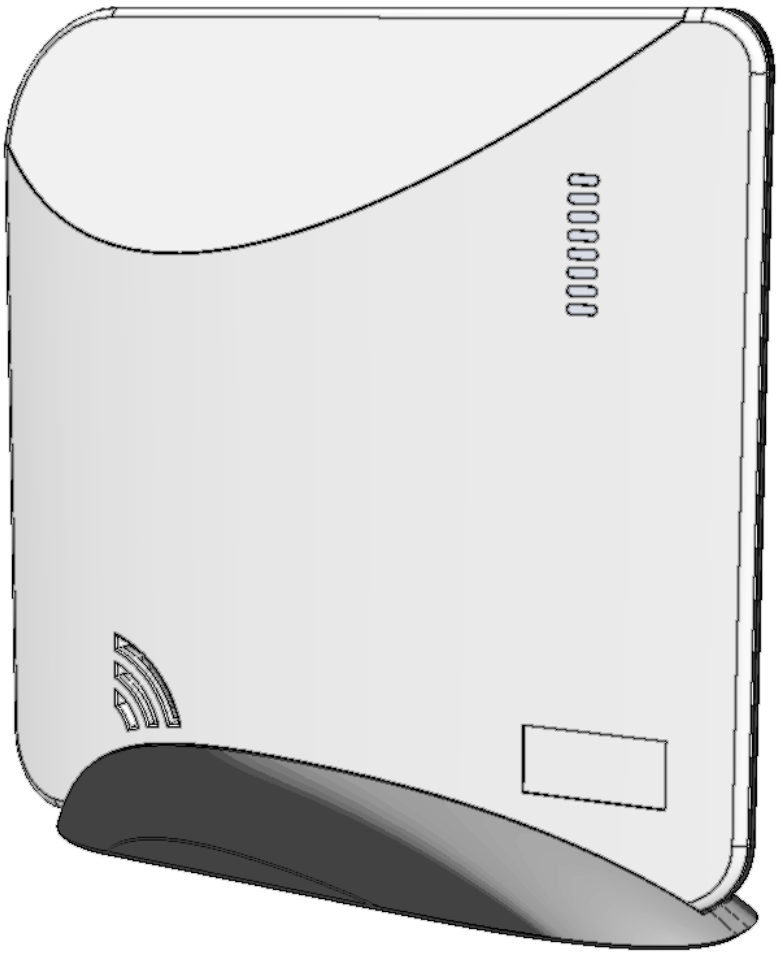
alula™



Connect+™ Security and Automation Platform
RE6100 Series Installation Guide

Meet Connect+

Connect+ is a professional wireless security panel designed to deliver home security and automation services. A secured and supervised Ethernet connection comes standard. Optional Cellular and Wi-Fi cards provide primary or backup communication channels. Its long-range encrypted wireless receiver easily provides whole home coverage. Wireless arming stations and mobile devices uncouple Connect+ from the entry wall and allow it to be installed at a location convenient for Internet and power connections.

FEATURES

- Cellular, Wi-Fi, or Ethernet communication channels
- Control from a user's mobile device
- Industry-leading wireless range
- Up to 50 users
- Up to 96 zones
- 2-way voice communication with RE6130
- 5 year warranty

ITEMS INCLUDED IN THE BOX

- The Connect+ panel
- Rechargeable backup battery
- 12-Volt power adapter
- 6-foot Ethernet cable
- Table-top mounting base
- A screw to secure the cover (required for UL installations)
- Installation guide
- Configuration guide
- Platform Guide

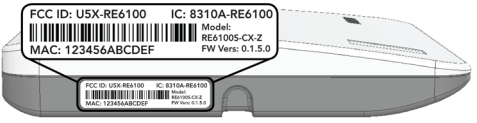
EXPANSION CARDS FOR INTERNET CONNECTIVITY

- Wi-Fi™ Card
- LTE Cellular Card (Verizon)

OTHER EXPANSION CARDS

- Z-Wave™ Card
- Existing Security Sensor Translator Card (allows the Connect+ panel to receive signals from existing wireless security sensors)
- Combo Z-Wave & Existing Sensor Translator Card

System Setup



1 ***Set up a new account*** with Alula following the instructions in the platform guide included. You will need the MAC address, which is located on the bottom the panel.

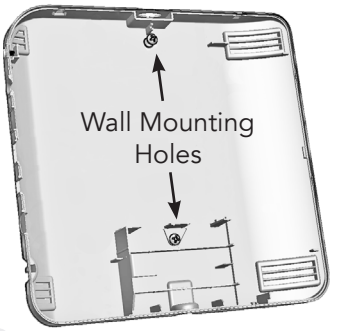
STOP DO NOT PROCEED UNTIL YOU HAVE FINISHED STEP 1

2 ***Find a location*** for the panel, keeping in mind it needs AC power and at least one network connection.

Panel Location Guidelines

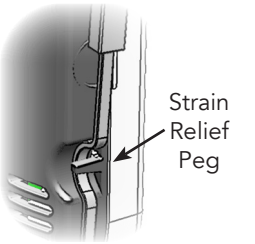
- Locate centrally on the main floor.
- Avoid mounting below ground level.
- Do not mount near ducts, appliances, or other large metal objects.
- Do not mount directly adjacent to other RF devices.

3 ***Mount the panel*** by sliding it downward into the table-top base. Alternatively, the panel can be mounted to a wall using the mounting holes in the back cover. You will need to remove the backup battery to reveal the lower mounting hole.



4 ***Connect the panel to the Internet*** by wiring its Ethernet port to the home router, or by installing a Cellular or Wi-Fi expansion card (or any combination of the above). The Wi-Fi approach requires enrollment into the home Wi-Fi router.

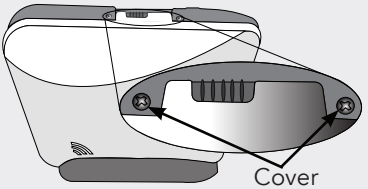
- If you are using Wi-Fi, then connect the Wi-Fi card to your existing home router by holding the Enroll/WPS button until the panel beeps twice (roughly ten seconds) and then pressing the WPS button on the router.



5 ***Power up the panel*** by inserting the power supply barrel into the power jack on the side. Route the power cable under the strain relief peg.

UL Installation Requirements

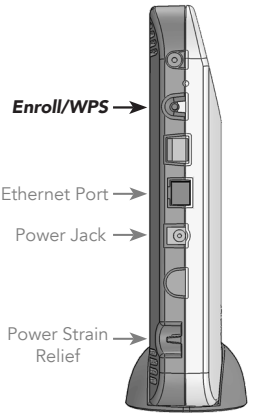
- Install the cover-securing screws.
- Do not connect the panel to an AC power receptacle controlled by a switch.
- The power supply must be secured to an outlet if installed in the USA.
- The power supply must NOT be secured to an outlet if installed in Canada.



6 ***Enroll sensors and peripherals*** by first pressing the Enroll/WPS button on the side of the panel until it beeps once (roughly 3 seconds) and then sending an enrollment signal from the sensor or peripheral. Alternatively, a device can be enrolled by scanning its bar code using the Connect+ Installer app or by entering its 8-character serial number on the Alula dealer portal.

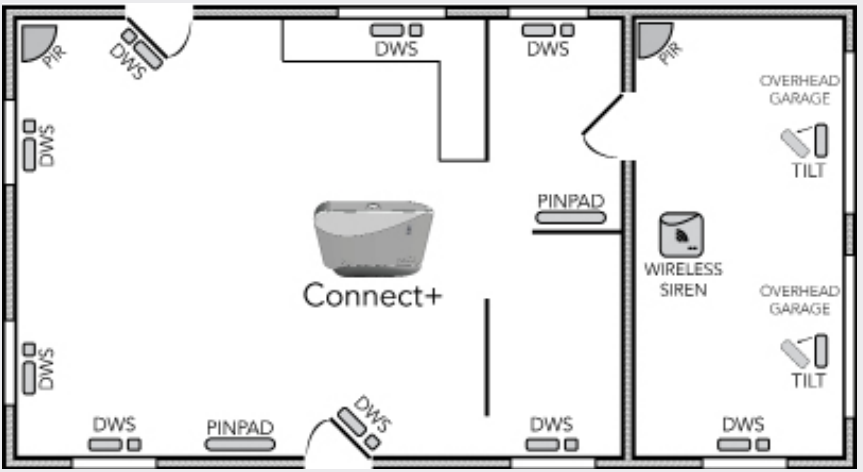
Enrollment Tips

- Enrollment signals are typically triggered by removing the battery tab or tampering the device. See the specific device manual for more information.
- The *Connect+ Installer* App can be used to enroll and configure sensors.
- The Alula dealer portal provides a way to enter and exit wireless enrollment mode.
- Wireless enrollment mode will end 5 minutes after the last sensor is enrolled.
- Enrolling a Keypad or other 2.4GHz peripheral will automatically end wireless enrollment mode.
- Tapping the Enroll/WPS button will end wireless enrollment mode.



7 ***Install your sensors & peripherals*** in desired locations around the house. Refer to the specific device manual for more information regarding installation and use.

Typical Burglary Protection Installation

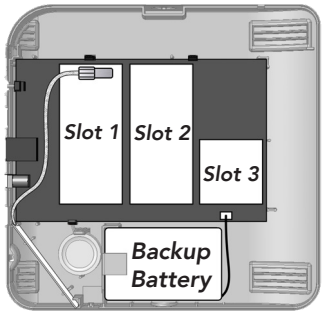


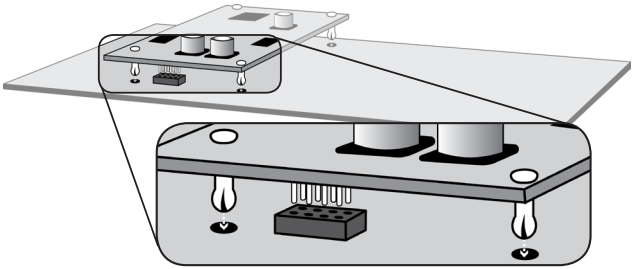
8 ***Configure the panel, sensors, and peripherals*** using the *Connect+ Installer* app or the Alula dealer portal. Configuration options are described in the configuration guide.

9 ***Finally, test the system*** after finishing installation, enrollment, and configuration. Verify proper operation of all installed sensors and peripherals using the Connect+ Installer app or the Alula dealer portal. All sensors and peripherals should score at least one bar on the RF signal strength indicator. See *Pro Tips - RF Signal Strength*.

Pro-Tips

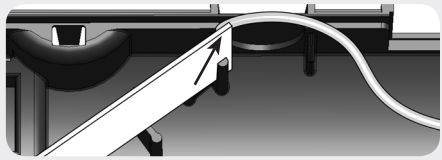
Install an expansion card by first disconnecting AC power and the battery. Cellular cards must use slot 1 and square cards must use slot 3. Always refer to the specific card manual for a full list of installation requirements. Next, **carefully align** the nylon retention posts and 8-pin connector while pushing the card firmly until all the posts are fully seated. Finally, reconnect the battery, AC power, and verify proper operation using the LED indicators on the expansion card.





Cellular Antenna Installation

- Route the antenna wire near the Ethernet jack as shown above.
- Install the antenna with the feed wire on the top side as shown to the right.



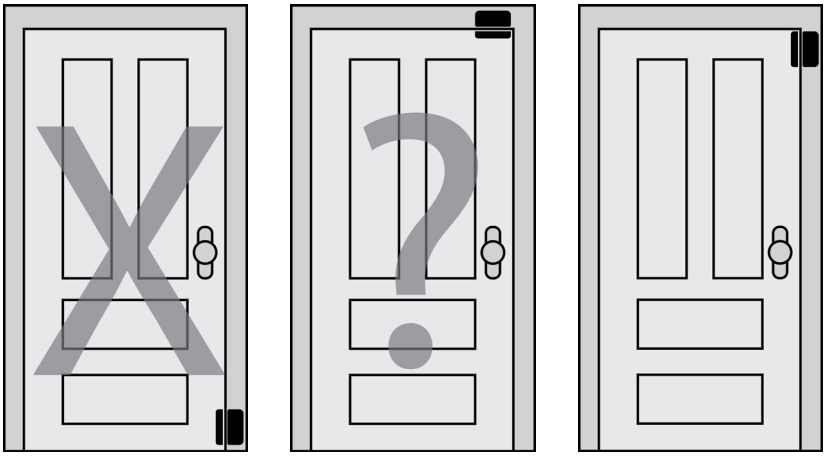
RF Signal Strength is an averaged signal-to-noise indication. Even in the absence of sensor transmissions, the panel experiences ambient RF energy (i.e. noise). The RF signal strength indication represents a sensor's signal relative to ambient noise. If multiple sensors score low signal strength, this could be due to one or more of the following:

1. **High ambient noise -** Ensure the panel is not mounted adjacent to other electronics.
2. **Panel isn't centrally located, or is mounted below ground -** Move the panel to a central location in the home that is above ground level.
3. **Panel is located near ducts, appliances, or other large metal objects** - Relocate the panel away from these types of objects.

Sensor Signal Strength Tips

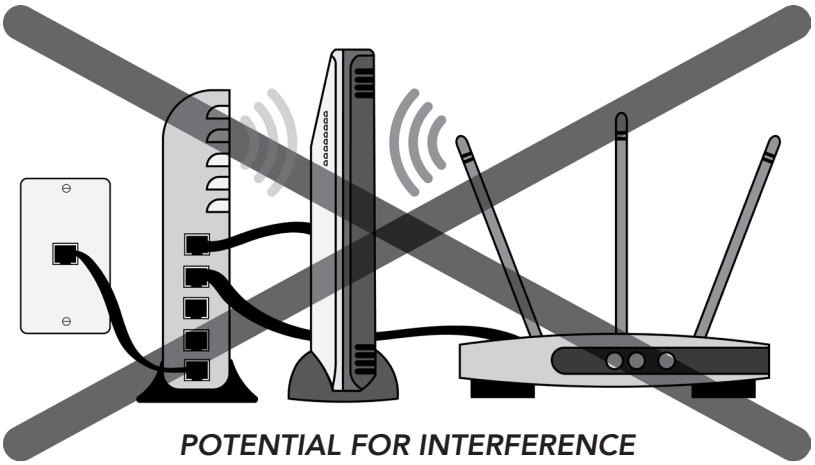
- The signal strength scale is from 0 to 100 (0 to 5 bars).
- There is **nothing wrong** with a sensor that has at least one bar (e.g. a signal strength of at least 20).
- Signal strength readings are averaged. If you move the panel or a sensor, it takes some time for the signal strength readings to update. Tripping a sensor several times will help update a sensor's signal strength faster.
- Before mounting a sensor permanently, expose a slight portion of its mounting tape and apply it (**very lightly)** to the desired location. If it performs well, mount it permanently. If it performs poorly, try rotating it by 90 degrees.
- *Do not test a mounting location by tripping a sensor in your hand*. Holding a sensor changes how it radiates RF energy. Sometimes these "hand effects" help, and sometimes they hurt.

Wireless performance of door window sensors is optimized when mounted vertically near the top corner of the door.



WRONG *OK* *BEST*

Routers, modems, and other electronic devices emit RF noise. For best results, avoid mounting the panel directly beside other electronic devices.



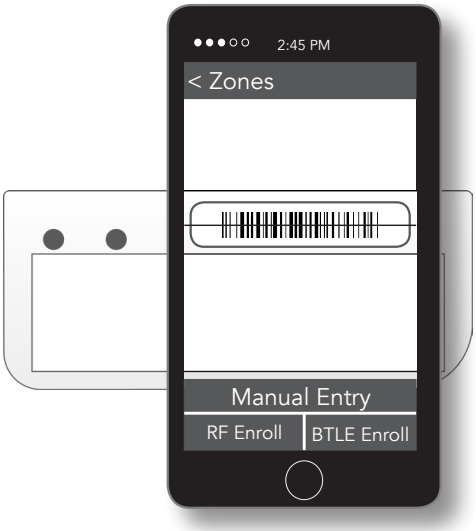
POTENTIAL FOR INTERFERENCE

- Put some space between the panel and the home router. A 6-foot cable is included for this purpose.

Trouble beeps can be suppressed so they only occur during a specific window of time each day.

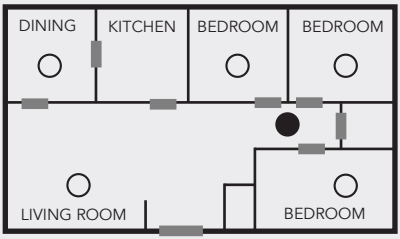
- Use the Connect+ Installer app or the Alula dealer portal to configure the trouble beep suppression period.
- Trouble beeps can be temporarily silenced for 24 hours using a Keypad or Keyfob.

The Connect+ Installer App can be used to enroll sensors by scanning the barcode.

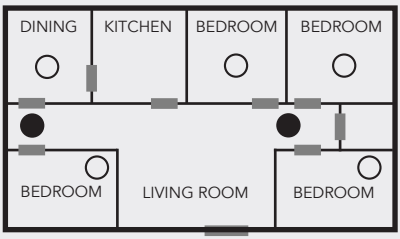


Smoke Alarms should be installed in accordance with Chapter 2 of "*ANSI/NFPA 72: National Fire Alarm and Signaling Code*" (National Fire Protection Association, Batterymarch Park, Quincy, MA 02169) when installed in the USA. Smoke alarms installed in Canada should be installed in accordance with "*Standard for the Installation of Residential Fire Warning Systems, CAN/ULC-S540*".

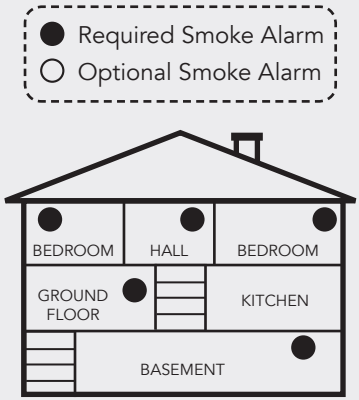
Smoke Alarm Placement



(Single Sleeping Area)



(Multiple Sleeping Areas)



(Multi-Floor Home)

NOTE: Regulations pertaining to smoke alarm installations vary. Contact your local fire department for more information.

Should the battery need replacing, remove the cover, disconnect the old battery, and connect a new battery. The battery connector is polarized and can be inserted only one way into the panel receptacle.

Emergency Planning

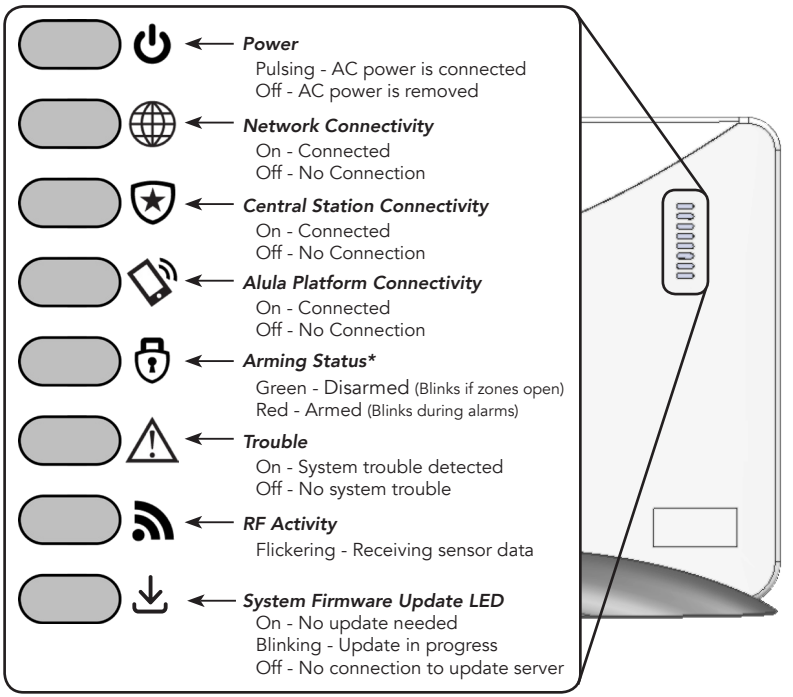
Emergencies happen, so have a plan.

Emergency Planning Tips

- Periodically discuss and rehearse emergency plans.
- Understand how to use your security system.
- Know the normal states of doors and windows: open, closed, or locked.
- Escape fast! (Do not stop to pack.)
- Use a different escape route if closed doors feel hot to the touch.
- Smoke is toxic. Stay low and breathe strategically when escaping a burning building.
- Designate a nearby landmark as a safe family re-grouping location.
- Emphasize that no one should return to the premises if there is a fire.
- Call 911 as soon as possible but do it in a safe location.
- Do not enter the premises if you arrive and hear sirens. Call for emergency assistance from a safe location.

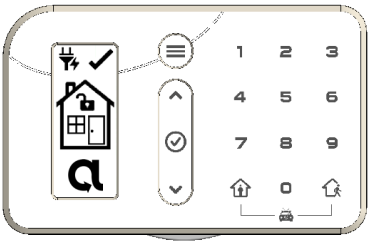
Using the Connect+ Panel

System Status Indication is provided via eight LEDs on the front of the panel. These LEDs may all be forced OFF to conserve battery power during an AC power failure.



* This LED will toggle between green and red while wireless enrollment mode is active.

Using the Keypad (See the Keypad manual for detailed operation)



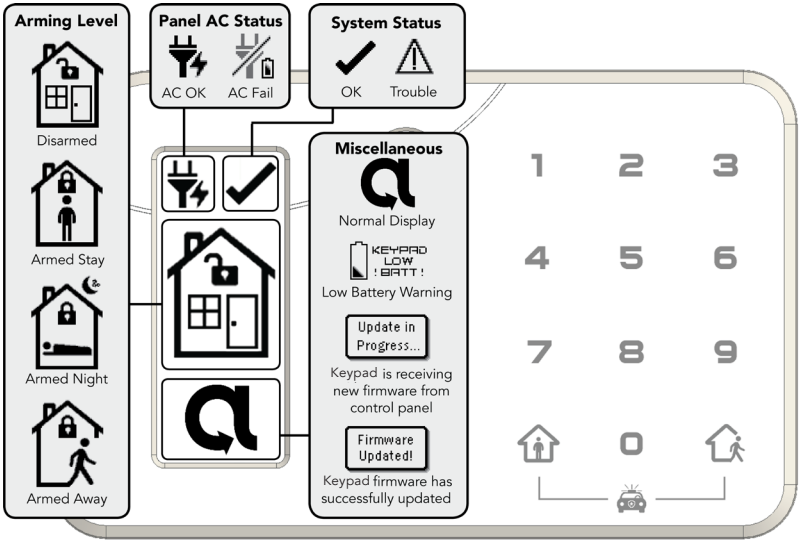
Disarm the system by entering a valid user code on the number pad.

Arm Away by pressing ARM AWAY until the Keypad clicks.

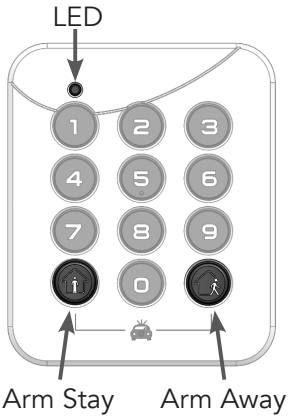
Arm Stay by pressing ARM STAY until the Keypad clicks.

Trigger a panic alarm by pressing ARM STAY & ARM AWAY together until the display indicates a panic alarm.

View real-time system status using the Keypad's display.



Using PINPad (See PINPad™ manual for detailed operation)



Disarm the system by entering a valid user code on the number pad.

Arm Away by pressing the "AWAY" button until the PINPad LED flashes red.

Arm Stay by pressing the "STAY" button until the PINPad LED flashes red.

Trigger a panic alarm by pressing the "STAY" & "AWAY" buttons together until the PINPad LED flashes red.

Connectivity Troubleshooting

Symptom	*Troubleshooting Steps*
Network Connectivity LED Off	**Ethernet Connections** 1. Ensure the Ethernet cable is fully inserted in both the panel and router/modem. **Wi-Fi Connections** 1. Ensure the Wi-Fi card is properly installed, and the Power LED on the card is pulsing. 2. Ensure the panel has been configured with the proper Wi-Fi credentials and the Wi-Fi LED on the expansion card is on solid. If the LED is blinking either the network is not in range, or the Wi-Fi credentials are incorrect (refer to *System Setup - Step 4*). **Cellular Connections** 1. Ensure the Cellular card is properly installed, and the Power LED on the card is pulsing. 2. Inspect the LED on the expansion card. • A solid LED indicates the panel is connected to the network. • A flashing LED indicates the panel has found a tower, and is attempting to connect to the network. Wait until the LED is solid. If the LED has been double flashing for more than ten minutes, try power cycling the panel.
Central Station Connectivity LED Off	1. Ensure the Network Connectivity LED is on. If it is off, see the network connectivity troubleshooting section above. 2. Ensure port TCP 9999 is open in the router/modem settings. 3. Ensure the panel is registered to an account with Alula and the account is active. 4. Ensure the panel has been configured with the proper central station reporting information: Account Number, Central Station Receiver Host and Port, Central Station Receiver ID and Line ID.
Alula Platform Connectivity LED Off	1. Ensure the Network Connectivity LED is on. If it is off, see the network connectivity troubleshooting section above. 2. Ensure port UDP 1234 is open in the router/modem settings. 3. Ensure the panel is registered to an account with Alula and the account is active.
System Firmware Update LED Off	1. Ensure port UDP 1235 is open in the router/modem settings. The panel and peripherals will not be able to receive firmware updates if this port isn't available or is already in use.

System Maintenance

System testing should be performed after installation is completed and whenever a problem occurs.

Smoke and CO alarms should be tested after installed and weekly by pressing the test button on the alarm. The panel will indicate it has properly received a test signal by sounding a temporal three sound for a Smoke alarm or a temporal four sound for a CO alarrm.

Critical functions and communication links of the system are automatically monitored and exercised to detect trouble conditions.

Regulatory

UL SYSTEM REQUIREMENTS

Control Unit, consisting of:

- Base Panel: RE6100 series
- Backup Battery: RE029 (6V, 2.5Ah, NiMH)
- Power Supply: RE012-6 (In: 100-240VAC; Out: 12VDC, 1A)
- PINPad (RE652) or Keypad (RE656), connected wirelessly
- Ethernet connection native to base panel or Cellular module (RE928RxS, RE928RxV, or RE927RxA)

Compatible ETL listed signal initiating devices:

- RE614 Smoke Alarm
- RE615 CO Alarm
- RE653 Outdoor Motion Sensor
- RE659 360 Motion Sensor
- RE661 Indoor Motion Sensor
- RE601 Door/Window Sensor
- RE622 NanoMax Door/Window Sensor
- RE610P Motion Detector

Optional devices, not ETL listed:

- Any of a wide array of Connect+ compatible sensors

UL1023 Household Burglar Alarm System:

- Control Unit
- At least one burglary signal initiating device
- Entry delay: 45 seconds or less
- Exit delay: 60 seconds or less
- Sensor supervisory: 24 hours or less
- Panel status volume: on
- Panel siren: on
- Auto force arm: on
- Siren timeout: 4 minutes or more

ORD-C1023-1974 Canadian Household Burglar Alarm System:

- Control Unit and installation as described for UL1023
- Power supply: RE012-6, Do NOT secure with a receptacle securing screw. Ne pas se connecter Connect+ à une prise contrôlée par un interrupteur.
- Siren timeout: 6 minutes or more

UL985 Household Fire Warning System (Not applicable with RE6130):

- Control Unit
- At least one smoke signal-initiating device enrolled into "Fire" zone profile.
- Smoke supervision: on
- Panel siren: on
- Siren timeout: 4 minutes or more
- Panel status volume: on

ULC-S545-M89 Canadian Household Fire Warning System (Not applicable with RE6130):

- Control Unit and installation as described for UL985
- Power supply: RE012-6, Do NOT secure with a receptacle securing screw. Ne pas se connecter Connect+ à une prise contrôlée par un interrupteur.
- Siren timeout: 6 minutes or more

Central Station Communicator Requirement is at least one of:

- UL1610 Central Station Burglar Alarm System: Ethernet connection native to base panel
  -OR-
- UL1635 Digital Alarm Communicator System: Cellular module RE928RSS, RE928RSV, or RE927RSA
- RF supervision: 4 hours
- Communication interface supervision: on
- Entry delay plus reporting delay must not exceed 60 seconds.
- Reporting delay is 30 seconds.

Network Equipment:

- Use a UL 60950-1 listed broadband router/modem for the 10/100 Ethernet port or Wi-Fi connection

UL 1610 Commercial Burglar Alarm System:

- Commercial: on
- The product shall be installed in accordance with National Electrical Code, ANSI/NFPA 70, the standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, the Standard for Central-Station Alarm Services, UL 827, CSA C22.1, Canadian Electrical Code, Part I, Safety and Standard for Electrical Installations, CAN/ULC S302, Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems, and CAN/ULC S301, Installation, Inspection and Testing of Intrusion Alarm Systems, and CAN/ULC S301, Standard for Signal Receiving Centre Intrusion Alarm Systems and Operations.
- Ethernet Port must be connected directly to a router without any Ethernet switches.
- Siren Test: Siren should be tested once a week. Trip alarm to sound the siren. Disarm system to silence siren. Contact Central Station if alarms will be reported.
- Intended use includes: Commercial Central Station, Encrypted Line Security, Single and Dual Signal Line Transmission
- Communication interface options need to have supervision enabled depending on panel setup. Ethernet, Slot 1, Slot 2.

CE SYSTEM REQUIREMENTS

Access Levels:

- Access Level 1: Person with no access to the security system features.
- Access Level 2: Regular users with access to all features on the security system with a code.
- Access Level 3: Master and Alarm company users that can do everything a level 2 user can do and also change system settings (e.g. add, modify, or delete users).
- Access Level 4: Manufacturer of equipment access. Typically used for system updates.

User Codes:

- Four or more invalid code attempts will disable the interface and trigger a tamper condition.
- There are 10,000 unique 4-digit PIN codes.
- There are 16,777,215 unique identification codes for logical keys (Keyfobs).

Priority of Indicators:

- Fire alarm
- CO alarm
- Panic alarm
- Burglary alarm
- Tamper alarm
- Auxiliary alarm
- Freeze alarm
- Heat alarm
- Water alarm
- Tamper indication
- Fault indication

Ancillary Control Devices:

- Up to 8 PINPads (RE652)
- Up to 8 Keypads (RE656) and/or mobile devices.
- PINPads and Keypads can issue panic alarms

ANSI-SIA CP-01 REQUIREMENTS

Required Equipment:

- RE6100 Connect+ Panel
- RE656 Keypad

Note: Combined entry delay and abort window should not exceed 1 minute.

Note: Programming at installation may be subordinate to other UL requirements for the intended application.

Nonprogrammable SIA Options

Nonprogrammable Options	**Setting**
Silent Exit	Annunciators Enabled
Progress Annunciation	Annunciators Enabled
Cancel Report Annunciation	Enabled
Recent Closing	Enabled (2 Minute Window)
Exit Error	Enabled
Restoration of Power	Panel will ignore sensor trips for the first sixty seconds after power-up
Cancel Alarm	Enabled
Remote Arming	Annunciators Enabled

SIA Setting Requirements

Programmable Options	**Default**	**Recommended Setting**	**Range**
Entry Delay	30 Seconds	30 Seconds	30-240 Seconds
Exit Delay	60 Seconds	60 Seconds	45-240 Seconds
Abort Time	30 Seconds	15-45 Seconds	1-45 Seconds
Auto Stay Arming	On	On	On/Off
Exit Delay Restart	On	On	On/Off
Swinger Threshold	Two Trips	Two Trips	1-6 Trips
Duress	Disabled	Disabled	Disabled, valid duress code
Cross Zoning	Disabled	Enabled for sensors that may cause false alarms	On/Off
Fire Alarm Verification	Disabled	Enabled unless sensor can self verify	On/Off
Alarm Abort Annunciation	On	On	On/Off
Alarm Cancel Annunciation	On	On	On/Off

User Information - Definitions

Report Delay: Consult with your installer to determine if your system is configured with a communicator delay. A communicator delay will prevent a report to the central station if the control panel is disarmed within _____ seconds (default is 30 seconds) after an intrusion alarm is triggered. Note that fire-type alarms and Carbon Monoxide alarms are normally reported without a delay.

Exit Delay: The period of time allowed, after Arming a security system, to exit the entry/exit door without tripping an alarm. Note: Enabling silent exit doubles the exit delay time

Entry Delay: The door used to enter the premise will start an entry delay when tripped. You will hear entry delay beeps when you trip the sensor: this will allow you time to disarm the system. Entering a user code will disarm the system.

Entry Delay Progress: Three beeps every four seconds and three beeps every two seconds during the last ten seconds of entry delay.

Exit Delay Progress: Two beeps every two seconds and two beeps every second during last ten seconds of exit delay time.

System Acknowledgment: Sounders will sound one beep to confirm disarm, two beeps to confirm stay arming and four beeps to confirm away arming.

Exit Delay Restart: The feature will recognize when you arm the system, leave your house and then quickly re-enter. If this happens, the system will restart your exit delay to give you the full exit delay again.

Auto Stay Arming: Determines whether the system automatically arms down to Stay if you arm the system to Away without exiting the system entry/exit door. This feature will not be enabled when arming from a keyfob.

Arming Level - Disarm: In this level, only 24-hour sensors are active.

Arming Level - Stay: Perimeter sensors are active. Interior sensors are not active.

Arming Level - Away: Perimeter and interior sensors are active.

Panic Alarm: To trigger panic alarm from Keypad, press and hold stay and away buttons at the same time.

Alarm Abort: If the panel beeps three times after disarming an alarm, then the alarm is aborted.

Alarm Cancel Report: If an alarm has previously been transmitted, a cancel signal will be transmitted when the alarm system is disarmed. The panel will sound two beeps three seconds after disarming when sending a cancel message.

Alarm Memory: After canceling an alarm, press status on Keypad to view alarm memory.

Duress Code: The user uses a unique code, which disarms the system and transmits a "Duress" alarm to the monitoring center.

Cross Zoning: Refers to two different sensors that must be tripped within two minutes of each other to report an alarm to the central station. When motion is detected by the first sensor, it starts a two minute timer. If the other sensors trip within two minutes, an alarm report will be sent to the central station.

Swinger Shutdown: This setting determines how many times the sensor will go into alarm during a single arming period. Once the sensor is in swinger mode it will not be active again until the alarm is canceled.

Note: Swinger shutdown does not affect Fire and Carbon Monoxide sensors.

Fire Alarm Verification: The panel immediately reports to the central station when a smoke alarm goes into alarm. With this option on, if a single smoke alarm goes into alarm, the panel will not report for 60 seconds unless another smoke alarm goes into alarm. If the first smoke alarm is cleared of an alarm within the first 60 seconds, no report will be sent to the central station unless it or a second smoke alarm goes into alarm within 5 minutes.

User Information - Testing the System

Before testing alarms, contact your central station and tell them you are testing the system.

Central station phone number _____

System account number _____

Test door/window sensors by first closing all doors and windows that have sensors. Verify the display on the keypad or mobile app indicates the system is in the ready state. Trip each sensor by opening the door or window and verify it shows open at the keypad or on the mobile app.

Test smoke alarms by pressing the test button until smoke alarm sounds. Check mobile app activity to verify fire walk test signal was reported. (The sirens will play one cycle of the temporal 3 siren pattern when a smoke test is pressed).

Test CO alarmss by pressing the test button until CO alarm sounds. Check mobile app activity to verify CO test signal was reported. (The sirens will play one cycle of the temporal 4 siren cadence when a CO test is pressed.)

Test glassbreak sensors using a glass break sound tester to trip sensor.

Testing Panic Alarms: Panic alarms will be reported to the central station and will cause the panel siren to sound. Ensure your central station knows you are testing the system. Press the panic button and verify the system goes into alarm. To test panic alarms on the RE656 Keypad and RE652 PINPad, press and hold the stay and away arming buttons to trigger a panic alarm.

Test panel communication by verifying the alarms you tripped were reported to and received by the central station.

When finished, remember to tell the central station you are done testing the system.

THIS PAGE IS INTENTIONALLY LEFT BLANK

Specifications

PHYSICAL	
Housing Body Dimensions	8.9 x 8.9 x 1.5 inches (22.6 x 22.6 x 3.8 cm)
Housing Base Dimensions	8.2 x 1.3 x 2.7 inches (20.8 x 3.3 x 6.7 cm)
Weight with Battery	26.8 ounces (760 grams)
Mounting Fastener	#6 or #8 screws (not provided)
ENVIRONMENTAL	
Operating Temperature	32 to 120 °F (0 to 49 °C)
Storage Temperature	-4 to 86 °F (-20 to 30 °C)
Maximum Humidity	85% non-condensing relative humidity
PANEL SPECIFICATIONS	
Radio Frequencies	433.92MHz, 2.4GHz
Power Supply Part Number	RE012-6 (US), RE012-7 (AUS), RE012-8 (CE)
Input	100-240VAC, 50/60 Hz, 0.5A
Output	12VDC, 1A
Battery Part Number	RE029
Backup	24 hours minimum (4 hours minimum for RE6130)
Specifications	6VDC, 2.5Ah, NiMH
Battery Charger	25mA (Trickle), 95mA (Fast)
Current Draw (RE6100, RE6110, RE6120)	150mA (Normal), 300mA (Alarm)
Current Draw (RE6130P-XW-X)	250mA (Normal), 400mA (Alarm)
Current Draw (RE6130P-LX-X)	150mA (Normal), 400mA (Alarm)
Tamper Indications	Cover opening and Wall removal
Sensors	Up to 96 Connect+ Compatible Wireless Security Zones
Interface Devices	Up to 8 PINPads (RE652) Up to 8 Keypads (RE656) and/or mobile devices, up to 4 Touchpads
Maximum Number of Users	50
CERTIFICATIONS	
RE6100	UL1023, UL985, UL1635, UL1610, ORD-C1023-1974, ULC S304, ULC-S545-M89, ETL, FCC, IC
RE6110	EN 60950-1, EN 300 220, EN 301 489, RCM
RE6120	EN50131-3, EN 60950-1, EN 300 220, EN 301 489, CE
RE6130P-XW-X	UL1023, UL1635, ORD-C1023-1974, ETL, FCC, IC
RE6130P-LX-X	UL1023, UL985, UL1635, ORD-C1023-1974, ULC-S545-M89, ETL, FCC, IC

Specifications subject to change without notice.

WARRANTY

Alula will replace products that are defective in their first five (5) years.

IC NOTICE

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) This device may not cause interference, and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux cnr d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:
(1) L'appareil ne doit pas produire de brouillage, et
(2) L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC: 8310A-RE6100

TRADEMARKS

Alula and Connect+ are trademarks owned by Alula Holdings, LLC.

FCC NOTICE

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

Changes or modifications not expressly approved by Alula could void the user's authority to operate this equipment.

FCC ID: U5X-RE6100

CE DECLARATION OF CONFORMITY

Hereby, Alula declares that this RE6120 is in compliance with the essential requirements and other relevant provisions of directive 1999/5/EC.

(This declaration can be translated to other languages via a myriad of translation tools found on the Internet.)

alula™ Z-Wave® User Guide

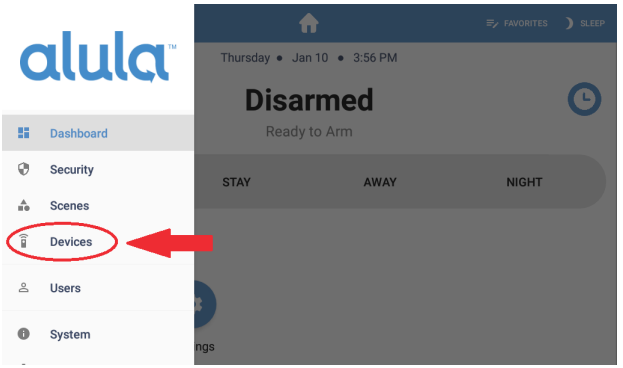
Connect+ Z-Wave Controller is a Z-Wave Plus® Product using the latest Security S2 Encryption. This product can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All non-battery operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.

Adding a Z-Wave Device

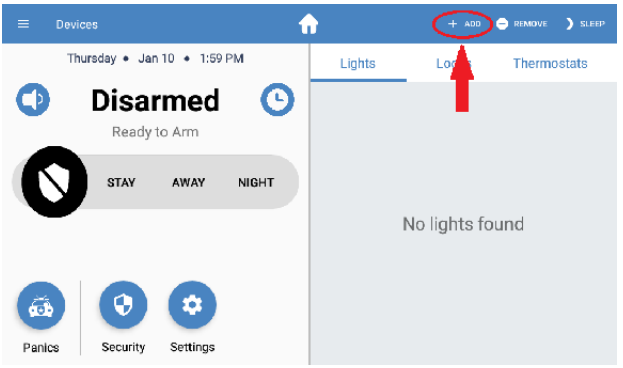
Follow these steps to add a new Z-Wave device:

Note: if the device to be added was previously enrolled, or from another network, it will need to be removed to clear any prior network settings before it can be added to the Connect+ network. If device failed to add, it must go through the removal process before attempting to add again.

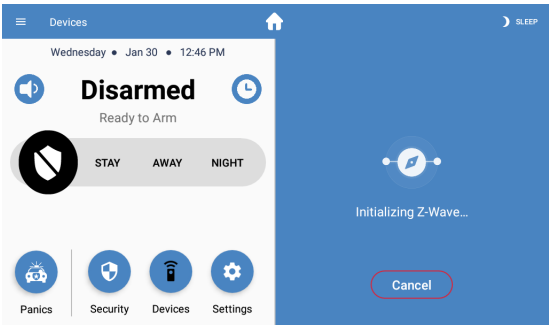
1. Navigate to the Devices screen using the left side menu on the Touchpad.

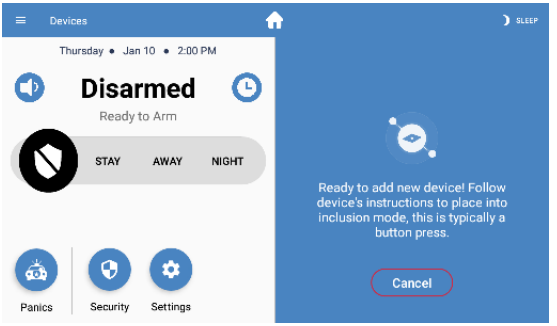


2. Touch the "+ Add" icon on the top right corner to start adding Z-Wave.



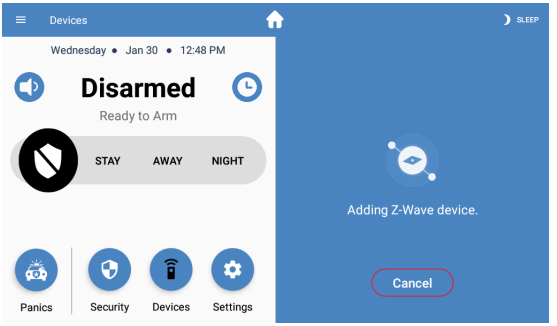
3. Connect+ will start the addition process and the following messages will display on the right side of the screen. This may take only a few seconds, or up to a minute to complete if the Connect+ controller is busy.



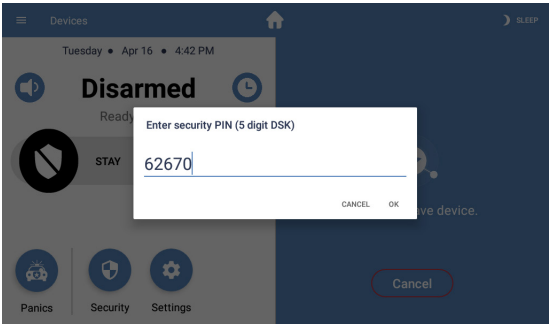


4. When the second message above is displayed, Connect+ is now ready to add the new device. Follow the new device's instructions to place it into inclusion mode. This is typically a button press.

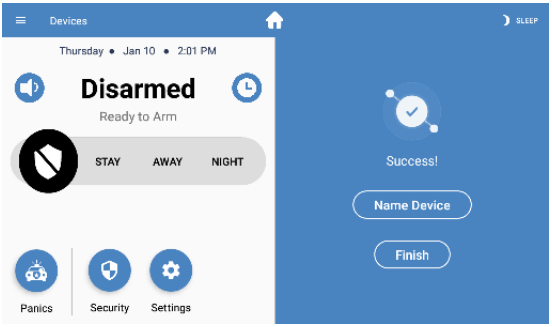
5. After putting the device into inclusion mode, the following message will display on the screen.



6.If the device being added supports Security S2, then you will be prompted on the screen to enter that device's 5 digit DSK pin to complete the enrollment



7.Depending on the device and number of supported command classes, this may take only a few seconds or up to a minute to complete.



Removing a Z-Wave Device

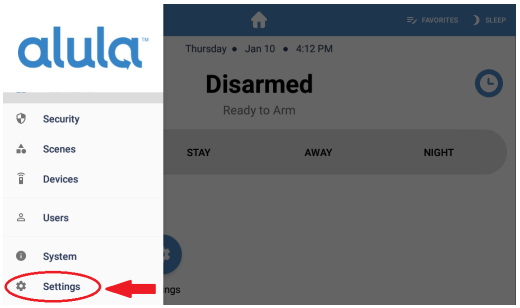
1. On the Z-Wave device page on the Touchpad, touch the "- Remove" icon in the top right corner.
2. Connect+ will start the removal process. Status messages will display on the right side of the screen, and follow similar steps to the Add process. You will be prompted to place the device into exclusion mode, which is typically a button press. Follow the device's instructions to place it into exclusion mode.
3. If removal fails, try again until successful.

Z-Wave Factory Reset

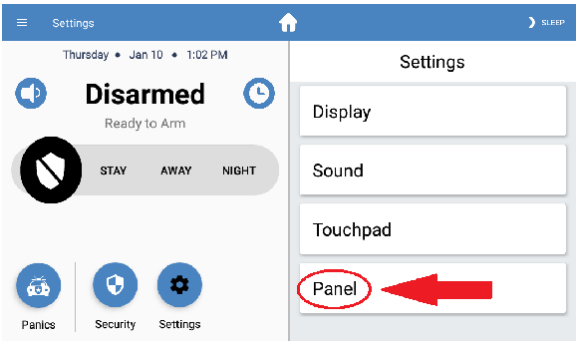
Two types of Z-Wave reset are supported: soft reset and hard reset. Soft reset will only reboot the Z-Wave controller and will retain all your devices. Use this if you are experiencing persistent network issues to attempt to correct them. A hard reset will set the Z-Wave controller in Connect+ back to its factory default and all network devices will be cleared. Perform a hard reset only when the network primary controller is missing or otherwise inoperable.

Note: Performing a hard reset will only factory default Connect+. Each device must also be factory defaulted, or go through the removal process before they can be re-added to a network.

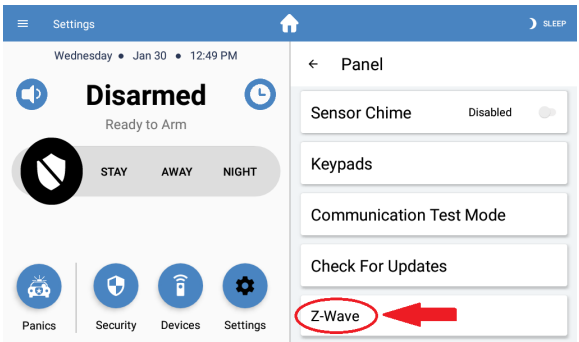
1. Navigate to the Settings screen from the left side menu, or the Settings icon on the home screen on the Touchpad.



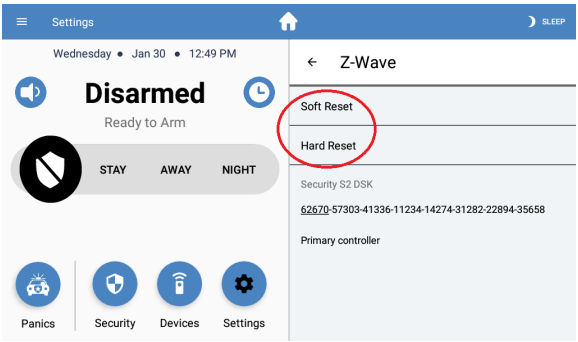
2. In the Settings menu, touch the last item “Panel” and enter your 4-digit security system PIN when prompted.



3. In the next sub-menu, scroll down and select the “Z-Wave” menu item.



4. Select either “Soft Reset” or “Hard Reset”. You will see a confirmation message on the screen before performing the reset action.



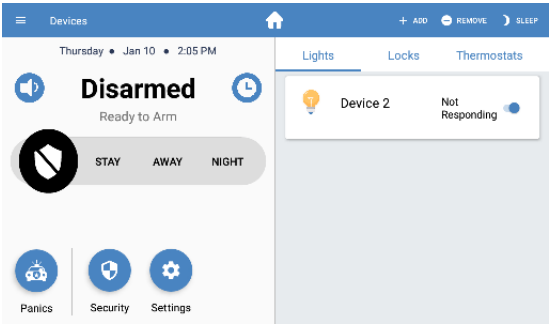
5. A hard reset typically takes 5-10 seconds to complete. A soft reset will take additional time to complete refreshing all devices on the network, approximately 30 seconds per enrolled device. On large networks this may take several minutes to complete before normal operation is expected to resume.

Remove or Replace a failed Z-Wave Device

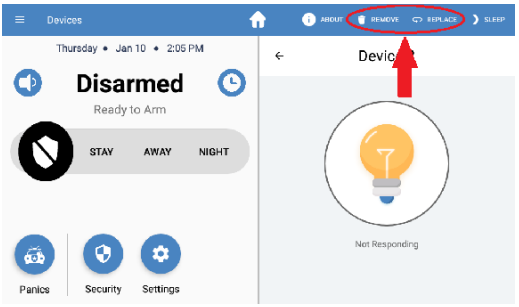
Use these steps if a Z-Wave device becomes unresponsive, lost, or defective and you are unable to remove the device through the normal removal process.

> Note: Before these options become available in the Touchpad, the Connect+ controller must place the device in a "Not Responding" state. If the device does not show either of these two messages on the display, then you must first attempt to send a command to the device, knowing it will fail. After the failure to send the command, the UI should now show the correct "Not Responding" state.

1. Once the device is in the Not Responding state, select the device in the list to display the device sub-display.



2. Both options "Delete" and "Replace" will be located on the top right of the screen. If these options are not present, then the device is either still operational, or you must perform the steps in the note above.



- The "Delete" option will remove this device from the network.
- The "Replace" option will remove the device, and enroll a new device in its place using the same node number. It will follow the same enrollment flow as adding a new device.

Z-Wave Learn Modes and including Connect+ into an existing network

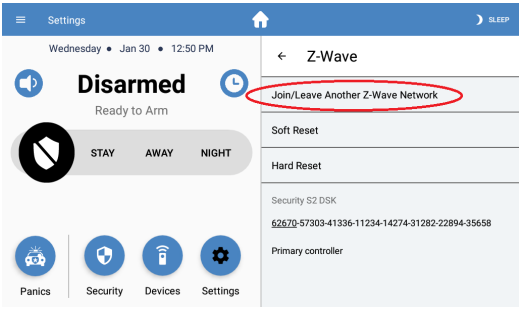
Connect+ has the ability to be included into another existing network started by another controller. This is useful if a network already exists using a third party controller and you wish to view and control that network with Connect+ at the same time. These command options are ONLY visible in the settings menu when they are supported and correct network conditions are met: inclusion modes are only allowed if Connect+ does not have its own network (no devices), and is not part of another network already. Exclusion modes are only allowed if Connect+ is already part of another network.

There are three "Learn Mode" commands available. First is Classic Learn Mode, used for both inclusion and exclusion to and from an existing network. This is an old style command used for direct line

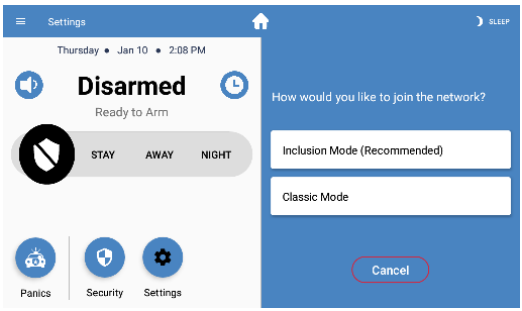
of site with a legacy controller that may not support the new learn modes. This mode is also used for controller replication, described in the Network Copy section of this manual.

The next two learn modes are Network Wide Inclusion Learn Mode (NWI), named just "Inclusion Mode" on the Touchpad, and Network Wide Exclusion Learn Mode (NWE), named "Exclusion Mode" on the Touchpad. These commands do not require direct line of site to the third party controller; however, it is recommended if possible.

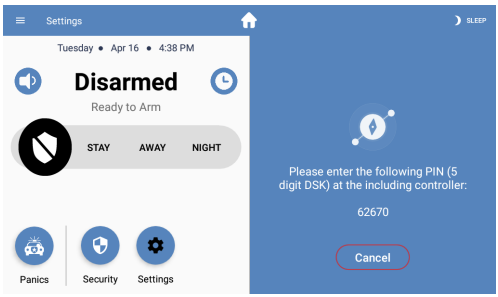
1. Navigate to the Z-Wave sub-menu as described in the Factory Reset section of this manual.
2. If network requirements are met as explained above, then the "Join/Leave Another Z-Wave Network" option will be visible in the menu, otherwise it will not be present.



3. BEFORE selecting a Learn Mode from the sub menu, place the primary controller on the other network into Add or Remove mode.
4. From the sub menu, select the Learn Mode to join the other existing network. The learn mode is only active for roughly 10 seconds. If another primary network is found in that time frame, it will attempt a connection. The join process may take a few seconds to several minutes to complete.



5. If the including controller supports Security S2, at this point Connect+'s own 5 digit DSK pin will be displayed on the screen. You will need to input this pin on the other including controller to complete the learn mode. Connect+ does not have a DSK sticker like other products, instead it will only be displayed when needed during this mode. The entire Connect+ DSK is located in the Z-Wave settings menu for reference if needed



6. After the Touchpad shows a successful learn mode completion, wait at least 30-45 ADDITIONAL seconds to allow new network initialization and device discovery to complete. The above message will be displayed on the Touchpad as a reminder.

Z-Wave Network Copy (Z-Wave Replication)

Replication is the process of updating network information from a primary controller to secondary controllers, such as node list and routing information. These steps are usually not required unless you have a multiple controller network.

If Connect+ is the primary controller, and secondary controllers don't automatically update:

1. Put Connect+ into Add mode, as described in that section.
2. Put the secondary controller into one of the two Inclusion Learn Modes. See instruction manual for that 3rd party secondary controller.
3. Allow add mode to complete.
4. This re-inclusion process will replicate new network information to the secondary controller.

If Connect+ is a secondary/inclusion controller and the network contains a SIS controller (typical), then Connect+ will automatically perform network replication/updates in the background and no manual process is required. Additionally if Connect+ is included into a network without an SIS, it will automatically attempt to acquire this role so manual replication is not required. However, if you suspect network changes have occurred and network information is out of date/sync, and you need to force the network to update, perform the following steps:

1. Reference the primary controller's manual for instructions to put it into replication mode.
2. When primary controller is ready, follow the steps to put Connect+ into "Classic Learn Mode" as described in the Learn Modes section of this manual.
3. This will re-include Connect+ and force update the network information.

Z-Wave Inclusion Controller

Connect+ can operate as an Inclusion Controller when enrolled into another network where the primary controller is a SIS. In this role, Connect+ is able to add and remove devices on the primary controller's behalf.

Note: If a security Z-Wave device is added by Connect+, Security S2 setup MUST be performed by the primary controller to complete the enrollment, which includes optional granting of security keys and entering the DSK 5 digit code if required. The primary controller must be available to perform these requirements to complete the enrollment.

Note: Because both controllers have to pass the new device enrollment back and forth, it may take additional time before the device shows up correctly, and status is shown in the Touchpad.

1. Add a device as specified in the Add Z-Wave Device section of this manual.
2. If S2 security is required, perform those steps using the other controller's interface.
3. The remainder of the enrollment will automatically complete. No further action is required.

If Connect+ is the primary controller, and another controller on the network includes a new Security S2 device, similarly the Touchpad must be ready to perform the DSK 5 digit code entry if required to complete the enrollment.

1. Before adding a new device using the other controller, make sure to have the Touchpad ready.
2. If S2 security is required, the other controller will hand over the enrollment to Connect+, and a DSK 5 digit code entry window will automatically appear on the Touchpad.
3. After entering the DSK if required, the remainder of the enrollment will automatically complete.

Z-Wave Network Maintenance

Connect+ strives to make the Z-Wave user experience as easy and hassle free as possible. To that end, Connect+ handles any network maintenance and optimization automatically, and most functions are not user accessible. Some of the things done automatically are:

1. Polling of device state information to keep UI up to date. Note on a large network it will take time to query each device.
2. Periodically check and attempt to locate missing or out of range devices.
3. Once or twice a day, Connect+ will perform a network maintenance routine, which includes checking and repairing node return routes and checking node neighbors. This operation will also be performed roughly 10 minutes after any new devices are added to the Connect+ network, to correct any routing problems after a device may be moved around the house after installation.
4. When Connect+ is enrolled onto another network, it will automatically attempt to query the primary controller for network updates, so a manual network copy (replication) is not required.

Z-Wave Basic Command Class

Connect+ can control, but does NOT support the Z-Wave Basic Command Class. Any received BASIC_GET or BASIC_SET commands are ignored. Connect+ is able to send BASIC_SET commands to any unknown or unsupported devices through the Touchpad. Note: Sending basic commands to a battery powered sleeping device will enter a queue or "mailbox", and will be sent to the device when it awakes.

Z-Wave Association

The Z-Wave Association Command Class is supported by the Connect+.
Group1: Lifeline group
Number of nodes supported: 4
Reports sent via the Lifeline group: Device Reset Locally Notification

Z-Wave Supported Command Classes

When Connect+ is the primary controller (typical), secure command classes are only supported using the S2 Access Control Security Class. If Connect+ is included into another network, then secure command classes are supported using the highest security level granted on enrollment into that network.

Command Class	Not-added	Non-securely added	Securely Added	
			Non-secure	Secure CC
COMMAND_CLASS_ZWAVEPLUS_INFO	Support	Support	Support	
COMMAND_CLASS_SECURITY	Support	Support	Support	
COMMAND_CLASS_SECURITY_2	Support	Support	Support	
COMMAND_CLASS_INCLUSION_CONTROLLER	Support	Support	Support	
COMMAND_CLASS_TRANSPORT_SERVICE	Support	Support	Support	
COMMAND_CLASS_ASSOCIATION		Support		Support
COMMAND_CLASS_ASSOCIATION_GRP_INFO		Support		Support
COMMAND_CLASS_POWERLEVEL		Support		Support
COMMAND_CLASS_MANUFACTURER_SPECIFIC		Support		Support
COMMAND_CLASS_VERSION		Support		Support
COMMAND_CLASS_CRC_16_ENCAP	Support	Support	Support	
COMMAND_CLASS_SUPERVISION	Support	Support	Support	
COMMAND_CLASS_DEVICE_RESET_LOCALLY		Support		Support

Z-Wave Manufacturer Specific Information

Manufacturer ID: 0x0353
Product Type ID: 0x0001
Product ID: 0x0001