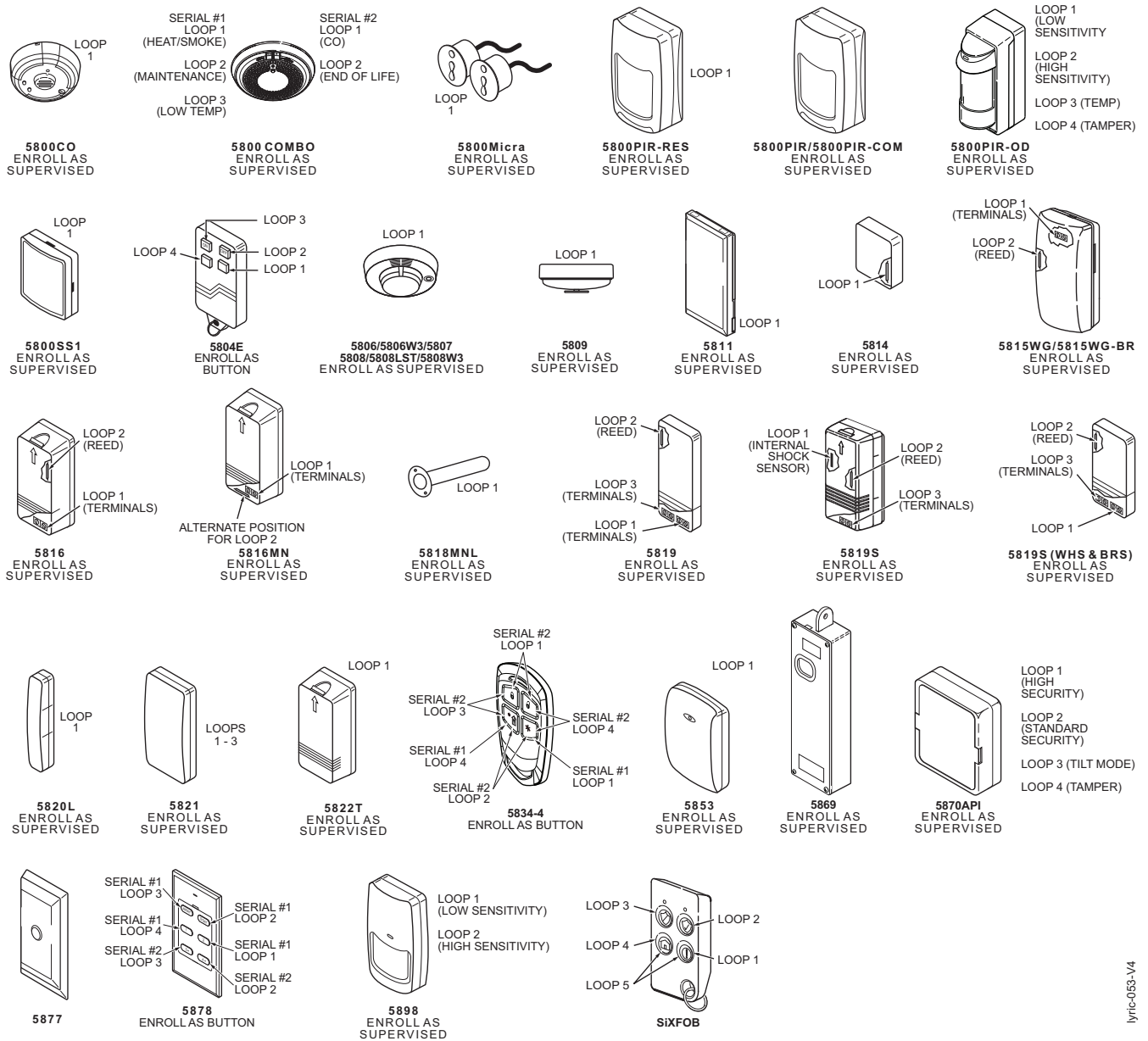
NOTES: (1) The 5806W3 smoke detector must be used in SIA applications.

(2) Button type devices send only fault and low battery signals; no restore or check-in signals.

Supervised RF devices send periodic check-in signals, faults, restore and low battery signals.

(3) The 5804E and 5834-4 encrypted (High-Security) devices must be activated while the system is in Go/No-Go Test Mode. Refer to the transmitter's Installation Instructions for complete details. The system will confirm the enrollment of the encrypted device by beeping two times.

(4) The 5800PIR-OD, 5800SS1, 5804E, 5814, 5821, 5877, and 5878 wireless transmitters have not been evaluated by ETL.

Mechanics of Programming

Programming

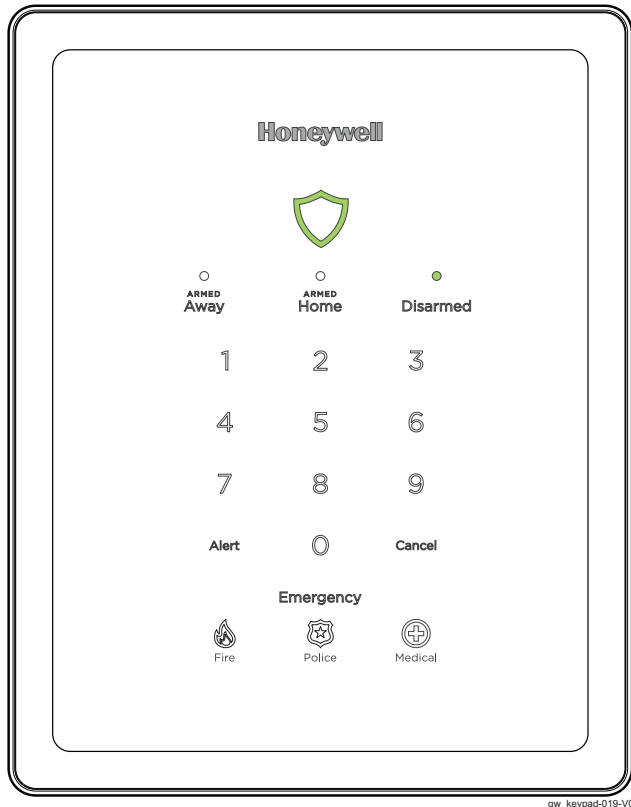The Lyric Gateway is programmed via AlarmNet 360™ using a smart (mobile) device or a laptop. There are numerous options for programming the Gateway, Sensors, Wireless Keys and Keypads and accessories. Refer to the Lyric Gateway Quick Installation Guide (p/n 800-21668) for information regarding programming.

Navigating

Gateway Touchpad

Gateway's touchpad can be used for Basic Security Functions. The touchpad provides a number of functions and indicators. The System Status Shield is lit Green when the system is ready or flashes Red when it is not. When the system is armed the System Status Shield is lit Red. Refer to the table below for additional indications and functions. Additional functions are available via the AlarmNet 360, MyHome Gateway and Total Connect Apps or the associated websites.

LYRIC™ Gateway

Key	Description
	System Status Shield – System status is displayed when the shield is lit as follows: Green (steady) – Ready to Arm and during sensor enrollment from AlarmNet 360 Green (flashing) – Zone is faulted Red (steady) – System is Armed Red (slow flash) – Entry/Exit delay countdown Red (rapid flash) – System is in Alarm White (steady) – Waiting for User Code entry
ARMED Away	Arm Gateway in Away mode (LED steady red when selected)
ARMED Home	Arm Gateway in Home mode (LED steady red when selected)
Disarmed	Disarm Gateway (LED flashes green until code is entered, then turns steady green)
Alert	Flashes red when an alert condition exists. Select to hear condition
Cancel	Cancel User Code entry or Emergency (Flashes white during an emergency) and silence beeping due to faults
Emergency	Activates Emergency keys
	Fire key - Initiates panic fire alarm within 5 seconds of activation.
	Police key - Initiates panic police alarm within 5 seconds of activation
	Medical key - Initiates panic medical alarm within 5 seconds of activation

Gateway Menu Mode

Entering the Master User Code or Installer Code +11 on the Gateway touchpad provides access to Menu Mode. The system announces the menu options based on the code that was entered.

Code Entered	Menu Option (System Announcement)
Master User (1234)	Press 20 to delete all enrolled MyHome Gateway apps
	Press 21 to enter MyHome Gateway app Enroll Mode
	Press 31 to enter or exit Access Point (AP) mode
	Press 41 to enter or exit WPS mode
Installer (4112)	Press 31 to enter Access Point mode
	Press 41 to enter or exit WPS mode.
	Press 51 to enter Go/No-Go Test mode

Keypad Lockout

In the event that 24 numeric keys (0-9) have been entered within a 15-minute window and a valid command is not executed, the system stops processing additional numeric key presses for a period of 15 minutes. Any numerical keys entered during that period will be ignored. CID Code 461 Wrong Code Entry will be entered in the Event Log and transmitted to the Central Station. When the 15-minute lockout window expires, a Restore message is sent to the Central Station and entered into the Event Log.

Mechanics of Programming (Continued)

**MyHome Gateway Smart Device Touch-screen Display**
The MyHome Gateway App is used to display screens on the Smart Device touch-screen. Variable icons and text are displayed on "screens". The screen displays status icons and associated text, the current time and date, system status information and menu choices. The Menu area includes a list of commands, or choices that apply to the current selection. The status area provides information about various system events and colored text also provides an indication of system status. A "Home Screen" is displayed whenever the App is opened.

Navigation Keys
Navigating through the screens is accomplished by lightly touching the icons or menu items on the Smart Device touch-screen. Once activated, the Gateway advances to the next screen. Selecting the "↺" key or the "Home" (cancel) key will return you to the previous screen or the home screen (as applicable) at any time. By touching (selecting) an icon or key the system, depending on the function, advances to another screen, toggles between options or scrolls through multiple options that can be selected. The system provides a prompt when a specific input is required.

Home Screen
System Status is displayed at the top of screen. In addition to the system status, the Home Screen displays the current date and time, current local weather and Security, Automation, TC Video, Smart Scenes and Settings icons .

gw-keypad-018-V0
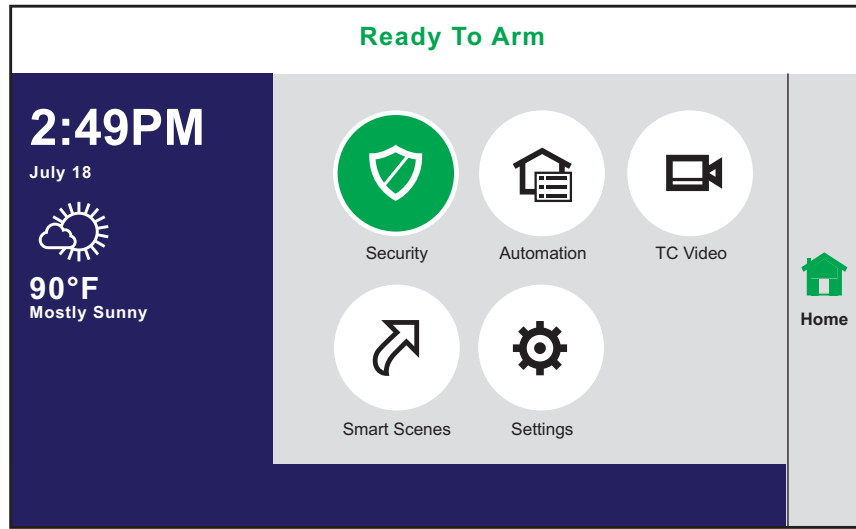
MyHome Gateway Home Screen with Total Connect Services

Icon	Function
Security	Provides access to Security Screen
Automation	Provides access to Automation Screen
TC Video	Provides access to Video Screen
Smart Scenes	Provides access to Smart Scenes Programming Screen
Settings	Provides access to System Settings Screen
Weather	Displays Current Local Weather

Mechanics of Programming *(Continued)*

Navigating Menus

Security Screen

System Status is displayed at the top of each screen and the time and date are displayed at the top left side of the Security Screen. The Security Screen displays the system status and selection "icons". The displayed pages and options may vary slightly depending upon the devices and services that are installed in or connected to the system.
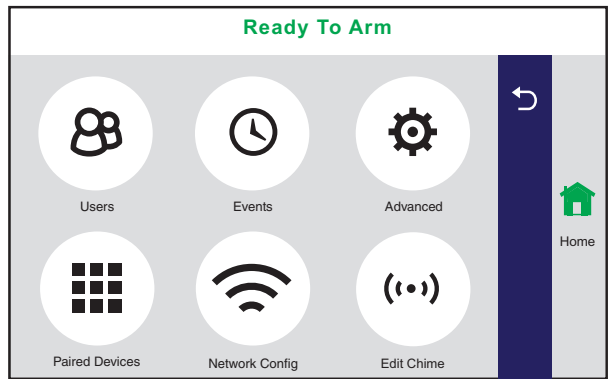

Security Screen

Selection	Function
Arm Away	Used to Arm the system in Away mode.
Arm Home	Used to Arm the system in Home mode.
Arm Custom	Used to Arm the system in Custom mode.
System	Provides information about system status.
Tools	Provides access to Master User Programming Menu (Master User Code required for access).
Zones	Provides access to Zone information and options.

Master User Menu Screen

The Master User Menu screen provides access to the User configurable features. Entering the Master User Code is required to access the User Tools Menu.

Refer to the Lyric Gateway User Reference Guide (p/n 800-21670 or higher) for additional information.

Master User Menu Screen

Programming

Master User Features

| SCREEN	ACTION
Master User Menu Screen	1. Select the "Security" icon. 2. Select "Tools" icon. 3. Enter the Master User Code 1234 on the displayed keypad. 4. Select the "Advanced" icon. 5. Select one of the following options: System Information — Walk Test Install Cellular Module — Comm. Test Install Backup Battery — Reboot Update Sensor Firmware* — Update Keyfob Firmware * Future use 6. The system advances to the screen for the selected option. Refer to the Lyric Gateway User Reference Guide (p/n 800-21670 or higher) for additional information regarding these options.

Mechanics of Programming (Continued)

Loading Factory Defaults

To load the factory defaults, refer to the following procedure. Refer to the Programming Values section of this manual to view the default values.

1. Remove the Gateway's rear cover, the panel's tamper alarm will sound.

2. Using a precision screwdriver, paperclip or equivalent, depress and hold the left (Default), recessed microswitch for 10-20 seconds and enter Installer Code when prompted.
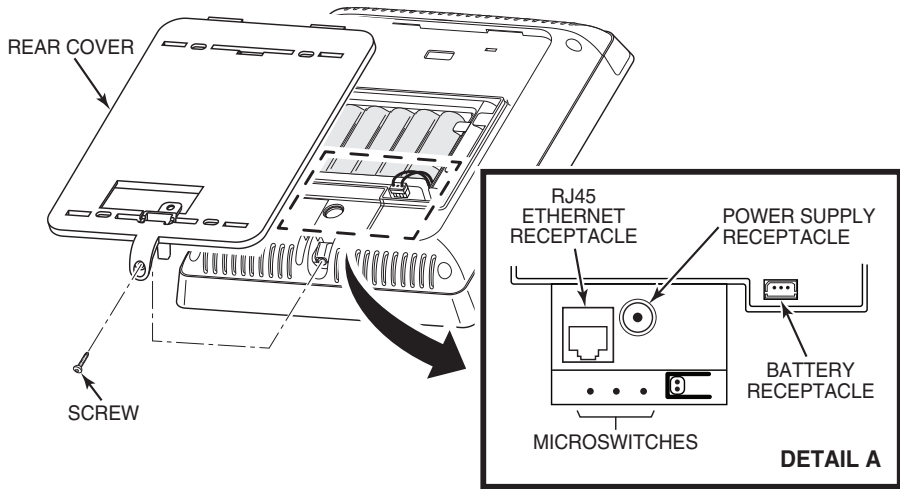
Recessed Microswitch Functions

Location	Function
Left	Factory Default
Center	Reboot
Right	WPS

Exit Programming Mode

1. Select the "↺" key to exit the current screen OR select the Home key to return to the Home Screen.

Deleting Wireless Sensors, Keys and Keypads

SiX™ Series or 5800 Sensors, Wireless Keys or Wireless Keypads must be deleted using AlarmNet 360. After entering AlarmNet 360 select the "Sensors", "Keyfobs" or "Keypads" programming option (as applicable).

NOTE: SiX™ Series sensors must be deleted from the Gateway before the device can be enrolled in another system.

1. Select the Sensor, Keyfob or Keypad to be deleted from the displayed list.

2. The system displays the programmed information for the associated device and confirm the deletion when prompted.

3. When programming is complete select " " to Sync Changes and send the information to the gateway.

Installing Z-Wave® Home Automation Devices

The Lyric Gateway supports Z-Wave Home Automation Devices that can be included or excluded via AlarmNet 360 or locally by the User. Smart Scenes are User programmable functions and can be programmed via remote services or locally via the MyHome Gateway App. Refer to the Lyric Gateway User Reference Guide for detailed programming information.

Programming via the AlarmNet 360 App

1. At the Installer Programming screen, select "Z-Wave Devices". The system displays the following options:

Option	Function
Include Devices	Include (enroll) new Z-Wave Devices
Exclude Devices	Exclude (delete) Z-Wave Devices
Factory Default Controller	Reset the Z-Wave controller to the factory default settings.
Retrieve Failed Devices	Reset a failed-Wave Device

2. When programming is complete follow the prompts to complete the function.

Zone Response Type Definitions

General Information

During programming, you must assign a zone type to each zone, which defines the way in which the system responds to faults in that zone. Zone types are defined below.

Response Type	Function	Characteristics
Not Used	Used to program a zone that is not used.	• None
Entry/Exit 1 (Burglary)	Usually assigned to sensors or contacts on primary entry and exit doors.	• Entry delay #1 is programmable. • Exit delay is independently programmable. • Exit and entry delays when armed in Away, Home (Stay), Arm Night (Stay) or Armed Custom mode. • No entry delay when armed in Instant modes. • Exit delay begins regardless of the arming mode selected.
Entry/Exit 2 (Burglary)	Usually assigned to sensors or contacts on secondary entry and exit doors that might be further from the keypad (typically used for a garage, loading dock, or basement door).	• Entry delay #2 is programmable. • Exit delay is independently programmable. • Secondary entry delay, if armed in the Away or Home (Stay) mode. • No entry delay when armed in the Instant mode. • Exit delay begins regardless of the arming mode selected.
Perimeter (Burglary)	Usually assigned to all sensors or contacts on exterior doors and windows	• Instant alarm, when armed in Away, Home (Stay), Home (Stay) No Delay, Arm Night (Stay) or Away Instant mode.
Interior, Follower	Usually assigned to a zone covering an area (i.e.: foyer, lobby, or hallway) that must be passed upon entry (after faulting the entry/exit zone) to reach the keypad. Provides an instant alarm if the entry/exit zone is not violated first, and protects an area in the event an intruder has hidden on the premises before the system is armed, or gains access through an unprotected area.	• Delayed alarm (using the programmed entry/exit time) if entry/exit or interior-with-delay zone is faulted first. • Instant alarm in all other situations. • Active when armed in Away or Away Instant mode. • Bypassed automatically when armed in Home (Stay), Arm Night (Stay) or Home (Stay) Instant mode.
Trouble by Day/ Alarm by Night	Usually assigned to a zone that covers a sensitive area (i.e.: stock room, drug supply room, etc.) It can also be used on a sensor or contact in an area where immediate notification of an entry is desired.	• Instant alarm, when armed in Away, Home (Stay), Arm Night (Stay) or Home (Stay) Instant, or Away Instant (night) mode. • Provides a latched trouble sounding from the keypad and, if desired, a Central Station report when disarmed (day).
24-hour Silent Alarm	Usually assigned to a zone containing an Emergency button (silent emergency).	• Sends a report to the Central Station but provides no keypad display or sounding. • In disarmed state sends a report to the Central Station displays "Not Ready to Arm" on the MyHomeGateway app's keypad and "Tools" button is disabled.
24-hour Audible Alarm	Usually assigned to a zone containing an Emergency button (audible emergency).	• Follows sounder timeout • Sends a report to the Central Station, and provides alarm sounds at the Gateway.
24-hour Auxiliary	Usually assigned to a zone containing a button for use in personal emergencies or to a zone containing monitoring devices (i.e.: water or temperature sensors, etc.).	• Sends a report to the Central Station and provides an alarm sound at the Gateway. (There is no timeout.)
Silent Burglary	Usually assigned to sensors or contacts on exterior doors and windows where sirens are NOT desired.	• Instant alarm, with No audible indication when armed in the Away, Home (Stay), Home (Stay) No Delay, Arm Night (Stay), or Away Instant mode. • Report sent to the Central Station.
Interior with Delay	Provides entry delay (using the programmed entry time), if tripped when the Gateway is armed in the Away mode. Bypassed when the Gateway is armed in the Home (Stay) or Home (Stay) Instant mode.	• Entry delay #1 (with programmed entry time) when armed in the Away mode. • Entry delay begins whenever sensors in this zone are violated, regardless of whether an entry/exit delay zone was tripped first. • No entry delay when armed in the Away Instant mode. • Exit delay regardless of the arming mode selected.
Carbon Monoxide Monitor	Can be assigned to any wireless zone with a carbon monoxide detector. This zone type is always active and cannot be bypassed.	• Local keypad and detector will sound when this zone type is alarmed. (Pulse Temporal 4).
Trouble	Used with Other response type.	• The system will provide a trouble sounding from the keypad (and a Central Station report, if desired).
Fire No Verification	Can be assigned to any wireless zone used as a fire zone. This zone type is always active and cannot be bypassed.	• Alarm sound will pulse (Temporal Fire) when this zone type is alarmed.

Zone Response Type Definitions (Continued)

Response Type	Function	Characteristics
Fire with Verification	Can be assigned to any wireless zone used as a fire zone. Fire with verification is available with smoke detector device type. It cannot be used with heat detectors, combination heat/smoke detectors or fire pull stations. This zone type is always active and cannot be bypassed.	• Alarm sound will pulse (Temporal Fire) when this zone type is alarmed and the alarm has been verified. • System verifies alarm by delaying reporting and alarm sounding for 30 seconds after alarm is detected. If the zone remains faulted after 30 seconds a fire alarm is provided. If any other fire zone is faulted during the 30 second delay window a fire alarm is immediately provided for that zone. An alarm for original fire zone will also be provided, if that zone is still faulted. If there are no fire alarms after the 30 second delay expires, the system will open a 60 second window. If any fire zone is faulted during that window a fire alarm will immediately be provided for that zone.
Arm–Stay	Special-purpose zone type used with 5800 and SiX™ Series wireless keys.	• Exit delay regardless of the arming mode selected. • System armed in Home (Stay) mode when zone is activated.
Arm–Away	Special-purpose zone type used with 5800 and SiX™ Series wireless keys.	• System is armed in the Away mode when the zone is activated.
Disarm	Special-purpose zone type used with 5800 and SiX™ Series wireless keys.	• Disarms the system when the zone is activated.
No Response	Assigned when no-alarm response is required.	• No reports to the Central Station. • No keypad sounding or chime and no display on screen. • System can still be armed.
Monitor	Can be assigned to any wireless zone used for asset protection. Works as a dynamic monitor of a zone fault/trouble (not alarm).	• Reports to the Central Station, if enabled. • Fault/restore events are logged by the system. • Restore will be stored in event log. • No keypad sounding or chime. • System can still be armed.
General Monitor	Assigned sensors or contacts on doors and windows or asset protection within the premises. Used to track activity of the occupant and alert occupant of the activity of others.	• No reports to the Central Station. • Fault/restore events are logged by the system. • Monitors entry into a monitored area. Activates a one-time announcement when faulted. •
General Response	Assigned sensors or contacts on doors and windows or asset protection within the premises. Used to track activity of the occupant and alert occupant of the activity of others.	• No reports to the Central Station. • Fault/restore events are logged by the system. • Monitors entry into a monitored area. Activates a zone announcement when faulted. • System re-triggers audible sounding until acknowledged. (Off sequence or wireless key)
Resident Monitor	Used to monitor a resident in an area deemed to be dangerous by a caregiver.	• No reports to the Central Station. • Monitors entry into a monitored area. Activates a zone announcement when faulted. • Fault/Restore events are not logged by the system.
Resident Response	Used to monitor a resident in an area deemed to be dangerous by a caregiver. Requires acknowledgement by caregiver.	• No reports to the Central Station. • Monitors entry into a monitored area. Activates a zone announcement when faulted. • System re-triggers audible sounding every ten seconds until acknowledged (Off sequence or wireless key). • Fault/Restore events are not logged by the system.
Garage (Burglary)	Assigned to Automatic Garage Door applications. Provides a status of the garage door close/open real time state.	• Associated With Entry Delay #2 Programmed Time. • Exit delays when armed in Away, Home (Stay) or Arm Night (Stay) mode. • No Entry Delay when armed Away or Home (Stay) Instant modes. • System can be armed with zone faulted. When zone is closed it will be included within protection points. If the point is subsequently violated, it will initiate an alarm.
Garage Monitor	Assigned to Automatic Garage Door applications. Provides a status of the garage door close/open real time state.	• Can be assigned to any wireless zone used for automatic "Garage Door" Open/Close status. • Will not initiate an alarm condition on the Gateway. • When zone is in the open state will display "FAULT." • Does not report alarms to Central Station. • Zone chimes, if enabled. • System can be armed if this zone type is in fault.

System Operation

Key/Touchscreen Operation

Touchscreen icons displayed on the Smart Device allow the user to arm and disarm the system, and perform other system functions, such as bypassing zones. Zone and system conditions (alarm, trouble, bypass) are displayed on the touchscreen. When an alarm occurs, the Gateway and Smart Device (if installed) will sound, and the zone(s) in alarm will be displayed. Pressing any key will silence the sounder for 10 seconds (only once). Disarming the system will silence both console and external sounders. When the system is disarmed, any zones that were in an alarm condition during the armed period will be displayed (memory of alarm). To clear this display, simply repeat the disarm sequence by selecting "Disarm" and entering the Security Code. The Gateway also features chime annunciation, and three Emergency (panic) key icons for Police (silent or audible), Fire and Medical emergency alarms. These keys can notify the Central Station of an alarm condition, if that service is connected.

Emergency Keys

There are three emergency (panic) keys that are active (if programmed) when the "Emergency" and any of the keys is selected. The keys will timeout if a selection is not made within ten seconds. The keys can be used to manually initiate alarms and send a report to the Central Station. Each can be individually programmed for 24-hour silent, audible, auxiliary or fire emergency responses. The panic function is activated when the respective key is pressed. It can be stopped if the "Cancel" key is pressed while it is flashing. The emergency (panic) functions are identified by the system as follows:

Zone	Function
995	Fire Emergency
996	Medical Emergency
999	Police Emergency

NOTE: The Emergency (panic) functions can only be activated from the Gateway touchpad or the Lyric Keypad.

Security Codes

Installer Code

The installer programs the 4-digit Installer Code initially as part of the programming procedure. The factory default Installer Code is **4-1-1-2**, but may be changed via AlarmNet 360. The Installer Code is the only code that allows entry into Installer Programming mode.

Master Code

In normal operation mode, the Master (Security) Code is used to enter the 4-digit User Security Codes and enter the Master User Tools Menu mode via the MyHome Gateway app.

Enter/Change the Master Code by Installer.

The factory default Master Code for the Lyric Gateway is set to 1-2-3-4. The Master Code is used to enter the 4-digit User Security Codes.

SCREEN	ACTION
	1. After entering the Master User Menu screen, select the "Users" icon. The system displays the User Code Programming screen. 2. Select "Master", then select "Edit". 3. Enter a new 4-digit Master (Security) Code on the displayed keypad. The system displays the new code on the left side of the screen. 4. Select "Done" when you are finished. 5. The system returns to the Master Code Programming screen.

Secondary User Codes

In normal operation mode, the Master (Security) Code can be used to assign up to 46 secondary 4-digit security codes, including a Guest Code and a Duress Code. The Master Code can also be used to individually remove secondary codes from the system. Refer to the Lyric Gateway User Manual for additional information.

System Operation *(Continued)*

Reset Master Code (MyHomeGateway app)

1. At the Master User Tools menu, select "Users" from the Master User screen menu.
2. Select "Master" followed by "EDIT' to reset the Master User Code.
3. Select "User Code".
4. Enter the Master Code "1-2-3-4" on the displayed keypad, then select "Done". The system returns to the previous screen.
5. Select "Save"
6. If confirmed, the Master Code will be reset back to "1-2-3-4". This will be logged in the System Event Log as "User: 1 Reset Master Code, E655". The system returns to the Master User Tools menu.

    OR

    If the reset failed, the system will display: "User Code Not Accepted". This will only occur if the code 1-2-3-4 has been assigned to another User in the panel.

<table>
<tr><td align="center">**Security Code Notes**</td></tr>
</table>

- The Master and Secondary security codes permit access to the system for arming, disarming, etc.
- The Installer Code can disarm the system only if it was used to arm it. In addition, the Installer Code cannot disarm the system if it was armed by pressing and holding a Quick-Arm button.
- The Guest Code can disarm the system only if it was used to arm it. In addition, the Guest Code cannot disarm the system if it was armed by pressing and holding a Quick-Arm button.
- Duress code sends a special code to the Central Station when used to perform any system operation. Instruct users to be careful not to use this code for normal usage.
- Opening/closing reports are sent for the Installer Code, with the appropriate subscriber number. Master Code and secondary user codes are sent as User No. 2 and 3-47 respectively, in Contact ID® format (with the appropriate user number).

Important Security Notice

Please inform the User about the security importance of their wireless key (key fob), and what to do if it is lost.

Explain that the wireless key is similar to their keys or access card. If lost or stolen, another person can compromise their security system. They should immediately notify the Dealer/Installer of a lost or stolen wireless key. The Dealer/Installer will then remove the wireless key programming from the security system.

System Operation (Continued)
System Displays

The following icons will be displayed on the MyHomeGateway Home screen along with specific zone status information (if applicable) to indicate system status.

DISPLAY	DEFINITION
	AC Loss
	Alarm (Intrusion)
	Ready To Arm
	Armed Away
	Armed Home (Stay)
	Armed Night Home (Stay)
	Armed Custom
	Restart Timer
	Battery Low
	Bypassed Zones
	CO Alarm
	Reporter Failure
	Low Batt 850 Keypad
	900 Cover Tamper

DISPLAY	DEFINITION
	901 Expansion Module Tamper
	950 Comm. Trouble
	988 RF Jam (5800 Series Wireless Device)
	990 RF Jam (SiX Series Wireless Device)
	Door Open
	Window Open
	Fire OR Heat Sensor
	Environmental
	Flood
	Glass Break
	Medical Alarm
	Keypad
	Motion
	Temperature

DISPLAY	DEFINITION
	Other
	Automation Icon (Z-Wave Node Failure OR Z-Wave Controller Not Ready)
	Garage Door Open

Zone Status Displays

The icons associated with the programmed zones are displayed on the Zones screen. The icon's color indicates the zone status (i.e.; yellow icon indicates the zone is faulted and a red icon indicate the zone is in alarm). In addition a bypass icon is displayed alongside the icon for a bypassed zone.

System Operation (Continued)

ETL Audio alarm verification has not been evaluated by ETL.

Audio Alarm Verification (Two-Way Voice Feature)

This feature allows the Central Station operator to listen, talk to or conduct a two-way conversation with an individual(s) at the premises. It also assists the operator in gathering information about the nature and location of the alarm that may be helpful in responding to police and fire departments. All Lyric Gateways are capable of supporting the Two-Way Voice feature. The Lyric Gateway does not make system announcements when the Two-Way Voice feature is active.

If a Wi-Fi connection is being used for Two-Way Voice (AAV), sufficient bandwidth must be available.
*   AAV requires a continuous Wi-Fi upload/download bandwidth of 90kbps for proper operation.
*   Wi-Fi bandwidth less than 90kbps may result in degraded performance.

Activation

✓ **Fire and CO alarms will prevent the Lyric Gateway from starting an AAV session. A new Fire or CO alarm will end an AAV session that is in progress.**

The Gateway sends the "alarm message" followed by a "Listen-in-to-Follow message" (Contact ID® code 606) to the Central Station. The Listen-in-to-Follow message causes the Central Station's digital receiver to temporarily hold the phone line for approximately 1 minute. When the Gateway receives the "kissoff" from the Central Station, indicating that the alarm message has been received, the Two-Way Voice (AAV) feature is activated in the (default) "Listen Mode" and sirens and keypad sounds are discontinued. The Gateway transmits a beep acknowledgment to the Central Station, once per second. The beep alternates between two tones and indicates that the Gateway is waiting for a session command from the Central Station operator. Once a command is issued the beep acknowledgement is discontinued, however, if a command is not issued within two minutes the system will "time out" and the call will be terminated.

Operator Commands

The Central Station operator begins the session, which last 5 minutes, by entering one of the valid AAV commands shown in the table below. The session may be extended 5 minutes, without changing the operating mode, by pressing the [7] key on the touch-tone phone. Selecting another operating mode also resets the session an additional 5 minutes. During the last minute of the 5 minute, session, the Gateway generates two beeps every 30 seconds to alert the Central Station operator that the session is about to time out. The Central Station operator may then extend the session by pressing the [7] key on the touch-tone phone. If the session is not extended, the phone line is disconnected and the session is ended. Sessions may be ended at any time by pressing the [9] key on the touch-tone phone.

During an AAV session the Gateway's shield will blink Green or Red and "Alert" will blink red. The pattern is dependent upon whether the alarm has been programmed for silent or audible emergency.

The AAV modes are described as follows:

NOTE: When entering AAV commands make sure the Central Station receiver has been disconnected from the phone line, otherwise AAV commands may not go through.

Key	Function
1	Talk Mode: Pressing the [1] key on the touch tone phone, enables one-way voice communication from the Central Station to the violated premises, and allows the operator to communicate through the Gateway's built-in speaker.
2	VOX (Voice) Mode: Pressing the [2] key on the touch-tone phone, enables two-way voice communications between the Central Station and the violated premises via the Gateway's built-in speaker and microphone..
3	Listen Mode: Pressing the [3] key on the touch-tone phone, Enables one-way audio from the violated premises to the Central Station. The Listen Mode is the start up default mode of the voice feature and allows the operator to listen through the Gateway microphone.
7	Extends the session 5 minutes without changing its operating mode.
9	Ends the session and disconnects the phone line.

System Operation (Continued)
Event Log
The Lyric Gateway Series event log is capable of recording and displaying up to 6,000 system events. These events are stored locally in the Gateway, in chronological order, and transmitted to the Central Station. When the maximum number of events is reached in the Event Log, the system will overwrite the oldest event first. The type of events that can be recorded is selectable and is programmed in the System Type programming field. The event log can be reviewed from the AN360 app's Installer Tools screen by selecting "Event Logs" or the Installer Advanced screen by selecting "Event Log". Refer to the Lyric Gateway User Manual for additional information. The Events and CID Codes displayed vary according to the options that are programmed. The tables below provide definitions of the events/codes that may be transmitted to the Central Station and/or displayed in the Gateway's Event Log.

NOTE: In the unlikely condition that the backup battery becomes fully discharged when AC power is lost, any system activity performed after the low battery notification will not be saved in the event log. Additionally, the Gateway will revert to the status condition as before the low battery notification.

Contact ID® Event Log Codes

CID 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
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 Stay	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

* AlarmNet 360 generates a special comm. fail message (E316) if it does not hear from a unit within 15 minutes after a delayed alarm is delivered. This message is meant to alert the Central Station that the system has been tampered with and may have been compromised.

System Operation (Continued)

Contact ID® Event Log Codes

CID Code	Definition	Event Log Display
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
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

Central Station Messages

The following messages are sent by the Gateway internal cellular or Wi-Fi devices for the conditions listed below.

Alarm Condition	Alarm Code	Restore Code
Power On / Reset	E33900950	
Primary Communication Path Supervision	E350C0951	R350C0951
Secondary Communication Path Supervision	E350C0952	R350C0952
Test	555555559	

Testing the System

TO THE INSTALLER
Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system.
The installer should assume the responsibility of developing and offering a regular maintenance program to the user as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to ensure the system's proper operation at all times.

Test Modes

The following tests are available to the Installer via the AlarmNet 360 app when the "Advanced" icon is selected from the Installer Tools screen:

Option	Function
System Information	System Information is displayed. Select OK to return to the previous screen.
Comm. Test	The Communications Test mode performs network diagnostics and sends test alarms to AlarmNet 360. Dependent upon the type of Communications device that is used, the following tests are available: • Test Ethernet/Wi-Fi • Test IP • Send Any • Send Cellular Message • Send Ethernet Message The results for the selected test will be displayed.

The following tests are available to the Installer via the Gateway touchpad.

Option	Function
Go-No-Go Test	Used to verify adequate RF signal strength from proposed transmitter locations.

The following tests are available to the Installer via the MyHome Gateway app when the "Advanced" icon is selected from the Master User screen:

Option	Function
Walk Test	The Walk Test mode allows each protection point to be checked for proper operation. Refer to the Lyric Gateway User Manual for additional information.

Testing the System

After installation is completed, the security system should be carefully tested, as follows:

Step	Action
1.	With the system in the disarmed state, check that all zones are intact. If the Status Shield is not lit green, select the "Security" icon on the Smart Device followed by the "Zones" icon to display the faulted zone(s). If necessary, restore faulted zone(s) so that the "Home" button lights. Fault and restore every sensor individually to assure that it is being monitored by the system.

Alarm Reporting (Armed System) Test (via AlarmNet 360)

Alarm messages will be sent to the Central Station during the following steps 1 and 2. Notify the Central Station in advance that tests will be in progress.

Step	Action
1.	Arm the system and fault one or more zones. Silence alarm sounder(s) and disarm the system by selecting "Disarmed" and entering the Security Code. Check entry/exit delay zones.
2.	Check the touchpad-initiated alarms that are in the system by selecting "Emergency" followed by applicable Panic keys. If the system has been programmed for audible emergency, the touchpad will emit a steady alarm sound, and "Alert" will flash red. In addition, "ALARM" and zone number will be displayed on Smart Device. Silence the alarm by selecting "Disarmed" and entering the Security Code. If the system has been programmed for silent emergency, there will be no audible alarms or displays, but a report will be sent to the Central Station.
3.	Notify the Central Station when all tests are finished, and verify results with them.
4.	To test the wireless part of the system and the RF receiver, perform the Go-No-Go Test.

NOTE: Go/No Go Test will be automatically terminated after 3-1/2 to 4 hours if the installer or user does not manually terminate it. This ensures that fire and panic zones will not remain disabled. During the final 5 minutes the system will emit double beeps indicating that the end of Test mode is nearing.

Testing the System (Continued)

Go-No-Go Test Mode

Conducting this test with your hand wrapped around the transmitter will cause inaccurate results. If a button is pressed on a transmitter that has been programmed to set Arm Away, Arm Home (Stay), or Disarm, the system will exit the Go/No Go Test mode and the programmed action will occur.

The Go-No-Go tests is used to verify adequate RF signal strength from the proposed transmitter location, and allow you to reorient or relocate transmitters if necessary, before mounting the transmitters permanently. This mode is similar to the RF Sniffer Mode, except that the wireless receiver gain is reduced. This will enable you to make sure that the RF signal from each transmitter is received with sufficient signal amplitude when the system is in the normal operating mode. During Go/No-Go mode the system beeps every 30-40 seconds.

Enter Go/No-Go Test mode
1.   Enter Installer Code (4112) + 51 (on the Gateway touchpad).

Exit Go/No-Go Test mode
1.   Select "Disarmed"+ Enter Installer Code (4112).

Rebooting the System

The Reboot function allows you to restart the system if required. To reboot the system perform the following via the AlarmNet 360 app when the "Advanced" icon is selected from the Installer Tools screen or the Installer Programming screen.

Step	Action
1.	Select the "Reboot" button. A confirmation screen appears.
2.	Select "Yes" to reboot the Gateway.

NOTE: After the reboot sequence is complete it is recommended that you perform a "Walk Test" to verify that all transmitters are operational in the system.

A hard reboot can also be performed locally at the Gateway using the following procedure.

Step	Action
1.	Remove the rear Gateway's cover, the panel's tamper alarm will sound.
2.	Using a precision screwdriver, paperclip or equivalent, depress the center (Reboot) recessed microswitch to reboot the panel.
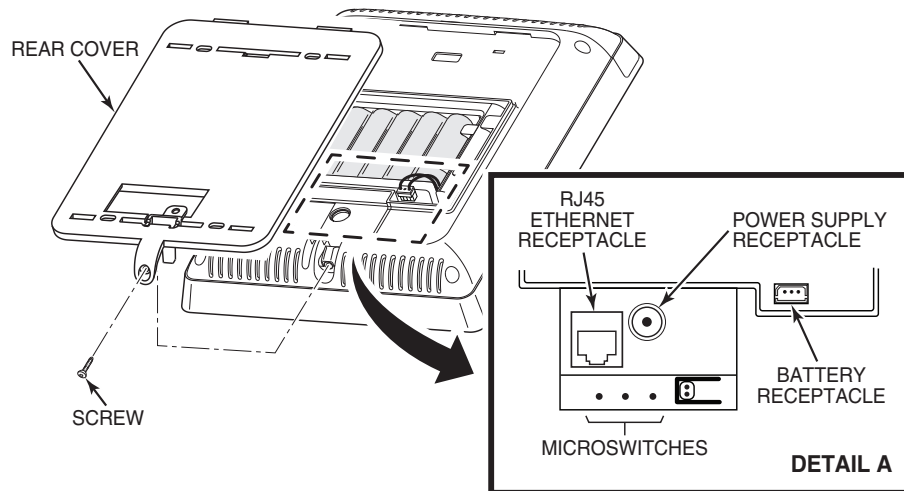
Network Configuration

System Information

The following information is available to the Installer via the AlarmNet 360 app when the "Advanced" icon is selected from the Installer Tools screen.

Cellular Information - Displays Cellular information if the Communication Path is enabled and the device is registered.

NOTE: Cellular Signal strength is displayed on the Cellular Information button and is indicated by a series of colored bars.

Bars		Signal Strength
4 Green		Excellent
3 Green		Good
2 Yellow		Weak —> Fair
1 Red		Fair —> No Connection

LYRIC-3G Communications Module

Message	Function
Cell Phone Type:	UMTS
Model:	Displays model number (i.e.; PHS8-USA)
IMEI:	Displays device's 15-digit serial number
Tower Connection Status:	Displays registration status (Home Network (Not Roaming), Not Registered, Searching, Registration Denied, Unknown, Roaming Network (Not Home)
Access Technology:	UMTS/HSDPA/HSPA (3G) OR GSM (2G)

LYRIC-CDMA Communications Module

Message	Function
Cell Phone Type:	CDMA
Model:	Displays model number (i.e.; SL3010T)
ESN/MEID:	Displays Device's 32-bit serial number
Tower Connection Status:	Displays registration status Home Network (Not Roaming), Not Registered, Searching, Registration Denied, Unknown, Roaming Network (Not Home)
Access Technology:	CDMA 1X

LYRICLTE Communications Module

Message	Function
Cell Phone Type:	LTE
Model:	Displays model number (i.e.; PLS8-US)
ESN/MEID:	Displays Device's 32-bit serial number
Tower Connection Status:	Displays registration status Home Network (Not Roaming), Not Registered, Searching, Registration Denied, Unknown, Roaming Network (Not Home)
Access Technology:	LTE, 3G OR 2G (Dependent upon Network availability as determined by the carrier's network)

Communicator ID – The following information is displayed:

Message	Function
APL:	Displays Advanced Protection Logic status (Enabled or Disabled)
City ID:	Displays programmed (2-digit) Central Station City ID
CS ID:	Displays programmed (2-digit) Central Station ID
Sub ID:	Displays programmed (4 digit) Subscriber Account Number
Supervision:	Displays programmed Supervision period
Old Alarm Time:	Displays programmed time
Rem ACC Comm::	Displays programmed Remote Access status (Enabled or Disabled)
Multi Mode Comm:	Displays programmed Multi Mode Comm. status (Enabled or Disabled)

Network Configuration *(Continued)*

The following information is available to the Installer and the User via the MyHome Gateway app's User Tools screen.

Ethernet Information OR WiFi Information – Displays Ethernet or Wi-Fi information for the Communication Path that is enabled.

NOTE: Wi-Fi Signal strength is are displayed on the WiFi Information button and is indicated by a series of colored bars.

Bars		Signal Strength
4 Green		Excellent
3 Green		Good
2 Yellow		Weak —> Fair
1 Red		Fair —> No Connection

Message	Function
SSID:	Displays information regarding connected router
WiFi Link:	Confirms physical link connection and speed (*** Mbps or Bad)
DHCP:	Displays status of server (OK, Bad or Off)
NIC IP Address:	Displays the communication device's assigned IP address
Subnet Mask:	Displays the 32-bit address mask used to indicate the portion (bits) of the IP address that is being used for the subnet address
Gateway IP Address:	Displays the IP address assigned to the Gateway
DNS Server IP Address:	Displays the IP address assigned to the DNS server

Programming Defaults

Programming Defaults/Options

The following table provides an overview of the Programming Fields, Options and Defaults, as viewed via the AlarmNet 360 App. Shaded fields are not programmable.

Programming Field	Options	LCP300-L Default	LCP300-LC Default
Communicator			
City ID	01-99	Blank	Blank
CS ID	01-FE	Blank	Blank
Sub ID	0001-9999	Blank	Blank
Advanced Protection Logic	Yes, No	Yes	Yes
Supervision	None, Daily, 30 Days	Daily	Daily
High Usage Plan	Yes, No	No	No
Communications Path (Internal Device)	IP, Cellular, Cellular and IP	IP	IP
Old Alarm Time	10 Minutes, 15 Minutes, 30 Minutes, 1 Hour, 2 Hours, 4 Hours, 8, Hours, 12 Hours, 24 Hours	10 Minutes	10 Minutes
IP Fault Time	1 – 99 Minutes	60 Minutes	60 Minutes
Use DHCP	Yes, No	Yes	Yes
NIC IP Address	Up to 12 digits (Viewable Only unless DHCP is disabled)	255.255.255.255	255.255.255.255
Subnet Mask	Up to 12 digits (Viewable Only unless DHCP is disabled)	255.255.255.255	255.255.255.255
Gateway IP Address	Up to 12 digits (Viewable Only unless DHCP is disabled)	255.255.255.255	255.255.255.255
DNS Server IP Address	Up to 12 digits (Viewable Only unless DHCP is disabled)	255.255.255.255	255.255.255.255
Cellular Fault Time	1 – 99 Minutes	60 Minutes	60 Minutes
Cellular 24 Hr Test/UL864 Comm. Fire	Yes, No	No	No
Cellular Rollover	Yes, No	Yes	Yes
System			
Alarm Report Delay	No delay, 15 Seconds, 30 Seconds, 45 Seconds	30 Seconds	No Delay
Burglary Alarm Sound	Yes, No	Yes	Yes
Daylight Savings Time	Yes, No	Yes	Yes
Time Zone Offset		(UTC-5:00 Eastern Time (US & Canada)	(UTC-5:00 Eastern Time (US & Canada)
Software Version	XX.XX.XXXXX.XXX (Viewable Only)	XX.XX.XXXXX.XXX	XX.XX.XXXXX.XXX
Temperature Unit	Fahrenheit, Celsius	Fahrenheit	Fahrenheit
Installer Language	English	English	English
User Language	English	English	English
Two-way Voice	(Programmed via AlarmNet 360)	No	No
Local Programming Lockout	Yes, No	No	No
Z-Wave Support	Yes, No	Yes	Yes
Display Alarm Cancel	Yes, No	Yes	Yes
Lack of Usage Notify	Usage Not Monitored, 1 Day, 7 Days, 27 Days, 90 Days, 180 Days, 365 Days	Usage Not Monitored	Usage Not Monitored
RF Jam	Disabled, RF Jam Log, RF Jam Log and Report	RF Jam Log	RF Jam Log
Alarm Options	Not applicable (LCP300-L) Unlimited, 1, 2, 10 (LCP300-LC)	N/A	Unlimited
Number of Reports	1, 2, 3, 4, 5, 6 (LCP300-L)	2	
(Swinger Shutdown)	1, 2, 3, 4, 5, 6, Unlimited (LCP300-LC)		4
First Test Report Offset	6 Hours, 12 Hours, 18 Hours, 24 Hours	6 Hours	6 Hours
Report Frequency	Never, Every Day, Every 7 Days, Every 30 Days	Never	Never
System	Not programmable	Yes	Yes
Reporter	Not programmable	Yes	Yes
Panel Sync Delay Time	0 Minutes - 120 Minutes	3 Minutes	3 Minutes
Z-Wave Door Lock	Disabled, Arm Stay, Arm Away, Arm Without Autostay	Disabled	Disabled
Area			
System Timer			
Area Number	1	1	1
Entry Delay 1	None, 15 Seconds, 30 Seconds, 45 Seconds, 60 Seconds, 90 Seconds, 2 Minutes, 3 Minutes, 4 Minutes	30 Seconds	30 Seconds
Entry Delay 2	None, 15 Seconds, 30 Seconds, 45 Seconds, 60 Seconds, 90 Seconds, 2 Minutes, 3 Minutes, 4 Minutes	30 Seconds	30 Seconds
Exit Delay	45 , 60, 90, 120 Seconds (LCP300-L) None, 15, 30, 45 , 60, 90, 120 Seconds (LCP300-LC)	60 Seconds	60 Seconds

Programming Defaults (Continued)

Programming Field	Options	LCP300-L Default	LCP300-LC Default
Burglary Bell Timeout	No, 4 Minutes, 8 Minutes,12 12 Minutes, 16 Minutes,	4 Minutes	4 Minutes
Fire Bell Timeout	No, 4 Minutes, 8 Minutes,12 12 Minutes, 16 Minutes,	4 Minutes	4 Minutes
System Operation			
Quick Arm	Yes, No	Yes	Yes
Quick Exit	Yes, No	Yes	Yes
Restart Exit Time	Yes, No	Yes	Yes
Chime Mode	Yes, No	Yes	No
Force Bypass	Yes, No	No	No
Exit Warning	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Display Exit Time	Yes, No	Yes	Yes
Power-Up In Previous	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Auto Stay Arming	Yes, No	Yes	Yes
Arm Confirm	All RF, None, RF Keyfob, RF Keypad	None	RF Keyfob
Reporter			
Arm Away	Yes, No	Yes	Yes
Arm Stay	Yes, No	Yes	Yes
Disarm	Yes, No	Yes	Yes
Exit Error	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Alarm Restore	Yes, No	Yes	Yes
Alarm Cancel	Yes, No	Yes	Yes
Test	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Test Restore	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Low Battery	Yes, No	Yes	Yes
Low Battery Restore	Yes, No	Yes	Yes
RF Low Battery	Yes, No	Yes	Yes
RF Low Battery Restore	Yes, No	Yes	Yes
Recent Closing	Not programmable (LCP300-L)	Yes	
	Yes, No (LCP300-LC)		Yes
Event Log Full	Yes, No	Yes	Yes
Trouble	Yes, No	Yes	No
Trouble Restore	Yes, No	Yes	Yes
Bypass	Yes, No	Yes	Yes
Bypass Restore	Yes, No	Yes	Yes
AC Loss	Yes, No	Yes	Yes
AC Loss Restore	Yes, No	Yes	Yes
Log All Events	Yes, No	Yes	Yes
Log Alarm Events	Yes, No	Yes	Yes
Log Open/Close Events	Yes, No	Yes	Yes
Log Trouble Events	Yes, No	Yes	Yes
Log Non Security Events	Yes, No	Yes	Yes
Log Bypass Events	Yes, No	Yes	Yes

Zone Programming

The programmed defaults are shown. Refer to the Programming Field Explanations for additional information.

Zones 1-64 are RF Zones (Refer to "SENSORS" in AlarmNet 360)

Zones 65-68 are 5800 Garage Door Zones (Refer to "SENSORS" in AlarmNet 360)

Zones 131-162 are Keyfob Zones (Refer to "KEYFOBS" in AlarmNet 360)

Zones 280-291 are Temperature Zones (Refer to "SENSORS" in AlarmNet 360)

Zones 850-857 are Keypad Zones (Refer to "KEYPADS" in AlarmNet 360)

Zones 995, 996 and 999 are Panic Zones (Refer to "SENSORS" in AlarmNet 360)

Programming Defaults (Continued)

NOTE: For Zone Programming Options refer to Explanation of Zone Assignment Table Headings

Zone No.	Loop No.	Device Type	Response Type	Alarm Report	Chime	Supervision	Arm Night	Zone Descriptor
1	2	Door	Entry Exit 1	Yes	Standard	Supervised	N/A	Front
2	2	Door	Entry Exit 1	Yes	Standard	Supervised	N/A	Back
3	2	Window	Perimeter	Yes	Standard	Supervised	N/A	
4	1	Motion Sensor	Interior with Delay	Yes	Disabled	Supervised	No	
5-64			See Programming Field Explanations					
65	1	Garage Door	Not Used	Yes	Standard	Supervised	N/A	Main
66	1	Garage Door	Not Used	Yes	Standard	Supervised	N/A	Main
67	1	Garage Door	Not Used	Yes	Standard	Supervised	N/A	Main
68	1	Garage Door	Not Used	Yes	Standard	Supervised	N/A	Main
131	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
132	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
133	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
134	1	Key Fob	No Response	N/A	N/A	Button	N/A	
135	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
136	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
137	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
138	1	Key Fob	No Response	N/A	N/A	Button	N/A	
139	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
140	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
141	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
142	1	Key Fob	No Response	N/A	N/A	Button	N/A	
143	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
144	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
145	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
146	1	Key Fob	No Response	N/A	N/A	Button	N/A	
147	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
148	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
149	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
150	1	Key Fob	No Response	N/A	N/A	Button	N/A	
151	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
152	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
153	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
154	1	Key Fob	No Response	N/A	N/A	Button	N/A	
155	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
156	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
157	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
158	1	Key Fob	No Response	N/A	N/A	Button	N/A	
159	3	Key Fob	Arm Away	N/A	N/A	Button	N/A	
160	2	Key Fob	Disarm	N/A	N/A	Button	N/A	
161	4	Key Fob	Arm Stay	N/A	N/A	Button	N/A	
163	1	Key Fob	No Response	N/A	N/A	Button	N/A	
280	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
281	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
282	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
283	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
284	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
285	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
286	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
287	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
288	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
289	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
290	N/A	Temperature	Monitor	Yes	Disabled	High Temp	N/A	
291	N/A	Temperature	Monitor	Yes	Disabled	Low Temp	N/A	
840-847			Smart Device Zones – See Zone Programming Notes					
850	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
851	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
852	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
853	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
854	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
855	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
856	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
857	N/A	SiX™ Keypad	N/A	N/A	N/A	60Min	N/A	
995	N/A	Fire	Fire No Verification	Yes	N/A	Panic Trigger	N/A	
996	N/A	Medical	24 Hour Auxiliary	Yes	N/A	Panic Trigger	N/A	
999	N/A	Police	24 Hour Silent	Yes	N/A	Panic Trigger	N/A	

Zone Programming References

Explanation of Zone Assignment Table Headings

Loop Number - Used with 5800 Devices. Entries are 1-4, depending on device being used. Refer to the transmitter's instructions or the figure provided for appropriate loop numbers.

Device Type- Dependent upon the Zone Number being programmed.

Response Type/Action - Dependent upon the Device Type that has been selected.

Alarm Report – Activate/Deactivate reporting option for the device.
Options: Yes, No

Chime – Enable/Disable chime sounding for the device (applies to Entry/Exit, Perimeter and Interior Response Types only).

Disabled	Melody Long	Alert 1	Doorbell 2
Standard	Ascend	Alert 2	Evolve
Melody	Ascend Long	Doorbell 1	

Supervision - Dependent upon the Zone Number being programmed.

Wireless Zone (Zone 1-68)	Key Zone (Zone 131-162)	Temperature Zone (Zone 280-291)	Keypad (Zone 850-857
RF Supervised RF Unsupervised	Button	High Temp Low Temp	60Min

Arm Night – Activate/Deactivate specific Motion Sensors at (applies to Motion Sensor Response Type only).
Options: Yes, No

Zone Description 1/2 – Enter Zone Descriptors on displayed keypad. System Announces pre-programmed voice descriptors.

Device/Response Type Matrix

Device Type	Response Type	Entry Exit 1	Entry Exit 2	Perimeter	Resident Monitor	Resident Response	General Monitor	General Response	Day/Night	Interior Follower	Interior With Delay	Fire No Verification	Fire With Verification	Carbon Monoxide	24 Hour Auxiliary	24 Hour Audible	24 Hour Silent	Monitor	Not Used	Arm Stay	Arm Away	Disarm	No Response	Silent Burglary	Garage	Garage Monitor	Trouble
Carbon Monoxide Detector														x													
Door		x	x	x	x	x	x	x																			
Environmental															x		x										
Fire													x						x								
Flood															x		x										
Garage Door																									x	x	
Glass Break			x	x	x	x	x																				
Heat Sensor													x														
Medical															x	x			x								
Motion Sensor			x	x	x	x	x	x	x	x	x																
Other		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Police															x	x	x		x								
Smoke Detector												x	x														
Temperature															x		x										
Window		x	x	x	x	x	x	x	x																		

Zone Programming References *(Continued)*

SiX™ Series Device Signal Strength

Signal strength for the enrolled SiX Series Devices is displayed on the Zone Programming Screen for the individual Zone that is programmed. Signal strength information is provided below.

Icon	Description	Signal Strength
	Four Green Bars	Greater than -27 dBm
	Three Green Bars	Greater than -45 dBm
	Two Green Bars	Greater than -63 dBm
	One Green Bar	Greater than -81 dBm
	Four Red Bars	Less than -81dBm (below threshold)

NOTE: The threshold for passing the Go/No-Go test is -84.5dBm.

Regulatory Agency Statements

Federal Communications Commission (FCC) Part 15

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:

T his 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 or relocate the receiving antenna.
• 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.

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 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' interferences nuisibles. (2) Cet appareil doit accepter toute interference reçue y compris les interferences causant une reception 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 Frequences 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 NOTES 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/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, 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, 24E and 27.

LYRICLTE-A: The external antenna must not exceed a maximum directional gain (including cable loss) of 3.25 dBi at 850 MHz, 5.5 dBi at 1700 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, 24E and 27.

LYRICLTE-C: The external antenna must not exceed a maximum directional gain (including cable loss) of 0.6 dBi at 850 MHz, 5.5 dBi at 1700 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 IC RSS-130, RSS-132, RSS-133, and RSS-139.

LYRICLTE-V: The external antenna must not exceed a maximum directional gain (including cable loss) of 7.31 dBi at 780 MHz and 7.35 dBi at 1700 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, 24E and 27.

WARNING
THE LIMITATIONS OF THIS ALARM SYSTEM

While this System is an advanced design security system, it does not offer guaranteed protection against burglary, 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. Finally, 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 on the nature of the fire and/or location 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 the protected area approaches the temperature range of 90° to 105°F (32° to 40°C), 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 are located 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 by noise 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.
- 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, 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. The security keypad (and remote keypad) should be tested as well.

Wireless transmitters are designed to provide long battery life under normal operating conditions. Longevity of batteries may be as much as 4 to 7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, high or low temperatures, as well as large swings in temperature, may all reduce the actual battery life in a given installation. This wireless system, however, can identify a true low battery situation, thus allowing time to arrange a change of battery to maintain protection for that given point within the system.

Installing an alarm system may make the owner eligible for a lower insurance rate, 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.

Agency Notices

1. For Residential Burglar Alarm installations with line security, total exit delay time must not exceed 60 seconds. For Burglar Alarm installations without line security, total exit delay time must not exceed 120 seconds.
2. Periodic testing must be at least every 24 hours.
3. Remote downloading without an alarm company technician on-site (unattended downloading) is not permissible for ETL installations.
4. As SIA limits for delay of alarm reporting and sounding can exceed UL Standard limits for commercial and residential applications, the following requirements per UL681 are provided:

   The maximum time that a control unit shall be programmed to delay the transmission of a signal to a remote monitoring location, or to delay the energizing of a local alarm sounding device to permit the alarm system user to enter and disarm the system, or to arm the system and exit shall not exceed:

   a) 60 seconds for a system with standard line security or encrypted line security,

   b) 120 seconds for a system without standard line security or encrypted line security, or

   c) 120 seconds for a system that does not transmit an alarm signal to a remote monitoring location.

SIA Quick Reference Guide

Programming Section	Feature	Range	Shipping Default	SIA Requirement
Installation and Setup Guide or Programming Guide				
Reporter	Exit Error	Not selectable	Enabled	Enabled
	Recent Closing	Not selectable	Enabled	Enabled
	Alarm Cancel	Enabled or Disabled	Enabled	Enabled
System	Number of Reports (Swinger shutdown)	1 to 6 Reports	2 Reports	2 Reports
	Alarm Report Delay (Abort Window)	No Delay, 15, 30 and 45 seconds	30 seconds	30 seconds*
Area	Entry Delay # 1	None, 15, 30, 45, 60 and 90 seconds and 2, 3 or 4 minutes	30 seconds	30 seconds minimum
	Entry Delay # 2	None, 15, 30, 45, 60 and 90 seconds and 2, 3 or 4 minutes	30 seconds	30 seconds minimum
	Exit Delay	45, 60, 90 and 120 seconds	60 Seconds	45 seconds minimum
	Restart Exit Time	Enabled or Disabled	Yes (Enabled)	Enabled
	Exit Warning	Not selectable	Yes (Enabled)	Enabled
	Auto Stay Arming	Enabled or Disabled	Yes (Enabled)	Enabled
	Cross Zone Delay	30 seconds and 2 minutes (in 30 second increments), 3 minutes	None (Disabled)	Enabled and two zones programmed
Zones	Fire Alarms	Zone Type "Fire with Verification" must be selected for Fire Zone	Disabled	Disabled
User Guide				
User Functions/ User Access	Duress	Duress Code is Programmed by Master User as User 48	Disabled	Disabled
System Functions/ Testing the System**	System Test	System tests provided as a User Function	n/a	n/a
	Communications	While the system is in Test mode, no alarm reports are sent to the Central Station	Disabled	Disabled

* Combined Entry Delay and Alarm Report Delay (Abort Window) should not exceed 1 minute.
** Refer to the User Guide for procedures on Testing the System.

Specifications

Lyric Gateway Residential Burglar and Fire Alarm Control Panel	
Physical:	
Dimensions:	8.82" (22.4cm) W x 6.97" (17.7cm) H x 1.4" (3.6cm) D
Electrical:	
Voltage Input:	110VAC, 60 Hz/9 Vdc from plug-in 2.5A power supply
Rechargeable Backup Battery:	Nickel-metal hydride battery pack rated at 7.2 Vdc
	(LCP500-4B rated at 1100 mAh)
	(LCP500-24B rated at 3700 mAh)
Environmental	
Operating Conditions:	32-122°F (0-50°C)
Communication:	
Formats Supported:	ADEMCO Contact ID® Reporting, 10 characters/sec
	SIA/DCS Format, 2225Hz Handshake, Data Tones, 2025/2235Hz, baud

Glossary

AES – Advanced Encryption Standard

APL – Advanced Protection Logic

dBM – decibels milliwatt (power ratio)

CDMA - Code Division Multiple Access is a channel access method used by various radio communication technologies that allows many users to occupy the same time and frequency allocations in a given band/space.

DHCP – Dynamic Host Configuration Protocol, which provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS – Domain Name System, which is a distributed hierarchical naming system used to resolve domain names (e.g., www.yahoo.com) into numerical IP addresses (e.g., 204.17.25.1).

Ec/Io – Signal to noise ratio of the current channel for CDMA (Measured in dB).

Eb/No – Signal to noise ratio of the current channel for UTMS (3G) (Measured in dB).

ESN – Electronic Serial Number (32 bit number that identifies a CDMA device)

Gateway IP Address – A gateway (sometimes called a router) is a computer and/or software used to connect two or more networks (including incompatible networks) and translates information from one network to the other. The Gateway IP address is the IP address for the Gateway.

GPRS – General Packet Radio Service

GSM – Global System for Mobile communications, which is an international standard for digital mobile phone systems used for cellular communication.

HSDPA – High-Speed Downlink Packet Access

HSPA – High-Speed Packet Access

ICCID – Integrated Circuit Card Identifier (SIM Card serial number)

IMEI – International Mobile Equipment Identity number

IP – Internet Protocol

IP Address – A unique number consisting of four parts separated by periods, sometimes called a "dotted quad.," for example: 204.17.29.11, assigned to every computer/workstation connected to the Internet. IP numbers can be "static" (assigned and unchanging) or "dynamic," assigned via DHCP at each and every startup.

ISP – Internet Service Provider

KBPS – Kilobits per second

MAC ID – Media Access Code; located on the module label.

MEID – Mobile Equipment Identifier (56 bit number that identifies a CDMA device)

NIC – Network Interface Card

RSCP – Received Signal Code Power (Ratio of RSSI and Ec/No)

RSSI – Received Signal Strength Indication

SCID – SIM Card ID

SSID – Service Set Identifier (Network Name)

Subnet Mask – A Subnet is a portion of a network that shares a network address with other portions of the network, and is distinguished by a subnet number. The Subnet Mask is a 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

UMTS – Universal Mobile Telecommunications Service

WEP – Wired Equivalent Privacy

WPA – Wi-Fi Protected Access

WPS – Wi-Fi Protected Setup

Contacting Technical Support

PLEASE, before you call Technical Support, be sure you:

- READ THE INSTRUCTIONS!
- Check all wiring connections.
- Determine that the power supply and/or backup battery are supplying proper voltages.
- Verify your programming information where applicable.
- Note the proper model number of this product, and the version level (if known) along with any documentation that came with the product.
- Note your Honeywell customer number and/or company name.

Having this information handy will make it easier for us to serve you quickly and effectively.

Technical Support: 1-800-323-4576

Technical Support Hours...Monday – Friday 8:30 am – 9:00pm EST

.... Saturday 9:00 am – 5:30 pm EST

MyWebTech: ....https://www.mywebtech/honeywell.com

- Notes -

- Notes -

- Notes -

- Notes -

– Index –

THIS EQUIPMENT SHOULD BE INSTALLED IN ACCORDANCE WITH THE NATIONAL FIRE PROTECTION ASSOCIATION STANDARDS ANSI/NFPA 70 NATONAL ELECTRIC CODE AND NFPA 72 NATIONAL FIRE ALARM CODE, CHAPTER 2 (NATIONAL FIRE PROTECTION ASSOC., BATTERYMARCH PARK, QUINCY, MA 02169). PRINTED INFORMATION DESCRIBING PROPER INSTALLATION, EVACUATION PLANNING AND REPAIR SERVICE IS TO BE PROVIDED WITH THIS EQUIPMENT.

LYRIC GATEWAY ALSO COMPLIES WITH THE FOLLOWING: CANADIAN STANDARDS ASSOCIATION (CSA) C22.1, CANADIAN ELECTRICAL CODE, PART 1, SAFETY STANDARD FOR ELECTRICAL INSTALLATIONS AND CAN/ULC-S540 INSTALLATION OF RESIDENTIAL FIRE WARNING SYSTEMS.

THIS DEVICE COMPLIES WITH PART 15 OF FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

RJ45 ETHERNET RECEPTACLE

POWER SUPPLY RECEPTACLE

BATTERY RECEPTACLE

MICROSWITCHES
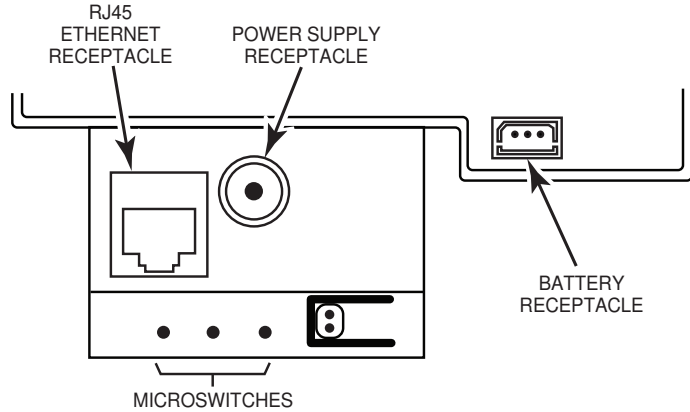
IMPORTANT NOTES ABOUT EXTERNAL ANTENNAS

IF AN EXTERNAL CELLULAR RADIO ANTENNA IS USED, THE ANTENNA MAY BE INSTALLED OR REPLACED ONLY BY A PROFESSIONAL INSTALLER.
LYRIC-3G/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, 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 DBIAT 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, 24E AND 27.
LYRICLTE-A: THE EXTERNAL ANTENNA MUST NOT EXCEED A MAXIMUM DIRECTIONAL GAIN (INCLUDING CABLE LOSS) OF 3.25 DBI AT 850 MHZ, 5.5 DBI AT 1700 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, 24E AND 27.
LYRICLTE-C: THE EXTERNAL ANTENNA MUST NOT EXCEED A MAXIMUM DIRECTIONAL GAIN (INCLUDING CABLE LOSS) OF 0.6 DBI AT 850 MHZ, 5.5 DBI AT 1700 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 IC RSS-130, RSS-132, RSS-133, AND RSS-139.
LYRICLTE-V: THE EXTERNAL ANTENNA MUST NOT EXCEED A MAXIMUM DIRECTIONAL GAIN (INCLUDING CABLE LOSS) OF 7.31 DBI AT 780 MHZ AND 7.35 DBI AT 1700 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, 24E AND 27.

WEEKLY TESTING IS REQUIRED TO ENSURE PROPER OPERATION OF THIS SYSTEM

THE LYRIC GATEWAY IS COMPATIBLE WITH THE FOLLOWING INTEGRAL RECHARGEABLE BATTERY PACKS:
LCP500-4B P/N 300-03864-AIO (STANDARD CAPACITY)
LCP500-24B P/N 300-03866-AIO (HIGH CAPACITY)

REPLACE EVERY FOUR YEARS

WARNING

THIS UNIT MAY BE PROGRAMMED TO INCLUDE AN ALARM VERIFICATION FEATURE THAT WILL RESULT IN A DELAY OF THE SYSTEM ALARM SIGNAL FROM THE INDICATED FIRE CIRCUITS. THE TOTAL DELAY (CONTROL UNIT PLUS SMOKE DETECTORS) SHALL NOT EXCEED 60 SECONDS. NO OTHER INITIATING DEVICES SHALL BE CONNECTED TO THESE CIRCUITS UNLESS APPROVED BY THE LOCAL AUTHORITY HAVING JURISDICTION.

CIRCUIT (ZONE)	CONTROL UNIT DELAY-SEC	SMOKE DETECTOR	
		MODEL	DELAY-SEC
01 - 64 ZONE TYPE - SUPERVISED FIRE WITH VERIFICATION	30 seconds	5806W3	10 seconds

gw_keypad-SOC-V1

LYRIC GATEWAY RESIDENTIAL BURGLAR AND FIRE ALARM CONTROL PANEL SUMMARY OF CONNECTIONS

NOTES: Connection of the fire alarm signal to a fire alarm headquarters or a Central Station shall be permitted with the approval of the local authority having jurisdiction. The burglar alarm signal shall not be connected to a police emergency number. The System must be checked by a qualified technician once every three years

SUPPORT, WARRANTY, & PATENT INFORMATION

For the latest documentation and online support information, please go to:
https://mywebtech.honeywell.com/

For the latest warranty information, please go to:
www.honeywell.com/security/hsc/resources/wa

For patent information, go to:
www.honeywell.com/patents

MyWebTech   Warranty   Patents

800-21666   10/16 Rev. A