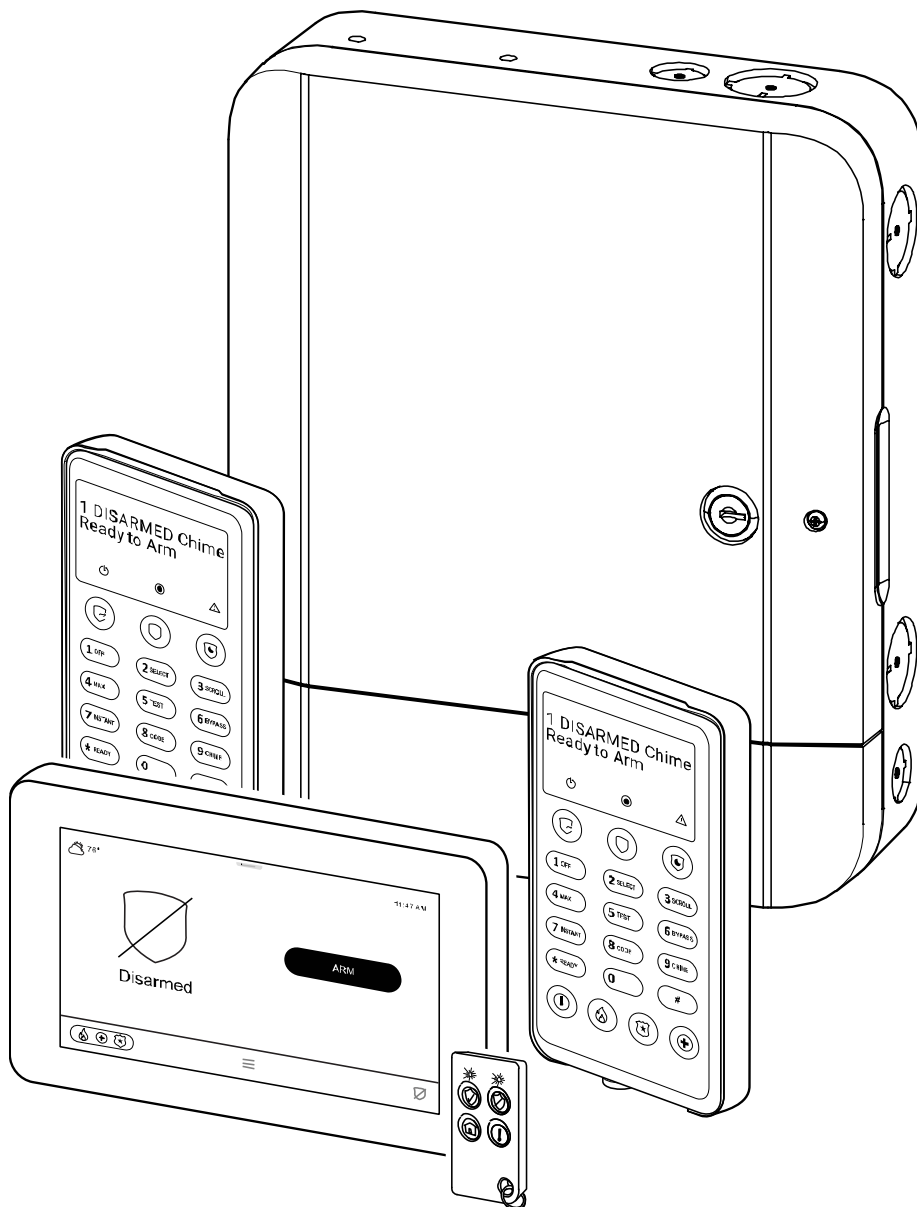


FIRST ALERT

VISTA Security System

VISTA H3/VISTA H3CN Security System

Installation and Setup 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

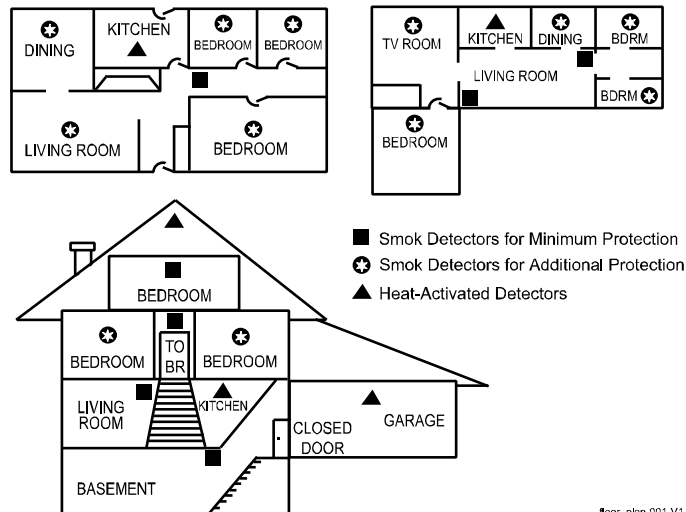
With regard to the number and placement of smoke/heat detectors, we subscribe to the recommendations contained in the National Fire Protection Association's (NFPA) Standard #72 noted below.

- 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 smoke detectors in kitchens, attics (finished or unfinished), or in garages is not normally recommended.
- For additional protection the NFPA recommends that you install heat or smoke detectors in the living room, dining room, bedroom(s), kitchen, hallway(s), attic, furnace room, utility and storage rooms, basements and attached garages.

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.



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 ensures 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).

This First Alert Pro security system is designed for use with devices manufactured or approved by Resideo Technologies, Inc., through its subsidiary Ademco Inc. ("Resideo"). Your security system is not designed for use with any device that may be attached to your security system's touchpad or other communicating bus if Resideo has not approved such device for use with your security system. Use of any such unauthorized device may cause damage or compromise the performance of your security system and affect the validity of your Resideo limited warranty. When you purchase devices that have been manufactured or approved by Resideo you acquire the assurance that these devices have been thoroughly tested to ensure optimum performance when used with your security system.

Table of Contents

System Features	1
Installation Steps	3
STEP 1 - Create an Account	3
STEP 2 - Mounting and Wiring the Control Panel	4
Cabinet Mounting and Tamperers	4
Securing (Locking) the Cabinet Door	5
Communication Modules	6
Installing the PROLTE Series Cellular Communications Module	6
Installing the PROLTE-ANT External Fixed Length Antenna	7
Installing the PROWIFIZW/PROWIFI Communications Modules	8
Installing the VISTAHTKVRWL Wireless Module	9
Installing the VISTAHIISO iBus Isolator Module	10
Hardwired Zones	11
Normally Open and Normally Closed Zones with 2K EOLR	11
Zone Voltages	11
2-Wire Smoke Detectors	12
4-Wire Smoke Detectors	12
Double-Balanced Zones	13
Zone Doubling	13
Sounder (Bell) Connections	14
Bell Supervision	14
iBus Technology	15
Introduction	15
Wiring	15
Using an external Power Supply	15
Wiring the VISTAHPKP English Keypads	16
Wiring the VISTAHEXPHW (8 Zone Expander) and VISTAHRELAY Relay Module	17
Wiring the VISTAHIISO iBus Isolator Module	18
VISTAHTKVR-B Installation	19
VISTAHTKVR-V Installation	19
Triggers 1 & 2 Outputs	20
Backup Battery	21
Battery Calculations Worksheet	22
Wiring the DC Transformer	23
Earth Ground	23
LED Behaviors	24
STEP 3 - Configure (Programming)	25
Configuring Wi-Fi using Bluetooth	25
Using the AN360 Application	25
Using the Total Connect 2.0 (TC2) Application	25
Wi-Fi Setup	26
Selecting Wi-Fi Network	26
Add Network Manually	26
WPS Setup	27
Wireless Access Point	27
Enrolling a VISTAHTCHWLC keypad for Local Programming	28
Accessing Tools Menu	30
System Information Screen	31
System Tests	31
Programming	32
Zone Response Type Matrix	33
PROSIX™ Series Devices	33
5800 Series Devices	36
Hardwired and iBus Zones	37
Zone Response Type Definitions	38
Zone Assignments	40
Cross Zoning	40
Programming Fields	41
Configuring Partitions and their Options	41
Adding Wireless Sensors (PROSIX, 5800, or VISTAHTKVRWL)	43
Onboard Hardwired Zone Configuration	45
Adding Keyfobs	46
Adding PROSIXLCDKP Keypads	46
Enabling/Disabling Panics	46

Delete Zones and Peripherals	46
Automation Rules (Relays and Triggers)	50
SIA Programming Default Values	52
Registration	53
Local Alarm Mode	53
Cellular	54
Wi-Fi Touchscreen Enrollment	54
Installer PIN	54
Default Options	54
Reboot	54
Shutdown System	54
Wireless Devices	55
Zones	55
Range	55
Frequency Agility	55
One-Go-All-Go	55
Smoke / CO Maintenance	55
Transmitter Supervision	55
Transmitter Battery Life	56
Testing Signal Strength	56
Keypad / Touchscreen Setup	56
PROSIXLCDKP Wireless Alpha Keypad	56
VISTAHTCHWLC Wireless Touchscreen	57
Step 4 – Confirm (System Operation and Testing)	58
Keypad / Touchscreen Displays and Operation	58
PROSIXLCDKP Wireless Alpha Keypad Displays and Operation	58
Keypad Menu Mode	59
Partitioning	61
Common Partition	61
Goto Command	61
System Clock	61
Scheduling	61
Audio Alarm Verification (AAV) (2-Way Voice)	62
Security Codes	63
Programming Security Codes via Touchscreens	63
Authority Levels	63
Fire Authority Access User	64
Disarming / Canceling an Alarm	65
Emergency Panic Keys / Icons	65
Event Log	65
Contact ID® Event Log Codes	66
Central Station Messages	67
Keypad Tamper Lockout	68
Keypad Displays	68
Testing the System	69
Communications Tests	69
Walk Test Mode	69
Normal Mode Test	70
Armed System Test	70
Step 5 – Commission	70
Specifications	71
Contacting Technical Support	71
Regulatory Agency Statements	72
Summary of Connections	75

System Features

The VISTA3/VISTA3CN is a hybrid Control Panel / Communicator with a combination of both wired and wireless devices that features easy installation and usage. Internal modules allow the Control Panel to communicate with Wireless Zone Transmitters, Z-Wave devices, and to the Central Station via Cellular Wireless and/or Internet (Wi-Fi and/or Ethernet).

System Features

- 4 Partitions provide protection for up to four individual protection areas (Partition 3 or 4 can be a Common Partition)
- Voice Announcement of System and Zone Status via VISTAHTCHWLC Touchscreens
- Automatic Stay Arming
- Night Stay Arming
- 100 User Codes (Standard, Guest, Arm Only, Partition Master, and Duress)
- Panic Functions - Police, Fire, Medical
- Supports Keypads and Touchscreens
- Audio Alarm Verification (AAV), (2-Way Voice)
 - Supported over Cellular or IP (Wi-Fi or Ethernet)
 - Requires VISTAHTCHWLC Wireless Touchscreen for Stations
- Event Log - 10,000 Events (Local viewing requires VISTAHTCHWLC Touchscreen)
- RF Jam Detection for all supported wireless technologies
- Exit Error (Detects difference between an actual alarm and exit alarm caused by leaving a door open after the exit delay expires)
- Built-in cabinet tamper or optional wall mount tamper

Home Automation

- Z-Wave Support (requires the PROWIFIZW Module)
- Enroll up to 78 Z-Wave Home Automation Devices including:
 - Thermostats (up to 5)
 - Door Locks (up to 5)
 - Devices (outlets, switches, lamps / appliances)
- Supports Z-Wave Network Wide Inclusion (NWI)
- Supports 100 Scenes

System Configuration Limits

- 64 Input Devices (Intrusion / Fire Zones)
 - 64 is the total number of zones the panel supports no matter what configuration used.
Example you could have a maximum of 56 PROSIX Series devices (sensors) or 56 5800 Series devices (requires VISTAHTKVRWL module), but not 56 of each.
 - 8 Onboard Hardwired Zones (Up to 16 2-Wire smokes on zone 1) (Wireless or iBus zones cannot be used for zones 1-8).
- 64 Output Devices (Triggers + Relays)
- Supported Modules and Keypads

Part Number	Description	System Configuration Limits
VISTAHPKP*	Hardwired Keypad	iBus, maximum 8 Hardwire
PROSIXLCDKP*	Wireless LCD Keypad	PROSIX, maximum 8 wireless keypads
VISTAHTCHWLC*	Wireless Touchscreen	Wi-Fi, maximum 8 wireless touchscreen keypads (Requires the PROWIFIZW/PROWIFI Module)
VISTAEXPHW**	Hardwired Zone Expansion Module	iBus, up to 56 zone expansion modules supported, however, the maximum number of iBus expansion zones supported are 56.
VISTAHRELAY	Relay Expansion Module	iBus, up to 64 relay modules supported, however the maximum number of relays used is 62. Two of the outputs are for the onboard triggers 1 and 2.
PROLTE-A Series	LTE Cellular Communications Module (US/Canada, AT&T network)	Control slot 1 and 1 module supported
PROLTE-V Series	LTE Cellular Communications Module (US, Verizon network)	
PROLTE-CN Series	LTE Cellular Communications Module (Canada, Bell network)	
PROWIFIZW	Wi-Fi with Z-wave	Control slot 2 and 1 module supported
PROWIFI	Wi-Fi Only	
VISTAHTKVRWL***	Universal Wireless Module	Control slot 3 and 1 module supported
VISTAHIISO	iBus Isolation Module	Only one module is supported.

* A maximum of 24 keypads are supported no matter how configured

** No matter how the system is configured, 64 zones is the limit. Eight of these zones are hardwired on the panel while the rest are iBus expansion or wireless (PROSIX or using the VISTATKVRWL Module).

*** The VISTATKVRWL module supports communication with certain previously installed wireless sensors and modules. Refer to the VISTATKVRWL Compatibility chart (p/n R800-26221) for a list of tested and approved vendor wireless devices.

System Features (Continued)

Alarm Output

- 12V Bell Output for Wired Sounders
- Steady Output for burglary/panic
- Temporal 3 Pulse Output for fire alarms
- Temporal 4 Pulse Output for carbon monoxide alarms
- 2 Amp Maximum Output
- Supervised with 820-ohm EOLR

Communication

- LTE Cell Communications (primary path when used with a wired internet connection)
 - PROLTEA (ATT)
 - PROLTEV (Verizon)
 - PROLTE-CN (Bell)
- Built-In Internet Communicator
 - Requires hardwired connection via Cat5e cable to the onboard ethernet port.
- Wi-Fi communication using the PROWIFIZW or PROWIFI
- ADEMO Contact ID Format

System Power

- Primary Power: Plug-in Power Supply, 110VAC to 14.3VDC, 2.65A output, p/n R300-112131 or R300-12131-CAN (Canada)
- Backup Battery: 12Vdc, 7AH (sealed lead acid type). Charging Voltage – 13.65Vdc

Programming

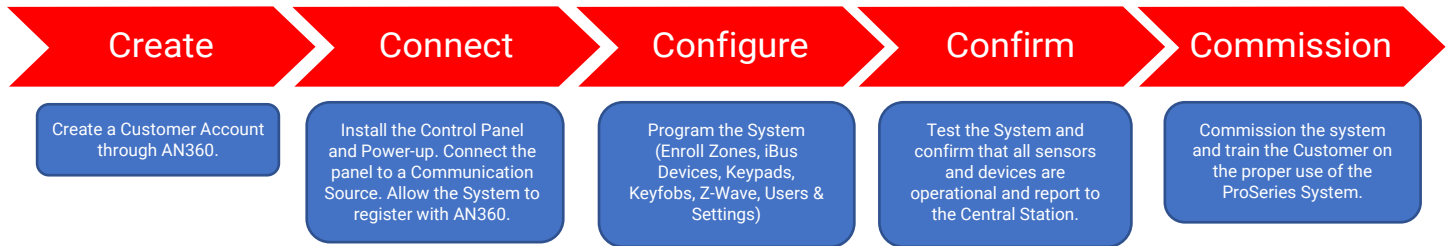
- Programming stored in Flash
- Can be uploaded, downloaded, or controlled using capable Cellular Module or Internet Communications
- Registered, programmed, and tested locally or via AlarmNet 360™. Use a PC or Smart Device to go to: www.alarmnet360.com or the AlarmNet360 App.

NOTE: Local programming requires a touch screen keypad.

Installation Steps

IMPORTANT:

Local programming is only achieved with the VISTAHTCHWLC touch screen Keypad. Please see the "Configure" step below for important information regarding enrollment.



STEP 1 - Create an Account

Registration, Programming, and Testing are conducted locally with the VISTAHTCHWLC keypad or through AlarmNet 360™ (AN360). On a laptop, PC, or Smart Device, go to www.alarmnet360.com or the AlarmNet360 App. Using these tools, create a customer account.

From AN360

1. Select Devices and Programming
2. Select + NEW ACCOUNT
3. Select Security/Fire
4. Enter the control's MAC and CRC
5. Fill out the Necessary Data as shown on the screen to the right.

NOTE: For Panel Type select **VISTA3/VISTA3CN** with the appropriate revision.

resideo alarmnet 360® 06-04-2024 11:26:51 (GMT) 06-04-2024 07:26:51 AM (EDT) Take A Tour Firmware Jobs What's New KK

New Account CANCEL FINISH

1 Customer Info 2 Security

INSTALLATION FOR

Dealer *
Search & select dealer

CUSTOMER INFO

☒ New Customer ☐ Existing Customer

Customer Type: *
☐ Residential ☐ Commercial

CUSTOMER NAME

First Name
Last Name

CONTACT DETAILS

Phone
Home > USA/CAN > (Primary)
Customer Email ?
+ Add another

SECURITY ACCOUNT

LOCATION

Location Name * ?
Dealer ID
Reference ID ?
Sold by ?
Installed by ?
Contract end date ?
MM/DD/YYYY

ADDRESS

Country *
United States of Ameri >
Address Line 1
Address Line 2
City
State/Territory
Select State >
ZIP

CONTROL PANEL

Type *
Select Panel Type >
Revision * ?
Select Panel Revision >

SELECT THE ACCOUNT TYPE

☒ Standard (Requires MAC) ☐ Draft

(Click here to identify the location of the MAC and CRC on your Device)

MAC *
ENTER MAC
CRC *
ENTER CRC

Alarm Reporting Number (City-CS-Sub) * ?
CONTINUE

CANCEL FINISH

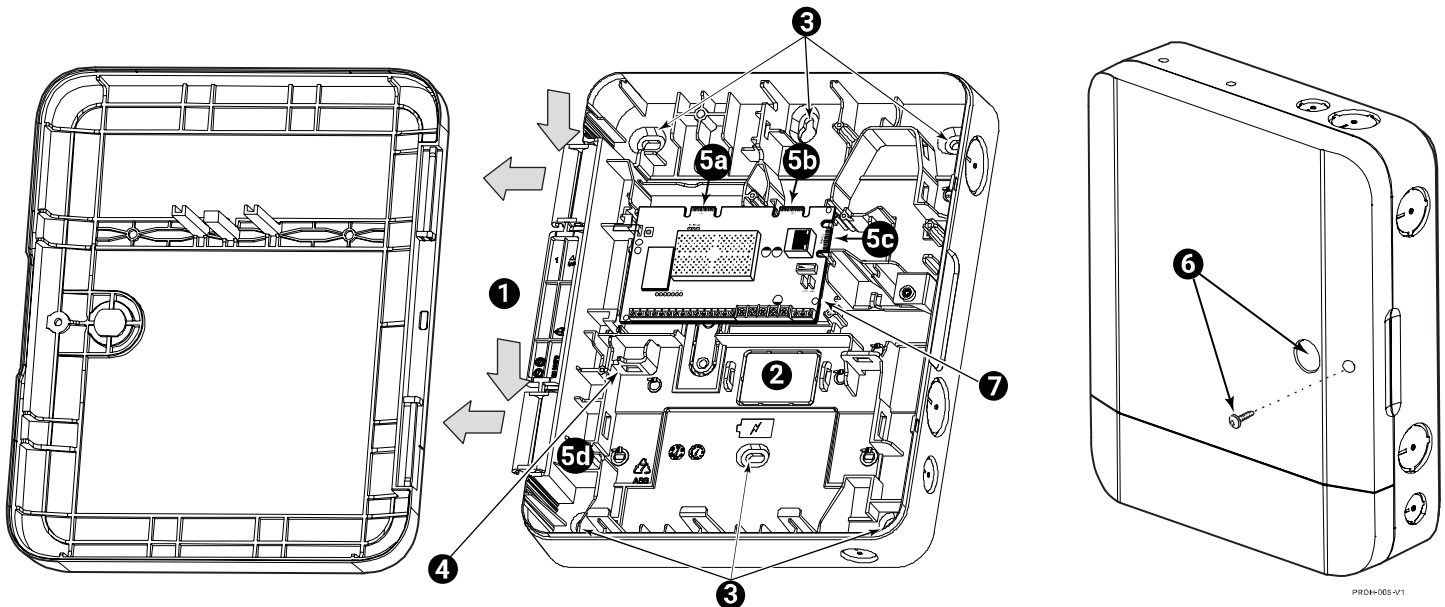
Terms & Conditions Privacy Statement Browser Requirements Copyright © 2024 Resideo Technologies, Inc. | Version: 1.2.154.5984

STEP 2 - Mounting and Wiring the Control Panel

Cabinet Mounting and Tamper

Mount the Control Panel cabinet to a sturdy wall in a clean, dry environment, which is not readily accessible to the public. Use fasteners or anchors (not supplied) with the cabinet mounting holes.

1. Open the cabinet door fully and, if required, remove it by pulling to the down, towards the back of the cabinet.
2. Use the rear wiring entry or remove the cabinet knockouts needed for the wiring entry.
3. Mount the control cabinet to a sturdy wall in a clean, dry area, which is not readily accessible to the general public, using fasteners or anchors (not supplied) with the six cabinet mounting holes.
4. Install Wall Tamper screw.
 - Secure the wall tamper with an anchor and screw. If an intruder attempts to pull the cabinet off the wall, the perforated tamper will remain on the wall, disengaging the rear tamper on the panel board.
 - If disarmed, it will go into trouble and, if armed, it will go into alarm and send the respective report.
5. Install the PROLITE Series Communicators [a], PROWIFIZW/PROWIFI [b], VISTAHTKVRWL Wireless Converter [c] and/or VISTAHSO [d].
6. When installation, wiring, and programming are completed, install the cabinet door, and secure it with the provided screw or option keylock (P/N CAMLOCK-HYB).
7. Cover Tamper
 - The cabinet door has a tamper post that, when closed, engages the tamper switch on the front of the panel board. When opened, it generates a trouble condition when disarmed or an alarm when armed and sends the respective report to the Central Station.
 - This tamper cannot be disabled and will not prevent arming when activated.
 - Required for the VISTAHTCHWLC enrollment process.

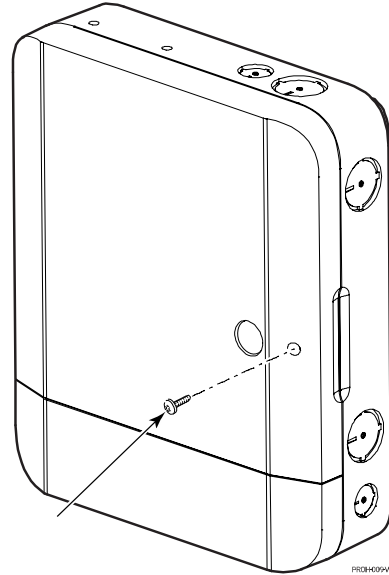


Mounting and Wiring the Control Panel (Continued)

Securing (Locking) the Cabinet Door

Locking the Cabinet

The cabinet can be closed and secured without a lock by using a screw in the front of the cover.

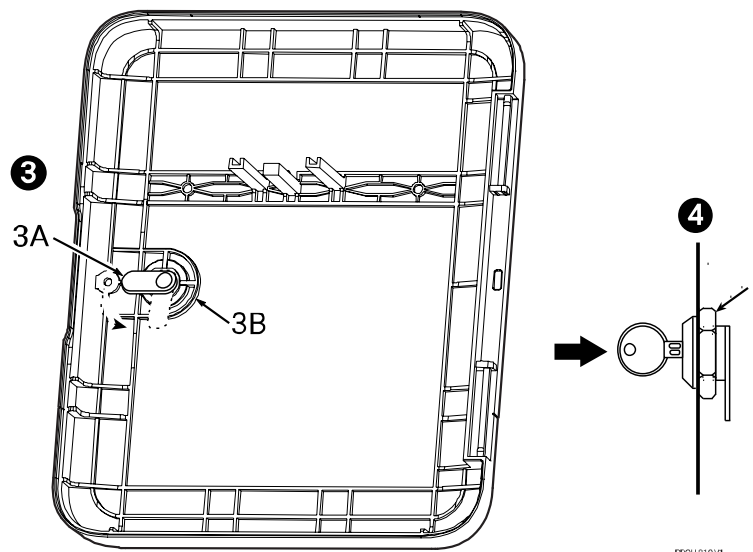
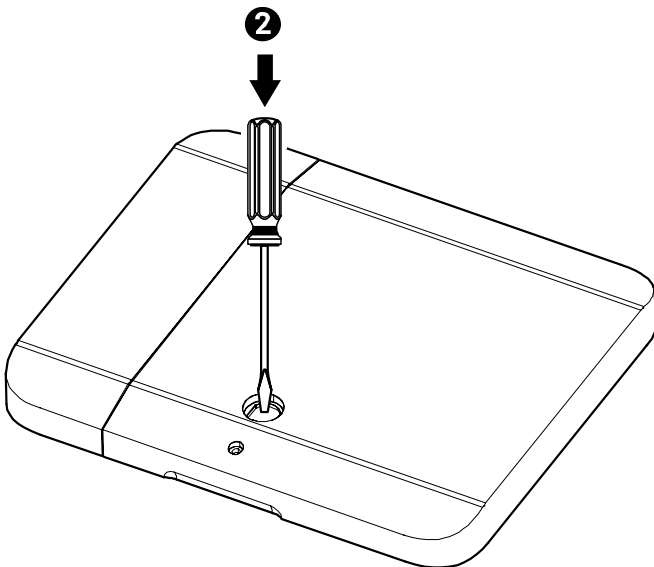


Optional Key Lock

If desired, a key lock can be installed (CAMLOCK-HYB).

1. Remove the cabinet door as shown earlier.
2. Remove the knockout from the front of the cabinet door by firmly pushing the knockout through from the front using your hand or a screwdriver.
3. Position the lock in the hole, making certain that the latch will connect with the latch bracket when the door is closed. Confirm the Lock (3A) and Unlock (3B) positions before moving to Step 4.
4. Slide the lock nut over the lock and turn clockwise until tightly against the plastic cover.

NOTE: May require a set of pliers to fully tighten it.



5. Reinstall the cabinet door by firmly pressing it back on the hinges.

Mounting and Wiring the Control Panel (Continued)

Communication Modules

The Control Panel supports Central Station reporting using Cellular and/or Internet communications as well as upload/download programming capability. The Control Panel requires either a cellular communicator and/or an internet connection to register with AlarmNet. If both cellular and internet paths are used, the Control Panel will use internet as primary and cell as a backup. Additionally, a Z-Wave module allows the Control Panel to support Home Automation functions while a VISTA HTKVRWL module is used to support other wireless technologies (refer to the User Guide p/n R800-28380 dated 1/24 or later for additional information). The Control Panel is compatible with the following Communication Modules:

Model	Description
PROLTE-A	LTE Cellular Communications Module (US/Canada, AT&T network)
PROLTE-V	LTE Cellular Communications Module (US, Verizon network)
PROLTE-CN	LTE Cellular Communications Module (Canada, Bell network)
PROWIFIZW	Wi-Fi / Z-Wave Communications Module
PROWIFI	Wi-Fi Communications Only (No Z-Wave)



RF Exposure

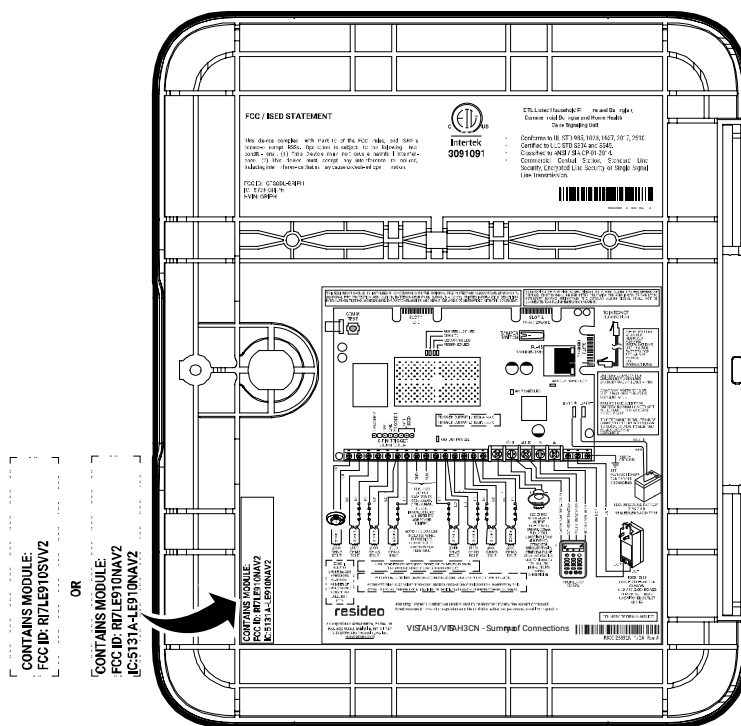
WARNING: The Control Panel must be installed to provide a separation distance of at least 7.8 in (20 cm) from all persons and not co-located or operated in conjunction with any other transmitter except in accordance with FCC multi-transmitter product procedures.



Ensure that all electrical power has been removed from the Control Panel before installing the module. Unplug the power supply and disconnect the backup battery and earth ground (if used).

Installing the PROLTE Series Cellular Communications Module

1. Affix the provided FCC/IC label (P/N 800-24257V1 or PROLTEB for the PROLTE-A/PROLTE-CN or 800-24256V1 for the PROLTE-V) on the VISTA H3/VISTA H3CN cabinet door.
2. Remove electrical power (if applied). Refer to the *System Shutdown* section for additional information.
3. Unplug the power supply.
4. Disconnect the battery.

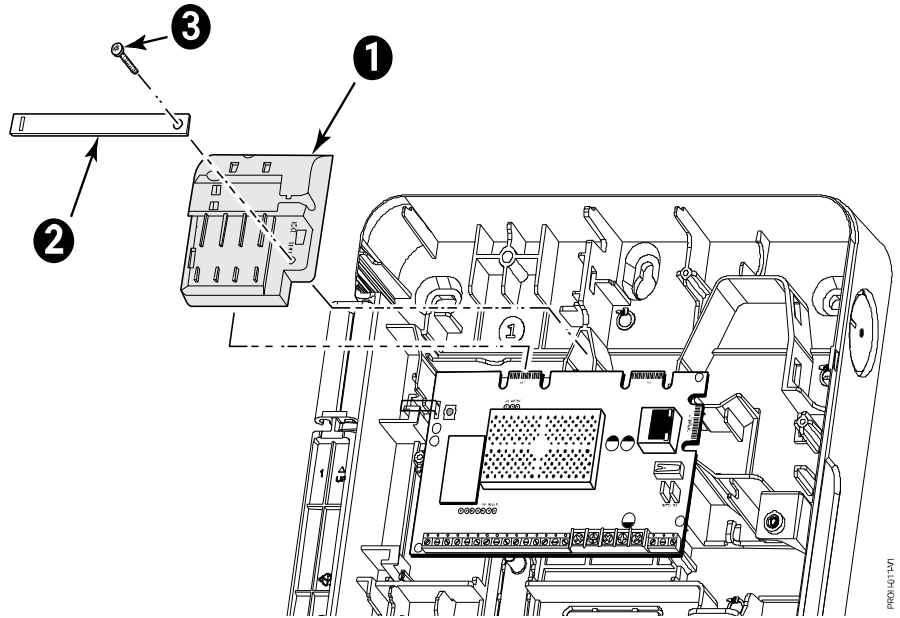


PROH-008-V1

Mounting and Wiring the Control Panel (Continued)

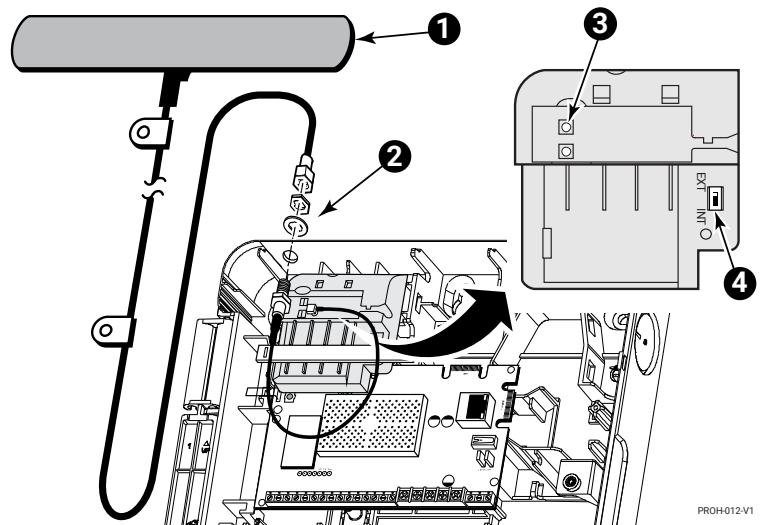
Installing the PROLTE Series Cellular Communications Module (Continued)

5. Install the PROLTE communicator [1] on the top left edge connector on the PCB. Ensure the receptacle is securely seated on the edge connector.
6. Install the retainer clip [2] and secure with the provided screw [3].
7. Reconnect the battery.
8. Plug the power supply into a 24-hour, 110VAC non-switched outlet.



Installing the PROLTE-ANT External Fixed Length Antenna

1. Find a suitable location for mounting the antenna [1] vertically.
2. Power down the Control Panel.
3. Remove the knockout [2].
4. Plug the SMA end of the cable [3] into the module's external antenna port and route the cable.
5. Set the switch on the module to EXT [4].
6. Permanently mount the antenna vertically using the double-sided self-adhesive and the included hardware.
7. Reconnect the backup battery and plug in the power supply.
8. Perform a Communication Test.



For registration, programming and signal status, visit AlarmNet 360 website or use an360 mobile app.

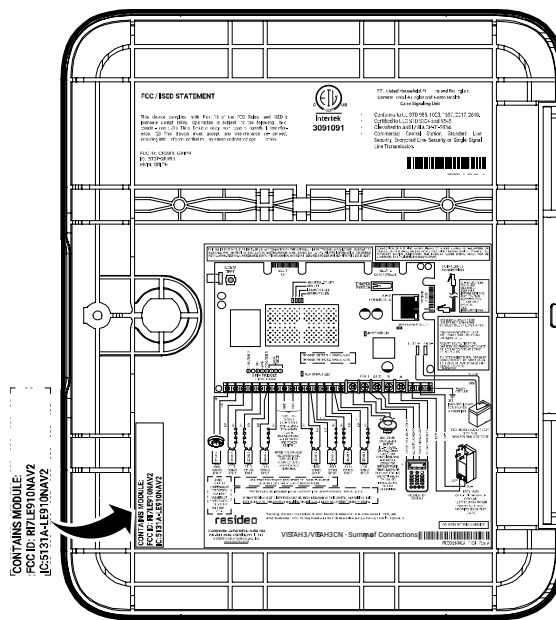
Mounting and Wiring the Control Panel (Continued)



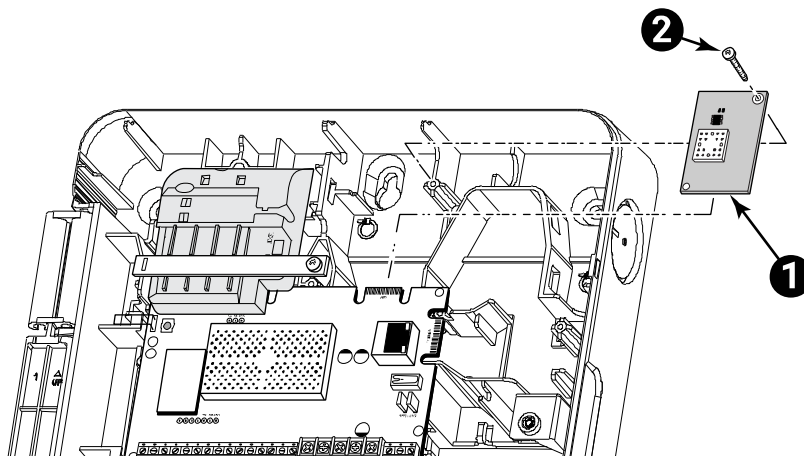
Ensure that all electrical power has been removed from the Control Panel before installing the module. Unplug the power supply and disconnect the backup battery and earth ground (if used).

Installing the PROWIFIZW/PROWIFI Communications Modules

1. Affix the provided FCC/IC label (PROWIFIZW P/N 800-24286V1) on the VISTA3/VISTA3CN cabinet door.
2. Remove electrical power (if applied), power down the control. Refer to the *System Shutdown* section for additional information.
3. Unplug the power supply.
4. Disconnect the battery and earth ground.



5. Install the PROWIFIZW/PROWIFI [1] on the top-right edge connector on the Control Panel's PCB. Ensure the receptacle is securely seated on the edge connector.
6. Secure the module with the provided screw [2].
7. Reconnect the battery.
8. Plug the power supply into a 24-hour, 110VAC non-switched outlet and power up the control panel.



NOTE:

In the event the Control Panel loses primary AC (<9.9VDC), it will power down the PROWIFIZW module after a few minutes to conserve battery. This will result in loss of wireless communication to the Control Panel and 2-Way Voice with all touchscreens and wireless keypads.

Mounting and Wiring the Control Panel (Continued)

Installing the VISTAHTKVRWL Wireless Module

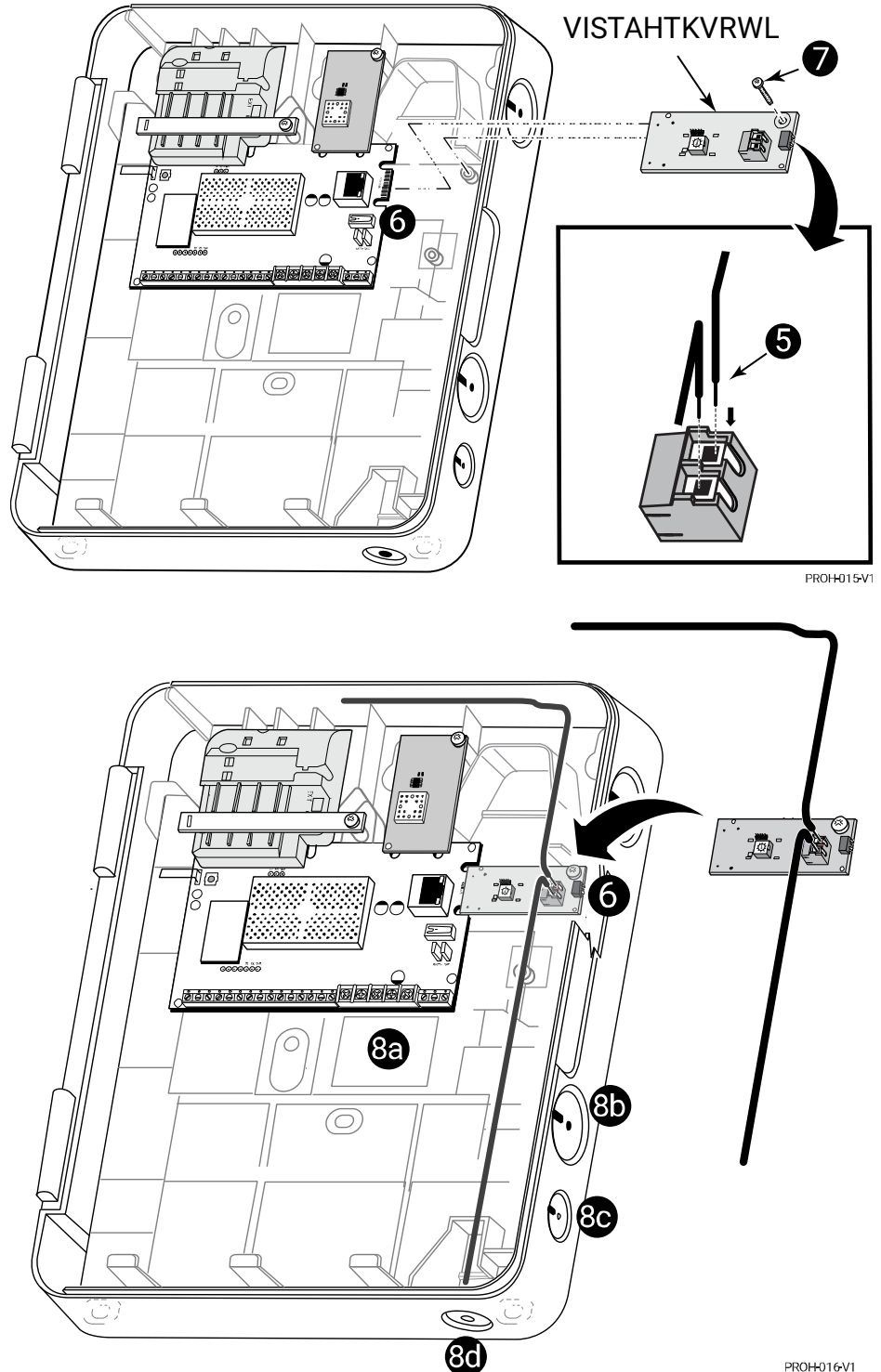


Ensure that all electrical power has been removed from the Control Panel before installing the module. Unplug the power supply and disconnect the backup battery and earth ground (if used).

1. Remove electrical power (if applied). Refer to the *System Shutdown* section for additional information.
2. Unplug the power supply.
3. Disconnect the battery and earth ground.
4. Set the rotary switch on the VISTAHTKVRWL module to the setting associated with the existing wireless sensors and modules and the Control Panel. See Dial Settings below for the supported wireless protocols. Only one wireless protocol can be used in addition to PROSIX.
5. Connect the VISTAHTKVRWL antenna to the module before installing the module.
6. Install the VISTAHTKVRWL module on the edge connector on the right-hand side of the PCB. Ensure the receptacle is securely seated on the edge connector. Route each antenna as shown.
7. Secure the module with the provided screw.
8. Route any wiring through the rear access [8a] or the knockouts on the bottom right [8b, 8c, 8d] to avoid interfering with the antennas.

NOTE: The green LED will blink once per each RF signal that it receives.

VISTAHTKVRWL Rotary Switch Setting	
Protocol	VISTA3
5800	5
2GIG	6
DSC	7
ITI/Qolsys	8
Bosch	9



NOTE: The VISTAHTKVRWL module supports communication with certain previously installed wireless sensors and modules. Refer to VISTAHTKVRWL Compatibility chart (p/n 800-25183) for a list of tested and approved vendor wireless devices.

Mounting and Wiring the Control Panel (Continued)

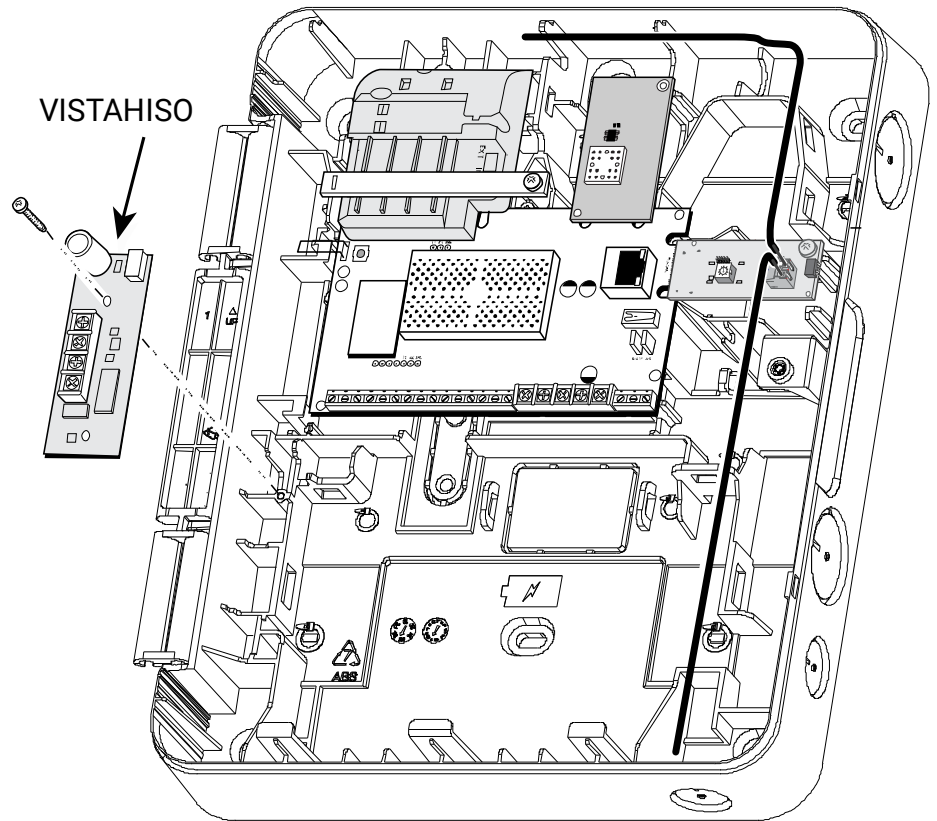
Installing the VISTAHISO iBus Isolator Module

The module is designed to be mounted in the control cabinet. Below the Control Panel PCB and to the left of the battery.

NOTE: Only one (1) VISTAHISO can be installed.

1. Remove electrical power (if applied).
Refer to the *System Shutdown* section for additional information.
2. Unplug the power supply.
3. Disconnect the battery and earth ground.
4. Using the two screws provided, mount the VISTAHISO to the cabinet as shown.

NOTE: Refer to section *Wiring the VISTAHISO iBus Isolator* for wiring information.



VISTAHISO-004V1

Mounting and Wiring the Control Panel (Continued)

Hardwired Zones

Each hardwired zone 1-8 can be used for burglary or fire devices and is defaulted for use with a 2K (red, black, red, gold) EOLR. Zone 1 must use a 2k ohm resistor, but zones 2-8 can scan the zone, detecting the current resistor value (done during zone setup in programming). Use the diagrams below to wire devices to the zone(s) with an EOLR. All devices and zones are setup, programmed, and tested locally or via AlarmNet 360.

While the diagrams below show 2 contacts per zone to show the concept, it is recommended to have only one contact per zone for the following reasons:

1. Allows each zone to have a Zone Descriptor specific to that contact e.g. Front Door, Kitchen Window, etc.
2. If a problem occurs with a contact, it will be easier to troubleshoot than having multiple contacts wired.

Normally Open and Normally Closed Zones with 2K EOLR

Normally Open Zones/ N.O. EOLR Zones

1. Connect open circuit devices in parallel across the loop; for EOLR zones, connect the EOLR across the loop wires at the last device.
2. Enable normally open/EOLR zones using Zone Programming mode, "Hardwire Type" prompt.

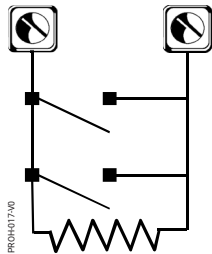
Normally Closed Zones/ N.C. EOLR Zones

1. Connect closed circuit devices in series in the high (+) side of the loop; for EOLR zones, connect the EOLR in series following the last device.
2. Enable normally closed/EOLR zones using Zone Programming mode, "Hardwire Type" prompt.

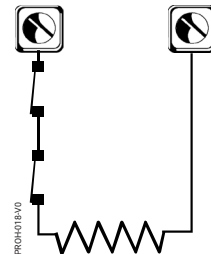
End of Line Resistor (EOLR) Notes

- If the EOLR is not at the end of the loop, the zone is not properly supervised, and the system may not respond to an "open" on the zone.
- Zone 1 is intended for EOLR only.

Normally Open device(s) in parallel with 2K EOLR



Normally Closed device(s) in series with 2K EOLR



IMPORTANT:

If the EOLR is not connected to the last device on the end of the line, the zone circuit will not be properly supervised.

Zone Voltages

Voltages on the zones will change with respect to the EOLR depending on the state of the contact. For Burg and Panic zones, an opened or a shorted condition will trigger the zone into a Fault or Alarm. For Fire and Carbon Monoxide (CO) zones, an open will trigger a Trouble, whereas a short will trigger an Alarm. **NOTE:** The table below represents voltages based off using the 2K Ohm resistor shipped with the panel. If using a different resistance, voltages will be different.

Wired Zones	2K EOLR (Normal)	Burg / Panic		Fire / Carbon	
		Opened (Fault/Alarm)	Shorted (Fault/Alarm)	Opened (Trouble)	Shorted (Alarm)
1 (2-Wire Smokes)	13.5VDC	13.8VDC	0VDC	13.8VDC	0VDC*
2-8	5.1VDC	12.8VDC	0VDC	12.8VDC	0VDC

* A two-wire smoke latched into alarm will pull the voltage down to 6.7VDC

NOTES:

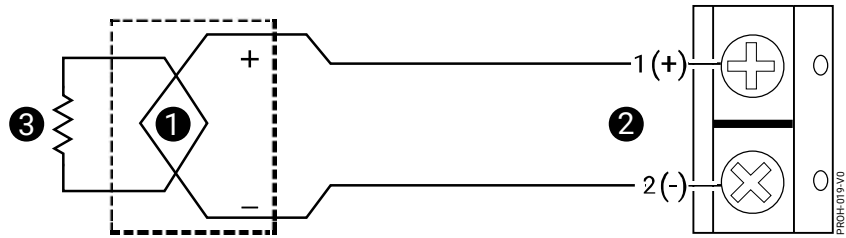
- 2-Wire Smoke voltage is measured between Z1 and GND and you should receive 12VDC. However, to verify the proper zone functionality meter between Z- (negative) and any ground on the panel and use the table above to verify voltages.
- 2-8 voltage is measured between Zn (n = 2 to 8) and GND and use the table above to verify proper voltages.
- Each zone has a 300-ohm tolerance above and below the necessary 2K resistance. (i.e., Resistances can swing from 2.3K down to 1.7K before the zones will activate.)
- Although zone 1 is a powered zone for 2-wire smoke detectors, it can be used for burglary devices instead. If 2-wire smokes are used, they must be connected on zone 1.

Mounting and Wiring the Control Panel (Continued)

2-Wire Smoke Detectors

1. Connect a maximum of Sixteen 2-wire smoke detectors [1] on zone 1 terminals [2], terminals 1 (+) and 2 (-), as shown. Observe proper polarity when connecting the detectors.
2. Connect the required 2K EOLR across the zone at the last detector [3] at the end of the line. You may need to refer to the instructions of your smoke detector for specific EOLR placement.

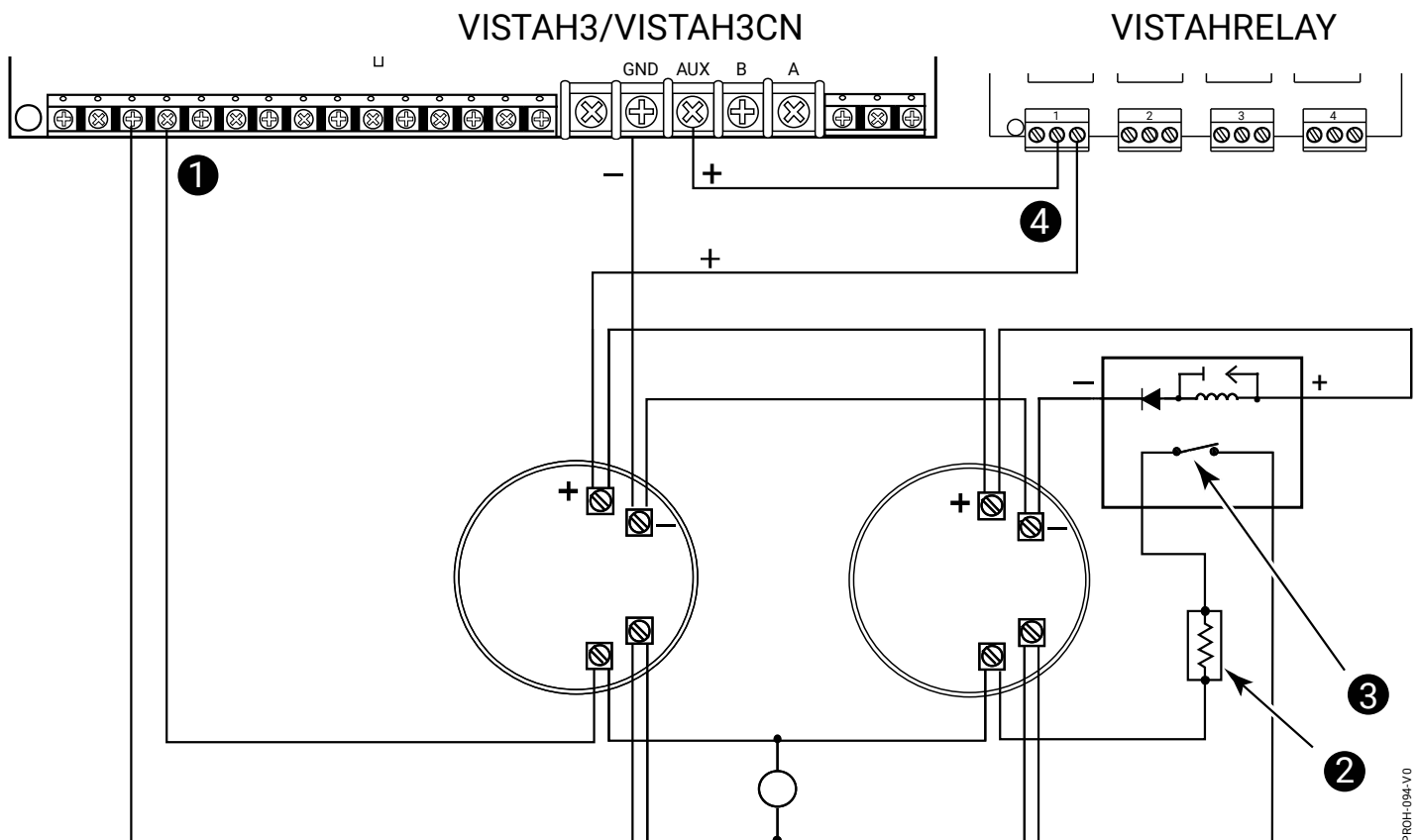
NOTE: Zone one supports two-wire smoke detectors only. When the smoke detector resets, the zone terminals reset, any programmed trigger or relay will not follow the reset logic.



3. After the fire alarm condition, the Control Panel will reset the power to the 2-wire smokes by dropping power momentarily from the zone terminals immediately after the second disarm.

4-Wire Smoke Detectors

1. Connect 4-wire smoked detector Alarm output to any zone (other than zone 1) [1] on the control panel or VISTAEXPHW.
NOTE: Verify the appropriate EOLR is installed based on the control panel (2K Ohm) or VISTAEXPHW (2.2K Ohm) [2] and the end of line supervision relay is installed [3] (Shown below with power on, so relay will be closed, opens when power lost creating a supervision trouble on the keypad).
2. Connect the power source using the onboard trigger with a slave relay or VISTAHRELAY [4] to reset the power.
3. Program the output as required for the smoke detector reset in Automation Rules.



Mounting and Wiring the Control Panel (Continued)

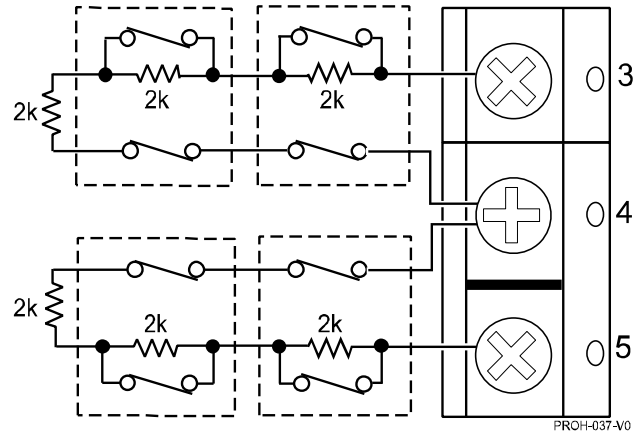
Double-Balanced Zones

Connect as shown below (resistor provided for one device). Compatible with zones 2-8 (showing zones 2 and 3)

IMPORTANT:

Double-balanced zones provide zone tamper protection, and should be used as burglary zones only.

Do not use double-balanced zones as fire zones.



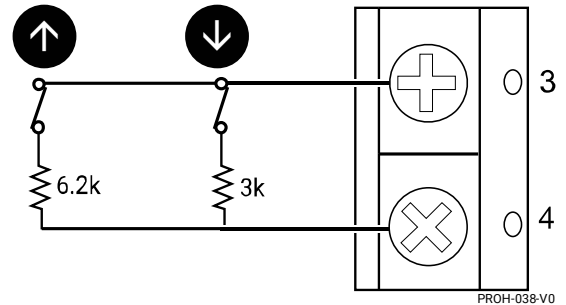
Zone Doubling

This feature provides two hardwired normally closed zones for each standard hardwired zone connected to the control's terminals. If enabled, hardwire zones are automatically paired to the next available zone number starting with zone 9.

Connect as shown (resistors supplied; use 3k, for the lower zone [↓], and 6.2k, for the upper zone [↑], 5% 1/4W or bigger resistors).

Do not use zone doubling for fire zones.

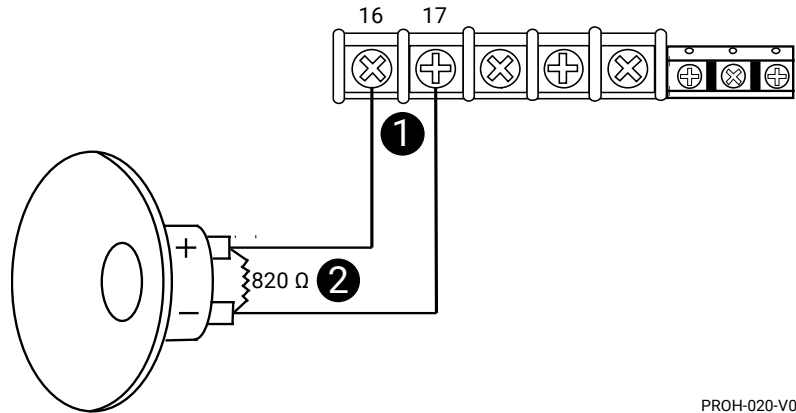
NOTE: A short across the EOL (i.e., at terminal) on either zone of a zone-doubled pair or on a double-balanced zone causes a tamper condition (displayed as CHECK plus zone numbers).



Mounting and Wiring the Control Panel (Continued)

Sounder (Bell) Connections

1. Make sounder connections to the Alarm Output terminals, Positive (+) to BELL [16] and Negative (-) GND [17].
2. The 12VDC sounder output [1] activates when an alarm occurs and is silenced when the first disarm command is entered.
3. For burglary alarms, the Alarm Output produces a steady voltage to the sounder.
4. For fire alarms, per NFPA requirements, the Control Panel will produce Temporal 3 Pulse voltage to the sounder. Temporal 3 Pulse sounding for fire alarm consists of 3 pulses – pause – 3 pulses – pause – 3 pulses, etc.
5. For Carbon Monoxide, it produces Temporal 4 Pulse voltage to the sounder. Temporal 4 Pulse sounding for CO alarm consists of 4 pulses – pause – 4 pulses – pause – 4 pulses, etc.



PROH-020-V0

Bell Supervision

Bell supervision is enabled by default which will supervise the sounder circuit for an opened condition while the Alarm Output is inactive and a shorted condition while active in alarm condition. Supervision requires the supplied 820-ohm resistor (gray, red, brown) [2] to be connected on the last sounding device on the end of the line. Do not connect the resistor directly to the bell output terminals because this will not properly supervise the bell circuit. The bell output will always have 4.6Vdc (without resistor) for supervision purposes, even if supervision is disabled in programming. Connecting the 820-ohm resistor will bring that voltage down to 0Vdc.

NOTES:

- If a high impedance sounding device is used, such as a siren driver, the bell supervision resistor may need to be installed at the device, else the 4.6V supervision voltage may trigger the siren driver while in the disarmed state.
- Total current drawn from this output cannot exceed 2 amps. Exceeding 2 amps will overload the power supply, or may cause the internal electronic circuit, protecting the sounder output, to activate, preventing the sounder from working.
- The control panel is reliant on the back up battery, as it supplies the current to drive the siren. If there is a Low Battery condition, the bell output may not operate properly.
- The Alarm Output's logic of "Sounding per Zone per Armed Period" will follow "Swinger Suppression" (default 2). E.g. If the Front Door triggers an alarm and the bell output times out after 4 minutes, the bell will restart if the Front Door is triggered again, but no more. Any burg zone will only trigger the sounder twice in an armed period, unless the option for Swinger Suppression is changed.

UL

- Use only UL Listed sounding devices for UL installations.
- Bell supervision is required for fire alarm installations.
- The total current drawn from the alarm output and the auxiliary power output, combined, cannot exceed 200mA. In addition, the sounding device must be a UL Listed audible signal appliance rated to operate in a 10.2-13.8 VDC voltage range and must be mounted indoors.

Mounting and Wiring the Control Panel (Continued)

iBus Technology

Introduction

The Control Panel utilizes the iBus to supervise and communicate with compatible hardwired expansion devices. iBus uses an RS-485 protocol and consists of a four-conductor bus: Power Positive, Power Negative, Data A (output) and Data B (input).

Terminal	Label	Description
17	GND (-)	Ground reference point for data and auxiliary power
18	AUX (+)	Positive Auxiliary Power: should read 12-13VDC
19	B	The "B" data: follows RS-485 Standards
20	A	The "A" data: follows RS-485 Standards

Wiring

The recommended wiring is stranded and twisted. When installing a four-conductor wire, the limitations below apply to Auxiliary Power. The data pair of wire can run up to 4000 feet on 22-gauge wire.

Wire Gauge (AWG)	Total Current of All Devices Connected to a Single Wire Run				
	50mA or less	100mA	300mA	500mA	600mA
#22	700ft (213m)	350ft (107m)	120ft (37m)	70ft (21m)	60ft (19m)
#20	1200ft (366m)	600ft (183m)	200ft (61m)	120ft (37m)	100ft (30m)
#18	1900ft (579m)	950ft (290m)	320ft (98m)	190ft (58m)	160ft (49m)
#16	3000ft (914m)	1500ft (457m)	500ft (152m)	300ft (91m)	260ft (76m)

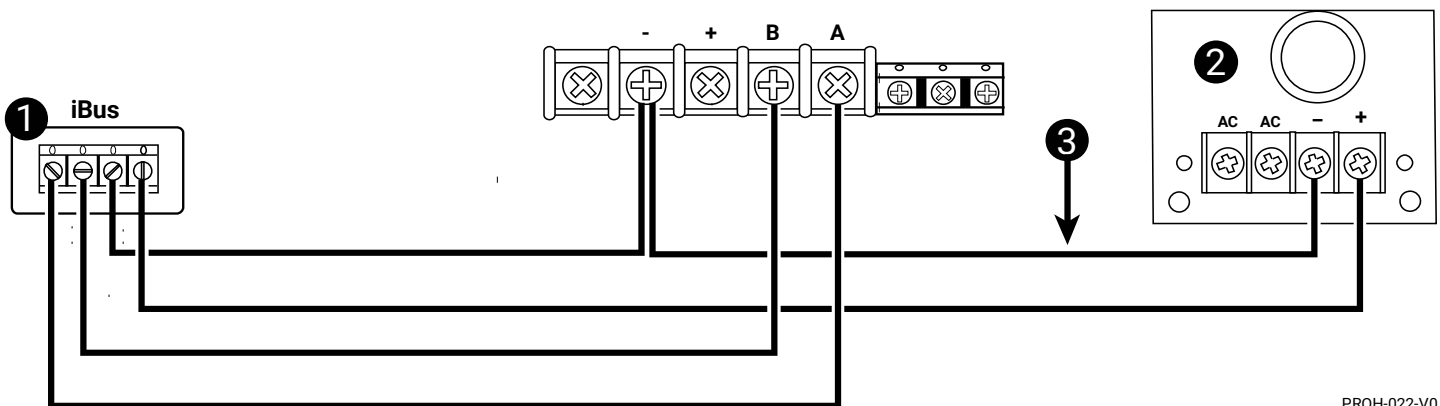


The length of all wire runs for all partitions combined must not exceed 3000 feet (914m) when unshielded quad conductor cable is used or 1500 feet (457m) if shielded cable is used.

Using an external Power Supply

It is our recommendation that if the iBus device(s) [1] are powered from an alternate power source [2], a common ground [3] must be used.

Number	Description
1	iBus device
2	Power Supply
3	Common Ground
-	Control GND (-)
+	Control AUX (+)
B	Control B
A	Control A



PROH-022-V0

Mounting and Wiring the Control Panel (Continued)

Wiring the VISTAHPKP/VISTAHLKP English Keypads

Connect the keypad terminals iBus A [1], iBus B [2], DC Power Ground [3], and DC Power Positive (+) [4] to the Control Panel's iBus terminals, GND [17], AUX [18], B [19] and A [20], as shown below and on the *Summary of Connections* diagram. Determine wire size using the Wire Run Chart in the *iBus Technology* section above.

PROGRAMMING NOTES:

- Keypads are not pre-enrolled (see note below). The keypad will display "Pairing with System" until they are learned into the Control Panel. They will learn in once the Control Panel has been put into "Learn Mode" locally with the VISTAHTCHWLC or via AlarmNet 360. Each keypad will provide a confirmation beep and updated display status once complete.

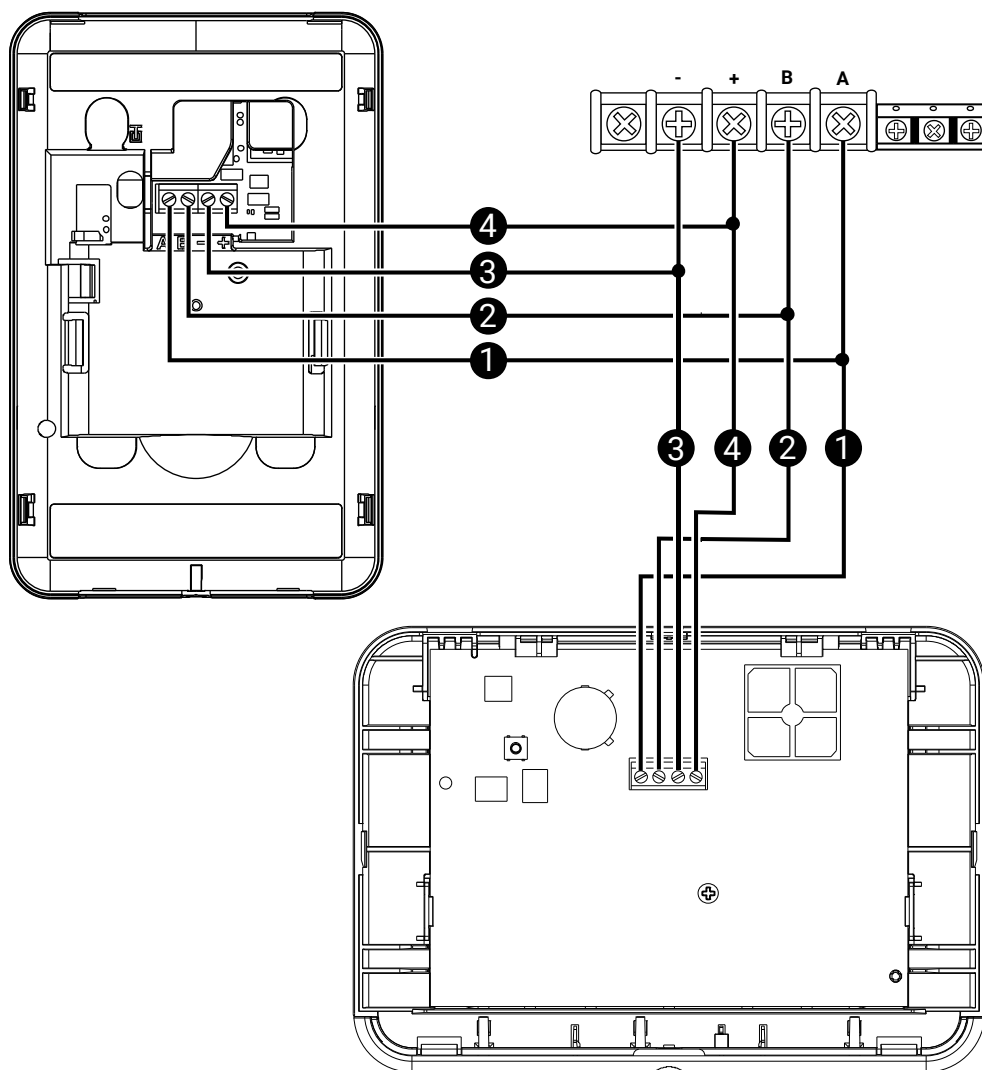
NOTE: When the panel is not registered to AN360 during first 15 minutes of bootup the panel will auto enroll all iBus keypads connected to control panel.

- The keypads display "Busy Standby" when the Control Panel is being programmed locally or from AlarmNet 360. It provides a single beep when programming is complete.
- If multiple keypads are connected, the Control Panel will learn them randomly.
- If you want to program names to the keypads, keep track of the keypad's serial numbers / MAC addresses so you'll know which one is which.

1	Green: iBus A
2	Yellow: iBus B
3	Black: Negative (-)
4	Red: Positive (+)

NOTES:

- For single 4-wire runs, determine the current drawn by all units, then refer to the wiring chart to determine the maximum length that can be safely used for each wire size.
- Keypads powered from power supplies that do not have a backup battery will not function if primary power is lost and the panel will produce a tamper message. Make sure to power the keypads either from the Control Panel's auxiliary power output or from a power source with a backup battery.



PROH-021-V1

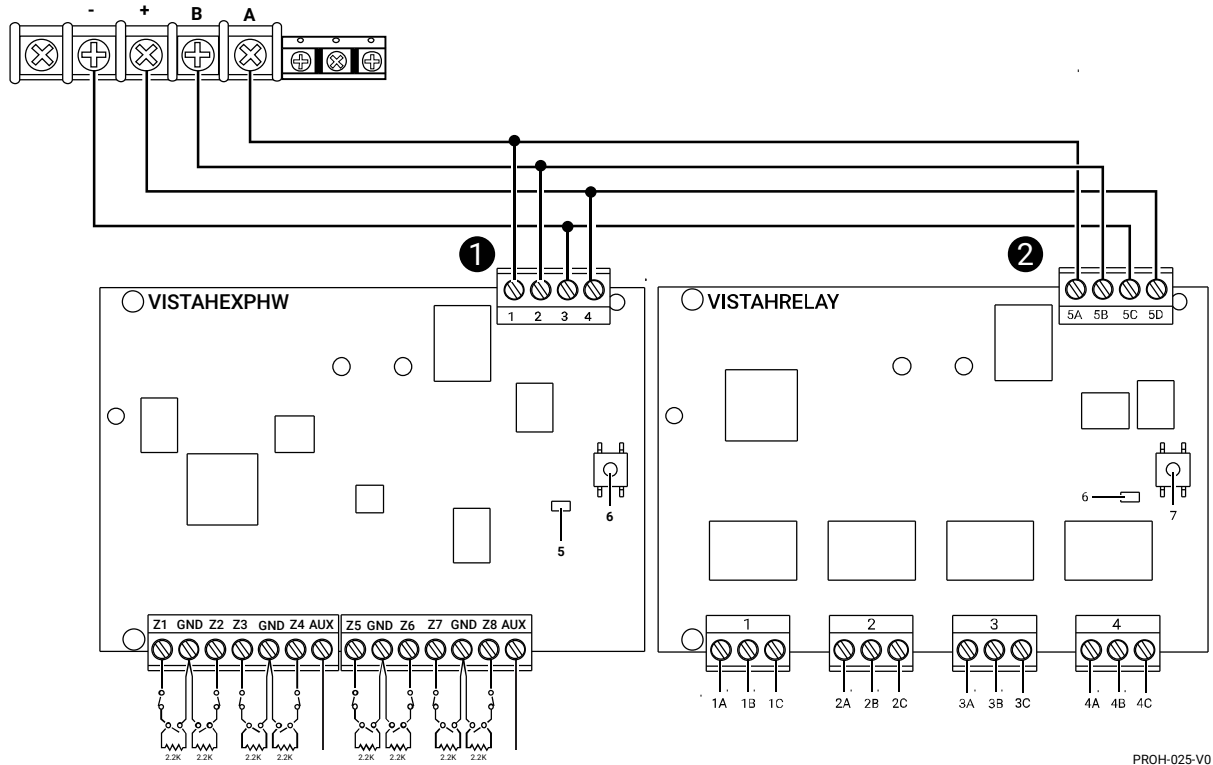
Control Panel LED Operation

- iBus/Active (Red)** - Lit solid if the keypad bus is active and operational.
- AUX (Green)** - Lit solid while proper current is being pulled from Auxiliary Power. If power is shorted or too much current is being pulled, the LED will turn off.

Mounting and Wiring the Control Panel (Continued)

Wiring the VISTAEXPHW (8 Zone Expander) and VISTAARELAY Relay Module

Connect the VISTAEXPHW [1] and VISTAARELAY'S [2] iBus data and power to the Control Panel's iBus terminals, GND, AUX, B and A, as shown below and on the *Summary of Connections* diagram. Determine wire size using the Wire Run Chart in the *iBus Technology* section above. For detailed installation instructions, refer to each module's Installation and Setup Guide (VISTAEXPHW: P/N R800-28389 and VISTAARELAY: P/N R800-28391).



PROH-025-V0

1 VISTAEXPHW

iBus	1	Yellow: iBus A
	2	Green: iBus B
	3	Black: Negative (-)
	4	Red: Positive (+)
ZONE ASSIGNMENTS	5	LED
	6	Tamper
	Z1	Zone 1
	-	Zone 1 & 2 Common
	Z2	Zone 2
	Z3	Zone 3
	-	Zone 3 & 4 Common
	Z4	Zone 4
	+	Auxiliary Power (+) *
	Z5	Zone 5
	-	Zone 5 & 6 Common
	Z6	Zone 6
	Z7	Zone 7
	-	Zone 7 & 8 Common
	Z8	Zone 8
	+	Auxiliary Power (+) *

* Auxiliary power is limited to the same power supply the module is connected to.

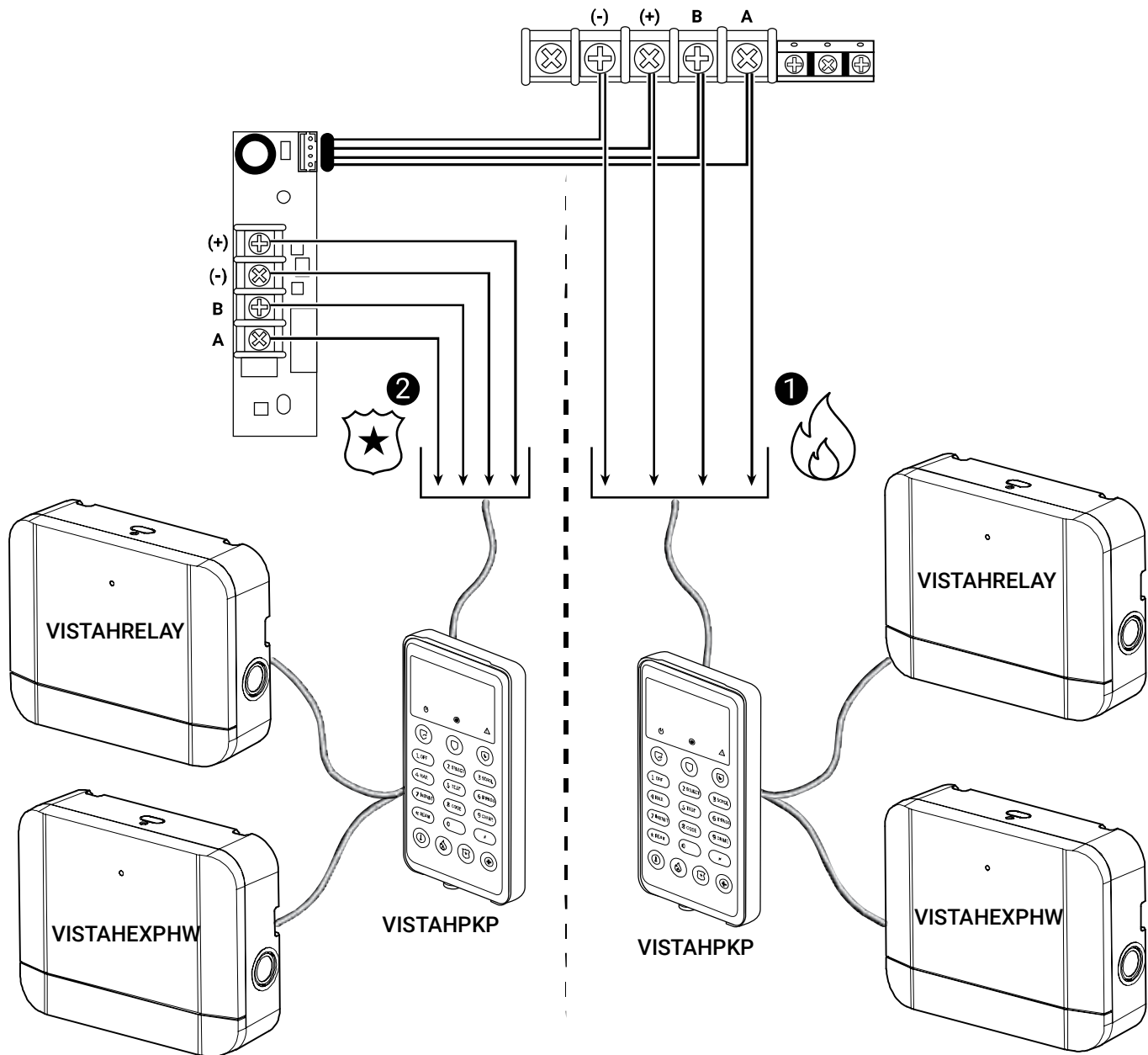
2 VISTAARELAY

Relay 1	1A	Normally Open
	1B	Common
	1C	Normally Closed
Relay 2	2A	Normally Open
	2B	Common
	2C	Normally Closed
Relay 3	3A	Normally Open
	3B	Common
	3C	Normally Closed
Relay 4	4A	Normally Open
	4B	Common
	4C	Normally Closed
iBus	5A	Yellow: iBus A
	5B	Green: iBus B
	5C	Black: Negative (-)
	5D	Red: Positive (+)
	6	LED
	7	Tamper

Mounting and Wiring the Control Panel (Continued)

Wiring the VISTAISO iBus Isolator Module

The iBus Isolator and Control Panel must be wired so that the Control Panel's iBus terminals connect to the harness from the VISTAISO. Additionally, the Control Panel's iBus Terminals also connect to all Fire Devices [1] following the instructions that are supplied with the devices. Wiring in this manner isolates the Fire Devices from the Burglary Devices in case of a short on the Burglary circuit. To connect the iBus Isolator, reference the following illustration and make these connections:



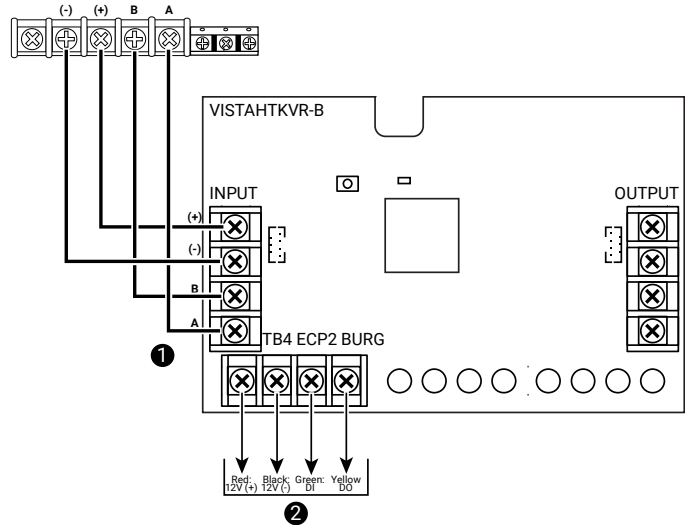
PRO1-088-V1

Mounting and Wiring the Control Panel (Continued)

VISTAHTKVR-B Installation

The VISTAHTKVR-B Gateway module allows compatibility for Enhanced Console Protocol (ECP) devices to operate on this control panel. It connects to the control's iBus bus wiring terminals and is mounted remotely. The VISTA H3 Control panel support 4 VISTAHTKVR-B modules, one for each partition. See the VISTAHTKVR-B Installation Guide (p/n R800-28650) for detailed setup instructions.

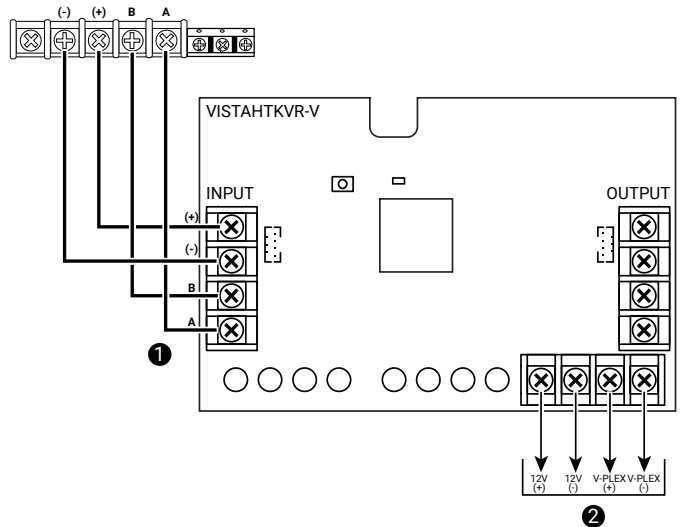
Connect the Control Panel's iBus to the iBus on the VISTAHTKVR-B [1]. Next, connect the compatible ECP devices (found in the VISTAHTKVR-B Installation Instructions) [2].



VISTAHTKVR-V Installation

The VISTAHTKVR-V Gateway module allows compatibility for Resideo V-Plex devices to operate on this Control Panel. It connects to the control's iBus bus wiring terminals and is mounted remotely. The VISTA H3 Control panel support 4 VISTAHTKVR-V modules, one for each partition. See the VISTAHTKVR-V Installation Guide (p/n R800-28651) for detailed setup instructions.

Connect the Control Panel's iBus to the iBus on the VISTAHTKVR-V [1]. Next, connect the compatible ECP devices (found in the VISTAHTKVR-V Installation Instructions) [2].



Mounting and Wiring the Control Panel (Continued)

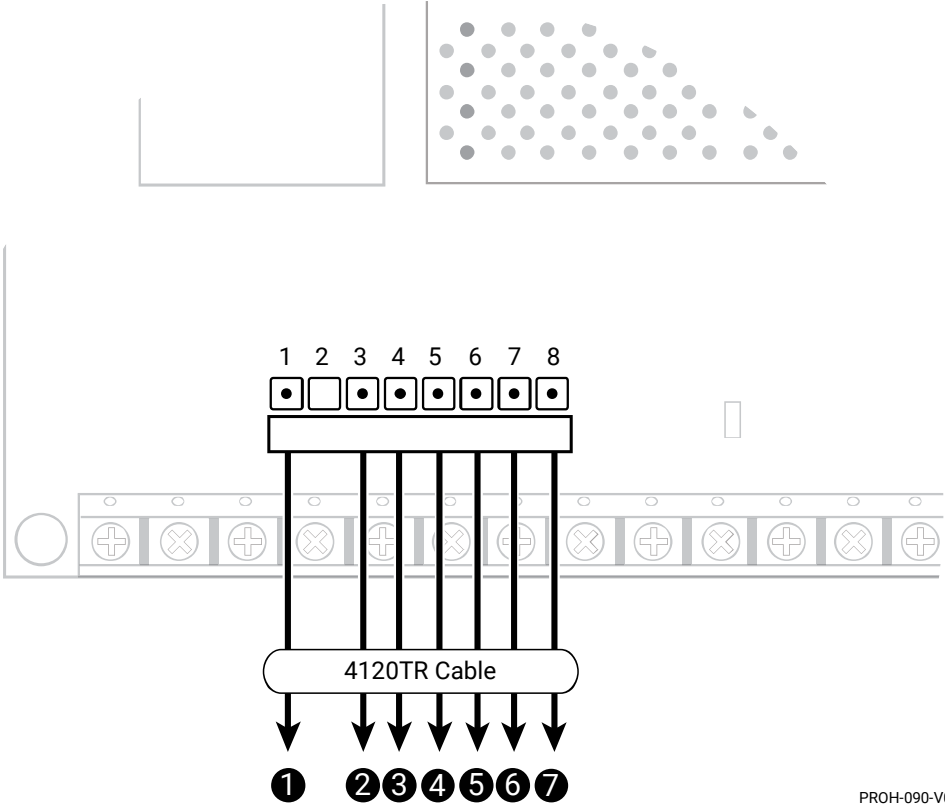
Triggers 1 & 2 Outputs

The control panel automatically recognizes the Trigger 1 as zone 300 and Trigger 2 as 301. Trigger outputs are normally high, and go low upon programmed condition. Use harness 4120TR Trigger Cable, not supplied)
Program these triggers using *Automation Rules* as you would for any other relay output.

When using these outputs, note:

- pin 1 = Trigger 2 (Zone 301):
180 ohms to ground when closed (output low), open when off (output high, normal default); can support 12V relay module that draws less than 20mA
- pin 5 = Trigger 1 (Zone 300):
180 ohms to ground when closed (output low); open when off (output high, normal default); or can support 12V relay module that draws less than 20mA

Pin	Description
Control Panel	
1	Trigger 2
2	Not Used (Key)
3	12+ (Positive)
4	GND -
5	Trigger 1
6	Not Used
7	Not Used
8	Not Used
4120TR Trigger Cable	
1	Red (Trigger 2)
2	Orange (+)
3	Yellow (-)
4	Green (Trigger 1)
5	Blue (Not Used)
6	Purple (Not Used)
7	Black (Not Used)



PROH-090-VI

Mounting and Wiring the Control Panel (Continued)

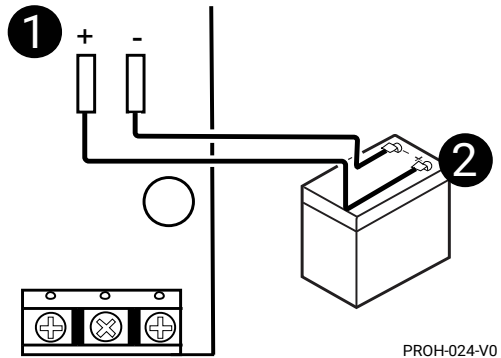
Backup Battery

1. Place the 12-volt backup battery in the cabinet.
2. Locate the battery connection spade connectors [1] above the DC power input and below the ethernet connector.
3. Connect the red and black flying leads from the Control Panel to the battery's positive and negative connection [2].

NOTE: The Control Panel features reverse polarity and short protection in case it is accidentally wired incorrectly.



IMPORTANT: The Control Panel will not power up on battery power only. There is no option to bypass this. Once powered up with the DC transformer, the battery will maintain power to the Control Panel if primary DC power is lost.



Battery Supervision

The Control Panel checks the battery connection to ensure the battery is connected every 2 minutes. If the battery is disconnected at the time of the 2-minute check, the keypad screen will display "System Battery Missing."

NOTES:

- It performs a 2-minute load test on the battery every 4 hours to ensure the battery can sustain a charge under a load.
- If the battery voltage falls below 11.5VDC during the test, then, the battery is unable to sustain a charge under a load and the Control Panel will initiate a Low Battery condition. At this point, the battery should be replaced.
- The 4-hour timer restarts when the panel is reset or when power is cycled.
- Entering Walk Test mode will NOT initiate any battery test.

Battery Saver

If the Control Panel loses primary power, it will shut down once the battery voltage falls below 10.2VDC, preventing the battery from being completely discharged. This will assist the Control Panel in recharging the battery when primary power is restored.

NOTES:

- The charging voltage to the battery is 13.65Vdc.
- The Green AC LED on the Control Panel will stay lit solid if primary power is present. If primary power is lost, this LED will turn off and the Red Battery LED will come on.

Mounting and Wiring the Control Panel (Continued)

Battery Calculations Worksheet

Table 1: iBus Power

iBUS Device Model	# of Units	Current (mA)		Total (mA)	
		Standby	Alarm	Standby	Alarm
VISTAHPKP		20	65		
VISTAHELAY		25	25		
VISTAHEXPHW		40	40		
iBUS Power Subtotal					

Table 2: Auxiliary Power Current Load

Device Model	# of Units	Current (mA)		Total (mA)	
		Standby	Alarm	Standby	Alarm
Auxiliary Power Subtotal					

Table 3: VISTA3/VISTA3CN Panel Current Load

Items	Current (mA)		Comments
	Standby	Alarm	
iBus Device Subtotal			Total iBus and Auxiliary Alarm power must be less than 1600mA
Auxiliary Power Subtotal			
Alarm Sounder	--		Alarm Sounder must be less than 2000mA (600mA for UL usage)
Panel (Include LTE Module)	70	360	
PROWIFIZW/PROWIFI Module	6	6	
VISTAHTKVRWL Module	25	25	
Total			

Table 4: Battery Capacity Calculation Worksheet

Capacity	Formula	Calculated Value
Standby Capacity	Total standby current X 4- or 24-hours X 1.2 contingency factor.	
Alarm Capacity	Total alarm current X 0.066 (4 min) 0.083 (5 min) or X 0.250 (15 min)	
Total Capacity	Add standby and alarm capacities	

Table 5: Battery Suggestion

Capacity	Recommended Battery	Comment
4AH	Yuasa NP4-12	
7AH	Yuasa NP7-12	
12AH	Yuasa NP12-12	Fits in large mercantile cabinet only.
14AH	Yuasa NP7-12	Connect two in parallel.
17.2AH	Yuasa NPG18-12	Fits in large mercantile cabinet only.

Mounting and Wiring the Control Panel (Continued)

Wiring the DC Transformer

Part Number	Description
R300-12131	14.3VDC transformer at 2.65A
R300-12131-CAN	14.3VDC transformer at 2.65A without secure tab (For Canada)

Connect the included transformer [1] to the DC+ [2] and GND [3] terminals on the Control Panel. Observe polarity since this is a 14.3VDC transformer. It features reverse polarity protection in case it is accidentally wired incorrectly and will not power up until polarity is correct. See Wire Run Chart below for wire size and distance.

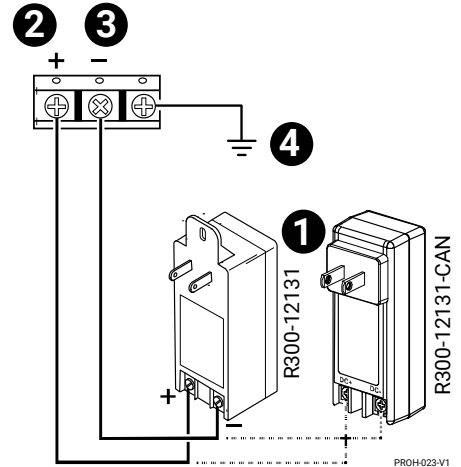
NOTES:

- If the DC voltage drops below 13VDC an "AC LOSS" message will be displayed and reported, if enabled.
- Do not connect the transformer to a receptacle that is controlled by a switch.
- The Green AC LED on the Control Panel will stay lit solid if primary power is present. If primary power is lost, this LED will turn off and the Red Battery LED will come on.



Use only the R300-12131 or R300-12131-CAN Power Supply. Do not plug the power supply into the AC outlet until after all wiring connections have been made.

Maximum Cable Length Between Control Panel and Transformer	Wire Gauge (AWG)
Up to 25ft (7.6m)	# 22
30 - 40ft (9.1 – 12.1m)	#20
50 - 60ft (15.2 – 18.2m)	#18
75 - 100ft (22.8 – 30.4m)	#16

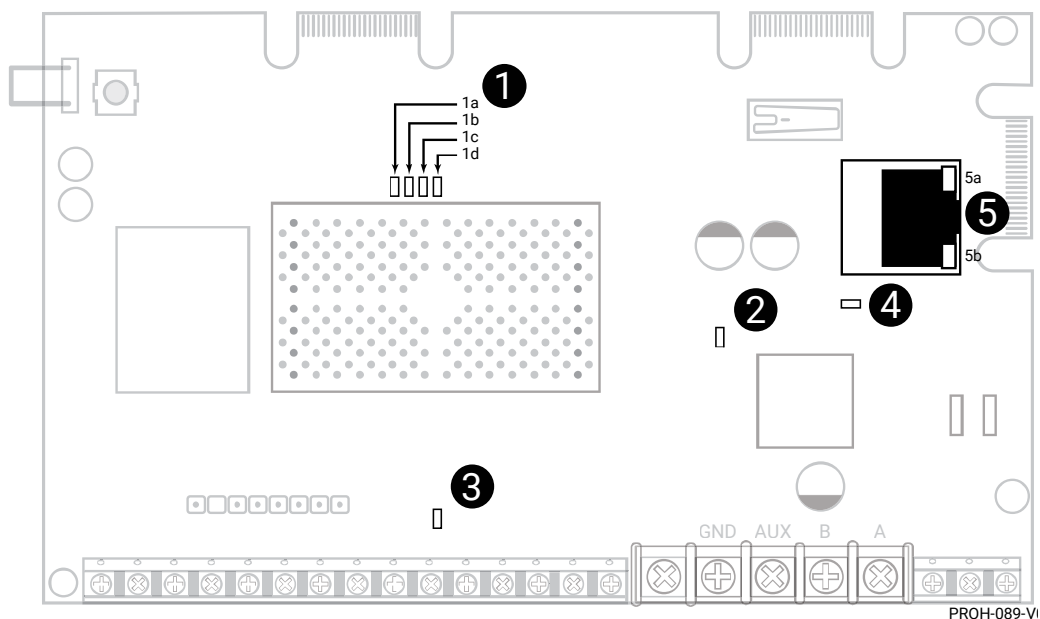


Earth Ground

If an earth ground connection is desired for additional protection in areas of severe electrical activity, the EGND terminal on the Control Panel [4] must be used as the ground connection point. To use a metal cold water pipe, use a non-corrosive metal strap (copper is recommended) firmly secured to the pipe to which the ground lead is electrically connected and secured. An AC Power Outlet Ground can also be used (available from 3-prong, 120VAC power outlets only).

Mounting and Wiring the Control Panel (Continued)

LED Behaviors



Number	Color	Description	ON	OFF	BLINKING
1a	Red	Auxiliary, Bell, & Open/Close	Armed	Not Armed	Program Mode
1b	Amber	Run LED: Used for Bluetooth (BLE) Pairing and Tablet Pairing Modes	Both BLE and Tablet pairing modes are active.	Neither BLE or Tablet pairing modes are enabled.	A. 200ms On/Off = Tablet pairing Mode. B. 200ms On/Off/On, then 1s off = BLE pairing Mode.
1c	Green	iBus	Ready to Arm	Armed, Not Ready to Arm	Program Mode
1d	Red	Not Used			
2	Yellow-Green	AC Power	AC Power Present	AC Power Lost	
3	Yellow-Green	Auxiliary Power Output	Aux Power On	Aux Power Off	
4	Red	Battery	AC Loss, Battery Power	System Powered by AC	
5a	Amber	Ethernet Link	Active Connection	No connection	
5b	Green	Ethernet Activity (RX/TX)		No communication	Data transferring

STEP 3 - Configure (Programming)

Configuring Wi-Fi using Bluetooth

Using the AN360 Application

1. Confirm Wi-Fi card is installed.
2. Apply power to the control panel.
3. From the Home Screen on your smart device, press the "Hamburger" icon located on the top left side.
4. Press "Connect a device to the internet".
5. In the Select Device menu, press on "Hybrid Panel" and then "Next".
6. Follow the on-screen instructions to active Bluetooth on your security panel. (Press the tamper or open the cover to active Bluetooth pairing for 30 minutes.)
7. Press "Get Started" and the app will begin searching for all security panels. The app will populate a list of available security panels that the installer can pair with. Select the correct MAC and press "Pair".
8. The app will ask the installer to enter the CRC of this panel. After typing the panel CRC, press "Pair Device".
9. This process may take a few moments but once connected to your panel, the app will display a list of available Wi-Fi networks. Select your desired network and press "Next".
10. Enter the password for the selected Wi-Fi network and press "Next".
11. The app will attempt to connect your panel to the chosen network. This process may take a few moments.

Local Alarm Mode Note: Removing, or not connecting, the ethernet connection activates the Wi-Fi interface. Allowing Wi-Fi network access.

Using the Total Connect 2.0 (TC2) Application

1. Confirm Wi-Fi card is installed.
2. Apply power to the control panel.
3. From the Home Screen, press on the "Hamburger" icon located on the top left side.
4. Press "Connect a device to the internet".
5. In the Select Device menu, press "Hybrid Panel" and then "Next".
6. Follow the on-screen instructions to active Bluetooth on your security panel. (Press the tamper or open the cover to active Bluetooth pairing for 30 minutes.)
7. Press "Get Started" and the app will begin searching for all security panels. App will show a list of available security panels that the installer can pair with. Select the correct MAC and press "Pair".
8. The app will ask the installer to enter the CRC of this panel. After typing the panel CRC, press "Pair Device".
9. This process may take a few moments, but once connected to your panel, the app will display a list of available Wi-Fi networks. Select your desired network and press "Next".
10. Enter the password for the selected Wi-Fi network and press "Next".
11. The app will attempt to connect your panel to the chosen network. This process may take a few moments.

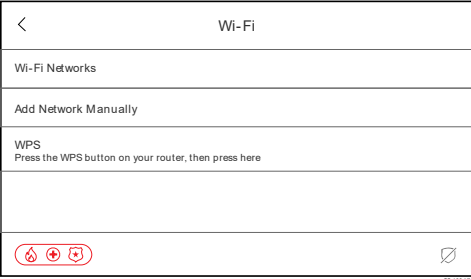
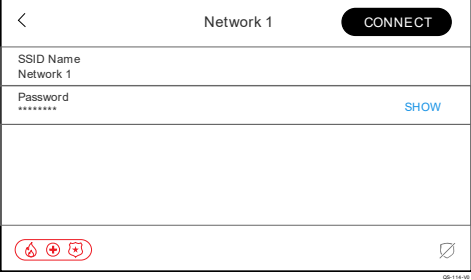
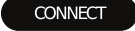
Configure Programming (Continued)

Wi-Fi Setup

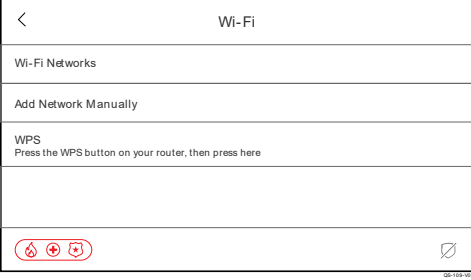
There are 3 different methods available to connect to the network. Select the best one for your application.

- “Wi-Fi Network” – Allows you to select your SSID (network name) from a list, then, type in your network password. This is the typical method.
- Add Network Manually – Best used when your SSID is not being broadcasted from your router. Enter both the SSID and password manually to connect.
- WPS (Wi-Fi Protected Setup) – Allows connection without knowing the network name or password. Your router must support this feature.

Selecting Wi-Fi Network

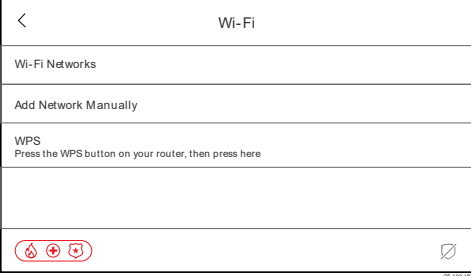
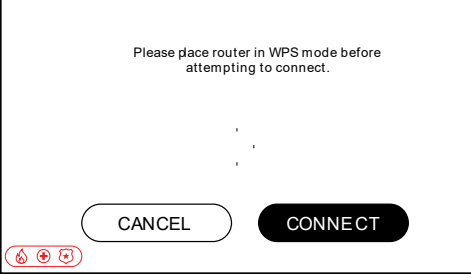
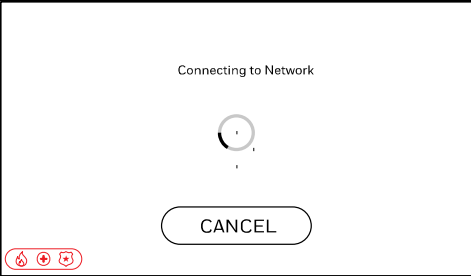
Touchscreen Display	Description
	1. Select . 2. Scroll down and select “Settings” . 3. From the right, select “Connectivity.” 4. Enter the Master or Partition Master code in the displayed keypad. 5. Select “Wi-Fi”. 6. Select “Wireless Touchscreen (this device)” or System. NOTE: Be cautious if your system is communicating via Wi-Fi. Best practice would be to alert your monitoring station and let them know you are testing the system to verify Wi-Fi communication is still functioning.
	7. The system scans all broadcasted networks. Select your network from the list provided. 8. Select “Password”. NOTE: Be sure to use a strong Wi-Fi password. Weak Wi-Fi passwords can allow an attacker to brute force into the network, which can lead to attempts to compromise the security panel. 9. Enter the password to your network in the displayed keyboard. 10. Select . 11. Verify all information has been entered correctly. 12. Select  and the system indicates connection status. 13. Once connected, it displays the connected network above the available networks. 14. Select  to go back in screens. NOTE: All entries are characters and case sensitive.

Add Network Manually

Touchscreen Display	Description
	1. Select “Add Network Manually”. 2. Select “SSID Name”. 3. Enter the SSID Name to your network in the displayed keyboard. 4. Select . 5. Select “Password”. 6. Enter the password to your network in the displayed keyboard. 7. Select . 8. Verify all information has been entered correctly. 9. Select  and the system indicates connection status.
	10. Once connected, it displays the connected network above the available networks. 11. Select  to go back in screens. NOTE: All entries are character and case sensitive.

Configure Programming (Continued)

WPS Setup

Touchscreen Display	Description
	1. Select "WPS".
	2. Activate WPS on your router. Refer to your router's instructions on how to do this. 3. Select CONNECT .
	4. The system displays connection status. NOTE: It may take a minute or two for the system to connect. If it does not connect typically within 2 or 3 minutes, depending on the router, the WPS session in the router stops and the process must be repeated or use a different connection method. If they do not connect, try bringing the Control Panel within a few feet of the router and see if they connect. Once connected, mount the Control Panel back in the desired location. 5. Once connected, it displays the connected network above the available networks. 6. Select < to go back in screens.

Wireless Access Point

The control panel can be used as a standalone wireless access point. This is useful for enrolling the VISTAHTCHWLC keypad without connecting to the home router. To use the control panel as an access point you need to access the control panel's "Add Wi-Fi Touchscreen" screen.

Configure Programming (Continued)

Enrolling a VISTAHTCHWLC keypad for Local Programming

To configure the VISTAHTCHWLC as a programming keypad, it must be enrolled using the integrated access point and the panel's Keypad Enrollment Mode. To enable the Keypad Enrollment Mode, perform the following steps.

1. Power up the Control Panel and the VISTAHTCHWLC keypad wait a minimum of one minute for the control panel to fully boot up.
2. On the main control panel, press and hold the control panel tamper for two (2) seconds and release for two (2) seconds. Perform this operation three (3) times. This forces the control panel into the local access point Keypad Enrollment Mode.

NOTE:

If there is a functioning keypad, the enrollment mode can also be enabled or disabled with the following commands:

Installer Code + 0 + 61	Enabled Keypad AP Enrollment Mode
Installer Code + 0 + 62	Disables Keypad AP Enrollment Mode
Installer Code + 0 + 63	Provides Keypad AP Enrollment Mode Status

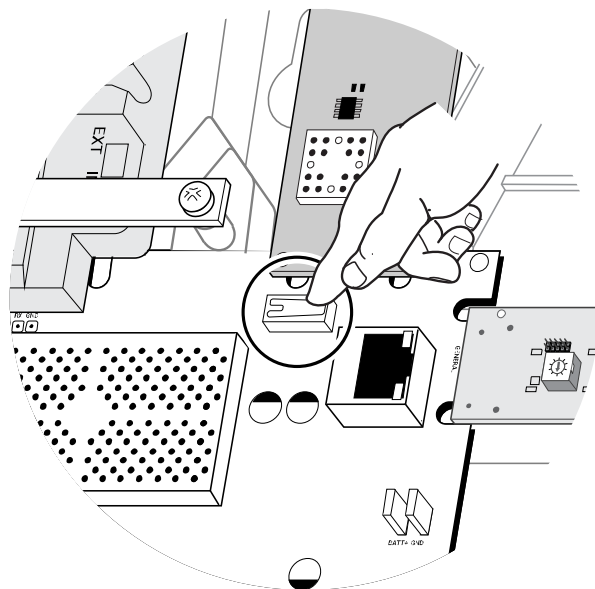
NOTE: When the panel is not registered to AN360 during first 15 minutes of bootup the panel will auto enroll all iBus keypads connected to control panel.

3. On the VISTAHTCHWLC, select "WPS Wi-Fi Pairing"

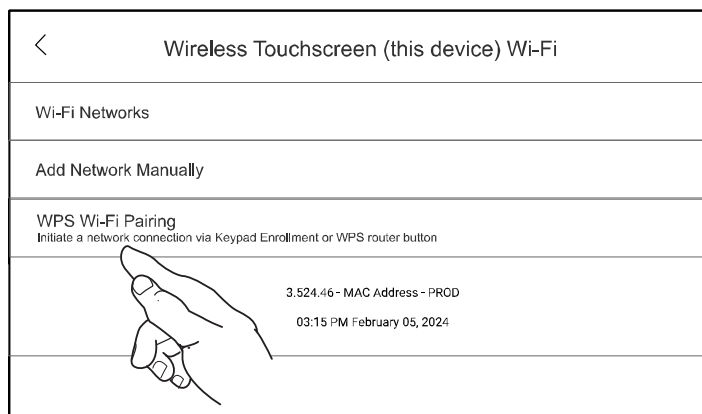
NOTE: Do NOT enter the customer's Wi-Fi information at this time.

IMPORTANT: If the screen does not display "WPS," or "Wi-Fi Pairing" mode then it has older firmware and will need to be updated prior to using the Touchscreen Enrollment Mode. AN360 does not allow Touchscreen Enrollment, so, to do so, you must connect the control and touchscreen to the same router (network) with internet access.

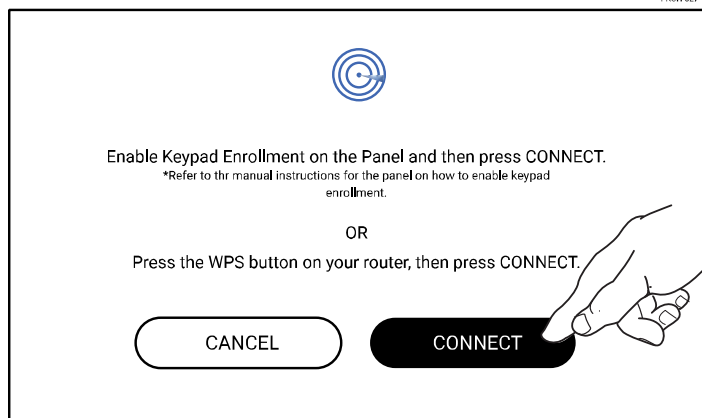
4. Press "Connect"



PROH-026-V0



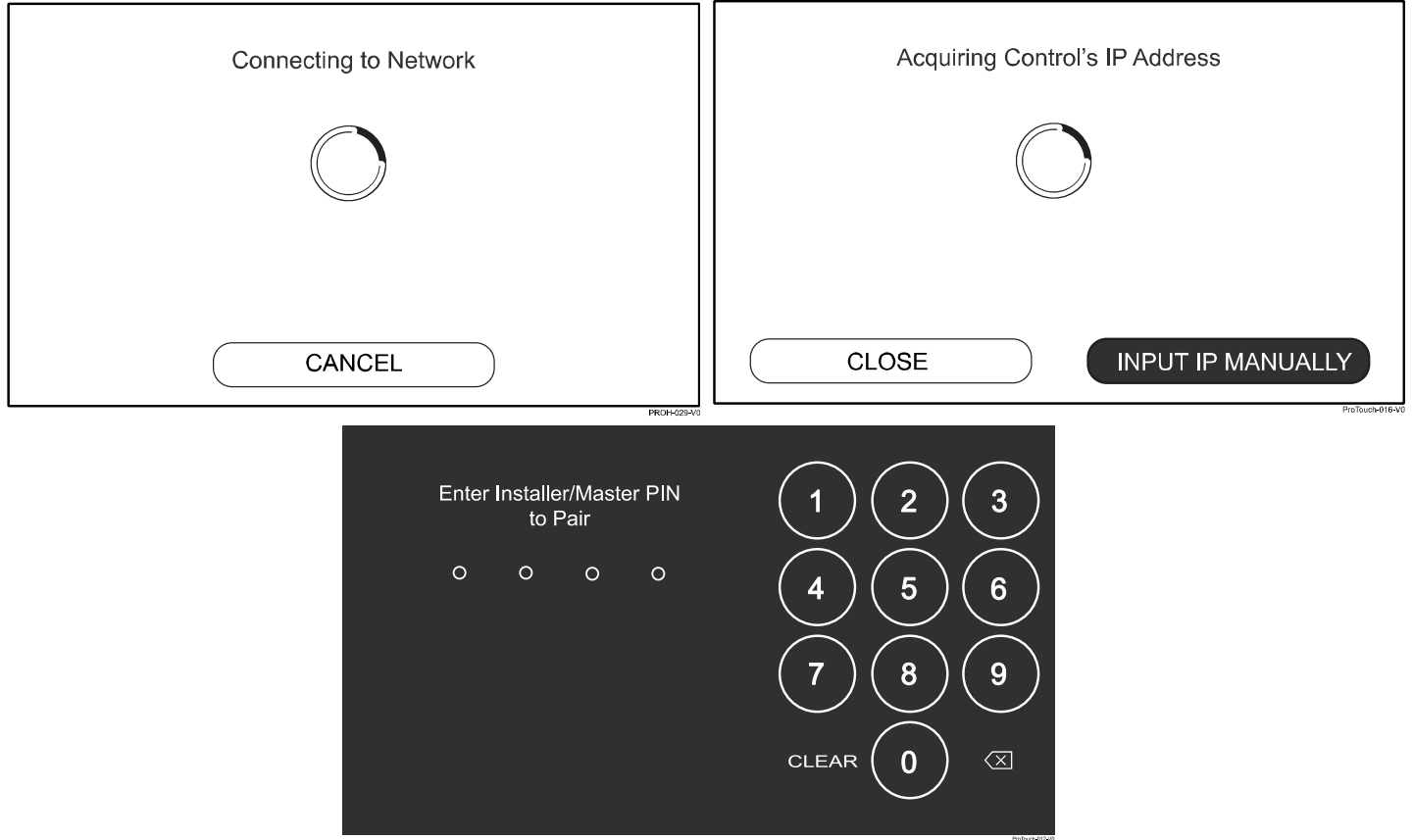
PROH-027-V0



PROH-028-V0

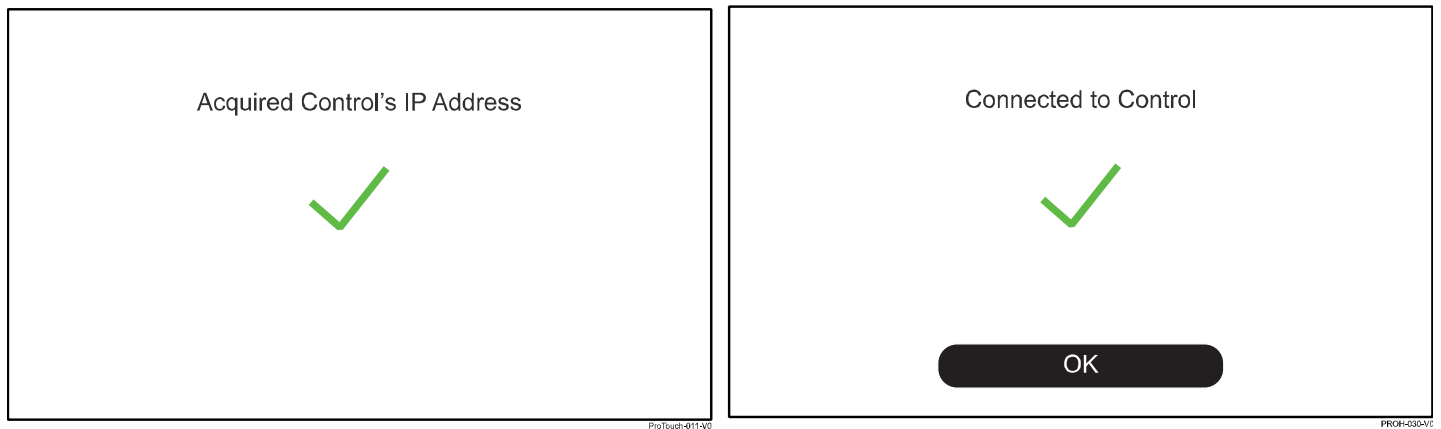
Configure Programming (Continued)

- Screen changes to "Connecting to Network" and when the VISTAHTCHWLC keypad acquires the control's IP Address, it prompts you to enter the installer code (default is 4112).



- Press "OK."

NOTE: A home screen appears once it confirms connection to the control panel.

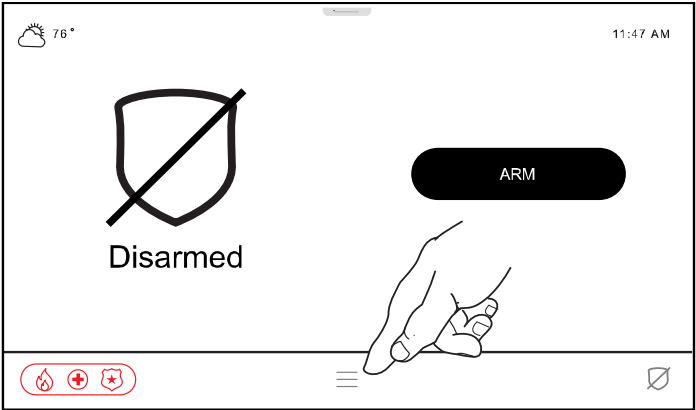


Configuring Programming (Continued)

Accessing Tools Menu

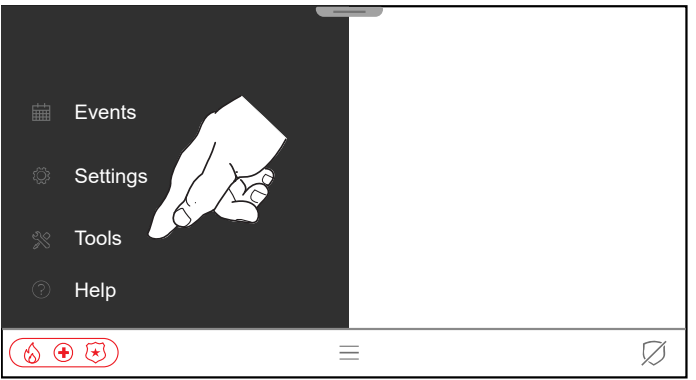
To access programming perform the following steps:

- 1. Press the Menu icon on the bottom center of the Home Page.

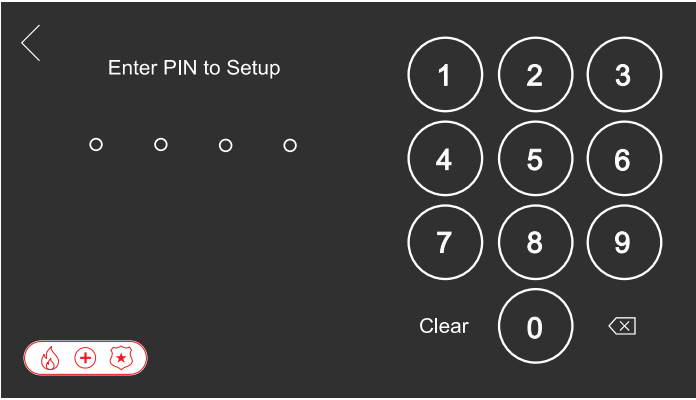


- 2. Scroll down and select the Tools option. From here you will find the following options:

Option	Description
System information	Access to firmware versions and ID numbers.
System Test	Communicator and Sensor Tests
Programming	General Panel Programming
Registration	Site initiated Registration for the AlarmNet Communicator(s)
Local Alarm Mode	Use without AlarmNet / Central Station Communication
Wi-Fi Touchscreen Enrollment	Secondary wireless Keypad Enrollment Mode setup
Installer Pin	Default is 4112
Default Option	Factory defaults control panel
Reboot System	Power cycles the system
Shutdown System	Shuts down the system (much like shutting down a PC) NOTE: AC power must be removed within 3 minutes, or the panel will reboot.



- 3.



- 3. Next enter the Installer Code to access the Tools menu.

<	Tools
System Information	
System Tests	>
Programming	>
Registration	
Local Alarm Mode	>
  	

<	Tools	>
Cellular		>
Wi-Fi Touchscreen Enrollment		
Installer PIN		
Default Options		
Reboot System		
  		

Configuring Programming (Continued)

System Information Screen

This is useful for support purposes, and the General Tab gives you access to the Firmware Version. Whereas the Main Control gives you access to the Panel Identification numbers.

< System Information	
✓	General
✓	Main Control
  	
	

PROH-042-V0

System Tests

Used for performing System Tests. See *Step 4 – Confirm* for more information.

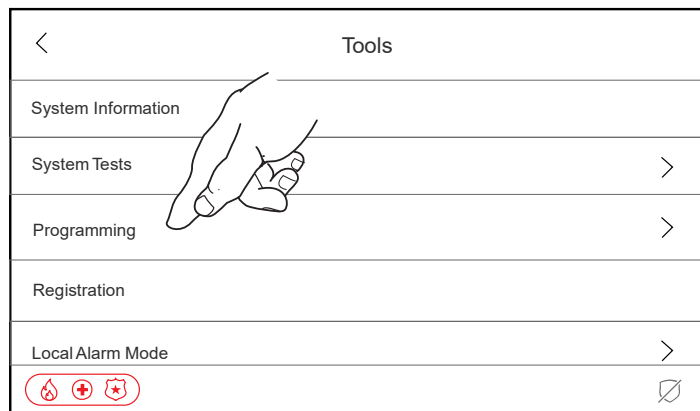
< System Tests	
Test Communicator	>
Test Sensors	
  	
	

PROH-045-V0

Configuring Programming (Continued)

Programming

1. Press Menu
2. Select Tools
3. Enter the Installer Code (4112)
4. Select Programming to access the programming.



5. Select the desired programming option:

Option	Description
Partitions	Enable Partitions
Peripherals	Program Zones, Keyfobs, and Keypads
iBus Devices	List discovered iBus Devices and presents their status
Z-Wave Peripherals	Z-Wave Management Screen
Users	User Programming Page
Advanced Settings	Communicator, System, and Reporter Setup
Panic Alarms	Enable/Disable Panics
Automation Rules	Relay/trigger/Z-Wave scene programming

Programming	
Partitions	1
Peripherals Sensors, Keyfobs, Keypads	27
iBus Devices	2
Z-Wave Peripherals	0
Users	2
Advanced Settings Communicator, System, Reporter	

Configure Programming (Continued)**Zone Response Type Matrix****PROSIX™ Series Devices****Burglary and Miscellaneous Devices**

Legend			PROSIXC2W								PROSIXCT								PROSIXMINICT				PROSIXGB	
X	= Available Programming Option		Door	Window	Motion Sensor	Glass Break	Flood	Temperature	Garage Door	Other	Door	Window	Temperature	Flood	Environmental	Medical	Police	Garage Door	Other	Door	Window	Garage Door	Other	Glass Break
✓	= Default																							
R	= Defaulted and Read Only (Non-Changeable)																							
Response Type	Entry Exit 1		✓	X						X	✓	X							X	✓	X		X	
	Entry Exit 2		X	X						X	X	X							X	X	X		X	
	Perimeter		X	✓	X	✓				X	X	✓							X	X	✓		X	✓
	Day/Night			X	X					X		X							X		X		X	
	Interior Follower				✓	X				X									X			X		X
	Interior with Delay				X					X									X			X		
	24 Hour Auxiliary						X	X		X		X	X	X	X	X	X		X			X		
	24 Hour Audible									X							✓		X			X		
	24 Hour Silent									X								X	X			X		
	Monitor						✓	✓		X			✓	✓	✓				X			X		
	Not Used																		✓			✓		
	No Response									X						X	X		X			X		
	Silent Burglary		X	X	X					X	X	X	X						X	X	X	X	X	X
	Garage									✓	X								✓	X		✓	X	
	Garage Monitor									X	X								X	X		X	X	
	Trouble						X	X		X			X	X	X					X			X	
	24h Medical									X						✓				X			X	
	Local Alarm									X										X			X	
Awareness		X	X	X						X	X								X	X				
24-Hour Awareness		X	X	X						X	X								X	X				
SIX Services (# of Loops)			8 (8 Hardwired Inputs)								2 (1 = Reed, 2 = External)								1 (Reed)				1	
Programming Properties	Others	Supervised	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Alarm Report	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Arm Night			X																			
		Supervision Time	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
	Sensitivity	Max Sensitivity																						✓
		Medium Sensitivity																						X
		Low Sensitivity																						X
		Lowest Sensitivity																						X
	Chime	Disabled	X	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	R	R	✓	✓	X	✓	✓	✓
		Standard	✓	X	X	X	X	X	X	X	X	✓	X	X	X	X			X	X	✓	X	X	X
		Melody	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Melody Long	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Ascend	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Ascend Long	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Alert 1	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Alert 2	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Doorbell 1	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Doorbell 2	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
		Evolve	X	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X
	Sound Options	Continuous Trouble Beeps	X	X	X							X	X							X	X			
Alarm on Siren		X	X	X							X	X							X	X				
Chime		X	X	X							X	X							X	X				
None		✓	✓	✓							✓	✓							✓	✓				
Siren Selection	Partition Only	✓	✓	✓							✓	✓							✓	✓				
	Partition and Main	X	X	X							X	X							X	X				
	Main Partition Only	X	X	X							X	X							X	X				

NOTES

1. No Chime options available with Awareness/24-Hour Awareness response type is selected.
2. Sound and Siren selections options are only available for Awareness/24-Hour Awareness Response types.

Configuring Programming (Continued)

Burglary and Miscellaneous Devices (Continued)

Legend			PROSIXSHOCK										PROSIX PIR		PROSIX FLOOD		PROSIX TEMP		PROSIX PANIC	PROSIX MED
X	= Available Programming Option		Door	Window	Temperature	Flood	Environmental	Medical	Police	Garage Door	Shock Detector	Other	Motion Sensor	Other	Flood	Other	Temp	Other	Police	Medical
✓	= Default																			
R	= Defaulted and Read Only (Non-Changeable)																			
Response Type	Entry Exit 1	✓	X									X		X		X		X		
	Entry Exit 2	X	X									X		X		X		X		
	Perimeter	X	✓								✓	X	X	X		X		X		
	Day/Night		X								X	X	X	X		X		X		
	Interior Follower											X	✓	X		X		X		
	Interior with Delay											X	X	X		X		X		
	24 Hour Auxiliary			X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X
	24 Hour Audible							X	✓		X	X		X	X	X	X	✓		X
	24 Hour Silent								X			X		X	X	X	X	X	X	
	Monitor			✓	✓	✓						X	X	X	✓	X	✓	X		
	Not Used											✓	✓	✓		✓		✓		
	No Response							X	X			X	X	X	X	X	X	X	X	X
	Silent Burglary	X	X							X	X	X	X	X		X		X		
	Garage									✓		X	X	X		X		X		
	Garage Monitor									X		X	X	X		X		X		
	Trouble			X	X	X					X	X	X	X	X	X	X	X		
	24h Medical							✓				X	X	X		X		X		✓
	Local Alarm											X	X	X		X		X		
	Awareness	X	X										X			X				
	24-Hour Awareness	X	X										X							
SIX Services (# of Loops)			3 (1 = Reed, 2 = External, 3 = Shock)										1		1		2 (1=Low Temp, 2 = High Temp)		1	1
Programming Properties	Others	Supervised	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	X
		Alarm Report	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Arm Night (See note 3)			X								X							
		Chime																		
		Pet Immunity											✓	X						
	Sensitivity	Supervision Time	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
		Max Sensitivity									X	X								
		Medium Sensitivity									✓	✓								
		Low Sensitivity									X	X								
		Lowest Sensitivity									X	X								
	Chime	Disabled	X	✓	✓	✓	✓	R	R	✓	✓	✓	✓	✓	✓	✓	✓	✓	R	R
		Standard	✓	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Melody	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Melody Long	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Ascend	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Ascend Long	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Alert 1	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Alert 2	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Doorbell 1	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Doorbell 2	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
		Evolve	X	X	X	X	X			X	X	X	X	X	X	X	X	X		
	Sound Options	Continuous Trouble Beeps	X	X									X							
		Alarm on Siren	X	X									X							
		Chime	X	X									X							
		None	✓	✓									✓							
	Siren Selection	Partition Only	✓	✓									✓							
		Partition and Main	X	X									X							
		Main Partition Only	X	X									X							

NOTES

1. No Chime options available with Awareness/24-Hour Awareness response type is selected.
2. Sound and Siren selections options are only available for Awareness/24-Hour Awareness Response types.
3. Arm Night will be disabled/hidden when Awareness/24Hr Awareness response type is selected.

Configuring Programming (Continued)

Fire and Siren Devices

Legend			PROSIX COMBO			PROSIX SMOKE		PROSIX HEAT	PROSIX CO	PROSIX SIREN	PROSIX SIREN-OD
X	= Available Programming Option		Smoke Detector	Carbon Monoxide Detector	Heat Sensor	Smoke Detector	Heat Sensor	Heat Sensor	Carbon Monoxide Detector	Wireless Siren	Wireless Siren
✓	= Default										
R	= Defaulted and Read Only (Non-Changeable)										
	Perimeter										
	Day/Night									✓	✓
	Interior Follower										
	Interior with Delay										
	Fire No Verification		✓		✓	✓	✓				
	Fire Verification		X			X					
	Carbon Monoxide			✓				✓			
	Awareness										
24-Hour Awareness											
SIX Services (# of Loops)			3 (1=Smoke, 2=CO, 3=Heat)			2 (1=Smoke, 2=Heat)		1	1	1	1
Programming Properties	Others	Supervised	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Alarm Report	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Arm Night*									
		Chime (Yes/No)								✓	✓
		One Go/All Go	✓	✓	✓	✓	✓	✓	✓		
		Supervision Time (minutes) (Read Only)	R	R	R	R	R	R	R	R	R
	Sensitivity	Low									
		High									
	Capture Type	Video									
		Image									
	Chime	Disabled	R	R	R	R	R	R	R	R	R
	Sound Options	Continuous Trouble Beeps									
		Alarm on Siren									
		Chime									
		None									
Siren Selection	Partition Only										
	Partition and Main										
	Main Partition Only										

NOTES

* Arm Night will be disabled/Hidden when Perimeter and Awareness/24-Hour Awareness response types are selected.

Configuring Programming (Continued)

Zone Response Type Matrix (Continued)

5800 Series Devices

Legend																
X	= Available Programming Option															
✓	= Default															
R	= Defaulted and Read Only (Non-Changeable)															
		Door	Window	Motion Sensor	Glass Break	Smoke Detector	Heat Sensor	Carbon Monoxide Detector	Temperature	Flood	Environmental	Medical	Police	Garage Door	Other	
Response Type	Entry Exit 1	✓	X												X	
	Entry Exit 2	X	X												X	
	Perimeter	X	✓	X	✓										X	
	Day/Night		X	X											X	
	Interior Follower			✓	X										X	
	Interior with Delay			X											X	
	Fire No Verification					✓	✓									
	Fire Verification					X										
	Carbon Monoxide							✓								
	24 Hour Auxiliary								X	X	X	X	X		X	
	24 Hour Audible												✓		X	
	24 Hour Silent												X		X	
	Monitor								✓	✓	✓				✓	
	Not Used														X	
	No Response											X	X		X	
	Silent Burglary	X	X	X	X										X	
	Garage														✓	
	Garage Monitor														X	
	Trouble								X	X	X				X	
	24h Medical												✓		X	
	Local Alarm														X	
	Awareness	X	X	X												
	24-Hour Awareness	X	X	X												
	5800 Loop	1	✓	X	X	X	X	X	X	X	X	X	X	X	X	X
2		✓	X	X	X	X	X	X	X	X	X	X	X	X	X	
3		✓	X	X	X	X	X	X	X	X	X	X	X	X	X	
4 (Tamper)																
Programming Properties	Others	Supervised	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
		Alarm Report	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
		Arm Night			X											
		Chime														
		Pet Immunity														
		One Go/All Go														
	Chime	Supervision Time	R	R	R	R	R	R	R	R	R	R	R	R	R	R
		Disabled	X	✓	✓	✓	R	R	R	✓	✓	✓	R	R	✓	✓
		Standard	✓	X	X	X				X	X	X			X	X
		Melody	X	X	X	X				X	X	X			X	X
		Melody Long	X	X	X	X				X	X	X			X	X
		Ascend	X	X	X	X				X	X	X			X	X
		Ascend Long	X	X	X	X				X	X	X			X	X
		Alert 1	X	X	X	X				X	X	X			X	X
		Alert 2	X	X	X	X				X	X	X			X	X
		Doorbell 1	X	X	X	X				X	X	X			X	X
		Doorbell 2	X	X	X	X				X	X	X			X	X
		Evolve	X	X	X	X				X	X	X			X	X
	Sound Options	Continuous Trouble Beeps	X	X	X											
		Alarm on Siren	X	X	X											
		Chime with Voice	X	X	X											
		None	✓	✓	✓											
	Siren Selection	Partition Only	✓	✓	✓											
		Partition and Main	X	X	X											
Main Partition Only		X	X	X												
NOTES		1. No Chime options available with Awareness/24-Hour Awareness response type is selected. 2. Sound and Siren selections options are only available for Awareness/24-Hour Awareness Response types.														

Configuring Programming (Continued)

Zone Response Type Matrix (Continued)

Hardwired and iBus Zones

NOTE: Applies to both Onboard and iBus Wired Expansion (VISTAHEXPHW) Modules

Legend																
X	= Available Programming Option	Door	Window	Motion Sensor	Glass Break	Smoke Detector	Heat Sensor	Carbon Monoxide Detector	Temperature	Flood	Environmental	Medical	Police	Garage Door	Other	
✓	= Default															
R	= Defaulted and Read Only (Non-Changeable)															
Response Type	Entry Exit 1	✓	X												X	
	Entry Exit 2	X	X												X	
	Perimeter	X	✓	X	✓										X	
	Day/Night		X	X											X	
	Interior Follower			✓	X										X	
	Interior with Delay			X											X	
	Fire No Verification					✓	✓									
	Fire Verification					X										
	Carbon Monoxide							✓								
	24 Hour Auxiliary								X	X	X	X	X		X	
	24 Hour Audible												✓		X	
	24 Hour Silent												X		X	
	Monitor							✓	✓	✓					X	
	Not Used														✓	
	No Response											X	X		X	
	Silent Burglary	X	X	X	X										X	
	Garage													✓	X	
	Garage Monitor														X	
	Trouble								X	X	X				X	
	24h Medical											✓			X	
	Local Alarm														X	
	Awareness	X	X	X												
	24-Hour Awareness	X	X	X												
		Alarm Report	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Arm Night			X											
		Chime														
	Chime	Disabled	X	✓	✓	✓	R	R	R	✓	✓	✓	R	R	✓	✓
		Standard	✓	X	X	X				X	X	X			X	X
		Melody	X	X	X	X				X	X	X			X	X
		Melody Long	X	X	X	X				X	X	X			X	X
		Ascend	X	X	X	X				X	X	X			X	X
		Ascend Long	X	X	X	X				X	X	X			X	X
		Alert 1	X	X	X	X				X	X	X			X	X
		Alert 2	X	X	X	X				X	X	X			X	X
		Doorbell 1	X	X	X	X				X	X	X			X	X
		Doorbell 2	X	X	X	X				X	X	X			X	X
	Evolve	X	X	X	X				X	X	X			X	X	

NOTES

1. No Chime options available with Awareness/24-Hour Awareness response type is selected.

Configuring Programming (Continued)

Zone Response Type Definitions

During programming, you must assign a zone type to each zone, which defines the way the system responds to each zone in both the armed and disarmed states. Zone types are defined below.

Type	Function	Characteristics
Not Used	Used to program a zone that is not used.	None
Door/Window Delay 1 (Entry/Exit 1)	Assigned to sensors or contacts on primary entry and exit doors.	- Entry delay #1 timing is programmable. - Exit delay is independently programmable. - Exit and entry delays when armed in Away, Stay or Night Stay mode. - No entry delay when armed in Stay, Away, or Night Instant modes. - Exit delay begins regardless of the arming mode selected.
Door/Window Delay 2 (Entry/Exit 2)	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 timing is programmable. - Exit delay is independently programmable. - Instant alarm when armed in the Stay/Night Instant or Away Instant mode. - Exit delay begins regardless of the arming mode selected.
Instant Perimeter (Perimeter)	Assigned to glass break sensors or contacts on exterior doors and windows	Instant alarm when armed in any mode and during entry/exit delays.
Interior Stay/Away (Interior Follower)	Assigned to motion detectors covering an area (i.e.: foyer, lobby, or hallway) that must be passed during entry/exit delays 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 gains access through an unprotected area.	- Follows entry/exit delays when the delays are active. - Instant alarm when armed in Away or Away Instant mode. - Bypassed automatically when armed in Stay, Night Stay or Night/Stay Instant mode.
Motion Away Standard Delay (Interior with Delay)	Assigned to motion detectors covering an area that includes an unprotected entry/exit door. Provides entry delay (using the programmed entry time), if tripped when the system is armed in the Away mode.	- Initiates Door/Window Delay #1 (with programmed entry time) when armed in the Away mode. - Provides Entry and exit delays when armed in the Away mode. - Instant alarm when armed in the Away Instant mode. - Bypassed when the system is armed in the Stay or Stay Instant mode. - Exit delay regardless of the arming mode selected.
Night Zone	Assigned to motion detectors covering an area such as a basement or garage that should not be passed through during the night. Provides an instant alarm if the entry/exit zone is not violated first and protects an area in the event an intruder gains access through an unprotected area. Assigned to motion detectors that are active in Night Stay mode.	- Follows entry/exit delays when the delays are active. - Instant alarm when armed in Away, Away Instant, or Night Stay mode. - Bypassed automatically when armed in Stay or Stay Instant mode.
Night Zone with Delay	Assigned to motion detectors covering an area such as a basement or garage that should not be passed through during the night. Provides an entry delay and protects an area in the event an intruder gains access through an unprotected area. Assigned to motion detectors that are active in Night Stay mode.	- Initiates Door/Window Delay #1 (with programmed entry time) when armed in the Away and Night Stay modes. - Instant alarm when armed in the Away Instant mode. - Bypassed in the Stay and Stay instant modes. - Provides Entry and exit delays when armed in Night Stay mode.
Day Zone (Day/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, Stay, Night Stay, Stay/Night Instant, or Away Instant mode. - Provides a latched trouble sounding from the keypad and, if desired, a Central Station report when disarmed (day).
24-hour Medical	Assigned to a personal emergency button or keypad panic. This zone type is always active.	- Instant alarm, when in the armed or disarmed state (always active). - Keypad sounding only, no siren output.
24-hour Auxiliary	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 keypad. (There is no keypad timeout.)
Silent Burglary (Silent Burglary)	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, Stay, Stay Instant, Night Stay, or Away Instant mode. - Report sent to the Central Station.

Configuring Programming (Continued)

Zone Response Type Definitions (Continued)

Type	Function	Characteristics
24-hour CO (Carbon Monoxide)	Assigned to any wireless zone with a carbon monoxide detector. This zone type is always active and cannot be bypassed.	Siren output, keypads and detectors provide Temporal 4 Pulse when this zone type is alarmed on all partitions.
Trouble Beeps Only (24-Hour Trouble)	Used with various response type.	The system provides a trouble sound from the keypad (and a Central Station report, if desired).
24-Hour Fire (No Verification)	Assigned to any wireless zone used as a fire zone. This zone type is always active and cannot be bypassed.	Siren output, keypads and detectors provide Temporal 3 Pulse when this zone type is alarmed on all partitions.
24-Hour Fire w/ Verification (Fire with Verification)	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.	- Siren output, keypads and detectors provide Temporal 3 Pulse on all partitions 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 is provided, if that zone is still faulted. If there are no fire alarms after the 30 second delay expires, the system opens a 60 second window. If any fire zone is faulted during that window a fire alarm is immediately provided for that zone.
Non-Reporting Output (No Alarm Response)	Assigned when no-alarm response is required. Used for activating scenes or Total Connect notifications.	- No reports to the Central Station. - No keypad sounding or chime and no display on screen. - System can still be armed.
Monitor Zone (Monitor)	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/restores events are logged by the system. - No keypad sounding or chime. - System can still be armed.
24-Hour Audible	Usually assigned to a zone containing an Emergency button (audible emergency).	Sends a report to the Central Station and provides an alarm sound at the keypad. (There is no keypad timeout.)
24-hour Silent	Usually assigned to a zone containing an Emergency button (silent emergency).	- Sends a report to the Central Station. - No keypad sounding or display changes
Garage	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, Stay or Night Stay mode. - No Entry Delay when armed in Away or Stay Instant modes. - System can be armed with zone in the faulted state. When the zone is closed it will automatically 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 controller. - When zone is in the open state will display "FAULT." - Does not report alarms to Central Station. - Zone will chime if enabled. - System can be armed if this zone type is in fault.
Local Alarm	Usually assigned to a zone containing an emergency button (audible emergency).	- Follows sounder timeout. - Provides alarm sounds at the keypad. - No reports to the Central Station.
Awareness	Used to make the user "aware" of events triggered by the device only during the armed state.	- Can be used with: RF6 or 5800 devices configured with the Device Type: Door, Window, or Motion. - Reports events to the Control Panel during any armed state (Away or Home/Stay). - Does NOT report to the Central Station. - Can NOT be used with cross zoning.
24-Hour Awareness	Used to make the user "aware" of events triggered by the device during the armed or disarmed state.	- Can be used with: Hardwired Zone, PROINDMV, PROOUTMV, RF6 or 5800 devices configured with the Device Type: Door, Window, or Motion. - Reports events to the Control Panel in any state (armed or disarmed). - Does NOT report to the Central Station. - Can NOT be used with cross zoning.

Configuring Programming (Continued)

Zone Assignments

1 - 64	1-8 Wired, 9-64 Wireless/iBus	930	RF6 Jam
251 - 266	Virtual zones for AlarmNet 360	931	RF5800 Jam
300	Trigger 1	932	WiseLink Jam
301	Trigger 2	934	Battery Missing
302	VISTAHRELAY Module #1 Relay #1	935	Low Battery
303	VISTAHRELAY Module #1 Relay #2	936	AC Loss
304	VISTAHRELAY Module #1 Relay #3	950	Comm. Failed
305	VISTAHRELAY Module #1 Relay #4	951	Report Failed
306-364	VISTAHRELAY Modules 2-15	952	Unregistered
600-663	iBus Device Supervisory Zones	995	Fire Emergency panic
768-799	32 – 4-button keyfobs	996	Medical Emergency panic
800-815	16 – PROSIX + iBus keypads Combined	997	Reserved
889-892	4 – Audio Devices	998	Silent Alarm
895	Bell Supervision	999	Police Emergency panic
900	Cover Tamper	1000-1031	Bluetooth (BLE) Zones

Cross Zoning

Up to 16 pairs of 2 zones for cross zoning can be configured. Each pair has a selectable cross zone delay time from none to four-minutes. This delay is the amount of time within which both crossed zones must be activated while in the armed state before an alarm occurs. If only one zone of a cross zone pair is tripped during the delay time, a trouble code (CID E378 Cross Zone Trouble) will be sent and logged for that zone at the end of the delay along with a console Trouble beeping. Restore (CID R378) is sent at disarm.

The options for delay time are: None, 30 Seconds, 1 Minute, 90 Seconds, 2 Minutes, 3 Minutes, and 4 Minutes

NOTES:

- Only Perimeter, Interior follower, and Day/Night zones will be available to Cross Zone. Each zone in a pair must be in the same partition.
- Cross Zoning is only available through AlarmNet 360 programming, there is no option to configure cross zoning through local mode.

Configuring Programming (Continued)

Programming Fields

Registration, Programming and Testing are conducted through the AlarmNet 360 Programming Tool. Or, if enabled, there is an option to locally program the control. On a laptop, PC or Smart Device, go to: www.alarmnet360.com or use the AlarmNet360 app.

Configuring Partitions and their Options

Field Name	Programming Options	Information
Select "P1: MAIN" OR "+ADD" to enable up to three additional partitions.		
Partition Name	Main Partition Partition-02 (If enabled) Partition-03 (If enabled) Partition-04 (If enabled)	Programmable and each partition should be given a name.
Partition Number	1 2 (If enabled) 3 (If enabled) 4 (If enabled)	Not programmable
Entry Delay 1	None 15 Seconds 30 Seconds 45 Seconds 60 Seconds 90 Seconds 2 Minutes 3 Minutes 4 Minutes	The time period in which you must disarm the system before an alarm condition occurs after activating a zone with response type entry/exit 1 or interior with delay assigned to it.
Entry Delay 2	None 15 Seconds 30 Seconds 45 Seconds 60 Seconds 90 Seconds 2 Minutes 3 Minutes 4 Minutes	The time period in which you must disarm the system before an alarm condition occurs after activating a zone with response type entry/exit 2 assigned to it. NOTE: Must be equal to or greater than Entry Delay 1
Exit Delay	45 Seconds 60 Seconds 90 Seconds 120 Seconds	The time period in which you have to exit the premises after arming the system to any mode.
Arm Ding	All RF None RF KeyFob RF Keypad	Confirmation of Arm and Disarm ding is provided when 'Arm Ding' via RF Fob or RF keypad is enabled in programming. The arm ding occurs after the exit delay has expired and the disarm ding occurs immediately after disarming with a keyfob or RF keypad, and is longer than arming confirmation ding.
Quick Arm	Enabled Disabled	Quick Arm allows arming the system without entering a user code. Press the Away, Stay, or Night Shield to arm.
Quick Exit	Enabled Disabled	Quick Exit allows the user to press the Quick Exit button to restart the exit delay AFTER exit delay has expired only when the system is armed in HOME or NIGHT mode. This is to allow for someone to enter or exit without having to disarm the system. If Quick Exit is not enabled the Quick Exit button will not appear on the TouchScreen for the user.
Chime Mode	Enabled Disabled	This toggles the chime feature on or off for the selected partition. The "Chime" feature of the system is controlled by the end user with a toggle command (Settings->Chime). Whether or not a zone will chime is determined during initial programming or by the user in the "Sensors" section of the Tools Menu.

Configuring Programming (Continued)

Field Name	Programming Options	Information
Force Bypass	Enabled Disabled	When Force Bypass is enabled for a Partition in programming, the user is presented with the "BYPASS & ARM" button from the Home Screen when a zone is faulted. When pressed the panel will Bypass all Faulted zones and Arm when Arm Away, Home, or Night is pressed. When Force bypass is not enabled this option is not presented, instead faulted zones must be bypassed from the Sensors screen before the user will be presented with the Arm option.
Auto Stay Arming	Enabled Disabled	When the Partition is armed to Away and an entry/exit door was not violated within the programmed exit delay time, the Partition will automatically arm HOME at the end of Exit Delay. The panel will Auto Stay Arm when armed Away via: Main Panel or Keypad. The panel will NOT Auto Stay arm when armed Away via: Keyfob or Total Connect NOTE: If O/C reports are being sent, the system will report both Away and Stay. If the panel is armed Instant the Instant mode will remain once it changes to Auto Stay Arm. It will Arm in the Stay Instant mode.
Restart Exit Timer	Enabled	Not programmable (always enabled) 'Exit Delay Restart' allows the user to press the 'Restart Timer' key any time DURING the exit delay after arming NIGHT, HOME or AWAY. to restart the Exit time. This can be done once during Away arming exit delay, and unlimited times during Home or Night arming exit delay. NOTE: When armed Away, if an entry/exit door is tripped a second time before the exit delay time expires, the Exit delay time will always restart.
Silent Exit	Disabled	Not programmable (always disabled) The Audible Exit warning can be enabled from any Touchscreen with each Arming by pressing 'Silent Exit' before pressing Arm Away. This will prevent the panel and remote keypads from giving Exit warning sounds for the entire duration of Exit time on this attempt. NOTE: When 'Silent Exit' is selected, the panel will DOUBLE the exit delay time.
Display Exit Timer	Enabled	Not programmable (always enabled) The Display will show the countdown of exit delay time in seconds on the screen of the Main Console and/or all keypads in that Partition.
Power Up in previous	Enabled	Not programmable (always enabled) If the panel is powered completely down (AC and Backup Battery), it will return to its' previous state when power is restored.
Remote Trigger	Enabled	If enabled, it allows Total Connect users to manually control the relays from the "Devices" screen/ta while using the Total Connect 2.0 app or website.
Common Partition	Enable Disabled	Only selectable for partition three or four. Select to enable the Common Partition for partition three or four.

Configuring Programming (Continued)

Adding Wireless Sensors (PROSIX, 5800, or VISTAHTKVRWL)

	Field Name	Programming Options	Information
1.	Select "+"		Located in the upper right-hand corner of the window.
2.			An "Add Peripheral" screen is displayed. This prompts you to learn the MAC address of the sensor.
3.	Learn the MAC Address	LEARN the MAC Address OR enter the serial number	For PROSIX and PROSIXLCDKP activate the sensor or keypad as instructed in the sensor's or keypad's installation guide and watch the led flash rapidly, and within 20 seconds go solid for 3 seconds indicating success. For 5800 or Takeover manually enter the serial number by selecting "Add Manually".
4.	Partitions	Main Partition	Choose partition to assign the sensor.
5.	Zone Number	Enter Zone Number	Defaults to the first available zone.
6.	Service / Loop	1,2,3,4 (5800) Reed (PROSIX) External (PROSIX) 1 - 8 Contact (PROSIXC2W)	Each transmitter may support multiple services, such as PROSIXCOMBO, PROSIXSMOKE, PROSIXCT, PROSIXSHOCK, etc. Select the correct service/Loop for this zone. Select Add Service to use more services on the device.
7.	Zone Description 1	Enter Zone Description 1	Enter Zone Descriptor 1. Choose from the presented list for Spoken Words, or enter spoken custom words (must have Wi-Fi and internet connectivity or cellular coverage). NOTES: - Custom Voice Descriptors can be created and added via Local Programming or the AN360 Programming Tool. - The control panel uses a text-to-speech feature, once the custom word is created, it requires the control panel to download the information (after exiting programming). This may take several minutes. - If a custom descriptor is used, the control panel does not display or announce the Device Type. - If a user enters the Device Type in Descriptor 1 or 2, the control panel will not display or announce the device type.
8.	Zone Description 2	Enter Zone Description 2	Enter Zone Descriptor 2. (Refer to Zone Description 1 above for more information)
9.	Device Type	Refer to Device/Response Type Matrix	This populates based on the PROSIX transmitter type learned. Choose from the options presented, and corresponding Response type. The 'Device Type' chosen will be Spoken as the Third Zone Descriptor (unless Other is selected)
10.	Response Type	Refer to Device/Response Type Matrix	Select the Zone Response type from the list presented based on the Device Type selected
11.	Supervision	RF Supervised RF Unsupervised	
12.	Alarm Report	Enabled Disabled	Enables/Disables Alarm Report to be sent to Central Station
13.	Sensor Version	Not programmable	
14.	Chime	Disabled, Standard, Melody, Melody Long, Ascend, Ascend Long, Alert 1, Alert 2, Doorbell 1, Doorbell 2, Evolve	This option is not programmable for the following Device Types: Smoke Detector, Heat Sensor, Carbon Monoxide Detector, Medical, Fire, Other, Temperature, Police
15.	Supervision Time	720 Minutes	Defaulted to 720 minutes

Configuring Programming (Continued)

	Field Name	Programming Options	Information				
	Pet Immunity	Enabled Disabled	Only available for SIX Motion Sensors				
	Arm Night	Enabled Disabled	Only available for any sensor with a Device Type of Motion Sensor.				
	Sensitivity	Refer to the Information column for sensitivity settings.	Only Available for PROSIX Glass Break (PROSIXGB) and Shock Sensors (PROSIXSHOCK) <table><tr><th>PROSIXGB</th><th>PROSIXSHOCK</th></tr><tr><td> • Maximum • Medium • Low • Lowest </td><td> • Maximum • Medium • Low • Lowest </td></tr></table>	PROSIXGB	PROSIXSHOCK	• Maximum • Medium • Low • Lowest	• Maximum • Medium • Low • Lowest
	PROSIXGB	PROSIXSHOCK					
• Maximum • Medium • Low • Lowest	• Maximum • Medium • Low • Lowest						
NOTE: Refer to the Installation Instructions for each device to verify the appropriate settings for the application.							
	One Go / All Go	Enabled Disabled	Only available for PROSIX Smoke/Heat/CO Devices				

Configuring Programming (Continued)

Onboard Hardwired Zone Configuration

NOTES:

- Onboard zones 1-8 are preconfigured and cannot be deleted. See response and input type below to program out the zone.
- To enroll iBus zones, first the module must be enrolled. When the module is powered up, verify the LED is red and press the "+" icon in the upper right-hand corner of the screen. A confirmation tone/beep occurs verifying enrollment completed.

	Field Name	Programming Options	Information
1.	Peripheral Type	Onboard-Hardwire	Non-programmable. Information only.
2.	Input Type	EOLR, NC, NO, Zone Double, Double Balance	EOLR Requires End of Line Supervision Resistor NC Normally Closed Zone with no resistor (not supervised) NO Normally Open Zone with no resistor (not supervised) Zone Double See <i>Zone Doubling</i> section Double Balance See <i>Double Balance</i> section
3.	Partitions	Main Partition	Choose partition to assign the sensor.
4.	Response Time	10msec, 350msec , 700msec, and 1200msec	This is the response time for the zone to react, refer to the device being installed installation guide if it requires a faster or slower response. NOTE: Only applies to zones 2-8
5.	Zone Number	Enter Zone Number	Defaults to the first available zone.
6.	Zone Description 1	Enter Zone Description 1	Enter Zone Descriptor 1. Choose from the presented list for Spoken Words, or enter spoken custom words (must have Wi-Fi and internet connectivity or cellular coverage). NOTES: - Custom Voice Descriptors can be created and added via Local Programming or the AN360 Programming Tool. - The control panel uses a text-to-speech feature, once the custom word is created, it requires the control panel to download the information (after exiting programming). This may take several minutes. - If a custom descriptor is used, the control panel does not display or announce the Device Type. - If a user enters the Device Type in Descriptor 1 or 2, the control panel will not display or announce the device type.
7.	Zone Description 2	Enter Zone Description 2	Enter Zone Descriptor 2. (Refer to Zone Description 1 above for more information)
8.	Device Type	Refer to Device/Response Type Matrix	Choose from the options presented, and corresponding Response type. The 'Device Type' chosen will be Spoken as the Third Zone Descriptor (unless Other is selected) NOTE: Set as Other and Response Type below as Not Used to disable the zone.
9.	Response Type	Refer to Device/Response Type Matrix	Select the Zone Response type from the list presented based on the Device Type selected
10.	Alarm Report	Enabled Disabled	Enables/Disables Alarm Report to be sent to Central Station
11.	Chime	Disabled, Standard, Melody, Melody Long, Ascend, Ascend Long, Alert 1, Alert 2, Doorbell 1, Doorbell 2, Evolve	This option is not programmable for the following Device Types: Smoke Detector, Heat Sensor, Carbon Monoxide Detector, Medical, Fire, Other, Temperature, Police
12.	Resistance Value	2kΩ – Scanned	The Zone resistance value can be scanned to determine what the current value is.
	Arm Night	Enabled Disabled	Only available for any sensor with a Device Type of Motion Sensor

Configuring Programming (Continued)

Adding Keyfobs

	Field Name	Programming Options	Information
1.	Select "+"		Located in the upper right-hand corner of the window.
2.	Learn the MAC Address	Learn MAC Address	When prompted, press the top two keys on the keyfob simultaneously to start the enrollment process.
3.	Choose the No. Of Keys	1 Button Key 2 Button Key 4 Button Key 6 Button Key 8 Button Key	Select Keyfob Type
4.	Keyfob version	N/A	Displays the version of the keyfob
5.	Available Starting Zone	768	Control panel will select the first zone to assign the keyfob to.
6.	Partition *	Main Partition	Select the Partition for the Keyfob
7.	User Name	Select User	Select a User from the Programmed List
8.	Button 0* *Number is variable depending on the Keyfob selected	See "Information"	Program an action for each button to be used: • 24 Hour Silent • 24 Hour Audible • 24 Hour Auxiliary • Fire No Verification • Arm Stay • Arm Away • Disarm • No Response

Adding PROSIXLCDKP Keypads

	Field Name	Programming Options	Information
1.	Select "+"		Located in the upper right-hand corner of the window.
2.			
3.	Learn MAC Address	Keypad MAC Address	Press any button on the keypad to pair with the control panel
4.	Zone	800-831	
5.	Zone Description 1		Enter Zone Description (Refer to Zone Descriptors above in the "Adding Sensors" section).
6.	Zone Description 2		
7.	Keypad Version		Not programmable
8.	Partition	Main Partition	Select the Partition for the Keypad
9.	Supervision Interval	15 Min	Not programmable

Enabling/Disabling Panics

	Field Name	Programming Options	Information
1.	Select "Panic Alarms"		
2.	Select desired panic to enable/disable	Fire, Medical, Police, and Silent Alarm	Touch the toggle switch to disable the panic on the Keypads. NOTE: The panics are enabled by default.

Delete Zones and Peripherals

To delete zones and other peripherals access the Peripherals screen (Tools → enter 4-digit installer code → Programming → Peripherals). Scroll to the available zone or peripheral to be deleted, check the box and press Delete. The control panel will confirm that you want to delete the selected zone(s).

NOTE: Refer to the *Zone Assignments* Table to remove iBus devices (such as the VISTAHRELAY).

Peripherals		DELETE
Door Perimeter • P1: Main • Zone: 7		
Door Perimeter • P1: Main • Zone: 8		
Door Perimeter • P1: Main • Zone: 9	☒	
Door Perimeter • P1: Main • Zone: 10	☒	
Door Perimeter • P1: Main • Zone: 11	☐	
Door Perimeter • P1: Main • Zone: 12	☐	
Door Perimeter • P1: Main • Zone: 13	☐	

Configuring Programming (Continued)

Field Name	Programming Options	Information
COMMUNICATOR		
Old Alarm Time	10 Minutes 15 Minutes 30 Minutes 1 Hour 2 Hours 4 Hours 8 Hours 12 Hours 24 Hours	The old alarm time sets how long an undelivered alarm is retried for delivery to the Central Station. If the message is not validated, it is retried until the old alarm time is reached or the message is validated. Once Old Alarm Time has been exceeded, the radio will clear the message from its buffer and can notify the Control Panel via trouble notification.
Communication Path (internal Device)	WiFi Cellular Ethernet WiFi and Cellular Ethernet and Cellular	Choose the communication path, each communicator connected will automatically marry to the panel's MAC and CRC upon registration.
Wi-Fi Fault Time / Ethernet Fault Time	0-99 Minutes 60 Minutes	In the event the module detects a Wi-Fi communication path failure, enter the time delay (in minutes) before the module notifies the Control Panel with a trouble message. The Control Panel can then notify the Central Station over an alternate path.
Cellular Fault Time	0-99 Minutes 60 Minutes	In the event the module detects a Cellular communication path failure, enter the time delay (in minutes) before the module notifies the Control Panel with a trouble message. The Control Panel can then notify the Central Station over an alternate path.
Use DHCP	Enabled Disabled	Not programmable
SYSTEM		
Alarm Report Delay	No Delay 15 Seconds 30 Seconds 45 Seconds	The Control Panel can delay the Central Station communication when a Burglary Alarm occurs. The delay applies to ALARM only, and will not apply to Fire, CO, or 24 hr panic zone types.
Burglary Alarm Sound	Enabled Disabled	When enabled, an audible alarm, which includes any zone type that would activate an external sounder, automatically increases the volume of the panel's internal sounder to 85dB. When disabled, audible alarms will sound from the panel at a low db sound, used for testing purposes. NOTE: External Sounders are not disabled when "Burg Alarm Sound" is disable.
Time Zone Offset	(UTC-5:00 Eastern Time (US & Canada))	
Daylight Savings Time	Enabled Disabled	
Temperature Unit	Fahrenheit Celsius	Select display for Z-Wave Thermostat devices
User Language	English	Select English, Spanish, French, or Portuguese
Bluetooth Disarm	Enabled Disabled	Handsfree disarm - Supports up to 6 cell phones with Bluetooth. Each is assigned to a user to disarm a selected Partition based on proximity. Once the Entry delay begins, if the User's assigned Cell phone is marked as having left and returned, the Partition will Disarm and Log/Report the Disarm based on that User.
Require PIN to View Cameras	Enabled Disabled	Enables the use of a PIN to access the camera home page.

Configuring Programming (Continued)

Field Name	Programming Options	Information
Installer Language	English	Select English, Spanish, French, or Portuguese
Lack of Usage Notify	Disabled 7 Days 27 Days 90 Days 180 Days	When enabled the system notifies the Central Station if an end user does not operate (arm/disarm) any partition in the security system within a specified amount of time. The time is reset per arm/disarm event. If triggered, the system will send a System Inactivity report of E654. There is no local annunciation indicating that the report has been sent to the CS.
RF Jam Log	Disabled RF Jam Log RF Jam Log and Report	Detects a condition that may impede proper RF reception (i.e., jamming or other RF interference). RF jamming occurs when something in our frequency range (345MHz [5800] and 2.4Ghz [RF6]) has been transmitting for 20 seconds or longer. In any Armed/Disarmed state it causes the display to show a triangle with an exclamation point inside and the message RF Jam with a rapid trouble beeping that can be silenced with any key press. If trouble reporting is enabled a report to Central Monitoring Station (E344 RF Receiver Jam) will be sent. Once the trouble is cleared a Restore report will be sent (R344) if Trouble Restore reporting is enabled. The reported zones are 930 for SIX Wireless, 931 for 5800 Wireless and 932 for WiseLink Jam. NOTE: The panel can still be Armed if an RF Jam condition exists.
Burglary Bell Timeout	No 0-60 Minutes	Select the time for timeout of the Burglary Alarm Sounder.
Fire Bell Timeout	No 0-60 Minutes	Select the time for timeout of the Fire Alarm Sounder.
Number of Reports (Swinger Shutdown)	1-6 2	Limits the number of messages sent per zone to the Central Station during an armed period, and how many times the local sounder will sound per zone per armed period.
First Test Report Offset	6 Hours 12 Hours 18 Hours 24 Hours	Select the time for the first test report following power-up of the Control Panel.
Customer Type	Residential Commercial	This option changes the text for the Home arming to Stay arming for commercial applications.
Report Frequency	Never Every Day Every 7 Days Every 30 Days	Select the Report Frequency for the Periodic Test report.
Panel Sync Delay Time	0 - 120 Minutes 3 Minutes	Select to set a delay time for the panel to sync back with AlarmNet 360 when a change is made locally.
Lockout Duration	2 – 15 Minutes 15 Minutes	Select a time period for the user code lock-out option.

Configuring Programming (Continued)

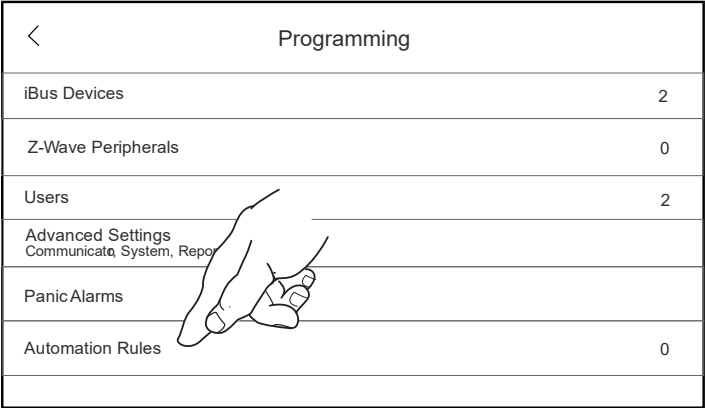
REPORT SELECTION		
Arm Away	Enabled Disabled	Panel can report Open-Disarm/Close-Arm by user. If enabled all users will report via any path enabled. Reports User 0-96 and keyfobs also report the user number associated with the fob. Remote Arms or Power up Armed reports as User 0. Panel will report Open even if Closing report is not enabled.
Arm Stay	Enabled Disabled	
Disarm	Enabled Disabled	
Exit Error	Enabled	Not programmable (Viewable only) If the system is armed and an entry/exit or interior zone is still open after the exit delay time has expired, an alarm will sound and the entry delay timer is started. If the system is disarmed before the end of the entry delay, the alarm sounding will stop and no message will be sent to the Central Station. The system status bar will display "ALARM CANCELED" as well as Alarm and the descriptor of the zone or zones that were left open. If the system is not disarmed before the end of the entry delay mentioned above, and an entry/exit or interior zone is still open, an E374 (Exit Error Alarm) message will be sent to the Central Station, along with the Alarm on faulted zone. The message "Alarm, Exit Error" will display in the system status bar and the alarm sounding will continue until the system is disarmed (or timeout occurs).
Alarm Restore	Enabled Disabled	If enabled, all alarm restores are sent to the Central Station.
Test	Enabled	Not programmable (Viewable only)
Test Restore	Enabled	Not programmable (Viewable only)
Low Battery	Enabled Disabled	If enabled, Low System battery report is sent to Central Station.
Low Battery Restore	Enabled Disabled	If enabled, Low System battery report restore is sent to Central Station.
RF Low Battery	Enabled Disabled	If enabled, RF Transmitter low battery report is sent to the Central Station.
RF Low Battery Restore	Enabled Disabled	If enabled, RF Transmitter low batter restore report is sent to the Central Station.
Recent Close	Enabled	Not programmable (Viewable only) If enabled, a Recent Closing is sent to the Central Station. A Recent Closing condition is similar to an Exit Error condition, but occurs if a Burg Alarm occurs on the panel within two minutes of the exit delay expiring. If a recent closing condition occurs, both recent closing E459 by user, and the alarm report are sent. This alerts the Central Station that the Alarm may be due to User error.
Event Log Full	Enabled Disabled	If enabled, and once the event log reaches its 10,000 event capacity it sends an event log full event to Central Station.
Trouble	Enabled Disabled	If enabled, reports Troubles to the Central Station.
Trouble Restore	Enabled Disabled	If enabled, reports Trouble restore to the Central Station.
Bypass	Enabled Disabled	If enabled, reports all zone bypasses to the Central Station.
Bypass Restore	Enabled Disabled	If enabled, reports all zone bypass restores to the Central Station.
AC Loss	Enabled Disabled	If enabled, AC Loss reports to the Central Station. NOTE: Randomized from 1-4 hours after AC Loss.
AC Loss Restore	Enabled Disabled	If enabled, AC Loss Restore reports are sent to the Central Station. NOTE: Randomized from 1-4 hours after AC is Restored.

Configuring Programming (Continued)

Automation Rules (Relays and Triggers)

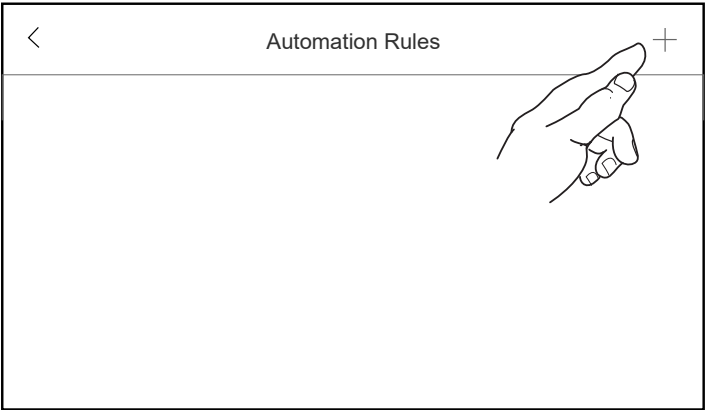
Use Automation Rules to program output function definitions (up to 100 functions) that provide automated control of any of the output devices (onboard triggers or relay modules), based on system events, events occurring on individual zones, or zones with certain zone types. Each output definition is identified by an Automation Rule Number, and includes a trigger and an action.

1. To access Automation Rules, scroll to the bottom of the programming section and select "Automation Rules"



2. Press the "+" sign in the upper right-hand corner to add a new rule.

NOTE: In AN360 this is called "Create Rule"



3. Fill out the appropriate information.

<	Edit Automation Rule	SAVE & ADD ANOTHER	SAVE
Name Automation Rule 1			
Trigger			
Trigger Type Zone Type			
Zone Type Entry Exit 1			
Partition			
Action			
Output Zone Number 300			
Output ZoneAction Closed			

PRCH-041-V0

Automation Rules (Continued)

			Field Name	Programming Options	Information																													
		1.	Name		Type in a name for the rule																													
Trigger	Zone Type	2.	Trigger Type	Zone Type Zone Number System Event	For Zone Type, go to step 3a and 4a. For Zone Number, go to step 3b and 4b. For System Event, go to step 3c and 4c.																													
		3a.	Zone Type	See Information for selectable options	Appears if "Zone Type" was selected: <table><tr><td>Entry Exit 1</td><td>24 Hour Silent</td><td>Monitor</td></tr><tr><td>Entry Exit 2</td><td>24 Hour Audible</td><td>Carbon Monoxide</td></tr><tr><td>Perimeter</td><td>24 Hour Auxiliary</td><td>Fire With Verification</td></tr><tr><td>Interior Follower</td><td>Fire</td><td>No Alarm Response</td></tr><tr><td>Trouble Day / Alarm Night</td><td>Interior Delay</td><td></td></tr></table>	Entry Exit 1	24 Hour Silent	Monitor	Entry Exit 2	24 Hour Audible	Carbon Monoxide	Perimeter	24 Hour Auxiliary	Fire With Verification	Interior Follower	Fire	No Alarm Response	Trouble Day / Alarm Night	Interior Delay															
		Entry Exit 1	24 Hour Silent	Monitor																														
		Entry Exit 2	24 Hour Audible	Carbon Monoxide																														
	Perimeter	24 Hour Auxiliary	Fire With Verification																															
	Interior Follower	Fire	No Alarm Response																															
	Trouble Day / Alarm Night	Interior Delay																																
	4a.	Partition	Any Partition or 1-4	Appears if "Zone Type" was selected and defines the partition in which the programmed zone type event is to cause the device action.																														
	Zone Number	3b.	Zone Number	1-64	Appears if "Zone Number" was selected. Auto populates the zones which have been programmed.																													
		4b.	Zone Number Event	Restore, Fault, Alarm, Trouble	Appears if "Zone Number" was selected.																													
System Event	3c.	System Event	See Information for selectable options	Appears if "System Event" was selected: <table><tr><td>Enter Walk Test</td><td>Disarm</td><td>AC Loss</td></tr><tr><td>Exit Walk Test</td><td>Silent Burglary</td><td>Low Battery</td></tr><tr><td>Arm Ding</td><td>Bell Time Out *</td><td>Comm. Fail</td></tr><tr><td>Start of Exit Delay</td><td>End of Exit Delay</td><td>Fire Zone Reset</td></tr><tr><td>Any Fault</td><td>Start of Entry Delay</td><td>Duress</td></tr><tr><td>Any Trouble</td><td>Any Burglar Alarm</td><td>Arm Night</td></tr><tr><td>Any Alarm</td><td>Chime</td><td>Audio Alarm Verification</td></tr><tr><td>Arm Stay</td><td>Any Fire Alarm</td><td>Siren Supervision Fail</td></tr><tr><td>Arm Away</td><td>Zone Bypassed</td><td>Any CO</td></tr><tr><td colspan="3">* or at Disarm, which ever happens first.</td></tr></table>	Enter Walk Test	Disarm	AC Loss	Exit Walk Test	Silent Burglary	Low Battery	Arm Ding	Bell Time Out *	Comm. Fail	Start of Exit Delay	End of Exit Delay	Fire Zone Reset	Any Fault	Start of Entry Delay	Duress	Any Trouble	Any Burglar Alarm	Arm Night	Any Alarm	Chime	Audio Alarm Verification	Arm Stay	Any Fire Alarm	Siren Supervision Fail	Arm Away	Zone Bypassed	Any CO	* or at Disarm, which ever happens first.		
	Enter Walk Test	Disarm	AC Loss																															
	Exit Walk Test	Silent Burglary	Low Battery																															
Arm Ding	Bell Time Out *	Comm. Fail																																
Start of Exit Delay	End of Exit Delay	Fire Zone Reset																																
Any Fault	Start of Entry Delay	Duress																																
Any Trouble	Any Burglar Alarm	Arm Night																																
Any Alarm	Chime	Audio Alarm Verification																																
Arm Stay	Any Fire Alarm	Siren Supervision Fail																																
Arm Away	Zone Bypassed	Any CO																																
* or at Disarm, which ever happens first.																																		
4c.	Partition	Any Partition or 1-4	Appears if "System Event" was selected and defines the partition in which the programmed system event is to cause the device action.																															
Action		5.	Output Zone Number	300-363	Assigns the Automation Rule just created to a specific Output Zone Number. This is the trigger or relay that will perform this rule upon the triggering event. Note that each defined Automation Rule is associated with only one output zone number. If more than one output device needs to perform this particular function, you need to define another Automation Rule with the same attributes, but assign the appropriate output zone number. To identify the available relays, visit "Peripherals" → scroll down to 300-363 zones. The relays are numbered as follows: <table><tr><th>Zn #</th><th>Description</th></tr><tr><td>300</td><td>Onboard Trigger 1</td></tr><tr><td>301</td><td>Onboard Trigger 2</td></tr><tr><td>302-363</td><td>VISTA4HRELAY Module # and Relay #</td></tr></table>	Zn #	Description	300	Onboard Trigger 1	301	Onboard Trigger 2	302-363	VISTA4HRELAY Module # and Relay #																					
		Zn #	Description																															
		300	Onboard Trigger 1																															
		301	Onboard Trigger 2																															
302-363	VISTA4HRELAY Module # and Relay #																																	
6.	Output Zone Action	Open, Close, Device closed for 2 seconds, 1 sec ON/OFF Toggle, Close/Open for Device Duration	Defines the action of the relay/trigger when the defined event occurs. Can Open, Close, Device close for 2 seconds, continuously pulse (1-second ON/OFF), toggle the device state, or Close or Open for a defined duration.																															
6a.	Device Duration	15-5400 seconds	Enter a value between 15 and 5400 seconds																															

Configuring Programming (Continued)

SIA Programming Default Values

Program Function	Programmed Default
PARTITIONS	
Partition Name	Main
Partition Number *	Partition 1
Entry Delay 1	30 Seconds
Entry Delay 2	30 Seconds
Exit Delay	60 Seconds
Arm Confirm (Arming Ding)	RF Keyfob
Quick Arm	Enabled
Quick Exit	Enabled
Chime Mode	Enabled
Force Bypass	Disabled
Auto Stay Arming	Enabled
Restart Exit Time	Enabled
Silent Exit*	Disabled
Display Exit Timer*	Enabled
Power-Up in Previous*	Enabled
Exit Warning*	Enabled
Remote Trigger	Enabled
COMMUNICATOR	
Old Alarm Time	10 Minutes
Communication Path (Internal Device)	Ethernet + Cellular
WiFi/Ethernet Fault Time	60 Minutes
Cellular Fault Time	60 Minutes
Use DHCP*	Enabled
SYSTEM	
Alarm Report Delay	30 Seconds
Burglary Alarm Sound	Enabled
Time Zone Offset	(UTC-05:00) Eastern Time (US & Canada)
Daylight Savings Time	Enabled
Temperature Unit	Fahrenheit
User Language	English
Bluetooth Disarm	Disabled
Require PIN to View Cameras	Enabled
Installer Language	English
Lack of Usage Notify	Disabled
RF Jam Log	Disabled
Burglary Bell Timeout	4 Minutes
Fire Bell Timeout	4 Minutes
Number of Reports (Swinger Shutdown)	2
First Report Offset	6 Hours
Customer Type	Residential
Report Frequency	Never
Panel Sync Delay Time	1 Minute
Lockout Duration	15 Minutes

Configuring Programming (Continued)

Program Function	Programmed Default
REPORTER	
Arm Away	Enabled
Arm Stay	Enabled
Disarm	Enabled
Exit Error*	Enabled
Alarm Restore	Enabled
Test	Enabled
Test Restore	Enabled
Low Battery	Enabled
Low Battery Restore	Enabled
RF Low Battery	Enabled
RF Low Battery Restore	Enabled
Recent Closing	Enabled
Event Log Full	Enabled
Trouble	Enabled
Trouble Restore	Enabled
Bypass	Enabled
Bypass Restore	Enabled
AC Loss	Enabled
AC Loss Restore	Enabled

* Not programmable

Registration

To access the Registration option, select the Menu  icon on the home screen, then select Tools → enter 4-digit installer code (default 4112) → scroll down to "Register".

The registration option is used to register the control panel with AlarmNet. If the panel is already registered, it will State the panel has already been registered. If it has not been registered, then the panel will attempt to register with AlarmNet through the selected communication path programmed earlier.

NOTE: All applicable IDs (PROWIFIZW, PROWIFI, and PROLTE Series Sims, MAC Addresses etc) are married to the control panels MAC address.

Local Alarm Mode

To access the Local Alarm Mode programming option, select the Menu  icon on the home screen, then select Tools → enter 4-digit installer code (default 4112) → scroll down to "Local Alarm Mode". Toggling this option on and off displays two messages:

Disabling

Disable Local Alarm Mode?

This will reboot the device and enable communicator setup.

CANCEL
YES, DISABLE

QS-176-V0

Enabling

Enable Local Alarm Mode?

This will disable communication with AlarmNet Services. Configuration will remain available. If an alarm event occurs, the local siren will sound but no alarm event will be reported.

If this device is registered to an account you must cancel the account to avoid future charges.

CANCEL
YES, ENABLE

QS-177-V0

NOTE:

Enabling "Local Alarm Mode" will:

- Remove all Cell setup/test options from view at the panel
- Disable the following features:
 - 'Communicator' and 'Reporter' sections in Installer Local Programming Mode
 - All Central Station Reporting of events
 - All connection with AN360 for remote programming, diagnostics, etc.
 - TC2 remote services

Configuring Programming (Continued)

Cellular

To access the Cellular Info option, select the Menu  icon on the home screen, then select Settings → enter 4-digit installer code (default 4112) → Connectivity → scroll down to "Cellular".

Used for support purposes to view the cellular information. If there are communication issues, you can test the signal strength (RSSI) here and determine if an antenna is required.

NOTE: Refer to the table below for ideal dB levels. If the dBm fall in the marginal or Bad column, it is recommended to add an antenna.

Good	OK	Marginal	Bad
-104dBm and higher	-105 to -114	-115 to -119	-120 and under

Cellular Info	
Model	LE910C1-SV
Carrier	Verizon USA
Registration Status	Registered Home
Signal Strength	-104 dB
SIM Status	Okay
Software Version	M0F.380009.2

Wi-Fi Touchscreen Enrollment

To access the Wi-Fi Touchscreen Enrollment screen, select the Menu  icon on the home screen, then select Tools → enter 4-digit installer code (default 4112) → scroll down to "Wi-Fi Touchscreen Enrollment".

The control panel can be used as a standalone wireless access point. This is useful for enrolling the VISTAHTCHWLC keypads without connecting to the home router. To use the control panel as an access point you need to access the control panel's "Add Wi-Fi Touchscreen" screen.

ADD Wi-Fi Touchscreen



You can enroll the Wi-Fi touchscreen through your home router or through the panel's built-in router. To use the panel's built-in router, use the SSID and password below or the WPS functions if available.

SSID: ProSeries_XXXXXXXXXX Password: XXXXXXXX

Installer PIN

The Installer PIN option allows you to change the installer PIN (code). The default code is 4112. It is often changed so installer-level access cannot be obtained once the installation is deployed to the customer.

Default Options

The default option sets the panel back to factory defaults.

NOTES:

- Defaulting the control panel removes all iBus devices, including keypads. You must re-enroll a VISTAHTCHWLC touchscreen keypad to perform local programming. See the *Enrolling the VISTAHTCHWLC Keypad for Programming* section for more information.
- If the control was defaulted, the panel will automatically reach out and download the latest version of the programming from AN360.

Reboot

The reboot option simply power cycles the control panel. Please note that, depending on the number of devices, it could take up to two-minutes to fully boot back up.

Shutdown System

Used to completely shut down the system.

- Verify the system is Disarmed.
- Access Menu → Tools → enter 4-digit installer code → Shutdown System.
- Select "OK."
- Wait 30 seconds for the panel to shut down.
- Unplug the power supply from the control panel.

NOTE: AC power must be removed within three minutes. Failure to do so results in the panel rebooting.

- Disconnect the battery.

Wireless Devices

Zones

All devices and zones are setup, programmed, and tested via AlarmNet 360. The Control Panel supports up to 64 total wireless zones; 64 of which can be PROSIX Series Wireless while any of them can be 5800 Series or another technology:

- PROSIX™ Series Wireless are both compatible with the VISTAH3/VISTAH3CN Control Panel.
- 5800™ Series Wireless technology requires the VISTAHTKVRWL Module. Communicates with wireless devices that transmit on the following frequencies 319.5MHz, 345MHz, 433.42 and 433.92MHz. Refer to the PROTAKEOVERH Compatibility chart for a list of compatible devices. Only one of these technologies can be used at one time.



IMPORTANT: Once paired, PROSIX Series transmitters cannot be used with another Control Panel until they are unpaired (deleted) from the current Control Panel. When being unpaired, the transmitters must be powered up and within range of the Control Panel, so the transmitters can receive the unpairing signal. Some PROSIX transmitters can be defaulted manually within 24hrs of being paired to the Control Panel. Check the installation instructions of specific transmitters for details.

Range

The range of any wireless device will ultimately depend on the building construction. The ranges specified below are typical for most installations.

- PROSIX Series Wireless has a nominal range of 300+ feet @ 2.4GHz. **NOTE:** PROSIXMINI's range is 200 feet.
- 5800 Series Wireless has a nominal range of 200 feet @ 345MHz.

Frequency Agility

Communications between the Control Panel and PROSIX Series transmitters are automatically monitored by the panel. When excessive environmental interference (i.e. from Wi-Fi routers) is detected on the 2.4GHz channel, the Control Panel will automatically switch to a quieter channel to allow clearer communication.

One-Go-All-Go

PROSIX Series transmitters are bi-directional, so they not only send signals to the Control Panel, but they also receive signals from the Control Panel. If enabled in programming, the Control Panel will send a signal to all smoke / CO devices, causing them all to sound when a fire or CO alarm is triggered. This also applies to PROSIX Series Keypads / Touchscreens and Sirens, which will all sound for burg alarms as well.

Smoke / CO Maintenance

The PROSIX Series smoke detectors and smoke / CO combo detectors can send Maintenance signals when they become too dirty to detect smoke or if they become too sensitive. End-of-Life (EOL) is also supported for CO detectors.

Transmitter Supervision

Each transmitter is supervised by a check-in signal that it sends to the Control Panel. If at least one check-in is not received from each supervised transmitter within a 4-hour period, the "missing" transmitter's zone number(s) and "Supervision" will be displayed and will initiate a trouble signal, no matter if the panel is armed or disarmed. The supervision for a transmitter can be disabled by programming it as "Unsupervised" so that it may be carried off the premises, such as a panic button. If set for Unsupervised, the Control Panel will ignore ONLY the supervision signals it receives from that transmitter but will still recognize all other signals, including Low Battery. Both PROSIX and 5800 Series transmitters have built-in tamper protection and will initiate a trouble condition if the Control Panel is disarmed and an alarm if it is armed. Wireless keys are not supervised.

- PROSIX Series Burg transmitters send a check-in signal every 60 minutes with a 4-hour panel check.
- PROSIX Series Life Safety transmitters send a check-in signal every 60 seconds with a 200-second panel check. These include smoke / CO detectors, sirens, and keypads.
- 5800 Series transmitters send check-in signal every 70-90 minutes with a 4-hour panel check.
- A power cycle of the Control Panel or a "System Reboot" via touchscreen will restart the 4-hour timer.
- In Canada, the RF supervision period is 3 hours for both Burg and Fire devices.

Wireless Devices (Continued)

Transmitter Battery Life

Batteries in the wireless transmitters may last from 4–10 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 any installation. The wireless system can identify a true low battery condition, thus allowing the dealer or end user time to arrange a change of battery and maintain protection for that point. Batteries should be replaced within 2 weeks of going into a low battery condition.



IMPORTANT: PROSIX and 5800 Series transmitters draw quick bursts of current during transmission, then sit idle with very nominal current draw. Most batteries are not designed for this type of use, therefore, only batteries listed as compatible should be used to attain the expected battery life. Each transmitter's Installation Instructions lists compatible battery manufacturers and their part numbers. When other non-approved batteries are used, the quick bursts of current draw kill the battery cells prematurely causing them to go low in a matter of months and can also cause unpredictable results. Other low-quality batteries have not been UL tested and pose a safety hazard if used.

Testing Signal Strength

This system does not have a specific test mode for checking wireless signal strength, however, the battery status and signal strength for PROSIX Series transmitters are displayed in AlarmNet 360.

Important Security Notice

Please inform the user about the security importance of their wireless keyfob and what to do if it is lost. Explain that the wireless key is similar to their key 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 fob. The Dealer/Installer will then remove the wireless key fob programming from the system.

Keypad / Touchscreen Setup

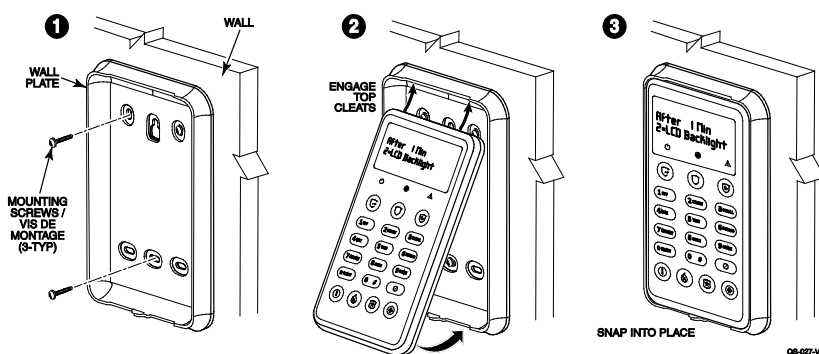
All keypads and touchscreens, wireless and hardwired, must be paired with the Control Panel. After putting the system into Keypad Enrollment Mode, power up each device or initiate the pairing sequence individually to get it paired with the system. They will not power up on battery only; they must be powered up with their supplied transformer.

PROSIXLCDKP Wireless Alpha Keypad

The PROSIXLCDKP wireless alpha keypad will attempt to pair automatically upon power up. If it is not paired during power up, any button can be pressed or power cycle the unit to restart the pairing process. It can be either wall or desk mounted. Desk mounting requires the optional PROSIXLCDDM kit. For additional information refer to the PROSIXLCDKP Installation and Setup Guide (p/n 800-25152 or later).

The keypad can be either wall or desk mounted using the optional PROSIXLCDDM kit. For additional information refer to the Installation and Setup Guide (p/n R800-25933).

When wiring the wall mount, use 14-gauge wire between the transformer and mounting plate. For proper wiring instructions, refer to the Installation and Setup Guide (p/n 800-25152).



Maximum Cable Length Between Keypad and Power Supply	Wire Gauge (AWG)
Up to 19ft (5.85m)	#22
Up to 30ft (9m)	#20
Up to 51ft (15.5m)	#18
Up to 75ft (23m)	#16



The keypad is powered by a 9Vdc, 1A plug-in adapter, P/N 300-07332US or 300-07332-CAN (Canada). Use the chart above to determine how long the wire run can be and at what gauge for the 300-07332US.

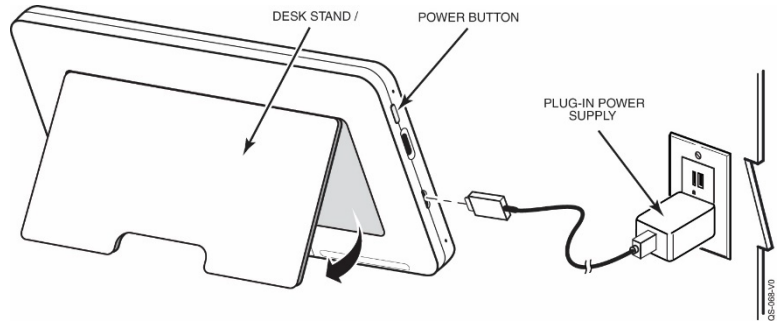
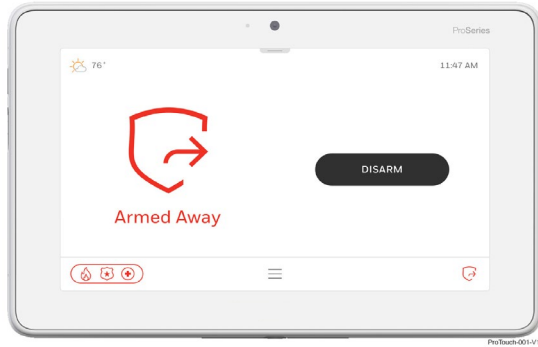


IMPORTANT: The wireless keypads use PROSIX technology, so once they are paired to the Control Panel, they cannot be used with another Control Panel until it is unpaired (deleted) from the current Control Panel. When being unpaired, the keypads must be powered up and within range of the Control Panel, so they can receive the unpairing signal.

Wireless Devices (Continued)

VISTAHTCHWLC Wireless Touchscreen

The VISTAHTCHWLC Touchscreen communicates to the Control Panel via the PROWIFIZW Wi-Fi module and does not require a network router. After powering up the VISTAHTCHWLC Touchscreen, it will display "Starting Up, Please Standby" and then enters Pairing Mode. Once the Control Panel is in "Keypad Enrollment Mode" touch "Pair" on the touchscreen and it automatically attempts to pair with the Control Panel. If it is not paired during power up, it will continue to display "Starting Up Please Standby" with a button labelled "Pairing Menu". Select "Pairing Menu", then select "Pair". Once paired, it will display its home screen with status of the Control Panel. It can be either wall mounted with the docking station or desk mounted with either the built-in desk stand or separate optional desk mount. The built-in desk stand option will angle the touchscreen at approx. 30°.



For best performance, the touchscreen should be powered by the supplied micro USB cable and the 5Vdc, 1.5A plug-in transformer to charge the Lithium Ion Polymer battery. The battery may not charge properly if it's plugged into any other USB port.

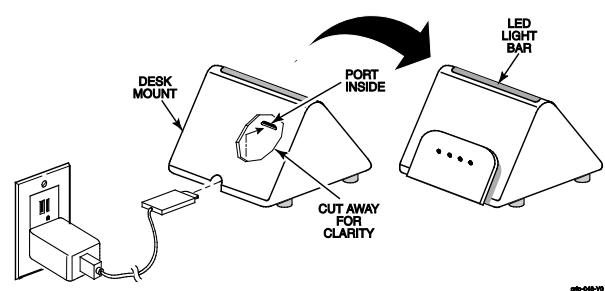
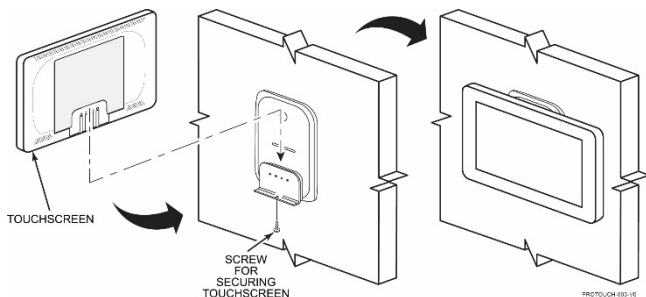
Wall / Desk Mounting (Optional)

The Touchscreen can be either wall or desk mounted using the optional PROWLTOUCHDM kit. For additional information refer to the Installation and Setup Guide (p/n R800-25845).

When wiring the wall mount, use 14-gauge wire between the transformer and mounting plate. For proper wiring instructions, refer to the Installation and Setup Guide (p/n R800-25845 or later).

The optional PROWLTOUCHDM desk mount kit requires the transformer and micro USB cable that was supplied with the Touchscreen for power. When the Touchscreen is installed on the desk mount, the LED Light Bar will light; indicating the unit charging.

NOTE: The Touchscreen must be completely seated to ensure it is connected and charging.



Step 4 – Confirm (System Operation and Testing)

Keypad / Touchscreen Displays and Operation

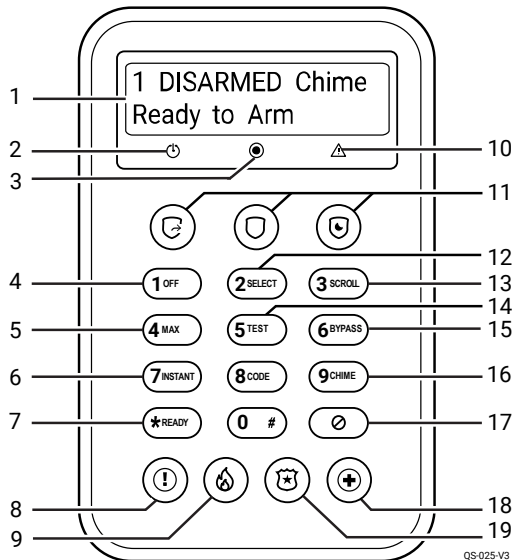
The keypads and touchscreens, in addition to controlling the system, display zone and system conditions (alarm, trouble, bypass), the built-in annunciator chimes when the appropriate zone is open and provides three programmable panic keys/icons for Fire, Police, and Medical alarms. These keys can notify the Central Station of an alarm condition if that service is connected.

During ...	Functions
Disarmed State	Arm/Disarm and perform other system functions, such as bypassing zones, clearing troubles, etc.
Alarm state	Console and external sounder (if installed) sound, and the keypad display the zone(s) in alarm state. Pressing any key will silence the keypad sounder for 10 seconds, but only once. Disarming the system will silence all sounds (bell output and keypads). Once disarmed, any zones that were in an alarm condition will be displayed (Alarm Memory). To clear alarm memory, simply repeat the disarm sequence.

PROSIXLCDKP Wireless Alpha Keypad Displays and Operation

The PROSIXLCDKP Wireless Alpha Keypad provides 2 lines with 16 characters per line allowing it to display programmed zone descriptors and full system status and messages, including the keypad's partition number indicated in the upper left corner.

Keypad Key Functions



KEY FUNCTIONS

1	2X16 Alpha LCD Display
2	Power LED
3	Status LED
4	Disarm Key
5	Arm Maximum (No Entry Delay)
6	Arm instant (No Entry Delay)
7	Scroll Status
8	Panic
9	Fire
10	Trouble LED
11	Quick Arm Keys (Away, Stay, & Arm)
12	Arm Away
13	Arm Stay
14	System Tests
15	Bypassing Sensors
16	Chime Mode
17	Not Used
18	Medical
19	Police

Keypad LED Meanings

LEDs	Off	Red	Green	Flashing Red	Yellow
 POWER			AC	Low Battery (no AC)	
 STATUS	Not Ready to Arm	Armed	Ready to Arm	Alarm / Alarm Memory	
 TROUBLE	Program mode				Device or System Trouble

System Operation (Continued)

Keypad Menu Mode

This mode displays keypad programmed information and provides access to Software Versions, Default, Partition and Keypad ID, Reset, and LCD Brightness. Access the menu mode by holding the **3** key for 2 seconds. Press **3** key to scroll or * key to exit. This mode will exit after 1 minute of no keypad activity. See below for settings and options.

Display	Meaning/Option
App: Boot:	Displays the keypad's current App and Boot versions
RF6:	Displays the keypad's SIX software version and the keypad MAC ID
Default Keypad	Prompts to Default Keypad. 1 = CONFIRM to remove keypad from Control Panel. NOTE: If the keypad is repowered within 24 hours, it will attempt to re-pair with the Control Panel. After 24 hours, it will need to be re-enrolled.
Partition= Keypad ID=	Displays Partition assignment and Keypad ID programmed in the Control Panel.
Reset Keypad	Prompts to Reset Keypad. 1=CONFIRM (restart)
LCD Brightness	Prompts to change LCD brightness. 2 will toggle from Low, Medium, and High
Backlight Adjust	Always Off, Always On, After 1 Min, After 5 Min, or After 15 Min
A: None	(Future Use)

Keypad Supervision

All keypads are supervised; however, wireless touchscreens are NOT supervised. If the system loses communications with a wireless keypad for 15 minutes, the system will latch into a trouble condition. If a touchscreen loses wireless connection to the Control Panel, it will display a black screen with "Please Standby". This message will clear and display status once it reconnects.

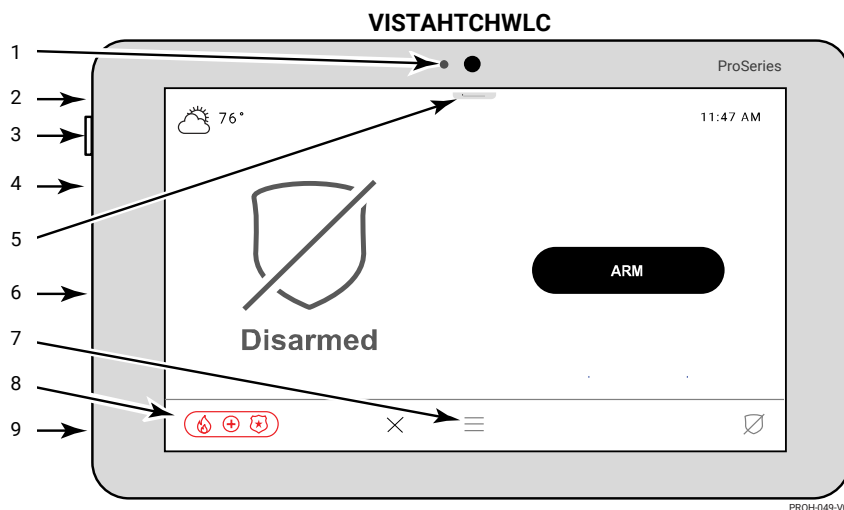
System Operation (Continued)

VISTAHTCHWLC Touchscreen Displays and Operation

System Status is displayed at the top of screen. In addition, the Home Screen displays the current date and time and selectable options are displayed on two pages. Select the ">" and "<" to navigate between the two home screen pages.

Navigating through the screens is accomplished by lightly touching the icons or menu items on the touchscreen. Once activated, it advances to the next screen. When the "Home" icon is selected, the system displays a keypad. By touching (selecting) an icon or key the touchscreen, depending on the function, advances to another screen, toggles between options or scrolls through multiple options that can be selected. The touchscreen provides a prompt when a specific input is required.

Number	Information
1	LED/Camera
2	Microphone
3	Power Button
4	Sd Card Port
5	Display & Audio Settings
6	Charge Port
7	Menu
8	Panic Keys
9	Microphone



Status LED	Meaning
Red - Steady	System Armed
Red - Flashing	Alarm or In Programming mode
Amber - Steady	System trouble
Amber - Flashing	Device trouble – System cannot be armed
Green - Steady	Ready to Arm
Green - Flashing	Device trouble - System can be armed
Off	Not ready to Arm

NOTE: The power button has 2 different functions:

- Press and Release will toggle the screen off and on
- Press and Hold to display the options of Power Off or Restart.

System Operation (Continued)

Partitioning

Up to 4 partitions can be used in the Control Panel which will allow different areas of the premises to work independently of each other; therefore, each can be armed and disarmed separately. Partition one is enabled by default, the other three partitions have to be enabled via AlarmNet 360 or local programming. Partition numbers display on the VISTAHPKP and PROSIXLCDKP keypad. The PROWLTOUCH touchscreen displays the partition name to indicate which partition is being viewed.

Common Partition

The Common Partition is programmable for partition 3 or 4 (programmable via AlarmNet 360 or local programming), otherwise, partition 3 or 4 can be a normal partition just like the first 2. The Common Partition is an area that is shared between 2 or 3 partitions, such as a hallway with offices on either side. The Common Partition will automatically arm once all the other partitions are armed. As soon as one of the other partitions is disarmed, the Common Partition will automatically disarm. The Common Partition cannot be armed otherwise, but it can be disarmed before any other partition is disarmed.

NOTES:

- When any independent partition is DISARMED, the Common Partition will automatically be DISARMED.
- When ALL independent partitions are ARMED, the Common Partition will automatically be ARMED.
- Common Partition can be Armed/Disarmed independently only if all other Partitions are Armed.
- All Users automatically show an Authority level in the Common Partition.
- 24-Hour zones assigned to the Common Partition will sound on all Partition Keypads, but can only be silenced from the Common Partition.
- Any faulted zone existing in the Common Partition will be automatically bypassed when the Common Partition arms.
- Can NOT be used with the Bluetooth disarm feature.

Goto Command

Allows users to access another partition from any keypad and operate that partition. Any security code that has been programmed into more than one partition can perform the Goto command by typing in the security code + * + single digit partition number 1, 2, 3, or 4. The user will be able to access only the partitions in which the security code is programmed. The keypad will timeout after 30 seconds of no keypad activity and automatically return to its home partition. Goto commands are not available on the touchscreens.



IMPORTANT: Fire and CO Alarms will display and sound on other partitions' keypads. The alarms can be silenced from each partition's keypad, but alarm memory can only be cleared from the partition's keypad / touchscreen from which the alarm occurred.

System Clock

The system clock is retrieved from AlarmNet 360 automatically once the system is communicating. The clock can be viewed only on the VISTAHTCHWLC touchscreens and cannot be changed. It is very important to make sure that it is correct, especially when using Schedules.

Scheduling

Scheduling is accomplished via Total Connect 2.0 and available to the user once a Z-Wave automation device has been enrolled into the system. Up to 100 scenes can be programmed with various options of controlling Z-Wave Automation and auto arm / disarm.

System Operation (Continued)

Audio Alarm Verification (AAV) (2-Way Voice)

If this feature is enabled, a hands-free voice session can take place after an alarm signal has been sent. The Central Station can initiate the voice session and talk to homeowner on site through any installed touchscreen without the homeowner needing to touch anything.

NOTES:

- AAV works on all partitions.
- An AAV session cannot be initiated for fire and CO alarms.
- All Touchscreens enrolled in the system can be used for Voice Stations.
- Only one Touchscreen at a time can be used as a station during an AAV session, starting with the lowest Touchscreen enrolled in the system. (All stations cannot be active simultaneously.)
- If the Control Panel loses primary AC power, it will power down the PROWIFIZW/PROWIFI module after a few minutes, resulting in loss of Wi-Fi communication to the touchscreens which will prevent AAV from working.

ATTENTION CENTRAL STATION OPERATOR:

Each session is automatically initiated in low-volume Listen mode. This means the operator can hear what is going on, on site, through all available touchscreen stations, but no one on site can hear the operator. Below is a list of commands that can be entered at any time during the session by the central station operator to control the voice session.

KEY	FUNCTION
1	Selects high-volume Talk Mode. Typically used with Key 3, Listen Mode, toggling back and forth.
2	Selects 2-Way Voice Mode allowing automatic switching between the site and the central station operator.
3	Selects Listen Mode. Typically used with Key 1, Talk Mode, toggling back and forth.
4	Selects next Touchscreen station in order from the lowest to the highest numbered Touchscreen stations.
7	Restarts the 5-minute voice session timeout. Sessions will automatically terminate after 5 minutes unless 7 (or any other command) is entered.
*8n	Selects touchscreen station number where "n" is the station number.
9	Terminates the voice session. If this is not entered, the communication line will stay connected for up to 5 minutes.

System Operation (Continued)

Security Codes

Up to 100 Security Codes (User Numbers) can be added, deleted, and partitioned to the Control Panel either through the keypads, touchscreens, AlarmNet 360, or Total Connect. There is only one Security Code defaulted in the system which is the Master Code, user number 02, and is defaulted to 1234. The Master Code can be used to enter additional 4-digit Security Codes via keypads and touchscreens while the system is in the Disarmed state. Security Codes cannot be added or changed while the partition is armed in any mode.

Programming Security Codes via 2x16 Keypads

Each of the commands listed below must be entered without any pauses, else the Control Panel will not see your command.

- The keypads will provide a single confirmation beep upon successful entry of each command.
- Security Codes cannot be duplicated.
- The user assumes access to the partition it is being programmed from. Use the Go To feature to switch between partitions.

The commands below will assume the Master Code is 1234. Be sure to use the current Master Code you have programmed in your Control Panel to perform the following commands.

Change System Master Code:	System Master Code + 8 + 002 + New Master Code TWICE or Installer Code + 8 + 002 + New Master Code
User 001 = Installer Code User 002 = Master Code	E.g. To change it from 1234 to 4321, type in 1234 8002 4321 4321
Add / Change Security Code:	System / Partition Master Code + 8 + User No. + New Security Code
	E.g. To add / change user 004 to 5678, type in 1234 8004 5678
Delete Security Code:	System / Partition Master Code + 8 + User No. + * + 0
	E.g. To delete user 05, type in 1234 8005 *0
Change Authority Level	System / Partition Master Code + 8 + User No. + * + 1 = Authority Level
03 = Standard 10 = Part. Master 05 = Arm Only 11 = Duress 04 = Guest	E.g. To change User 003 to Guest, type in 1234 8003 *104
Add Fire Authority to User:	System / Partition Master Code + 8 + User No. + * + 9 + 1
	E.g. To add Fire Authority to user 003, type 1234 8003 *91
Remove Fire Authority to User:	System / Partition Master Code + 8 + User No. + * + 9 + 0
	E.g. To remove Fire Authority to user 003, type 1234 8003 *90

Programming Security Codes via Touchscreens

1. Use the Master / Partition Master Code to access the Tools page.
2. Next, select the Users icon. It displays all current users.
3. The bottom of the screen provides options to EDIT, ADD NEW, or DELETE.
4. To EDIT, first select a User, then select EDIT. You can now change the user's Name, User Code, Partition and Authority Level. Be sure to touch the Save button in the upper right corner.
5. To ADD NEW, simply touch that button and you will have options to add a user's Name, User Code, Fire Authority Access, Partition, and Authority Level. Be sure to touch the Save button in the upper right corner. If a duplicate Security Code is entered, it will prompt "User code not accepted!". Touch OK and change the Security Code to one that is not programmed.
6. To DELETE a user, first select a User, then select DELETE. It will prompt "Are You Sure?". Select "Yes" or "No".

Authority Levels

- **Standard User** – Can arm, disarm, and bypass zones.
- **Arm Only** – Can arm but cannot disarm.
- **Guest** – Can arm but cannot disarm unless it was used to arm. Additionally, it cannot disarm if the system was armed via the Quick Arm feature (#2, #3, #4, #7, AWAY, and STAY keys).
- **Partition Master** – Is defaulted to User Number 02 in partition 1 and can add and delete Security Codes just like the Master Code, except it cannot change or delete the Master Code.
- **Duress** – Also known as an ambush code is a code that will arm/disarm the system, but silently alerts authorities that there's a concerning issue on the premise.

NOTE: Names can be applied to Security Codes so that the panel can report and log the name of the person(s) who are arming and disarming the Control Panel. These names can only be programmed via touchscreen or AlarmNet. If programmed in via AlarmNet, the names will reflect in the touchscreens. Security Codes can be scheduled via AlarmNet user portal to operate during selectable times of selectable days.

System Operation (Continued)

Fire Authority Access User

The fire system is global on this control panel., meaning it is active in every partition when a fire or CO alarm is activated. Every partition keypad will display that fire alarm. To silence and clear that alarm, the user must have Fire Authority Access enabled. To enable a user to be fire authority access only with no Burglary partition access, simply do not provide authority levels in the partitions provided. This user will only be able to silence and clear fire alarms.

NOTES:

- System master always has the Fire Authority Level by default.
- Installer code has Fire Authority Level access by default.
- Other users can be granted the Fire Authority Level by system and partition master users.
- System master can provide partition masters with Fire Authority. If partition masters have Fire Authority, they can grant the Fire Authority Permission to other users of that partition along with System master.
- Fire sounders can only be silenced by a Fire Authority Level user.
- Fire alarms can only be cleared by a Fire Authority Level user and from any partition.
- Burglar sounders can be silenced by any user with access to the relevant partition(s).
- Burglar alarms can be cleared by any user with access to the relevant partition(s).
- If Fire and Burg alarms are present in a system, the user having Fire Authority can clear the fire alarm. If that user has access to the burglar alarm partition(s) those are cleared automatically when code + off is entered (when clearing a fire alarm).
 1. First code + off: sounders of fire and burg alarms are silenced for the partition the user has access. But non accessible partitions burg sounders continue.
 2. Second code+ off clears the fire alarm and all accessible partition's burglar alarms. Non-accessible partition's burglar alarms continue.
- If new alarms occur after silencing an initial alarm but before clearing the alarm, the sounders continue.
- All CO Alarms will behave exactly same as Fire Alarms

System Operation (Continued)

Disarming / Canceling an Alarm

Anytime an alarm occurs, two disarm commands are required. The first will silence all sounds while the second disarm command will clear alarm memory. There are several ways to disarm the system from any alarm:

- From a keypad, type in a valid user code + **1**. To disarm the second time, type in a valid user code + **1**.
- From a touchscreen, type in a valid user code on the displayed keypad. To clear alarm memory, touch the keypad icon to display the keypad again and type in a valid code again.

If the alarm signal has been sent, the Cancel signal will be sent once the first disarm is entered. If the Abort Window is enabled (30 seconds by default) and the system is disarmed from an alarm before the abort window expires, no signals are sent.

Emergency Panic Keys / Icons

The system features three Emergency Panics for 24-hour silent, audible, fire or medical alarms. The Emergency Panic buttons can be used to manually initiate their respective alarms and send their reports to the Central Station. These functions are identified by the system on the keypads and touchscreens as follows:

VISTAHPKP/PROSIXLCDKP			There are 3 ways to activate an Emergency Panic alarm: 1. Press the Panic button and within 10 seconds press the desired Emergency button (Fire, Police, Medical / Personal). 2. Press desired Emergency button and within 10 seconds press the Panic button. 3. Press desired Emergency button and within 10 seconds press the same key. NOTE: Only the programmed Emergency keys will light up when the Panic key is pressed. If the Emergency key does not light up, it is not programmed.
Zone	Emergency Keys		
995	Fire		
999	Police		
996	Medical / Personal		
VISTAHTCHWLC			To activate an Emergency Panic alarm: 1. Touch the Panic Icon located in the bottom left corner of the screen. 2. Within 10 seconds, touch the desired Emergency Icon (Fire, Police, Medical / Personal) NOTE: Only the programmed Emergency Icons will be displayed. If it is not displayed, it is not programmed.
Zone	Emergency Keys		
995	Fire		
999	Police		
996	Medical / Personal		

Event Log

The Control Panel's event log is capable of recording and displaying up to 10,000 system events. These events are stored locally in the Control Panel, 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 as new events come in. The type of events that can be recorded is selectable via AlarmNet. The event log can be viewed through the touchscreens by navigating to Tools, enter the Master Code, then select Events. Refer to the Control Panel's User Manual for additional information. The Events and CID Codes displayed vary per 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 by the Control Panel. Each event in the log is preceded with an "E" or a "R". E means a new event while the R indicates the event has been restored.

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

System Operation (Continued)**Contact ID® Event Log Codes**

CID Code	Definition	Event Log Display
100	Medical Alarm	Medical Alarm
110	Fire Alarm	Fire Alarm
121	Duress Alarm	Duress Alarm
122	Silent Alarm	Silent Alarm
123	Audible Alarm	Audible Alarm
131	Perimeter Alarm	Perimeter Alarm
132	Interior Alarm	Interior Alarm
134	Entry/Exit Alarm	Entry/Exit Alarm
135	Day/Night Alarm	Day / Night Alarm
137	Sensor Tamper Alarm	Tamper Alarm
143	Base Unit & Keypad Failure	
145	Base Unit & Keypad Tamper	Exp Module Tamper
146	Silent Burglary Alarm	Silent Burglary
150	24-Hour Non-Burglary Alarm	24 Hr Non-Burglary Alarm
162	Carbon Monoxide Alarm	CO Alarm
301	AC Loss Trouble	AC Loss
302	Low System Battery Trouble	System Low Battery
305	System Reset Trouble	System Reset
311	Battery Discharged or Not Installed	Battery Dead/Missing
316	System Tamper	System Tamper
338	Expansion Module Battery Failure	Exp Module Batt. Failure
341	Base Unit & Keypad Tamper Trouble	Cover Tamper
342	Expansion Module AC Loss	
344	RF Jam Detected	RF Jam Detect
350	Communication Path Trouble	Comm. Path Trouble
353	Cellular Communication Transmitter Trouble	
354	Failure to Communicate Event	Failure to Communicate
360	Authorized New Registration	
373 *	Fire Trouble	Fire Trouble
374	Exit Error Alarm	Exit Error Alarm
378	Cross Zone Trouble	Cross Zone Trouble
379	Anti-Mask V-Plex Sensor Trouble	
380	Sensor Trouble	Sensor Trouble
381	Loss of RF Supervision Trouble	Superv Loss-RF
382	Loss of Supervision, Wired Devices	
383	Sensor Tamper Trouble	Sensor Tamper
384	RF Low Battery	RF Low Battery

* An E373 Fire Trouble will be generated anytime a fire zone goes into trouble. This will happen if a wired zone has an open condition. For wireless zones, a tamper or missing check-in will cause this and will not show as an E383 nor E381. The best way to find out which one it is, is by the timing. A missing check-in will happen at a 4-hour interval, starting from the last system reset, whereas a tamper may have a more random timing.

System Operation (Continued)

Contact ID® Event Log Codes (Continued)

CID Code	Definition	Event Log Display
385	Smoke Detector High Sensitivity Trouble	High Sense
386	Smoke Detector Low Sensitivity Trouble	Low Sense
394	Carbon Monoxide End of Life	Carbon Monox End of Life
401	Armed Away / Max by User	R401 - Arm Away / Maximum E401 - Disarmed
406	Cancel	Cancel
407	System Disarmed Remotely	Disarmed Remotely
408	Quick Arm Away	Quick Arm
441	Armed Stay / Instant by User	R441 - Arm Stay / Instant E441 - Disarmed from Stay Quick Arm - Stay / Instant
459	Recent Close - Alarm within 5 minutes of arming	Recent Closing
461	Wrong Code Entry - Keypad Lockout	Wrong Code Entry
570	Zone/Sensor Bypass	Zone Bypass
601	Manual Trigger Test Start	Manual Trigger Test Start
602	Periodic Test Report	Periodic Test Rep
607	Walk Test Mode Start	Walk Test Start
623	Event Log 90% Full	Event Log 90% Full
627	Programing Mode Entry	Program Mode Entry
628	Programing Mode Exit	Program Mode Exit
654	System Activity	System Activity

Central Station Messages

The following Contact ID messages are sent by the Control Panel's cellular and internet communicator for the conditions listed.

Alarm Condition	Alarm Code	Restore Code
Power On / Reset	E339 00 950	
Primary Communication Path Supervision	E350 C0 951	R350 C0 951
Secondary Communication Path Supervision	E350 C0 952	R350 C0 952
Communications Failure	E359 00 950	R359 00 950
Communications Failure Reminder	P359 00 950	
New Registration	E360 00 000	
Authorized Substitution Registration	E361 00 000	
Unauthorized Substitution Registration	E362 00 000	
Test	5555 55 559	

System Operation (Continued)

Keypad Tamper Lockout

When there are 30 numeric keys (0-9) entered within a 15-minute window and a valid command is not executed, the system stops processing additional numeric key presses for 15 minutes.

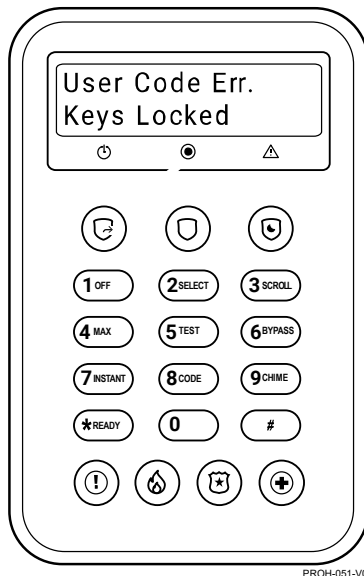
- Any numerical key press during the lockout generates a beep.
- In a partitioned system, keypads changed to a locked-out partition (GOTO command) will be locked out in that partition for the duration of that partition's lock out period.
- When a 15-minute lockout window occurs, a message (Event 461 "Wrong Code Entry") is transmitted to the Central Station and entered in the Event Log.
- When the 15-minute lockout window expires, a Restore message is sent to the Central Station and entered in the Event Log.

NOTES:

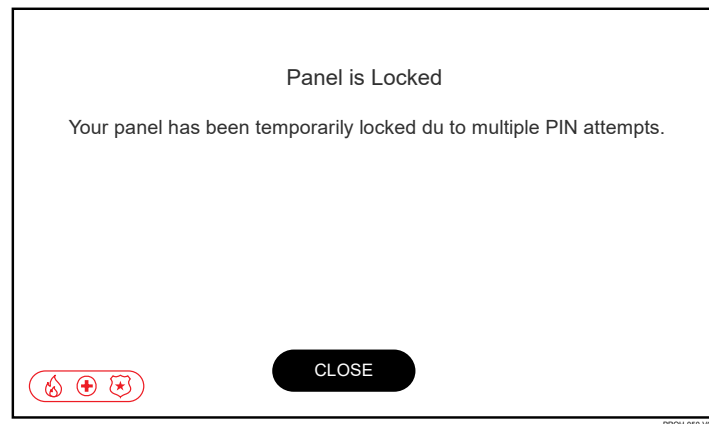
- The display is cleared when the time expires, or the lockout is terminated by either an Alarm occurring or Entry Time beginning.
- Power cycle of the panel will clear this and allow normal keypad operation.
- Applies to all Alpha and Fixed English keypads, and Touchscreens.
- Touchscreens will not process commands.
- RF fobs will work during a keypad lockout.
- Duress codes will not operate during a lockout.

Keypad Displays

VISTAHPKP/PROSIXLCDKP Keypad



VISTAHTCHWLC Display



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 components parts. Recommendation must be included for a specific program of frequent testing (at least annually) to ensure the system's proper operation at all times.

The following test modes can be initiated by keypad or touchscreen command:

- Comm. (Communication) Test
- Sensor Test
- Normal Mode Test
- Armed System Test



IMPORTANT: Notify the Central Station to put the account on test so they do not dispatch authorities.

Communications Tests

This can be tested locally from the touchscreen keypad or AN360. From the VISTAHTCHWLC Touchscreen, navigate to Tools → enter the Installer Code or Partition Master Code → System Tests → Test Communicator. From this screen there are four options to choose from:

- a. Test Wi-Fi
- b. Test Ethernet
- c. Test Cellular
- d. Test All

NOTES:

- When using internet, the Control Panel supervises the physical connection to the network router. This is called the Wi-Fi/Ethernet Fault time. If no network traffic for the programmed amount of time, the panel will provide a trouble display. This trouble condition will automatically clear from memory once the connection is restored.
- Communication Tests can only be initiated from partition 1.

Walk Test Mode

Alarm signals will not be sent during Walk Test Mode.

1. Walk Test can be initiated from keypads, touchscreens or from AlarmNet 360 website.
2. From the PROSIXLCDKP Keypads, type in the Installer Code or Partition Master Code + 5 + 1. Each keypad will emit a periodic beep once every minute as a reminder that it is still in Walk Test mode.
3. From the VISTAHTCHWLC Touchscreen, navigate to Tools → enter the Installer Code or Partition Master Code → System Tests → Test Sensors.
4. Upon entering Walk Test, the Bell and all keypads (excluding touchscreens) will sound for 2 seconds.
5. Fault each zone (wireless keys, doors, windows, motion detectors, etc.) and listen for the Chime beeps from the keypads and touchscreens. All protection zones and wireless keys will Chime in Walk Test mode. The touchscreens will also annunciate the zone's Voice Descriptor. Identification of each faulted protection point should appear on the display, and clear when the zone is physically restored.
6. To exit Walk Test Mode, simply type in a disarm command on any keypad or touchscreen or it will timeout and exit automatically after 4 hours.

Testing the System (Continued)

Normal Mode Test

With the system in the disarmed state, check that all zones are physically restored with no faults on the system. If the system is “not ready” check the keypads or touchscreens for the faulted zone(s). Restore the faulted zone(s) so that the “Status” LED lights green. Fault and restore every sensor individually to assure that the zones will fault and restore properly from the keypads and touchscreens.

Armed System Test

Alarm signals will be sent to the Central Station during the following test.

1. Arm the system and activate zones. Keep in mind that the Swinger Shutdown is defaulted at 2 reports per armed period (selectable 1-6), so only the first 2 signals per zone will be sent no matter how many times that zone is activated. Disarm the system twice to clear alarm memory and re-arm the system to test additional zones. The Abort Window is set to 30 seconds (selectable None–45 seconds), which means the Control Panel will wait this amount of time before sending the alarm signals after the alarm is initiated. If disarmed before the Abort Window time expires, no signals are sent.

NOTE: Swinger Shutdown and Abort Window do not apply to 24hr zones such as Fire, Carbon Monoxide, and Emergency keys (Panics).

2. Initiate each of the keypad’s Emergency keys to ensure proper operation and reports to the central station. 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 complete and verify the reports with them.

Step 5 – Commission

Commission the system through AN360, send the Welcome Emails from Total Connect 2.0 and train the Customer on the proper use of the ProSeries Hybrid Security/Fire System.

Specifications

Dimensions	10.44" W x 12.2" H x 3.5" D (265.2mm x 309.9mm x 87.7mm)
Electrical	14.3VDC, 2.65A from plug-in power supply, Part No. R300-12131 or R300-12131-CAN (Canada)
Alarm Sounder	10.5-13.8VDC, 2.0 Amp output (with battery installed) can drive 12V Bell or 702 Siren
Auxiliary Power Output	10.5-13.8VDC, 950mA max.
Backup Battery	12VDC, 7AH (sealed lead acid type). Charging Voltage: 13.65VDC
Communication Formats	4-digit Contact ID
Zone Resistance Tolerance	2k ohms with ± 300 ohms tolerance.
Agency Listings	
- Household Fire Warning System Units [UL985:2015 Ed.6+R:12Jul2018] - Household Burglar-Alarm Units [UL1023:2017 Ed.7] - Commercial Premises Security Alarm Units and Systems [UL2610:2021 Ed.2+R:31Jan2023] - Home Health Care Signaling Equipment [UL1637:2017 Ed.5] - General-Purpose Signaling Devices and Systems [UL 2017:2008 Ed. 2 +R:27Jan2016] - Standard for Control units, Accessories and Receiving Equipment for Intrusion Alarm Systems [ULC S304:2016 Ed.3+R1;R2] - Control Panel Standard – Features For False Alarm Reduction [ANSI/SIA CP-01:2014] - Standard for Residential Fire Warning System Control Units [ULC S545:2002 Ed. 2] - California State Fire Marshal (CSFM) Listed: 7167-1645:0523 - The Fire Alarm Verification Feature (Delay of fire alarm signal), not approved for use in California. - Burglary and other non-fire functions were not examined.	

Contacting Technical Support

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

- READ THE INSTRUCTIONS!
- Check the Troubleshooting section, starting on the next page, to assist with various issues.
- 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 customer number and/or company name.

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

Resideo Technical Support.....	1-800-645-7492 or 1-877-667-8324 (Canada)
AlarmNet Technical Support	1-800-222-6525
Hours of Operation.....	Monday – Friday: 8:30am – 8:30pm EST
MyWebTech:	https://mywebtech.honeywellhome.com/

Regulatory Agency Statements

Federal Communications Commission (FCC) & ISED Statements

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

CLASS B DIGITAL DEVICE STATEMENT

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

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio and television reception. It has been type tested and found to comply with the limits for a Class B computing device in accordance with the specifications in Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC ISED Statement

This device complies with Part 15 of the FCC Rules, and ISED's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, 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 ISED. Son fonctionnement est soumis aux conditions suivantes: (1) Cet appareil ne doit pas causer d'interférences nuisibles. (2) Cet appareil doit accepter toute interférence reçue y compris les interférences causant une réception indésirable.

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

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.

RF Exposure Warning

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



Mise en Garde

Exposition aux Fréquences Radio: La/les antenne(s) utilisée(s) pour cet émetteur doit/doivent être installée(s) à une distance de séparation d'au moins 20 cm (7,8 pouces) 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 ISEDs.

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

PROLTE-A: The external antenna gain shall not exceed 6.63 dBi for 700MHz and 850MHz, 6.0 dBi for 1700MHz and 8.5 dBi for 1900MHz. 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.

PROLTE-V: The external antenna gain shall not exceed 6.94 dBi for 700MHz, 6.0 dBi for 1700MHz, and 9.01 dBi for 1900MHz. 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.

PROLTE-CN: The external antenna gain shall not exceed 6.63 dBi for 700MHz, 6.0 dBi for 1700MHz and 8.51 dBi for 1900MHz. Under no conditions may an antenna gain be used that would exceed the ERP and EIRP power limits as specified IC RSS-130, RSS-132, RSS-133, and RSS-139.

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.
- Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily out of service. Telephone lines are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.
- This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 10 years, the electronic components could fail at any time.

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

Wireless transmitters (used in some systems) 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.

Warning: this unit includes an alarm verification feature that will result in a delay of the system alarm signal from the indicated circuits. The total delay (control unit plus smoke detectors) shall not exceed 60 seconds. No other smoke detector shall be connected to these circuits unless approved by the local authority having jurisdiction.

Avertissement: Cette unité peut être programmée pour utiliser une fonction de vérification d'alarme d'incendie qui entraîne un délai dans la signalisation des alarmes provenant des circuits dédiés à l'incendie. Le délai total (unité de commande et détecteurs de fumée) ne doit pas dépasser 60 secondes. Aucun autre détecteur de fumée ne doit être raccordé à ces circuits sans l'approbation des autorités compétentes locales.

Note: Each protected circuit within this control is supervised.



Table of Contents



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

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

Training, Documentation and Technical Support

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

READ THE INSTRUCTIONS AND VIEW THE INSTRUCTIONAL VIDEOS

- Visit: mywebtech.honeywellhome.com
- 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 Home customer number and/or company name.

Keeping this information handy will make it easier for us to serve you quickly and effectively. For technical support please call 1-800-645-7492.



Instructional Videos



MyWebTech

SUPPORT & WARRANTY

For the latest documentation and online support information, please go to:
www.resideo.com

For the latest warranty information, please go to:
www.security.honeywellhome.com/warranty



resideo

www.resideo.com

Resideo Technologies, Inc
2 Corporate Center Drive
P.O. Box 9040, Melville, NY 11747
© 2024 Resideo Technologies, Inc. All rights reserved



R800-28381B 1/24 Rev B