Alarm.com Universal Communicator (AUC) LX30B - Installation Guide - Model: LX30B-QxxT

For a panel-specific quick install guide, see Alarm.com Universal Communicator (AUC) LX30B - Quick Install Guide.

The Alarm.com Universal Communicator (AUC) is a takeover device for upgrading compatible older POTS security systems. The LX30B-AUC provides the best of Alarm.com security, including arming and disarming remote control through the Alarm.com Customer app and notifications like Unexpected Activity Alerts and location-based arming reminders.

The LX30B can retrofit any security system meant to use telephone lines, or POTS, with DTMF. To make installation as easy as possible, we've tested and verified many of the most popular panels to provide specific wiring and programming guidance. For more information about verified and unverified panels, see Which control panels are compatible with Alarm.com Universal Communicators?.

For more information about specifications, see LX30B Alarm.com Universal Communicator (AUC) - Data Sheet.

For more information about supported features, see What features are available when using an Alarm.com Universal Communicator (AUC)?.

Compatibility requirements

- LX30B-AUC firmware version must be 2.19.4+.
- Verify compatibility of the panel and desired protocol (CID or SIA). For more information about the panels that have been verified, see Which control panels are compatible with Alarm.com Universal Communicators?.
- Verify that the panel is not using zone numbers greater than 126.
- For keyswitch integration, verify each of the following:
  - For remotely viewing panel arming status, verify a PGM slot is available.
  - For remotely changing panel arming status, verify a hardwired zone is available.
  - A *Universal Communicator* service package is required.
  - The Customer app version must be 5.6+ on iOS and Android.

Before you start - Important safety instructions

This document provides information about mounting, wiring, and troubleshooting of the Alarm.com Universal Communicator (AUC). It is written under the assumption that the installer is qualified and possesses the necessary skills to install this device.

Read all the safety and operating instructions listed below before installation and use.

- The device should be assembled, installed, and serviced by qualified personnel in accordance with the instructions.
- The device should be checked by qualified personnel once a year (on average).
- The device should work in a safe environment with parameters in accordance with the device's specifications.
- Operating temperature: nominal: +68ºF (+20ºC), acceptable: +14ºF… +131ºF (-10ºC… +55ºC). Humidity 0% ... 93% (without condensation).
- Do not install the device near any heat sources; such as radiators, heat registers, stoves, or other appliances that produce heat.
- The device is intended only for indoor and dry installation. __
- Do not install in dirty, dusty places, places with high humidity (with condensation), or near water, chemical vapors or in the same room with medical equipment, the function of which may be disrupted.
- If damaged, the device should be disconnected then replaced only by trained, qualified personnel. Before disconnecting the device, it is necessary to disconnect the power supply.
- Do not repair the device yourself, repairs are made only by the manufacturer's service.
- The device should always be cleaned with a dry cloth. Do not use water, detergents or chemicals — they may damage the device.
- Avoid mounting the Universal Communicator near sources of significant electromagnetic interference, or in rooms where metal is the predominant structural material due to the potential for cellular signal attenuation.

Caution: To reduce the risk of fire or electric shock, do not expose the device to rain or moisture.

Create an Alarm.com account

Before installing the Alarm.com Universal Communicator (AUC), first create a new Alarm.com customer account using the Partner Portal or MobileTech app.

During the account creation process, you are prompted to enter the following information for the *System Information*:

- 15-Digit Module Serial Number - the IMEI number located on the Alarm.com Universal Communicator (AUC) device
- Panel Manufacturer
  - If the panel's manufacturer is not listed, select **Other**.
- Panel Model Number
- Panel Firmware Version (optional)
- AC Power Failure cold start option
  - For more information, see AC Power Failure cold start restoral on Alarm.com Universal Communicators (AUC).

Note: On AUC firmware version below 2.25.4:

- A field for *Communicator Phone Number* is required during account creation. If the phone number programmed locally is known, enter the number here. Otherwise, 555555 is the default for the AUC and local panel programming should be updated to match. The phone number should be no longer than 16 digits.
- An upgrade to 2.25.4 will automatically begin after 24 hours of creating the account.

One of the following service packages must be selected for use with the AUC:

- *Wireless Signal Forwarding* (not available in Canada)
- *Universal Communicator Residential*
- *Universal Communicator Commercial*

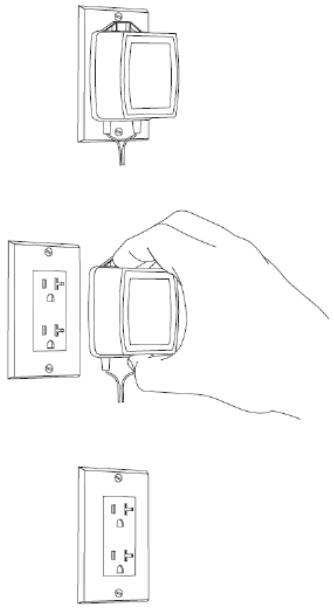
For more information about creating a customer account, see How to create an Alarm.com customer account.

Disarm and power down the panel

Prior to disconnecting power from the panel, verify the following:

- The control panel is disarmed and does not have any alarms in memory.
- There are no local trouble conditions at the panel.

Next, remove panel AC power and disconnect the backup battery.

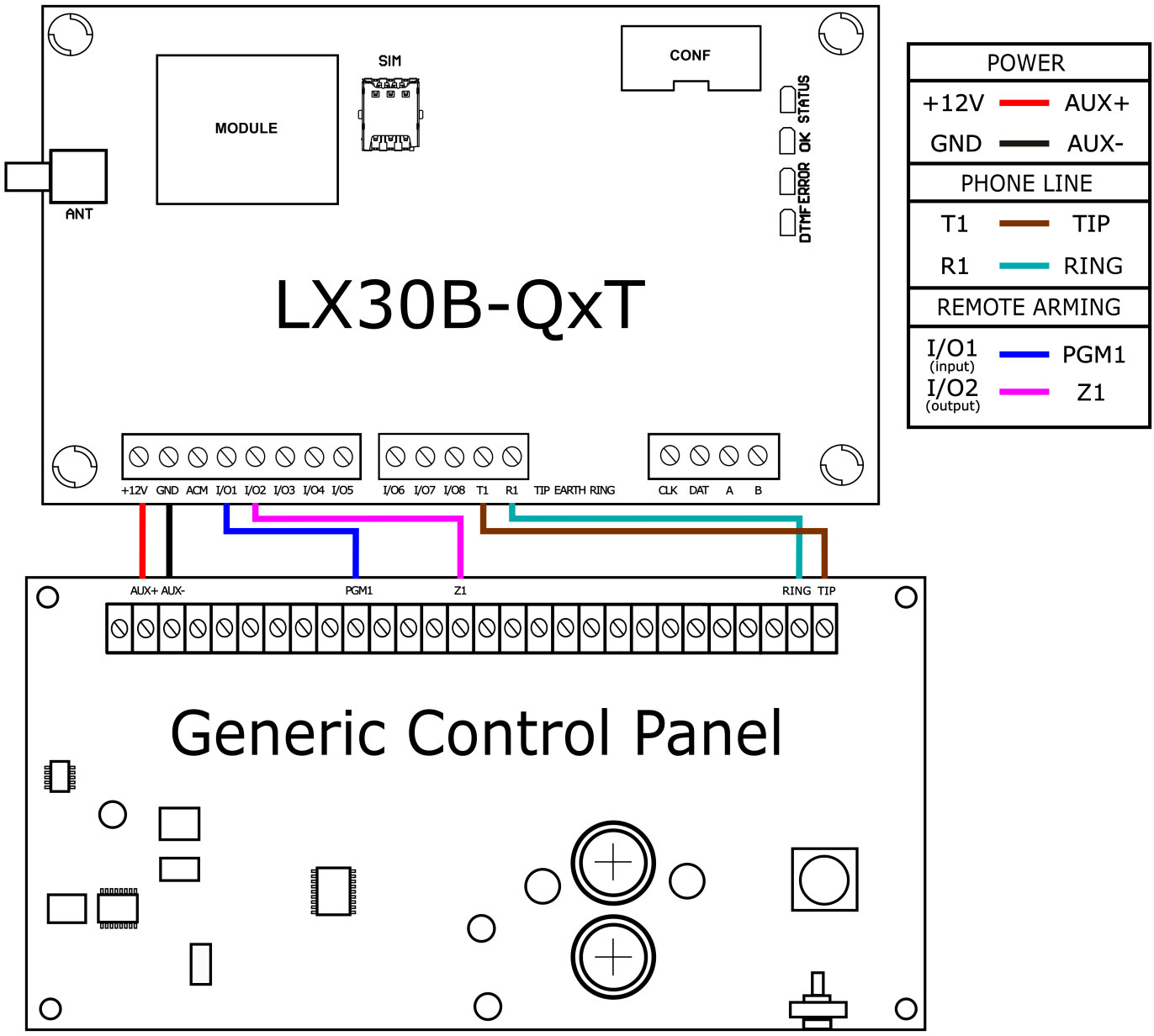


Wire the Universal Communicator

Wiring

The following diagram is a reference for a generic control panel using the keyswitch integration for remote arming (I/O1 and I/O2). The specific terminal names may vary based on panel type. Any wired zone or PGM can be used if supporting remote arming and status, but the instructions use Z1 (zone 1) and PGM1.

Important: Depending on the panel model, an end-of-line resistor may be required for the keyswitch zone. Refer to the panel manufacturer documentation and support



.For more information about Smart Connector (keybus integration) wiring, see Alarm.com Universal Communicator (AUC) - Smart Connector User Guide or the panel-specific setup guide.

Click to expand for the list of panels with available panel-specific setup guides: ^

- Aritech ATS1500
- Bosch ICP SOL2-P/SOL3-P
- DSC Impassa
- DSC MaxSYS PC4020A V3.52
- DSC PC1404
- DSC PC585

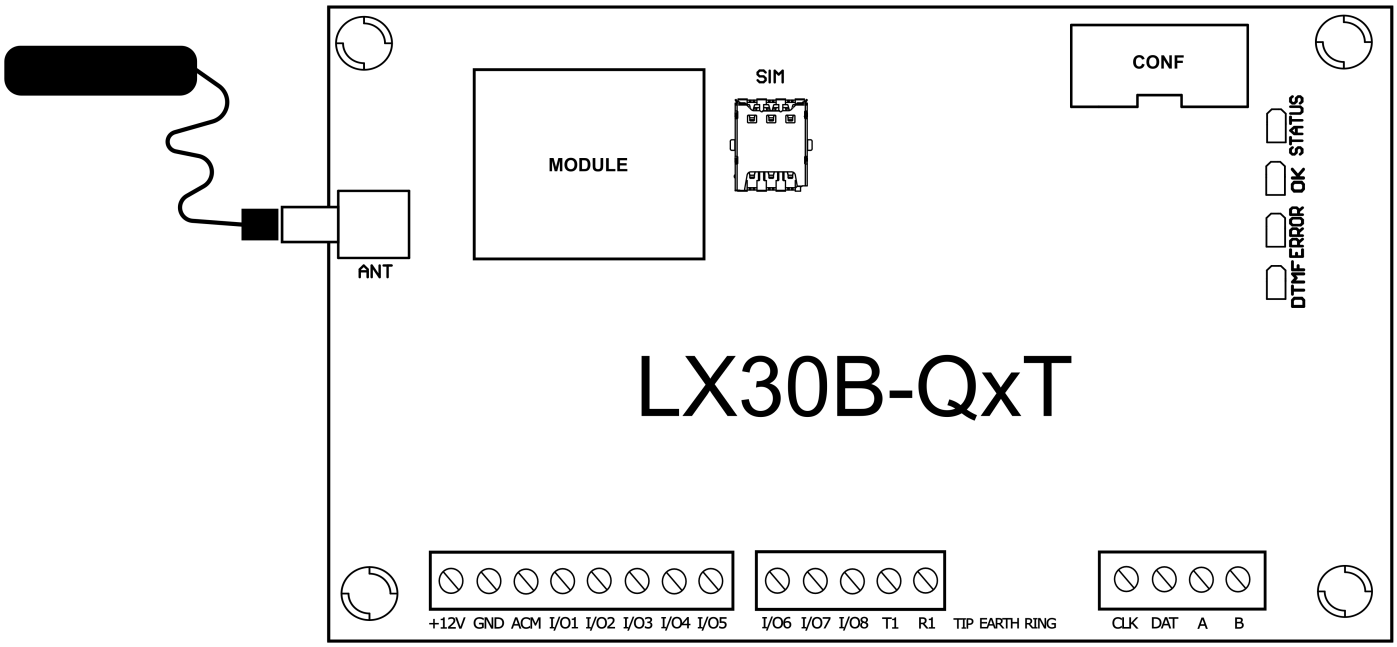
- DSC Power832 (PC5010)
- DSC PowerSeries Neo
- DSC PowerSeries PC1616/PC1832/PC1864
- GE Concord 4
- GE Concord Express
- GE Hills NX-4V2
- GE Hills NX-6V2 (EU)
- GE Hills NX-8E
- GE Hills NX-8V2
- HKC SW-10270
- HKC SW-1070
- Honeywell Galaxy 2-12
- Honeywell Galaxy 3 48C
- Honeywell Galaxy Dimension 96
- Honeywell Galaxy Dimension 96 (Double Balanced version)
- Honeywell Galaxy Flex FX050
- Honeywell Galaxy Flex FX100
- Honeywell Vista 120
- Honeywell Vista 15P/20P/21IP
- Honeywell Vista 4140XMPT2
- Honeywell Vista 48D
- Honeywell Vista128BPT
- Honeywell Vista48LA
- Honeywell Vista50P
- Intelbras AMT 1000 SMART
- Intelbras AMT 2018 E SMART
- Intelbras AMT 4010 SMART
- Jablotron JA-100K
- Jablotron JA-14K
- NAPCO Gemini P9600
- PIMA HUNTER 8 (Captain 8)
- PIMA HUNTER Pro 832
- Paradox EVO192
- Paradox EVO48
- Paradox EVOHD
- Paradox MG5000
- Paradox MG5050
- Paradox SP1738

- Paradox SP4000/6000
- Paradox SP5500
- Paradox SP7000
- Siemens SPC5320
- Texecom Premier 412/832
- Texecom Premier Elite 12-W
- Texecom Premier Elite 24
- Texecom Premier Elite 64-W
- Visonic PowerMaster 30

To wire the panel

1. To power the LX30B-AUC, connect the LX30B-AUC terminals **+12V** and **GND** to panel terminals **AUX+** and **AUX-** (or equivalent panel terminals).
2. To allow communication, connect the LX30B-AUC terminals **T1** and **R1** to panel terminals **Ring** and **Tip** (or equivalent panel terminals).

   Note: The control panel POTs terminals only need to have the AUC wires (T1 and R1) connected. No other wires or devices should be connected to the control panel dialer terminals when using an AUC.
3. To remotely track the panel arming status, connect the LX30B-AUC terminal **IO1** to panel terminal **PGM1** (or equivalent panel terminal).
4. To remotely change the panel arming status, connect LX30B-AUC terminal **IO2** to panel terminal **Z1** (or equivalent panel terminal).
5. Connect the antenna to the LX30B-AUC, screw it into the antenna coax terminal.
6. Install the AUC inside the panel enclosure, routing the cables and 4G/LTE antenna outside the enclosure. Then replace the panel enclosure cover.



Note: The antenna's coax connection with the module is different from the snap MMCX connection of other Alarm.com modules.

Recommendations

- The maximum distance from the LX30B-AUC to the control panel is 10 feet (or about 3 meters).
- Use wire gauge 14-22 AWG. No version of CAT5/CAT6 cable is sufficient.
- The connectors configured as Outputs are OC type. Do not connect the output directly to a positive voltage relative to the ground. Do not apply a voltage higher than 12V. The maximum current that can be controlled should not be greater than 100mA.
- Do not connect power to the Universal Communicator until the antenna is connected, as this could damage the radio module.

Confirm communication with Alarm.com

1. Power on the panel.
    - Connect the backup battery and restore AC power to the control panel. Wait 10 minutes before using the keypad or sending commands to allow the AUC to initialize.
2. Verify LEDs:
    - Verify the *OK* LED (green) flashes at least two times to indicate two bars of signal strength.
    - Verify the *DTMF* LED (yellow) flashes when sending data to the AUC. The Status LED (blue) will flash as confirmation of the handshake.
    - For more information about the LEDs, see Alarm.com Universal Communicator (AUC) - Module LED Guide.

3. Test alarm signals to confirm successful communication with Alarm.com and the monitoring station.

If there is no communication:

If the panel does not automatically signal, verify the following is configured locally in programming. Consult the security panel manufacturer documentation and support for assistance with local use, navigation, and programming of the panel.

1. Enable the panel telephone line (PTSN dialer) (depending on the panel).
2. Select DTMF mode for tone dialing (depending on the panel).
3. Verify the selected communication protocol (CID or SIA) on the panel, for the AUC, and for the monitoring station all match.
4. Verify a monitoring account number is programmed locally.
5. Verify a monitoring phone number is programmed locally. Enter up to 16 digits.
    - If on firmware version below 2.25.4, verify the monitoring station phone number programmed locally and the AUC Communicator Phone Number on the Partner Portal or MobileTech app match.

Some panels have panel-specific setup guides available. For panel-specific setup guides, see Alarm.com Universal Communicator (AUC) - Panel Setup Guides.

Expand all

For additional information about the settings, click to expand the following sections:

Set monitoring station account number^

Locally at the keypad, program the account number on the panel per manufacturer instructions. Any number can be locally programmed.

An account number must be programmed locally to ensure the panel sends signals, since most panels will not send signals if the account number field is empty. Any number can be entered into local programming since signals are sent to the monitoring station using the account number designated on the customer account's monitoring settings on the Partner Portal or MobileTech app.

Set monitoring station phone number^

The phone number programmed depends on the AUC firmware version being used, which can be checked on the packaging:

- On firmware version 2.25.4+:
    - The monitoring station phone number must be locally programmed with any value for signals to reach the monitoring station. The AUC phone number is set to "ANY" by default.

- Below firmware version 2.25.4:
  - The monitoring station phone number programmed at the panel and AUC must match for signals to reach the monitoring station.
  - A field for *Communicator Phone Number* is required during account creation. If the phone number programmed locally is known, enter the number here. Otherwise, *555555* is the default for the AUC.

Important: It is possible to change the phone number the Alarm.com Universal Communicator (AUC) expects the panel to use by updating the *Communicator Phone Number* using the *Command Catalog* on the Partner Portal or MobileTech app.

The monitoring station phone number is the phone number the panel dials when transmitting signals over a phone line. If the *Communicator Phone Number* is not set to "ANY" (available on firmware version 2.25.4+), then the phone number programmed locally must match the phone number the AUC expects the panel to use.

Set monitoring station signaling protocol

The communication protocol programmed at the panel, AUC, and used by the central monitoring station receiver must all match for successful signals to the monitoring station.

Verify which protocols the panel can use with the AUC. If the panel can use both CID and SIA, CID is recommended because that is what the Alarm.com Universal Communicator expects by default. For more information about supported protocols for each panel, see Which control panels are compatible with Alarm.com Universal Communicators?.

Important: If SIA must be used, it is possible to change the signaling protocol the Universal Communicator expects the panel to use by updating the *Reporting Protocol* using the *Command Catalog* on the Partner Portal or MobileTech app.

The signaling protocol dictates the format of signals sent to the central monitoring station (i.e. CID or SIA).

Set additional programming options

Depending on the brand of the control panel, there may be additional settings to configure to ensure the panel send signals to the AUC. Some examples include the following:

- Enable alarm reporting
- Enable panic reporting
- Enable arming/disarming reporting

Set up remote arming

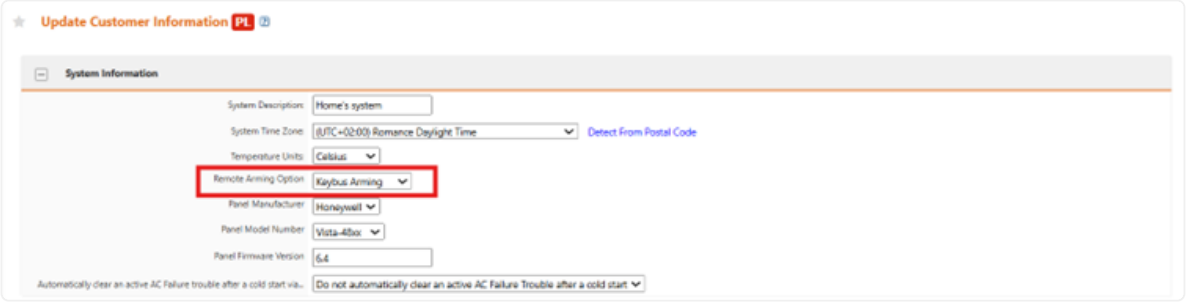
If the panel supports Smart Connector, it is recommended to set up remote arming using the Smart Connector configuration.

The keyswitch and PGM can also be programmed to set up remote arming using the AUC.

To set up Smart Connector:

This feature is only compatible with select Honeywell Vista, DSC, and Paradox panels. For more information about Smart Connector, see Alarm.com Universal Communicator (AUC) - Smart Connector User Guide.

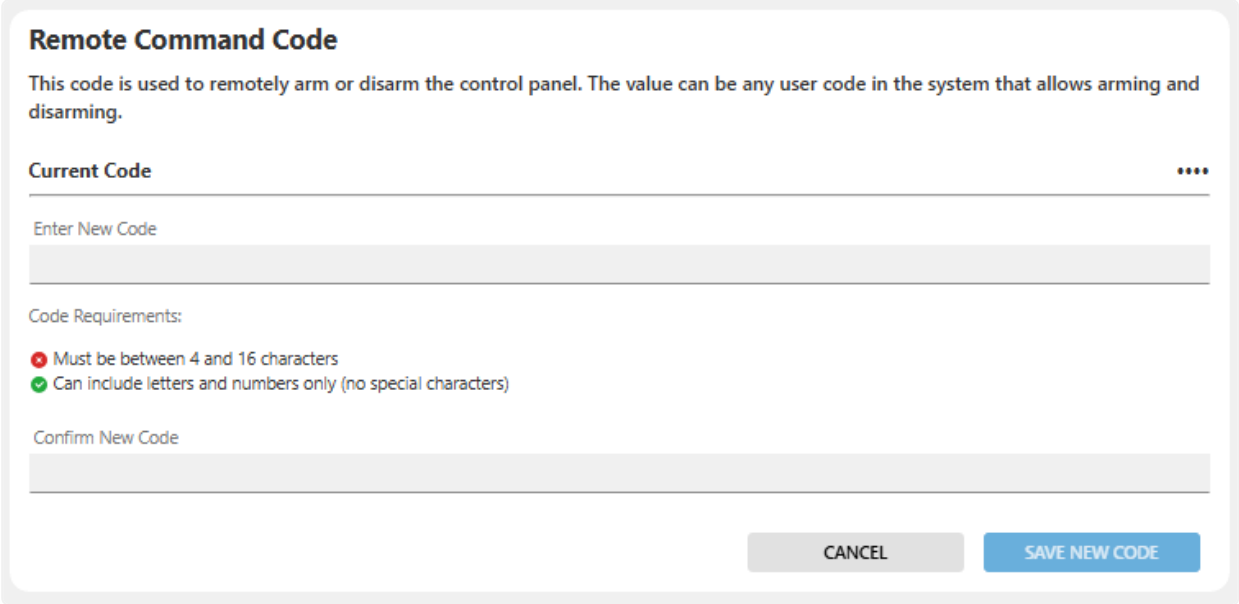
1. Verify that the account has an LX30B communicator with firmware version 2.22.3+.
2. For Honeywell Vista panels, the following must be programmed:
   a. Using the keypad, enter [installer code] **[800]** to enter programming mode.
   b. Then program keypad address 23 for partition 1. To do this, enter **[*] [196]** and then **[1] [0]**.
   c. If using 2 partitions (optional), program keypad address 22 for partition 2. To do so, enter **[*] [195]** and then **[2] [0]**.
   d. If using 3 partitions (optional), program keypad address 21 for partition 3. Enter **[*] [194]** and then **[3] [0]**.
   e. Disable Auto-Stay Arm by entering **[*] [8] [4]** and then **[0]**.
   f. Enable Contact ID event sending by Long Range Radio (LRR) by entering **[*] [29]** and then **[1]**.
   g. After the programming is complete, exit programming mode by entering **[*] [99]**.
3. For DSC and Paradox panels, no additional panel programming is required for Smart Connector to function properly.
4. Select the correct Remote Arming Option on the Partner Portal:
   - If creating a new account, in the *System Info* section under the *Remote Arming Option*, select **Keybus Arming**.
   - If modifying an existing account:^
     a. Find the customer account on the Partner Portal.
     b. In *Customer Information*, click **Edit**.
     c. In *System Information*, use the *Remote Arming Option* dropdown menu to select **Keybus Arming**.
        - If unable to see this option, verify the LX30B version is 2.22.3+.



5. Enter the remote command code using the Customer website or Customer app. This is the code that will be used to properly implement all arming commands for the account.

   Note: Only the primary login or logins with master control are able to edit the *Remote Command Code*.

   - To set the remote command code using the Customer website:^
     a. Log in to the Customer website using the primary login or a login with master control.
     b. Click **Settings**.
     c. Click **Control Panel Settings**.
     d. In *Remote Command Code*, enter a system user code that allows for arming and disarming.



     e. In *Confirm New Code*, enter the user code again.
     f. Click **Save New Code**.

   - To set the remote command code using the Customer app:^
     a. Log in to the Customer app using the primary login or a login with master control.
     b. Tap **Security System**.
     c. Tap ⚙.
     d. Tap **Smart Connector Settings.**
     e. In *Remote Command Code*, enter a system user code that allows for arming and disarming.
     f. In *Confirm New Code*, enter the user code again.
     g. Tap **Save New Code**.
6. Have the customer arm or disarm the system. Once the system is first armed or disarmed, the correct number of

partitions will populate in the Customer app, Customer website, Partner Portal, and MobileTech app.

To set up PGM and Keyswitch programming:

1. A PGM can be programmed to report the panel arming status to Alarm.com. Program an output (PGM) on the panel per manufacturer instructions with the following settings:
   - Definition: System arming status
   - Activation Type: Latched mode
2. A keyswitch zone can be programmed to change the panel arming status remotely using Alarm.com. Momentary (recommended) or state/latched keyswitch arming may be available for configuration. To verify compatibility, see Which control panels are compatible with Alarm.com Universal Communicators?.

   Important: For remote arming, our configuration is meant to arm the panel away.

   - To set up momentary keyswitch arming (recommended): ^
     a. Program a keyswitch zone on the panel per manufacturer instructions with the following settings:
        - Definition: Keyswitch
        - Activation Type: Timed mode (also called instant, impulse, or momentary mode)
        - Activation Length: 3 seconds
     b. Verify momentary keyswitch arming is set up on the Partner Portal or MobileTech app:
        a. Log in to the Partner Portal or MobileTech app.
        b. Find the customer account.
        c. Click **Command Catalog**.
        d. In *Arming Settings*, click **Configure Keyswitch Arming**.
        e. Using the *Output mode* dropdown, select **Impulse (Momentary)**.
        f. Using the *Output reaction time* dropdown, select **3 seconds**.
        g. Click **Apply Settings**. Allow a few minutes for the settings to save on the panel.

   - To set up state (latched) keyswitch arming: ^
     a. Program a keyswitch zone on the panel per manufacturer instructions with the following settings:
        - Definition: Keyswitch
        - Activation Type: Latched mode (also called state mode)
     b. Verify state (latched) keyswitch arming is set up on the Partner Portal or MobileTech app:
        a. Log in to the Partner Portal or MobileTech app.
        b. Find the customer account.
        c. Click **Command Catalog**.
        d. In *Arming Settings*, click **Configure Keyswitch Arming**.
        e. Using the *Output mode* dropdown, select **State (Latched)**.
        f. Click **Apply Settings**. Allow a few minutes for the settings to save on the panel.
3. Once programming is set up, arm and disarm the panel locally using the keypad to update and initialize the panel

status on Alarm.com.

4. Verify remote arming and status updates function properly using the Customer website or Customer app.

Troubleshooting

If the LX30B-AUC is not communicating, see Alarm.com Universal Communicator (AUC) - Troubleshooting Guide.

Regulatory information for LX30B-QxxT

FCC

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 received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference in radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to the 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:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user ‘s authority to operate the equipment.

Contains FCC ID: XMR2023EG915QNA

IC / ISED Notice

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

Cet appareil numérique de classe B est conforme à la norme canadienne ICES-003.

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient des émetteurs/récepteurs sans licence qui sont conformes aux RSS sans licence d'Innovation, Sciences et Développement économique Canada. L'exploitation est soumise aux deux conditions suivantes :

1. Cet appareil ne doit pas provoquer d'interférences.
2. Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable de l'appareil.

Contains IC: 10224A-023EG915QNA

RF Exposure

This equipment complies with FCC and ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated at a minimum distance of 20cm between the equipment and your body. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. Please contact intsupport@alarm.com for more information on Canadian RF exposure compliance.

Cet appareil est conforme aux limites d'exposition aux radiofréquences établies par la FCC et l'ISED pour un environnement non contrôlé. Cet appareil doit être installé et utilisé à une distance minimale de 20 centimètres entre l'appareil et votre corps. Cet appareil et son ou ses antennes ne doivent pas être situés ou fonctionner en conjonction avec une autre antenne ou un autre émetteur. Veuillez communiquer avec intsupport@alarm.com pour obtenir plus d'information sur la conformité aux exigences canadiennes en matière d'exposition aux radiofréquences

Mexico CRT

IFT #: RDEBLX25-15808
La operación de este equipo está sujeta a las siguientes dos condiciones: (1) es posible que este equipo o dispositivo no cause interferencia perjudicial y (2) este equipo o dispositivo debe aceptar cualquier interferencia, incluyendo la que pueda causar su operación no deseada.

BS EN Grade Certification

This module are certified to EN 50130-4, EN 50130-5, EN 50131-1, EN 50131-10, EN 50136-1, and EN 50136-2.

It has passed tests to be classified as EN Security Grade III, Environmental Class II, and meets rigorous Alarm Transmission System requirements of up to classes SP5.

Contact Us

Alarm.com Incorporated

8281 Greensboro Drive, Suite 100
Tysons, Virginia, 22102

USA
Get in Touch (https://www.alarm.com/contact)